Report from

"Smart Networks and Services Partnership Stakeholder Workshop"

July 4th, 2019

Version: 0.2

Editor:
Rui L. Aguiar, Instituto de Telecomunicações and Universidade de Aveiro

Rapporteurs:
Daniel Corujo, Instituto de Telecomunicações and Universidade de Aveiro

Jyrki Huusko, VTT Technical Research Centre of Finland

Marco Ruffini, Trinit College Dublin

Executive Summary

The next Research and Innovation programme proposed by the Commission beyond 2020, Horizon Europe, has now entered into its preparatory phase. In that context, the area of Smart Networks and Services has been identified by the Commission as a potential research area for a partnership implementation. The current ideas for such a partnership focus on the future connectivity and service infrastructure supporting the digital society and the digital transformation of our economic sectors. A value chain approach could reinforce and leverage European strongholds in connectivity and create opportunities in multiple related domains, notably the device domain, taking into account the myriad of innovative IoT devices that will be connected, and the cloud computing domain enabling big data and AI based applications. In this regard, there are also new opportunities offered by edge computing and the emerging requirement to provide services close to the user. In addition, cybersecurity emerges as a very important research issue in the context of European strategic autonomy, cutting across the various building blocks of such a device-network-service infrastructure, with blurring boundaries between these constituting elements. In terms of operational implementation, it is envisaged that this partnership will build on the successful structures of the 5G PPP with an extended scope and strategic reinforcement.

The workshop exchanged some technical ideas on challenges associated to the development of these new areas into the future Smart Networks and Services.

Contents

1 Workshop objectives and overview

This document reports of the conclusions obtained from the “Smart Networks and Services Partnership Stakeholder Workshop”, a top-level scientific event that took place in Brussels, Belgium, on the 4th of July, 2019. The workshop was organized by Networld2020 European Technology Platform.

The objective of this Workshop was to present, discuss and conclude on what will be the main content and points of discussion for the high-level research public funding structure for the coming years. To achieve this objective, the Networld 2020 ETP defined for this workshop a set of key sessions composed by panels of top world experts from industry and academia. These panels were arranged focusing on three key challenges for Next Generation Systems, namely the Internet of Things, Cloud Computing and Cybersecurity.

Each panel was chaired by an expert on the area, where each invitee provided a vision for the key elements to be considered in upcoming research. At the end of these presentations, the floor was opened for debate involving the participants as well.

The summary and conclusions from this Workshop are captured in this document.

The planned programme was:

8:30-9:00	**Registration**
9:00 – 9:15	**Welcome and EC Introduction** *Peter Stuckmann (EC), Rui Aguiar(Networld2020)*
9:15-9:30	**Networld 2020/Smart Networks Task Force Introductory statements** *Werner Mohr (Nokia, Networld2020)*
9:45 – 12:00	**Next-generation IoT** *Chair: Maziar Nekovee (Sussex University)* *Hakon Lonsethagen (Telenor), Joseph Eichinger (Huawei), Nicola Ciulli (Nextworks), Ovidiu Vermesan (Sintef)*
12:00- 13:00	**Lunch** (networking lunch on site)
13:00 – 15:00	**Next-generation Cloud Computing** *Chair: Rui Aguiar (Instituto de Telecomunicações)* *Aurora Ramos (Atos). Benny Koren (Mellanox), Josef Urban (Nokia)*
15:00- 15:15	**Coffee**
15:15 – 17:15	**Cybersecurity for smart networks and services** *Chair: Werner Mohr (Nokia)* *Emmanuel Dotaro (Thales), Fabio Martinelli (CNR), Ghassan Karame (NEC), Luis Barriga (Ericsson)*
17:15-17:30	**Wrap up, way forward** *Bernard Barani (EC), Rui Aguiar (Instituto de Telecomunicações, Networld2020))*

2 Presentation on EC Framework and partnership approach

Presenters:

- Rui Aguiar (Instituto de Telecomunicações and Universidade de Aveiro)
- Peter Stuckman (EC)

This session introduced the EU Programmes and Horizon Europe Pillars, highlighting partnership proposals sent. The commission considers that the EU is still strong in the mobile and last mile, but would be important to see an increase for devices and the cloud, in order to boost business.

Therefore, a partnership encompassing these aspects would be appreciated, despite that there is still the need to better determine which type of partnership should be pursued.

3 Presentation on Networld2020 and Smart Networks Task Force

Presenters:

- Werner Mohr (Nokia)

Smart Networks and Services perceives a joint vision of digitalization, AI and ubiquitous computing. The concept is aimed at supporting the grand challenges (e.g., climate, environmental resource management, aging, urbanization), and how to enable human-centric digitalization. A myriad of opportunities exists, with the necessary technology solution needing smart network and services. Its main building blocks are composed of communication, software, AI and cybersecurity, all considered in this workshop and presented next.

4 Panel Session “Next-generation IoT”

Panel Participants:

- Panel Chair: Maziar Nekovee (Sussex University)
- Hakon Lonsethagen (Telenor)
- Artur Hecker (Huawei)
- Nicola Ciulli (Nextworks)
- Ovidiu Vermesan (SINTEF)

Operators stand at the center of service distribution for telecommunications provisioning, where not only huge opportunities reside, but also a challenge for continuous transformation. The recent, and continuously increasing massification of connected devices creates a complex standpoint for that service provisioning, in the sense that the telco vision of “connecting users to what matters the most” is being subject to uncertainties associated to the continuous evolution of devices, radio access networks, security mechanisms, management and operational capabilities. It is important to perceive telcos as continuously being effective delivering services, and not a bottleneck. Moreover, the flexibility and dynamic mechanisms provided by 5G which have attracted a number of verticals to such networks, has also exposed telecommunications to a whole set of new procedures to other multi-stakeholder industries, associated with business processes, standardization, technical evolution and even societal and human factors. For example, these different processes can have widely distinct cycle and update times. It is thus important to consider that the flexibility of current and upcoming networks needs to follow the inherent differences of such processes existing in other areas.

Such capabilities turn the 5G network as the definite ice-breaker for IoT, by inviting vertical engagement. Concretely, 5G allowed for actual latencies and reliabilities for critical services to be deployable over the same infrastructure where consumer communications reside. However, IoT will continuously play an even greater role in Beyond 5G, either because different deployment scenarios might not fall within the three main 5G use case scenarios (i.e., eMBB, mMTC and ULLRC), or simple because some of them might be even achievable using 4G technologies. Beyond this, IoT is moving into the field of integrated intelligence whose added data extraction and association monetization capabilities explode the number of potential new use cases, requiring solutions at distributed points of the network, composing deployments acting as micro or even nano datacenters, or even the objects themselves.

This also opens up the ground for a more profound integration the communications and the IoT (e.g., the devices) domains, considering the plethora of aspects raising for such integration. These aspects range from going beyond the Internet as the generic concept for the “network” in a IoT vision (i.e., considering underlying connectivity deployments akin to quantum networks, nano-nets, molecular networks, amongst others), to the babel of protocols, platforms and ad-hoc solutions that currently exist in both networking and IoT. Under the umbrella of a great need for simplification, several proposals can be made to steer research towards finding solutions. Concretely, shifting the focus towards the use cases themselves instead of the verticals will ensure greater impact towards the state of the art, without the need of reinventing the wheel or developing redundant solutions. Additionally, solution providers should steer away from producing a one-size-fits-all solutions, focusing instead on heterogeneity and dedicated platforms, emphasizing collaboration between both networks and IoT: aspects such as duplication of R&D efforts, developing a portfolio of common approaches and avoiding the need to craft solutions at each new purpose or platform, would be greatly benefited.

Finally, the distributed deployment aspect would also benefit security-based principles, using distributed ledger and edge solutions for IoT, where processes such as device authentication, smart contracts for devices, micro payments and traceable data usage or integrity could be moved. This would allow such services to be supported under a shift of computing action from the core to the edge, raising the notion of “computation anywhere” (e.g., an aspect that can be applied to the AI/ML capabilities previously mentioned).

Challenge areas (some more closer to Network, others closer to IoT):

- Network and communication systems: integration of IoT and network services, AI/ML-enabled network and services for IoT, configuration/orchestration/Open device management, spectrum efficiency and pricing
- Edge cloud and fog: convergence of protocols and SDN/NFV, evolution of fog and edge computing and processing, support for swarm computing;
- Privacy, network & service security: network and IoT security in highly virtualized networks, network & IoT security and reliability for mission critical infrastructure, services, AI/ML and services support of network & IoT security, IoT and distributed ledger technologies (DLTs)

5 Panel Session “Next-generation Cloud Computing”

Panel Participants:

- Panel Chair: Rui Aguiar (Instituto de Telecomunicações and Universidade de Aveiro)

- Aurora Ramos (ATOS)
- Benny Koren (Mellanox)
- Josef Urban (Nokia)

Despite the capabilities introduced by 5G networks, as well as supportive technologies, such as Software Defined Networking, Network Function Virtualization, Service Function Chaining, amongst others, there are still many gaps and research challenges. In fact, full automation aspects by means virtualization aspects themselves might be even fully unleashed only in Beyond-5G deployments due to the way telecommunications networks are still being designed. This Beyond 5G capability from cloud computing can have a profound impact on allowing connectivity dynamically adapting itself to changing requirements, employing next generation cloud computing principles and mechanisms, as well as new security aspects. It is still observable that the majority of cloud service providers have not yet started SDN deployment, with only proof of concepts or trials being done. In this way, research challenges encompass the need to pursue a true unification of the network and cloud resource management, assisting it with cloud-native NFV orchestration (which can be perceived as still being missing as VNF’s are broken into micro-services and cloud network functions), while being supported by intelligent network management through the application of AI to NFV and SDN management, as well as providing actual solutions for multi-access edge computing. Particularly on this last case, the challenge still resides for proper device management, edge workload management, data abstractions in cloud and edge computing (as there is no good abstraction methods supporting both cloud and edge). This is further complemented with the need for increasing the dynamicity of the cloud ecosystem, with services being transparently deployed into the edge, independently of belonging to IoT scenarios or as resulting from the optimization of NFV constructs.

The reliance on cloud computing also raises new possibilities on how we perceive server processing. Today, virtualization and computing are done in single host CPU’s, running applications and infrastructure components in server CPUs (commonly based in x86 architectures). This has led to both application and infrastructure tier segregation. The possibilities envisioned by cloud-based network deployments, concerning the distribution of infrastructure components. As an example, security procedures can be distributed into Smart Network Interface Cards, instead of being centralized on the server’s CPU. In fact, security is one of the big challenges in data centers However, for cloud computing, the traditional perimeter-based security model is broken, and there is need for privacy and adopting cryptography to protect the data, along with the support of new security regulations requirements (GDPR). An innovative security approach at the datacenter can be the application of the “zero” principle, with zero utilization (provision of transparent encryption acceleration by offloading security from the CPU into other processing entities), zero trust (by allowing to rent real CPU’s into your customers, letting them install whatever they want, while providing security controls built around applications), and zero trust (where security is automated and adaptive, without human intervention). Another challenge related with security in cloud computing is storage security, with the need of new cryptography solutions for protecting the storage. Finally, the ultimate outtake for de-centralized processing would be to have data being analyzed as it moves, allowing for greater performance and scalability, through the realization of distributed collection operations.

One of the main constructs for cloud computing is software and its ability to be almost everywhere. Software is bringing several new key enablers into cloud computing such as AI, hyper-scalability, ubiquitous connectivity and human centricity. Nonetheless, software itself still brings some research challenges associated, such as enabling cognitive adaptability,

guaranteeing dependability, advanced human interaction, overcoming complexity, and building digital trust. The complexity aspect is key in this discussion, in the sense that it impacts several KPIs associated to network deployments based on cloud computing. Concretely, latency, through the use of edge computing, is one of those aspects. Edge could benefit from the existence of accelerator solutions, such as the Smart Network Interface Cards, but also other principles such as energy-aware programming and services, and AI/ML-enabled programmable and adaptable function placement. Nonetheless, such heterogeneous deployment environment requires greater interoperability measures. For example, in order for a system to become more adaptable, deep learning mechanisms for smart networks are needed, as well as changing procedures such as “re-engineering software engineering” to enable cognitive adaptability. Again, security as a core issue here is well. As more and more software is deployed, the more dramatic becomes the increase in the number of existing software vulnerabilities. With the reliance on AI/ML and automation, we can apply into software principles of “trusted computing as a service”, with automated compliance assurance.

Challenge areas:

- There is the need to integrate cloud computing with enhanced AI-based virtual network architectures, as well as integrated and unified management of network and cloud resources
- New business models that bring closed both telco and cloud stakeholders
- Data labelling for application of Big Data management
- Moving from a CPU-centric computing model to a data-centric in-network computing model. This requires a more intelligent and faster connectivity.
- Added value (particularly from Europe) when software is proprietary (considering that even though hardware typically comes from outside of Europe, it is software development that provides the greatest challenge as “Silicon is nothing without software”
- Software certification is needed, in the sense that standards need to be unified (particularly if we considering integration between the telco and computing realms). However, it is difficult. For example, there is no standard to certify AI/ML software models. A potential answer could be in certifying development models rather than software itself.

6 Panel Session “Cybersecurity for smart networks and services”

Panel Participants:

- Panel Chair: Werner Mohr (Nokia)
- Emmanuel Dottaro (Thales)
- Fabio Martinelli (CNR)
- Ghassan Karame (NEC Laboratories Europe)
- Luis Barriga (Ericsson)

Cybersecurity expresses an holistic concern that was identified in the other two panels as well. As such, new initiatives and procedures are required, in order to provide secure environments not only to the end users, but to the deployment of new operational mechanisms and features in novel technical and technological solutions. Service robustness has been being critically impacted by attacks, generating billions in losses. Blockchain, and distributed ledger technologies for that matter, have been heralded as key identity and access solution providers,

by creating a consensus layer between actors. However, the blockchain technology by itself provides only one layer of what can be perceived as a full solution stack, with that layer itself requiring protection as well (e.g., the hash-gossip protocol features a 20 min timeout which can be exploited, and also imposes limited throughput, requires proper decentralization and has privacy issues as well. It does provide some very interesting applications, such as ICANN decentralization, marketplaces (e.g., for leasing equipment) and achieving policy consensus, but the determination of appropriate applications of blockchain is necessary.

The cheer scalability of technological deployment environments such as the IoT, particularly when considering massive IoT and Critical IoT, is a key driver for security architecture redesign. 5G security research taught us that secure systems need to be use-case driven, and there are further complexities raising from the changing threat landscape, new technologies surfacing and new regulations. Many vectors are needed, and not necessarily only need to consider attacks by external entities: users themselves can, for example, undergo illegal roaming, or might want to rely on third party operators which can compromise a small number of IoT devices, but might be able to bring down an entire base station or gateway and affect several other services. Moreover, the heterogeneity of features is also implied, with authentication procedures needed to become more uniform (e.g., mobile network related solutions still mandate the need for SIM authentication). This is further exacerbated by the fact that you can’t actually control the end device, and only the access side of the network. But the issue is not only related with hardware (e.g., low cost of devices) or firmware (e.g., the lightweight need of devices often opts for low-grade security mechanisms): the growing trend of Continuous Integration / Continuous Delivery should also be integrated with a software certification process, considering as well that virtualization has the ability to change the perception of the underlying hardware over which the software is running. Software creates a much more dynamic environment, which reduces the effectiveness of legacy perimetric security. In the end, involved processes currently rely on humans, and thus automation is required. Here, AI/ML could be helpful, but there is a large uncertainty on how AI models can be shared and certified. Moreover, AI can be harmful in the sense that it can be used by the attacker to dynamically develop new attack models. There are also some aspects related with policies which could provide greater prevention to attacks in general, namely for a platform allowing the publication of identified patterns of attack and their signature.

One important aspect is how to reflect the 5G-aimed provision of an end-to-end service, when considering as well end-to-end security. This provides several existing, but also novel, opportunities and challenges, composing interactions involving autonomous systems, mass transportation, constant monitoring of daily aspects of citizens, self-sustainable mobile devices, fake news, quantum computers, cryptocurrencies, digital twins, AI capabilities, just to name a few. This creates a truly complex and heterogeneous system at several levels, with different perceptions. Such perceptions, besides widely varying, have different scopes concerning for example, the different involved vertical sectors, or even national strategies.

Indeed, these different perspectives hinder the adoption of potential useful, but specific, solutions, which might make sense in one aspect, but might not be applicable in end-to-end systems. In this sense, security provisioning is also tightly coupled with business models, particularly the ones involving mission critical availability. By having 5G now involving different verticals and actors beyond the telco world, there is a need for co-design, co-development, co-deployment, in all stages of the end-product life-cycle.

Challenge areas:

- There is an increase in complexity that will increase security threats as well.
- It is important to assess that security is traversal and needs to be implemented at all levels, Security-by design of IoT devices needs to be checked, and available to stakeholders, who need to understand hot to use it and how to interpret its results.
- How to allow security checks to be done in large systems.
- There is the need for EC support on how to deal with policy issues.
- Several SDO’s exist, with specific focus in regards to security. Despite that it is not their task to solve all transversal security issues individually, this might be solvable in a collective way, or at least to create measures ways to mitigate attacks.
- Moreover, the security models vary widely by geography, which raise the need for harmonization in regulation, which can also go beyond the technological point of view.
- How to deploy a certification procedure in IoT, in a realizable, and cost-effective way?
- Other regulations, such as GDPR, are currently hard to check for compliance.
- Security and networks need to work together, possibly also including the verticals, with the PPP being a tool to allow that.

7 Wrap up and way forward

Speakers:

- Rui Aguiar (Instituto de Telecomunicações and Universidade de Aveiro)
- Bernard Barani (EC CNECT E1)

Networks are becoming more and more complex, with many technologies crossing between one another, having their borders increasingly disappearing. It is important for this working group to organize itself so that its members can work together towards a common goal on the subject of the Future Network.

The key aspects discussed are summarized in the following:

- One of the main aspects that was raised in the panels throughout the Workshop was that there needs to be a distinction between what a network is, which are the borders, and what a device is. It will potentially affect how people do business from now on, considering the technological onset.
- With different actors involved, there are different ways that challenges, opportunities and requirements are being looked upon, analyzed and met. Individual perceptions can produce undesirable on non-understandable outcomes by some actors, ranging from (e.g.) the robotics sector not perceiving the need for Cybersecurity (due to cloud-based smart manufacturing) or even security solution providers avoiding IoT-based deployments, claiming that they are not fully securable.
- Software becomes a key driver, which raises unprecedented new concerns, due to the associated dynamics. It is thus important to improve its quality and certification process possibilities.
- Still considering software, new possibilities arise on how quality and security could be decoupled according to the more traditional development side.
- New solutions, besides providing new approaches, can come at the cost of potentially providing new dangers, particularly considering cybersecurity
- Security is something that is not only critical, but in scope of 5G and beyond, still needs to be handled

In this sense, it is verifiable that the value chain where 5G-based solutions are being deployed, is very vast. Therefore, ICT actors should be open to create new opportunities in line with that value chain.

Regarding the scope of the Networld2020 partnership, there a need to strike a balance between broad scope and extension, and focus. It is important to remain competitive, with the current 5G race, and therefore the focus is a justifiable measure. It is important as well to acknowledge what has been being done in European research, not only within the partnership but also outside, and grow from them.

8 Workshop Speakers

The Workshop distinguished speakers in the different panel sessions were:

- Peter Stuckmann (EC CNECT E1)
- Rui Aguiar (U. Aveiro and Instituto Telecomunicações)
- Werner Mohr (Nokia)
- Hakon Lonsethagen (Telenor)
- Artur Hecker (Huawei)
- Nicola Ciulli (Nextworks)
- Ovidiu Vermesan (SINTEF)
- Aurora Ramos (ATOS)
- Benny Koren (Mellanox)
- Josef Urban (Nokia)
- Lutz Schubert (Ulm University)
- Emmanuel Dottaro (Thales)
- Fabio Martinelli (CNR)
- Ghassan Karame (NEC Laboratories Europe)
- Luis Barriga (Ericsson)
- Bernard Barani (EC CNECT E1)