A Programmable and Virtualized Network & IT Infrastructure for the Internet of Things

How Can NFV & SDN Help For Facing The Upcoming Challenges

Nathalie Omnes, Marc Bouillon, Gael Fromentoux, Olivier Le Grand
Orange Labs IMT/OLN/CNC/NCA
22300 Lannion, France
Nathalie.omnes@orange.com

Abstract—**The Internet of Things (IoT) revolution has major impacts on the network & Information Technology (IT) infrastructure. As IT in the past decade, network virtualization is simultaneously on its way with for instance Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). NFV and SDN are approaches enhancing the infrastructure agility thus facilitating the design, delivery and operation of network services in a dynamic and scalable manner. IoT will push the infrastructure to its limit with numerous and diverse requirements to fulfill, we therefore believe that the agility brought by the combination of NFV and SDN is essential to face the IoT revolution.**

In this article, we first highlight some IoT challenges that the network & IT infrastructure will face. The NFV and SDN benefits are presented from a network operator point of view. Following a description of the IoT ecosystem and a recall of some of the IoT stakeholders expectations, a new multi-layered IoT architecture involving SDN and NFV and based upon network & IT resources is put forward. Finally, the article illustrates how the proposed architecture is able to cope with the identified IoT challenges.

Keywords—IoT, SDN, NFV, infrastructure services

I. Introduction

In line with the successful evolution of IT infrastructures to virtualization in the past decade, **the next generation network infrastructure will be virtualized and will natively integrate IT resources**. In this article, we refer to this convergent infrastructure as the **network & IT infrastructure**. Yet, a new framework needs to be drawn. It must fulfill the network requirements in terms of performance, availability, context management and hardware selection. The ETSI is currently defining a new standard, Network Functions Virtualization (**NFV**), on which the next generation network infrastructure could be based. As stated in [1], it will further benefit from the advantages of IT virtualization: agility enhancement, exploitation and maintenance automation. Let us define an **infrastructure service** as a service relying on network & IT resources, by extension of well-known network services. **Dynamic and flexible infrastructure services** are thus coming up.

Software-Defined Networking (**SDN**) aims at programming network functions, including control layer functions, by using software technology and thanks to novel interfaces. In particular, SDN allows interconnecting virtual IT resources with virtual or physical network resources. The induced benefits are important: no more human intervention is needed for interconnection. While NFV alone allows deploying infrastructure services on open hardware, SDN further provides a tool for dynamic resources control.

The network operators are able to create catalogs of infrastructure services and related policies, like QoS parameters and bandwidth, with the help of forwarding graphs. This ability, essential for the next generation virtualized network & IT infrastructure, requires the combination of NFV and SDN.

In the Internet of Things (**IoT**) ecosystem, the traffic generated by machines may exceed the one generated by humans. This ecosystem is further organized into different application domains also called verticals [2] such as health, domotics or vehicular. Each vertical has in particular its own data model and authentication method. In this context, building value added infrastructure services is a real challenge. How infrastructure services for IoT could benefit from the combination of NFV and SDN principles is at the heart of our in-depth thinking.

The paper is organized as follows: Firstly, some IoT challenges towards the network & IT infrastructure are presented in section II. The NFV and SDN benefits from a network operator point of view are presented in section III, while section IV highlights the main actors of the IoT ecosystem.

A new NFV and SDN based network & IT architecture able to overcome the issues raised in section II is then drawn-up in section V. We illustrate this architecture in section VI and highlight the benefits of this architecture before concluding in section VII.

II. IoT challenges the network & IT infrastructure

A. *IoT market, services, and use cases*

Internet of Things (**IoT**) is a promising market, expected to be a major source of growth for the Information and Communications Technology (**ICT**) industry in the future. Actually, starting from a potential of 1.5 billion connected devices in 2014 [3], the number of objects could reach 70

978-1-4799-1866-9/15/$31.00 ©2015 IEEE

billion by 2020. Finding precise definitions for IoT, Machine to Machine (**M2M**) and Internet of Objects (**IoO**) is not easy [4]. IoT is a broad term referring to a next-generation Internet that not only connects people's devices, but also enables objects or machines to connect to each other, exchange information, or perform actions without human intervention. Most of these objects will be connected using gateways, probably around 75% of them.

Currently, numerous actors are involved in the IoT ecosystem, including mobile operators, software developers, integrators and alternative access technology providers. Furthermore, IoT involves many different application domains: manufacturing (including production, distribution, and tracking), health (with in-home care, fitness, and well-being), transport, administration, insurance, public safety (with video surveillance), local community, mass-market (with home automation), agriculture... Besides, across the above-mentioned application domains, numerous applications can be associated with IoT: metering, road safety, traffic management, tracking, monitoring… Hundreds of applications have already been identified [4]. Nevertheless, this will only represent a small part of the future applications and uses-cases.

For example, video surveillance, face recognition, robotics, control of complex devices will have a strong impact on the network and IT infrastructure. Another challenge is the need for interaction between actors evolving so far in radically different spheres such as what is found between telecommunication and energy networks in smart grid.

B. IoT requirements against network

Currently, traffic is mainly generated by humans interacting with computers, servers and objects. With M2M, objects will progressively generate more and more traffic. The consequence on the network & IT infrastructure is not yet fully understood.

The amount of traffic generated by each of these objects ranges from a few bytes per month for smart metering to megabytes per second for medical imaging.

Security and privacy are legitimately seen as critical for some applications such as health or industrial processes monitoring, leading to strong constraints in terms of data protection or access control.

Mobility or nomadism may also be required. It can be offered by cellular or alternative networks, such as the "Sigfox" one.

Scalability, QoS and robustness is essential, as IoT will change the order of magnitude of service control, network control and information processing. The challenge will be to ensure Quality of Service (QoS) for IoT, control congestion and avoid side effects on legacy services.

Optimizing the procedures and/or protocols to reduce the device's power consumption is another tight requirement for most devices.

C. Architecture requirements for IoT

Building a single end-to-end infrastructure addressing the complete set of IoT constraints is almost impossible. One reasonable goal, however, may be to share components that will answer to different IoT requirements in a converged layer. Though designed for different services, sharing equipments and functions is possible. Let us now have a look at some founding principles for building up this new infrastructure.

We firstly expect the IoT infrastructure to exceed the legacy one: traditional access networks could be used as a backhaul while new specific flat/mesh access networks, such as unlicensed spectrum based solutions or *ad hoc* networks may appear.

Secondly, because the IoT ecosystem involves many different actors, the frontiers between these actors must be specified. We expect the Internet Service Provider (ISP) to provide value-added functions through enablers together with advanced connectivity.

Thirdly, each IoT application domain currently has a different way to handle information. A set of primitives and network functionalities fitting with the converged layer needs must thus be specified.

Fourthly, initiatives like "oneM2M" [5] specify a generic architecture based on IP as the federative layer.

Finally, the management plane will have to evolve to manage data related to billions of things having various characteristics and behaviours, and connecting through new types of networks. Efficient data and information processing technologies, such as big data, data mining and autonomic management will have to be integrated for the management plane to scale.

D. IoT infrastructure services

The vertical integration of numerous IoT application domains leads to a multitude of silos. Yet, by sharing architecture components, cost-efficient value-added infrastructure services can be offered to corporate customers and wholesale markets. This includes for example naming or Domain Name System (DNS) of "things", messaging and event processing, enhanced routing, data trusted repository, device management including monitoring and fault management, security enforcement services, including access control by authentication, device wake-up, allowing the optimization of mobile radio resource allocation, energy consumption and interworking.

All these infrastructure services rely not only upon network resources but also on new assets introduced by data centres. As we will see in the next section, network & IT virtualization, by providing resources isolation and enhanced flexibility, is particularly relevant in the IoT context.

E. IoT overall impact on architecture

The unpredictable and fluctuating IoT ecosystem will push the network & IT infrastructure to its limit. It is thus crucial for this infrastructure to be agile, scalable, flexible and reliable. The risk is for the network & IT infrastructure to break down because of the IoT data flood. Actually, some use cases will have strong impact over the whole infrastructure.

Firstly, low latency use cases require lowering the transfer delay at the transport level and the processing delay at the IT level. This may mean moving the resources closer to users in regional or local platforms.

Secondly, high network throughput use cases require important network bandwidth. For network optimization and cost issues, it should be profitable in this case to implement servers closer to the devices. These use-cases encompass for instance public safety and video surveillance.

These uses cases will require strong collaboration between all actors involved in the value chain and will require the adaptation of the infrastructure layer

Designing a system able to cope with numerous use cases and infrastructure services is another big challenge. We have to be aware that technical solutions will evolve. The infrastructure will have to be flexible to cope with IoT and Service Level Agreements (SLA) diversity. For instance we have to discriminate SLAs not only by traditional QoS parameters but also by typical IoT features: volume of generated bits on a long period, number of device connections, very low energy consumption and unpredictable activity.

Due to the diversity of IoT actors, possible business models, services and derived requirements, the economic model for infrastructure services for IoT is quite uncertain. Starting from a new and dedicated infrastructure investment would be very hazardous for operators in this context. Hopefully, virtualization allows the isolation of IoT use-cases from other ones by using end to end infrastructure resources' slicing. IoT infrastructure services may then be deployed on the same infrastructure as other infrastructure services including legacy ones. Deploying a single infrastructure will further reduce the operating expenditure (OPEX) and capital expenditures (CAPEX).

Thus a multi-access mediation layer able to control, to manage and to have an end to end view on the resources including device, network and IT needs to be built. A possible implementation of this mediation layer is One M2M [5] common service layer. In any case, programmability and virtualization technologies will help us in that domain.

III. NFV & SDN, A NEW OPPORTUNITY

NFV and SDN are new opportunities for building up a new infrastructure. Let us have a look at these two concepts.

A. NFV, Network Functions Virtualization

Virtualization will soon allow decoupling network functions from network hardware. This will altogether reduce the network cost and enable new use cases, such as the dynamic deployment of infrastructure services.

To achieve this, an architecture framework is currently under standardization by the ETSI Industry Specification Groups (ISG) NFV (see [6], [7]), specifying how infrastructure services shall be deployed on a virtualized infrastructure. Within NFV, infrastructure services are referred to as network services. This architecture framework relies on 3 different hierarchical levels, as depicted in the Figure 1.

NFV inherits from carrier-grade and end-to-end management strict constraints. It thus faces drastic performance, availability and resilience challenges. NFV further handles the network services' lifecycles including on-boarding, instantiating, monitoring and deleting.

The phase 1 NFV documents address the general architecture and components. Protocols, APIs, and data models will be addressed in the second step, solving interoperability issues.

At the lowest level, a Network Functions Virtualization Infrastructure (**NFVI**) is a virtual resource providing computing, storage and network facilities. NFVI resources are controlled and managed by the Virtualized Infrastructure Manager (**VIM**).

In the intermediate level, a Virtual Network Functions (VNF) is a network application running on top of one or several NFVI resources. Furthermore, the VNF Manager (VNFM) is responsible for controlling and managing VNF resources, while the Element Management System (EMS) performs the typical management functionality for one or several VNFs.

Finally, at the upper level, the NFV Orchestrator (**NFVO**) controls and manages infrastructure services. The NFVO coordinates the resource allocation to infrastructure services and VNFs, either by a direct interaction with the VIM or via the VNF Manager. The NFVO takes into account deployment policies based on various criteria including affinity rules, location constraints and performance criteria.

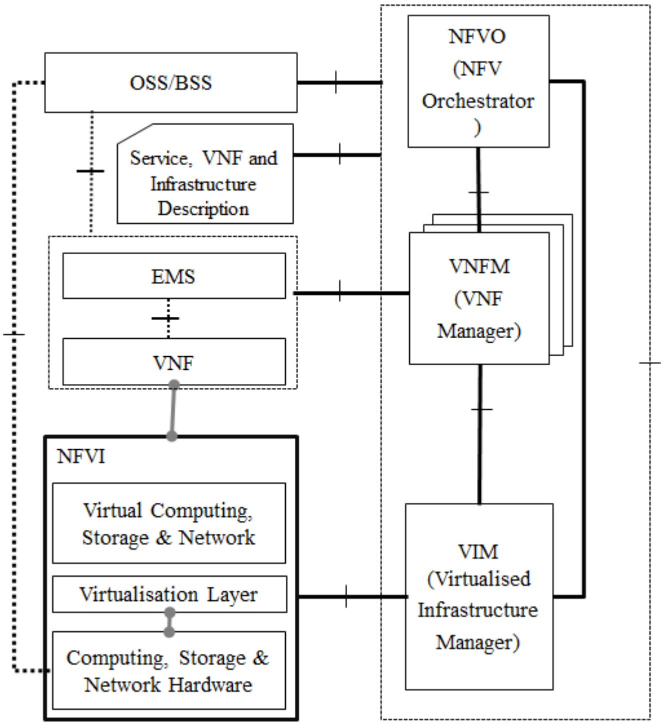
OSS/BSS
Service, VNF and Infrastructure Description
EMS
VNF
NFVI
Virtual Computing, Storage & Network
Virtualisation Layer
Computing, Storage & Network Hardware
NFVO (NFV Orchestrator)
VNFM (VNF Manager)
VIM (Virtualised Infrastructure Manager)

Figure 1 Network Function Virtualisation (NFV) overview

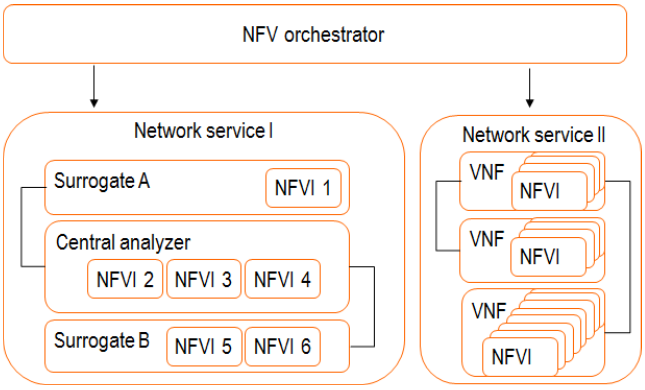

Figure 2 NFV infrastructure services deployment

Let us illustrate these levels on a video surveillance infrastructure service. Consider a fleet of cameras distributed over a given territory, for example across a city. These **cameras** each have their own storage and computing abilities, enabling them to raise alerts when they record actions that are likely to be outlaw, such as an aggression. In this case, they start transferring their recorded video to a surrogate.

Unlike the cameras, **surrogates** are dynamically instantiated on the NFV infrastructure, as depicted on the Figure 2. A VNF is created for each surrogate, and each VNF is made of one or several NFVI. They are thus able to store large films for potentially reusing them later on as proofs. Furthermore, they are able to analyze more accurately the images, performing face recognition. In case of aggression, the face of the offender may thus be recognized and an alert rose.

Each surrogate dynamically provides information to a **central analyzer**, corresponding to another VNF. This component may cross the recorded video analysis with the police record of the offender, for the police to be able to take the most appropriate decision.

The reason for doing NFV is the ability to program infrastructure services instead of re-architecting the infrastructure for every new usage. Therefore, NFV allows reducing the time to market. NFV has the main advantages of automating the exploitation and maintenance, reducing the operational cost and enhancing the flexibility. Yet, despite the undeniable advantage of NFV, finding a migration path from today's networks to NFV is a great issue.

B. *Software-Defined Networking (SDN)*

Unlike NFV, SDN got its start on campus networks, as researchers came up with the idea of making the behaviour of the network devices programmable [8]. As stated in [9], SDN relies on three pillars, illustrated in the Figure 3:

1. The control and data planes are decoupled.
2. Control logic is moved to an external entity, the SDN controller or Network Operating System (**OS**).
3. The network is programmable through software applications running on top of the Network OS that interacts with the underlying data plane devices.

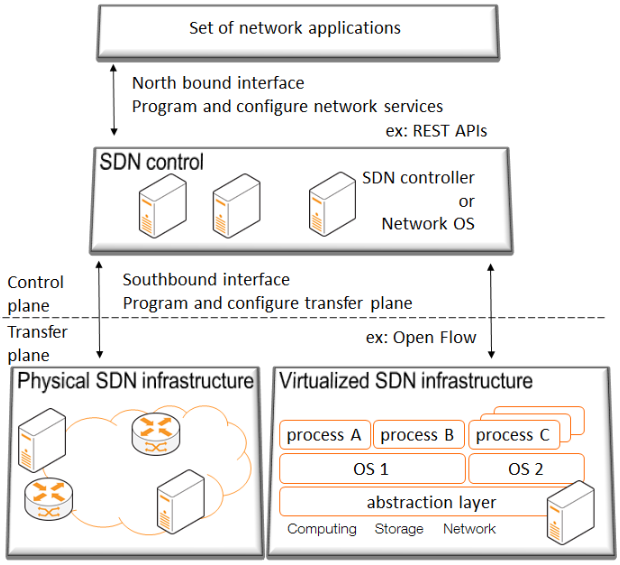

Figure 3 Software Defined Networking (SDN) overview

As shown on the Figure 3, the SDN controller layer exposes a southbound interface to the network elements. The latest can be physical or virtual resources, for example if NFV and SDN are combined.

One of the main reasons for taking on SDN is to find a way out of the network vendor specific vertical integration. As a matter of fact, a single SDN controller can handle different application domains. Furthermore, SDN has the main advantage of simplifying and thus reducing the cost of network operation and maintenance.

With SDN, network policies are defined in the management plane, enforced in the control plane and executed in the data plane. OpenFlow is one example of SDN southbound interface, and REST APIs another example at the northbound interface.

Coming back to the cameras example presented in the previous section III.A, SDN would typically be used for dynamically creating secured network links between each surrogate and the central analyzer.

C. *NFV & SDN benefits for IoT*

NFV and SDN address common objectives: allow network services to be automatically deployed and programmed. More precisely, SDN is a tool typically used for dynamically establishing a connection between VNFs. Furthermore, the infrastructure services addressed by SDN are rather basic connectivity services, while the NFV infrastructure services address a larger scope and provide a framework for virtualization and orchestration.

Thanks to NFV architecture and processes, the infrastructure services layer is decoupled from the resources layer. In addition, network & IT resources will soon be allocated and managed per infrastructure services. Thus, by isolating IoT use-cases, the risks to impact other infrastructure services, flood or break down the whole infrastructure is prevented.

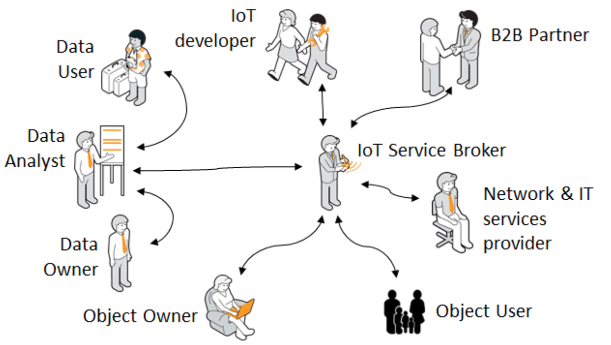

Figure 4 IoT ecosystem actors

Up to now, the rollout of infrastructure services requires a new network configuration. The latest most often relies on human resources even though SDN allows automating it. We have seen M2M resulting in the decrease of human interaction with connected objects. Reducing the human interaction thanks to **SDN automated configuration is thus all the more convenient**.

IV. IoT Ecosystem and Actors

The IoT ecosystem involves a handful of actors presented in the Figure 4. The IoT store is further presented in [10].

As we have seen in section II, the IoT ecosystem is broken up into several application domains living side by side without being interconnected. Providing an overall view over these multiple application domains is thus crucial, and this is the role of our first actor: the **IoT Service Broker**. This actor aggregates connected objects issued from different universes and makes the link between these application domains, B2B partners and end-users.

IoT Developers are responsible for designing and developing connected objects. The IoT Service Broker provides IoT developers access to infrastructure services, such as an overview of the designed objects, the profile of the end-users using these objects or statistics concerning the type of usage. These actors are mainly involved in the pre-sale process, during product specification.

The Object Owner buys and maintains the connected objects, while **the Object User** only uses it.

Furthermore, **the Data Owner** owns the right to store and operate all data collected from connected objects. The analysis of these data is performed by the **Data Analyst**. Finally, the **Data User** has access to part of the data, depending on the offered IoT infrastructure services.

Last but not least, the **B2B partner** contracts with the IoT Service Broker to benefit from infrastructure services, including for example the management of a fleet of connected objects such as electricity meters or probes. The infrastructure service implies providing up-to-date information regarding the objects' state and collected data, alarms when predefined thresholds are raised, and all information on any particular object upon the partner's request. Please note the rollout of such fleet of connected objects is out of our scope.

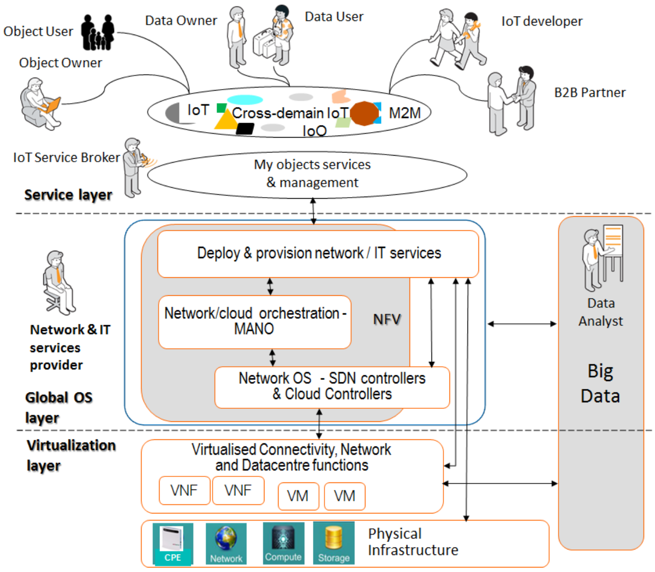
Object User
Data Owner
Data User
IoT developer
Object Owner
B2B Partner
IoT
Cross-demain IoT
M2M
IoO
IoT Service Broker
My objects services & management
Service layer
Deploy & provision network / IT services
Network/cloud orchestration - MANO
NFV
Network OS - SDN controllers & Cloud Controllers
Network & IT services provider
Global OS layer
Data Analyst
Big Data
Virtualization layer
Virtualised Connectivity, Network and Datacentre functions
VNF
VNF
VM
VM
CPE
Network
Compute
Storage
Physical Infrastructure

Figure 5 Infrastructure services NFV/SDN architecture

V. NFV/SDN network & IT infrastructure

Let us now present the architecture that will allow dynamically deploying IoT infrastructure services. These infrastructure services can be dynamically instantiated thanks to the combination of NFV and SDN. The resources are organized into virtualized resources thanks to NFV. The creation of the infrastructure services relies on different layers as represented on the Figure 5.

The Service Layer embeds all service-level functions: the IoT referential and the presentation of infrastructure services.

The **Global OS layer** embeds the infrastructure services' inventory and description, the network & IT orchestration or NFVO and the SDN controllers.

The **NFVO** manages the resources to fulfill the infrastructure services' lifecyles. In particular, it is responsible for creating new gateways when required, based on the infrastructure services descriptors received from the above "Deploy & provision network / IT resources" functions.

The **SDN controller** layer is responsible for the end-to-end control of the network & IT resources. It manages the dynamic configuration and re-configuration of all network elements.

Finally, the **virtualization layer** organizes the hardware resources onto virtual machines made available to the above layers.

VI. Illustrating Example : IoT Gateway

IoT is only at its early stages, and all future possible use cases cannot yet be foreseen. Nevertheless, heterogeneity is likely to last. Thus, gateways are essential to implement the needed access and network technologies and provide the widest integration. Access technologies include for example Zigbee, Bluetooth, Bluetooth Low Energy, powerline communications, Ethernet, Zware or Wifi. Gateways also ensure interoperability between different types of objects and physical technologies, allowing a real IoT experience for the objects users. These gateways will allow connecting objects, correlating information and triggering actions.

Furthermore, gateways could implement security functions, enhancing security by confidentiality and integrity services, as described in [5]. Thus multiple gateways implementing intelligence for objects and applications issued from diverse application domains will be deployed.

With the proliferation of objects and gateways, there will be for sure a strong need to manage and control these gateways from the network & IT infrastructure.

Another structuring question is where to locate the computing power. Locating it on the edge gateways will raise some power consumption issues and exclude heavy processing. Conversely, locating it on a central server will be damaging in case of network unavailability and will raise latency issues for real time applications such as smart factory. Thus a hybrid model is required, distributing the computing power between the local area network, network operator cloud and OTTs' (Over The Top) clouds. The operator cloud located in edge nodes could be mandatory to improve global efficiency and reduce latency.

In the middle term, NFV and SDN could be part of the network operator domain. We therefore recommend IoT gateways, which draw the frontier between the operator domain and the private domain, to be deployed on a NFV/SDN digital infrastructure. Yet, some security and robustness issues still need to be addressed.

As shown in the literature and by the previous section, associating NFV with SDN is an opportunity for the infrastructure operator. In addition, third parties have access to infrastructure services upon which they can build their own offers. The infrastructure services can indeed be opened to numerous third party actors such as application developers, services providers, or even IoT virtual operators.

VII. Conclusion and Perspectives

The proliferation of IoT objects and services is a major challenge to address in the coming decade. Currently, IoT is divided into multiple application domains living side by side without being interconnected.

Hopefully, network virtualization and programming is simultaneously evolving, for example with NFV and SDN. Currently, the rollout of a new infrastructure service may need to deploy dedicated servers. Yet tomorrow, thanks to NFV, open hardware servers will be shared between many infrastructure services. The rollout of a new infrastructure service will thus only require to automatically deploy software components on these open hardware servers. While enhancing the infrastructure agility, this paves the way to **software-oriented innovation within infrastructure services.**

We actually believe the combination of NFV and SDN will answer to the IoT requirements and use cases, including in particular stringent scalability, privacy and cost requirements.

However, the NFV and SDN working groups shall be aware of the IoT strictest robustness and security constraints. Data users are indeed expecting a better control of their privacy and thus of their personal data over the future Internet. Nevertheless privacy shall preserve the roles and benefits of intermediate servers, which implement essential functions such as caching.

From the exploitation and maintenance automation point of view, managing too many infrastructure services may be inefficient. In that context the M2M ETSI and One M2M standards are very promising by specifying common services layers seen as a mediation layer between applications and basic infrastructure service. The next step will be to implement common, mediation or advanced infrastructure services using NFV/SDN framework.

References

[1] Margaret Chiosi, Network Functions Virtualisation, White Paper #3, October 14-17, 2014 at the "SDN and OpenFlow World Congress", Dusseldorf-Germany

[2] UIT-T Y.2066

[3] 15 milliards d'objets connectés et moi, émoi…, Gabriel Siméon, Libération, November 3, 2013

[4] Internet of Things, Outlook for the top 8 vertical markets, Samuel Ropert, Idate, September 2013

[5] oneM2M Functional Architecture Baseline Draft, document number oneM2M-TS-0001 - V-2014-08, 2014-08-01

[6] Network Functions Virtualization (NFV); Architecture Framework, ETSI GS NFV 002 v1.1.1 (2013-10)

[7] Antonio Manzalini & al, Software-Defined Networks for Future Networks and Services, White Paper based on the IEEE Workshop SDN4FNS, 29th January 2014

[8] Prayson Pate, NFV and SDN: What's the Difference?, SDN central, march 2013

[9] D. Kreutz, M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, Software-Defined Networking : A Comprehensive Survey, IEEE, october 2014

[10] Gael Fromentoux and Nathalie Omnès, Network & IT Infrastructure Services for the IoT Store in Proc. IoTaaS 2014, October 27-28, 2014, Rome, Italy

[11] Chris Gallon, Carrier Software Defined Networking, Fujitsu, march 2014

[12] 4G Americas' Recommendations on 5G Requirements and Solutions, october 2014