5G Network: Challenges and Cognizance

AMAN ULLAH

Department of Computer Science
Alpha College of Science
Pattoki
PAKISTAN
a.ullah@mail.com

Abstract: - 5G technology is a brand new paradigm strongly supported by European Commission to overcome the demands of future networks and aiming to tackle the unconventional and manifold enterprise business necessities of vertical sectors like Industry 4.0, Smart Cities, Smart Grids, unconventional resource virtualization, on-demand service-oriented resource allocation etc. The accommodation of such features requires multipronged efforts in exclusive network generation domains at various levels. In this paper, we check out how the relative 5G network features mission the current era of networks, both fixed and wireless and data centres from end users' point of view. Furthermore, we offer some insights into how emerging technology consisting of network function Virtualization (NFV) and software defined Networks (SDN) can be applied to ensure above mentioned features and 5G network realization for individual and commercial users.

Key-Words: - orchestration, NFV, SDN, 5G, optical networks, Wi-Fi networks.

1Introduction

The 5G promises of a whole networked society with unlimited access to data requires specific features beyond current 4G offers. Some of those capabilities encompass support for new form of smart devices, for very excessive mobile data volumes, integration of heterogeneous access technologies, ubiquitous access for customers, a better frequency reuse in Wi-Fi technologies etc. To supply a viable solution meeting all 5G necessities, a large change on the network planning and design paradigm is inevitable. One of the main pillars of such revolution is the manner that new network capabilities become part of the value chain. Historically, this kind of procedure demands deployment of specialized devices with 'tough-wired' functionalities. It implies that any model to the ever growing and heterogeneous market necessities needs a big funding to change installed hardware [1]. Due to rapid developments in SDN and NFV, the idea of getting computing and storage resources at networks has been envisioned in conjunction with the virtualization of networks and network functions that permits the automation of network service provisioning and management. Given the virtualization of networks and network functions, the 5G options of multi-tenancy and end-to-end security becomes even more difficult. In terms of multi-tenancy, the challenge stays however the isolation among totally different tenants, utilizing virtual networks presumably over similar physical infrastructure, may be ensured at all levels. For guaranteeing end-to-end security in 5G networks, a holistic approach is needed that considers not solely the physical however conjointly the virtual resources of the network. These challenges need a considerable amendment on the network devices, from being solely network devices to cloud-enabled devices upgraded with novel processor architectures.

Besides, elementary modifications on the data centre (DC) infrastructures, it is crucial to satisfy the requirements of future Internet and 5G applications. On the IT part of DCs, the quantity of virtual machines (VMs) created by totally different server virtualization technologies has been increasing and it will grow subsequently in few years [2]. Therefore, it is important to own intelligent DC management system for approximate utilization of resources to accommodate instantiated VMs for better performance. Moreover, DC networks with the standard tree-like architectures are reaching their limits and can't address the necessities of evolving 5G applications in terms of latency and energy efficiency [3]. This creates a genuine challenge on the DC operators to revise the network design and develop applicable technologies with low power consumption, low latency and high level of flexibility at comparatively low prices.

In this paper, among all abovementioned 5G requirements, we will concentrate on how end-to-end security and multi-tenancy solutions are often visualized for both 5G networks and future

DC networks in line with the 5G demands.

2 Multi-tenancy on 5G Infrastructures

Traditionally, to provide coverage in a single point of Presence (PoP), actual set up of physical infrastructure is essential. Such strategy will increase operators' CAPEX and appreciably hampers enterprise agility, particularly when thinking about the excessive mobile cell densification[4]. Furthermore, the static nature of physical ownership makes it less attractive to address situations with dynamic capacity requirements. It could be effortlessly translated to greater operators' costs, which in flip will increase the carrier fee for customers. To cope with this difficulty, the concept of multi-tenancy has been inducted in 3GPP and is expected to play essential role in 5G networks. In a multi-tenant state of affairs, an infrastructure provider can have access rights to third parties including network operators, vendors or service providers. Sharing the underlying infrastructure increases service dynamicity and reduces both energy consumption and general price commpared to the case wherein parallel structures are mounted in one PoP to assist connectivity for exclusive parties. Figure 1 indicates architecture to strengthen multi-tenancy in the cellular communications infrastructures based on a sizeable evolution of the 5G radio heads closer to cloud-enabled devices, as recommended in 5G SESAME project. The important element of this architecture is a Cloud-permit Small cell (CESC), owned by means of a Small Cell Network Operator (SCNO), which comprises of a micro-server incorporated with the small cell to support each edge services and radio connectivity presaging the cell into physical and virtual network functions and virtual network functions (VNF), thus permitting a multi-tenancy architecture to assist the Multi-Operator Core Network (MOCN) requirements. The CESCs clustering permits the advent of a micro scale virtualized execution infrastructure inside the shape of a decentralized data centre while improving both the process power and the virtualization capabilities. The hardware structure of the Light DC visualizes that every micro server must communicate with all others through a devoted LAN ensuring low latency and high required for sources sharing. This type of clustering is accomplished through a general Ethernet switch, presumably configured correctly by enabling the networking among CESCs. It also results in backhaul connections to the operators Evolved Packet Core (EPC) and all links leading to the control devices. All management and orchestration duties, such as useful resource allocation and service lifecycle management over the underlying decentralized infrastructure are accomplished by means of a centralized unit known as CESC supervisor. The resulting outcome permits virtual small cell network operators (VSCNO) to have interaction among sharing models based on logical slicing of the network infrastructure [5].

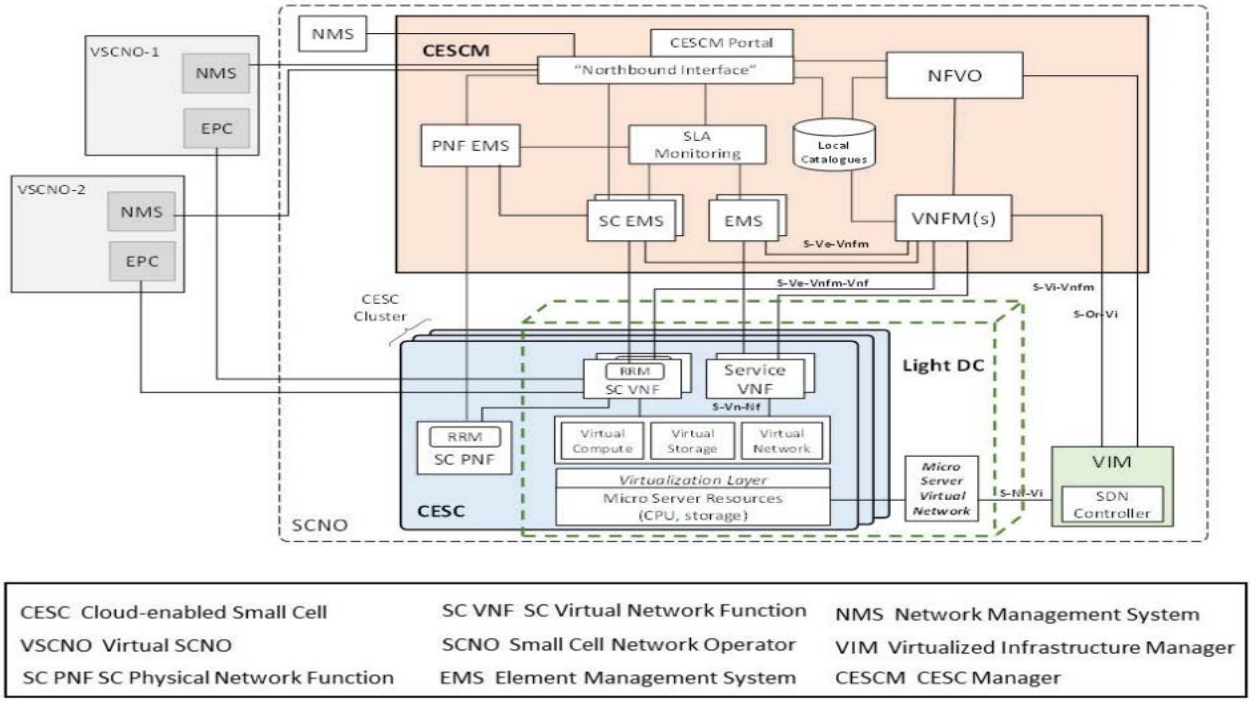

Figure 1. Possible multi-tenancy architecture for 5G

2.1 5G network security

Securing a network and its services is a complex and time consuming process which has scaled up every other notch especially with the creation of SDN and NFV in 5G networks. It allows to construct a constant and sturdy protection environment [6]. On the other hand, network functions and services in SDN/NFV environments require exhaustive approach towards end-to-end security for

both physical and virtual assets which guarantees automatic alignment of security regulations on the eve of network changes. Security functions are heavily dependent upon network monitoring information. It has become even more critical in SDN/NFV based networks which require consistent and careful monitoring as compared to conventional non-SDN/NFV networks. We need all this due to the fact that SDN/NFV based network deployment permits dynamic and automated provisioning, network orchestration, functions and applications. Consistent automated security monitoring of physical and virtual resources is a difficult task. The figure 2 displays security management architecture recommended in CHARISMA project. Furthermore, this architecture is mapped on ETSI MANO framework which is based on control, management and orchestration plane mostly deployed in converged access networks. The proposed security management systems consists of two components called security policy management (SPM) and security & monitoring analytics (SMA). The function of SPM is to enable end-to-end security policies management at service level. Its role is to translate a service level security policy into specific security requirements. The physical and virtual resources transmit monitoring information to SMA. As shown in figure 2, the monitoring data is assembled at service level (VNFs), physical resource level (server machine etc) and virtual service level (VMs). The SMA extracts required information, to be passed over to SPM, by executing smart analytic algorithms. The SMP will analyze these information in accordance with defined services policies and then appropriate action will be taken, The most important feature of this architecture is that it takes multi-tenancy environment as well which leads security policy management on per tenant basis.

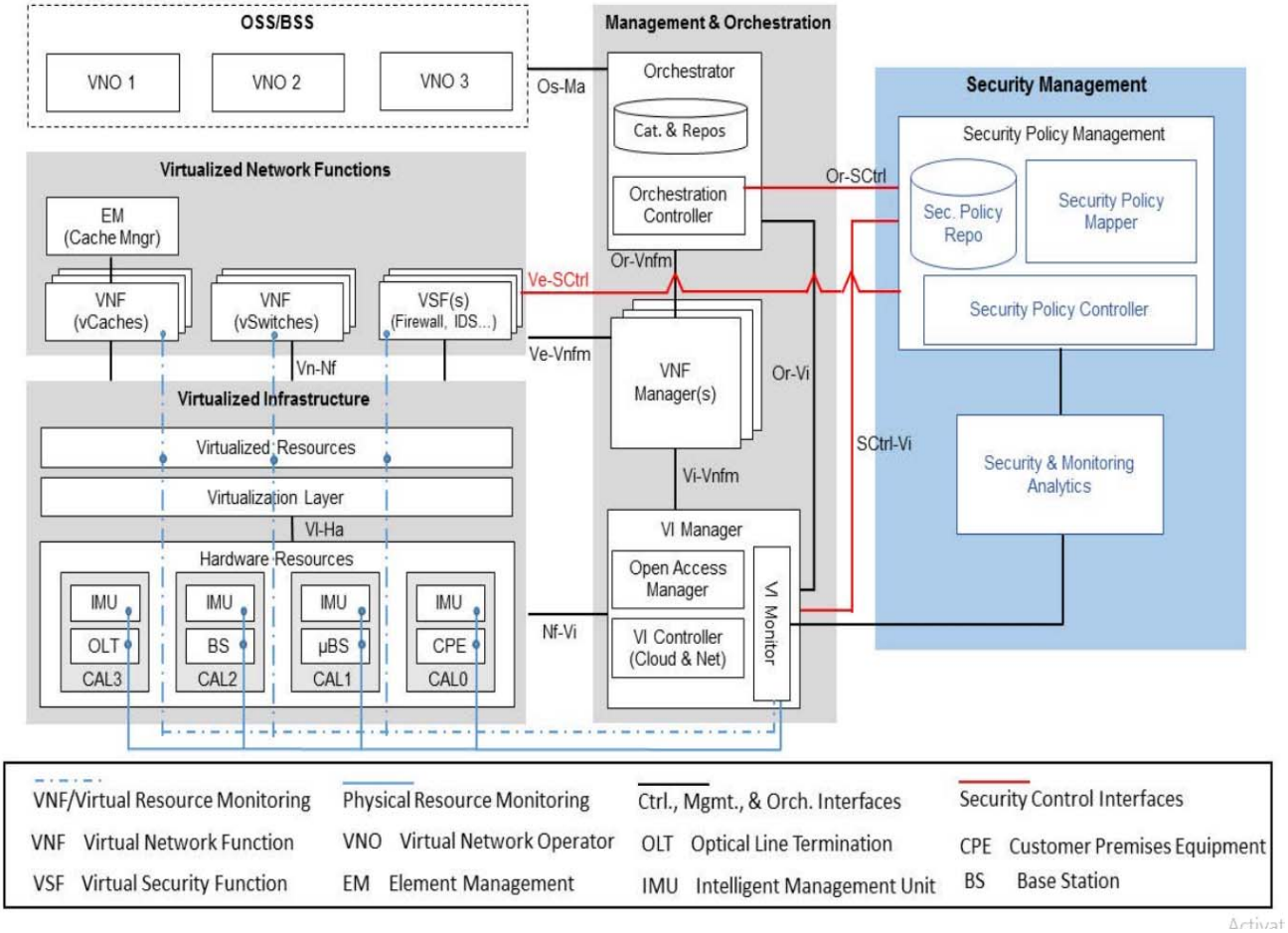

Figure 2. S*ecurity management architecture based on ETSI MANO framework.*

2.2 5G networks and future data centres

To play their important role on the 5G systems, future DCs require enormous vertical change in comparison to the contemporary DC architectures at all tiers, through introducing disruptive ameliorations within data plane. Significant advances to manipulate control plane are also required. Figure 3 indicates a scheme for future DC network deployments, as proposed inside the FP7 COSIGN venture that, at data plane level, will chase the gradual adoption of optical technologies to enable scalable top-of-rack switches, ultra-low latency and excessive extent DC interconnects to support growing 5G requirements.

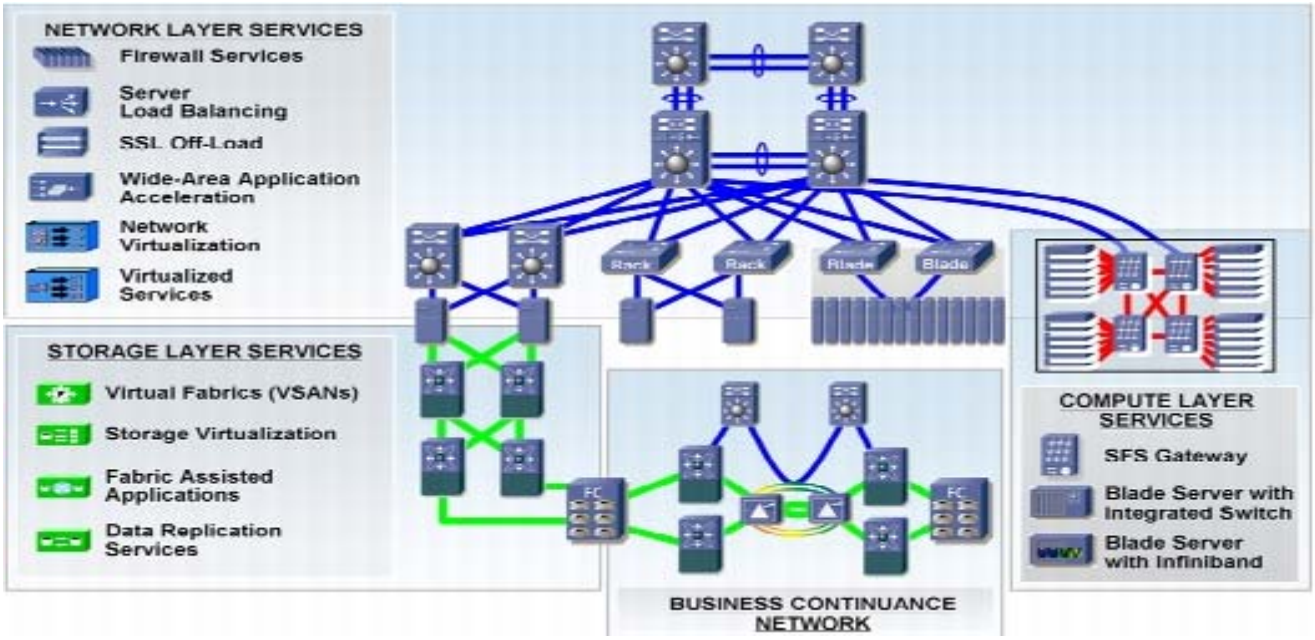

Figure 3. Future DC networks architecture

The heterogeneity that one of these data plane brings, demands, on the control plane, that the capabilities from high performance optical technology are leveraged even as the underlying DC network complexity is not visible. By deploying SDN and network virtualization concepts, DC network infrastructures may be abstracted, partitioned and/or aggregated into visualized resource pools that can be provisioned dynamically and flexibly. In DC environments, benefits of optical data plane can be maximized by adopting SDN based control plane and service orchestration framework. On the other hand, evolving 5G services and architectures can be supported when resources are provisioned dynamically. Therefore, functionalities and automation mechanisms for completely optical DC environments need to be able to manipulate and co-ordinate the orchestrator combination of network and different IT assets at all layers. This could lead complicated DC programs and services demands leverage the advantages that current and future optical data plane technologies and SDN-based control plane introduce.

3 Conclusion

5G networks are designed to fulfill evolving requirements of rising commercial enterprise paradigms. In this paper, we indexed a number of crucial research challenges of 5G architecture by considering security and multi-tenancy features of 5G networks in addition to DC community assessment to satisfy 5G wishes. Furthermore, we presented possible procedures to effectuate multi-tenancy and security tendencies for a 5G network and defined a layout for future DC network to facilitate 5G targets. The works described are hot

research topics that shall make a solid contribution to the realization of 5G networks.

References:

[1] "5G Infrastructure Public Private Partnership (PPP): The next generation of communication networks will be 'Made in EU'", European Commission, Digital agenda for Europe, Feb. 2014.

[2] "Virtualization in Small Cell Networks", SCF154.05.02, Small Cell Forum, 2015.

[3] Security Management and Monitoring for NFV (NFV-Sec013), Release 2, European Telecommunications Standards Institute (ETSI), 2015.

[4] N. Baldo L. Giupponi and J. Mangues-Bafalluy " Big Data Empowered Self Organized Networks " in 20th European Wireless Conference 2014 pp. 1 – 8 .

[5] S. Mwanje L.C. Schmelz A. Mitschele-Thiel . " Cognitive Cellular Networks: A Q-Learning Framework for Self-Organizing Networks " IEEE Transactions on Network and Service Management vol 13 no. 1 pp. 85 – 98 ; January 2016

[6] S. Mwanje, G. Decarreau, C. Mannweiler, M. Naseer-ul-Islam and L. C. Schmelz, "Network management automation in 5G: Challenges and opportunities," *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, Spain, 2016, pp. 1-6.
doi: 0.1109/PIMRC.2016.7794614