Efficient Deployment of Service Function Chains (SFCs) in a Self-Organizing SDN-NFV Networking Architecture to Support IOT

Kwang-Man KO
Dept. of Computer Engineering, Sangji University
Gwangwon, South Korea
kkman@sangji.ac.kr

Ali Mohammed Mansoor
Dept. of Software Engineering, Faculty of Computer Science and Information Technology, University of Malaya
Kuala Lumpur, Malaysia
ali.mansoor@um.edu.my

Rodina Ahmad
Dept. of Software Engineering, Faculty of Computer Science and Information Technology, University of Malaya
Kuala Lumpur, Malaysia
rodina@um.edu.my

Soon-Gohn Kim,
Dept. of Computer Engineering, Joongbu University
Chungnam, South Korea
sgkim@joongbu.ac.kr

***Abstract*—**SDN and NFV provide the underlying cloud-centric operational infrastructure necessary to drive new revenue streams and exploit new market opportunities, such as IoT and M2M. In this paper, we introduce an in-progress a new dynamic fine-grained (two-layer) functions placement and migration mechanism for SDN/NFV-enabled network in IoT/5G infrastructure that considers load balancing and fault tolerance and congestion avoidance while respecting the specific requirements of the IoT application and utilizing the network resources.

Keywords—Software-Defined Network; Network Function Virtualization; Self-Organizing Networks; Mobile Cloud Computing; Internet of Thing;

I. INTRODUCTION

Software Defined Networking (SDN), Network Function Virtualization (NFV), Internet of Things (IoT), Self-Organizing Networks (SON), Cloud computing and Fog computing are predicted to shape the future of the communication networks, the emergence of 5G era [1,2]. IoT is attracting significant attention due to its capability of connecting various devices from the real world to the network. Starting with simple data collection and visualization, the IoT is now evolving continuously to include the remote control of devices and optimization of the systems in use. This trend is expected to lead to an increase in and diversification of the connected devices, as well as an expansion in the patterns of data usage [3]. In the new connected world, a huge number of IoT devices (billions) with different characteristics and requirements is expected to be deployed and communicate in real time. How IoT is efficiently deployed is a notable research question [4]. "A network architecture that was designed for millions of humans making voice calls is simply not suitable to reliably allow billions of devices (or "things") to communicate in near real time," analyst Gartner [5], which says this is likely to trigger significant investments in cloud-centric, software-driven infrastructures [5,6].

The IoT concept incorporates the vision of ubiquitous virtual connectivity of billions of physical objects or "things" through a global network infrastructure with interoperable, self-configuring and scalable capabilities. "Things" might be part of various application domains and therefore are represented by different types of devices that have heterogeneous technical parameters and communication capabilities. This imposes various technical challenges in terms of adaptation, context awareness, device discovery and management, scalability, managing a large data volumes, privacy, and security [7].

Although, NFV goals can be achieved using non-SDN mechanisms, approaches relying on the control and data forwarding planes separation can enhance performance, simplify compatibility with existing deployments, and facilitate operation and maintenance procedures. In the same way, NFV is able to support SDN by providing the infrastructure upon which the SDN software can be run. Finally, the modern variant of a data center (the cloud and it's self-service aspect) relies on automated management that may be obtained from SDN and NFV. The role of NFV, decoupling of software and hardware, in this path is possibly the most important, since the vast traffic volume expected to be created through IoT connected devices and 5G networks cannot be efficiently and cost effectively supported with existing infrastructure deployments [8]. SDN concept lies on the decoupling of the network data plane and control plane leading to centralized management of control plane and de-centralized data plane management. With such implementation, the operations of data forwarding, routing and network function control are decoupled which serve an important architecture for the management of large scale complex networks, which may require re-policing or re-configurations from time to time. This is made possible by making the network directly programmable via an open interface [8,9].

Cloud computing, SDN and NFV are abstractions of different resources: compute for cloud computing, network for SDN, and functions for NFV. The advantages that accrue from each of them are similar; agility, cost reduction, dynamism, automation, resource scaling etc. Network Functions will be migrated to the cloud to make the cloud carrier-grade in terms of performance, reliability, security, communication between functions,

etc. The relation between Cloud computing, SDN and NFV is visualized in Fig. 1.

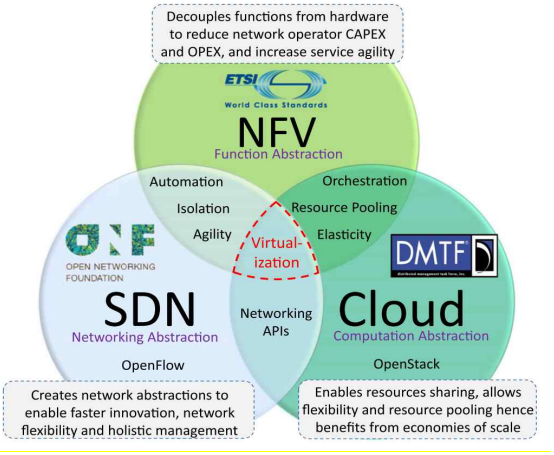

Fig. 1. SDN, NFV and Cloud[9]

Although, SDN and NFV have started being developed independently, however it can be said that the former acts as complementary to each other. SDN is tightly coupled with NFV, with the former having less stringent requirements as far as real-time processing is concerned. SDN focuses on Layer 2 and 3 network elements and operations while a SDN controller provides the northbound interface on which many additional services can be built as shown in Fig. 2. Coupling of SDN and NFV implementation can lead to flexibility with the development of non-proprietary communication protocols and the automation of network functions. Their combination enhances the performance of many IT services already run on cloud services. SDN and NFV are two of the most prominent technologies to serve as key enablers for the IoT networks of the near future [8-11].

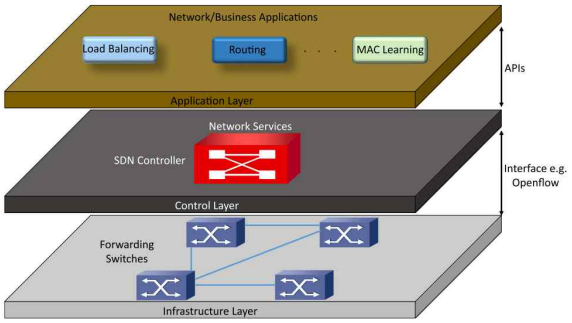

Fig. 2. SDN/NFV Architecture from [9].

In this paper, we proposed and are developing the distributed and concurrent offloading framework that based on the idea of offloading computation-intensive or data-intensive modules of IoT applications running on mobile devices to a mobile edge server with excellent computing resources and processing power, and then the high resource servers are running and they returns the results to mobile edge sides.

II. Research Motivations: Why SDN/NFV in IoT?

Virtualized and software-driven infrastructures will allow the incubation of a wide range of composite services. SDN and NFV provide the underlying cloud-centric operational infrastructure necessary to drive new revenue streams and exploit new market opportunities, such as IoT and M2M. Service delivery has to become more agile to allow flexible configuration changes in order to respond to immediate business needs in real time. This is because the sheer volume of data and analysis are increasing exponentially, as well as the potential number of possible configurations. Cloud Service Providers need to invest in appropriate network infrastructures that can handle new digital and IoT partner[5]. SDN and NFV solutions are expected to be relevant in addressing different challenges in an IoT environment including the following:

Interoperability: Network management decisions such as routing, scheduling can be done at the SDN controller and moreover, the programmability allows for any updates for new proposals or even clean state approaches.

Discoverability: The ability to self-configure and adapt to the environment without human intervention brings about requirements such as resource and service discovery.

Security: Security threats can be easier to attack through the improved visibility SDN provides to the network. SDN can also provide a dynamic, intelligent, self-learning layered model of security that provides access rules to ensure authorization for people who are allowed to change the configuration of devices

Efficiency: NFV can help the service providers to build network intelligence both in a centralized and distributed way to control the traffic, to enable flexible distribution of hardware resources for eliminating bottlenecks and also provide analytics at the edge of the network for latency reduction. It also helps in securing network resources to meet the needs of IoT applications.

Management: The SDN controller manages and supervises the entire network. The centralized position of the SDN controller makes it suitable to have a global vision of the network topology and conditions, performing network control such as routing and QoS control.

Scalability: The rapid growth of the deployment of miniaturized devices (sensors, actuators, etc.) in IoT environment, the data produced by these devices grow unboundedly. Thus, handling of this massive produced data is a significant challenge in IoT. SDN can improve scalability issues in IoT network where the SDN controller oversees the network domain and communicates with other SDN controllers to exchange aggregated network-wide formation. The distributed SDN model tends to share the load among several controllers and spreads functionality across several nodes. Also, network functions (NFs) can be migrated (offloading of computational tasks), extended or created to adapt the new network status as well as users and applications to solve the scalability issue.

Service Delivery: SDN/NFV makes service chain shorter and simpler by increasing the network capacity without changing hardware making it easier to spin up IoT applications. With SDN/NFV, Service Function chaining (SFC) enables network

operators to configure dynamically in software without having to make changes to the network at the hardware level where new services can be added without the need of upgraded support for new devices as required in the traditional networking approach.

Application Specific Requirements: Supporting real-time applications is a must requirement in an IoT environment where it is expected to monitor different things at different time periods. SDN is able to strengthen network controlling ability through perform dynamic adaptation of control logic by the devices in real-time and supporting application specific requirements with control logic that jointly act at the network and processing level enhancing the entire system's QoS/QoE.

III. Research Challenges and Objectives

Currently, there is some work involving SDN/NFV combination to enhance either of them; including: a ForCES-based framework [12], NFV-based monitoring for SDN [13], and an abstraction model for both the forwarding model and for the network functions [12]. As these efforts show, the unique demands of NFV will potentially necessitate a massively complex forwarding plane, blending virtual and physical appliances with extensive control and application software, some of it proprietary [14]. There exist various challenges and research issues when end-to-end network slicing with SDN/NFV in general and when comes to deploying IoT [3-5, 10]; many challenges are related to algorithm and system design regarding of function deployment.

To design and develop a new dynamic fine-grained (two-layer) functions placement and migration mechanism for SDN/NFV-enabled network in IoT/5G infrastructure (as depicted in Fig. 3.) that considers load balancing and fault tolerance and congestion avoidance while respecting the specific requirements of the IoT application and utilizing the network resources. To design and develop new dynamic traffic engineering techniques for SDN/NFV-enabled network with effective traffic that consider the IoT different traffic characteristics and efficient enable end-to-end communication as depicted in Fig. 3.

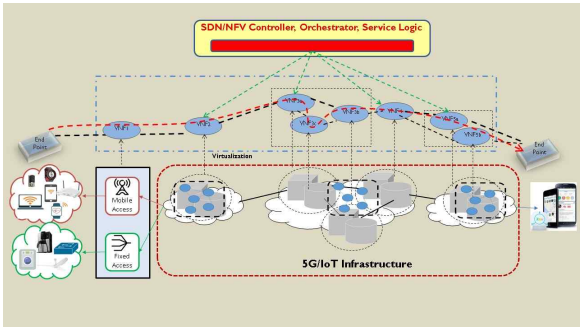

Fig. 3. New dynamic fine-grained functions placement and migration mechanism

To combine the function placement and migration algorithms with the traffic engineering technique. Apply artificial intelligence (machine learning) techniques on the top of the proposed algorithms to optimize the performance and make the network adaptive and self-organizing with respect to real-time decisions based on different IoT traffic characteristics.

Software and Simulation: Simulation is the only feasible way for conducting our work as it will involve. OpenDaylight : OpenDaylight [16] is an SDN control platforms that supports a broader integration of technologies in a single control platform [17]. Led by the community and supported by the industry, it is an open source framework to accelerate adoption, foster new innovation and create a more open and transparent approach to SDN and NFV. Optimization using CPLEX: Developed algorithm can be further supported with optimization process in order to optimize certain parameters. This can be done through integrating our algorithms with optimization tool such as CPLEX.

V. Conclusion

In this paper, we introduce an in-progress a new dynamic fine-grained (two-layer) functions placement and migration mechanism for SDN/NFV-enabled network in IoT/5G infrastructure that considers load balancing and fault tolerance and congestion avoidance while respecting the specific requirements of the IoT application and utilizing the network resources.

Acknowledgement

This paper was supported by Joongbu University. This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2017030223).

References

1. ERICSSON mobility report, https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf , June 2016.
2. '5G Vision, the 5G Infrastructure Public Private Partnership, The next generation of communication networks and services'. https://5g-ppp.eu/.
3. Matsuda Naohisa, Takagi Kenki, Horiuchi Sho, Aoki Hiroki, Akutagawa Aiko, "SDN/NFV solutions providing new values to network, systems; IoT Network Implemented with NFV", Special Issue on Telecom Carrier Solutions for New Value Creation, 2016.
4. Ngoc-Thanh Dinh, Youngki Park, Hunjung Lee, Younghan Kim,"End-to-End Network Slicing with SDN/NFV For Internet of Things: Research Challenges and Issues", KICS, 2017
5. http://www.gartner.com/newsroom/id/3213418
6. Stefan Nastic, et., al., "Provisioning Software-defined IoT Cloud Systems", International Conference on Future Internet of Things and Cloud, 2014
7. Katov, A. N., Anggorojati, B., Kyriazakos, S., Mihovska, A. D., & Prasad, N. R. (2016). Towards Internet of Services - SDN-enabled IMS Architecture for IoT Integration. In 18th International Symposium on Wireless Personal Multimedia Communications, IEEE Press. 2015
8. Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, Raouf Boutaba, "Network Function Virtualization: State-of-the-art and Research Challenges", IEEE Communications Surveys and Tutorials, 25-09-2015.
9. Diego Kreutz, M. V. Ramos, Paulo Verissim, "Software-Defined Networking:A Comprehensive Survey"
10. Nikos Bizanis and Fernando A. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey", IEEE Access, 2016
11. NFV & SDN Migration Challenges: Interoperability, co-existence and specific services as the drivers and opportunities for NFV & SDN migration, ISPM, 2015

12. E. Haleplidis, J. Hadi Salim, S. Denazis, and O. Koufopavlou, “Towards a network abstraction model for SDN,” J. Netw. Syst. Manage., vol. 23, no. 2, pp. 309–327, Apr. 2015.
13. T. Choi et al., “SuVMF: Software-defined unified virtual monitoring function for SDN-based large-scale networks,” in Proc. 9th Int. CFI, New York, NY, USA, 2014, pp. 1–6.
14. Z. Michael et al., “OpenFlow-enabled SDN and network functions virtualization,” Open Netw. Found., Palo Alto, CA, USA, Tech. Rep.,Feb. 2014.
15. X. Meng, V. Pappas, and L. Zhang. Improving the scalability of data center networks with traffic-aware virtual machine placement. In Proc. of IEEE INFOCOM'10, 2010. 7, 11, 32, 33, 34, 99, 105.
16. “OpenDayLight,” 2017. [Online]. Available: http://www.opendaylight.org/project.
17. D. Kreutz et al., “Software-defined networking: A comprehensive survey,” Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.
18. https://www.sdxcentral.com/articles/contributed/sdn-iot-securing-internet-things/2016/09/
19. ETSI GS NFV 002 V1.2.1 (2014-12), “Network Functions Virtualization (NFV), Architectural Framework”.
20. ETSI GS NFV 001 V1.1.1 (2013-10), “Network Functions Virtualization (NFV) Use Cases”.
21. ETSI GS NFV-SWA 001 V1.1.1 (2014-12), “Network Functions Virtualization (NFV), Virtual Network Functions Architecture”.