2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)

SDN/NFV-based Network Infrastructure for Enhancing IoT Gateways

Do Sinh[1], Luong-Vy Le[2], Bao-Shuh Paul Lin[1,3], Li-Ping Tung[3]
[1]Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan
[2]College of Electrical and Computer Engineering, National Chiao Tung University, Hsinchu, Taiwan
[3]Microelectronics & Information Research Center, National Chiao Tung University, Hsinchu, Taiwan
Email: dosinhuda.cs04g@nctu.edu.tw, leluongvy.eed03g@nctu.edu.tw, bplin@mail.nctu.edu.tw, lptung@nctu.edu.tw

Abstract – The interconnection of billion smart devices opens new challenges for network integration in Internet of Things (IoT) environments, in which IoT gateways play significant roles as an intermediate component of smart devices and communication networks; therefore, a large amount of data are collected and exchanged via these gateways, whose applications are expected to reduce data processing, storing, and forwarding in IoT networks. On the other hand, recently, SDN/NFV have been considered as emerging technologies and enablers for improving network performance and management due to the full capacities of scalability, flexibility, and elasticity. Hence, applying SDN/NFV for IoT gateways is expected to ease the complexity of the interconnection into the edge network as well as facilitate the interconnection of multiple network protocols, and multiple co-existing tenants on the same physical network. In this paper, firstly, the authors investigate several popular IoT gateways such as NB-IoT and 6LoWPAN to propose a suitable SDN/NFV-based architecture for IoT networks. Secondly, P4 and ONOS controller are used to implement deep programming at the customer side of a network that is suitable for deploying massive IoT environments and developing their applications in the manner of horizontal scalability. Finally, several experiments were demonstrated and implemented in a real NB-IoT gateway, which is a new gateway designed as an outdoor small cell for IoT.

Keywords—Software-Defined Network (SDN); Network Functions Virtualization (NFV); Internet of Things (IoT); Wireless Sensor Network (WSN); P4; PSA (Portable Switch Architecture); ONOS (Open Network Operating System).

I. INTRODUCTION

IoT- a massive surge of smart and interconnected "things" is a popular concept recent years in that network communications play crucial roles to seamlessly connect "smart things" with heterogeneous connectivity across multiple vendors. The "smart things" or "things" in this context refer to various electronic devices embedded sensors and actuators, which can be programmed for special purposes such as GPS tracking in smartphones, tablets, etc. Furthermore, the development of cloud-based networks, embedded systems, and SoC (System on Chip) makes "things" more intelligent so that they can interconnect to any things at any times in anywhere through the Internet. Currently, many living sectors are applied IoT applications to improve the current situations within the "smart" prefix as smart-home, smart-city, smart- grid, smart-car, smart-metering, etc. Research [1] noted that the next generation of cellular technologies must enable a wide range of IoT services, which can reach up to 5 billion IoT connections by 2025. Research [2] supposed that the short-range IoT connected will reach 16 billion devices and wide-area IoT connected will reach 2.1 billion devices by 2022. Since IoT covers a wide variety of use cases in diversity requirements and environments, inter-networking is an essential challenge for it because there is no single network protocol that can adequately implement for all use cases. Fig 1. shows a summary of LPWA (Low Power Wide Area) standard network as an example.

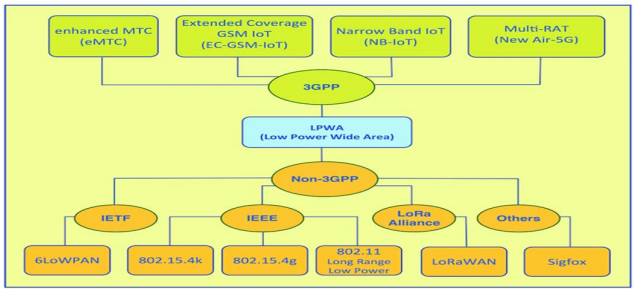

Fig. 1. LPWA standards

In 3GPP (The 3rd Generation Partnership Project), standards for IoT are presented in the Releases 12 and 13, and additional work will be introduced in Release-14. Table 1. shows a summary of the characteristics of the eMTC, NB-IoT, and EC-GSM-IoT.

In Non-3GPP, standards for IoT are developed by numerous members such as Lora Alliance with LoRaWAN, IETF with 6LoWPAN, IEEE with 802.15.4 k and g, 802.11 LRLP, and others with Sigfox, DASH7, etc. Table 2. shows a summary of the technical features of some technologies.

Smart devices use IP Protocol to communicate in networks; however, devices within the same network can use non-IP protocols to reduce their power consumption and memory due to the complexity of TCP/IP stacks. Therefore, IoT gateways have important roles in flexibly supporting wide-spread

978-1-7281-2980-8/19/$31.00 ©2019 IEEE
DOI 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00192

Table 2. Summary for eMTC, NB-IoT and EC-GSM-IoT

id	3GPP for the Internet of Things			
		eMTC (LTE Cat M1)	***NB-IoT***	***EC-GSM-IoT***
1	Deployment	in-band LTE	in-band & Guard band LTE, standalone	in-band GSM
2	Coverage	<100Km	<35Km	<35Km
3	Bandwidth	1.08 MHz	180 KHz	200 KHz per channel. Typical system bandwidth of 2.4MHz
4	Peak rate	1 Mbps for download (DL) and upload (UL)	DL: ~50 kbps UL: 20kbps - 50kbps	For DL and UL:70kbps - 240kbp
5	IP or/and Non-IP protocol	Non-IP: End-device, SGW, via the MME; Optionally support Non-IP PDN via PGW and non-IP via SCEF (Service Capability Exposure Function) in the future. IP: SGW⇔PGW	Non-IP: End-device, SGW, via the MME and the signaling data bearer; Optionally support Non-IP PDN via PGW and non-IP via SCEF in the future. IP: SGW⇔PGW	Non-IP: End-device⇔ SGSN-MME; Not to mention the support for Non-IP Data delivery in the future. IP: SGW⇔PGW

Table 1. Summary for LoRaWAN, Sigfox, and 6LoWPAN

id	Non-3GPP for the Internet of Things			
		LoRaWAN	***Sigfox***	***6LoWPAN***
1	Deployment	ISM band (<1GHz band)	ISM band (<1GHz band)	ISM band (<1GHz band and 2.4GHz band)
2	Coverage	5-15km	10-50km	10-100m
3	Bandwidth	125 KHz-500 KHz for 915 band 125KHz-250KHz for 868 MHz band	100Hz-1.2kHz	5MHz for 2.4 GHz band; 2MHz for 915 MHz band; 600 kHz for 868.3 MHz band
4	Peak rate	980bps-21.9kbps (for 915 band) 250bps-50kbps (for 868 MHz band and 780 MHz band)	100bps-600bps	20kps-40kbps for <1GHz band, and up to 250 kbps (2.4 GHz band)
5	IP or/and Non-IP protocol	Non-IP to/from Gateway. Network Server (at Gateway) use IP connectivity to route messages to the right Applications. Devices and Applications have an identifier (DevEUI, AppEUI)	Non-IP to/from Sigfox Base Station (using packet ID to identify end-devices); Backend server (at Base Station) uses IP connectivity	Non-IP for Mesh routing in the PAN (Personal Area Network) space using PAN identifier. IP Packet between IPv6 domain and the PAN domain

internet-based applications. For example, in the context of non-IP devices, the IoT gateways connect with smart devices using non-IP protocols on the customer side and using IP protocol on the other side (servers). Moreover, the diversity of device vendors and heterogeneous connectivity in IoT ecosystems impose the IoT gateways to be powerful enough to work with a wide range of use cases with various requirements. As a result, the gateways must be evolved to serve the connectivity fabrics for any protocol such as IP and non-IP protocols.

Currently, SDN/NFV and P4 are considered as the key features to evolve a network by supporting deep programming on the data plane and make the network more scalable, flexible, and elastic without depending on proprietary network protocols. In other words, they enable multiple network protocols deployed simultaneously on the same physical network that will be suitable for enhancing the IoT gateways. Moreover, SDN/NVF and P4 based CORD (Central Office Re-architected a Data Center) have been applied as a tendency to deploy DCN (Data Center Network) at both the core and the edge cloud to reduce the OPEX (the Operations Expense) and CAPEX (the Capital Expense) for network operators. The P4 programming language is defined to program the data plane. P4 and ONOS Controller allow us to configure and re-configure P4-based switches embedded on IoT gateways during runtime. On the other hand, NFV provides ways to virtualize the network elements by software components or modules to increase network scalability and efficiency. Therefore, it is necessary to propose an approach that can provide connectivity fabrics for IoT gateways when applying SDN/NFV and P4 based switches into the IoT gateways.

The rest of paper is organized as follows. Section II presents related work. Section III elaborates the proposed architecture, which includes IoT gateways and other supporting components. Section IV presents the measurement results and analyzes network performance. Section V discusses future works, and Section VI concludes the present study.

II. RELATED WORK

To work with different protocols between sensing and network domains, studies [3] and [4] proposed SDN-based architectures for horizontal IoT services, in which an OpenFlow-based switch was used as a gateway that enables sending and receiving instructions from different protocols. The gateway was used with the purpose of protocol converting between two domains. Research [5] proposed a method to address the gap between two sensing domains through software-defined data plane that can work as a bridge based on

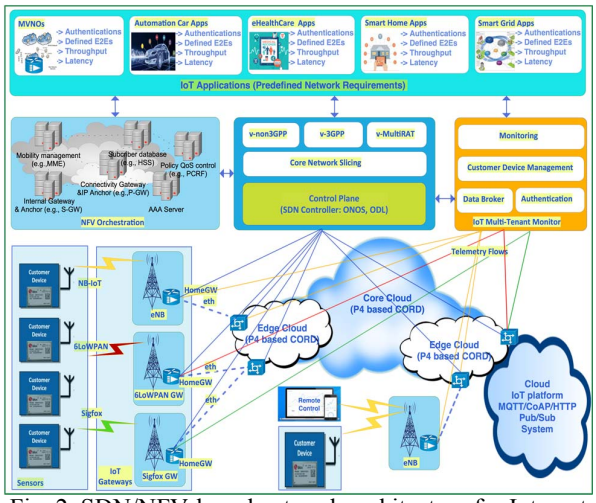

Fig. 2. SDN/NFV-based network architecture for Internet of Thing platform and integrated IoT gateways

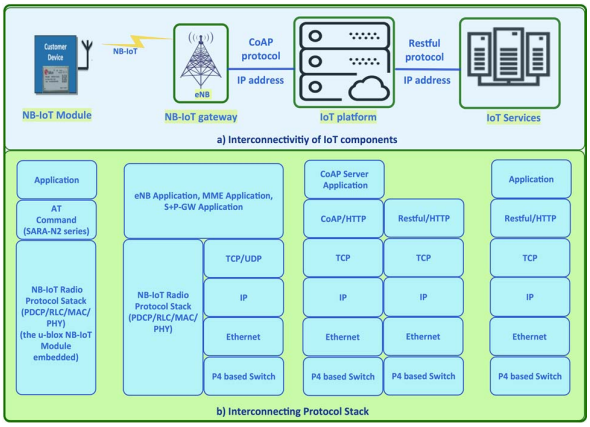

Fig. 3. a) Inter-connections among IoT components; b) Protocol stacks

a context-aware forwarding/processing packets. In this scenario, an SDN model was extended to support packet manipulation at Layer 7 by extending the programming functions of OpenFlow convention. In general, these approaches require more capability of computing resource and memory at the gateways; therefore, they are difficult to deploy in large-scale network environments.

To deal with this challenge, several approaches for deploying large-scale software running on IoT gateways were proposed, recently. For example, research [6] proposed an approach of using Docker containers to build gateway functions in a large-scale network. Studies [7] and [8] defined agents running on gateways for controlling software-defined IoT systems. Research [9] provided a server-side building and packaging software to automatically push and pull-based provision on the gateways.

When the volume of IoT networks is larger, it is difficult to deploy, configure, and maintain IoT gateways. To deal with this problem, SDN/NFV are used to build VNFs (Virtual Network Functions), which are stored in forms of VM (Virtual Machine) images or containers. As a result, the NFV orchestration can easily create, activate, or change the states of an individual instance or a function running on an IoT gateway. We believe that the development of NFV Orchestrations, SDN controllers, and building software in Cloud will offer a feasible and powerful IoT infrastructure in which various network functions can be deployed on the IoT gateways.

Due to the drastic increase in IoT traffic communicated over networks, it is necessary to provide efficient approaches for data storage, processing, and transmitting, and reducing amount of data forwarded to the core. One big advance of applying SDN/NFV and P4-based switches-enabled IoT gateways is the possibility of providing fabric E2E connectivity among IoT gateways, dynamic scaling, and pre-processing data at the gateways.

In addition, studies [10] and [11] explored technical relationships among the development of IoT, Big Data Analytics (Big Data), Cloud Computing (Cloud), and SDN in the future 5G era. They showed that 5G networks with high data rate and low latency provide a capability of transmitting a huge amount of data generated by IoT applications faster and cheaper as well as handle various requirements of IoT applications. Moreover, SDN/NFV can provide a scalable network to transport large data in an optimal way; cloud and Big Data can be used for data processing and storage. NFV plays important roles in setting up instances for each gateway in an easy way. Thus, 5G architectures should integrate these technologies for developing IoT networks and applications, for example offloading IoT gateways functions in a large-scale IoT ecosystem.

On the other hand, to work as a bridge for communicating between sensing domains and network domains, IoT gateways must meet the following requirements:

- Provide a connectivity fabric to the Internet without depending on proprietary network protocols.

- Meet requirements of data storage, processing, and transmitting based on the 5G, Big Data, Cloud, and SDN technologies.

- Ensure that networks can be deployed easily at large scale.

- Provide controlling and monitoring capabilities for users to manage their IoT applications such as identify, configure, maintain, and control smart devices.

III. SDN/NFV BASED NETWORK ARCHITECTURE FOR IOT PLATFORM AND INTEGRATED IOT GATEWAYS

In the past few years, we have been focusing on investigating and applying the Internet of Things, 5G, Big Data, Cloud, and SDN/NFV technologies to our experimental platform [10-14]. This paper investigates and explores these technologies to propose a comprehensive architecture that is suitable for development IoT platform as described in Fig 2.

The IoT platform collects data from various IoT applications through the IoT gateways and then forwards

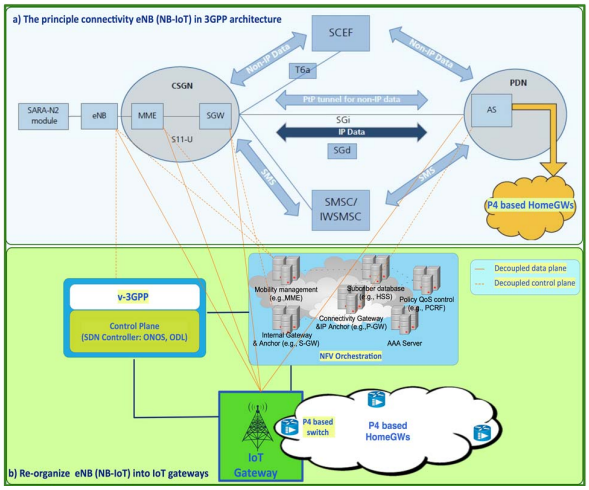

Fig. 4. Re-organized NB-IoT gateways

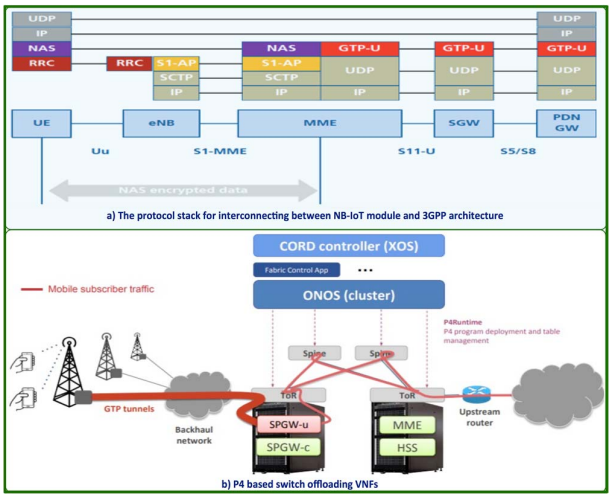

Fig. 5. P4-based switch offloading VNFs

relevant data to associating applications. The HomeGWs interconnect the gateways and IoT platforms, among gateways, and among IoT platforms in Cloud environments. An IoT platform usually contains several IoT servers deployed as VNs (Virtual Machines) to provide IoT services and applications such as data processing.

The Customer Devices send and receive data to the IoT platform via the IoT gateways. They communicate with each other by utilizing several technologies such as NB-IoT (Narrow Band Internet of Things), 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network), and Sigfox. In this paper, the authors focus on using NB-IoT for exploring the proposed architecture. The Fig 3. shows an example of the inter-connections among Customer Devices, IoT gateways, IoT platforms, and IoT services using a NB-IoT gateway (eNB), CoAP (Constrained Application Protocol), and Restful protocol. Fig. 3 a) shows a principal model for the interconnectivity of IoT components, and b) shows internetworking protocol stacks among components. The NB-IoT used as customer devices in this model is u-blox SARA-N2 series [15]. It communicates with a cell tower, called NB-IoT network (eNB), over the radio interface (NB-IoT Radio Protocol Stack: PDCP – Packet Data Convergence Protocol, RLC – Radio Link Control, MAC – Medium Access Control, and PHY – Physical Channel). The eNB links to the IoT platform via a P4-based switch network and a SPGW-u, which is an integrated component of SGW and PDN GW User plane as shown in see Fig 5. The IoT platform the customer device. On the other hand, IoT service components connect to the IoT platform to retrieve the data and send downlink packets to the customer device. The IoT platform holds downlink packets until the customer device is awake to receive them.

CoAP (Constrained Application Protocol), a datagram-based client/server application protocol for devices in constrained networks, is designed for web transfer protocol. The CoAP client built at an IoT Gateway can use commands such as GET, PUT, POST, and DELETE to request and response to the CoAP servers located in IoT platform components.

SARA-N2 supports AT commands to control SARA-N2 modules by using either UDP socket commands (Non-IP Data) or datagram commands (IP Data). IP data are transported through the SGi interface as shown in Fig 4 (a). Fig 4 (b) describes the re-organized architecture of an IoT gateway, whose functions can be deployed as VNFs (Virtual Network Functions) running on a DCN in form of VM (Virtual Machine) or container images under the control of using SDN controller and NFV Orchestration. SCEF (Service Capability Exposure Function) is a new node especially designed for machine type data. It is used for delivering non-IP data over the control plane and providing an abstract interface for network services (e.g. authentication and authorization, discovery and access network capabilities). Non-IP data is transferred in the same way as the conventional traffic to application servers (AS) over the radio bearer via the SGW (Serving Gateway) and the PGW (Packet Data Network Gateway). In this architecture, depending on IoT applications and requirements, the VRAN (virtual RAN) and VCN (virtual Core Network) can be sliced to meet predefined network requirements such as throughput and latency.

The last component in Fig 2 is the IoT Multi-Tenant Monitor, which is used to slice the network and monitor the QoS of services based on their pre-defined requirements. Its functions are described below:

- Manage and provide service for tenants or users through communicating with the network components such as MME (Mobility Management Entity), HSS (Home Subscriber Server), SPGW-c (Serving and Packet Data Network Gateway Control plane) for registration and service management purposes. On the other hand, user's status and parameters are recorded for the Customer Device Management to implement the network slicing and QoS monitoring.

- Connect to the IoT platform to implement Big Data analytics, storage, Pub/Sub systems, cloud computing, cloud machine learning, etc. as shown in Fig 6. Moreover, the IoT platform is also synergistic with IoT Multi-Tenant Monitor and SDN Controller to fulfill fully-managed services running on

the IoT platform, such as allocate the resource of the IoT platform through the Authentication, Data Broker modules, and Telemetry Flow components.

- Control the Customer Device through different services built based on results of data analytics by using end-device applications to modify the configuration of the Customer Devices.

- Collect Telemetry Data Flows (Telemetry Flows) of applications running on the Customer Devices, IoT Gateways, network Nodes for building network management applications such as congestion control and QoS control. The Telemetry Flows have significant roles in providing an real-time network control and monitoring on the data plane based on the pre-defined QoS at each IoT gateway. Fig 6 shows a summary of technical relationships among the IoT gateway, IoT platform, and IoT Multi-Tenant Monitor.

IV. IMPLEMENTATION AND EVALUATION

Experiment environment: Fig 7 (a) shows the devices used in our experiments: an eNB embedded Lite EPC software was used as a NB-IoT gateway; NB-IoT Customer Devices were used to demonstrate how they internetwork with the NB-IoT Gateway.

The NB-IoT gateway consists of several blocks of hardware specifications: Intel Atom x7-E3950 by Apollo Lake SoC; 8G DDR3L; 1x DP, 2x GbE, 2x COM ports, 2x USB2.0, 2x USB3.0, 2x mPCIe, 1x USIM, 1x mSATA; especially, it involves an eNB and an EPC running on Linux 4.4.0-104-low-latency. It's configuration parameters are assigned as below:

- NB-IoT deployment bands: According to the 3GPP Release 13, a set of frequency bands that have been assigned for NB-IoT are: 1, 2, 3, 5, 8, 12,13, 17,18,19, 20, 26, 28, and 66. From Release 14, several bands are added :11, 25, 31 and 70. In this experiment, we assigned band 20 (uplink: 832 – 862MHz; and downlink: 791-821MHz); frequency parameters with EARFCN (Evolved-UTRA Absolute Radio Frequency

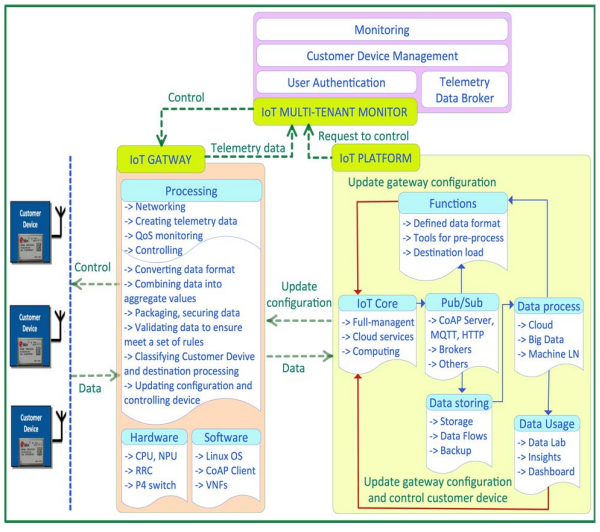

Fig. 6. Relationship among the IoT gateway, Platform and

Fig. 7. Communication between Customer devices and NB-IoT gateway

Channel Number) for the downlink is 6390 (856MHZ), and for the uplink is 24390 (815MHZ).

- NPDSCH (Narrowband Physical Downlink Shared Channel) supporting the Reference Signal Power (RSP) is from -60 to 50dB. In this system, RRC RSP is -10dB and Receiver Gain (Rx) is 16dB.

- Lite EPC is a software program running on the NB-IoT gateway to inform the eNB where it can offload VNF functions from the core of the P4-based network.

- The Customer devices use their embedded u-box NB-IoT modules (this demo use SARA-N2 series with AT commands) to send UDP packets to the NB-IoT gateway.

The first experiment describes the connection of the Customer Devices and the gateway. Fig 7 (b) shows the result of connecting Customer devices to NB-IoT gateway and sending UDP data packets.

The second experiment aims to demonstrate how the NB-IoT gateway can connect and send data to an offloaded MME by setting up a NAS encrypted data connection as shown in the Fig 5 (a). On the other hand, it also demonstrates how the NB-IoT gateway records the status and parameters of the connected customer devices and sends to the IoT Multi-Tenant Monitor component (shown in Fig 6) for implementing service slicing and QoS monitoring. In this experiment, we used an off-the-shelf Dell PowerEdge III Server platform with two quad-core Intel Xeon 5400, CPU 3.16GHz, 64GB memory, 2xGbE NICs, Linux 4.15; Mininet version 2.2.2; P4 Runtime package; and ONOS Controller version 1.14.0 to build a P4 based CORD network as described in our previous study [16]. We also used two VMs, one for offloading MME function and the other for collecting Telemetry data and running QoS services. Fig 8 (a)

shows the deployment network topology. Fig 8 (b) describes the result of sending UDP data to the IoT Multi-Tenant Monitor for collecting network states. Fig 9 shows communication messages between NB-IoT gateway and MME VM Server after offloading MME via NB-IoT gateway.

The last experiment demonstrates how to control IoT traffic with different QoS levels. In this experiment, traffic flows were generated by GPS sensors embedded in three real customer devices. The data flows from different customer devices were sent to the NB-IoT Gateway and then forwarded to the Monitor Server with different QoS policies controlled by the IoT Multi-tenant Monitor. Fig 10 shows the traffic profile generated by a GPS sensor when turning on the location tracking feature in real-time. Fig 11 shows the latency profiles of the GPS tracking traffic sent from the three customer devices to the Monitor Server before and after applying network slicing. There were three slices associating with three QoS priorities, namely, Green, Yellow, and Red slices, which were managed and controlled by the IoT Multi-tenant Monitor. The Green slice was assigned with default or normal QoS level, in which the GPS tracking traffic was forwarded without QoS controlling, the Yellow slice was assigned with the highest QoS priority or QoS class. The Red slice was allocated with the lowest QoS class. As a result, with the QoS control, the Red traffic had the highest latency while the Yellow traffic obtained the lowest latency.

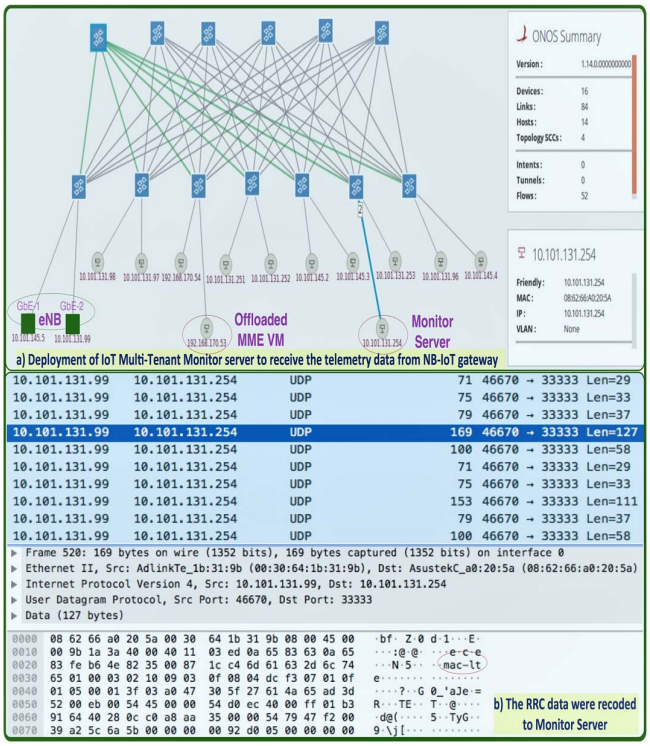

Fig. 8. Recording data from the NB-IoT gateway to the IoT Multi-Tenant Monitor

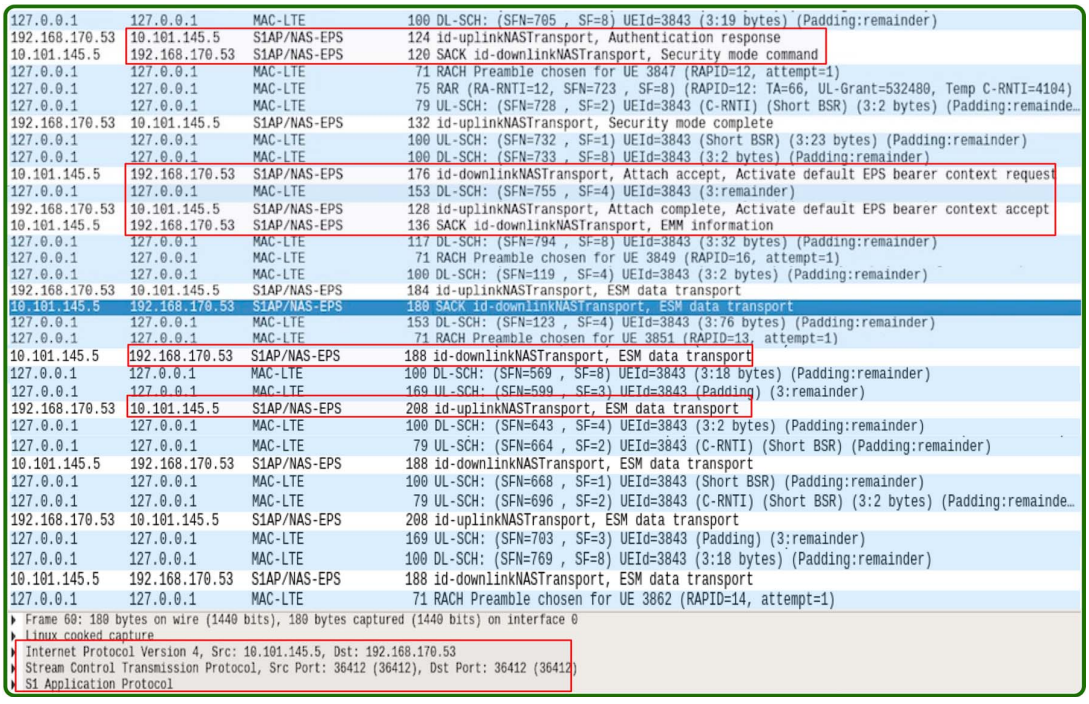

Fig. 9. Communication between the NB-IoT gateway and the offloaded MME

In summary, the results of three experiments demonstrate different functions of the NB-IoT gateway:

- Support various protocols dynamically adapted to the network infrastructure: MAC-LTE/UDP (shown in Fig 7 (b); UDP/IP for recording data from the NB-IoT gateway to the IoT Multi-Tenant Monitor (shown in Fig 8 (b); S1 Application protocol/Stream Control Transmission/IP (shown in Fig 9) for communicating between the Customer devices to the NB-IoT gateways and the MME. These functions can be implemented by re-programming the pipeline of the P4-based switches.

- Offload functions of the EPC to Cloud to reduce its complexity. For example, in our experiment, the MME is separated from the NB-IoT gateway and offloaded to the P4-based CN (core network) as shown in Fig 9.

- Collect necessary data such as Telemetry Data Broke for the IoT Multi-Tenant Monitor to build its applications such as slice the GPS tracking traffic from Customer devices with different QoS policies (shown in Fig 11).

V. FUTURE WORK

Applying SDN/NFV to enhance the 5G architecture for IoT environments such as offloading the whole EPC system such as HSS, PCRF, etc. to the cloud. This work will support deploying 5G networks at scalability and addressing various

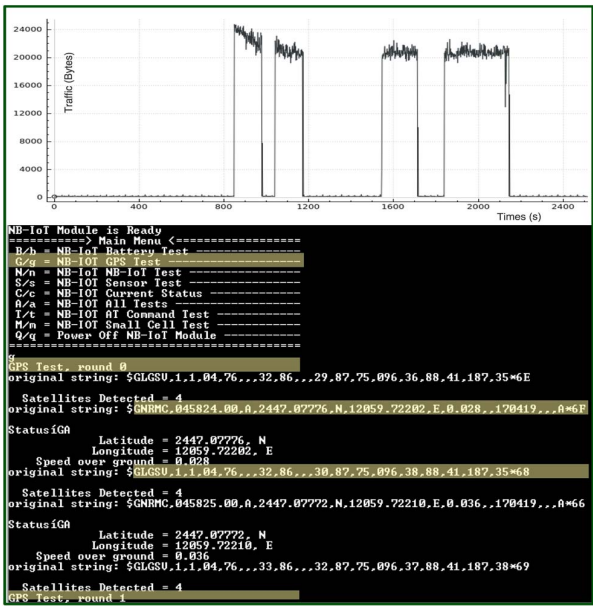

Fig. 10. The test of GPS sensor–embedded in Customer Devices

Fig. 11. Recording IoT data to Server and monitoring the network QoS slices

service requirements. Moreover, we also focus on applying Big Data and Machine Learning our architecture to make it more intelligent and efficient, such as building self-optimization and self-healing applications.

VI. CONCLUSION

In this study, the authors have focused on exploring SDN/NFV network architectures for enhancing IoT gateways that meet diversified requirements of multi-tenant services and devices. For example, provide fabric connectivity without depending on the proprietary network protocol; offload network functions such as MME, HSS, PCRF, etc. to the DCN or Cloud to reduce the complexity of the IoT gateways. Moreover, several key features of the IoT gateways were demonstrated through the experiments implemented on the real NB-IoT gateway, P4 based CORD, and ONOS Controller. Moreover, the utilization of open sources such as P4 and ONOS has significant roles in deploying networks with scalability such as offloading VNF to cloud. Finally, the deeply programmable data plane was also explored and demonstrated through applying network slicing to control QoS of GPS tracking traffic with different pre-defined E2E latencies.

ACKNOWLEDGMENT

This paper is particularly supported by "the Center for Open Intelligent Connectivity from the Featured Areas Research Center Program within the framework of Higher Education Sprout Project" by the Ministry of Education (MOE) in Taiwan, and the Ministry of Science and Technology of Taiwan under Grants: MOST 107-2221-E-009-056.

REFERENCES

[1] Qualcomm, "Paving the path to Narrowband 5G with LTE Internet of Things (IoT)," *Qualcomm Technol. Inc.*, p. 36, 2016.

[2] 5G Americas whitepaper. February 2017. Wireless Technology Evolution Toward 5G: 3GPP Release 13 to Release 15 and Beyond, "Release 15 overview."

[3] Y. Li, X. Su, J. Riekki, T. Kanter, and R. Rahmani, "A SDN-based architecture for horizontal Internet of Things services," *2016 IEEE Int. Conf. Commun. ICC 2016*, 2016.

[4] R. Vilalta *et al.*, "End-to-End SDN Orchestration of IoT Services Using an SDN/NFV-enabled Edge Node," *Opt. Fiber Commun. Conf.*, p. W2A.42, 2016.

[5] P. Du, P. Putra, S. Yamamoto, and A. Nakao, "A context-aware IoT architecture through software-defined data plane," *Proc. - 2016 IEEE Reg. 10 Symp. TENSYMP 2016*, no. 1, pp. 315–320, 2016.

[6] A. Krylovskiy, "Internet of Things gateways meet linux containers: Performance evaluation and discussion," *IEEE World Forum Internet Things, WF-IoT 2015 - Proc.*, pp. 222–227, 2015.

[7] S. Nastic, M. Vogler, C. Inzinger, H. L. Truong, and S. Dustdar, "RtGovOps: A runtime framework for governance in large-scale software-defined IoT cloud systems," *Proc. - 2015 3rd IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2015*, pp. 24–33, 2015.

[8] N. Pazos, M. Muller, M. Aeberli, and N. Ouerhani, "ConnectOpen - automatic integration of IoT devices," *2015 IEEE 2nd World Forum Internet Things*, pp. 640–644, 2015.

[9] M. Vögler, J. M. Schleicher, C. Inzinger, S. Nastic, S. Sehic, and S. Dustdar, "LEONORE - Large-scale provisioning of resource-constrained IoT deployments," *Proc. - 9th IEEE Int. Symp. Serv. Syst. Eng. IEEE SOSE 2015*, vol. 30, pp. 78–87, 2015.

[10] B.-S. P. Lin, F. J. Lin, and L.-P. Tung, "The Roles of 5G Mobile Broadband in the Development of IoT, Big Data, Cloud and SDN," *Commun. Netw.*, vol. 08, no. 01, pp. 9–21, 2016.

[11] B.-S. Paul Lin, Y.-B. Lin, L.-P. Tung, and F. Joseph Lin, "Exploring Network Softwarization and Virtualization by Applying SDN/NFV to 5G and IoT," *Trans. Networks Commun.*, vol. 6, no. 4, 2018.

[12] D. Sinh, L. Le, L. Tung, and B. P. Lin, "The Challenges of Applying SDN / NFV for 5G & IoT," *14th IEEE - VTS Asia Pacific Wirel. Commun. Symp. (APWCS), Incheon, Korea, Sep 2017*.

[13] D. Sinh, L. V. Le, B. S. P. Lin, and L. P. Tung, "SDN/NFV - A new approach of deploying network infrastructure for IoT," *2018 27th Wirel. Opt. Commun. Conf. WOCC 2018*, pp. 1–5, 2018.

[14] L. V. Le, B. S. P. Lin, L. P. Tung, and D. Sinh, "SDN/NFV, Machine Learning, and Big Data Driven Network Slicing for 5G," *IEEE 5G World Forum, 5GWF 2018 - Conf. Proc.*, pp. 20–25, 2018.

[15] www.u-blox.com, "NB-IoT Application Development Guide Technology architecture and AT command examples Application Note NB-IoT Application Development Guide-Application Note Title NB-IoT Application Development Guide Subtitle Technology architecture and AT command examples," 2018.

[16] S. Do, L. V. Le, B. S. Paul Lin, and L.-P. Tung, "SDN/NFV Based Internet of Things for Multi-Tenant Networks," *Trans. Networks Commun.*, vol. 6, no. 6, 2018.