
This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Adem, Anteneh; Costa Requena, Jose; Kantola, Raimo
SDN Network Slicing for URLLC NB-IOT

Published in:
International Conference on Electronics, Information, and Communication

DOI:
[10.1109/ICEIC49074.2020.9051156](https://doi.org/10.1109/ICEIC49074.2020.9051156)

Published: 01/04/2020

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Adem, A., Costa Requena, J., & Kantola, R. (2020). SDN Network Slicing for URLLC NB-IOT. In *International Conference on Electronics, Information, and Communication* Article 9051156 IEEE.
<https://doi.org/10.1109/ICEIC49074.2020.9051156>

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

SDN Network Slicing for URLLC NB-IOT

Anteneh Adem

Mobile communications Dep., CUMUCORE
Espoo, FINLAND
anteneh.adem@cumucore.com

Jose Costa-Requena, Raimo Kantola

COMNET Dept., Aalto University
Espoo, FINLAND
{jose.costa, raimo.kantola}@aalto.fi

Abstract—Current mobile networks are considering mobile devices i.e. User Equipment (UE) associated to a single user. 3GPP has integrated Machine to machine communications and Narrow-Band IoT requirements only in recent releases. The Internet of Things (IoT) devices are autonomous, large in number and often lacking user interface. Different proprietary management solutions have been proposed and implemented to collect data and manage the IoT devices. This paper presents the results of analyzing 3GPP standards for managing device subscriptions such as the User Data Convergence (UDC). The UDC combined with the usage of SDN delivers network slicing to deliver Ultra Reliable Low Latency (URLLC) for Nb-IoT traffic required for industrial communications. A prototype of the design was developed and tested to check the feasibility and this paper presents the results that show the solution could work under the right setup

Keywords— *User Data Convergence, NB-IOT, CIOT, SDN, Network Slicing*

I. INTRODUCTION

In current mobile networks, User Equipment (UE) is the mobile device connected to the network. The people have their own personal UE and use it for personal communications. However, the latest Ericsson report indicates, “of the 29 billion connected devices by 2022, 18 billion will be IoT (or machine-to-machine) devices” [1]. In 5G networks, machine-to-machine communications will produce a significant part of the traffic in the system. Therefore, 5G mobile network is a key enabler of industrial internet and machine-to-machine communications. The concept of UE includes not only personal mobile devices but also sensors and actuators that have different communication requirements. The main difference is that IoT devices will often do not have a user interface. This creates the problem of configuring the devices manually. Moreover, a single user could have several personal UE devices in addition to many IoT devices under his subscription. Managing all these devices (i.e. configuring and updating their software), is a non-trivial task. IoT creates the need to process and manage the subscription data of these devices efficiently. Currently industry is deploying proprietary solutions to acquire the data and manage the IoT devices (AWS, Microsoft, Google IOT platforms). However, proprietary solutions will lead to a market fragmentation. Instead, a standardized solution is required to support an interoperable solution. The future mobile network can play a key role in solving these problems.

It can facilitate the bulk subscription and over the air configuration of IoT devices. Moreover, mobile network already has standardized interfaces to store and access mobile devices configuration available only for mobile operators. Therefore, extending the mobile networks storage systems to be accessible for IOT service providers through standardized interfaces available will guarantee interoperability and scalability.

In the past, the Home Location Register (HLR) in 2G/3G and later Home Subscriber Server (HSS) in 4G were the only entities that stored and provided all the UE information for authentication, location identification and service provisioning. These systems store UE data for people-to-people communication. 3GPP has taken the first steps to redesign these storage systems and has defined the concept of User Data Convergence (UDC). It separates the UE data storage from the application logic that uses the data. The UDC provides a flexible data storage design and simplicity and allows new applications that access the data using a Subscribe/Notify mechanism. In this paper, we show the design of the UDC extensions required for storing and managing the IoT devices and their subscription data.

The remaining of the paper is structure as follows. Section 2 reviews the existing data repositories used in the mobile networks in the past such as HLR, HSS. This section also describes the concept of UDC. Section 3 describes the design and prototype implementation of UDC for the performance tests. Section 4 we describe the usage of SDN for creating network slices. Section 5 presents the results highlighting the usage of SDN to deliver Ultra Reliable Low Latency slice for NB-IOT devices to be used in industrial environments or critical communications. Section 6 presents conclusions and future work.

II. MOBILE NETWORKS USER DATA REPOSITORIES

The architecture of mobile network designed the data repositories for large-scale access of user credentials for authentication and authorization. These repositories have been evolving over time and this section describes those repositories starting from the HLR used in 2G followed by the HSS used in 3G and 4G later.

A. HLR in 2G and HSS in 3/4G

In 2G mobile networks, some permanent user data are stored in a network element called HLR and Authentication Center (AUC). Home Location Register (HLR) stores all permanent subscriber data (i.e. subscription information) and some temporary subscriber data (e.g. Visitor Location Register (VLR) Number) for Circuit Switching (CS) and Packet Switching (PS) domain of mobile networks. In addition to storing subscriber data, the HLR provides logical functions such as access authorization, mobility management, call establishment support and facilitates a host of services [2]. The HLR is in the core network as shown in the Figure 1 together with other network elements like MSC and SGSN. The HLR communicates with the Mobile Switching Center (MSC) and Serving GPRS Support Node (SGSN) with standard interfaces define in [3].

The authentication center stores authentication information used to authenticate subscribers of the PS and CS domain. The AUC transfers the authentication and ciphering data of the visiting user to the other network elements through the HLR, using different interfaces as depicted in Fig. 1. The protocol used over the interface between the HLR and AUC, H-interface, is nonstandard [3]. The term HLR/AUC refers to an entity, which performs the functionalities of an HLR and AUC.

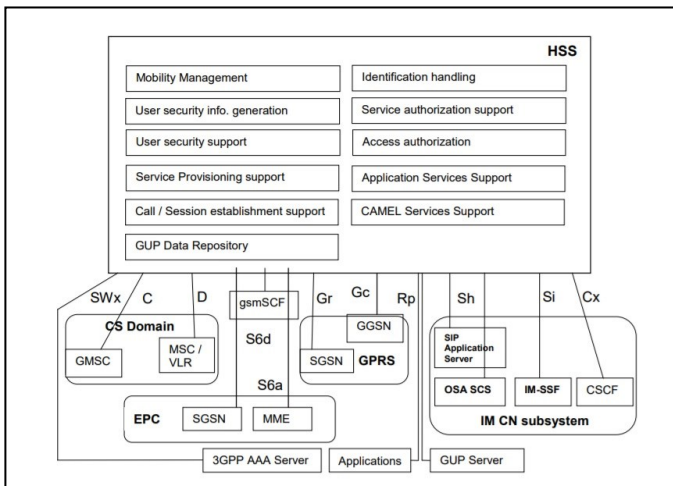


Fig. 1. HSS repository interfaces to 2G, 3G and 4G mobile core network.

In 3G and 4G, the mobile networks evolved and the HLR becomes the Home Subscriber Server (HSS). The HSS is the heterogeneous master database that stores user related information like user identification, user security information, user location information and user service profile information. The CS and PS domain HLR/AUC is a subset of the HSS.

In addition to CS and PS domain users, HSS stores data for IMS domain users. While storing heterogeneous information, the HSS hides the heterogeneity of the information from Application servers that access it [3]. In addition to storing user data, HSS provides logical functionalities such as mobility management, user security information, service, and access authorization for the CS, PS and IMS domain. It has a standard interface to enable network elements found in the above-mentioned domains to communicate with it. Fig. 1, shows the

logical functionalities of the HSS and standard interfaces between HSS and other network elements. It also shows the location of the HSS in the core network and interfaces with the rest of 3G and 4G network nodes.

B. UDC in 4/5G

In 4G, is identified the lack of convergence for storing user and service information. Thus, when adding IMS or Voice over Long-Term Evolution (VoLTE) services a new HSS will store only the service information while another HSS store basic user security information as before in 3G/3G. Therefore, the data has been scattered in different repositories.

Currently user data is stored in different network elements like the HLR, HSS, AUC and application servers. As described in the previous section, these network elements are responsible for both the storage and use of subscription and security data. Due to the lack of separation and a standard interface between the application logic that accesses the data and the data storage system, it is difficult or impossible to introduce new applications that provide some services by accessing the stored user data. In addition to this, the scattering of user data over multiple network elements and the existence of multiple reference points to these network elements complicates user data management, user data view and user data mining.

In order to mitigate the above-mentioned problems, 3GPP has introduced the concept of User Data Convergence (UDC) [4]. With the UDC concept, the user data storage and the application logic that accesses and uses the data are separated through standardized interfaces as shown in Fig. 2. User data that used to be stored in network element like HSS and HLR/AUC is converged and stored in a new entity called User Data Repository (UDR).

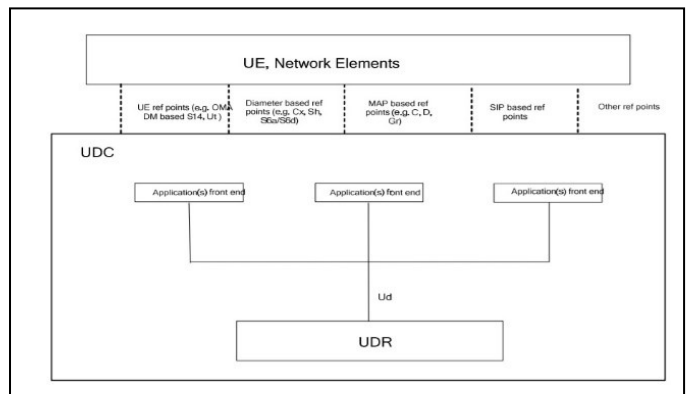


Fig. 2. HSS repository interfaces to 2G, 3G and 4G mobile core network.

The main building blocks of UDC are the UDR, the Application Front Ends and the Ud interface. “The User Data Repository (UDR) is a functional entity that acts as a single logical repository that stores converged user data” [5]. User data like subscription data that used to be traditionally stored scattered in different network elements like HSS, HLR and some Application servers is now logically converged and stored in the UDR. The UDR data is accessed from Application Front Ends

Application Front Ends should only access the data that is required by their application logic. To achieve this, UDR should perform authentication of Application Front Ends (FE) and authorization of data access based on the data the FEs are trying to access. The information model developed for the storage system should enable a separate view of the converged user data stored for each Application Front End. This means Application FEs will only access the part of the converged user data that contains the data relevant to them. The information model of the UDR should also be flexible enough to allow integration of a new Application Front End information or modification of information model of existing Application Front End without affecting operation of other Front Ends.

Application Front Ends are systems that only implement the application logic and store or access their data from the UDR. They might store the data temporarily during processing of some request but will discard it after completion of the operation. The network elements whose data storage and application logic are separated can keep isolated the application logic and become Application Front End (FE), e.g. a legacy HSS could store the data in the UDR and then becomes an HSS Application Front End. The interface between the Application FEs and the UDR is the Ud interface. Using this interface Application FEs can read, write, modify or delete data stored in the UDR. Additionally, Application FEs can subscribe for notifications of change of data stored in the UDR. Two protocols are chosen to be used on this interface by 3GPP [6]. One is Lightweight Directory Access Protocol (LDAP) [7], which is used for the purpose of retrieving, adding, deleting and modifying data stored in the UDR. The other is Simple Object Access Protocol (SOAP) [8], which is used by the Application FEs to subscribe and unsubscribe for notification of change of data. UDR use it to send notification data to Application FEs that subscribe to notification.

III. UDC PROTOTYPE

UDC aims to solve the problem of having different repositories to store user and service data. However, 5G networks are posing new requirements and challenges for data repositories. 5G aims to address limitations of previous 2G, 3G and 4G standards and be a potential key enabler for IoT. The 5G networks have requirements beyond providing connectivity to end users. 5G is targeting users and machines with a wider set of requirements in terms of authentication, service data and user provisioning information.

There are radio technology standards, namely Long-Term Evolution, Category M1 (LTE-M), Narrow Band IoT (NB-IoT) and Extended Coverage Global System for Mobile communications (GSM) IoT (EC-GSM-IoT), that are developed by 3GPP to meet some of these requirements. Since the radio technology standards are not enough, 3GPP has developed enhancements in the core network elements to support transmission of small data efficiently and to support transmission of non-IP data. These enhancements are called Control Plane (CP) Cellular IoT (CIoT) EPS optimization, User Plane (UP) CIoT optimization, attachment without PDN and support of non-IP data. To support these enhancements, Mobility Management Entity (MME) should have the capability to transfer small user data using signaling. And a

new network element called Service Capability Exposure Function (SCEF) is introduced to support non-IP data transfer.

An information model is used in the UDR to model a managed object at a conceptual level. The information model for the UDR is based on the Common Baseline Information Model, see Figure 4, defined in 3GPP TS 32.182[32]. As stated in 3GPP TR 22.985[4], UDR information model should start with Common Baseline Information Model.

The Common Base line information model defines the relation between subscription and services, services and End Users and so on as shown in Fig. 4. It also defines the relation between EPS, General Packet Radio Service (GPRS), CS and IMS services and some of the information object classes that are related to these services. For the purpose of analyzing the proposed solution in this thesis, a Specialized Information Model for IMS and EPS is designed to store user data. The design is mainly based on the principle that the design shall be flexible enough to easily add a new information model for a new application or to add new data in the existing information model. This section describes the extensions made on the information model to manage IoT devices. Before modifying the current information model, the additional information required for storing IoT devices was identified. 3GPP has identified some features required for Machine Type Communication (MTC).

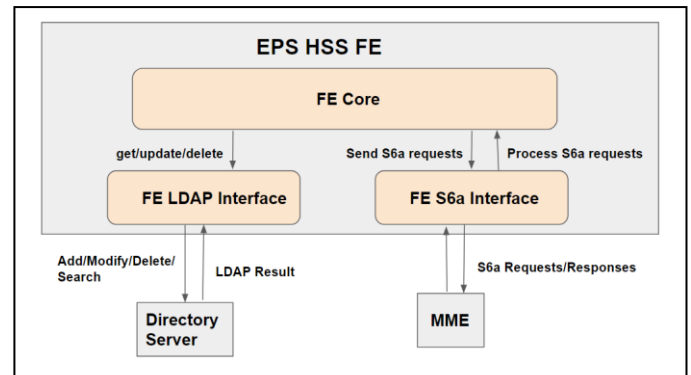


Fig. 3. NB-IoT information element in LDAP UDR.

The parameters identified by 3GPP are Low Mobility, Time Controlled, Small Data Transmissions, Infrequent Mobile Terminated, MTC Monitoring, Secure Connection and Grouped Based MTC Features. These features can be considered as permanent IoT device data as they do not change frequently. Therefore, this static data can be stored as a service profile data for IoT devices in the UDR.

After identifying the IoT device specific data, the current information model was extended to hold the IoT specific data. The extended information model is proposed to allow bulk subscription of IoT devices and facilitate management of these devices. Even though IoT devices could use both EPS and IMS services. We consider that IoT devices are using EPS services, so the extended information model assumes that each IoT device will have an IMSI number.

A. Extension for bulk subscription

To achieve bulk subscription of many IoT devices, a new information model is designed to allow sharing of one EPS Service Profile information object among multiple IMSI information objects. The information contained in one IMSI information object uniquely identifies one IoT device. During bulk subscription of IoT devices which use the same EPS service, a new EPS Service Profile information object is created to hold the information about the EPS services. IMSI information objects are created for each IoT device, and each IMSI information object will hold an information that points to the EPS Service Profile information object as shown in Fig. 4. In case of having 100 IoT devices where each IoT device has a unique IMSI number, there will be 100 IMSI information objects. Therefore, if these 100 IoT devices use the same EPS service, one EPS Service Profile information object will be created for each of them. These 100 IMSI information objects will hold an information element that points to this EPS Service Profile information object.

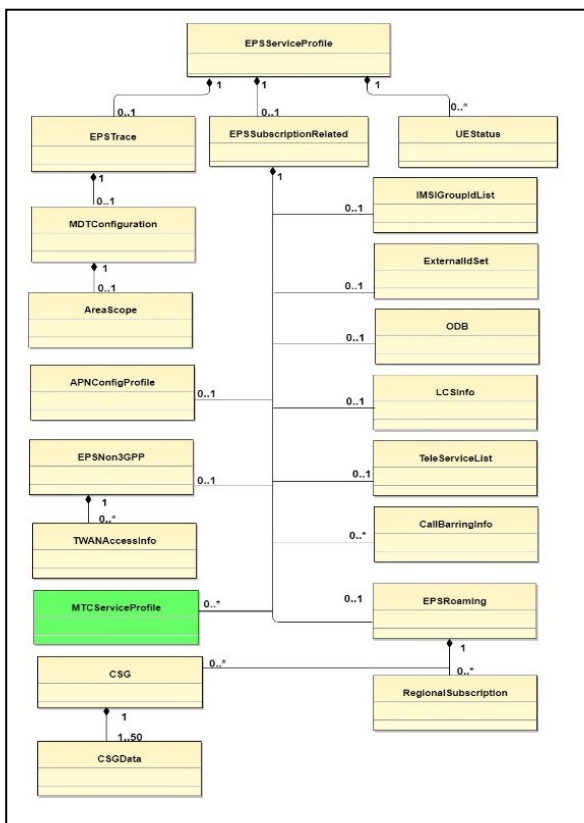


Fig. 4. NB-IOT information element in LDAP UDR.

Fig. 4 shows highlighted in green how the current EPS information model extended to hold IoT device specific data. The ‘MTCServiceProfile’ class is added into the information model. The UDC prototype includes the implementation of the EPS HSS Application Front-End. These modules are called FE Core, FE LDAP Interface and FE S6a Interface. The ‘FE LDAP Interface’ and ‘FE S6a Interface’ modules communicate with the core module with a well-defined interface. There is no interface between the ‘FE LDAP

Interface’ and ‘FE S6a Interface’ module. The EPS HSS Application FE uses its ‘FE LDAP Interface’ module to get/update user data from a Directory Server. This data is required during processing of messages received from the MME. This data is not permanently stored, it is only temporarily stored in memory during processing of the message. After the message is processed, the data is discarded. The only data that is permanently stored in memory is the configuration data, like the MME Names and IP addresses. This means that the EPS HSS FE Application functions are stateless, and all the messages received are processed independently irrespective of the message sent or received previously.

B. FE Core module

This module handles the main logic of EPS HSS FE application. It processes Update Location Request, Authentication Information Request, Cancel Location Request, Purge UE Request and Notify Request messages received from an MME. This module receives the messages to be processed from the ‘FE S6a Interface’ module.

C. FE S6a Interface module

This module handles the communications with the MME based on S6a specifications defined in 3GPP [8]. This module parses the S6a messages received from the MME and checks if the received message is valid. If it is valid, it passes the message to the ‘FE Core’ module for further processing. The ‘FE S6a Interface’ module only passes part of the message that the ‘FE Core’ module needs for processing the message. This module uses an open source Diameter protocol implementation called ‘freeDiameter’.

D. FE LDAP Interface module

This module handles the Ud interface with an LDAP Server. The ‘FE LDAP Interface’ module interacts with the ‘FE Core’ module to fetch, delete and update user data stored in a Directory Server (DS). The ‘FE LDAP Interface’ module and the ‘FE Core’ module are aware of the schema of the data stored in the DS. This module acts as an LDAP client to access the data stored in an LDAP server.

E. SOAP Subscription/Notification design

One of the functionalities expected from the UDR is a subscription and notification functionality. These functionalities are used to receive data when changes occur in the data stored in the UDR. A new plug-in software module that handles the Subscribe/Notify functionalities is implemented.

The new design of the UDR that supports IoT devices requires a customized EPS network. One of the customizations required is on the S6a interface where 3GPP has no standardized commands and AVPs necessary to carry the IoT device specific data. The S6a has been extended to include the

proposed information model for IoT devices. The prototype will use experimental codes that 3GPP reserved for future use.

IV. SDN BASED NETWORK SLICING FOR NB-IOT

Mobile network operators are already adopting new technologies in their infrastructures such as NFV and SDN for network scalability and management. Moreover, large number of sensors are added to mobile networks after including NB-IOT features in the radio access network. However, the networks still must fulfil requirements in terms of latency and enough bandwidth for other communications. However, traditional telecommunications manufacturers offer integration of NFV and SDN that still use legacy solutions proposed in mobile networks from the 80's in the early adoption of IP on mobile networks. Instead, we propose a disruptive SDN/NFV approach where the goal is to provide fast, scalable and more flexible deployments of network slicing that allows to isolate the traffic and fulfil the expected requirements.

The proposal provides the innovative integration of SDN in the mobile backhaul disrupting the current usage of mobile protocols to handle mobility and QoS. The usage of SDN has been focused in fixed networks and in cellular network but keeping legacy transport protocols such as GTP for the mobility management. The proposed usage of SDN in the backhaul will enable the implementation of slices that are managed by the slice manager specified in 3GPP TS 23.501.

The setup consists of multiple NB-IOT devices (Arduino with u-blox NB-IOT chipset) connected to Nokia FZM commercial eNB running on 1.8GHz at the minimum transmission power 24dB and with 30dB attenuator to avoid interferences with commercial mobile operators. The eNB was connected to Cumucore mobile core that includes basic 4G and 5G core functions extended with NB-IOT support. The Cumucore mobile core includes the SCEF which receives the data from the sensors and encapsulates it over UDP to be sent to external servers for data processing. The SCEF is connected to SDN mobile network that is managed from Cumucore Network Slice Manager (i.e. Cumucore product name Mobile Backhaul Orchestrator).

V. NB-IOT UDC PERFORMANCE EVALUATION

The testing of the end to end system includes UDR and SDN network management integrated with commercial devices as part of live network. Firstly, the mobile operator will register the IMSI of the NB-IoT devices in the HSS which is now part of the UDC and will indicate which slice is allocated to each device. The operator will indicate which devices will be allocated to URLLC slice. Next, the NB-IoT sensor is deployed in the field and register or attach to the network for the first time. In this first attach request, the MME must request all the information from the UDC. After this first attach the device information is stored locally in the MME database for subsequent authentication/authorization requests. After the initial attach the NB-IoT sensor is available and operator can

subscribe to events associated to the sensor or receive the data from the sensor.

With this setup we analyze the performance of the system with two types of devices to show the effect of the information model added to UDC as shown in Table 1. The first type of devices is normal UE that use existing 3GPP defined AVPs for traditional user subscription. For the second type of devices the MME will emulate S6a commands coming from NB-IoT including the newly defined AVPs for sensor subscriptions.

TABLE I. CASES WITH DIFFERENT NUMBER OF NB-IOT DEVICES AND TRADITIONAL UE

#	Traditional UE pre-registered in UDR (a)	NB-IoT devices pre-registered in UDR (b)	Total ULR commands sent to UDR (c)	ULR commands/ sec per MME for Traditional UE (d)	ULR commands/sec per MME for NB-IoT dev. (e)
1	1000	1000	10000	50	0
2	1000	1000	10000	0	50
3	2000	2000	10000	50	0
4	2000	2000	10000	0	50
5	5000	5000	10000	50	0
6	5000	5000	10000	0	50
7	1000	1000	10000	500	0
8	1000	1000	10000	0	500

^a Each traditional UE is registered in UDR with own separate EPS service profile.

^b Each NB-IoT device is registered in UDR sharing the same EPS service profile.

^c The ULR commands sent to the UDR are split between the two MME emulators.

^d Each MME emulator sends N ULR commands/second which is equivalent to have N devices attach/second

In addition to the difference in AVPs we assume that all the IoT devices had bulk subscription for the same EPS service. Thus, the EPS Service Profile data fetched from the DS during processing of each S6a command for each IoT device is the same EPS Service Profile entry.

The performance test will measure the delay in accessing device information during the attach process. This transaction consists of S6a command named Update Location Request (ULR) that MME sends to the HSS Application FE when a new device registers or attaches to the network. This command is chosen because the AVP in the message is modified to support IoT devices compared to the command used by normal subscriber's UE. Moreover, the ULR is delay sensitive since the UE should receive an attach response within 15seconds according to the timer T3410 defined in 3GPP specifications [9]. The transport protocol used on the S6a interface is Stream Control Transmission Protocol (SCTP).

For IoT devices, 24 entries (i.e. EPS service profile entries) that are shared by all IoT devices are inserted in directory server database. Additionally, one entry (i.e. IMSI information entry) is inserted for each IoT device. Whereas for traditional users, a total of 24 entries are inserted in to directory server database for each traditional user. Additionally, one entry (i.e. IMSI information entry) is inserted for each traditional user.

In the performance the transmission delay and the propagation delay are insignificant. This is because the distance between the machines is less than 1m and the link capacity interconnecting them is 1Gbps which is very high compared to the Update Location Request/Answer command packet sizes.

For analyzing the delay, ULR and Update Location Answer (ULA) command packets are captured using tcpdump on the machines running the HSS FE and the 389 DS. Then the captured packets were analyzed using network protocol analyzer tool Wireshark.

This test case shows that the UDR has severe limitations for managing IoT devices where there is a high amount of subscriptions (i.e. 5000 traditional users and 5000 IoT devices). The results show when the system is stable under load, so it can be used for both traditional and IoT users. The results show the UDR system performs badly under a higher load condition. The results show the system performs badly and it can affect the attach request timer requirement.

After this finding, a further analysis was done on the overall system by using a linux system monitoring tool vmstat to gather current system information in two cases. In the first case neither the LDAP server nor the EPS HSS FE were running. In the second case both the LDAP server and the EPS HSS FE were running, and Test Case #1 was performed. The first case was done to differentiate the effect, on the system information, of running Test Case #1. The result of the analysis shows the block sent to a block device increased significantly every time those high jitters occur. This shows the LDAP server is writing significantly more data into the disk. And generally, writing to or reading data from disk degrades LDAP server performance. This indicates those jitters could be caused by the LDAP server.



Fig. 5. Testbed results with packet delivery in different network slices.

Another observation in Figure 5 results is the impact of the SDN managed network slice with the packet delivery. The results show that the non-URLLC slice might have packet loss when congestion increases.

VI. CONCLUSIONS

The main goal of this study was the study of 3GPP proposed UDC system for user data storage system considering IoT devices. The designed storage system allows bulk subscription of IoT devices and additionally facilitates management of IoT devices. As there is no existing standard EPS system that can utilize the designed system, an EPS HSS Application is developed to test the system. A prototype was developed using an LDAP 389 Directory Server to implement the user data storage. EPS service profile was defined for traditional and IoT devices. These entries were inserted in the LDAP server and the system was tested by sending ULR commands to the EPS HSS Application. The ULR commands are sent to the LDAP server by the EPS HSS Application. The delay between the ULR commands received by the Application and the corresponding ULA message sent by the EPS HSS Application is measured. This delay is analyzed to test the performance of the prototype system.

In addition to the extended UDR a SDN based controller is used to create the network slices. The UDR stores the information about devices that will be allocated each network slices. The SDN controller enforces different policies to the network switches to ensure the URLLC slice will maintain the required network resources to guarantee low latency and reliability. The result of the test shows the feasibility of the design and URLLC slice isolates the NB-IOT traffic from selected users.

Overall, the result shows the feasibility of designing a user data storage system for future mobile networks that besides managing the traditional HSS data takes into consideration the needs of IoT devices. The prototype including SDN controller also demonstrates the effective deployment of URLLC network slice for communication that requires low latency and high availability.

REFERENCES

- [1] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529-551, April 1955. (references)
- [2] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
- [3] I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
- [4] K. Elissa, "Title of paper if known," unpublished.
- [5] R. Nicole, "Title of paper with only first word capitalized," *J. Name Stand. Abbrev.*, in press.
- [6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
- [7] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.
- [8] 3GPP, "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol," TS 29.272 V13.8.0, Jan. 2017.
- [9] 3GPP, 2017. "Non-Access-Stratum(NAS) protocol for Evolved Packet System(EPS); Stage 3". TS 24.301, 3rd Generation Partnership Project