5G Evolution of Cellular IoT for V2X

Andreas Kunz[1], Lewis Nkenyereye[2], JaeSeung Song[2*]
Lenovo, Oberursel, Germany[1]
Sejong University, Seoul, Republic of Korea[2]
email: akunz@lenovo.com, nkenyele@sejong.ac.kr, jssong@sejong.ac.kr[*]

Abstract —The Third Generation Partnership Project (3GPP) is currently studying the extension of the Cellular Internet of Thing (CIoT) towards the newly defined 5G architecture. While Machine Type Communication (MTC) was defined before only for the Evolved Packet System (EPS), new functionality is defined already in 5G Phase 1 that could be utilized also for CIoT in 5G, which officially is part of 3GPP 5G Phase 2. This paper introduces the new features in the 3GPP 5G architecture as well as the protocol enhancements and latest developments on the Machine to Machine Communication (M2M) platform with CIoT to satisfy the network and communication requirement. Based on a traffic accident data collection scenario within the automotive industry under consideration of Vehicle to Everything (V2X) communication, we discuss how an M2M platform can be deployed to fulfill the ultimate objectives of 5G cellular IoT. We consider oneM2M, a global initiative that aims at providing a unique architecture for M2M interoperability as a special form of M2M/IoT platform. We describe how oneM2M platform can be adopted for the traffic accident use case to provide interfaces that facilitate the communication between the vehicle-mounted devices, the V2X Control Function and V2X application server.

Index Terms – CIoT, 3GPP, 5G, IETF, V2X, oneM2M

I. INTRODUCTION

Already in 3GPP Release 10, the 3GPP system architecture group (3GPP SA2) started to work on Machine Type Communications (MTC) for Universal Mobile Telecommunications System) and Long Term Evolution (LTE) core networks [1][2][3]. The main focus at this time was basically the prevention of system overload and signaling congestion due to the expected huge number of devices (User Equipment, UE). The feature evolved over the years with continuous improvements in every Release up to Release 15. The latest version of the MTC specification 3GPP TS 23.268 [1] has an extensive set of features as follows:

- Device Triggering
- Packet Switched (PS)-only Service Provision
- Core Network assisted RAN parameters tuning
- UE Power Saving Mode
- Group Message Delivery
- Monitoring Events
- High latency communication
- Support of informing about potential network issues
- Resource management of background data transfer
- Evolved UMTS Terrestrial Radio Access (E-UTRAN) network resource optimizations based on communication patterns provided to the Mobility Management Entity (MME)
- Support of setting up an Application Server (AS) session with required Quality of Service (QoS)
- Change the chargeable party at session set-up or during the session
- Extended idle mode Discontinuous Reception (DRX)
- Non-IP Data Delivery (NIDD)
- Support of Packet Flow Description (PFD) management via Service Capability Exposure Function (SCEF)
- Mobile Subscriber Integrated Services Digital Network Number (MSISDN)-less Mobile Originated (MO)-Short Message Service (SMS) via T4 (see Fig. 1)
- Enhanced Coverage Restriction Control via SCEF
- Multimedia Broadcast Multicast Service (MBMS) user service for UEs using power saving functions
- Enhancements to Location Services for CIoT
- MBMS user service for NarrowBand (NB)-LTE or LTE-M (Machine) UE categories
- Network Parameter Configuration via SCEF

All those features are limited to the Universal Mobile Telecommunications System (UMTS) and Evolved Packet System (EPS) and cannot be used currently within the new 5G system, except the Non-IP data transport feature. Fig. 1 depicts the specified Release 15 MTC architecture for the non-roaming scenario for simplicity with the different control plane and user plane connectivity options of the MTC UE to the network, of course not all need to be supported by the UE. The grey highlighted functional entities were introduced in the context of MTC in 3GPP and are described below. The UE can be connected to the mobile network via different 3GPP Radio Access Network (RAN) technologies, i.e. Global System for Mobile Communications (GSM), General Packet

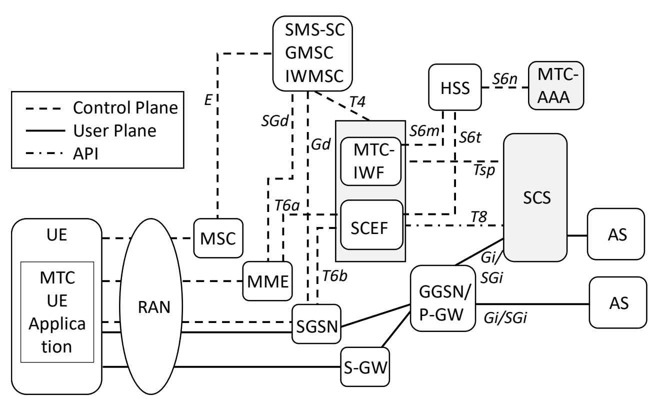

Figure 1: 3GPP MTC Release 15 Architecture

Radio Service (GPRS), UMTS or LTE to the mobile core network. LTE further offers radio optimization for low power (LTE-M) or as a different radio technology (RAT) a narrow band version (NB-LTE) for achieving battery lifetimes up to 10 years. MTC offers different transport possibilities for different use cases either via control or user plane. A UE can be triggered via SMS for a certain action and could transmit data via SMS or via IP or Non-IP data. SMS can be sent via the Mobile Switching Centre (MSC) or the Mobility Management Entity (MME) to the SMS-Service Centre (SMS-SC) and then to the interworking function (MTC-IWF/SCEF) to the Application Server (AS), which may belong to a 3rd party. The MTC-IWF was first specified in Release 10 and evolved to the SCEF in later Releases for exposing 3GPP network functionality to the MTC service provider/AS. IP data can be transferred via the gateway nodes Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) in UMTS/GPRS or via Serving Gateway (S-GW) and Packet Gateway (P-GW) in EPS. Non-IP data is encapsulated in Non-Access Stratum (NAS) signaling between UE and MME and can be then further transported via the SCEF to the SCS/AS or via SGW/PGW (reference point not shown in Fig. 1). Non-IP Data delivery within a Point to Point (PtP) tunnel to the gateway is supported in EPC to the PGW but also already supported generally in 5G to the User Plane Function (UPF).

The remainder of the paper is organized as follows. Section II provides and overview of the new 5G architecture and the new concepts compared to EPC and Section III describes the features of 5G Phase 1, which could be applicable to CIoT as well as an outlook on current work of the ongoing study in 3GPP. Section IV explains the CIoT service layer CIoT and Section V the CIoT example use case in the V2X domain. Finally, Section VI provides a conclusion and an outlook to the upcoming work in 3GPP and oneM2M.

II. 5G Architecture Overview

The 3GPP 5G architecture is specified in TS 23.501 [4] and its procedures in TS 23.502 [5]. Obviously, the major changes to the EPC as specified in TS 23.401 [6] are the concept of network slicing and the Software-Based Architecture (SBA). A network slice is defined in [4] as “a logical network that provides specific network capabilities and network characteristics”. Further SBA paves the way to ´the virtualization of network functions, easier extensibility, modularized services of each network function and openness for exposure of network information to 3rd parties.

Fig. 2 shows the non-roaming 5G architecture in SBA representation. The 5G architecture has a clear split between control plane and user plane functionalities. The RAN node or also called gNB is the 5G base station for 3GPP access. It has to be noted that for non-3GPP access, e.g. WLAN access, the current architecture can be applied as well with an additional interworking function for untrusted access. A UE can now send Non-Access Stratum (NAS) signaling not only via 3GPP access. The User Plane Function (UPF) is the gateway node to the Data Network (DN), which could be operator services like the IP Multimedia Subsystem (IMS), internet access or 3rd party services. The Access and Mobility Management Function (AMF) and the Session Management Function (SMF) provide the services similar to the MME in EPC, e.g. terminate the NAS signaling of the UE via N1, idle or connected mode mobility or protocol data unit (PDU) connectivity service. The Authentication Server Function (AUSF) takes care of the authentication of the UE and Unified Data Management (UDM) is responsible for subscription related information. The Network Function (NF) Repository Function (NRF) supports the service discovery of NFs and maintains the NF profiles of the available NF instances. The Network Slice Selection Function (NSSF) selects the set of Network Slice Instances serving a particular UE. The Policy Control Function (PCF) provides policy rules to CP functions for enforcement, the Application Function (AF) provides application related information to the policy framework for policy control. The Network Exposure Function (NEF) is somehow the 5G version of the SCEF in EPC and is responsible for exposure of capabilities and events, secure provision of information from external application to 3GPP network and translation of internal-external information.

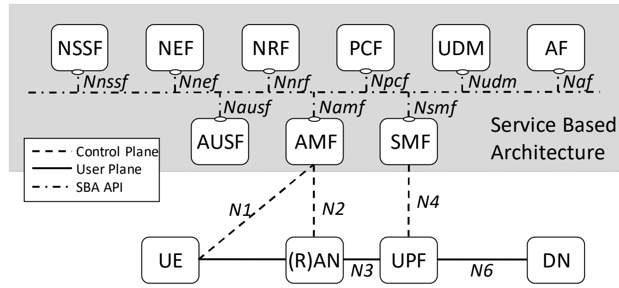

Figure 2: 5G Architecture in SBA representation

III. CIoT Concepts in 5G

A. Non-IP transport in 5G

From the beginning, different transport modes were considered in the 5G architecture [4]. A UE can request the establishment of a Packet Data Unit (PDU) Connectivity Service via PDU Sessions to exchange of PDUs between a UE and a data network identified by a Data Network Name (DNN). A PDU Session can support one of the following PDU Session types: IPv4, IPv6, IPv4v6, Ethernet, Unstructured. The unstructured PDU Session type is corresponding to the Non-IP transport mechanism and is achieved via different Point-to-Point (PtP) tunneling techniques based on UDP/IP encapsulation to transmit unstructured data to the destination (e.g. application server) in the DN via the N6 reference point.

B. Mobile Initiated Connection Only (MICO) Mode

A UE may register to the network with a MICO mode indication, the AMF then will then perform the relevant authorization of the use of the feature based on several parameters. The AMF serving area may be the whole PLMN (Public Land Mobile Network) and it may set the "all PLMN" registration area in order to prevent any mobility related re-registrations to the same PLMN. Periodic re-registration are still performed. The UE in MICO mode is only reachable

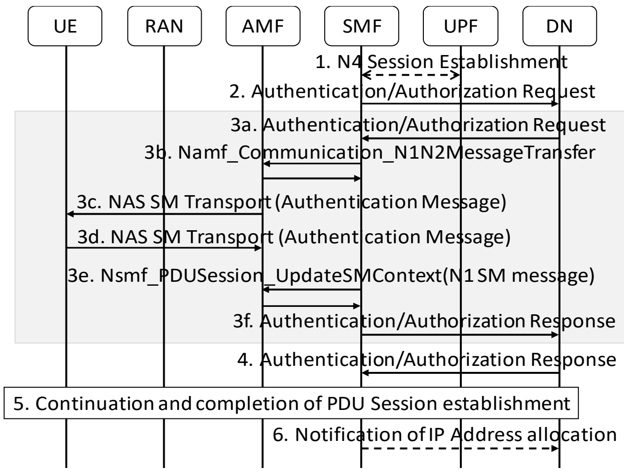

Figure 3: Secondary Authentication Call Flow

when it is in Connected mode in the AMF and it does not listen to any paging messages.

C. Network Exposure

Capabilities of network functions can be exposed to external application server via the NEF. Three capabilities for exposure were currently defined: *Monitoring*, *Provisioning* and *Policy/Charging* capabilities.

Monitoring Capability: specific events for UE in 5G System are monitored. The capability consists of identification of the suitable 5G network function for the event, its configuration, detection and reporting to the authorised external party.

Provisioning Capability: UE behavioural information can be provisioned via the NEF to a NF. The capability consists of authorisation of the provisioning external third party, receiving, storing and distributing the information to relevant NFs.

Policy/Charging Capability: based on the request from external party, the QoS and charging policy for the UE is used, e.g. request for session and charging policy, enforce QoS policy, apply accounting functionality.

D. Secondary Authentication

A secondary authentication/authorization can be performed during the establishment of a PDU Session to a DN and may perform only DN authorization without DN authentication as shown in Fig. 3 [5].

First, the UE provided in a previous PDU Session Establishment Request the authorization/authentication information to a DN-specific identity (SM PDU DN Request Container) and N4 session establishment between SMF and UPF is triggered (Step 1). The SMF acts like an EAP authenticator and sends the SM PDU DN Request Container to the DN-AAA (Authentication Authorization Accounting) server via the UPF (Step 2). Then the following steps are expected:

- Step 3a: The DN-AAA server sends a Authentication/Authorization message towards the SMF via the UPF.
- Step 3b: The DN Request Container information is sent with the `Namf_Communication_N1N2MessageTransfer` service operation to the AMF.
- Step 3c: The AMF sends the N1 NAS message to the UE.
- Steps 3d-3e: The UE responds with a N1 NAS message containing DN Request Container information to the AMF and further to the SMF by invoking the `Nsmf_PDUSession_UpdateSMContext` service operation.
- Step 3f: The SMF sends the DN Request Container information (authentication message) to the DN-AAA server via the UPF.

The DN-AAA server confirms the successful authentication/authorization of the PDU Session (Step 4). The PDU Session establishment continues and completes (Step 5). In the last the SMF notifies the DN-AAA with the IP address allocated to the UE together with the Generic Public Subscription Identifier (GPSI), if requested or configured in Step 4.

E. Current 3GPP Phase 2 Study Items

3GPP TS 23.724 [7] defines three main objectives of CIoT. First objective is to enable CIoT/MTC functionalities in 5G Core Network (CN). This means that the existing CIoT/MTC functionalities from the pre-5G networks are enabled in 5G CN with potential connectivity to (WideBand) WB-EUTRA (eMTC) and/or NB-IoT for 5GS capable devices. For example, selected key functionalities are monitoring, non-IP data delivery, small data transmission, additional power saving, overload control (as relevant in 5G CN), high latency communication, reliable communication and equivalent to group communication and messaging. Current 5G Phase 1 specification (TS 23.501 [4]) supports already the network attach/registration without PDN connection as well as non-IP PDN Connection type. In addition, regulatory requirements have to be fulfilled at the same level as in EPC.

The second objective is to support the co-existence and migration from EPC based eMTC/NB-IoT to 5G CN. Solutions are studied where the same service is offered to some UEs connected to EPC and some UEs connected to 5G CN. Only solutions are considered that support 5G-NAS signaling to access the 5G CN, i.e. no EPC NAS for 5G-CN is allowed, which rules out legacy IoT devices support in 5G.

The last objective is to enhance 5G System to address 5G service requirements (see TS 22.261 [8] and TR 38.913 [9]). Two requirements have been identified with respect to those:

- The association between subscription and address/number of an IoT device should be changeable
- Restricted Registration procedure should be supported to allow IoT device provisioning for eSIM profiles

IV. IoT Service Layer with CIoT

In this section, we introduce an overview of interworking function and architecture between 3GPP and IoT service layer

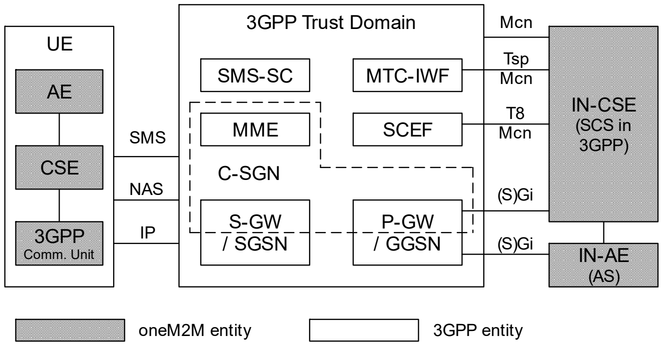

Figure 4: 3GPP-oneM2M Interworking Architecture

platform. In particular, this section is written from IoT service layer perspective which explains how IoT service layer sees 3GPP 5G CIoT and interconnects to the CIoT core for IoT services.

A. Background of 3GPP Interworking

Considering IoT devices having ubiquity of standards-based mobile connectivity, IoT service layer standards bodies are looking at an interworking service to be connected with 3GPP CIoT. oneM2M[1] is a partnership project for standardizing specifications for IoT common service layer platforms [10][11]. Similar to 3GPP, oneM2M is a project established based on an agreement between eight standards development organizations (SDOs), Telecomm. Technology Association (TTA), Association of Radio Industries and Businesses (ARIB), Alliance for Telecomm. Industry Solutions (ATIS), China Communications Standards Association (CCSA), Electronics Telecomm. Standards Institute (ETSI), Telecomm. Industry Association (TIA) and the Telecomm. Technology Committee (TTC).

Recent progress in oneM2M to collaborate with 3GPP Core Network is to include the Service Capability Exposure Function (SCEF) API. This API exposes underlying network services to oneM2M service layer platforms and vice versa. Thanks to the SCEF API, IoT service layer and 3GPP Core Network can provide more intelligent services than before. For example, IoT applications running on top of oneM2M service layer platform can share application specific information with the 3GPP Core Network to trigger sleeping IoT devices awake.

B. Overview of 3GPP-oneM2M Interworking

In oneM2M, the Common Service Entity (CSE) provides common service IoT control functions in IoT/M2M devices (e.g., Cloud server, gateway and end devices) while an Application Entity (AE) represents an IoT application. IoT servers, which is typically located on a cloud are represented as an Infrastructure Node (IN). The Service Capability Server (SCS) in the 3GPP reference architecture can be mapped to IN-CSE in oneM2M as shown in Fig. 4. IN-CSE connects to the 3GPP Trust Domain to communicate with UEs which is equipped with oneM2M applications via three interfaces, i.e., `SGi`, `T8` and `Tsp`. These interfaces are designed to provide various protocols (IP for `SGi`, RESTful API for `T8` and Diameter for `Tsp`) used by IoT applications.

In order to define interworking with 3GPP network, oneM2M [12] introduces how oneM2M entities can utilize IoT/M2M service functions provided by 3GPP Core Network. For example, as SCEF exposes 'Monitoring', the specification describes how IN-CSE communicates with the 3GPP SCEF entity via `T8` interface (which is `Mcn` interface in oneM2M). Similarly, a 3GPP UE hosted oneM2M AE and CSE can use a Group Messaging service (via MBMS) by the 3GPP Communications Unit.

As oneM2M service platform is designed based on RESTful, a set of APIs defining the related procedures and resources for the interaction between the SCEF and the IN-CSE (SCS) are standardized on `T8` interface. Two specifications, 3GPP TS 23.682 [1] and 3GPP TS 29.122 [13], are developed for the T8 APIs to describe the architectural level description and the protocol level description of the T8 APIs, respectively. From the oneM2M side, a specification is developed defining how an IN-CSE interworks with a SCEF via the T8 APIs [12]. For the services provided by SCEF, detailed requests and responses exchanged between the IN-CSE and the IN-CSE are specified. In addition, detailed mechanisms how an IN-CSE generates and processes T8 requests and responses are described. In the next section, Group Management Interworking which is one of the interworking services defined in both 3GPP and oneM2M is explained to show how interworking is performed.

C. Group Management Interworking

The Group Management (GMG) CSF is defined in oneM2M to handle group related IoT/M2M services. Various features such as creation of a group, management of group members, performing fanout operations to group member resources are defined in this group management service. In the group management interworking function, oneM2M application can get a benefit when the same content is sent to the members of a group that are located in a particular geographical area as 3GPP provides MBMS capabilities.

Let us consider a situation where a lot of UEs (with oneM2M AE/CSE) are located in a particular area for example a sport stadium with a big football match. If an IoT application should send an urgent message to the UEs at the stadium, the application can send the message using 3GPP MBMS multicast capability provided by SCEF and BM-SC as specified in 3GPP TS 29.122 [13]. Thanks to the MBMS capability, the group message from the IoT application does not need to be duplicated at the underlying network.

Fig 4. describes how a group message delivery is performed using MBMS interworking. In this procedure we assume that a MBMS group has already been established so that 3GPP core network and oneM2M group hosing CSE knows required information to deliver a group message (Step 1). The IN-

[1] http://www.onem2m.org

AE/CSE sends a group message delivery request with the group resource identifier and the payload to the Group Hosting CSE (Step 2). If the message contains proper parameters such as the `multicastType` is configured with `3GPP_MBMS_group`, the group Hosting CSE sends the Group Message Delivery Request to the SCEF to activate the MBMS bearer (Step 3). The request shall contain the specified information in 3GPP TS 29.122 [13] including `tmgi` (specifying the MBMS network bearer), `groupMessagePayload` (the actual value to be delivered), and `messageDeliveryStartTime` (specifying the next start time of the time intersection). The MBMS bearer activation procedure is then processed by the 3GPP Core Network [6] followed by replying back the Group Message Response to the Group Hosting CSE (Steps 4 and 5). Now all the members UEs of the given group receive the group message based on the 3GPP MBMS delivery procedures (Step 6 and 7). After a successful delivery, the member hosting CSE replies response message within a certain time to the Group CSE where the received response messages are aggregated and returned to the IN-AE/CSE (Steps 8 and 9).

V. End-To-End CIoT Use Case in Vehicle Domain

In the following section, we first overview the significance of CIoT to support V2X communications for the vehicular domain. We then present a traffic accident collection information system as a vehicular domain use case. The use case highlights how we can integrate M2M platform with 5G cellular IoT to efficiently support V2X communications.

A. CIoT in Vehicular Domain

Lately, cars manufacturers also referred as Original Equipment Manufacturer (OEM) are equipping the modern vehicles with several sensors such as Vehicle Speed Sensor (VSS), Gas leakage sensors (GLS), Vehicle Noise Sensors (VNS), Alcohol Sensor (ALS) [14]. However, the information within the collected data is not fully exploited. Therefore, connecting the future vehicles to the internet and other peer devices (vehicles, smartphones or infrastructures) to form IoT is a promising paradigm. Nevertheless, the vehicles come with additional challenges due to several factors including the speed and high mobility. In addition, the OEMs have to integrate the services and applications which currently face the following issues among others:

- *Communication*: The 3GPP TS 23.285 [15] within the Release 14 specifies V2X features that do not provide adequate solutions for the communication between the V2X Application Server (V2X AS) and the (UE). Moreover, the communication between the V2X AS and V2X Control Function requires an efficient IoT platform to provide secure and efficient M2M communications
- *Interworking*: In the conventional IoT, different standards bodies are providing guidelines and specifications to create tailored IoT applications. However, this approach isolates the inter-working of the IoT applications due to the heterogeneity of the underlying platforms. Consequently, the OEMs for the car industry will face the same drawbacks for the internet of vehicles (IoV).

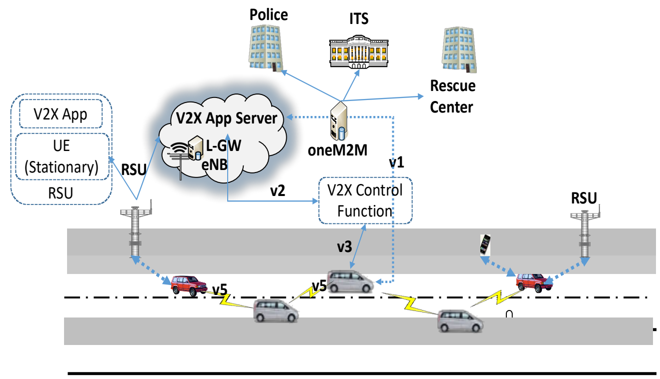

Figure 6: Traffic Accident Data Collection

B. Traffic Accident Information Collection Use Case

The ultimate goal of the Intelligent Transportation System (ITS) is to guarantee a better environment for the road users including the vehicles users and pedestrians. For instance, the road accidents cause traffic jam due to the towing of the vehicles involved in the accident (for severe accidents) but also due to the waiting for the appropriate services (police and insurance companies) to collect useful information related to the accident. However, in the future IoV paradigm, such duties could be performed by the surrounding vehicles as illustrated in Fig. 6. Additionally, rescue teams can timely intervene to the accident scene if some preliminary data are forwarded to them beforehand. Likewise, the police would efficiently handle the affected area if a general idea of accident location is provided to them. All these data can be provided by other entities within the accident site including other vehicles, pedestrian’s devices or fixed infrastructures.

The vehicle domain is made by the following entities:

- **ITS Authority:** It is in charge of for managing ITS applications and services using oneM2M Platform. All the participants in the ITS services subscribe to oneM2M for accreditation.
- **Police Station:** It is registered for ITS services using M2M platform and is in charge of traffic control
- **Rescue Center:** It registers to oneM2M platform for ITS services and is responsible for rescue operations.
- **ITS-Station (ITS-S):** It is an M2M Device mounted in the vehicles with computing capabilities. The ITS-S has a digital camera for capturing images or videos based on the driver commands. The ITS-S can communicate with oneM2M Platform using wireless network. The ITS-S can use DSRC to communicate RSUs.
- **Road Side Unit (RSU):** It is a fixed infrastructure installed on roads. The RSU can communicate with the inbuilt vehicle’s ITS-S using Dedicated Short Range Communication (DSRC); or to oneM2M platform using wired or wireless communications.

When an accident occurs, the ITS-S mounted in the vehicle performs several steps. First, an accident report is generated by the ITS-S. This step can be automatically launched for instance upon the opening of airbags. Also it can be manually activated by the driver. The traffic accident report is then signed by the ITS-S and sent to oneM2M platform. Note that the connection between the ITS-S and oneM2M platform can be done through a wireless network or via a nearby RSU using DSRC. The oneM2M platform verifies the signature on the accident report. The report will be securely sent to designated ITS service providers such as the Rescue Center or the Police. Lastly, the ITS service providers (Police or Rescue Center) might continue to communicate to ITS-S through oneM2M platform if additional data are required. Upon receiving all the essential data, the service providers agree on an intervention plan and head to the accident scene.

The oneM2M platform will facilitate the following in the described scenario as shown in Fig. 6:

- The platform will provide an interface that enables the communication between the V2X application server and ITS-S devices mounted in the vehicles
- The oneM2M platform shall facilitate the communication between the V2X Control Function and the V2X Application Server.

VI. Conclusion And Outlook

In this article, we introduced the recent 3GPP standards activities related to the extension of the cellular Internet of Things. The last development and protocol improvements which could be utilized for CIoT in 5G Phase 2 are presented. The integration of oneM2M as an M2M/IoT platform could speed up the achievement of 5G Phase 2 targeted performances. We use a traffic accident data collection use case to illustrate the need of M2M/IoT platform for the next cellular IoT. To achieve interoperability for 5G CIoT for V2X services, an M2M communication platform is required. We considered oneM2M platform, a worldwide standard initiated by major standards organizations to offer unique architecture for M2M communications in IoT. We also described a V2X use case for traffic accident information collection system. We highlighted several areas in which oneM2M platform can support by providing communication interfaces. Specifically, oneM2M platform can facilitate the communication between the V2X AS and vehicle devices and the communication between the V2X AS and the V2X Control Function. In future work, we aim to provide detailed architectures that show how oneM2M can be incorporated in 5G SBA and the core components that will be involved in the current LTE/EPC.

Acknowledgements

Prof. Song and Nkenyereye were supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-01456, AutoMaTa) and the Smart City R&D project of the Korea Agency for Infrastructure Technology Advancement (KAIA) grant funded by the Ministry of Land, Infrastructure and Transport (MOLIT), Ministry of Science and ICT (MSIT) (Grant 00000000000000).

References

[1] 3GPP TS 23.682, "Architecture enhancements to facilitate communications with packet data networks and applications", v15.4.0, Mar. 2018.
[2] T. Taleb, A. Kunz, "Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions," IEEE Commun. Mag., Mar. 2012.
[3] S. Husain, A. Kunz, A. Prasad, K. Samdanis, J. Song, "Mobile Edge Computing with Network Resource Slicing for IoT", Conference: IEEE World Forum - IoT (WF-IoT), Feb. 2018, Singapore.
[4] 3GPP TS 23.501 "System Architecture for the 5G System; Stage 2, (Release 15)", v15.1.0, Mar. 2018.
[5] 3GPP TS 23.502 "Procedures for the 5G System; Stage 2, (Release 15)", v15.1.0, Mar. 2018.
[6] 3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 15)", v15.3.0, Mar. 2018.
[7] 3GPP TR 23.724, "Study on Cellular Internet of Things (IoT) support and evolution for the 5G System", v0.2.0, March 2018.
[8] 3GPP TS 22.261 "Service requirements for next generation new services and markets" , v16.3.0, Apr. 2018.
[9] 3GPP TR 38.913 "Study on scenarios and requirements for next generation access technologies", v14.3.0, Aug. 2017.
[10] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, J. Song, "Toward a Standardized Common M2M Service Layer Platform: Introduction to oneM2M", IEEE Wireless Commun., Vol. 21, No. 3, Jun. 2014, pp. 20-26.
[11] J. Song, A. Kunz, M. Schmidt, P. Szczytowski, "Connecting and Managing M2M Devices in the Future Internet," Springer Journal of Mobile Netw. and Applications, Vol 19, Nov. 2014, pp. 4-17.
[12] oneM2M TS-0026, "3GPP Interworking", v0.8.1, Apr. 2018.
[13] 3GPP TS 29.122, "T8 reference point for Northbound APIs; (Release 15)", v15.1.0, Mar. 2018.
[14] S Olariu, I Khalil, M Abuelela, Taking VANET to the clouds. Int. J. Pervasive Comput. Commun.**7**(1), 2011, pp. 7–21.
[15] 3GPP TS 23.285 "Architecture enhancements for V2X services", v15.0.0, Mar. 2018