Interworking Architecture Between oneM2M Service Layer and Underlying Networks

Syed Husain[1], Andreas Kunz[2], JaeSeung Song[3], Takashi Koshimizu[4]

NTT DOCOMO, Tokyo, Japan[1&4]
NEC Laboratories Europe, Heidelberg, Germany[2]
Sejong University, Seoul, Korea[3]

Emails: shusain2016@gmail.com, andreas.kunz@neclab.eu, jssong@sejong.ac.kr, koshimizu@nttdocomo.com

Abstract — In the realization of end-to-end Machine-to-Machine (M2M) applications it is necessary to provide interworking architectures between the service layer platforms and underlying communication networks. The oneM2M and 3GPP standards organizations have recently taken the initiative to develop such interworking architectures. This paper aims to provide an overall view of these interworking architectures, which enables exposure of various underlying network services for M2M applications running on top of the service layer, such as device triggering, device location, device management, etc.

Index Terms – M2M, IoT, MTC, oneM2M, 3GPP, WiFi, LTE, Interworking.

I. Introduction

The Internet-of-Things (IoT), or more prosaically Machine-to-Machine (M2M), has received significant attention lately from both industry and academia as an emerging paradigm that manages billions of devices, gateways, sensors, and actuators connected to the Internet [1]. The work in [2] estimates that by 2020 there will be more than 20 billion devices on the IoT. The Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) technologies will enable constraint devices to stay connected and exchange information with other machines or M2M Applications. In the case of smart devices such as smart phones, existing networks such as 3G, WiFi, and Long Term Evolution (LTE) will provide an indispensable part of IoT. This will boost the traffic in cellular systems, for example, some telecom players [3] – [4] expect 1,000 times higher global traffic volumes in 2020 than in 2010.

Due to the current fragmentation of the M2M market, lately there have been many initiatives, alliances, and standardization efforts for allowing interoperability for offering a richer set of services compared to the traditional silos. Since many IoT/M2M capable devices require to be connected to M2M service platforms via underlying communication networks such as 3GPP mobile networks, M2M related standards have taken the initiative to support architectural interworking functions between the service layer platform and the underlying communication network. Two global joint initiative projects of European, U.S., Japanese, Korean, and Chinese telecommunications standardization organizations - oneM2M and the 3rd Generation Partnership Project (3GPP) - which produce global specifications for the M2M service layer and mobile networks respectively, are collaborating with each other to develop interworking functions and mechanisms.

oneM2M has collected a number of use cases that cover a wide area of industry segments, including enterprise, healthcare, and network management. In particular, some use cases such as healthcare (e.g., sending location information together with patient health data over 3GPP underlying network) and optimized M2M interworking (e.g., using data transmission interval of the mobile terminal in order to mitigate data traffic in the mobile network) show obvious benefits of supporting the underlying network interworking functions in order to provide enriched IoT services and optimize mobile network performance.

This article begins with an overview of existing M2M standard architectures for both the service layer platform and the 3GPP underlying network (Section II) followed by introducing multiple use cases for interworking (Section III). We then introduce an interworking architecture and required features such as identifier mapping and device triggering (Section IV). After that we present two detailed example procedures showing how individual function blocks are communicating with each other to support interworking (Section V). Finally, we conclude the article with a brief discussion for future standardization work (Section VI).

II. Existing M2M Standard Architectures

Before discussing detailed interworking functions and mechanisms between oneM2M and 3GPP systems, we need to understand the oneM2M service layer platform [5, 16] and 3GPP Machine Type Communications (MTC) architectures [4, 17].

A. oneM2M Service Layer Platform Architecture

As mentioned in Section I, oneM2M has developed one globally agreed architecture specification [7] for end-to-end M2M systems addressing many important M2M communication aspects, such as identification, addressing to reach target entity, management, registration, and security.

978-1-4799-7470-2/14/$31.00 ©2014 IEEE

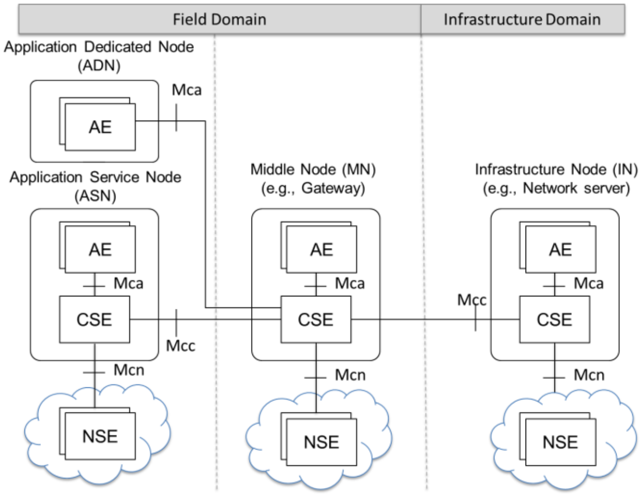
Field Domain
Infrastructure Domain
Application Dedicated Node (ADN)
AE
Mca
Application Service Node (ASN)
Middle Node (MN) (e.g., Gateway)
Infrastructure Node (IN) (e.g., Network server)
AE
Mca
CSE
Mcc
Mcn
NSE
AE
Mca
CSE
Mcn
NSE
Mcc
AE
Mca
CSE
Mcn
NSE

Figure 1: oneM2M functional architecture

Figure 1 shows the oneM2M functional architecture specified in oneM2M technical specification TS-0001 [7]. The architecture is composed of two domains, *field domain* and *infrastructure domain*. An M2M node is a generic concept that can have the role of an end device, a gateway, or a network server. End devices (e.g., sensors and actuators) and gateways are deployed in the field domain. M2M devices are connected to the M2M network server via underlying communication network. This connectivity is provided by various access networks such as wireless network e.g., 3GPP 3G/LTE and fixed line networks e.g., Asymmetrical Digital Subscriber Line (ADSL). In order to provide security services for M2M applications, the oneM2M architecture will include various security related features such as authentication, authorization, confidentiality and integrity.

Depending on the capabilities and deployment scenarios, there exist four different types of functional entities in the oneM2M system. As labeled in Figure 1, these are named as the Application Dedicated Node (ADN)/Application Service Node (ASN), Middle Node (MN), and Infrastructure Node (IN). Three M2M nodes (ASN, MN and IN) can comprise each of two logical functional entities: Application Entity (AE) and Common Services Entity (CSE). On the other hand, ADN usually resides in a constrained M2M device so that it only contains at least one AE without any CSE. The AE is not defined by oneM2M and it represents application logic of M2M solutions, while the CSE represents a set of Common Service Functions (CSFs) providing various M2M services and it is the entity specified by oneM2M. The oneM2M architecture for interworking with underlying networks defines an entity called Network Services Entity (NSE) that provides services from underlying networks, such as device triggering, location, and device management to the CSEs.

oneM2M focuses on specifying the interfaces used to interact with external entities (AEs and NSEs). More precisely oneM2M defines all interfaces for the reference points `Mca` and `Mcc`. In addition, it specifies how to use the underlying network specific interface that comprises the `Mcn` reference point. AEs communicate over the `Mca` reference point with the CSE. The `Mcc` reference point enables communication between two adjacent CSEs. The `Mcn` reference point connects a CSE with the service entities in the underlying network to enable a CSE to use services provided by the underlying networks.

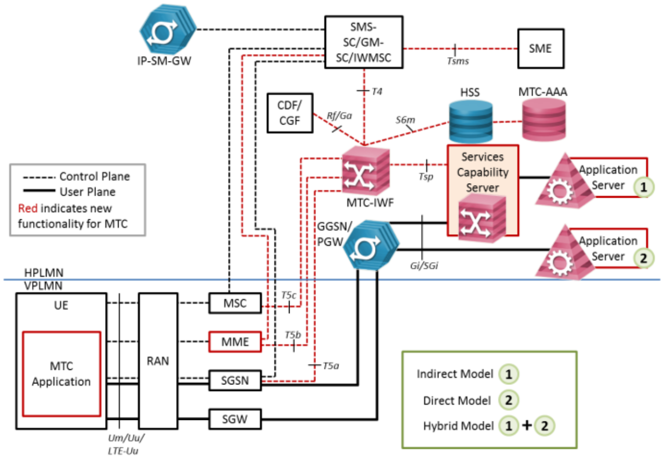

Figure 2: 3GPP MTC architecture

B. 3GPP MTC Architecture

3GPP initiated studies on MTC [8] in Release 10 but due to the broad scope of this project, many aspects of MTC were deferred from Release to Release. In the current 3GPP Release 13, work has been initiated on unfinished MTC aspects. One of these aspects is on providing end-to-end communication between the MTC application in the user equipment (UE), i.e., the MTC device, and the MTC application server, which could be located in the 3GPP network or outside. The 3GPP system provides the necessary functionality for data transport, subscriber management, device triggering, etc. The architecture of the 3GPP system can be found in [9] including a detailed description of the procedures and functional entities. A short explanation is given below.

Figure 2 shows the MTC architecture specified in Release 11 on top of the 3GPP network architecture. In this architecture the UE is connected via the radio interface to the Radio Access Network (RAN) called eNodeB (eNB). All signalling messages from the UE (and eNB) are sent to the Mobility Management Entity (MME), which is the main control node and responsible for all session and mobility related aspects, e.g., paging, location, handover handling, etc. The user plane data from the UE is routed from the eNB to the Serving Gateway (SGW) and further to the Packet Data Network Gateway (PGW), which provides connectivity to the internet and other networks. The Home Subscriber Server (HSS) is the database for all subscription related information, from where subscriber profiles are downloaded for network attached UEs to the relevant serving nodes, e.g., Serving GPRS Support Node (SGSN), Mobility Management Entity (MME), and Mobile Switching Centre (MSC). The MTC application server (AS) may be located in an external network and use a Service Capability Server (SCS) for additional value added services (e.g., device triggering, location). The SCS may belong to the Mobile Network Operator (MNO) or to the external network service provider. The MTC architecture foresees three different ways of communication between the AS and the 3GPP system, i.e., either indirect via an SCS and an interworking function (MTC-IWF), directly via user plane (requires knowledge of the UE's IP address), or a combination of both.

The major change to the system introduced in Release 11 is the MTC-IWF, which is responsible for PLMN topology hiding and relays/translates signalling protocols towards the SCS/AS. The currently specified main task is device triggering via Short Message Service (SMS) using T4 reference point. The T5 reference point to the serving nodes is shown in the architecture but left unspecified in Release 11. For this reason a new functionality for SMS via the MME got specified including SMS for devices with packet switch subscription only, which do not have Mobile Station International Subscriber Directory Number (MSISDN).

III. Interworking Use Cases

To provide some background material for our further discussion and a better understanding, we present couple of interworking use cases based on oneM2M and 3GPP specifications [10, 11, 12] covering use cases in energy management, enterprise, residential, healthcare, public services, transportation, etc. These use cases helped in the development of M2M service requirements, which eventually led to the development of necessary interfaces/protocols needed for deployment of standardized M2M services. The goal of oneM2M is to provide a horizontal common services platform that can be used in a standardized manner linking a multitude of dispersed application and devices through fixed and mobile access networks, e.g., 3GPP, 3GPP2, BBF, WLAN, Zigbee.

A. Overview of the use cases

Example of a healthcare use case: A heart patient goes through triple bypass surgery. This patient is hospitalized for a week. The doctors discharge the patient when he appears to have recovered and out of danger. Due to high insurance costs the patients are generally kept in the hospital to a minimum. What is required after such patients leave the hospital is to have a 24 hour monitoring service. With such M2M technologies is a myriad of sophisticated sensor devices possible: Sensing devices that measure patient's blood pressure, temperature, heart rate, and other bodily functions, can be attached to the patient before he is sent home. Such sensing devices will transmit all the required data to the server in the hospital 24/7. When there is any indication that the patient's condition is abnormal, a call (or page) to the doctor on duty is delivered through the use of the 3GPP underlying network. It is important that the exact location of the patient is known, before dispatching the ambulatory service. In this scenario, the sensing devices are connected through the 3GPP access network, and are sending data to the application server, which is interpreting the data. The underlying network is used to provide the location of the patient and call (or page) the doctor immediately. Moreover, if the sensing devices stop sending data for some reason (i.e., malfunction or detachment of the sensing device from the patient, the system detects this immediately and alarms are sent out to the hospital staff to contact the patient's home to determine what is wrong. All these actions are done using the M2M technology.

Example of a network optimization use case: Many IoT/M2M data generated by sensor devices can be characterized by transmission of small data packets. Measuring temperature from a thermometer sensor and sending the value to the network server only require small bytes. However, frequent small data transmission from a large number of sensor devices can easily cause the network to be overloaded by the mobile station changing its state frequently (i.e., between idle and connected modes). On the other hand, if the mobile terminal is continually stayed in the connected state unnecessarily, it causes higher power and radio resource consumption causing faster drain of battery.

In order to tackle these challenges, the underlying network such as 3GPP requires adjusting several configuration parameters such as the duration M2M device is staying in the connected mode, the interval for radio reception signal, etc., based on the data transmission interval of the mobile station. It is beneficial for the underlying network to be informed about a change of data transmission rate of a connected M2M device. However, such information is not easily detected by the mobile network since these are usually available at the service layer.

B. Background on use cases in 3GPP

Work was carried out in 3GPP in [10] to look into the use cases and potential requirements on the 3GPP system when exposing network information and capabilities to 3rd party applications in order to receive benefits from such applications. The normative phase on defining requirements is still ongoing on already standardized requirements for MTC in [11].

The 3GPP study differentiates two basic types of use cases:

1. M2M service enablement related use cases
2. Application related use cases

In the first category, two use cases were described:

- Communication patterns: this use case describes optimization for devices for which communication patterns were predicted. The MTC AS can exchange information with the 3GPP network via an API/interface and is authorized to provide control information (communication interval) for particular MTC devices. The information is stored in the subscription information of the MTC device and used in the mobile network to optimize its resources.
- M2M service provider setting for MTC Server communication with its MTC devices: the MTC Server

hosts a Service Enablement Framework (SEF, e.g., from oneM2M) of the MTC Service Provider. Specific 3GPP services can be exposed to the SEF so that the 3GPP operator can charge for them. Examples of such services include:

- Broadcast/multicast certain M2M data to a group of MTC devices.
- Providing QoS and Prioritization for individual M2M sessions to/from individual devices.
- Scheduling of suitable M2M traffic to a different time – e.g., in case of high network load.

The following use cases were explored in the second category of application related uses cases:

- Background traffic use cases: the network allows the application to schedule the background traffic transfers to avoid peak load.
- Use case on "Connection Properties Exposure": Connection properties relate to the currently available maximum data rate of the UE which is shared among all applications of the UE. The 3rd party application can use this information to optimize the data towards the UE.
- Real-time exposure of UEs footprint: The MNO provides a real-time snapshot of the UE footprint to the 3rd party. A real-time snapshot request may be amount and location of UEs in a specific area.
- Charging model choice: the 3rd party application can request different charging models for a specific user.
- Monitoring on application usage use cases: the application server requests e.g., location monitoring feature from the MNO for a specific UE and detects e.g., theft.

IV. ONEM2M INTERWORKING WITH UNDERLYING NETWORKS

In this section, we describe details of oneM2M interworking with underlying networks in particular for the 3GPP network. Since both oneM2M and 3GPP M2M/MTC architectures specify different identifier schemes, an interworking mechanism for mapping identifiers is also discussed.

A. General oneM2M Interworking with underlying networks

The oneM2M service layer platform has been architected with the capability to interwork with a wide variety of underlying networks. The functional entity that represents the services provided by the underlying network is called Network Services Entity (NSE) as depicted in Figure 1. The reference point `Mcn` allows communication between an underlying network and the CSE. The CSE can request a wide range of services offered by the underlying network. Some examples of such services are: messaging, payments, location, device triggering, and device management. As described in [12], the oneM2M architecture also offers a different reference point for Call Data Records (CDRs) related communication, which could result in an internal interface or an interface towards the underling network depending on the chosen architecture option.

The oneM2M services platform supports several underlying networks for the same system, this is particularly needed for entities that act like gateways and require communicating with two different underlying networks depending on what is the other endpoint in the communication. For example, for the use cases that we are considering of monitoring a patient, the mobile device of the patient can act as a gateway, which means that in the mobile device there should be a CSE installed together with a dedicated M2M application represented by AE. The mobile device by means of the AE collects the measurements from the dedicated sensors (e.g., blood pressure); the communication between the sensors and the mobile device could use a Bluetooth network, while the communication towards the correspondent AE in the infrastructure side (Application server belonging to the hospital) is using a 3GPP network. For the same use case, there might be other underlying network possible, as an example the mobile phone could use WiFi as alternative communication networks towards the infrastructure.

One of the characteristics of the oneM2M architecture is the ability to allow access to several different underlying networks and to provide to the application developers and service enablement providers the ability to manage all these underlying networks by means of the Communication Management and Delivery Handling (CMDH) CSF. The M2M service provider has the ability to define a profile and policies for each supported underlying network. Policies allow selecting the best communication path depending on preferences and availability of a specific network. Moreover, with CMDH CSF, the M2M service provider indicates if a message can be buffered, in case of current unavailability of a network, and how long the message can be buffered. The oneM2M common services platform defines several parameters that a M2M service provider can set in order to utilise the capabilities of the system and the underlying networks best according to the service. The details of those parameters are not discussed in this paper, since they depend on service and underlying network.

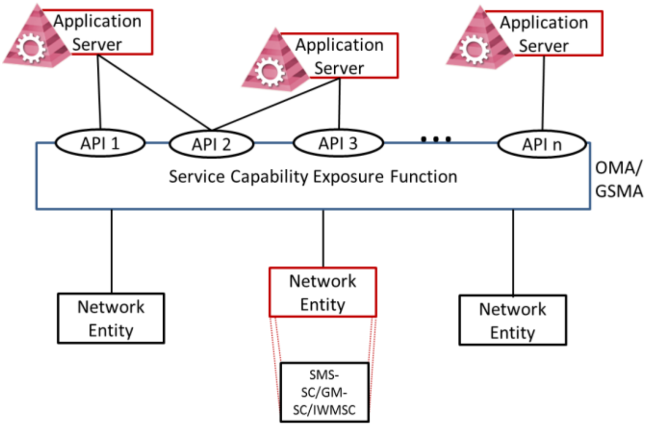

Figure 3: Potential Service Capability Exposure Architecture

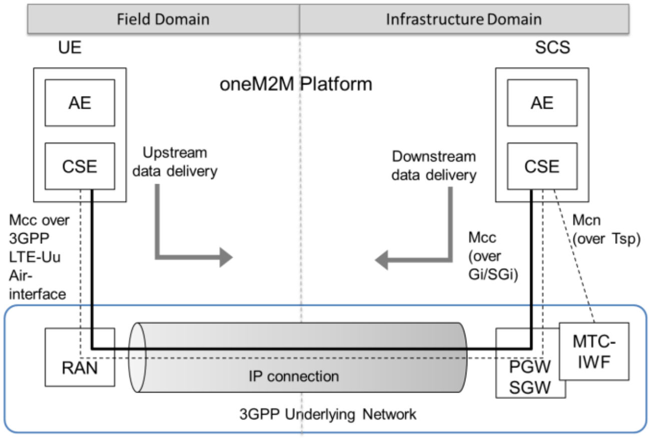

Figure 4: High-level interworking procedures

B. 3GPP as an underlying Network

Detailed activities are underway of being studied in 3GPP in [14]. Potential service exposure architecture may look like as the one shown in Figure 3, where a certain set of network capabilities are exposed to the AS by means of APIs.

In the above example an AS could use the API to send and receive SMS via the 3GPP network and the Service Capability Exposure Function is responsible to map and select the responsible SMS node (SMS-SC/GMSC/IP-SM-GW) in the operator network. ASs can be connected to several APIs that provide different network capabilities, e.g., location, SMS, MMS, payment etc., and the Service Capability Exposure Function provides the relevant functionality per API for authentication & authorization, policy enforcement, accounting etc.

C. Identifier Interworking

oneM2M defines a wide set of identifiers which are needed for the purpose of interworking and addressing. The defined identifiers are: *M2M Service Provider Identifier, Application Entity Identifier, Application Identifier, CSE Identifier, M2M Node Identifier, M2M Service Subscription Identifier, M2M Request Identifier, M2M External Identifier, Underlying Network Identifier, Trigger Recipient Identifier and M2M Service Identifier*. The identifiers that are relevant for interworking with 3GPP network are the M2M External Identifier (`M2M-Ext-ID`) and the Trigger Recipient Identifier (`Trigger-Recipient-ID`).

The `M2M-Ext-Id` is generally used by the M2M service provider to identify the device in the 3GPP network where a specific CSE is residing. Such identifier could be for example an `MSISDN` or assume the value of the external identifier as defined in [8] and [15]. The external identifier assumes the form of `<Local identifier>@<domain identifier>` and uniquely identifies the UE in a 3GPP network. Every communication happening on the `Mcn` reference point (see Figure 1) would require the `M2M-Ext-Id` for requests towards the UE/CSE. The `M2M-Ext-ID` will be provided over the `Tsp` interface (see also Figure 2) between the CSE and the MTC-IWF. `Tsp` interface offers a triggering request [8] which allows the M2M Service Provider to contact a CSE (UE for 3GPP) without active communication between the CSE (SCS for 3GPP) in the infrastructure domain and the CSE (UE for 3GPP) in the field domain (i.e., the current UE's IP address is unknown to the CSE in the infrastructure domain). In order to issue this request, the M2M Service Provider needs to provide the `Application-Port-Identifier` over `Tsp` for addressing the proper entity in the UE. The `Trigger-Recipient-ID` is the identifier from oneM2M that will map to the Application-Port-Identifier and in general it could address a CSE or a AE.

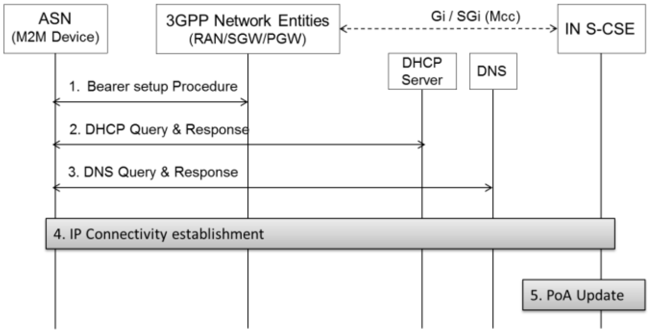

Figure 5: ASN CSE initiated interworking procedures

V. INTERWORKING PROCEDURES

In this section, we introduce a set of interworking procedures. We describe a generalized oneM2M and underlying network procedures followed by detailed procedures for interworking with 3GPP.

A. General oneM2M Procedures

As shown in Figure 4, the application entities residing on the M2M device, on one end, and on the oneM2M infrastructure node, on other end, need to have IP connectivity established between them in order to be able to converse and exchange data. For the M2M devices that are served by the 3GPP radio access network (RAN) this IP connectivity is established through the 3GPP underlying network. The SCS on the oneM2M Infrastructure Domain can initiate IP connectivity towards the UE in the oneM2M Field Domain when downstream data has to be delivered. On the other hand the M2M device can also initiate IP connectivity (if not already established) towards the SCS for upstream data delivery to the application servers. Figure 4 shows the essential oneM2M and 3GPP system entities/interfaces that enable this IP connectivity. In this section two detailed procedures are described for the establishment of IP connectivity between CSE in the field domain and the CSE in the infrastructure domain.

Upstream (Field Domain CSE initiated, Figure 5): Subsequent procedures are triggered either when the CSE in the field domain powers on, or resulting from device triggering, or as a consequence of an AE registered to the CSE requests to perform a RESTful CRUD (`Creation`,

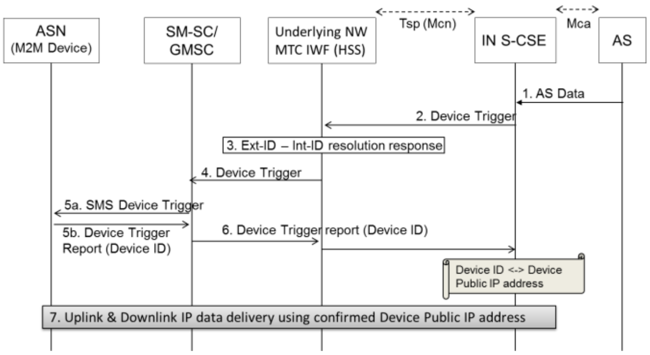

Figure 6: AS initiated interworking procedures

`Retrieve`, `Updating` and `Deletion`) operation on a resource residing on a target CSE. Establish 3GPP bearer(s) if not already available by using the procedures available in the 3GPP network.

The CSE sends a query to a Dynamic Host Configuration Protocol (DHCP) server to find a particular Domain Name System (DNS) server IP address. The DHCP server responds with the IP address of a corresponding DNS server. Additionally, it is also possible to include one or a list of domain names, i.e., Fully Qualified Domain Name (`FQDNs`) of target CSEs.

The CSE performs a DNS query to retrieve the target CSE(s) IP addresses from which one is selected. If the response does not contain the IP addresses, an additional DNS query is needed to resolve a `FQDN` of the target CSE to an IP address. After reception of domain name and IP address of the target CSE, the CSE can initiate communication towards the target CSE via the IP connection. The target CSE at this time shall be informed of the just established `Trigger-Recipient-ID` of the target CSE to use for subsequent downstream communication triggering.

Once the M2M Service Connection (`Mcc`) is established, in the target CSE shall update the CSE-PoA attribute field (Point of Access, e.g., IP address of the CSE) of the CSE with the new established IP address. The target CSE holds the state information and needs to be informed when the connection is closed.

Downstream (Infrastructure Domain CSE initiated procedures, Figure 6). This procedure is generally triggered by an AE in the infrastructure domain which requests to perform one of the Restful CRUD operations on a resource residing on a target CSE in the field domain, the request is sent via the `Mca` reference point to the CSE. The request from AE includes the address (URI) of the target resource. If a new connection needs to be set up and the CSE has no contact details for a MTC-IWF, it may determine the IP address(es)/port(s) of the MTC-IWF by performing a DNS query using the `M2M-Ext-ID` assigned to the target CSE, or using a locally configured MTC-IWF identifier.

The CSE buffers the original request information and sends the Device Trigger Request message that contains information as specified in 3GPP TS 23.682 [6]. Such information includes:

- `M2M-Ext-ID` or `MSISDN`;
- `SCS-Identifier`, (is set to the `CSE-ID` of the CSE in the infrastructure domain);
- Trigger reference number (a generated number used to correlate the request with the response);
- Validity period, (which indicates how long the request is valid);
- Priority (this field allows to set the priority on or off);
- `Application Port ID`, (is set to the target CSE `Trigger-Recipient-ID`, which would contain the `CSE-ID` of the target CSE since it is the triggering application addressed in the device from 3GPP point of view);
- Trigger payload, (optional information can be set to the payload).

The MTC-IWF initiates the T4 trigger delivery procedure according to the TS 23.682 [6], based on the information received from HSS and local policy. As a result of the device triggering procedure the target CSE is initiated based on the received Application Port ID by the UE.

The MTC-IWF sends the Device Trigger Report message (containing the `M2M-Ext-ID` or `MSISDN` and trigger reference number) to the CSE with a cause value indicating whether the trigger delivery succeeded or failed and the reason for the failure. The CSE acknowledges to the MTC-IWF with the conformation of the received Device Triggering Report. Once the connection over `Mcc` is established, the `CSE-PoA` attribute of the target CSE shall be updated at the CSE with the new established IP address of the target CSE.

After all the steps in Figure 6 are performed successfully, the communication is established and now the initial request with the information stored and buffered by the CSE at Step 1 can be re-issued over the reference point `Mcc`.

In the flow presented above not all parameters allowed in the Device Triggering Request message from 3GPP `Tsp` interface are used. Optionally the following content information is allowed to be included in a payload:

- It could contain a resource (or attribute) identifier (as expressed inside the target CSE) and the actual content for the resource (or attribute) of any of the resources stored in the target CSE.
- Or any other instructions for initiating a specific procedure. For example, to execute a command.
- Or it could contain of the URI of an entity outside the oneM2M domain where the target CSE should connect to. How the actual setup with an entity outside the oneM2M domain is performed it is outside the scope of oneM2M specification.

VI. Discussion and Conclusions

The majority of IoT/M2M capable devices are connected to the infrastructure via the underlying networks. There exist many obvious use cases describing the essential features of an interworking between the IoT/M2M service layer architecture and the underlying networks. Although functions and procedures for the interworking have to be clearly standardized, neither of oneM2M and 3GPP MTC architectures have clearly addressed the complete set of functions and procedures in their specifications.

In this paper we present and describe an interworking architecture between the oneM2M common services platform and the underlying network (in particular the 3GPP MTC architecture). This paper attempts to (1) introduce the current status of standardized interworking architectures and (2) provide a direction for future standardization of underlying network interworking. The oneM2M and 3GPP specifications in this article are based on their Releases 1 and Release 12, respectively. In future, the interworking architectures can be enhanced with additional features such as network management planning, mobility status exchange and device management. Another dimension in enhancing the interworking architecture is to widen the current scope to cover different underlying network technologies such as WLAN.

In the meantime there are many initiatives that are trying to address the current need of interworking. As an example GSMA has started in 2014 a new program called Connected Living with the main focus on 3GPP network. The program will produce a set of guidelines for M2M application developers and module manufacturers in order to efficiently use the capability of the mobile network and avoid undesired congestion. These guidelines address 3GPP Release 9 while future releases of 3GPP are already incorporating the same type of guidelines. Another aspect of the GSMA program is to identify the SIM and network capabilities that are relevant for M2M/IoT application and to also address the gaps in the current 3GPP releases.

V. Acknowledgements

The authors would like to thank Mrs. Barbara Pareglio from GSMA for her extensive contribution and valuable criticism on this article and Mr. Genadi Velev from NEC for his constructive discussions. All authors made equal contributions to the study and the publication. Prof. Song was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the "Establishing IT Research Infrastructure Projects" supervised by the NIPA (National IT Industry Promotion Agency) (I2221-14-1012)

References

[1] J.Song, A. Kunz, M. Schmidt, and P. Szczytowski. “Connecting and managing m2m devices in the future internet,” Mobile Networks and Applications, pp. 1–14, 2013.

[2] P. Curwen and J. Whalley, “Making Use of Superfast Connectivity”, Fourth Generation Mobile Communication, Springer, pp. 211-230, 2013

[3] Cisco, “Global Mobile Data Traffic Forecast Update,” 2010–2015 White Paper, February 2011

[4] Nokia Siemens Networks 2011, 2020: Beyond 4G Radio Evolution for the Gigabit Experience, White Paper, February 2011, available online

[5] Swetina, J.; Lu, G.; Jacobs, P.; Ennesser, F.; Song, J., "Toward a standardized common M2M service layer platform: Introduction to oneM2M," *Wireless Communications, IEEE* , vol.21, no.3, pp.20,26, June 2014

[6] T. Taleb and A. Kunz, “Machine type communications in 3gpp networks: potential, challenges, and solutions,” *Communication. Magazine, IEEE*, vol. 50, no. 3, pp. 178–184, 2012.

[7] oneM2M-TS-0001, “oneM2M Functional Architecture Technical Specification”, v0.8.0, Jul, 2014. [Online]. http://www.onem2m.org/

[8] 3GPP TS 23.682 “Architecture enhancements to facilitate communications with packet data networks and applications”

[9] 3GPP TS 23.401 “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”

[10] 3GPP TR 22.853 “Study on Service Exposure and Enablement Support (SEES) requirements”

[11] 3GPP TS 22.368 “Service requirements for Machine-Type Communications (MTC); Stage 1”

[12] oneM2M-TR-0001, “oneM2M Use Case collection”, v0.0.5, Sep, 2013. [Online] http://www.onem2m.org/

[13] oneM2M-TS-0002, “oneM2M Requirements Technical Specification” *v0.6.2*, Oct. 2013. [Online]. http://www.onem2m.org/

[14] 3GPP TR 23.708 “Architecture Enhancements for Service Capability Exposure;”

[15] 3GPP TS 23.003 “Numbering, addressing and identification”

[16] Floeck, M.; Papageorgiou, A; Schuelke, A; Song, J., "Horizontal M2M platforms boost vertical industry: Effectiveness study for building energy management systems,” *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, vol.15, no.20, pp. 6-8 March 2014

[17] A. Ksentini, Y. Hadjadj-Aoul, T. Taleb, "Cellular-Based Machine-to-Machine: Overload Control," IEEE Network Magazine, Vol. 26, No. 6, Nov/Dec pp. 54-60, 2012