# Remote Subscription Management of M2M Terminals in 4G Cellular Wireless Networks

Isam Abdalla
Department of Computer Science
University of Texas at Dallas
Richardson, TX USA
isam.abdalla@utd.edu

Subbarayan Venkatesan
Department of Computer Science
University of Texas at Dallas
Richardson, TX USA
venky@utd.edu

***Abstract*—Machine to Machine (M2M) communication is the backbone of large-scale urban sensing, one of the enabling technologies of the Smart City. Some smart grids are already using M2M for efficient energy management and residential smart meters. The 4th Generation (4G) wireless networks are expected to be used for the majority of the M2M traffic. M2M communication over 4G networks faces some deployment challenges. One of the challenges is the difficulty of managing the subscription of M2M terminals. The challenge is how can an M2M operator, like a utility company, activate or change the subscription of an M2M terminal, like a smart meter, remotely, without requiring a person be at the equipment location. The current subscription management scheme that has been used for human subscribers is based on using the Universal Subscriber Identity Module (USIM) application to store subscriber information in a Universal Integrated Circuit Card (UICC). An operator change requires a new UICC from the new operator. This scheme is not suitable for M2M terminals due to the large number of terminals and the nature of their deployment in remote areas. The UICC in the M2M terminals are, in some cases, permanently sealed to prevent tampering and are thus not removable.**

**This paper discusses the challenges of subscription management of M2M terminals communicating over the 4G networks. We present a solution to remotely manage the M2M subscription. The solution which is based on the Evolved Packet Core (EPC) of the 4G cellular network facilitates Over-The-Air (OTA) subscription activation or change for M2M terminals.**

***Keywords- M2M; 4G wireless system; ;EPC ;***

## I. INTRODUCTION

Machine to Machine (M2M) communication is the backbone of large-scale urban sensing, one of the enabling technologies of the Smart City. The growth in M2M communication is projected to reach over 50 billion devices connected to the Internet by 2020[1]. The list of M2M applications includes smart grid, smart utility meters, connected cars, electronic health care monitoring devices, large-scale urban sensing and many other usage that can have a big impact on the management of the infrastructures and service delivery in the smart city.

The cellular wireless networks are expected to be used for the majority of M2M devices. There are many factors that make the cellular wireless networks an attractive medium for M2M communication, such as the relatively low cost of a wireless module, ease of deployment of M2M over wireless and the reuse of the existing infrastructures that provide a wide coverage area. Any M2M device, such as a smart utility meter or a traffic monitoring device, can be installed anywhere in the network coverage area without the need for costly wired communication expenses. This facilitates the planning of the smart city and speeds up service delivery.

The cellular wireless network, however, was designed for User Equipments (UE) used in Human to Human (H2H) communication. Some of the functionalities that are required for H2H communication are not needed for M2M communication. The existing numbering scheme, for example, is not suitable for identifying the large number of M2M devices. The large number of M2M device can easily overload the network without careful scheduling of the radio resources. Management of the subscription of M2M devices is one of the of the major challenges to M2M operator due to the existing semi-manual process that can be very labor-intensive, and thus costly, for large number of M2M devices such as utility meters. This poses some deployment issues for smart infrastructure communication over the cellular wireless network

In this paper we discuss the challenges of subscription management in the 4th Generation (4G) cellular networks and propose a solution to automate the process. The solution is based on the Evolved Packet Core (EPC) of the Long Term Evolution (LTE) networks.

### *A. Typical M2M communication model*

The M2M communication model we are using in this paper is an overlay network over the LTE wireless networks. Machines are typically communicating with a server or more than one server. The communication is data centric which may include sending text, voice or video as a data packet stream to a server or servers.

A typical M2M communication model over LTE cellular networks is depicted in Fig 1. The main additions in this model to the typical LTE network are the M2M terminal and the M2M Application Server. The M2M terminal has a radio module that enables it to connect to the radio access nodes of the cellular network. The Terminal uses IP connectivity to communicate with an M2M application server which is connected to the operator EPC.

978-1-4673-2129-7/12/$31.00 ©2012 IEEE

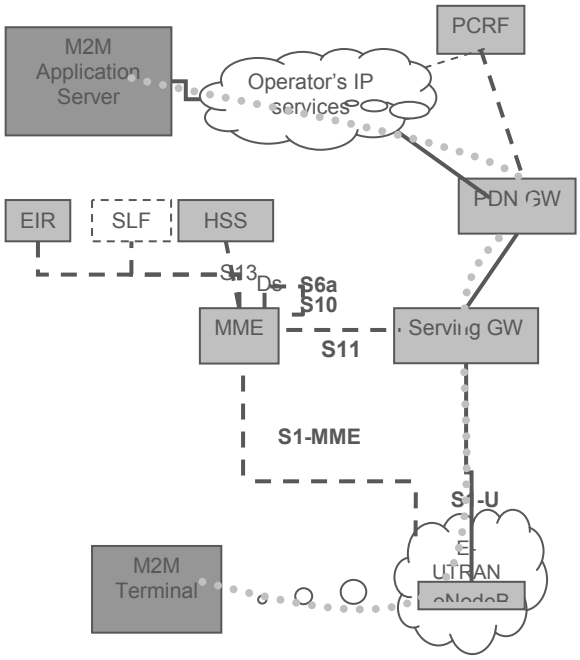


Figure 1. Typical M2M solution over 4G networks

The wireless module of the M2M terminal behaves like any other User Equipment (UE) used for human subscribers. The M2M terminal is required to have a service contract with a network operator. The M2M terminal registers with the operator network when it is powered up. After the terminal is authenticated, IP bearers are established between the terminal and the Packet Data Network Gateway (PDN-GW). The terminal can then obtain the M2M application server IP address and use it to exchange application layer data with the server, as shown by the dotted line in Fig 1.

### *B. Subscription Management in 4G Cellular Networks*

The subscription management in the 4G cellular wireless networks, which is carried over from its predecessors, is an example of how its design is geared towards H2H communication. The subscription management scheme is based on using the Universal Subscriber Identity Module (USIM) application to store subscriber information in a Universal Integrated Circuit Card (UICC). The detailed characteristics of the USIM application are presented in [3] and those of the UICC in [4]. The UICC is issued by the network operator and is valid for the duration of the subscription. When the user wants to change the subscription to another operator, a new UICC, with the new subscription data must be obtained from the new operator. The user has to manually remove the old UICC and install the new one.

### *C. M2M Impact on Subscription Management*

The Third Generation Partnership Project (3GPP) identified subscription management as one of the major obstacles to M2M market growth [2]. The existing subscription management procedures require manual maintenance work on all installed machines in the field. This involves sending service technicians to the field which involves extra monetary cost in addition to the environmental cost. The study in [2] suggested that alternatives for dynamic provisioning of USIM parameters to a large number of M2M terminals within a short timeframe are needed. The study suggested that the market for M2M communication may grow faster if the M2M operators can select their network operator knowing that they are not tied to this operator forever.

Another problem with the existing subscription management procedure is that M2M terminals may be installed in unattended accessible location. This leaves the terminals vulnerable to tampering or sabotage by simply removing the UICC. The study in [5] discussed the equipment tampering problem and suggested options to ensure that the M2M equipment is tamper resistant. The three options presented are as follows:

- Option 1: Mechanically attach the UICC to the M2M equipment to make it non-removable, or render it permanently unusable if removed.
- Option 2: This option is replacing the UICC with a new protected non-removable module that is integrated in the M2M device. The new module is used to store the USIM application and the subscription data.
- Option 3: The USIM application is implemented on a removable UICC, but appropriate techniques are applied to discourage removal, or invalidate the UICC if removed, to make the UICC removal unproductive or even counterproductive for the attacker.

All of these options require that the USIM and the subscription data stored in a non-removable UICC or equivalent media which by itself exacerbates the operator change problem. The study also suggested two alternatives for a downloadable subscription application to facilitate remote subscription management. The study refers to the downloadable subscription application as the Machine Communication Identity Module (MCIM). The MCIM is defined as a collection of M2M security data and functions for an M2M terminal to access the wireless network. The two alternatives for a downloadable MCIM presented in [5] are:

- A Trusted Run-time Environment (TRE) based downloadable MCIM application.
- A UICC based downloadable MCIM application.

The type of the MCIM is not expected to have a major impact on how the MCIM is downloaded to the M2M terminal for the purpose of activating a new subscription. This paper assumes, without loss of generality, that a non-removable UICC or equivalent media is used to store a downloadable MCIM.

### *D. Related Work*

The problem of remote subscription management in the wireless networks is discussed within various

telecommunication industry and standardization bodies. The Third Generation Partnership Project 2 (3GPP2) addressed the problem in [6] and proposed the Over-The-Air Service Provisioning (OTASP) and Parameter Administration (OTAPA) features. The two features are supported in the 3GGP2 networks. OTASP and OTAPA partially automate the provisioning procedure but still require that the users call a service center to fully activate their subscription. The 3GPP2 also proposed an IP based version of OTA in [7]. This version also assumes a subscription is already activated and provides support for extra provision.

The 3GPP studied the problem in [5] and discussed the two main subscription management scenarios: (1) Initial subscription activation and (2) subscription change to a different operator. The study focused on the security aspects of changing subscription for M2M terminals out in the field without direct human intervention after contract expiry and allocating the M2M terminal to a network operator at initial power up. The study proposed two options one for TRE based MCIM and another for UICC based MCIM. The TRE based MCIM solution adds four new entities to the network to facilitate both initial subscription activation and change of operator. The UICC based MCIM solution proposed procedural steps for change of operator but did not support remote activation of the initial subscription.

In this paper we define a provisional identity to be used in M2M terminals that don't have an existing subscription with any network operator. We then propose an MCIM type agnostic solution that supports both initial activation and change of operator scenarios. The solution is based on the EPC network architecture.

The rest of the paper is organized as follows: in section II we present a proposal for a provisional identity for M2M terminal in the EPC. In section III we describe our proposed solution for initial subscription activation. In section IV we describe our solution for the M2M terminal change of subscription scenario. In section V we analyze the proposed solution and highlight its merits. We evaluate the performance impact of our solution in section VI and conclude the paper in section VII.

## II. PROVISIONAL M2M IDENTITY IN 4G NETWORKS

All devices are required to register with the cellular network to be granted access to any service other than emergency calls. The registration is performed when the device initiates the Attach Procedure by sending an Attach Request message. The details of the Initial Attach procedure are described in [8] and [9]. The M2M terminal includes its identity in the Evolved Packet System (EPS) mobile identity subfield. The EPS mobile identity contains two parameters of interest: (1) identity type and (2) identity value. The identity type is currently defined as 3-bits with the values listed in table I.

The concept of the provisional identity for the M2M terminals is first discussed in [5]. The discussion in [5], however, did not include any details or definition of a structure for the provisional identity. We propose a new provisional identity for the M2M terminals, Provisional M2M Identity (P-MID), for use in the 4G wireless networks. The new identity is not dependent on any operator network.

TABLE I. TYPES OF EPS MOBILE IDENTITY

| bit3 | bit 2 | bit1 [a] | Type of identity |
|---|---|---|---|
| 0 | 0 | 1 | IMSI |
| 1 | 1 | 0 | GUTI |
| 0 | 1 | 1 | IMEI |

a. All other values are reserved

The structure of the P-MID is hierarchical to facilitate quick identification of mobile M2M devices. The Organization Unique identity (OUID) identifies the equipment manufacturer of the M2M terminal. The Machine Identity (MID) is the equipment manufacturer's unique identifier of the M2M device. P-MID is used by M2M equipment manufacturers as an initial identify for the devices. The structure of the new identity is shown in Fig 2.

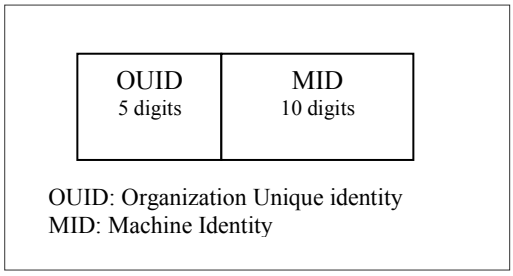


Figure 2. The structure of P- MID

We also propose adding a new EPS mobile identity type of P-MID. The P-MID EPS identity type value is chosen from the current reserved values as shown in table II.

TABLE II. MODIFIED TYPES OF EPS MOBILE IDENTITY

| bit3 | bit 2 | bit1 [a] | Type of identity |
|---|---|---|---|
| 0 | 0 | 1 | IMSI |
| 1 | 1 | 0 | GUTI |
| 0 | 1 | 1 | IMEI |
| 1 | 1 | 1 | P-MID |

a. All other values are reserved

The P-MID is stored in the M2M terminal and in the Provisional Machine Server (PMS), a new EPC entity. The PMS is a clearing house server that contains a master database of M2M devices that are in the deployment stage. The PMS profile is identified by the PMID and contains the device initial security credentials for authentication and the security keys to be used for secure communication with the network. The profile also contains the Access Point Number (APN) of the network to which the device will connect to be configured. The device will be restricted to only access this APN.

In the next sections, we use the P-MID and PMS to describe our proposal for remote subscription management of M2M terminals.

## III. INTIAL SUBSCRIPTION ACTIVATION

In this section we present our proposal for remote initial subscription activation of M2M terminals.

### A. Assumptions

We assume the following preconditions are satisfied:

- The M2M terminals are configured with the P-MID and other default security credentials before delivery to the end user.
- The M2M terminals P-MID and other default security credentials are stored in the PMS before the device is deployed in the field.
- The new subscription data is already added into the new operator HSS and the MCIM with new subscription data is added into the M2M Configuration Server (MCS), described below.

### B. Modified EPC Architecture

We introduced the PMS in the previous section as a master database that contains the profile of the M2M terminals. The PMS is used to authenticate M2M terminals, whose initial subscription has not been activated yet, during the initial attach. It performs authentication and authorization of the provisionally configured M2M terminals, and handles requests for the M2M profile from other entities such as the Mobility Management Entity (MME).

We also propose another server, MCS. The MCS is an application server that can be owned by a network operator, an equipment manufacturer or the M2M service provider. The MCS contains a database of the M2M terminals that are to be configured and the MCIM application associated with the terminal. The records in the MCS are kept until the MCIM is downloaded and correctly configured in the terminal. The modified EPC architecture, with the addition of the PMS and MCS is shown in Fig 3.

The MME interfaces to the PMS in the same manner it does with the Home Subscriber Server (HSS). The only difference is that the MME sends queries related to M2M terminals that are identified by P-MIDs to the PMS instead of the HSS.

### C. Modified Attach Procedure

All devices are required to register with the cellular network to be granted access to any service other than emergency calls. The device must first execute the Initial Attach procedure to connect to the 4G EPC. Following a successful attach procedure, a context is established for the UE in the MME. A default bearer is also established between the device and the PDN-GW to allow the device to have an always-on IP connectivity to the network operator IP services. The details of the Initial Attach procedure are described in [8] and [9].

The most important part of the Attach procedure is authenticating the device and obtaining its service profile from a subscription server. The device profile is added to the

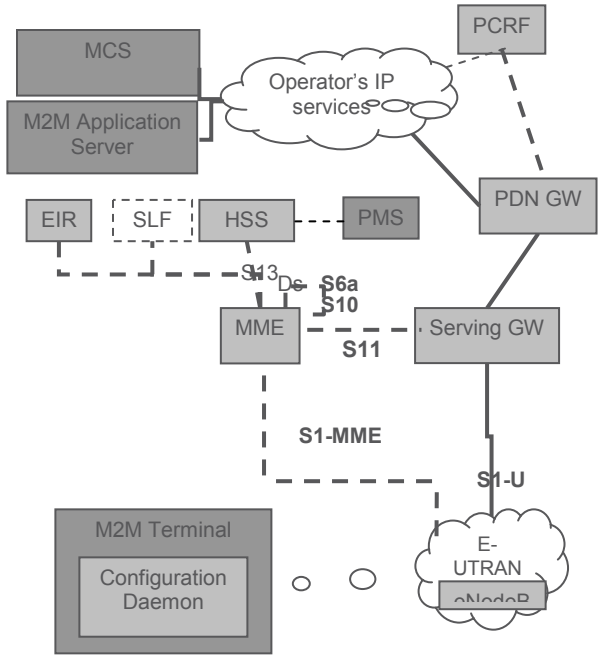


Figure 3. Modified EPC architecture

subscription server when a service contract is agreed with the network operator. For a newly deployed M2M terminal this profile is stored in the PMS. This requires some changes to the Attach procedure to handle M2M terminals with no active subscription in addition to UEs and M2M terminals with active subscription.

The device initiates the Attach Procedure by sending an Attach Request message to the MME as depicted in the message flow shown in Fig 4. The initial attach procedure is modified as follows to support the new P-MID:

- The M2M terminal initiates the attach procedure by sending an Attach Request message to the MME.
- UEs and M2M terminals with active subscription set the identity type in the EPS mobile identity to IMSI, as is currently done, and include their assigned IMSI.
- Newly deployed M2M terminals with no active subscription set the identity type in the EPS mobile identity to P-MID, and include their preconfigured P-MID.
- The MME checks the identity type in the EPS mobile identity of the received Attach Request message and sends profile related queries to the HSS if the type is IMSI or to the PMS if the type is P-MID.
- The PMS processes the request and retrieves the terminal profile including the authentication vector.
- The MME proceeds with the authentication using the security keys received from either the HSS or the PMS.

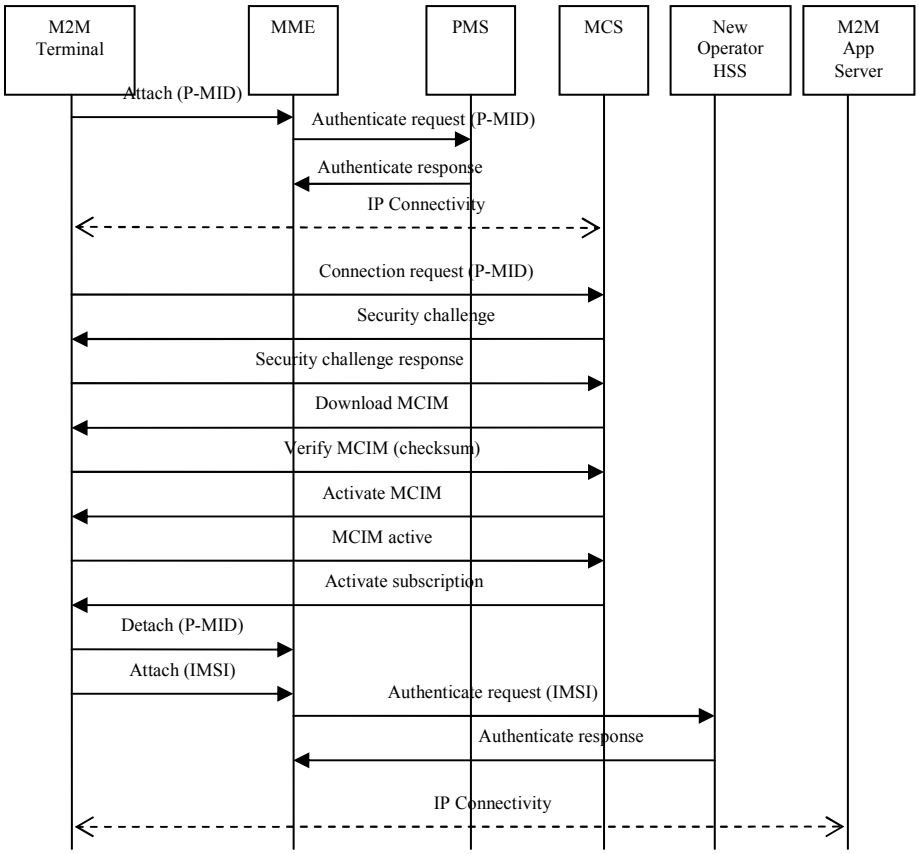


Figure 4. Initial subscription activation message flow

- The MME accepts or rejects the attach request based on the responses received from either the HSS, for UEs and activated M2M terminals, or the PMS for M2M terminals with no active subscription.
- The rest of the processing of the attach request, such as default bearer setup, remains the same.
- The M2M terminals authenticated by the PMS are restricted to connect only to the MCS network with the APN retrieved from the PMS profile.

The M2M terminal now has IP connectivity to the MCS and can start the configuration process as described below.

### *D. Remote Configuration Support in M2M Terminals*

We outline in this section the functionality needed in the M2M terminal to support remote subscription management. We propose a configuration daemon software module that handles communication with the MCS. The configuration daemon handles all the remote activation commands on behalf of the M2M terminal.

We propose using an extension of the Open Module Alliance - Device Management (OMA-DM) interface [10] for communication between the MCS and the configuration daemon. The extension adds new Management Objects (MO) to encapsulate the remote subscription management data and command exchange between the M2M terminal and the MCS.

### *E. M2M Terminal Configuration with an MCIM*

We describe in this section the configuration process steps the M2M terminal use to activate its initial subscription. The M2M terminal performs the following configuration process:

- The M2M terminal sends an application layer connection request to the MCS over the secure IP connection established during the initial attach procedure.
- The M2M terminal includes its P-MID in the connection request message to the MCS.
- The MCS uses the P-MID to retrieve the M2M terminal profile and sends a security challenge, based on a shared secret, to the terminal.
- The terminal calculates the security challenge response and sends it to the MCS.
- The MCS verifies the security challenge response and starts downloading the MCIM to the terminal.

- The configuration daemon in the terminal verifies the checksum and sends a verification message to the MCS.
- The MCS sends an activate MCIM command to the configuration daemon in the terminal.
- The configuration daemon in the terminal starts an activation timer and activates the MCIM.
- If the activation is successful, the activation timer is stopped and an MCIM active response is sent to the MCS.
- If the activation timer expires, the configuration is aborted and an activation failure response is sent to the MCS.
- The MCS sends an activate subscription to the configuration daemon in the terminal to start using the new subscription data.
- The Terminal detaches from the network,
- The terminal initiates the initial attach procedure using the IMSI and other credentials obtained during the configuration process.
- The attach request is processed at the MME and the new operator's HSS is contacted to complete the attach procedure.
- The M2M terminal establishes connectivity to the M2M application server over the new operator network.

The M2M terminal is now connected to the new operator network. The configuration process is depicted in the message flow shown in Fig 4.

## IV. SUBSCRIPTION CHANGE TO A NEW OPERATOR

In this section we present our proposal for remotely changing the subscription of M2M terminals to a new network operator.

### *A. Assumptions*

We assume the following preconditions are satisfied:

- The new subscription data is already added into the new operator HSS.
- There are no contractual issues that prevent the M2M operator from switching their service from the current operator to the new operator.
- The MCIM with new subscription data is added into the MCS.
- The M2M terminal has established connectivity to the M2M application server over the current operator network.

### *B. Subscription change process*

We describe in this section the configuration process steps the M2M terminal uses to change the subscription of M2M terminals to a new network operator. The configuration process is depicted in the message flow shown in Fig 5. The M2M terminal performs the following configuration process:

- The M2M operator triggers a batch process on the M2M application server to send a "Start Configuration" command to the configuration daemon in the M2M terminals.
- The M2M terminal sends an application layer connection request to the MCS over the secure IP connection established during the initial attach procedure.
- The M2M terminal includes its P-MID in the connection request message to the MCS.
- The MCS uses the P-MID to retrieve the M2M terminal profile and sends a security challenge, based on a shared secret, to the terminal.
- The terminal calculates the security challenge response and sends it to the MCS.
- The MCS verifies the security challenge response and starts downloading the MCIM to the terminal.
- The configuration daemon in the terminal verifies the check sum and sends a verification message to the MCS.
- The MCS sends an activate MCIM command to the configuration daemon in the terminal.
- The configuration daemon in the terminal starts an activation timer and activates the MCIM.
- If the activation is successful, the activation timer is stopped and an MCIM active response is sent to the MCS.
- If the activation timer expires, the configuration is aborted and an activation failure response is sent to the MCS.
- The MCS sends an activate subscription to the configuration daemon in the terminal to start using the new subscription data.
- The Terminal detaches from the current operator network.
- The terminal initiates the attach procedure using the new IMSI obtained during the configuration process.
- The attach request is processed at the MME and the new operator's HSS is contacted to complete the attach procedure.
- The M2M terminal establishes connectivity to the M2M application server over the new operator network.

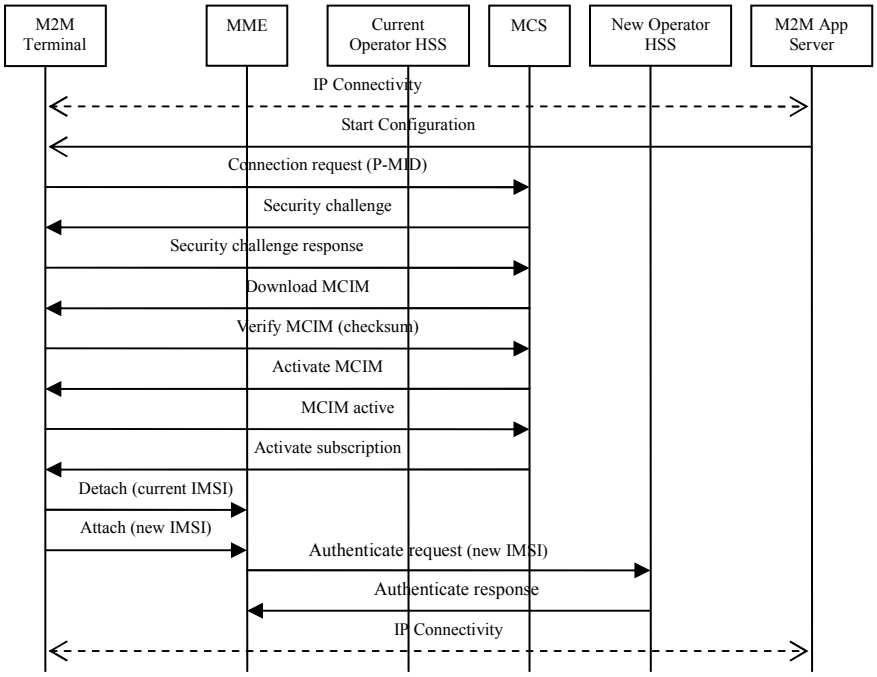


Figure 5. Subscription change message flow

The M2M terminal is now connected to the new operator network.

## V. ANALYSIS

In this section we analyze our solution against the main technical evaluation criteria listed in [5].

*a) Security:* This criteria evaluates risks of theft of or tampering with the subscription. The security of our solution is implemented at different levels. The terminal is authenticated during the initial attach procedure using the shared secret key retrieved from the PMS and the one securely stored in the terminal by the supplier. This step authenticates both the terminal and the network since the two has to agree on the shared secret key. This is similar to the security mechanism currently used in H2H UE, where the secret key is stored in the USIM application in the UICC and in the HSS. A similar authentication process is repeated between the MCS and the terminal at the start of the configuration process.

One of the security aspects considered in [5] is the trust model which outlines the tasks each entity or role is trusted to reliably perform. The roles identified in the trust model in [5] that are relevant to our solution are: M2M Subscriber, M2M Terminal Supplier, Visited Network Operator and Selected Home Operator. We assume that the statements in [5] about the tasks that each of the above roles is expected and trusted to perform are satisfied. We also extend the trust model to the two entities added in our solution: the PMS and the MCS.

The PMS is trusted by the Visited Network Operator to:

- Correctly authenticate the identity of provisionally configured M2M terminals.
- Reject authentication requests with invalid P-MIDs.

The MCS is trusted by the M2M subscriber and the selected Home Operator to:

- Securely store the downloadable MCIMs and P-MIDs of the M2M terminals to be configured for the selected Home Operator.
- Correctly authenticate connection requests from M2M terminals.
- Securely download and activate the MCIM in the M2M terminal.
- Correctly verify MCIM activation in the M2M terminal and abort the configuration if any anomaly is detected.
- Correctly and securely activate the new subscribtion in the M2M terminal.

*b) Initial choice of operator:*This criteria tests how well-suited the solution is for the initial choice of the operator. Our solution opens the possiblity of procuring M2M terminals that are operator independent. The M2M operator can register their terminal in the PMS, obtain the downloadable MCIM from their chosen network operator and store it in the MCS. The automated over the air subscription activation process is started as soon as the M2M terminal is powered up.

*c) Operator change:* This criteria tests how well-suited the solution for network operator change. Our proposal provides an automated solution that does not require any in the field service. The M2M operator obtains the downloadable MCIM from their chosen network operator and stores it in the MCS. The automated over the air subscription activation

process is triggered from the M2M operator application server. This gives the M2M operator complete control of when to switch to another network operator.

*d) Remote Management:* Our proposal is an automated over the air subscription activation process. The process does not require any in the field technicians. The initial subscription activation is triggered by the configuration daemon as soon as the M2M terminal is powered up. The operator change is remotely triggered from the M2M operator application server.

*e) Flexibility to adapt to new requirements:* The proposed solution can be adapted to add any future requirements by software upgrades to the configuration daemon and to the MCS. New OMA-DM MOs can be added in the future for any new provisioning requirements without any need for hardware changes.

*f) Suitability to mass market deployment:* Our solution is cost effective since any number of terminals can automatically go through the initial subscription activation or change of operator without human intervention, apart from storing the subscription information in the network server, which is already part of the existing subscription management process. The solution is also scalable to the very large deployments envisioned within the M2M use cases. The capacity needed for configuration is mainly in the MCS and the PMS. The functionality of both entities can easily be distributed across multiple physical servers.

*g) Impact on subscription management systems:* Our proposal does not change the operator's existing subscriber management systems. We, however, modify the process to remove the need to issue new UICC cards for each M2M terminal and replace it with issuing a downloadable MCIM application. This adds a new requirement to support issuing and distributing the MCIM to M2M operators. This requirement does not add any complexity to the existing system and can help reduce the operator cost of managing M2M terminal subscription.

*h) Impact on network infrastructure:* We propose adding two servers to the network, the PMS and the MCS. Both servers don't need to be part of any operator network. A new or modified interface is needed for communication between the MME and the new PMS. The new interface can be a modification of the existing MME-HSS interafce. The solution also requires changes to the MME handling of the initial attach procedure which can be done by a software upgrade.

*i) Impact on terminal:* Our proposal requires terminals that support downloadable MCIM. In addition we propose a new software module to implement the configuration daemon.

*j) Impact on 3GPP specifications:* The solution does not require any major changes to existing specifications. New specifications are needed to define the new MME-PMS interafce. The extension to OMA-DM also needs to be standardized to ensure compatiblity between terminals and the MCS.

The above analysis shows that our proposed solution meets the main evaluation criteria in [5]. The solution is a scalable cost effective process which can be translated into a plausible subscription management model by the network operators.

## VI. PERFORMANCE EVALUATION

In this section we evaluate the performance of our solution using two main metrics: (1) Additional processing delay of the Attach procedure (2) additional signaling messages overhead.

The total processing delay of the initial Attach procedure for UEs and M2M terminal with active subscription, $T_{attach}$, can be expressed by the following equation

$$T_{Attach} = T_{access} + T_{MME} + T_{HSS} \quad (1)$$

$T_{access}$ : processing delay in the radio access network

$T_{MME}$ : processing delay in the MME

$T_{HSS}$ : processing delay in the HSS

There is no impact to $T_{access}$ or $T_{HSS}$ since our proposal is independent of the access network and does not change the existing handling of the initial attach in the HSS. The two can be expressed as a constant, Tc, in equation (1) as follows

$$T_{Attach} = T_{MME} + \Delta T_{MME} + Tc \quad (2)$$

The change in the MME processing, $\Delta T_{MME}$, is the extra processing at the MME to check the type of identity, which can be implemented as a simple "if" check in software. We conclude that $\Delta T_{MME}$ is very small and has no significant impact on the overall processing time of the Attach procedure for UEs and M2M terminals with active subscription.

The processing delay of M2M terminals with no active subscription that are using our solution can also be expressed as follows

$$T_{Attach} = T_{MME} + \Delta T_{MME} + T_{PMS} + T_{access} \quad (3)$$

$T_{PMS}$ : processing delay in the PMS

$\Delta T_{MME}$ is negligible as shown in the above analysis. $T_{PMS}$ is equivalent to $T_{HSS}$ in equation (1). We note here that the PMS is not updated with the terminal location which results in an estimated 29 ms [11] saving over the HSS. This shows that the overall processing delay for M2M terminal using our solution can be smaller than the processing delay of the existing Attach procedure.

The signaling message overhead in our solution consists of the extra Detach and Attach procedures after the MCIM is downloaded to the M2M terminal. This overhead is only incurred when an M2M terminal is configured to activate a new subscription. This overhead is not different from the existing manual subscription change where a UICC change would result in a Detach from the old operator network when the old UICC is removed and an Attach is performed after the new UICC is inserted.

We note here that the MCIM download and the commands to activate the subscription are carried in the bearer path. This part of the process is an application layer message exchange and has no signaling overhead as far as the operator network in concerned.

## VII. CONCLUSION

Recent market trends analysis is showing an accelerated growth in the demand for M2M communication over the wireless cellular networks. This growth is driven by the need for large-scale urban sensing and remote access to machines that control many of the services used in many infrastructures such as the smart grid, efficient traffic management, remote measurement, data acquisition and utility metering.

This growth poses some challenges to the existing wireless cellular networks design, deployment and operation. One of the main challenges is the difficulty for the M2M operator to change the subscription from one network operator to another. This challenge can slow the penetration of M2M communication over cellular networks. This can become one of the main deployment issues for smart infrastructure in urban areas.

We discussed in this paper the challenges of subscription management of M2M terminals communicating over the 4G LTE cellular networks. We proposed a new provisional identity for M2M terminal. We used the new identity in a solution to remotely manage the M2M subscription. The solution, which is based on the Evolved Packet Core of the 4G cellular system, facilitates Over-The-Air (OTA) subscription activation or change for M2M terminals. The proposal does not require major changes in the existing call processing entities in the EPC architecture.

## REFERENCES


[1] Ericsson white paper: “more than 50 billion connected devices”, 284 23-3149 Uen, February 2011

[2] 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Facilitating Machine to Machine Communication in 3GPP Systems; (Release 8) 3GPP TR 22.868 V8.0.0 (2007-03).

[3] Characteristics of the USIM Application, 3GPP TS 31.102

[4] UICC-Terminal Interface, Physical and Logical Characteristics, 3GPP TS 31.101

[5] 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment(Release 9), 3GPP TR 33.812

[6] CELLULAR RADIO TELECOMMUNICATIONS INTERSYSTEM OPERATIONS: Over-The-Air Service Provisioning (OTASP) & Parameter Administration (OTAPA) , 3GPP2 N.S0011-0 Version 1.0

[7] IP Based Over-the-Air Device Management (IOTADM) for cdma2000 Systems, 3GPP2 C.S0064-0 Version 2.0 January 2011

[8] 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access(Release 11), 3GPP TS 23.401 V11.0.0 (2011-12).

[9] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3(Release 11), 3GPP TS 24.301 V11.1.0 (2011-12)

[10] OMA Device Management Protocol, OMA-TS-DM_Protocol-V1_2-20070209-A

[11] Shiann-Tsong Sheu; Youn-Tai Lee; Shaojung Lu; , "Load analysis for MTC devices in idle mode or detached state," Computer Symposium (ICS), 2010 International , vol., no., pp.424-428, 16-18 Dec. 2010.