Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

ANÁLISIS DE ESPECIFICACIONES ESTABLECIDAS PARA LAS COMUNICACIONES MACHINE-TO-MACHINE Y PROPUESTAS DE CASOS DE USO

TRABAJO FIN DE MÁSTER

Jhoanlye Avendaño Espina

2013

Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

Máster Universitario en
Ingeniería de Redes y Servicios Telemáticos

TRABAJO FIN DE MÁSTER

ANÁLISIS DE ESPECIFICACIONES ESTABLECIDAS PARA LAS COMUNICACIONES MACHINE-TO-MACHINE Y PROPUESTAS DE CASOS DE USO

Autor
Jhoanlye Avendaño Espina

Director
Manuel Alvarez-Campana

Departamento de Ingeniería de Sistemas Telemáticos

2013

Resumen

La comunicación Machine-to-Machine (M2M) se puede considerar como una categoría dentro de las tecnologías de la información y las comunicaciones (TIC), que combina las comunicaciones con tecnologías de computación y energía para permitir la interacción a distancia entre maquinas y humanos, con sistemas y procesos físicos.

Este tipo de comunicaciones representan un nuevo modelo de negocio que surge de la transmisión automática de datos y mediciones desde localidades remotas por medios de comunicación fijos o inalámbricos, considerado como el concepto básico de la telemetría. Desde su concepción a principios de la década pasada se ha experimentado un crecimiento importante en el número de soluciones propietarias que implementan esta tecnología. Esto ha motivado a las organizaciones a ser más activas en el proceso de estandarización de M2M.

Algunas de estas organizaciones de desarrollo de estándares (SDO) realizaron estudios sobre el impacto que pudiera tener el uso masivo de dispositivos M2M, y en la actualidad se encuentran desarrollando varios estándares con especificaciones y recomendaciones para regularizar y adaptar las redes a las particularidades de estas comunicaciones. En el presente trabajo se realiza un análisis de los principales documentos de estandarización desarrollados hasta la fecha por organizaciones consideradas por nosotros como las más activas y maduras en el desarrollo de estándares M2M, con la finalidad de proveer mejor comprensión de los conceptos y escenarios que allí se mencionan, como son ETSI, 3GPP e IEEE;.

En este documento se evidencia la tendencia a considerar las comunicaciones M2M como una aplicación en un servidor central que utiliza la red de comunicaciones para transmitir datos a los dispositivos remotos. Típicamente M2M se basa en tecnologías comunes y ubicuas como redes de sensores, redes móviles e internet. El ETSI se enfoca en proponer una arquitectura para la capa de servicios que sea independiente de la red de acceso encargada de transportar los datos, el 3GPP por su parte atiende los requisitos funcionales de la arquitectura de red para soportar las comunicaciones entre maquinas también denominadas MTC, por último el IEEE realiza mejoras en la interfaz de aire de la red WiMAX para soportar eficientemente las comunicaciones M2M.

En este mismo contexto se estudian las arquitecturas básicas, características de seguridad, y los elementos claves propuestos por cada organismo. Para finalizar se proponen algunos casos de uso en escenarios que consideramos pertinentes para desplegar aplicaciones que se beneficien de las comunicaciones M2M; con la finalidad de ampliar los casos de uso que han propuesto los SDO.

Abstract

Machine-to-Machine communication is a category inside the Information and Communications Technologies (ICT) that integrate communications with power and computer technologies, allowing remote interaction between machines and humans, with physics process and systems.

This kind of communications represents a new business model which originated from which we consider as the basic concept of telemetry technology, automatic measurement and transmission of data from remote locations by wire o wireless means. Since it origins at early 2000, it has faced an important growth of vertical implementations. This has motivated some organizations to be more active in M2M standardization process.

Some of this Standards Development Organizations (SDO) has realized studies about the impact that may have the massive use of M2M devices, and are developing at the moment some standards with recommendations and specifications to adapt and enhance communications networks, to this particular communications. In order to provide better understanding of scenarios and concepts introduced by SDO's, we have analyzed in this work main standards documents developed to date by standards organizations that we considered as most active and complete in M2M standards development, which are ETSI, 3GPP and IEEE.

This document exposed the tendency to consider M2M communications as an application over a central server which uses telecommunications network to transmit data to remote end-devices. Typically M2M is based on universal and common technologies as sensor networks, mobile networks and internet. ETSI has focused it work in the development of an end-to-end service layer architecture independent of access network technologies; in the other hand 3GPP, is addressing functional requirements of network architecture to support M2M, also known as machine type communications (MTC); finally IEEE, has proposed enhancements to WiMAX air interface to provide improved support for machine-to-machine applications.

In this context, we studied basic architecture, security characteristics and key elements proposed by standards development organizations. Finally, has presented some relevant use cases in scenarios where could be interesting to deploy a machine–to-machine communication system.

Índice general

Índice de figuras

Índice de tablas

Siglas

3GPP	Third Generation Partnership Project
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AAI	Advanced Air Interface
ABS	Advance Base Station
AEC	Automotive Electronics Council
AKA	Authentication and Key Agreement
AMS	Advance Mobile Station
BAN	Body Area Network
BS	Base Station
BSF	Bootstrapping Server Function
CMAC	Cipher-based Message Authentication Code
CoRE	Constrained RESTful Environments
CSN	Connectivity Service Network
DA	Device Application
DCD	Downlink channel descriptor
DER	Distributed Energy Resources
DL	Downlink
DSA	Dynamic service addition
DSCL	Device Service Capabilities Layer
DSD	Dynamic service deletion
DTC	Diagnostic Trouble Code
E-UTRAN	Evolved UTRAN
EMS	Engine Management System
ESMIG	European Smart Metering Industry Group
ETSI	European Telecommunications Standards Institute

FMDID	Fixed M2M Deregistration ID
GA	Gateway Application
GBA	Generic Bootstrapping Architecture
GSCL	Gateway Service Capabilities Layer
H2H	Human-to-Human
HAN	Home Area Network
HLR	Home Location Register
HSS	Home Subscriber System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
M2M	Machine-to-Machine
M2M SC	Machine-to-Machine Service Capabilities
M2MCID	M2M multicast connection identifier
M2MGTEK	M2M Group Traffic Encryption Key
MAC	Medium Access Control Layer
MAK	MBS authorization key
MAMC	M2M ACK MAC Control
MBS	Multicast and broadcast service
MGID	M2M Group Identifier
MGMC	M2M Group MAC Control
MME	Mobile Management Entity
MS	Mobile Station
MSC	Mobile Switching Centre
MTC	Machine Type Communication
MSBF	M2M Service Bootstrap Function
NA	Network Application

NAF	Network Application Function
NAN	Neighborhood Area Network
NAS	Non-Access-Stratum
NSCL	Network Service Capabilities Layer
OFDM	Orthogonal frequency division multiplexing
OMA	Open Mobile Alliance
P2P	Peer to Peer
PHY	Physical layer
PLC	Power Line Communications
PLMN	Public Land Mobile Network
QoE	Quality of Experience
QoS	Quality of Service
RAU	Routing Area Update
RFID	Radio Frequency Identification
RNG-REQ	Ranging request
RNG-RSP	Ranging response
RMD	Remote Monitoring Device
ROLL	Routing Over Low power and Lossy networks
RPM	Remote Patient Monitoring
SCD	System configuration descriptor
SCL	Service Capabilities Layer
SDO	Standards Developing Organizations
SFID	Service flow ID
SGSN	Serving GPRS Support Node
SME	Short Message Entity
SMCG	Smart Metering Coordination Group
SMS-SC	Short Message Service – Service Center

SS	Subscriber Station
STID	Station Identifier
SVT	Stolen Vehicle Tracking
TAU	Tracking Area Update
TCU	Telematics Control Unit
UCD	Uplink channel descriptor
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
UTRAN	Universal Terrestrial Radio Access Network
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VLR	Visitor Location Register
WiMAX	Worldwide Interoperability for Microwave Access
WLL	Wireless Local Loop
xAE	Application Enablement
xCS	Communication Selection
xGC	Generic Communication
xRAR	Reachability, Addressing and Repository
xREM	Remote Entity Management
xSEC	Security

1 Introducción

Luego de muchos años de haber aparecido la idea de ampliar el alcance de los dispositivos conectados a internet, más allá de aquellos controlados por humanos utilizando sus servicios para satisfacer gustos y necesidades, emergen las comunicaciones M2M. Base de lo que hoy en día se conoce como la internet de las cosas (IoT), refiriéndose a la interconexión en red de objetos de uso diario por parte de la sociedad. La visión inicial de la tecnología constaba de un número enorme de dispositivos interconectados trabajando silenciosamente para mejorar y generar nuevos servicios de valor agregado que brindaran seguridad, comodidad, confianza y calidad de vida a los usuarios. Las comunicaciones M2M se refieren básicamente a la comunicación entre equipos electrónicos, fijos o móviles, con o sin una pequeña intervención por parte de los humanos [1].

Se estima que para finales de esta década el número de dispositivos conectados a internet sea mucho mayor que el número de habitantes, por lo que esas proyecciones hacen que la industria se vuelque a explorar todas las oportunidades que las comunicaciones M2M ofrecen, permitiendo la aparición de un nuevo modelo de negocio. El término M2M es muy amplio y se refiere a diversos mercados verticales, diferentes tecnologías de comunicación y un gran alcance geográfico.

M2M tiene la capacidad de mejorar los procesos en muchas industrias como las de energía, seguridad pública, salud, automotora, manufactura, entre muchas otras; lo mismo ocurre con las tecnologías de red de acceso que van desde las redes de corto alcance como ZigBee, BlueTooth, RFID hasta redes de gran cobertura como las redes móviles celulares GPRS, UMTS y LTE, o redes satelitales. El alcance geográfico de las aplicaciones M2M no tiene límite, puede ser local como el que utiliza una persona para controlar los electrodomésticos en su hogar, o global en el caso de un sistema de monitorización de fallas en un vehículo que puede circular por todo el territorio nacional o incluso internacional.

A pesar de las predicciones de un gran mercado para esta tecnología, resulta que en la actualidad se mantiene muy pequeño y poco desarrollado. Luego de una década de desarrollo gradual, se han documentado un sin fin de casos de uso para M2M, de los cuales algunos no han llegado a progresar de los prototipos, y solo unos pocos han ayudado a la creación de modelos de negocio y establecer requisitos de servicio.

Esto posiblemente se haya visto afectado porque las típicas instalaciones de sistemas M2M pueden o no hacer uso de redes comerciales, y en su lugar en muchas de ellas se establece una red local propietaria M2M. Por eso la recomendación es enfocar el

desarrollo del modelo de negocio hacia aplicaciones M2M de área extensa, en donde los flujos de datos se realizan a través de operadoras de red comercial o proveedores de servicio de comunicación.

El crecimiento esperado de este mercado traerá un incremento sin precedente del tráfico de datos en la red, por eso no sorprende el hecho de que asociaciones y organismos de estandarización como el ETSI, 3GPP, e IEEE están ampliamente involucrados en el desarrollo de estándares y recomendaciones en el contexto de las comunicaciones M2M. Para poder acoplarse en esta prometedora área de las comunicaciones M2M se debe tener primero un conocimiento profundo de la arquitectura básica M2M y sus principios.

El objetivo principal de este trabajo es colaborar en la comprensión de los aspectos importantes involucrados en las comunicaciones M2M como son su arquitectura básica, requisitos de servicios, características de seguridad, escenarios, entre otros. Partiendo del análisis de algunos estándares desarrollados hasta la fecha por importantes organizaciones como ETSI, 3GPP e IEEE, los cuales se han encargado de atender gradualmente la evolución de estas comunicaciones para que puedan ser soportadas eficientemente por las redes de comunicación actuales.

Igualmente el trabajo busca aportar nuevos casos de uso que permitan determinar nuevos requisitos del sistema M2M, producto de las interacciones entre los dispositivos y el sistema.

El resto del trabajo se organiza de la siguiente forma. En el capítulo 2, se definen conceptos básicos relacionados con las comunicaciones M2M, con una breve descripción de los trabajos desarrollados por las organizaciones de estandarización involucradas con en las comunicaciones M2M, y también se mencionan las principales tecnologías de red utilizadas para el acceso, desde LAN hasta WAN.

Luego de una pequeña revisión de la tecnología, en el capítulo 3, nos dedicamos a analizar las especificaciones realizadas por los SDO, empezando por el ETSI donde se observa una tendencia clara para desarrollar un middleware M2M que ayude a solventar el problema de la heterogeneidad de las aplicaciones M2M. La heterogeneidad de protocolos inhibe la interoperabilidad entre los objetos inteligentes. Su intención es desarrollar interfaces (API's) abiertas que provean medios para que los dispositivos expongan sus capacidades de servicio, de modo que los dispositivos remotos puedan utilizarlos. La estructura del ETSI busca el desarrollo y mantenimiento de una arquitectura end-to-end para el sistema M2M, y además atender otras cuestiones como direccionamiento, localización, seguridad, gestión, entre otras.

El análisis continúa con los documentos propuestos por el 3GPP, donde se han atendido los requisitos que los servicios M2M y las comunicaciones M2M imponen a las redes de comunicaciones móviles, que hasta ahora están optimizadas para atender servicios Humano-a-Humano (H2H), que son sustancialmente diferentes a los servicios provistos en los sistemas M2M. Los grupos de trabajo del 3GPP además han provisto mejoras a la arquitectura y la interfaz de acceso de radio para soportar estas comunicaciones. Finalmente la revisión del IEEE muestra los avances para mejorar el bajo consumo de potencia, el soporte a un gran número de dispositivos, transmisión de ráfagas pequeñas, y seguridad de los dispositivos, dentro de la familia de estándares que forman las bases de WiMAX.

En el capítulo 4, se describen los entornos de aplicación (medición inteligente, red inteligente de distribución de energía, aplicaciones automotoras, e-salud, consumidor conectado, y automatización de la ciudad) que han sido considerados por los SDO como los principales ambientes para el desarrollo del M2M, y se describen algunos casos de uso utilizados para determinar los requisitos que debe tener un sistema M2M. Básicamente la mayor parte de las soluciones previstas están relacionadas con el uso de telemetría que ayudara a lograr el consumo eficiente de energía en las ciudades dentro del marco de las redes de energía inteligente (*SmartGrids*). En este capítulo, también se proponen algunos casos de uso para colaborar con la detección de nuevos requisitos del sistema.

2 Estado de la Tecnología

2.1 ¿Qué es M2M?

Durante mucho tiempo se intento dar un significado al acrónimo M2M, pero luego de algunos como Machine-to-Man o Machine-to-Mobile, finalmente ha sido asociado al término **Machine-to-Machine,** pertenece a una categoría de las tecnologías de la comunicación e información (TIC) que combina tecnologías de computación, energía y comunicaciones, para permitir la interacción autónoma de ordenadores, sensores inteligentes, procesadores embebidos y/o dispositivos móviles con sistemas y procesos remotos, con muy poca o incluso sin intervención humana [1].

M2M (machine-to-machine) sugiere un nuevo concepto de negocio, basado en la tecnología de telemetría original, que es utilizado para la transmisión automática y medición de datos desde orígenes remotos por medios cableados, de radio o de otra índole. El M2M representa una tecnología de red moderna que involucra básicamente tres tecnologías bastante conocidas: redes de sensores, Internet y ordenadores personales; quienes juntos crean lo que se conoce con el nombre de comunicación M2M.

Las comunicaciones M2M expanden el papel de la telemetría más allá de su uso común en la ciencia y la ingeniería, y la coloca en situaciones cotidianas, como las que ocurren a diario en entornos empresariales, del sector público o incluso de índole particular.

Este nuevo concepto encierra una gran promesa en la promoción del uso de la telemetría por parte de empresas, entes gubernamentales y personas particulares, por ejemplo, estas comunicaciones se pueden utilizar para controlar de manera más eficiente el estado de una infraestructura pública critica, con menor intervención humana, evitando de este modo la exposición a situaciones peligrosas que pudiesen poner en riesgo la integridad física de trabajadores.

Muchos de los casos de las comunicaciones M2M involucran una serie de dispositivos similares que ejecutan acciones con una aplicación, en otros casos estos dispositivos no se comunican directamente con la aplicación, por capacidades reducidas, sino que lo hacen mediante otro dispositivo, conocido como Gateway, que permite la comunicación efectiva. La figura 1, tomada de [1], refleja lo mencionado anteriormente.

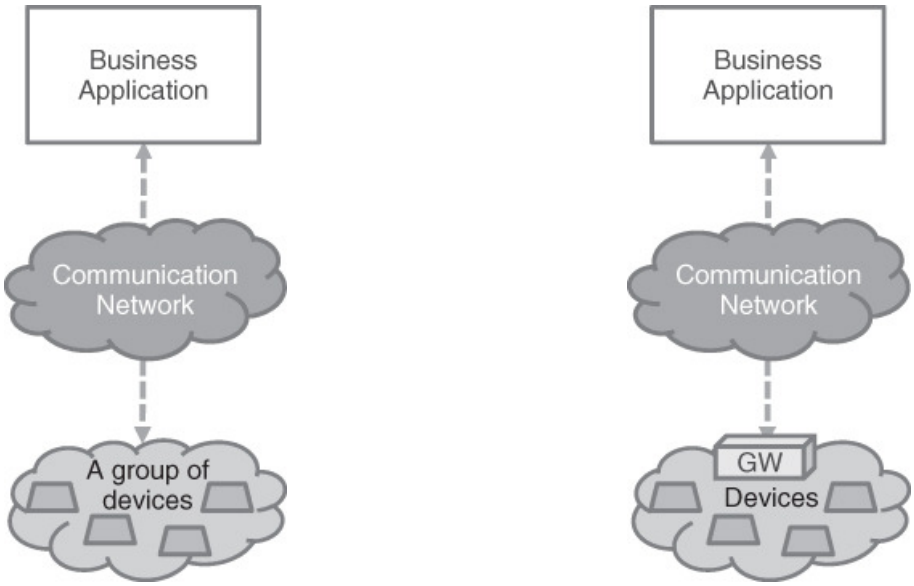


Figura 1. Base de la comunicación M2M

Para permitir esta conectividad entre dispositivos y aplicaciones, deberá establecerse una red de área M2M que proveerá el enlace físico y de acceso al medio (MAC) a todos los dispositivos que se conecten a ella, para luego conectarse con cualquier red pública mediante un enrutador o Gateway, el término "red de área M2M" fue introducido por el Instituto Europeo de Estándares en Telecomunicaciones (ETSI). En general, existen cuatro etapas comunes en las aplicaciones M2M, que son:

- Recolección de los datos
- Transmisión de los datos seleccionados a través de una red de comunicación
- Evaluación y análisis de los datos
- Respuesta a la información disponible

Los dispositivos a utilizar en estas comunicaciones deberán satisfacer aspectos calves, para permitir la interoperabilidad del sistema, como recursos de procesamiento limitados, bajo consumo de potencia, estar incorporados dentro de otros dispositivos, entre otras; sin duda estas restricciones tendrán un impacto en el desarrollo de los sistemas M2M, que también tendrán características particulares como son, control e interacción humana limitada, un numero potencialmente grande de dispositivos finales M2M, uso exclusivo de redes de conmutación de paquetes y un bajo volumen de tráfico por cada dispositivo final. Por su parte las aplicaciones también deberán tener cualidades específicas para atender requisitos de servicios muy diversos y que en algunas oportunidades serán críticos y salvadores de vida.

Es importante mencionar que existen algunas diferencias entre los dispositivos M2M y lo que se ha denominado como el internet de las cosas (IoT), ya que aun cuando comparten muchas similitudes una no es un subconjunto de la otra. En el caso del IoT, se habla de objetos pasivos, como los que funcionan con etiquetas RFID, que son controlados por sistemas de información y comunicación, sin embargo estas etiquetas pudieran ser procesadas por un escáner M2M para una aplicación especifica. Mientras que en las comunicaciones M2M, aun cuando son iniciadas por dispositivos, pueden ocurrir interacciones como las existentes entre maquina y humano.

Por las características de esta tecnología es lógico pensar que su utilización en entornos de ciudades inteligentes "Smart Cities" puede ser de gran utilidad, ya que las ciudades deben manejar un gran volumen de información y además de diversa naturaleza, por esta razón las comunicaciones M2M pueden proporcionar el soporte necesario para proveer una comunicación capaz de manejar ese flujo de información aprovechando las distintas tecnologías de acceso disponibles y además permitiendo garantizar una latencia acotada y reducida, ya que en la mayoría de los casos el requerimiento de la información es en tiempo real.

2.2 Estándares M2M.

Existe una iniciativa global por parte de los principales organismos de estandarización "SDO" (como son ARIB, ATIS, CCSA, ETSI, TIA, TTA y TTC), conjuntamente con la OMA, con el fin de crear una actividad cooperativa para la normativa de M2M. Algo similar a lo ocurrido para la conformación del 3GPP, en esta oportunidad el proyecto se ha denominado "oneM2M Partnership Project" el cual fue establecido oficialmente en julio del año 2012; sin embargo se espera que las primeras publicaciones se realicen en la segunda mitad del 2013.

Pese a eso, algunas empresas ofrecen sus propios estándares para la arquitectura M2M, mientras tanto las organizaciones continúan trabajando de forma independiente en el desarrollo de algunas especificaciones que permitan regular y facilitar el desarrollo de la tecnología. Basados en el 3er taller sobre M2M realizado por el ETSI [2] en octubre del 2012, las comunicaciones M2M dependen de muchas tecnologías a través de múltiples industrias, lo que a su vez conlleva a un ámbito de estandarización bastante amplio. La figura 2, exhibida durante el mismo taller del ETSI, es un bosquejo de la infraestructura básica en M2M, y en la que además se observan algunos de los organismos involucrados en busca de la estandarización de la tecnología. A pesar de que el ETSI no es la única fuente de estándares en el área de M2M, es el que más avanzado esta de todos los demás.

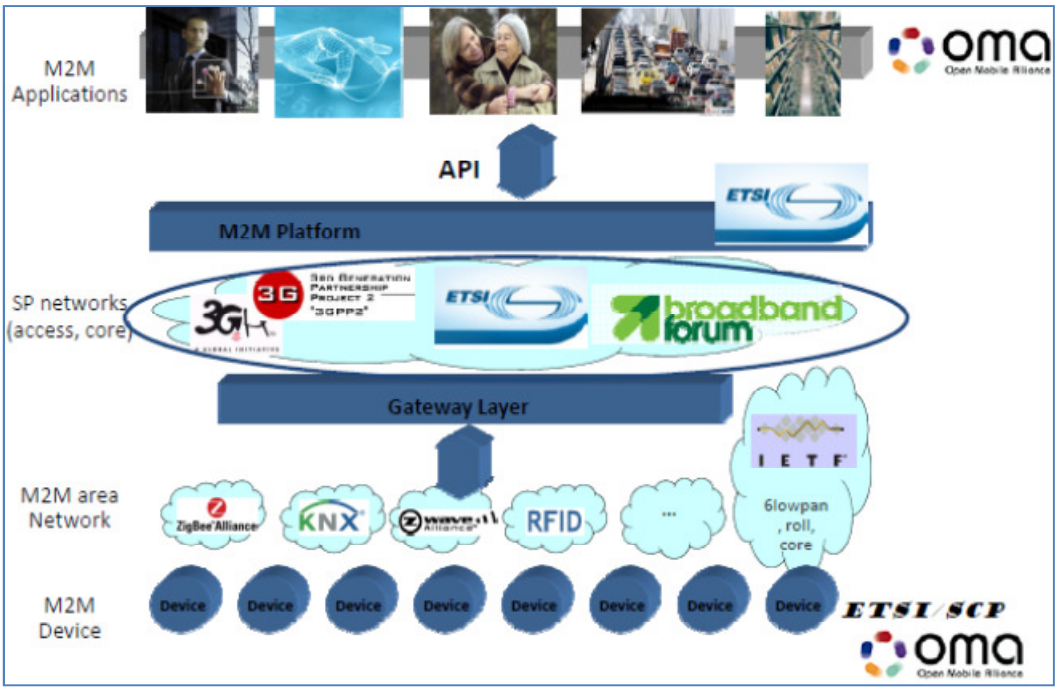


Figura 2. Infraestructura básica M2M (aportado por el ETSI)

El ETSI realizo el lanzamiento de la primera versión en 2012, la cual consta de 3 etapas y se enfoca en desarrollo de una arquitectura end-to-end con énfasis en la capa intermedia para los servicios (middleware), que involucra direccionamiento, localización, calidad de servicio, gestión, interfaces y otras cuestiones, de forma que los servicios sean independientes de las tecnologías existentes en las redes de acceso. Además, se especifican varias capacidades de servicios que permiten ofrecer las funcionalidades requeridas por diferentes aplicaciones M2M [3] [4] [5].

El 3GPP, por su parte mantiene y desarrolla las especificaciones y reportes técnicos para los sistemas de comunicaciones móviles; por este motivo se encargo de definir las características y requisitos para, las que definió como, comunicaciones tipo maquina (MTC) en [6], en esta especificación técnica se definen 2 escenarios para MTC, dispositivos MTC comunicados con uno o más servidores MTC y dispositivos MTC comunicados con otros dispositivos MTC.

En el primer caso los servidores MTC están conectados al proveedor de red y es así como se comunican con los dispositivos MTC, y en la otra forma los dispositivos pueden conectarse directamente entre ellos sin la necesidad de servidores intermedios.

Sin embargo, debido a que en el documento anterior solo se habían definido los requisitos necesarios de la red para soportar las comunicaciones MTC en redes de telefonía móvil celular "3GPP Release 11" se avanzó realizando una recomendación

técnica [7], para atender y solucionar los problemas encontrados, que estaban básicamente relacionados con la falta de control de congestión y datos para redes con amplio número de dispositivos MTC y su respectivo direccionamiento IP.

Como solución se plantea la gestión de dispositivos M2M basada en grupos y el uso de direcciones IPv6.

Entre tanto el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), estandariza la interfaz de aire y las funciones relacionadas con el bucle local inalámbrico (WLL), por medio de la especificación IEEE 802.16p [8], en la que se define un punto de agregación para dispositivos no compatibles con 802.16 u otros dispositivos M2M que si lo son.

En la tabla 1 se encuentra un resumen del alcance de las actividades realizadas por los organismos de estandarización activos en las comunicaciones M2M, quienes en su mayoría aun se encuentran desarrollando la primera versión.

SDO	Actividades M2M
ETSI	ETSI TS 102 689: especifica los requisitos de funcionamiento de cada elemento de red para un servicio M2M end-to-end. ETSI TS 102 690: define la arquitectura funcional end-to-end, identificando las entidades e interfaces involucradas. ETSI TS 102 921: contiene las especificaciones para las interacciones en los puntos de referencia de la arquitectura.
3GPP	3GPP TS 22 368: estudia las mejoras que se necesitan en la red para las comunicaciones entre dispositivos MTC. 3GPP TS 22 888: evalúa las mejoras en la red pertinentes en la arquitectura "Release 11" para solventar los problemas planeados en la especificación TS 22 368; además, se encuentra alineado con comités técnicos para comunicaciones M2M ETSI. 3GPP TS 23 682: introduce mejoras a la arquitectura propuesta inicialmente en TS 22 888, para facilitar la comunicación MTC con servidores externos.
IEEE	802.16p (WiMAX): optimización de la interfaz aire para bajo consumo de potencia, transmisión masiva, ráfagas pequeñas, y autenticación de dispositivos. Temas futuros: Gateway M2M, características avanzadas y cooperación entre redes M2M. 802.11 (WiFi): actualización de la interfaz de aire para permitir el uso del espectro sub-GHz. 802.15.4 (Zigbee): optimización de la interfaz aire para redes inteligentes
IETF	Está involucrado en la mayoría de los estándares relacionados con la optimización de las capas 1 y 2 de las redes capilares para sistemas M2M. 6LoWPAN: es un protocolo de comunicación basado en IPv6, ideado para hacer frente a las limitaciones de dispositivos con pocos recursos. Además se incluyen los protocolos ROLL y CoRE.

OMA	Ha desarrollado algunas especificaciones referentes a arquitecturas de habilitadores de servicio e interfaces abiertas que son independientes de las plataformas y redes subyacentes.
TIA	Se encuentra desarrollando y manteniendo los estándares de un medio físico agnóstico. Lo que permite la monitorización y comunicación bi-direccional de eventos y datos entre dispositivos inteligentes y otros dispositivos [9].
ITU	Se encarga del área de redes de sensores inteligentes, por medio de los grupos de trabajo de sensores ubicuos.
GSMA	Define una serie de módulos GSM para resolver problemas operacionales, como tarjeta UICC, interfaz de radio, gestión remota, autenticación y otros.

Tabla 1. Actividades realizadas por los SDO, para la estandarización de M2M.

La colaboración entre las organizaciones de estándares de diferentes industrias es necesaria para reducir sustancialmente los costos de desarrollo y mejorar el tiempo de comercialización de los sistemas M2M. Afortunadamente esta necesidad ha sido reconocida por las comunidades M2M y han unido esfuerzos para aumentar el número de colaboraciones entre ellos. De esa forma se han diseñado interfaces abiertas y arquitecturas de sistema estándar, además de una serie de plataformas comunes de software y hardware.

La experiencia previa demuestra que los primeros sistemas propietarios M2M (verticales) que se han implementado, en su mayoría tienen una gran dificultad para la escalabilidad; siendo esto la base para el desarrollo de nuevos sistemas horizontales en la industria M2M que permitan alcanzar una internet integrada; algo particularmente importante para los usuarios finales que en su mayoría serán residenciales.

2.3 Redes de Acceso

Las comunicaciones M2M poseen en general cinco características: control e interacción humana limitada, potencial número elevado de dispositivos, bajo volumen de tráfico por dispositivo, poco complejas y uso de redes de conmutación de paquetes. Anteriormente se describió que estas comunicaciones se basan en una arquitectura de red jerárquica, por ejemplo red de área personal (PAN), redes de área local (LAN) como la red de área residencial (HAN) y red de vecindario (NAN), y red de área amplia (WAN).

Para lograr una arquitectura unificada en las comunicaciones M2M, las redes M2M deberán ser transportadas sin problema alguno utilizando diferentes tecnologías de comunicación.

Empezando por la comunicación entre los dispositivos electrónicos inteligentes, Red M2M, que por sus características se podrán utilizar tecnologías como Bluetooth, ultra-banda ancha (UWB), Zigbee, WiFi, RFID y muchas más, algo que dependerá

básicamente del rango de cobertura requerido y el ámbito de cada aplicación. En la tabla 2 se describen algunas características de las tecnologías utilizadas para estas redes también conocidas como redes sensoriales inalámbricas.

Este tipo de red provee conectividad rápida y a bajo costo entre múltiples nodos dispersos sin una infraestructura preexistente, el cual es el caso de la mayoría de las aplicaciones reales M2M.

Igualmente encontramos las redes de banda ancha móvil que podrán utilizarse para la conexión entre los dispositivos M2M (sensores) y la plataforma M2M, ya que ofrecen una cobertura de radio sobre un área geográfica amplia, y soporta un gran número de componentes M2M remotos y distribuidos, además de soportar movilidad. Entre estas redes encontramos principalmente las redes celulares como el sistema universal de telecomunicaciones móviles (UMTS), interoperabilidad mundial para acceso por microondas (WiMAX) y la evolución a largo plazo (LTE).

Aunque el uso de redes fijas no se descarta para las comunicaciones machine-to-machine, se entiende que será muy limitado o nulo.

Característica	WiFi (IEEE 802.11x)	Bluetooth (IEEE 802.15.1)	UWB (IEEE 802.15.3)	ZigBee/6LoWPAN (IEEE 802.15.4)
Cobertura	<100m	<10m	<10m	10-100m
Banda de Frecuencia	2.4 GHz, 5GHz	2.4 GHz	3.1 – 10.6 GHz	2.4 GHz, 868MHz, y 915MHz
Velocidad	11b<11Mbps 11g<54Mbps 11n<144Mbps	1-3 Mbps	480 Mbps con radio impulsivo	20, 40 y 250Kbps
Tamaño Red	32 nodos	2 a 8 por picored	2	<65536
Potencia	Alta	Media	Alta	Baja
Vida Batería	Horas	1 semana	Horas	>1 año
Tipo Datos	Video, audio, archivos y foto	Video, audio, archivos y foto	Video, audio, archivos y foto	Pequeños paquetes
Aplicación principal	WLAN	WPAN	WPAN	Control y monitorización

Tabla 2. Características de tecnologías de redes sensoriales inalámbricas.

3 Revisión de Especificaciones M2M

3.1 Propuesta del ETSI.

El ETSI considera la red M2M como una estructura formada por 5 partes [4]: (1) Dispositivos M2M, los cuales se encuentran usualmente embebidos dentro de algún dispositivo inteligente y son capaces de responder a peticiones o enviar información, ejecutando aplicaciones M2M que utilizan capacidades de servicio M2M. (2) Red de área M2M, permite las conexiones entre toda clase de dispositivos inteligentes y las puertas de enlace. (3) Puerta de enlace (Gateway's), actúan como una entrada para otras redes, además de proveer interacción e interconexión entre los dispositivos. (4) Red de comunicación, la cual permite conexiones entre las puertas de enlace y las aplicaciones. (5) Aplicaciones, transfieren datos a través de diversos servicios, y son utilizadas por motores de procesos de negocio específicos; básicamente analizan los datos, toman acciones y reportan resultados.

Estos 5 elementos básicos de la arquitectura M2M conforman 3 dominios, como se aprecia en la figura 3:

- **Dominio de Gateway y dispositivos,** la primera parte de la arquitectura está compuesta por 3 elementos: dispositivos M2M, red de área M2M y Gateway´s M2M.

Dispositivos M2M, quienes pueden conectarse al dominio de red por **Conexión directa,** donde los dispositivos se conectan a través de la red de acceso y ejecutan los procedimientos de registro, autenticación, autorización, gestión y aprovisionamiento con el dominio de red. La segunda opción es **Gateway como proxy,** allí la conexión de los dispositivos con el dominio de red se realiza mediante uno o múltiples Gateway M2M, y para conectarse a este Gateway los dispositivos utilizan la red de área M2M. Esta conexión tiene esa denominación ya que el Gateway M2M actúa como un proxy para el dominio de red de cara a los dispositivos M2M.

Red de área M2M, cumple la función de proporcionar conectividad entre dispositivos y Gateway M2M. Entre los ejemplos de estas redes capilares se encuentran: tecnologías de redes personales como Zigbee, Bluetooth, IEEE 802.15.1, entre otras; o redes locales como PLC, M-BUS o KNX.

Gateway M2M, es un Gateway que ejecuta aplicaciones M2M utilizando sus capacidades de servicio M2M. Se utilizan para dar servicio a dispositivos preexistentes (como sensores), que no poseen capacidades de servicio M2M, mediante las aplicaciones del Gateway que recolectan y procesan diversos datos específicos que luego son enviados al dominio de red.

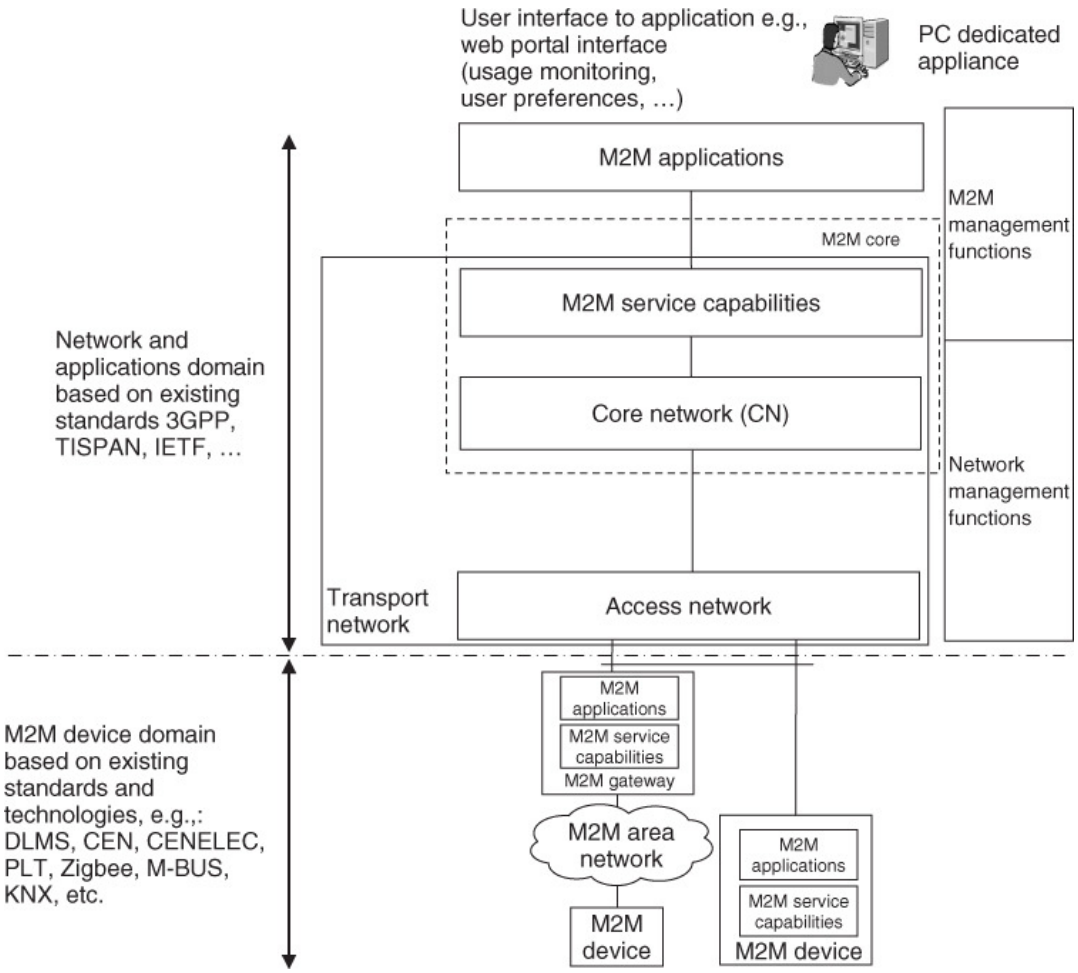


Figura 3. Arquitectura de alto nivel M2M (tomada del ETSI).

- **Dominio de red,** dentro de este dominio se encuentra tanto la red de comunicaciones como las capacidades de servicio M2M, y está formado por:

Red de acceso, permite la comunicación de los elementos del dominio M2M con el núcleo de la red, se incluyen redes como xDSL, HFC, WiMAX, satelital y redes celulares de segunda, tercera y cuarta generación (UTRAN, eUTRAN), entre otras.

Núcleo de red, es el encargado de proveer conectividad IP, interconexión con otras redes, itinerancia, además de las funciones de servicio y control de la red. En esta se incluyen los núcleos de red conocidos de redes 3GPP, ETSI TISPAN y otros más.

Capacidades de servicio M2M, es la encargada de proveer las funciones M2M que compartirán las aplicaciones, exponer funciones mediante una serie de interfaces abiertas, utilizar las funcionalidades del núcleo de red, además de optimizar y simplificar el desarrollo de aplicaciones sin importar las especificaciones de la red.

- **Dominio de aplicaciones,** tal como su nombre lo expresa se encuentran las aplicaciones que ejecutan la lógica del servicio y utilizan las capacidades de servicio M2M por medio de la interfaz abierta que se haya definido.

Adicionalmente dentro del dominio de red descrito, el ETSI define 2 funciones de gestión (Red y M2M), de la siguiente forma:

Gestión de red, consiste en todas aquellas acciones requeridas para gestionar tanto la red de acceso como el núcleo de la red como son: supervisión, aprovisionamiento, gestión de fallas, entre otros.

Gestión de M2M, involucra las funciones necesarias para gestionar las capacidades de servicio M2M dentro del dominio de red. Entre estas funciones encontramos la MSBF (M2M Service Bootstrap Function), cuyo objetivo es facilitar la creación de credenciales de seguridad permanentes en la capa de servicios M2M del dispositivo M2M y también la iniciación de capacidades de servicio M2M en el dominio de red.

Estas credenciales se almacenan en un lugar seguro llamado MAS (M2M Authentication Server), que puede ser un servidor AAA que se comunique con la función MSBF por medio de una interfaz con protocolo "Diameter", para así almacenar las credenciales de seguridad. De esta forma la gestión de los dispositivos y Gateway M2M se realiza directamente por medio de una de las capacidades del servicio M2M.

3.1.1 Capacidades de Servicio M2M.

En la capa de capacidades de servicio M2M (xSCL, Service Capabilities Layer) se ofrecen una serie de funcionalidades las cuales son expuestas en interfaces lógicas llamadas puntos de referencia, las cuales pueden apreciarse en la arquitectura funcional que se describe en la figura 4 (dIa, mIa y mId).

Por otra parte se aprecia que estas capacidades de servicio M2M (M2M SC, por sus siglas en ingles), pueden interactuar con el núcleo de la red por medio de interfaces abiertas conocidas y especificadas por los organismos competentes.

Dentro de la estructura del modelo de capas se han definido una serie de capacidades de servicio M2M específicas, las cuales se pueden implementar en los dominios de la arquitectura M2M y de ese modo ofrecer diferentes funcionalidades que dependerán del lugar donde se haya implementado la M2M SC, pudiendo ser la **Red**, el **Gateway** o el **Dispositivo**. Esto mismo ocurre con las aplicaciones M2M que podrán implementarse en diversos elementos de la arquitectura.

Entre las principales capacidades de servicio encontramos:

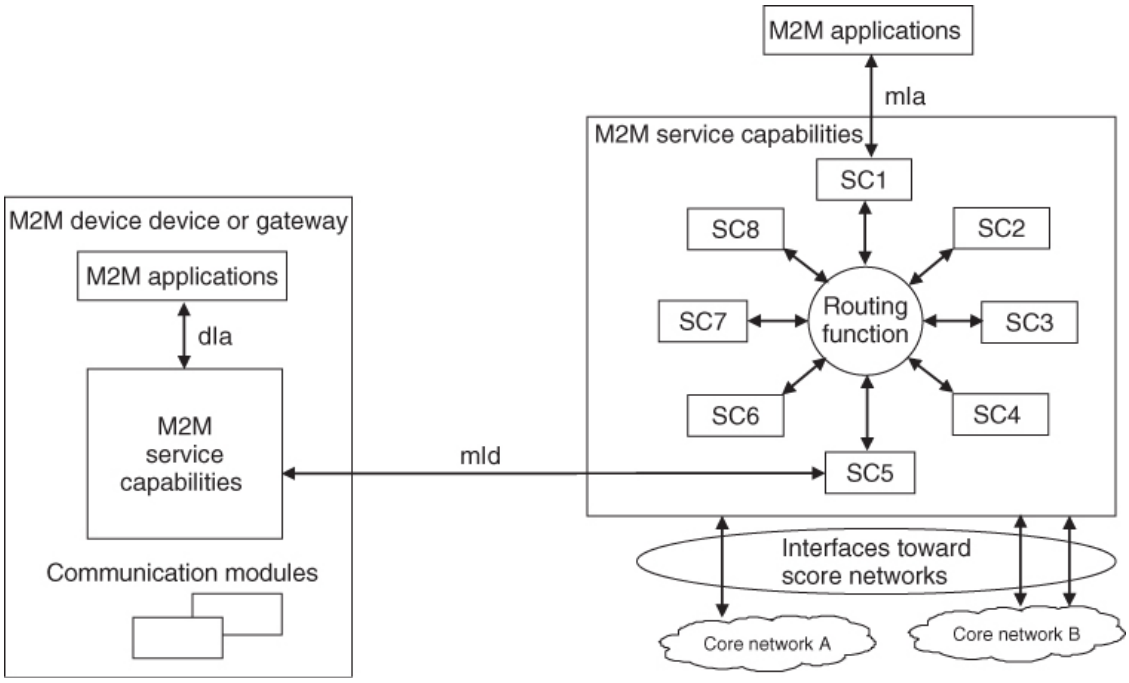


Figura 4. Arquitectura funcional de las comunicaciones M2M (tomada del ETSI).

Habilitación de Aplicación (xAE), ofrece la posibilidad de exponer todas las funcionalidades implementadas en la capa M2M SC a través de un único punto de contacto que serian las interfaces lógicas mIa o dIa, y también permite a las aplicaciones registrarse en su respectiva capa M2M SC.

Comunicación Genérica (xGC), proporciona el punto de contacto entre las capas M2M SC, es decir, la interfaz mId. Su principal función es proveer el establecimiento y liberación de las sesiones de transporte y participar en la negociación de claves de seguridad que permitan la protección de los datos que se intercambian entre las capas.

Accesibilidad, Direccionamiento y Repositorio (xRAR), es la encargada de realizar la función de mapeo entre el nombre de un dispositivo o Gateway con direcciones de red enrutables, de igual forma permite crear, eliminar y listar un grupo de dispositivos o Gateway's, y gestiona el almacenamiento de datos de las capas y aplicaciones para que estén disponibles ante cualquier petición.

Selección de la Comunicación (xCS), cuando algún elemento del sistema puede ser alcanzado por diferentes redes esta capacidad permite la elección de la red preferida basada en políticas, además de seleccionar alguna red alternativa en caso de ocurrir un fallo de comunicación.

Gestión de Entidad Remota (xREM), mediante esta capacidad se proveen funciones de gestión de configuración, gestión de fallas y gestión de prestaciones. Se soportan

diferentes protocolos de gestión de modo que es posible gestionar diversos dispositivos, y contiene un mecanismo encargado de notificar el protocolo a utilizar.

Seguridad (xSEC), esta capacidad provee funcionalidades como soportar el "bootstrap" del servicio M2M, soportar la utilización de jerarquía de claves para autentificación y autorización, y también ejecuta la autentificación mutua y el acuerdo de claves.

3.1.2 Puntos de Referencia.

Adicionalmente se han definido puntos de referencia específicos para cada una de las posibles interacciones que ocurren en la arquitectura de modo que el punto de referencia **mIa**, es la interfaz para la comunicación entre las aplicaciones de red (NA) y la capa de capacidades de servicio que se encuentran en el dominio de red (NSCL), y ofrece funciones como el registro de aplicaciones, la lectura y/o escritura de información en cualquiera de las capas SCL y la solicitud de acciones para la gestión de dispositivos.

La interfaz **dIa** permite a las aplicaciones alojadas en un dispositivo (DA) acceder a la capa de capacidades de servicio del dispositivo (DSCL) o un Gateway (GSCL), y también permite a las aplicaciones de Gateway (GA) acceder a la capa de capacidades de servicio del Gateway (GSCL), se encarga de ofrecer funcionalidades similares al punto de referencia anterior.

Finalmente **mId** es la interfaz de comunicación entre la capa de capacidades de servicio de un dispositivo (DSCL) o Gateway (GSCL) con la capa de capacidades de servicio en el dominio de red (NSCL) y viceversa, este punto de referencia además de ofrecer las funcionalidades de los anteriores está involucrado en acciones relacionadas con la seguridad, como es el establecimiento de jerarquía de claves.

En la figura 5, se encuentra un diagrama que representa la asignación de los puntos de referencia en los diferentes escenarios M2M que han sido considerados por el ETSI, en el mismo se distinguen, además de las interfaces, los siguientes elementos:

Gateway (G), este elemento debe proveer todas las capacidades de servicio M2M de la capa (GSCL), la cual utiliza el punto de referencia mId para comunicaciones con la capa (NSCL), y el punto de referencia dIa para la comunicación con las aplicaciones de dispositivos y Gateway (DA, GA).

Dispositivos (D), es aquel que provee las capacidades de servicio M2M de la capa (DSCL), que a su vez utiliza el punto de referencia mId para comunicaciones con la capa (NSCL), y el punto de referencia dIa para la comunicación con DA.

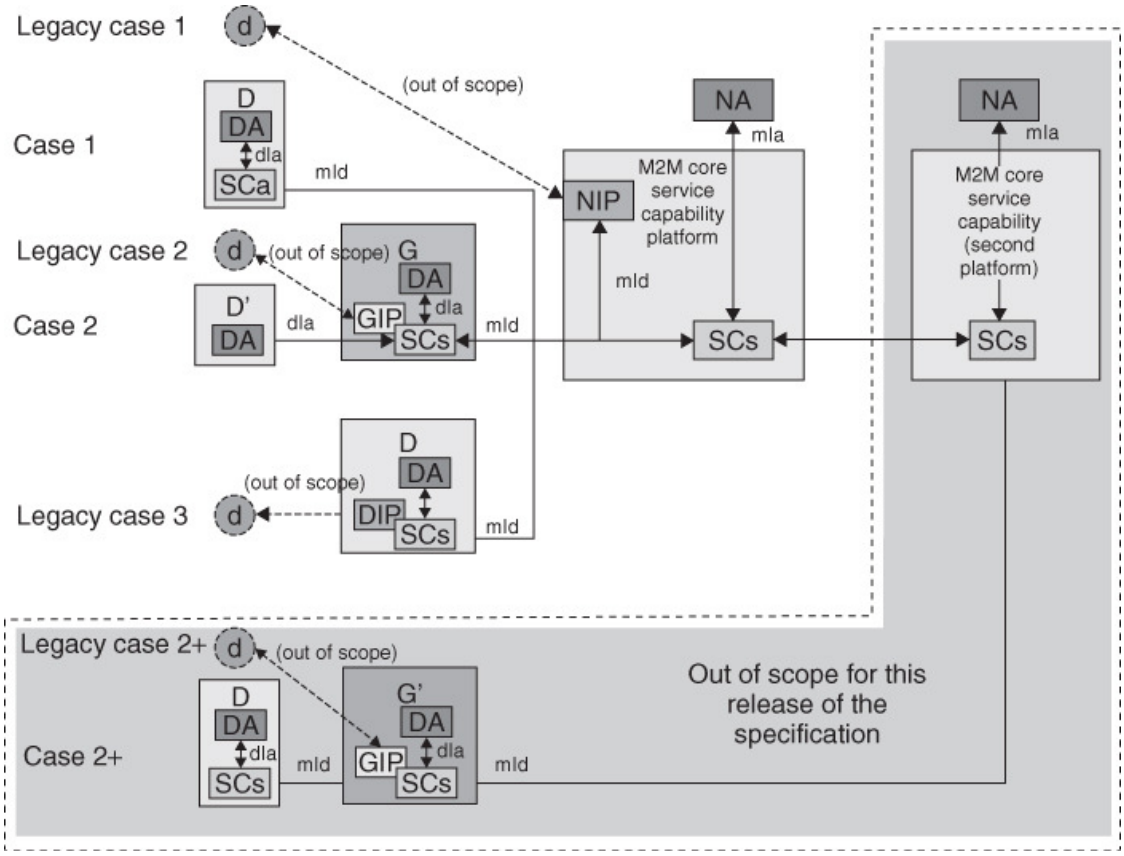


Figura 5. Estructura de las interfaces lógicas en los diferentes escenarios M2M (tomada del ETSI).

Dispositivos' (D'), este tipo de dispositivo no provee las capacidades de servicio M2M de la capa (DSCL). Sin embargo, albergan aplicaciones DA que se comunican hacia la (GSCL) por medio del punto de referencia dIa.

Dispositivos (d'), por ultimo encontramos estos dispositivos que no cumplen con el modelo de capas M2M del ETSI. Por lo tanto no utilizan las interfaces lógicas definidas, sino que por el contrario se conectan a cualquiera de las capas SCL mediante una capacidad de servicio M2M que se ha establecido como opcional y se ha denominado **Proxy de Interoperabilidad xIP** (NIP, GIP, DIP). Este escenario se ha considera fuera del alcance del presente estándar.

3.1.3 Identificación y Direccionamiento.

Para la comunicación efectiva entre diferentes entidades del sistema M2M se han definido una serie de identificadores que luego se deben convertir en direcciones de red entendibles para la red exterior.

Encontramos identificadores para aplicaciones **(App-ID),** nodos **(M2M-Node-ID),** capas **(SCL-ID),** proveedor de servicios **(M2M-SP-ID),** entre otros. Cada uno de ellos deberá ser globalmente único para que permita diferenciar todas las conexiones que se

pudieran establecer entre diferentes elementos del sistema M2M; algunos de estos identificadores deberán ser asignados de forma estática por el proveedor de servicios, mientras que otros se asignaran a medida que ocurran las interacciones del sistema

Una vez se han identificado los elementos presentes en la comunicación M2M es necesario el direccionamiento, cuyo principal objetivo es contactar a una determinada capa SCL en la cual se ha registrado una aplicación X, y luego ubicar el dispositivo o Gateway correcto donde reside esa aplicación para permitir el intercambio de información efectivo entre las entidades.

En otras palabras la accesibilidad y el enrutamiento desde y hacia diferentes aplicaciones están ligados con la capa SCL en la cual se encuentre registrada la aplicación, y a su vez con el nodo M2M D/G que se encuentra conectado a la red de acceso, por lo tanto para alcanzar cualquier aplicación es necesario hacerlo primero con la capa SCL en la cual se encuentra registrada.

Para completar esta acción se ha definido un punto de contacto denominado **"M2MPoC",** el cual es el encargado de aportar toda la información necesaria, desde la óptica de la red, para contactar con una SCL; ya que la información que se encuentra disponible en este punto puede ser traducida en direcciones de red.

Este punto de contacto se proporciona al sistema M2M cuando la capa SCL se registra en el mismo, de modo que para los dispositivos (D) será al momento de registrarse la capa DSCL, mientras que para aquellos dispositivos que no implementan el modelo de capas (D'), ocurrirá cuando se registre la capa GSCL. La información contenida en estos puntos M2MPoC dependerá de la red de acceso y los dispositivos de transporte M2M.

El hecho de que la información de enrutamiento contenida en los M2MPoC dependa de las características de la red de acceso, define el criterio con el cual se deben actualizar los puntos de contacto. La forma más fácil de obtener la información de enrutamiento de una SCL es mediante la asignación estática de direcciones publicas a los dispositivos y Gateway's, ya que esto permitiría implementar traducción de direcciones con DNS estático o dinámico. En cualquiera de los casos el M2MPoC deberá contener un identificador URI que cumpla con el debido RFC 3986 [10].

3.1.4 Marco de Seguridad.

En la figura 6 se observa la arquitectura M2M enfocada desde el punto de vista de la seguridad. Los principales componentes para la seguridad en estas comunicaciones son las capacidades de servicio NSEC, NGC, y NREM.

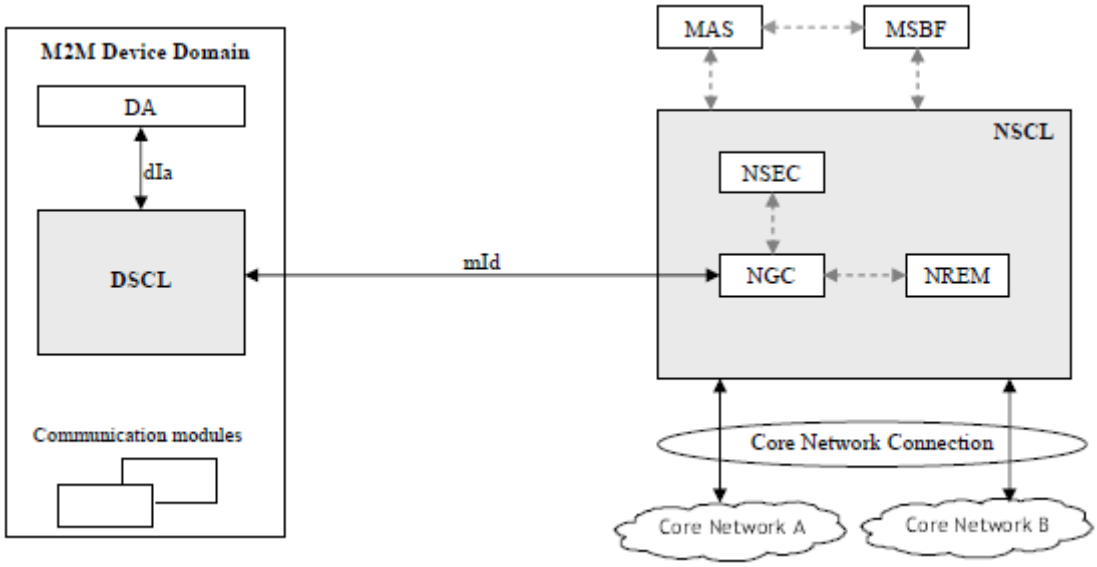


Figura 6. Arquitectura funcional para el marco de la seguridad en M2M (tomada del ETSI).

Para los procesos de autentificación y autorización de las comunicaciones se establecen claves con diferentes niveles (jerarquía de claves), las cuales se clasifican así:

Kmr, es la clave raíz del sistema M2M y se utiliza para la autenticación mutua entre los nodos D/G y el proveedor de servicios M2M. En el nodo de red la clave es almacenada en un ambiente seguro dentro del servidor MAS para evitar su uso por entidades no autorizadas, mientras que del lado de los dispositivos D/G se almacena dentro de un ambiente seguro controlado por el proveedor de servicios. Solo existe una Kmr por cada grupo de nodos D/G que se encuentran registrados en el sistema.

Kmc, es la clave de conexión M2M y se deriva de la clave raíz una vez se completa con éxito la autenticación mutua entre un nodo D/G y el proveedor de servicios de Red. A pesar de que la clave se genera en el servidor MAS, luego se almacena en el dominio local por medio de la NSEC. Se genera una clave diferente cada vez que se establezca una nueva conexión entre un nodo D/G y un nodo de Red, y cuando finaliza esa conexión expira la clave correspondiente.

Kma, es una clave opcional relacionada con las aplicaciones, son generadas por la NSEC partiendo de las Kmc. Se basa en un secreto compartido entre el dominio de red y las aplicaciones que se encuentran en los dispositivos y Gateway's que permita establecer asociaciones seguras para el intercambio de información sobre la interfaz mId. En la figura 7 se representa el esquema de jerarquía mencionado.

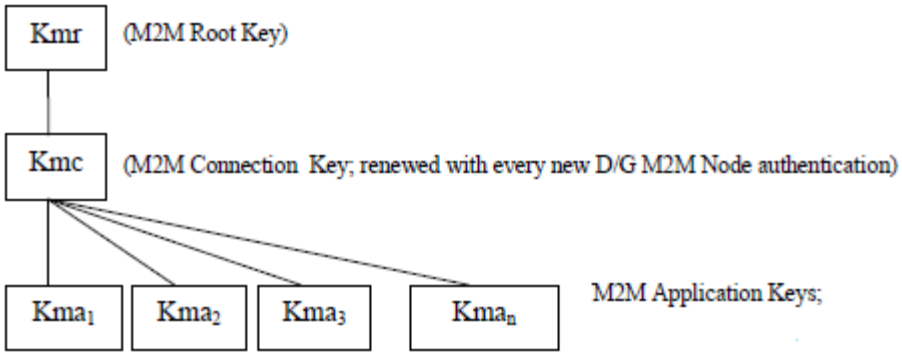


Figura 7. Esquema de claves jerárquicas M2M (tomada del ETSI).

La seguridad en la interfaz mId es muy importante ya que la misma debe soportar autentificación, integridad, protección, confidencialidad y privacidad de los datos, y se podrá lograr por cualquiera de los métodos siguientes:

Seguridad de la red de acceso, en caso de que se implemente en la red de acceso algún mecanismo de seguridad, y que por la relación que hay entre esta y la red M2M, se le permita al sistema M2M confiar en la seguridad de la red de acceso, se podrá sustituir la capa de seguridad M2M y utilizar la capa subyacente de seguridad de la red. Sin embargo esta opción no es muy recomendable y en todo caso se debe hacer un estudio profundo antes de realizar esta sustitución.

Seguridad del canal, se debe proporcionar el establecimiento de un canal seguro entre D/GSCL y la NSCL, utilizando protocolos como TLS (Transport Layer Security) o IPSec. Las claves Kmr y Kmc deben ser secretos compartidos por los nodos para que les permita realizar la autenticación mutua. Por último, el establecimiento del canal seguro solo puede realizarse una vez finalizado el procedimiento de conexión del servicio M2M, y una vez concretado es cuando debe comenzar el intercambio de información en la interfaz mId.

Seguridad de un objeto del sistema, la seguridad en un sistema M2M también puede alcanzarse a nivel de los objetos. Cuando se realiza la seguridad del canal, quiere decir que toda la información recibirá el mismo tratamiento, y en caso de que solo una parte de los datos enviados requieran ser cifrados, igualmente se realizara el cifrado de todos. Si se aplica la seguridad al nivel de los objetos esto permite mejorar la eficiencia en el uso de los recursos del sistema, de modo que cada pieza de datos puede ser tratada con protección de identidad y cifrada de forma independiente y sin importar que tratamiento se le dé al resto de la información.

Los sistemas M2M deberán implementar al menos uno de los dos últimos mecanismos (seguridad del canal o del objeto) en la D/GSCL y la NSCL. Mientras que

para proteger la interfaz mId se deberá implementar alguno de los tres, o también existe el caso donde pudieran combinarse más de uno.

Los requisitos de seguridad, en los diferentes nodos M2M, para la gestión de las claves y para los procedimientos de conexión del servicio M2M estarán definidos por las capacidades de seguridad del sistema M2M que se mencionaron anteriormente NSEC, GSEC y DSEC, donde cada una cumplirá un papel importante en el establecimiento de una comunicación segura.

3.1.5 Establecimiento de la comunicación M2M.

Cuando se implementa el modelo de capas (SCL) descrito anteriormente para establecer las comunicaciones M2M se deben cumplir una serie de etapas, de las cuales destacan 6 procedimientos principales que se aprecian en el diagrama de flujo de la figura 8.

Lo primero que debe ocurrir es el **arranque de la red**, en la cual se configura el dispositivo o Gateway M2M con la información mínima que necesita para acceder y registrarse en la red de acceso, fija o móvil. Como ejemplo se pueden citar los equipos que dispongan de una tarjeta electrónica (UICC), en la cual se carga toda la información para el registro.

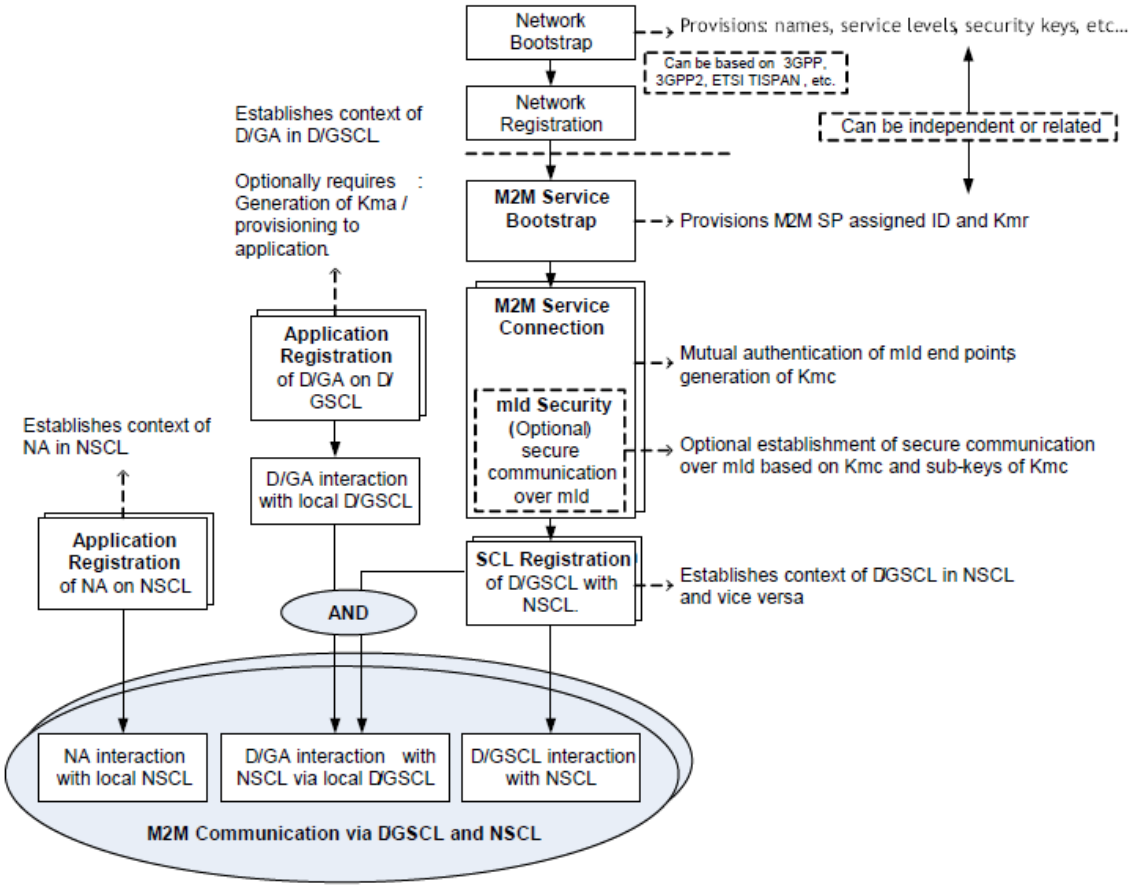


Figura 8. Diagrama de flujo de eventos M2M (tomada del ETSI).

Una vez se configurada la información inicial de la red entonces debe producirse el **registro en la red**, específicamente el registro de dispositivos y Gateway's M2M en la red de acceso, este proceso dependerá del estándar adecuado para la red utilizada; como ejemplo puede ser el proceso que se lleva a cabo en una red 3GPP donde se autentifican mutuamente ambos extremos (red de acceso y equipos), acordando entre otras cosas las claves de seguridad para esa sesión, al igual que la asignación de direcciones IP.

Se puede notar que esos 2 procesos iniciales dependen principalmente de la red de acceso elegida, por tanto deberán estar bien regulados por sus respectivos estándares y se consideran fuera del alcance del estándar M2M desarrollado por el ETSI.

Arranque del Servicio M2M.

El establecimiento de la comunicación continúa con el **arranque del servicio M2M**, se produce entre un dispositivo o Gateway y el servidor MAS que se encuentra en el dominio de red, en donde se proveen a los equipos las credenciales SCL permanentes (identificadores y la clave Kmr); las cuales se utilizaran luego para la autenticación mutua y el intercambio seguro de información entre las capas tipo D/G y la capa de red NSCL. Dependiendo el nivel de confianza que pueda existir entre el proveedor de red y el proveedor de servicios M2M, este procedimiento podría obviarse si las credenciales se provisionan previamente en los equipos. Por último, si los equipos soportan "validación de integridad" esta validación deberá completarse antes de iniciar el proceso de arranque del servicio M2M.

Del estándar se sugieren un par de principios por los cuales es posible completar este procedimiento, uno es dependiente y el otro independiente de la red de acceso. En el primero se asume la existencia de una relación comercial de confianza entre ambos proveedores (red y servicios) de forma que permita el intercambio de información por medio de la interfaz de red provista sin comprometer la seguridad de la comunicación, esto se conoce como arranque **Asistido por la Red de Acceso**.

Dentro de este modelo encontramos 3 opciones diferentes para completar el proceso de arranque del servicio M2M, la primera opción se ejecuta basada en los protocolos de la arquitectura **GBA** (Generic Bootstrapping Architecture), y es iniciado por los nodos M2M D/G a través de la interfaz Ub; existen 2 modos de realizar este arranque, uno es basado en el equipo (GBA-ME) y el otro en la tarjeta electrónica UICC que puedan contener los equipos (GBA_U), este último es un poco más seguro ya que evita que las claves generadas se compartan por completo en la red, sin embargo depende de tarjetas que soporten el proceso GBA, tal y como se describe en la especificación TS 133 220 [11].

Por otra parte los nodos conjuntamente con la función de arranque del servicio (MSBF) deben ejecutar una autenticación HTTP "Digest" basada en el protocolo AKA, que de ser exitosa le asegura a ambos extremos que están compartiendo la misma clave, y que esta será utilizada como la clave raíz M2M (Kmr); luego la MSBF es la encargada de proveer tanto al nodo M2M como al servidor MAS, los identificadores M2M-Node-ID y SCL-ID. Como resultado final de este proceso se obtiene una asociación segura entre un nodo M2M D/G y la función de arranque del servicio M2M, que consta de claves compartidas y del identificador de la transacción de arranque (B-TID), en la especificación TS 124 109 [12] se encuentran más detalles relacionados al proceso de arranque del servicio.

La segunda opción se basa en el uso del protocolo de autenticación extensible **EAP**[13], utilizando las credenciales de la red de acceso que se encuentran en el modulo de identidad del suscriptor **(EAP-SIM)** o el mecanismo de autenticación y acuerdo de claves **(EAP-AKA),** se debe resaltar que cualquiera sea el caso elegido para implementar un procedimiento de arranque del servicio M2M basado en EAP se debe realizar sobre el protocolo para transportar autenticación para redes de acceso **PANA**[14] por lo que finalmente la solución a implementar será sobre **EAP/PANA**. Por otra parte el procedimiento de arranque del servicio M2M basado en EAP/PANA es indiferente a las credenciales y métodos de autenticación utilizados entre los nodos M2M D/G y la MSBF lo que le permite ser utilizado en arranque del servicio asistido por la red y arranque del servicio independiente de la red de acceso. Mas detalles sobre estos mecanismos para autenticación y distribución de claves están en [15] y [16].

La tercera y última opción para el arranque del servicio asistido por la red de acceso está basada en EAP, pero en esta oportunidad se utiliza el procedimiento de autenticación en la red de acceso para generar la clave raíz Kmr, de esta forma en lugar de realizar una doble autenticación del nodo M2M D/G (una para la red de acceso y otra para el arranque del servicio) solo se cumple la primera etapa, lo que sin duda ayudaría a realizar un arranque del servicio más rápido, sin embargo la relación entre ambos proveedores deberá ser de extrema confianza puesto que se deben compartir toda la información de las claves, así que este escenario es más probable de ocurrir cuando se trate del mismo operador de red y servicio M2M. Además este mecanismo aplica solo en caso de redes que realizan autenticación mutua entre dispositivos y servidor AAA como son Ethernet, WiFi, WiMax, entre otras.

El segundo principio para el arranque del servicio M2M se conoce como arranque **Independiente de la Red de Acceso**, esta alternativa se presenta para los casos donde la red de acceso no facilita el arranque del servicio, por lo general ocurre cuando no existe una relación comercial entre ambos proveedores, o entre el fabricante de los

nodos D/G y el proveedor de servicios M2M, o incluso en aquellas situaciones donde en la red de acceso no se implementen características de seguridad que ofrezcan suficiente fiabilidad para realizar el proceso de arranque del servicio M2M. Una característica de estos mecanismos, es que también pueden utilizarse para realizar el arranque del servicio a pesar de que el proceso pueda ser asistido por la red de acceso, si así lo prefiriere quien realice el despliegue de la solución M2M.

Como se indico anteriormente el protocolo EAP no depende de las credenciales de la red de acceso y por eso es el que mejor se adapta ante estas situaciones; se debe utilizar inicialmente para la autenticación mutua entre los nodos M2M D/G y la MSBF, y luego combinarse con algún protocolo de generación de claves. Finalmente se podrán utilizar cualquiera de los métodos EAP para autenticación mutua y generación de claves como **EAP-TLS** [17], **EAP-IBAKE** [18], entre otros; pero siempre combinado con PANA como protocolo de transporte para EAP y los parámetros del arranque M2M.

Para ejecutar el proceso con EAP, el Dispositivo o Gateway M2M es el encargado de implementar la funcionalidad peer de EAP, mientras que la MSBF deberá fungir como el servidor de autenticación. Igualmente para poder transportar la información necesaria sobre PANA, los nodos D/G M2M deben implementar las funcionalidades de un cliente PANA (PaC), y el nodo de red M2M la funcionalidad del agente de autenticación PANA (PAA), tal y como se describe en las respectivas especificaciones. Con relación al protocolo AAA que debe implementarse en la interfaz entre el nodo de red y la MSBF no hay un mandato para el uso de alguno en específico sino que se mencionan los protocolos RADIUS y Diameter como posibles candidatos, esto implica que ambos deberán implementar funcionalidades adicionales como cliente AAA (nodo de red) y servidor AAA (MSBF).

Como última opción para completar el proceso de arranque del servicio M2M está la autenticación mediante el protocolo de "seguridad en la capa de transporte" **TLS**, el cual presenta 2 variantes **EAP-TLS** [19] quien utiliza igualmente el protocolo PANA como medio de transporte EAP, y **TLS sobre TCP**. En ambos casos el proceso se inicia con la autenticación mutua entre el nodo D/G y la MSBF mediante el saludo TLS (handshake) el cual se basa en certificados de dispositivo y certificados de servidor; luego de completar el proceso y que se establezca la conexión segura se genera la clave raíz Kmr y se envía conjuntamente con el identificador M2M-Node-ID desde la MSBF hacia el nodo D/G; por último la MSBF envía los parámetros que se han generado hacia el servidor MAS para su almacenamiento.

Conexión del Servicio M2M.

Cuando la implementación del sistema M2M se basa en la seguridad de la red de acceso, no es necesario generar la clave Kmc para la seguridad de la conexión en el

punto de referencia mId, por esta razón se considera que el procedimiento para la conexión del servicio M2M es opcional. Sin embargo como esta decisión se toma por quien implemente el servicio, tanto los nodos M2M D/G como los nodos de red M2M deben estar configurados para soportar este procedimiento.

Al igual que ocurre con el procedimiento de arranque del servicio M2M, la conexión del mismo dependerá de la relación existente entre los proveedores de red y servicios M2M, destacando así métodos basados en **GBA, TLS–PSK,** y **EAP/PANA**. En cualquier situación deberán cumplirse, primero la autenticación mutua entre ambos extremos de la conexión (interfaz mId), D/G SCL y NSCL, y luego la generación de la clave de conexión M2M, Kmc.

En aquellos casos donde el proveedor de servicios sea el mismo que el proveedor de la red, se recomienda realizar el proceso mediante GBA, el cual iniciara con la autenticación mutua entre el nodo D/G y la función BSF (procedimiento de arranque del servicio). Luego de completar la autenticación y obtener la clave raíz Kmr, se utilizan los parámetros relacionados con esa asociación (B-TID) para generar la clave de conexión, denominada Kmc, que permitirá establecer una sesión segura entre el dispositivo o Gateway y el nodo de red (NSCL) mediante un túnel TLS; es decir, que se combinan las credenciales de seguridad con el mecanismo de autenticación basado en claves compartidas (TLS- PSK) para de esta forma generar la Kmc a partir de la Kmr; este método se encuentra detallado en [12].

El segundo método basado TLS-PSK establece que el proceso será asistido por el servidor MAS, donde se encuentra almacenada la clave raíz Kmr generada durante el procedimiento de arranque del servicio M2M basado en cualquiera de los protocolos descritos en la sección 2.5.1. A diferencia del anterior basado en las credenciales GBA, el saludo TLS-PSK se ejecutara entre el nodo M2M D/G y el servidor MAS según lo desarrollado en el RFC 4279 [20].

Por último la conexión del servicio M2M igualmente puede realizarse basada en el protocolo EAP/PANA, donde también se utilizan las credenciales que se han obtenido del procedimiento de arranque como el M2M-Node-ID y la clave Kmr para la autenticación entre el nodo D/G y el servidor MAS por intermedio de la capa NSCL, lo que conlleva a realizar la conexión en 2 fases, primero el protocolo EAP es soportado sobre PANA para la conexión entre las capas D/G SCL y la NSCL (interfaz mId), y luego EAP se soporta sobre un protocolo AAA en la interfaz entre la NSCL y el MAS. Se puede ejecutar el proceso de autenticación mutua por cualquiera de los métodos EAP-SIM, EAP-AKA antes mencionados o EAP-GPSK [21]. Una vez completado el proceso entonces se genera la clave de conexión Kmc, mediante una fórmula. En caso

de que se requiera liberar la conexión se deberá seguir el procedimiento establecido por el protocolo PANA para la liberación de conexiones.

El proceso de conexión del servicio deberá repetirse para cada una de las sesiones que desee establecer un nodo D/G con la capa NSCL. Igualmente en caso de que el proveedor de servicios soporte validación de la integridad (IVal), el nodo de red deberá obtener desde el servidor MAS, durante el proceso de conexión, los atributos de seguridad IVal que poseen los nodos D/G que intentan establecer una sesión con la NSCL.

Gestión de Recursos

En el ETSI ha decidido adoptarse una arquitectura de RESTful para administrar el estilo de como se realiza el intercambio de información entre las aplicaciones de los dispositivos o Gateway's (DA, NA) y su respectiva capa de capacidad del servicio M2M (xSCL). Como es conocida, una arquitectura RESTful es aquella donde se intercambian representaciones de recursos que se encuentran identificados con un URI (Uniform Resource Identifier) o identificador uniforme de recursos, el cual es único para cada uno.

Se puede considerar que cada uno de estos recursos son pequeños cubos que almacenan información de alguna aplicación y se ubican en la capa SCL respectiva. En la figura 9, se representa a alto nivel, el proceso del flujo de datos entre una aplicación y la capa NSCL. Si una aplicación en un dispositivo (DA), requiere enviar información a otra aplicación en el dominio de Red (NA), debe hacerlo mediante la respectiva capa, es decir la NSCL. Por lo tanto la aplicación DA deberá escribir los datos en un recurso de la NSCL y la aplicación destino NA deberá leer ese recurso.

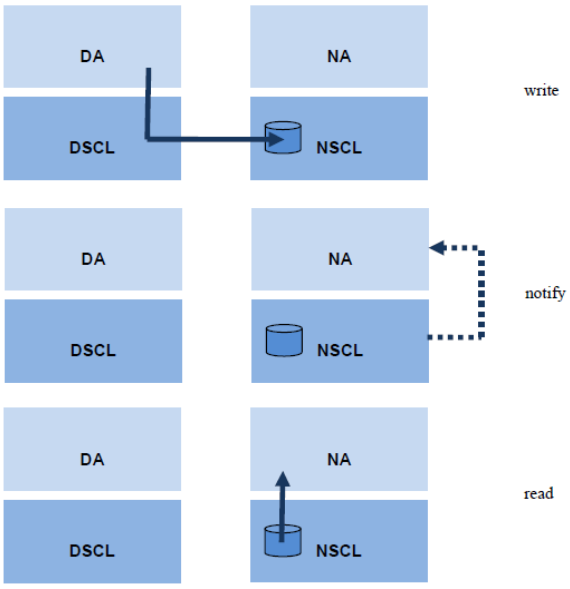


Figura 9. Recursos SCL para el intercambio de datos M2M (tomada del ETSI).

También pudiera darse el caso donde se configura el sistema de modo que cuando la aplicación realice la escritura de los datos, sea la NSCL quien notifique a la aplicación destino, de modo que esto permita facilitar el sincronismo entre DA y NA.

Cuando se manejan los recursos en una arquitectura de este tipo se utilizan las 4 operaciones o métodos básicos conocidos como "CRUD" (por sus siglas en ingles), las cuales son:

Crear: para crear un recurso.

Obtener: para leer los datos de un recurso.

Actualizar: para escribir datos en un recurso.

Borrar: para eliminar un recurso.

Sin embargo, como es común definir en una arquitectura RESTful otras operaciones adicionales para describir con mayor precisión acciones que no encajan directamente con las operaciones básicas, en esta especificación se han definido un par de operaciones nuevas:

Notificar: para reportar una notificación relacionada con un cambio de un recurso. Esta es una operación que pudiera asignarse como respuesta ante una operación de lectura "Obtener", en el caso de implementarse el modo síncrono, o bien como respuesta ante la operación de escritura "Actualizar" si se implementa el modo asíncrono.

Ejecutar: para ejecutar una tarea específica de gestión a través de un recurso. Es equivalente a la operación básica "Actualizar" pero sin carga de datos.

Lo importante de esto es, que el mismo grupo de operaciones puede manipular una gran diversidad de recursos, evitando la necesidad de desarrollar clientes o infraestructuras dedicadas para cada aplicación que se implementa. De esta manera, la misma arquitectura subyacente puede ser reutilizada en múltiples aplicaciones.

La implementación más común de REST es http, en donde las operaciones REST se asignan a métodos HTTP: CREAR se relaciona con HTTP POST, LEER con http GET, por su parte ACTUALIZAR con HTTP PUT, y finalmente BORRAR con HTTP DELETE.

3.2 Propuesta del 3GPP.

Muchas de las aplicaciones M2M actuales utilizan infraestructuras propias para el transporte de los datos, esto probablemente se deba a que una infraestructura inalámbrica local y privada es una solución simple para monitorizar alguna función

específica en una residencia. Sin embargo, existen muchas otras aplicaciones donde es más apropiado el uso de una red de telecomunicaciones públicas para el envío de los datos desde los dispositivos M2M hacia un servidor M2M, por ejemplo una aplicación de monitorización remota de pacientes que pueden estar dispersos a lo largo de todo el territorio. Se espera que en el futuro próximo, con la aparición de nuevas aplicaciones, aumente el número de dispositivos conectados a estas redes existentes.

El impacto que los dispositivos y aplicaciones M2M tienen sobre las redes móviles públicas es muy diferente en comparación con los clásicos dispositivos y servicios orientados a las comunicaciones entre humanos. A pesar de que las comunicaciones M2M son básicamente conexiones de datos, tienen un comportamiento diferente al observado en los servicios de internet actuales.

Para las operadoras de telecomunicaciones, es importante conocer cómo deben adaptar sus redes para este tipo de comunicaciones. Se asume que las comunicaciones M2M crecerán por mucho tiempo y posiblemente lleguen a sobrepasar los niveles de los tipos de tráfico tradicionales. Si las redes de telecomunicaciones móviles se optimizaran solo para las comunicaciones humano-humano y el acceso a internet, entonces el conectar un gran número de dispositivos y aplicaciones M2M tendría un efecto negativo en la eficiencia de esas redes y los servicios entregados.

Para los dueños y desarrolladores de aplicaciones M2M es importante conocer y entender la infraestructura de la red subyacente, sobre la cual se ejecutaran sus aplicaciones. Una pequeña diferencia en la manera como las aplicaciones M2M organizan la comunicación de sus datos, puede significar una gran diferencia en el impacto sobre la red. Esto ha motivado el desarrollo de especificaciones por parte del 3GPP, que serán evaluadas en las siguientes secciones.

En el 3GPP, el grupo de servicios y requisitos “3GPP WG SA1”, inicio en el 2008 el estudio de las mejoras necesarias en la red para las comunicaciones tipo maquina, cuya finalidad era definir los requisitos del servicio para M2M. El 3GPP ha adoptado el nombre de comunicación tipo máquina (MTC) para referirse a M2M, tomando en cuenta también la posibilidad de una comunicación entre una maquina y un humano que serian comunicaciones M2H o H2M.

El trabajo ha resultado en un documento de requisitos y especificaciones de servicio para MTC (3GPP TS 22.368) [6] [22] [23]. Esto sentó las bases para la especificación de arquitecturas y protocolos por parte de otros grupos dentro del 3GPP. Sin embargo queda claro que figuraban muchos más requisitos de los que podrían manejar los grupos de arquitecturas y protocolos en una sola versión. En el reporte técnico de mejoras del sistema para MTC (3GPP TR 23.888) [7], se realizan los primeros estudios

relacionados con los problemas claves descritos, y se plantean sus soluciones para mejorar la arquitectura de red. Adicionalmente existen otro grupo de especificaciones del 3GPP que complementan las actualizaciones necesarias en la arquitectura de red para que las comunicaciones MTC se realicen adecuadamente, entre estas se encuentran las interacciones con servidores M2M externos (3GPP TS 23.682) [24], y los protocolos en la interfaz de comunicación (Tsp) entre la función MTC en la red y los servidores M2M externos (3GPP TS 29.368) [25].

Para ayudar a comprender los terminados utilizados por el 3GPP en las comunicaciones tipo maquina (MTC), y además complementar el vocabulario para las especificaciones del 3GPP (3GPP TR 21.905) [26], se detallan los siguientes conceptos:

Dispositivo MTC, es un equipo terminal (UE) con capacidad para comunicaciones MTC a través de la PLMN.

Servidor MTC, se comunica con los dispositivos MTC a través de la PLMN, y tiene además una interfaz con los usuarios MTC. Puede funcionar como servidor de aplicaciones (AS) o servidor de capacidades de servicio (SCS) para los SA.

Usuario MTC, es quién se beneficia de los servicios ofrecidos por el servidor MTC.

Suscriptor MTC, es el proveedor de servicios M2M, que en algunos casos podrá ser el mismo operador de la red.

3.2.1 Escenarios

Los trabajos del 3GPP en comunicaciones MTC iniciaron para la arquitectura representada en el estándar para las comunicaciones móviles versión 10, *"release 10"*. El trabajo realizado se enfoco en las mejoras para la red móvil con la finalidad de actualizar la red y que fuese capaz de soportar la comunicación entre una gran cantidad de dispositivos MTC (fijos y móviles), además de las comunicaciones tradicionales entre humanos H2H.

La mayoría de los escenarios para las comunicaciones MTC se basan en un gran número de dispositivos MTC que se comunican con un servidor central. Como ejemplo de esta comunicación cliente-servidor podría ser una compañía eléctrica que hace la medición remota del consumo de energía mensual de cada uno de sus clientes. En la figura 3 se pueden apreciar los 2 primeros escenarios considerados por el 3GPP; la comunicación dispositivo-servidor puede ocurrir con el servidor MTC fuera del dominio del operador de red figura (10a), y también con el servidor controlado por el operador de la red figura (10b).

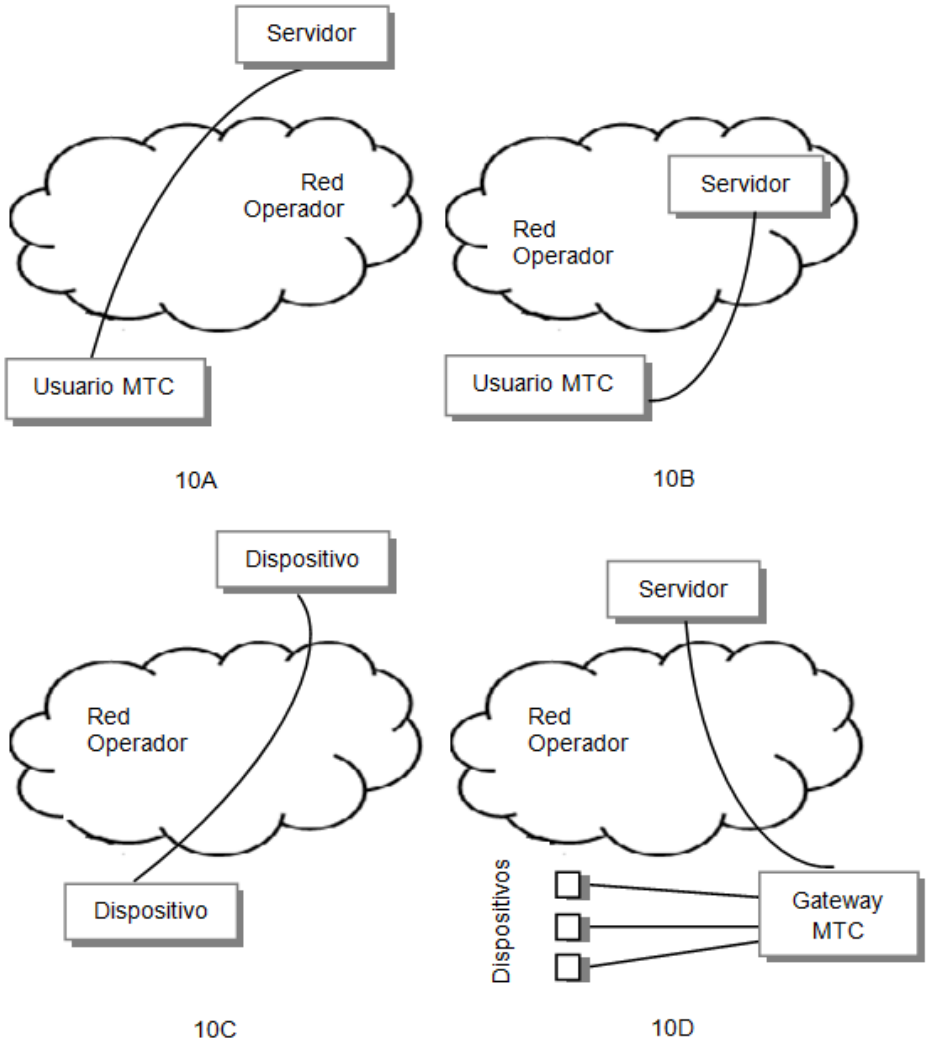


Figura 10. Escenarios para las comunicaciones MTC. (10a) servidor MTC no controlado por el operador de red, (10b) comunicación entre dispositivo MTC y servidor MTC controlados por el operador de red, (10c) comunicación directa entre dispositivos MTC, (10d) comunicación dispositivo-servidor mediante un Gateway MTC.

Este primer escenario (dispositivo-servidor) no posee realmente una taza de dispositivos a servidores de N:1, pueden haber múltiples servidores para redundancia y balanceo de carga, sin embargo el número de dispositivos típicamente será mayor al número de servidores. Esto se debe a que, la mayoría de los dispositivos MTC no tiene por qué conocer el servidor en particular con quien se están comunicando, se configuran simplemente para comunicarse con un servidor y no para realizar la selección previa de uno en especifico.

Adicionalmente se considera otro escenario en donde los dispositivos MTC se comunican directamente entre ellos, sin la intervención de un servidor MTC, tal y como se aprecia en la figura (10c). Un ejemplo de estas comunicaciones puede ser una aplicación en donde el sistema de alarma de una casa, haga contacto directamente con

el dueño de la misma ante una emergencia, mediante el envió de un SMS a su teléfono móvil.

El escenario dispositivo-dispositivo es mucho menos popular que el dispositivo-servidor, el cual constituye la gran mayoría de las aplicaciones M2M. Sin embargo, en el futuro, cuando haya más dispositivos de toda clase conectados a la red, se incrementara la demanda de aplicaciones que requieran la comunicación directa entre dispositivos.

En las comunicaciones directas entre dispositivos, estos elementos MTC deberán ser capaces de seleccionar el otro dispositivo MTC al cual deseen conectarse, lo que producirá una conectividad M:N, y por su parte los escenarios de negocio deberán ser adaptados. Debido a la baja popularidad, de momento, el 3GPP decidió no considerar este tipo de escenario durante el desarrollo de las especificaciones para los estándares de telecomunicaciones versión 10 y 11.

Por último, merece la pena agregar que en el caso de que existan muchos dispositivos MTC en una sola área, se considera más beneficioso adoptar un escenario con un Gateway MTC, como el de la figura (10d). Un ejemplo se considera el hecho de un automóvil con varios dispositivos MTC colocados en diferentes lugares para monitorizar las funciones del vehículo, y que se mueven siempre juntos.

Con esta topología los dispositivos MTC pueden compartir un solo enlace a través de la red de comunicaciones móviles pública; y la comunicación entre los dispositivos y el Gateway MTC (MTC GW) se puede alcanzar utilizando una tecnología de redes locales como (LAN, WLAN, Bluetooth, ZigBee, entre otras).

A partir de los escenarios anteriores se definen una serie de situaciones que se pueden presentar utilizando las comunicaciones MTC, y que se resumen en la tabla 3.

Caso	Descripción
Activación desde una entidad centralizada	Ejemplo de dispositivos de medición controlados por una entidad centralizada (Servidor MTC), que sondea o consulta al dispositivo MTC cuando necesita una medición. Para asegurar una respuesta a tiempo, el servidor MTC deberá indicar específicamente para cuando necesita la información.
Aplicación MTC vulnerable a robo o vandalismo.	Detección por parte de la red cuando un dispositivo MTC ha sido manipulado o robado. Dispositivos estacionarios que están en áreas remotas, cuando la red detecte que se han movido realizara automáticamente la desactivación de la cuenta correspondiente.

Aplicaciones MTC controladas por el tiempo	Comunicación a bajo costo cuando la operación se realiza durante los periodos de bajo tráfico en la red, esto puede ser ofrecido por el operador de la red dependiendo de la carga de tráfico.
Congestión en la interfaz aire	Optimización en la interfaz aire para gestionar la congestión causada por la concurrencia masiva de dispositivos MTC intentando transmitir al mismo tiempo y en la misma localidad.
Congestión en el núcleo de la red	Cuando varios dispositivos están afiliados con un solo usuarios, se considera que forman un grupo MTC, que se conecta a su vez con un servidor MTC. Se requiere optimización en la red para manejar todos los dispositivos, del grupo, que están distribuidos en la red e intercambian simultáneamente datos con el servidor.
Congestión en la red de señalización	Proveer medios al operador de red para gestionar la congestión en el plano de control que causa un número elevado de mensajes de señalización simultáneos, que podrían generar los dispositivos MTC cuando se reactive el servicio luego de una caída de tensión.
Control de acceso con plan de facturación	Prevenir el intercambio de tarjeta UICC. Cuando una tarjeta que se utiliza normalmente en módulos MTC (con una tarifa especial) se intercambia para otro terminal, el acceso deberá ser rechazado.
Consumo de potencia extra bajo	Cuando los dispositivos MTC tengan gran movilidad (seguimiento de animales o correspondencia) y solo se alimenten de baterías, deberán tener una vida útil mayor al promedio.
Consumo de potencia extra bajo con dispositivos MTC controlados por el tiempo.	Los dispositivos MTC operan solo durante periodos de tiempo predefinidos, para ahorrar el consumo de energía y extender la vida útil de la batería. El dispositivo deberá estar en capacidad además de recibir notificaciones aperiódicas para casos especiales.
Activación de dispositivos MTC por ubicación.	Se necesita un mecanismo eficiente que permita activar únicamente, mediante sondeo, a dispositivos en una región específica; en base a la información de ubicación provista por la aplicación o usuario MTC.
Seguridad extremo a extremo para dispositivos en itinerancia.	Los dispositivos MTC se encuentran en cualquier lugar y podrán disponer de movilidad, que en algunas ocasiones implica conexión a la red de otros operadores. Pero el proveedor de la aplicación MTC no puede considerar el dominio de los otros operadores de red como parte del dominio seguro que ofrece el proveedor de red local.

Tabla 3. Casos particulares en sistemas MTC.

3.2.2 Requisitos de Servicio.

Todas esas situaciones anteriores suponen diferentes comportamientos de carga en la red, por lo que se requieren funciones de control para prevenir la sobrecarga en la red, y además diferenciar entre los servicios ofrecidos a diferentes suscriptores con diferentes requisitos de servicio.

De hecho, algunos de los escenarios considerados son particularmente más tolerantes a condiciones adversas, y pueden aceptar bajos niveles de prestaciones en la red al momento de ejecutar sus servicios de comunicación, mientras que otros son iguales o más exigentes que los servicios actuales que existen en las redes móviles.

Basados en los escenarios anteriores y las posibles situaciones, se derivan una serie de requisitos comunes para el buen funcionamiento del servicio MTC entre los que se encuentran, además de los generales, requisitos para la activación de dispositivos, identificación, direccionamiento IP, tarificación, seguridad, y gestión remota de dispositivos MTC.

Además, como es sabido todas las aplicaciones MTC no tienen las mismas características, esto conlleva a que una sola optimización en la red no sea suficiente para satisfacer las necesidades de todas las aplicaciones MTC. Por consiguiente, se definieron unos requisitos de servicio específicos que se adaptan a situaciones particulares de las comunicaciones MTC, a los que se denomino **Características MTC**.

Lo que se busca es el desarrollo de funcionalidades específicas en la arquitectura existente para conseguir el uso eficiente de los recursos.

Estas características MTC, requieren el desarrollo de funciones de red que provean una estructura capaz de ofrecer diversas opciones para optimizar la red, con la finalidad de adaptarla a los requisitos propios de cada aplicación. Estas funcionalidades pueden ser activadas independientemente para cada suscriptor.

A medida que se han ido realizando actualizaciones a las especificaciones MTC y en combinación con el avance de las especificaciones propias de las redes móviles 3GPP (Versión 10, 11 y 12), se han descartado algunas de las características por considerarlas funciones genéricas de la red.

En la tabla 4 se encuentra un resumen de las 14 características específicas MTC consideradas en un principio por el grupo de trabajo del 3GPP.

3.2.3 Modelos de comunicación.

Apoyado en el escenario de comunicación dispositivo-servidor que se definió inicialmente, se han previsto algunos modelos de comunicación para el tráfico

extremo-a-extremo entre una aplicación MTC en el UE y una aplicación MTC en una red externa que utiliza los servicios provistos por el sistema 3GPP.

Característica MTC	Descripción
Movilidad reducida	Aplica a dispositivos MTC que no se mueven, se mueven muy poco, o lo hacen en cierta localidad.
Tiempo controlado	Útil para aplicaciones que permitan enviar/recibir información en un momento definido; la transmisión se realiza solo durante intervalos de tiempo determinados.
Tiempo tolerante	Dispositivos MTC a los que se les prohíbe el acceso temporal a la red de acceso, y pueden retrasar la transferencia de sus datos.
Solo conmutación de paquetes (PS)	Dispositivos MTC que solo requieren servicios PS, en lugar de conmutación de circuitos (CS).
Poca transmisión de datos	Solo enviar o recibir pequeñas cantidades de datos, utilizando la mínima señalización posible.
Solo origen en el móvil (MO)	No se permite la opción de finalizar en el móvil (MT) y se reducen los procesos de gestión de la movilidad.
Finalizado en el móvil (infrecuente)	Aunque se esperan principalmente comunicaciones MO, la red deberá mantener información actualizada del estado de los dispositivos MTC.
Monitorización de dispositivos MTC	Supervisar el comportamiento de un dispositivo MTC de acuerdo a sus características, cambio de SIM o localidad, robo.
Alarma de prioridad	Mensaje de alarma con preferencia sobre cualquier otra característica MTC en caso de robo o vandalismo.
Conexión segura	Asegurar la conexión entre dispositivos MTC y servidores MTC.
Activación por ubicación especifica	Corresponde al caso donde solo se activan dispositivos MTC en un área específica, basados en la información de su ubicación.
La red provee el destino para el enlace de subida	La red debe proveer una dirección IP de destino para el tráfico de subida, “uplink”, desde el dispositivo MTC.
Transmisión infrecuente	El periodo entre dos transmisiones consecutivas desde el dispositivo MTC, envío o recepción de datos, es muy grande.
Características MTC basadas en grupo	Gestión optimizada de todos los dispositivos MTC que pertenecen a un mismo grupo MTC (políticas de control, direccionamiento IP y otras)

Tabla 4. Características MTC.

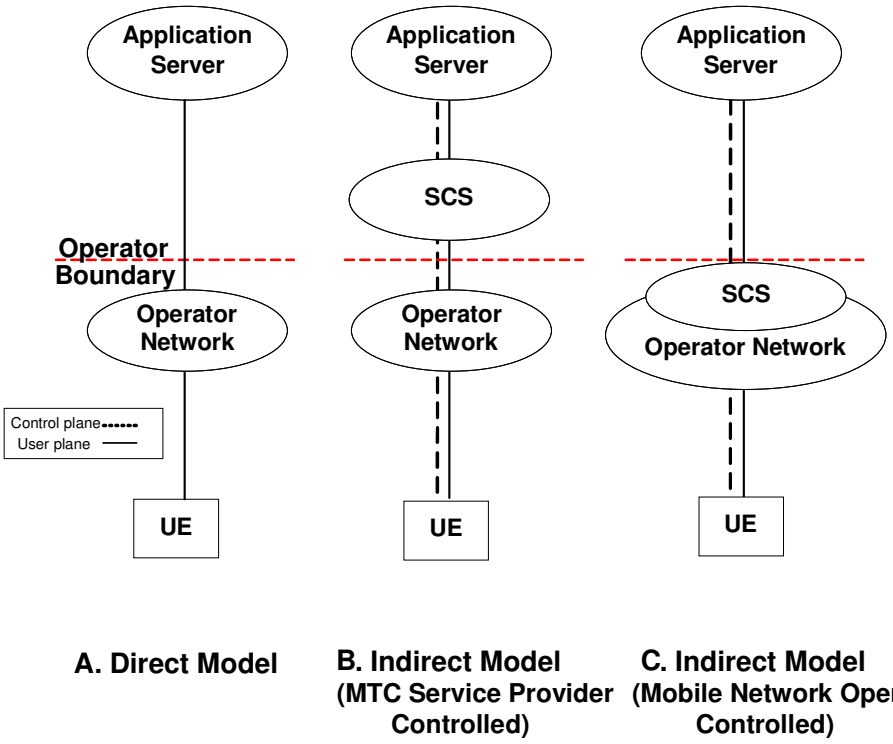


Figura 11. Modelos de comunicación MTC, directo e indirecto (tomada del 3GPP).

En el modelo de comunicación directa, la aplicación MTC que está en un servidor de aplicaciones (AS) se comunica directamente con el dispositivo (UE), tal y como sucede con cualquier otra aplicación OTT (Over-The-Top) en la red del operador 3GPP. Se puede apreciar en la figura 11a.

En el modelo indirecto, el AS se conecta indirectamente con la red del operador por intermedio de un servidor de capacidades de servicio (SCS) que le permitirá utilizar servicios de valor agregado, como activación de un dispositivo por el plano de control, para la comunicación MTC con el UE.

El servidor SCS puede estar desplegado fuera del dominio del operador de red, y se conoce como controlado por el proveedor de servicios MTC (figura 11b). Cuando el servidor SCS se despliega dentro del dominio del operador de red 3GPP, puede ser controlado por el operador y se considera como una función de red interna. En este caso, la seguridad y privacidad para la comunicación entre la red móvil y el servidor SCS es opcional (figura 11c).

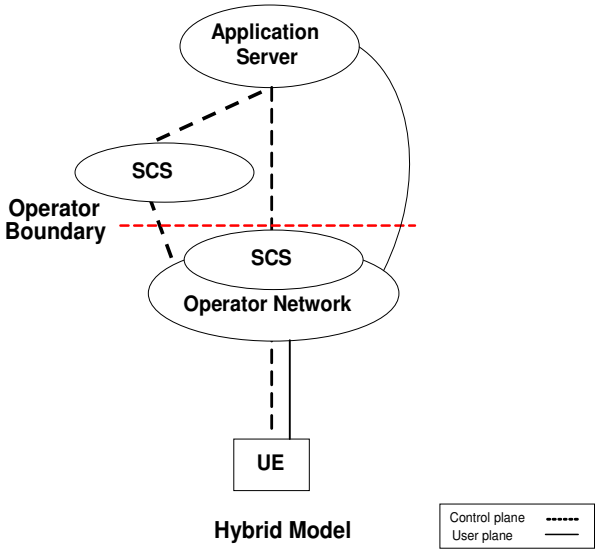


Figura 12. Modelo hibrido de comunicación MTC (tomada del 3GPP).

En el modelo hibrido, el AS utiliza los modelos directo e indirecto de forma simultánea, con la finalidad de conectarse de forma directa con la red móvil para ejecutar acciones relacionadas a la comunicación con el UE (plano de usuario), mientras utiliza también los servicios agregados provistos por el SCS (plano de control). Al igual que en el modelo indirecto, el SCS puede estar controlado por el proveedor de servicios MTC o por el operador de red móvil (figura 12).

3.2.4 Arquitectura para comunicaciones MTC.

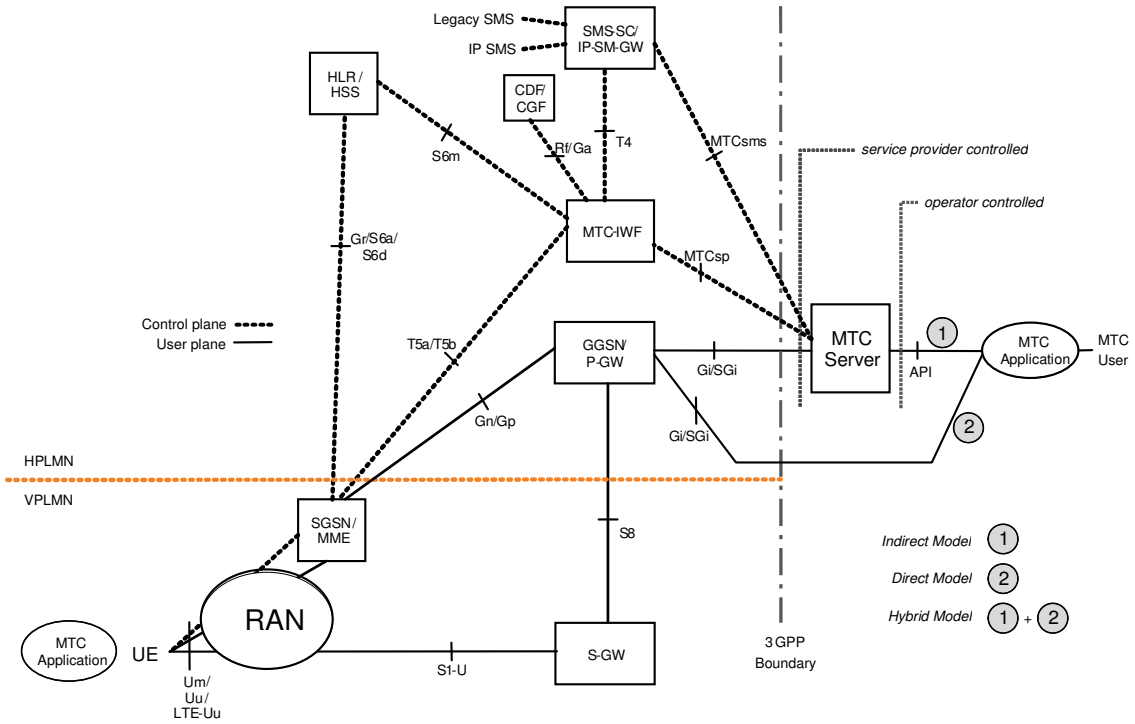


Figura 13. Arquitectura de referencia para MTC (tomada del 3GPP).

Con base en lo descrito anteriormente, el grupo de trabajo (3GPP SA WG2) establece la arquitectura de referencia inicial que se observa en la figura 13, y que se documenta en [7]. En donde la comunicación extremo-a-extremo, entre la aplicación MTC que se encuentra en el UE y la aplicación MTC que se encuentra en el servidor, utiliza los servicios de telecomunicación provistos por la red 3GPP, y opcionalmente los servicios de un proveedor de servicios MTC externo.

Se aprecia la incorporación de un elemento de red adicional para soportar los modelos de comunicación hibrido e indirecto, el cual se denomina función de interfuncionamiento **MTC-IWF**. Encargado de ocultar la topología interna de la red móvil y traducir las acciones demandadas por el servidor MTC para ejecutar la funcionalidad requerida. Además se definen una serie de interfaces o puntos de referencia entre todos los elementos involucrados en la comunicación MTC y se establecen los requisitos que deben cumplir cada uno de ellos.

Una vez establecida una primera visión, el trabajo se enfoca en las mojeras necesarias en la red para soportar las comunicaciones MTC de forma optimizada. Se desarrolla una lista de temas claves de la arquitectura que debían ser discutidos y resueltos. Finalmente se describen 15 temas, los cuales se resumen en la tabla 5.

Problema Clave	Descripción
Optimización basada en grupo	Agrupar los dispositivos MTC para facilitar el control, gestión, entre otras. Y así reducir la redundancia de señalización.
Dispositivos MTC en comunicación con uno o más servidores	Requisitos de servicio común para las comunicaciones entre los dispositivos MTC y los servidores MTC.
Direccionamiento IP	Dispositivo MTC utilizando una dirección privada IPv4, y por lo tanto no son accesibles desde el servidor MTC.
transmisión de pocos datos on-line	Los dispositivos envían/reciben frecuentemente pequeñas cantidades de datos
transmisión de pocos datos off-line	Los dispositivos envían/reciben frecuentemente pequeñas cantidades de datos.
Movilidad baja	Los dispositivos MTC no se mueven frecuentemente.
Suscripciones MTC	Activación/desactivación de las características MTC.
Activación de un dispositivo MTC	El servidor MTC consulta a los dispositivos MTC cuando requiere alguna información.
Control de tiempo	La transmisión de los datos ocurre solo en un periodo de

	tiempo predefinido.
Monitorización MTC	Monitorizar dispositivos MTC en zonas con alto riesgo.
Desacoplamiento del servidor MTC de la arquitectura 3GPP	El servidor MTC puede ser implementado fuera del dominio de la red móvil.
Control de congestión de señalización	Congestión y sobrecarga en la señalización relacionada con las comunicaciones MTC.
Identificadores MTC	Atender el hecho del gran número de dispositivos MTC y la escasez de números MSISDNs.
Sobrecarga potencial por la itinerancia de dispositivos MTC	Desbalance entre la carga de señalización y datos en la red móvil visitada (VPLMN).
Bajo consumo de potencia	Dispositivos MTC ahorradores de energía.

Tabla 5. Problemas claves de la arquitectura MTC.

El grupo de trabajo no tuvo el tiempo suficiente para desarrollar las soluciones de todos estos problemas planteados dentro del (3GPP Release 10). Así que luego de priorizarlas se acordó enfocar el trabajo en "suscripción MTC" y "control de congestión de señalización", y dejar los demás temas para ser resueltos en las siguientes versiones (11 y 12) del estándar.

Suscripción MTC.

El suscriptor MTC es visto como cualquier otro suscriptor de la red móvil, al igual que los dispositivos MTC no se consideran una clase nueva de teléfonos móviles, sino simplemente un UE.

La suscripción a una característica MTC específica por parte de un dispositivo MTC se logra de la misma forma que se hace con los servicios adicionales ofrecidos por los operadores móviles. Se realiza el vinculo de la identidad del suscriptor (IMSI) que se encuentra en el modulo de identidad del suscriptor (USIM) del dispositivo MTC, con la suscripción MTC que hay en el servidor de suscriptores local (HSS), y que contiene la característica MTC deseada.

Las características suscritas se incluirán en el perfil del usuario, el cual se descarga a los nodos de servicio local cada vez que el usuario realice la conexión a la red o ejecute alguna actualización de enrutamiento o rastreo (RAU o TAU). Los nodos locales son la entidad de gestión de movilidad (MME) en E-UTRAN o el nodo de soporte para el servicio GPRS (SGSN) en UTRAN. Ambos podrán ejecutar verificación de

compatibilidad y deshabilitar cualquier característica MTC que no sea compatible con otra característica activada, ya que se pudiera crear un conflicto.

Se deja fuera del alcance de esta especificación el hecho de que algún suscriptor MTC (proveedor de servicios) pueda modificar el estado (activación/desactivación) de las características previamente suscritas, ya que puede ser realizado mediante una interfaz web. Sin embargo, el operador de la red podrá igualmente restringir la activación de una característica MTC en caso de incompatibilidad con otra ya activada.

Control de congestión de señalización.

Sin duda el principal aporte durante el desarrollo del estándar versión 10, fue el relacionado con el control de congestión y sobrecarga de señalización MTC.

Debido a que la congestión en la red no se debe exclusivamente al elevado número de dispositivos MTC que tienen estos sistemas, sino que también puede ocurrir por una gran carga de señalización de muchos UE, la funcionalidad utilizada para gestionar el control de congestión en MTC se basa en la descrita para los sistemas GPRS [27] [28], en donde se consideran 2 escenarios responsables de sobrecarga por un gran número de elementos UE: **comportamiento sincronizado de una aplicación** en todos los dispositivos para hacer algo al mismo tiempo; y **dispositivos en itinerancia** que se mueven a la misma vez hacia una red local, cuando falla su red servicio.

Para hacer frente a esta situación el dispositivo se podrá configurar de cuatro formas diferentes (cada UE podrá soportar una o varias): **baja prioridad de acceso**, una vez configurado el UE le señalara esta condición al MME, durante el intercambio de mensajes de señalización NAS, mediante un indicador de baja prioridad de acceso; y además durante el procedimiento de establecimiento de la conexión RRC establecerá adecuadamente su baja prioridad de acceso. De esta forma la red estará en capacidad de utilizar esa información para decidir si acepta o no, alguna petición NAS o establecimiento de conexión RRC proveniente de este UE.

Cuando los mensajes del UE son rechazados se utilizan las herramientas provistas para reintentar la conexión "temporizadores de espera extendidos", en la cual el dispositivo no envía una nueva solicitud de conexión hasta que el tiempo expira o en caso de que el MME/SGSN ejecute el control de congestión basado en el nombre del punto de acceso (APN), entonces cuando haya congestión rechazara todas las solicitudes provenientes de un elemento conectado a ese APN hasta que expire el temporizador de cuenta regresiva que se establece para cada UE.

Si el dispositivo se configura para "**conectarse con IMSI al cambiar de PLMN**", se deberá rechazar cualquier actualización TAU con identidad temporal (GUTI) y

únicamente solicitar la IMSI. Esto reducirá la carga de procesamiento de mensajes en la red local cuando haya un fallo en la otra red.

Si el dispositivo se configura para **"el mayor límite de tiempo mínimo de búsqueda periódica de PLMN"**, entonces el UE reintentara acceder nuevamente a la red preferida que ha fallado luego de que expire el temporizador. Si el tiempo es muy corto no permite que la red se restablezca ante cualquier fallo, por lo que las otras redes vecinas experimentaran mas carga.

Por último si el dispositivo es configurado para **"manejo especifico del USIM en estado invalido"**, entonces recordara cuando un modulo USIM es invalido y se mantendrá en la lista negra de la red aun cuando se apague y encienda el UE.

Luego de solventar esos 2 temas, el grupo de trabajo se dedicó a atender otros problemas como la arquitectura MTC, el direccionamiento IP, los identificadores, y la activación de dispositivos, además se desarrolla en profundidad de la característica MTC mencionada anteriormente "servicios solo PS". A continuación se describen los detalles de las soluciones propuestas para cada caso.

Arquitectura MTC mejorada.

En la figura 14, se observa la arquitectura utilizada por los UE durante las comunicaciones MTC para conectarse a la red de acceso (UTRAN, E-UTRAN, GERAN, etc.) por medio de la interfaz de radio (Um/Uu/LTE-Uu). Para hacerlo más simple solo se muestran y etiquetan las interfaces relacionadas con la comunicación MTC y no las de la red interna 3GPP.

El servidor de capacidades de servicio SCS se conecta con la red móvil por medio del MTC-IWF que está en la red local HPLMN para comunicarse con el MTC UE. El SCS ofrece capacidades de servicio que podrán ser utilizadas por una o múltiples aplicaciones MTC, además en un UE pueden haber una o múltiples aplicaciones MTC. Igualmente las aplicaciones MTC correspondientes en la red externa están alojadas en uno o múltiples servidores AS.

El SCS provee una interfaz API para permitir que diferentes AS´s puedan utilizar las capacidades de servicio ofrecidas. La interfaz entre SCS y AS no está estandarizada por el 3GPP, pero se espera que esto sea realizado por otros organismos de estandarización; como el ETSI, que por su parte lo ha hecho con el punto de referencia (mIa).

En general, la aplicación MTC estará en un servidor AS dentro del dominio del operador de red o en la red externa y utilizara el servidor SCS para las capacidades que

este ofrece; como la solicitud de activación de dispositivos por plano de control. En la misma figura se observan reflejados los 3 modelos de comunicación considerados.

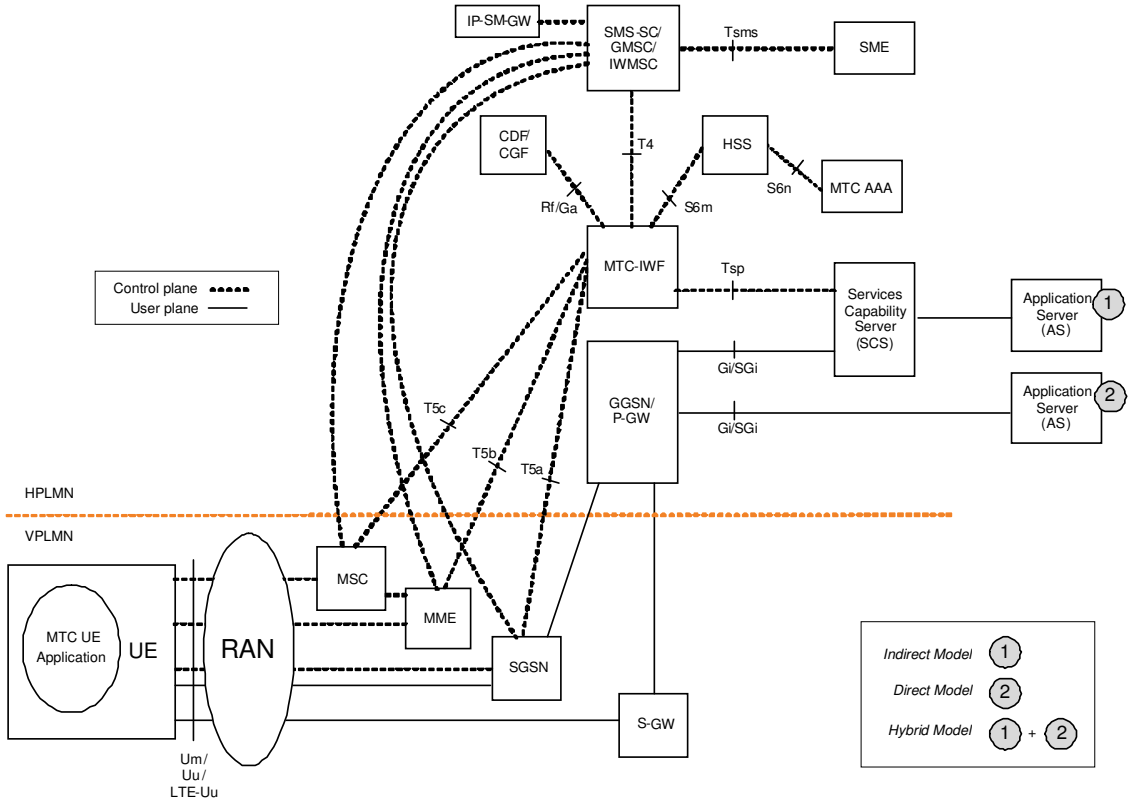


Figura 14. Arquitectura 3GPP mejorada para comunicaciones MTC (tomada del 3GPP).

A continuación se describen los elementos de red y puntos de referencia importantes en la comunicación MTC:

MTC-IWF: es una entidad funcional que interpreta los protocolos de señalización utilizados en la interfaz Tsp, para invocar alguna funcionalidad especifica en la PLMN. Puede ser un elemento de red independiente o una función integrada a otro elemento y siempre estará en la red local HPLMN. Principalmente soporta la funcionalidad de activación de dispositivos sobre las interfaces Tsp y T4. Adicionalmente puede generar los registros CDR´s, para tarificación de dispositivos, sobre la interfaz Rf/Ga.

Interfaz Tsp: es una interfaz estandarizada por el 3GPP [29] para facilitar los servicios de valor agregado motivado por las comunicaciones MTC y provisto por un SCS. Por ejemplo, entrega la solicitud de activación de un dispositivo desde el SCS hacia el MTC-IWF, y luego reporta el resultado de dicha solicitud.

Interfaz Tsms: es una interfaz no estandarizada por el 3GPP que abarca todas las variedades propietarias existentes de interfaces entre SMS-SC y SME. Puede ser utilizada por cualquier entidad de red fuera de la red 3GPP para enviar la activación de un dispositivo, encapsulada en un MT-SMS *(Mobile Terminating-SMS)*, como si fuera una aplicación OTT.

Interfaz T4: es utilizada por el MTC-IWF (actuando como un SME) para el enrutamiento de una solicitud de activación, como ejemplo el envío de un MT-SMS hacia el SMS-SC en la HPLMN. Reporta el resultado (exitoso o fallido) de la entrega de la solicitud de activación de dispositivo enviada al UE.

Interfaces T5a/b/c: de momento no están estandarizadas por el 3GPP Rel-11, están destinadas a proveer rutas optimizadas para la entrega de solicitudes de activación de dispositivos y posiblemente otros servicios, como transmisión de pocos datos, hacia el dispositivo MTC-UE. Proveen al MTC-IWF información de carga/congestión en los nodos de servicio (SGSN/MME/MSC).

Interfaz S6m: es utilizada por el MTC-IWF para solicitar al registro de localización local y/o servidor de suscriptor local (HLR/HSS) por la relación entre un MSISDN o identificador externo con el numero IMSI, recuperar la información de un nodo de servicio, y autorizar una solitud de activación a un UE en particular.

Interfaz S6n: es una interfaz entre la entidad de autentificación, autorización y contabilidad de MTC (MTC AAA) y el HSS/HLR, que permite solicitar a este último la relación entre un IMSI con su respectivo identificador externo durante el proceso de salida de la red.

Direccionamiento IP.

Con respecto al direccionamiento en las comunicaciones MTC, estaría demás decir el problema que hay con la poca cantidad de direcciones IPv4 disponibles, y más aun con la cantidad prevista de dispositivos MTC, es por eso que el mecanismo direccionamiento con IPv6 es la principal opción a considerar. Sin embargo, mientras sigue ocurriendo la transición, el 3GPP ha considerado varios principios y soluciones para el direccionamiento con direcciones IPv4, los cuales fueron descritos en [30].

Identificadores MTC.

En los organismos reguladores de algunos países se han expresado preocupaciones sobre los requisitos de numeración de los nuevos servicios MTC (agotamiento de E.164 MSISDN). Un gran número de servicios MTC han sido implementados sobre redes GSM de conmutación de circuito y por lo tanto han consumido números MSISDN, aunque esos servicios no requieran números "que se puedan marcar". Por ese motivo la arquitectura 3GPP ha sido mejorada para permitir la entrega de servicios de

comunicación utilizando un identificador alterno, que se ha denominado "identificador externo". Los identificadores MTC e dividen en:

Identificadores internos, utilizados dentro de la red 3GPP para identificar el UE que tiene una suscripción MTC, o a la suscripción en sí.

Identificadores externos, utilizados fuera de la 3GPP (en la interfaz Tsp), para referirse al UE que está utilizando una suscripción MTC, o a la suscripción en sí.

El IMSI se utiliza como un identificador interno de la red 3GPP. El identificador externo debe ser globalmente único y tendrá 2 componentes: el identificador de dominio usado para identificar en donde pueden ser accedidos los servicios provistos por el operador de red, y el identificador local el cual es utilizado para derivar u obtener el IMSI. Esta combinación de identificadores de dominio y local hará que el identificador externo sea único. Un identificar externo tendrá el formato de un URI o NAI (<identificador local>@<identificador de dominio>) y es relacionado con el identificador local mediante el MTC-IWF.

Un operador de red sin problemas de agotamiento de MSISDN podrá continuar utilizándolos como identificadores externos, e igualmente el operador podrá utilizar el IMSI como identificador externo basado en sus políticas.

Activación de dispositivos.

Uno de los requisitos claves para una red 3GPP es poder activar dispositivos desde la red para que ejecuten ciertas tareas relacionadas con las aplicaciones. Dado que la mayoría de las aplicaciones MTC son aplicaciones de datos, es importante para el SCS estar en capacidad de alcanzar un dispositivo en el dominio PS; esto requiere que el dispositivo tenga asignada una dirección IP.

Por lo tanto la activación de un dispositivo será relevante para aquellos que no siempre tienen una dirección IP asignada. Ya que para los dispositivos que tiene asignación permanente de IP, "siempre activos" en el dominio PS, el SCS o AS pueden comunicarse directamente con ellos. Como el caso de los dispositivos solamente LTE.

Para atender este requisito se define la activación de dispositivos desde el plano de control como un mecanismo mediante el cual el SCS envía cierta información al dispositivo por medio de la red móvil para activarlo y que este ejecute las acciones de la aplicación que incluyen el inicio de la comunicación con el SCS (para el modelo indirecto) o un AS en la red (par el modelo hibrido).

El mensaje de solicitud de activación del dispositivo contiene información que permite a la red encaminar el mensaje al dispositivo apropiado y además le permite al dispositivo encaminar el mensaje hacia la aplicación apropiada. La información

destinada a la aplicación, conjuntamente con la información para encaminarla, constituyen lo que se conoce como la carga de activación. Una vez que esta es recibida por el dispositivo provee información a la aplicación que podrá activar acciones relacionadas con la aplicación, y como resultado podrá ejecutar las acciones indicadas en el mensaje.

La activación de un dispositivo está basada en suscripciones; el MTC-IWF autoriza las solicitudes de activación de dispositivos basado en los datos existentes en el HSS respecto a un usuario móvil en específico y elije el mecanismo de entrega de la solicitud que aplica para el tipo de dispositivo en particular.

La interfaz Tsp permite al MTC-IWF recibir las solicitudes desde el SCS. Se debe utilizar un procedimiento que permita la selección del dominio, para así asegurar que la solicitud de activación se envía al MTC-IWF correcto. A pesar del hecho que se han discutido diferentes mecanismos en el 3GPP Rel-11, para el momento de realizar este trabajo el único mecanismo que se ha definido es "activación de dispositivo mediante la interfaz T4", el cual utiliza el formato SMS con la finalidad de enviar la solicitud al dispositivo.

En la figura 15, se expone el procedimiento de activación de un dispositivo a través de la interfaz Tsp. El SCS envía el mensaje de activación de dispositivo al MTC-IWF mediante la interfaz Tsp y este a su vez lo reenvía a la entidad adecuada por la interfaz T4. Finalmente, el mensaje de activación alcanza al MTC-UE gracias al mecanismo de entrega de SMS del 3GPP. El paso 6 hace mención a la posibilidad de activación mediante la interfaz T5, sin embargo para esta especificación no se ha desarrollado ningún mecanismo que soporte la entrega del mensaje de activación utilizando esta interfaz.

Prestación de servicios "solo PS".

A diferencia de la mayoría de las aplicaciones humano-a-humano (H2H), la gran mayoría de las aplicaciones MTC solo requieren servicios basados en PS. Pero, debido a que se espera el uso de SMS para la activación masiva de dispositivos MTC, uno de los requisitos es el control de la carga que estas comunicaciones causaran en los elementos de red que también se utilizan en las comunicaciones H2H como el MSC y VLR.

La prestación de servicios solo PS, implica proveerle a un MTC UE todos sus servicios suscritos por medio del dominio PS. Esta provisión conlleva una suscripción que permite únicamente servicios que son exclusivos del dominio PS. Seguramente, algunos operadores de red estarán de acuerdo en evitar la sobrecarga que supondrán

los dispositivos MTC para el dominio CS, y no querrán que se ejecute señalización con el MSC.

Inicialmente se desarrollo una opción para implementar SMS en un ambiente solo PS, y se detalla en [31], pero en la práctica esta opción no se ha tomado en cuenta básicamente porque los dispositivos actuales tienen la necesidad de utilizar los servicios del dominio CS.

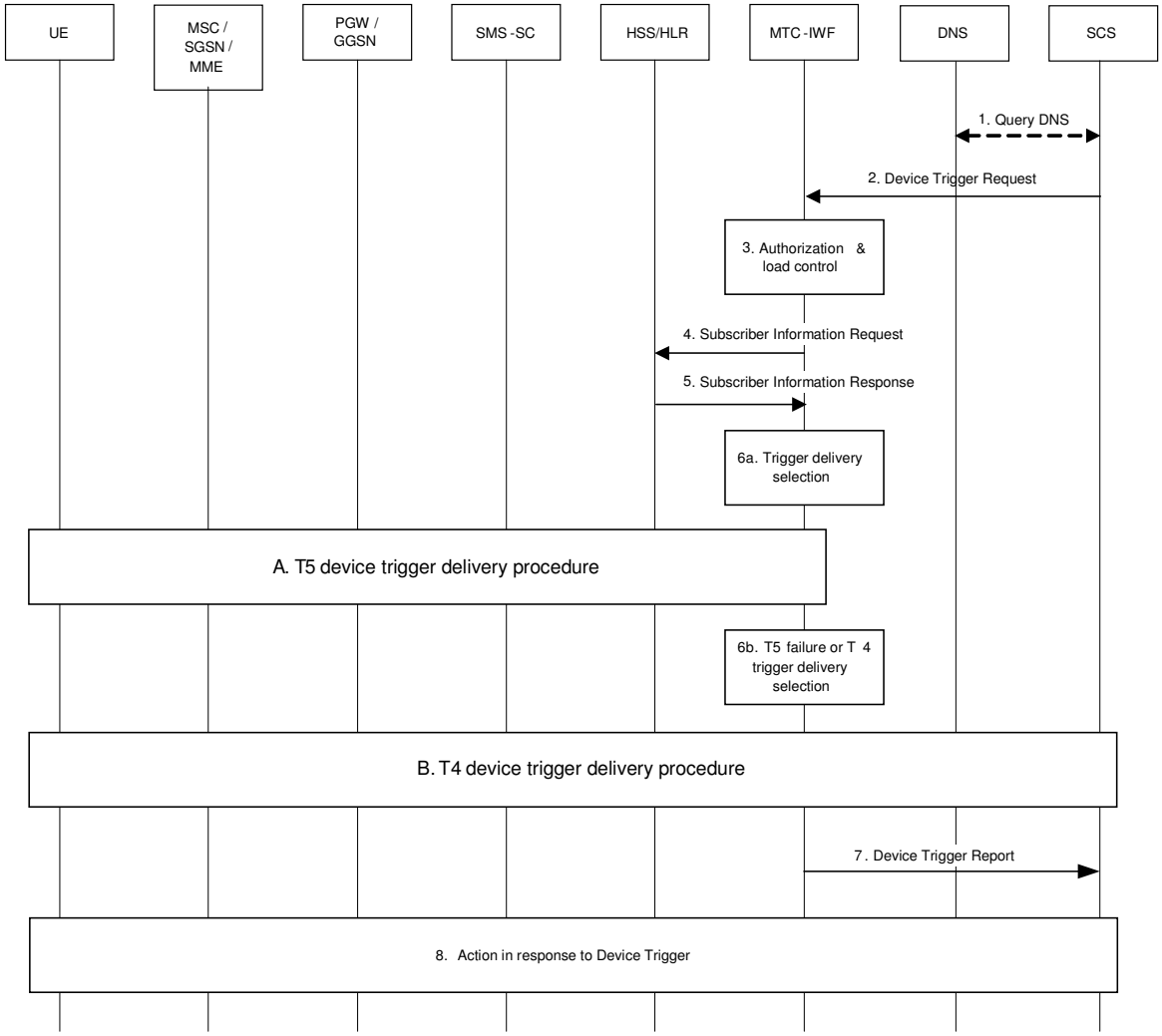


Figura 15. Procedimiento de activación de un dispositivo MTC (tomada del 3GPP).

En un sistema 2/3G, el nodo de servicio SGSN puede proveer la función de envío y recepción de SMS, como es el caso de provisión de SMS sobre señalización NAS (del dominio PS). De modo que, el dispositivo no necesitaría tener una suscripción CS.

En la actualidad existe una mezcla de dispositivos nuevos y antiguos, así como redes que proveen capacidades diferentes. Los procedimientos nuevos introducen mecanismos en donde los dispositivos, al registrarse en la red, serán capaces de

intercambiar sus capacidades con las de la red y así elegir el mecanismo para la entrega de SMS que ambos soporten, eliminando el proceso de ensayo y error que se realiza normalmente. Los problemas que esto suponía para las redes 2/3G fueron atendidos en [28], y entre las mejoras están:

Se crean 2 perfiles de suscripción, uno para casos donde los dispositivos no tienen acceso a los servicios del dominio CS y utilizan SMS exclusivamente en el dominio PS, y otro donde el dispositivo tiene preferencia por utilizar el dominio PS si la red está en capacidad de soportarlo también. Durante los **procedimientos de conexión y gestión de movilidad**, la red provee un indicativo al dispositivo donde informa si está en capacidad de soportar servicios SMS y si el SGSN soporta estos servicios. Finalmente, si los **dispositivos no necesitan el dominio CS** para otro servicio diferente a SMS, evitaran suscribirse a este dominio si la red indica capacidad SMS en el dominio PS.

Por otra parte EPS, aunque es un sistema basado en paquetes, para realizarse la entrega de un SMS sobre señalización NAS a un UE, que se encuentra en la red de acceso E-UTRAN, inicialmente se tenía que involucrar al MSC. Este envío del SMS mediante el MSC, se conoce como "SMS sobre SGs", en el cual el soporte SMS radica en la interfaz (SG) entre el MME y el servidor MSC. Esto le permite a un usuario conectado a la red E-UTRAN formar una suscripción destinada a un servicio solo PS para intercambiar mensajes SMS del dominio CS.

Sin embargo, para mejorar la eficiencia deshabilitando todos los procesos relativos al dominio CS entre el MME y el MSC, se definió la funcionalidad para soportar SMS en el MME [32]. Luego de completar el proceso de conexión que allí se detalla, la solicitud de activación del servicio enviada desde el SCS puede ser entregada por el MTC-IWF hacia el MME por medio del SMS-SC. Específicamente, el MTC-IWF obtiene el identificador del MME que sirve al MTC UE, consultando al HSS por la información del suscriptor. Finalmente el mensaje de activación del dispositivo es entregado por el MME al MTC UE de acuerdo al procedimiento de activación de dispositivos anterior.

3.3 Propuesta del IEEE.

El comité de estándares IEEE 802 LAN/MAN es el encargado de desarrollar y mantener los estándares y recomendaciones para las redes de área local y metropolitana. Dentro del mismo existen diversos grupos de trabajo entre los que se encuentra el grupo de estándares para el acceso inalámbrico de banda ancha "IEEE 802.16" (WirelessMAN), cuya familia de estándares forma las bases para el estándar de interoperabilidad global para el acceso microondas (WiMAX); igualmente dentro de este existen varios grupos de tareas atendiendo el impacto de las comunicaciones M2M en la red de acceso inalámbrica.

Dentro del IEEE 802.16 hay un grupo dedicado a las comunicaciones Machine-to-machine que inicio en noviembre del 2010 a desarrollar el proyecto P802.16p, el cual fue aprobado como un estándar IEEE en el mes de agosto del 2012 (IEEE 802.16p-2012, mejoras en la interfaz de aire para soportar aplicaciones machine-to-machine en redes de acceso inalámbrico banda ancha) [33].

En este documento se han realizado varios cambios en protocolos MAC y especificaciones en la capa física PHY para mejorar el soporte a un gran número de aplicaciones M2M en donde las comunicaciones con los dispositivos requieren cobertura inalámbrica de área extensa en bandas con licencia y que son automatizadas, con mínima o incluso sin ninguna intervención humana para el control u observación.

Estas mejoras en el MAC y las pequeñas modificaciones en PHY (acceso múltiple OFDMA), propician el apoyo al bajo consumo de energía en el dispositivo, soporte de un numero elevado de dispositivos por la estación base, tratamiento eficiente de transmisión de pequeñas ráfagas de datos, y mejorar la autentificación del dispositivo para evitar la manipulación y así asegurar una correcta detección y notificación.

Paralelamente desde diciembre del 2011 el grupo estuvo trabajando en el proyecto P802.16.1b en donde se plantearon mejoras y modificaciones leves en la capa física de las redes inalámbricas de área metropolitana (WirelessMAN) para soportar las aplicaciones M2M. Se aprobó en agosto de 2012 y se publico bajo el nombre (IEEE 802.16.1b-2012, mejoras en la interfaz aire avanzada para los sistemas de acceso inalámbrico banda ancha) [34].

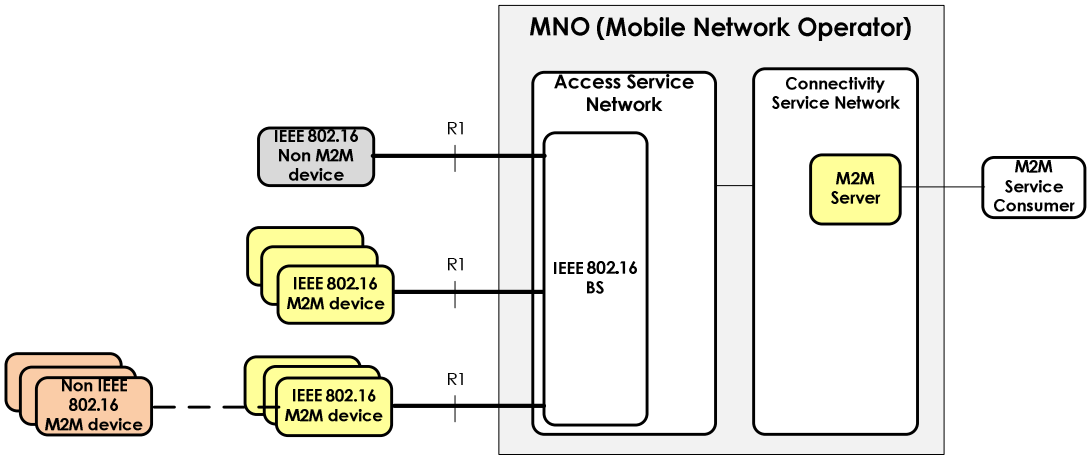
3.3.1 Arquitectura IEEE 802.16.

Como base para el estándar 802.16p se desarrolla en el 2010 un reporte técnico que contiene los escenarios de uso, requisitos, y modificaciones al estándar necesarias para soportar las comunicaciones M2M [35], en la figuras 16 se refleja la arquitectura de alto nivel del sistema para las comunicaciones M2M basadas en el estándar 802.16.

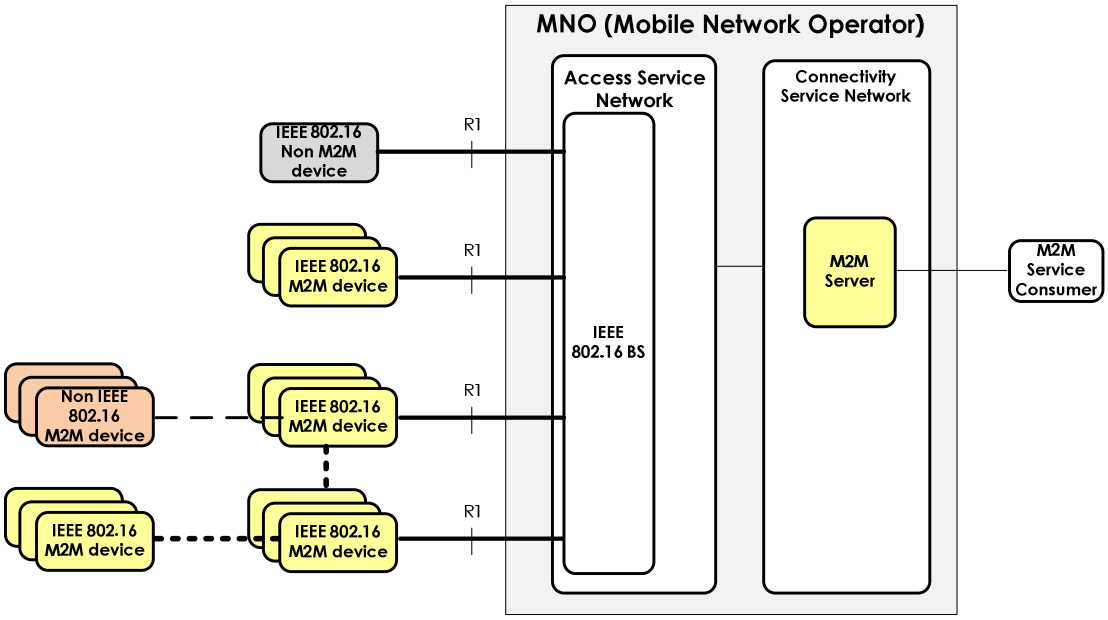
En la primera imagen (16a) encontramos la arquitectura básica del servicio donde destacan elementos como el **dispositivo M2M IEEE 802.16**, que es una estación móvil (MS) con funcionalidades M2M, y que se conecta con la estación base (BS) IEEE 802.16 en la red de acceso por medio de la interfaz R1. El **servidor M2M** es una entidad capaz de comunicarse con uno o más dispositivos M2M para proveer servicios M2M específicos. El servidor podrá estar alojado dentro o fuera de la red de conectividad del servicio (CSN), y además tiene una interfaz para comunicarse con cualquier **consumidor del servicio M2M**. Este consumidor puede ser alguna empresa que utiliza los servicios M2M. Finalmente, las aplicaciones M2M se ejecutan en los dispositivos y servidores M2M IEEE 802.16.

Esta arquitectura de servicios básica soporta dos tipos de comunicación M2M:

- Comunicación entre uno o más dispositivos M2M 802.16 y un servidor M2M 802.16, y
- Comunicación punto a multipunto entre dispositivos M2M 802.16 y la estación base 802.16.



(a)



(b)

Figura 16. Arquitecturas del sistema para las comunicaciones M2M basadas en IEEE 802.16. (a) Arquitectura básica, (b) Arquitectura avanzada (tomada de IEEE).

Nótese que en la arquitectura básica se le permite a un dispositivo M2M actuar como un punto de agregación para los dispositivos sin características M2M 802.16. Estos dispositivos diferentes utilizan otras interfaces de radio como PLC, IEEE 802.11 e IEEE 802.15; no se requieren cambios en la interfaz de aire 802.16 para soportar esta función de agregación.

Entre tanto la arquitectura avanzada de la imagen (16b), incorpora la función de agregación no solo para dispositivos no-M2M sino también para dispositivos con capacidad de comunicación M2M IEEE 802.16, en este caso se deben realizar cambios en la interfaz aire para soportar esta función de agregación para ambos tipos de dispositivos, lo cual está fuera del alcance del proyecto P802.16p. También se contempla la posibilidad de conectividad (P2P) entre dispositivos M2M.

En este mismo documento se comentaron aspectos como requisitos y características de las comunicaciones M2M, y su posible impacto en el grupo de estándares 802.16. Se consideran muchas características para estas comunicaciones M2M, pero en función de facilitar la culminación de la primera etapa del estándar, se recomienda trabajar con aquellas que se relacionan con implementaciones basadas en la arquitectura básica, para luego continuar con la arquitectura avanzada. De forma que se asegura el lanzamiento del mercado al estándar y luego a medida que este crece y se van considerando nuevas aplicaciones se incorporan mas mejoras y optimizaciones al estándar en fases siguientes.

Luego en septiembre de 2012, se culmina el documento con los requisitos del sistema M2M basados en la arquitectura básica y donde se contemplan cuatro requisitos funcionales.

Bajo consumo de energía

El sistema deberá optimizarse para situaciones como dispositivos de baja o nula movilidad, aplicaciones controladas por el tiempo, tolerantes al tiempo y con tráfico poco frecuente, además deberá soportar gestión eficiente de recursos de radio para dicho tráfico, y soportar periodos de inactividad mayores para incrementar ahorro de energía de los dispositivos M2M.

Gran numero de dispositivos

En este apartado el sistema deberá ser capaz de soportar e identificar muchos dispositivos bien sea de forma individual o en grupos, los dispositivos deberán tener la capacidad de asociarse a uno o varios grupos, se debe proveer un mecanismo eficiente para la gestión de grupos, asignación de recursos, acceso a la red y entrega confiable de la información de control o datos de las aplicaciones, y reducir la sobrecarga y congestión que producen en la red tal numero de dispositivos M2M. Finalmente, el

sistema deberá ser capaz de distinguir entre un apagado normal (asociado a un corte de energía voluntario) o anormal (asociado a un corte de energía involuntario).

Transmisión de ráfagas pequeñas de datos

Se deberá soportar la transmisión eficiente de este tipo de información, y además minimizar la información de señalización y protocolos de control.

Autentificación de dispositivos

Debe soportar integridad y autentificación de dispositivos, además de establecer una conexión segura mediante verificación de la validez entre dispositivo y la red.

3.3.2 Estándar 802.16p

Entre las mejoras propuestas a la interfaz aire WirelessMAN-OFDMA en el documento de enmienda IEEE 802.16p se incluyen, entre otras, las siguientes:

Direccionamiento y conexiones.

Varias estaciones base ubicadas en una área cercana de la red se pueden agrupar en una zona M2M e identificarse mediante un identificador de grupo denominado "M2M-GROUP-ZONE-ID", el cual podrá ser difundido por la estación base en el mensaje de descripción del canal de bajada (DCD). Una estación base podrá pertenecer solamente a una zona M2M.

Adicionalmente se define un identificador de conexión de multidifusión o multicast M2M (M2MCID), que es único para cada flujo de datos de bajada que comparten un grupo de dispositivos M2M dentro de la misma zona M2M. Un dispositivo podrá compartir más de una conexión, cada una identificada con su respectivo M2MCID, y todas pertenecerán a la misma zona M2M.

La asignación de los M2MCID se realizara durante el procedimiento de adición dinámica del servicio (DSA) y será liberado durante el procedimiento de eliminación dinámica del servicio (DSD) o por una salida explicita de la red.

El M2MCID asignado deberá mantenerse en el dispositivo M2M aun cuando se encuentre en modo reposo, y en caso de ocurrir algún cambio en el identificador la estación base podrá activar la actualización de localización para el grupo de dispositivos mediante un mensaje *paging* o de paginación, que contiene el nuevo M2MCID; o cuando el dispositivo ejecute el reingreso a la red (mediante la actualización de localización basada en tiempo) la BS podrá actualizar el identificador mediante el mensaje de respuesta RNG-RSP.

Durante el proceso de operación normal del dispositivo, la estación base podrá actualizar el M2MCID para un grupo de dispositivos M2M utilizando el mensaje de control (MGMC).

Cualquiera sea el método utilizado para la actualización del identificador M2MCID, el dispositivo M2M deberá enviar un acuse de recibo (ACK) a la estación base, que durante la operación normal será el mensaje de control (MAMC).

En caso de la BS no recibir el acuse de recibo desde algunos dispositivos, activara el procedimiento de actualización de localización para esos dispositivos en el siguiente ciclo de paginación.

Acceso a la red y registro de nuevo suscriptor.

La alineación inicial o *ranging*, es el proceso por el que se adquieren los ajustes de potencia y el desplazamiento de tiempo correcto para iniciar la transmisión desde la estación del suscriptor o abonado (SS).

Durante la alineación inicial basada en contención, lo primeo que realiza una estación de suscriptor es sincronizar con el canal DL y aprender las características del canal UL a través del mensaje de gestión UCD MAC. Luego la estación SS debe encontrar el intervalo de alineación inicial, que es asignado por la estación base y consta de una o más oportunidades de transmisión. En el caso de portadora sencilla y capa física OFDM, la estación deberá enviar el mensaje de solicitud de alineación inicial (RNG-REQ) durante el intervalo inicial; mientras que para una capa física OFDMA, el proceso deberá comenzar con el envío de códigos de alineación inicial CDMA en el canal UL dedicado para tal fin, en lugar de enviar la petición en los slots de contención.

Cuando un dispositivo M2M intenta ingresar o reingresar a la red, y esta acción no se debe a una solicitud de la red, sino que pudo ser activada por un evento, se debe aplicar un proceso aleatorio para seleccionar el momento de inicio del procedimiento de ingreso a la red desde una ventana cuyo tamaño será mayor o igual al tamaño mínimo de la ventana de acceso.

El dispositivo M2M podrá ejecutar el procedimiento de alineación utilizando la ventana de inicio con el tiempo de espera asignado previamente en el mensaje de difusión paging, en donde este tiempo de espera asignado deberá ser diferente al que es asignado por el mensaje UCD.

Estación móvil en modo reposo.

El modo reposo es un mecanismo que busca otorgarle a la estación móvil la posibilidad de estar disponible periódicamente ante cualquier difusión de mensajes en el canal de bajada (DL), sin necesidad de registrarse en una estación base especifica cuando se desplaza en un área cubierta por diferentes BS. Esta restricción en la actividad de la MS a solo intervalos definidos permite que se ahorre consumo de energía y recursos de la red.

Se utiliza el mensaje de difusión paging (MOB_PAG-ADV), en el que se incluye un código de reporte M2M, que permite realizar un sondeo a los dispositivos M2M para que transmitan periódicamente datos pero no en tiempo real. En caso de que el dispositivo no reciba el mensaje de paginación dentro del tiempo de espera estimado, podrá enviar los datos pendientes por el canal de subida sin esperas adicionales.

Se contempla el uso de paginación grupal para los dispositivos M2M, en este caso se utiliza el identificador M2MCID en el mensaje de paginación para identificar al grupo de dispositivos M2M, en lugar de un identificador individual.

Además, se define un modo de reposo específico para aplicaciones M2M, en donde se le asigna un temporizador al dispositivo M2M durante el inicio del modo reposo, a través del mensaje de registro DREG-CMD. Cuando un dispositivo recibe este mensaje deberá ejecutar la actualización de localización periódicamente antes de que expire el temporizador de reposo M2M, y en cada actualización este temporizador se reiniciará.

Soporte a la multidifusión para M2M.

La estación base proveerá un servicio de multidifusión para un grupo de dispositivos M2M que comparten un flujo de datos en el canal de bajada. El establecimiento de este flujo se realizara mediante el procedimiento de adición DSA, en el cual se le asigna el identificador M2MCID. La estación base será la encargada de realizar la asociación entre el flujo de servicio y el M2MCID durante el intercambio de mensajes de señalización DSA y la podrá modificar siguiendo el procedimiento de desconexión DSC o también con un mensaje de actualización del M2MCID.

Antes de enviar los datos por el canal DL la estación base deberá notificarlo a los dispositivos con un indicador de tráfico multidifusión en el mensaje de paginación. En este mensaje también podrán incluirse la petición de reingreso a la red y el tiempo de inicio de la transmisión de datos de multidifusión desde la BS hasta el dispositivo, este tiempo deberá ser menor que el tiempo de inicio del próximo intervalo de paginación.

De modo que con todos los datos anteriores el dispositivo M2M pueda estar preparado para la recepción de los datos en el canal DL y ejecutar acciones previas como colocar un temporizador de espera de datos multidifusión durante el estado de reposo o incluso para apagarse hasta el momento indicado donde se inicia la transmisión desde la estación base.

Si no se incluye el tiempo de inicio de la transmisión en el mensaje, el dispositivo igualmente deberá comenzar a recibir los datos sin haber finalizado el estado de reposo.

Apagado anormal.

Cuando se produce un apagado de este tipo, el dispositivo M2M puede intentar reportar el evento. Por ellos se consideran dos escenarios, durante la operación normal y durante el estado de reposo.

Si el dispositivo tiene asignado recursos para la transmisión de los datos podrá hacer uso del mismo para enviar un encabezado de reporte de apagado anormal; si por el contrario no tiene recursos asignados el dispositivo activara el procedimiento de solicitud y asignación de ancho de banda, enviará el reporte y deberá iniciar un temporizador para mantenerse en espera de la confirmación desde la estación base; si el temporizador expira debe iniciar nuevamente el procedimiento de notificación.

Transmisión de ráfagas pequeñas.

Si a un dispositivo M2M en reposo se le asigna, durante el reingreso a la red, un ancho de banda suficiente para enviar pequeñas ráfagas de contenido M2M en el mensaje RNG-REQ, podrá hacerlo identificando la ráfaga de datos con el respectivo identificador de flujo (SFID). Si la estación base recibe los datos correctamente, entonces enviara al dispositivo la confirmación en un campo del mensaje RNG-RSP.

En caso de no ser suficiente el ancho de banda asignado para ejecutar la acción anterior, entonces el dispositivo deberá incluir una solicitud de ancho de banda en el mensaje RNG-REQ, para el flujo correspondiente (SFID). La estación base deberá enviar el acuse de recibo de esta solicitud en el mensaje REQ-RSP, y si lo acepta deberá asignar el ancho de banda solicitado en el canal UL, una vez completado el procedimiento de reingreso a la red por parte de ese dispositivo.

Capa de seguridad

Se establece una jerarquía de claves de autentificación de multidifusión para M2M. Partiendo de la clave de autorización (MAK), se genera la clave de cifrado de trafico grupal M2M (M2MGTEK).

Esta clave es compartida por todos los dispositivos M2M que pertenecen a un grupo de multidifusión, y se utiliza para cifrar los paquetes de este flujo de datos. Además se utiliza para cifrar los mensajes de gestión de acceso al medio que se envían desde la estación base a los dispositivos. Los componentes utilizados para generar la clave son, la clave MAK que es generada por la red, la semilla de seguridad del grupo M2M (MGSS) que es común para todos los dispositivos, el identificador del grupo M2MCID, y un número que equivale al conteo de claves M2MGTEK utilizadas.

Si un dispositivo se desliga del grupo, se genera una nueva semilla MGSS y la estación base la transmite a todos los miembros actuales del grupo, tanto a los que están en modo de conexión como en reposo. Adicionalmente se debe construir un

contador inicial único de 128-bit que será utilizado conjuntamente con la clave M2MGTEK en todos los mensajes de multidifusión que se envían.

Por último, también se brinda soporte a la validez del dispositivo M2M, donde se puede utilizar un procedimiento de autentificación basado en EAP para transportar el certificado de validez de un dispositivo a la red.

3.3.3 Estándar 802.16.1b

En este estándar se proponen algunas mejoras a la interfaz aire avanzada "WirelessMAN-Advance", mejor conocida como, WiMAX versión 2, en donde se incluyen las siguientes:

Identificadores y Direccionamiento

Se utilizara el identificador de la estación móvil (STID) de 12-bits, el cual es asignado por la estación base durante el ingreso a la red, para identificar a los dispositivos M2M. La estación base podrá asignar el mismo identificador a varios dispositivos, y cuando dos o más dispositivos M2M compartan el mismo STID, esta asignará la trama donde es válido el identificador para cada dispositivo.

Al igual que en el estándar anterior se define una zona M2M como la agrupación de múltiples estaciones base avanzadas (ABS) y se identifica con el M2M-GROUP-ZONE-ID, que se envían desde la estación base en el mensaje de configuración inicial AAI-SCD. Las estaciones base podrán formar parte, a la vez, de hasta cuatro zonas M2M.

El flujo de datos multidifusión compartido por los miembros de un grupo se identifica mediante el MGID, los dispositivos podrán estar asociados a varios flujos siempre y cuando pertenezcan a la misma zona M2M. El MGID será asignado por la BS luego del ingreso inicial del dispositivo M2M a la red siguiendo el procedimiento DSA y cumplirá las mismas características de asignación, modificación y mantenimiento que se explicaron para el identificador de conexión M2MCID.

Por último, se introduce un identificador de desconexión para dispositivos M2M fijos (FMDID), con el que se busca identificar exclusivamente a aquellos que ingresan al modo reposo, y se les retira cuando reingresan a la red.

Seguridad

Se incorpora una nueva clave de 128-bits a la jerarquía de claves, denominada clave de autentificación del canal UL (CMAC_SIG_KEY_U) para autentificación, y la clave MGTEK se usa para el cifrado de las transmisiones multidifusión de un grupo M2M. El método AES-CTR [36] es el recomendado para cifrar las ráfagas de datos.

Cuando ocurra un apagado anormal en el dispositivo, este deberá notificarlo a la estación base, por esto el dispositivo deberá estar en capacidad de enviar los datos cifrados basados en algoritmo CMAC [37] conjuntamente con cifrado AES.

En general las mejoras de seguridad planteadas son similares a lo realizado en el estándar 802.16p.

Asignación de recursos continua

Para aquellas aplicaciones M2M con prioridad alta, patrón de tráfico periódico, y una carga de datos parcialmente estable se realiza una asignación permanente de recursos UL al dispositivo donde se encuentra alojada, durante un periodo mayor. Esto permitirá reducir la sobrecarga de señalización que se produce en cada asignación. Esta asignación será realizada desde la estación base y podrá ser modificada o desasignada en cualquier momento. Además se proveen canales de alineación inicial dedicados para los dispositivos M2M y esquemas de prioridad de acceso.

Ingreso a la Red

En caso de que un dispositivo M2M requiera ingresar por primera vez o reingresar a la red motivado por un evento, deberá ejecutar el proceso de alineación inicial con la estación ABS en donde se le asignaran los ajustes como tiempo de espera, potencia, y frecuencia para sincronizar estos parámetros del canal UL con la estación base.

Si durante ese proceso el servicio UL que desea utilizar el dispositivo está condicionado por una ventana de acceso mínima, el dispositivo M2M deberá ejecutar un procedimiento aleatorio que le permita seleccionar un tiempo de inicio de transmisión adecuado.

Adicionalmente se podrá configurar un campo del mensaje AAI-SCD para restringir a los dispositivos M2M, desde la estación base, el uso de canales de alineación inicial para el reingreso a la red durante ciertas tramas. Para esto, se podrán configurar 4 clases de acceso distintas que a su vez podrán utilizar el canal durante 4 supertramas continuas. Además para aquellos dispositivos fijos se podrán omitir las actualizaciones de localización y la alineación periódica, ya que por su condición inmóvil seria un gasto innecesario de recursos intentar reajustar parámetros que muy probablemente resulten en el mismo valor.

Modo reposo

Se asignara igualmente un temporizador específico para los dispositivo M2M que ingresen al modo reposo, el cual vendrá indicado en el mensaje AAI-DREG-RSP, de esta forma el dispositivo sabrá que debe ejecutar una actualización de localización antes de que expire y luego reiniciar el temporizador.

Con respecto a la paginación grupal, se deberán incluir en el mensaje de paginación (AAI-PAG-ADV), el índice de la zona M2M conjuntamente con el identificador del grupo M2M (MGID), para sondear a todos los dispositivos de un grupo M2M, y si además se activa el campo "M2M report code" se le permitirá a los dispositivos la transmisión periódica de los datos almacenados; la periodicidad dependerá del ciclo de paginación que se establezca.

Cuando los dispositivos M2M inicien el modo reposo y no requieran una transmisión de datos constante se podrá asignar, en el mensaje (AAI-DREG-RSP), un valor alto al atributo "ciclo de paginación", y además en base a eso se podrá establecer un tiempo de espera de paginación mayor, de modo que permanezcan más tiempo de lo normal en estado de reposo, algo que indudablemente favorecerá a alcanzar el tan anhelado ahorro de energía.

Para reingresar a la red desde el modo en reposo los dispositivos M2M utilizaran los recursos de alineación dedicados asignados por la ABS en el mensaje AAI-SCD, pero en caso de que esto no suceda podrán hacerlo utilizando los recursos de control esenciales del sistema.

Para evitar la congestión que puede producir el reingreso de muchos dispositivos se designa a uno de los miembros del grupo para que realice las funciones de alineación en nombre de todos, utilizando parámetros del grupo (MGID), por lo que la estación base enviara el resultado del proceso a todos los miembros del grupo.

Transmisión de ráfagas pequeñas

Para realizar esta función se han previsto dos opciones relacionadas directamente con el estado en el que se encuentre el dispositivo M2M, si se encuentra en modo reposo los datos podrán incluirse en el campo SMS de los mensajes de alineación inicial AAI-RNG-REQ/RSP, mientras que cuando el dispositivo se encuentre conectado a la red se utilizara el mensaje de control de acceso al medio AAI-L2-XFER para enviar y recibir pequeñas ráfagas de datos dentro de su carga útil (*payload*).

Soporte a la multidifusión

Cada estación base podrá establecer una conexión para manejar el flujo de datos de multidifusión hacia un grupo de dispositivos identificados por el mismo MGID, esta conexión deberá respetar unos parámetros de tráfico y calidad de servicio previamente acordados. Cuando los dispositivos se encuentren en estado de reposo la ABS deberá incluir en el mensaje de paginación el indicador de trafico multidifusión y apenas finalice la transmisión de esos datos, la estación deberá notificarlo a los dispositivos mediante el mensaje AAI-MTE-IND, para que los dispositivos regresen al estado de reposo.

4 Casos de Uso.

Las comunicaciones M2M tienen el potencial para mejorar los procesos existentes en la mayoría de las industrias, como el cuidado de la salud, automotora, manufactura, energía, y seguridad pública, por nombrar solo algunas. Igualmente en términos de tecnología, M2M aplica a un gran número de de tecnologías de comunicación inalámbrica de corto alcance encargadas de conectar los sensores con tecnologías de acceso tanto fijas como inalámbricas, a través de un encaminador, y/o Gateway. Por ese motivo estimar la cantidad de dispositivos actualmente desplegados y su potencial crecimiento, no es una tarea fácil.

El alcance geográfico de las soluciones M2M puede ser local o hasta global, como es el caso del seguimiento a flotas de vehículos de las empresas de transporte multinacional, o una pequeña casa con electrodomésticos controlables de forma remota y conectados a una aplicación de gestión de energía que se ejecuta en un servidor local.

En los casos de uso se describen las interacciones entre las partes involucradas en alcanzar una meta, por una parte, uno o más elementos externos al sistema, y por otra parte, el sistema M2M considerado. Aquí se trata al sistema como una caja negra que ofrece funcionalidades utilizadas por los agentes externos.

De este modo los casos de uso se describen de forma neutral sin asumir ninguna arquitectura física en particular. Además, no deben ser confundidos con funcionalidades, características o requisitos, sino que por el contrario un caso de uso puede estar relacionado con uno o varios de los requisitos o funcionalidades, y viceversa.

4.1 Entornos de aplicación.

Definitivamente existen muchas aplicaciones M2M con distintas características. El 3GPP ha dividido las posibles aplicaciones MTC en 7 grandes áreas (3GPP TR 22.368), tal y como se aprecia en la tabla 6.

A continuación describiremos algunas características esenciales que hasta cierto punto comparten varias aplicaciones dentro de una misma área de aplicación.

Seguridad

Las aplicaciones de seguridad son principalmente utilizadas en la protección de objetos o personas, en ambos casos las personas podrán estar dotadas de dispositivos portátiles que contengan un modulo de comunicaciones M2M, y opcionalmente con función de GPS, que se encargaría de enviar información automáticamente o bajo demanda hacia una aplicación que podrá monitorizar su estado y posición.

Área de Servicio	Aplicaciones MTC
Seguridad	Sistemas de vigilancia Respaldo a líneas terrestres Control de acceso físico Seguridad coche/conductor
Rastreo y Seguimiento	Gestión de flotas Gestión de ordenes Pague mientras conduce Rastreo de activos Navegación Información del tráfico Peajes Optimización del tráfico
Pagos	Puntos de Venta (PoS) Maquinas expendedoras Maquinas de juegos
Salud	Monitorización de signos vitales Apoyo a ancianos y discapacitados Telemedicina Diagnostico remoto
Control y Mantenimiento Remoto	Sensores Iluminación Bombas Válvulas Control de ascensores Control de maquinas expendedoras Diagnostico de vehículos
Medición	Energía Gas Agua Calefacción Control de redes eléctricas Medición industrial
Dispositivos de Consumo	Marco de fotos digitales Cámara digital Libro electrónico (eBook)

Tabla 6. Áreas de utilidad y posibles aplicaciones MTC según 3GPP.

Con esto se busca mejorar la seguridad y/o la monitorización remota ante eventos imprevistos. Los servicios deberán ser implementados en aplicaciones alojadas en un dispositivo con capacidades M2M que podrá ser una tarjeta. Debido al almacenamiento de datos sensibles, se debe asegurar la protección del modulo M2M contra robo y mal uso.

Dentro de esta también se busca mejorar las capacidades de monitorización e interacción de los sistemas de supervisión y control de acceso físico a lugares determinados, bien sea con el uso de tarjetas inteligentes o cámaras de video con capacidades M2M [38].

Estas aplicaciones se caracterizan por ser sensibles al retraso, tener baja carga de datos, cuando no se requiera la transmisión de audio y video, requieren conexiones seguras, además de acceso prioritario ante otras aplicaciones.

Rastreo y seguimiento

Estas aplicaciones están relacionadas principalmente con la industria automotora, aunque también se podrán considerar algunas basadas a la localización y seguimiento de alimentos en ambiente de producción o cadena de suministro.

Las aplicaciones de gestión de flotas se enfocan en incrementar la eficiencia operativa e incrementar el aumento de los ingresos. Estos servicios son muy amplios e incluyen diagnostico remoto, sistemas de navegación, entre otros. Para estos casos existe un criterio común establecido por el comité técnico del Consejo Electrónico Automotriz (AEC), quien es el encargado de dictar los estándares para componentes electrónicos confiables y de alta calidad.

En estas aplicaciones las empresas instalan un dispositivo M2M que se incorpora al vehículo y recolecta información de localización, tiempos, atascos, datos de mantenimiento y condiciones ambientales del producto que se transporta , que puede ser enviada a una aplicación central que permita rastrear el vehículo para optimizar la ruta y el plan de entrega de las encomiendas. Un criterio a considerar en este caso de uso es que los módulos utilizados para las comunicaciones M2M deberá ser capaz de funcionar normalmente por un tiempo mayor o igual a la vida útil del vehículo.

Entre las características que presentan estas aplicaciones tenemos dispositivos altamente móviles, poca carga de datos, y tanto las políticas como la facturación podrán realizarse basadas en grupos.

Pagos

Hoy en día la mayoría de los terminales de puntos de venta utilizados en bares y restaurantes, están conectados por medios cableados. Esto provoca que estén ubicados permanentemente en un sitio y para realizar la transacción la persona debe ir al lugar donde se encuentra el terminal. Esto crea inconvenientes a los anfitriones y trabajadores, así como para el cliente. Lo más conveniente sería conectar los terminales PoS a través de una red inalámbrica local con ciertas condiciones de seguridad.

La incorporación de dispositivos M2M en este ambiente permite posibilidades adicionales para las aplicaciones, ya que estos pueden ser instalados en los terminales PoS, parquímetros, entre otros, para proveer la comunicación necesaria para transacciones en línea con tarjeta de crédito o debito, ofreciendo también un canal de comunicación seguro [39]. Los dispositivos M2M para estas aplicaciones necesitan aprobar requisitos de seguridad específicos para realizar transacciones financieras.

Estos sistemas son típicamente fijos o con poca movilidad, ya que la mayoría de las maquinas expendedoras (*vending*) son estacionarias, los terminal PoS utilizados en los restaurantes tiene movilidad reducida, la excepción ocurre en maquinas expendedoras ubicadas en transportes como trenes las cuales tienen gran movilidad.

Las transacciones con tarjetas de créditos típicamente requieren poca transmisión y recepción de datos, la mayor parte de las transacciones son originadas por el terminal, y requieren soporte de seguridad mejorado para la protección de datos.

Salud

La monitorización remota de pacientes típicamente involucra el uso de conectividad Bluetooth entre el equipo de monitorización y el dispositivo que actúa como Gateway, que a su vez da acceso a la red WAN. Las aplicaciones de cuidados para el hogar utilizan una variedad de sensores que se comunican mediante una red local, denominada por el ETSI como red de área M2M, y que se conectan a internet utilizando un Gateway residencial y una conexión banda ancha [40].

Los equipos recolectores de datos en un sistema de cuidado de salud son típicamente sensores para monitorizar varias medidas como presión sanguínea, temperatura, frecuencia cardiaca, colesterol, entre otros.

Este tipo de sensores podrá estar conectado con un Gateway que se desplace con la persona, como un teléfono móvil, que a su vez actúa como un concentrador de todos los datos recolectados, y los envía hasta los servidores de monitorización en donde se ejecutan las aplicaciones M2M.

Esto permitiría que la población mayor pudiera estar complemente monitorizada en tiempo real, y en caso de algún inconveniente se podrá enviar una ambulancia al lugar. Por lo general este tipo de aplicaciones se caracterizan por tener baja movilidad, son sensibles a retardos, requieren prioridad alta y ofrecen baja carga de datos.

Control y Mantenimiento a distancia

Un ejemplo típico son las maquinas expendedoras, en donde el mantenimiento y recarga se realiza por personal dedicado quien tiene que visitar los lugares donde se encuentren estas maquinas a intervalos regulares de tiempo para verificar los niveles de llenado, recargarla, realizar el mantenimiento preventivo e identificar daños.

Los dispositivos M2M podrán agregar la posibilidad de optimizar las operaciones, ya que pueden proveer información confiable del estado de la maquina, como niveles reales de productos, estado de mantenimiento, posibles daños, entre otras. Igualmente se podrá enviar información hasta las maquinas para actualizar precios o ejecutar mantenimiento remoto, reduciendo el tiempo necesario de visitas a estas maquinas expendedoras.

Dentro de esta área también corresponden aplicaciones orientadas a las redes inteligentes de energía, y la eficiencia energética. Por ejemplo, se pueden colocar sensores de ocupación en las habitaciones de la vivienda para verificar si está o no ocupada, y en caso de que la habitación esta vacía las luces se apagaran automáticamente [41].

Este ejemplo se puede extender a otros sensores (temperatura externa, consumo de electricidad en el calentador de agua, entre otros) en la casa para controlar el consumo de energía, de igual forma estos sensores y actuadores estarán conectados con el Gateway M2M de la residencia, por medios fijos o inalámbricos. Adicionalmente se pueden controlar las válvulas y sensores ubicados en instalaciones críticas y remotas, evitando que el personal responsable deba asistir al sitio para realizar mediciones o evaluar el estado del elemento.

Se espera que los sensores y actuadores desplegados consuman poca potencia, de modo que el usuario final no tenga que reemplazar sus baterías antes de mucho tiempo, hay que recordar que en la práctica algunos de estos sensores estarán en lugares difícil acceso.

Este caso también podrá referirse a monitorización de energía, con lo que el usuario podría estar informado de su consumo actual de energía, de forma global o especifica (por equipo), con posibilidad de acceso remoto para que el usuario pueda disponer la información actualizada aun cuando no se encuentre en casa. Se le podrá notificar al

usuario con una alarma en caso de que se produzca un nivel de consumo diferente al habitual.

Como características de este tráfico tenemos que tienen movilidad baja o nula, sensibles al retraso y también requieren prioridad de acceso, los dispositivos M2M pueden direccionar, facturar y establecer las políticas basados en grupo, puesto que seguramente una aplicación dispondrá de muchos dispositivos M2M con comportamiento similar.

Mediciones

Las empresas de servicios públicos pueden desplegar servicios de medición inteligente con la instalación de dispositivos de medición con capacidades M2M los cuales envían información automáticamente o bajo demanda hacia el servidor de aplicaciones en donde se podrá realizar la facturación directa sobre la medición realizada. Con esto aumentaría la eficiencia del servicio puesto que se pudiera entregar un consumo de luz, gas o agua más acertado y en tiempo real, sin intervención humana [42].

Los dispositivos de medición típicamente se encuentran en ambientes duros con espacio limitado, por lo que los módulos M2M deberán ser pequeños. El hecho de que estos dispositivos se encuentren aislados y sin vigilancia invita a realizar una protección eficaz de los datos, incluyendo el caso de robo o mal uso del modulo M2M. Sin duda que el intercambio de información en la interfaz aire entre los equipos de medición y el servidor de aplicaciones para la actualización de los datos en ambos extremos (transmisión/recepción) también deberá asegurarse contra ataques que intenten modificar los datos.

Otro caso que se deriva en esta área es la figura de prepago de los servicios básicos, donde el consumidor podrá adquirir una cuota mensual por los servicios de agua, gas, y luz; la información correspondiente con el volumen de servicios contratados se envía hasta los medidores M2M, los cuales la almacenan y monitorizan diariamente el consumo actualizado en el hogar, y cuando se alcanza la cuota contratada se suspende el suministro del servicio. Se puede incluir opcionalmente algún tipo de alarma que indique que se está llegando al final del consumo para que el usuario pueda tomar las acciones pertinentes.

Estas aplicaciones disponen de dispositivos prácticamente fijos o con muy poca movilidad, poca carga de datos, con dispositivos con funciones similares se puede realizar gestión basada en grupos, y en algunos casos las aplicaciones son sensibles a retardo y requieren acceso prioritario.

Dispositivos de Consumo

La función principal de estas aplicaciones está en la distribución de contenido multimedia. Los sistemas multimedia incluyen almacenamiento en el servidor, transporte (redes Wi-Fi, Bluetooth, UWB), y utilización de los contenidos realizado por dispositivos como televisión, libro electrónico, teléfono inteligente, entre otros.

La intervención de las comunicaciones M2M podrá ayudar a la toma de decisiones por parte de los dispositivos, por ejemplo cuando se utiliza una cámara de video o fotográfica al regresar a casa el servidor podrá consultar si existe información nueva para almacenarla y que se encuentre disponible para ser reproducida por cualquiera de los otros dispositivos multimedia del hogar.

En dichas aplicaciones la carga de datos es mayor porque se intercambia contenido multimedia, pero por el contrario son tolerantes a retrasos y también se pueden controlar basadas en el tiempo.

El ETSI ha basado su trabajo de estandarización de la tecnología M2M en una serie de casos de uso que se desprenden de 6 familias, como se aprecia en la tabla 7.

Estándar	Área	Estado
TR 102 691	Mediciones Inteligentes	Publicado
TR 102 935	Red Inteligente de Energía	Publicado
TR 102 898	Aplicaciones Automotoras	Publicado
TR 102 732	e-Salud	Borrador
TR 102 857	Consumidor interconectado	Borrador
TR 102 897	Automatización de la Ciudad	Borrador detenido

Tabla 7. Familia de Estándares ETSI, para casos de uso M2M.

De los 6 reportes técnicos iniciados se han finalizado 3 para la fecha de realización de este trabajo. Los reportes desarrollados no intentan ser cerrados pero si sirven como una aproximación para todos los diversos servicios de valor agregado. La intención era cubrir la mayor parte de los casos de uso para asegurar que se involucrasen los requisitos M2M del sistema presentes en la mayoría de las aplicaciones M2M.

Debido a la diversidad de posibles casos de uso, el ETSI comprendió la necesidad de establecer un método que permita desarrollarlos paso a paso, por eso se estableció una plantilla que es fundamental para aportar algo de formalismo en la descripción, y facilitar la compresión de los requisitos de cada caso de uso. En la tabla 8 se observan las seis secciones que conforman la estructura para la descripción de un caso de uso desarrollado según el ETSI [43].

Sección	Descripción
Descripción general del caso de uso	Objetivos/metas en términos de alto nivel del caso de uso, identificando los problemas principales.
Partes Interesadas	Identificar que o quiénes son los referentes del caso de uso (consumidor, operador de red, entidad de facturación).
Descripción del escenario	Describir textualmente como utilizan el sistema las partes interesadas, se pueden establecer condiciones previas del caso.
Intercambio de información	Descripción paso a paso del flujo de información (registro, recuperación o entrega de datos) implicado en el caso de uso.
Requisitos nuevos potenciales	Lista de nuevos requisitos que se derivan del caso de uso
Fuentes del caso	Hacer referencia a la entidad o documento que lo desarrolló.

Tabla 8. Estructura ETSI para describir casos de uso M2M.

4.1.1 Medición Inteligente

Los casos de estudio relacionados con esta área se definieron en [43], el trabajo estuvo bastante relacionado y conducido por el mandato M/411 de la comisión europea para medición inteligente, cuya objetivo es crear estándares que permitan la interoperabilidad entre los instrumentos de medición de los servicios públicos (agua, gas, electricidad), que a su vez ayude a mejorar los medios por los cuales se notifican los consumos reales de los clientes para adaptar la producción a sus demandas. La medición inteligente busca principalmente mejorar la eficiencia en el consumo de la energía.

Las mediciones inteligentes permiten eliminar la necesidad de aproximar las facturas, que los humanos deban realizar lecturas de los contadores, y por el contrario proveen información acertada y a tiempo de la cantidad consumida del servicio contratado a las empresas generadoras, distribuidoras, y a los clientes. También pueden proveer otros servicios como, capacidad de controlar el consumo en tiempo real.

En un reporte del grupo de coordinación de las mediciones inteligentes (SMCG), conjuntamente con otras organizaciones incluyendo el ETSI, se documento una lista de funcionalidades que deben proveer los sistemas de medición inteligente [44]. Esta lista, agrupada en 6 categorías, representa las propuestas de nuevas funcionalidades que se deben soportar además de las típicas ofrecidas por los medidores convencionales. Las 6 categorías de funcionalidades se describen a continuación:

- **Lectura remota de los registros metrológicos y provisión hacia una empresa:** capacidad de proveer remotamente el valor registrado en el medidor, a la empresa interesada utilizando una interfaz estándar, bajo una planificación de tiempo predefinida o bajo demanda.
- **Comunicación mutua entre el sistema de medición y la empresa:** capacidad del sistema de medición para capturar datos relativos a la usabilidad, calidad y estado de la red, eventos, estado del medidor, y cualquier otra información que no está relacionada con la medición en sí, y enviarla hasta la empresa. Capacidad de la organización para configurar el sistema de medición remotamente y realizar actualizaciones de firmware/software. Capacidad del sistema de medición para recibir información que es enviada desde el proveedor del servicio hasta el consumidor.
- **Medidor que soporta sistemas avanzados de tarificación y pago:** capacidad del sistema de medición para permitir al cliente pagar por adelantado el uso de un servicio, conectarlo a la fuente y desconectarlo luego del consumo predeterminado o por agotamiento de cierto tiempo. Con respecto a la tarificación el sistema estará provisto de varias tarifas registradas durante diferentes franjas horarias permitiendo conocer tarifa actual, hora critica, entre otras.
- **Medidor capaz de habilitar y deshabilitar un servicio remotamente:** capacidad para permitirle a la empresa controlar o configurar de modo seguro limitación en el suministro del servicio, habilitar y deshabilitar el servicio mediante parámetros configurables establecidos en el medidor.
- **Comunicación con dispositivos individuales dentro de las instalaciones del consumidor:** capacidad del sistema para exportar datos de forma segura hacia algún dispositivo individual o en un sistema de gestión de energía dentro la edificación para su análisis.
- **Proveer información desde el medidor hasta alguna pantalla o equipo auxiliar local a través de un portal web o Gateway:** capacidad del sistema para proveer información del uso total y otros valores metrológicos y no metrológicos hacia un monitor visual externo.

En la figura 17 se detalla el despliegue típico de equipos en el escenario de medición inteligente. Se observan los dispositivos como válvulas, medidores de luz, gas, y agua, los cuales se conectan a los centros de datos mediante un Gateway. El centro de datos recolecta la información de los equipos y además está en capacidad de controlar los dispositivos de forma remota a través del Gateway de comunicación, quien también provee una interfaz hacia los dispositivos de automatización del hogar como sensores, televisores, electrodomésticos, y generadores de electricidad instalados en el hogar.

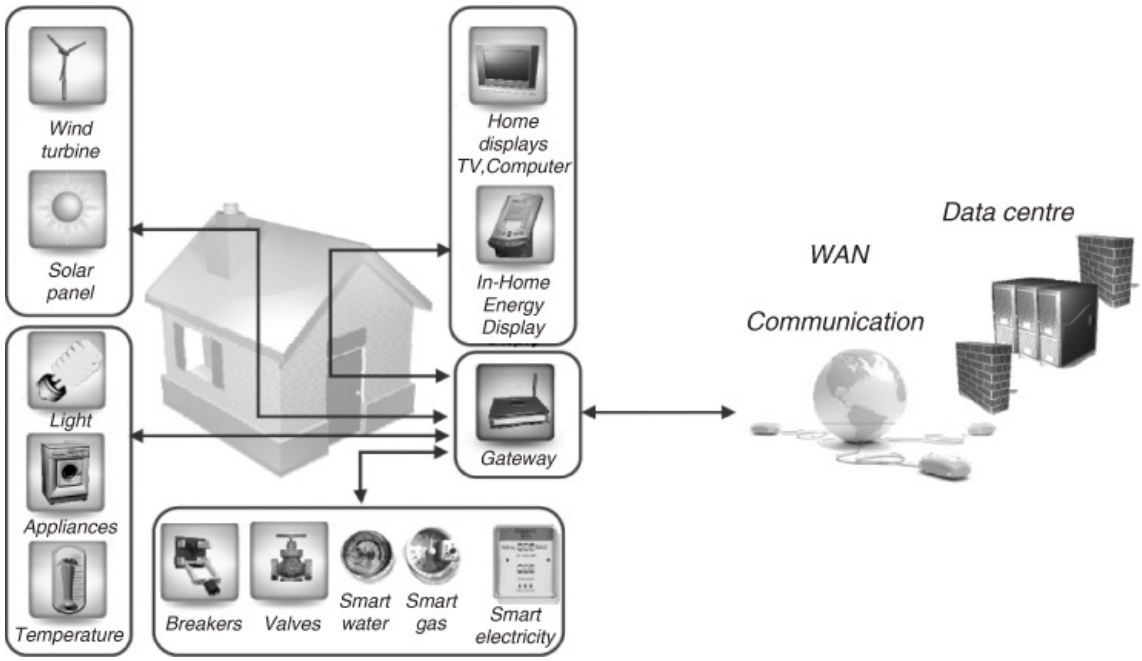


Figura 17. Escenario típico de un sistema de medición inteligente.

Ejemplo de caso de uso descrito por el ETSI**: Gestión de datos de interrupción del servicio**.

Descripción general

El operador de la red de distribución proveerá datos relacionados con una interrupción del servicio, programada, hacia el sistema de medición inteligente. De igual forma, el sistema de medición inteligente podrá enviar información relacionada con una interrupción del servicio, no programada, hacia el operador de la red de distribución y/o la entidad de facturación.

Partes interesadas

Operador de la red de distribución: organización responsable de gestionar la red de provisión de servicios públicos (luz/gas/agua) hacia las instalaciones del cliente.

Entidad de facturación: organización responsable de facturar servicios al cliente.

Consumidor: persona u organización que contrata y utiliza los servicios públicos en sus instalaciones.

Escenario

Condiciones previas: el sistema de medición inteligente está instalado y configurado para detectar cualquier corte de corriente y enviar las notificaciones al operador de la red de distribución. Además, El sistema de medición reconoce al

operador de la red de distribución y a la entidad de facturación, y tiene direcciones de comunicación para ambos.

Condiciones posteriores: el operador de red recibe la información solicitada con relación a la interrupción del servicio y es consciente de que ha ocurrido una falla.

Activador: se interrumpe súbitamente el servicio hacia el sistema de medición inteligente, o el operador de la red de distribución decide realizar un corte planificado.

Intercambio de información

Fuljo básico para corte de suministro inesperado:

1. El operador envía una solicitud de información al sistema de medición.
2. El sistema de medición valida la solicitud.
3. El sistema de medición recupera toda la información detallada del corte.
4. El sistema envía la información al operador de red o a la entidad de facturación.
5. El operador y/o la entidad reciben la información.

Flujo básico para corte de suministro planificado:

1. El operador envía al sistema la información detallada del corte planificado.
2. El sistema valida el mensaje.
3. El sistema muestra un mensaje con los detalles al consumidor.
4. El consumidor acepta el mensaje.
5. El sistema de información le envía al operador, el mensaje de confirmación.

De estos flujos básicos se desprenden varios alternativos, que dependen de la aparición de fallas en alguno de los pasos, la lista completa la pueden encontrar en [43].

Requisitos potenciales

- El sistema M2M debe soportar sincronización de tiempo segura y precisa.
- La aplicación M2M deberá estar en capacidad de establecer en los dispositivos M2M un reporte periódico de eventos, o bajo demanda.
- Los extremos del sistema M2M deberán ser capaces de verificar la integridad de los datos intercambiados.
- Para recibir información de los dispositivos y Gateway M2M, el sistema deberá soportar mecanismos de recepción de información programada, y no solicitada.
- Soportar autenticación mutua entre el usuario final y aplicación o la capacidad de servicio M2M.
- Soportar autenticación de dispositivos y Gateway M2M.

Fuente del caso

Grupo de industrias de medición inteligente europeas (ESMIG) [45].

4.1.2 Red Inteligente de Energía

Una red inteligente de energía o *smart grid* (SG), fue definida por el grupo experto de la comisión europea como, aquella capaz de integrar de manera eficiente el comportamiento y las acciones de todos los abonados que la conforman, para asegurar un sistema energético sostenible y eficiente con pocas perdidas, y altos niveles de calidad y seguridad en el suministro [46].

Una red inteligente tendrá numerosos electrodomésticos interconectados de forma compleja de modo que puedan reportar el consumo de energía u otra información de monitorización, hacia elementos centrales. El desarrollo de especificaciones para estas redes ha sido guiado por el mandato de estandarización (M/490), realizado por la comisión europea y distribuido a todos los organismos de estandarización para apoyar el despliegue de las SG.

Es común aceptar que las redes eléctricas se basan principalmente en una infraestructura de monitorización de sensores a gran escala, conjuntamente con el despliegue constante de infraestructuras de medición inteligente. El trabajo del ETSI para apoyar el despliegue de las redes inteligentes de energía utilizando comunicaciones M2M se documento en el reporte técnico (TR 102 935) [47].

Dentro del ETSI se propuso una arquitectura de 3 capas principales para la red inteligente de energía:

- Capa de energía, que consiste en:
  - Generación masiva
  - Recursos energéticos distribuidos (DER)
  - Distribución de energía (voltaje medio/bajo)
  - Transmisión de energía (alto voltaje)
- Capa de control y conectividad, que consiste en:
  - Soporte de tecnologías de información ICT.
  - Comunicación entre dispositivos
  - Respuesta a variaciones en la demanda energética
- Capa de servicios, que consiste en:
  - Mercado: operadores y participantes en el mercado eléctrico.
  - Proveedor de servicio: provee servicios al cliente de la red eléctrica.

El grupo de trabajo M2M del ETSI enfoca su estudio en las capas 2 y 3 (control y conectividad, y servicios) debido a que el objetivo principal es evaluar el impacto que tienen las redes inteligentes de energía sobre la arquitectura funcional propuesta, en el documento (ETSI TS 102 690), para las comunicaciones M2M.

En la figura 18 se observa la arquitectura de comunicación diseñada para la red inteligente de energía [48]. La energía se envía desde la planta de generación hacia los usuarios finales a través de dos componentes, primero la subestación de transmisión de energía localizada cerca de la planta de generación, y luego un grupo de estaciones de distribución.

Esta topología de red se divide en varias redes más pequeñas que representan los despliegues característicos de una ciudad o área metropolitana, las cuales están conformadas por muchos barrios. En cada barrio hay cientos o miles de edificaciones, y en cada edificación hay varios apartamentos. Por este motivo, la arquitectura de comunicación se deriva de la planificación real de un área metropolitana.

La arquitectura de comunicación está dividida en un número de redes jerárquicas denominadas, redes de área de barrio o vecindario (NAN), redes de área de edificación (BAN), y redes de área domestica (HAN). Para facilitar la descripción se considera que el área de servicio de cada barrio está cubierta por una estación de distribución y que cada red NAN está formada por varias redes BAN. Por otra parte como cada BAN, contiene varios apartamentos, entonces una red BAN estará formada por varias HAN.

Además, en el diagrama se representan los medidores inteligentes descritos en el caso de uso anterior, los cuales son piezas claves en el desarrollo de una red inteligente de energía. En el diagrama están representados como NAN Gateway, BAN Gateway, y HAN Gateway.

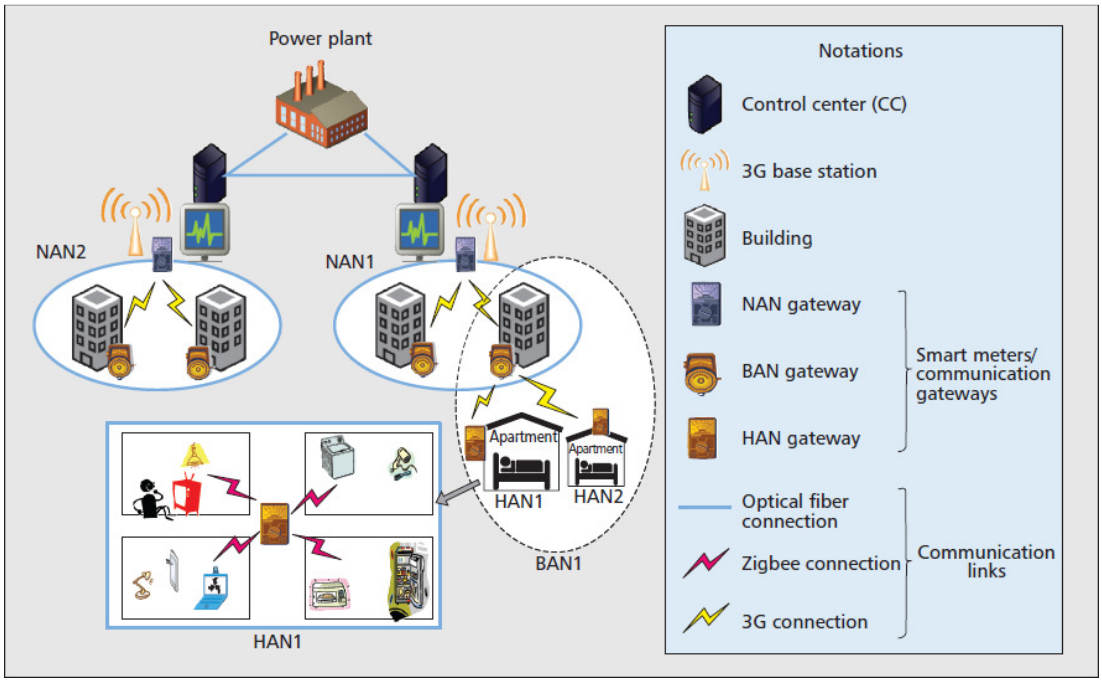


Figura 18. Arquitectura de comunicación de las redes inteligentes de energía.

Ejemplo de caso de uso descrito por el ETSI**: Gestión de la energía en el hogar**.

Descripción general

Este caso de uso se enfoca en la recolección y agrupación, en el Gateway de energía del hogar, de los datos recibidos desde los medidores. Consiste en el envío de datos de la red eléctrica hacia el Gateway, luego este último envía esos datos hacia una plataforma de energía M2M para su agregación y procesamiento. Los datos podrán enviarse a dispositivos de usuario o a una plataforma de servicios remota. En la figura 19 se representa el diagrama de referencia para este caso de uso, identificado en [47].

Partes interesadas

Consumidor: es la persona que utiliza la electricidad, y además puede ejercer acciones específicas como detectar el elemento encargado del aumento inusual en el consumo de un electrodoméstico y solucionar el problema, modificar el consumo de energía de acuerdo a recomendaciones del proveedor de servicios, entre otras.

Proveedor de servicios: es el encargado de desplegar las redes de sensores, proveer la infraestructura de interconexión de los medidores inteligentes, proveer el Gateway de energía para recolectar y transmitir los datos, entre otras actividades.

Operador de telecomunicación: provee los servicios de acceso a la red de comunicación a través del Gateway de energía, asegura el transporte de los datos, provee mecanismos de privacidad dependiendo del nivel requerido.

Escenario

Condiciones previas: el Gateway de energía del hogar esta conectado a todos los dispositivos y medidores del hogar, para recolectar información total o individual del consumo en el hogar.

Condiciones posteriores: los terminales de los usuarios y el centro de control reciben la información relacionada con el consumo de los electrodomésticos y la procesan para exhibirla al usuario.

Activador: se cumple el período de actualización establecido previamente o se hace una petición de información por parte del usuario o el centro de control.

Intercambio de información

1. El usuario o centro de control envía una solicitud de información al Gateway.
2. El Gateway valida la solicitud.
3. El Gateway recolecta toda la información detallada del consumo.
4. El Gateway envía la información al usuario o el centro de control.
5. El usuario y/o la plataforma de servicios reciben la información.
6. Los datos son mostrados en un equipo terminal de usuario.

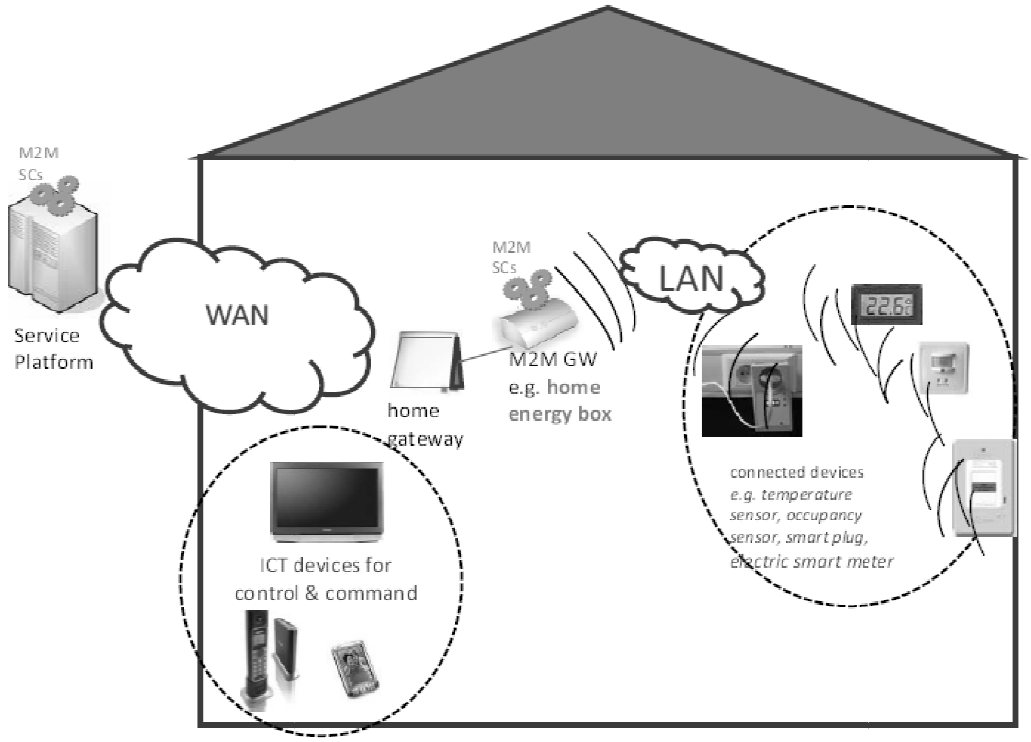


Figura 19. Diagrama de referencia para caso de uso "gestión de la energía en el hogar".

Requisitos potenciales

- Seguridad, autentificación y cifrado de datos.
- Capacidad para transportar documentos XML.
- Permitir comunicación bidireccional en tiempo real entre los extremos con la presencia de NAT.
- Proveer acceso selectivo a estructuras de datos y primitivas.

4.1.3 Aplicaciones Automotoras

El reporte técnico (ETSI TR 102 898), publicado en abril de 2013 [49], describe una serie de casos de uso relacionados con el sector automotor. La figura 20 representa el escenario considerado por el ETSI para la industria automotora en redes con capacidad de comunicación M2M.

En las redes automotoras, los vehículos pueden comunicarse entre ellos (V2V), o con una infraestructura (V2I), los casos de uso pueden dividirse en 2 grandes categorías seguridad (seguimiento de vehículo, diagnostico remoto), y navegación conectada (gestión del tráfico, servicios de entretenimiento, conectividad a internet).

Con respecto a la primera, los servicios telemáticos en el vehículo pueden ser utilizados para recuperar vehículos robados. Las características físicas del vehículo se almacenan la unidad de control telemática (TCU) y se transmiten hacia una central de

gestión de vehículo robado (SVT), los datos deben incluir información del GPS, parámetros del motor, y de ser posible video capturado por una cámara externa.

Si además, la TCU esta interconectada con el sistema de gestión del motor (EMS) se podrá regular la velocidad e incluso inmovilizar el vehículo a distancia. Los requisitos de ancho de banda son bajos cuando no se incluye la opción de video, por ese motivo los servicios de datos móviles 2G serán suficientes para transportar la información básica.

El diagnostico remoto podrá ser útil en diferentes situaciones como recordar mantenimiento preventivo, notificar una falla, o realizar una llamada por avería del vehículo. Cualquiera sea el motivo para activar el diagnostico remoto, la TCU recopilara la información general del estado vehículo y la enviara a su dueño o al fabricante, incluyendo los códigos de diagnostico (DTC) cuando contiene un problema.

Por otra parte, los servicios de navegación son claves en la búsqueda de soluciones a los problemas de congestión en las carreteras que enfrentan día a día los conductores. El número de vehículos en las vías ha aumentado rápidamente, superando las infraestructuras viales.

El impacto de esta congestión no es solo hacia el bienestar de las personas, sino que además incrementa el consumo de combustible, que a su vez incrementa los costos y las emisiones. Las redes vehiculares buscan atender esta necesidad mediante comunicaciones M2M bidireccionales entre vehículos e la infraestructura que transmite información del tráfico.

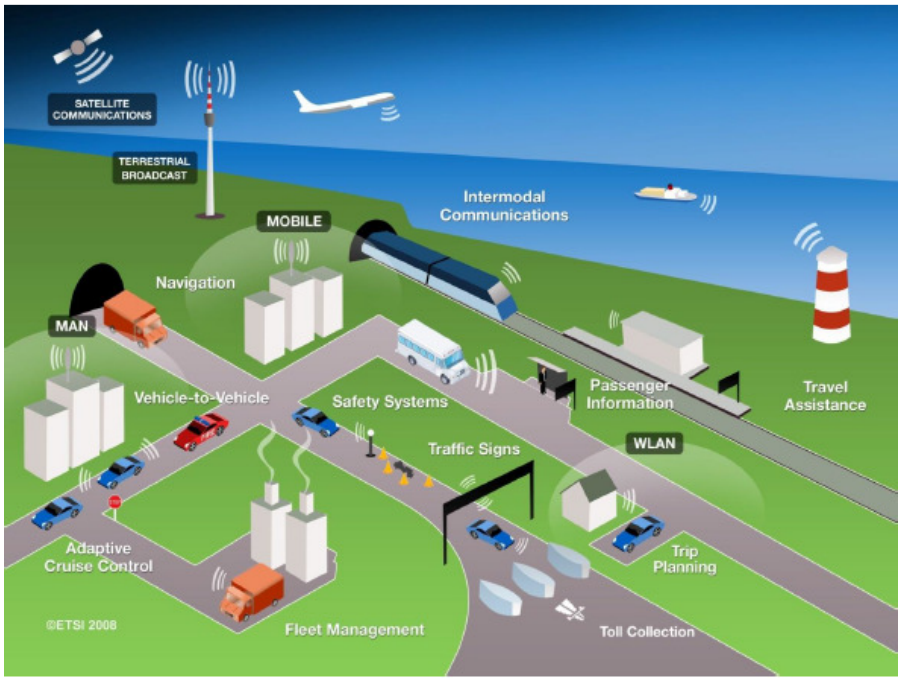


Figura 20. Escenario automotor para las comunicaciones M2M.

Entre las aplicaciones que se pueden realizar basadas en la información disponible en la infraestructura vial se encuentra la gestión de tráfico en tiempo real, donde la emisión constante de reportes de tráfico ayudara a cambiar la ruta para evitar atascos en cualquier punto de la ruta hacia el destino final.

La selección de la ruta puede ser optimizada utilizando un servicio provisto por el fabricante del vehículo o algún proveedor externo, que realice una planificación basada en el tráfico en tiempo real. La velocidad de transmisión requerida para estos servicios no deberá ser muy elevada puesto que solo se necesita capturar información del tiempo, coordenadas, velocidad, e identificación del vehículo, lo cual deberá ser tan solo algunos bytes.

Finalmente gracias a la cobertura amplia de las redes de acceso inalámbrico (Wi-Fi, WiMAX y 3GPP), puede ser posible desplegar un servicio confiable de información para el conductor y pasajeros con contenido en línea y entretenimiento en los vehículos. Que pueden incluir correo electrónico, redes sociales, noticias, televisión, video conferencia, entre otras.

Los servicios de retransmisión de audio y video necesitan un ancho de banda amplio y estable para mantener un buen nivel de calidad de servicio, aunque siempre aceptan un cierto nivel de pérdida de paquetes; mientras que los servicios de contenido estático son menos susceptibles a las variaciones de ancho de banda disponible y en algunos casos hasta tolerantes ante retardos.

Ejemplo de caso de uso descrito por el ETSI**: Gestión de flota y seguimiento de vehículo robado**.

Descripción general

El sistema M2M es utilizado por el vehículo para enviar periódicamente su localización, bien sea para su uso en la gestión de flota de vehículos o para seguimiento de un vehículo robado. La importancia de este caso de uso radica en que puede ser la guía para la configuración y despliegue de una red de comunicación M2M para gestión de flotas y/o seguimiento ante algún robo. Además que este caso de estudio presenta requisitos de servicio M2M diferentes a los anteriores porque involucra dispositivos con alta movilidad.

Las dos aplicaciones pueden ser tratadas bajo un mismo caso, porque se fundamentan en lo mismo y son topologías muy similares, además que el intercambio y tipo de información son iguales (coordenadas obtenidas por GPS). Sin embargo la incorporación de servicios de valor agregado podrá hacer la diferencia entre ambas.

Partes interesadas

Dueños del activo: son las personas u organizaciones responsables del vehículo que se está siguiendo. Están en capacidad de realizar una consulta para determinar la ubicación del activo y recibir el reporte de localización mediante comunicaciones M2M.

Activos de alto valor: son los vehículos con dispositivos M2M incorporados capaces de interactuar con alguna tecnología de detección de localización como GPS o mecanismos de la red móvil como Cell-ID, y que además utilizan la red de comunicaciones móvil para enviar directamente el reporte de localización hacia un servidor de aplicación M2M.

Infraestructura de localización: son elementos externos a la arquitectura M2M encargados de aportar la localización del vehículo.

Red de telecomunicación: los dispositivos M2M instalados en los vehículos interactúan con la red de comunicaciones móviles que sirve el área donde se encuentra.

Servidor de seguimiento: es el servidor de aplicación M2M que podrá realizar consultas (localización/velocidad) sobre los dispositivos M2M instalados, aunque también los dispositivos M2M pueden estar programados para enviar esta información al servidor periódicamente o luego de suceder un evento especifico.

Escenario

Condiciones previas: el vehículo tiene instalado un dispositivo M2M, que está conectado con el sensor de medición de velocidad, los dispositivos de detección de la localización y además cuenta con un servicio activo de datos móviles, con cualquier red de telecomunicación móvil que brinde cobertura durante su ruta. Además el dueño del activo tiene correctamente instalado un servidor de aplicación M2M que interactúa con los dispositivos M2M.

Condiciones posteriores: el dueño de la flota recibe información relacionada con el tiempo, la velocidad, y localización de los vehículos.

Activador: se cumple el tiempo estimado para reportar la localización (intervalos regulares, horas preestablecidas), se hace una petición desde el servidor M2M, o si ocurre un evento que activa el envío del reporte, por ejemplo si se cruza un determinado perímetro geográfico.

La imagen 21 muestra el diagrama de referencia para este caso de uso, donde se aprecian vehículos con dispositivos M2M conectados a un servidor central M2M, mediante una red de telecomunicaciones.

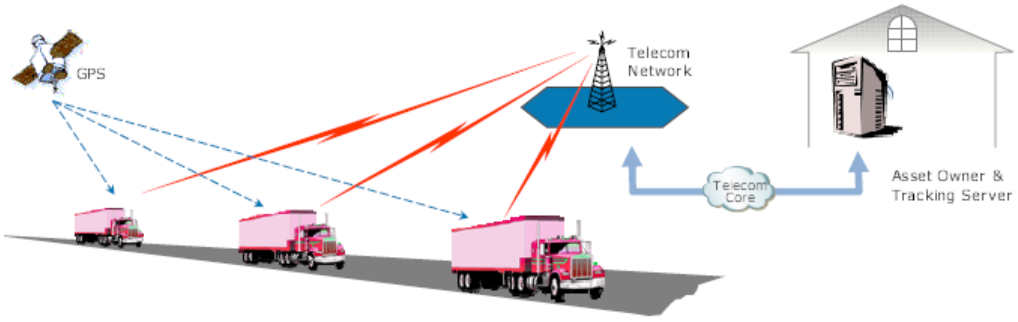


Figura 21. Diagrama de referencia para caso de uso "gestión de flota".

Intercambio de información

1. El servidor de aplicación M2M envía los parámetros establecidos hacia los dispositivos M2M (tiempos planificados para realizar la medición, intervalo para envío de reporte, y eventos que motivan el envío del reporte).
2. Se despliega la flota con capacidades M2M.
3. El dispositivo M2M realiza la medición, motivada por planificación o evento.
4. La infraestructura de localización envía la información al dispositivo.
5. El dispositivo M2M realiza la conexión con el servidor M2M por medio de la red de telecomunicaciones móvil.
6. Se cargan los datos en el servidor.
7. El servidor procesa los datos y muestra la información gráficamente.

Requisitos potenciales

- Capacidad de los dispositivos M2M para recibir, almacenar, y ejecutar tareas basadas en planificación.
- Habilidad de los dispositivos para sondear y verificar la ocurrencia de eventos.
- Capacidad de los dispositivos para establecer comunicación independiente con el proveedor de red de comunicación.
- Capacidad del dispositivo para mantener comunicación del servicio M2M aun cuando se traslade a altas velocidades.
- Habilidad de los dispositivos para ser contactados por la red de comunicaciones.

4.1.4 e-Salud

El ámbito de la salud también está siendo considerado como uno de los que se puede beneficiar por el desarrollo de estándares para las comunicaciones M2M, actualmente se está realizando un reporte técnico (ETSI TR 102 732) [50], que recopila la descripción de diversos casos de uso para aplicaciones e-Salud, actualmente está en estado de borrador y su ultima actualización fue realizada en marzo del 2011.

Actualmente existe un incremento en el despliegue de aplicaciones e-Salud y sus respectivos dispositivos para las siguientes situaciones:

Monitorización de pacientes a distancia (RPM): permite al personal sanitario monitorizar y diagnosticar las condiciones de salud, recolectando, almacenando, recuperando y analizando a distancia la información relacionada con la salud del paciente. Los dispositivos RPM permiten atender a los pacientes sin la necesidad de que estos tengan que dirigirse a hasta el hospital, típicamente se utilizan uno o más sensores para monitorizar los signos vitales de los pacientes como la frecuencia cardiaca y los datos se envían utilizando un Gateway que se conecta a la red de telefonía móvil.

Gestión de enfermos: otra aplicación común es apoyar la atención a distancia de pacientes con enfermedades como diabetes o arritmias cardiacas. En estas aplicaciones tiene importancia la implementación de una alarma para llamar la atención del médico ante cualquier situación crítica que merezca su atención.

Independencia de adultos mayores: su intención es brindarle a los ancianos un estilo de vida independiente, y que puedan mantenerse en sus hogares sin necesidad de asistir al hospital para un chequeo rutinario. Consiste en monitorizar las funciones básicas del paciente (temperatura, pulso, presión sanguínea) para asegurar que se está siguiendo el tratamiento que le ha impuesto el médico para controlar alguna función.

Mejorar la salud y entrenamiento personal: se pueden utilizar para almacenar indicadores de salud y actividad física durante una sesión de ejercicios, como frecuencia cardiaca o respiratoria, consumo de energía, intensidad del ejercicio, entre otras. Luego esta información puede ser cargada en un servidor, para ser utilizada por el médico del paciente como parte de su perfil de salud, o por el entrenador personal para proveer una realimentación del progreso en la actividad física.

Para realizar la adquisición de información de los pacientes se deben utilizar los sensores correctos, por esta razón los pacientes deberán utilizar diferentes sensores para cada función o signo vital que se quiera monitorizar, que por sus limitaciones muchas veces requieren enviar los datos hasta un equipo central a corta distancia (Gateway) que se encargara de recolectar la información y enviarla hasta el servidor de aplicación M2M que la procesa y activa la acción correspondiente.

La figura 22, representa las distintas aplicaciones M2M para el área e-Salud, y además se observan ejemplos de los sensores utilizados para esas aplicaciones.

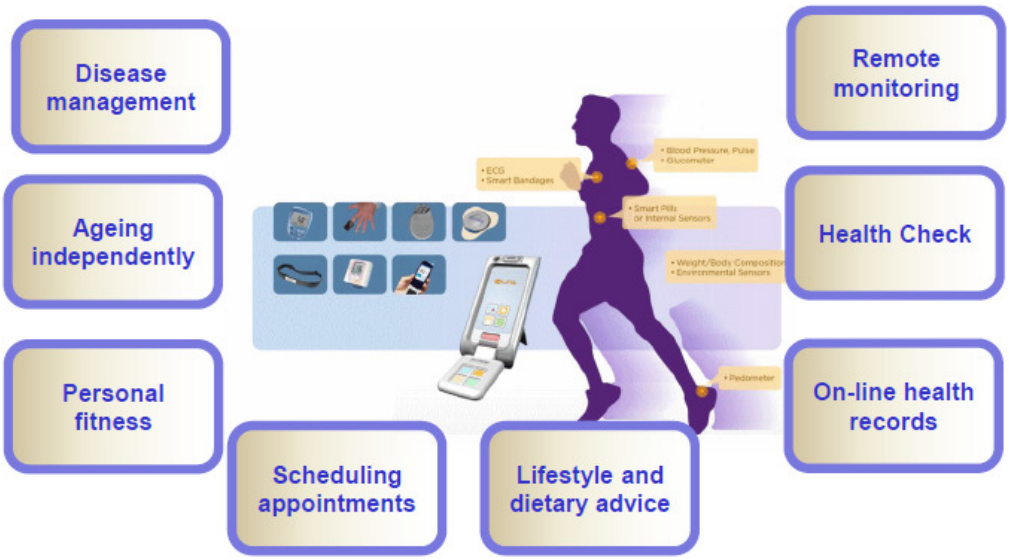


Figura 22. Escenario e-Salud para las comunicaciones M2M.

Ejemplo de caso de uso descrito por el ETSI**: monitorización medición de señales del cuerpo de muy bajo voltaje**.

Descripción general

En este escenario donde es necesario capturar señales de bajo voltaje con el propósito de monitorizar la salud del paciente a distancia. El proceso de adquisición de los datos puede ser perturbado por las actividades de los equipos de transmisión de radio, GSM/GPRS, que podrán estar ubicados dentro del mismo dispositivo M2M.

Cuando el proceso de monitorización deba realizarse de forma constante, la adquisición de los datos podrá verse interrumpida por las mismas actividades típicas del dispositivo M2M para la transmisión celular. Es sumamente importante evitar o reducir cualquier interferencia en las señales del cuerpo para asegurar un sistema confiable, aun cuando no esté catalogado como un servicio para salvar vidas.

Una vía para atender esta necesidad puede ser controlar el transmisor de radio para suspender las actividades de transmisión durante el momento de la medición y restablecerlo luego de finalizar la medición.

Partes interesadas

Paciente: es la persona que utiliza equipos de monitorización a distancia para capturar mediciones, datos o eventos, relacionados con su salud. Estas mediciones pueden realizarse en instalaciones sanitarias, o en la residencia, o lugar de trabajo del paciente.

Dispositivo de monitorización remota (RMD): es un dispositivo con capacidades M2M y formado por un sensor, interfaz de usuario, y una interfaz hacia la red M2M

que utiliza para enviar la información recolectada del paciente, hacia el proveedor de capacidades de servicio M2M o la aplicación M2M. El dispositivo podrá recibir comandos desde la aplicación y utilizar un Gateway para comunicarse con la red M2M. Se aconsejan dispositivos con poco consumo de potencia y protocolos poco complejos.

Proveedor de capacidades de servicio M2M: es una entidad de red que provee servicios de comunicación M2M a la entidad de aplicación M2M, y se comunicara con el RMD para recolectar datos o enviar comandos.

Entidad de aplicación M2M: es un término creado para envolver y tratar como una sola, a todas aquellas aplicaciones de alto nivel que están más allá del alcance del sistema M2M, y también a otras partes interesadas propias de la monitorización de pacientes a distancia (RPM).

Escenario

Inicialización: el RMD está preparado para ser utilizado y comunicarse por una acción del paciente o del médico. Para las aplicaciones criticas, esta etapa podrá requerir autentificación del dispositivo de monitorización por parte del proveedor de capacidades servicios M2M y/o la entidad de aplicación.

Telemetría del paciente: los datos capturados de las mediciones deben ser comunicados cuando vence el periodo establecido, por demanda, o por un evento que lo propicie. En las aplicaciones críticas los RMD deben ser monitorizados constantemente por las capacidades de servicio M2M. Por el tipo de información que se envía se debe asegurar privacidad de los datos.

Configuración remota: se debe permitir la configuración remota de los RMD, individual o en grupo, desde la aplicación central; el dispositivo deberá enviar un acuse de recibo para cada mensaje recibido.

Intercambio de información

Registro: el dispositivo se comunica con el proveedor de capacidades de servicio M2M para su inicialización en el sistema, el proveedor mantiene la información que describe al RMD, el paciente, y la aplicación a la que se enviaran los datos para su procesamiento.

Recuperación de datos: capacidad para localizar y recuperar los datos solicitados, estará sujeta a derechos de acceso y políticas locales.

Entrega de los datos: capacidad para entregar los datos al proveedor de capacidades de servicio M2M de modo seguro, y confirmar la entrega de los datos.

Requisitos potenciales

- Registro e inicialización de dispositivos.
- Configuración y control de dispositivos a distancia.
- Alarma se señalización para indicar falla durante la inicialización.
- Soporte al almacenamiento seguro de datos sensibles.
- Soporte de prioridad para comunicaciones de servicios sensibles a retardos.
- No causar interferencia a los dispositivos médicos electrónicos.
- Indicación de la actividad de radio transmisión.
- Control de la actividad de radio transmisión.

4.1.5 Consumidor interconectado

El reporte técnico (ETSI TR 102 857) [51], relacionado con los casos de uso para consumidor conectado aun se encuentra en una fase de desarrollo precoz, sin embargo ya se han logrado definir algunos casos de uso. Esta área atiende la tendencia a implementar soluciones M2M en los equipos electrónicos del cliente como marcos de fotos digitales, libros electrónicos, o electrodomésticos.

El hecho de poder interconectar cualquiera de nuestros equipos electrónicos que típicamente tenemos en el hogar haciendo uso de comunicaciones M2M, origina diversas aplicaciones M2M orientadas a simplificar tareas cotidianas como, cargar las fotos de un paseo en un marco de fotos digital, descargar revistas o noticias electrónicas actualizadas en nuestros lectores electrónicos, o verificar el nivel de tinta en una impresora conectada en red. La figura 23 representa el escenario típico, para las aplicaciones M2M de consumidor interconectado, considerado por el ETSI.

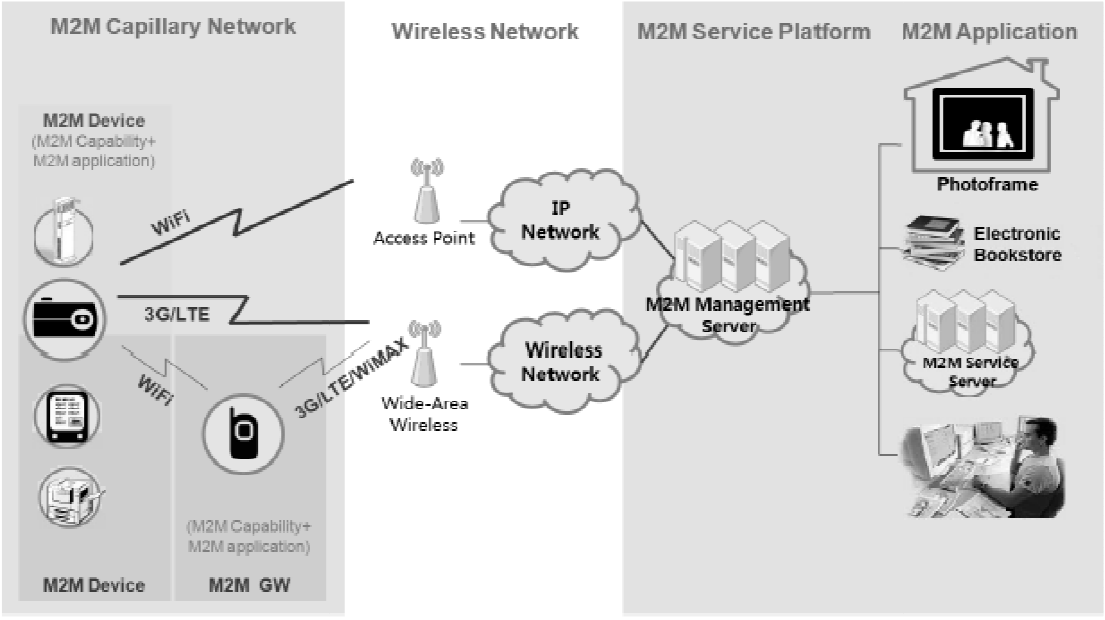


Figura 23. Escenario, Consumidor Interconectado, para las comunicaciones M2M.

Ejemplo de caso de uso descrito por el ETSI**: control remoto de electrodomésticos**.

Descripción general

El propósito de este caso es que un usuario pueda solicitar, durante su ausencia de casa, el encendido, apagado, y/o modificación de los parámetros de funcionamiento de electrodomésticos instalados en su hogar.

Partes interesadas

Electrodomésticos con capacidad M2M: actúan como dispositivos M2M con capacidad de comunicación a la red de acceso inalámbrica, y podrán disponer de una interfaz de usuario y una interfaz hacia la red M2M, podrá ser controlado a distancia por el usuario a través de la red inalámbrica, dependiendo sus capacidades el dispositivo podrá conectarse directamente a la red o a través de un Gateway M2M.

Usuario: es una persona o entidad autorizada para controlar los electrodomésticos en el hogar haciendo uso de sus propios dispositivos, principalmente portátil, con conexión a la red de datos (teléfono móvil, tableta, ordenador, entre otros).

Operador de telecomunicación: provee los servicios de acceso a la red de comunicación a través del Gateway M2M, asegura el transporte de los datos, provee mecanismos de privacidad dependiendo del nivel requerido.

Proveedor de capacidades de servicio M2M: entidad de red que puede ser el mismo operador de la red de comunicación que provee servicios de comunicación M2M entre las entidades de aplicación M2M, para facilitar la comunicación utilizando las capacidades funcionales M2M en ambos extremos de la comunicación.

Entidad de aplicación M2M: es el término creado para involucrar a todas aquellas aplicaciones o elementos que están más allá del alcance M2M, como servidores de páginas web que ayudan al control a distancia de los electrodomésticos enviando y recibiendo los comandos de control, enviando y recibiendo los resultados de cada comando, y también mostrando el resultado de los mismos.

Escenario

Inicialización: los electrodomésticos con capacidades de servicio M2M se conectados a la red inalámbrica y ejecutan su registro en el sistema M2M, o en caso de ser necesario establecen la conexión con el Gateway M2M. En esta etapa se debe capturar y almacenar características de los elementos involucrados.

Solicitud de operación remota: el usuario utiliza su dispositivo portátil u ordenador para enviar la petición de encendido o apagado a distancia de alguno de los electrodomésticos.

Exhibición del resultado: El resultado de la operación se envía desde el electrodoméstico M2M hacia el usuario a través de la red inalámbrica.

Intercambio de información

1. Los electrodomésticos se registra en el sistema M2M.
2. El cliente envía una solicitud de control sobre algún electrodoméstico a través de la red inalámbrica.
3. Se verifica si el cliente está autorizado para realizar la solicitud.
4. Se envían los datos solicitados desde el electrodoméstico hacia el sistema M2M.
5. El proveedor de capacidades M2M lo envía hasta la entidad M2M, quien finalmente la retransmite hasta el dispositivo del usuario.
6. El usuario recibe la confirmación del resultado de su petición.

Requisitos potenciales

- El dispositivo M2M deberá ser capaz de registrar sus capacidades de servicio en el sistema M2M.
- Los dispositivos y Gateway M2M deberán ejecutar control de acceso para verificar los permisos del usuario, dispositivos y Gateway M2M mientras se establecen las conexiones del servicio M2M.
- Dispositivos y Gateway M2M deberán ser capaces de gestionar los accesos simultáneos que se puedan producir desde diferentes entidades hacia un mismo dispositivo o Gateway.

4.1.6 Automatización de la ciudad

Es el área que menos avanzada se encuentra, de hecho el reporte técnico que se estaba desarrollando fue detenido en abril del 2013. Sin embargo, hasta cierto punto las aplicaciones en esta área abarcan situaciones que involucran algunas de las mencionadas anteriormente para optimizar las actividades que se desarrollan en una ciudad. Y también, otros casos de uso como el control del tráfico, la iluminación de las vías, y/o la industria de transporte público, en donde los módulos de comunicación M2M pueden ser introducidos en la infraestructura de la ciudad o vehículos de transporte [52].

El tráfico en las ciudades depende de muchas variables, sin embargo para nadie es un secreto que es el principal problema en grandes ciudades donde a menudo ocurren atascos productos de accidentes, o trabajos de construcción. Esto se puede mejorar con un sistema de gestión del tráfico que integre sensores de flujo de tráfico, pantallas de información, y señales de tráfico cambiantes, que puedan reaccionar ante las variaciones constantes de tráfico y así gestionarlo de modo más eficiente, para reducir el consumo de combustible, contaminación del aire, congestión, y tiempo consumido en el tráfico.

Otra de las ideas es proveerles a los pasajeros del sistema de transporte público información actualizada de la disponibilidad de los vehículos de transporte, para que puedan planificar sus movimientos diarios y seleccionar rutas alternativas en caso de congestión vehicular.

El tercer segmento importante de los casos de uso para la automatización de la ciudad es la regulación del alumbrado público, que obviamente no tienen que iluminar todo el día con la misma intensidad, y una gestión inteligente de ellos puede ayudar a reducir su consumo de energía e indirectamente ayudar a disminuir la contaminación. A continuación describiremos mejor uno de los ejemplos de caso de uso considerado por el ETSI**: sistema de información al pasajero del transporte público**.

Descripción general

Los vehículos de transporte público (autobús, tren o metro), no llegan siempre a tiempo a sus paradas, para optimizar el tiempo disponible de las personas es necesario que los usuarios puedan conocer el tiempo real de llegada de un vehículo a su respectiva parada. Y de esta forma decidir la ruta más conveniente.

Escenario

Las localizaciones reales, de los diferentes vehículos de transporte público, en determinados puntos de control se envían hasta un sistema centralizado, que se encarga de compararla con la ubicación esperada según la planificación. Basado en la diferencia de tiempo el sistema pude calcular el retardo acumulado y determinar el tiempo de llegada estimado para la próxima parada.

La ubicación del vehículo se puede determinar por puntos de control en el camino que deben diferenciar todas las líneas de autobús que cruzan por ese mismo lugar, no es suficiente que el sensor pueda determinar simplemente que ha pasado un autobús. Otro método podrá ser el uso dispositivos de seguimiento GPS/GPRS que envíen la posición del vehículo a intervalos regulares, pero esto estará restringido solo a vehículos terrestres, para evitar los problemas de cobertura en el subterráneo. Aunque también pudiera implementarse una combinación de ambos métodos.

Intercambio de información

Cálculo basado en puntos de control:

1. Se captura el número de línea del autobús en el punto de control y se envía al sistema central.
2. El sistema central calcula la diferencia de tiempo que hay entre la hora actual y la estimada según la planificación.
3. Se envía el retardo calculado a las siguientes paradas, para agregarlo al tiempo de llegada que se muestra en cada una en ese momento.

Cálculo basado en elementos GPS/GPRS:

1. El vehículo se equipa con un dispositivo de seguimiento GPS/GPRS, que envía regularmente la posición actual, con la identificación de numero de línea.
2. El sistema recibe la información y establece el patrón tiempo/ubicación, que utiliza para calcular el retardo.
3. Envía el tiempo de espera actualizado a las pantallas de las siguientes paradas.

4.2 Casos de Uso Propuestos.

A continuación se describen detalladamente algunos casos de uso que hemos considerado relevantes, en los cuales la incorporación de la tecnología M2M aportara un alto valor para alcanzar mejoras en los servicios prestados; siempre en la búsqueda de la eficiencia.

4.2.1 Monitorización Remota de Urgencias

Descripción general

Le hemos denominado de esta forma, ya que se busca realizar la monitorización de los signos vitales de pacientes víctimas de accidentes de tránsito que son atendidos inicialmente por las unidades móviles de los servicios de urgencias y que requieren posteriormente ser trasladados hasta el hospital.

Con este tipo de solución, los datos capturados por los sensores de los instrumentos de medición que se encuentran dentro de las ambulancias (como el monitor de pulso, temperatura, peso, presión sanguínea, entre otros), se enviaran hacia los sistemas de apoyo (Ordenadores) que se encuentran en la sala de urgencias del hospital, sin necesidad de que exista un previo registro electrónico (EHR) de información relacionada con la salud del paciente.

De tal forma que el personal sanitario que se encuentra en la sala de urgencias pueda tener conocimiento previo del estado de salud en el que ingresara un paciente, y con esto podrá preparar rápidamente los recursos que considere necesario (como quirófano, médicos especialistas, salas de parto, entre otros), para la atención oportuna del mismo.

A estas aplicaciones se debe incorporar la función de alarma, para que se pueda activar una alarma que llame la atención del personal en el hospital con la finalidad de reaccionar a tiempo ante las situaciones críticas. Debido a la gran cantidad de nodos M2M que pudieran existir, y para disminuir la carga de datos en la red se pudiera adoptar una transmisión periódica, no muy frecuente, de los datos capturados por los sensores, lo que permitirá tener información actualizada, pero no en tiempo real.

Partes interesadas

Dentro de la propuesta las partes involucradas serian los pacientes (a los cuales se les realizara mediciones), los equipos de medición remota (deberán ser dispositivos M2M conectados con sensores, una interfaz de usuario, y una interfaz hacia la red M2M). Estos equipos recolectaran la información y la enviaran, por medio del Gateway de la red M2M, a la capa de capacidad de servicio M2M que le corresponda.

En lo que respecta a los dispositivos se pueden considerar tres formas diferentes para el desarrollo de los mismos, en la primera los sensores dispondrán tanto la aplicación M2M (DA), como la capacidad del servicio M2M (DSCL), y será entonces el elemento central del instrumento de medición (monitor) que funcione como Gateway, y en donde se implemente la aplicación y la capa de capacidad de servicio (GA y GSCL).

La segunda opción se lograría manteniendo las mismas características anteriores para el monitor, pero solo implementando la aplicación (DA) en los sensores, es decir que sean dispositivos tipo D', y que se comunicara con la capa GSCL que se encuentra en el monitor para gestionar los servicios M2M.

La solución que parece más factible es instalar una unidad central que podrá ser una CPU, o un teléfono móvil para que funcione como Gateway M2M, en la cual se implemente la aplicación GA y la capacidad del servicio GSCL; y que el dispositivo M2M sea el instrumento de medición en sí, incluyendo sus sensores, igualmente el dispositivo podrá ser tipo D o D', dependiendo la complejidad y requerimientos que añada cada caso. Como es sabido estos dispositivos deberán cumplir condiciones estrictas como bajo consumo de energía, alta seguridad, protocolos no muy complejos y que sean fáciles de configurar.

El personal sanitario será el encargado de realizar y evaluar las mediciones remotas para determinar las intervenciones clínicas apropiadas en cada caso. Finalmente, Igual que en la mayoría de los casos también estarán involucrados el proveedor de servicios de red, que podrá ser el mismo proveedor de servicios M2M, así como otros proveedores de aplicaciones o servicios de valor agregado comúnmente denominados entidades de aplicación M2M.

Escenario

Condiciones previas: el equipo de monitorización a distancia está instalado y configurado dentro de la ambulancia, y posee una interfaz con el modulo o Gateway M2M para enviar los valores capturados hasta el proveedor de servicio M2M luego de la acción del auxiliar sanitario. Además, el modulo M2M está conectado a la red de telecomunicación móvil que le brinda un servicio de conexión de datos, y el operador

del centro de atención de urgencias tiene correctamente instalado un servidor de aplicación M2M para interactuar con el RMD.

La inicialización del servicio puede involucrar acciones como registro del dispositivo, establecimiento de canales de comunicación hacia las entidades de aplicación M2M, establecimiento de capacidades de comunicación M2M, y provisión de un canal de comunicación seguro.

Condiciones posteriores: por ser mediciones críticas el estado del dispositivo RMD deberá ser verificado frecuentemente por la red de capacidades de servicio M2M o la entidad de aplicaciones M2M. Los paquetes se envían hacia la aplicación M2M por un medio seguro para proveer privacidad de los datos, y el personal sanitario en la sala de urgencias recibe los datos con los valores del paciente monitorizado.

Activador: el operador enciende el RMD e inicia el envío de la información una vez se colocan todos los sensores en el paciente, y luego cada vez que se cumpla el periodo de reporte establecido previamente se envían las mediciones actuales.

Intercambio de información

1. El RMD se comunica con la capacidad de servicio M2M correspondiente para el proceso de inicialización en el sistema M2M.
2. Se completa el registro del dispositivo y se almacenan los datos que podrán ser utilizados para verificar frecuentemente el estado del dispositivo RMD.
3. Se establece un canal de comunicación seguro utilizando la jerarquía de claves.
4. El dispositivo realiza la medición de los valores y la envía a través la red de acceso móvil hacia el servidor de aplicación.
5. El servidor de aplicación procesa los datos, y los representa gráficamente para que sean analizados por el personal médico.
6. El servidor de aplicación verifica constantemente el estado del dispositivo RMD.

La figura 24 muestra la arquitectura del caso de uso propuesto, en el sistema se hace uso de la infraestructura de telecomunicación existente, y se basa en, el **dispositivo de monitorización remota RMD M2M** utilizado para medir los signos vitales del paciente mediante sensores que conforman una red BAN, que podrá ser cableada o inalámbrica. El **Gateway M2M** se encargara de recolectar la información enviada por el RMD para reenviarla hacia el servidor M2M a través de la infraestructura de comunicaciones móvil, red 3GPP, finalmente el **servidor M2M** recibirá los datos y los procesara para que las aplicaciones M2M puedan cumplir su función..

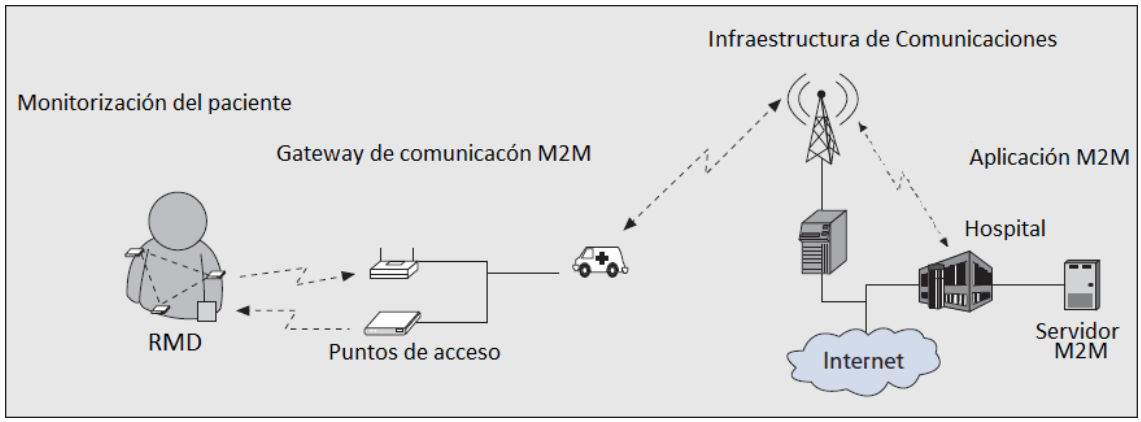


Figura 24. Caso de Uso propuesto para e-Salud.

4.2.2 Actualización de firmware.

Descripción general

Se busca una actualización automática del firmware de cualquiera de los artefactos del hogar con capacidad de servicios M2M (Televisor, lavadora, nevera, consolas de video juego, entre otros).

La actualización será siempre originada por una entidad encargada de verificar las versiones de firmware que ejecutan los artefactos instalados en la vivienda. Para este caso lo más conveniente es disponer de un Gateway M2M que se encargue de recolectar todas las comunicaciones M2M desde los dispositivos para enviarlas a través de un enlace con la red de comunicación.

Partes interesadas

Usuarios: son las personas que pueden utilizar los artefactos con capacidad M2M para obtener un beneficio específico de cada uno.

Artefactos con capacidad M2M: son todos aquellos electrodomésticos instalados en la vivienda del usuario y que poseen capacidad para comunicarse con la red M2M utilizando la red de comunicaciones fija o inalámbrica.

Entidad de actualización: es la organización responsable de generar las actualizaciones necesarias para corregir fallos y mantener el funcionamiento correcto y estable de los dispositivos.

Proveedor de red de acceso: es el encargado de proveer la red de comunicación para el transporte de los datos entre los artefactos y las entidades de actualización.

Proveedor de capacidades de servicio M2M: puede ser el mismo operador de la red de comunicación que provee servicios de comunicación M2M entre las entidades de actualización y los electrodomésticos M2M.

Escenario

Condiciones previas: el modulo M2M se encuentra instalado y configurado dentro del electrodoméstico, y tiene una interfaz hacia la red de comunicaciones inalámbrica, a través de la cual realiza el registro en el sistema M2M.

Condiciones posteriores: la entidad de actualización luego de confirmar la necesidad de actualización envía los datos hacia el electrodoméstico y este último ejecuta la actualización del firmware.

Activador: la entidad de actualización tiene una nueva versión del firmware para el artefacto, y realiza una consulta al dispositivo para verificar la versión que está utilizando, si es una versión diferente, la entidad inicia el proceso de actualización.

Intercambio de información

1. Los artefactos eléctricos establecen una conexión con el Gateway M2M de la vivienda.
2. La entidad de actualización envía la consulta a los artefactos eléctricos para conocer la versión que están ejecutando.
3. El Gateway recibe la petición y valida los permisos de la entidad para realizar la consulta.
4. El Gateway envía la petición hasta el artefacto.
5. El artefacto responde la petición mediante el Gateway.
6. La entidad recibe la respuesta y compara las versiones.
7. La entidad envía los datos para la actualización del firmware.
8. El artefacto descarga desde el Gateway M2M los datos y realiza la actualización.
9. El artefacto envía la confirmación de ejecución de la operación, y los datos de la versión de firmware que está ejecutando, hacia la entidad de actualización.

La figura 25 representa el escenario para el caso de uso propuesto.

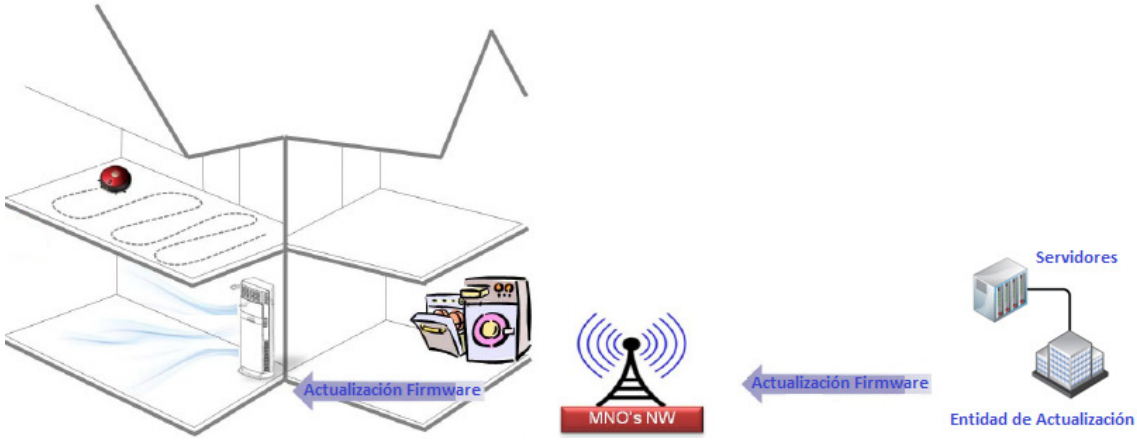


Figura 25. Caso de Uso propuesto para consumidor conectado.

4.2.3 Sistema de vigilancia público

Descripción general

El propósito de este caso es que se puedan recibir datos desde cámaras de video, colocadas en lugares remotos y desasistidos, que permitan detectar intrusos y comunicarlo inmediatamente a los responsables de seguridad de esas instalaciones.

Estas cámaras son utilizadas en lugares críticos donde usualmente no existe tránsito de personas o vehículos de ningún tipo, de modo que lo contrario se considera como actividad sospechosa (periferia de centros de reclusión policial, frontera con otro país, pozos petrolíferos, bases de puentes), y toda aquella infraestructura considera importante dentro de la ciudad que pudiera ser blanco de algún intento por destruirla o de ingresar indebidamente.

Partes interesadas

Videocámara de vigilancia con capacidades M2M: actúa como un dispositivo M2M con capacidad de comunicarse con la red inalámbrica, y la red M2M. Este dispositivo almacena eventos en tiempo real, activados por movimiento, y los envía a través de una interfaz inalámbrica a un operador de sistema de vigilancia, esta comunicación podrá realizarse en algunos casos a través de un Gateway M2M.

Operador de sistema de vigilancia o cliente: es una organización capaz de recibir la los datos de imágenes capturadas en lugares donde no debe ocurrir transito alguno de personas. Seguramente será alguna división de seguridad perteneciente al ayuntamiento o sede de gobierno nacional encargada de controlar la seguridad en la infraestructura vigilada.

Operador de red de acceso: es el encardo de proveer los servicios de comunicación para el transporte de los datos desde las cámaras de vigilancia hasta el servidor de aplicación M2M encargado de procesar la información.

Proveedor de capacidades de servicio M2M: puede ser el mismo operador de la red de comunicación que provee servicios de comunicación M2M entre las entidades de aplicación M2M. Además se comunica con los dispositivos del cliente para adaptar el contenido a sus requisitos y reproducir la secuencia de video.

Entidad de aplicación M2M: es el término creado para involucrar a todas aquellas aplicaciones o elementos que están más allá del alcance M2M, como páginas web para la reproducción del video que reciben y exhiben las secuencias de video grabadas.

Escenario

Condiciones previas: la cámara de video con capacidad M2M está asociada a la red inalámbrica y una vez encendida ejecuta el registro en el sistema M2M, también puede

ocurrir cuando reciba una solicitud de video. En esta etapa se debe capturar y almacenar características de los elementos involucrados para poder determinar si es necesario adaptar los contenidos antes de su reproducción.

Condiciones posteriores: el proveedor de capacidades de servicio recibe los datos y adapta el contenido a las especificaciones apropiadas, y lo envía hasta el dispositivo que se encarga de exhibirlo en el formato correcto.

Activador: la videocámara M2M podrá recibir una petición desde el cliente para enviar secuencias de video grabadas y almacenadas, o también enviar automáticamente los datos de la grabación en tiempo real, cuando se detecte movimiento.

Intercambio de información

1. La videocámara se registra en el sistema M2M.
2. El cliente envía una petición de secuencia de video mediante la red inalámbrica, o la cámara detecta algún movimiento e inicia la grabación.
3. Se verifica si el cliente está autorizado para solicitar/recibir los datos.
4. Se envían los datos desde la videocámara hacia el sistema M2M.
5. El proveedor de capacidades M2M adapta el contenido.
6. Finalmente lo envía a la aplicación del cliente.

4.2.4 Seguridad y prevención de accidentes automovilísticos.

Descripción general

Mientras se conduce un vehículo con capacidad M2M en carretera, en caso de ocurrir una emergencia, la información de los sensores de detección de emergencia (sistema de frenos, acelerador, sensor de impacto, sensor de funcionamiento del motor) se envía a través de la red de comunicaciones móviles hacia la infraestructura de comunicación de información de la carretera (comunicación V2I), con capacidades M2M que se encuentren a su alcance.

Luego esta infraestructura será la encargada de difundir constantemente la notificación de emergencia hacia los demás vehículos con capacidad M2M, esta información podrá incluir, además de la ubicación del accidente, indicaciones para limitar la velocidad del vehículo mientras circule por esa área.

Esto podría ser muy útil para aquellos casos donde ocurren accidentes en curvas pronunciadas, pendientes y/o en condiciones ambientales desfavorables donde la línea de vista del conductor es bastante limitada y por lo tanto, influye en su tiempo de respuesta para ejecutar alguna maniobra.

Para evitar accidentes o futuros accidentes producto de uno que haya ocurrido anteriormente (choques en cadena), las emergencias deben detectarse y notificarse rápidamente para ayudar a los conductores a responder oportunamente. Se debe garantizar calidad de servicio y retardo bajo para estos mensajes que deben transmitirse desde el vehículo que notifica el evento hacia los demás vehículos que lo reciben, en cuestión de milisegundos. Debido a los atributos de estas comunicaciones (mensajes pequeños, y se transmite únicamente durante una emergencia), se requiere poco ancho de banda, y conexiones de datos momentáneas.

Partes interesadas

Conductores: son los dueños de los vehículos con capacidades M2M que pueden interactuar con los elementos internos del vehículo (sensores, dispositivo de navegación) y además se comunican con los servidores M2M a través de una red de comunicaciones móvil.

Operador de la infraestructura de información: es la organización propietaria de la infraestructura de información de carretera que su vez mantiene los servidores de aplicación M2M que reciben, procesan, y transmiten información relacionada con el estado del tráfico, desde y hacia los vehículos.

Operador de red de telecomunicación: es quien opera la red de telecomunicaciones móvil utilizada por el vehículo en la zona donde se está desplazando. Este a su vez podrá ser el operador del servicio de información de carretera.

Escenario

Condiciones previas: el modulo M2M se encuentra instalado y configurado dentro del vehículo para que tenga una interfaz con los sensores que miden la velocidad, el sistema de frenado, el sistema de tracción, y el sensor de impactos externo. Adicionalmente debe tener una interfaz con dispositivos que detecten la localización del vehículo bien sea mediante GPS o GPRS, y disponer de un servicio de datos de una red de telecomunicación móvil, que le permita establecer un enlace para enviar información al servidor M2M en el momento que ocurra una emergencia, o recibirla cuando el sistema de información de tráfico tenga algún mensaje para el vehículo.

Condiciones posteriores: en caso de una emergencia detectada por el vehículo, el servidor de aplicación M2M recibirá la notificación y la procesara para enviarla a los demás vehículos que se encuentren la carretera. En caso de una emergencia detectada por otro vehículo el servidor notificara la situación y el modulo M2M en el vehículo al recibirla la procesa y realiza las acciones correspondientes (disminuir la velocidad).

Activador: básicamente la fuente que estimula este proceso será un evento (emergencia), ya que cuando el conductor realice un frenazo, disminuya la velocidad

súbitamente, haya perdida de tracción, o impacte con algún objeto fijo o móvil, el modulo M2M enviara inmediatamente la notificación al sistema de información.

También puede considerarse el hecho de que el sistema de información pueda notificar otras situaciones como trabajos de reparación en la vía, o condiciones ambientales extremas.

Intercambio de información

Flujo básico para emergencia detectada por el vehículo:

1. El modulo M2M establece un enlace de comunicación y contacta con el servidor de información del trafico para iniciar el registro.
2. El modulo M2M envía los datos relacionados con la emergencia, conjuntamente con la información de localización, hacia el servidor.
3. El servidor recibe la información y la procesa.
4. El servidor envía periódicamente el reporte con la información del evento, y una orden para limitar la velocidad en un determinado tramo de la carretera.
5. El vehículo recibe el mensaje, y ejecutara el procedimiento necesario para evitar que su velocidad supere lo impuesto por el sistema de información en el área correspondiente a la emergencia.

Flujo para emergencia o advertencia notificada por otro sistema:

1. El servidor de información M2M recibe la notificación sobre algún evento.
2. El servidor envía periódicamente el reporte con información del evento, y las acciones que se requieren por parte de los vehículos.
3. El vehículo recibe la notificación, y la procesa.
4. El servidor recibe la notificación de cese del evento y lo notifica a los vehículos.

5 Conclusiones y trabajos futuros

- Las tecnologías de comunicación M2M pueden ser aplicadas para el beneficio de un amplio rango de aplicaciones y servicios en las ciudades inteligentes. Principalmente se deben reducir los costos de implementación mediante el uso de estándares abiertos que aseguren interoperabilidad entre soluciones de distintos proveedores trabajando conjuntamente con diferentes socios. Afortunadamente tanto las comunidades de investigación como los organismos de estandarización han reconocido este potencial, y se encuentran en el proceso de atender los retos para futuras redes de comunicaciones M2M grandes.

- La estandarización es un habilitador clave para el rápido y sostenible desarrollo del mercado de las comunicaciones M2M. Para alcanzar este crecimiento, será necesario reemplazar los despliegues verticales M2M realizados hasta la fecha, por unos horizontales con una arquitectura M2M común compartida entre todos los elementos del sistema, como la planteada por el ETSI. El propósito principal de la estandarización (basada en diferentes casos de uso), es el de extraer la mayor cantidad de características principales de las comunicaciones M2M, para simplificar el desarrollo de nuevos servicios.

- En este trabajo se han descrito los esfuerzos realizados por el 3GPP (versión 10 y 11) para realizar mejoras en la arquitectura MTC, que están conduciendo a resolver los problemas importantes relacionados con el control de suscripciones y congestión, que ocurren cuando existen muchos mensajes de señalización a la vez en la red, además de lo pertinente con direccionamiento, identificación y activación de dispositivos. La naturaleza diversa de las comunicaciones M2M presentan un reto importante para ofrecer un servicio optimizado a todas las aplicaciones. Sin embargo dentro del 3GPP se ha trabajado cuidadosamente para seleccionar y priorizar los requisitos claves del servicio que provean solución a la mayor cantidad de aplicaciones.

- Las mejoras realizadas por el IEEE, se han enfocado principalmente en evolucionar la interfaz aire de la tecnología WiMAX, con pequeños cambios en las especificaciones del canal físico, y protocolos MAC, que han logrado atender los requisitos principales para soportar comunicaciones M2M como dispositivos con bajo consumo de potencia, estaciones base que soportan muchos dispositivos, multidifusión, y gestión de grupos de dispositivos.

- El interés mostrado por los SDO para simplificar el desarrollo de aplicaciones M2M, reducir el solapamiento que hay entre algunos estándares que se están desarrollando, e incrementar la disponibilidad de nuevas soluciones M2M capaces de operar en diferentes escenarios, ha generado la creación del proyecto oneM2M para producir especificaciones de la capa de servicios M2M que sean independientes del medio de acceso y aplicables a nivel mundial.

- Para el momento de escribir este trabajo algunas especificaciones ETSI y 3GPP continúan evolucionando, por lo que algunos detalles podrían haber sufrido algunos cambios.

- En los organismos de estandarización no se toman en cuenta las diferencias que pueden existir entre la legislación local, regional o nacional. Por eso, para evitar inconvenientes en el uso de las aplicaciones M2M, es necesario que se involucren organismos reguladores certificados en todos los niveles. Una de las tareas de estas autoridades es, asegurar el consentimiento para que se utilicen numero nacionales (MSISDN) en las mediciones inteligentes.

- El numero de maquinas interconectadas cambiara notablemente en el futuro cercano. Por eso es de gran importancia comprender las interacciones en las comunicaciones M2M. Durante nuestro trabajo nos enfocamos en analizar algunos principios de comunicación y arquitecturas básicas propuestas por las organizaciones de estandarización, y reflejamos los esfuerzos realizados por los grupos de trabajo de esas organizaciones y sus recomendaciones con relación a problemas pendientes de solucionar en las comunicaciones M2M. Además propusimos 4 casos de uso que pueden ser útiles como bases para implementar futuras aplicaciones.

- Algunos años atrás, las comunicaciones M2M atrajeron el interés de muchas industrias, y seguramente lo seguirán haciendo durante los próximos años, ya que desde la perspectiva de sus funciones y usos potenciales M2M estará favoreciendo el surgimiento del internet de las cosas (IoT), como una de sus tecnologías principales, en el futuro cercano. Sin embargo esta tecnología representa tanto oportunidades como retos en un mercado que, a pesar de las motivaciones económicas y de negocio para invertir en el futuro, se encuentra fragmentado; algo que indudablemente es un obstáculo que pone en riesgo el crecimiento esperado de M2M.

- Mientras más servicios se despliegan, el tráfico en la red continuara su ascenso proporcional al número de nuevos dispositivos M2M que accedan a la red. Conjuntamente con los esfuerzos de estandarización para disminuir los problemas de congestión, y su efecto en la calidad de la experiencia (QoE) del usuario, se debe realizar una categorización de la calidad del servicio (QoS) requerida por el tráfico de datos M2M que transita por la red, para ayudar a colocar la QoE en niveles aceptables por los usuarios, que permitan el despliegue en el mercado de más servicios M2M.

5.1 Trabajos futuros

Para dar continuidad a los trabajos que han realizado hasta ahora los organismos de estandarización consideramos oportuno realizar, entre otras, las siguientes actividades:

- Se debe completar el lanzamiento de la versión 2 del ETSI enfocada en la interoperabilidad con el 3GPP, la arquitectura para cobros, y algunas mejoras adicionales en la arquitectura funcional. Así como también los casos de uso (e-salud, consumidor interconectado) y demás especificaciones que se encuentran en fase de borrador para eliminar las lagunas que aun existen.

- Acelerar el crecimiento y progreso de la alianza oneM2M de cara a aumentar la publicación de documentos de estándares que sirvan de base para la globalización de la capa de servicios M2M. También se debe estimular la coordinación, entre los grupos de trabajo internos, para acordar terminología y definiciones unificadas en la elaboración de los casos de usos M2M.

- Completar dentro del 3GPP versión 12, el desarrollo de nuevas mejoras y optimizaciones con el propósito de resolver 5 de los problemas o requisitos claves de la arquitectura MTC, como transmisión de pocos datos, consumo bajo de energía, optimización basada en grupo, monitorización de dispositivos y continuar realizando mejoras a la activación de dispositivos M2M. Uno de los retos importantes del 3GPP será soportar comunicaciones M2M en LTE, esto permitirá la migración desde redes antiguas como GPRS hacia LTE que ofrece mejor eficiencia en el uso del espectro.

- Dentro del IEEE aun se necesitan mayores esfuerzos en el futuro para cubrir las necesidades de la industria, desarrollando nuevos canales físicos y mejorando control de acceso al medio (MAC). Por ese motivo, es conveniente la finalización del estándar para WLAN “802.11ah” que opera en frecuencias de radio de 1GHz, ofreciendo una alternativa a las mejoras ya publicadas para WiMAX.

Bibliografía

[1] BOSWARTHICK, D., HERSENT, O. y ELLOUMI, O. (2012): *"Introduction to M2M"* in *M2M Communications a System Approach,* (1-20) U.K.: John Wiley & Sons, Ltd.

[2] ETSI Machine-to-Machine Communications. Disponible en: http://www.etsi.org/website/technologies/m2m.aspx Ultima visita: Marzo, 2013.

[3] ETSI TS 102 689: "M2M service requirements", v1.1.5, 2012.

[4] ETSI TS 102 690: "Functional architecture", v1.1.1, 2011.

[5] ETSI TS 102 921: "mIa, dIa and mId interfaces", v1.1.1, 2012.

[6] 3GPP TS 22.368 v11.6.0, "Service requirements for machine-type communications," Sep.2012.

[7] 3GPP TR 23.888 v11.0.0, "System improvements for machine-type communications,"Sep.2012.

[8] IEEE 80216p-10_0005, "Machine-to-machine (M2M) communications technical report," Nov.2010.

[9] TR-50 standards http://www.tiaonline.org/standards/committees/-committee.cfm?comm=tr-50 Ultima visita: Marzo, 2013.

[10] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[11] ETSI TS 133 220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)", v7.6.0, 2006.

[12] ETSI TS 124 109: "Universal Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details (3GPP TS 24.109)", v8.0.0, 2009.

[13] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[14] IETF RFC 5191: "Protocol for Carrying Authentication for Network Access (PANA)".

[15] IETF RFC 4186: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)".

[16] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)"

[17] IETF RFC 2716: "PPP EAP TLS Authentication Protocol".

[18] IETF RFC Draft: "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange".

[19] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[20] IETF RFC 4279: "Pre-Shared Key Cipher suites for Transport Layer Security (TLS)".

[21] IETF RFC 5433: "Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method".

[22] 3GPP TS 22.368 v10.5.0, “Service requirements for machine-type communications”, Junio 2011.

[23] 3GPP TS 22.368 v12.2.0, “Service requirements for machine-type communications”, Marzo 2013.

[24] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications", Enero 2013.

[25] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)", Abril 2013.

[26] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications", Enero 2013.

[27] 3GPP TS 23.401, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”, Junio 2010.

[28] 3GPP TS 23.060, “General Packet Radio Service (GPRS); Service description; Stage 2”, Abril 2013.

[29] 3GPP TS 29.368: "Tsp interface protocol between the MTC Interworking Function (MTC-IWF) and Service Capability Server (SCS)", Octubre 2012.

[30] 3GPP TS 23.221, “Architectural requirements”, Diciembre 2012.

[31] 3GPP TS 23.204: "Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2", Enero 2013.

[32] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2", Abril 2013.

[33] IEEE 802.16p-2012, “IEEE Standard for Air Interface for Broadband Wireless Access Systems - Amendment 1: Enhancements to Support Machine-to-Machine Applications”, Octubre 2012.

[34] IEEE 802.16.1b-2012, “IEEE Standard for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems - Amendment: Enhancements to Support Machine-to-Machine Applications” Oct.2012.

[35] IEEE 80216p-10_0005, “Machine-to-machine (M2M) communications technical report” Nov.2010.

[36] NIST Special Publication 800-38A—Recommendation for Block Cipher Modes of Operation—Methods and Techniques.

[37] NIST Special Publication 800-38B—Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

[38] Spadacini, M.; Savazzi, S.; Nicoli, M.; Nicoli, S., "Wireless networks for smart surveillance: Technologies, protocol design and experiments," Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE, vol., no., pp.214, 219, 1-1 April 2012.

[39] Hu, Liang & Chi, Ling & Li, Hong-tu & Yuan, Wei & Sun, Yuyu et al., “The classic security application in M2M: the authentication scheme of mobile payment.(machine to machine)(Report)”, KSII Transactions on Internet and Information Systems, vol. 6, no. 1, pp. 131, 147, January 2012.

[40] Zhong Fan; Siok Tan, "M2M communications for e-health: Standards, enabling technologies, and research challenges," Medical Information and Communication Technology (ISMICT), 2012 6th International Symposium on, vol., no., pp.1, 4, 25-29 March 2012

[41] Wahle, S.; Magedanz, T.; Schulze, F., "The OpenMTC framework — M2M solutions for smart cities and the internet of things," World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a, vol., no., pp.1, 3, 25-28 June 2012

[42] Schneps-Schneppe, M.; Namiot, D.; Maximenko, A.; Malov, D., "Wired Smart Home: Energy metering, security, and emergency issues," Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on, vol., no., pp.405, 410, 3-5 Oct. 2012.

[43] ETSI TR 102 691: "Smart Metering Use Cases", v1.1.1, 2010.

[44] Smart meters co-ordination group, final report (Version 0.7, 2009-12-10): "Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441".

[45] ESMIG Document ESMCR003-002-1.0 (October 2009): "Smart Metering Functionality Use Cases", Engage Consulting Limited (assigned by ESMIG).

[46] "EU Commission Task Force for Smart Grids – Expert Group 1: Functionalities of smart grids and smart meters - Final Deliverable" (September 2010)

[47] ETSI TR 102 935: "Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform", v2.1.1, 2012.

[48] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Lwaski and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," IEEE Communications Magazine, vol.49, no.4, pp.60-65, Apr.2011.

[49] ETSI TR 102 898: "Use cases of Automotive Applications in M2M capable networks", v1.1.1, 2013.

[50] ETSI TR 102 732: "Use cases of M2M applications for eHealth", v0.4.1, 2011.

[51] ETSI TR 102 857: "Use cases of M2M applications for Connected Consumer", v0.3.0, 2010.

[52] ETSI TR 102 897: "Use cases of M2M applications for City Automation", v0.1.1, 2010.