ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

TEMA: ESTUDIO DE LOS MECANISMOS DE SEGURIDAD Y LOS CRITERIOS DE CALIDAD (QoS) EN LAS REDES MÓVILES DE TERCERA GENERACIÓN UMTS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ESPECIALISTA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTOR: BYRON RAÚL AVILÉS RODRÍGUEZ

DIRECTOR: DR. LUIS CORRALES PAUCAR

QUITO, MARZO 2003

DECLARACIÓN

Yo Byron Raúl Avilés Rodríguez declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo según lo establecido por la Ley, Reglamento de Propiedad Intelectual y por la normatividad institucional vigente.

Byron Raúl Avilés Rodríguez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Sr. Byron Raúl Avilés Rodríguez bajo mi supervisión.

Dr. Luis Corrales Paucar

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a mis padres por el esfuerzo y confianza que han puesto en mi persona. También quiero agradecer al Dr. Luis Corrales Paucar por su correcto asesoramiento y ayuda para la consecución del presente proyecto de titulación.

CONTENIDO

CAPÍTULO II

DESCRIPCIÓN DE LOS MECANISMOS DE SEGURIDAD EN UMTS

CAPÍTULO III

CALIDAD DE SERVICIO (QoS) EN REDES UMTS

CAPÍTULO IV
SERVICIOS Y APLICACIONES EN LAS REDES UMTS DE ACUERDO A LAS DIFERENTES CLASES DE QoS

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

RESUMEN

El acelerado crecimiento que han venido sufriendo las comunicaciones móviles de voz y el aumento de la demanda de servicios multimedia obligan a las operadoras de redes de segunda generación al uso de un nuevo sistemas de comunicaciones denominado UMTS (*Universal Mobile Telecommunications System*, Sistema Universal de Telecomunicaciones Móviles), el cual posibilita el acceso a Internet y en general a servicios multimedia móviles.

Para conseguir que tales servicios sean una realidad en las redes móviles de tercera generación UMTS es fundamental asegurar la calidad de servicio extremo a extremo a través de la implementación de diferentes mecanismos tanto en la red central de UMTS como en la red de acceso de radio.

En los sistemas de segunda generación actualmente utilizados, una de las principales debilidades ha sido la seguridad, lo que ha propiciado el incremento del fraude con la consiguiente insatisfacción del usuario y pérdidas económicas a los operadores de la red. Es por ello que los sistemas de comunicaciones UMTS han desarrollado un conjunto de mecanismos de seguridad que tratan de ser una solución a los problemas de seguridad existentes en 2G[1].

Son estas las razones que impulsaron el desarrollo del presente proyecto de titulación, en el cual se han planteado los siguientes objetivos:

- El estudio general de los sistemas de telecomunicaciones móviles.
- El estudio y conocimiento de los mecanismos de seguridad en las redes móviles UMTS.
- El estudio y conocimiento de lo que implica calidad de servicio en las redes móviles UMTS.
- Establecimiento de las diferentes aplicaciones y servicios que pueden ser suministrados por la red UMTS.

[1] Se denomina 2G a los sistemas de comunicaciones móviles de segunda generación, cuya característica principal es de ser una tecnología digital ofreciendo algunos servicios de transmisión de datos, en contraste a los de sistemas de primera generación que se basan en tecnología analógica y son estrictamente para voz.

A fin de conseguir el cumplimiento de tales objetivos el presente proyecto se ha organizado en cinco capítulos:

- En el capítulo uno se desarrolla una introducción a los sistemas de comunicaciones de primera y segunda generación, siguiendo con los factores del porqué de la aparición de los sistemas de tercera generación y sus requisitos. Finalmente se describe la arquitectura del sistema UMTS.
- En el capítulo dos se realiza un estudio de los diferentes servicios de seguridad que deben estar presentes en UMTS y los diferentes dominios que conforman la arquitectura de seguridad en UMTS. Además se describe diferentes mecanismos para conseguir las diferentes propiedades de seguridad. Finalmente se realiza un pequeño análisis de la seguridad en UMTS en comparación con GSM (*Global System for Mobile Communications*, Sistema Global para Comunicaciones Móviles).
- En el capítulo tres se analiza la arquitectura de calidad de servicio en las redes UMTS, en donde se describe el concepto de servicio portador. Posteriormente se estudia las funciones de gestión, las diferentes clases y parámetros de calidad de servicio existentes en UMTS. En su parte final se efectúa un análisis de las distintas tecnologías y mecanismos usados en la red central y en la red de acceso terrestre de UMTS para la consecución de calidad de servicio.
- El capítulo cuarto versa acerca de las más importantes aplicaciones y servicios existentes en un entorno de tercera generación para comprender su importancia con respecto a otros sistemas. Además se realiza un modelo de desarrollo de servicios en donde se involucran consideraciones técnicas de calidad de servicio y seguridad, con el objetivo de garantizar el correcto funcionamiento de un determinado servicio.
- Finalmente, en el capítulo quinto, se establecen conclusiones y recomendaciones, las cuales serán dadas basándose en todo el estudio realizado.

Se incluye también un conjunto de anexos como complemento del estudio.

PRESENTACIÓN

El presente proyecto de titulación es una contribución teórica acerca de los mecanismos de seguridad y calidad de servicio en las redes móviles de tercera generación, los cuales son conceptos de gran importancia para la entrega de servicios en un entorno inalámbrico.

Del estudio de la seguridad en los sistemas UMTS se ha podido deducir que primeramente se necesitó definir los servicios de: autenticación, confidencialidad e integridad. Una vez que se fijan los servicios antes mencionados se debe pasar a la descripción de la arquitectura de seguridad en UMTS. Del trabajo aquí realizado se ha identificado que los dominios de seguridad serían: de acceso, de red, de usuario, de aplicación y configurabilidad, los cuales son el conjunto de características de seguridad que proporcionan a los diferentes elementos de la red un acceso seguro a la información.

Para que las características de seguridad sean obtenidas se ha llegado a definir que es necesario el uso de diferentes mecanismos de seguridad como identificación por identidad temporal, autenticación y acuerdo de claves, confidencialidad e integridad de conexión de acceso.

Debido a la capacidad de la red UMTS de ofrecer servicios multimedia con una alta variabilidad en la tasa de transmisión se encontró que es fundamental la aplicación del concepto de calidad de servicio en este tipo de redes. Esto implica el estudio de la arquitectura de calidad de servicio que considera la descripción de los servicios portadores UMTS, de acceso por radio RAB (*Radio Access Bearer*, Portador de Acceso por Radio), de red central, etc. También implica el análisis de las diferentes clases de servicio como: Conversacional, *Streaming*, Interactiva, *Background*, y los distintos parámetros como la velocidad de transmisión, proporción de bit errados, retardo, etc.

Con el objetivo de garantizar una adecuada calidad se ha visto la necesidad de aplicar distintas tecnologías como MPLS (*Multi Protocol over Label Switching*, Conmutación de Etiquetas sobre Multi Protocolo), Servicios Diferenciados en la

red central y mecanismos de gestión de recursos, control de admisión, control de potencia, etc, en la red de acceso terrestre.

Como resultado del estudio realizado se presenta un análisis de los más importantes servicios y aplicaciones en UMTS y además una estimación de la red para un adecuado desarrollo de servicios considerando los conceptos de calidad y seguridad que deben existir en el sistema UMTS.

CAPÍTULO I

CARACTERÍSTICAS DE LOS SISTEMAS DE COMUNICACIONES MÓVILES

CAPÍTULO 1

CARACTERÍSTICAS DE LOS SISTEMAS DE COMUNICACIONES MÓVILES

En el presente capítulo primeramente se realiza una descripción de la tecnología de los diferentes sistemas de comunicaciones móviles, con un marcado interés en los sistemas de tercera generación. Además se efectúa una descripción de la arquitectura del sistema de comunicaciones UMTS, indicando sus distintos dominios. Todo esto se hace para tener una idea del entorno de funcionamiento del sistema de comunicaciones UMTS. Esto conllevará a tener un marco adecuado para la realización de los siguientes capítulos.

1.1 CARACTERÍSTICAS DE LOS SISTEMAS DE COMUNICACIONES MÓVILES[1]

Los sistemas de comunicaciones móviles han constituido uno de los ámbitos de desarrollo tecnológico de mayor crecimiento en los últimos tiempos, con seguridad representan un paso enorme en términos de velocidad de implantación de un nuevo servicio para la sociedad humana en toda la historia. Ninguna tecnología hasta el momento ha pasado tan rápidamente de su puesta en marcha inicial a su utilización masiva por millones de personas en todo el planeta.

[1] Referencia [1]: Serie Mundo Electrónico, "Telecomunicaciones Móviles", Alfa Omega México D.F.

El desarrollo del mercado de las telecomunicaciones, cuyos dos motores principales son las comunicaciones móviles e Internet, está siendo espectacular, y todas las perspectivas indican que va a seguir siéndolo en las próximas décadas.

Este crecimiento ha sido posible en primer lugar gracias a los acuerdos en materia de estandarización llevados a cabo por organismos intergubernamentales como la ITU (*International Telecommunications Union*, Unión Internacional de Telecomunicaciones) o la ETSI (*European Telecommunications Standars Institute*, Instituto de Estándares de Telecomunicaciones Europeo) que han posibilitado la formación de economías de escala en el ámbito de un mercado común, resultando en una reducción del precio de los terminales y la consiguiente extensión del mercado a un mayor número de clientes potenciales. En segundo lugar, gracias a la propia evolución tecnológica, que ha permitido mejorar las prestaciones ofrecidas por los servicios ofertados no sólo desde el punto de vista del usuario final, reflejadas en una mayor velocidad de transmisión, una mejor calidad de recepción y una mayor confidencialidad de las comunicaciones, sino también desde la perspectiva de los operadores, en términos de una mayor capacidad y un uso más eficiente de los recursos radioeléctricos.

La evolución de los sistemas de comunicaciones inalámbricos, se indica en la Figura 1.1 desde su introducción hasta la actualidad, y a continuación se especifican las diferentes generaciones de sistemas móviles.

1.1.1 COMUNICACIONES MÓVILES DE PRIMERA GENERACIÓN

La primera generación (1G) fue analógica y limitada en capacidad de *roaming* (seguimiento), el servicio básico de voz era de baja calidad y los teléfonos se diseñaron principalmente para uso en vehículos.

A continuación se mencionan algunos sistemas de primera generación:

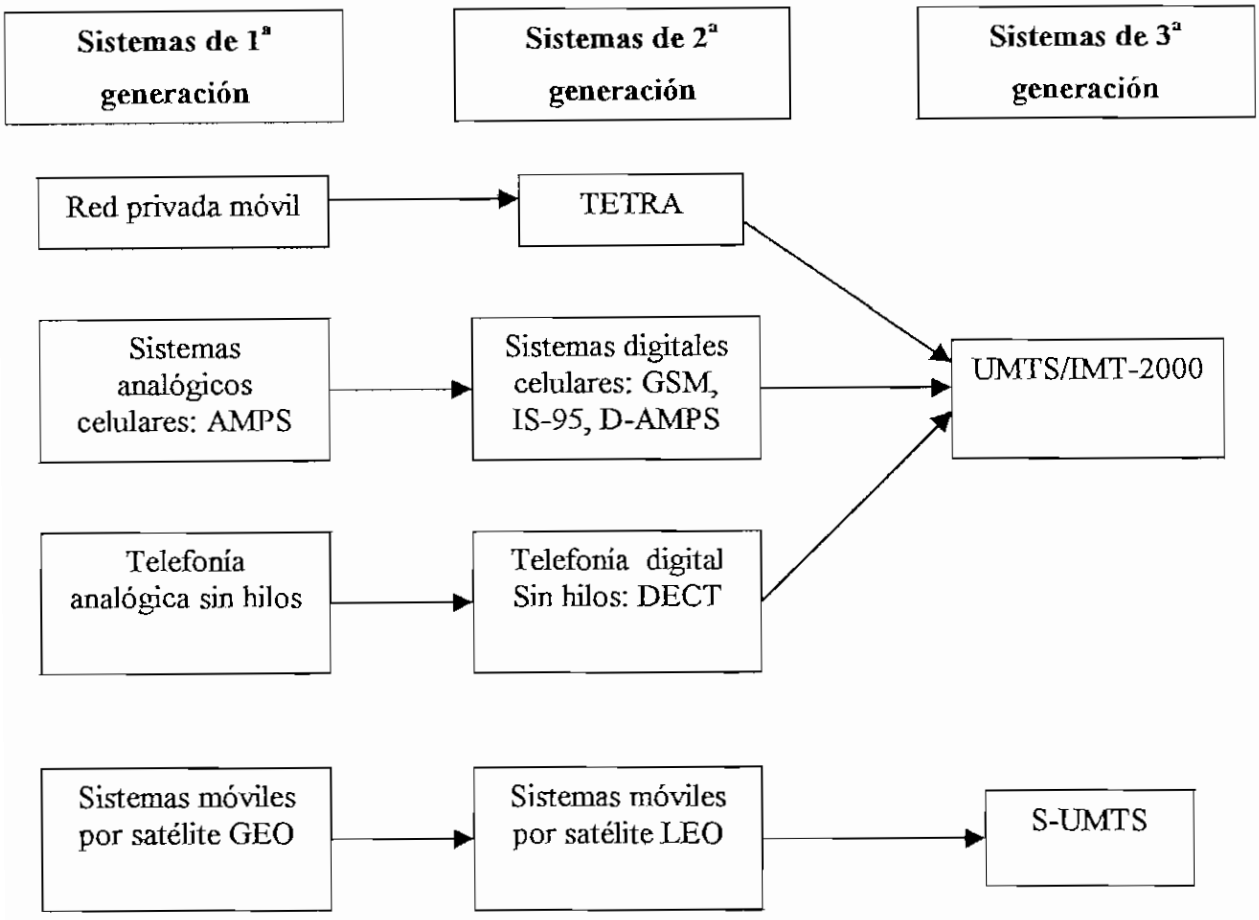


Figura 1.1 Evolución de los sistemas de telecomunicaciones móviles

Sistemas de telefonía pública

Son sistemas que permiten a un usuario generar llamadas de voz hacia cualquier otro usuario, ya sea de la red telefónica fija o móvil. El aspecto clave de estos sistemas para poder ofrecer un uso eficiente del espectro radioeléctrico sobre un elevado número de usuarios es la división de la región de cobertura en un conjunto de células, cada una servida por una estación base, de modo que es posible reutilizar las mismas frecuencias en células ubicadas a una cierta distancia. Dentro de estos sistemas destacan por ejemplo AMPS (*American Mobile Phone System*, Sistema Telefónico Móvil Americano) en Estados Unidos, NMT (*Nordic Mobile Telephone*, Telefónica Móvil Nórdica) desarrollado por Ericsson en Suecia, y empleado en varios países europeos, TACS (*Total Access Communications System*, Sistema de Comunicaciones de Acceso Total), surgido

en Europa como versión de AMPS y NTT (*Nipon Telephone and telecommunications*, Telecomunicaciones y Telefonía Japonesa), desarrollado en Japón. Todos estos sistemas eran de marcado ámbito nacional y no albergaban la posibilidad de interconectividad entre redes de diferentes países.

Sistemas de telefonía privada (sistemas troncales)

Destinados a dar servicio de voz a grupos cerrados de usuarios, que no requieren del acceso a la red telefónica pública. Este tipo de sistemas acostumbran a ser operados por las compañías propietarias, tras la adjudicación de unos determinados canales.

Sistemas de telefonía sin hilos (extensiones inalámbricas de la red fija)

Estos sistemas, concebidos esencialmente para aplicaciones domésticas, se basan en la conexión de un transmisor/receptor de radio a la línea telefónica fija, lo que permite sustituir el terminal fijo por otro inalámbrico en una cierta área de cobertura reducida con una baja capacidad de movilidad. Si bien los primeros sistemas de estas características fueron introducidos sin ningún tipo de legislación, rápidamente surgieron algunos estándares como CT0[1] o CT1[2].

Sistemas de radiomensajería

Permite dirigir mensajes alfanuméricos de aviso de forma unidireccional hacia terminales móviles. Estaban basados en el protocolo POCSAG (*Post Office Code Standars Advisory Group*, Código de Correo del Grupo Asesor de Estándares). Con objeto de permitir la operatividad internacional, surgieron algunos sistemas fruto de consorcios entre países como Eurosignal, entre Francia, Alemania y Suiza en 1971.

---

[1] CTO (*Cordless Telephone 0*, Teléfono sin hilos 0), es la primera norma publicada para los teléfonos sin cordón de tipo analógico que trabajan en la banda de VHF.

[2] CT1 (*Cordless Telephone 1*, Teléfono sin hilos 1), es una norma para teléfonos inalámbricos analógicos, cuyas frecuencias de trabajo se ubican en la banda de UHF.

1.1.2 COMUNICACIONES MÓVILES DE SEGUNDA GENERACIÓN

Con la irrupción de la tecnología digital en el ámbito de las comunicaciones móviles surgieron los sistemas denominados de segunda generación, que permitían mejorar las prestaciones ofrecidas por los de primera generación aprovechando las características de dicha tecnología. Como ventajas principales se distinguen:

- La capacidad para incrementar la calidad de recepción gracias a la posibilidad de incorporar técnicas de corrección de errores.
- La mayor privacidad en las comunicaciones fruto del empleo de técnicas de criptografía sobre las secuencias de bits transmitidas.
- La posibilidad de emplear nuevas técnicas de acceso múltiple como las basadas en división en tiempo TDMA[1] (*Time División Multiplex Accessing*, Acceso Múltiple por División de Tiempo) o en código CDMA[2] (*Code División Multiplex Accessing*, Acceso Múltiple por División de Código), que permiten mejorar la eficiencia en el uso del espectro radioeléctrico.
- La mayor capacidad para la transmisión de datos con diferentes velocidades binarias.

Entre los sistemas de segunda generación destacan los enumerados a continuación.

Sistema de Comunicaciones GSM

En la línea de los sistemas NMT o TACS, en 1982 se planteó el desarrollo de un sistema que fuera un estándar a nivel europeo y que proporcionara la capacidad de interconexión entre redes de diferentes países. De este modo surgió el denominado GSM (*Global System for Mobile Communications*, Sistema Global para Comunicaciones Móviles), trabajando en la banda de 900 MHz con una

[1] TDMA es una técnica de acceso múltiple que atiende a las llamadas en diferentes intervalos de tiempo dentro de la misma frecuencia.
[2] CDMA es la técnica de acceso múltiple por división de código, la cual permite que los usuarios compartan todo el espectro disponible, pero usando diferentes secuencias de código para separar las comunicaciones.

técnica de acceso híbrida FDMA/TDMA[1], y que gracias a su rápido desarrollo ha logrado imponerse no sólo en Europa sino también en otros países. Esto constituye uno de los grandes logros de GSM que le ha permitido imponerse a otros sistemas como los desarrollados en Japón (sistema JDC, *Japanese Digital Cellular*, Celular Digital Japonés) o en Estados Unidos (sistema D-AMPS, *Digital AMPS*, como evolución de AMPS).

Al margen del servicio básico de voz, este tipo de sistema presenta capacidades para la transmisión de datos, aunque únicamente en modo de conmutación de circuitos y con velocidades reducidas, lo que no lo hace especialmente apropiado en un entorno de tráfico variable, como el que típicamente se encuentra en aplicaciones de datos como la conexión a Internet. A modo de ejemplo, GSM es capaz de soportar una velocidad de transmisión únicamente de hasta 9.6 Kbps, tras la incorporación de códigos correctores de errores, para adaptarse a los requerimientos más elevados en cuanto a probabilidad de error de los sistemas de transmisión de datos.

Fruto de la evolución de GSM para ofrecer una mayor capacidad y nuevos servicios diferenciados, ha surgido el denominado DCS-1800 (*Digital Cellular System* –1800 MHz, Sistema Celular Digital –1800 MHz) que trabaja en la banda de 1800 MHz.

Sistemas de telefonía privada TETRA

La evolución de los sistemas troncales hacia la tecnología digital se ha reflejado en el desarrollo del estándar TETRA (*Trans European Trunked Radio*, Radio Troncalizado Trans Europeo), el mismo que constituye un sistema de radiocomunicaciones privados con nuevas funcionalidades, como por ejemplo:

- Mejor calidad de voz, en condiciones de trabajo con un alto nivel de ruido.
- Seguridad de funcionamiento garantizada, ya que utiliza mecanismos de confidencialidad junto con la facilidad de autenticación de los terminales.

[1] FDMA/TDMA es una técnica híbrida de acceso múltiple en donde la comunicación se soporta sobre un canal físico constituido sobre una portadora, elegida entre las disponibles, que se utiliza para una comunicación concreta sólo durante un cierto intervalo de tiempo.

- Facilidad de llamadas punto-multipunto para organizaciones que necesitan coordinar actividades de un grupo de usuarios dispersos en el espacio pero dedicados en la realización de una tarea común; este tipo de llamada, con un corto tiempo de establecimiento, facilita enormemente la coordinación de actividades en el desarrollo de la tarea y en especial en organizaciones en que los usuarios son coordinados desde un puesto central de operaciones.
- Transmisión de datos con una velocidad de transmisión máxima de 28.8 kbps.

Sistema sin hilos DECT

La segunda generación de las extensiones inalámbricas de la red fija se ha plasmado en la especificación, por parte de ETSI, del estándar DECT (*Digital Enhanced Cordless Telecommunications*, Telecomunicaciones Digitales Sin Hilos Aumentada). DECT es un sistema de telefonía inalámbrica diseñado para soportar altas densidades de tráfico en distancias cortas, típicamente 300 metros. A mas de ello se debe mencionar que este sistema es de tipo multiusuario, es decir que permite el uso simultaneo de un mismo tranceptor de radio o estación base por parte de diferentes usuarios, lo cual representa una gran diferencia con respecto a los sistemas de primera generación CT0 y CT1 que solo son de tipo monousuario.

La técnica de acceso empleada por DECT es del tipo FDMA-TDMA-TDD[1], con una capacidad total de 10 de señales portadoras por 12 canales diferentes por portadora, lo que da un total de 120 canales bidireccionales de 32 Kbps. Una descripción rápida permitirá comprender fácilmente lo indicado:

- FDMA (*Frequency División Multiplex Accessing*): El espectro radioeléctrico utilizado es compartido por un total de 10 señales portadoras diferentes, separadas 2 MHz cada una de ellas, ocupando un espectro limitado a un total de 20 MHz.

[1] FDMA-TDMA-TDD es una técnica de acceso multiple FDMA/TDMA que utiliza para la separación entre el enlace ascendente y el descendente el método de duplexación por división de tiempo TDD.

- TDMA (*Time División Multiplex Accessing*): Cada una de las portadoras permite la transmisión bidireccional de 12 canales diferentes, en distintos instantes de tiempo, y en un formato de ráfagas. Dichos canales poseen una capacidad neta de 32 Kbps, cada uno de ellos.
- TDD (*Time División Duplexing*): La separación de los sentidos de transmisión se efectúa en el dominio del tiempo, operando ambos a la misma frecuencia de radio. Por tanto, se trasmite al mismo ritmo, una ráfaga en sentido ascendente y su correspondiente en sentido descendente a continuación.

Mientras tanto en Japón, el sistema que se ha desarrollado en este ámbito ha sido PHS (*Personal Handyphone System*, Sistema Telefónico Personal), implantado con gran éxito, mientras que en Estados Unidos se ha desarrollado el estándar PACS (Personal Access Communications Services, Servicios de Comunicaciones de Acceso Personal).

Sistemas de radiomensajería

Los sistemas de radiomensajería de segunda generación son tecnologías que ofrecen a más del servicio básico de envío de mensajes alfanuméricos de forma unidireccional hacia los terminales móviles otro tipo de servicios, como por ejemplo:

- La retransmisión de mensajes si no ha existido confirmación de éxito por parte del terminal móvil.
- Facilidades relacionadas con la tarifación del servicio, el cual permite establecer y aplicar diferentes criterios de tarifación a los usuarios.
- Facilidades relacionadas con la seguridad, que permiten proteger a los usuarios frente a los accesos ilegales a través del uso de encriptación de los mensajes.

Dentro de estos sistemas se encuentra al estándar ERMES (*European Radio Message System*, Sistema de Mensajes de Radio Europeo), de mayor capacidad que POCSAG y que posee todos los servicios anteriormente mencionados.

También es importante destacar que el sistema móvil GSM ofrece para el envío y recepción de mensajes cortos unidireccionales a través del denominado SMS (*Short Message Service*, Servicio de Mensajes Cortos).

Redes locales inalámbricas (*Wireless LAN*)

La función principal de este tipo de redes es proporcionar conectividad y acceso a las tradicionales redes cableadas (Ethernet, Token Ring, etc), como si de una extensión de estas últimas se tratara, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas. Son ideales para lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas. Los requerimientos de movilidad son mucho más reducidos que en los sistemas de telefonía, lo que permite una mayor velocidad de transmisión en entornos de interiores, del orden de 1 Mbps. Los dos principales estándares que han surgido para este tipo de aplicaciones son IEEE 802.11 e HIPERLAN (*High Perfomance Radio LAN*, LAN de Alto Rendimiento de Radio), logrando este último velocidades de hasta 20 Mbps. Se debe mencionar que, a diferencia del resto de sistemas, orientados a conexión, los sistemas para redes locales inalámbricas están orientados a transmisión por paquetes, lo que exige el empleo de protocolos específicos para gestionar el acceso al medio de transmisión, tales como CSMA/CD[1] (*Carrier Sense Múltiple Access/Collision Detection*, Acceso Múltiple por Detección de Portadora, con Detección de Colisiones).

1.1.3 COMUNICACIONES MÓVILES DE TERCERA GENERACIÓN

Para abordar el estudio de los sistemas de comunicaciones móviles de tercera generación, se ha considerado importante realizar en esta tesis un análisis del por que la aparición de estos sistemas, así como de los requisitos y del plan de frecuencias necesarios en el entorno de 3G, con el objetivo de dar una visión de su importancia en el mercado de las telecomunicaciones.

[1] CSMA/CD: Es un tipo de protocolo en el que las estaciones escuchan el canal y sólo transmiten cuando el canal esta desocupado. Si se produce una colisión el paquete es transmitido tras un intervalo de tiempo aleatorio.

1.1.3.1 Factores para la aparición de los sistemas de tercera generación

La aparición de los denominados sistemas de comunicaciones móviles de tercera generación, surge principalmente debido a los siguientes factores:

a) Por el intenso crecimiento de la penetración en el mercado de los sistemas de segunda generación, en ciertos países el número de líneas móviles ha llegado incluso a superar el número de líneas de telefonía fija. En relación a este aspecto, se debe tener en cuenta que si bien un teléfono fijo tiene un ámbito de uso familiar, el teléfono móvil presenta un uso unipersonal, lo que le permitirá un grado de penetración superior. Este crecimiento tenderá a llevar a la saturación los actuales sistemas de segunda generación, por lo que se hace patente la búsqueda de nuevas bandas de frecuencias y de nuevos sistemas que permitan hacer frente a la demanda con un uso de los recursos más eficiente.

En la Figura 1.2 se muestra, las previsiones de crecimiento en los usuarios de telefonía móvil para la próxima década.

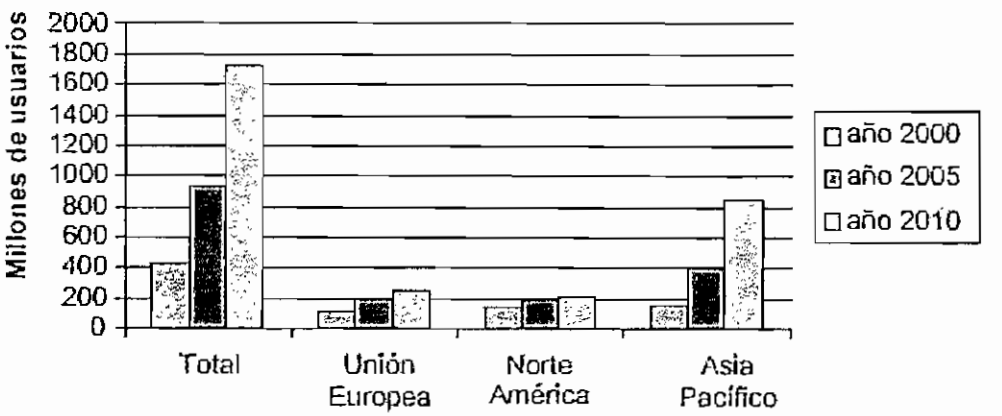


Figura1.2 Previsiones de crecimiento de los usuarios de telefonía móvil[1]

b) El intenso crecimiento del uso de Internet ha producido la aparición de nuevas oportunidades de negocios, por lo que es imprescindible combinar los beneficios

[1]Referencia [16]: UMTS FORUM, "Report on Candidate Extension Bands for UMTS/IMT-2000 Terrestrial Component", Report No.7.

de las comunicaciones móviles y el acceso a Internet. Esta combinación puede suponer un enorme mercado potencial de cara a los próximos años.

Si bien los sistemas celulares de segunda generación como GSM son capaces de ofrecer acceso a Internet, lo hacen en modo circuito, lo que presenta enormes limitaciones no sólo en términos de la velocidad de transmisión empleada, sino también de la eficiencia en el uso de los recursos, pues este tipo de aplicaciones se caracterizan por generar la información a ráfagas con lo que durante buena parte del tiempo el circuito no es utilizado. Estas limitaciones redundan por un lado en una reducida capacidad para ofrecer este tipo de servicios, y por el otro en un precio de conexión para los usuarios mucho más elevado del que se puede llegar a ofrecer en una red fija.

En consecuencia, es deseable el diseño de nuevos sistemas que sean capaces de hacer frente a estas limitaciones con un uso más efectivo de los recursos, capaces de adaptarse a las nuevas características del tráfico mediante técnicas de transmisión orientadas a paquetes, constituyendo éste uno de los retos al que los sistemas de tercera generación deberán hacer frente.

c) El aumento de la demanda en servicios multimedia de alta velocidad, tales como vídeo, audio, videoconferencia, juegos interactivos, acceso a bases de datos que se ha venido experimentando en los últimos años, ha motivado un mercado de enorme atractivo para compañías operadoras y proveedores de servicio. Por ello, la integración de todos los servicios antes mencionados dentro del marco de una red móvil, plantea una serie de retos en los sistemas de tercera generación, pues se deben gestionar los escasos recursos radioeléctricos adecuadamente, para poder ofrecer dichos servicios bajo parámetros de calidad de servicio (retardo, velocidad de transmisión, etc) similares a los de la red fija pero haciendo frente a las peculiaridades de la transmisión por radio en entornos móviles.

El mercado potencial de este tipo de servicios se puede apreciar a través del gran interés que han expresado los usuarios por algunos de ellos, como por

ejemplo, el grado de interés por parte de los usuarios para una descarga de música es del 76%[1], para observar un video clip es del 63%[1] y para un intercambio de fotos es del 78%[1] respectivamente.

d) Por último, se debe indicar el creciente número de personas que debido a su movilidad requieren de una herramienta de uso global que sea capaz de comunicarse con la red de datos en cualquier punto, independiente del lugar donde se encuentre. Por tal motivo se debe lograr un sistema de comunicaciones móviles que permita una movilidad universal con operación entre redes pertenecientes a países diferentes, llegando incluso a reunir bajo un sistema común las tres zonas geográficas de mayor influencia que son Europa, Estados Unidos y Japón.

Por todos los factores antes mencionados, los sistemas de tercera generación están siendo diseñados específicamente para satisfacer los nuevos requisitos de información. Con ellos las comunicaciones entre personas se verán sustancialmente mejoradas respecto a los sistemas anteriores. Esta mejora se dará gracias al aumento sustancial de la tasa de transmisión de datos en los accesos a la información y servicios de redes tanto públicas como privadas. Todo esto, junto con la continua evolución de los sistemas de segunda generación actuales, creará un sinfín de nuevas oportunidades de negocio no solo para los fabricantes de equipos de telecomunicaciones y las operadoras, sino también para los proveedores de contenidos y de aplicaciones que usan la red.

El ámbito de actuación de los sistemas de tercera generación se pretende mostrar gráficamente en la Figura 1.3, como una forma de englobar bajo un único sistema los diferentes entornos existentes, en función de la cobertura ofrecida, desde los sistemas vía satélite hasta los más reducidos entornos de interiores, con objeto de permitir una movilidad universal de terminales capaces de soportar aplicaciones personalizadas de muy variada naturaleza.

[1]Referencia[23]: Tommi Roman , "3G Wireless Opportunity Space", Helsinki University of Technology, pág42.

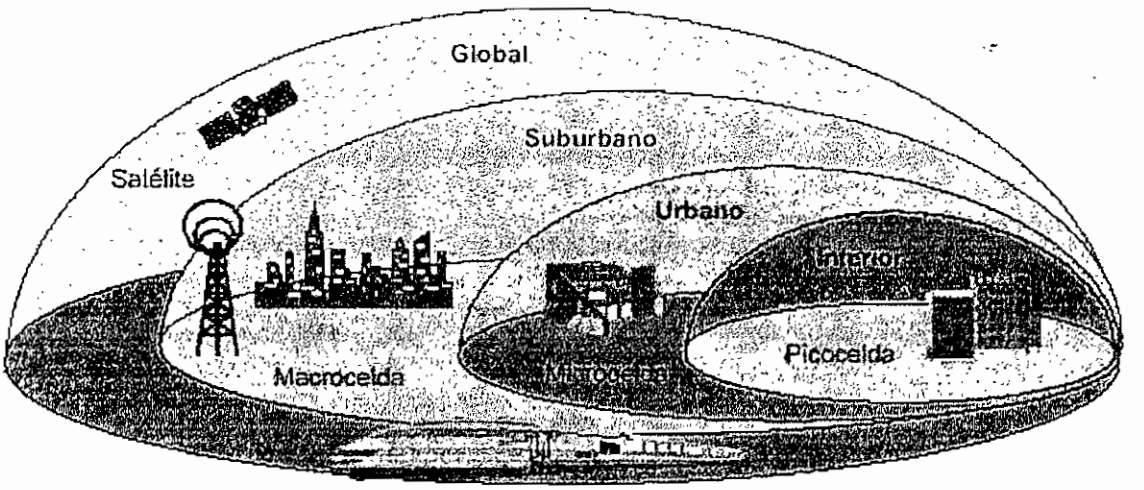


Figura 1. 3 Ámbito de movilidad en los sistemas de tercera generación

Entre los sistemas de tercera generación que destacan se puede indicar a UMTS y CDMA 2000, los cuales han tenido mayor aceptación por los entes involucrados en la estandarización.

Mas adelante en la sección 1.2 se describirá el sistema de comunicaciones UMTS.

1.1.3.2 Requisitos para la tercera generación

Para asegurar el éxito de los servicios 3G, se debe proporcionar a los usuarios unas comunicaciones eficientes, con una alta velocidad y calidad y, además, fáciles de utilizar. Como resultado de ello, el diseño de los sistemas de tercera generación se aborda desde la perspectiva de los siguientes requisitos[1]:

- Velocidades de transmisión mucho más altas: 144 Kbps en alta movilidad, 384 Kbps en espacios abiertos y 2 Mbps en baja movilidad.
- Velocidades variables bajo demanda en función de las características de cada servicio.

[1] Referencia [24]: José Manuel Huidobro, "La Evolución Hacia La 3ª Generación De Comunicaciones Móviles" .

- Capacidad de ofrecer servicios con diferentes requerimientos de calidad dentro de una misma conexión, como por ejemplo voz, vídeo o transferencia de datos en modo paquete.
- Capacidad de soportar un amplio abanico de requerimientos de retardo, para acomodar desde servicios en tiempo real hasta servicios de datos de tipo best effort (sin calidad de servicio garantizada).
- Capacidad de soportar requerimientos de calidad desde un 10^{-2} hasta un 10^{-8} de tasa de error de bit.
- Coexistencia de sistemas de segunda y tercera generación y posibilidad de efectuar handovers[1] entre sistemas diferentes.
- Soporte de tráfico asimétrico entre los enlaces ascendente y descendente, como sería el caso habitual de la navegación por Internet.
- Alta eficiencia espectral.
- Coexistencia de los modos de operación FDD y TDD.
- Ambientes de funcionamiento marítimo, terrestre y aeronáutico.
- Soporte tanto de conmutación de paquetes (IP) como de circuitos.
- Capacidad de ser un estándar global que cubra las necesidades de un mercado de masas.

1.1.3.3 Plan de Frecuencias para los Sistemas de Tercera Generación

En la Conferencia Mundial de Radio WARC (*World Administrative Radio Conference*), se dispuso de 230 MHz de espectro radioeléctrico, sin asociarlo a ninguna tecnología, en las bandas de 1885-2025 MHz y 2110-2200 MHz para uso mundial en el interfaz aire de los sistemas de tercera generación, incluyendo tanto la componente terrestre como las comunicaciones móviles por satélite (MSS, *Mobile Satelite Services*), tal y como se presenta en la Figura 1.4. Si bien esta banda es común tanto para Europa como para los países asiáticos como China o Japón, no ocurre lo mismo en Estados Unidos, donde dicha banda ya había sido asignada a algunos operadores de sistemas de segunda generación PCS (*Personal Communications Systems*, Sistemas de Comunicaciones Personales), y no se ha dispuesto de más espectro para los sistemas de tercera

[1] *Handover*: Traspaso de la conexión entre diferentes sistemas debido al movimiento del terminal, capacidad del sistema, etc.

generación, por lo que la solución planteada por el momento ha sido la de reutilizar la banda de PCS.

Otro aspecto diferente en la asignación ocurre en Europa y Japón donde la totalidad de la banda no será empleada por IMT-2000, sino que la parte de las frecuencias más bajas se mantiene ocupada por los sistemas DECT y PHS, respectivamente.

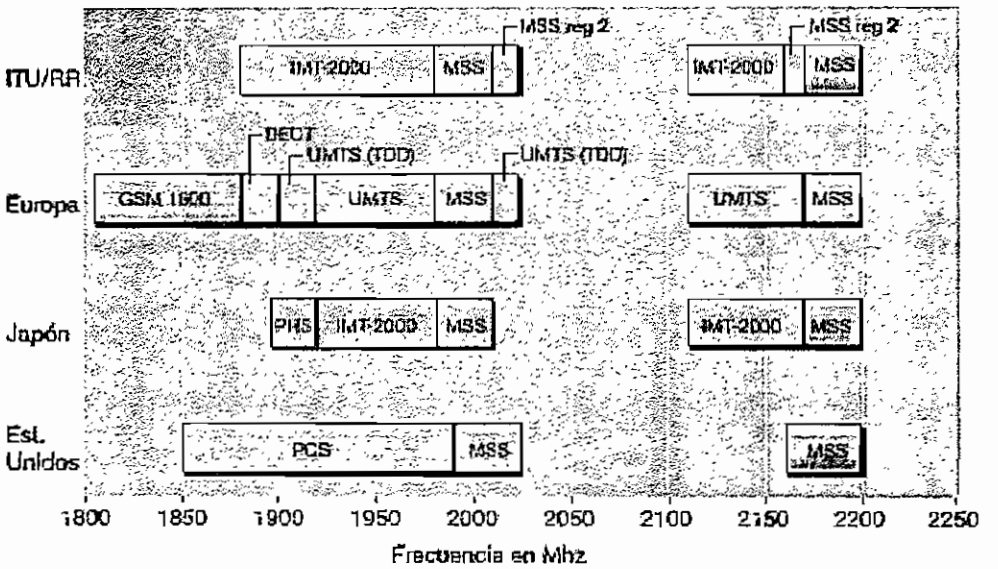


Figura1.4 Bandas asignadas para los sistemas de tercera generación[1]

En relación a Europa, la banda total asignada a UMTS se subdivide en dos bandas, 1920 a 1980 MHz y 2110 a 2170 MHz, destinadas al modo de operación FDD para los enlaces ascendente y descendente, respectivamente, y dos bandas, 1885 a 1920 MHz y 2010 a 2025 MHz, destinadas al modo de operación TDD. Esto se puede observar en la Figura 1.5.

[1]Referencia [2]: John B. Groe, Lawrence E. Larson, "CDMA Mobile Radio Design", Artech House Publishers Boston 2000, pág:251-254.

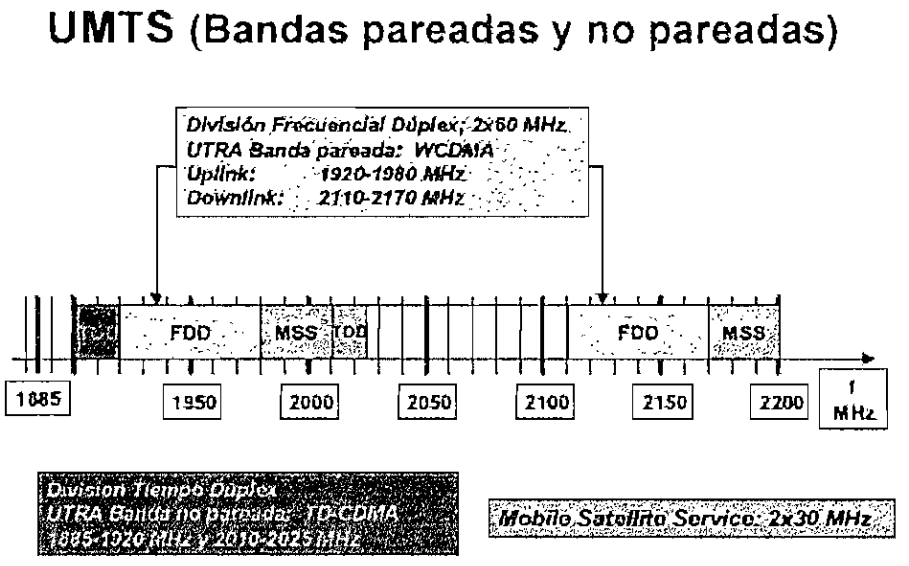


Figura 1.5 Asignación de espectro para UMTS en Europa

1.2 SISTEMA DE COMUNICACIONES UMTS

Las siglas UMTS son la abreviación de *Universal Mobile Telecommunications System* (Sistema Universal de Telecomunicaciones Móviles), y constituye la visión europea de sistemas con capacidades 3G como parte de la familia de estándares IMT-2000. UMTS es la evolución del sistema de comunicaciones GSM a la tercera generación, por lo que está siendo mayoritariamente adoptado en la Unión Europea.

La tecnología de acceso por radio usada por este sistema es WCDMA (*Wideband CDMA*, CDMA de Banda Ancha), la cual se basa en una técnica de acceso múltiple por división en código con espaciado de 5 MHz entre canales, y con modos de duplexado FDD (*Frequency Division Duplex*, Duplexación por División de Frecuencia) y TDD (*Time Division Duplex*, Duplexación por División de Tiempo), para el funcionamiento con bandas pareadas y con bandas no pareadas, respectivamente. La Figura 1.6 muestra una representación gráfica de estos modos de operación.

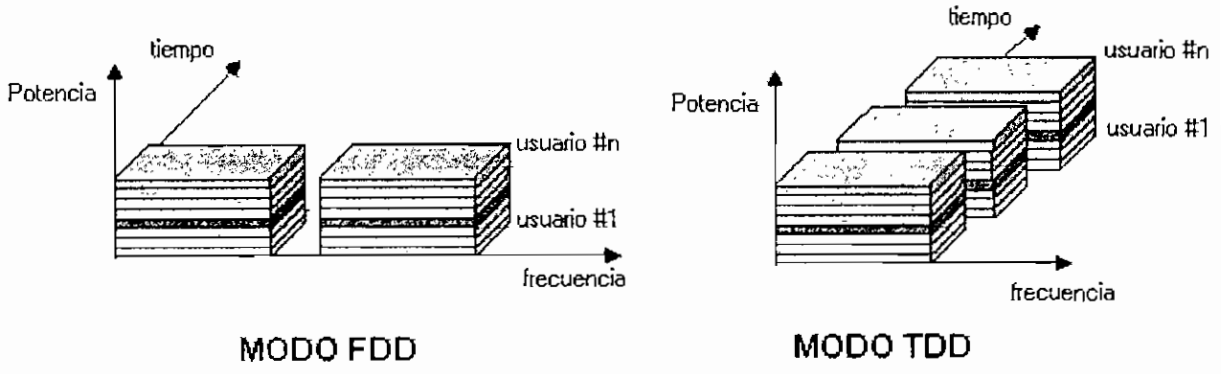


Figura 1.6 Modos de operación de WCDMA[1]

Entre las ventajas de WCDMA es que representa un interfaz de gran flexibilidad para acomodar diferentes servicios con distintas velocidades. Las principales características de esta técnica de acceso son:

- Integración en la capa física de diferentes velocidades de transmisión con una sola portadora.
- Factor de reúso de frecuencias igual a la unidad.
- Soporte para utilizar sistemas receptores avanzados.
- Gestión basada en la carga.

Dentro de la concepción UMTS se debe proporcionar servicio satelital, fijo terrestre y móvil terrestre, con el objetivo de dar cubrimiento a nivel mundial. Este aspecto, hará que exista una macrodiversidad de celdas capaces de prestar el servicio dependiendo de la zona donde se encuentre el usuario, pero como mínimo en la mayoría de los casos existirá la prestación satelital como último recurso.

UMTS, en la componente terrestre, tiene una estructura jerárquica, esto es, está compuesta por tres tipos de celdas: Macro Celda, Micro Celda y Pico Celda con un mínimo de 5 MHz de ancho de banda por Celda (Figura 1.3).

[1]Referencia [25]: Revista de Telecomunicaciones de Alcatel, "Normalización de los sistemas móviles 3G", pág:15.

La Macro Celda tiene radios desde 1 km hasta 35 km y se destinan para ofrecer cobertura rural y carreteras para vehículos o similares que se mueven a alta velocidad (transmisión de datos de 114 kbps). La Micro Celda tiene radios desde 50 m hasta 1 km; ofrecen servicio a usuarios fijos o que se mueven lentamente con elevada densidad de tráfico (urbana) con velocidades de 384 kbps. Las Pico Celdas tiene radios hasta a 50 m; ofrecen coberturas localizadas en interiores, con velocidades del orden de los 2 Mbps. Toda esta diversidad de formas para proporcionar servicios impulsará de manera notable la introducción de UMTS dado que a su vez generará solución a la problemática de cubrimiento en zonas en la cual la telefonía tradicional difícilmente tendrá acceso por factores netamente económicos.

1.2.1 ARQUITECTURA DEL SISTEMA UMTS[1]

Para describir la arquitectura de UMTS se emplea el término dominio, el cual se define como la agrupación de diferentes entidades físicas. Entre dos dominios relacionados se definen puntos de referencia o interfaces.

Como se observa en la Figura 1.7 la arquitectura se divide en dos dominios básicos, *Dominio de Equipamiento de Usuario*, es decir, el equipamiento utilizado por el usuario para acceder a los servicios UMTS, y *Dominio de Infraestructura*, que consiste en dos nodos físicos que ofrecen aquellas funciones requeridas para incluir la interfaz de radio y soportar los requerimientos de los servicios de telecomunicación de los usuarios. Este dominio es un recurso compartido que provee servicios a todos aquellos usuarios autorizados dentro de su área de cobertura. El punto de referencia entre ambos dominios es "Uu", interfaz de radio UMTS.

[1]Referencia [3]: 3rd Generation Partnership Project, 3GPP TS 23.101, "Technical Specification Group Services and System Aspects General UMTS Architecture".

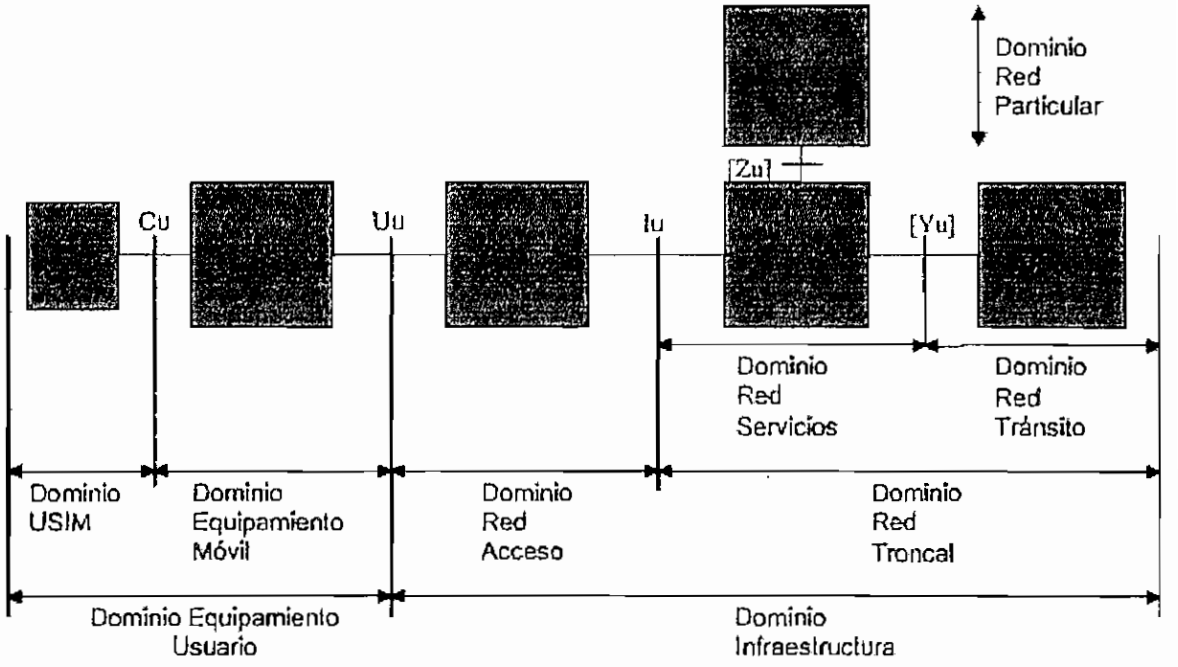


Figura 1.7 Dominios de UMTS y puntos de referencia

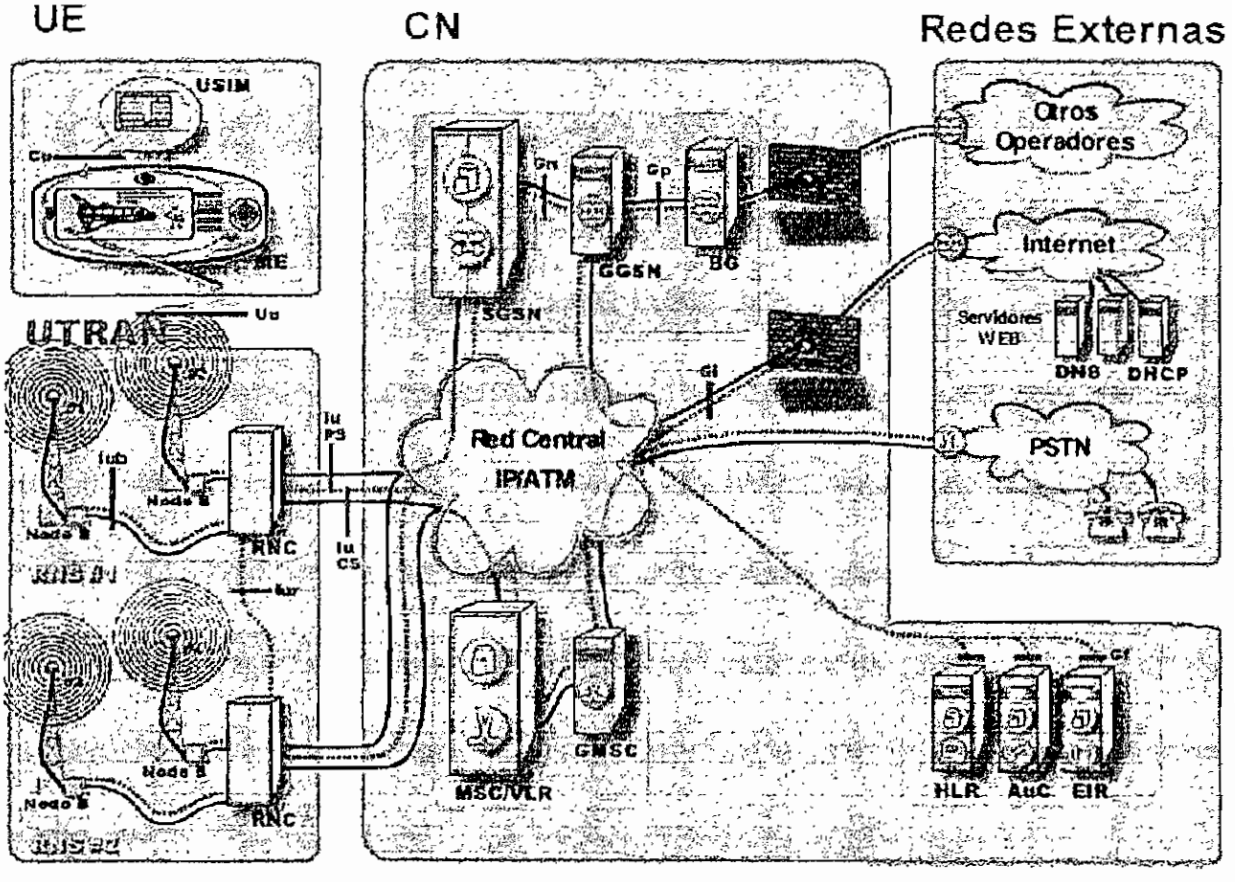


Figura 1.8 Arquitectura de UMTS con sus diferentes nodos

En la Figura 1.8 se puede observar de una manera detallada las entidades más importantes que conforman la arquitectura de UMTS, y además de ello, cómo están interconectadas en el sistema.

1.2.1.1 Dominio de Equipamiento de Usuario (UE)

Este dominio engloba a una variedad de tipos de equipamiento (terminales) con diferentes niveles de funcionalidad, y pueden asimismo ser compatibles con uno o más accesos de interfaces existentes (fijas o por radio). El dominio de equipamiento de usuario se subdivide en *Dominio de Equipamiento Móvil (ME)* y *Dominio del Módulo de Identificación de Servicios de Usuario (USIM)*.
El punto de referencia entre estos dominios se denomina "Cu".

1.2.1.1.1 Dominio de Equipamiento Móvil (ME)

Este dominio ejecuta la transmisión por radio y contiene aplicaciones. El equipamiento móvil puede ser subdividido en dos subgrupos: *Terminación Móvil (MT)* que ejecuta la transmisión por radio y *Equipamiento de Terminal (TE)* que contiene las aplicaciones extremo a extremo. Estos niveles se utilizan en la descripción funcional de las comunicaciones pero no se definen puntos de referencia entre ambos.

1.2.1.1.2 Dominio USIM

Este dominio contiene datos y funciones, en general registradas en una tarjeta específica, que sin ninguna ambigüedad y de forma segura le identifican. Este dispositivo se asocia a un usuario determinado y permiten su identificación independientemente del ME que utilice.

1.2.1.2 Dominio de Infraestructura

Este domino se divide en *Dominio de Red de Acceso*, en contacto con el Equipamiento de Usuario, y en *Dominio de Red Troncal (Core Network)*. Esta división tiene como objetivo simplificar y asistir el proceso de funcionalidad relativo

al proceso de desacoplamiento y está en la línea con el principio modular adoptado por UMTS.

El dominio de Red de Acceso comprende principalmente las funciones específicas a las técnicas de acceso, mientras que el dominio de la red Troncal puede ser utilizado con flujos de información independientemente del modo de acceso.

1.2.1.2.1 Dominio de Red de Acceso (UTRAN)

El dominio de la Red de Acceso de Radio Terrestre UMTS (UTRAN) consiste de las entidades físicas que gestionan los recursos de la red de acceso y que ofrecen al usuario mecanismos de ingreso al dominio de red troncal (CN).

La UTRAN es definida entre dos interfaces. La interface Iu entre la UTRAN y CN que es dividida en dos partes, la Iu PS para el dominio de conmutación de paquetes y el Iu CS para el dominio de conmutación de circuitos; y la interface Uu entre la UTRAN y el Equipo de Usuario.

Entre estas interfaces existen dos nodos, el RNC y la estación base también llamada nodo B.

RNC

El Controlador de la Red de Radio (RNC) es responsable por una o más estaciones base y el control de sus recursos de radio. También es el punto de acceso al servicio para los servicios que UTRAN proporciona al CN. El RNC es enlazado con el CN por dos conexiones, una al dominio de conmutación de paquetes, el SGSN, y una al dominio de conmutación de circuitos, el MSC.

Otros trabajos importantes del RNC son la confidencialidad y la protección de integridad. La identidad del suscriptor, y las claves de confidencialidad toman lugar en el RNC. Estos son entonces usados junto con las funciones de seguridad, f8 y f9 que serán abarcadas en el capítulo 2.

Nodo B

La estación base se denomina como Nodo B en UMTS y su trabajo es realizar la conexión física de radio entre el terminal y la red. El Nodo B recibe señales del RNC por la interface Iub y convierte estas a señales de radio sobre la interface Uu. También realiza algunas operaciones básicas de administración de los recursos de radio como "el control de potencia de vuelta interno" (*inner loop power control*). Esta es una característica para prevenir el problema de "Cerca-Lejos" (*near-far*); el cual es que si todos los terminales envían señales con la misma potencia, estos bloquearán al Nodo B interrumpiendo la señal de los terminales que se encuentran más alejados. Para prevenir esta situación, el Nodo B verifica el poder recibido de los diferentes terminales y les ordena que deben reducir o aumentar la potencia, así el Nodo B recibirá en forma proporcional la misma cantidad de potencia de cada terminal (ver en el Capítulo 3 la parte de control de potencia).

1.2.1.2.2 Dominio de Red Troncal (Core Network)

Este dominio consiste de las entidades físicas que dotan soporte a las especificaciones de red y servicios de telecomunicaciones, incluyendo funcionalidades como la gestión de información de localización del usuario, control de las características de red y servicios, mecanismos de transferencia (conmutación y transmisión) de señalización y de información generada por el usuario.

El dominio de red troncal se subdivide en Dominio de Red de Servicios, Dominio de Red Particular y Dominio de Red de Tránsito. La interface entre el dominio de red de servicios y el dominio de red particular se denomina [Zu] y el punto de referencia entre el dominio de red de servicios y el dominio de red de tránsito [Yu].

1.2.1.2.2.1 Dominio de Red de Servicios

Es el dominio incluido dentro del dominio de Red Troncal al cual está conectado el Dominio de Red de Acceso. Contiene aquellas funciones que son locales al punto

de acceso de usuario y aquellas cuya ubicación varía cuando el usuario se mueve. Es responsable de marcar la ruta de las llamadas y transportar la información/datos del usuario del origen al destino y de interactuar con el dominio particular para consultar datos/servicios específicos de usuario y con el dominio de tránsito para datos/servicios no específicos.

Las responsabilidades de este dominio incluyen las siguientes áreas:

- Ofrecer y gestionar recursos fijos, conexiones y rutas.
- Recuperar toda la información sobre el coste de los servicios ofrecidos y transmisión de dicha información al entorno particular y a otros operadores de red.
- Interacción con el dominio de entorno particular para identificar, autentificar, autorizar y ubicar a usuarios.

La red de servicios es dividida en dos partes:
El dominio de conmutación de paquetes (PS) y
El dominio de conmutación de circuitos (CS)

El dominio PS ofrece servicios de datos para los usuarios por conexiones a Internet y a otras redes de datos, y el dominio CS ofrece servicios de telefonía estándar a través de otras redes de telefonía. Los nodos en el CN son interconectados por el backbone del operador a redes de tecnologías de alta velocidad como ATM.

En esta parte del CN se encuentran las siguientes entidades:

SGSN

El Nodo de Soporte de Servicios GPRS (SGSN) es el principal nodo del dominio de conmutación de paquetes. Este es conectado al UTRAN por la interface Iu PS y al GGSN por la interface de Gn. El SGSN es responsable por todas las conexiones de conmutación de paquetes para el suscriptor. Este apoya a dos tipos de datos del suscriptor, información de suscripción e información de localización.

GGSN

El Nodo de Soporte de Entrada a GPRS (GGSN) es un SGSN que es interconectado a otras redes de datos. Todas las comunicaciones de datos pasan a través de un GGSN entre el suscriptor y las redes externas. Como el SGSN, este apoya a dos tipos de datos, información del suscriptor e información de la localización.

VLR

VLR es la base de datos para la gestión y ubicación de los suscriptores móviles en el área controlada por el MSC asociado. Cuando MSC necesita datos relativos a una estación móvil en ese momento localizada en su área, obtiene la información necesaria de VLR. Si una estación móvil inicia la actualización de su localización es MSC quien informa a su VLR, el cual dispondrá de datos actuales. Asimismo, cuando el suscriptor activa un servicio suplementario o modifica datos referentes a un servicio, MSC informa (a través de VLR) a HLR quien guarda dicha información y, si es necesario, actualiza VLR. Ambos el MSC y el SGSN tienen VLRs conectados a ellos.

Los siguientes datos son almacenados en el VLR:

- Identidad Internacional del Usuario Móvil (IMUI).
- Identidad de Usuario Móvil Temporal (TMUI).
- Área de ubicación (LA) de el suscriptor.
- Nodo SGNS actual que el suscriptor está conectado.
- En adición el VLR puede apoyar más información acerca de que servicios están asignados al suscriptor.
- Ambos el nodo SGSN y el MSC son implementados como un nodo físico con el VLR y por lo tanto nombrado como VLR/SGSN y VLR/MSC.

MSC

El Centro de Conmutación Móvil (MSC) esta a cargo de las conexiones de conmutación de circuitos entre terminales y redes. Realiza todo de la conmutación

y funciones de señalización para los suscriptores en su área de cobertura. La funcionalidad del MSC en UMTS es similar a las funciones del MSC de GSM.

Las conexiones de conmutación de circuitos van sobre la interfaz Iu CS entre la UTRAN y MSC; de ahí pasan por GMSC a las redes externas.

GMSC

Un GMSC es responsable de realizar las funciones de ruteado a la ubicación de el equipo móvil. Cuando las redes externas tratan de conectarse a la red UMTS, un GMSC recibe los requisitos para el establecimiento de la conexión y pregunta al HLR del actual MSC del usuario. Este entonces rutea la llamada al MSC.

Todas las conexiones de conmutación de circuitos que no han terminado dentro del mismo operador son conectados a través del GMSC a las redes externas.

1.2.1.2.2.2 Dominio de Red Particular

Este dominio contiene aquellas funciones de la red troncal de ubicación permanente sin importar la localización del punto de acceso de usuario. El USIM se relaciona por suscripción con el dominio de red particular, que contiene la información específica del usuario y gestiona la información de suscripción. Asimismo puede ofrecer servicios específicos, potencialmente no pertenecientes al dominio de red de servicios.

Las responsabilidades de este dominio incluyen las siguientes áreas:

- Ofrecer, distribuir y gestionar las cuentas de suscripción.
- Ofrecer y mantener el servicio de perfiles de usuarios, incluyendo el control de acceso a dichos perfiles.
- Negociación con los operadores de red de las características necesarias para ofrecer servicios UMTS a usuarios.

Dentro de este dominio se definen los siguientes nodos:

HLR

HLR contiene los datos de suscripción del usuario e información de direccionamiento. Es accesible desde SGSN por la interfaz Gr y desde GGSN por la interfaz Gc.

HLR es una base de datos a cargo de la administración de los suscriptores móviles. Una red móvil puede consistir de muchos HLRs, dependiendo del número de suscriptores, la capacidad de cada HLR y la organización interna de la red.

La base de datos consiste de la identidad internacional del usuario móvil (IMUI), y el protocolo de paquetes de datos (PDP). El HLR y el AuC son dos nodos de la red pero frecuentemente implementados en el mismo nodo físico.

AuC

AuC posee todos los datos necesarios para la autenticación, cifrado e integridad de cada usuario. El AuC transmite los datos requeridos para la autenticación y cifrado a través del HLR hasta el VLR, MSC y SGSN que necesitan autenticar al abonado móvil.

El AuC es asociado con un HLR , y son implementados como un nodo físico. Esto lo hace fácil para la integración de base de datos, pero deben ser mantenidos estrictamente separados. El AuC almacena la claves secretas K para cada suscriptor.

EIR

El registro de identidad del equipo (EIR) es responsable por guardar las identidades internacionales del equipo móvil (IMEI). La base de datos de los números IMEI es dividido en tres listas, blancas, grises y negras. La lista blanca contiene todos los números de IMEI que pueden acceder a la red. Un terminal es ubicado en la lista gris cuando este esta siendo observado o puesto a prueba en la red, y si este es completamente bloqueado para el acceso, será ubicado en la

lista negra. Cuando un terminal es robado, este será ubicado en la lista negra y se negará el acceso a la red. El EIR también puede ser usado para mantener series especificas de terminales fuera de la red en el caso de que estos no estén funcionando acorde a las especificaciones.

1.2.1.2.2.3 Dominio de Red de Tránsito

Este dominio está localizado entre el dominio de red de servicios y la parte remota. Si para una llamada determinada la parte remota está localizada en la misma red que el UE origen entonces no se activa ninguna instancia del dominio de tránsito.

Dentro de este dominio se encuentra el siguiente nodo:

BG

La Pasarela Límite (BG) es una entrada entre la Red Terrestre Móvil Pública (PLMN) y redes externas. La función de este nodo es bastante similar a un firewall de Internet, que mantiene al suscriptor dentro de una red segura contra ataques externos.

1.2.1.3 Comunicación Funcional entre dominios

En el aspecto funcional UMTS se divide en los denominados estratos, los cuales son agrupamientos de protocolos relacionados con algún aspecto de los servicios proporcionados por uno o varios dominios[1].

Los estratos en UMTS son:

- Estrato de Transporte,
- Estrato de Servicios,
- Estrato Particular y
- Estrato de Aplicación

[1]Referencia [3]: 3rd Generation Partnership Project, 3GPP TS 23.101, "Technical Specification Group Services and System Aspects General UMTS Architecture".

Estrato de Transporte

Esta capa soporta el transporte de los datos del usuario y las señales de control de la red de otros estratos a través de UMTS, incluyendo consideraciones del formato físico de transmisión.

El Estrato de Acceso se define como la parte del Estrato de Transporte localizada entre el nodo final del dominio de Red de Servicios y el MT.

Estrato de Acceso

Es la agrupación funcional de las partes de la infraestructura y del equipamiento de usuario así como de los protocolos entre estas partes específicas de la técnica de acceso. Permite servicios relacionados con la transmisión y administración de datos a través del interfaz de radio y además con las otras partes de UMTS.

Estrato de Servicios

En este estrato se engloban los protocolos y funciones para dirigir y transmitir datos e información, generadas por la red o los usuarios, desde el origen hacia el destino. El origen y destino pueden estar o no dentro de la misma red.

Estrato Particular

Este estrato contiene los protocolos y funciones relacionados con el manejo y almacenamiento de la información de abonado. También incluye las funciones que permiten a otros dominios actuar sobre la red particular. Las funciones principales de este estrato son: la gestión de los datos de suscripción, control de usuario (incluyendo facturación y cobro), y autenticación.

Estrato de Aplicación

Este estrato representa el proceso de aplicación en si mismo, el cual se suministra al usuario final. Incluye protocolos extremo a extremo y funciones que hacen uso de servicios suministrados por los estratos particular, de servicios y de transporte e infraestructura para soportar servicios y/ó servicios de valor añadido.

Las funciones extremo a extremo son aplicaciones que son utilizadas por los usuarios al borde o fuera de toda la red. Las aplicaciones pueden ser accesibles para los usuarios autentificados, los cuales están autorizados a acceder a estas aplicaciones. Los usuarios podrían acceder a las aplicaciones por medio del uso de un diverso equipamiento de usuario.

La Figura 1.9 muestra las interacciones entre los dominios UMTS, el cual refleja las rutas de comunicación entre los dominios locales y de servicios.

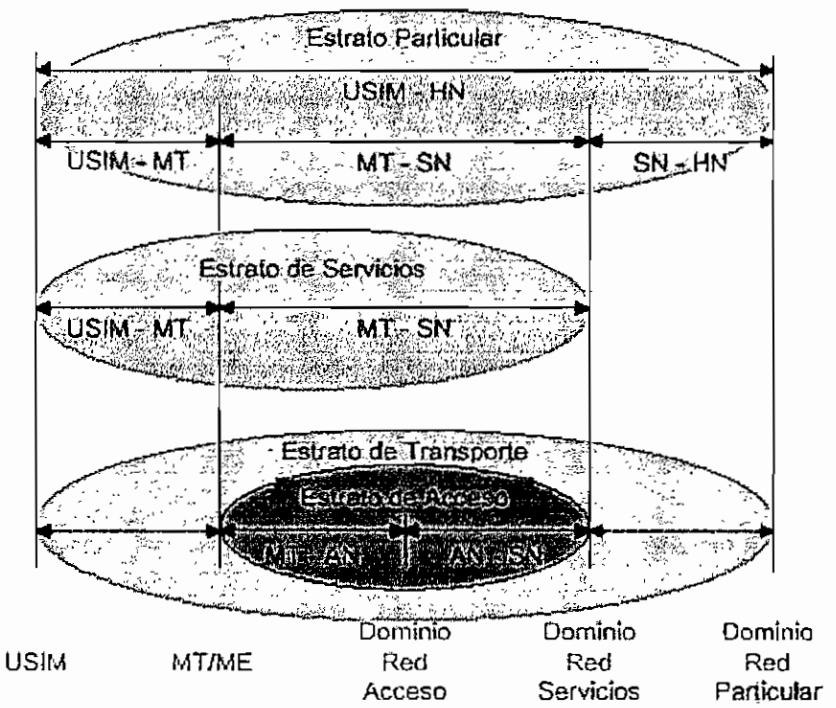


Figura1.9 Flujos funcionales entre los dominios de USIM, MT/ME, Red de Acceso, Red de Servicios y Red Particular

Los flujos directos entre dominios no contiguos son transportados a través de todos los dominios e interfaces localizados en los caminos de comunicación entre estos dominios finales. Las líneas punteadas indican que el protocolo usado no es específico de UMTS, en algunos casos pueden darse protocolos diferentes. De cualquier manera, para facilitar las capacidades del *roaming*, es deseable estar de acuerdo en los protocolos usados.

1.2.2 EVOLUCIÓN DE GSM HACIA UMTS

La evolución de las redes GSM hacia UMTS se basa en tres tecnologías que son:

- HSCSD (*High Speed Circuit-Switched Data*, Alta Velocidad de datos en Conmutación de Circuitos).
- GPRS (*General Packet Radio Service*, Servicios de Radio Generales de Paquetes).
- EDGE (*Enhanced Data-rates for GSM Evolution*, Aumento de la Tasa de Datos para la Evolución de GSM).

Estas diferentes etapas hacia UMTS se observan en la Figura 1.10.

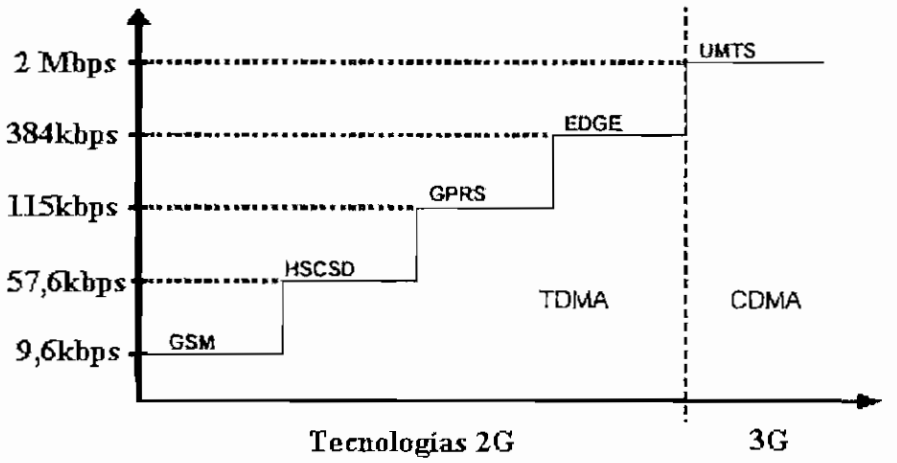


Figura 1.10 Evolución de GSM hacia UMTS

HSCSD (*High Speed Circuit-Switched Data*)

HSCSD aumenta la capacidad de transmisión de GSM agrupando hasta 8 ranuras de tiempo de un canal, con velocidades de Nx9,6 Kbps con valores de N desde 1 hasta 8. Aquí el número de ranuras de tiempo utilizado puede ser variable dependiendo de la saturación de la celda donde se encuentre el móvil, pero el ancho de banda no se utiliza eficientemente, pues se trata de una conmutación de circuitos. Aunque requiere pocas inversiones en red, no parece ser muy adecuado y su adopción no se está llevando a cabo, salvo en contadas ocasiones.

GPRS (*General Packet Radio Service*)

GPRS añade conmutación de paquetes a todos los niveles de la red GSM (radio, nodos de conmutación, red de transmisión, tasación, etc.) agregando nuevas entidades funcionales. Con GPRS 8 usuarios pueden compartir una única ranura de tiempo que antes se asignaba a uno sólo. Además, cada usuario puede utilizar hasta 8 ranuras de tiempo logrando 115 Kbps teóricos, aunque en la práctica son bastante menos. Requiere la instalación de nuevas entidades funcionales en la red GSM, como son los nodos SGSN y GGSN y hace un uso eficiente del ancho de banda, por lo que resulta la solución más adecuada.

EDGE (*Enhanced Data-rates for GSM Evolution*)

También llamado GSM384, utiliza un esquema de modulación 8PSK que alcanza velocidades de transmisión de 384 Kbps, o sea 48 Kbps por ranura de tiempo GSM. Tiene aplicación en ambiente urbano con movimientos lentos o casi estacionarios. Se acerca a las velocidades IMT-2000 (particularmente en exteriores), por lo que es una buena opción para aquellos operadores GSM que no han conseguido una licencia UMTS.

CAPÍTULO II

DESCRIPCIÓN DE LOS MECANISMOS DE SEGURIDAD EN UMTS

CAPÍTULO II

DESCRIPCIÓN DE LOS MECANISMOS DE SEGURIDAD EN UMTS

En la telefonía móvil el desarrollo de la seguridad representa un aspecto relevante para la provisión de servicios y para la satisfacción del usuario, por lo que es de mucha importancia realizar un estudio de aquella, especialmente en las redes UMTS, ya que representan el futuro de las comunicaciones sin cable.

Con este objetivo, en este capítulo se describe la especificación de seguridad en UMTS, y se estudia su arquitectura así como los mecanismos de seguridad implantados en esta red. Además de ello se realiza un análisis comparativo de la seguridad en UMTS con la del sistema de segunda generación GSM .

2.1 FINALIDAD DE LA SEGURIDAD EN LAS REDES MÓVILES

Las comunicaciones móviles, en el tramo de la estación móvil a la estación base requieren medidas de seguridad mucho mas severas que en el caso de una red alambrada convencional.

El enlace entre las estaciones base normalmente se realiza por cables (cobre, fibra óptica, etc.) con lo que se consigue algo más de seguridad. Sin embargo, las porciones finales que emplean canales de radio están abiertas a todo tipo de posibles escuchas clandestinas, así como a una posible suplantación tanto de la estación móvil emisora como la de la receptora.

En consecuencia, las funciones relacionadas a la seguridad de las redes móviles apuntan a dos metas:

- Proteger la red de accesos desautorizados
- Proteger la intimidad de los usuarios

Para evitar los accesos desautorizados a la red debe llevarse a cabo la autenticación de la identidad de cada usuario en el momento en el que accede a la red. Por otro lado, para preservar la intimidad de los usuarios, la información se transmite encriptada[1], evitando así posibles escuchas a través del canal. A continuación se explicará los principios de seguridad en las redes UMTS.

2.2 PRINCIPIOS DE SEGURIDAD EN UMTS

La tercera generación de redes celulares, como ya se mencionó en el anterior capítulo, ha anunciado una nueva era de comunicaciones inalámbricas de banda ancha que acoge un sinnúmero de servicios de entretenimiento e información, que no han sido posibles con la corriente tecnológica de la segunda generación. No obstante, en principio, los diseñadores encargados de la arquitectura de seguridad para UMTS han buscado construir sobre lo que ya está trabajando y funcionando eficazmente, particularmente en la infraestructura de GSM. Esto se debe porque tiene sentido construir sobre la tecnología probada; y también del hecho innegable que para un periodo de años UMTS tendrá que coexistir y operar con las redes de segunda generación.

Los grupos de trabajo responsables del desarrollo de la arquitectura de seguridad y protocolos para UMTS adoptaron tres principios básicos[2]:

a) La arquitectura de seguridad de UMTS se construirá sobre las características de seguridad de los sistemas de segunda generación. Esto

[1]Encriptar: Es el proceso de codificar un mensaje, mediante claves secretas conocidas por el emisor y el receptor, para garantizar la seguridad de la comunicación en su recorrido.
[2]Referencia [4]: 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.120, "Security Principles and Objectives".

quiere decir que se conservan las propiedades fuertes de los sistemas de 2G.

b) La introducción de UMTS mejorará la seguridad de los sistemas de segunda generación. Algunas dificultades y desventajas de los sistemas 2G serán modificadas.

c) La seguridad de UMTS también ofrecerá nuevas cualidades y nuevos servicios seguros no presentes en los sistemas 2G.

Tomando en cuenta los anteriores principios, los grupos de trabajo han perfilado que rasgos de los sistemas de segunda generación (específicamente GSM) serán retenidos, cuáles debilidades de la segunda generación deberían ser cambiados y en dónde la arquitectura de seguridad en UMTS introducirá nuevas capacidades. En los siguientes apartados se indicarán las fortalezas y debilidades de GSM desde la perspectiva de UMTS, así como las nuevas características de éste.

2.2.1 FORTALEZAS DE GSM DESDE LA PERSPECTIVA DE UMTS

Las características de seguridad de la segunda generación que serán confirmados por UMTS son los siguientes elementos del sistema:

- La autenticación del suscritor para el acceso al servicio: Los problemas con los algoritmos inadecuados han sido encaminados.
- La encriptación de la interfaz de radio: La fortaleza de encriptación es mayor que la de los sistemas de segunda generación, esto se debe a las amenazas planteadas por computadoras cada vez más potentes que en manos de personas indeseadas tratarían de realizar ataques a la red de comunicaciones.
- La confidencialidad de la identidad de suscriptor sobre la interfaz de radio.
- El SIM (módulo de identidad del suscriptor en GSM) como un módulo de seguridad trasladable (es decir, es una tarjeta inteligente).

- Las características de funcionamiento de la seguridad del sistema son independientes del usuario.

2.2.2 DEBILIDADES DE GSM DESDE LA PERSPECTIVA DE UMTS

Algunas de las características de los sistemas de 2G han sido encontradas débiles y deberían por tanto ser corregidas en 3G. Estas características son:

- El posible ataque al sistema usando una estación base falsa[1].
- La encriptación no se extiende hacia el CN (Core Network)
- Hay la posibilidad de secuestro de canal en redes que no ofrecen confidencialidad.
- Falta de uniformidad de encriptación y autenticación por el proveedor de servicios que crea oportunidades de fraude.
- Los mecanismos para la integridad de los datos son inexistentes. Tales mecanismos sumados al incremento de la fiabilidad del sistema proporcionarán protección contra la suplantación de estaciones base.
- El fraude y la intervención legal no fueron considerados en la fase de diseño de los sistemas 2G.
- Hay una ausencia de conocimiento de parte del HE[2] (ambiente local) de cómo el SN[3] usa los parámetros de autenticación para el seguimiento de los suscriptores.
- Los sistemas de segunda generación no tienen la flexibilidad para añadir y mejorar las funcionalidades de seguridad.

---

[1] Estación base falsa: Un delincuente simula el sistema móvil celular en cuestión, con una "estación base" que obliga activamente a los terminales móviles de sus cercanías a transmitir información secreta.
[2] HE (ambiente local): El HE es responsable por permitir a un usuario obtener servicios UMTS en un modo consistente, a pesar de la ubicación del usuario o el terminal usado
[3] SN (red de servicios): El SN proporciona al usuario el acceso a los servicios de HE.

2.2.3 NUEVAS CARACTERÍSTICAS DE SEGURIDAD EN UMTS

En marzo del 2000 el N. Asokan of the Nokia Research Center proporcionó un resumen de las nuevas características de seguridad para UMTS, las cuales se refieren a:

- Aumentar el apoyo para la seguridad y la encriptación de datos en el CN (*Core Network*).
- Aumentar las longitudes de las claves para combatir los ataques. Claves para la encriptación de la señal serán de 128 bits.
- Reforzar la confidencialidad de identidad de usuario a través del uso de diferentes parámetros de entrada.
- Suministrar el apoyo para la integridad de los datos así como la confidencialidad a través de los mecanismos de integridad y confidencialidad respectivamente.

Las características de seguridad antes mencionadas, constituyen el resultado del ambiente que poseerán los sistemas de tercera generación. Los puntos más importantes del entorno que existirá en tales sistemas son los siguientes:

a) Habrá nuevos y diferentes proveedores de servicios (operadores virtuales), en adición a los proveedores de servicios de telecomunicaciones inalámbricas. Estos incluirán servicios de datos, contenidos etc.
b) Los sistemas UMTS serán posicionados como los medios de comunicación preferidos por los usuarios, sobre los sistemas de líneas fijas.
c) Cada vez más habrá servicios prepago en lugar de las subscripciones post-pagadas.
d) Los usuarios habrán incrementado el control sobre su perfil de servicio y sobre las capacidades de sus terminales.
e) Los servicios de datos serán tan importantes o más que los servicios de voz.
f) Los teléfonos móviles serán usados como plataforma para el comercio electrónico.

2.3 SERVICIOS DE SEGURIDAD DE UMTS

Los servicios de seguridad están basados en tres principios básicos[1]:

- Autenticación
- Confidencialidad
- Integridad

2.3.1 AUTENTICACIÓN

La autenticación es suministrada para garantizar la identidad de un suscriptor. Un nodo que quiere autenticar a alguien tiene que mostrar su propia identidad. Esto puede hacerse mostrando la información solo a los nodos involucrados en la comunicación.

La autenticación en UMTS es dividida en dos partes:

- Autenticación del usuario hacia la red
- Autenticación de la red hacia el usuario.

Ambos procesos toman lugar dentro del intercambio de mensajes entre ellos, lo que reduce los mensajes de envió de un lado a otro. Después de estos procesos el usuario estará seguro de que la red a la que se conecta prestará los servicios y seguridades ofrecidos; mientras la red estará segura que la identidad exigida al usuario es la verdadera.

La autenticación es importante para otros mecanismos como la confidencialidad, e integridad tal como se apreciará en el desarrollo de este capítulo. Para la red de servicios (SN) es muy importante saber la identidad real del usuario por que así podrá estar seguro que se pagará por los servicios que está ofreciendo. El usuario por otro lado, quiere que la autenticación asegure que está pagando por los servicios que esta ocupando realmente.

[1] Referencia [5]: 3 rd Generation Partnership Project, 3G Security, UMTS 33.20, "Security Principles".

2.3.2 CONFIDENCIALIDAD

La confidencialidad en UMTS se logra cifrando las comunicaciones entre el suscriptor y la red, y refiriéndose al suscriptor por identidades temporales (local), en lugar de usar la identidad global IMUI. La confidencialidad del usuario es entre el suscriptor y el VLR/SGSN.

Las propiedades que deben ser confidenciales para evitar que un intruso acceda a la información del usuario en forma desautorizada son:

- La identidad del suscriptor
- La situación actual del suscriptor
- Los datos del usuario (ambos voz y datos deben ser mantenidos confidencialmente).

Si la Red de Servicios no apoya la confidencialidad de datos de usuario, el suscriptor debe ser informado y tiene la oportunidad de negarse a las conexiones.

2.3.3 INTEGRIDAD

A veces el origen de un mensaje tiene que ser verificado. Aunque este podría venir de una autenticación previa, el mensaje puede haber sido manipulado. Para evitar esto la protección a la integridad es necesaria.

El método para protección de integridad en UMTS es generar marcas que son agregadas a los mensajes. Las marcas pueden ser generadas solamente en los nodos que saben las claves secretas K. Ellas son almacenadas en el USIM y el AuC. Es muy importante ofrecer protección de integridad, ya que frecuentemente pueden existir varias entidades involucradas en la prestación de un servicio.

En la capa física, los bits son íntegramente chequeados por el checksum de CRC, pero estas medidas solo son incluidas para lograr comunicaciones de datos libres de errores a través del aire, y no son equivalentes a los niveles de integridad de transporte.

2.4 ARQUITECTURA DE SEGURIDAD EN UMTS[1]

Una de las metas para el diseño de la arquitectura de seguridad en UMTS es crear un marco que pueda evolucionar durante el tiempo. Por tal razón se han definido una serie de módulos llamados "Dominios", los cuales son un conjunto de capas asociadas a una serie de elementos, junto con la implementación de objetivos en esas capas. En la arquitectura de UMTS existen cinco de esos dominios. Estos son:

- Seguridad de acceso a red.
- Seguridad del dominio de red.
- Seguridad del dominio de usuario.
- Seguridad del dominio de aplicación.
- Visibilidad de seguridad y configurabilidad.

A continuación se realiza una explicación de cada uno de ellos.

2.4.1 SEGURIDAD DE ACCESO A LA RED

Son el conjunto de características de seguridad que proporcionan a los usuarios acceso seguro a la infraestructura de UMTS y en particular los protege contra los ataques a la conexión de radio. Los elementos (subdominios) importantes relacionados a este dominio son:

2.4.1.1 Confidencialidad de la Identidad de Usuario

En este subdominio la información de las identificaciones permanentes vinculadas al usuario son resguardadas contra escuchas. Dentro de la confidencialidad de la identidad de usuario se puede encontrar las siguientes características.

[1]Referencia[6]: 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.102, "Security Architecture".

Confidencialidad de la identidad de usuario (IMUI)

Evita que la identidad permanente de un usuario (IMUI), al que se le están ofreciendo determinados servicios, pueda obtenerse a partir de la conexión de radio.

Imposibilidad de seguimiento de usuario

Impide que un intruso pueda averiguar los servicios ofrecidos a un usuario concreto a partir de la conexión de radio

Confidencialidad de la ubicación de usuario

Previene que la presencia de un usuario a un área específica pueda ser descubierta en la conexión de radio.

Existen diversos mecanismos para conocer la identidad de usuario, el primero permite al usuario identificarse en el canal de radio por medio de una identidad temporal por la cual ya es conocido en SN., el segundo método permite al usuario identificarse por medio de una identidad permanente encriptada y el tercero le permite transmitir la identidad permanente sin encriptar.

Tanto el segundo como tercer mecanismo se aplican en el caso de que la identidad temporal de usuario no se conozca en SN.

A fin de no permitir el seguimiento de los servicios ofrecidos a un usuario, se obliga a no utilizar por mucho tiempo la misma clave temporal. Es necesario también, que cualquier dato de señalización o usuario que pueda revelar la identidad, se transmita en modo cifrado por la conexión de radio.

2.4.1.2 Autenticación de Entidad

Ambos, el terminal móvil y la estación base de la red de servicios se autentican el uno al otro, con el objetivo de prevenir ataques de personificaciones falsas de ambos lados de la comunicación.

Para lograr los objetivos mencionados se asume que la autenticación de usuario sucede en cada establecimiento de conexión entre red y usuario. Para ello se ofrece un mecanismo que utiliza un vector de autenticación[1] entregado por el HE del usuario a SN y establece una CK e IK[2] secretas entre el usuario y SN.

2.4.1.3 Confidencialidad de datos de usuario y datos de señalización

A través de una encriptación reforzada, tanto los datos de usuario como los relacionados a la señalización son protegidos sobre el enlace de acceso de red. Se proponen en UMTS las siguientes características de seguridad con respecto a la confidencialidad de datos.

Acuerdo de algoritmo de cifrado

Propiedad por la cual la estación móvil (MS) y la SN pueden negociar de forma segura el algoritmo a utilizar.

Acuerdo de clave de cifrado

Propiedad en la cual la estación móvil (MS) y la SN pueden fijar la clave a utilizar con el algoritmo de cifrado.

Confidencialidad de datos de usuario

Característica que permite la transmisión de los datos de usuario por la interfaz de radio sin peligro de escuchas.

Confidencialidad de datos de señalización

Característica que permite la transmisión de los datos de señalización por la interfaz de radio sin peligro de escuchas.

El establecimiento de la clave de cifrado se efectúa mediante el mecanismo de "autenticación y establecimiento de clave". La protección a la confidencialidad se

[1] Ver tabla 2.1.- Vector de autenticación.

[2] CK e IK: Son las claves secretas que forman parte del vector de autenticación, y que son usadas para realizar el proceso de confidencialidad e integridad respectivamente.

realiza mediante el mecanismo denominado "confidencialidad de conexión de acceso".

2.4.1.4 Integridad de datos

La entidad receptora en una sesión de comunicación es capaz de verificar que los mensajes recibidos no fueron alterados durante el recorrido, y si estos provienen de la parte exigida. Se ofrecen las siguientes propiedades relacionadas con la integridad de datos.

Acuerdo de algoritmo de integridad

Consiste en que el MS y SN pueden negociar seguramente el algoritmo de integridad.

Acuerdo de clave de integridad

Funcionalidad que permite fijar la clave de integridad a utilizar con el algoritmo de integridad.

Integridad de datos y autenticación del origen de datos de señalización

Propiedad por la cual la entidad receptora (MS o SN) es capaz de verificar que los datos de señalización no han sido alterados y que provienen de la entidad que lo proclama.

El acuerdo de claves de integridad se realiza mediante el mecanismo de "autenticación y de acuerdo de claves". La protección a la integridad se realiza mediante el mecanismo denominado "integridad de conexión de acceso".

2.4.1.5 Identificación de equipamiento móvil

En ciertos casos SN puede realizar una petición a MS para recibir la identidad del equipamiento móvil del terminal (IMEI)[1]. Esta identidad sólo se enviará después

[1] IMEI: Una identidad internacional del equipamiento móvil" es nn único número que se asignará a cada equipo uióvil por el fabricante de MS.

de proceder a la autenticación de SN. Por tal motivo, el IMEI debe guardarse seguramente en el terminal. Sin embargo, debido a la exposición de esta identidad a la red no es una característica de seguridad.

2.4.2 SEGURIDAD DEL DOMINIO DE RED

Es el conjunto de características de seguridad que permiten a los nodos de la infraestructura de red del proveedor intercambiar información de señalización con seguridad garantizada y además de ello proteger contra ataques a la red.

2.4.2.1 Autenticación de Entidad

Es la capacidad de los elementos de la infraestructura de red, incluyendo las diferentes partes de los proveedores de servicio, a autenticarse el uno al otro antes del intercambio de datos sensibles. Las siguientes características están relacionadas con la autenticación de elementos de red.

Acuerdo de mecanismo de autenticación

Propiedad por la que dos entidades de la red negocian de forma segura el mecanismo para autenticación y acuerdo de claves.

Autenticación de elemento de red

Propiedad por la cual un elemento de la red corrobora la identidad de otro.

Para conseguir estas propiedades se utiliza el mecanismo de autenticación de entidades, cada vez que se intercambian datos entre ellos.

24.2.2 Confidencialidad de datos

La protección de datos intercambiados entre elementos de red de posibles escuchas se logra vía encriptación. Las siguientes entidades son relacionadas con la confidencialidad de datos.

Acuerdo de algoritmo de cifrado

Propiedad por la cual dos elementos de red pueden negociar de forma segura el algoritmo a utilizar.

Acuerdo de clave de cifrado

Funcionalidad que permite a dos elementos de red, fijar la clave a utilizar con el algoritmo de cifrado.

Confidencialidad de datos

Propiedad por la cual los datos transmitidos entre dos elementos de red no pueden ser interpretados.

Las dos primeras entidades pueden conseguirse en el transcurso del proceso de autenticación de los elementos de red. La clave de cifrado fijada entre ambos, se utiliza posteriormente para proteger los datos de señalización y de usuario.

24.2.3 Integridad de datos y autenticación del origen de datos de señalización

Cuando un elemento de la red transmite información de señalización a otro, el nodo receptor puede confirmar que la información no se ha alterado en el recorrido, y que esta es originada del elemento de red del cual es informado como origen.

2.4.3 SEGURIDAD DEL DOMINIO DE USUARIO

Este dominio comprende al conjunto de características de seguridad, que aplican a la interacción entre un usuario y su terminal móvil. Una meta importante en este dominio es minimizar el daño y fraude que pueden ocurrir cuando un terminal móvil se roba. Los siguientes subdominios son relacionados con este dominio.

2.4.3.1 Autenticación de Usuario - USIM

Este subdominio tiene que ver con la relación entre un suscriptor individual y el módulo de identidad del suscriptor (USIM) en su terminal UMTS. Para poder acceder al USIM el propietario debe conocer una clave secreta como por ejemplo un PIN para iniciar una sesión de comunicación.

2.4..3.2 Conexión USIM -Terminal

Como la tarjeta inteligente que posee al USIM es removible, es necesario poseer una relación segura entre el USIM y el terminal UMTS. Esto se logra a través de una clave secreta compartida en el USIM y el terminal que es insertada por el proveedor de servicios cuando el servicio es inicializado. El enlace entre USIM-terminal previene que el USIM de un usuario sea insertado en otro terminal y usado sin autorización.

2.4.4 SEGURIDAD DEL DOMINIO DE APLICACIÓN

Este dominio comprende las características de seguridad que permiten un intercambio seguro de mensajes a nivel de aplicaciones entre el terminal y el sistema. En la arquitectura UMTS, la provisión necesita ser hecha por operadores de redes u otros proveedores de servicios para crear aplicaciones que residan sobre el USIM o el terminal. En este apartado se incluye :

Mensajes seguros entre USIM y red

Para facultar el desarrollo de aplicaciones residentes en USIM es necesario disponer de la certeza de la transmisión segura de mensajes entre la red y las aplicaciones, con el nivel de seguridad designado por el operador de red o el proveedor de la aplicación.

Confidencialidad de tráfico de usuario en la red

Este apartado comprende a las funcionalidades para la protección de los datos de usuario en toda la red (no sólo en la conexión de radio y en la red de acceso) contra el ataque de escuchas.

2.4.5 VISIBILIDAD DE LA SEGURIDAD Y CONFIGURABILIDAD

Es el conjunto de capacidades que el usuario del sistema utiliza para informarse de qué características de seguridad están en operación y qué servicios están siendo empleados, dando una certeza de los servicios de seguridad.

2.4.5.1 Visibilidad

El sistema a través de mecanismos proporcionados por la infraestructura UMTS, debe ser capaz de notificar el uso de confidencialidad en la red de acceso, confidencialidad en toda la red y el nivel de seguridad de la red visitada, a petición del usuario.

2.4.5.2 Configurabilidad

El usuario a través de mecanismos proporcionados por la infraestructura UMTS puede determinar que servicios de seguridad deben estar en operación antes que un usuario emplee un servicio. Esta lógica se puede aplicar, por ejemplo al habilitar y deshabilitar la clave personal PIN del USIM, o la decisión de aceptar llamadas que no son encriptadas.

La Figura 2.1 proporciona una ilustración del entorno global de UMTS en donde se muestra la interacción de los cinco dominios con los diferentes elementos del entorno.

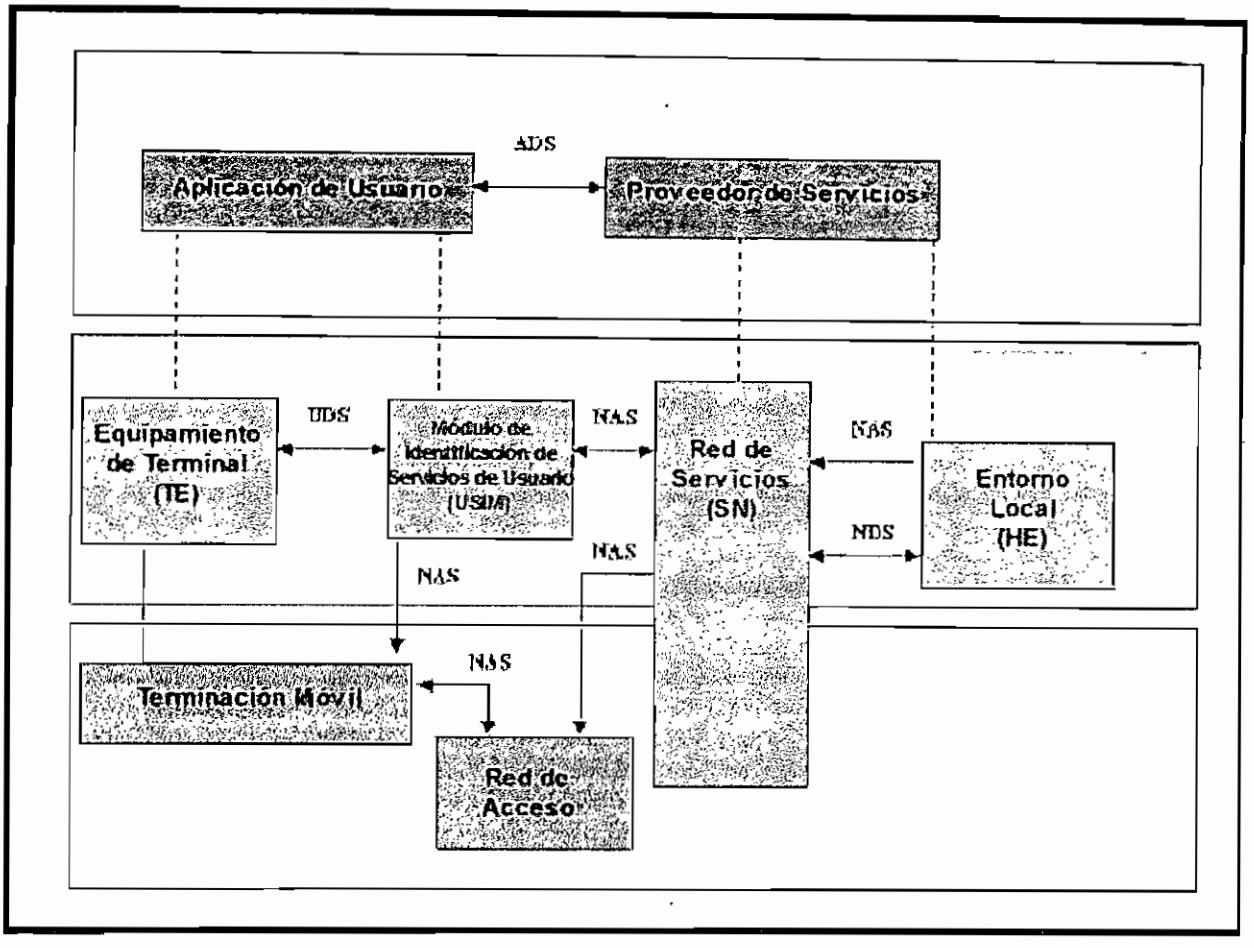


Figura 2.1 Relación de los diferentes dominios de seguridad en el entorno UMTS[1]

Las siguientes abreviaturas son empleadas por los dominios de seguridad en UMTS en la Figura 2.1.

NAS: Seguridad de acceso a red.

NDS: Seguridad del dominio de red.

UDS: Seguridad del dominio de usuario.

ADS: Seguridad del dominio de aplicación.

[1]Referencia [27]: Howard Wolfe Curtis, "Subscriber Authentication and Security in Digital Cellular Networks and Under the Mobile Internet Protocol", pág:112.

2.5 MECANISMOS DE SEGURIDAD EN UMTS[1]

2.5.1 IDENTIFICACIÓN POR IDENTIDAD TEMPORAL

Este mecanismo permite la identificación de un usuario por medio de la identidad de usuario móvil temporal (TMUI). Esta identidad sólo tiene sentido localmente, es decir, dentro de su área de ubicación en la que el usuario está registrado. Fuera de esta área TMUI debe ir acompañado de la identidad de área de ubicación (LAI) para evitar ambigüedades. La asociación entre la identidad temporal y la identidad permanente se guarda en el VLR/SGSN en el cual está registrado el usuario. El TMUI es usado para identificar al usuario sobre el acceso de radio.

El propósito de este mecanismo es asociar una nueva identidad (TMUI) a un usuario, para que sea conocido desde aquel momento por esta nueva identidad. Este procedimiento debe realizarse después del inicio del proceso de cifrado.

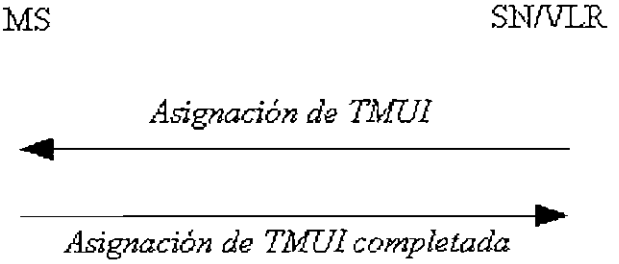


Figura 2.2 Asignación TMUI

El procedimiento de este mecanismo es el siguiente:

1) Primeramente es iniciado por el VLR, quien genera una nueva identidad temporal y guarda esta identidad y la identidad permanente (IMUI) en su base de datos. El TMUI debe ser imprevisible.

2) VLR envía el TMUI al usuario y, si fuera necesario el parámetro LAI.

[1]Referencia[6]: 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.102, "Security Architecture".

3) Al recibir la identidad temporal el usuario almacena esta información y elimina la asociación con la identidad TMUI previa. Posteriormente devuelve un ACK[1] a VLR.

4) Si recibe el ACK, VLR elimina la asociación con la identidad vieja (TMUIo) y el IMUI, si existía, de su base de datos.

5) Si VLR no recibe el ACK de una asignación exitosa de una identidad temporal del usuario, la red mantendrá la asociación entre la nueva identidad temporal IMUI-TMUIn y entre la vieja identidad temporal IMUI-TMUIo. En el caso de recibir un transacción originada por el usuario, la red permitirá al usuario identificarse bien por TMUIo o por TMUIn, lo que permitirá a la red determinar la identidad temporal almacenada en MS. La red mantendrá la asociación con la identidad de MS y eliminará la otra de su base de datos. Para transacciones originadas por la red, ésta identificará a MS por su identidad permanente (IMUI) y al establecer una conexión de radio forzará al usuario a eliminar cualquier identidad temporal almacenada. Cuando la red recibe un ACK de que han sido eliminadas las identidades temporales almacenadas en la estación móvil, borra cualquier asociación entre la identidad permanente y las posibles identidades temporales del usuario.

2.5.2 ACTUALIZACIÓN DE UBICACIÓN

En el caso de que sea el usuario quien se identifique utilizando TMUIo/LAIo, siendo el par asignado por el VLR visitado (VLRn), la identidad permanente, puede ser obtenida directamente de la base de datos.

En caso de que un usuario se identifica utilizando TMUIo/LAIo, no siendo el par asignado por el VLRn visitado, este intercambiará información con el anterior VLRo, (VLRn pedirá a VLRo la identificación permanente de usuario). Este mecanismo está integrado dentro del mecanismo de distribución de datos de

[1] ACK: Acuse de recibo

autenticación entre VLRs. Si VLRo no es accesible o no puede recuperar el IMUI, VLRn puede pedir la identidad permanente directamente al usuario.

2.5.3 IDENTIFICACIÓN POR IDENTIDAD PERMANENTE

Este mecanismo permite la identificación del usuario en el canal de radio mediante la identidad permanente del usuario (IMUI).

Este mecanismo es invocado por SN cuando el usuario no puede ser identificado por su identidad temporal y siempre que el usuario se registra por primera vez en una SN.

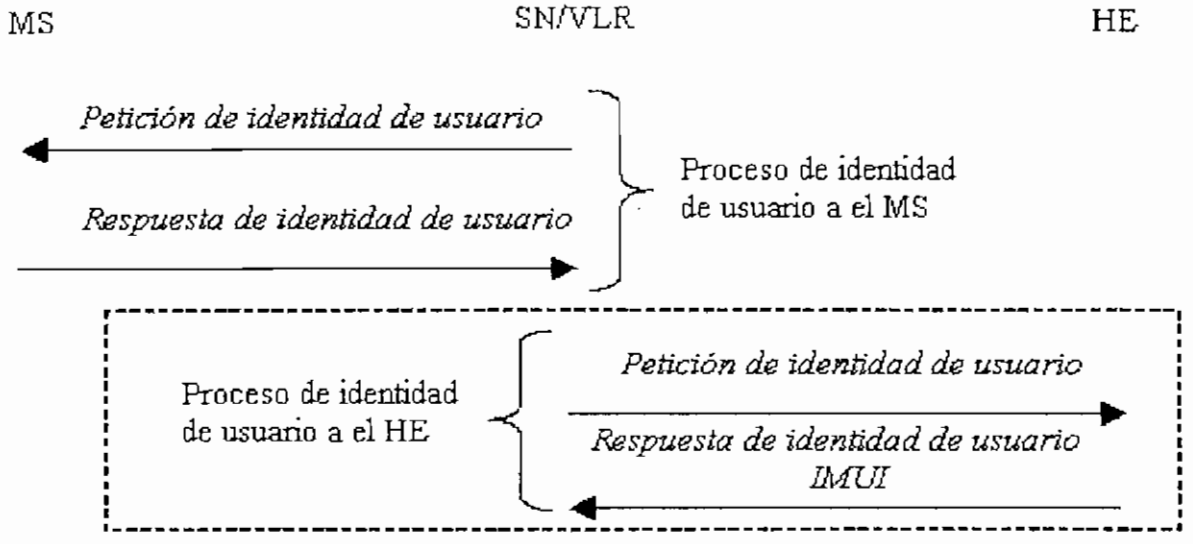


Figura 2.3 Ilustración de la identificación por identidad permanente

El proceso de este mecanismo se describe a continuación:

1) El mecanismo lo inicia SN/VLR quien realiza la petición al usuario de enviar su identidad permanente.

2) Si la estación móvil envía IMUI, el proceso ha finalizado. Si no es así, SN/VLR transmite EMSI (Identidad de suscriptor móvil encriptada) al HE con la petición de IMUI.

3) El HE deriva IMUI a partir de EMSI, y lo devuelve a SN/VLR.

2.5.4 AUTENTICACIÓN Y ACUERDO DE CLAVES (AKA)

Este mecanismo es usado por los sistemas móviles de tercera generación para la realización del proceso de mutua autenticación entre el equipamiento de usuario (UE) y la red de servicios (SN). Es por ello, que esta sección representa una parte importante en el desarrollo de esta tesis.
La autenticación y el acuerdo de claves toma lugar en el USIM , en el VLR y en el HLR/AuC[1]. Este proceso se observa en la Figura 2.4.

Los pasos para la autenticación y el establecimiento de claves son los siguientes:

1) El proceso de autenticación es iniciado por el SN/VLR que envía una petición de autenticación al HE.

2) El HE/AuC responde enviando una cadena ordenada de n vectores a SN/VLR. Cada vector de autenticación (AV) puede ser usado para lograr una autenticación y una sesión de establecimiento de claves entre el SN y el USIM en la estación móvil. Cada vector de autenticación consiste de cinco elementos que son mencionados en la siguiente tabla:

Tabla 2.1 Vector de autenticación (AV)

Parámetros que conforman el vector de autenticación (AV)	Descripción
RAND	Número aleatorio
XRES	Respuesta esperada
AUTN	Valor de autenticación usado para autenticar el SN a el UE.
CK	Clave de cifrado
IK	Clave de integridad

[1]Referencia [7]: 3 rd Generation Partnership Project, 3G Security, UMTS 33.22, "Universal Mobile Telecommunications System (UMTS); Security Features".

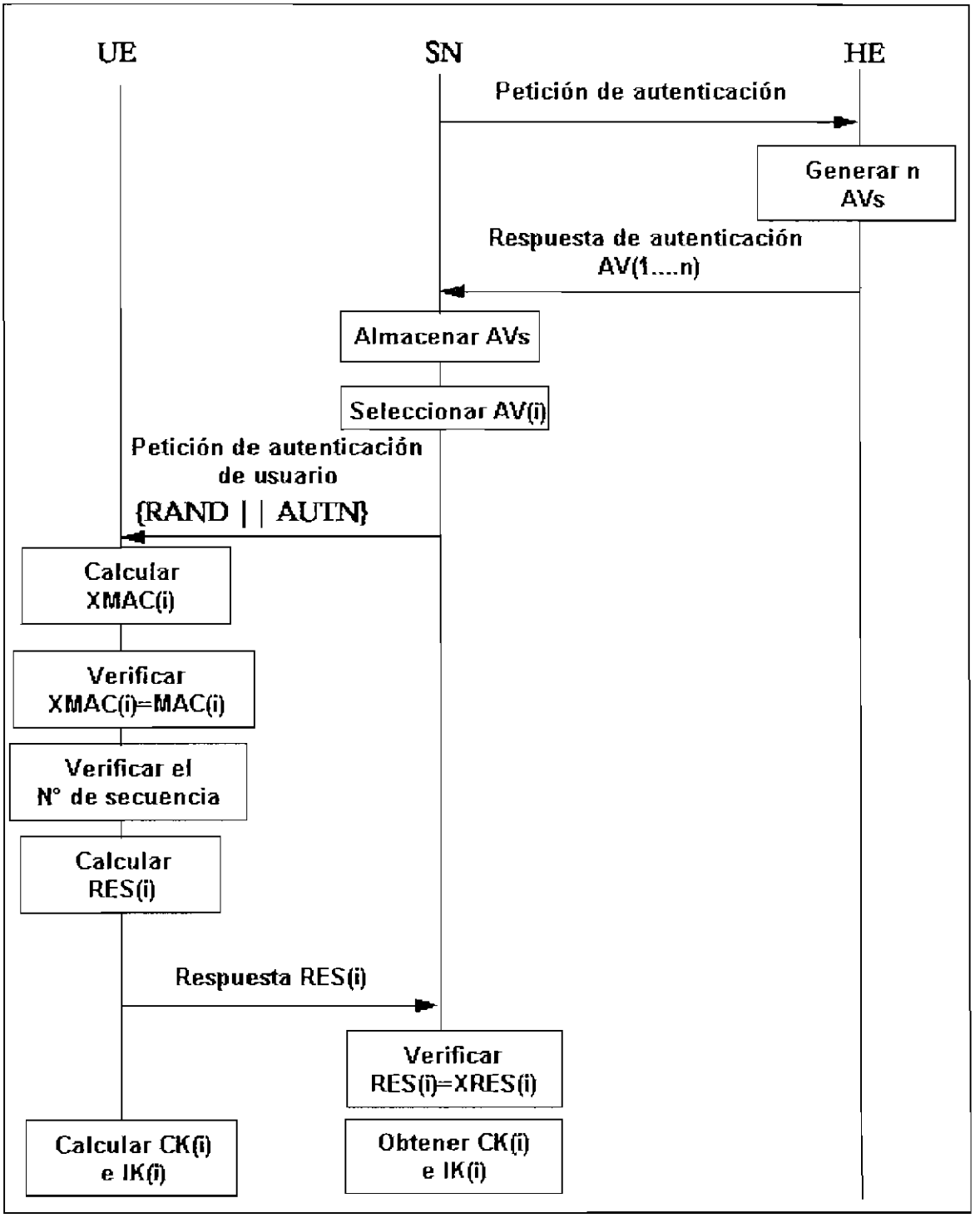


Figura 2.4 Esquema del proceso de autenticación y establecimiento de claves en el entorno de UMTS[1]

[1]Referencia [28]: Jonas Kullenwall, "Study of security aspects for Session Initiation Protocol", Linköping University, pág:58.

3) VLR/SGSN selecciona el siguiente vector de autenticación de la cadena y envía al usuario los parámetros RAND y AUTN.

4) El USIM extrae el valor MAC del parámetro AUTN y calcula su propio valor XMAC basado en la clave secreta K[1]. Si los valores MAC y XMAC son iguales entonces SN es autentificado por el usuario. Si son diferentes envía un mensaje "Rechazo de autenticación del usuario" indicando la causa y abandona el proceso, al recibir este mensaje VLR/SGSN inicia un proceso de "Reporte de fracaso en la autenticación" hacia HLR. VLR/SGSN puede decidir iniciar una nueva identificación y un nuevo proceso de autenticación con el usuario.

5) Antes que la estación móvil valide el parámetro AUTN, este verifica si el número de secuencia (SQN)[2] está en el rango correcto. Si no lo está envía un "Fracaso de sincronización" y abandona el proceso.

6) Si SQN es correcto, calcula RES =f2(RAND, K) y lo incluye en el mensaje "Respuesta de autenticación de usuario" que enviará a VLR/SGSN.

7) Al recibir el mensaje "Respuesta de autenticación de usuario", VLR/SGSN compara RES con el valor almacenado XRES del mismo AV, si son iguales la estación móvil ha sido autentificada.

8) Finalmente USIM calcula CK = f3(RAND, SQN, K) e IK = f4(RAND, SQN, K). El USIM guardará las claves CK e IK originales hasta la siguiente ejecución con éxito de AKA, así como también mantendrá el valor de RAND, con fines de resincronización. Mientras tanto, VLR/SGSN recupera las claves CK e IK del vector de autenticación. Las claves CK e IK son usadas para la protección de la confidencialidad e integrad sobre la interface de radio respectivamente.

---

[1] Clave K: Es la clave secreta compartida por el USIM y AuC. Esta clave es de mucha importancia dentro del proceso de autenticación y establecimiento de claves.

[2] SQN: es introducido para prevenir que la red trate de usar los mismos AVs para múltiples procesos de autenticación y generación de claves.

2.5.4.1 Distribución de datos de autenticación de HE a SN

El propósito de este procedimiento es enviar a VLR/SGSN una cadena de vectores de autenticación nuevos.

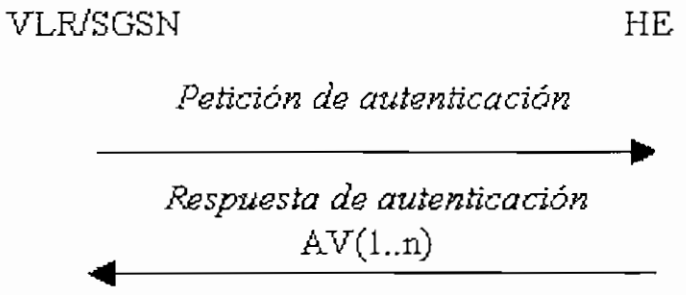


Figura 2.5 Distribución de información de autenticación de HE a SN

VLR/SGSN envía un mensaje de "Petición de autenticación". Al recibir la petición, HE/AuC envía la respuesta a VLR/SGSN conteniendo una cadena ordenada de vectores de autenticación AV(1..n).

2.5.4.2 Generación de vectores de autenticación (AV)

En UMTS para generar los diferentes valores que componen AV se utilizan cinco funciones, las mismas que son descritas en la Tabla 2.2.

Cuando se inicia el proceso de un nuevo AV es necesario la existencia de varios parámetros de entrada a las cinco funciones, por lo que el AuC primeramente genera un número nuevo SQN y un valor aleatorio RAND. A más de las entradas antes mencionadas son necesarias la clave secreta compartida K y el campo de autenticación y gestión de claves AMF para un correcto funcionamiento de las diferentes funciones (Figura 2.6).

Tabla 2.2 Funciones para la generación de (AV)

Función	Descripción
f1	Función de autenticación para calcular MAC
f2	Función de autenticación de mensajes para calcular RES y XRES
f3	Función generadora de claves utilizada para calcular CK (clave de cifrado)
f4	Función generadora de claves utilizada para calcular IK (clave de integridad)
f5	Función generadora de claves utilizada para calcular AK

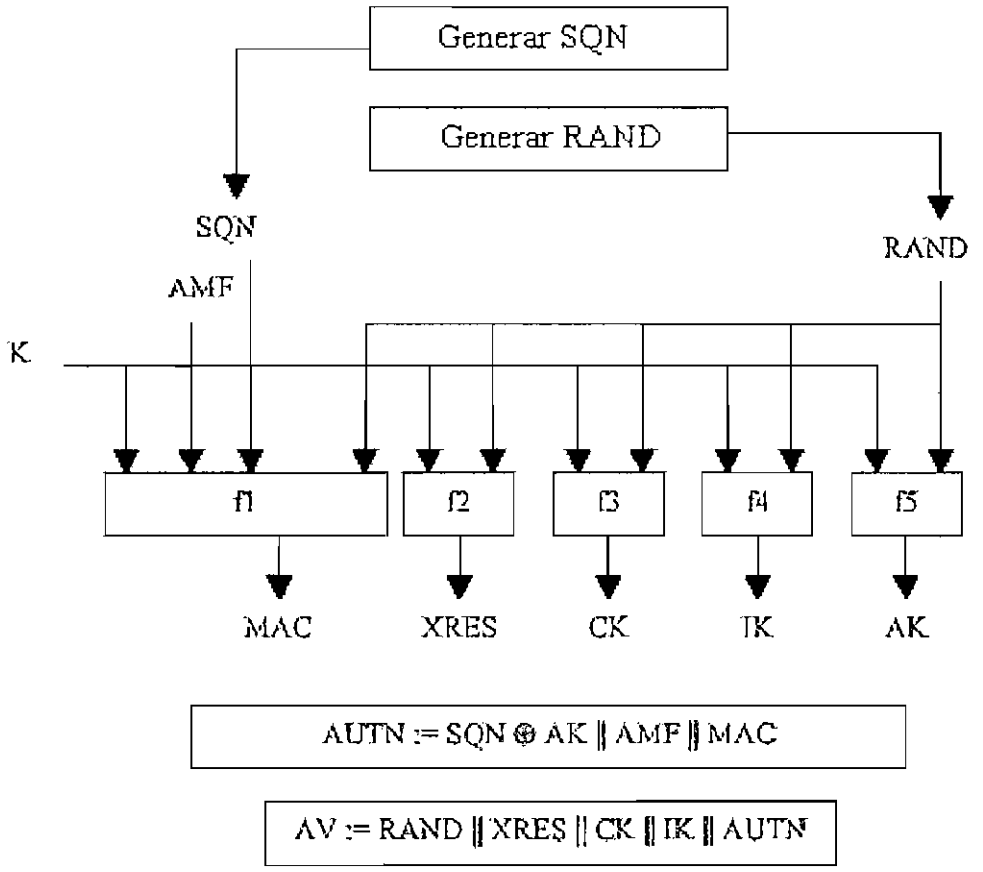


Figura 2.6 Generación de vectores de autenticación

Las funciones antes mencionadas conjuntamente con las entradas generan los siguientes valores[1]:

MAC = f1(SQN, RAND,AMF,K)

XRES = f2(RAND, K).

CK = f3(RAND, K)

IK = f4(RAND, K)

AK = f5(RAND, K)

Una vez generados los anteriores valores, se obtienen el valor de autenticación AUTN y el vector AV respectivamente. Es importante indicar que para obtener el valor de AUTN se hace mención a los símbolos ⊕, ||, en donde:

- El símbolo ⊕ representa una operación de seguridad entre dos diferentes parámetros. El objetivo es que uno de los parámetros enmascara al otro, es decir que a través de esta operación se obtiene un valor diferente a los otros dos, por lo que es imposible la consecución de los parámetros iniciales si no se cuenta con uno de ellos.
- El símbolo de concatenación || representa que un cierto parámetro está conformado por varios valores y que pueden ser obtenidos independientemente en el receptor.

A continuación se indicará los parámetros que conforman el valor AUTN en una forma más detallada.

SQN⊕AK

El propósito de realizar la operación OR exclusiva entre SQN y la clave de anonimato AK es enmascarar al SQN, esto quiere decir hacer más difícil la obtención de este parámetro a personas indeseadas.

[1]Referencia[6]: 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.102, "Security Architecture".

AMF

En el valor de autenticación de cada vector de autenticación, se incluye un campo de autenticación y gestión de claves, AMF. Este campo puede tener diferentes usos, puede ser utilizado para indicar el algoritmo y la clave a utilizar, puede usarse ,en otros casos, para indicar la diferencia máxima admisible entre SEQ_{MS} y SEQ_{HE}[1].

MAC

Como ya se mencionó anteriormente el parámetro MAC es usado por la estación móvil para auntenticar a la SN. Cuando el USIM recibe el MAC, este lo compara con el XMAC que es generado localmente. Si son iguales el USIM ha autentificado que el par RAND AUTN es originado en su HE.

Con los valores descritos se construye el valor de autenticación AUTN.

$$AUTN = SQN \oplus AK \,||AMF\, ||MAC.$$

Finalmente ya con todos los parámetros se genera el vector de autenticación.

$$AV = RAND\, ||XRES\, ||CK\, ||IK\, ||\, AUTN$$

El AUTN es generado en el AuC y enviado con el número aleatorio RAND al VLR/SGSN .

2.5.4.3 Distribución de datos de autenticación dentro de una red de servicios

El propósito de este procedimiento es dar a un MSC/VLR o SGSN nuevo los datos de autenticación de un MSC/VLR o SGSN previamente visitado dentro del mismo dominio de red de servicios.

La Figura 2.7 muestra el proceso a seguir estudiado en esta tesis.

[1]SEQ: Es un contador secuencial, encargado de verificar si el número de secuencia (SQN) está en el rango correcto.

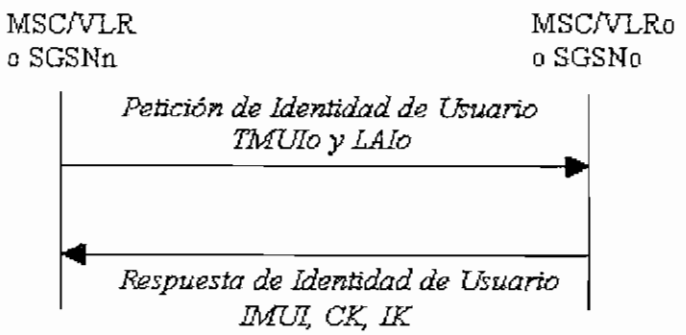


Figura 2.7 Distribución de datos de autenticación en un dominio de red de servicios

MSC/VLRn o SGSNn inicia el proceso después de recibir una petición de actualización de ubicación del usuario, donde el usuario esta identificado por medio de una identidad temporal de usuario TMUI y la identidad de área de localización LAI.

MSC/VLRo o SGSNo pertenece a la misma red de servicios que MSC/VLRn o SGSNn. Los pasos seguidos en el proceso son:

1) MSC/VLRn (o SGSN) envía un mensaje "Petición de Identidad de Usuario" al MSC/VLRo (o SGSNo) conteniendo TMUIo y LAIo.

2) MSC/VLRo (SGSNo) busca la información en la base de datos, si la encuentra envía un mensaje "Respuesta de Identidad de Usuario" conteniendo IMUI, el número de vectores de autenticación no utilizados y puede incluir también el contexto de seguridad actual CK, IK. Después de la transmisión del mensaje elimina los vectores de autenticación enviados y los elementos del contexto de seguridad actual. Si no encuentra la información requerida envía un "Respuesta de Identidad de Usuario" indicando que la identidad del usuario no es accesible.

3) Si MSC/VLRn o SGSNn reciben un mensaje conteniendo IMUI, crean una entrada y almacenan la información recibida. Si no ha sido posible identificar al usuario, se inicia un proceso normal de identificación.

2.5.4.4 Proceso de Resincronización[1]

El proceso de resincronización toma lugar siempre que los números de secuencia del USIM y del AuC no estén dentro del rango específico. La diferencia entre ellos se descubre en el USIM cuando este compara el SQN_{HE} recibido con el SQN_{MS} guardado. A continuación se indica el análisis de este proceso:

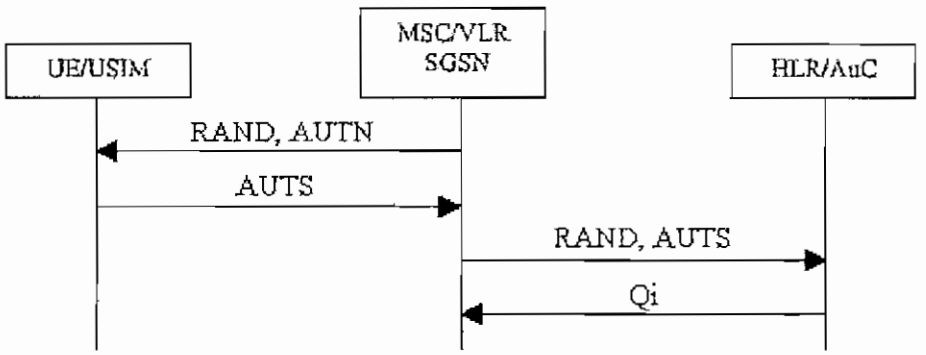


Figura 2.8 Mecanismo de resincronización

1) El VLR/SGSN envía un "Petición de autenticación de usuario (RAND y AUTN)" al USIM.

2) USIM verifica que SQN_{HE} esté dentro del rango de SQN_{MS}. Si SQN_{HE} está fuera de rango, el USIM genera el valor de autenticación de sincronización AUTS[2].

3) Cuando el USIM encuentra que el número de secuencia del AuC está fuera de rango envía al VLR/SGSN un "Fracaso de sincronización" conjuntamente con AUTS.

4) VLR/SGSN envía un "Petición de autenticación" con un indicador de error de sincronización a AuC junto con los parámetros, RAND enviado a MS en la petición

[1]Referencia [8]: 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.105, "Cryptographic Algorithm Requirements".

[2] Dentro del parámetro AUTS se encuentra el número de secuencia SQN_{MS} que será enviado al AuC para continuar el proceso de resincronización. Se debe indicar que SQN_{MS} es enmascarado por AK, y además AUTS está conformado por el parámetro MACS (AUTS = $SQN_{MS} \oplus AK \| MACS$).

de autenticación de usuario previa y AUTS recibido por VLR/SGSN en respuesta a la petición hecha al usuario.

5) Cuando AuC recibe AUTS, este obtiene el valor SQN_{MS} y verifica que este en el rango correcto. Si lo está envía a VLR/SGSN un mensaje "Respuesta de autenticación" con un conjunto de vectores de autenticación (Qi) que se encontraban almacenados y que se tiene la certeza que serán aceptados por el USIM.

6) Si SQN_{MS} no está en el rango correcto, AuC reajusta el valor de SQN_{HE} a SQN_{MS} y envía un mensaje "Respuesta de autenticación" con un nuevo conjunto de vectores de autenticación (Qi) a VLR/SGSN.

7) VLR/SGSN al recibir los nuevos vectores de autenticación elimina los anteriores para ese usuario.

2.5.5 NOTIFICACIÓN DE ERRORES DE AUTENTICACIÓN DE SGSN/VLR A HLR

El objetivo de este mecanismo es notificar a HLR los errores producidos durante el proceso de autenticación (Figura 2.9).

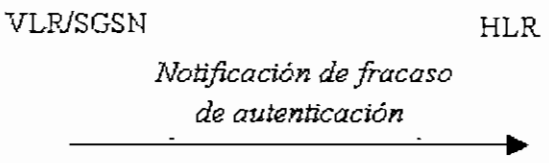


Figura 2.9 Notificación de error de autenticación

El proceso es invocado por VLR cuando el proceso de autenticación fracasa. Los reportes de error de autentificación deben contener:

- El código de causa de fracaso. Las posibles causas de fracaso son cualquier característica de la red que estuvo equivocada o la contestación del usuario que estuvo equivocada.
- La dirección de VLR/SGSN.
- RAND. Este número identifica al AV que fracasó en la autenticación

La recepción de un mensaje de error puede inducir a HLR a cancelar la ubicación de un usuario y además puede almacenar los datos recibidos para que sean procesados con la intención de detectar posibles situaciones de fraude que pudieran realizarse.

2.5.6 ESTABLECIMIENTO DE CONEXIÓN

Para establecer una conexión entre la red y la estación móvil, esta debe indicar a la red la clase de MS/USIM y los algoritmos de cifrado e integridad que soporta.

La red comparará sus capacidades y preferencias de integridad así como los requerimientos de suscripción del MS, a partir de estos datos actuará según las siguientes reglas:

1. Si el MS y la red no tienen versiones de UIA (algoritmo de integridad de UMTS) comunes, la conexión finalizará.
2. Si existe al menos una versión de UIA común, la red seleccionará una de ellas para aplicar a la conexión.
3. Si el MS y la red no tienen versiones de UIA comunes y la red puede utilizar una conexión no protegida, se usará este modo.

La red comparará sus capacidades y preferencias de cifrado así como los requerimientos de suscripción del MS, a partir de estos datos actuará según las siguientes reglas:

1. Si el MS y la red no tienen versiones de UEA (algoritmo de encriptación de UMTS) comunes ni está preparada para usar una conexión no cifrada, la conexión finalizará.
2. Si existe al menos una versión de UEA común, la red seleccionará una de ellas para aplicar a la conexión.
3. Si el MS y la red no tienen versiones de UEA comunes y la red puede utilizar una conexión no cifrada, se usará este modo.

Debido a la separación de gestión de movilidad para servicios PS y CS, un dominio de CN puede, independientemente del otro, establecer una conexión con un MS. El cambio de los algoritmos de cifrado y de integridad en el establecimiento de una segunda conexión MS-CN no está permitido. Las preferencias y requerimientos especiales para el modo de integridad y cifrado deben ser iguales para ambos dominios.

2.5.6.1 Tiempo de vida de clave de cifrado y clave de integridad

Para asegurar que claves viejas no sean usadas por un periodo ilimitado de tiempo, el USIM mantiene contadores que delimita el número máximo de veces que puede ser utilizada una clave (indican cuantas veces han sido usadas las claves).

El límite máximo para el uso de las claves es definido por el operador y cuando el USIM encuentra que estas han sido usadas por mas tiempo de lo permitido, esto permitirá al VLR/SGSN usar nuevos vectores de autenticación.

2.5.6.2 Identificación de clave de cifrado y clave de integridad

La identificación de las claves se realiza mediante KSI (identificador de conjunto de claves). KSI es un número asociado con las claves de integridad y cifrado derivadas en el proceso de autenticación y la red lo envía junto con el mensaje "Authentication request".

La finalidad de KSI es permitir a la red identificar las claves de integridad y cifrado sin necesidad de lanzar un proceso de autenticación. Esto permite la reutilización de las claves en los siguientes establecimientos de conexión.

2.5.7 CONFIDENCIALIDAD DE CONEXIÓN DE ACCESO

Los datos de usuario y alguna información de señalización necesitan protección de confidencialidad. La necesidad de tal protección en la transmisión es realizada por medio de una función de confidencialidad (f8) que es aplicada sobre canales dedicados entre UE y RNC.

En la Figura 2.10 se observa el uso del algoritmo de cifrado f8.

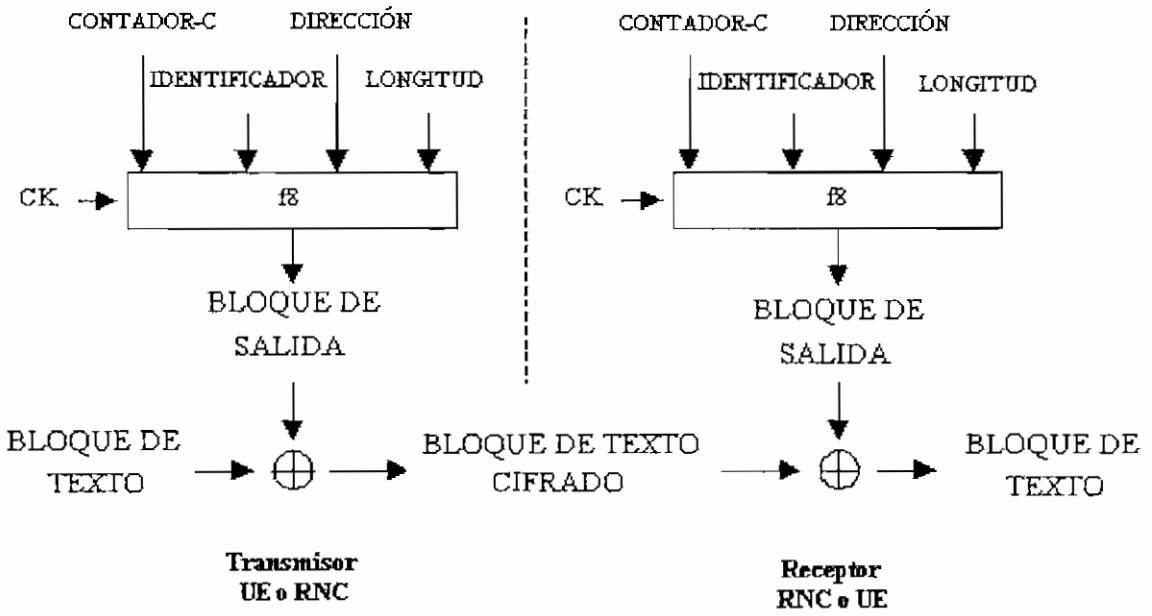


Figura 2.10 Algoritmo de cifrado f8

La función f8 mediante los parámetros de entrada genera un bloque de salida, el cual enmascara a la información del usuario denominado como bloque de texto. Después de este procedimiento se envía la información cifrada a través de la interfaz de radio Uu.

Tabla 2.3 Parámetros de entrada para el algoritmo de cifrado

Parámetros	Descripción
CONTADOR-C (*COUNT-C*)	Contador variable en el tiempo
CK	Clave de cifrado
IDENTIFICADOR (*BEARER*)	Identificador de canal lógico
DIRECCIÓN (*DIRECTION*)	Dirección de transmisión
LONGITUD (*LENGTH*)	Longitud del flujo

El contador *COUNT-C* es incrementado en cada mensaje enviado o recibido protegido por confidencialidad. Existen contadores separados para el enlace ascendente y para el enlace descendente. Esto junto con el identificador de dirección (*DIRECTION*), aseguran que los parámetros de entrada nunca sean los mismos dentro de una conexión.

La clave de cifrado CK es generada en el AuC y enviada al VLR/SGSN como parte del AV. Cuando la autenticación del suscriptor ha sido completada exitosamente, la clave es enviada del VLRN/SGSN al RNC. El USIM genera la clave de cifrado durante el proceso de autenticación.

El identificador de canal lógico *BEARER* es utilizado para distinguir entre los diferentes portadores lógicos de radio asociados con el mismo usuario sobre el mismo enlace físico. Esto se realiza para evitar tener los mismos parámetros de entrada.

El identificador de dirección es usado para distinguir entre los mensajes que se envían de los que se reciben, para prevenir que la función use los mismos parámetros de entrada. El identificador de dirección posee el valor 0 para mensajes que van desde el USIM al RNC (enlace ascendente), y posee valor 1 para los mensajes que van desde el RNC al USIM (enlace descendente).

El parámetro longitud de flujo *LENGTH* es utilizado para dar la longitud del bloque de salida.

2.5.8 INTEGRIDAD DE CONEXIÓN DE ACCESO

En su mayoría los mensajes de señalización de control que se envían entre la estación móvil y la red son considerados sensibles y deben ser protegidos por integridad.

Sobre los mensajes transmitidos entre la estación móvil y la red, se aplicará una función de algoritmo de integridad (f9) sobre la información de señalización. La protección por integridad es obligatoria para los mensajes de señalización en UMTS.

La función f9 añade una marca a los mensajes para asegurar que sean generados en el USIM o en SN en nombre de HE, esto asegura que el mensaje no sea modificado.

La integridad consistirá en la generación de un MAC por mensaje. El proceso de generación se puede observar en la Figura 2.11.

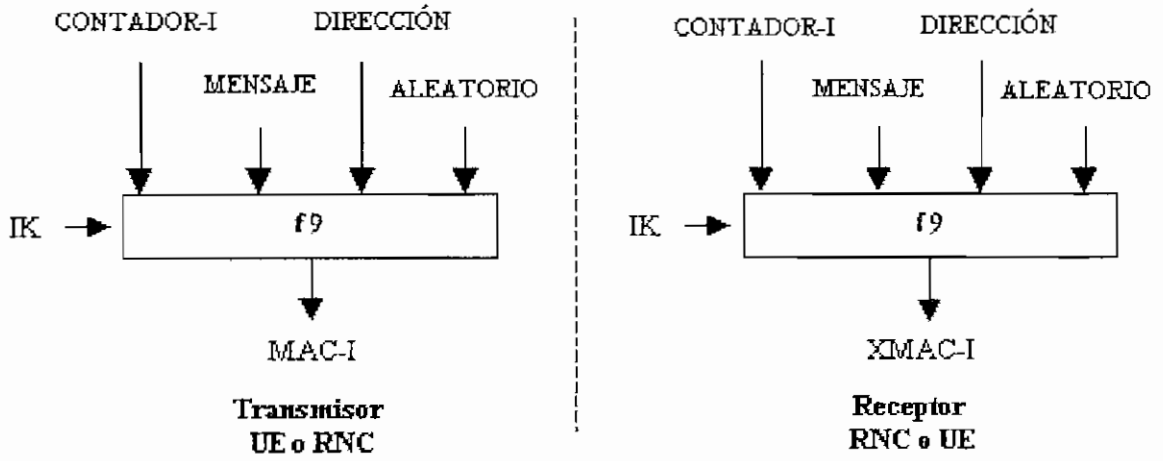


Figura 2.11 Método para la protección por integridad

Tabla 2.4 Parámetros de entrada a la función f9

Parámetro	Descripción
CONTADOR-I (*COUNT-I*)	El número de secuencia de integridad
IK	Clave de integridad
ALEATORIO (*FRESH*)	Número aleatorio generado por la red
DIRECCIÓN (*DIRECTION*)	Bit de dirección: 0 (UE→RNC) o 1 (RNC→UE)
MENSAJE (*MESSAGE*)	Mensaje de señalización

A partir de los parámetros que se indican en la Tabla 2.4, el usuario calcula el MAC asociado al mensaje con la función f9. Una vez calculado el MAC se añade al mensaje y se envía por la conexión de acceso a radio.

El receptor calcula XMAC-I sobre el mensaje recibido y verifica el resultado comparándolo con el MAC-I del mensaje.

El contador *COUNT-I* es incrementado por cada mensaje protegido por integridad. Hay contadores separados para el enlace ascendente y el descendente y, junto con el bit de dirección, aseguran que los parámetros de entrada nunca permanezcan dentro de la misma conexión, previniendo la repetición de ataques.

La clave de integridad IK se genera en el AuC y el USIM. El VLR/SGSN recibe el IK en el AV del AuC, y lo envía al RNC después de autenticar el USIM.

El parámetro aleatorio *FRESH* se usa para proteger a la red contra la repetición de ataques. Un valor *FRESH* es asignado a cada usuario y es generado por RNC. El tiempo de vida de un valor *FRESH* es la duración de una conexión y un nuevo *FRESH* se generará para la próxima conexión.

El bit de dirección se usa para distinguir a los mensajes que se envían de los mensajes que se reciben. Esto tiene como objetivo prevenir que los mensajes que se envían usen los mismos parámetros de entrada que los mensajes que se reciben. El bit de dirección posee el valor 0 para los mensajes del USIM al RNC

(enlace ascendente), y valor 1 para los mensajes del RNC al USIM (enlace descendente).

El propio mensaje (*MESSAGE*) es una entrada importante a la función. Sólo haciendo esto, la integridad del mensaje puede protegerse. Si cualquiera cambia el mensaje entre el transmisor y el receptor, este último no conseguirá un XMAC-I igual al MAC-I recibido. Esto hará que el receptor simplemente rechace el mensaje.

2.6 ANÁLISIS DE LA SEGURIDAD EN UMTS EN COMPARACIÓN CON GSM

En este apartado se pretende realizar un pequeño análisis de la seguridad en UMTS teniendo como comparación el sistema de segunda generación GSM.

ENCRIPTACIÓN EN LA INTERFAZ DE RADIO

En el sistema de segunda generación GSM, la encriptación de la interfaz de radio es solamente entre la estación base y el móvil. Además de ello, muchas de las estaciones base son conectadas a los controladores de las estaciones base por enlaces de microonda que rara vez están cifradas. Por ello en UMTS el RNC debe ser responsable por la confidencialidad en lugar del Nodo B para evitar las debilidades de los sistemas 2G antes mencionadas.

NODOS QUE ESTÁN A CARGO DE LAS CLAVES

La integridad y la protección a la confidencialidad son ejecutadas en las estaciones base en el sistema GSM, pero en UMTS son realizadas en el CN, por lo que se reduce el número de nodos que almacenan las claves de cifrado e integridad. Este punto es muy importante ya que si pocos nodos se ocupan de las claves es más fácil controlar su uso. Por tal motivo en UMTS se debe tener un control estrito sobre los nodos que poseen las claves CK e IK.

AUTENTICACIÓN

La autenticación del usuario en UMTS es realizada de una manera similar a la autenticación en GSM.

El problema de las falsas estaciones base en GSM es causada por la carencia de autenticación de la red por parte del usuario. Las estaciones falsas son un gran problema, ya que los suscriptores GSM pueden usar esa estación pero sin confidencialidad ni ninguna autenticación, por lo que se podría obtener toda la información del usuario. En cambio en UMTS se evita este problema haciendo que la autenticación sea entre usuario y red, y viceversa, con lo que la seguridad aumenta considerablemente.

OPERACIONES DE SEGURIDAD

En UMTS las operaciones de seguridad son independientes del usuario. El USIM y la red automáticamente realizarán los mecanismos de AKA, uso de la integridad y la protección de la confidencialidad. Esto es similar en GSM, pero una característica extra es añadida en UMTS; esta es que el usuario disponga de mayor visibilidad de las operaciones de seguridad disponibles. Para ello se dispondrá de:

- *Indicación de encriptación en la red de acceso*, propiedad que permite al usuario conocer si los datos de usuario están protegidos por confidencialidad en la conexión de red de radio, en concreto cuando se establecen llamadas no cifradas.

- *Indicación de encriptación completa*, propiedad que permite al usuario conocer si los datos de usuario están protegidos por confidencialidad en todo el camino de comunicación.

- *Indicación del nivel de seguridad*, propiedad que permite al usuario conocer el nivel de seguridad que ofrece la red visitada, en particular cuando el usuario se mueve a una red con inferior nivel de seguridad (3G a 2G).

Por lo anteriormente mencionado, los terminales UMTS deben ofrecer la posibilidad de que sean configurados por el usuario; es decir, que se tenga la confirmación visual de qué nivel de seguridad poseen los servicios que se están ofreciendo, para que el usuario tenga la posibilidad de utilizarlos o no.

PROTECCIÓN A LA INTEGRIDAD

La protección a la integridad en UMTS se realiza obligatoriamente sobre los mensajes de señalización y no necesariamente a los datos de usuario. Los mensajes que han sufrido modificaciones sin la autorización debida serán borrados en el lado del receptor y rechazados, haciendo que protocolos de alto nivel realicen la petición de retransmisión. Los datos de usuario deben ser siempre protegidos por confidencialidad, ya que así de una manera indirecta son protegidos por integridad. Mientras tanto en los sistemas 2G el servicio de integridad no es ofrecido.

MECANISMO DE ENCRIPTACIÓN

El mecanismo de encriptación en UMTS es más "sólido"[1] que el existente en 2G, por ejemplo la longitud de las claves en UMTS está sobre los 128 bits mientras que en GSM está alrededor de los 64 bits[2].

2.7 POSIBLES AMENAZAS A LA SEGURIDAD EN UMTS[3]

Las posibles amenazas en el sistema de comunicaciones UMTS pueden ser relacionadas según el punto de ataque a la red. Es por ello que en este proyecto de titulación se ha considerado que las amenazas en UMTS son las que se indican a continuación.

---

[1]Se considera el término sólido como una combinación entre el diseño del algoritmo de encriptación y la longitud de la clave.
[2]Referencia [30]: Arturo Quirantes, "La seguridad de los teléfonos móviles".
[3]Referencia [9]: 3rd Generation Partnership Project, 3G Security, 3GPP TS 21.133, "Security Threats and Requirements".

2.7.1 AMENAZAS ASOCIADAS AL TERMINAL DE USUARIO

Integridad de datos

Intrusos o personas desautorizadas al uso de un terminal móvil pueden modificar o borrar datos almacenados en el terminal, lo que puede dar como resultado el acceso desautorizado a éste. Esto se logra debido a que al poseer información diferente a la original el terminal puede recibir mensajes falsos como por ejemplo una petición de identidad permanente sin que éste se de cuenta de ello.

Una medida preventiva a la amenaza antes mencionada sería repeticiones del mecanismo de autenticación con una determinada frecuencia de tal manera que el intruso no tenga la oportunidad de reunir la cantidad de información necesaria para descifrar los datos secretos del usuario.

Robo de terminal y la tarjeta USIM

Debido a que el equipo terminal es cada vez más pequeño y ligero es susceptible a que más fácilmente sea robado. Esto conllevará a plantear dos escenarios:

- Robo del terminal sin la tarjeta USIM
- Uso de un terminal con la tarjeta USIM robada.

El robo del terminal sin la tarjeta USIM implicará una pérdida para el propietario con respecto al valor del terminal. Si el robo incluye la tarjeta USIM, entonces la pérdida es mayor ya que el ladrón podrá acceder y cargar el pago de todos los servicios que el usuario ha contratado con su proveedor.

Además es importante mencionar que una manera de efectuar fraude incluso con terminales desautorizados por el proveedor de servicios sería en manipular la identidad del terminal IMEI e insertar una tarjeta USIM válida, con lo que se tendría acceso a los servicios que el proveedor ofrece.

Las medidas para estas amenazas serían:
Informar al proveedor de servicios del robo para que éste no conecte las llamadas con el terminal o la tarjeta USIM robados.

El uso de un número de identidad personal PIN para que un intruso no pueda utilizar la tarjeta USIM.

Terminal y tarjeta USIM prestados

Otra amenaza es de que el propietario presta su terminal y su tarjeta USIM a personas que emplean mal sus privilegios, quizás excediendo las limitaciones de uso convenidas.

Clonación de la tarjeta USIM

La clonación de la tarjeta USIM es la amenaza que consiste en que los intrusos pueden obtener parámetros importantes como la identidad permanente del usuario (IMUI), la clave secreta K, etc. La manera que un delincuente puede hacer esto es tener físicamente la tarjeta USIM a través del robo momentáneo sin que el usuario se de cuenta de ello, con lo cual el delincuente podría escuchar las llamadas de los suscriptores e incluso efectuar llamadas que serían cargadas a la cuenta del suscriptor.

Una medida por parte del operador para esta acción maliciosa sería la detección y suspensión de esa tarjeta cuando se producen llamadas simultáneas con la misma identidad de usuario realizadas en lugares geográficamente diferentes.

2.7.2 AMENAZAS A LA SEGURIDAD EN LA INTERFAZ DE RADIO

La interfaz de radio entre el equipo terminal y la red de servicios representa una posible amenaza en la seguridad de UMTS. Las amenazas asociadas a esta parte de la red son las que se mencionan a continuación.

Acceso desautorizado de datos

Esta amenaza se refiere a que intrusos pueden escuchar los datos de usuario y de señalización durante el establecimiento de una comunicación (por ejemplo los parámetros RAND y AUTN), con el objetivo de efectuar ataques sobre el sistema.

También los intrusos pueden iniciar sesiones de comunicación para obtener el acceso a la información como por ejemplo la tasa de transmisión, retardo, destino de mensajes asociados sobre la interfaz de radio.

Las medidas para prevenir esta amenaza sería que el operador seleccione de forma adecuada los mejores algoritmos para de esta manera fortalecer los procesos de autenticación y confidencialidad que se realizarán en la interfaz de radio.

Amenazas a la integridad

Intrusos pueden modificar, insertar, borrar ya sea el tráfico de usuario y el de control sobre la interfaz de radio.

Para evitar este problema el operador de la red debe tener actualizado el algoritmo de integridad para que sea utilizado sobre los datos de usuario y de control.

Acceso desautorizado a los servicios

Un intruso puede hacerse pasar por un usuario suscrito al sistema. El intruso primero se hace pasar como una estación base hacia el usuario y entonces secuestra su conexión después que la autenticación ha sido realizada.

Esta amenaza se produce generalmente cuando el usuario se encuentra en una red de menor seguridad como GSM por lo que se requiere que todos los operadores utilicen el proceso de autenticación del usuario hacia la red y viceversa.

2.7.3 AMENAZAS A LA SEGURIDAD EN EL NÚCLEO DE RED (CN)

Interconexión entre diferentes operadoras UMTS

La seguridad entre diferentes operadores UMTS depende del buen funcionamiento de cada uno de ellos. Es decir si un suscriptor está usando una

red diferente a su red local en la cual no están activos los diferentes mecanismos de seguridad podría producirse un ataque al suscriptor.

También se debe tener en cuenta al hecho que al estar las diferentes operadoras compitiendo por los mismo suscriptores, una de ellas podría realizar ataques a los suscriptores de la otra operadora para que éstos cambien de operador.

Para impedir esta amenaza los terminales de la operadora local deben poseer mecanismos que desconecten al suscriptor si la red visitante no puede manejar los protocolos de autenticación, confidencialidad e integridad en una manera correcta. Otra solución sería crear una normativa por parte de los organismos de control como el SENATEL (Secretaría Nacional de Telecomunicaciones del Ecuador) para impedir que las diferentes operadoras, a pretexto de captar mayor suscriptores, afecten los intereses de la otra operadora y del usuario suscrito a ella.

Interconexión de la red UMTS a otro tipo de red

La interconexión de la red UMTS con otro tipo de red como Internet abre la oportunidad del ataque de los *hackers*[1], los cuales pueden causar gran daño al sistema.

El propósito del ataque de los *hackers* podría ser el robo de información de los abonados para después venderlos. Esto podría causar un gran daño económico al usuario ya que recibiría altas facturas por pagar y al proveedor del servicio porque perdería suscriptores debido a la desconfianza e ineficiencia que sienten hacia su proveedor.

Para proteger al sistema UMTS contra los *hackers* una regla importante es siempre tener actualizado los sistemas de seguridad entre la red UMTS y las redes externas, es decir las pasarelas de borde (BG). Además los sistemas de seguridad deben notificar si intrusos están intentando irrumpir en el sistema.

---

[1]Hackers: Persona o grupo de personas que ganan acceso a seguridades de una red por placer o desafío, algunas veces para robar información o para sabotear el sistema.

Rechazo del servicio

En un ataque de negación o rechazo del servicio el objetivo del *hacker* no es coleccionar información, sino causar daño e inconvenientes a otros usuarios y al proveedor del servicio. En un típico ataque de negación del servicio el *hacker* genera una alteración del tráfico, que en el peor de los casos bloquea al servidor, de tal manera que no es posible suministrar servicios a ningún abonado, por ejemplo el *hacker* envía peticiones al servidor e ignora todos los acuses de recibo que el servidor envía de regreso. Consecuentemente el servidor ocupa recursos para las conexiones entrantes que nunca ocurren.

Un ataque de negación de servicio puede ser muy peligroso ya que puede causar grandes daños económicos. Una manera de combatir este tipo de ataques es realizar una autenticación entre los elementos de red.

Amenazas administrativas

Esta amenaza se relaciona a que un trabajador deshonesto al tener acceso a la base de datos de los suscriptores puede vender la información secreta de suscripción, produciendo grandes daños al usuario y proveedor de red.

Para prevenir este riesgo se debe limitar el acceso a la base de datos a un reducido número de empleados.

CAPÍTULO III

CALIDAD DE SERVICIO (QoS) EN REDES UMTS

CAPÍTULO III

CALIDAD DE SERVICIO (QoS) EN REDES UMTS[1 2 3 4]

En este capítulo se abordará la arquitectura de la QoS en redes UMTS. Primeramente se explicará el concepto de portador como una manera de comprender la QoS, siguiendo con una descripción de los diferentes servicios portadores. Luego se realiza una breve descripción de las diferentes clases de QoS, siguiendo con una explicación de los parámetros de QoS en UMTS. Finalmente, se elaborará una descripción del funcionamiento de la red con QoS.

3.1 CALIDAD DE SERVICIO EN REDES MÓVILES[5]

La calidad de servicio (QoS) se define como el efecto global de las prestaciones del servicio que determinan el grado de satisfacción de un usuario del servicio que está recibiendo.

En la recomendación de la ITU E.800 se limita la QoS a la identificación de parámetros que pueden ser directamente observados y medidos en el punto en el que el servicio es accedido por el usuario.

La idea general detrás de QoS es asegurar la comunicación extremo a extremo entre entidades de las cuales al menos una de ellas es móvil.

---

[1]Referencia [10]: 3 rd Generation Partnership Project, 3GPP TS 23.107, "Quality of Service (QoS) Concept and Architecture".
[2]Referencia [11]: 3 rd Generation Partnership Project, TSGS1#3, "UMTS Quality of Service".
[3]Referencia [35]: Nortel Networks, "Introduction to Quality of Service (QoS)",
[4]Referencia [39]: J. Sánchez, "Mixing Conversational and Interactive Traffic in the UMTS Radio Access Network", (UPC).
[5]Referencia [21]: Jae-Il Jung, IEEE Communications Magazine, "Emerging Data Communications Standards", pág:108-109.

También se puede decir que la QoS se caracteriza por los aspectos combinados de factores de funcionamiento aplicables a todos los servicios, tales como: la accesibilidad de servicio, la integridad de servicio; y otros factores específicos a cada servicio.

Además de ello, la QoS va a depender de la calidad que puedan ofrecer cada subred. Por ello se necesitan mecanismos globales que gestionen esta calidad y negocien con las subredes la calidad de servicio individualmente. Cada subred tiene que proporcionar mecanismos locales de calidad de servicio. Así, la calidad de servicio global será consecuencia de las calidades de servicio negociadas en cada una de las subredes.

3.1.1 REQUISITOS DE QoS

Los requisitos de QoS pueden ser definidos de acuerdo al punto de vista del usuario y de los aspectos técnicos de la red, es por ello que los requisitos que deben estar presentes para una adecuada prestación y funcionamiento de los diferentes servicios son los siguientes:

Requisitos del usuario final

- Al usuario final solo importa la QoS que él percibe.
- Parámetros claros y pocos numerosos.
- Las definiciones de QoS deben ser capaces de soportar aplicaciones actuales y futuras.
- La QoS debe ser proporcionada extremo a extremo.

Requisitos generales de QoS

- Mecanismos de control específicos de UMTS.
- Se debe permitir la evolución independiente de las redes troncal y de acceso.
- Cabecera e información transmitida y almacenada de tamaño reducido.
- Los mecanismos de QoS deben permitir el uso eficiente de la capacidad de radio.
- Comportamiento de QoS dinámico y cantidad de parámetros baja.

3.2 ARQUITECTURA DE QoS EN LAS REDES UMTS[1]

UMTS utiliza una arquitectura de capas para la provisión de QoS (Figura 3.1), teniendo cada servicio portador sobre una capa específica servicios individuales, usando los servicios proporcionados por las capas inferiores. Cada servicio portador en una capa específica ofrece sus servicios individuales utilizando servicios ofrecidos o proporcionados por las capas inferiores.

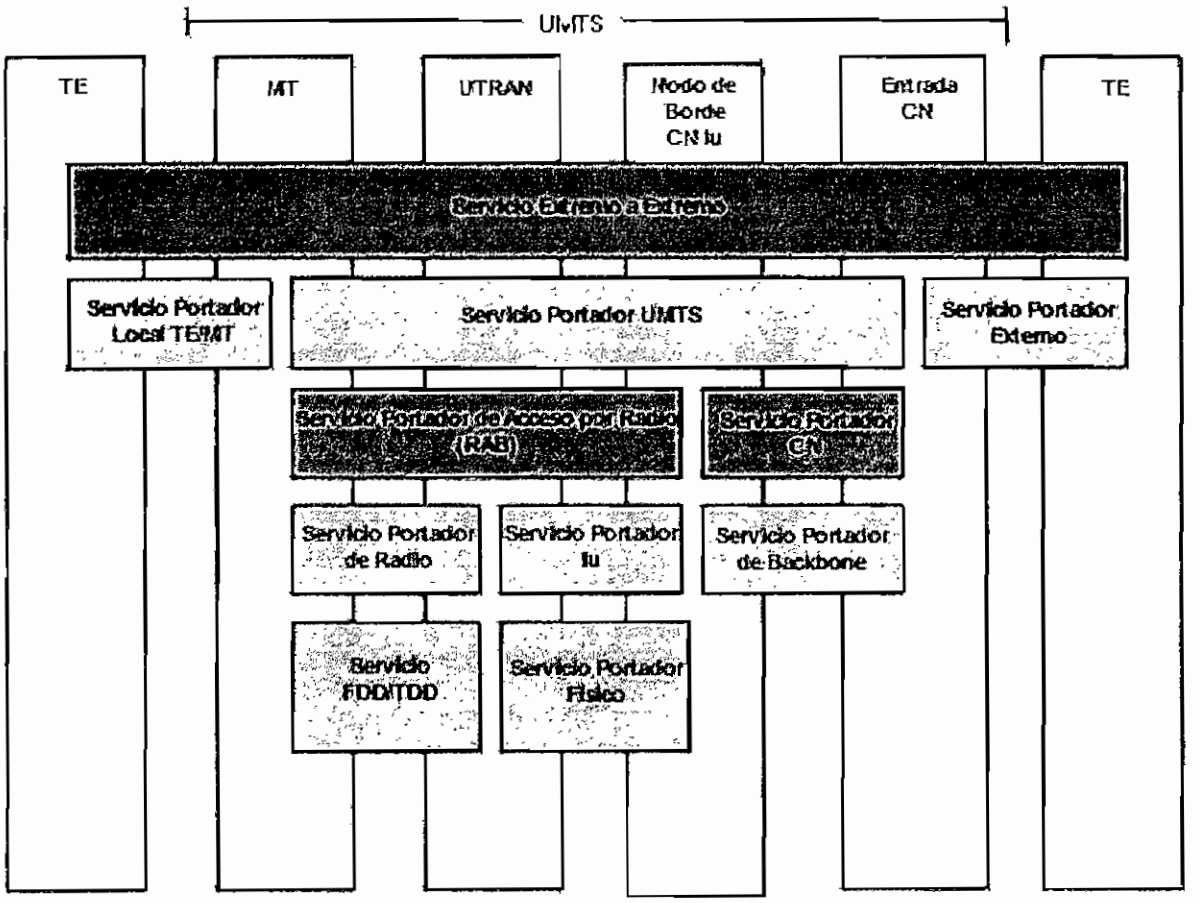


Figura 3.1 Arquitectura de QoS en UMTS

Para llevar a cabo una determinada QoS en la red se ha de establecer un Servicio Portador desde la fuente hasta el destino final del servicio (extremo a extremo), con características y funcionalidades claramente definidas.

[1]Referencia [10]: 3 rd Generation Partnership Project, 3GPP TS 23.107, "Quality of Service (QoS) Concept and Architecture".

Un Servicio Portador incluye todos los aspectos que permiten la provisión de una QoS controlada; por ejemplo:

- El transporte en el plano de usuario
- La funcionalidad de la gestión de la QoS
- Señalización de control

3.2.1 SERVICIO EXTREMO A EXTREMO

Los servicios de red son considerados extremo a extremo, esto significa de un Equipo Terminal (TE) a otro TE. Un servicio de extremo-a-extremo puede tener una cierta Calidad de Servicio (QoS) que es suministrada por la red a un usuario de ésta.

El TE se conecta a la red UMTS utilizando una Terminación Móvil (MT), y el tráfico de éste tiene que pasar por diferentes servicios portadores para llegar de la fuente al destino El servicio extremo a extremo utiliza sobre la capa aplicación los servicios portadores de las redes situadas por debajo y es típicamente llevado sobre otras redes, y no solamente sobre UMTS.

Así pues, el servicio extremo a extremo utilizado por el TE se llevará a cabo utilizando un Servicio Portador Local TE/MT, un Servicio Portador UMTS y un Servicio Portador Externo tal como el Internet.

Cabe mencionar que el servicio extremo a extremo es proporcionado por una traducción con servicios externos como el Internet. Con respecto al operador, son los varios servicios proporcionados por el servicio portador UMTS que el operador ofrece.

3.2.2 SERVICIO PORTADOR UMTS

El concepto de QoS en UMTS está basado sobre una jerarquía de servicios portadores como se muestra en la Figura 3.1, en donde los portadores de acceso de radio (RAB) proporcionan el transporte a través de la red de radio. Para poder

diferenciar los flujos de tráfico en la red, se ha definido cuatro servicios relacionados con cada aplicación, los cuales son: servicio conversacional, servicio de transferencia continua (*streaming*), interactivo, y de segundo plano (*background*).

Cuando un usuario pide un servicio, la aplicación negocia vía CN un portador de acceso de radio (RAB) con ciertos atributos en la red de radio. Por ejemplo, conversacional RAB tiene atributos para garantizar la velocidad de transmisión, mínimo retardo, y pueden por tanto transportar el flujo de tráfico en tiempo real.

Así, UMTS permite a un usuario/aplicación negociar las características del portador que son apropiadas para transportar la información. También es posible cambiar las propiedades del portador vía un proceso de renegociación del portador en el curso de una conexión activa.

La negociación de un portador es iniciada por una aplicación, mientras la renegociación puede ser iniciada por la aplicación o por la red (situaciones de *handover*).

Como se describió en los párrafos anteriores, es el servicio portador UMTS quien proporciona la calidad en UMTS. Este consiste de dos partes:
- Servicio portador de acceso por radio
- Servicio portador de CN (*Core Network*)

3.2.3 SERVICIO PORTADOR DE ACCESO POR RADIO (RAB)

El servicio portador de acceso por radio proporciona el transporte confidencial de señalización y datos del usuario entre el MT y el nodo de borde CN Iu[1] con la QoS adecuada al Servicio Portador UMTS negociado. Este servicio es basado sobre las características de la interfaz de radio y se mantiene para un MT móvil.

[1]Nodo de borde CN Iu: En la arquitectura de QoS en UMTS, al nodo entre UTRAN y CN (nodo SGSN) se le denomina de esta forma.

3.2.4 SERVICIO PORTADOR DE RED CENTRAL (*CORE NETWORK*) DE UMTS

El servicio portador de red central de UMTS conecta el nodo de borde CN Iu con la entrada CN[1] hacia la red externa.

El rol del servicio portador de CN es el de controlar eficientemente y utilizar el *backbone* de la red para que el servicio portador UMTS sea suministrado. Para la red dorsal basada en IP existen varias soluciones como: Servicios Diferenciados (DiffServ) o los Servicios Integrados (IntServ), pero el 3GPP ha escogido como la solución más adecuada DiffServ debido a que es menos complicada.

3.2.5 SERVICIO PORTADOR DE RADIO Y EL SERVICIO PORTADOR Iu

El servicio portador de acceso por radio es realizado por el servicio portador de radio y el servicio portador Iu.

El papel del servicio de portador de radio es cubrir todos los aspectos del transporte en la interface de radio entre MT UTRAN[2].

El servicio portador Iu junto con el servicio portador físico proporcionan el transporte entre UTRAN y el CN. Los servicios portadores Iu para tráfico de paquetes deberán proporcionar diferentes servicios portadores para obtener diferentes QoS. El operador tiene la facultad de decidir que capacidades de QoS en la capa IP o en la capa ATM son usadas. Para los servicio portadores Iu basados en IP, DiffServ o IntServ han sido discutidos como posibles soluciones.

3.2.6 SERVICIO DE *BACKBONE* DE RED

El servicio de *backbone* de red es seleccionado según la decisión del operador, pero este debe permitir la transmisión de los diferentes portadores UMTS. Es

---

[1] Entrada CN: Se denomina al nodo entre CN y una red externa (nodo GGSN).
[2] Este servicio portador usa el FDD/TDD UTRAN.

importante notar que este servicio no es específico a UMTS pero puede reusar una norma existente.

3.3 FUNCIONES DE GESTIÓN DE LA QoS EN LA RED

El propósito del estudio de esta sección es dar una breve apreciación de la funcionalidad necesaria para proporcionar QoS en UMTS. Las funciones en este tipo de red están clasificadas en dos diferentes planos, los mismos que se denominan de control y de usuario.

El plano de control se encargan de establecer, modificar y mantener un servicio portador UMTS con un específico QoS. Dentro de este plano se tiene:

- Gestor de servicio
- Función de traducción
- Control de admisión/capacidad
- Control de suscripción

El plano de usuario mantiene el tráfico de datos dentro de ciertos límites definidos por parámetros de QoS específicos. El servicio portador de UMTS con diferentes parámetros de QoS será soportado por las funciones de gestionamiento de QoS. Estas funciones asegurarán la provisión de la negociación de QoS para un servicio portador UMTS. En el plano de usuario se encuentran las siguientes funciones:

- Función de clasificación
- Gestor de recursos
- Acondicionador de tráfico

A continuación se describirán las funciones antes mencionadas.

3.3.1 FUNCIONES DE GESTIÓN DE QoS PARA EL SERVICIO PORTADOR UMTS EN EL PLANO DE CONTROL

Gestor de servicio

Coordina las funciones del plano de control para el establecimiento, modificación y mantenimiento del servicio que es responsable, y proporciona a todo el plano de usuario funciones de gestionamiento de QoS con los parámetros pertinentes. El gestor del servicio ofrece servicios a otras instancias. Esta función puede realizar una traducción de un atributo para pedir servicios de las capas más bajas. Además puede interrogar a otras funciones de control para recibir permiso para la provisión de un servicio.

Las características más importantes son: el establecimiento, modificación y mantenimiento.

Función de traducción

Para sustentar QoS de extremo a extremo tiene que ser llevado sobre diferentes redes tal como Internet. Así hay la necesidad para una traducción de funciones entre los atributos del servicio portador UMTS y parámetros de QoS de redes externas. En otras palabras, la función de traducción convierte los requerimientos de QoS externos a una forma entendible a la red UMTS. De la entrada externa, la función de traducción deriva parámetros relacionados a las diferentes capas de los servicios portadores en UMTS.

En resumen, convierte requerimientos de otras redes a requerimientos de la red UMTS.

Control de admisión/capacidad

Contiene información acerca de todos los recursos disponibles de una entidad de red y acerca de todos los recursos asignados a los servicios portadores UMTS. Además de ello, decide si aceptar o no una petición de un servicio portador UMTS, para la obtención de los recursos requeridos que pueden ser

suministrados por la entidad de red y reserva tales recursos si han sido asignados al mencionado servicio portador UMTS.

Es decir, la función de control de admisión/capacidad verifica la capacidad de la entidad de red para proporcionar el servicio pedido.

Control de suscripción

Esta función verifica la suscripción del usuario frente a sus requerimientos, por lo que se debe realizar una correcta administración del servicio portador UMTS del respectivo usuario, para utilizar los pedidos de servicio con los parámetros de QoS especificados.

3.3.2 FUNCIONES PARA EL SERVICIO PORTADOR UMTS EN EL PLANO DE USUARIO

Función de clasificación

Esta función asigna las unidades de datos a los portadores que estén definidos, es decir asigna las unidades de datos a los servicios establecidos de un MT de acuerdo a los parámetros relacionados si el MT tiene múltiples servicios portadores establecidos. El servicio portador UMTS apropiado se deriva de la cabecera (header) de la unidad de datos o de las características de tráfico de los mismos.

Gestor de recursos

Distribuye los recursos disponibles entre todos los usuarios que desean compartir tal recurso. El administrador de recursos distribuye los recursos según el QoS requerido. Ejemplos para la gestión de recursos son: administración del ancho de banda, y el control de potencia para el portador de radio.

Acondicionador de tráfico

Realiza una adaptación entre el QoS negociado para un servicio y el tráfico de la unidad de datos. El tráfico condicionado se realiza por comprobación del tráfico a lo negociado (función policía). La función de comprobación compara el tráfico de la unidad de datos con los parámetros de QoS relacionados. La unidad de datos que no esté de acuerdo a los parámetros relevantes, será excluida en caso de congestión. La configuración del tráfico de datos es acorde al QoS del servicio.

3.4 CLASES DE QoS EN UMTS

En este proyecto se define como clases de servicio al conjunto de parámetros de calidad de transmisión que delimitan las características de un cierto flujo de información. Cada uno de los flujos de información generados y que deben ser transmitidos por la aplicación tendrá asignada una clase de QoS. Las conexiones asociadas a una clase de QoS generarán información siguiendo un patrón de tráfico[1].

Se define como patrón de tráfico a la estadística con la que una cierta conexión genera paquetes de información. Los modelos de generación de tráfico se caracterizan por variables aleatorias; por tanto, el conocimiento completo de un cierto patrón de tráfico implica la definición de todos los momentos estadísticos de las variables aleatorias que definen el patrón.

Es evidente que el planteamiento de un sistema de comunicaciones que pueda dar cabida a la infinidad de patrones de tráfico posibles, cada uno de ellos con sus requerimientos de calidad representa una tarea inabordable. Es por ello que debe arbitrarse una solución viable y aplicable a un entorno real. Una solución consiste en la definición de un conjunto limitado de clases de QoS a las que deban acogerse todas las conexiones activas en el sistema y sus correspondientes aplicaciones. Este conjunto debe ser lo suficientemente amplio como para

[1] Referencia [31]: Luis Gonzaga, "Calidad de Servicio (QoS) Garantizada", UPC, pág:189-192.

abarcar, de un modo suficientemente preciso, la totalidad de las conexiones que puedan requerir servicio del sistema, y a su vez lo suficientemente restringido como para simplificar en lo posible la implementación real de los mecanismos de gestión de recursos.

Por tanto, cuando una aplicación quiera ser servida por el sistema de transmisión, deberá analizar cada una de sus conexiones o flujos de información activos. Este análisis debe permitir decidir cuál de las clases de QoS definidas en el sistema resulta más adecuada a las necesidades de calidad de transmisión y se ajusta mejor al patrón de tráfico de cada conexión. Esta decisión deberá hacerse siempre basándose en un análisis de los requerimientos, para asegurar así el cumplimiento de los requisitos necesarios para todas y cada una de las conexiones activas.

De este modo, el sistema de comunicaciones verá las conexiones de todas las aplicaciones como un conjunto determinado de clases de servicio, cuyas características son conocidas a priori, lo que permite una planificación eficiente de la gestión del tráfico. Tanto el dimensionado de los accesos, enlaces y redes de comunicaciones, como la gestión de todo el funcionamiento del sistema para poder garantizar la calidad de servicio de las conexiones activas resultan realizables con un grado de complejidad abordable.

En general, los servicios pueden ser divididos en diferentes grupos. En UMTS se ha considerado cuatro clases de tráfico:

- Conversacional
- Transferencia continua (*streaming*)
- Interactiva
- Segundo plano (*background*)

El principal factor para distinguir entre las diferentes clases es la sensibilidad del tráfico frente al retardo. Por ejemplo, en la clase conversacional se debe tener cuidado al retardo punto a punto, el cual debe ser el menor posible y con una

variación también pequeña; mientras en la clase background el retardo punto a punto no es una característica crítica.

3.4.1 CLASE CONVERSACIONAL

Esta clase se aplica a los servicios de tiempo real, la cual es caracterizada por el hecho de que el retardo de extremo a extremo es bajo. El retardo máximo de extremo a extremo es dado por la percepción humana; por consiguiente el límite para un retardo aceptable debe ser estricto.

Con internet y multimedia un número de nuevas aplicaciones requieren esta clase de calidad, por ejemplo:

- Conversación telefónica.
- Voz sobre IP.
- Videoconferencia.

Una falla de la red para proporcionar un bajo nivel de retardo resultará en una calidad inaceptable.

3.4.2 CLASE DE TRANSFERENCIA CONTINUA (*STREAMING*)

Es una técnica para transferir datos tal como estos puedan ser procesados en forma unidireccional (normalmente de la red al usuario). Las técnicas de streaming están llegando a cobrar gran importancia debido al crecimiento del Internet ya que la mayoría de usuarios no tienen suficiente acceso para descargar grandes archivos rápidamente. Con streaming el usuario puede empezar ha desplegar los datos antes de que el archivo entero haya sido transmitido.

Para trabajar en forma unidireccional, el lado del receptor debe ser capaz de almacenar los datos y enviarlos como un flujo uniforme a la aplicación que está procesando los datos y convirtiéndolos a sonido o gráficos.

Ejemplos de aplicaciones dentro de esta clase son:

- Descargas de video
- Descargas de audio

3.4.3 CLASE INTERACTIVA

Se trata de aplicaciones caracterizadas por una petición seguida de una respuesta por parte de un servidor . Aquí lo importante no es el retardo, extremo a extremo, sino ida y vuelta (desde que el cliente efectúa la petición, hasta que recibe la respuesta asociada). También hay que garantizar una tasa de errores baja (BER bajo). Ejemplos de aplicaciones dentro de esta clase basadas en esquemas de petición-respuesta son:

- Los navegadores web (*web browsing*)
- Recuperación de base de datos y
- Acceso a los servidores.

3.4.4 CLASE DE SEGUNDO PLANO (*BACKGROUND*)

Esta clase se realiza a aplicaciones donde el retardo extremo a extremo no es la característica crítica. Lo que hay que garantizar es que los datos que sean transmitidos tienen que ser recibidos con una tasa de errores baja. Ejemplos de aplicaciones dentro de este servicio son:

- El correo electrónico y
- El servicio de mensajes cortos (SMS).

En la Tabla 3.1 se resume las características más importantes de las diferentes clases de QoS.

Tabla 3.1 Clases de QoS en UMTS

Clase de QoS	Requerimientos retardo transferencia	Variaciones retardo transferencia	Bajo BER	Velocidad binaria garantizada	Ejemplo
Conversacional	Estricto	Estricto	No	Si	VoIP, Videoconferencia, Audio-conferencia
Flujo continuo	Limitado	Limitado	No	Si	Servicios de difusión (audio, video), Noticias, Deportes
Interactivo	Tolerante	No	Si	No	Navegación Web, Juegos, M-commerce
Segundo plano	No	No	Si	No	E-mail, SMS

3.5 PARÁMETROS DE CALIDAD DE SERVICIO[1]

En UMTS los parámetros de QoS describen el servicio proporcionado por la red al usuario, el cual consiste en generar su perfil de QoS.

Estos parámetros deberán tener una relación directa con la percepción que el usuario final deba tener de la calidad de la conexión. Así por ejemplo, para el caso de una aplicación de transmisión de voz en tiempo real, deberán establecerse relaciones entre los parámetros de la transmisión (retardo máximo de los paquetes, diferencia máxima entre retardos de paquetes, tasa máxima de paquetes perdidos, BER máximo etc.).

Será por tanto el tipo de aplicación o usuario al que se le deba dar servicio lo que condicionará el tipo y los valores de los parámetros que marcarán la definición de cada clase de QoS.

[1]Referencia [11]: 3 rd Generation Partnership Project, TSGS1#3, "UMTS Quality of Service".

Para realizar un análisis de la calidad de servicio se ha considerado en esta tesis un conjunto acotado de parámetros de servicio, que se detallan a continuación:

3.5.1 PARÁMETROS DEL SERVICIO PORTADOR UMTS

Los parámetros del servicio portador UMTS describen el servicio suministrado por la red UMTS al usuario del servicio portador UMTS. Un conjunto de parámetros de QoS (perfil de QoS) especifica este servicio. El servicio portador UMTS establece o modifica diferentes perfiles de QoS.

Clase de tráfico

Define las clases de tráfico para que el servicio portador UMTS sea optimizado. La ventaja de usar este parámetro es que UMTS puede hacerse una idea acerca de la naturaleza de la fuente de tráfico y optimizar el transporte de la red.

Velocidad máxima (máximo flujo)

Es definido por el máximo número de bits transferidos dentro de un periodo de tiempo que le es permitida a una cierta conexión. Los propósitos de este parámetro son:

- Limitar la razón de bits entregada a redes externas o aplicaciones si estas están sujetas a tales limitaciones. Por tanto este valor puede usarse para impedir que una única conexión pueda copar una cantidad excesivamente grande de recursos del sistema.

Velocidad garantizada

Garantiza el número de bits entregados por UMTS a un punto definido de la red dentro de un periodo de tiempo, dividido por la duración del periodo. El propósito de este atributo es facilitar la asignación de recursos dentro de UMTS; es decir, a través de este parámetro se pretende administrar el acceso a los recursos de la red UMTS de acuerdo a las diferentes aplicaciones.

Tamaño máximo de SDU (octeto)

Es usado por el mecanismo de gestión de recursos y describe el tamaño máximo de SDU permitido.

Proporción de error en SDU (tasa errores SDU)

Indica el fragmento de SDU perdido o alterado. Este parámetro es usado para configurar protocolos, algoritmos y esquemas de detección de errores.

Tasa de error binario residual (BER)

Indica la tasa de error binario residual inadvertido en los SDUs entregados. Este es usado para configurar los protocolos de la interface de radio, algoritmos y esquemas de detección de errores.

Suministro de SDUs erróneos (y/n/-)

Señala si los SDUs detectados como erróneos serán entregados o no.
Si son detectados implica que mensajes de error serán entregados con respecto al SDU erróneo. En este caso, se emplean algoritmos de detección de errores.
Si no son detectados, implica que se descartarán mensajes de error. Algoritmos de detección de error se emplean también en este caso.
(-) implica que la entrega tomará lugar a pesar de la detección del error.

Retardo de transferencia (ms)

El retardo de transferencia se define por el tiempo transcurrido entre una petición a transferir información y su entrega a otro punto de red . El propósito de este atributo es especificar la tolerancia al retardo para la aplicación y permite al UTRAN ajustar los formatos de transporte.

Asignación/retención de prioridad

Es un parámetro específico de la suscripción, no negociable de la estación móvil, que describe la importancia de escoger el portador UMTS en comparación a otros portadores UMTS para la asignación y la retención. El propósito es diferenciar

entre los portadores cuando se realiza asignación y retención de un portador en el caso de que los recursos sean escasos y prioriza entre los de alta prioridad sobre los de baja prioridad.

Como se dijo anteriormente, una clase de servicio estará definida por un subconjunto de estos parámetros, así como los valores correspondientes para cada uno de ellos. A continuación se discutirá algunos atributos con respecto a las diferentes clases de tráfico.

Clase conversacional

La velocidad máxima indica el límite superior de la velocidad y el portador UMTS no requerirá transferir tráfico que exceda la velocidad garantizada. Tanto la velocidad máxima como la garantizada son usados para la asignación de recursos dentro de UMTS. Para este tipo de tráfico se hace fundamental garantizar un bajo retardo.

Clase Streaming (transferencia continua)

Similar a la clase conversacional, en donde existe cortos periodos de silencio. Como en la clase conversacional, la máxima velocidad especifica el límite superior de la velocidad y el portador UMTS no requiere la transferencia de tráfico que exceda la velocidad garantizada.

Clase interactiva

Esta clase es optimizada para la comunicación interactiva. Para ser capaz de limitar la razón de datos entregados se incluye la velocidad máxima. Los portadores dentro de la clase interactiva no darán ninguna calidad garantizada para que la calidad real dependa de la carga del sistema. En su lugar, esta clase usa un manejo de prioridades de tráfico. Los datos de un portador UMTS con alta prioridad de tráfico, tendrán una mayor prioridad sobre los datos de otros portadores dentro de esta clase. Por tanto ninguna garantía absoluta puede darse.

Clase background (segundo plano)

Esta clase es optimizada para la comunicación máquina a máquina que no es sensible al retardo como por ejemplo los servicios de email. Las aplicaciones background toleran un alto retardo en comparación con la clase interactiva. UMTS solo transfiere esta clase de tráfico cuando hay suficiente capacidad en la red. Para ser capaz de limitar la razón de datos entregados por aplicaciones, la velocidad máxima es incluida. Ninguna garantía es necesaria excepto mantener una tasa de errores baja.

En la Tabla 3.2 se indican los atributos del servicio portador UMTS y su importancia para cada clase de tráfico.

Tabla 3.2 Parámetros de QoS del servicio portador UMTS

Clase de tráfico	Conversacional	Flujo continuo	Interactiva	Segundo plano
Velocidad máxima	X	X	X	X
Máximo tamaño SDU	X	X	X	X
Tasa errores SDU error ratio	X	X	X	X
Tasa error binario residual	X	X	X	X
Suministro de SDUs erróneos	X	X	X	X
Retardo transferencia	X	X		
Velocidad garantizada	X	X		
Asignación/retención prioridad	X	X	X	X

3.5.2 RANGOS DE VALORES DE LOS PARÁMETROS

Para el servicio portador UMTS se define una lista de valores o rango de valores para cada parámetro. Esta lista define los valores posibles que serán usados para un parámetro considerando cada posible condición de servicio.

En la Tabla 3.3 se indica los valores o rango de valores de los parámetros del servicio portador UMTS. Los rangos de valores reflejan la capacidad de la red UMTS.

Tabla 3.3 Rango de valores de los parámetros del servicio portador UMTS[1]

Clase de tráfico	Conversacional	Flujo continuo (*streaming*)	Interactiva	Segundo plano (*background*)
Velocidad máxima (kbps)	< 2 048	< 2 048	< 2 048	< 2 048
Máximo tamaño SDU (bytes)	<=1 500 or 1 502	<=1 500 or 1 502	<=1 500 or 1 502	<=1 500 or 1 502
Suministro de SDUs erróneos	Si/No/-	Si/No/-	Si/No/-	Si/No/-
Tasa de error binario residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$
Tasa de errores SDUs	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Retardo de transferencia (ms)	100 – valor máximo	250 – valor máximo		
Velocidad garantizada (kbps)	< 2 048	< 2 048		
Asignación/retención de prioridad	1,2,3	1,2,3	1,2,3	1,2,3

3.6 DESCRIPCIÓN DE FUNCIONAMIENTO DE UNA RED UMTS CON CALIDAD DE SERVICIO[2]

3.6.1 PROTOCOLOS DE COMUNICACIÓN CON CALIDAD DE SERVICIO

Para obtener una red con calidad de servicio extremo a extremo se requiere un número diferente de tecnologías que en conjunto darán el resultado deseado. Por ello en esta tesis se ha realizado un modelo de capas con el intento de comprender en donde cada tecnología puede ser usada.

Se pueden distinguir tres niveles para ofrecer calidad de servicio:

Tabla 3.4 Protocolos que ofrecen QoS

Protocolos de aplicación	RSVP, RTSP, RTP
Protocolos de red y transporte	Servicios Diferenciados (Diffserv)
Protocolos de bajo nivel (capa 2)	ATM, MPLS

[1]Referencia[10] 3 rd Generation Partnership Project, 3GPP TS 23.107, "Quality of Service (QoS) Concept and Architecture".
[2]Referencia [35]: Nortel Networks, "Introduction to Quality of Service (QoS)".

- Protocolos de bajo nivel (capa 2).

ATM es quizá el protocolo más adecuado por su gestión de la calidad de servicio, el cual actúa sobre la interfaz Iu . También puede utilizarse la comunicación con etiquetaje de flujo MPLS (*Multi Protocol over Label Switching*, Conmutación de Etiquetas sobre Multi Protocolo) sobre las interfaces Gn y Gi

- Protocolos de red y transporte (a nivel de la capa 3 en IP).

A nivel de la capa 3, el 3GPP recomienda el uso de los servicio diferenciados IP (DiffServ) como el soporte de la calidad de servicio para suministrar la diferenciación de clases IP (Figura 3.2).

- Protocolos de aplicación.

En este nivel se han desarrollado distintos protocolos para gestionar la reserva de recursos como RSVP *(Resource Reservation Protoco*l, Protocolo de Reservación de Recursos).

MPLS usa un protocolo llamado LDP (*Label Distribution Protocol*, Protocolo de Distribución de Etiquetas) para el establecimiento del camino de etiquetas conmutadas (LSPs). Otros protocolos se encargan de la transmisión y sincronismo de audio y vídeo como RTSP *(Real-time Streaming Protocol*, Protocolo de Flujo Continuo en Tiempo Real) o RTP *(Real-time protocol*, Protocolo en Tiempo Real).

Estos protocolos calculan y asignan una anchura de banda equivalente a la duración de la llamada, que normalmente es de minutos para las comunicaciones telefónicas y de horas para las sesiones IP.

En la Figura 3.2 siguiente se observa como sería el funcionamiento de la red UMTS con algunos de los protocolos antes mencionados[1].

---

[1] Referencia [32]: Revista de Telecomunicaciones de Alcatel – 1er Trimestre 2001, "QoS implementation in UMTS networks", pág 44.

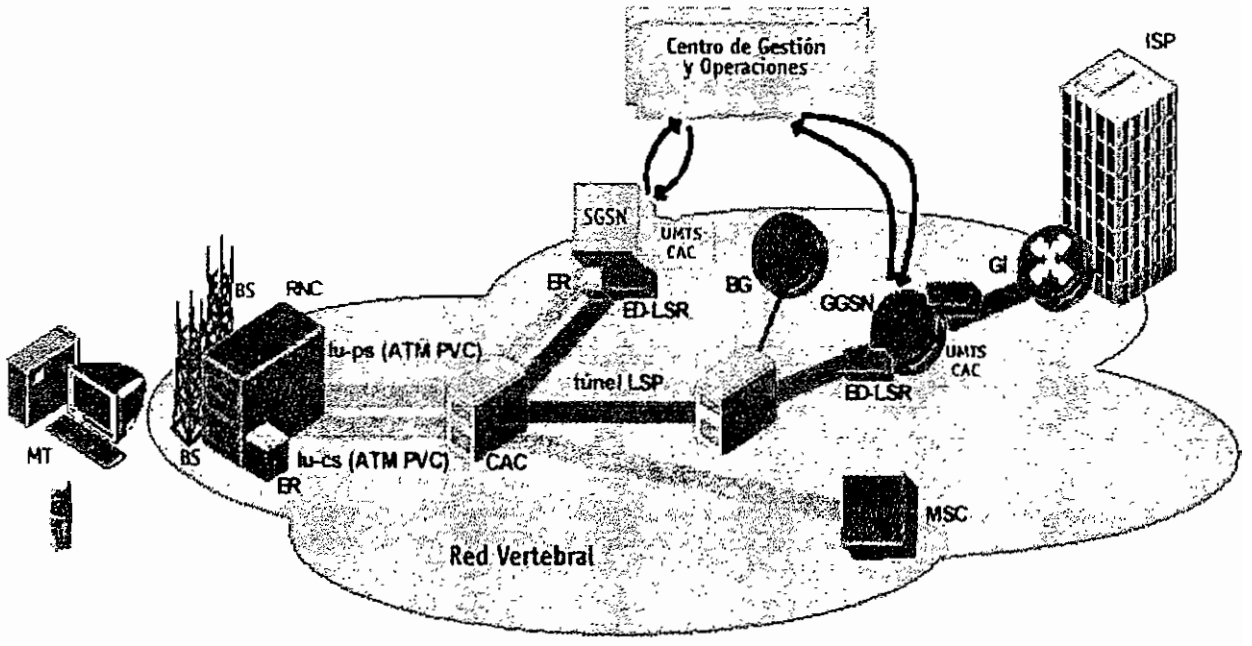


Figura 3.2 Funcionamiento de UMTS con QoS

3.6.2 GESTIÓN DE LA QoS EN LA RED CENTRAL UMTS

Las características QoS soportadas por la red central UMTS deben permitir diferenciar los servicios ofrecidos, asegurando la asignación de los recursos necesarios para el suministro de un servicio adecuado a un abonado, respetando las necesidades de los otros abonados y garantizando la calidad del servicio negociada.

Por ello las siguientes tecnologías que serán analizadas en esta tesis tratan de ofrecer una adecuada QoS a los diferentes servicios ofrecidos.

3.6.2.1 Utilización de MPLS

MPLS es una tecnología utilizada en UMTS para suministrar QoS a nivel de capa 2. La principal ventaja de MPLS, consiste en la clara separación entre las funciones de *routing* (es decir el control de la información sobre la topología y tráfico en la red), de las funciones de *forwarding* (es decir el envío en sí de datos entre elementos de la red). Por lo que MPLS integra sin discontinuidades los

niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del *routing* con la simplicidad y rapidez de la conmutación de nivel 2 .

En consecuencia, MPLS puede funcionar sobre cualquier tecnología de transporte y no solo sobre ATM; con lo que se asegura la continuidad de la política de QoS en el caso de una arquitectura de red dorsal IP mixta.

En UMTS, el SGSN, el GGSN y la pasarela de borde (BG), son routers periféricos de camino etiquetado (*Edge* LSR). La red dorsal UMTS está constituida por routers del núcleo de red de camino etiquetado (*Core* LSR).

Los túneles de camino etiquetado (LSP) se establecen dinámicamente sobre la base de tablas de encaminamiento IP y su ancho de banda se puede renegociar de acuerdo a las necesidades del usuario. Así se optimizan los recursos de la red.

En la Figura 3.3 se puede observar el esquema de funcionamiento de MPLS[1].

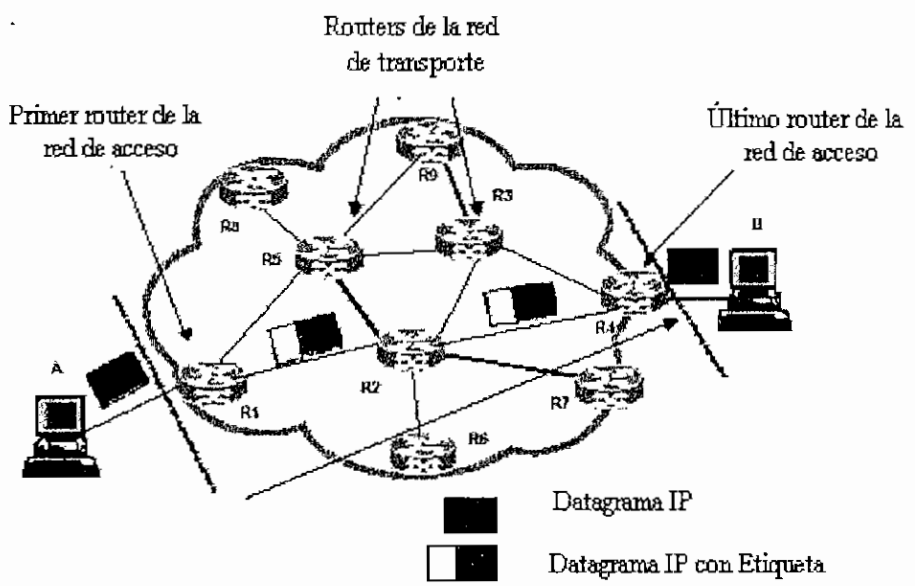


Figura 3.3 Esquema de Funcionamiento de MPLS

[1] Referencia [33]: Aplicaciones MPLS, "MPLS. Ingeniería de Tráfico y RPV de Proveedor", pág:3.

3.6.2.2 Servicios Diferenciados (DiffServ o DS)

Una solución para otorgar calidad de servicio es poner en marcha mecanismos de gestión con el objetivo de diferenciar entre el conjunto de paquetes que circulan por la CN en UMTS.

Una manera de mejorar el servicio del mejor esfuerzo[1], es tratar a los paquetes de manera diferente, tomando la decisión de cómo procesarlos dependiendo del contenido del encabezado del paquete.

El principio de los servicios diferenciados se logra reservando ciertos bits en el encabezado del paquete IP y definiendo en él, el tipo de servicio que se le debe aplicar al paquete de acuerdo a las políticas que se hayan especificado para ese propósito. Si existen similitudes entre diferentes paquetes, es posible clasificar los paquetes en grupos y tomar decisiones de cómo procesar los paquetes dependiendo del *grupo* al que pertenezca un paquete.

Los campos que son de utilidad en el encabezado para el manejo del paquete son los campos de dirección fuente y destino, tipo de servicio y el protocolo. El enrutador basándose en estos datos puede tomar una decisión de cómo procesar el paquete.

A diferencia de la arquitectura de *servicios integrados*, en donde es necesario el hacer una reservación del canal, de manera análoga al servicio telefónico, y donde existe una señalización para mantener la reservación, en la arquitectura de servicios diferenciados, los paquetes son clasificados únicamente en el dispositivo de acceso a la red, (es decir en SGSN y GGSN) y ya dentro de la red, el tipo de procesamiento que reciban los paquetes va a depender del contenido del encabezado.

El esquema de servicios diferenciados delimita las funciones que se tienen que realizar en los nodos de ingreso a la red y en los nodos internos de la red. Los

[1]Servicio del mejor esfuerzo: Este servicio trata los paquetes sin hacer ninguna diferenciación entre los diferentes tipos de flujos.

nodos de acceso a la red se encargan de la clasificación y de especificar el contenido del campo DS (Differentiate Service) [1]. Los nodos internos del núcleo de red se encargan del reenvío de los paquetes dependiendo del contenido del campo DS. La clasificación que se haga del paquete, queda especificada en el contenido del campo "Tipo de Servicio" o ToS del encabezado del paquete IP.

La Figura 3.4 muestra una arquitectura de servicios diferenciados. La red consta de dos tipos de nodos: de acceso a la red e internos.

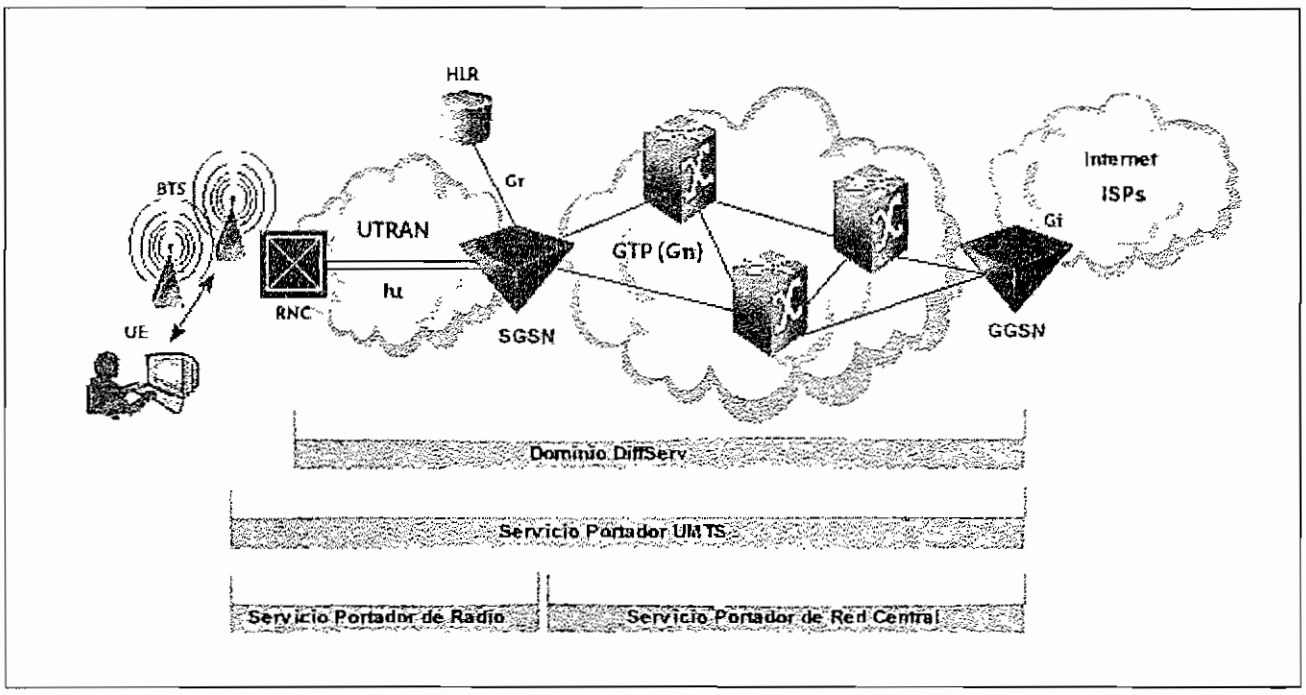


Figura 3.4 Arquitectura de UMTS con DiffServ[2]

3.6.2.2.1 Nodos Internos

Los nodos internos son los que se encargan de realizar las funciones de reenvío de paquetes de acuerdo a las clases de tráfico que se tienen especificadas en UMTS.

[1] Ver Anexo 3 para la definición del campo de DS
[2] Referencia [34]: Nortel Networks, "Benefits of Quality of Service (QoS) in 3G wireless Internet", pág:10.

Los nodos internos pueden manejar los paquetes en forma diferente dependiendo del contenido del campo ToS. De los 8 bits de este campo, solamente se utilizan los primeros 6 bits. Los dos bits restantes se encuentran reservados para aplicaciones futuras. Estos seis bits forman el campo DiffServ (DS) del encabezado del paquete de IP. Cada una de las 64 (2^6) posibles combinaciones puede significar una forma diferente de tratar los paquetes por parte de los enrutadores. A cada una de estas posibles formas de tratar al paquete se le llama "*Per Hop Behavior*" (PHB).

3.6.2.2.2 Nodos de Acceso

Los nodos de acceso (SGSN y GGSN) a la red realizan una serie de acciones a los paquetes como: Clasificación, Control de la tasa (*rate control*), acondicionamiento del tráfico. Es decir, este nodo realiza la diferenciación del tráfico de acuerdo a las diferentes clases de servicio, las cuales están relacionadas con las clases de servicio de UMTS (Figura 3.5).

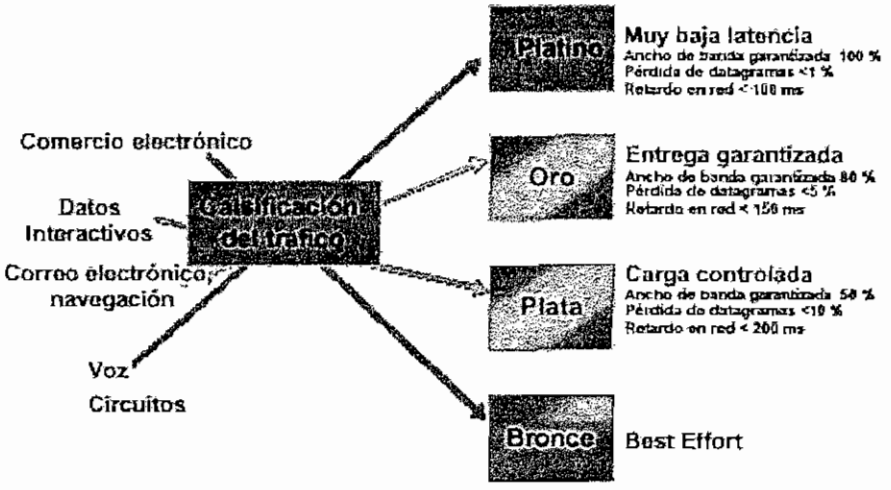


Figura 3.5 Clases de Servicio en DiffServ[1]

[1] Referencia [33]: Aplicaciones MPLS, "MPLS. Ingeniería de Tráfico y RPV de Proveedor", pág:11.

Cuando un usuario de otra red diferente por ejemplo un ISP se conecta al nodo de acceso de UMTS, el nodo cambia (marca) el valor del campo DS por el valor del PHB que se le debe aplicar al paquete dentro de la red.

El valor del campo DS que corresponde a un PHB se le llama DSCP (DiffServ Code Point). La especificación del DiffServ indica que los códigos DiffServ deben ser asignados por el proveedor de servicios. Entonces, la manera en que se lleva a cabo la diferenciación de servicios es mapeando estos códigos a su PHB correspondiente en cada uno de los nodos de la trayectoria dentro de la red.

3.6.2.3 Control de Admisión de Llamadas (CAC)

CAC es el procedimiento que decide si una conexión se establece o se rechaza. CAC usa la descripción de tráfico de la conexión y el pedido de QoS como entrada a su algoritmo. Una conexión se acepta si la capacidad está disponible, si se obtiene el QoS pedido y además si no se alterará otra conexión existente y su acuerdo sobre QoS.

El CAC basado en el gestionamiento de policía prevendrá la congestión en la red y la carga excesiva, mientras asegurará a cada sesión aceptada los recursos requeridos y la asignación de tales recursos dependerá de las condiciones de carga en la red.

El control de admisión de llamada se realiza en cada activación de contexto de protocolo de datos en modo paquete o en cada establecimiento de llamada en modo circuito, y en cada modificación de QoS.

Por otra parte, para garantizar la QoS a todos los niveles (no sólo en el nivel de aplicación) el CAC tiene en cuenta los recursos disponibles de la capa de transporte IP (por ejemplo, el ancho de banda suministrado de cada clase DiffServ).

En UMTS, dentro del servicio portador UMTS, los recursos de CN son esencialmente manejados por el CAC, el cual es realizado por el SGSN, y el GGSN; los cuales son los pilares fundamentales para el establecimiento de una sesión. El servicio garantizado de una sesión es mantenido por la función de policía o el contrato de QoS que es acordado por ellos.

Las funciones de policía de QoS son suministradas y almacenadas en el HLR . Cada suscriptor es enlazado a una función de policía de QoS o a múltiples funciones de policía. Cada función de policía refleja la suscripción del servicio y los parámetros de QoS asociados.

Dentro del servicio portador UMTS, el SGSN opera como el punto de exigencia de policía (PEP), el cual tiene la función de controlar el CAC. Sobre la activación de una sesión de datos, el terminal enviará una petición de QoS a su SGSN. El SGSN realizará el control de admisión de llamadas basado sobre el pedido de QoS y la suscripción de policía. Si se obtienen todas las condiciones de CAC, el SGSN enviará el QoS negociado como parte del pedido de sesión al GGSN.

El GGSN aplicará la función PDP (punto de decisión de policía) para modificar el QoS negociado basado sobre las condiciones de carga de la red y responde al SGSN con el final QoS negociado.

Sobre el receptor, al perfil final del QoS negociado el SGSN lo traducirá en parámetros de QoS equivalentes de radio y los enviará al controlador de la red de radio (RNC) para pedir la asignación de recursos de radio. En respuesta a este pedido, el RNC realizará el control de admisión de llamadas[1] sobre los recursos de radio basados sobre la actual condición de carga de la celda. Si los recursos de radio son asignados exitosamente por el servicio portador de Radio, el SGSN informará al terminal que la sesión es establecida con el último QoS negociado. El terminal y la aplicación pueden elegir o rechazar los recursos asignados, si consideran que son insuficientes y en tal caso la sesión es tomada como

[1] El control de admisión de llamadas en el RNC se conoce con el nombre de RAC.

terminada y el suscriptor posiblemente recibirá un mensaje indicando recursos de red escasos.

3.6.2.4 Contrato de nivel de servicio (SLA)

Para garantizar la QoS extremo-a-extremo a través de las redes externas, son necesarios contratos de nivel de servicio (SLA) entre la red UMTS y cada una de las redes externas.

SLA[1] especifica el contrato negociado entre dominios (redes) adyacentes. La parte técnica de un SLA es llamada especificación de nivel de servicio, que define el servicio que es proporcionado a un cliente con la compañía de parámetros, tales como máximo flujo, tamaño de ráfaga.

Los SLAs pueden establecerse entre el operador UMTS y cada operador de red de datos en modo paquete (PDN) como una intranet o un ISP, y entre operadores UMTS y otros operadores UMTS/GPRS.

Para cumplir los SLA, se debe dimensionar el número, tipo y ancho de banda de las interfaces de los nodos.

3.6.3 QoS EN LA RED DE ACCESO TERRESTRE UMTS (UTRAN)

3.6.3.1 Aspectos generales de la QoS en la UTRAN

Los servicios portadores de acceso radio (RAB) se establecen dinámicamente para dar soporte a una o varias aplicaciones (por ejemplo, la telefonía y la navegación por la web) para un usuario móvil determinado. La UTRAN puede tratar uno o más RAB simultáneamente por usuario al mismo tiempo, manteniendo cada RAB sus propias exigencias de QoS.

---

[1] Referencia [36] : S. Blake , "An Architecture for Differentiated Services", RFC 2475.

Para que la UTRAN pueda contribuir a asegurar la QoS extremo-a-extremo para los usuarios, cada RAB está particularizado por los parámetros de QoS que dependen de las características de la aplicación. La red central es quien se ocupa de traducir las características de la aplicación en atributos de QoS de RAB. La UTRAN obtiene simplemente de la red central (CN) los parámetros de QoS de la RAB cuando tales parámetros se han establecido.

La función de la UTRAN es establecer y mantener el RAB con los niveles de QoS requeridos. El RAB siempre se establece bajo petición de la CN, la cual retiene la propiedad del mismo desde el principio hasta el fin de su vida.

Una vez que el UTRAN ha sido asignado a un nivel de QoS dado, este no debería reducirse por la UTRAN sin una petición de modificación previa de la CN. En particular, este requerimiento se aplica a los terminales móviles, los cuales experimentan frecuentemente fluctuación en las condiciones de propagación de radio pasando de una celda a otra.

Por otro lado, es esencial la supervisión de la QoS para asegurar que se cumplan, pero no se excedan, las exigencias de la misma, así como facilitar el flujo del tráfico y evitar la congestión. Por ejemplo, retardando el tráfico que no es en tiempo real (NRT) a favor de los servicios de alta prioridad en tiempo real (RT).

Es por ello que para que un sistema de tercera generación pueda ofrecer una cierta QoS garantizada, deben considerarse una serie de funciones esenciales para administrar la QoS dentro de la UTRAN. Por tal motivo, debido a su importancia serán descritas a continuación:

3.6.3.2 Protocolo de Acceso al Medio (MAC)

Dado que en el sistema UMTS los usuarios no disponen continuamente de un recurso asignado, esto es, de una secuencia código sobre la que transmitir, se hace evidente la necesidad de definir un conjunto de reglas que permitan a los

usuarios acceder de forma eficiente al sistema, consiguiendo un recurso, y llegar a notificar al gestor de recursos sus requerimientos de transmisión para que posteriormente sean regulados en función de la calidad que se deba garantizar. En resumen la misión principal del protocolo de acceso al medio es especificar como los diferentes usuarios acceden a los recursos para iniciar la trasmisión de la información .

Aunque hasta la fecha se han estudiado un gran número y variedad de protocolos como S-ALOHA, CSMA/CD, ISMA, etc; todos ellos tienen en común que contienen un cierto grado de aleatoriedad en el acceso. Cuando mayor es este grado de aleatoriedad, mayor es su flexibilidad, pero peor es su comportamiento cuando tratan de preservar unos ciertos requisitos de retardo máximo en el acceso. Por tanto, cuando una cierta QoS debe ser garantizada, el grado de aleatoriedad debe ser reducido en la medida de lo posible.

Los esquemas de acceso basados en TDMA y FDMA presentan como característica el hecho de que un canal (frecuencia - ranura temporal) únicamente puede ser utilizado por un usuario a la vez, de modo que, en el marco de un acceso aleatorio como por ejemplo S -ALOHA, el intento de transmitir por parte de dos o más usuarios en un mismo canal producirá la pérdida por colisión de los paquetes involucrados en dicha transmisión.

Por el contrario, cuando se considera como técnica de acceso un esquema WCDMA, donde los usuarios comparten frecuencia y tiempo, y la discriminación entre señales se lleva a cabo mediante el uso de códigos diferentes para cada uno, los protocolos de acceso múltiple como S-ALOHA o ISMA adquieren una nueva dimensión al permitirse el acceso simultáneo de varios usuarios al sistema. En estas circunstancias, el límite de usuarios en el canal deja de ser 1 para pasar a depender directamente de la interferencia entre los diferentes usuarios que acceden, así como de otros parámetros inherentes al mecanismo de acceso usado tales como la ganancia de procesado[1] y el número de bits enviados y que

[1] Ganancia de procesado: Es la relación entre el periodo de bit Tb y el periodo de chip Tc en la técnica de acceso WCDMA.

finalmente se traducen en una cierta probabilidad de que el paquete transmitido sea o no correctamente recuperado.

Por último, se debe tener en cuenta que los protocolos de acceso múltiple no especifican la técnica de acceso a utilizar en el nivel físico ya que están situados en una capa superior de la estructura OSI.

3.6.3.3 Mecanismo de Gestión de Recursos

El propósito de este mecanismo es efectuar una apropiada gestión de los recursos para que las transmisiones se lleven a cabo ordenadamente según la QoS de cada una. Dicho de otra forma, el hecho de haber adquirido un recurso no da permiso directamente para llevar a cabo la transmisión, sino que debe ser el RNC quien, en base a las peticiones del conjunto de terminales, confirme o no dicho permiso tras la aplicación de un cierto algoritmo de gestión de recursos cuya misión es, por lo tanto, especificar cuando un usuario determinado, de entre el conjunto de usuarios del sistema, tiene permiso para transmitir en cada instante de tiempo, así como la cantidad de información que se puede enviar, es decir bajo las condiciones de cada clase de servicio.

Para la técnica UMTS uno de los algoritmos que actualmente se han considerado es el denominado WFQ[1] con priorización PQ[2] (ver Figura 3.6).

En este algoritmo se propone asociar a cada clase de tráfico con una cola separada o individual. Así por ejemplo una cola es dedicada para la clase de tráfico1, la cual tiene una prioridad estricta sobre las otras. Un máxima capacidad es asignada a cada clase de tráfico. De acuerdo a la máxima capacidad de WFQ el control de admisión limita el tráfico para cada clase de tráfico con la finalidad de evitar un cuello de botella.

---

[1]Revisar Anexo 4: Algoritmo WFQ.

[2]Referencia [37]: S. I. Maniatis, E. G. Nikolouzou, I. S. Venieris, "Convergence of UMTS and Internet Services for End-to-end Quality of Service Support".

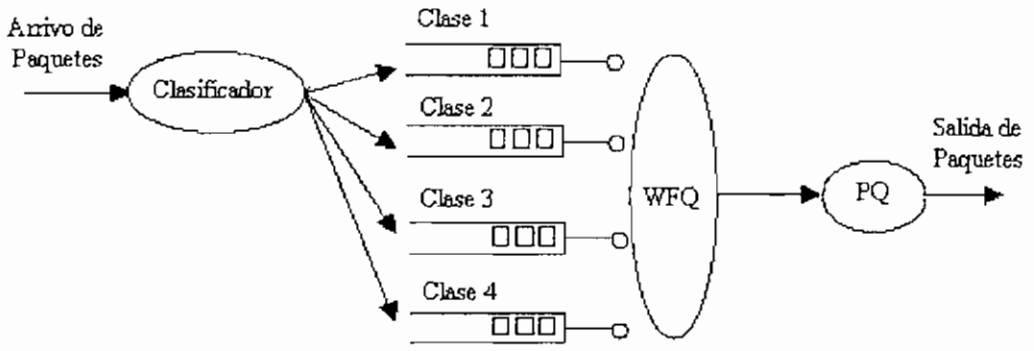


Figura 3.6 Un mecanismo de gestión de recursos en UMTS

Para la parte de priorización todos los usuarios que intentan transmitir deben ser clasificados de acuerdo a la clase de servicio (primer nivel de priorización) y si en caso de que dos o más usuarios pertenezcan a la misma clase de servicio, un segundo nivel de priorización es considerado.

Para este segundo nivel de priorización se ha definido el concepto de "Credito de Servicio (SCr)"[1], el cual mide la diferencia entre el servicio exigido y el servicio ofrecido. Sobre esta situación el valor de SCr de cada pedido dirigirá a determinar la prioridad de cada conexión, así el más alto valor tendrá el más alto nivel de prioridad. Por ello el SCr es un parámetro conveniente para determinar la prioridad entre las diferentes demandas.

El cálculo del valor de SCr está basado en la siguiente expresión:

$$SCr_{nuevo} = SCr_{anterior} + (b_{min} / b_{básica}) - num\_of\_tx\_ok \qquad \text{(Ec 3.1)}$$

donde:

$SCr_{anterior}$ = Anterior valor de SCr que ha sido actualizado

b_{min} = Tasa mínima garantizada para la conexión. Este valor representa la tasa de transmisión que una conexión ha contratado con el sistema.

$b_{básica}$ = Tasa básica de transmisión de la conexión. Este valor representa la tasa de transmisión que una conexión ha recibido del sistema.

[1]Referencia [38]: Luis Almajano, Jordi Pérez-Romero, "Packet Scheduling Algorithms for Interactive and Streaming Services under QoS Guarantee in a CDMA System", (UPC)..

num_of_tx_ok = Es el número de paquetes de datos de la conexión transmitidos con éxito durante el último intervalo de tiempo del sistema.

3.6.3.4 Control de Admisión (RAC)

Esta funcionalidad es responsable de determinar si un nuevo usuario que quiera incorporarse al sistema puede ser aceptado o no, de modo que el número total de usuarios que puede verse involucrado en los procesos establecidos por el protocolo de acceso y el algoritmo de gestión de recursos esté limitado. En definitiva, el control de admisión será responsable de indicar quien puede llegar a aplicar el conjunto de reglas fijado por el protocolo de acceso (Figura 3.7).

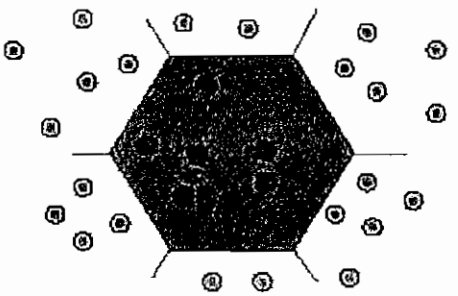


Figura 3.7 Control de admisión

El control de admisión se activa cada vez que el recurso radio de una celda ha de compartirse por un usuario o un RAB suplementario, o cuando hay un cambio de celda (transferencia intercelular).
El estudio del control de admisión en UMTS pasa por determinar a través de un cierto criterio de máxima degradación el máximo número de usuarios de cada clase de servicio que pueden tolerarse en el sistema para garantizar la QoS .

Los criterios de máxima degradación de la calidad de servicio para definir el control de admisión, suelen ser de tipo estadístico y están relacionados con parámetros de QoS estudiados en las secciones anteriores de este capítulo.

Es por ello que el control de admisión es el algoritmo que determina si una solicitud de conexión debe ser aceptada o rechazada en función de la interferencia o carga que añade a las conexiones ya existentes. Por lo tanto, es responsable de decidir si una nueva RAB puede ser establecida. El control de admisión considerado hace uso de la estimación del incremento de carga que genera en la red de radio el establecimiento de la solicitud de conexión.

Asumiendo que se tienen N usuarios admitidos en el sistema, se debe verificar que el usuario (N + 1) cumpla[1]:

$$\eta = (1+i).\sum_{j=1}^{N} \frac{1}{\frac{W}{\nu_j.\left(\frac{E_b}{N_o}\right)_j.R_j}+1} + (1+i)\frac{1}{\frac{W}{\nu_{N+1}.\left(\frac{E_b}{N_o}\right)_{N+1}.R_{N+1}}+1} \leq \eta_{max} \quad \text{(Ec 3.2)}$$

donde:

η = Factor de carga.

W = Tasa de codificación o chip (3.84 Mcps en sistemas WCDMA).

ν_j = Factor de actividad de la fuente de tráfico, el cual es obtenido en términos estadísticos.

E_b/N_o = Proporción de energía de la señal por bit con respecto a la densidad de potencia del ruido para el usuario j-ésimo.

R_j = Tasa de bit del usuario j-ésimo.

i = Factor de interferencia entre celdas (interferencia entre la celda adyacente y la celda actual).

La UTRAN rechaza las peticiones que no pueden ser atendidas según la ecuación 3.2 y el algoritmo de gestión de recursos, o las pone en espera durante un cierto tiempo si existe la posibilidad (ver Figura 3.8). Es decir, por ejemplo, para una solicitud de conexión de un usuario interactivo se debe comprobar la ecuación 3.2 ya que se debe proporcionar cierto tipo de QoS en términos de tasa o retardo. El

[1]Referencia [39]: J. Sánchez, "Mixing Conversational and Interactive Traffic in the UMTS Radio Access Network", (UPC)..

control de admisión para una solicitud de un usuario de la clase conversacional también debe comprobar la ecuación 3.2. Si se cumple la condición, la solicitud es aceptada; caso contrario, se deberá activar el control de congestión dependiendo de la carga real instantánea para reducir la carga provocada por los usuarios de clase interactiva y proporcionar espacio para la solicitud. Únicamente si no es posible liberar suficiente capacidad de los usuarios interactivos se rechazará la solicitud de conexión conversacional.

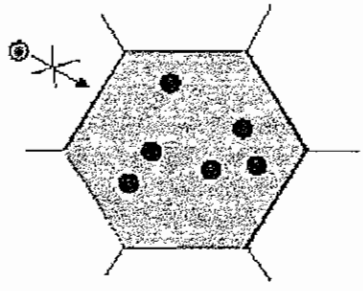


Figura 3.8 Rechazo de una petición que no puede ser atendida

Se debe tener en cuenta que, desde el punto de vista del usuario, el rechazo de una llamada durante la fase de establecimiento es más fácil de aceptar que cortar una comunicación en curso debido a un fallo en la conmutación de la llamada en curso.

3.6.3.5 Control de Congestión

Otra funcionalidad que se suele considerar se denomina control de congestión, que consistente en habilitar mecanismos de control para hacer frente a posibles situaciones en las que, debido a la variabilidad del tráfico, se pudieran comprometer las garantías de los usuarios aceptados en el sistema.

El control de congestión debe actuar cuando los usuarios admitidos no pueden satisfacer los requerimientos de QoS durante un cierto periodo de tiempo debido a una sobrecarga en el sistema o también se activa para facilitar que los usuarios de clase conversacional puedan ser admitidos en el sistema.

Para detectar si la red está en congestión o no, se toma en consideración el criterio de que cuando el factor de carga es superior a un cierto umbral ($\eta \geq \eta_{máx}$) durante un cierto periodo de tiempo ΔT la red está congestionada[1].

Después de haber detectado que existe congestión en la red se deben activar otros mecanismos como:

- Priorización, la cual consiste en ordenar en una tabla los diferentes usuarios empezando por el de baja prioridad hasta el de mayor prioridad en función de los requerimientos de QoS.
- Reducción de la carga. Este mecanismo se encarga de no aceptar ninguna solicitud de conexión y de limitar la máxima velocidad de transmisión de cierto número de usuarios, empezando por el usuario menos prioritario de la tabla de prioridades.
- Chequeo de la carga. Después de haber reducido la carga se debe volver a comprobar la condición que activa o desactiva el control de congestión. Si la congestión persiste, se debe realizar una nueva reducción de carga. Se considera que la congestión se ha solucionado si el factor de carga es inferior a cierto umbral ($\eta \leq \eta_{máx}$) durante un cierto periodo de tiempo ΔT

3.6.3.6 Control de potencia

El control de potencia es unos de los mecanismos fundamentales del sistema WCDMA que se ha considerado en esta tesis, pues al ser esta una técnica de acceso limitada por interferencias en la que las señales comparten tiempo y frecuencia, los desajustes en la potencia emitida por parte de los diferentes usuarios, provocan el efecto denominado cerca-lejos[2] (near-far effect), el cual consiste en que si todos los usuario emiten con la misma potencia, las señales de los emisores más cercanos llegarían a la estación base con más potencia que las

[1] Referencia [40]: Frank Yong Li, "Providing Conformance of the Negotiated QoS using Traffic Conditioning for Heterogeneous Services in WCDMA Radio Access Networks", Norwegian University.
[2] Referencia [41]: Carlos Díaz, "Arquitectura de Protocolos en la Red de Acceso UMTS", pág 18-19.

de los lejanos, quedando estas últimas enmascaradas, es decir, empeoraría su recepción (ver Figura 3.9).

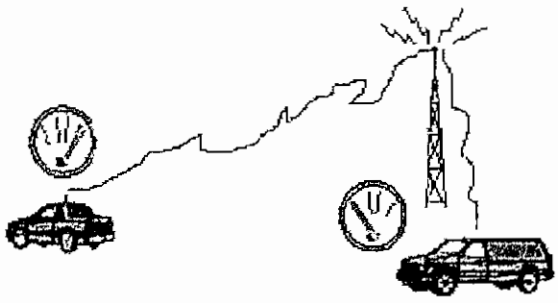


Figura 3.9 Efecto Cerca-Lejos

Para resolver este problema es preciso utilizar técnicas de control de potencia, de forma que todas las señales lleguen a la estación base con el mismo nivel de potencia. Esto se consigue haciendo que cada usuario emita con una potencia distinta en función de su distancia, condiciones de propagación y carga del sistema. Al utilizar control de potencia, se reduce la interferencia y por lo tanto se maximiza la capacidad total del sistema y además se reduce el consumo de los terminales móviles que se encuentren más cerca de la estación base. El control de potencia debe tener tres características: exactitud, rapidez para compensar los desvanecimientos, y un gran rango dinámico para controlar móviles cercanos y alejados.

Hay dos tipos de algoritmos de control de potencia en UMTS: control de potencia en lazo abierto y control de potencia en lazo cerrado[1].

Control de Potencia en Lazo Abierto

Se produce cuando un usuario decide acceder al sistema. Inicialmente, este nuevo usuario no estará controlado en potencia, con lo cual accederá al sistema con un nivel de potencia inicial que será una variable aleatoria. Si esta potencia inicial no es suficiente para ser atendido, la incrementará a intervalos constantes

[1]Referencia [22]: Dejan M. Novakovic, "Evolution of the Power control techniques for Ds-cdma toward 3G wireless communication systems", IEEE Communications Surveys, pág 3-14..

en dB, hasta que reciba confirmación de la estación base de que su señal ha sido recibida. Si desde un primer momento la potencia hubiera sido excesiva, habría entrado directamente a ejecutar los algoritmos de control de potencia.

Control de Potencia en Lazo Cerrado

Con esta técnica, la estación base realiza medidas de la potencia que recibe del móvil y le envía una serie de comandos para que este suba o baje la potencia de transmisión. En el enlace ascendente el RNC establece el BER para el servicio solicitado y a partir de ella calcula el SIR[1] objetivo enviándoselo al Nodo B. El Nodo B estima el SIR y lo compara con el recibido determinando si la potencia del móvil debe ser incrementada o decrementada. Esta operación se realiza 1500 veces por segundo y recibe el nombre de Inner Loop. Por otro lado cada 10 ms el RNC calcula el SIR y ajusta el SIR objetivo. A este proceso se le conoce con el nombre de Outer Loop y es controlado por la capa RRC (Control de los recursos de radio). En el downlink los usuarios reciben distinta interferencia de las demás células en función de su posición, y por lo tanto hay que variar las potencias para tener un SIR fijo (esta situación se da por ejemplo en el borde celular). En este caso el UE manda unos bits de control TPC al Nodo B en función del SIR estimado y del que tiene como objetivo. En la Figura 3.10 se muestra el procedimiento.

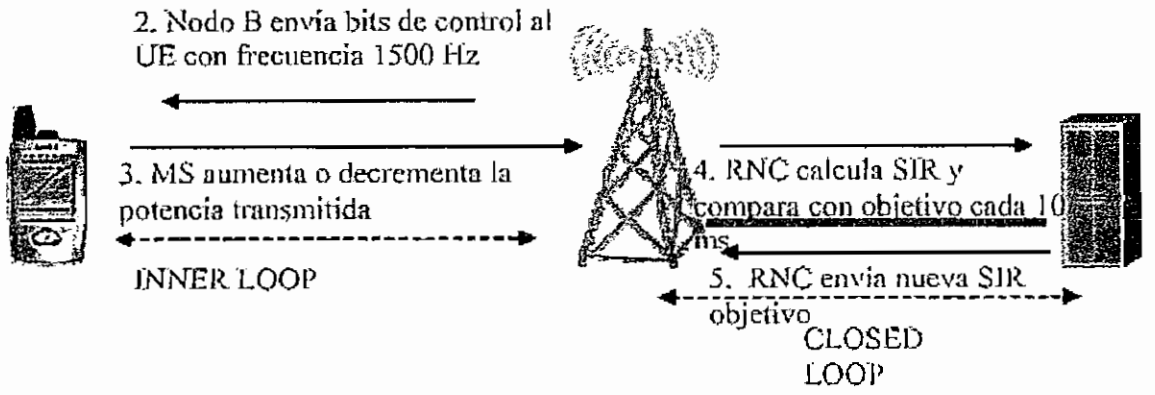


Figura 3.10 Control de potencia en bucle cerrado

[1] SIR o S/I es la relación señal a interferencia

3.6.3.7 Acondicionador de tráfico

Como se mencionó en secciones anteriores, un acondicionador de tráfico mantiene la concordancia entre el QoS negociado para un servicio y el tráfico de unidad de datos. El condicionado del tráfico es realizado por comprobación del tráfico (*traffic policing*), el cual consiste en el hecho de monitorear el tráfico para que cumpla el patrón acordado y por conformación del tráfico (*traffic shaping*), cuyo objetivo es regular el tráfico a transmitir con el objeto de eliminar la congestión en la red debido a las características de gran variabilidad del tráfico.

Un mecanismo de conformación de tráfico es empleado por el flujo de tráfico en el enlace ascendente sobre cada UE. Los paquetes recibidos en el Nodo B son enviados al RNC y la función de comprobación del tráfico los manipula para prevenir que excedan sus características de tráfico (Figura 3.11).

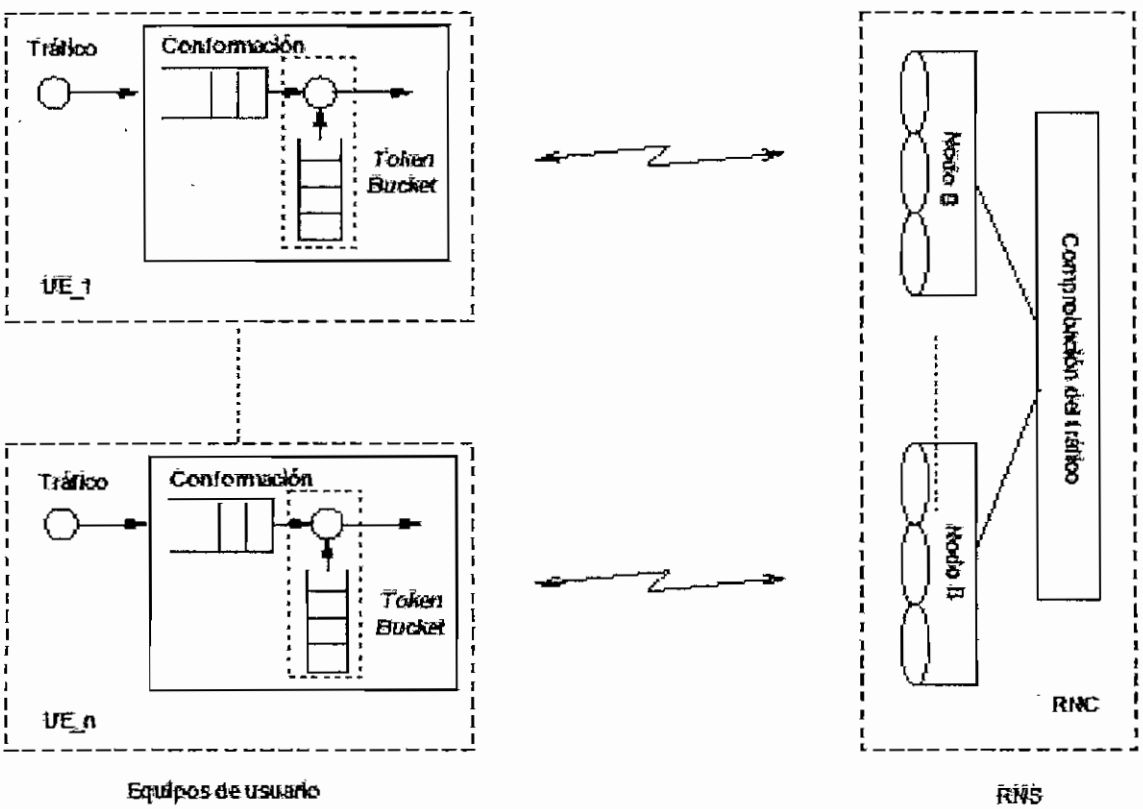


Figura 3.11 Acondicionador de tráfico

Es de relevancia indicar que el conformador de tráfico que ha sido adoptado como referencia en UMTS por la 3GPP es el denominado algoritmo *Token Bucket*, que a continuación será descrito.

Algoritmo *token bucket*

El objetivo de este algoritmo es regular el tráfico a una tasa de transmisión (r, rate) y acomodar las ráfagas de tráfico a un tamaño b (b, bucket size)[1]. El funcionamiento del algoritmo es el siguiente: el cubo contiene *tokens* generados a una tasa *r* (Figura 3.12). El cubo puede admitir como máximo *b tokens*, estando al inicio lleno. Para que se transmita un bit se tiene que coger un *token* del cubo y eliminarlo. Mientras existan *tokens* en el cubo, la fuente puede insertar el tráfico a la red a la tasa deseada. Cuando se acaban los *tokens* tendrá que esperar al próximo *token* que se genere, lo que implica que la tasa de transmisión disminuye a r. En esencia, lo que permite *token bucket* es poder transmitir en un determinado intervalo de tiempo paquetes a una tasa de valor r.

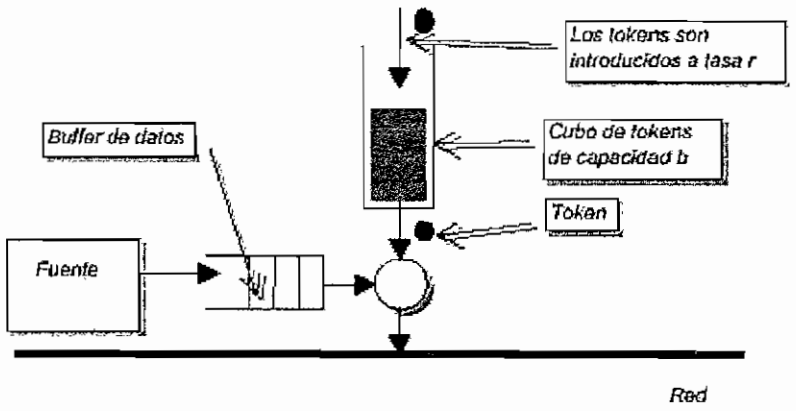


Figura 3.12 Algoritmo *Token bucket*

De acuerdo al algoritmo descrito, la cantidad de datos enviados D(T) sobre cualquier intervalo de tiempo T obedece a la regla:

[1]Referencia [40]: Frank Yong Li, "Providing Conformance of the Negotiated QoS using Traffic Conditioning for Heterogeneous Services in WCDMA Radio Access Networks", Norwegian University.

$$D(T) \leq r.T + b \quad \text{(Ec 3.3)}$$

En otras palabras la conformación del tráfico según *token bucket* puede decirse que los datos están acomodados o conformados si la cantidad de datos sometidos durante cualquier periodo de tiempo escogido no exceda $(r.T + b)$.

Comprobación del tráfico en el RNC

La función de comprobación del tráfico compara la conformación del tráfico de datos de usuario con el predefinido acuerdo de servicio.

También se debe indicar que todos los paquetes han pasado el control de admisión de llamadas antes de realizar esta nueva fase.

Esta función primeramente realiza una clasificación, la cual consiste simplemente en chequear la cabecera de cada paquete recibido y enviar la información correspondiente para posteriormente realizar la comprobación, de acuerdo a las diferentes clases de servicio así como del estado de la conformidad del tráfico.

Dependiendo de los parámetros de un paquete enviados por el proceso de clasificación, la función de comprobación en el RNC realiza la política correspondiente para cada paquete individual. Los paquetes no marcados con los parámetros relevantes de ese servicio son llamados "no acordados", mientras los que poseen esos parámetros son llamados "acordados". Como se muestra en la Figura 3.13 los paquetes de datos denominados "no acordados" serán reconocidos solo si el canal no está congestionado, es decir si el total del nivel de interferencia de todas las llamadas actuales no exceden el umbral, de lo contrario simplemente serán descartados. Para los paquetes de datos denominados "acordados", el cálculo de la carga tomará en cuenta solamente los paquetes "acordados". Si la carga excede el umbral los paquetes "no acordados" serán

descartados. Un paquete que este de acuerdo a todos los parámetros también puede ser descartado si existe excesiva carga en el canal.

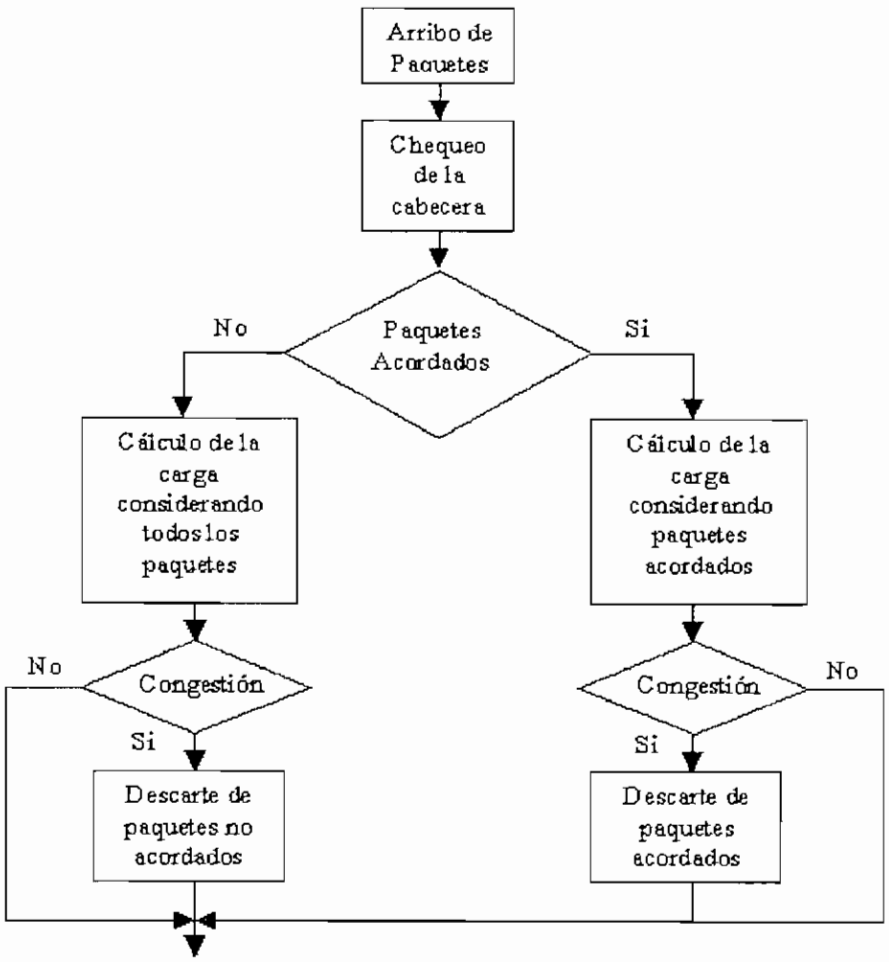


Figura 3.13 Comprobación del tráfico en el RNC

3.6.3.8 Control de *Handover*

Es muy complicado introducir un modelo de *handover* dado a la topología heterogénea de la red UMTS. Por otra parte es quizá la principal razón para las interrupciones del enlace. Durante el *handover* voz y datos pueden ser perdidos. Además la frecuencia del *handover* aumenta al disminuir el radio de las celdas o si la velocidad de los usuarios móviles aumenta.

En UMTS hay dos clases de *handovers*: *handovers* intra sistema y *handovers* inter sistema.

Los *handovers* intra sistema son clasificados en dos clases: *handovers* intra-frecuencia y *handovers* inter-frecuencia.
Los *handovers* intra-frecuencia son clasificados en dos clases:

1. Denominado *soft handover* (handover suave) es aquí donde el equipo del usuario se conecta a dos sectores de diferentes estaciones base simultáneamente.
2. Llamado *hard handover* (handover duro) y que consiste en que el equipo del usuario se conecta solo a un sector en un determinado tiempo, lo que provoca un cierto retardo.

Los *handovers* inter-frecuencia se refiere cuando un usuario se traslada por ejemplo de una macro celda a una micro celda.

Por otro lado los *handovers* inter sistema son *handovers* entre WCDMA y GSM o entre WCDMA y algún otro sistema.

Soft handover

En *soft handover* el equipo del usuario se conecta a dos o más estaciones base al mismo tiempo. Esto significa que la misma información fluye a través de muchas estaciones base y el RNC tiene la tarea de recibir todas esas señales. El equipo del usuario entra en estado de *handover* si la diferencia entre las señales medidas de varias estaciones base están dentro del valor de umbral.

Como se muestra en la Figura 3.14b, cuando el móvil está en el borde de la celda entre BS1 y BS2, y se mueve hacia BS2, existen varias etapas en el proceso de *handover*, las cuales se pueden observar en la Figura 3.14a.

Tomando como referencia la Figura 3.14a, en el punto 1 la fuerza de la señal desde BS1 llega a ser igual a un valor de umbral inferior. Por otro lado, basado sobre las medidas del equipo de usuario el RNC identifica que hay una señal vecina disponible que tiene adecuada fuerza para mejorar la calidad de la conexión. Por tanto, la añade a la señal que está activa.

Sobre este evento, el equipo de usuario tiene dos conexiones simultaneas al UTRAN y así se beneficia de la suma de las señales, que consiste de la señal de BS1 y de BS2 (punto 2). En este punto la calidad de la señal de BS2 empieza a llegar a ser mejor que la de BS1. Por tanto el RNC mantiene este punto como el comienzo para el cálculo del límite del *handover*. En (3) la fuerza de la señal de BS2 empieza a ser igual o mejor que el valor del umbral inferior. Así su fuerza es adecuada para satisfacer el QoS requerido de la conexión. Por otro lado, la fuerza de la suma de las señales excede el valor de umbral superior, causando interferencia adicional al sistema. Como resultado, el RNC elimina la señal de BS1 a la señal activa.

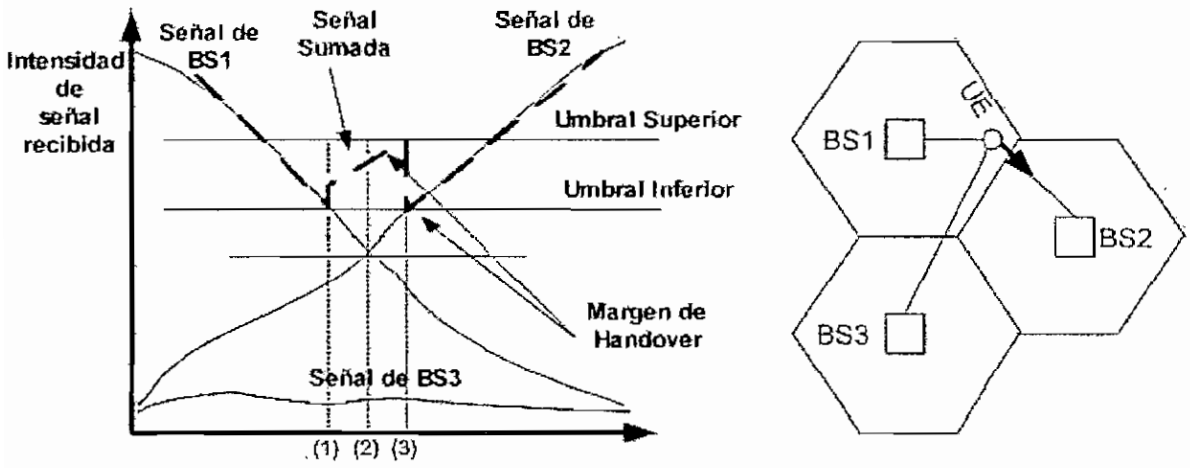


Figura 3.14 ***Soft handover***[1]

Si no es posible para el UE usar *soft handover*, este tiene que usar *hard handoff*. Esto puede pasar debido a razones de carga, cobertura, etc con lo que habrá algo de retardo.

[1]Referencia [42]: Smaragdakis Georgios, "TCP Performance over UMTS Network", Technical University of Crete, pág 37-39.

CAPÍTULO IV

SERVICIOS Y APLICACIONES EN LAS REDES UMTS DE ACUERDO A LAS DIFERENTES CLASES DE QoS

CAPÍTULO IV

SERVICIOS Y APLICACIONES EN LAS REDES UMTS DE ACUERDO A LAS DIFERENTES CLASES DE QoS

En este capítulo se abordarán los más importantes servicios y aplicaciones en un entorno 3G. Además de ello se describirá un marco para el desarrollo de servicios en un ambiente de tercera generación, en el que se considerarán los requerimientos técnicos que debe poseer la red UMTS para el correcto funcionamiento de los diferentes servicios.

4.1 CONCEPTOS DE SERVICIOS Y APLICACIONES[1] [2] [3]

Los conceptos de servicios y aplicaciones en UMTS son definidos a continuación:

4.1.1 SERVICIOS

Los servicios son un portafolio de opciones ofrecidas por los prestadores de servicios a los usuarios. Los servicios son elementos que el proveedor de servicios puede elegir para cobrar por separado o como un paquete. Ellos serán el factor de diferenciación entre los proveedores de servicio en el ambiente de tercera generación, y también con respecto a los sistemas de segunda generación. Es probable que los usuarios seleccionen su proveedor de servicios preferido basados en las opciones disponibles en su portafolio.

---

[1]Referencia [43]: EURESCOM Project P921, "Review of foreseen UMTS applications".
[2]Referencia [18]: UMTS FORUM, "Enabling UMTS/Third Generation Services and Applications", Report N°11.
[3]Referencia [19]: UMTS FORUM, "Support of Third Generation Services using UMTS in a Converging Network Environment", Report N°14.

4.1.2 APLICACIONES

Las aplicaciones son el conjunto de actividades llevadas a cabo para responder a las necesidades de los usuarios en una situación dada, como por ejemplo para propósitos tales como negocio, educación, comunicación personal o entretenimiento. Esto implica la utilización de software y hardware que podrían realizarse de una manera automática y podrían accederse localmente o remotamente. En el último caso se solicita el uso de servicios de telecomunicaciones.

Es importante indicar que las aplicaciones no aparecen sobre la factura del usuario.

Una aplicación es implementada en el dominio de equipamiento terminal (TE) en UMTS, la cual intercambia información con el dominio de terminación móvil (MT). A más de las definiciones descritas anteriormente, es importante indicar que el contenido es la información que el usuario necesita y por la cual está dispuesto a pagar , en tanto la calidad con la que recibe esa información está de acuerdo a lo contratado.

Después de haber mencionado los diferentes conceptos se procederá a estudiar las más importantes aplicaciones y servicios presentes en una red UMTS.

4.2 APLICACIONES EN UMTS[1]

Las aplicaciones son el conjunto de características sobre los cuales los usuarios finales pueden realizar operaciones. A continuación se mencionarán las más importantes aplicaciones:

[1]Referencia [18]: UMTS FORUM, "Enabling UMTS/Third Generation Services and Applications", Report N°11, pág: 18-43.

Aplicaciones multimedia

Las aplicaciones multimedia son los habilitadores para los servicios de banda ancha con cualquier requerimiento en tiempo real (telefonía) y/o en tiempo no real (acceso a Internet, transferencia de archivos). UMTS toma cuidado de la demanda del ancho de banda en combinación con la movilidad global. En los sistemas 2G existen aplicaciones multimedia pero muy limitadas debido al ancho de banda, por lo que UMTS se convierte en una gran oportunidad de nuevos negocios.

Comercio móvil

El comercio electrónico y su subconjunto, el comercio móvil, tendrán un impacto importante sobre los ingresos de las operadoras a mediano plazo. Mediante el comercio electrónico se hará compras y transacciones financieras directamente de un terminal móvil, lo que no es realizable con la tecnología de 2G.

Aspectos de Seguridad

Una de las más grandes preocupaciones en el comercio móvil es la seguridad. Por tal motivo múltiples aplicaciones serán soportadas a través del uso de las tarjetas inteligentes o USIM que, como se vio en el Capítulo 2, es en donde los procesos de encriptación y autenticación son realizados. Es por ello la importancia del estudio de la seguridad en UMTS, ya que muchas transacciones comerciales serán efectuadas a través de este medio, por lo que será un aspecto tecnológico decisivo en la entrega de servicios. También se debe mencionar que las transacciones comerciales en 2G son menores debido a la débil seguridad existente en tales sistemas.

La Figura 4.1 ilustra el potencial del comercio móvil en UMTS. El UMTS forum espera que casi el 50% de suscriptores de telefonía móvil en todo el mundo sean suscriptores de Internet móvil en el 2010.

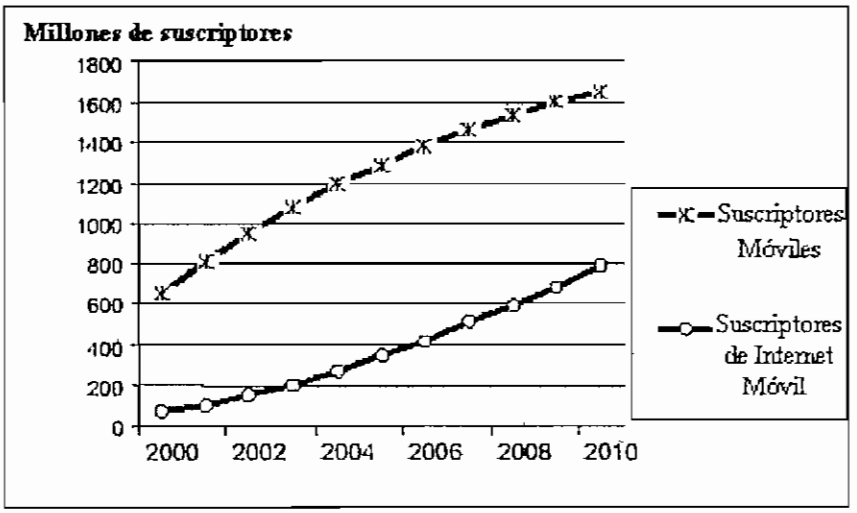


Figura 4.1 Suscriptores móviles en el mundo[1]

Mensajería multimedia unificada

El incremento del volumen de comunicaciones está resultando en una carga excesiva de información. La transmisión de mensajes multimedia aparece como una solución para el mencionado problema. Los mensajes multimedia consistirán en la transmisión de fax, voz, aplicaciones de software, imágenes y archivos de datos.

Esto puede ser por tanto una aplicación que puede entregar un significativo valor agregado al usuario final. Teniendo tan solo un buzón electrónico y un número para voz, fax y e-mail (todos los mensajes, tipos y formatos) mejora el tiempo de eficiencia para el usuario final. Los usuarios pueden ahorrar tiempo solamente teniendo que chequear el buzón con el acceso móvil y fijando el acceso para todos sus mensajes.

La mensajería multimedia ofrecerá nuevas características técnicas más allá del e-mail, fax y que no se encuentran en los sistemas 2G, como:

- La utilización de un conjunto de protocolos que interoperarán con el estándar existente para correo electrónico.

[1] Referencia [18]: UMTS FORUM, "Enabling UMTS/Third Generation Services and Applications", Report N°11, pág: 24.

- Transmisiones óptimas basadas sobre las clases de servicio.
- Mayor seguridad que consistirá en identificación personal y medidas de prevención del fraude.
- Los mensajes multimedia consistirán en reconocimiento de voz.

Posicionamiento

UMTS permite determinar la ubicación de un usuario con lo que se puede habilitar un gran número de servicios, aunque con propiedades diferentes de acuerdo a parámetros de posicionamiento tales como: la disponibilidad, exactitud y confiabilidad.

Cada método de posicionamiento (terrestre o satelital) tiene diferentes valores asociados con esos parámetros (diferentes niveles de exactitud). Es probable que aplicaciones que usan información de localización tengan diferentes requisitos en cuanto a los valores de los parámetros.

Los sistemas de tercera generación con su estructura de celdas (pico/micro/macro celdas como se observa en la Figura 4.2) ofrecerán una capacidad de localización que será suficiente para soportar muchas clases de servicios basados en la localización como la facturación basada en la zona, lo que no existe en 2G.

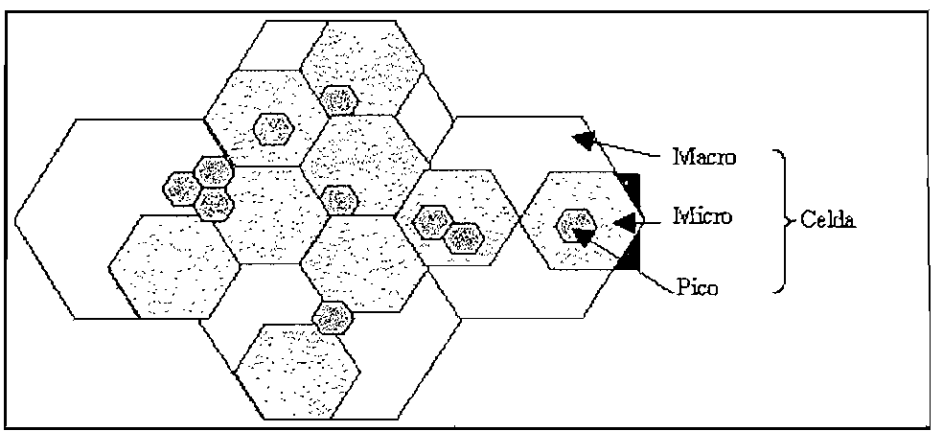


Figura 4.2 Estructura de celdas en UMTS

Además de la estructura de celdas para determinar la localización de un terminal, se puede utilizar la técnica RTT (*Round Trip Time*) [1] efectuada por las estaciones base y que consiste en medir el tiempo entre la emisión de una trama en el sentido descendente (desde la estación base hacia el terminal móvil) y la recepción de la trama correspondiente en el sentido ascendente (desde el terminal móvil hacia la estación base). Utilizando esta técnica, la estación base puede calcular la distancia entre ella y el terminal móvil con una mayor precisión.

Difusión interactiva

La difusión es principalmente de uno a muchos, pero gracias a las técnicas digitales y a la capacidad de ancho de banda que existirán en UMTS se permitirá la provisión interactiva de servicios multimedia a una gran audiencia de usuarios móviles. Por ello las difusoras están contemplando el uso de sistemas de comunicaciones móviles como UMTS para aumentar su contenido multimedia. Los operadores móviles están buscando proporcionar acceso a los usuarios a tales contenidos y así proporcionar una amplia gama de servicios.

4.3 SERVICIOS EN UMTS[2]

Esta sección en el presente trabajo identifica las más importantes categorías de servicio, las cuales serán diferenciadas por las diferentes clases de QoS. También es importante mencionar que los servicios que se indican a continuación deben poseer las prestaciones básicas de seguridad, las cuales son: autenticación y confidencialidad. Si la red no apoya con estas prestaciones, el usuario debe ser informado de esta situación y debe tener la posibilidad de acceder o negarse a las conexiones.

---

[1]Referencia [44]: Revista de Telecomunicaciones de Alcatel, "Servicios móviles basados en la posición: puntos fundamentales", 1er Trimestre 2001, 73-74.

[2]Referencia [13]: 3 rd Generation Partnership Project 3GPP, TS 22.105, "Services & service capabilities".

Para un mejor apreciación, en la Figura 4.3 se indica la estructura de servicios que podrían ser ofrecidos por los proveedores en un entorno de tercera generación.

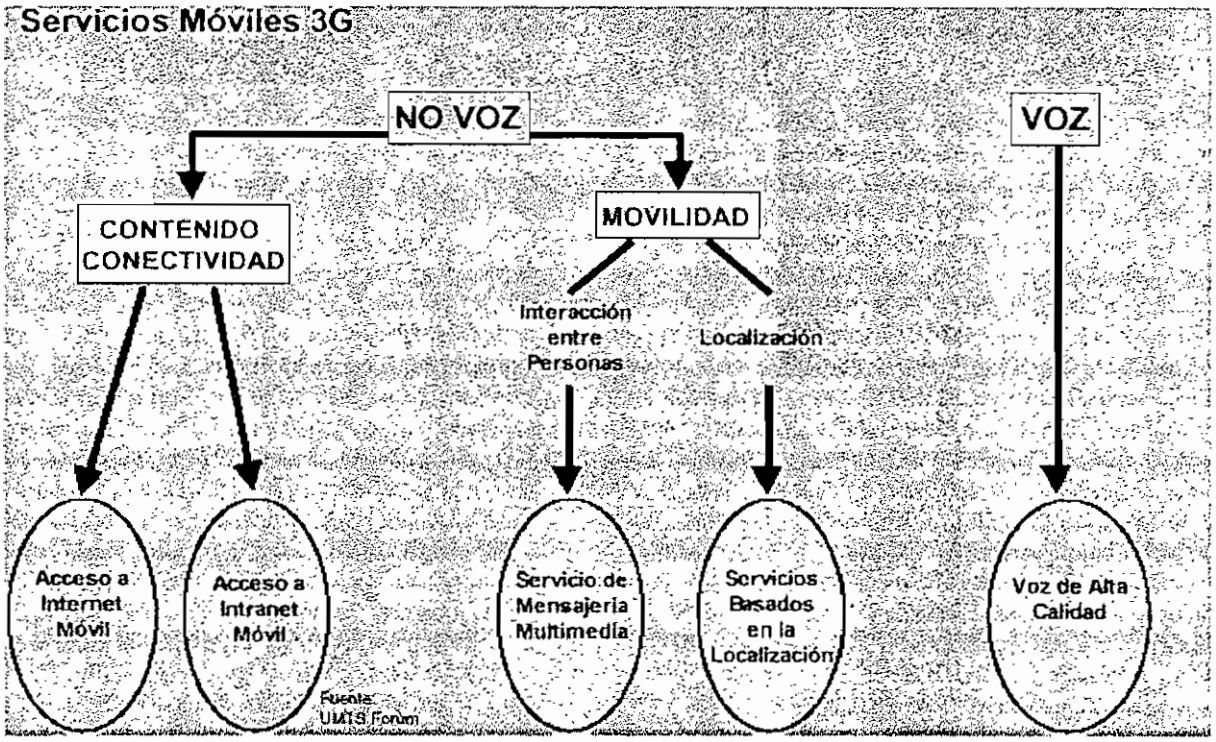


Figura 4.3 Servicios móviles 3G

A continuación se describirá los diferentes tipos de servicios.

4.3.1 SERVICIOS EN TIEMPO REAL

Los requerimientos de QoS en tiempo real son dados por la percepción humana debido a la naturaleza de tales servicios. Por tanto, ellos aumentan los requerimientos acerca de la calidad de servicio, poniendo estrictas demandas sobre el retardo de transferencia y el jitter. Sin embargo, estos servicios tienen requerimientos menos exigentes sobre la proporción de pérdidas de paquetes.

Servicio de Voz

El requerimiento sobre el retardo de transferencia es el parámetro que más se debe considerar en este tipo de servicio. Para evitar dificultades en las comunicaciones de voz, la recomendación de la ITU-T G.114 sugiere los siguientes límites:

- 0 a 150 ms rango preferido
- 150 a 400 ms rango aceptable
- sobre los 400 ms rango inaceptable

Debido a que el oído humano es altamente intolerante a las variaciones de retardo (jitter), se lo debe reducir a un nivel tan bajo como 1 ms. Con respecto a la pérdida de información, el oído humano es tolerante a una cierta cantidad de distorsión de la señal, colocando la máxima razón de error de marco o trama (FER) en 3%.

Servicio de video y audio en tiempo real

La transmisión de video y audio en tiempo real es un típico servicio de comunicación que puede ser soportado por los sistemas de tercera generación para los usuarios móviles. Este servicio implica un sistema *full duplex*, llevando video y audio para un ambiente conversacional. Por tanto, se aplican los mismos requerimientos de retardo que para los servicios de voz. Una vez más, la percepción humana es tolerante a algunas pérdidas de información. Se espera obtener una calidad de video aceptable en la región de 1%.

En la actualidad, es decir en los sistemas 2G, este servicio no ha sido tan exitoso debido a la carencia de ancho de banda, pero en UMTS este servicio es posible debido a que soporta los requerimientos de ancho de banda y de movilidad, permitiendo que tome lugar independientemente de la ubicación. Dentro de esta clase de servicio se puede mencionar a:

Servicios de educación

Los servicios de aprendizaje en lugares remotos pueden ser proporcionados vía UMTS, en donde la instalación de líneas sería un costo muy elevado (áreas rurales o de baja densidad). La habilidad de UMTS para proporcionar gran ancho de banda, con una aceptable QoS, combinado con el bajo costo de instalación de la infraestructura, permitirá a estudiantes y profesores acceso a la educación y material de soporte en tiempo real.

Servicio de transmisión de datos

La transmisión de datos en tiempo real se caracteriza por estrictos límites sobre los requerimientos de retardo, como por ejemplo valores de 250 ms. La diferencia entre los servicios de voz y video con esta categoría es la cero tolerancia para la pérdida de información. Dentro de este servicio se puede nombrar a:

Juegos Interactivos

Los requerimientos para juegos interactivos dependen del juego específico que se este utilizando, pero es claro que requerirán muy cortos retardos. UMTS ofrecerá la posibilidad de jugos interactivos independientemente de la ubicación y el tiempo. Esto permitirá a los usuarios jugar con cualquier usuario alrededor del mundo.

Los sitios web permitirán a los usuarios jugar por diversión o por dinero, siendo este último posible si el usuario abre una cuenta y deja un deposito en efectivo, por lo que se necesita altos grados de seguridad en la transacción.

En la Tabla 4.1 se muestra los valores de algunos parámetros para los servicios mencionados anteriormente.

Tabla 4.1 Servicios en tiempo real/Conversacional-Expectativas de funcionamiento para el usuario final[1]

Parámetros de funcionamiento					
Servicio	Aplicación	Velocidad	Retardo	Variación del Retardo	Pérdida de Información
Audio	Telefonía	4-25 kbps	<150 msec preferido <400 msec aceptable	< 1 msec	< 3% FER
Video	Videotelefonía	32-384 kbps	< 150 msec preferido <400 msec aceptable		< 1% FER
Datos	Telemetría control	<28.8 kbps	< 250 msec		Cero
Datos	Juegos interactivos	< 1 KB	< 250 msec		Cero
Datos	Telnet	< 1 KB	< 250 msec		Cero

4.3.2 SERVICIOS *STREAMING* (TRANSFERENCIA CONTINUA)

Streaming significa ver video o escuchar audio de una manera unidireccional (de la red al usuario). Los requerimientos de QoS son caracterizados por la necesidad de preservar la relación de tiempo entre los paquetes de información.

El resultado de tales requerimientos para este esquema de comunicación será el soporte de servicios *streaming* en tiempo real (ver Tabla 4.2).

Audio *streaming*

Audio *streaming* espera proporcionar mejor calidad que la telefonía convencional, por tanto deben ser más estrictos los requerimientos sobre el BER.

No obstante, como en los mensajes de audio no hay elementos conversacionales involucrados, los requerimientos de retardo pueden ser relajados.

[1] Referencia [13]: 3 rd Generation Partnership Project 3GPP, TS 22.105, "Services & service capabilities", pág:15.

Video en sentido único

Como con el audio *streaming* la principal característica es que no hay un elemento conversacional, significando que los requerimientos de retardo no serán tan estrictos.

Tabla 4.2 Servicios Streaming -Expectativas de funcionamiento para el usuario final[1]

Parámetros de funcionamiento					
Servicio	Aplicación	Velocidad	Retardo	Variación del Retardo	Pérdida de Paquetes
Audio	Música de alta calidad	5-128 kbps	< 10 sec	< 2sec	< 1% Proporción de paquetes perdidos
Video	Transmisión de imágenes en movimiento (películas)	20-384 kbps	< 10 sec	<2 sec	< 2% Proporción de paquetes perdidos
Datos	Grandes transferencias de datos	< 384 kbps	< 10 sec		Cero
Datos	Transmisión de fotos		< 10 sec		Cero

Servicio de datos *streaming*

El servicio de datos *streaming* tiene como cualidades una mayor tolerancia al retardo y cero pérdidas de información. Por tal motivo, este servicio puede abarcar a:

Telemetría (monitoreo)

Monitoreo cubre una amplia gama de aplicaciones, pero generalmente es tomado en cuenta para actividades de baja prioridad como por ejemplo, la detección de una señal para efectuar el control en un determinado sistema, en donde se permiten valores de retardo no tan estrictos, pero que no toleran pérdidas de información.

[1]Referencia [13]: 3 rd Generation Partnership Project 3GPP, TS 22.105, "Services & service capabilities", pág:16.

Transmisión de imágenes (fotos)

En la transmisión de imágenes desde un simple error de bit puede tener grandes efectos sobre la calidad de la imagen, por lo que en esta categoría se debe en general tener cero pérdidas de información. En cuanto a los requisitos de retardo no son muy estrictos.

4.3.3 SERVICIOS INTERACTIVOS

Los servicios interactivos se refieren a los usuarios que están pidiendo datos a un equipo remoto (servidor). Ejemplos de interacciones son los navegadores web (*web browsing*), y la recuperación de base de datos. Para el tráfico interactivo las características fundamentales para QoS son: el modelo de contestación de demanda al usuario final y preservar la carga del contenido. Por tanto el retardo de ida y vuelta es uno de los atributos claves en combinación con un BER bajo (ver Tabla 4.3).

Mensajes de voz

Los requerimientos para la pérdida de información son esencialmente los mismos que para el servicio de voz en la clase conversacional, pero con una diferencia clave, que aquí hay mayor tolerancia al retardo puesto que no hay ninguna conversación directa involucrada. Un retardo de unos pocos segundos aparece ser razonable para esta aplicación.

Datos

Como una regla general, un requerimiento clave para la transferencia de datos es garantizar esencialmente cero pérdidas de información. Las diferentes aplicaciones por tanto tienden a distinguirse por el retardo que puede ser tolerado por el usuario final desde que el contenido es pedido a la fuente hasta que es presentado al usuario. Es por ello, que dentro de este servicio se puede mencionar a los navegadores web.

Navegadores web

Esta categoría se refiere a recuperar y ver el componente HTML de una página Web. Desde el punto de vista del usuario, la principal factor de rendimiento es cuan rápido una página aparece después de que ha sido pedida. Un valor de 0.5 segundos sería deseable.

Tabla 4.3 Servicios Interactivos -Expectativas de funcionamiento para el usuario final[1]

Parámetros de funcionamiento					
Servicio	Aplicación	Velocidad	Retardo	Variación del retardo	Pérdida de Información
Audio	Mensajes de voz	4-13 kbps	< 1 sec preferible < 2 sec acceptable	< 1 msec	< 3% FER
Datos	Navegadores Web - HTML		< 4 sec /página		Cero
Datos	Transacciones comerciales		< 4 sec		Cero
Datos	Acceso a servidores		< 4 sec		Cero

4.3.4 SERVICIOS *BACKGROUND*

Servicios *background* usualmente se refiere a servicios en donde el destino no está esperando los datos dentro de un cierto tiempo. Estos servicios son por tanto mas o menos insensibles al retardo. No obstante, un requerimiento clave es usualmente que la información debe ser entregada con un bajo BER. Ejemplos de servicios son: e-mail y SMS (*Short Message Service,* Servicio de Mensajes Cortos).

Servicios de baja prioridad de transferencia

Un ejemplo en esta categoría es el servicio de mensajes cortos (SMS). Un valor de retardo aceptable se ha propuesto en 30 segundos.

[1] Referencia [13]: 3 rd Generation Partnership Project 3GPP, TS 22.105, "Services & service capabilities", pág:16.

E-mail

E-mail puede tolerar retardos de varios minutos o incluso horas dependiendo de la expectativa del usuario. Pero es claro que la información tiene que ser entregada sin errores.

4.3.5 SERVICIOS BASADOS EN LA LOCALIZACIÓN

Estos servicios proporcionarán una adecuada información dependiendo de la ubicación del usuario, por lo que estos servicios entregarán un valor añadido al cliente. Entre los servicios que se encuentran en esta clasificación se encuentran:

Navegación, reservación dependiendo de la actual ubicación del usuario.
Traducción de servicios dependiendo de la información de roaming.
Servicios de asistencia de usuario final: asistencia de carretera y servicios de emergencia.
Monitoreo de la ubicación de personas: incluye datos para el cuidado de la salud, llamadas de emergencia.
Servicios de rastreo para encontrar personas extraviadas.
Activadores de servicio son automáticamente inicializados cuando el usuario final entra a una determinada área.
Modelos de facturas dependiendo de la localización de la fuente y el destino de la comunicación (familia y amigos, trabajadores móviles, usuarios de corporaciones móviles).

En la siguiente sección se mencionará el servicio de telemedicina como ejemplo de servicio de localización.

Telemedicina

Los sistemas de salud están descubriendo en las telecomunicaciones una forma de mejorar la comunicación de los doctores con sus pacientes. Las implementaciones en UMTS soportarán un mejoramiento en la relación entre doctores y pacientes. Los doctores en desplazamiento serán significativamente

más eficientes a través del acceso a la información de una base de datos y la habilidad de consultar a expertos o colegas vía videoconferencia.

Unos cuantos servicios de telemedicina pueden ser identificados:

- Monitoreo de pacientes en sus hogares o en su sitio actual
- Si los doctores se encuentran desplazándose pueden acceder a los records de sus pacientes, ordenar prescripciones y servicios médicos tales como test de laboratorio, consultando una base de datos.
- Servicios de consulta, permitiendo a los pacientes pagar y recibir prescripciones de sus doctores.
- Al desplazar a un accidentado a un hospital en una ambulancia, los paramédicos pueden recibir información concerniente al paciente para facilitar el pre-tratamiento y además puede haber una comunicación interactiva con un doctor en ese tiempo crítico.

La seguridad y la privacidad del intercambio de datos entre el doctor y el paciente estarán garantizados a través de la autenticación, encriptación e integridad de datos en UMTS.

A más del análisis realizado en las secciones anteriores, es importante mencionar el concepto de VHE (*Virtual Home Environment,* Entorno Local Virtual), ya que este aporta nuevas capacidades que van a poder ser aprovechadas por los servicios en UMTS y que no existían en los sistemas de segunda generación como GSM. En la siguiente sección se estudia tal concepto.

4.3.6 VHE (*Virtual Home Environment*)

Se define al concepto de VHE como la posibilidad de que el usuario móvil tenga en cualquier momento y en cualquier lugar la posibilidad de acceder a servicios con calidad similar a los establecidos en su red local[1]. Según este concepto, la red

[1]Refcrencia [12]: 3 rd Generation Partnership Project, 3GPP TR 23.927, "Virtual Home Environment; Open Service Architecture".

visitada emula para cada usuario particular las condiciones de su entorno de origen. De este concepto surgen dos componentes claves:

1.- La personalización. VHE permite un alto grado de personalización de servicios, lo cual quiere decir que los servicios se ejecutan a partir de perfiles personales. Estos perfiles personales determinan donde, cuando y como un usuario quiere recibir sus llamadas. Los perfiles deben ser modificables desde cualquier localidad, y los que se gestionan dentro del terminal (o USIM) deben ser recuperables ante pérdidas de conexión, batería o robo del terminal; es decir, deben tener respaldo (*back up*) en la red. Además se debe citar que un usuario puede tener más de un perfil, por ejemplo: en horas laborables un perfil de entorno de trabajo, en horas no laborables un perfil diferente, con otras opciones y servicios. El control del perfil se puede realizar de forma estática, la cual se haría en base en una petición expresa del usuario o en forma dinámica que se refiere a un cambio automático siguiendo ciertos criterios como la localización, la hora, el terminal en uso, etc.

2.- El acceso universal. VHE permite el acceso a todos los servicios de la red local desde cualquier red visitada, es decir que con este concepto se desea conseguir que el servicio mantenga las mismas características, ventajas, capacidades e interfaces de usuario, que en la plataforma local en la que fue definido por el proveedor del servicio. Esta condición es muy significativa ya que el usuario puede utilizar servicios locales en la red visitada, incluso si no tiene suscripción en esta última.

Para la implementación de VHE se deben tomar en cuenta las siguientes áreas:

- El acceso universal implica no solo cobertura, sino también que el operador de red tendrá que asegurar niveles de seguridad y QoS.
- La gestión de perfiles personales implica un control de servicios a través de operadores, por tanto el VHE requiere de acuerdos para dejar el control de servicios a la red local.
- El concepto de VHE implica una alta movilidad de usuarios y, por tanto, de servicios que tendrán que facturarse entre operadores, por ello se

requieren acuerdos entre estos y los proveedores para distribuir el valor del servicio entre todas las entidades involucradas.

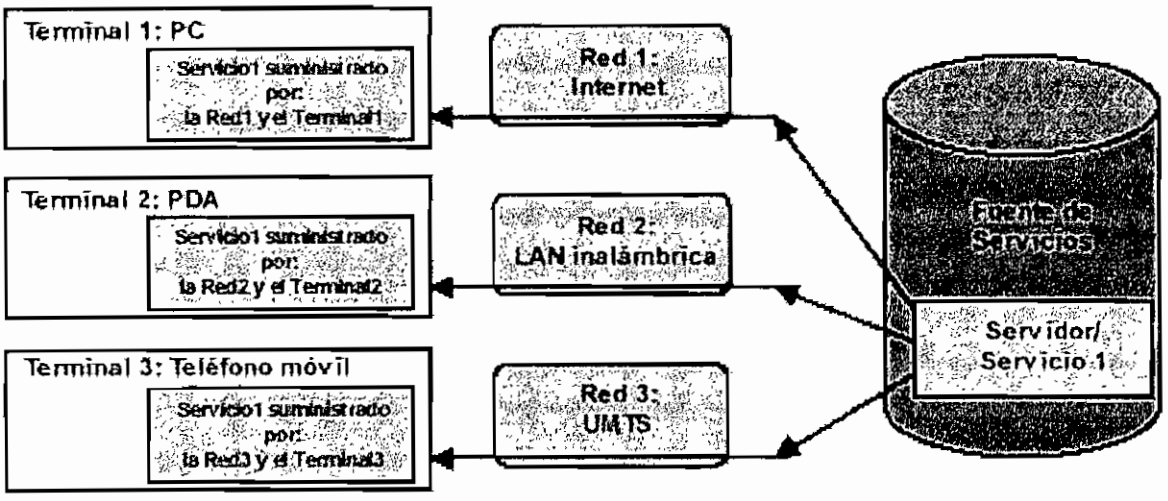


Figura 4.4 Concepto de VHE[1]

Como se observa en la Figura 4.4 el VHE es un concepto para suministrar la portabilidad del perfil de servicio de un usuario por los diferentes tipos de red y entre terminales.

Para ofrecer el VHE se diseña una arquitectura llamada OSA (*Open Service Access*) que proporciona la capacidad de independizar los elementos de la red de servicios de los propios servicios y aplicaciones desarrollados sobre ellos, de forma que cualquier empresa desarrolladora cumpliendo con las interfaces OSA puede desarrollar una aplicación sin tener un conocimiento expreso de la red; es decir, en UMTS las partes de la arquitectura que ofrecen y controlan los servicios se separan de los elementos de red encargados de aspectos propios de las comunicaciones. A continuación se efectuará una pequeña descripción de la arquitectura de OSA.

La arquitectura de OSA

Open Service Architecture (OSA) es un estándar del 3GPP (Figura 4.5), que define una arquitectura que permite al operador de red y a las aplicaciones de

[1]Referencia [45]: TW (Forschungszentrum Telekommunikation Wien), "UMTS Applications Development".

terceras partes utilizar la funcionalidad de la red móvil, a través de una interfaz abierta y estandarizada.

Con esta arquitectura se permite la aparición de proveedores de servicios independientes del operador de red. Los proveedores deben tener un acuerdo con el operador para ofrecer servicios a sus clientes utilizando las capacidades portadoras y recursos del operador. La característica anterior es un aspecto diferenciador con otras arquitecturas como por ejemplo CAMEL en la cual el operador proporciona el servicio completo.

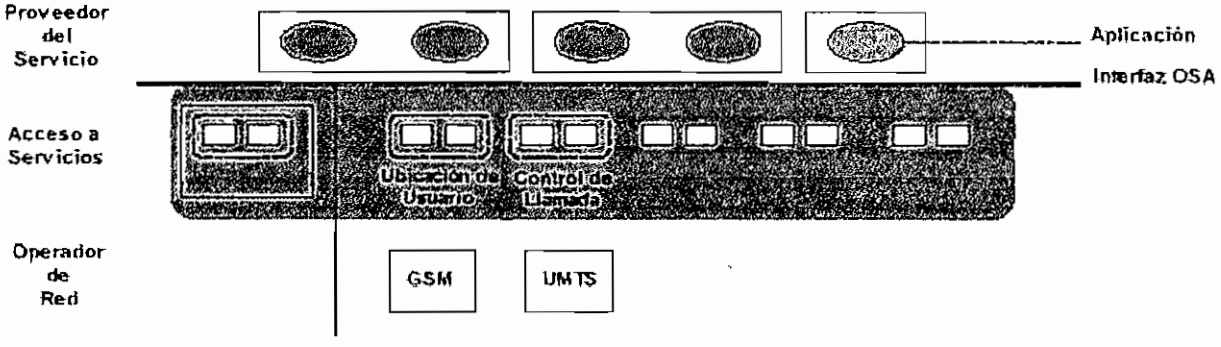


Figura 4.5 Arquitectura OSA

La arquitectura OSA permite a nivel de los proveedores de servicio la implementación de aplicaciones con valor añadido. Esas aplicaciones accederán a los recursos que suministra el operador de red a través de la interfaz abierta OSA. En el nivel de operador de red residen los operadores de GSM, UMTS, etc.

Después del análisis efectuado en los párrafos anteriores se procederá ha describir en este proyecto un marco para el desarrollo de servicios tomando las consideraciones tecnológicas existentes en UMTS y que además fueron estudiadas en los capítulos 2 y 3.

4.4 MARCO PARA EL DESARROLLO DE SERVICIOS

La descripción de un marco para el desarrollo de servicios se ha considerado importante en este proyecto debido a que los nuevos avances tecnológicos que poseerá UMTS y el crecimiento de servicios de Internet cambiarán las estrategias de desarrollo de servicios en los sistemas de comunicaciones móviles, debido a que los proveedores de servicios no necesariamente residirán en el dominio del operador. Además de ello, el marco que será descrito también puede involucrar a otros actores o entidades del mercado que aparecerán en la entrega de servicios.

A continuación se realiza tal descripción, la cual trata de involucrar todas las actividades que se deben ejecutar para un desarrollo satisfactorio de un servicio en un ambiente inalámbrico.

4.4.1 PASOS PARA EL DESARROLLO DE SERVICIOS

El criterio para la creación de los diferentes pasos se basa en tres aspectos importantes, los cuales son: aspectos tecnológicos, negocios y usuarios. Estas tres áreas que al parecer no tienen nada en común se relacionan de diferentes maneras, por ejemplo el precio de los servicios depende de múltiples factores. La tecnología influye en el precio del servicio debido a su costo y versatilidad. Los usuarios influyen debido a la cantidad de dinero que están dispuestos a pagar. Por su parte los negocios influyen en la manera que está dispuesto el mercado.

La Figura 4.6 presenta la relación de las tres áreas referidas.

Los aspectos tecnológicos en UMTS poseerán mayor influencia en las áreas de usuarios y negocios que otro tipo de redes, debido a que, por ejemplo, en GSM no existe una política de QoS (solo se basa en el concepto del mejor esfuerzo) y la seguridad es menor que en los sistemas de tercera generación, lo que sin duda afecta a la satisfacción de los usuarios con la consiguiente menor recaudación de dinero por un servicio ofrecido. Es por ello que UMTS se abre como un abanico

de nuevas oportunidades de desarrollo de nuevos servicios, lo que marcará la nueva tendencia del mercado mundial en el ámbito de las telecomunicaciones.

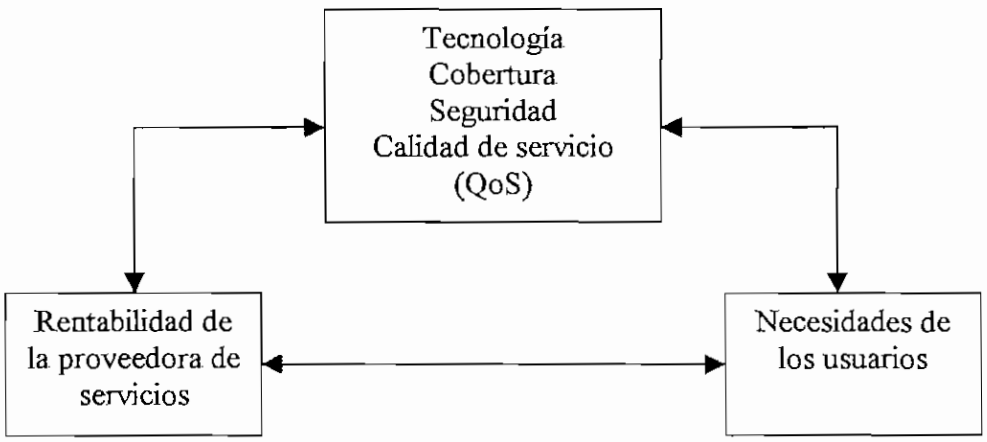


Figura 4.6 Relación de la tecnología, negocios y los usuarios[1]

Debido a lo anteriormente mencionado, en este proyecto se propone que los diferentes pasos para el desarrollo óptimo de servicios en UMTS deben ser los siguientes:

Estrategia de desarrollo de nuevos servicios

La estrategia de nuevos servicios dependerá de las metas de los proveedores de servicio y las capacidades de los operadores de telecomunicaciones móviles para soportar un nuevo servicio.

El desarrollo de nuevos servicios en los sistemas móviles UMTS requiere el entendimiento de: aspectos tecnológicos como la seguridad y la QoS, requerimientos de los clientes, y requerimientos del mercado. Una estrategia de servicio puede ser definida en términos del mercado, de las clases de servicio, criterios de beneficio, etc.

[1]Referencia [34]: Nortel Networks, "Benefits of Quality of Service (QoS) in 3G wireless Internet", pág:7.

Definida la estrategia, las operadoras estarán en una mejor posición para empezar a generar la idea del nuevo servicio.

Generación de ideas

Dentro de los proveedores de servicios debe haber un mecanismo para asegurar un continuo flujo de posibilidades de nuevos servicios que caben en las estrategias del proveedor. Muchos métodos están disponibles, tales como, entrevistas, puntos de referencia en términos de aprender de las ofertas del competidor, ideas colectivas de empleados y clientes con buzones de sugerencia, etc. El personal que interactúa con el cliente, puede ser una buena fuente de ideas para servicios complementarios y mejorar los servicios existentes.

Para encontrar que clases de características deberían y podrían ser añadidas al caso del concepto de servicio, se sugiere que una investigación del mercado debe hacerse por medio de una compañía consultora.

Desarrollo del servicio

El desarrollo empieza cuando buenas ideas caben en las estrategias del proveedor de servicios. Las mas atractivas ideas que tienen potencial para llegar a ser exitosas y factibles son desarrolladas y claramente definidas para que el proveedor de servicios introduzca específicas características, es decir los principios del servicio planteado.

El desarrollo del servicio incluye estimar los requerimientos del sistema. La descripción del servicio define el trabajo asociado con el enlace a la infraestructura de red UMTS y el proceso de negocios. El concepto de servicio debe validarse en términos de la viabilidad técnica; es decir, si la red UMTS puede ser capaz de entregar o no ese servicio. Es por ello que en esta sección se define la capacidad del sistema y el equipamiento técnico que existirá en UMTS.

Análisis del negocio

El análisis del negocio consiste en la proyección de los ingresos, y análisis de costos. Como resultado del análisis, el plan de negocios debe ser evaluado acorde a los objetivos del proveedor de servicios para determinar si la idea de un nuevo servicio posee los mínimos requerimientos.

Comercialización

El lanzamiento comercial es el punto en el proceso en donde el servicio se activa y es introducido al mercado. Monitorear todos los aspectos del servicio durante la introducción es necesario para refinarlo si es imprescindible. Los cambios necesarios podrían ser por ejemplo en el proceso de entrega, contenido, etc.

En la Figura 4.7 se puede apreciar los pasos para el desarrollo de servicios.

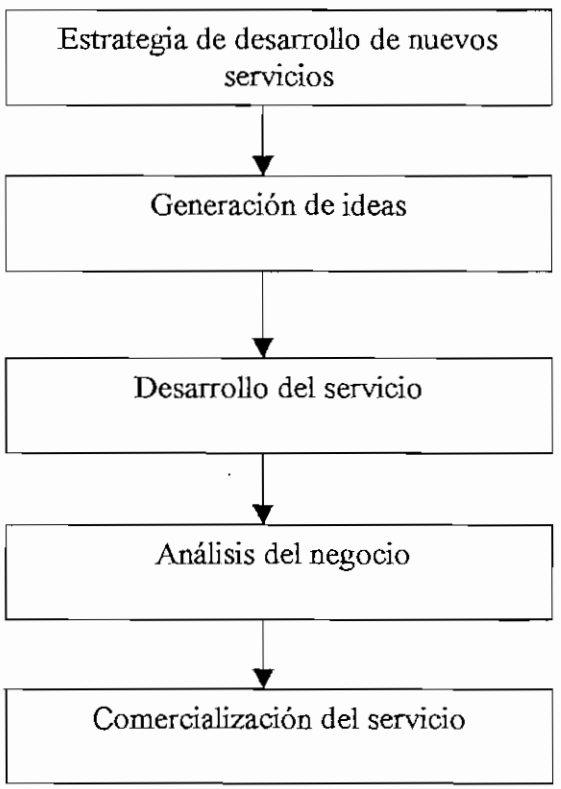


Figura 4.7 Pasos para el desarrollo de servicios[1]

[1]Referencia [46]:Katja Koivu, "Data service development in mobile networks", Helsinki University of Technology, pág:27.

4.4.2 REQUERIMIENTOS TÉCNICOS PARA EL DESARROLLO DE SERVICIOS

Los requerimientos tecnológicos tienen que ser tomados en cuenta durante el desarrollo del servicio. Los requerimientos tecnológicos determinan el criterio de factibilidad para la implementación de un servicio. Si el criterio no se cumple, el desarrollo del servicio tiene que detenerse ya que no tiene los fundamentos para que se realice. Es por ello que la descripción de los requerimientos técnicos constituyen la base para el desarrollo de servicios.

En esta parte del proyecto se introduce el análisis de los requerimientos tecnológicos que deben estar presentes para un desarrollo óptimo de servicios, teniendo en cuenta primeramente la generación del concepto del servicio (Figura 4.8).

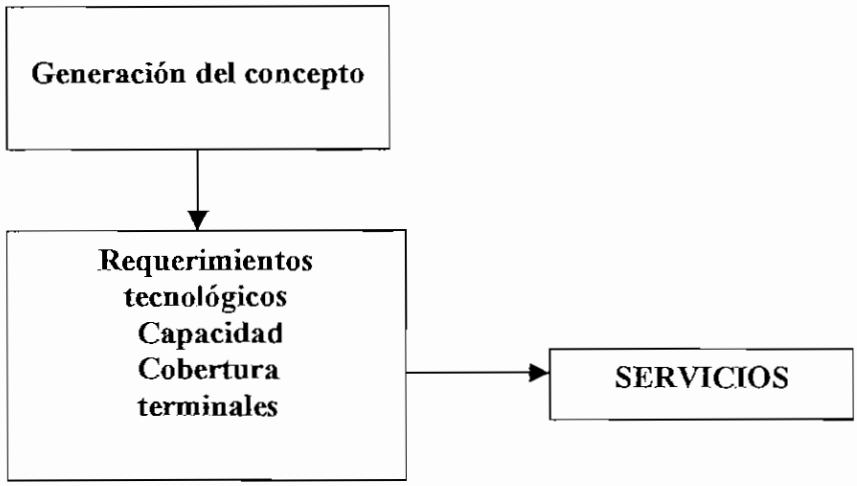


Figura 4.8 Requerimientos tecnológicos dentro del marco para el desarrollo de servicios

4.4.2.1 Generación del concepto

La generación del concepto consiste en convertir las ideas reunidas en detallados escenarios de servicio que incluyen toda la información necesaria para una apropiada implementación.

Un escenario de servicio es básicamente una pequeña descripción acerca de un usuario ficticio que necesita emplear algunos servicios en una determinada

situación. El escenario de servicio proporciona información básica del perfil del usuario, también define los principales requisitos de calidad del servicio y seguridad que deben estar presentes. Aunque el escenario de servicio es irreal es respaldado con datos reales de usuario recogidos durante la generación del concepto, los cuales son en otras palabras lo que espera un usuario del servicio.

Los escenarios deben incluir la siguiente información:

- Objetivo del servicio (qué usuario necesita llevar a cabo el servicio o a quién va dirigido).
- Nivel de QoS considerando sus diferentes clases.
- Análisis del entorno en donde se efectúa la movilidad.
- Nivel de seguridad.

Así por ejemplo para ofrecer un servicio de transmisión de datos que comprenda navegación por Internet se tendrá[1]:

Tipo de usuarios	Personas con un nivel adquisitivo medio
Clase de servicio	Interactivo
Nivel QoS	Tasa: 13 kbps BER: 10^{-6} Retardo: 1 segundo (aceptable) 100 ms (ideal)
Nivel de Seguridad	Baja (no se realiza encriptación a la información)
Cobertura	Funcionamiento en áreas abiertas y locales cerrados

[1]Referencia [47]: M.Lasanen, "Modem requirements for baseband, RF/IF subsystem and DLC/MAC layer", IST (information society technologies), pág:29.

Para ofrecer un servicio de transmisión de datos interactivo que involucra transacciones comerciales el escenario de servicio podría ser[1]:

Tipo de usuarios	Personas de negocios con un nivel adquisitivo medio y alto.
Clase	Interactivo
Nivel QoS	Tasa: 32 kbps BER: 10^{-8} –10^{-6} Retardo: 1 segundo 100 ms (preferible)
Nivel de Seguridad	Alta (algoritmos de encriptación y confidencialidad son aplicados)
Cobertura	Funcionamiento en áreas abiertas y locales cerrados

Una vez que el escenario del servicio ya ha sido definido, es posible realizar la estimación de los requerimientos tecnológicos que deben estar presentes (Figura 4.9).

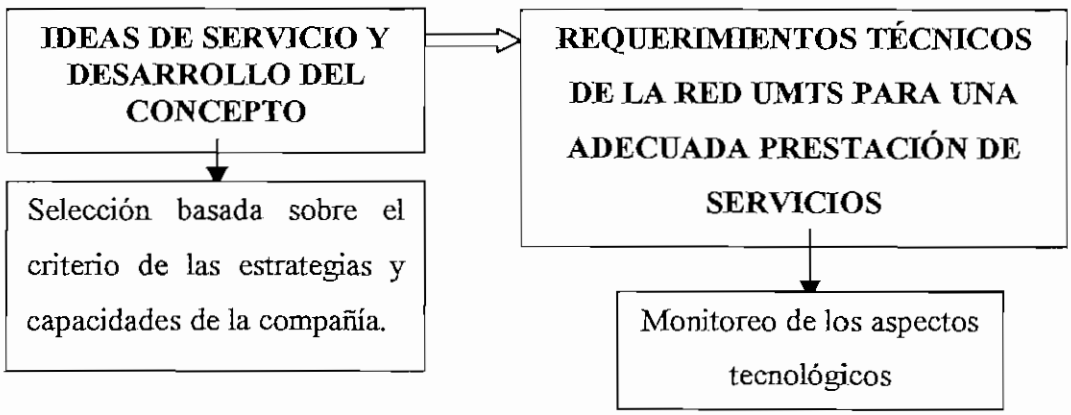


Figura 4.9 Marco para el concepto de desarrollo de servicios[2]

[1] Referencia [47]: M.Lasanen, "Modem requirements for baseband, RF/IF subsystem and DLC/MAC layer", IST (information society technologies), pág:27.
[2] Referencia [48]: Nokia Networks, "Radio Network Planning Process and Methods for WCDMA", pág:2.

4.4.2.2 Estimación de los requerimientos técnicos en la red UMTS para una adecuada prestación de servicios

Una vez planteado el escenario del servicio se realizará por parte del operador las estimaciones de los requerimientos de cobertura, capacidad, terminales para que la red UMTS pueda soportar el servicio deseado. Por tanto, esto conllevará a un despliegue óptimo de las estaciones base y al cumplimiento de los objetivos de QoS establecidos para la prestación de servicios.

En el sistema UMTS es conveniente advertir que en muchos casos la complejidad del análisis teórico de los modelos del sistema de radio es tal, que no existen soluciones en forma de funciones matemáticas, por lo que debe recurrirse a la realización de simulaciones por computador o efectuar simplificaciones para obtener las estimaciones. Por tanto, a continuación se presenta un ejemplo de cálculo para obtener la estimación aproximada de la capacidad teórica de una celda WCDMA y del área máxima de ésta para conseguir una adecuada prestación de servicios.

Estimación de la capacidad

La estimación de la capacidad consiste en determinar el número de canales (códigos) necesarios para dirigir el tráfico de las diferentes clases de QoS. Para obtener la capacidad teórica primeramente se parte de la ecuación de carga (3.2), considerando N usuarios se obtiene:

$$\eta = (1+i).\sum_{j=1}^{N} \frac{1}{\frac{W}{v_j.\left(\frac{E_b}{N_o}\right)_j.R_j}+1} \quad \text{(Ec 4.1)}$$

La ecuación de carga anterior puede ser simplificada a:

$$\eta = \frac{(E_b/N_o)_j}{W/R_j} \cdot N \cdot v_j \cdot (1+i) \quad \text{(Ec 4.2)}$$

en donde:

η = Factor de carga.

W = Tasa de codificación o chip (3.84 Mcps en sistemas WCDMA).

ν_j = Factor de actividad de la fuente de tráfico, el cual es obtenido en términos estadísticos.

E_b/N_o = Proporción de energía de la señal por bit con respecto a la densidad de potencia del ruido para el usuario j-ésimo.

R_j = Tasa de bit del usuario j-ésimo.

i = Factor de interferencia entre celdas (interferencia entre la celda adyacente y la celda actual).

Tomando en cuenta las tablas 4.1, 4.2 y 4.3 de este capítulo se tiene que las tasas de bit del portador aceptables para diferentes servicios están entre: 4-25 kbps para servicios de voz en tiempo real, de 32-384 kbps para video y de 16-128 kbps para datos. Por tanto para el dimensionamiento de una celda suponiendo diferentes escenarios de servicio se tomará en cuenta las siguientes tasas de bit de usuario:

Tabla 4.4 Tasas de bit usadas en el cálculo[1]

Servicio	Clase de QoS	Aplicación	Tasas de bit de usuario (kbps)
Audio	Conversacional	Telefonía	12
Datos	Flujo continuo	Telemetría	16
Datos	Interactivo	Transacciones comerciales	32
Audio	Flujo continuo	Transmisión de música	64
Video	Flujo continuo	Transmisión de imágenes	128
Video	Conversacional	Videotelefonía	384

[1] Referencia [49]: Takis Mathiopoulos, "UMTS: the evolution of GSM toward IMT-2000", University of British Columbia, pág:16.

Para hacer el dimensionamiento de una celda con las velocidades de usuario o de portador indicadas anteriormente se debe estimar un margen de interferencia o aumento de ruido ya que este valor afecta la capacidad y cobertura de una celda. Un valor estimado para este caso puede ser 3 dB (ver Anexo 5).

Con un aumento de ruido máximo igual a 3 dB y la ecuación 4.3, se puede calcular el factor de carga.

$$noise\_rise = 10 \cdot \log_{10}\left(\frac{1}{1-\eta_{UL}}\right) \ [dB] \text{ (Ec 4.3)}$$

$$2 = \frac{1}{1-\eta_{UL}}$$

$$\eta_{UL} = 0.5$$

A más del parámetro indicado se debe considerar otros como:
La razón E_b/N_0, la cual se relaciona a la QoS en la interfaz de radio; es decir, se relaciona a la tasa de bit del portador, el BER, la movilidad, etc.
El factor de actividad de usuario (vj) que determina la actividad del canal.
La proporción de interferencia (i), que toma en cuenta la interferencia de celdas adyacentes con la interferencia de la celda actual con el propósito de garantizar una adecuada QoS.

Es por ello que a continuación se indican los diferentes valores de los parámetros antes mencionados, los cuales han sido recomendados por la 3GPP.

Tabla 4.5 Valores de los parámetros W, i, v_j [1]

Parámetro	Valor
W (Tasa de chip)	3.84 Mcps (fijo)
i	0.65 (valor típico)
v_j	Audio en tiempo real 67% Datos 100% Video 100%

[1]Referencia [50]: Zhi-Chun Honkasalo, "Radio Network Planning", WCDMA for UMTS, edited by Harri Holma, págs: 10-11.

Tabla 4.6 Valores de la relación E_b/N_o[1]

Servicio	Clase de QoS	Aplicación	E_b/N_o (dB)
Audio	Conversacional	Telefonía	4.0
Datos	Flujo continuo	Telemetría	3.0
Datos	Interactivo	Transacciones comerciales	3.0
Audio	Flujo continuo	Transmisión de música	2.0
Video	Flujo continuo	Transmisión de imágenes	1.5
Video	Conversacional	Videotelefonía	1.5

Despejando la ecuación 4.2 y usando los datos anteriores se obtiene el número de canales, así por ejemplo para un servicio de voz:

$$N = \frac{\eta_{UL} \cdot W / R}{E_b / N_o \cdot \nu \cdot (1+i)}$$

$$N = \frac{0.5 \times (3840000/12000)}{2.512 \times 0.67 \times (1+0.65)}$$

$$N = 57.62 \rightarrow 58$$

Realizando el mismo cálculo para las demás tasas de usuario se logra conseguir el número de canales por sector, y además, con una probabilidad de pérdida del 2%[2] se puede estimar la intensidad de tráfico. Los resultados se muestran en la Tabla 4.7.

[1]Referencia [50]: Zhi-Chun Honkasalo, "Radio Network Planning", WCDMA for UMTS, edited by Harri Holma, pág: 18.

[2] Dentro del reglamento para el Servicio Móvil Celular (Resolución N° 421-27-CONATEL) se indica que el valor máximo permitido para evitar que exista bloqueo de llamadas es del 2%.

Tabla 4.7 Estimación de la capacidad por sector

Aplicación	Tasa de bit (kbps)	Número de canales por sector	Intensidad de tráfico (Erl/sector)
Telefonía	12	58	47.76
Telemetría	16	36	27.343
Transacciones comerciales	32	18	11.491
Transmisión de música	64	11	5.842
Transmisión de imágenes	128	6	2.276
Videotelefonía	384	4	1.092

Además de ello, la capacidad de la celda puede ser incrementada utilizando el método de sectorización. La sectorización es una técnica común usada en sistemas móviles celulares cuya característica es usar antenas direccionales en un sitio de la celda para recibir y transmitir. Típicamente una celda es dividida en tres sectores como se muestra en la Figura 4.10.

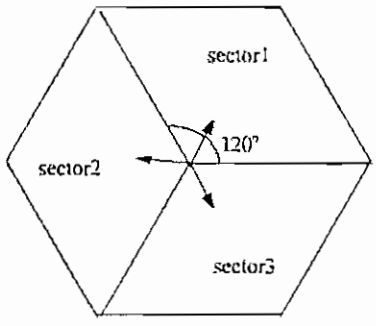


Figura 4.10 Sectorización de una celda

Teóricamente la sectorización incrementa la capacidad de la celda por un factor de 3, debido a que solamente una tercera parte del total de las transmisiones móviles es recibida en un sector dado, por lo que el número de canales será:

Tabla 4.8 Estimación de la capacidad por celda

Aplicación	Tasa de bit (kbps)	Número de canales por celda	Intensidad de tráfico (Erl/celda)
Telefonía	12	174	143.28
Telemetría	16	108	82.029
Transacciones comerciales	32	54	34.473
Transmisión de música	64	33	17.526
Transmisión de imágenes	128	18	6.828
Videotelefonía	384	12	3.276

Si para una operadora celular existe una disponibilidad de espectro de 3*15 MHz, y sabiendo que el espaciado entre portadoras en WCDMA es 5 MHz, entonces el número de canales físicos (canales de radio frecuencia) será:

$$número\_canales\_fisi\cos = \frac{45MHz}{5MHz/canal} = 9 \ \ canales$$

En WCDMA, en teoría, el factor de reuso de frecuencias es 1, pero en la práctica se ha llegado a establecer que un factor de reuso de frecuencias óptimo es 2/3, con lo que los 9 canales de RF deben ser asignados de acuerdo al último factor.

Estimación de la cobertura

La estimación de los requerimientos de cobertura se refiere a determinar el alcance de la emisión radioeléctrica producida por la estación base. Es decir, a través de las características de las condiciones de propagación de radio en una determinada zona, se procede a calcular las pérdidas básicas por propagación

para de esta manera obtener el radio de la celda. En este punto se debe tener en cuenta las restricciones que impone el entorno: edificios, calles, carreteras, etc.

Considerando lo anteriormente mencionado, para determinar la cobertura de la celda primeramente se procede a obtener las pérdidas por propagación máxima (Lp).

$$L_p = P_{móvil} + G_{móvil} + G_{base} - S_{base} - L_M - L_C \quad \text{(Ec 4.4)}$$

en donde:

L_p = Pérdidas por propagación máxima

$P_{móvil}$ = Potencia de salida del móvil [dBm]

G_{base} = Ganancia de la antena del tranceiver [dBi]

$G_{móvil}$ = Ganancia de la antena del móvil [dBi]

S_{base} = Sensibilidad del tranceiver [dBm]

L_M = Margen de desvanesimiento [dB]

L_C = Pérdidas del cable [dB]

De la información del Anexo 6 y teniendo en cuenta un margen de interferencia de 3dB se tiene que: $P_{móvil}$ = 24 dBm, G_{base} = 18 dBi, $G_{móvil}$ = 2 dBi, S_{base} = -109.2 dBm, L_M = 4 dB, L_C = 2dB. Reemplazando en la ecuación 4.4 resulta:

$$L_p = 24 + 2 + 18 - (-109.2) - 4 - 2$$
$$L_p = 147.2dB$$

Para calcular el radio de la celda máxima se usa el modelo de propagación de Okumura-Hata, debido a que constituye un modelo punto multipunto idóneo para los sistemas móviles celulares. Teniendo además en cuenta una torre de 30 m de altura y una frecuencia f igual a 1970 MHz, se tiene:

$$L_p = 69.55 + 26.16 \times \log f - 13.82 \times \log h_1 + (44.9 - 6.55 \times \log h_1) \times \log d \quad \text{(Ec 4.5)}$$
$$\log d = 0.337$$
$$d = 2.17km$$

Por tanto el área de la celda será:

$$A = \frac{3}{2}\sqrt{3} \cdot d^2 \quad \text{(Ec 4.6)}$$

$$A = 12km^2$$

Si la planeación de la red UMTS es realizada en un área aproximada de 6x25 km^2, entonces el número de radiobases será igual a 13.

Estimación de los requerimientos de retardo

La estimación de los requerimientos de retardo dentro del desarrollo de servicios es de vital importancia, debido a que representa el principal factor para distinguir la QoS ofrecida a los diferentes usuarios.

Por tanto, cada servicio dado no debe sobrepasar un cierto retardo, por lo que debe ser ajustado a un presupuesto de retardo. Este presupuesto es el tiempo en que los datos deben llegar a su destino, el mismo que restringe a las herramientas de control de errores a que la operación de éstas no retarden demasiado la información. Concedido el uso de esas herramientas, un cierto número de errores en la transmisión de radio pueden ser corregidos dentro del específico marco de tiempo. Es decir, si se tiene estrictas demandas sobre el retardo, simplemente no se tiene el tiempo para complejos códigos de control de error, y por tanto se debe tener un buen canal con un bajo BER para satisfacer los varios requerimientos de retardo.

Es así que, por ejemplo, para determinar el retardo para una transmisión de imágenes a una tasa de 128 kbps se efectúa el siguiente cálculo aproximado:

$$t_{retardo} = t_{paquete} + t_{Checksum} + 2.t_{propagación}$$

$$t_{retardo} \approx \frac{1000 \times 8}{128000} + \frac{40 \times 8}{128000} + 2.\frac{2170}{3 \times 10^8}$$

$$t_{retardo} \doteq 65.014ms$$

Al anterior valor se debe añadir el retardo del SGSN al RNC (20 ms en promedio)[1] y del SGSN al servidor (80 ms en promedio)[1], lo que da como resultado un retardo extremo a extremo de 165.014 ms, el cual debe ser cumplido para ese servicio. A continuación se presenta una tabla donde se indica los valores de retardo para diferentes servicios.

Tabla 4.9 Valores de retardo permitidos[2]

Servicio	Clase de QoS	Aplicación	Retardo (ms)
Audio	Conversacional	Telefonía	40
Datos	Flujo continuo	Telemetría	100
Datos	Interactivo	Transacciones comerciales	100
Audio	Flujo continuo	Transmisión de música	200
Video	Flujo continuo	Transmisión de imágenes	165
Video	Conversacional	Videotelefonía	90

Requerimientos de seguridad

Para que se cumplan los objetivos de seguridad planteados para cada servicio el operador de la red, a más de tener presente los mecanismos de seguridad estudiados en el capítulo 2, debe escoger los algoritmos adecuados para que la red y/o la estación móvil no sufran ataques de personas desautorizadas.

Es por ello que, por ejemplo el operador puede hacer uso, para el servicio de autenticación, del algoritmo MILENAGE, el cual se basa del algoritmo RIJNDAEL. En cambio para la parte de confidencialidad e integridad en el intervalo aéreo (entre el móvil y la estación base) se puede utilizar el algoritmo denominado KASUMI.

[1]Referencia [42]: Smaragdakis Georgios, "TCP Performance over UMTS Network", Technical University of Crete, pág: 73-74.
[2]Referencia [49]: Takis Mathiopoulos, "UMTS: the evolution of GSM toward IMT-2000", University of British Columbia, pág:16.

Se debe considerar que para todos los servicios se usará el algoritmo MILENAGE, mientras que el algoritmo KASUMI será utilizado dependiendo del tipo de servicio. Es decir que de acuerdo a la importancia de la información un servicio tendrá un nivel más alto que otro. Así, por ejemplo, para una aplicación de comercio móvil se usarán los algoritmos MILENAGE y KASUMI, mientras para una aplicación de charla móvil se usará solamente MILENAGE.

Requerimientos de terminal

Los equipos terminales constituyen un elemento importante para el despliegue de servicios en una red UMTS, debido a que a través de ellos el usuario obtiene la percepción final de la calidad de servicio. Por tal motivo, los terminales deben tener ciertos requerimientos que permitan el funcionamiento óptimo de los diferentes servicios, es por ello que:

Los terminales UMTS deben ser compatibles con las redes actuales 2G, de modo que se puedan aprovechar los recursos de las distintas redes con el objetivo de dar un servicio de cobertura global a través de un único terminal.

Los equipos terminales deben soportar altas tasa de transmisión como por ejemplo de 384 Mbps para servicios multimedia.

Los dispositivos móviles deben ser dotados de un sistema operativo abierto, es decir que permita ejecutar aplicaciones procedentes de diferentes orígenes. En la actualidad se puede encontrar los siguientes sistemas operativos[1]:

Palm OS. Sistema operativo del fabricante de PDAs Palm, que ha encontrado gran aceptación y cuenta con multitud de aplicaciones desarrolladas por terceras personas.

Windows CE 3.0. Sistema operativo de Microsoft, que incorpora el navegador Internet Explorer y las herramientas de Office.

[1]Referencia [19]: UMTS FORUM, "Support of Third Generation Services using UMTS in a Converging Network Environment", Report N°14, pág:41.

Es importante indicar que el terminal móvil debe poseer una capacidad suficiente de memoria para que permita el almacenamiento de los diferentes programas de aplicación. Por tal razón, el UMTS Forum especifica un valor 64 Mbytes en RAM[1] y 48 Mbytes en ROM. Además de ello para el funcionamiento de las nuevas aplicaciones multimedia como por ejemplo audio de alta calidad, se necesitará un procesador que realice 100 millones de instrucciones por segundo[1].

Los dispositivos móviles deben obedecer a las exigencias de funcionalidad de los usuarios, por lo que su peso estará por debajo de los 150 gramos y preferentemente poseerán pantallas de color, de tal manera que permitan el desligue presentaciones gráficas de alta calidad (Figura 4.11).

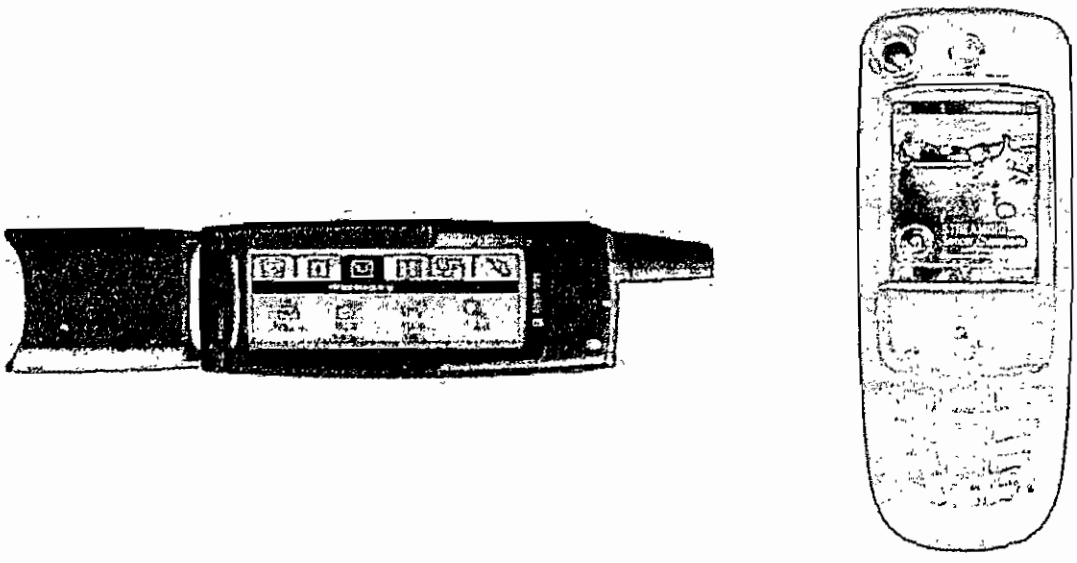


Figura 4.11 Terminales móviles en UMTS[2]

Los requerimientos de terminal anteriormente mencionados deben ser tomados muy en cuenta por el operador, debido a que el dispositivo de usuario determinará si un servicio puede ser desplegado.

Es importante indicar que una vez que la estimación técnica ha sido realizada el operador estará en la capacidad de decidir la puesta en funcionamiento de un servicio.

[1]Referencia [20]: UMTS FORUM, "Key Components for 3G Devices", Report N°15, pág:21-22, 54.
[2]Referencia [51]: 3G Phone, www.cellular.co.za.

4.4.2.3 Monitoreo de los aspectos tecnológicos

El monitoreo de los aspectos tecnológicos dentro de UMTS constituye una parte importante dentro del desarrollo de servicios ya que el resultado de este dará las pautas para la optimización de los elementos de red considerando los diferentes escenarios de servicio.

Por tanto, el objetivo del monitoreo es refinar la prestación de un servicio a través de los datos obtenidos de ella. Las pautas con respecto a la forma de monitoreo darán la base para una exitosa estimación de servicios.

Las pautas del monitoreo en la Tabla 4.8 muestran algunas consideraciones de los diferentes aspectos tecnológicos para lograr ese fin.

Tabla 4.8 Pautas de monitoreo

Aspectos tecnológicos	Instrucciones	Información necesaria del servicio
QoS	Monitoreo del nivel de calidad. Es el nivel alto, moderado, o bajo?	Estimación y demandas para la calidad de contenido y tolerancia a: -bloqueo -BER -interferencia -retardo, etc.
Seguridad	Los requerimientos de seguridad dependen de los datos que serán transmitidos	Información de los niveles de seguridad, transacciones de dinero, etc.

Para el monitoreo de QoS en UMTS, se debe tener presente la estimación de: niveles de cobertura, mecanismos de gestión de recursos, algoritmos de control de admisión, algoritmos de control de potencia, etc, los cuales determinarán los valores de diversos parámetros como, por ejemplo: la relación Eb/No, nivel de pérdidas, nivel de interferencia, retardo, etc.

Se debe indicar que en el monitoreo de la QoS de un servicio dado, los parámetros de este son considerados de acuerdo a su importancia o nivel crítico;

es decir, que parámetros pueden llegar a ser cuellos de botella en el funcionamiento del servicio.

Mientras tanto, para el monitoreo de la seguridad la información necesaria del servicio será obtenida del tiempo de uso y el nivel de seguridad que el operador haya dado a un determinado servicio.

Monitoreo de la QoS

Una vez que se tiene definida la información más importante de un servicio, se procede a su recopilación, por medio de dispositivos especiales, como los denominados analizadores de red.

Analizadores de la red UMTS

Por medio de analizadores de red[1] aplicados a diferentes nodos de la red se puede obtener datos precisos de diferentes parámetros que especifican el funcionamiento de un servicio como el aumento de interferencia, retardo, tasa de bit de usuario efectiva, etc.

En la Figura 4.12 se muestra una manera de cómo se puede conseguir información de la red a través del mencionado analizador.

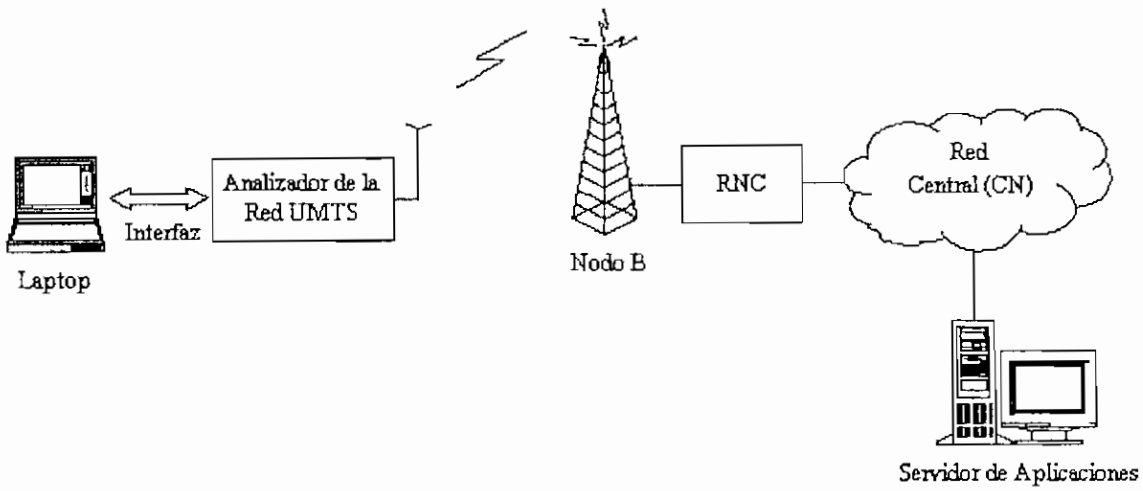


Figura 4.12 Evaluación de la red UMTS a través del uso de un Analizador

[1] En el Anexo 7 se muestra un analizador que puede ser utilizado para el monitoreo de la QoS.

En el gráfico anterior el analizador es ubicado en el lado del usuario con el objetivo de obtener los parámetros que el usuario percibiría. Es por ello que el analizador debe ser capaz de: establecer un canal de comunicación, hacer una petición o recibir información de un servidor remoto, almacenar la información requerida y finalizar la sesión como si se tratará de un equipo terminal normal.

Los parámetros obtenidos por medio del mencionado analizador serán ingresados a un software especializado el cual mediante una técnica adecuada verificará si aquellos valores son los óptimos para un determinado servicio. Este monitoreo o evaluación determinará si un servicio satisface con las especificaciones planteadas para un determinado escenario de servicio, el cual debe cumplir con los requisitos exigidos por los organismos de estandarización como la 3GPP y que además fueron estudiados en los capítulos anteriores.

Se debe tener en cuenta que al monitorear de la manera indicada anteriormente se obtienen parámetros finales del servicio, pero si se desea recopilar los valores de los parámetros dentro de la red, se debe examinar lo que ocurre en los diferentes nodos. Es por ello que a más del monitoreo de extremo a extremo realizado por el analizador, el cual emula a un terminal móvil (Figura 4.12), se efectúa un análisis en los diferentes nodos de la red UMTS, como por ejemplo en el nodo RNC (Figura 4.13).

Así en el nodo RNC se monitoreará:

- El valor del aumento del ruido, el cual está relacionado directamente con el funcionamiento del algoritmo de control de admisión, cuya misión es determinar si la inclusión del nuevo usuario degrada o no al sistema.
- La cantidad de pérdidas de paquetes, la magnitud del retardo en este nodo, a través de la evaluación del algoritmo de gestión de recursos como por ejemplo WFQ.
- El valor de la relación Eb/No, el valor de la proporción de interferencia de otras celdas con la celda en uso, los cuales serán determinados por los mecanismos de control de potencia.

Es decir, en este nodo se ejecutará un monitoreo de los parámetros que están relacionados a los mecanismos de control de recursos de radio.

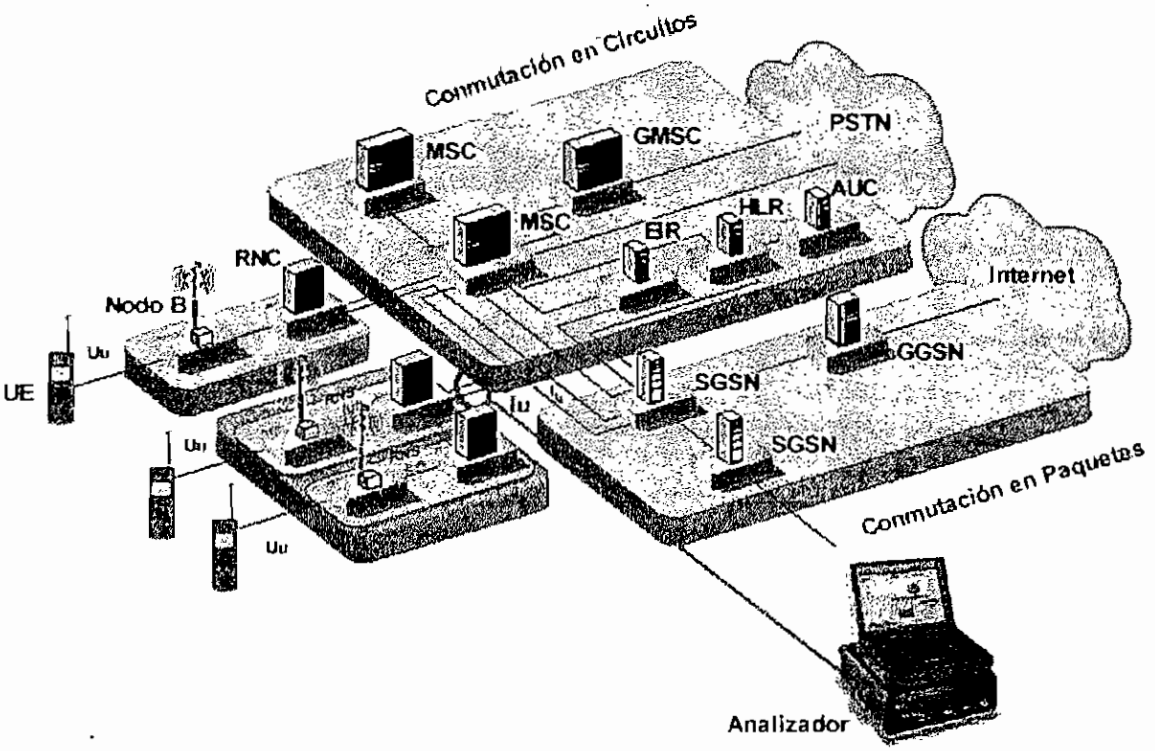


Figura 4.13 Monitoreo en el nodo RNC

Es importante indicar que para efectuar el monitoreo del retardo en los diferentes nodos de la red como SGSN se debe tener en cuenta un presupuesto de retardo para cada servicio. Este presupuesto debe ser repartido entre todos los nodos y mecanismos que intervienen para el establecimiento del servicio portador, por lo que cada nodo debe cumplir con una cierta fracción del retardo extremo a extremo. Otros parámetros como FER, prioridad del manejo del tráfico también son monitoreados.

Monitoreo de la seguridad

En este proceso de monitoreo también es posible examinar las características de seguridad en los diferentes dominios de la red UMTS. Las diferentes características de seguridad que podrían ser evaluadas serían: la encriptación de la interfaz de radio, la autenticación, la protección a la integridad, etc. Es

importante también indicar que una posible forma de monitoreo de la seguridad sería mediante el desarrollo de perfiles de la conducta de usuario. El perfil representaría un método de legitimar a los usuarios mediante la comparación del tiempo de consumo de un servicio con los demás tiempos de uso de sesiones pasadas almacenados en el HLR. Si existe un excesivo uso del servicio habrá la posibilidad de que la seguridad esta siendo violada por personas desautorizadas. Otra forma de monitorear la seguridad es probar la robustez de los algoritmos de autenticación, integridad a través de simulaciones de ataques realizadas por software con el fin de encontrar los puntos débiles de tales algoritmos y con ello tener la posibilidad de decidir si son mantenidos, mejorados o rechazados, considerando las exigencias del servicio.

Una vez que el monitoreo ha sido realizado se puede efectuar un refinamiento ya sea del servicio o de la red. Un refinamiento del servicio involucra a la revisión del escenario del servicio, esto quiere decir que se deben revisar los parámetros planteados. Por otro lado, un refinamiento de la red puede ser el aumento del número de nodos B, la revisión de la probabilidad de cobertura, revisión de los mecanismos de gestión de recursos, etc.

Se debe considerar que el monitoreo debe ser efectuado por parte del operador de la red UMTS y no por el proveedor de servicios, ya que el proveedor puede estar fuera del dominio de la red UMTS, por lo que no puede tener acceso a los equipos e información que estos producen. Por tal motivo, entre el operador y el proveedor debe haber algún convenio cuando este último quiere desarrollar un servicio.

4.4.3 IMPORTANCIA DE UMTS CON RESPECTO A GSM EN EL MARCO DEL DESARROLLO DE SERVICIOS

Es meritorio indicar que a través del marco descrito se puede palpar la importancia de la red UMTS y sus aspectos tecnológicos en el desarrollo de nuevos servicios con respecto a otro tipo de redes. Es así como en el análisis efectuado anteriormente se indicó que, para desarrollar nuevos servicios con valor agregado, se necesitan cumplir ciertos requisitos tecnológicos (QoS,

seguridad, etc) que solo son posibles gracias al uso de la tecnología UMTS y por tanto no pueden ser desarrollados en los sistemas de segunda generación como GSM debido a un conjunto de limitaciones como por ejemplo:

- Capacidad gráfica de los teléfonos, muy limitada para la aplicación de servicios como navegación web, videoconferencia, etc.
- Velocidad de GSM muy por debajo de la que se ofrece para tecnologías de tercera generación, ya que originalmente GSM fue diseñado para transmisiones de voz y no para servicios multimedia o transmisión de datos en tiempo real, mientras que UMTS esta diseñado para soportar transmisiones multimedia.
- La interface de radio de GSM no puede dar ninguna garantía sobre la capacidad disponible para las transmisiones de los usuarios dada sus limitaciones.
- No existe diferenciación de servicios en GSM, solo se basa en el método del "mejor esfuerzo" (best effort), por consiguiente puede provocar una pérdida de paquetes, lo que difiere en UMTS que realiza una clasificación de los diferentes servicios de acuerdo a los parámetros de QoS.
- Características de seguridad débiles en GSM, lo que puede dar lugar al fraude y no posibilita el despliegue de nuevos servicios debido al temor de los suscriptores a ser estafados.

Por tanto, el uso de la red UMTS considerando criterios de QoS y seguridad traerá nuevas oportunidades de servicios con el consiguiente incremento de las ganancias para el proveedor de servicios y el operador comparado con las redes de segunda generación como GSM.

4.5 DESCRIPCIÓN DE LA SEGURIDAD Y CALIDAD DE SERVICIO (QoS) EN EL ECUADOR

4.5.1 SITUACIÓN ACTUAL

La telefonía celular actualmente en el Ecuador ha sido una de las mayores áreas de crecimiento en los últimos años, así por ejemplo en el 2001 el servicio de telefonía celular se incrementó en un 78%[1]. Sin embargo, a pesar del gran éxito

[1]Referencia [52]: Artículo de la revista Conectados, "Celulares: en busca del servicio perdido", www.conectados.com.ec.

que ha tenido la telefonía celular en el país las empresas operadoras tanto Otecel (BellSouth) como Conecell (PortaCelular) no brindan una adecuada calidad de servicio a sus usuarios. Esto se debe en parte a que la tecnología utilizada por las actuales operadoras (basada en la técnica de acceso TDMA) brinda una menor capacidad de usuarios por celda y también a la poca inversión que éstas realizan para la ampliación de la infraestructura para soportar el tráfico del sistema.

El servicio prestado por las operadoras desde mediados del 2002 ha desmejorado notablemente registrando altos valores de congestión, así por ejemplo según la Superintendencia de Telecomunicaciones el promedio de no acceso a la red durante el mes de diciembre del 2002 en todo el país fue del 15%, lo que contrasta con el valor permitido en el reglamento que es del 2%, por lo cual se evidencia varios problemas como:

- El usuario debe realizar varios intentos de llamada para lograr una comunicación exitosa con el número de destino.
- El usuario registra un alto porcentaje de cortes de llamada.
- El usuario escucha otras conversaciones en la comunicación que se está cursando.

En cuanto a la seguridad las operadoras no ofrecen una adecuada protección a sus usuarios contra el fraude. Esto se puede apreciar debido que con la tecnología usada actualmente en el Ecuador es posible el "escaneado" de códigos de celulares encendidos en un radio de 200 metros, los que más tarde los falsificadores convierten y adaptan a teléfonos robados, mediante un software que operan desde una computadora portátil. Después los teléfonos alterados se arriendan a terceros para efectuar llamadas internacionales; comunicaciones de larga distancia que en definitiva se cargan en la cuenta del titular del número. Esto ocurre porque al cursar una llamada con la tecnología actual en el país el celular transmite dos tipos de datos: un MIN (*Mobile Identication Number*, Número de Identificación Móvil) o número de identificación móvil de 10 dígitos que se deriva del número del teléfono; un ESN (*Electronic Serial Number*, Número Serial Electrónico) o número de serie electrónico de 32 bits programado por el fabricante. El par MIN/ESN es una marca única del celular, que permite a la

compañía saber a quién cobrar la cuenta. Cuando el teléfono transmite su par MIN/ESN es posible escucharlo con un escáner especializado y capturar el par. A través de un software, otro teléfono es modificado para que contenga el par MIN/ESN y se cometa el fraude.

4.5.2 MIGRACIÓN DE LAS REDES ACTUALES DE SEGUNDA GENERACIÓN HACIA LA TERCERA GENERACIÓN

Dada la situación actual que atraviesa la telefonía móvil en el Ecuador y al vertiginoso avance tecnológico, las operadoras han considerado la migración de sus redes actuales para poder mejorar sus servicios y brindar otros nuevos.

Desde esta perspectiva la empresa Conecell (PortaCelular) ha considerado que la mejor vía de migración hacia la tercera generación será la implementación de GSM para enseguida evolucionar a GSM-GPRS y después implementar el GSM-GPRS-EDGE para finalmente adoptar UMTS. Se debe considerar además que tal migración requerirá aparatos telefónicos multimodo para GSM-GPRS-EDGE-UMTS. Tales aparatos multimodo permitirán el traspaso de una red a otra, lo que hará viable una prestación perfectamente consistente de servicios GSM básicos (voz y mensajes) a lo largo de toda la red, además del ofrecimiento de UMTS en las partes de tráfico más intenso. Esto también posibilitará que las operadoras implementen la infraestructura 3G solamente de acuerdo con la demanda, minimizando así el monto de sus inversiones.

En cambio la empresa Otecel (BellSouth) ha estimado que la mejor vía de migración será la utilización de CDMA2000, cuyas ventajas en comparación a GSM son:

- Es un sistema certificado de tercera generación, mientras GSM se considera de segunda generación.
- Permite mayor número de usuarios por portadora, ya que utiliza la técnica de acceso CDMA.
- Los teléfonos trasmiten con baterías más pequeñas y de mayor duración.

Entre algunas desventajas se puede citar que:

- Existe 56 proveedores de CDMA 200 en todo el mundo en comparación a los 100 que existen para GSM.
- Al ser CDMA 2000 una tecnología nueva existen menos usuarios que GSM, el cual posee más de 550 millones de usuarios.
- El precio nominal de la infraestructura para CDMA 2000 es superior al de la infraestructura para GSM, debido a que este último al ser una tecnología establecida el precio de lo equipos es menor[1].

Finalmente se debe citar que las dos caminos de migración que han emprendido las dos empresas celulares que operan en el Ecuador son válidas, ya que propician a diversificar y mejorar los servicios ofrecidos a los usuarios.

4.5.3 SEGURIDAD Y CALIDAD DE SERVICIO (QoS) EN LAS REDES CELULARES ACTUALES

Los sistemas de segunda generación que actualmente funcionan en el país como se mencionó anteriormente, presentan graves deficiencias en la seguridad y calidad que éstos ofrecen a sus abonados, por lo que a continuación se pretende dar algunas consideraciones para mejorar la seguridad y la calidad de servicio, teniendo en cuenta la visión del estudio realizado en este proyecto de titulación.

4.5.3.1 Consideraciones para la seguridad

La seguridad ofrecida a los usuarios por parte de las dos empresas celulares que operan en el Ecuador se basan principalmente en la utilización del mecanismo de autenticación. Este mecanismo si bien ofrece un cierto grado de protección es insuficiente a las técnicas de fraude que existen actualmente. Por ello, se sugiere a las empresas celulares tener en cuenta las siguientes consideraciones.

- Utilizar mecanismos de confidencialidad por lo menos en el acceso por radio, ya que actualmente son inexistentes en las redes TDMA. Además si tal mecanismo

[1] Referencia [53]: CDMA Technology, "TDMA to CDMA2000 white paper", www.cdg.org.

es implementado se sugiere que las claves de cifrado estén sobre los 128 bits para una mayor protección.

- La información importante del usuario que es transmitida por la red de radio, como por ejemplo el número de identificación móvil MIN y el número de serie electrónico ESN, deben ir encriptadas para evitar que sean usadas por personas desautorizadas.

- Si se quiere utilizar mecanismos de mutua autenticación como el usado en UMTS, es preferible implementarlo dentro del proceso de migración, debido a que los terminales actuales no son capaces de efectuar tal mecanismo.

- Con los presentes sistemas móviles celulares para efectuar un acceso seguro a las diferentes redes de datos como es el caso de Internet, se recomienda que si se usa la tecnología WAP (*Wireless Application Protocol*, Protocolo de Aplicación Inalámbrica) se proteja con el protocolo WTLS (*Wireless Transport Layer Security*, Seguridad del Nivel de Transporte sin Cable) en clase 2 para dotar de mayor seguridad entre el equipo terminal y la plataforma WAP.

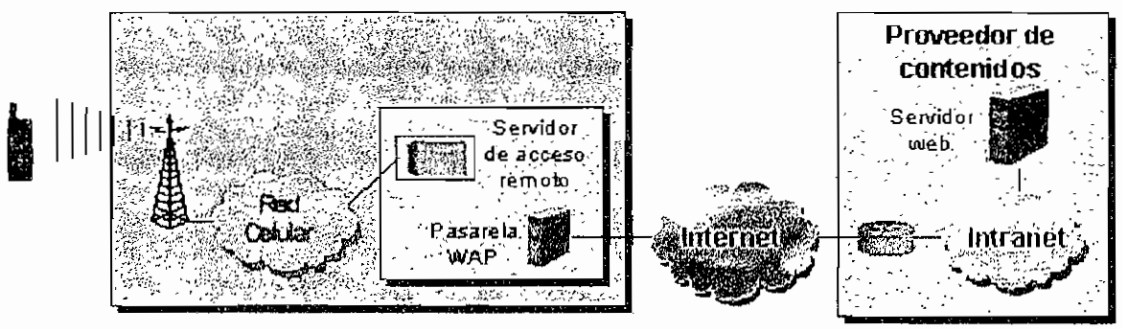


Figura 4.14 Conexión entre el proveedor de contenidos y la red celular

Al utilizar la tecnología WAP también se debe tener presente que para lograr que los prestadores de servicio tengan control de la seguridad, deben realizar un contrato con el propietario de la pasarela que puede ser el operador móvil, para garantizar la confidencialidad de la información que transitan por la pasarela WAP (Figura 4.14). Adicionalmente se puede establecer una VPN (*Virtual Private*

Network, Red Privada Virtual) entre el proveedor de servicios y el operador móvil para garantizar la seguridad de los datos en tránsito.

4.5.3.2 Consideraciones para la calidad de servicio (QoS)

Los sistemas de segunda generación presentes en el Ecuador fueron diseñados básicamente para el transporte de voz en modo de conmutación de circuitos y en mínima proporción para el transporte del tráfico de datos. Por lo tanto, la calidad de servicio tiene que ser referida a:

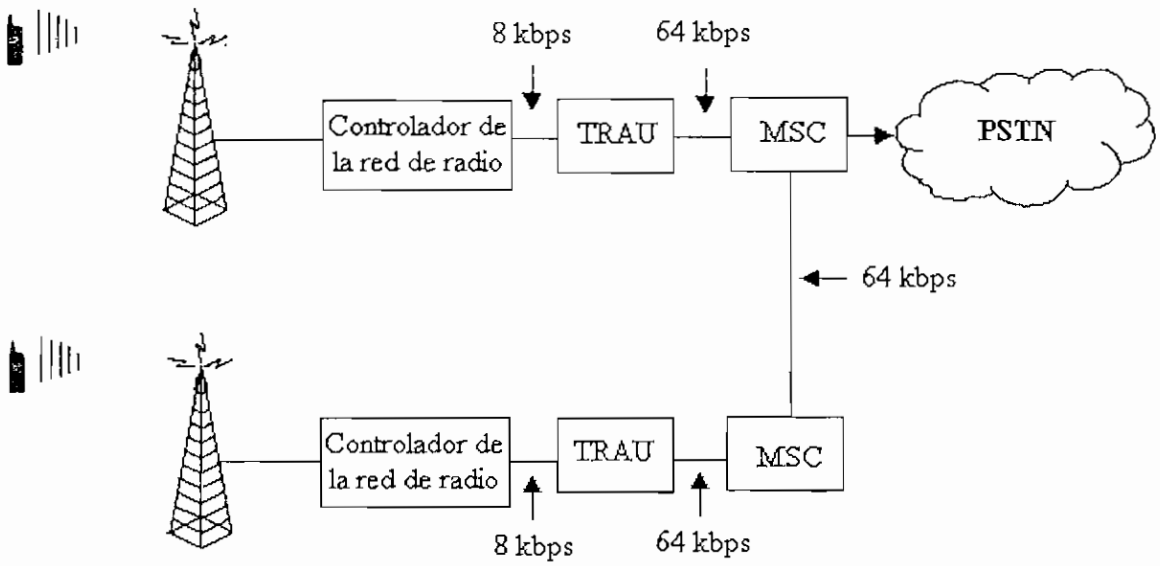
- Una correcta planificación de frecuencias para evitar la interferencia intercelda y un efectivo uso del espectro.
- Una correcta cobertura de radio en diferentes zonas geográficas.
- Un adecuado dimensionamiento de la capacidad de usuarios por celda.

Todo lo anteriormente mencionado tiene como propósito que la probabilidad de bloqueo no sobrepase el valor permitido (según la Superintendencia de Telecomunicaciones un valor aceptable es del 2%).

A más de las consideraciones indicadas anteriormente, en este proyecto de titulación se sugiere a las operadoras el uso de la tecnología TFO (*Tandem Free Operation,* Operación sin Transcodificación)[1] con el objeto de mejorar la QoS ofrecida.

La tecnología TFO consiste en la supresión de los estados intermedios de codificación y decodifcación (transcodificación) entre las llamadas que se originan de una estación móvil y cuyo destino es otra estación móvil. Es decir elimina el proceso de conversión de la señal digital de voz de 8 kbps a una señal PCM de 64 kbps (Figura 4.15).

[1]Referencia [54]: Anne Kumar, "Tandem Free Operation Simulator for Wireless Communications", McGill University, págs: 9-15.



En donde:
TRAU= Unidad de transcodificación
MSC= Centro de conmutación móvil
PSTN= Red telefónica conmutada pública

Figura 4.15 Proceso de codificación en la red celular[1]

El esquema TFO permite el paso transparente entre terminales móviles. Esto significa que en el estándar de la trama PCM, la señal TFO pasará solamente en un slot PCM.

Con ello, los beneficios de usar TFO son:

- Aumento de la calidad de voz en las diferentes llamadas de un móvil a otro móvil debido a la disminución de la distorsión que provoca la transcodificación.
- Eliminación del retardo dado la eliminación de la transcodificación en las estaciones base.
- Ahorro del ancho de banda en la red terrestre.
- Puede ser usado tanto en la tecnología TDMA como CDMA, lo que beneficia el proceso de migración.

[1] Referencia [55]: Graham Rousell, "The implications of ETSI Tandem Free Operation (TFO) in GSM Networks".

Es importante indicar que para el uso del protocolo TFO se debe realizar una programación en los equipos móviles y en los controladores de la red de radio.

El acceso a Internet a través de las redes actuales TDMA se realiza mediante el uso de la tecnología CDPD (*Cellular Digital Packet Data*, Red Celular de paquetes de datos Digitales), la cual es una red inalámbrica de datos diseñada sobre la red celular. CDPD permite velocidades de transmisión de hasta 19.2 kbps utilizando un canal de radio frecuencia completo, por lo que es un sistema caro y no permite el despliegue de aplicaciones de alto nivel como videoconferencia. En este tipo de red no se puede garantizar el servicio de extremo a extremo ya que por ejemplo el uso de tecnologías como MPLS y DiffServ no serían factibles a lo largo de toda la red, debido a que se tendría que hacer una modificación a la arquitectura de CDPD. Por lo tanto, para garantizar en lo posible QoS a los usuarios, se debe tener un plan de frecuencias diferente al de voz teniendo en cuenta las zonas donde existe mayor demanda con el objetivo de evitar interrupciones del sistema. Considerando que la trasmisión de datos en los próximos años crezca del 3% actualmente a un 15-20%[1], es imprescindible que las operadoras tengan presente el concepto de QoS en el proceso de migración que pretenden realizar, por lo que se sugiere que:

En la fase inicial de la introducción de una red central IP, ésta debe trabajar en forma paralela a la red celular existente, es decir por ejemplo la transmisión de voz será separada del transporte de datos hasta que se complete la migración.
Al ser la tecnología CDMA 2000 que se pretende introducir en el país basada en la transmisión de datos en modo de paquete se recomienda el uso de la arquitectura de servicios diferenciados (DiffServ) en la red central (CN) y en la interface entre la red de acceso de radio y la red central, ya que CDMA 2000 en sus normas solamente toma en cuenta el servicio del mejor esfuerzo (best effort).
Los equipos terminales deben ser capaces de funcionar con las tecnologías existentes y futuras, es decir TDMA y CDMA, permitiendo además el soporte de aplicaciones de voz y multimedia.

[1] Referencia [56]: Siemens, "UMTS opening up a world of opportunities", pág: 3.

4.5.4 MARCO REGULATORIO PARA EL USO DE UMTS EN EL ECUADOR

El uso de la tecnología UMTS en el Ecuador se enmarca en el reglamento para "La prestación del Servicio Móvil Avanzado (SMA)" (Resolución No. 498-25-CONATEL-2002).

Este reglamento define al Servicio Móvil Avanzado (SMA) como un servicio final de telecomunicaciones del servicio móvil terrestre, que permite toda transmisión, emisión y recepción de signos, señales, escritos, imágenes, sonidos, voz, datos o información de cualquier naturaleza.

Mediante esta resolución se pretende dar una normativa que tenga en cuenta los cambios y avances tecnológicos de los sistemas móviles, es decir el reglamento antes mencionado tiene como objeto regular la prestación del Servicio Móvil Avanzado (SMA) en el Ecuador.

En resumen este reglamento define que:
La duración del título habilitante para la instalación, prestación y explotación del SMA será de 15 años y su renovación estará de conformidad con el Reglamento General a la Ley Especial de Telecomunicaciones Reformada.

Las bandas de frecuencia para la implementación de SMA estarán en el rango de 1710 MHz a 2025 MHz; y, 2110 MHz a 2200 MHz; las cuales han sido asignadas de acuerdo a las recomendaciones de la ITU y al plan Nacional de Frecuencias existente en el Ecuador.

El SMA se prestará a través de redes públicas de telecomunicaciones, las mismas que deben tener un diseño abierto, esto es que no tengan protocolos ni especificaciones de tipo propietario.

Los prestadores del SMA deben cumplir varias obligaciones como: prestar el SMA en forma continua y eficiente, con los parámetros y metas de calidad del servicio establecidos en el título habilitante, establecer y mantener un sistema de recepción de reclamos de sus usuarios y reparación de daños en su sistema, etc.

Los prestadores del SMA tienen varios derechos como por ejemplo pueden denunciar ante la Superintendencia de Telecomunicaciones las prácticas de competencia desleal, interferencias y demás infracciones que atenten al normal funcionamiento de su servicio.

Al igual que los prestadores de servicio los usuarios tienen varios derechos y obligaciones que cumplir. Por ejemplo un usuario tendría derecho a recibir en forma oportuna una factura de los servicios cobrados; mientras que una obligación del usuario sería, cumplir con las condiciones acordadas en el contrato de prestación del SMA, en especial efectuar puntualmente los pagos referentes a la prestación del servicio.

El SMA se prestará en régimen de libre competencia, por lo que se podrá establecer o modificar libremente las tarifas a los usuarios, de forma que se asegure su operación y prestación, cumpliendo con los parámetros de calidad del servicio. El CONATEL regulará tales tarifas cuando existan distorsiones a la libre competencia en un mercado determinado.

También es importante mencionar que recientemente el CONATEL adjudicó a una tercera operadora el derecho para la explotación del Servicio Móvil Avanzado de Telecomunicaciones, mediante concesión, para el uso de frecuencias esenciales en las bandas C y C', comprendidas en: Banda C: 1895 Mhz-1910 Mhz, y Banda C': 1975 Mhz-1990 Mhz. Es por ello que podría darse en un futuro próximo la implementación del sistema UMTS, lo que generaría una mayor competencia en el mercado celular, mejores planes tarifarios y una mejor calidad de servicio, lo que sin duda beneficiará a todos los usuarios.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- UMTS hace posible la aparición de nuevos servicios móviles que son inexistentes en los sistemas de segunda generación, por lo que producirá el surgimiento de nuevas oportunidades de negocio entre los distintos actores involucrados en la entrega de servicios.

- El uso de la seguridad en UMTS representa un aspecto clave para tratar de eliminar el fraude existente en los sistemas de segunda generación, a través de mecanismos y algoritmos más poderosos que los usados en los anteriores sistemas.

- La arquitectura de seguridad en UMTS al ser divida en dominios posibilita la actualización o reemplazo de componentes de la arquitectura de seguridad sin la necesidad de rehacer toda la red, lo que constituye una fortaleza con respecto a las redes de segunda generación.

- El proceso de autenticación y acuerdo de claves AKA en UMTS incrementa la seguridad con respecto a GSM. Esto se debe a que la autenticación es realizada en el usuario y en la red, lo que no sucede en los sistemas de segunda generación que solamente autentica al usuario en el sistema.

- En UMTS el uso de la visibilidad de la seguridad y la configurabilidad en los terminales dará mayor confianza a los usuarios para que exista un mayor consumo de los servicios que se consideran inseguros, por lo que

habrá un incremento en las ganancias económicas del proveedor de servicios.

- La QoS recibida tiene un gran impacto en la satisfacción de los abonados, por lo tanto la capacidad de proporcionar una mejor QoS será un factor de distinción entre los operadores UMTS.

- El uso de una arquitectura de capas para la provisión de calidad de servicio en UMTS, permite la existencia de un servicio portador extremo a extremo, que no es posible en redes de segunda generación debido a la inexistencia de una arquitectura parecida.

- La diferenciación de la QoS puede proporcionar un ahorro significativo del ancho de banda sobre las interfaces en UMTS, porque los flujos de datos diferidos pueden transmitirse con retardos más largos que los transmitidos en tiempo real.

- La provisión de QoS en sistemas de tercera generación incorpora una característica importante con respecto a los sistemas 2G y su evolución, la cual es el soporte para la negociación por parte del usuario/aplicación de las características del servicio portador UMTS.

- En la red de acceso de radio, UTRAN, la utilización de mecanismos de gestión de radio implicará una administración efectiva de los recursos, los mismos que son escasos en esta parte de la red.

- El conjunto de tecnologías usadas tanto en la red central CN como en la red de acceso de radio UTRAN, permiten garantizar una calidad de servicio conveniente para cada servicio portador UMTS que ha sido negociado.

- Las redes UMTS ofrecen un modelo muy flexible para la creación de servicios tanto por parte del operador como de terceros, debido a

interfaces abiertas que permiten acceder a la funcionalidad de la red de forma independiente a la tecnología que la red emplee.

- El marco de desarrollo de servicios en UMTS permitirá el diseño de servicios que sean exitosos tanto para el proveedor de servicios, en términos de beneficio económico, como para el usuario, en términos del grado de satisfacción del servicio. También proporcionará al operador de la red, a través del escenario de servicio, las pautas para un mejor despliegue de los diferentes componentes de la red.

- En el marco de desarrollo de servicios, los requerimientos tecnológicos de la red UMTS tienen un fuerte impacto en el éxito de un servicio. Por lo tanto, tienen que ser tomados en cuenta durante el desarrollo del servicio.

- La estimación de la capacidad y la cobertura en el desarrollo de servicios debe ser tomada en cuenta, ya que ésta posibilitará o no el despliegue de servicios con diferentes parámetros de calidad de servicio en una determinada área.

- El monitoreo de los parámetros que definen la calidad de servicio en UMTS permiten evaluar el funcionamiento de los mecanismos de gestión de recursos, algoritmos de control de admisión, algoritmos de control de potencia, etc que son utilizados en UTRAN.

- El monitoreo de la seguridad en la red trata de evitar perjuicios tanto para la red como para el suscriptor a través de la creación de perfiles de la conducta de usuario, lo que sin duda ayudará a detectar intrusos en la red

5.2 RECOMENDACIONES

- El crecimiento de los usuarios en la telefonía móvil junto con el surgimiento de nuevos servicios abre la posibilidad a las diferentes operadoras que existen en el Ecuador el uso del sistema de comunicaciones UMTS, ya que al poseer éste mayores capacidades que los sistemas de segunda generación, permitirá la entrega de servicios que sean del agrado del usuario.

- Cuando se habla de calidad de servicio las operadoras deben tener en cuenta que en definitiva es el usuario quien decide si está satisfecho con la QoS suministrada o no; por lo tanto, los estudios de dimensionamieto deben considerar la opinión del usuario para el funcionamiento adecuado de la red.

- Se recomienda al operador el uso de la técnica de *soft handover* en lugar de *hard handover* para minimizar el retardo de los paquetes que podría existir al realizarse un traspaso entre dos sectores.

- Para implementar calidad de servicio extremo a extremo, el operador de la red UMTS debe estar constantemente monitoreando el nivel de servicio entre UMTS y las redes externas

- Para determinar si las estimaciones de la cobertura y la capacidad son adecuadas para el tráfico mixto que existirá en UMTS, se recomienda realizar una simulación para comprobar si los diferentes parámetros (como por ejemplo el margen de interferencia) son adecuados para el correcto funcionamiento de los diferentes servicios.

- Se recomienda a las empresas celulares en el Ecuador el conocimiento de los requerimientos de funcionamiento para un óptimo despliegue de servicios en UMTS, debido a que ello conllevará a una diferenciación entre las distintas operadoras.

REFERENCIAS BIBLIOGRÁFICAS

Libros:

[1] Serie Mundo Electrónico, "Telecomunicaciones Móviles", Alfa Omega México D.F, 1999.

[2] John B. Groe, Lawrence E. Larson, "CDMA Mobile Radio Design", Artech House Publishers Boston 2000.

Especificaciones de la 3GPP (www.3gpp.org):

[3] 3rd Generation Partnership Project, 3GPP TS 23.101, "Technical Specification Group Services and System Aspects General UMTS Architecture", v 5.3.0, 2002-01.

[4] 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.120, , "Security Principles and Objectives", v 3.0.0, 1999-05.

[5] 3 rd Generation Partnership Project, 3G Security, UMTS 33.20, "Security Principles", v3.1.0, 1999-02.

[6] 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.102, "Security Architecture", v 5.0.0, 2002-06.

[7] 3 rd Generation Partnership Project, 3G Security, UMTS 33.22, "Universal Mobile Telecommunications System (UMTS); Security Features", v 1.0.0, 1999-02.

[8] 3 rd Generation Partnership Project, 3G Security, 3GPP TS 33.105, "Cryptographic Algorithm Requirements", v3.8.0, 2001-06.

[9] 3rd Generation Partnership Project, 3G Security, 3GPP TS 21.133, "Security Threats and Requirements", v4.1.0, 2001-12.

[10] 3 rd Generation Partnership Project, 3GPP TS 23.107, "Quality of Service (QoS) Concept and Architecture", v5.3.0, 2002-01.

[11] 3 rd Generation Partnership Project, TSGS1#3, "UMTS Quality of Service", Report 3GPP_TSG_SA_WG1_QoS.

[12] 3 rd Generation Partnership Project 3GPP, TR 23.927, "Virtual Home Environment; Open Service Architecture", v0.1.0, 1999-04.

[13] 3 rd Generation Partnership Project 3GPP, TS 22.105, "Services & service capabilities", v5.2.0, 2002-06.

[14] 3GPP TS 22.101, "Services Aspects; Service principles", 4.2.0, 2001-01.

[15] 3GPP TS 22.127, "Service requirement for the Open Service Access (OSA)", v4.0.0, 2001-01.

Reportes del UMTS Forum (www.umts-forum.org):

[16] UMTS FORUM, "Report on Candidate Extension Bands for UMTS/IMT-2000 Terrestrial Component", Report No.7, 2000.

[17] UMTS FORUM, "Minimum Spectrum Demand per Public Terrestrial UMTS Operators in the initial phase", Report No.5, 2000.

[18] UMTS FORUM, "Enabling UMTS/Third Generation Services and Applications", Report N°11, 2000, pág: 18-43.

[19] UMTS FORUM, "Support of Third Generation Services using UMTS in a Converging Network Environment", Report N°14, 2002, pág:41.

[20] UMTS FORUM, "Key Components for 3G Devices", Report N°15, 2002, pág:21-22, 54.

Revistas de la IEEE:

[21] Jae-Il Jung, IEEE Communications Magazine, "Emerging Data Communications Standards" , Agosto de 1996, pág 108-109.

[22] Dejan M. Novakovic, "Evolution of the Power control techniques for Ds-cdma toward 3G wireless communication systems", IEEE Communications Surveys, Fourth Quarter 2000, pág 3-14.

Referencias de Internet:

[23] Tommi Roman , "3G Wireless Opportunity Space", Helsinki University of Technology, URL: http://www.tuta.hut.fi/studies/Courses_and_schedules/Isib/TU-91.167/Seminar_papers/Old_seminar_papers/roman_tommi.pdf, Enero del 2001, pág 42.

[24] José Manuel Huidobro, "La Evolución Hacia La 3ª Generación De Comunicaciones Móviles", URL: www.cibertele.com/publicaciones/

[25] Revista de Telecomunicaciones de Alcatel, "Normalización de los sistemas móviles 3G", 1er Trimestre 2001, URL: www.alcatel.com, pág:15.

[26] Información UMTS, URL: http://www.gsmspain.com/info_tecnica/umts/

[27] Howard Wolfe Curtis, "Subscriber Authentication and Security in Digital Cellular Networks and Under the Mobile Internet Protocol", Report University of Texas at Austin, Mayo 2001, pág 112, URL: http://www.portelligent.com/

[28] Jonas Kullenwall, "Study of security aspects for Session Initiation Protocol", Linköping University, Abril 2002, pág 58, URL: http: // www.ep.liu.se /exjobb/isy/2002/3234/exjobb.pdf

[29] Juha Salvela, "Access Security in Third Generation Mobile Networks", URL: http://www.hut.fi/~salvela/netsecu.html.

[30] Arturo Quirantes, "La seguridad de los teléfonos móviles",16 de marzo del 2001, URL: http://www.ugr.es/~aquiran/cripto/informes/info026.htm.

[31] Luis Gonzaga, "Calidad de Servicio (QoS) Garantizada", UPC, febrero del 2001, URL: http://www.tdcat.cesca.es/, pág 189-192.

[32] Revista de Telecomunicaciones de Alcatel – 1er Trimestre 2001, "QoS implementation in UMTS networks", URL: www.alcatel.com, pág 44.

[33] Aplicaciones MPLS, "MPLS. Ingeniería de Tráfico y RPV de Proveedor", URL: http://pegaso.ls.fi.upm.es/disenyo_planif/mpls-TRAF-RPV.PDF, pág. 3, 11.

[34] Nortel Networks, "Benefits of Quality of Service (QoS) in 3G wireless Internet", URL: http: // a240.g.akamai.net/ 7/ 240 / 5107 / 20020706034338 / www.nortelnetworks.com / products/library/collateral/66028.25-09-01.pdf, pág 7,10.

[35] Nortel Networks, "Introduction to Quality of Service (QoS)", URL: http://www.nortelnetworks.com/products/library/collateral/56058.25-09-01.pdf, Septiembre 2001.

[36] S. Blake , "An Architecture for Differentiated Services", RFC 2475, 1998.

[37] S. I. Maniatis, E. G. Nikolouzou, I. S. Venieris, "Convergence of UMTS and Internet Services for End-to-end Quality of Service Support", National Technical University of Athens, URL: http: // www.ing.unipi.it /ew2002 / proceedings / 139.pdf

[38] Luis Almajano, Jordi Pérez-Romero, "Packet Scheduling Algorithms for Interactive and Streaming Services under QoS Guarantee in a CDMA System", (UPC), URL: http: // www.gcr.tsc.upc.es / proceedings /conferences2002 /Packet_Scheduling_Algorithms.pdf

[39] J. Sánchez, "Mixing Conversational and Interactive Traffic in the UMTS Radio Access Network", (UPC), URL: http:// www.gcr.tsc.upc.es/ proceedings/conferences2002/Mixing_Conversational.pdf

[40] Frank Yong Li, "Providing Conformance of the Negotiated QoS using Traffic Conditioning for Heterogeneous Services in WCDMA Radio Access Networks", Norwegian University, URL: http://www.nik.no/2001/12-li.pdf

[41] Carlos Díaz, "Arquitectura de Protocolos en la Red de Acceso UMTS", URL: greco.dit.upm.es/~david/TAR/trabajos2002/ 02-Arquitectura-red-acceso-UMTS-Carlos-Diaz-Motero-res.pdf, pág 18-19.

[42] Smaragdakis Georgios, "TCP Performance over UMTS Network", Technical University of Crete, URL: http :// www.ccs.neu.edu /home /vassilis /SmaragdThesis02.pdf, pág 37-39, 73-74.

[43] EURESCOM Project P921, "Review of foreseen UMTS applications", URL : http://ftp.eurescom.de/~public-web-deliverables/P900-series/P921/D2/doc/UMTS applications.doc.

[44] Revista de Telecomunicaciones de Alcatel, "Servicios móviles basados en la posición: puntos fundamentales", 1er Trimestre 2001, URL: www.alcatel.com, pág 73-74.

[45] FTW (Forschungszentrum Telekommunikation Wien), "UMTS Applications Development", URL: www.ftw.at.

[46] Katja Koivu, "Data service development in mobile networks", Helsinki University of Technology, URL: http://www.cs.hut.fi/~pmrg/Publications.html, pág:27.

[47] M.Lasanen, "Modem requirements for baseband, RF/IF subsystem and DLC/MAC layer", IST (information society technologies), URL: http://www.vtt.fi/ele/research/els/projects/windflexdeliverables/deliverables_d21.pdf, 31-05-2000, pág:29.

[48] Nokia Networks, "Radio Network Planning Process and Methods for WCDMA", URL: lib.hut.fi/Diss/2002/isbn9512259028/article3.pdf, pág:2.

[49] Takis Mathiopoulos, "UMTS: the evolution of GSM toward IMT-2000", University of British Columbia, URL: http: // www.ece.ubc.ca /~alexp/ wireless_termpaper.pdf, pág:16.

[50] Zhi-Chun Honkasalo, "Radio Network Planning", WCDMA for UMTS, edited by Harri Holma, URL: http://lib.hut.fi/Diss/2002/isbn9512259028/article4.pdf, 2001, págs: 10-11, 18.

[51] 3G Phone, URL: www.cellular.co.za.

[52] Artículo de la revista Conectados, "Celulares: en busca del servicio perdido", URL: www.conectados.com.ec.

53] CDMA Technology, "TDMA to CDMA2000 white paper", URL: www.cdg.org.

[54] Anne Kumar, "Tandem Free Operation Simulator for Wireless Communications", McGill University Montreal Canada, URL: http://www.tsp.ece.mcgill.ca/Theses/2001/KumarP2001.pdf, Enero del 2001, págs: 9-15.

[55] Graham Rousell, "The implications of ETSI Tandem Free Operation (TFO) in GSM Networks", URL: http: // www.coherent.com / tech / articles / mobile Europe 0999.html, Mobile Europe.

[56] Siemens, "UMTS opening up a world of opportunities", URL : http://www2.siemens.no/multimedia/archive/00050/umts_50271a.pdf, pág: 3.

ANEXO 1

ABREVIATURAS

ACK (Acknowledgement)

AK (Anonymity Key)

AKA (Authentication and Key Agreement)

AMF (Authentication Management Field)

AMPS (American Mobile Phone System)

ATM (Asynchronous Transfer Mode)

AuC (Authentication Centre)

AUTN (Authentication Token)

AUTS (Synchronisation Authentication Token)

AV (Authentication Vector)

BER (Bit Error Rate)

BG (Border Gateway)

BS (Bearer Service)

CAC (Call Admission Control)

CDMA (Code Division Multiple Access)

CK (Cipher Key)

CN (Core Network)

CoS (Class of Service)

CRC (Cyclic Redundancy Check)

CS (Circuit Switched)

CSMA/CA (Carrier Sense Múltiple Access/Collision Avoidance)

CT (Cordless Telephone)

Cu (Punto de referencia entre el USIM y el ME)

CS (Circuit Switched)

D-AMPS (Digital AMPS)

DCA (Dynamic Channel Assignement)

DCS-1800 (Digital Cellular System –1800 MHz).

DECT (Digital Enhanced Cordless Telecommunications)

DS (Differentiate Service)

DSCP (DiffServ Code Point)

EDGE (Enhanced Data-rates for GSM Evolution)

EIR (Equipment Identity Register)

EMSI (Encrypted Mobile Subscriber Identity)

ETSI (European Telecommunications Standars Institute)

ERMES (European Radio Message System)

FDD (Frequency Division Duplex)

FDMA (Frequency División Multiplex Accessing)

FER (Frame Erasure Ratio)

FFQ (Fluid Fair Queueing)

Gc (Interfaz entre GGSN y HLR)

GGSN (Gateway GPRS Support Node)

GMSC (Gateway MSC)

GPRS (General Packet Radio Service)

GPS (Generalized Processor Sharing)

Gr (Interfaz entre SGSN y HLR)

GSM (Global System for Mobile communications)

3GPP (3rd Generation Partnership Project)

HE (Home environment)

HIPERLAN (High Perfomance Radio LAN)

HLR (Home Location Register)

HSCSD (High Speed Circuit-Switched Data)

IETF (Internet Engineering Task Force)

IK (Integrity Key)

IMEI (International Mobile Equipment Identity)

IMT-2000 (International Mobile Telecommunications 2000)

IMUI (International Mobile User Identity)

IP (Internet Protocol)

IPv4 (Internet Protocol version 4)

IPv6 (Internet Protocol version 6)

ITU (International Telecommunications Union)

JDC (Japanese Digital Cellular)

K (Secret Key)

KSI (Key Set Identifier)

LA (Location area)

LAI (Location Area Identity)

LDP (Label Distribution Protocol)

Iu (Punto de referencia entre los dominios de acceso y red troncal)

MAC (Medium Access Control)

ME (Mobile Equipment)

MPLS (Multi Protocol over Label Switching)

MS (Mobile Station)

MSC (Mobile Switching Center)

MSS (Mobile Satelite Services)

MT (Mobile Termination)

NTT (Nipon Telephone and telecommunications)

OSA (Open Service Access)

PACS (Personal Access Communications Services).

PCS (Personal Communications Systems)

PDU (Packet Data Unit)

PDP (Packet Data Protocol)

PHB (Per Hop Behaviour)

PHS (Personal Handyphone System)

PIN (Personal Identification Number)

PLMN (Public Land Mobile Network)

PNNI (Private Network – Network Interface)

POCSAG (Post Office Code Standars Advisory Group)

PS (Packet Switched)

QoS (Quality of Service)

RAB (Radio Access Bearer)

RAC (Radio Admission Control)

RAN (Radio Access Network)

RAND (Random challenge)

RLC (Radio Link Control)

RNC (Radio Network Controller)

RRC (Radio Resource Controller)

RSVP (Resource Reservation Protocol)

RTP *(Real-time protocol)*.

RTSP *(Real-time Streaming Protocol)*

SAP (Service Access Point)

SDU (Service Data Unit)

SGSN (Serving GPRS Support Node)

SIM (Subscriber Identity Module)

SLA (Service Level Agreement)

SMS (Short Message Service)

SN (Serving Network)

SQN (Sequence number)

TACS (Total Access Communications System)

TDD (Time Division Duplex).

TDMA (Time División Multiplex Accessing)

TE (Terminal Equipment)

TETRA (Trans European Trunked Radio)

TMUI (Temporary Mobile User Identity)

ToS (Type of Service)

UDP (User Datagram Protocol)

UE (User Equipment)

UEA (UMTS Encryption Algorithm)

UIA (UMTS Integrity Algorithm)

UMTS (Universal Mobile Telecommunication System)

USIM (User Services Identity Module)

UTRA (Universal Mobile Telecommunications System Terrestrial Radio Access)

UTRAN (UMTS Terrestrial Radio Access Network)

Uu (Interfaz entre y la parte de la red fija UMTS)

UWC-136 (Universal Wireless Communicatios-136)

VC (Virtual Clock)

VHE (Virtual Home Environment)

VLR (Visitor Location Register)

WARC (World Administrative Radio Conference)

WCDMA (Wideband CDMA)

WFQ (Weighted Fair Queueing)

WIMS W-CDMA (Wireless multimedia and Messaging Services W -CDMA)

WLAN (Wireless LAN)

XRES (Expected Response)

ANEXO 2

GLOSARIO DE TÉRMINOS

AUTS: El valor de sincronización es generado en el USIM cuando el número de secuencia del AuC esté fuera de rango con respecto al número de secuencia del USIM. La secuencia de número del USIM es entonces enviado en el AUTS a el AuC para continuar con el proceso de resincronización.

Canal lógico: Un canal lógico es un flujo de información dedicado a la transferencia de un tipo específico de información sobre la interface de radio. Los canales lógicos son suministrados sobre la capa MAC.

Clave de cifrado: Es un código usado junto a un algoritmo de seguridad para codificar y decodificar a un usuario y/o datos de señalización.

Clave K: Es la clave secreta compartida por el USIM y AuC. Esta clave es de mucha importancia dentro del proceso de autenticación y establecimiento de claves. En el proceso de autenticación si al calcular el valor XMAC en el USIM resulta diferente del valor MAC, entonces quiere decir que la clave compartida K no es la misma, por lo que la estación móvil abandona el proceso.

Comunicaciones Personales: Tendencia en las telecomunicaciones hacia la personalización del servicio, cuya expresión máxima es la identificación de un usuario mediante un único número de abonado que identifica al usuario ante los distintos terminales y no por los distintos terminales a los que tiene acceso.

Encriptación: Codificación, mediante claves secretas conocidas por el emisor y el receptor, de un mensaje para garantizar la seguridad de la comunicación en su recorrido.

Entorno Local (HE): El HE es responsable por permitir a un usuario obtener servicios UMTS en un modo consistente, a pesar de la ubicación del usuario o el terminal usado (dentro de las limitaciones de la red de servicios y el terminal actual).

El HE es el responsable total por la provisión de un servicio o un conjunto de servicios a los usuarios asociados a una suscripción. A continuación se indican las responsabilidades de HE:

- La provisión, asignación y administración de las cuentas del suscritor.
- La provisión y mantenimiento de perfiles del usuario para los subscriptores y los usuarios asociados, incluso la provisión y control de acceso de los mencionados perfiles por parte de los usuarios y subscriptores.
- Negociación con los operadores de red para proporcionar servicios UMTS a sus usuarios, como interacción on- line para que los usuarios sean identificados, localizados, autenticados y autorizados para el uso de los servicios.

Estación base falsa: Un delincuente simula el sistema móvil celular en cuestión, con una "estación base" que obliga activamente a los terminales móviles de sus cercanías a transmitir información secreta.

Fiabilidad: Pérdida de datagramas.

IMEI: Una "Identidad Internacional del Equipamiento Móvil" es un único número que se asignará a cada equipo móvil en la PLMN y será incondicionalmente implementado por el fabricante de MS.

IMSI: Es la identidad internacional del suscriptor móvil, que esta formada de una cadena de cifras decimales, que identifica internacionalmente a un abonado del servicio móvil GSM.

IMUI: Es la identificación única de un usuario. El IMUI es almacenada en el USIM en el lado del suscriptor, y en la base de datos del HE en el lado de la red en el momento de la suscripción.

IMUN: El IMUN (el número de usuario móvil internacional), es el número telefónico asignado a un usuario UMTS.

Jitter: Fluctuaciones del retardo (muy crítico en servicios de comunicaciones de tiempo real).

Latencia: Tiempo de transferencia en la red.

MACS y XMACS: El MACS (el código de autenticación para la resincronización) y XMACS son usados para autenticar al USIM antes de reajustar el número de secuencia del AuC.

Cuando el USIM encuentra un fracaso en la sincronización genera el MACS y lo envía al AuC, este por otro lado genera su propio XMAC y los compara. Si estos valores son iguales, el mensaje de fracaso en la sincronización "synchronisation

failure" es autentificado y el número de secuencia del AuC será restablecido al valor al número de secuencia del USIM.

MT (Mobile termination): La terminación móvil es el componente de la estación móvil que apoya las funciones específicas a la gestión de la interface de la radio (Um).

NP (Network Performance): La habilidad de una red o parte de la misma de ofrecer las funcionalidades necesarias para la comunicación entre usuarios.

Pasarelas de medios: Las pasarelas de medios (media gateways) desempeñarán un papel fundamental en la evolución hacia la nueva arquitectura, mediando en el cruce entre las tecnologías existentes y de nueva transmisión, y los tipos de red.

PDP: Protocolo de datos en modo de paquete, ejemplo IP o X.25

PDP (punto de decisión de policía): Es una entidad específica en el concepto Diffserv el cual es responsable por determinar las acciones que son aplicables a los paquetes. El PDP es usado para controlar las acciones que son realizadas por el punto de exigencia de policía (PEP). PEP es usualmente ubicado en un nodo Diffserv y es responsable por la imposición (exigencia) y ejecución de las acciones de policía.

Perfil de QoS: Un perfil de QoS comprende varios parámetros de QoS. Un perfil de QoS es asociado con cada sesión de QoS. El perfil de QoS define las expectativas de funcionamiento tomadas sobre la red del portador.

Petición de QoS: Un perfil de QoS se pide al principio de una sesión de QoS. Los pedidos de modificación de QoS son también posibles durante el tiempo de vida de una sesión de QoS.

PIN: Número de identificación personal. Un código usado por un número telefónico móvil junto con una tarjeta USIM para completar una llamada.

Plano de usuario: El plano de usuario es usado para el transporte de información de usuario (voz por medio de circuitos conmutados, paquetes por Internet), control de la información empaquetada en varios canales de transporte y enviados transparentemente sobre enlaces de radio.

Plano de control: El plano de control es usado para señalización. En el dominio de conmutación de circuitos se basa en SS7 (en el CN), mientras en el dominio de conmutación de paquetes se basa en IP (en el CN).

QoS negociado (Negotiated QoS): En respuesta a un pedido de QoS, la red negociará cada atributo de QoS a un nivel que está de acuerdo con los recursos disponibles de la red. Después de la negociación de QoS, el portador de la red intentará siempre proporcionar los recursos adecuados para apoyar todos los perfiles de QoS negociados.

QoS suscrito: Quiere decir que la red no concederá un mayor QoS que el suscrito. Un usuario final puede tener varias suscripciones de QoS. Para la seguridad y la prevención de daño a la red, el usuario final no puede modificar os perfiles de suscripción de QoS.

Retardo extremo a extremo: Tiempo de transferencia entre entidades del nivel de aplicación.

Retardo del servicio: El tiempo transcurrido de la invocación de la petición del servicio a la correspondiente indicación de petición del servicio al receptor del servicio, indicando la llegada de la aplicación.

RNC (Controlador de la Red de Radio): Este equipo en el RNS está a cargo de controlar el uso y la integridad de los recursos de radio.

RNS (Radio Network Subsystem): Toda la red o solamente la parte de acceso de un UTRAN ofrecen la asignación y la liberación de recursos de radio específicos para establecer medios de conexión entre un UE y el UTRAN. Un RNS es responsable por los recursos y la transmisión/recepción en un conjunto de celdas.

SAP (Puntos de acceso al servicio): En el modelo de referencia OSI, son los puntos que a través de ellos los servicios son ofrecidos a una capa más alta.

SDU: Unidad de datos de servicio. Es la carga de datos de usuario.

SEQ: Es un contador secuencial, encargado de verificar si el número de secuencia (SQN) está en el rango correcto.

Para cada usuario, HE mantiene un contador SEQ_{HE}. El mecanismo asegura que un número secuencial es aceptado si pertenece a los anteriores 50 números secuenciales generados.

Servicio de mejor esfuerzo (best effort): Cuando se desarrolló el concepto de conmutación de paquetes, se aplicó un servicio de *mejor esfuerzo*, el cual trata los paquetes sin hacer ninguna diferenciación entre los diferentes tipos de flujos. Todos los paquetes reciben la misma prioridad al momento de ser procesados por el enrutador de paquetes (el cual se encarga de decidir cual paquete es el que

va a pasar primero al enlace). De esta manera, los paquetes son más sensibles a los retardos.

Servicios asimétricos: La velocidad de transmisión de datos al abonado es mucho mayor que la velocidad de retorno, por ejemplo, la navegación por el Web, donde la descarga de ficheros requiere el movimiento de cantidades de información mucho mayores en un sentido, hacia el usuario, que desde este.

Servicios simétricos: La velocidad de transmisión de datos al abonado es similar a la de transmisión al proveedor del servicio, por ejemplo la video-telefonía.

Señalización: El intercambio de información especialmente concerniente con el establecimiento y control de conexiones, y con la administración en una red de telecomunicaciones.

Sesión de QoS: El periodo entre la apertura y cierre de una conexión de la red cuyas características son definidas por un perfil de QoS. Múltiples sesiones de QoS pueden existir cada una con un diferente perfil de QoS.

SIM: En un contexto de seguridad, este módulo es responsable de realizar la autenticación y acuerdo de claves en GSM. Se debe indicar que este no es capaz de realizar la autenticación y acuerdo de claves en UMTS.

SN (Red de Servicios): El SN proporciona al usuario el acceso a los servicios de HE.

El SN tiene la función de proporcionar recursos fijos para conmutar y gestionar los servicios ofrecidos a los usuarios.

Las responsabilidades de SN caen en las siguientes áreas:

- La provisión y gestionamiento de los recursos fijos, conexiones y ruteo.
- La interacción con y provisión de medios para HE para identificar, autenticar, autorizar y localizar a los usuarios.
- La interacción y provisión de medios para la administración del terminal.

SQN: SQN es introducido para prevenir que la red trate de usar los mismos AVs para múltiples procesos de autenticación y generación de claves.

SQN_{MS}: Es un contador que es igual al número de secuencia más alto SQN en un parámetro de AUTN aceptado por el usuario.

Suscriptor: La responsabilidad para el pago (factura) incurrido por uno o más usuarios puede ser emprendida por otra entidad designada como suscriptor.

Esta división entre el uso y el pago por los servicios no tiene impacto sobre la estandarización.

TE Equipo terminal (Terminal Equipment): Equipo que proporciona las funciones necesarias para la operación de los protocolos de acceso por el usuario (la fuente: GSM 01.04). UN grupo funcional en el lado del usuario de una interface de la usuario-red (la fuente: ITU-T I.112).

Un TE es conectado a la red UMTS por el uso de un MT.

Throughput: Es un parámetro que describe la velocidad del servicio. El número de bits de datos útiles transferidos en una dirección entre puntos específicos de referencia por unidad de tiempo.

TPC (Transmit Power Control): Son bits de control del canal físico DPCCH utilizados por el emisor en el algoritmo de control de potencia y sirve para indicar su incremento o decremento.

UDP: Protocolo de datagrama de usuario.

UE: Es el equipamiento de usuario, y es el sinónimo de estación móvil (MS) en GSM.

UEA: Algoritmo de encriptación de UMTS. El mismo algoritmo de encriptación tiene que ser usado en el USIM y en el RNC. El USIM informa al RNC que algoritmos este soporta. El RNC entonces escoge por preferencias de la red y de las regulaciones existentes que algoritmo de encriptación se usará.

UIA: Es el algoritmo de integridad de UMTS. Este estará en el USIM y en el RNC. Ellos podrán estar en diferentes dominios del operador. Debido a esto diferentes nodos pueden soportar diferentes algoritmos. Para identificar los diferentes algoritmos usados, cada UIA tendrá su propio identificador de 4 bits. El USIM proporcionará al RNC la información sobre que UIAs este soporta para que decida (por preferencia del operador) que UIA se usará consecuentemente.

USIM: En un contexto de seguridad, este módulo es responsable de realizar la autenticación y acuerdo de claves en UMTS. También este es capaz de realizar la autenticación y acuerdo de claves en GSM permitiendo a un suscriptor fácilmente el traspaso a una red GSM.

Usuario: Es una entidad que no forma parte de UMTS, que usa los servicios de UMTS. Ejemplo: una persona que usa una estación móvil UMTS como un teléfono portátil.

Es una entidad lógica, identificable que usa los servicios.

Usuario final: Como usuario final se entiende cualquier nivel superior del sistema de comunicaciones que tenga unas necesidades de calidad determinadas.

Vector de autenticación: Autenticación temporal y establecimiento de clave que permite al VLR/SGSN participar en UMTS AKA con un usuario particular. En UMTS un vector de autenticación consiste de cinco elementos:

Un número aleatorio RAND

Una respuesta de usuario XRES

Una clave de cifrado CK

Una clave de integridad IK, y

Un valor de autenticación (AUTN).

ANEXO 3

Definición del campo de servicios diferenciados (DS)

Para aplicar la diferenciación de servicios se definió un campo que sustituyera las actuales definiciones del campo "Tipo de Servicio" en Ipv4.

Los primeros 6 bits son utilizados como parte del código mientras que los últimos dos bits deben ser ignorados por los nodos que tengan implementado DiffServ. La estructura del campo DS se muestra a continuación:

Tabla 1 Campo ToS del protocolo Ipv4

0	1	2	3	4	5	6	7
DSCP						SU	

Donde:

DSCP = DiffServ Code Point

SU = Sin uso

Cada código mapea un PHB determinado. Actualmente existen 4 PHB especificados para ser usados dentro de una red de servicios diferenciados:

- comportamiento por omisión (Default Behavior)
- Selector de clase
- Tránsito expedito (Expedited forwarding)
- Tránsito asegurado (Assured forwarding)

Comportamiento por omisión (o mejor esfuerzo)

Es el comportamiento que todas las redes que implementen DiffServ deben de incorporar. Este comportamiento equivale a un servicio de mejor esfuerzo. Todos

los paquetes que no tengan especificado un comportamiento, utilizan el servicio de mejor esfuerzo para moverse a través de la red. El código que representa el comportamiento por omisión es el 0x000000.

Seleccionador de clase (CS PHB)

Este comportamiento define hasta ocho clases distintas en la red. El formato del código toma en cuenta los primeros 3 bits del octeto 0xXXX000. Los tres primero bits representan un número del 0 al 7. El número de menor valor representa una prioridad menor (es decir, los tres primeros bits son cero, el cual corresponde al comportamiento por omisión o de mejor esfuerzo) mientras que un número mayor representa una prioridad mayor. No es necesario que un nodo (puede ser un nodo interno) soporte las ocho clases. Puede agrupar las clases para soportar por ejemplo 2 prioridades. Los códigos con número 1 al 3 pueden representar una prioridad baja, mientras que los códigos con los números del 4 al 7 representan una prioridad alta. De esta forma, el nodo sigue siendo compatible con la especificación DiffServ, aún sin tener ocho clases definidas.

Tabla 2 Códigos para el selector de clase

Clase	Código
0	0x000000
1	0x001000
2	0x010000
3	0x011000
4	0x100000
5	0x101000
6	0x110000
7	0x111000

Los nodos que utilizan este PHB pueden implementarlo utilizando los manejadores de colas SPQ, WFQ, WRR o CBQ por ejemplo.

Tránsito expedito (EF PHB)

Este PHP tiene asociado una tasa de transmisión la cual la define el ISP. La función de este PHB es proveer las herramientas necesarias para proveer un

servicio extremo-extremo con bajas pérdidas, bajo retardo, bajo jitter y un ancho de banda asegurado dentro de un dominio DiffServ.

El principio de operación es que la tasa de partida de los paquetes debe ser igual o mayor a una tasa configurada por el administrador. Esta tasa no puede ser menor que la tasa de llegada de paquetes. Esto significa que si tenemos una serie de paquetes del mismo tamaño que llegan a un nodo, éstos saldrán del nodo con la misma tasa de entrada. La idea es reducir el exceso de retardo y jitter en lo posible.

La figura siguiente nos muestra el principio de operación del EF PHB.

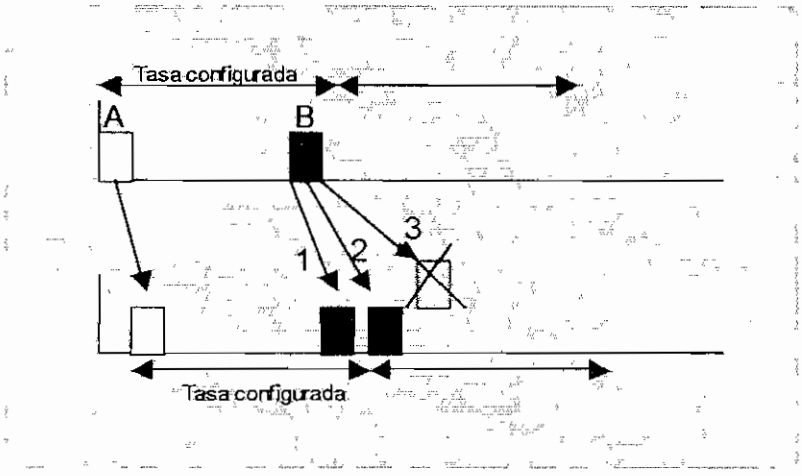


Figura 1 Modelado y descarte de paquetes

Cuando el paquete llega antes de su tiempo programado de llegada, existen tres opciones en los nodos de ingreso e internos para su tratamiento:

1. Reenviar el paquete inmediatamente
2. Reenviar el paquete en el tiempo configurado
3. Descartar el paquete

Las opciones que toman los nodos de acceso e internos son diferentes: los nodos de acceso por lo general tomaran las opciones 2 y 3 para evitar que la fuente se apropie de un mayor ancho de banda del que se tiene configurado. Para los

nodos internos, es altamente recomendada la opción 1, ya que la aplicación de la opción dos podría provocar retardos acumulados.

El EF PHB requiere un alto control sobre la tasa de transmisión de paquetes en los nodos de acceso a la red y de un rápido reenvío de paquetes en los nodos internos de la red.

La finalidad de este PHB es la de proveer enlaces de alta calidad, con respecto a retardo y pérdidas. EF puede ser utilizado para proveer enlaces que simulen enlaces dedicados, con bajos retardos y bajas variaciones en el ancho de banda.

Transito asegurado (AS PHB)

Este PHB define cuatro clases, a las cuales se les tiene que asignar espacio en el buffer y ancho de banda de manera independiente en cada nodo. Cada una de estas clases se le especifica tres niveles de descarte. Es importante señalar que no es necesario implementar los tres niveles de descarte. Si el operador de la red, no espera que existan muchas condiciones de congestión, el número de niveles de descarte se puede compactar a dos.

Tabla 3 Códigos DS recomendados para AS PHB

	Clase 1	Clase 2	Clase 3	Clase 4
Baja probabilidad de descarte	001010	010010	011010	100010
Media probabilidad de descarte	001100	010100	011100	100100
Alta probabilidad de descarte	001110	010110	011110	100110

QCUDI, "Propuesta del grupo de trabajo QCUDI", URL: http: // telematica.cicese.mx/i2/Informes/InformeQcudi.doc.

ANEXO 4

ALGORITMO WFQ

Este planificador fue introducido con el nombre de *Weighted Fair Queueing* (WFQ) en *[Demers89]* aunque luego se ha rebautizado como PGPS *(Packet General Processor Sharing*). Es un intento de aproximarse a un modelo de flujo perfecto (denominado GPS: *General Processor Sharing*) con un procesador compartido entre los distintos flujos de acuerdo a unos pesos predeterminados. De esta forma, el ancho de banda se reparte proporcionalmente entre los distintos flujos.

En los algoritmos WFQ, cuando llega una trama se calcula y asocia una etiqueta *(Time Stamp*, TS) que va a determinar el orden de salida y se envía a la cola de su conexión. La siguiente trama a transmitir será la que tenga el valor TS más pequeño.

TS se calcula de acuerdo a siguiente la fórmula:

$$TS_1^0 = 0$$

$$TS_1^k = \max(TS_i^{k-1}, v(t)) + \frac{L_i^k}{\rho_i}$$

donde:

v(t) es la función de tiempo virtual calculada a la llegada del paquete.

TS_i^{k-1} corresponde al *time stamp* de la trama anterior.

L_i^k es el tamaño del paquete en bits.

ρ_i es el ancho de banda deseado para la sesión *i*.

La función *v(t)* se calcula así: si *B(t)* representa el conjunto de sesiones con algún paquete en cola *(backlogged)* en el planificador en el instante *t* y *V* el número total de sesiones, entonces:

$$v(t) = \frac{\sum_{j=1}^{V} \phi_j}{\sum_{i \in B(t)} \phi_i}$$

Donde ϕ es un número real que indica la porción de ancho de banda del enlace requerido por la sesión que cumple la siguiente condición:

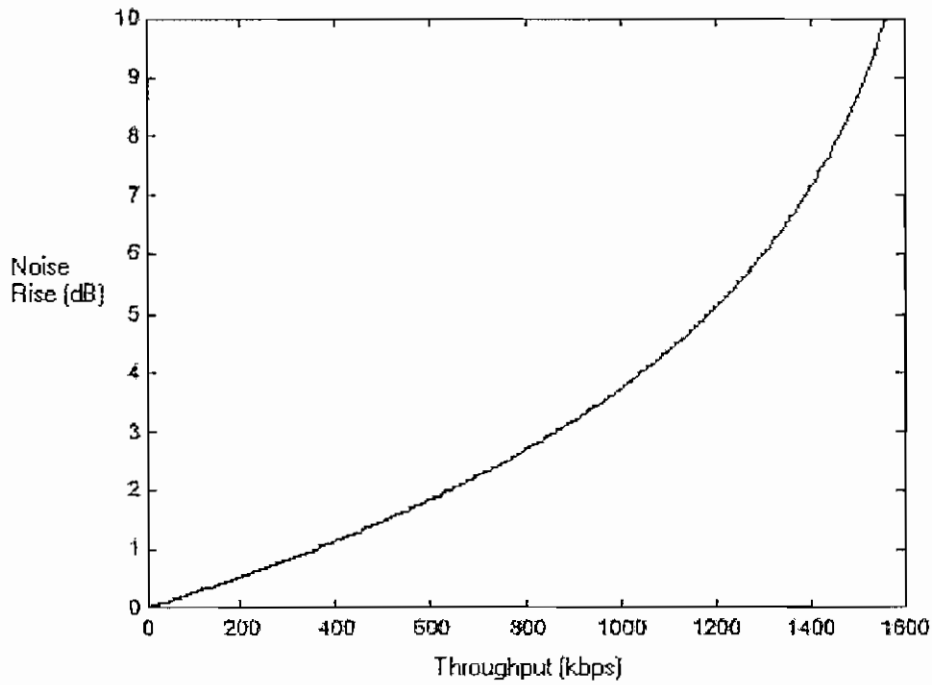
$$\rho_i \leq \frac{\phi_i}{\sum_{j=1}^{V} \phi_j} r$$

donde *r* es la capacidad de enlace. Por ejemplo, se puede usar $\phi_i = \rho_i / r$.

Cuando una sesión tiene tráfico pendiente, se cumple que $v(t) \leq TS_i^{k-1}$ por lo que *v(t)* no influye en *TS*. En caso contrario, al recibir la primera trama después de un periodo sin tráfico, se tiene en cuenta *v(t)* para actualizar la sesión. La dificultad del planficador WFQ reside en calcular *v(t)*, por lo que se han propuesto otros algoritmos que simplifican su cálculo.

ANEXO 5

CURVA DEL AUMENTO DE RUIDO EN FUNCIÓN DEL THROUGHPUT



$$\eta_{UL} = (1+i).\sum_{j=1}^{N} \frac{1}{\frac{W}{v_j.\left(\frac{E_b}{N_o}\right)_j.R_j}+1}$$

$$noise\_rise = 10 \cdot \log_{10}\left(\frac{1}{1-\eta_{UL}}\right)\_[dB]$$

Dan Ouchterlony, "New service opportunities in 3G:A relative system resource usage model for UMTS QoS classes", URL: http: // www.i.kth.se /i96_oun/exjobb/docs/, página:44.

ANEXO 6

Parámetros para el presupuesto del enlace

Table 1. Reference link budget of non-real-time 384 kbps data service (3 km/h, outdoor user, Vehicular A type channel, no soft handover)

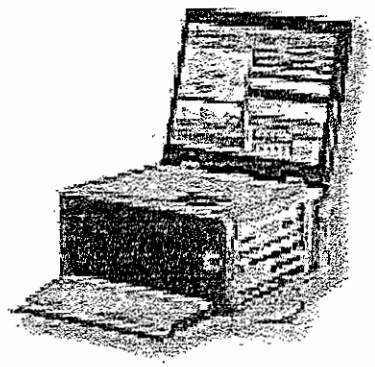
Table 1

Transmitter (mobile)	
Max. mobile transmission power [W]	0.25
As above in dBm	24.0
Mobile antenna gain [dBi]	2.0
Body loss [dB]	0.0
Equivalent Isotropic Radiated Power (EIRP) [dBm]	26.0
Receiver (base station)	
Thermal noise density [dBm/Hz]	-174.0
Base station receiver noise figure [dB]	5.0
Receiver noise density [dBm/Hz]	-169.0
Receiver noise power [dBm]	-103.2
Interference margin [dB]	3.0
Receiver interference power [dBm]	-103.2
Total effective noise + interference [dBm]	-100.2
Processing gain [dB]	10.0
Required Eb/No [dB]	1.0
Receiver sensitivity [dBm]	f[load]
Base station antenna gain [dBi]	18.0
Cable loss in the base station[dB]	2.0
Fast fading margin [dB]	4.0
Max. path loss [dB]	f[load]
Coverage probability [%]	95
Log normal fading constant [dB]	7.0
Propagation model exponent	3.52
Log normal fading margin [dB]	7.3
Soft handover gain [dB], multi-cell	0.0
Indoor loss [dB]	0.0
Allowed propagation loss for cell range [dB]	f[load]

Harri Holma, Zhi-Chun Honkasalo, "Radio Network Planning", 2001 John Wiley & Sons Ltd, página: 7.

ANEXO 7

Equipo para el monitoreo de la QoS Acterna 8630-3G/UMTS



The high-performance portable test solution for 3rd generation
The industry's first modular wireless network analyzer targeting for simultaneous and accurate monitoring of all critical UMTS, GPRS, GSM and SS#7 interfaces. Facilitates fast fault detection and analysis of network performance with real-time statistics, call or session trace and estimation of QoS parameters.

Highlights

- Troubleshooting and interworking problem resolution
- Promotes efficient UMTS network trials, deployment and optimization
- In-depth 3G protocol analysis with user defined filters and statistics
- Accurate monitoring of multiple interfaces in real-time

Applications

- Troubleshooting of telecom networks equipments in labs
- Resolution of interworking problems during validation and integration phases, trials and network deployment
- Signaling load testing with versatile statistics
- Support for operation and maintenance with proprietary decodes

PC Requirements

- Notebook or PC with Pentium II 450 MHz or higher
- 128 MB RAM
- 500 MB available hard disk space

http://www.acterna.com/united_kingdom/products/descriptions/8630/8630-3G/index.html#feature