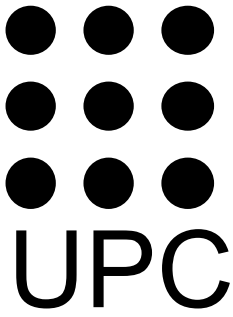


ESCOLA TÈCNICA SUPERIOR D'ENGINYERIA

DE TELECOMUNICACIÓ DE BARCELONA

Contribución a la evaluación de parámetros de diseño en la función de handover para un sistema de comunicaciones móviles avanzado. Propuesta de gestión de claves.

TESIS DOCTORAL

Tesis doctoral presentada en la Universitat Politècnica de Catalunya para la obtención del título de Doctor Ingeniero de Telecomunicación

Autor: **Antonio Barba Martí**

Director: **José Luis Melús Moreno**

Tribunal nomenat pel l'Il.lm Senyor Rector de la Universitat Politècnica de Catalunya, el dia de de 1996

President Dr.

Vocal Dr.

Vocal Dr.

Vocal Dr.

Secretari Dr.

Realitzat l'acte de defensa i lectura de la Tesi Doctoral el dia de de 1996

Qualificació:

EL PRESIDENT ELS VOCALS

EL SECRETARI

Agradecimientos

Este trabajo no se podría haber realizado sin la ayuda de los medios del departamento y la colaboración de muchas personas.

Quisiera expresar mi agradecimiento especialmente a Jose Luis Melús por ser mi director de tesis y a otros profesores que me han acompañado durante todo este tiempo, a Sebastià Sallent, Vicente Casares, Josep Paradells y a Emilio Sanvicente por su apoyo en el departamento.

Deseo agradecer también a mi familia el soporte moral prestado y recordar a los que faltan, que nunca olvidaré.

Deseo agradecer también el apoyo del resto de compañeros del departamento a través de su amistad, a mis amigos de La Pineda, Tarragona, Salou, Barcelona, San Cugat del Vallés, y los de más lejos, Madrid, y del extranjero.

Finalmente, quisiera agradecer la presencia de todos los miembros del tribunal de tesis.

Resumen

Las nuevas tendencias globalizadoras de la economia y la apertura a nivel internacional de numerosos países en el mundo con la formación de grandes bloques, como por ejemplo, la Unión Europea han propiciado la aparición de una nueva generación de sistemas de comunicación móvil que integra los operadores de diferentes países y que permite el uso de satélites para una mayor cobertura mundial. Este tipo de comunicaciones, basadas en sistemas móviles de tercera generación permitirán en el futuro dar soporte a abonados para realizar cualquier tipo de comunicación sin restricciones en el área de servicio, la forma, ni instante de tiempo elegido. Estos sistemas, se denominan Universal Mobile Telecommunication System (UMTS) y Future Public Land Mobile Telecommunication System (FPLMTS) y tienen prevista su entrada en funcionamiento a partir del año 2000.

En este tipo de entornos se plantea el estudio del handover como uno de los procedimientos de movilidad con requerimientos de prestaciones más fuertes. Se especifica sobre diversas clases de celdas (macroceldas, microceldas y picoceldas) y sobre diferentes tipos de dominios de gestión y seguridad en los que está estructurado el sistema UMTS.

Como consecuencia del análisis de requerimientos de esta nueva red, se propone una gestión inteligente del handover. Para ello, y en base a determinados parámetros de la red y a mediciones realizadas en el radioenlace, se evalua un algoritmo de selección de la celda más óptima. Entre los parámetros y mediciones considerados directamente relacionados con la gestión de tráfico en la red, se encuentran la probabilidad de bloqueo en el handover y en el establecimiento de una llamada. Entre las mediciones realizadas a partir del radioenlace a tener en cuenta por el terminal móvil, se encuentra el nivel de señal, calidad en la transmisión (por efecto de atenuaciones, desvanecimientos, etc).

Otros parámetros a considerar se refieren a la movilidad del terminal móvil (tales como velocidad, distancia del terminal móvil a cada una de las estaciones base, tiempo de duración de la llamada, etc). Éstos estarán relacionados con el período de obtención de las muestras y/o parámetros, necesarios para la evaluación del algoritmo propuesto.

El algoritmo de handover descrito se aplica a un escenario formado con clusters de microceldas integrados en celdas mayores denominadas macroceldas paraguas. Se utilizan canales prioritarios en las microceldas, con asignación de buffers para procesar determinado tipo de peticiones cuando exista un elevado índice de congestión. Además se utilizan las celdas paraguas para procesar el tráfico de desbordamiento de las microceldas.

Como resultado, se plantea una función que permite determinar óptimamente una serie de celdas candidatas en la fase de decisión de entre las celdas monitorizadas por el terminal móvil a las que puede invocarse un handover. Se plantea la función para diversos escenarios de redes posibles constatando un resultado óptimo tanto para las prestaciones en la ejecución del handover como para su integración en la gestión del sistema. Adicionalmente, y a modo de aplicación, se estudia el handover desde un punto de vista de las implicaciones en seguridad que plantea.

Ya desde los años ochenta, las comunicaciones móviles analógicas tuvieron aplicación en entornos donde se transmitia información sensible (p.e. policia, gobierno, militares...) sin embargo, la red no proporcionaba medidas especiales de seguridad para proteger la información. Hubo que esperar a la entrada de los sistemas digitales de segunda generación a finales de los años ochenta (p.e. GSM ó DECT) para que se adoptaran servicios de protección a la información del usuario.

Dada la gran cobertura de estas redes, se requiere de una adecuada arquitectura de seguridad para proteger la información tanto de los usuarios como del mismo sistema. El aspecto más característico y principal foco de amenazas en este tipo de redes es el radioenlace, por ser un medio abierto a cualquier intruso. De los procedimientos de movilidad que afectan al radioenlace, el handover es el que más requerimientos de prestaciones y dificultades plantea para la adecuada provisión de servicios de seguridad al usuario. En general, se exigen retardos muy pequeños para afectar lo menos posible la comunicación entre la estación base y el terminal móvil.

Se plantean diversos servicios de seguridad como confidencialidad e integridad de la señalización o de la información de usuario, o bien autentificación y control de acceso en el cambio de dominios con la consiguiente gestión de claves para su integración en el handover. Por tanto, se pueden plantear handovers con distintos grados de seguridad, entre entornos con distintas celdas dentro de una misma entidad de control o bien entre dominios de seguridad y/o entornos administrativos distintos.

Dentro del handover, se hace énfasis en dos fases, decisión y ejecución. Se propone un algoritmo de decisión inteligente que integra una gestión de claves (clave pública de la nueva estación base, NBTS) y que permite la confidencialidad e integridad, mediante algoritmos de clave pública, de la información de señalización a partir de ese instante de tiempo.

En la tesis, se parte del trabajo que se ha realizado previamente dentro de proyectos europeos como MONET y ATDMA del RACE. Se ha trabajado en los requerimientos que debía

satisfacer UMTS, se han especificado una serie de amenazas al sistema y se han planteado unos servicios que lo protegen de los riesgos detectados en seguridad.

El estudio de los mecanismos disponibles para la puesta en funcionamiento de los servicios de seguridad propició el desarrollo de una arquitectura de seguridad basada en el uso de algoritmos de clave pública y de certificados, inspirada en la recomendación X.509. La propuesta surge debido a la similitud de funcionamiento y distribución de las bases de datos en la red fija UMTS y la especificada por X.500. Después de un pormenorizado análisis de funciones y protocolos, se propone el uso de los certificados y algoritmos de clave pública para la protección de la señalización en la red de acceso a UMTS. Para su validación, se analiza el procedimiento más representativo y más crítico en cuanto a prestaciones, el handover.

En la fase de ejecución, se distribuye la clave pública del terminal, así como las claves secretas para la confidencialidad e integridad de información de usuario (uso de algoritmo de clave secreta). En el caso de cambios de dominios de seguridad y/o red, la política de seguridad del operador de red decide sobre la necesidad de invocación de autentificación y control de acceso.

Como resultado, se han planteado protocolos de ejecución en el handover, se han configurado unos modelos y hecho simulaciones donde se han evaluado los diferentes tipos de protocolos sobre redes avanzadas de comunicaciones móviles en entornos de macroceldas y microceldas. Dada una arquitectura UMTS con unos determinados requerimientos de prestaciones en el handover, se ha analizado una variante de protocolo de ejecución de handover con la gestión de claves adecuada para proporcionar los servicios de confidencialidad e integridad de información de usuario así como las necesidades de autentificación según el cambio de entidades y entornos efectuado. Se analizan prestaciones relacionadas con el retardo (debido a diversas causas: tráfico, bit-rate del radioenlace, velocidad de procesado en el cifrado (descifrado), longitud de paquetes, etc) de los protocolos mediante programas constatando que se cumplen los requerimientos especificados por el sistema UMTS. Se observa, sin embargo, que la mayor dificultad estriba en los handover entre picoceldas, por ser entornos de reducidas dimensiones y con mayor densidad de usuarios llamantes. Por tanto, se constata la necesidad de diseñar una arquitectura con enlaces mucho más rápidos entre estaciones base para soportar las grandes cantidades de información de señalización con los retardos especificados para picoceldas.

Después de un detallado estudio comparativo sobre una arquitectura de bases de datos distribuida, se ha escogido una arquitectura de seguridad basada en X.509. Se utilizan certificados para la gestión de claves y el uso de algoritmos criptográficos de clave pública

(como RSA) para confidencialidad e integridad de la información de señalización. La confidencialidad e integridad de la información de usuario se realiza con algoritmos de flujo de clave secreta dado el elevado bit - rate (< 2 Mbps) especificado en UMTS.

Los programas se han realizado tomando como base el uso del algoritmo RSA con la posibilidad de trabajar a 64 Kbps. Se han estudiado diferentes velocidades de cifrado así como la posibilidad de uso de otros tipos de firmas digitales. Se observa que uno de los principales inconvenientes del uso de certificados en la gestión de claves en el handover es la longitud de éstos. Dado que el bit - rate sobre el radioenlace es limitado, el retardo en el envío de estos certificados puede llegar a ser excesivo para los requerimientos de calidad de servicio exigidos. Por ello se ha empezado a plantear el uso de curvas elípticas para la realización de las firmas digitales en los certificados por requerir claves con menos bits si bien esta evolución no se contempla en la presente tesis.

Introducción. Objetivo de la tesis

I. Ámbito de la tesis

El marco de la presente tesis es el de un sistema de comunicaciones móviles avanzado como puede ser UMTS. Dentro de este sistema, se estudia el procedimiento de movilidad más crítico en cuanto a prestaciones, el handover. En éste, se determinan los parámetros de diseño que permitan caracterizar adecuadamente la selección de celdas candidatas previa a la ejecución del handover. Se definen los protocolos que rigen el handover y se analizan todo tipo de prestaciones.

La tesis también se enmarca dentro de los esfuerzos realizados por parte del programa RACE en el ámbito de los sistemas móviles más avanzados. Concretamente, trata de dar respuesta al tema de seguridad, mediante una arquitectura de seguridad híbrida, basada en algoritmos de clave pública para la protección de la señalización y en algoritmos de clave secreta para la protección de la información de usuario. Es de destacar que es la primera vez que se propone en un sistema móvil celular concreto algoritmos de este tipo.

Dentro de este marco de trabajo, se plantea una gestión de claves para el caso del handover, como uno de los procedimientos de movilidad más críticos en cuanto a prestaciones que deberán soportar los futuros sistemas de comunicación móviles. Junto al handover, se estudia la gestión de recursos que hay integrada en éste y su compatibilidad con la arquitectura de seguridad propuesta.

II. Declaración de objetivos

Los objetivos de esta tesis pueden definirse de la siguiente forma:

- Definir unos parámetros válidos para especificar la selección de celdas en el handover.

- Plantear la integración del algoritmo de selección de celdas en las fases de decisión y ejecución del handover en un entorno de red móvil inteligente.

- Dada una red móvil avanzada, se propone una arquitectura de seguridad hibrida que permita cumplir con las especificaciones propuestas (p.e. en UMTS) sobre seguridad.

- Aplicar y validar esta arquitectura de seguridad basada en el uso de algoritmos de clave pública, el soporte de certificados en los canales de señalización y en el uso de algoritmos de

clave secreta para protección de la información de usuario mediante el diseño de un "forward handover" que sea seguro.

- Para que el impacto de los servicios de seguridad planteados en el handover sobre las prestaciones del sistema sea poco importante, se especifica una gestión de claves que permite cumplir con las especificaciones de calidad de servicio definidas en redes como UMTS.

III. Estructura de la tesis

La estructura de la tesis está formada por una serie de cinco capitulos, conclusiones y anexos. En el capítulo 1 se describe el funcionamiento de la red UMTS, la distribución de bases de datos, su semejanza con X.500, la inteligencia de la red y el entorno de procedimientos de movilidad entre los que se incluye el handover.

En el capitulo dos, se describe el handover con los diferentes tipos y criterios que se siguen para invocar un handover. Se hace un análisis de los parámetros de diseño que constituyen la base del algoritmo de selección de celdas haciendo especial énfasis en el tratamiento de los niveles de tráfico.

En el capitulo tres, se estudia más especificamente el control de las entidades funcionales que permitirán definir un protocolo de decisión de celdas candidatas en el handover. La discusión de diversos tipos de escenarios con los parámetros y mediciones obtenidos de la red. También se analiza la fase de ejecución dentro de la gestión inteligente del sistema.

En el capitulo cuatro se analizan los aspectos de seguridad a tener en cuenta en el handover, la gestión de claves, opciones en los procedimientos para los servicios de seguridad y su integración en el handover. En este capitulo además, se analiza la arquitectura de seguridad en UMTS detallando especialmente la red fija y los requerimientos, amenazas, servicios definidos y mecanismos de seguridad posibles en el handover. Se propone la recomendación X.509 como base para la arquitectura de seguridad del sistema y la realización de una gestión de clave pública mediante certificados para la protección de la señalización.

En el capitulo cinco se estudian las fases de ejecución para los diversos casos de handover y los diferentes tipos de celdas. Se analiza la problemática de aplicar los servicios de seguridad al handover, se ven las distintas opciones, características y requerimientos. Se integra una gestión de claves en los tipos de protocolos de handover, entre macroceldas. Se analizan los tipos de protocolos forward/backward de handover para cada posible cambio de entorno/dominio. Se analizan los resultados según diferentes condiciones de tráfico de las estaciones base, nodos de la red, longitudes de las tramas de los protocolos, tramas de

seguridad, retardos de procesamiento, etc. Se comparan las prestaciones de los tipos de protocolos, se observa el impacto de la seguridad en las prestaciones. Se constata el cumplimiento de los requerimientos en prestaciones especificados.

Finalmente, se introduce un capitulo de conclusiones y se añaden unos anexos para complementar con más detalles el contenido de la memoria.

IV. Artículos Publicados

[AB1] A. Barba, E. Cruselles, J. L. Melús. *The CPNs in UMTS. Security aspects.* Fourth WINLAB Workshop on Third Generation Wireless Information Networks. p. 317-328. New Jersey, 1993.

[AB2] A. Barba, J. L. Melús. *Security architecture in the UMTS network.* Second IEEE Network Management and Control Workshop, p. 55-66, New York, 1993.

[AB3] A. Barba, F. Recacha, J. L. Melús. *Security architecture in the UMTS network. A comparison with the FPLMTS network.* International II Conference on Universal Personal Communications, p. 854-860, Ottawa, 1993.

[AB4] A. Barba, F. Recacha, J. L. Melús. *Security architecture in the third generation networks.* SICON/ICIE '93. p. 421-425, Singapur, 1993.

[AB5] A. Barba y J. L. Melús. *Directory services for UMTS. Security aspects.* 44th VTC Vehicular Technology Conference. p. 1606-1610. Estocolmo, 1994.

[AB6] E. Cruselles, F. Recacha, A. Barba, J. L. Melús. *Seguridad en comunicaciones móviles. Mecanismos y servicios.* Mundo Electrónico, p. 22-31. Abril 1994.

[AB7] F. Recacha, A. Barba, E. Cruselles y J. L. Melús. *Comunicaciones móviles. Seguridad en redes GSM.* Mundo Electrónico, p. 42-51. Octubre 1994.

[AB8] J. L. Melús, A. Barba, F. Recacha y E. Cruselles. *Seguridad en comunicaciones móviles. El estándar DECT.* Mundo Electrónico, p. 58-63, Jun-Julio 1995

[AB9] A. Barba, J. L. Melús, F. Recacha y E. Cruselles. *Comunicaciones móviles. Seguridad en sistemas de 3ª generación UMTS.* Mundo Electrónico, p. 62-69, Septiembre 1995

[AB10] A. Barba y J. L. Melús. *Cell management in the handover.* International Conference on Personal Wireless Communications (ICPWC´95), Sidney (Canada), Junio 1995.

[AB11] A. Barba y J. L. Melús. *Decision phase of a forward handover in an intelligent mobile network.* Wireless ´95, p. 489-499, Calgary, Julio 1995.

[AB12] A. Barba y J. L. Melús. *Traffic evaluation in the decision phase of a handover.* Fourth IEEE International Conference on Universal Communications (ICUPC´95) p. 354-358. Tokyo, Noviembre 1995.

[AB13] A. Barba y J. L. Melús. *Gestión de claves en un handover avanzado según una arquitectura de seguridad UMTS.* III Reunión española sobre Criptología, Barcelona, Nov. 1994.

[AB14] A. Barba y J. L. Melús. *The key management mechanism in the handover. performances related to an advanced mobile network*. IEEE SICON/ICIE´95 p. 411-415. Singapur, Julio 1995.
[AB15] A. Barba y J. L. Melús. *Key management in the handover. Application to third generation mobile systems*. Personal, Indoor and mobile radio communications (PIMRC´95) p. 300-305. Toronto, Septiembre 1995.
[AB16] A. Barba, J. M. Pulido, J. L. Melús. *Diseño de protocolos de gestión de movilidad entre redes privadas y UMTS*. IX Symposium nacional de la URSI. p. 1184 - 1189. Las Palmas de Gran Canaria, Septiembre 1994.
[RACE2] RACE 2066/ASCOM/MF3/DS/P/04/b1 Scenarios of threats for the UMTS network (draft). 1992.
[RACE3] RACE 2066/ASCOM/MF3/DS/P/010/b1, Specification of security services and service levels (draft). 1992.
[RACE4] RACE 2066/ASCOM/MF3/DS/P/011/b1, Allocation of security services to network components (draft). 1992.
[RACE5] RACE 2066/ASCOM/MF3/DS/P/046/b1, Specification of security services and service levels (final). 1993.
[RACE6] RACE 2066/ASCOM/MF3/DS/P/047/b1, Scenarios of threats for the UMTS network (final). 1993.

V. Siglario

AC: Authentication Center o CAU
BCPN: Business Customer Premises Network
BISDN: Broadband Integrated Services Digital Network
BS: Base Station
BTS: Base Transceiver Station
CAU: Centro de Autentificación
CPN: Customer Premises Network
CSS: Cell Site Switch
DAP: Directory Access Protocol
DCPN: Domestic Customer Premises Network
DDB: Distributed Databases
DECT: Digital European Cordless Telephone
DSP: Directory System Protocol
ETSI: European Telecommunications Standards Institute
FPLMTS: Future Public Land Mobile Telecommunication System
GSM: Global System for Mobile Communication
LE: Local Exchange
MCPN: Mobile Customer Premises Network
MS: Mobile Station
MT: Mobile Terminal
PCN: Personal Communication Network
PCS: Personal Communication Services
PDC: Personal Digital Cellular
SC: Security Center
SID: Subscription Identity Device
RACE: Research Advanced Communications in Europe
TIA: Telecommunications Industry Association
TX: Transit Exchange
UIT: Union Internacional de Telecomunicaciones
UMTS: Universal Mobile Telecommunication System
UPT: Universal Personal Telecommunications
USDC: U. S. Digital Cellular
WARC: World Administrative Radio Conference

VI. Notación

Xp: Clave pública del terminal móvil
Xs: Clave privada del terminal móvil
Xc: Clave secreta para confidencialidad de la información de usuario
Xi: Clave secreta para integridad de la información de usuario
Xp[I]: I cifrada por Xp
Xs[I]: I cifrada por Xs
CAp: Clave pública de la Autoridad de Certificación
CAs: Clave privada de la Autoridad de Certificación
OBTSp: Clave pública de la estación base anterior
OBTSs: Clave privada de la estación base anterior
NBTSp: Clave pública de la nueva estación base
NBTSs: Clave privada de la nueva estación base
CAH: Autoridad de Certificación de la cual el terminal móvil está abonado
CCA: Autoridad de Certificación común entre CAH y NCAV
OCAV: Autoridad de Certificación del anterior dominio visitado por el terminal móvil
NCAV: Autoridad de Certificación del nuevo dominio visitado por el terminal móvil

X{I}: Firma digital de I por el usuario X (con el uso de una función Hash)
CA(X): Autoridad de Certificación de X
Fir (a; b): Mensaje resultante (b, a{b}) siendo a{b} la firma digital de b con la clave procedente de a.
X1<<X2>>: Certificado de usuario X2 enviado por la autoridad de certificación X1
Certificado: Fir (CAs; Contenido del certificado)
A -> B: Camino de certificación formado por una cadena de certificados de A a B.

Entidades funcionales:
LC: Controlador de enlaces
RA: Asignación de recursos
RC: Control de enrutado
ME: Evaluación de mediciones
HDC: Control de decisiones del handover
HE: Ejecución del handover
HT: Terminación del handover
HCA: Ajuste de criterios del handover
TC: Controlador de tráfico

Prefijos:

N relativo a componentes de la red fija

M relativo a terminal móvil

BTSn para el número de estación base (n).

VII. Indice

Capitulo 1

Características del sistema móvil celular UMTS

1.1 Introducción

Los recientes avances tecnológicos están permitiendo cada vez más un flujo interrelacionado de personas a escala mundial. En esta nueva era de globalización económica cada vez se hace más necesario el soporte de una red de comunicaciones móviles de cobertura mundial.

El sistema UMTS/FPLMTS surge como un intento de cubrir estas necesidades de comunicación. Para ello, se requiere de una nueva arquitectura de red inteligente que se integre en el sistema definido y que posibilite la gestión correcta de la información transmitida así como de los nodos del sistema [VO1].

En este capitulo se introduce al lector en los sistemas de comunicación móviles. Primero se describe brévemente la evolución de la telefonía móvil hasta nuestros dias y posteriormente se especifican los elementos principales, que formarán los sistemas futuros, tales como UMTS o FPLMTS. Se define la arquitectura de red en UMTS, tanto en la red de acceso como en la estructura de directorios de la red fija. Se plantea además, la necesidad de implementar terminales móviles inteligentes dentro de una red de gestión inteligente.

Una vez se ha definido préviamente el entorno en el cual se va a operar, se desarrolla con más detalle la estructura de bases de datos distribuida del sistema dejando para más adelante su impacto en un procedimiento de movilidad tal como el handover.

Finalmente, se especifican los procedimientos de sesión, establecimiento de llamada y los distintos procedimientos de movilidad que enmarcan al handover y a su seguridad y que se van a detallar en los capitulos posteriores.

1.2 Sistemas actuales de comunicaciones móviles

Dentro de los sistemas actuales de telefonía móvil se puede considerar una primera generación de sistemas analógicos (AMPS, NMT, TACS,...) que apareció en los años 80, y que en la actualidad ya están completamente saturados y superados tecnológicamente. Estos sistemas carecian de servicios de seguridad para la protección de información del usuario.

Los avances en tecnología digital permitieron una mejora de prestaciones que se concretó en la definición de mecanismos y servicios proporcionando un soporte de seguridad al sistema. Se trata de las redes actuales de segunda generación (década de 1990) basadas en sistemas digitales (GSM, DECT, CT2, TIA, Bell,...) que tratan de superar las graves deficiencias de los sistemas anteriores [RS2, DG1-2].

Dentro de las ventajas que incorporan estos nuevos sistemas, puede destacarse en general una mejora en la calidad y prestaciones de los servicios soportados. Ello se debe en gran medida a la tecnologia digital, que permite mucha mayor flexibilidad en el funcionamiento, disponiendo de diversos canales de señalización separados y la posibilidad de operar entre diversos entornos y países.

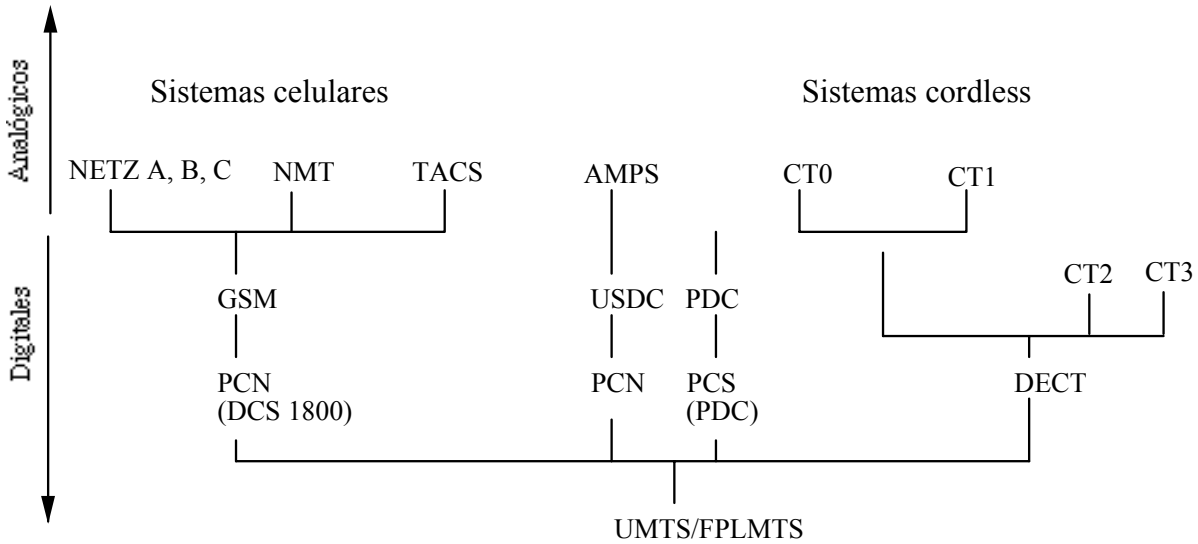


Fig. 1.1. Esquema donde se muestra la evolución de los sistemas de comunicaciones móviles desde sus orígenes hasta nuestros dias.

Simultáneamente, en 1989, el Reino Unido permitió el desarrollo de la Personal Communication Network (PCN), basada en estándares de ETSI GSM. La nueva recomendación DCS 1800 aprobada en 1991 para Europa es un sistema celular digital a 1800 Mhz incorporando una serie de servicios de telefonía personal [WG1].

La evolución de estos sistemas PCN junto con su interconexión/integración con redes preexistentes es un paso intermedio hacia el concepto de sistemas de la tercera generación. La tercera generación (UMTS/FPLMTS) [RACE1, HB1] surge a partir de servicios celulares incorporando diferentes estándares, sistemas telefónicos sin hilos, DECT, incluyendo su interconexión con GSM [MM1, LH1] y sistemas de satélites con cobertura mundial [SH1].

1.3 Descripción de los sistemas de telefonía móvil de la tercera generación

La red UMTS, tal como esta definida, permitirá dar soporte a los abonados para realizar cualquier tipo de comunicacion sin restricciones en el area de servicio, en la forma, ni en el instante de tiempo elegido. El sistema tendrá que ser capaz de poder transportar muchos tipos de información diferente y servir en muchos entornos de población diferentes. Entre ellos se pueden destacar, el entorno urbano con alta densidad de tráfico, entornos rurales dispersos, interiores de edificios y vehiculos que pueden estar moviéndose a gran velocidad (p.e. coches, trenes,...).

Dado que UMTS dará acceso a servicios de información avanzados a una mayor población (millones de abonados) que los sistemas anteriores y a multitud de entornos, requerirá que la tecnología de los sistemas terminales así como de la red sea notablemente mejorada.

El sistema estará totalmente integrado por operadores de red de los diversos países proporcionando cobertura mundial y con tasas de velocidad de hasta 2 Mbps proporcionado gran capacidad y calidad a los más variados servicios. Las bandas de frecuencia asignada para FPLMTS por WARC es de 230 Mhz de espectro no contiguo entre 1885 y 2200 Ghz [SH1].

Requerimientos de los sistemas de comunicación móvil de tercera generación
Dentro de los principales objetivos de diseño sobre los cuales se está definiendo UMTS, está la iniciativa de que llegue a ser parte integral del sistema de red digital de servicios integrados de banda ancha (BISDN) [MH1]. Colateralmente pueden distinguirse otros requerimientos importantes tales como los siguientes [RACE21]:

- Una distinción funcional entre provisión de servicios y provisión de red en UMTS.

- Los interfaces internos del sistema UMTS serán estandarizados para permitir implementaciones de múltiples fabricantes.
- UMTS será un sistema con un mínimo de funciones integradas pero capaz de soportar el mayor número de aplicaciones.
- UMTS habrá de ser modular, flexible en su capacidad y con fácil introducción de avances tecnológicos.
- UMTS tendrá que permitir integrar telefonía celular, cordless, paging (búsqueda) y servicios de datos en una única infraestructura, y también tendrá que ser capaz de soportar aplicaciones como sistemas de bucle de abonado local sin cables.
- El sistema de telefonía básico deberá de funcionar con un coste efectivo mínimo siendo los otros servicios más avanzados fácilmente implementables sin mayor complejidad ni coste para la red.
- El nivel de seguridad de la parte de red móvil ha de ser tan elevado como la parte de red fija.

Este último requerimiento, como se verá más adelante, comporta importantes efectos en el funcionamiento del sistema.

1.4 Arquitectura de la red UMTS

El entorno donde van a integrarse los servicios para el usuario, a través de operadores de red y de servicio es en la red UMTS. Esta red, está compuesta por una red de acceso y una red fija, cada una de ellas conteniendo sus propias bases de datos. La red de acceso comprende diversas entidades que proporcionarán funcionalidades que soportarán la cobertura de los radioenlaces. Es decir, ejerceran funciones de soporte en los interfaces de radio, en la gestión de sus recursos y en el mantenimiento y operación del handover.

La red fija UMTS comprenderá entidades que proporcionarán funcionalidades para soportar gestión de movilidad, operaciones con bases de datos e interconexión con otras redes. Todos los interfaces con la parte fija de la red estan previamente establecidos y no existe distinción entre entidades de la red fija UMTS y entidades de otras arquitecturas (p.e. B-ISDN, UPT). Estas podrían ser (parcialmente) coincidentes o (totalmente) distintas, dependerá de su nivel de integración. En la fig. 1.2 se representa la arquitectura de la red UMTS. A continuación, se describen brevemente los diferentes componentes que forman la red UMTS [RACE24-25]:

- Estación base (Base Transceiver Station, BTS):
La estación base proporciona la gestión del radioenlace, representando la funcionalidad necesaria para el establecimiento, mantenimiento y liberación del radioenlace .

- Centro de conmutación de celda (Cell Site Switch, CSS):
La CSS representa la funcionalidad de conmutación básica en la red de acceso. En las BCPNs podría representar una PBX fija, o bien una NT2 dentro de un entorno ISDN.

- Central de interconexión local (Local Exchange, LE) e Interconexión de tránsito (Transit Exchange, TX):
Estos grupos representan la red fija existente, es decir, la infraestructura de conmutación sobre la cual se soportarán los servicios y procedimientos UMTS.

- Punto de control del servicio y movilidad (Mobility and Service Control Point, MSCP):
Esta entidad comprende la funcionalidad necesaria para el control de los procedimientos de movilidad y operación de servicios en una cierta área; puede acceder, modificar y borrar información en la MSDP. Las MSCPs estarían asociadas con la red fija (MSCP(LE/TX)) y con la red de acceso (MSCP(Publica/Privada)).

En la red de acceso la MSCP(P/B) se separa de la CSS(P/B) por tener diferente funcionalidad los entornos públicos (P) de los de negocios privados (Business, B). Además, la MSCP está preparada para soportar servicios y control de servicios de la red inteligente.

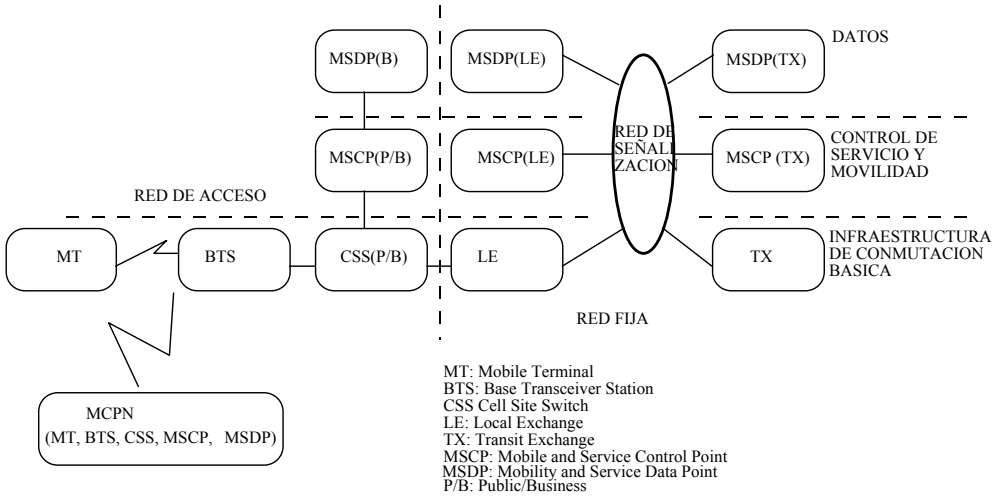


Fig. 1.2. Arquitectura de red UMTS.

- Punto de datos de servicio y movilidad (Mobility and Service Data Point, MSDP):
El MSDP puede identificarse como una entidad que forma la base de datos distribuida UMTS (DDB). Esta entidad almacena información concerniente a datos del terminal, perfil de abonado y de servicio, datos de red, datos de localización, etc. Contiene también la funcionalidad de los datos que comprende el control y comunicación en las DDB.

- Terminal móvil (Mobile Terminal, MT):

El MT comprende las funciones ubicadas en la parte del radioenlace correspondiente al terminal móvil. El MT será un "terminal multimodo inteligente" con subsistemas programables. Éstos permitirán seleccionar el tipo de control de frecuencias, entrelazado a ser usado por el canal, codificador, método de acceso múltiple, tipo de modulación, control de ráfaga, secuencia de 'spreading', frecuencias portadoras etc. La generación de las claves de cifrado para confidencialidad e integridad sería realizada por una tarjeta inteligente (Subscriber Identity Device, SID).

1.5 Dominios en redes privadas (Customer Premises Networks, CPNs)

Los dominios son áreas administrativas bajo la supervisión de un operador UMTS (o CPN). Cada operador de red puede dar cabida a varios proveedores de servicio con distintos dominios. El área de cobertura de estos servicios viene dada por el acceso a una base de datos o a un conjunto de bases de datos interconectadas (DDBs) dentro de una red privada o determinado dominio.

Las CPN o redes privadas pueden verse externamente como subredes UMTS [AB1]. Existen CPNs según los diversos entornos posibles en UMTS: domestico, de oficinas o empresas o bien móviles. A diferencia de GSM u otros sistemas anteriores, en UMTS está permitido el realizar handovers entre redes distintas, eso comporta la adopción de servicios de seguridad tales como autentificaciones, controles de acceso, cambio de claves, etc,... que dependerán en última instancia de la politica de seguridad del sistema.

Se pueden clasificar las CPNs según diversos criterios, como por ejemplo, según el interface entre la CPN y la red adyacente UMTS (pública). Este interface determina las funciones que son soportadas por la CPN en si misma y las funciones que realiza la red publica. De esta forma, se pueden distinguir los siguientes tipos:

- CPN simple con acceso transparente
- CPN compleja con acceso UNI usuario - red (User - Network Interface, UNI)
- CPN con acceso UNI mejorado para MCPN (CPN móviles)

CPN simple con acceso transparente

Este tipo de CPN contiene simplemente un receptor radio y un transmisor de radio de corto alcance y actua como un relevador entre un usuario UMTS con su área de cobertura y la red UMTS adyacente. La CPN simple es análoga a una estación base de telefonía cordless, diferenciándose de esta en que proporciona acceso a un móvil, no a una red fija.

CPN compleja con acceso UNI

Las CPN tienen un interfaz con la red fija UMTS adyacente del tipo usuario - red (UNI) idéntico al que existe entre un terminal móvil normal y la red UMTS. Puede ocurrir que la CPN únicamente implemente el control de servicios portadores o que disponga también de la capacidad de gestionar llamadas internamente como por ejemplo, las PABX.

CPN con acceso UNI mejorado para MCPN
Este tipo de CPN permite el establecimiento de llamada, localización, búsqueda, handover y transferencia de perfil de información. La funcionalidad de control de movilidad en la CPN podría ser diferente de la proporcionada por la red pública. La CPN podría ser un móvil tal como un tren, barco o avión [NS1].

1.6 Tipos de peticiones y distribución de información en las bases de datos

En este apartado a modo de introducción, se describen brévemente los mecanismos sobre los cuales funciona el intercambio de información entre las bases de datos de la red fija y el terminal móvil del usuario.

Durante el funcionamiento normal de la red, el usuario con el terminal móvil va desplazándose sobre las distintas celdas en las que tiene cobertura el sistema. En la ejecución de los procedimientos de movilidad, ciertos datos son transferidos, o bien obtenidos, modificados o renovados entre las bases de datos (DDB) del resto de la red. Cuando se considera el modelo funcional UMTS, puede entenderse el servicio de DDBs como proporcionado por las entidades funcionales SDF (que representan la base de datos) en respuesta a peticiones desde las entidades funcionales SCF (que representan los elementos de control de la red).

Los servicios DDB son descritos mediante cuestiones DDB (queries), esto es, peticiones que permiten la interrogación y modificación de datos DDB. Varias cuestiones DDB se realizan durante el establecimiento de llamada, registro, renovación de registro (location updating) y otros procedimientos de movilidad.

Se asume que los datos son almacenados en la DDB en forma de entradas (entries o records) de información relacionada. Las entradas consisten de varios campos o atributos (fields o attributes). Cada atributo está caracterizado por su tipo (type) y su valor(es) (value(s)). Las cuestiones DDB actuan sobre la creación y borrado de información (entradas) tanto como la obtención y la modificación de atributos.

Las peticiones DDB pueden ser de dos tipos, las modificaciones DDB que crean, borran, etc entradas DDB y las interrogaciones DDB que leen, renovan, etc valores de atributos de entradas de DDB seleccionadas.

Los datos son estructurados en dominios bajo áreas administrativas con la supervisión de un operador UMTS. Estos dominios pueden clasificarse a su vez formando distintos niveles aplicando distintas politicas de seguridad. Los proveedores de servicio son la autoridad que tiene la completa responsabilidad para la provisión de un servicio o un conjunto de servicios a los usuarios finales. Como se verá, eso puede afectar a las disciplinas de control de acceso a determinados servicios. Los proveedores de servicios a su vez, pueden dividirse en dos categorias, los públicos y los privados, comportando politicas de seguridad no siempre coincidentes.

El área de cobertura de un servicio es un área donde un proveedor de servicio dado es responsable de la provisión de uno o más servicios. Para realizar esa tarea, un proveedor de servicio tiene acceso a una base de datos o a un conjunto de bases de datos interconectadas (DDBs). Es importante hacer una distinción entre las distintas clase de datos, los datos usables directamente, que pueden ser procesados para responder a una petición de base de datos y los punteros que dan indicaciones de la posición de los datos usables perdidos en los dominios DDB y necesarios para soportar la provisión de un servicio.

En el caso del establecimiento de una llamada, los datos concernientes a los grupos llamantes y llamado son intercambiados entre proveedores de servicio formando parte de distintos dominios. Se define el dominio UMTS visitado como aquel dominio en el que el terminal móvil (usuario) se está moviendo. En contraposición al dominio UMTS de abonado (home) en el cual el terminal móvil (usuario) tiene una suscripción válida. Durante la ejecución de los procedimientos de movilidad ciertos datos podrían ser transferidos (o modificados, obtenidos, etc) entre diferentes dominios UMTS. Se llama dominio UMTS originante a aquel dominio en el cual se genera una cuestión. Notar que el dominio UMTS originante podría ser idéntico al dominio de abonado o visitado.

Existen básicamente dos técnicas para la difusión de información almacenada en la red: la fragmentación y la réplica de datos. En la réplica de datos, el conjunto completo de datos UMTS (estáticos y dinámicos) se mantiene en el dominio de abonado, donde una cuestión siempre se satisface, mientras que un subconjunto de esos datos (p.e. perfil de usuario) podría ser copiado al dominio visitado, posiblemente durante el registro de posición. Este conjunto de datos es siempre un subconjunto de los datos UMTS de abonado.

En la opción de fragmentación de datos, el dominio de abonado retiene parte de los datos UMTS y el dominio UMTS visitado contiene el resto de datos UMTS. El conjunto de datos en los dominios UMTS de abonado y visitado son siempre disjuntos.

En ambos casos, siempre que ocurra un cambio en el dominio visitado, los datos tendrán que ser creados dentro del nuevo dominio visitado y borrados del antiguo dominio visitado para mantener consistente la base de datos distribuida. Como se verá más adelante, esta renovación de información de las bases de datos se integrará en el procedimiento de handover entre dominios y/o redes distintas.

1.7 Protocolos en X.500. Relación con UMTS

En X.500, la información se almacena de forma distribuida, en entidades llamadas Distributed Service Agents (DSAs). El acceso a esa información es a través de Directory User Agents (DUAs). Cada DSA mantiene alguna información. Colectivamente los DSA mantienen toda la información y son conocidos como la Directory Information Base (DIB). En este caso, existe una clara semejanza con la estructura de bases de datos jerárquicamente distribuida de UMTS (Ver anexo 5).

Arbol de información de directorios

El directorio mantiene información acerca de objetos (p.e. redes, gente, organizaciones,...). Esta información se mantiene en las Bases de Información de Directorios (Directory Information Base, DIB) en forma de entradas (entries).

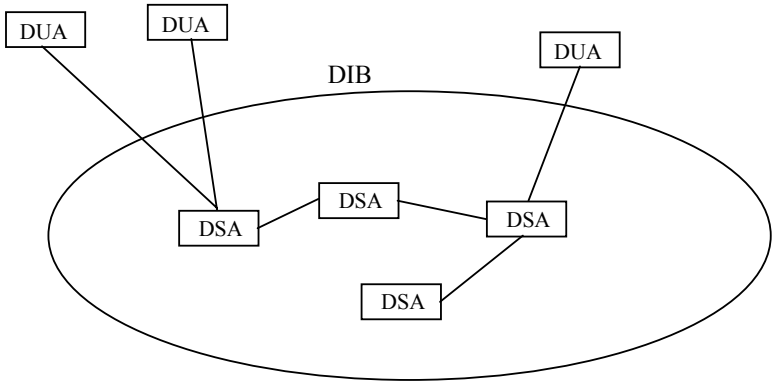


Fig. 1.3 Estructura de bases de datos X.500.

Las entradas se mantienen en una estructura de árbol llamada Arbol de Información de Directorios (Directory Information Tree, DIT). Eso refleja la relación jerárquica entre objetos, que es clave en el diseño de X.500 y UMTS. Las entradas al mismo nivel en el DIT pertenecen a la misma clase de objetos, siendo todas del mismo tipo.

De forma asociada con cada clase de objeto, existen un conjunto de atributos. Un atributo consiste de un tipo atributo junto con uno o más valores de atributos. En UMTS, los perfiles de servicio y usuario son almacenados en las bases de datos ISN de forma similar.

Cada entrada en el directorio se identifica, dentro de su nivel jerárquico, por un nombre denominado Relative Distinguished Name (RDN). Cada RDN es un conjunto de uno o más valores de atributos con los tipos de atributos siendo determinados por la clase de objetos de la entrada. Las entradas dentro del DIT se identifican únicamente por un Distinguished Name (DN). El DN de una entrada es una secuencia de RDNs.

Como el directorio es distribuido, cada DSA tendría algún conocimiento de su lugar en el directorio con relación a sus niveles. Este conocimiento se mantiene en forma de referencias, las cuales se definen de varios tipos; referencias subordinadas y referencias superiores. Las referencias son asociadas con entradas que actuan como punteros a otras entradas no mantenidas en la misma DSA, que son inmediatamente subordinadas a sus entradas asociadas. Un sistema parecido se tiene en GSM con las bases de datos VLR y HLR. De forma similar se mantiene en UMTS una interacción con la información con bases de datos jerárquicamente distribuidas (ISN).

Además de las referencias, un DSA puede almacenar los resultados de peticiones previas. Esto se denomina 'caching' y permite al DSA mantener copias de la información mantenida en otras DSAs. Aspecto este importante desde el punto de vista de gestión de claves en seguridad para la aplicación de la recomendación (X.509). También permite recordar a un DSA los caminos del árbol de directorios tomados en peticiones anteriores, cuya información se almacena en forma de 'Cross references'. Tal como se verá más adelante, esto no resulta incompatible con el sistema UMTS.

Conclusiones

Las conclusiones que se pueden obtener en relación a la red fija especificada en UMTS y en X.500 pueden resumirse de la forma siguiente: En cuanto a las relaciones de acceso, se tiene que el DAP permite soportar las relaciones entre una entidad de acceso MSCP(LE) y la MDSP(LE) requeridas por UMTS.

Respecto a las relaciones DDB internas: Tanto el DSP como el DAP presentan el conjunto de características requerido para soportar las relaciones de DDB internas de UMTS. Es decir,

-Soporte de nombres jerárquicos
- Soporte de operaciones internas elementales
- Se soportan los mecanismos de Chaining, Multicasting y Referral

- Se soportan las técnicas de Restart y Continuous partial response
- El mapeo a una estructura de señalización no es complejo
- Seguridad y control de acceso son ya consideradas
- Ellas no excluyen el agrupamiento de operaciones en una sóla primitiva.

En la parte de desventajas, es decir, requerimientos de DDB UMTS no soportados por X.500 se tiene:

- Soporte de una lista de parámetros reducida.
- Soporte de la técnica Passing
- Soporte para el mecanismo de respuesta parcial 'Partially Continuous'
- Capacidad de soporte de todos los mecanismos de respuestas parciales para agrupación de operaciones.
- Soporte para un mecanismo simple de mantener la consistencia de los datos copiados.
- Soporte para gestión de transacciones básicas, para soporte de movimiento de datos.

Por tanto, para las relaciones entre operaciones internas con las DDB, puede ser viable un protocolo basado en el DSP.

Para las relaciones entre DDB de operadores, puede utilizarse tanto un DAP como un DSP. Sin embargo, el protocolo DAP parece ser más adecuado a causa de las consideraciones en seguridad y su capacidad de esconder el procesamiento local de una petición.

Algunas de las funcionalidades requeridas por los protocolos DSP y DAP para soportar las relaciones DDB UMTS podrían ser facilmente implementadas por el mecanismo de establecimiento de asociaciones (p.e. ACSE/ROSE o TCAP). Éstos podrían proporcionar algunas de las gestiones de transacciones requeridas (usando operaciones enlazadas), y proporcionar los servicios connectionless requeridos por la técnica passing.

Por último, hacer constatar que no resulta complicada la implementación del protocolo DDB UMTS sobre los niveles de señalización basados en SS7.

1.8 Estructura de directorios en la red fija. Bases de datos distribuidas

En la estructura de red fija se dispone de una serie de bases de datos distribuidas formando una estructura jerárquica que permite almacenar tanto la información de perfiles de abonados como de la propia red. Las bases de datos distribuidas están compuestas de nodos de

almacenamiento de información (Information Storage Nodes, ISN), de los cuales pueden identificarse varios tipos [RACE11-12]:

ISN_S: Son nodos que contienen datos UMTS, información de directorios y funciones de control internas DDB. Pueden dividirse en nodos de almacenamiento de datos residentes y nodos de almacenamiento de datos visitados. Ambos tipos no son mutuamente excluyentes y podrían coexistir en la misma ISN_S. No configuran ninguna jerarquía.

ISN_D: Son nodos que contienen información de directorio y funciones de control, pero no datos UMTS. Están organizados jerárquicamente y pueden ser de los tipos siguientes: ISN_{DN} que son nodos que están arriba en la jerarquía y son responsables de las relaciones entre redes e ISN_{Dn} que forman el resto de nodos de manera opcional.

ISN_I: Son los nodos responsables del interfaz con el resto de los sistemas UMTS. Éstos reciben peticiones de las entidades UMTS que están fuera de la bases de datos y las transforman en comandos internos y peticiones, que envian a las ISN_S apropiadas. Estos nodos son también responsables de recoger los resultados y devolverlos a la entidad originante.

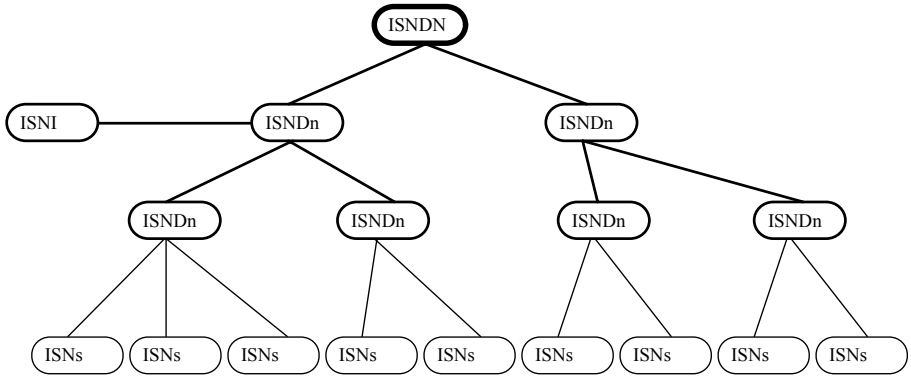


Fig. 1. 4 Estructura jerárquica y distribuida de bases de datos (MSDP) en la red fija UMTS.

X.500 y la estructura de directorios UMTS

En este apartado se estudian las similitudes entre la estructura de la red fija UMTS y la definida por el estándar X.500 de la ITU. X.500 define un conjunto de sistemas de procesamiento de información y una estructura de almacenamiento de información (denominado en conjunto Directorio) que se aprovechan en la definición del sistema UMTS [RACE11-13, ITUT1-11].

Los datos almacenados en las DDB UMTS se identifican con un único identificador UMTS y un identificador de atributos. Estos datos se almacenan en diversos tipos de ISN´s que a continuación se comparan con la estructura de directorios X.500.

Relación ISN_{Dn} a DSA:
Es una función del nodo ISN_{Dn} el mantener operativa la información con identificadores, permitiendo cuestionar para el correcto enrutamiento a los nodos. También mantener referencias entre ISN_{Dn} para formar una estructura jerárquica con las DDB. Las ventajas de un mapeo de este tipo pueden describirse como: La información dentro de los ISN_{Dn} puede ser estructurada jerárquicamente. Por otra parte, a cada ISN_{Dn} le sería posible referenciar a un nodo superior ISN_{Dn} a través del uso de una referencia superior asociada con cada DSA. Por ultimo, la comunicación entre ISN_{Dn} podría ser soportada por el protocolo DSP.

Relación ISN_{DN} a DSA:
Los nodos ISN_{DN} requieren que se cumpla con tres requerimientos: El ISN_{DN} debe ser capaz de almacenar datos similares a un ISN_{Dn}. Además, debe ser capaz de comunicar con los ISN_{Dn} dentro del operador de red al que sirve y también con otros operadores de red.

Para la comunicación entre ISN_{DN}, es de gran importancia la seguridad. La resolución de una petición debe evitar revelar información acerca de la red demandante, es decir, 'chaining' no sería permitida entre ISN_{DN} sino que podría resolverse mediante el protocolo DAP.

Relación ISN_s a DSA:
Un DSA es capaz de implementar un ISN_s de almacenamiento de datos con la restricción de que tales datos deben ser lógicamente estructurados en una manera jerárquica y en la forma de entradas con tipos de atributos asociados y valores.

Por tanto, si tanto ISN_s como ISN_{Dn} fueran mapeados a DSAs, entonces un protocolo DSP podría soportar las comunicaciones entre ellos. Una única petición X.500 podría atravesar la jerarquía de DDB UMTS y obtener o modificar los datos almacenados en ISN_s. Sin embargo, si los ISN_{Dn} fueran mapeados a los DSA y los ISN_s no, para soportar 'chaining' (ver anexo 2) entre ellos, se requeriría de un protocolo de interconexión para modificar y obtener datos.

Por otra parte, las DDB UMTS requieren mover y copiar grandes cantidades de información entre los ISN_s. Esta función es desarrollada en X.500 mediante un servicio de réplica llamado 'shadowing' que copia datos de DSA a DSA. Sin embargo, el intercambio de información es en grandes bloques y únicamente temporal y no se registra en el árbol DIT lo cual no favorece el seguimiento de móviles en UMTS. Una forma más simple de soportar la copia y el movimiento de datos en UMTS es mediante los protocolos DSP y DAP. Sin embargo, sería necesario realizar mejoras en la funcionalidad para soportar la gestión de transacciones requerida.

En cuanto a la estructura de directorios X.500, se observa que es muy estática. Puede percibirse en la estructura de protocolos X.500 que no estaba prevista una renovación de entradas tan rápida (p.e. en el caso del handover en UMTS), presentando operaciones complejas, con largas listas de parámetros y orientadas a grandes volúmenes de información.

1.9 Red inteligente para comunicaciones móviles

Para las comunicaciones móviles, se necesitan todas las funciones de red inteligente usuales en las redes de cableado fijo más otras relacionadas con la movilidad de servicio de abonado y gestión de llamada. Estas incluyen obtención y renovación de información de localización, autentificación, enrutado de llamadas, handover, tarificación y mantenimiento. Estas funcionalidades de servicio adicionales causarán un dramático aumento en el tráfico de señalización, especialmente en los entornos de microceldas con altas densidades de terminales móviles con frecuentes renovaciones de localización. Los sistemas de telefonía móvil actuales incorporan las funciones mencionadas anteriormente mediante dos redes inteligentes interconectadas, una para el sistema móvil y otra para la red fija a la que está conectada (p.e. ISDN) [ML1].

Las redes de la tercera generación exigen sistemas de redes inteligentes integrados, tanto en el acceso móvil como en la red fija. Dado un mosaico de celdas de movilidad en una determinada área geográfica, un gran operador de telefonía celular podría dar cobertura con celdas a muchas carreteras, otro operador en la red ferroviaria, otro operador en diversos edificios de oficinas limítrofes, etc. Para disponer de un entorno de gestión común eficaz donde la optimización en la cobertura de las celdas, asignación de canales y de recursos en la red sea posible conjuntamente para las más diversas necesidades de tráfico cambiantes sólo puede ser posible con la integración de los múltiples sistemas en una única red inteligente UMTS [VO1].

En el caso del handover en UMTS, el estándar de red inteligente CS-2 (series Q.1200 del CCITT) tendrá que adoptar una arquitectura distribuida consistiendo de múltiples instancias de funciones de control de servicio (SCF's). Esto es necesario para evitar señalización innecesaria en la red y minimizar los retardos incurridos.

Desde el punto de vista de seguridad, un escenario de red inteligente también proporciona mejores prestaciones para el soporte de sevicios de seguridad así como en la gestión interna del sistema.

Por otra parte, dadas las características de red avanzada que tiene que desempeñar UMTS, se está diseñando un terminal móvil tal que sea un terminal inteligente multimodo capaz de adaptar sus subsistemas de radio dependiendo del servicio requerido, la carga de teletráfico y el 'status' del radiocanal. Este terminal móvil dispondrá de lector de tarjetas inteligentes en donde situar el Subscriber Identity Device (SID) para la provisión de los parámetros de seguridad y los datos relativos al abonado [RS1].

Un terminal multimodo inteligente puede disponer de diversos subsistemas programables como codificadores (decodificadores) de fuente, codificadores (decodificadores) de canal, ensambladores (desensambladores) de paquetes, moduladores de banda base, front - ends de RF, estimadores de canal, filtros, etc. El codificador de fuente acepta datos de fuentes tales como voz, imágenes y señales de datos. La entidad de gestión forma el centro del terminal, recibe información de la actividad del codificador de fuente, conociendo el tipo de servicio móvil que se está proporcionando, el 'status' del canal y la información de teletráfico y otra información recibida de la estación base controla el codec de fuente. La entidad de gestión selecciona el tipo de FEC y entrelazado a ser usado por el subsistema codificador de canal; el método de acceso múltiple, tamaño de paquete y su encabezamiento para el ensamblador de paquetes; el tipo de modulación, control de ráfaga, secuencia de ensanchado para el modulador de banda base, frecuencia portadora, amplificación y filtrado por el módulo de RF del front - end.

Esta aproximación proporciona flexibilidad a operadores de red y a proveedores de servicio, permitiendo evolucionar según progrese la tecnología.

1.10 Procedimientos relacionados con el establecimiento de sesiones/llamadas en UMTS

Se define sesión de usuario (terminal) como el periodo continuo de tiempo durante el cual un usuario (terminal) tiene una asociación segura con un único proveedor de servicio para el propósito de usar uno o más servicios (llamadas). Para la sesión de usuario, el proveedor de servicio debe conocer el SID (Subscriber Identity Device) envuelto en la asociación. Una sesión de usuario consta de tres fases: inicio o establecimiento de la sesión; fase activa de la sesión y liberación de la sesión.

En la fase activa de la sesión pueden realizarse una o más llamadas consecutivas (entrantes o salientes) y/o registros de usuario. Los procedimientos de autentificación y de obtención del perfil de usuario que son comunes a los procedimientos UMTS dentro de la sesión de usuario se realizarian en la fase de inicio o establecimiento.

Para permitir el registro simultáneo del mismo usuario en diversos terminales para diferentes servicios (p.e. telefonía y fax) y posiblemente para soportar UPT se ha introducido el concepto de sesión de terminal, ya definido. En este caso, el proveedor de servicio no distingue para las autentificaciones entre los diferentes SIDs asociados con el terminal.

Una llamada se define como una asociación entre dos o más usuarios o entre un usuario y una entidad de red, que es establecida por el uso de las diversas capacidades de la red. El establecimiento de llamada comprende todas las funciones que se requieren para establecer, mantener y liberar una llamada. Para que exista un establecimiento de llamada en UMTS, al menos uno de los usuarios registrados en la llamada ha de ser un usuario UMTS.

La idea diferencial en UMTS es la separación de las fases entre el control de llamada y el control de conexión permitiendo controlar mejor las entidades funcionales de la red para la secuencia del protocolo. En la secuencia de procedimientos para el establecimiento de llamada se puede distinguir [AB16]:

Establecimiento de señalización de conexión
- Interrogación
- Paging

Establecimiento de conexión de servicios portadores
Terminación de la llamada
Fase de la llamada activa
Liberación de llamada y liberación de conexión.

En el establecimiento de señalización de conexión se establecen la relación de señalización extremo a extremo entre el usuario originante y la red y entre la red y el usuario llamado. Una vez se ha establecido la conexión originante, el establecimiento de llamada puede continuar. La relación de señalización es usada para la negociación de servicios, chequeo de perfil, chequeo de capacidades, pase del número marcado, etc. En esta fase se realiza una gestión de claves de sesión así como opcionalmente autentificaciones de usuario/terminal móvil con la red.

El establecimiento de conexión de servicios portadores comporta la creación de conexiones portadoras reales para ser usadas por los usuarios finales en la comunicación.

La fase de terminación de la llamada identifica los mensajes de respuesta enviados entre la red y los usuarios finales una vez que la conexión está preparada para usar. Estos mensajes comportan los mensajes de alerta y ringing para telefonia.

En la fase de la llamada activa, los mensajes de señalización intercambiados sirven para mantener la llamada activa actual (p.e. handover) o bien para negociar y hacer cambios en la fase activa de la llamada actual (p.e. añadiendo o borrando usuarios a la llamada o bien añadiendo o borrando conexiones portadoras a (o desde) una llamada activa).

Una vez los usuarios finales de una llamada han terminado su comunicación, empieza la fase de liberación de llamada y de liberación de conexión. Esta etapa realiza la liberación del acceso y servicios portadores de la red envueltos en la llamada mediante la liberación de las conexiones de red/usuario usadas para gestionar la llamada.

1.11 Procedimientos relacionados con la gestión de movilidad

Para poder contrastar mejor la aportación de mecanismos y servicios de seguridad en el handover, se describen a continuación diversos procedimientos relacionados con la gestión de movilidad. Estos procedimientos de movilidad en UMTS son utilizados en general para mantener la localización de usuarios y terminales por parte de la red. La localización del terminal se mantiene por medio del registro de localización y renovación de localización (location registration y location updating). La localización del terminal se identifica por medio de áreas de localización. Cada vez que el terminal móvil cambia de área de localización, se requiere de un registro de localización o renovación de localización. Cuando se realiza una renovación de localización, se utiliza la información de localización previa. En el caso de registro de localización, la información sobre localización previa del terminal no está disponible.

En principio, la renovación de localización concierne a la renovación de la localización del terminal en la red, no a la localización de cada usuario individual. La localización del usuario se mantiene por medio del registro de usuario (user registration), y se identifica normalmente en terminos del terminal móvil al cual el usuario está registrado. En este caso, el registro de usuario y el registro/renovación de terminal estan estrictamente separados funcionalmente. Como una estrategia alternativa, la localización de cada individuo podría ser renovada durante cada renovación de localización. En el caso de múltiples usuarios registrados en el mismo terminal móvil y haber un cambio en el área de localización, la localización de los usuarios puede renovarse colectivamente.

Cuando los usuarios dentro de UMTS mueven su suscripción (Subscriber Identity Device, SID) entre terminales móviles, se realiza un registro de usuario para notificar a la red acerca del terminal móvil al cual el usuario está asociado. La red proporcionará una asociación entre las identidades del usuario (via SID), el terminal móvil y el área de localización dentro de la

cual el terminal móvil está localizado en las bases de datos. En el momento que se separen será necesario un procedimiento de desregistro de usuario (User Deregistration) deshaciendo la asociación correspondiente.

Para permitir el inicio de un procedimiento de renovación de localización, el terminal móvil debe ser capaz de identificar cuando tiene lugar un cambio en el área de localización. Para hacer eso posible, la estación base transmite continuamente identificadores de área UMTS a los terminales móviles.

Además, un usuario podría manualmente iniciar una renovación de localización, por ejemplo, en el caso de un usuario que cambia de área de localización en una región en donde existe solape de áreas de localización incluso de diferentes redes. Desde el punto de vista de la red, la renovación de localización es similar en ambos casos.

Por último, se llama handover al procedimiento en el que un terminal móvil con una llamada en progreso cambia de radiocanales y/o conexiones con la red fija (sin necesariamente cambiar su punto de conexión a la red) mientras mantiene la llamada. Su estudio detallado se deja para los capitulos posteriores.

1.12 Referencias

[AB1] A. Barba, E. Cruselles, J. L. Melús. *The CPNs in UMTS. Security aspects.* Fourth WINLAB Workshop on Third Generation Wireless Information Networks. p. 317-328. New Jersey, 1993.

[AB16] A. Barba, J. M. Pulido, J. L. Melús. *Diseño de protocolos de gestión de movilidad entre redes privadas y UMTS.* IX Symposium nacional de la URSI. p. 1184-1189. Las Palmas de Gran Canaria, Septiembre 1994.

[DG1] David J. Goodman. *Cellular Packet Communications.* p. 1272-1280. IEEE Transactions on communications. Agosto 1990.

[DG2] David J. Goodman. *Trends in Cellular and Cordless Communications,* IEEE Communications Magazine, vol.29, No. 6, p.31-40, June 1991.

[HB1] Hans de Boer et al. *Network aspects for the third generation mobiles,* GLOBECOM '91, p. 1517-1522.

[HM1] Henning Maab, Oliver Schreyer, Martin Stahl. *Directory Services for Mobility Management in Private Telecommunication Networks*, ICC 1993, p. 1252-1256.

[ITUR1] FPLMTS Network architectures. Task group 8/1. CCIR Study groups. January 92.

[ITUR2] Security principles for FPLMTS. Task group 8/1. CCIR Study groups.22/10/1992.

[ITUT1] The Directory: Overview of concepts, Models and Services. X.500. 04-1992.

[ITUT2] The Directory: The Models. X.501. 04-1992.

[ITUT3] The Directory: Authentication Framework. X.509. 04-1992.
[ITUT4] The Directory: Abstract Service Definition. X.511. 04-1992.
[ITUT5] The Directory: Procedures for Distributed Operation. X.518. 05-1992.
[ITUT6] The Directory: Protocol Specifications. X.519. 05-1992.
[ITUT7] The Directory: Selected Attribute Types. X.520. 05-1992.
[ITUT8] The Directory: Selected Object Classes. X.521. 05-1992.
[ITUT9] The Directory: Replication. X.525. 05-1992.
[ITUT10] Directory Access Protocol: Protocol Implementation Conformance Statements PICS. X.581. 05-1992.
[ITUT11] Directory Systems Protocol: Protocol Implementation Conformance Statements PICS. X.582. 05-1992.
[JB1] J. Bursztejn. *Interoperability and/or convergence of mobile systems.* p. 9-12. RACE Mobile Telecommunications workshop. Amsterdam. 1994.
[JI1] James I. Yu. *IS-41 for mobility management.* p. 158-162. ICUPC'92 Dallas, 1992.
[JI2] James I. Yu. *Overview of EIA/TIA IS-41.* p. 220-224. PIRMC '92 Boston. 1992.
[KJ1] Kai Jakobs, Frank Reichert. *New Applications in Mobile Communication. The Directory.* 41st VTC Conference, p. 485-490, San Louis, 1991.
[LH1] L. Hanzo, R. Steele. The Pan-European mobile radio system. Part I y II. BT. Marzo-Abril 1994.
[MC1] Michael H. Callendar. *Future Public Land Mobile Telecommunication Systems.* IEEE Personal Communications p. 18-22. 4º trim. 1994.
[MH1] Mitts Hakan. *Universal wireless accesss to ATM.* p. 329-333. RACE Mobile Telecommunications Workshop. Portugal, 1995
[ML1] Mikko Laitinen y Jari Rantala. *Integration of intelligent network services into future GSM networks.* IEEE Communications Magazine. p. 76-86. Junio 1995.
[MM1] Michel Mouly y Marie-Bernadette Pautet. *Current evolution of the GSM systems.* IEEE Personal Communications. p. 9-19. Octubre 1995.
[MM2] M. B. Pautet and M. Mouly. *GSM protocol architecture: Radio sub-system signalling*, 41st IEEE Vehicular Technology, pags 326 - 332. 1991.
[NS1] Nuno Silva, Carlos Belo. *Structure and mobility functions for the MCPN.* p. 472-477. RACE Mobile Telecommunications Workshop. Amsterdam. 1994.
[PO1] Peter Olanders. *DECT standardisation. 'status' and future activities.* p. 1064-1069. PIMRC´94.
[RACE1] RACE 1043/RNL/FN12/DS/A/067/b1. Fixed Network activities. 1991.
[RACE11] RACE 2066/PTTNL/MF1/DS/P/014/a1, Stage 2 (draft) specification of communications between databases. October 1992.
[RACE12] RACE 2066/PTTNL/MF1/DS/P/032/a1, UMTS Distributed Database functionalities. June 1993.
[RACE21] RACE 2066/LMF/GA1/DS/P/028/b1. UMTS functional requirements. 1993.

[RACE24] RACE 2066/GA3/DS/P/29/b1, UMTS Functional Model (draft). 1993

[RACE25] RACE 2066/FACE/GA3/DS/P/033, UMTS Network Architecture Draft. July 1993.

[RS1] Raymond Steele. *Global PCN and the intelligent multimode terminal.*

[RS2] Raymond Steele. *The evolution of personal communications.* IEEE Personal Communications. p. 6- 11. 2º trim. 1994.

[SH1] Stein Hansen. The standardization of UMTS in ETSI SMG5. p. 185-194. DMR V.

[VO1] Victor O. K. Li, Xiaoxin Qiu. Personal Communication Systems (PCS). Proceedings of the IEEE. p. 1210-1243. Septiembre 1995.

[WG1] Wolfgang Groenen. *GSM and beyond digital cellular mobile technology on its way to global services.* p. 81-86. DMR VI.

Capitulo 2

El procedimiento de handover

2.1 Introducción

En este capitulo se especifican las características generales del handover en un sistema de comunicaciones móviles avanzado. Se hace referencia a los requerimientos y criterios sobre el inicio de la invocación del procedimiento de handover. Se definen los diversos tipos según la secuencia adoptada para construir el nuevo camino dentro del proceso del handover o bien la forma en la que se establece el camino a la nueva celda.

Por otra parte, se describen los aspectos más importantes sobre los criterios utilizados por el algoritmo de selección de celdas en la fase de decisión así como por el algoritmo relativo a la activación de un handover. Se analizan las características y parámetros de diseño en el handover para la introducción de una red inteligente.

El objetivo consiste en configurar el marco de trabajo bajo el cual se definan los algoritmos de gestión del handover y finalmente la integración de su seguridad.

2.2 Definición de handover

Aquí se considera el termino handover como la situación en que un terminal móvil con una llamada en progreso cambia de radiocanales y/o conexiones con la red fija (sin necesariamente cambiar su punto de conexión a la red) mientras mantiene la llamada.

El handover se puede presentar en diversas situaciones según sea el origen de la invocación, por ejemplo, el requerido por el radioenlace, que es el más frecuente en las redes

convencionales y está estrictamente relacionado con los parámetros del radioenlace como la relación señal a ruido, la potencia de señal recibida o via control de calidad (parámetros relacionados como relación señal a ruido o BER). El handover se activa como resultado de la monitorización de los parámetros del radioenlace en comparación con unos determinados valores prefijados.

Otro ejemplo de tipo de handover puede originarse por el propio abonado al requerir ciertas funciones debidas al servicio de abonado/usuario, tales como perfil de servicio, tarificación, acceso a determinados servicios, etc.

Por último, el handover originado por la red se basa en los parámetros de calidad del sistema desde un punto de vista global. La activación del handover sería decidido por una red inteligente que tuviera el conocimiento y control del 'status' completo del sistema celular, por ejemplo, el 'status' de los diferentes canales de radio en terminos de los niveles de ruido completos o utilización de los recursos radio, el 'status' de la utilización de los recursos de la red fija, como son: la óptima distribución de las cargas de tráfico o la óptima utilización de recursos físicos durante la fase activa de la llamada, el 'status' de las alarmas de la red y las situaciones de fallos [PC1, LC1, BJ1].

El proceso del handover puede dividirse en dos fases: la fase de decisión cuando la red y/o el terminal móvil deciden que es necesario ejecutar el handover a una determinada celda candidata y la fase de ejecución para encontrar y establecer las nuevas conexiones via red y radio.

Se pueden definir dos tipos de handovers según la secuencia adoptada para construir el nuevo camino dentro del proceso del handover. Se refiere a los recursos utilizados a la hora de intercambiar la información relacionada con el handover de un enlace al otro:

- Backward handover:
Es el procedimiento mediante el cual, el terminal móvil cambia su punto entrante a la red fija, después de que ha sido establecida la conexión con la nueva estación base. El enlace de señalización se mantiene para realizar el handover con la anterior estación base durante todo el proceso, sirve para intercambiar la información de señalización y se conmuta al final a la nueva estación base. Por otra parte, no permite el reestablecimiento de la llamada si se produce un decaimiento en el enlace de señalización durante el handover.

- Forward handover:
En este caso, el enlace de control de señalización se establece con la nueva estación base antes de liberar el enlace de comunicaciones con la anterior estación base y sirve para

transmitir la información del handover. Permite el reestablecimiento de la llamada si hay un decaimiento en el enlace de señalización durante el handover. Este tipo de handover sólo es posible si la asignación de canal es controlado completamente por el terminal móvil.

El handover también puede clasificarse según la forma en la que se establece el camino a la nueva celda y la conexión se cambia desde la celda actual a la nueva celda [BJ1]. Así pues de esta forma:

- Hard handover: El terminal móvil tiene que cambiar de radiocanal (frecuencia) al nuevo camino con posiblemente una corta interrupción de la conexión en progreso. El nuevo camino se construye de forma avanzada a la red de forma que la interrupción es tan pequeña como sea posible. La conmutación y el reenrutado de la información al nuevo camino se realizan simultáneamente.

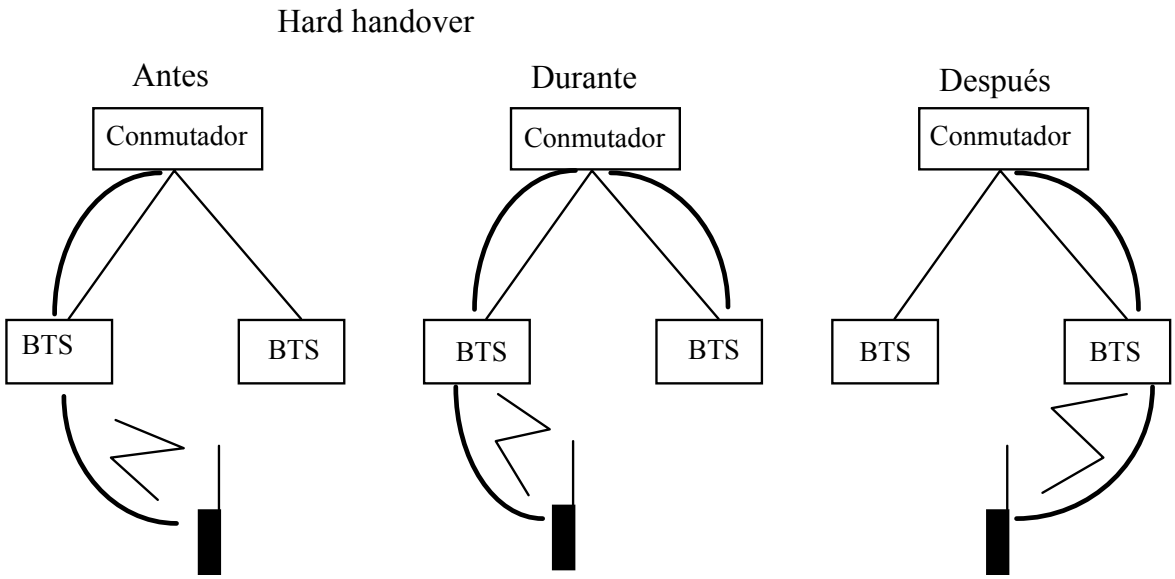


Fig. 2.1 Procedimiento de hard handover.

- Seamless handover: El nuevo camino se establece en paralelo con el antiguo y el flujo de información se transmite por el terminal móvil en ambos caminos, es más, durante un instante el camino activo es el antiguo. Entonces, se activa el nuevo a través de una conmutación en la red. El antiguo camino se para y sus enlaces son liberados.

- Soft handover: En este handover hay dos caminos y sus correspondientes flujos de información activos, al menos durante un determinado tiempo.

Los mejores rendimientos en el intrahandover se consiguen mediante técnicas DCA (Dynamic channel assignment) en donde cada terminal móvil mide la interferencia percibida en su canal y decide cambiar de radiocanal de forma completamente descentralizada. Si bien

cabe la actuación de un sistema de gestión de recursos según los distintos grados de congestión en las celdas. Este tipo de funcionamiento es propio de las redes más avanzadas y compatible con un seamless forward handover objeto de nuestro trabajo.

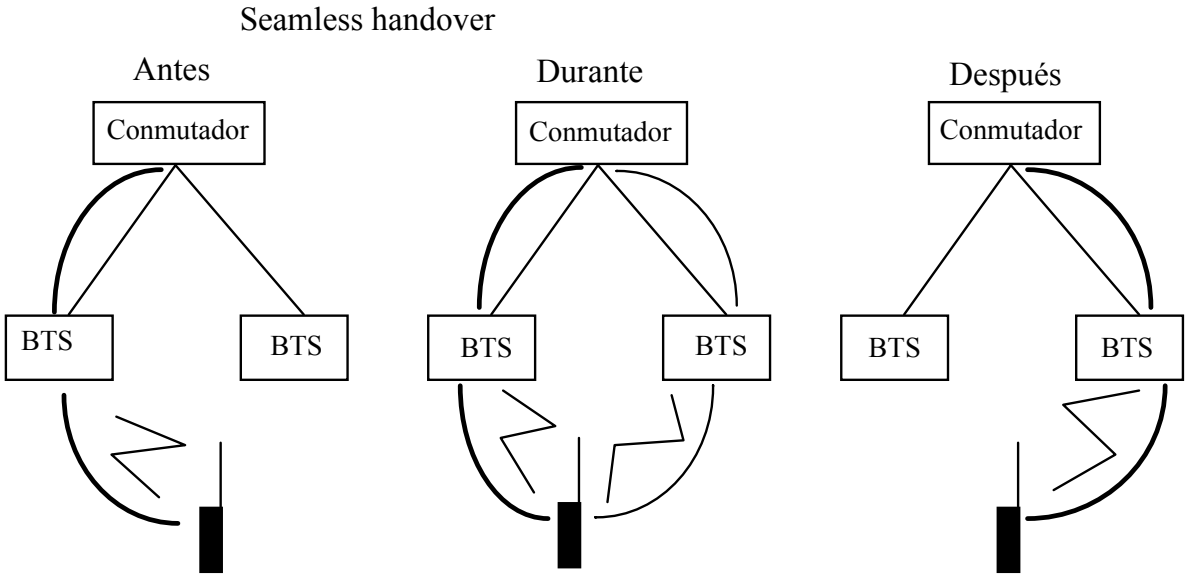


Fig. 2.2 Procedimiento de seamless handover.

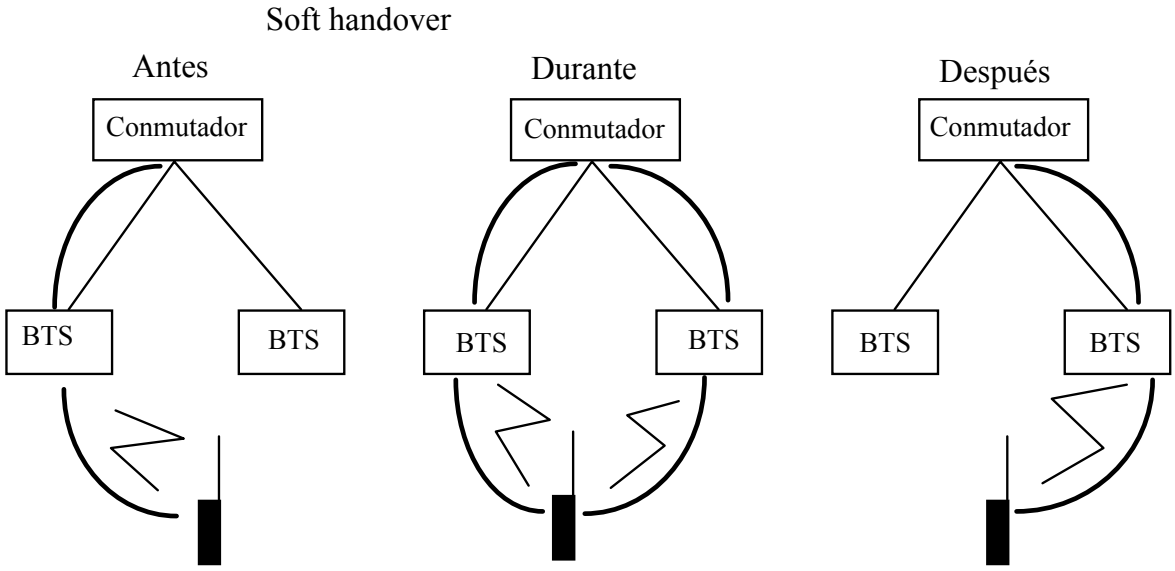


Fig. 2.3 Procedimiento de soft handover.

Además, como se estudiará en los últimos capitulos, existe la posibilidad de integrar funcionalidades de seguridad en el control del handover, como por ejemplo, en la sincronización con la fase de iniciación del handover. Ello comportaría la invocación simultánea de los procedimientos de gestión de claves con la fase de iniciación del handover. Dependiendo de la política de seguridad establecida, se procedería a involucrar determinados servicios de seguridad en la fase de ejecución de handover. Eso supone el iniciar el handover con retardo, tener un ahorro de procesamiento y la señalización posterior, posibles problemas

de implementación en el caso de handovers controlados por el terminal y en definitiva, una ejecución de handover rápida.

2.3 Requerimientos en el handover. Aspectos de calidad de servicio y prestaciones

Se pueden distinguir básicamente dos grandes grupos de requerimientos en el handover, requerimientos operacionales y requerimientos funcionales [RACE14, 16, 21]. Los requerimientos operacionales en el handover pueden ser de tres tipos: requerimientos de usuario; requerimientos de operador y requerimientos del proveedor de servicio.

De manera similar, los requerimientos funcionales en el handover pueden abarcar los siguientes ámbitos: interfaz de usuario, operación de red y mantenimiento, servicios, seguridad, uso de recursos de red, uso de recursos de radio, handover entre dominios de operadores de red y handover entre dominios de proveedores de servicio. Para la adecuada valoración de una solución óptima en el handover, se distinguen parámetros como la calidad de servicio resultante o bien las prestaciones de red [JL1].

Calidad de servicio (CdS): Puede definirse como el efecto colectivo de los parámetros de prestación de servicio que determinan el grado de satisfacción de un usuario del servicio. La calidad de servicio (CdS) refleja el punto de vista del servicio proporcionado al usuario.

Prestaciones de red (PdR): Puede definirse como la capacidad de la red para realizar todas las funciones requeridas bajo ciertas condiciones, en un intervalo de tiempo dado y reflejando el punto de vista del proveedor de servicio (a diferencia de la CdS en que actua el usuario).

Calidad / Parámetro	Tasa de bit muy baja (QCIF, CCITT)	Calidad mejorada (FCIF, CCITT)	Alta calidad (PAL, NTSC)
Resolución	176*144	352*288	525 ó 625 lineas
Tasa de repetición	5	7,5	15
Retardo propagación (un sentido)	440 ms	340 ms	190 ms
Retardo recuperación (debido a handover)	300 ms	200 ms	100 ms
Retardo recuperación (por cambio fuente)	3 s	2 s	1 s
Bit rate	4,8 - 64 Kbps	p * 64 Kbps	1,5 - 2 Mbps

Tabla 2.1 Comparación entre distintas calidades de video.

La calidad de servicio orientada a la red es la calidad del servicio portador, ésta es necesaria para proporcionar a cierto terminal la calidad de servicio orientada a usuario requerida. Se pueden identificar los siguientes parámetros de CdS específicamente relacionados con el handover:

- Bit-rate conseguido durante el handover
- Tiempo de interrupción de la transferencia de información de usuario debido a handover
- Bit error rate observada durante el handover
- Tasa de fallos en el handover.

En comunicaciones interactivas, el retardo de transferencia aceptable máximo es de 400 - 500 ms. El retardo de codificación/decodificación máximo es del orden de 300 ms.

Ancho de banda de audio	Ratio MOS (calidad) (1(mala)-5(excelente))	Minimo bit rate requerido (Kbps)	Notas
15 Khz 7 Khz (3,1 Khz) 3,1 Khz	4,5 4,3 4,0 < 3,5	>= 64 24 - 64 16 <= 8	HIFI o calidad FM (64 Kbps ADPCM) Calidad casi transpar. Calidad comunicac.

Tabla 2.2 Relación aproximada entre bit rate y calidad de audio.

Servicio	BER máximo	Retardo
Voz (32, 16, 8 Kbps)	10^{-3}	Sensible
Datos asincronos	10^{-9}	Insensible
Facsimil	10^{-4}	Insensible
Paquetes de datos	10^{-9}	Insensible
Video de baja resolución (64-128 Kbps)	10^{-5}	Sensible

Tabla 2.3 Prestaciones requeridas para servicios de telecomunicación.

2.4 Iniciación del handover

El handover puede ser ejecutado bien por el terminal móvil o bien por la red fija. En el caso de ejecución por parte del terminal móvil, se habla de un forward handover y en el caso de ejecución por parte de la red fija sa trata el caso de un backward handover. En ambas

situaciones es la red quien soporta la mayor parte de carga de procesado antes de poder ejecutar propiamente el handover.

En la iniciación del handover, se parte de las mediciones realizadas sobre el sistema (radioenlace, tráfico en celdas,...) y se decide activar el handover a una determinada celda candidata. El proceso del handover puede dividirse en dos fases: la fase de decisión cuando la red y/o el terminal móvil deciden que es necesario ejecutar el handover, y la fase de ejecución para encontrar y establecer las nuevas conexiones via red y radio.

A continuación, se presenta una clasificación de los criterios de iniciación del handover que influyen en la decisión y/o ejecución en el handover:

- Impacto del radioenlace
- Impacto de la red:
  Criterios de gestión de red: Utilización óptima de recursos y criterios de mantenimiento.
  Criterios orientados a servicio
- Uso por parte del abonado:
  Criterios orientados a servicio

En la fase de decisión del handover, un algoritmo determina la lista de celdas candidatas y por tanto la celda objetivo del handover. Este algoritmo debe recoger el impacto o efecto de todos los parámetros anteriores para el correcto funcionamiento del sistema móvil. Una vez la red dispone de toda la información, incluida la enviada por el terminal móvil, ésta la procesa y obtiene una celda objetivo. Paralelamente, y de forma general, otro algoritmo de ejecución activa propiamente el procedimiento de handover en base a determinados parámetros de nivel de señal y relación señal ruido del enlace. En el caso de determinadas operaciones de mantenimiento o a petición del abonado por criterios orientados a servicio, la red también puede ejecutar el handover.

Por tanto, la activación del handover requiere de una red inteligente que disponga del conocimiento y control completo del sistema celular. Este nivel de conocimiento más alto es bastante diferente del conocimiento que se refiere de la calidad del radioenlace en un único enlace, propio de los sistemas más convencionales.

2.5 Impacto del radioenlace en el handover

El handover originado por efectos del radioenlace puede ser debido al control en la potencia de la señal o via control de calidad (parámetros relacionados como relación señal a ruido o BER).

Se estudia el impacto de las técnicas de acceso múltiple de radio en el handover. En UMTS se estima que pueden ser: Time Division Multiple Access (TDMA) o bien, Code Division/Spread Spectrum Multiple Access (CDMA/SSMA) [NW1, SS1, GF1, MA1, AV1, CS1, RACE14].

Técnicas TDMA

En un sistema TDMA se comparte la misma portadora por diferentes comunicaciones cada una transmitiendo en un segmento temporal diferente. Esta definición puede aplicarse tanto a conmutación de circuitos TDMA como a esquemas de acceso múltiple de conmutación de paquetes como PRMA (Packet Reservation Multiple Access).

En este caso, la adaptación al medio es importante, un ejemplo de adaptación es la asignación de slots temporales a usuarios basándose en un algoritmo de control de errores. En general, la red fija tendrá que implementar funcionalidades del handover derivadas de la necesidad de usar procedimientos de aprendizaje, por la posibilidad de variaciones y/o requerimientos y parámetros del sistema de handover cambiantes por la predicción de riesgos, costes y beneficios de posibles configuraciones futuras del sistema.

La idea de usar macrodiversidad en TDMA es una opción prevista básicamente para compensar los decaimientos de señal en la cobertura de microceldas. El terminal móvil con varios enlaces con la red fija (micro, pico y macro estaciones base) podría seleccionar la mejor calidad para obtener la recuperación de la información.

Uno de los grandes requerimientos para proporcionar macrodiversidad es la necesidad de sincronización con las BTS a nivel de slot y de trama. De esta forma, el terminal móvil tiene que transmitir sólo un paquete a cada BTS en lugar de diferentes paquetes a diferentes BTSs.

La macrodiversidad podría ser aplicada tanto al enlace ascendente como en el descendente, sin embargo, en el caso de esquemas TDMA, resulta complicado la recepción por parte del terminal móvil de diferentes enlaces con BTS con diferentes sincronizaciones y frecuencias portadoras por problemas de complejidad y retardos de procesado en el mismo terminal. Este problema podría reducirse en el caso de las BTS con el uso de estructuras tipo MAN.

El tipo de medidas en el handover y la forma de realizarlas depende de los multiples esquemas de acceso adoptados. En un sistema UMTS es posible que diferentes tipos de

celdas puedan usar diferentes mecanismos de acceso y por tanto disponer de diferentes algoritmos de handover. En consecuencia, la red debe ser capaz de adaptar los parámetros del sistema según los diferentes algoritmos cuando se pasa de entornos (macroceldas) a diferentes (microceldas) caracterizados por decisiones de handover y mecanismos de control diferentes.

Los niveles de decisión en el handover se adaptan según la configuración del entorno y se relacionan con el nivel de señal recibida mínimo, mínima calidad aceptable del enlace, distancias, etc.

La elección del algoritmo de handover intracelda está estrictamente relacionado con el nivel y la estabilidad de la interferencia. De hecho, debido a la rapidez por la cual los usuarios acceden a los slots de tiempo disponibles, las muestras de interferencia podrían variar muy rápidamente haciendo difícil la predicción de la calidad en futuros slots temporales. De ahí que no es seguro que los handover intraceldas (basados en medidas de interferencia) garanticen una mejora en la calidad de la comunicación en el radioenlace.

En los esquemas TDMA, como se muestra más adelante, el procedimiento de forward handover sería preferible por su rapidez y el menor uso de recursos. Además, permite la posibilidad de reestablecimiento de llamada en caso de fallo en el enlace de señalización. Por ello el forward handover es adecuado para condiciones de propagación con rápidas degradaciones (p.e. en el efecto esquina de calle en las microceldas). Por el contrario, el backward handover es más seguro en condiciones de propagación menos fluctuantes y las prestaciones del handover dependen del entorno de operaciones y de la disponibilidad de recursos.

Por tanto, el mecanismo de handover será escogido por el terminal móvil según las condiciones externas. De hecho, las prestaciones de cada tipo de mecanismo dependerán del tipo de entorno en la red hacia el cual el handover es dirigido. Para informar al terminal móvil acerca de las condiciones del entorno y permitir la elección del mecanismo de handover cada BTS tiene distribuir mensajes en un canal de control común incluyendo, junto a otra información, el tipo de celda y la identidad de la red.

Finalmente, hay que decir que la macrodiversidad y la duplicación de información no son buenas opciones en TDMA ya que reducen la capacidad e incrementan el nivel de interferencia.

Técnicas CDMA

Los sistemas CDMA (SSMA) son aquellos que emplean técnicas de espectro ensanchado para proporcionar acceso múltiple a un medio compartido. En un sistema de espectro ensanchado la señal transmitida es ensanchada sobre una banda de frecuencia mucho mayor que el ancho de banda mínimo requerido para transmitir la información a ser enviada. Este ancho de banda adicional es empleado para proporcionar algunas propiedades como el incremento de la inmunidad al ruido e interferencias y/o capacidades de acceso múltiple.

Existen dos grandes tipos de sistemas CDMA: El Direct Sequence (DS) y el Frequency Hopping (FH). Sin embargo, los esquemas DS son considerados más adecuados que los FH para ser empleados en sistemas de comunicación móvil.

La macrodiversidad será usada normalmente en el caso de handover intrafrecuencia. Sin embargo, en casos como en el cambio de dominios, se requerirá handover interfrecuencia (con hard handover). La elección entre ambos dependerá también de otros factores como la carga de tráfico en las celdas, el retardo, etc, la ocupación de recursos con la macrodiversidad harán que la única salida válida sea el soft handover.

La funcionalidad de combinación permite combinar diferentes flujos relacionados con la misma fuente originaria posiblemente proviniendo de diferentes estaciones base para reproducir un único flujo de datos. El 'multicasting' es la funcionalidad dual. Tanto la combinación como el 'multicasting' en el enlace descendente se realizan en el terminal móvil a nivel físico realizando la macrodiversidad directamente con el receptor tipo RAKE. En el enlace ascendente, tanto la combinación como el 'multicasting' se realizan a nivel de enlace en la estación base.

Una de las propiedades más destacables de los esquemas CDMA es su capacidad flexible, les permite incrementar la capacidad a pesar de proporcionar baja calidad. En general, la máxima capacidad se obtiene equilibrando el tráfico en combinación con las celdas vecinas.

CDMA/DS:
En este caso, el ensanchado se obtiene multiplicando la información digital original por una estructura de señal como el ruido, por ejemplo, una secuencia de código pseudo ruido, cuya chip rate es mucho más alta que la información rate. La señal original se recompone en el receptor mezclando la señal recibida con un código ensanchado sincronizado generado localmente.

La característica fundamental de estos sistemas y que afecta de manera importante en el handover es el control de potencia. Éste es necesario para ecualizar la potencia recibida de todos los transmisores en el receptor. La potencia recibida, en general es función de la

distancia entre las estaciones y de las condiciones de propagación en el canal. La señal de control podría ser derivada de la relación señal a ruido o del bit error rate recibido, en general, se prefiere esta última opción.

Otro aspecto clave en los sistemas CDMA es la posibilidad de que en microceldas y macroceldas se comparta la misma frecuencia de radio para los dos radioenlaces, el de subida y el de bajada. El problema está también en los niveles de señal recibida para ambos tipos de celda.

Para sistemas CDMA/DS, el soft handover con macrodiversidad es la opción natural. Sin embargo, por razones tecnológicas es difícil que sea rápido. En este caso, la conexión física a la nueva estación base se realiza antes de liberar el enlace previo. El uso de macrodiversidad exige que las celdas utilizadas pertenezcan al mismo grupo (dependientes de una misma CSS). Esta técnica permite ser utilizada para combatir los decaimientos de señal en la propagación del tipo NLOS (Non line of sight).

Entre las ventajas que se pueden obtener con la macrodiversidad está: una mejor área de cobertura; reducción de los efectos de interferencias y decaimientos; ahorro de espectro y mejora del bit rate de salida o bien ahorro en el sistema hardware (reducción de BTS´s).

Entre los inconvenientes, se puede especificar el potencial incremento en el nivel de interferencias en el enlace descendente debido al incremento generalizado en el número de estaciones base co-canal y también como incremento de complejidad de las entidades de gestión del sistema que podrían encontrar dificultades usando el control de potencia mientras mantienen enlaces simultáneos.

CDMA/FH:
Tanto en sistemas FH, como en sistemas DS, se ensancha la señal sobre un ancho de banda mayor que el requerido para transmitir la información. Sin embargo, en cada instante, sólo se emplea un canal del ancho de banda de la señal. Se utiliza un canal particular sólo para un pequeño espacio de tiempo, siendo la señal saltada sobre un número de canales distribuidos pseudoaleatoriamente. FH podría considerarse como un proceso de modulación en dos pasos consistiendo de modulación de datos y modulación en salto de frecuencias. Sólo la técnica con muchos símbolos por hop se considera una forma válida de proporcionar diversidad en sistemas TDMA y FDMA o bien en sistemas DS. En general, el handover en sistemas FH es complicado y más lento que en sistemas TDMA, llegando a ser problemático en el ámbito de microceldas por las prestaciones requeridas, ya que se requiere de canales de control para permitir a las estaciones móviles hacer controles de potencia de las estaciones base del entorno.

2.6 Impacto de la red y el abonado en el handover

El impacto de la red o el abonado en la activación del handover se basa en los parámetros de prestaciones del sistema no directamente relacionados con la calidad del radioenlace de una única comunicación sino de la calidad del sistema desde un punto de vista global.

Criterios de gestión de red

Los requerimientos de gestión de red establecidos en sistemas celulares avanzados están relacionados con la óptima distribución de las cargas de tráfico y la óptima utilización de recursos físicos durante la fase activa de la llamada. En este sentido, se definen criterios para valorar el impacto de la red en el handover como son el criterio para el uso de recursos de radio óptimos y el criterio para el uso de entidades fijas óptimas. Se establece también un criterio basado en el mantenimiento relacionado con el problema de alarmas y detección y manipulación de fallos en la red.

Criterio de utilización de recursos de radio óptimos:

Existen criterios de utilización de recursos de radio óptimos, en donde la red afecta al handover para obtener una distribución de tráfico más uniforme en sus servicios portadores o la distribución de cargas entre celdas adyacentes durante la fase activa de la llamada. Para ello, la red tiene un control jerarquizado distribuido del 'status' del sistema en terminos del nivel de las intensidades de tráfico y del nivel en la utilización de los recursos de radio.

Cuando una celda está congestionada y las celdas adyacentes no lo están, y se adopta un esquema de asignación de canales fijo, la red puede decidir de realizar el handover para distribuir la demanda de tráfico entre las celdas. En este caso, la red puede forzar varios handover en terminales que estén en la periferia de celdas congestionadas hacia celdas adyacentes no congestionadas mediante una determinada gestión en la red.

Por otra parte, se espera que en redes como UMTS, los canales puedan asignarse dinámicamente a las estaciones base para compensar las variaciones de tráfico. Eso se conoce como handover intracelda, y se basa en el proceso denominado Dynamic Channel Allocation (DCA). El DCA por tanto, resultaría un caso particular de tipo de handover que puede aplicarse tanto a macroceldas como a microceldas. Según el DCA, todos los canales pueden ser usados en cada celda. En éste, se chequea continuamente la calidad del canal utilizado, en términos de CIR o RSSI.

Respecto a la capacidad máxima del sistema, ésta se obtiene cuando las macroceldas pueden estar completamente llenas con microceldas y se obtiene concentrando el máximo tráfico

posible en las microceldas. Esto implica que las macroceldas serán usadas sólo en los siguientes casos:

- Cuando un terminal móvil está en un área no servida por una microcelda.
- Cuando la microcelda está congestionada.
- Cuando la macrocelda está temporalmente usada como celda paraguas.

Criterio de utilización de entidades fijas óptimas:
En este caso, se supone que la red es inteligente y permite la distribución óptima de componentes en la red fija para asumir adecuadamente la carga de tráfico de señalización y de tráfico de información correspondiente al sistema.

En cuanto a la movilidad de usuarios, se sugiere para sistemas de arquitectura mixta el uso de canales para estaciones base microcelulares para terminales a baja velocidad (p.e. portables) y canales de estaciones base macrocelulares para terminales de movimiento rápido (p.e. coches). De esta forma, se minimizan los handovers una vez que los canales han sido asignados a las respectivas celdas.

El reenrutado del flujo de información en la red fija durante la fase activa de la llamada puede ser necesario si la red debe asegurar que el tráfico siempre fluya a través del camino más corto. Para conseguir esto, la red puede forzar un handover para cambiar la conexión de la red fija (cambiando de conexión en la red fija pero no necesariamente del canal de radio). La elección del punto de conexión de nuevo a viejo (puenteo) en la red fija es vital para la óptima explotación de los recursos de red.

Criterios orientados a servicio
El criterio orientado a servicio puede utilizarse en la activación de handovers tanto por la red como por petición de los abonados. En el primer caso, los diferentes orígenes de handover derivan de la provisión en red de diferentes servicios con alto nivel de calidad. En el segundo caso, los requerimientos de servicio por el abonado se consideran para identificar su relación con el inicio del handover.

Casos originados por la red:
Estos casos se deben a la continuidad de la calidad de servicio, por ejemplo, cuando se identifica una degradación de la calidad del servicio (BER, señal a ruido,...), podría requerirse el activar el handover a un diferente canal por parte de la red para soportar el servicio de diversidad macroscópico.

Por ejemplo, cuando se identifica una degradación de la calidad del servicio (debida a fallos o a mantenimiento,...) podría ser necesario activar el handover a un diferente canal por parte de la red para obtener una mejor calidad de servicio. También, en el caso de identificarse por ejemplo, una brecha de seguridad por parte de la red en un área de servicio específico durante una llamada activa entonces podría iniciarse un handover a una diferente celda para que el problema fuera solventado.

La red podría identificar la posibilidad de abrir al usuario (con un terminal multimedia) un servicio de distribución adicional durante una llamada activa. En este caso se activaría un handover a una diferente celda si el usuario estuviera abonado a ese servicio.

Casos originados a petición del abonado:
El terminal móvil podría iniciar una petición a la red por un componente de servicio adicional (p.e. más ancho de banda, servicios suplementarios) durante una llamada activa y la red activar un handover para conectar el terminal móvil a una nueva celda donde podría proporcionarse la componente del servicio pedido.

En el caso de activación debida a diferencias de tarificación correspondiente a un servicio. El conocimiento del servicio podría ser usado como un criterio para handover originados por el abonado cuando en una localización particular el mismo servicio es proporcionado por diferentes proveedores de servicio con diferentes tarifas. Esta información podría utilizarse por parte del usuario para hacer una petición por un handover durante una llamada activa para cambiar de proveedor de servicio.

Un usuario podría estar dentro de un determinado grupo para un servicio y podría pedir por un servicio suplementario o un servicio de valor añadido adicional que no está proporcionado en un área de servicio específica. Cuando el usuario entra en una subarea donde el servicio previamente demandado está disponible, podría iniciarse un handover para tal fin.

Por otra parte, cuando un usuario cambia de posición, el handover podría utilizarse en base al perfil de servicio del usuario. Ese handover podría originarse por el usuario aún teniendo la red que asegurar los controles de acceso requeridos si se trata de handovers entre celdas que son responsabilidad de operadores de red diferentes con sistemas de gestion diferentes.

2.7 Referencias

[AA1] Anthony S. Acampora and Mahmoud Naghshineh. *Control and quality-of-service provisioning in high-speed microcellular networks.* p. 36-43. IEEE Personal Communications. 2º cuatr. 1994.

[AV1] Audrey M. Viterbi y Andrew J. Viterbi. *Erlang capacity of a power controlled CDMA system.* IEEE Journal on selected areas in communications. p. 892- 900. Agosto 1993.

[BJ1] Bijan Jabbari, Giovanni Colombo, Akihisa Nakajima y Jayant Kulkarni. *Network issues for wireless communications.* IEEE Communications Magazine. p. 88-98, Enero 1995.

[CS1] C. M. Simmonds and M. A. Beach. *Network planning aspects of DS-CDMA with particular emphasis on soft handoff.* 43 rd VTC Secaucus (NJ) p. 846-849. 1993.

[DC1] David Chess, Benjamin Grosof, et al. *Itinerant agents for mobile computing.* IEEE Personal communications. p.34-49, Octubre 1995.

[GF1] G. Falciasecca, G. Riva et al. *General approach for the comparison of spectrum efficiency of digital mobile radio systems.* p. 77-83. BT. Enero-Febrero 1994.

[JL1] Jan Lucénius. *Service parameters in UMTS.* p. 547-556. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[KM1] Kenji Minato, Ikuo Yoda, Nobuo Fujii. *Distributed operation system model using directory service in telecommunication management network.* p. 1207-1211. Globecom '93 IEEE Houston. 1993.

[LC1] L. Carrasco Martorell, I. Berberana Fernández de Murias. *El handover, un servicio de la red inteligente.* Comunicaciones de Telefónica, p.74-80. Julio-Dic. 1993.

[MA1] Magnus Almgren, Hakan Andersson y Keneth Wallstedt. *Capacity enhancements in a TDMA system.* 43 rd VTC Secaucus (NJ) p. 277-280. 1993.

[NW1] N. Wilson, R. Ganesh et al. *CDMA versus dynamic TDMA for access control in an integrated voice/data PCN.* ICUPC'92 Dallas, p. 267-272. 1992.

[PC1] P. C. Mason, A. N. Brydon and J. M. Cullen. *UMTS handover requirements in the context of an intelligent network architecture.* PIMRC'93 Yokohama, p. 715-720.

[PM1] P. Mermelstein, A. Jalali y H. Leib. *Integrated services on wireless multiple access networks.* p. 863-867, ICC´93. Geneve.

[RACE14] RACE 2066/CSELT/MF2/DS/P/035/b1. UMTS Stage 2 specification of handover and switching schemes. 1993.

[RACE16] RACE 2066/PKI/NESSY1/DS/P/067/b1, Conclusions concerning radio resource management strategies. Sept. 1994.

[RACE21] RACE 2066/LMF/GA1/DS/P/028/b1. UMTS functional requirements. 1993.

[ST1] S. C. Swales, T. Busby, et al. *A comparison of CDMA techniques for third generation mobile radio systems.* 43 rd VTC Secaucus (NJ), p. 424-427. 1993.

Capitulo 3

Evaluación de parámetros de diseño para la selección de celdas en el handover

3.1 Introducción

Con el fin de mejorar y completar de forma óptima el procedimiento de handover, se plantea una nueva especificación de parámetros para su introducción en el algoritmo de decisión de selección de celdas. Se hace especial énfasis en el impacto que supone tratar determinada información sobre tráfico y los niveles de congestión de las celdas con el objetivo de gestionar los handover del sistema a nivel global.

La implementación de una gestión de parámetros en el handover soportada por una red inteligente requiere disponer de cierta información de gestión previa. Un análisis conjunto de la red y de la trayectoria del móvil permitirá preveer con suficiente antelación la necesidad de hacer un handover y a qué celdas. Esto supondrá disponer de ciertas ventajas por ejemplo, para la gestión de claves y para mejorar las prestaciones del sistema.

En este capitulo, primero se especificará la gestión de parámetros que se lleva a cabo en el radioenlace dentro de un mismo dominio. Se observará su efecto en el handover y se optimizarán los parámetros que determinan el algoritmo de selección de celdas. Se determinará un algoritmo de celdas candidatas en base a la movilidad de los terminales móviles desde un punto de vista tanto teórico como experimental. Para ello se estudiarán diversos entornos de operación introduciendo parámetros relativos al tráfico así como medidas obtenidas en los radioenlaces. Se propondrá un algoritmo de decisión que permitirá una integración óptima de una gestión de claves que se verá con detalle en el capitulo cinco. Finalmente, se incluirán diversos resultados y conclusiones.

3.2 Algoritmo de decisión del handover entre celdas

El sistema de gestión de una red como UMTS se organiza en varias áreas, configuración, prestaciones, alarmas, tarificación y seguridad. Un sistema ideal debería tratar todo el sistema de la forma más interrelacionada posible de manera que se puedan optimizar todos los mecanismos de gestión de la red. Por lo tanto, la información útil para el algoritmo de gestión del handover procederá tanto de la red como del mismo terminal móvil o MCPN. En determinados casos, el móvil puede ser lo suficientemente inteligente como para preprogramar una ruta, o al menos proporcionar una dirección de movimiento al centro gestor del sistema.

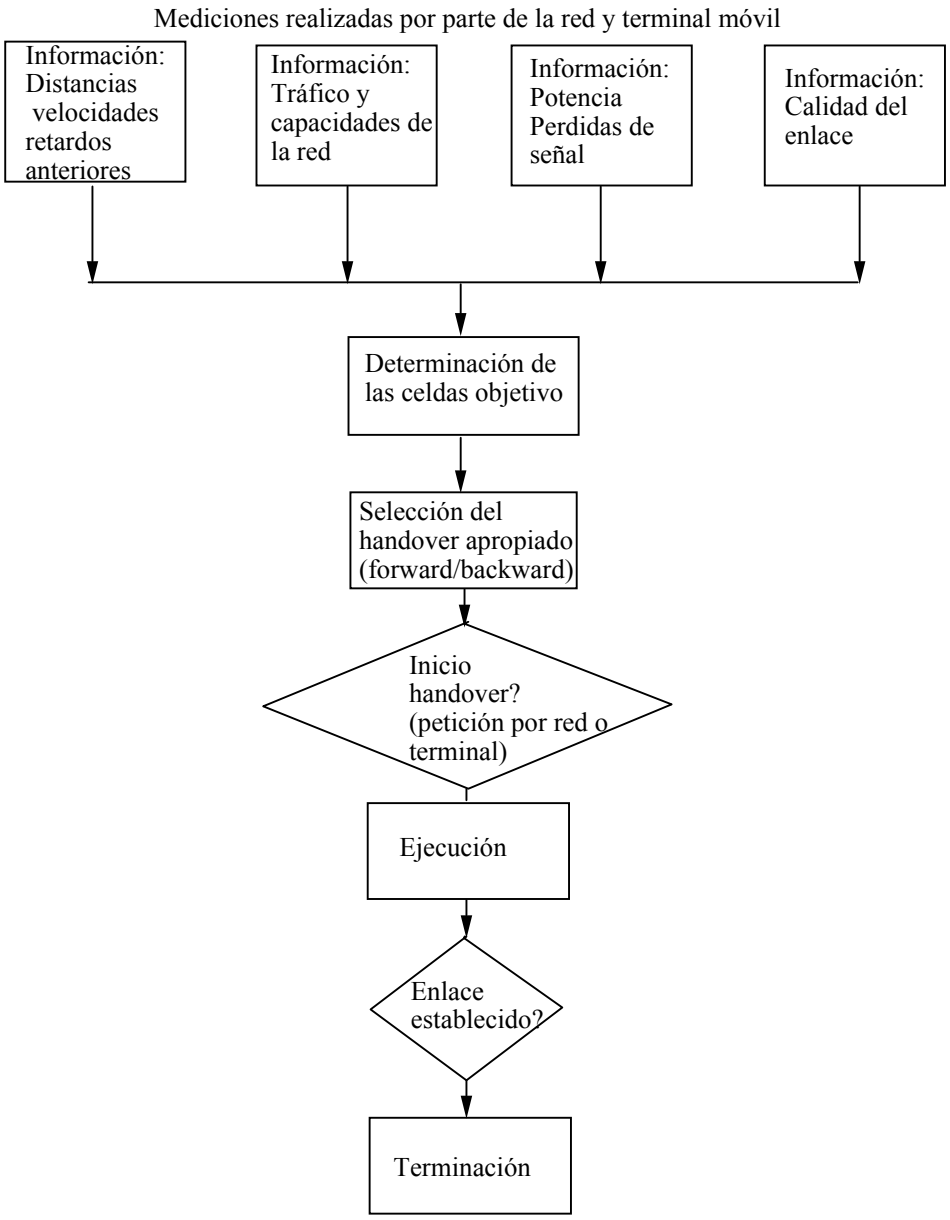


Fig. 3.1 Esquema de las fases de decisión y ejecución en un handover.

El caso más crítico, donde es de dificil aplicación una gestión adecuada del handover, ocurre cuando el móvil (bien sea MCPN o un único terminal móvil) se desplaza rápidamente entre celdas provocando numerosos handovers entre diferentes entornos de red y sin una ruta predeterminada. En el caso habitual, las MCPN, sean trenes, aviones o coches inteligentes (Intelligent Vehicle Highway Systems, IVHS) recorren caminos conocidos de antemano o que al menos el sistema de gestión de la MCPN reconoce. Es en esos casos cuando la gestión de claves en un handover invocado por red inteligente puede obtener los mejores resultados.

En nuestro caso, con el objetivo de optimizar el handover, el algoritmo de decisión parte de una serie de mediciones que constituyen una serie de parámetros relativos al control de potencia o señal, posición y de parámetros de entrada relacionados con el tráfico. Mediante un algoritmo de selección de celdas y la información obtenida anteriormente el sistema permite discriminar formando una lista de celdas candidatas en que celda el handover es más óptimo. De manera simultánea, tanto el terminal móvil como las entidades de la red fija deciden periódicamente sobre la conveniencia de realizar un handover supervisando en cada momento la situación del terminal móvil en la celda siguiendo un determinado algoritmo de ejecución. A continuación, se define con detalle la base de este algoritmo de decisión.

3.2.1 Parámetros de entrada al algoritmo de decisión de handover

Las mediciones se realizan tanto por parte del terminal móvil como por parte de la red. Los parámetros obtenidos son utilizados como entrada al algoritmo de decisión del handover. A continuación se especifican los parámetros relacionados con el radioenlace que son intercambiados entre el terminal móvil y la red.

a) Parámetros radio

El terminal móvil realiza de forma periódica medidas en la parte del radioenlace y las envia a la estación base. Las principales medidas son del tipo:

- **RSSI:** Intensidad de la señal recibida
- **BER:** Bit error rate (o bien relación señal-ruido)
- Balance de potencias entre celdas y terminal móvil

Estas medidas también se realizan sobre los diferentes radioenlaces de las estaciones vecinas. Por otra parte, los parámetros anteriores tienen que transmitirse a alta frecuencia ya que su variación es rápida y permiten invocar el algoritmo de ejecución de handover.

Otros parámetros de interés que forman la base del algoritmo de decisión son, por ejemplo, la distancia actual entre la estación base y el terminal móvil (distancia MT-BTS) y la potencia transmitida por la estación base **Pot_BTS_max**, parámetro que es distribuido por ésta

periódicamente. La **Pot_BTS_max** es medida en el canal de broadcast (BCCH) de cada estación base. Esto es porque el BCCH se transmite con una potencia casi constante y este canal puede ser sintonizado por todos los terminales móviles, incluso por los que no corresponden a la celda. Los siguientes parámetros se utilizan en el algoritmo de decisión y no requieren de un procesado tan rápido:

- **Tipo_celda.**
- **Id_celda.**
- **Id_LAI.**
- **Identificadores** de las BTS adyacentes.
- **Pot_MT_max**: Potencia máxima disponible por un terminal móvil en un canal de tráfico.
- **Pot_BTS_max:** Potencia máxima de emisión de la BTS (30 dBm).
- **Nivel_per**: Máximo valor de pérdidas aceptable por una celda (por debajo de la cual, una celda adyacente es considerada una celda candidata (120 dB)).
- **Nivel_per_hist**: Nivel de histéresis para extender el margen de pérdida en el enlace (5 Db).
- **Margen_HA**: Margen de handover que es la ventana de histéresis programada para cada par de celdas (actual y adyacente) (15 dB).
- **HA**: Diferencia entre la potencia de radiofrecuencia permitida máxima en el enlace de bajada y la potencia debida al control de potencia de la estación base (la real).
- **RXLEV:** Nivel de señal recibida asignada en la portadora BCCH.
- **RSSI_min:** RSSI mínima tolerable (sensibilidad del receptor) (- 97 dBm).
- **NBTSp**: Clave pública de la nueva estación base.
- **Dis_MT_BTS:** Distancia de activación (máxima distancia permisible entre un terminal móvil y su estación base).
- **DBTSact, DBTSady:** Distancia del MT a las BTS actual y adyacente (dirección).

Nota: En paréntesis se han especificado los valores tomados como referencia en los cálculos realizados para la evaluación del handover.

Diversos autores han estudiado el impacto que supone el conocimiento de la velocidad del terminal móvil en la determinación de la celda candidata para el handover. Sin embargo, dado que su conocimiento no siempre es posible y su determinación puede ser compleja, en nuestro algoritmo no se tendrá en cuenta.

b) Parámetros de tráfico

La red mide distintos parámetros de tráfico. Cada estación base distribuye algunos de éstos como por ejemplo, la capacidad disponible, que es el máximo bit - rate de un enlace que la estación base puede asignar a un handover entrante. La estación móvil utiliza estos

parámetros cuando determina la estación base objetivo hacia la cual intenta el handover. Además de estos parámetros locales, la red mide parámetros de tráfico globales:

- Carga de tráfico ofrecida por celda.
- Densidad de terminales móviles.
- Capacidad de los canales de reserva asignados a establecimiento de llamada o a handover.
- Posibilidad de buffers para contener ráfagas de peticiones.
- Gestión de configuación de número de canales disponibles en celdas.

Por otra parte, el terminal móvil también realiza mediciones propias para la toma de decisión en la activación de handover, tales como la:

- Capacidad_requerida: Capacidad necesaria para mantener el servicio en un enlace en particular.

Las medidas de tráfico son utilizadas además de las medidas de radio (realizadas por ambos, terminal móvil y estación base) para ajustar los parámetros de trabajo del terminal móvil usados en el criterio de decisión.

3.2.2 Distribución de información en el handover

A causa de los requerimientos de retardo en UMTS, especialmente en entornos de microceldas, la elección de las celdas candidatas sería realizada durante la fase de decisión, antes de que el proceso de handover empiece. En principio, tanto la red como el terminal móvil pueden activar un handover basándose en los parámetros intercambiados y en las celdas candidatas adyacentes.

Cada terminal móvil tendrá almacenada información acerca de la idoneidad de cada celda para activar el handover mediante el intercambio con la red del vector Tj, (H1,...,Hn) donde cada Hi da información de cada celda como candidata. Cada función Hi es a su vez la recopilación de las funciones fi, vectores (f1,...,fn) que particularizan los diversos efectos, tráfico, atenuación, distancia, etc de cada celda sobre el terminal móvil (j). Es decir:

- Tj = (H1, H2,...,Hn): Función asociada al terminal en relación a las celdas candidatas en el handover.
- Hi = (f1i,...,f7i): Función que determina la idoneidad de cada celda (i) como candidata a handover para un determinado terminal móvil (j). Incluye la función FHAi además de otros parámetros de gestión.

Las entidades de la red que intervienen en la gestión inteligente de handovers pueden pertenecer a la red de acceso, a la red fija o a ambas. En principio, no se establecerá ninguna distinción entre ambos entornos al considerar el sistema de gestión distribuido.

En la Fig. 3.2 se muestra una distribución de posibles celdas en las que se puede realizar un traspaso con respecto a una celda origen (situación del móvil, i=1). En principio, se admite la posibilidad de conocer la ruta hasta una celda destino (i=8), priorizando los posibles handovers que hubieran en esa dirección. En las figuras 3.3 y 3.4 se muestran otros esquemas en los que se determina el tipo de información que condiciona la activación inteligente o no en base a la selección de las celdas candidatas por parte de la red.

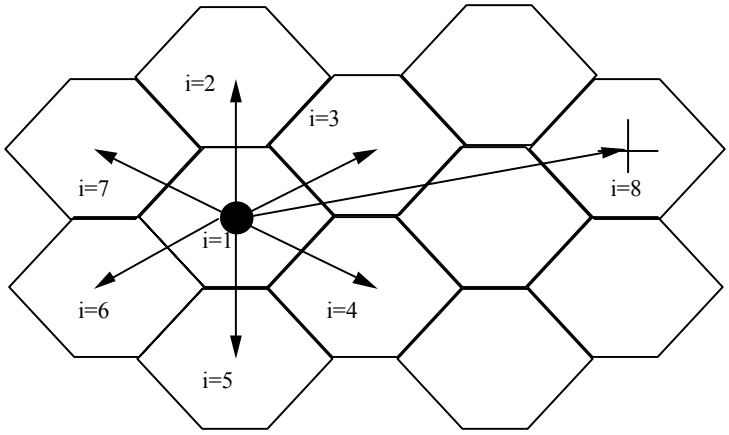


Fig. 3.2 Distribución de las celdas candidatas en torno a un terminal móvil (j) o MCPN en la celda i=1.

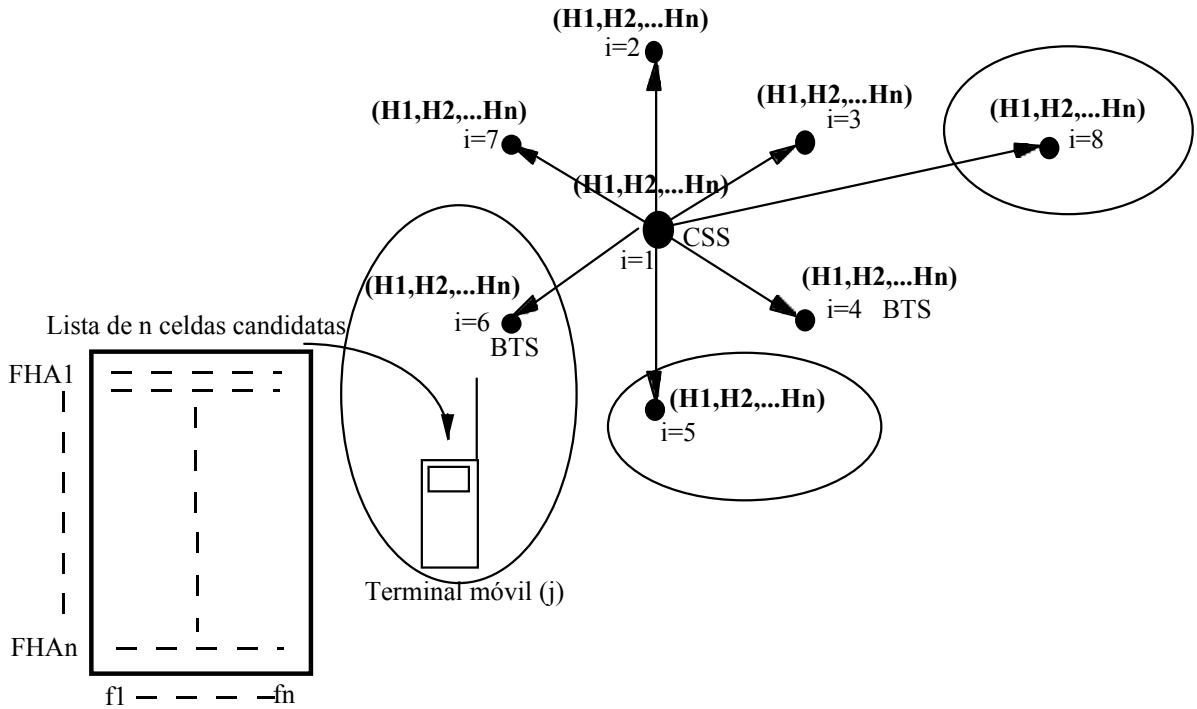


Fig. 3.3 Esquema simplificado de distribución de las funciones H intercambiadas entre las CSS de la red fija y los terminales móviles (j) para la determinación de las celdas candidatas en un handover inteligente.

En la red de acceso, las entidades de control que realizan mediciones y procesan información de gestión de la red para el handover son la MSCP(LE) y MSCP(CSS) y en la red fija el MSCP(TX). En general, las mediciones se establecen sobre un determinado nivel de señal (calidad de servicio) del terminal móvil. Cuando se produce un descenso en el nivel de potencia recibido, por razones del movimiento o alteraciones en el radioenlace, será preciso actuar antes de que este se deteriore excesivamente activando la ejecución de un handover.

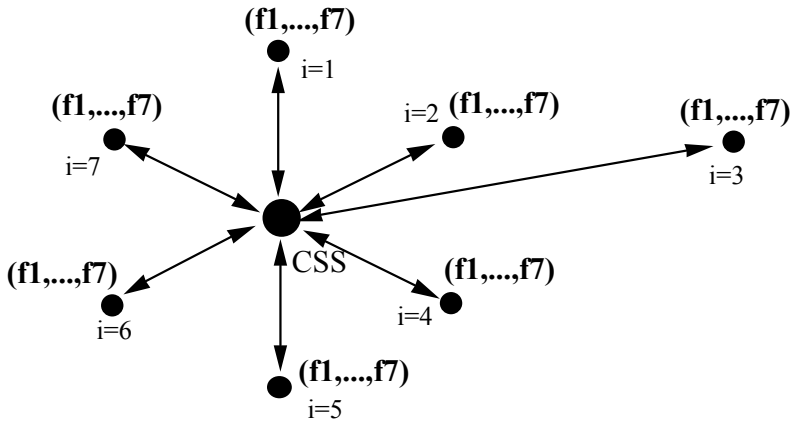


Fig. 3.4 Esquema simplificado del intercambio de información (fi) entre las CSS de la red fija y los terminales móviles para la determinación de cada celda candidata.

3.2.3 Periodos de medición en el handover

Se dispone de dos grupos de parámetros como resultado de las mediciones efectuadas en el sistema. Un grupo reducido de parámetros, distribuidos a una frecuencia mayor corresponden a la fase de ejecución del handover, mientras que otro grupo, de distribución más lenta son los que activan la selección de celdas candidatas. Se definen los siguientes términos:

Tmt: Periodo entre mediciones para la ejecución.
Tst: Periodo entre selección de mediciones para la ejecución.
Tmc: Periodo entre mediciones para las celdas candidatas.
Tsc: Periodo entre mediciones para la selección de celdas candidatas.

De forma que antes de seleccionar una celda o activar el handover, se realiza una acumulación de medidas a fin de obtener con mayor precisión los parámetros de entrada al algoritmo:

$Tst = m * Tmt$
$Tsc = n * Tmc$

siendo m y n el número de medidas realizadas en cada parámetro temporal.

Por otra parte, la frecuencia de aparición de desvanecimientos en entornos de microceldas/picoceldas limita en buena parte la frecuencia de emisión de parámetros y mediciones requeridos para la evaluación e invocación del handover. De este modo, sería recomendable que el periodo de medición (Tmt) para los parámetros de evolución rápida del handover que directamente afectan a la invocación del handover no fuera superior a los 100 ms. La frecuencia en las mediciones de los parámetros que afectan a la selección de celdas candidatas es de evolución más lenta proponiéndose como mínimo de 1 segundo.

A continuación, se describen los requerimientos del handover según el tipo de celda:

Entorno: picocelda
Radio celda: 20 m
Velocidad media o máxima del MT: 10 Km/h
Distancia para un área de solape de 10%: 2 m (sombra)
Máximo tiempo para cubrir el área de solape: 720 msec
Tiempo de finalización del handover: < 100 ms

Entorno: microcelda
Radio celda: 200 m
Velocidad media o máxima del MT: 50 Km/h a 200 Km/h
Distancia para un área de solape de 10%: 20 m (NLOS)
Máximo tiempo para cubrir el área de solape: 360 msec
Tiempo de finalización del handover: < 100 ms

Entorno: macrocelda
Radio celda: 10 Km
Velocidad media o máxima del MT: 50 Km/h a 500 Km/h
Distancia para un área de solape de 10%: 1 Km (LOS)
Máximo tiempo para cubrir el área de solape: 7'2 s
Tiempo de finalización del handover: < 500 ms

Se observa que el paso de micro a microceldas podría exigir un paso intermedio a celda paraguas en el caso de no cumplirse los requisitos de velocidad exigidos en el handover. Debido a estas exigencias se habla de dos tipos de handover, lento (para handover con retardo menor de 0'5 seg. caso LOS) y rápido (para handover con retardo menor de 0'1 seg. caso NLOS).

Además, se requiere de técnicas PRMA como método de acceso para compensar los rápidos decaimientos de señal en enlaces NLOS debidos a los efectos de sombras provocados en las esquinas de calles al transitar los terminales móviles en ángulo recto (>20 db en pocos metros).

Para determinar los promedios de mediciones para el handover entre micro o pico celdas ha de considerarse, en primer lugar, que éstas deben ser disponibles antes que cualquier desvanecimiento. Además, deben de ser suficientes para filtrar desvanecimientos del tipo Rayleigh. En entornos de micro o pico celdas, se sugiere una distancia promedio equivalente a 5 longitudes de onda, que corresponde a 80 cm para 1900 Mhz. Asumiendo una velocidad de 10 m/s (real en coches para entornos urbanos) la ventana promedio para realizar el handover no sería mayor que 80 ms por lo que se consideran límites de unos 100 ms.

Para el caso de macroceldas, la situación de desvanecimientos no suele ser tan forzada con lo que se aceptan retardos para el handover de hasta medio segundo.

Por tanto, debido al área de solape entre celdas en los casos más críticos, se puede definir un Tst de unos 300 ms, con lo que el número de mediciones m para la activación de un handover sería aproximadamente de 3 (en GSM, el FACCH actua cada 57 ms, con lo que m sería aproximadamente igual a 6). Además, debe cumplirse que para una determinada longitud de trama (d), un número determinado de celdas detectadas (x) y (m1) medidas por trama:

(m*d*x)/m1 da lugar a determinar aproximadamente Tst
(d*x)/m1 ha de ser mayor que Tmt
cumpliéndose para unas longitudes de trama de 10 ms (UMTS), m1 = 1 medidas por trama y unas 10 celdas detectadas por el móvil.

Por otra parte, para la selección de celdas candidatas, si se tiene en cuenta que el área de solape en una microcelda es de unos 20 m y la velocidad máxima autorizada de un móvil en ciudad es de unos 50 Km/h (15 m/s), en un segundo el móvil podría cambiar de celda. Aún así, se considera que el mayor número de usuarios de las microceldas serán peatones. Por ello, el periodo de selección de celdas candidatas y las mediciones deben cumplir que:

1 < Tsc < 3 segundos
0.3 < Tmc < 1 segundos
siendo n aproximadamente igual a 3.

Se pretende que la frecuencia de selección sea variable ya que requiere de determinados cálculos por parte de la red así como de la intervención de importantes recursos de ésta. Dado

que no todos los terminales móviles se están moviendo en un determinado momento y no requieren de handovers ni de la selección de celdas.

3.3 Arquitectura de control en el handover

Dentro de cada componente del sistema UMTS en el cual intervienen funciones relacionadas con el handover (p.e. BTS, CSS, MT), existen entidades funcionales de control [RACE30]. Entre éstas, se destacan las siguientes:

Controlador de enlace (LC):
Es la entidad funcional asociada con cada enlace de la llamada, y consiste de un controlador de portadora por cada servicio portador de llamada. Según cada tipo de servicio, se especifican un conjunto de modos de transporte para tener los requerimientos de calidad adecuados a las diversas condiciones de propagación e interferencia en el radioenlace.

Asignador de recursos (RA):
Esta entidad se asocia a cada estación base para modelar el control de admisión, la asignación de canales a los portadores, y cualquier retardo asociado debido a colisiones o a colas de espera para peticiones.

Controlador de enrutado (RC):
Es responsable de la función de handover, se asocia a cada llamada y a cada móvil. Se estudia con mayor detalle a continuación.

Controlador de tráfico (TC):
Entidad responsable de establecer, liberar las llamadas y monitorizar la calidad de la llamada en su totalidad.

Control del sistema (SC):
Entidad de control a nivel superior que gestiona las diversas funciones de movilidad.

Centro de autentificación (CAu):
El CAu es el centro que gestiona las autentificaciones (mutuas) del terminal móvil con el operador de red, así como determinada gestión de claves. Se deja para otros apartados un estudio más detallado.

3.3.1 Funciones del controlador de enrutado

El controlador de enrutado tiene dos funciones básicas: proporcionar macrodiversidad, caso de que esta funcionalidad esté disponible en el sistema y procesar handovers.

Cuando se proporciona macrodiversidad en el sistema, el handover sólo constituye una subfunción de la función de macrodiversidad. Los mecanismos para proporcionar macrodiversidad y handovers en el sistema son muy similares.

Se analizan los diferentes tipos de handover (HA) según estén realizados con procedimientos 'forward' o 'backward'. Así como los mensajes enviados en cada tipo de procedimiento. Para ello se hará uso de un modelo de sistema simplificado correspondiente al controlador de enrutado (RC).

En el controlador de enrutado, se pueden identificar las siguientes funciones para el control de macrodiversidad y para el handover (decisión y ejecución):

Evaluación de mediciones (ME):
Función que se encarga de recoger las mediciones distribuidas por el LC y determinar que BTS monitorizar.

Control de decisiones del handover (HDC):
Función que determina los enlaces y/o celdas objetivo y qué procedimiento de handover usar.

Ejecución del handover (HE):
Función que procesa los handovers, principalmente con el establecimiento de un nuevo enlace.

Terminación del handover (HT):
Función que se invoca cuando tiene que liberarse un enlace.

Ajuste de criterios del handover (HCA):
Función que permite la adaptación de un criterio de decisión según el entorno de radio y las condiciones de carga de tráfico.

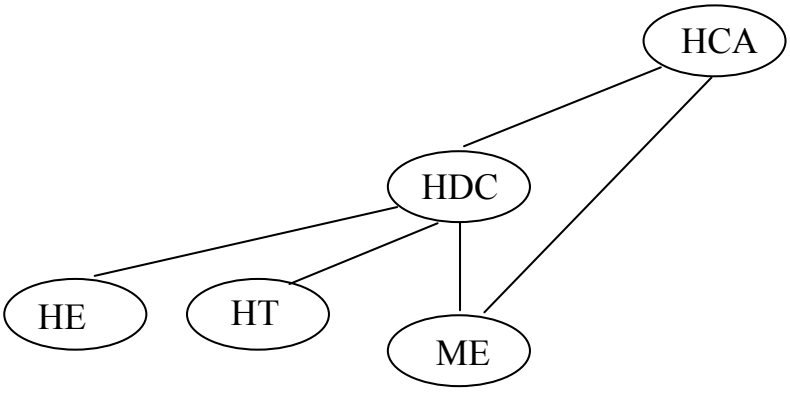


Fig. 3.5 Arquitectura interna del controlador de enrutado.

Los mensajes se intercambiarán principalmente entre el RC y otros grupos lógicos tales como el de asignación de recursos, controladores de enlaces o bien controladores de trafico.

Como ya se ha definido anteriormente, el proceso de handover puede dividirse en dos fases bien diferenciadas: decisión y ejecución.

En la fase de decisión, tanto el terminal móvil como los diversos componentes de la red analizan el 'status' del sistema (tráfico, niveles de señal, ...) y toman una decisión acerca de la necesidad de invocar un determinado tipo de handover (HA) y seleccionan: los enlaces y la celda objetivo, el procedimiento de handover apropiado (forward o backward) y el instante de comienzo del handover. Los intercambios de información utilizan las entidades funcionales descritas y las que se recogen a continuación con más detalle. Es importante hacer una descripción de éstas para poder plantear un protocolo de handover completo.

Como se verá más adelante, en la fase de ejecución se utilizará mayoritariamente el forward handover, reservándose el procedimiento backward para handovers entre operadores de red distintos. El forward handover se ejecuta inicialmente por parte del terminal movil, mientras que en el backward handover, es la anterior estación base la que toma la iniciativa. Se decriben a continuación, las entidades funcionales definidas en ambas partes.

Notación utilizada:

Prefijos: N relativo a componentes de la red fija (CSS)
M relativo a terminal móvil
BTSn para el número de estación base (n).

LC: Controlador de enlaces
RA: Asignación de recursos
RC: Control de enrutado
- Control de decisiones del handover (HDC)
- Ejecución del handover (HE)
- Terminación del handover (HT)
- Ajuste de criterios del handover (HCA)
- Evaluación de mediciones (ME)

TC: Controlador de tráfico

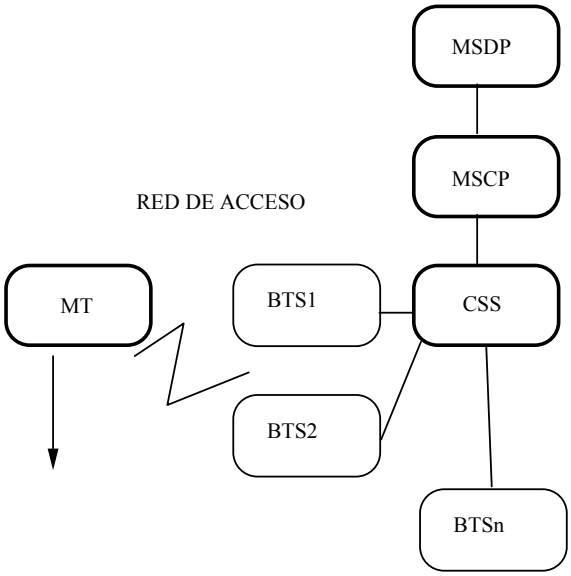


Fig. 3.6 Esquema de un handover con n celdas candidatas.

3.3.2 Funciones del controlador de enrutado en el terminal móvil

Dentro del terminal móvil, la entidad que está más relacionada con el handover es el controlador de enrutado. En este controlador, pueden distinguirse las siguientes funciones.

Evaluación de mediciones (MME):

El objetivo de la función MME es evaluar la calidad de la señal en todos los enlaces (actuales y los correspondientes a BTS adyacentes). La valoración del 'status' de los enlaces y la comparación respecto a determinados niveles y diversos criterios de handover, permite decidir una acción de handover e invocar un comando al MHDC. Los datos procedentes de medidas de radio se supone que son procesados en el LC. Las subfunciones MME son las siguientes:

a) Recepción de mediciones de radio y otros datos por parte de los enlaces de señalización (BCCH) de la actual BTS y de las celdas adyacentes (desde el grupo funcional del controlador de enlace, MLC, que hace estas medidas) a través de los mensajes M2a y M2c y a la entidad MME con M3a y M3b.

b) Distribución de datos de radio procesados a las funciones MHCA (mensaje M5a) y NME (mensajes M4a, M4b).

c) Transmisión de datos de radio procesados a la función MHDC (mensaje M5b) (opcionalmente de forma periódica).

d) Transmisión al LC por parte del RC de la identificación de las BTS a ser monitorizadas (M1). Concretamente, el resultado de la incorporación y desincorporación de las BTS a ser monitorizadas.

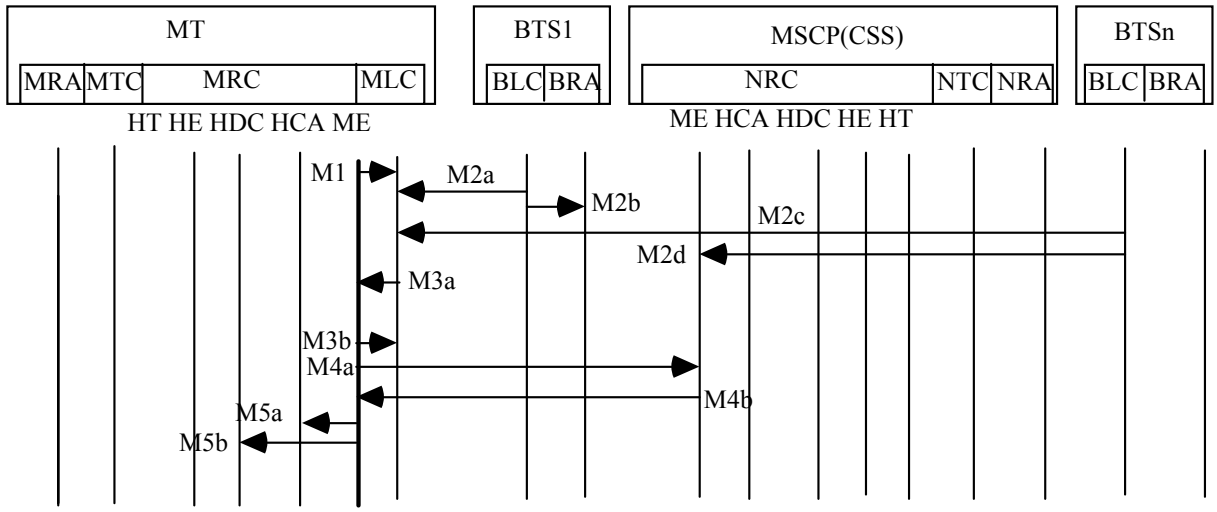


Fig. 3.7 Esquema de los mensajes que interactuan con la MME.

En definitiva, hay una distribución por parte del LC de datos procesados y resultados de mediciones a: MHCA, NME y MHDC.

Control de decisiones del handover (MHDC):

La función MHDC se procesa en paralelo a la función MME. Cuando la función MME ha detectado una función de handover o cuando se recibe un comando de handover por parte de la red, se inicia un handover (en caso de handover directo desde la red). Generalmente la función MHDC se encarga de las siguientes funciones (procedimientos P7 y P9):

- Determinar los enlaces y/o celdas objetivo hacia las cuales se activa un handover.
- Escoger, de acuerdo a un criterio definido, qué procedimiento de handover usar.
- Decidir cuando invocar la acción de handover.

Subfunciones incluidas en el MHDC:

a) Recepción de instrucciones de handover de operaciones y mantenimiento con origen en la red. Se incluyen los parámetros de trabajo enviados desde el Control del Sistema via NHCA (mensaje M8a).

b) Recepción desde el LC de la lista de BTS preferidas (M5b).

c) Determinación de los enlaces y/o celdas destino de acuerdo a un algoritmo de decisión de handover basado en criterios de parámetros de tráfico y evaluación de radio (procedimiento P7).

d) Selección del procedimiento de handover apropiado (backward o forward) basado en los criterios definidos por el citado algoritmo (P7).

e) En caso de recibir desde el NRC un comando handover (caso de activación por red), la MHDC transmite la lista de celdas candidatas al NHDC (M10, M11b).

f) Caso de no activación por red, el MHDC decide la activación del handover según los criterios de activación definidos en el algoritmo de decisión y pasa a llamar a la función MHE (M11a).

g) Cuando se decide un handover, tanto por parte del terminal móvil como por parte de la red, se llama a la función MHE (M11a).

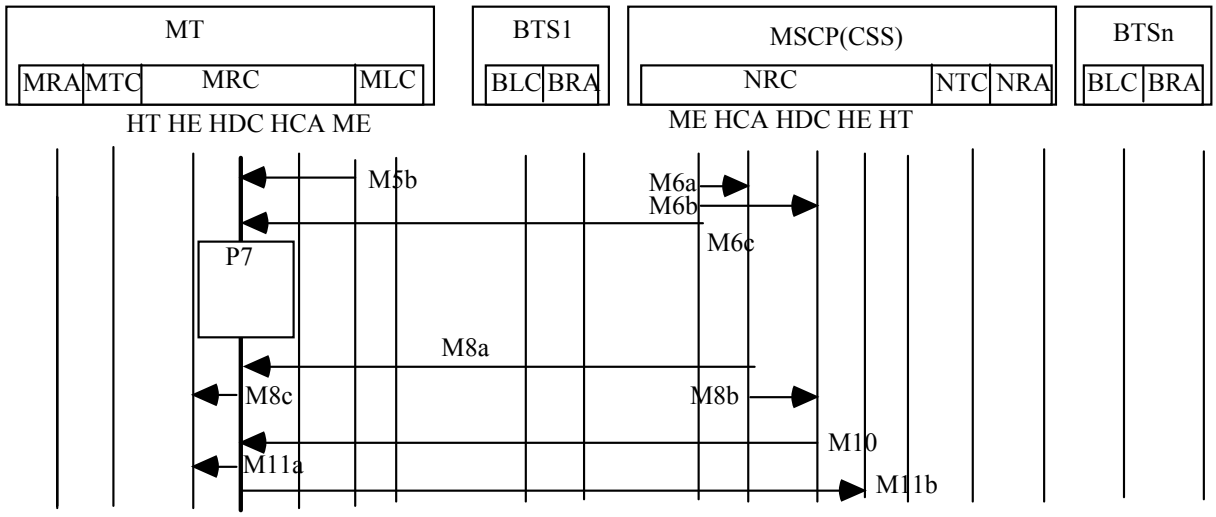


Fig. 3.8 Esquema de los mensajes que interactuan con la MHDC.

h) Cuando recibiendo un mensaje desde el MHE de reconocimiento de establecimiento de enlace, el MHDC llama al MHT.

i) Interacción con la función MHT para liberación de enlaces al final de un MHE, o cuando uno de los enlaces tiene que ser liberado (en una fase de macrodiversidad). Si no hay fase de macrodiversidad asumida en el handover, las funciones f) y g) son procesadas antes de llamar la función MHE.

Ejecución del handover (MHE):
Una vez se ha decidido la acción de handover por parte de la MHDC, se llama a la función de ejecución. Básicamente, se establece un nuevo enlace entre el MT y la parte de la red. Para hacer eso, el grupo funcional que controla el enrutado (RC) interacciona con el MLC. Las subfunciones del MHE son:

a) Transmisión de una petición de ejecución de handover junto con la información relevante concerniente a los nuevos enlaces y/o celdas en caso de que se decida usar un forward handover. Este mensaje se envia al NRC (M11b).

b) Establecimiento del nuevo enlace. Esta función invoca una comunicación punto a punto entre el MT y la red.

c) Enrutado de la información de usuario a los nuevos enlaces.

d) Transmisión de un mensaje de reconocimiento a la función MHDC cuando los nuevos enlaces se han establecido.

Terminación del handover (MHT):
Se distingue esta función de la función MHE para tener una arquitectura lo más independiente de si la macrodiversidad es operativa o no en el sistema. Esencialmente, esta función tiene que determinar que enlace liberar y cuando. La MHT se invoca por la función MHDC en la última fase del handover. Esta función, al igual que MHE, interactua con el grupo funcional LC.
Es de notar que cuando no se usa macrodiversidad, la función MHT se invoca antes que la función MHE. Se distinguen dos subfunciones en MHT:

a) Determinación del enlace a ser liberado. Esta acción está basada en la calidad, BER y demás criterios. Esta subfunción sólo actua cuando hay macrodiversidad.

b) Liberación del enlace determinado. Esta acción corresponde a la transmisión de un mensaje al grupo funcional LC.

Ajuste de criterios del handover (MHCA):
Define y mantiene las decisiones más apropiadas para la activación de un handover. El ajuste de los criterios se realiza permanentemente y de forma dinámica (P9). El ajuste puede realizarse por parte del terminal móvil o por parte de la red. Se identifican las siguientes subfunciones:

a) Obtener valores para los niveles de activación y para cada criterio de decisión de los MRC, de acuerdo a los contextos existentes. Estos valores son computados por el Control del Sistema y recibidos desde el NHCA.

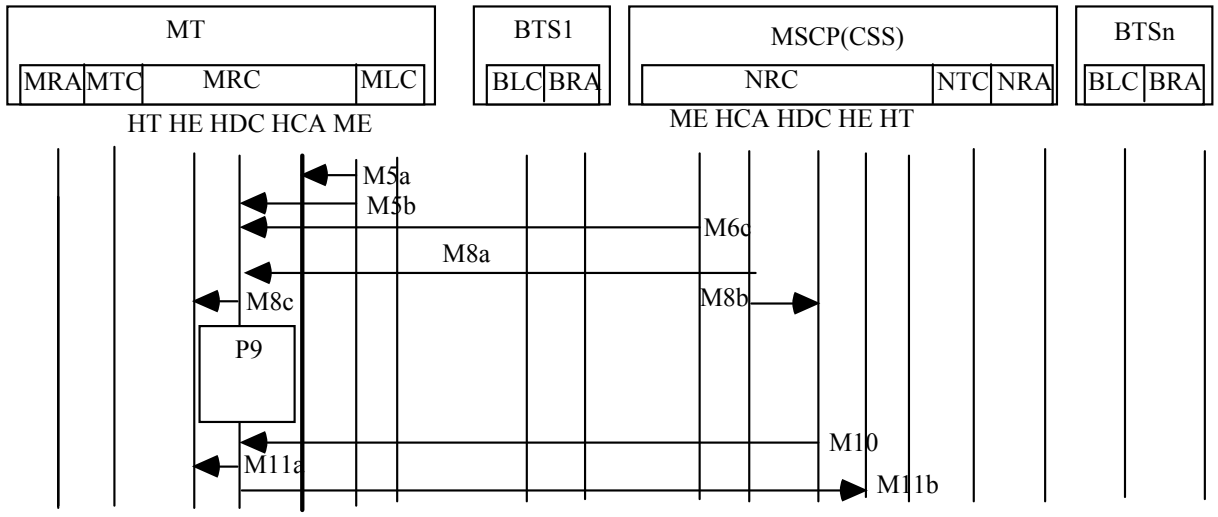


Fig. 3.9 Esquema de los mensajes que interactuan con la MHCA.

b) Selección de los criterios de decisión relevantes entre el conjunto de criterios programados de acuerdo al entorno de datos desde el MME (M5a). (p.e. si se trata de un handover entre macroceldas, se activa un criterio de distancias).

c) Transmisión de valores de niveles de disparo y criterios de decisión relevantes a HDC.

3.3.3 Funciones del controlador de enrutado de la red

Este tipo de funciones en la red, describen en general una estructura similar a la dispuesta en el terminal móvil.

Evaluación de mediciones (NME):

Las funciones NME básicamente, recogen datos procedentes del LC y los transmiten de forma periódica al MHDC y al HCA (en la parte de la red y del terminal móvil). Se pueden identificar las siguientes subfunciones:

a) Recepción de medidas de radio y otros datos recogidos de los enlaces de señalización existentes con el terminal móvil (desde el grupo funcional de controlador de enlaces) (M4a).

b) Distribución de datos de radio procesados a las funciones NHCA (M6a) y MME (M4b).

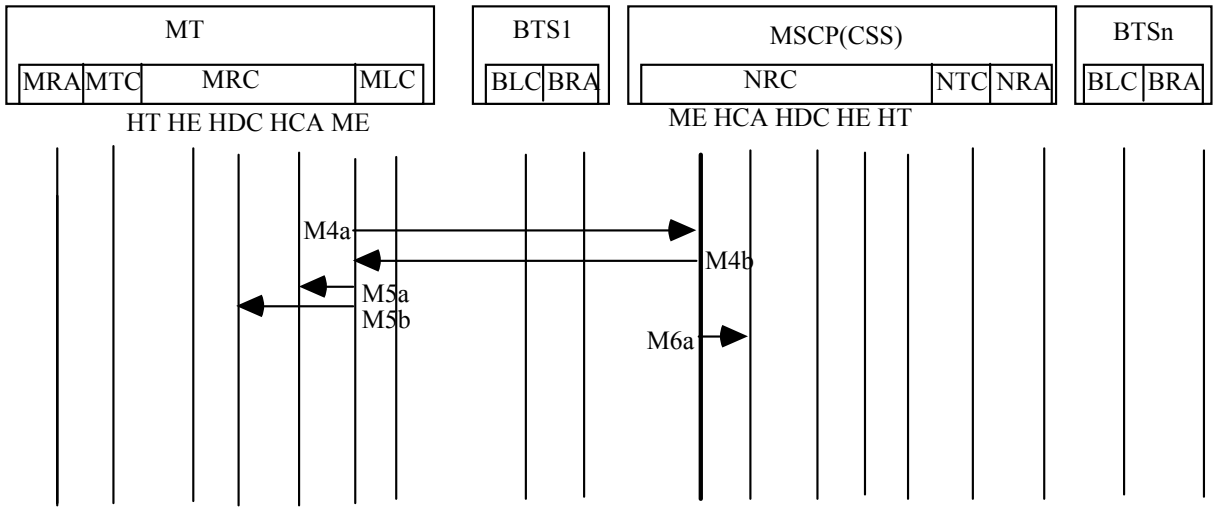


Fig. 3.10 Esquema de los mensajes que interactuan con la NME.

Control de decisiones del handover (NHDC):

En caso de forward handover, el control de decisión en el handover se deja al controlador de enrutado en el MT. El NHDC no tiene la responsabilidad para decidir qué enlaces o celdas escogería el MT.

En el caso de backward handover, el MHDC podría escoger la celda objetivo. Esto es, el NHDC tendrá que escoger, de acuerdo a la información de NTC sobre las características de transporte y según la información NRA acerca de los recursos disponibles, qué celda escoger. Estas informaciones sólo se requieren cuando tiene que iniciarse un handover por parte de la red. Por eso, NHDC interactua con NRA y NTC para conseguir esta información, y los criterios de decisión de los enlaces considerados como objetivos. Se pueden definir las siguietes subfunciones:

a) Recepción de instrucciones de handover de operaciones y mantenimiento con origen en la red. Se incluyen los parámetros de trabajo enviados desde el Control del Sistema via NHCA y MHCA (M8b).

b) El handover iniciado por la red puede activarse debido a efectos de gestión del sistema (p.e. uso de recursos del sistema y mantenimiento) o a efecto de los servicios. Si este es el caso, la NHDC pide del MHDC la lista de celdas candidatas y escoge entre ellas la más apropiada según las restricciones dispuestas por la red. Entonces, transmite la identificación de la celda candidata junto con el mensaje de comando handover al MHDC.

Además, como se pretende evitar el acceso a la red de terminales no autorizados que consuman recursos, la entidad NHDC, interactuando con NRA, prevendrá a los terminales móviles no autorizados de procesar handovers.

Ejecución del handover (NHE):
Su propósito es establecer un enlace cualquiera desde la red al interfaz aire (p.e. LC) cuando se inicia un backward handover, o desde el interfaz aire (p.e. LC) a la red cuando tiene que iniciarse un forward handover. Las funciones a definir son las siguientes:

a) Transmisión de una petición de ejecución de handover junto con la información relevante concerniente a los nuevos enlaces y/o celdas en caso de que se decida usar un backward handover. Este mensaje se envia a la BTS objetivo (para asignación de recursos) via la red (NRC) (M11a, M11b).

b) Transmisión de una petición de ejecución de handover junto con la información relevante concerniente a los nuevos enlaces y/o celdas en caso de que se decida usar un forward handover (M11a, M11b). Este mensaje se envia a la NRC una vez que el enlace se ha establecido entre MT y BTS.

c) Enrutado de la información de usuario a los nuevos enlaces.

d) Transmisión de un mensaje de reconocimiento a la función MHDC cuando se han establecido los nuevos enlaces.

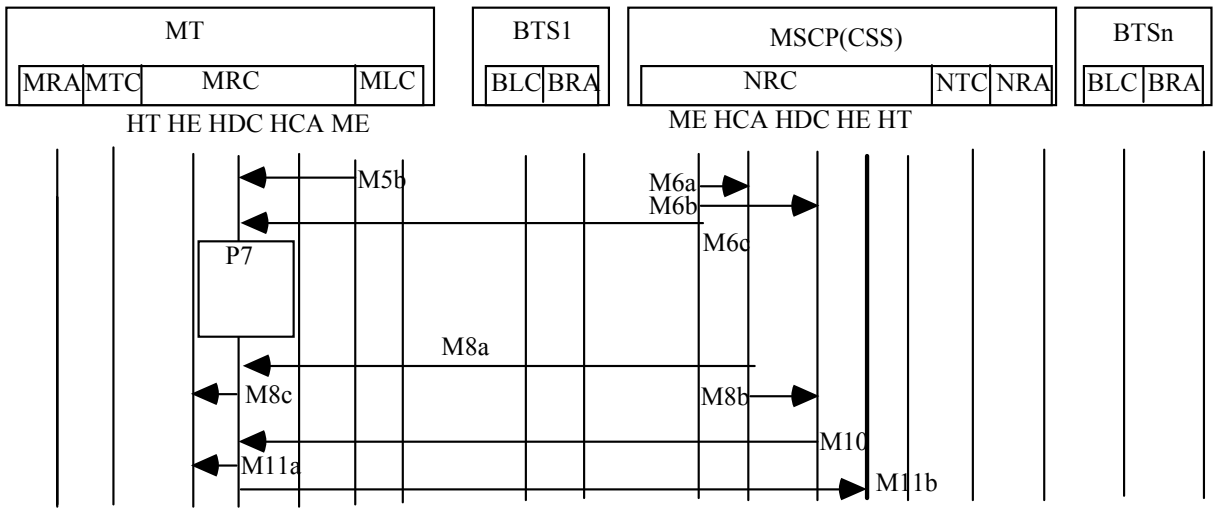


Fig. 3.11 Esquema de los mensajes que interactuan con la NHE.

Terminación del handover (NHT):
Esta función se activa cuando se recibe un mensaje al MT bien sea desde la red o via el radioenlace. Se definen las siguientes subfunciones:

a) Transmisión de un mensaje al grupo funcional NLC, de liberación de enlace (con identificación del enlace a liberar), cuando el mensaje de liberación de enlace ha sido enviado por el MT a través de la red (usando el radioenlace).

b) Transmisión de un mensaje a la red, de liberación de enlace cuando el mensaje de liberación de enlace ha sido enviado por el MT a través del radioenlace.

Ajuste de criterios del handover (NHCA):
Esta función recibe datos del Control del Sistema, MME, NME y MHCA. Envía a la función MHCA de un MT en particular los valores de activación del handover adecuados. Las subfunciones son las mismas que en el MT. El Control del Sistema es el proceso que recoge todos los datos de todos los lugares relevantes y los usa para ajustar los parámetros de trabajo del MT. Se identifican las siguientes subfunciones:

a) Obtener valores para los niveles de activación y para cada criterio de decisión de los NRC, de acuerdo a los contextos existentes. Estos valores se computan por parte del Control del Sistema y se reciben desde el MHCA.

b) Selección de los criterios de decisión relevantes entre el conjunto de criterios programados de acuerdo al entorno de datos desde el NME y MME. (p.e. si se trata de un handover entre macroceldas, se puede activar un criterio de distancias).

c) Transmisión de valores de niveles de disparo y criterios de decisión relevantes a HDC.

3.4 Fase de decisión

En esta fase, los mensajes intercambiados entre grupos funcionales antes de la ejecución del handover no dependen del procedimiento seleccionado (forward o backward). A continuación, se especifican los posibles 'status' de una BTS respecto a un terminal móvil:

a) BTS actual.
b) BTS monitorizada que está en la lista de BTS preferidas para la invocación del handover.
c) BTS monitorizada que no está en la lista de BTS preferidas para la invocación del handover.

d) BTS no monitorizada.

Si la BTS está en la situación a), b) ó c) envía periódicamente al MRC mediciones realizadas en el radioenlace así como otros tipos de datos a través del canal BCCH siendo siempre broadcast. En el caso a) también se activan el LCCHd, y si el TCH está activo, también se invoca el ACCHru. La mayor parte de los parámetros enviados por el BCCH en modo broadcast son en forma periódica y a baja frecuencia por tener variaciones lentas.

A continuación, se describen los procedimientos o funciones que tienen lugar en la fase de decisión de un handover, así como los mensajes intercambiados para la consecución de los mismos.

Función P1:
El MME envia al MLC la lista de celdas monitorizadas sin tener en cuenta todavía las celdas candidatas. Mensajes generados:

M1a: Tipo de canal: Interno del MT
Contenido: Lista de celdas monitorizadas (preferidas y no preferidas)

Función P2:
La actual BTS y la BTS monitorizada envian mediciones del radioenlace y otros datos recogidos al MT. Es en este procedimiento donde se envian las claves públicas de las nuevas estaciones base (NBTSp) a los terminales móviles, concretamente, en el mensaje M2c. En el MT, la información es distribuida por el canal BCCH al MLC. Se generan los siguientes mensajes:

M2a: Tipo de canal: BCCH de la actual BTS
LCCHd asociado con el MT y en caso de un TCH activo, su ACCHru asociado.
Contenido: Lista anterior de parámetros sobre la actual BTS
Calidad del TCH ascendente que es enviado en el ACCH ru
Distancia MT-BTS que es enviada en el LCCHd si la celda es una macrocelda.
M2b: Tipo de canal Dentro de la red fija.
Contenido: Envia la misma información que M2a desde la BLC de la actual BTS a la subfunción NME.
M2c: Tipo de canal: BCCH de una BTS genérica.
Contenido: Lista anterior de parámetros sobre las BTS adyacentes. Contiene la NBTSp.

M2d: Tipo de canal Dentro de la red fija.
Contenido: Misma información de M2c enviada desde BLC de una BTS genérica a NME.

Función P3:

El MLC distribuye continuamente al NME la información broadcast desde todas las BTS monitorizadas y medidas directamente en MLC, además, la información medida en MT es enviada a la red para tener la misma información en MRC y en NRC. Todos los datos después del procesado en el MRC se usan para el criterio de decisión del handover y determinación de las celdas candidatas. Mensajes generados:

M3a: Información de tráfico del radioenlace descendente. MLC envia la nueva información broadcast en el BCCH monitorizado al MME incluyendo todos los parámetros necesitados por el criterio de decisión HA y la determinación de las celdas candidatas.

Tipo de canal: Dentro del terminal móvil.

M3b: Información de mediciones del radioenlace ascendente. MME envia las mediciones del radioenlace al MLC.

Tipo de canal: MT interno
Contenido: Actualización de la información enviada en M1.

Función P4:

Las mediciones entre las entidades MME y NME se intercambian periódicamente. Se generan los siguientes mensajes:

M4a: Este mensaje permite ajustar a la red los parámetros de trabajo. MME envia las medidas de radio tomadas en el MLC al NME.

Tipo de canal: LCCHfu
Contenido: Calidad del enlace TCHd.
La RXLEV de la actual y las celdas vecinas (BCCHs) así como la subfunción NME tiene que tener la misma información almacenada en MME.

M4b: Este mensaje permite al MT procesar el procedimiento de decisión de handover.

Tipo de canal: ACCHru
Contenido: Calidad del enlace TCHu.

Función P5:

El MME envia los parámetros radio a la subfunción MHCA para seleccionar, de acuerdo a los datos del entorno, el criterio de decisión adecuado. Realmente la única posibilidad es excluir el criterio basado en la distancia entre el MT y la BTS en caso de entornos sin macroceldas. MME envia los parámetros de radio también al MHDC, esta subfunción es procesada en paralelo al MME. Los objetivos del MHDC son:

a) Testear si se precisa un procedimiento handover (Criterio de decisión handover)

b) Determinar el enlace objetivo (Determinación de la celda candidata)

c) Determinar que procedimiento usar (backward o forward)

Mensajes generados: (a diferentes frecuencias)

M5a: Medidas en el enlace de monitorización. La información es enviada de MME a MHCA

Tipo de canal: MRC interno

Contenido: Todas las mediciones de tráfico y radio que son recibidas en M3a.

M5b: Medidas en el enlace de monitorización. La información se envia desde el MME al MHDC.

Tipo de canal: MRC interno

Contenido: Mismo que en el M4a.

Función P6:

Se trata del proceso P5 descrito anteriormente pero que ocurre en el lado de la red, p.e. la subfunción NME envia datos acerca del entorno al NHCA y NHDC con diferentes frecuencias. Mensajes generados: (a diferentes frecuencias)

M6a: Medidas en el enlace de monitorización. La información es enviada de NME a NHCA

Tipo de canal: NRC interno

Contenido: Mismo que M5a.

M6b: Medidas en el enlace de monitorización. La información es enviada de NME a NHDC

Tipo de canal: NRC interno

Contenido: Mismo que M5a.

M6c: El NME envia este mensaje al MHDC cuando:

a) La calidad de comunicación en el enlace actual no se satisface según las mediciones efectuadas en el criterio de handover.

b) La calidad de uno (al menos) de los enlaces de comunicación vecinos es la adecuada despúes de comparar las mediciones del enlace con el criterio de handover.

Tipo de canal: LCCHfd

Contenido: Mismo que M3a.

Función P7:

La subfunción MHDC se activa y se procesa en paralelo con el MME. Cada vez que son distribuidos nuevos datos de radio (M4b), nuevos niveles de disparo o instrucciones de operación y mantenimiento en el handover, el MHDC ejecuta en paralelo los siguientes algoritmos:

- Algoritmo de decisión de handover
- La determinación de los enlaces y/o celdas objetivo entre el conjunto de celdas preferidas basados en determinados algoritmos.

Si se requiere de un handover, se pasa al P11, en caso contrario, si no se precisa ningún handover, el terminal móvil recibirá mediciones de radio y otros datos recogidos y se procederá a repetir los mensajes M2a, M2b, M2c y M2d empezando el proceso de P2 de nuevo.

Función P8:

Como se indica en el controlador de enrutamiento, el proceso P7 puede activarse cuando se sobrepasan los niveles de disparo y criterios de decisión del handover desde la NHCA. Cuando el NHCA recibe niveles de disparo renovados del control del sistema, se encarga de enviarlos al MHCA. Finalmente, el MHCA renueva al MHDC enviando los nuevos parámetros. Mensajes generados:

M8a: Información de niveles de disparo enviada desde NHCA a MHCA

Tipo de canal: LCCHfd de la actual BTS

M8b: Información de niveles de disparo enviada desde NHCA a NHDC

Tipo de canal: Dentro de la red fija

Contenido: Mismo que M8a.

M8c: La información de nuevos niveles de disparo y criterios de decisión seleccionados es enviada desde MHCA a MHDC

Tipo de canal: MRC interno

Contenido: Mismo que M8a.

Función P9:

Con el envio de nuevos datos de radio al MHDC (M8a), el MHDC, que está siempre activo, ejecuta el mismo proceso definido en P7, y se envian las nuevas listas de preferencias. Si se precisa un handover, se ejecuta el siguiente proceso P11, en caso contrario se retorna al P2.

Función P10:

Caso infrecuente de activación de handover por parte de la red. El comando de handover es transmitido al MRC cuando hay envios de gestión de sistema o envios de servicios. En este caso, la red escoge el enlace(s) y celda(s) objetivo y transmite sus identificaciones al MT. Mensajes generados:

M10: NHDC envia la identificación de la celda objetivo a MHDC y fuerza la ejecución del handover por la estación móvil.

Tipo de canal: LCCHfd

Contenido: Identificadores de enlace(s) y celda(s) objetivo.

Función P11:

Una vez que la acción de handover ha sido decidida por el MHDC, se llama a la subfunción MHE del MRC y se generan los siguientes mensajes:

M11a: El mensaje muestra la activación de MHE por parte del MHDC. En esta etapa el enlace o celda objetivo ya es conocido.

Tipo de canal: MRC interno

M11b: El mensaje muestra la activación de NHE por parte del MHDC. En esta etapa el enlace o celda objetivo ya es conocido.

Tipo de canal: LCCHfu

Notación:

Prefijos: N relativo a componentes de la red fija (CSS)
M relativo a terminal móvil
BTSn para el número de estación base (n).

LC: Controlador de enlaces
RA: Asignación de recursos
RC: Control de enrutado
- Evaluación de mediciones (ME)

- Control de decisiones del handover (HDC)
- Ejecución del handover (HE)
- Terminación del handover (HT)
- Ajuste de criterios del handover (HCA)

TC: Controlador de tráfico

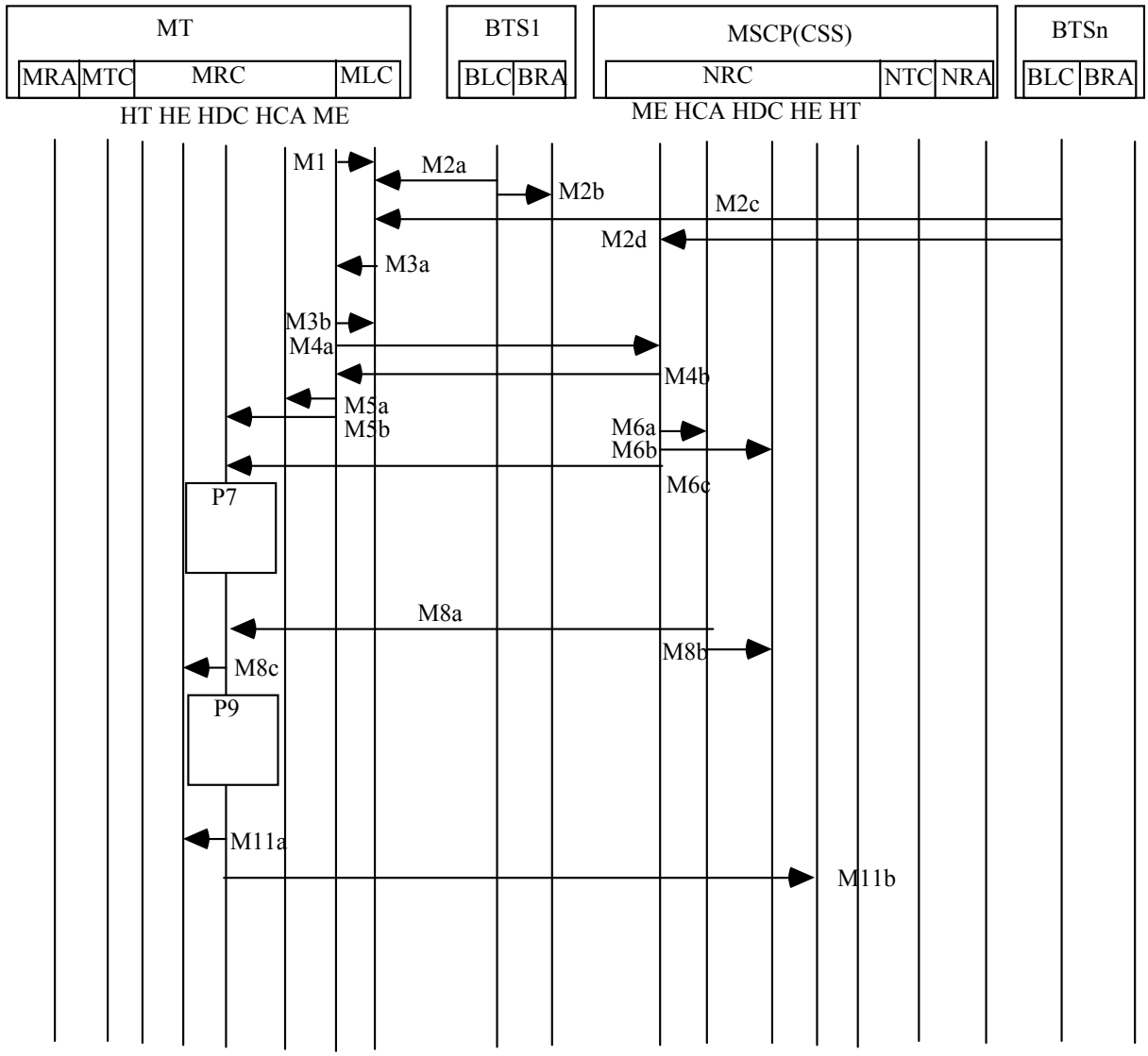


Fig. 3.12 Protocolo del forward handover donde la estacion móvil escoge la celda objetivo.

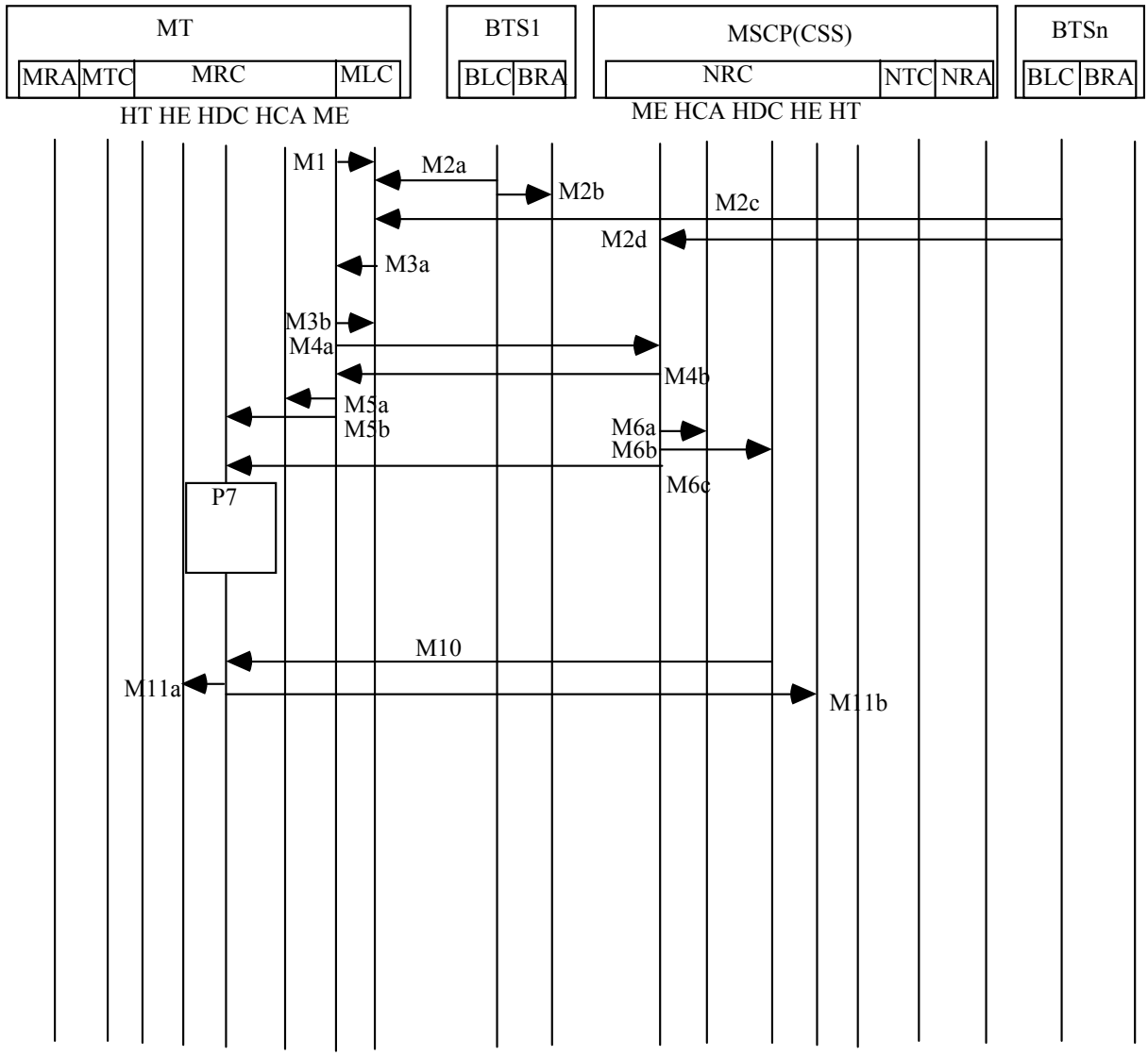


Fig. 3.13 Protocolo del forward handover donde la red escoge la celda objetivo.

3.5 Algoritmo para la determinación de las celdas candidatas

En la determinación de celdas candidatas se han obtenido expresiones que minimizan la probabilidad de bloqueo en una celda y se han medido las atenuaciones recibidas en el terminal móvil para proceder al handover, ya sea invocado por el terminal movil o bien por parte de la red. Sería pues conveniente disponer de una expresión en la que todos estos efectos se manifestaran conjuntamente. Por ello, se puede definir una función de handover FHAi, que mediante ciertas ponderaciones, permita gestionar la lista de celdas candidatas en el handover según el estado de la red. Para la determinación de la función que permita obtener estas celdas candidatas se escogen los siguientes criterios:

3.5.1 Condición de capacidad

Las celdas con mayor capacidad disponible (número de slots) tendrán prioridad para el handover. La función f1 relacionada con la capacidad disponible del sistema actuará de forma que se cumplan las condiciones siguientes:

Capacidad de la celda candidata (enlace ascendente) ≥ Capacidad requerida (enlace ascendente)
Capacidad de la celda candidata (enlace descendente) ≥ Capacidad requerida (enlace descendente)

Al comienzo del algoritmo, la probabilidad de bloqueo se estudia en cada celda. Esta probabilidad se obtiene por medio de los datos enviados por las BTS de acuerdo al número de canales disponibles, establecimientos de llamada y handovers procesados. Los resultados obtenidos son comparados con la capacidad asignada para cada celda. El parámetro usado será la probabilidad de bloqueo bien sea en el establecimiento de llamada o bien en el handover, que dependerá del tipo de gestión utilizado en la celda y de la movilidad del terminal.

PB: Probabilidad de bloqueo en el establecimiento de la llamada a la celda candidata.
Pfh: Probabilidad de bloqueo en el handover a la celda candidata.

f1 = (1 - PB) si el terminal móvil está estático o no ha realizado handovers previamente.
f1 = (1 - Pfh) si el terminal móvil está moviéndose, ha realizado handovers previamente o la celda candidata dispone de un tratamiento prioritario para peticiones de handover.

3.5.2 Distancia del terminal móvil a la estación base

En este caso, la distancia del terminal móvil respecto de la estación base actual tiene que ser mayor que la distancia respecto a la estación base de la celda candidata. Este parámetro es usado básicamente en entornos de macroceldas. Cada terminal móvil dispone de información referente a la distancia que utiliza para determinar la función f2.

DBTSact: Distancia desde el terminal móvil a la BTS actual.
DBTSady: Distancia desde el terminal móvil a la BTS candidata.
DIS_MT_BTSact, DIS_MT_BTSady: Distancia de activación (máxima distancia permisible entre un terminal móvil y su estación base).

$$f2 = \frac{\frac{DBTSact}{DIS\_MT\_BTSact}}{\frac{DBTSact}{DIS\_MT\_BTSact} + \frac{DBTSady}{DIS\_MT\_BTSady}}$$

3.5.3 Condición del mismo tipo de celda

El handover tendrá prioridad con las celdas del mismo tipo. En general, se puede asignar un parámetro relacionado con la prioridad a determinadas celdas en función de su mismo tipo. Se pueden distinguir los siguientes tipos de handover según el tamaño de la celda:

- macrocelda a macrocelda
- macrocelda a microcelda
- microcelda a macrocelda
- microcelda a microcelda
- outdoor celda a indoor celda
- indoor celda a outdoor celda

Los distintos tipos de celda hacen referencia a los siguientes diversos tipos de entornos:
1.- Áreas urbanas de alta densidad, servidas por macroceldas y microceldas
2.- Áreas urbanas de baja densidad, servidas por sólo macroceldas
3.- Áreas rurales, servidas por sólo macroceldas
4.- Carreteras principales y autopistas, servidas por microceldas con el soporte de celdas paraguas
5.- Entorno indoor, dividido en residencial y de negocios, servido por picoceldas.
6.- MCPNs

A continuación, se describen brévemente cada uno de los casos anteriores:

Handover Macro - Micro/Picoceldas

Este tipo de handover se produce generalmente cuando se pasa de un entorno con menor densidad de tráfico a uno de mayor densidad. Puede significar un cambio de red administrativa si bien también puede darse el caso de cambiar de entorno debido al movimiento del terminal móvil (p.e. como en el caso 4 de tipos de celdas del apartado anterior). En ambas situaciones, la gestión de red en base al tráfico y/o capacidades del sistema suele ser importante (p.e. celdas paraguas).

Handover Micro/Picoceldas - Macroceldas

Este tipo de handover se produce generalmente cuando se pasa de un entorno con mayor densidad de tráfico a uno de menor densidad. Se reproducen situaciones similares a la salida de ciudades, edificios, etc. No presenta especiales requerimientos de prestaciones o seguridad que no queden englobados en casos anteriores.

Handover entre CPNs

Handover entre distintos entornos administrativos (se sobreentiende CPNs complejas) y/o macroceldas de entornos públicos que además requieren de un control de acceso:

a) CPN a entorno público
b) CPN a MCPN
c) CPN a CPN
d) MCPN a entorno público
e) MCPN a CPN
f) MCPN a MCPN
g) Entorno público a CPN
h) Entorno público a MCPN

Se considera como ventajoso para el sistema, que terminales móviles con gran movilidad como los situados en coches, trenes, etc, tengan prioridad en las macroceldas, para evitar traspasos continuos, mientras que terminales utilizados por peatones, por tanto, con menor velocidad sean utilizados en microceldas y picoceldas. Se puede definir pues una función f3 que defina el acceso según el tipo de celda candidata.

	f3: **Celda candidata**		
Tipo de celda actual	Picocelda	Microcelda	Macrocelda
Picocelda	1	0.3	0.3
Microcelda	0.3	1	1
Macrocelda	0.3	0.6	1

Tabla 3.1 Valores que adopta la función f3 según los tipos de celda que intervienen en el handover.

3.5.4 Condición de pérdidas de camino mínimas

En este caso, el algoritmo planifica una probabilidad de corte considerando desvanecimientos de Rayleigh y/o pérdidas de tipo lognormal según cada escenario. Tienen prioridad las celdas con pérdidas menores en el radioenlace.

$P_{out}(r)$: Probabilidad de corte en la celda adyacente

$f4 = (1 - P_{out}(r))$

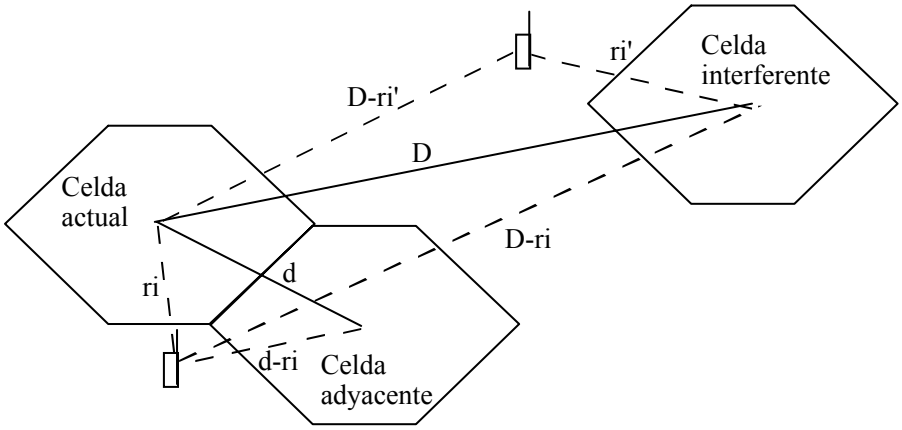


Fig. 3.14 Distancias vectoriales entre el terminal móvil y celdas adyacentes.

3.5.5 Balance de potencias

El sistema recibe periódicamente información de las estaciones base monitorizadas desde las cuales se determinan las estaciones base candidatas al handover. En el caso de que se trate de una estación base diferente de la actual, el sistema define una función f5 que trata de integrar la información obtenida a partir de cualquiera de los siguientes criterios.

(Mín (Max señal en el canal (celda actual), Potencia máxima) - Pérdidas en el radioenlace (celda actual) - Pérdidas permitidas) -
(Mín (Max señal en el canal (celda adyacente candidata), Potencia máxima) - Pérdidas en el radioenlace (celda adyacente candidata)) > 0

Se consideran las pérdidas en el radioenlace, como la diferencia entre la señal transmitida en la estación base respecto a la señal recibida en el terminal móvil.

Lady: Pérdidas debido a la celda candidata

Lact: Pérdidas debido a la celda actual

$$f5 = \frac{Lact}{Lact + Lady}$$

3.5.6 Función objetivo FHAi

La función FHAi que describe la selección de celdas candidatas en el handover puede definirse de la siguiente forma:

$$FHAi = (f1*K1 + f2*K2 + f3*K3 + f4*K4 + f5*K5)(1 + f6*K6 + f7*K7)$$

Siendo:

K1: Peso correspondiente al número de canales disponibles de la celda.

K2: Peso correspondiente a la distancia entre el terminal móvil y las celdas candidatas.

K3: Peso correspondiente al control de acceso o condición de mismo tipo de celda por parte de la red.

K4: Peso correspondiente a las pérdidas debidas a la señal recibida.

K5: Peso correspondiente a balances de potencia en el terminal móvil o MCPN.

K6: Peso correspondiente a la gestión del handover por acción manual en el terminal móvil.

K7: Peso correspondiente a la importancia de la gestión del handover por parte de la red.

Estos valores, en principio arbitrarios para cada red, deberian ser cuidadosamente ponderados por el operador de red (p.e. con la ayuda de un sistema experto que proporcionara esa información). En general, siempre que se cumpla la siguiente condición en la celda monitorizada, se obtiene una celda candidata:

FHAi > nivel de disparo => Celda candidata para la activación del handover.

Los valores de las funciones FHAi obtenidas se agrupan en forma de lista de celdas candidatas a fin de que la celda con una función FHAi más alta se seleccione como celda objetivo para el algoritmo de ejecución del handover. Al mismo tiempo, esta lista va renovándose periódicamente según se va recibiendo información de la red y del terminal móvil.

3.6 Determinación de las fi y ki relacionadas con la atenuación y los desvanecimientos de la señal en el radioenlace

Los modelos de propagación más usados comunmente utilizan tres componentes básicos para determinar la atenuación de la señal: desvanecimientos de Rayleigh, sombreado lognormal y

pérdidas debidas al camino dependientes de la distancia. Se utilizará la información que se obtiene de estos parámetros para ajustar las funciones fi y las ponderaciones Ki en la función FHAi definida previamente. Para hallar la atenuación de la señal respecto a la distancia en el radioenlace se parte de la formulación de [DP1] para señal directa y reflejada.

Una manera simplificada de expresar la potencia de señal que recibe el terminal móvil respecto a la señal emitida por la estación base es de la forma:

$$P_r = P_0\left(\frac{h_1 h_2}{r^2}\right)^2 = P_0 + 3\text{dB} - 40\log r$$

en donde, P_0 es la potencia de emisión, h son las alturas de las antenas en emisión y recepción y r es la distancia entre el terminal móvil y la estación base.

Se puede obtener una expresión de la atenuación en el radioenlace según:

$$E(r) = m(r) + G_\sigma$$

donde G_σ es una distribución log-normal con media 0 y desviación estandard σ dB.

m(r) es el nivel relativo normalizado a una distancia r = R (radio celda) y es de la forma:

$$m(r) = 10\log\left(\left(\frac{r}{R}\right)^{-\alpha}\right)$$

con α entre 3 y 4 y un valor de σ entre 6 y 7 dB para áreas urbanas.

3.6.1 Probabilidad de corte media

Para calcular la probabilidad de corte en una posición determinada, es necesario conocer las funciones de densidad de probabilidad de la potencia de la señal deseada y de las señales interferentes.

Dada la probabilidad de corte en cualquier zona dentro de una celda determinada, la probabilidad de corte media puede calcularse de la siguiente forma [KS1]:

$$Pc = \frac{\int_0^{2\pi}\int_0^{R_c(\theta)} rP_{out}(r,\theta)\,dr\,d\theta}{\int_0^{2\pi}\int_0^{R_c(\theta)} r\,dr\,d\theta}$$

donde P_{out} es la probabilidad de corte en un punto concreto dentro del área considerada y Pc es la probabilidad de corte media.

Sólo desvanecimientos de Rayleigh

Si únicamente influyen desvanecimientos de Rayleigh en la variación de la señal recibida, entonces, la probabilidad de corte es de la forma:

$$P_{out}(r) = 1 - \exp[-\gamma * \kappa * r^n]$$

siendo n el exponente de propagación (entre 3 y 4), γ la relación señal a ruido mínima y κ se obtiene a partir de $P_{out}(Rc)$.

La probabilidad de corte media resulta ser:

$$P_c = 1 - \frac{\sqrt{\pi}}{2} \frac{\operatorname{erf}\left[\sqrt{-\ln[1 - P_{out}(R_c)]}\right]}{\sqrt{-\ln[1 - P_{out}(R_c)]}}$$

Sólo sombreados lognormales

Si únicamente influyen sombreados de tipo lognormal en la variación de la señal recibida, entonces, la probabilidad de corte es de la forma:

$$P_c = P_{out}(R_c) - \frac{1}{2}\exp[b*(2a + b)]*\operatorname{erfc}[a + b]$$

donde

$$a = \frac{\alpha(R_C)}{\sqrt{2}\sigma}$$

$$b = \frac{\sqrt{2}\sigma \ln(10)}{10n}$$

siendo $\alpha(R_C)$ el margen en dB por el cual la media de la potencia de señal recibida excede el mínimo de potencia de señal requerida.

$$P_{out}(R_c) = \frac{1}{2}\operatorname{erfc}\left[\frac{\alpha(R_C)}{\sqrt{2}\sigma}\right]$$

Desvanecimientos lognormales y de Rayleigh.

En este caso, se valoran conjuntamente ambos tipos de desvanecimientos. La probabilidad de corte en función de la distancia entre el móvil y la estación base es de la forma:

$$P_{out}(r) = 1 - \frac{1}{\sqrt{\pi}}\int_{-\infty}^{+\infty} \exp(-y^2)\exp\left[-\frac{\pi}{4}\left[\frac{r}{R_C}\right]^n 10^{\frac{\left|-\left(\alpha(R_c)+\sqrt{2}\sigma y\right)\right|}{10}}\right]dy$$

Para el caso de hallar la probabilidad de corte media dentro del radio R_c de la estación base, se obtiene:

$$P_c = 1 - \frac{1}{\sqrt{\pi}}\int_{-\infty}^{+\infty} \exp(-y^2)\frac{\operatorname{erf}\left[\sqrt{\frac{\pi a(y)}{2}}\right]}{\sqrt{a(y)}}dy$$

donde el exponente de propagación (n) es 4 siendo:

$$a(y) = 10^{\frac{\left|-\left(\alpha(R_c)+\sqrt{2}\sigma y\right)\right|}{10}}$$

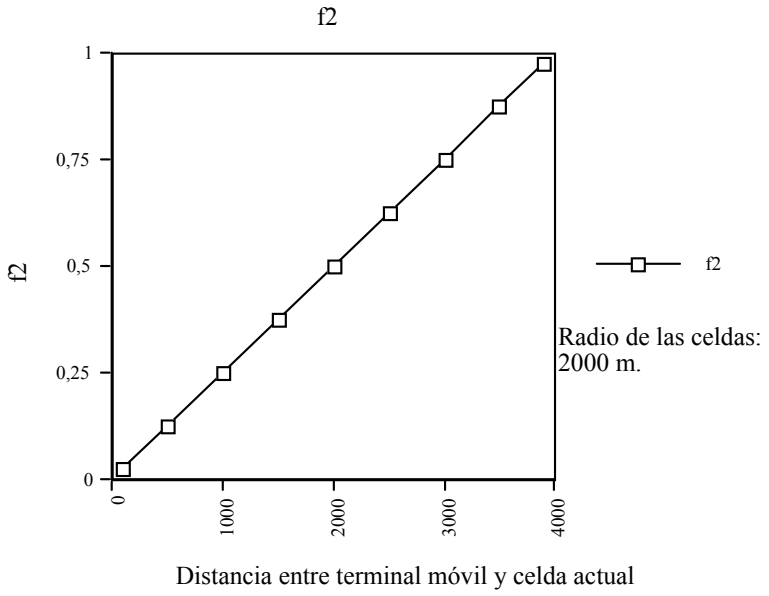
3.6.2 Determinación de f2

Para determinar f2, se ha buscado una función lineal dependiente de la distancia entre la celda actual y la celda candidata. Siendo:

DBTSact: Distancia desde el terminal móvil a la BTS actual.
DBTSady: Distancia desde el terminal móvil a la BTS candidata.
DIS_MT_BTSact, DIS_MT_BTSady: Distancia de activación (máxima distancia permisible entre un terminal móvil y su estación base).

$$f2 = \frac{\frac{DBTSact}{DIS\_MT\_BTSact}}{\frac{DBTSact}{DIS\_MT\_BTSact} + \frac{DBTSady}{DIS\_MT\_BTSady}}$$

En la gráfica, puede observarse el comportamiento lineal de la función f2.



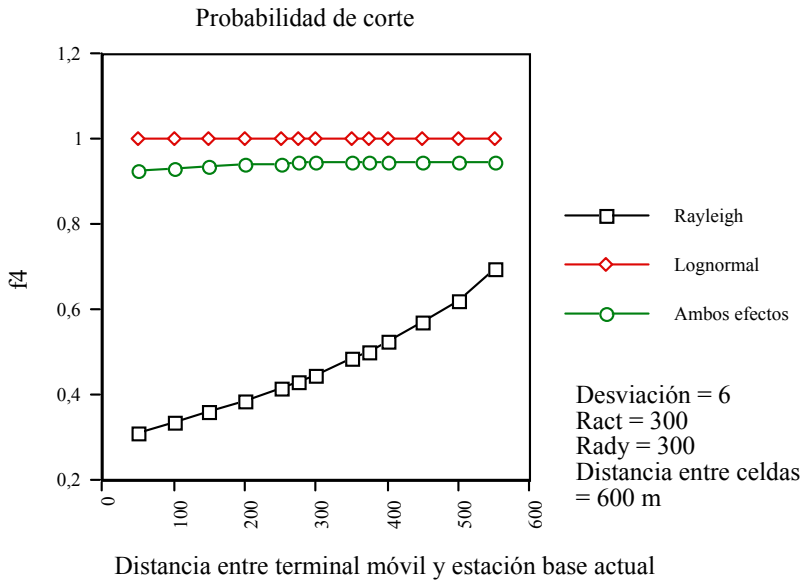
Gráfica 3.1 Distribución de f2 con la distancia entre la celda actual y una celda candidata.

3.6.3 Determinación de f4

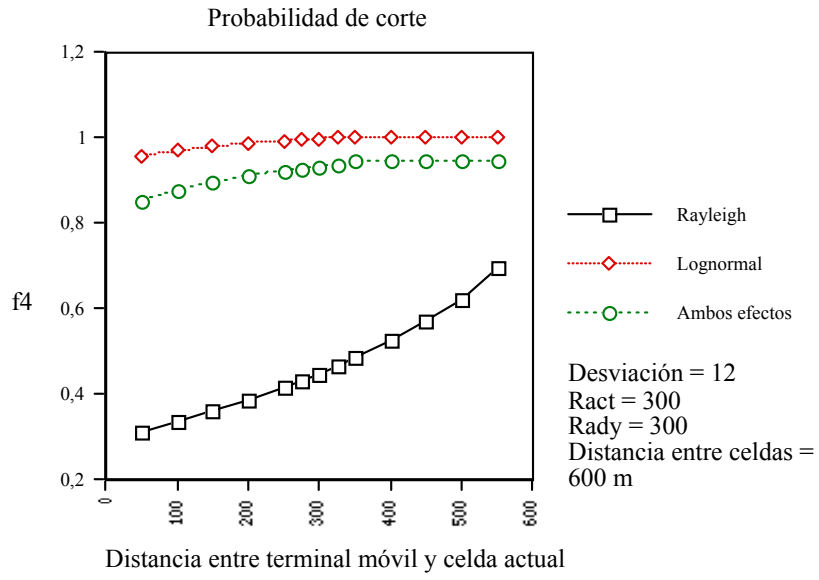
Se toma f4 como el opuesto de la probabilidad de corte respecto de la estación base $P_{out}(r)$. Es decir, sólo interesará hacer un handover a una celda candidata si ésta tiene una $P_{out}(r)$ baja y por tanto, su opuesto un valor alto para un mayor peso en la función FHAi. Esto es:

f4 = (1 - $P_{out}(r)$) en la celda adyacente candidata.

Se observa en ambas gráficas que cuanto más alejado está el terminal móvil de la celda adyacente candidata, más baja es f4, de forma que es coherente con su menor posibilidad de ser celda candidata.



Gráfica 3.2 Función f4 con desviación igual a 6.

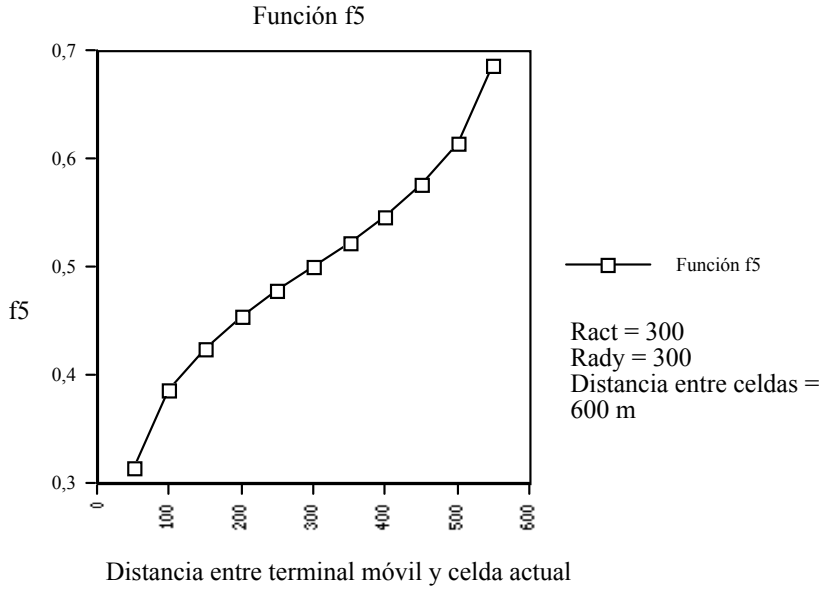


Gráfica 3.3 Función f4 con desviación igual a 12.

3.6.4 Determinación de f5

La función que define al efecto de la atenuación de la señal en el radioenlace es formalizado por f5 y se define como:

$$f5 = \frac{Lact}{Lact + Lady}$$



Grafica 3.4 Función f5

que no es más que una función normalizada de la atenuación de la señal en la celda actual respecto de celda adyacente. De esta forma, se potencia el handover a la celda candidata sólo en el caso de que la atenuación en la celda actual sea grande.

De la gráfica se concluye el efecto de una f5 creciente conforme el móvil se desplaza a la estación base adyacente.

3.6.5 Determinación de K2

El valor de K2 puede obtenerse a partir del hecho de que el factor distancia únicamente resulta decisivo en celdas de gran tamaño. Sólo cuando el retardo en el envío y recepción de los paquetes en el radioenlace es apreciable tiene sentido definir la distancia como parámetro importante a la hora de decidir un handover a otra celda. Por tanto, sólo se considera su efecto en el caso de tratar macroceldas o celdas grandes. Se considerará pues:

K2 = 1 si se trata de una macrocelda (o microcelda).
K2 = 0 si se trata de una picocelda.

3.6.6 Determinación de K3

Con la determinación de K3 se define la importancia de mantener la conexión en el handover a celdas del mismo tipo. Eso es importante en el caso de terminales móviles ubicados en coches, trenes, etc que al circular a mayor velocidad hacen difícil su seguimiento en celdas muy pequeñas. Desde un punto de vista ideal, sería deseable una relación entre la velocidad del móvil y K3. El inconveniente consiste en que es difícil determinar la velocidad del

terminal móvil con la información que proporciona por si mismo, por ello se puede hacer una aproximación más simple, tal como la siguiente:

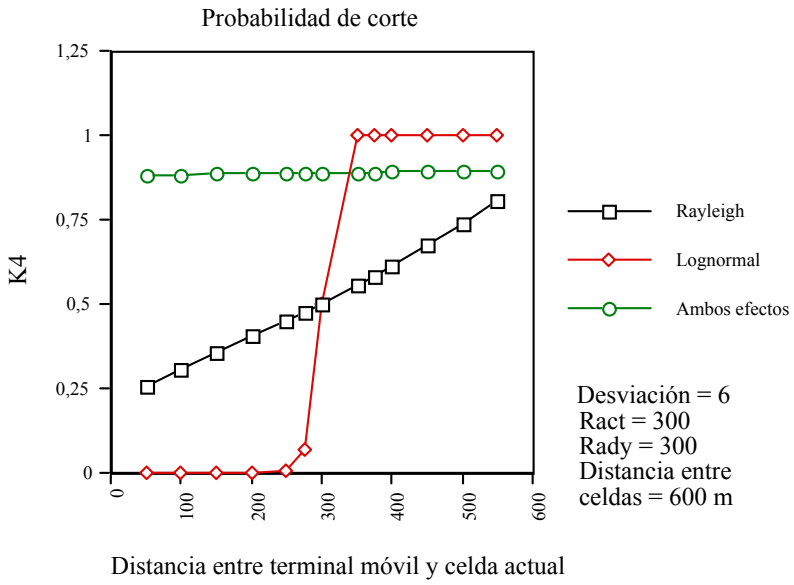
K3 = 1 si es un terminal móvil de un vehiculo (coche,...)
K3 = 0 si se trata de un terminal móvil de un peatón.

3.6.7 Determinación de K4

El peso que se otorga a la probabilidad de corte media formalizada por f4 se define como:

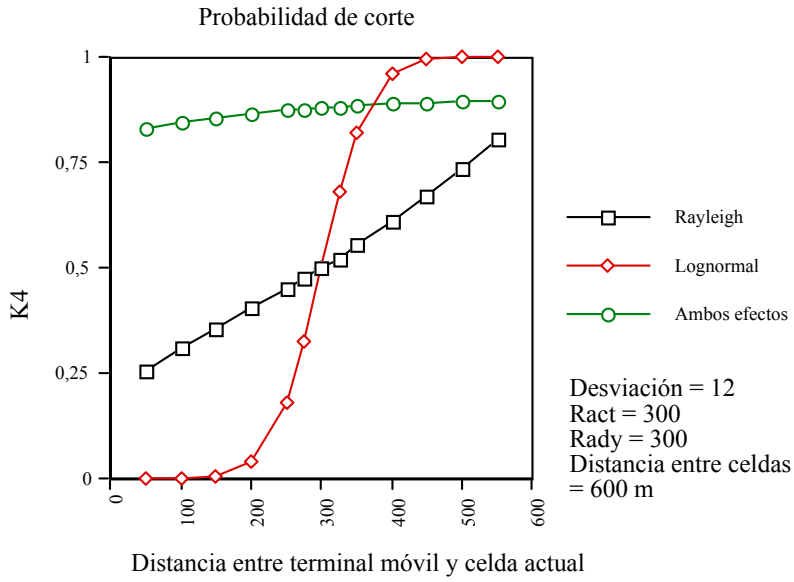
$$K4 = \frac{P_c act}{P_c act + P_c ady}$$

que no es más que un peso normalizado de la probabilidad de corte media en la celda actual respecto de celda adyacente. De esta forma, se potencia el handover a la celda candidata sólo en el caso de que la probabilidad de corte media en la celda actual sea grande.



Gráfica 3.5 Parámetro K4 para una desviación igual a 6.

En ambas gráficas se observa que cuanto más cerca está el terminal móvil de la estación base actual, menos peso tiene K4 por cuanto la probabilidad de corte es menor. A medida que el terminal se acerca a la celda adyacente, el efecto de K4 se incrementa para denotar una mayor propensión de esa celda como candidata al handover. Es de destacar también el efecto de utilizar separadamente desvanecimientos de Rayleigh y/o lognormales para determinar K4.



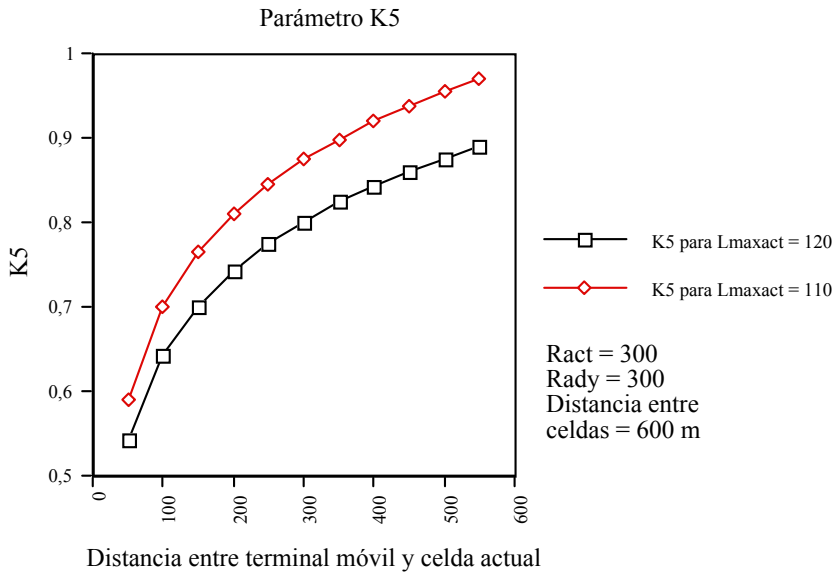
Gráfica 3.6 Parámetro K4 para una desviación igual a 12.

3.6.8 Determinación de K5

Para la determinación de K5, se introduce un cociente valorando el nivel de atenuación de la señal en la celda actual respecto de un máximo permisible. Esto es:

$$K5 = \frac{Lact}{L\,max.act}$$

De esta forma, se potencia el handover a la celda candidata sólo en el caso de que la atenuación de la señal en la celda actual sea grande.



Gráfica 3.7 Parámetro K5 en función de la distancia y el nivel máximo permitido de atenuación.

De la gráfica se deduce que según la distancia entre el terminal móvil y la celda actual, K5 es creciente y por tanto, conforme se acerca el terminal a la celda adyacente aumenta su carácter de celda candidata para handover.

3.7 Parámetros utilizados para evaluar el tráfico en un conjunto de celdas adyacentes

El objetivo de efectuar estas mediciones es poder evaluar con la mayor precisión posible, la probabilidad de bloqueo que puede sufrir una celda de cara a la evaluación de una lista de celdas candidatas. Para ello, se considera que i es el número de BTSs que son monitorizadas o mantienen contacto con el área de cobertura de la celda en la que el móvil está inicialmente, (en nuestro caso i=1).

Las mediciones que se efectuen en la BTS se basarán en el número de handovers intra-celda. Las mediciones que se obtengan en el CSS vendran determinadas por los resultados ofrecidos por las diferentes BTS, según los parámetros siguientes:

Sean:
N: Capacidad en canales de una determinada celda i.
∂_i: Número total de canales ocupados por handover a la celda i.
$ß_i$: Número total de canales ocupados por establecimiento de llamada desde la celda i.
ii_i: Número de intentos de handover entrantes entre celdas intra CSS (por celda originante).
i_i: Número de handovers entrantes entre celdas intra CSS (por celda originante).
oi_i: Número de intentos de handover salientes entre celdas intra CSS (por celda destino).
o_i: Número de handover salientes entre celdas intra CSS (por celda destino).

En el CSS además se generaran otras mediciones provenientes del mismo CSS con arreglo a los siguientes parámetros:
y: Número de causas de handover controladas por el CSS.
x: Número de handovers fallidos controlados por CSS.
x_c: Número de handovers fallidos con exitoso reestablecimiento controlados por CSS.
x_s: Número de handovers fallidos sin exitoso reestablecimiento controlados por CSS.

A partir de la información anterior se puede establecer que:

$$y = x + (ii_i + oi_i) + (i_i + o_i)$$
$$x = x_c + x_s$$

Siguiendo la estructura jerarquizada de la red, y de forma similar, se procedería a realizar mediciones y calculos en los MSCP(CSS), MSCP(LE) y MSCP(TX) para los distintos casos de handover.

Esa información puede complementarse en el caso de sistemas más inteligentes con referencias de trayectorias seguidas por la estación móvil para determinar con más seguridad desde el sistema de gestión de red la idoneidad de realizar determinados handovers y a qué celdas. Lo que permite hacer cálculos sobre el máximo flujo de móviles en una determinada dirección o bien la ocupación de canales en una celda en un momento dado.

Para optimizar la capacidad de la red y minimizar la probabilidad de bloqueo de la llamada en un handover, se determinan los siguientes parámetros:

ii_i: Permitirá obtener el parámetro Λ_{Rh}
i_i: Permitirá obtener el parámetro Λ_{Rhc}
∂_i: Permitirá obtener el parámetro Nh
$ß_i$: Permitirá obtener el parámetro N - Nh

siendo:
Λ_{Rh} : Tasa media de intentos de handover por celda.
Λ_{Rhc} : Tasa media de handover cursados por celda.
Nh: Número de canales en la celda dedicados a handover.
N - Nh: Número de canales en la celda dedicados a establecimiento de llamada.

Estas tasas medias de intentos de handover o bien de handovers cursados por celda permitirán determinar de manera más efectiva las probabilidades de bloqueo del terminal móvil en los establecimientos de llamada o en el handover tal como se verá con más detalle en los siguientes apartados.

3.8 Tasas de generación de llamada y handover

Junto al estudio de la movilidad, es conveniente realizar un análisis de las tasas de llamada y de handover en el sistema de celdas. Esto es, aportar información acerca del tráfico y de la carga de señalización soportada por el sistema. De esta forma se puede definir:

Λ_a : Número medio de nuevas llamadas por segundo por unidad de área.
Λ_R : Número medio de nuevas llamadas por segundo por celda.
R: Radio de celda hexagonal.

$$\Lambda_R = \frac{3\sqrt{3}}{2} R^2 \Lambda_a$$

Λ_{Rh} : Tasa media de intentos de handoff por celda.
γ_o: Ratio de intentos de handover a tasa de origen de nuevas llamadas por celda.

$$\gamma_o = \frac{\Lambda_{Rh}}{\Lambda_R}$$

Si una fracción de origen de nuevas llamadas es bloqueada P_B, entonces, la tasa media sobre la cual se cursan las nuevas llamadas es de la forma:
$\Lambda_{Rc} = \Lambda_R(1 - P_B)$
Si se tiene en cuenta una fracción de intentos fallidos de handover, P_{fh} entonces, el número medio de peticiones de handover cursadas es:
$\Lambda_{Rhc} = \Lambda_{Rh}(1 - P_{fh})$
y por tanto, el ratio γ_c de número medio de intentos de handover al número medio de llamadas nuevas cursadas es de la forma:

$$\gamma_c = \frac{\Lambda_{Rhc}}{\Lambda_{Rc}} = \gamma_o \frac{(1 - P_{fh})}{(1 - P_B)}$$

Junto al análisis de movilidades, se requiere especificar los tiempos que afectan a las tasas de handovers. Éstos son los siguientes [SS1]:

T_H: Tiempo de mantenimiento del canal
T_M: Duración de la llamada o mensaje
T_n: Tiempo desde el cual un móvil reside en la celda en la cual se origina la llamada.
T_h: Tiempo desde el cual un móvil reside en la celda en la cual la llamada es traspasada.
Pueden definirse de la siguiente forma:

$T_M = \frac{1}{\mu_M}$ Duración de llamada distribuida exponencialmente.

$T_H = \frac{1}{\mu_H}$ Duración de llamada en ese canal.

Sean T_{Hn} y T_{Hh} los mínimos entre los retardos T_n de T_h y la duración de la llamada.
$T_{Hn} = \min(T_M, T_n)$
$T_{Hh} = \min(T_M, T_h)$

Se supone además, que las llamadas tienen duración exponencial y que las velocidades de los terminales móviles están distribuidas uniformemente entre 0 y V_{max}.

$$f_{T_M}(t) = \begin{cases} \mu_M e^{-\mu_M t}, \text{para}, t \geq 0 \\ 0, \text{para}, t < 0 \end{cases} \quad \text{con} \quad F_{T_M} = 1 - e^{-\mu_M t}$$

$$f_V(v) = \begin{cases} \frac{1}{V_{max}}, \text{para}, 0 \leq v \leq V_{max} \\ 0 \end{cases}$$

Las funciones de distribución acumuladas T_{Hn}, T_{Hh} pueden expresarse como:

$$F_{T_{Hn}}(t) = F_{T_M}(t) + F_{T_n}(t)\left(1 - F_{T_M}(t)\right)$$
$$F_{T_{Hh}}(t) = F_{T_M}(t) + F_{T_h}(t)\left(1 - F_{T_M}(t)\right)$$

La distribución de tiempo de mantenimiento de canal puede escribirse como:

$$F_{T_H}(t) = \frac{\Lambda_{Rc}}{\Lambda_{Rc} + \Lambda_{Rhc}} F_{T_{Hn}}(t) + \frac{\Lambda_{Rhc}}{\Lambda_{Rc} + \Lambda_{Rhc}} F_{T_{Hh}}(t)$$
$$= F_{T_M}(t) + \frac{1}{1 + \gamma_c}\left(1 - F_{T_M}(t)\right)\left(F_{T_n}(t) + \gamma_c F_{T_h}(t)\right)$$

por otra parte, la función de densidad de probabilidad es de la forma:

$$f_{T_H}(t) = \mu_M e^{-\mu_M t} + \frac{e^{-\mu_M t}}{1 + \gamma_c}\left(f_{T_n}(t) + \gamma_c f_{T_h}(t)\right) - \frac{\mu_M e^{-\mu_M t}}{1 + \gamma_c}\left(F_{T_n}(t) + \gamma_c F_{T_h}(t)\right)$$

Es importante hallar las funciones de distribución de T_n y T_h ya que permitirán hallar las probabilidades que definen los tiempos de ocupación de los móviles en cada una de las celdas según la velocidad y tamaño de éstas o bien la duración de la llamada.

Para ello, se puede definir la posición de un móvil en una celda, se representa mediante su distancia r y dirección ϕ desde la estación base. Para encontrar pues las distribuciones de T_n y de T_h, se han de obtener las funciones de densidad de r y ϕ:

$$f_r(r) = \begin{cases} \frac{2r}{R_{eq}^2}, \text{para}, 0 \leq r \leq R_{eq} \\ 0 \end{cases}$$
$$f_\phi(\phi) = \begin{cases} \frac{1}{2\pi}, \text{para}, 0 \leq \phi \leq 2\pi \\ 0 \end{cases}$$

En la figura 3.15, se muestra una celda hexagonal (radio R) junto con su aproximación circular (radio Req) , con los valores de, r, Z, x, y, θ, ϕ. Se define Z como la distancia recorrida por el móvil hasta el extremo de la celda, que se supone a velocidad constante y con

dirección según un ángulo θ respecto al vector r. Se puede expresar a su vez x = rcosθ, y = rsenθ.

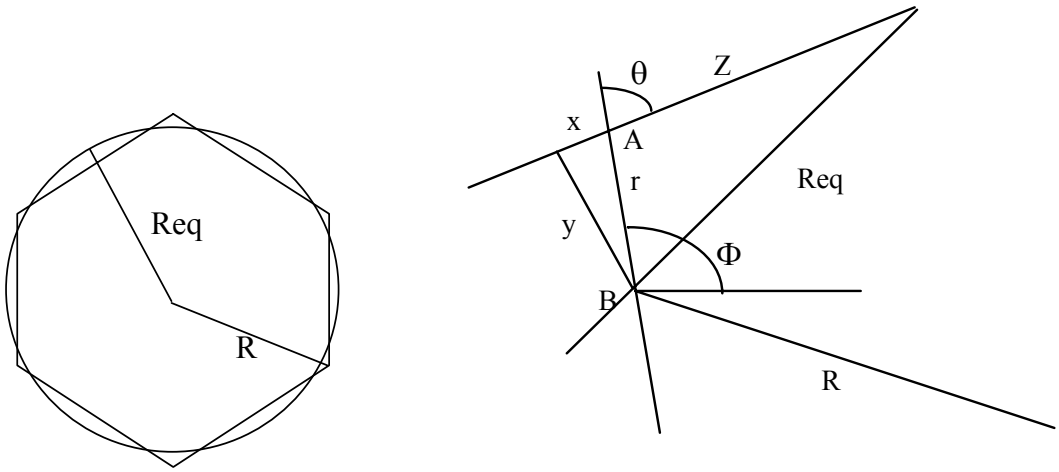


Fig. 3.15 Diagrama de una celda donde se muestran los distintos parámetros utilizados.

Se supone el centro de la celda en el punto B. La posición del terminal móvil estaría en la posición A a una distancia r y dirección ϕ de la estación base. Siendo el ángulo θ dado por la dirección del móvil (con respecto a un vector desde la estación base al móvil), la distancia Z desde el móvil al borde a la aproximación tomada del círculo es:

$$Z = \sqrt{R_{eq}^2 - (r\,\mathrm{sen}\,\theta)^2} - r\cos\theta$$

Al ser ϕ distribuido uniforme en un circulo, Z es independiente de ϕ y por simetria se puede tomar θ con la función de densidad siguiente:

$$f_\theta(\theta) = \begin{cases} \frac{1}{\pi}, \text{para}, 0 \le \theta \le \pi \\ 0 \end{cases}$$

se definen las nuevas variables aleatorias x e y como:

$$x = r\cos\theta$$
$$y = r\,\mathrm{sen}\,\theta$$

entonces:

$$Z = \sqrt{R_{eq}^2 - y^2} - x$$
$$W = x$$

ya que se supone el móvil equiprobablemente localizado en el circulo aproximado, se tiene:

$$f_{XY}(x,y) = \begin{cases} \frac{2}{\pi R_{eq}^2}, \text{para}, -R_{eq} \le x \le R_{eq}; 0 \le x^2 + y^2 \le R_{eq}^2; 0 \le y \le R_{eq} \\ 0 \end{cases}$$

$$f_{ZW}(z,w) = \frac{|z+w|}{\sqrt{R_{eq}^2 - (z+w)^2}} f_{XY}(x,y)$$
$$= \frac{2}{\pi R_{eq}^2} \frac{|z+w|}{\sqrt{R_{eq}^2 - (z+w)^2}}, \text{para}, 0 \le z \le 2R_{eq}, -\tfrac{1}{2}z \le w \le -z + R_{eq}$$

la función de densidad de probabilidad de la distancia Z es entonces:

$$f_Z(z) = \int_{-\frac{z}{2}}^{R_{eq}-z} \frac{2}{\pi R_{eq}^2} \frac{(z+w)}{\sqrt{R_{eq}^2 - (z+w)^2}} dw, \text{para}, 0 \le z \le 2R_{eq}$$
$$= \begin{cases} \frac{2}{\pi R_{eq}^2} \sqrt{R_{eq}^2 - \left(\frac{z}{2}\right)^2}, \text{para}, 0 \le z \le 2R_{eq} \\ 0 \end{cases}$$

$$F_Z(z) = \begin{cases} \frac{2}{\pi R_{eq}^2} \left[\frac{z}{2} \sqrt{R_{eq}^2 - \left(\frac{z}{2}\right)^2} + R^2 \text{sen}^{-1}\left(\frac{z}{2R_{eq}}\right) \right], \text{para}, 0 \le z \le 2R_{eq} \\ 1, \text{para}, z \ge 2R_{eq} \end{cases}$$

se asume que la velocidad v del móvil es constante durante el trayecto de la celda y está distribuida uniformemente en el intervalo $[0, V_{max}]$ con función de densidad de probabilidad:

$$f_V(v) = \begin{cases} \frac{1}{V_{max}}, \text{para}, 0 \le v \le V_{max} \\ 0 \end{cases} \quad (*)$$

entonces, se puede expresar T_n como:

$$T_n = \frac{Z}{V}$$

con función de densidad de probabilidad:

$$f_{T_n}(t) = \int_{-\infty}^{\infty} |w| f_Z(tw) f_V(w) dw$$

$$= \begin{cases} \dfrac{2}{V_{max}\pi R_{eq}^2}\int_0^{V_{max}} w\sqrt{R_{eq}^2 - \left(\frac{tw}{2}\right)^2}\,dw = \dfrac{8R_{eq}}{3V_{max}\pi t^2}\left[1 - \sqrt{\left\{1 - \left(\dfrac{tV_{max}}{2R_{eq}}\right)^2\right\}^3}\right], \\ \text{para}, 0 \le t \le \dfrac{2R_{eq}}{V_{max}} \\ \dfrac{2}{V_{max}\pi R_{eq}^2}\int_0^{\frac{2R_{eq}}{t}} w\sqrt{R_{eq}^2 - \left(\frac{tw}{2}\right)^2}\,dw = \dfrac{8R_{eq}}{3V_{max}\pi t^2}, \\ \text{para}, t \ge \dfrac{2R_{eq}}{V_{max}} \end{cases}$$

con función de distribución:

$$F_{Tn}(t) = \int_{-\infty}^{t} f_{Tn}(x)dx$$

$$= \begin{cases} \dfrac{2}{\pi}\text{arcsen}\left(\dfrac{V_{max}t}{2R_{eq}}\right) - \dfrac{4}{3\pi}\tan\left[\dfrac{1}{2}\text{arcsen}\left(\dfrac{V_{max}t}{2R_{eq}}\right)\right] + \dfrac{1}{3\pi}\text{sen}\left[2\text{arcsen}\left(\dfrac{V_{max}t}{2R_{eq}}\right)\right], \\ \text{para}, 0 \le t \le \dfrac{2R_{eq}}{V_{max}} \\ 1 - \dfrac{8R_{eq}}{3\pi V_{max}}\dfrac{1}{t}, \\ \text{para}, t \ge \dfrac{2R_{eq}}{V_{max}} \end{cases}$$

Si se asume que el móvil se mueve con cualquier dirección con igual probabilidad, la variable aleatoria θ tiene como función de densidad de probabilidad:

$$f_\theta(\theta) = \begin{cases} \dfrac{1}{\pi}, \text{para}, \dfrac{-\pi}{2} \le \theta \le \dfrac{\pi}{2} \\ 0 \end{cases}$$

siendo la distancia Z:

$$Z = 2R_{eq}\cos\theta$$

con función de distribución:

$$F_Z(z) = \Pr\{Z \le z\}$$

$$= \begin{cases} 0, \text{para}, z < 0 \\ 1 - \dfrac{2}{\pi}\arccos\left(\dfrac{z}{2R_{eq}}\right), \text{para}, 0 \le z \le 2R_{eq} \\ 1, \text{para}, z > 2R_{eq} \end{cases}$$

La función de densidad se expresa tal como:

$$f_Z(z) = \frac{d}{dz} F_Z(z)$$
$$= \begin{cases} \frac{1}{\pi} \frac{1}{\sqrt{R_{eq}^2 - \left(\frac{z}{2}\right)^2}}, \text{para}, 0 \le z \le 2R_{eq} \\ 0 \end{cases}$$

El tiempo en la celda T_h es el tiempo en el que el móvil viaja la distancia Z con velocidad V.

$$T_h = \frac{Z}{V}$$

siendo la función de densidad:

$$f_{T_h}(t) = \int_0^{\infty} |w| f_Z(tw) f_V(w) dw$$

$$= \begin{cases} \frac{1}{\pi V_{max}} \int_0^{V_{max}} \frac{w}{\sqrt{R_{eq}^2 - \left(\frac{tw}{2}\right)^2}} dw = \frac{4R_{eq}}{\pi V_{max}} \frac{1}{t^2} \left[1 - \sqrt{1 - \left(\frac{V_{max} t}{2R_{eq}} \right)^2} \right], \\ \text{para}, 0 \le t \le \frac{2R_{eq}}{V_{max}} \\ \frac{1}{\pi V_{max}} \int_0^{\frac{2R_{eq}}{t}} \frac{w}{\sqrt{R_{eq}^2 - \left(\frac{tw}{2}\right)^2}} dw = \frac{4R_{eq}}{\pi V_{max}} \frac{1}{t^2}, \\ \text{para}, t \ge \frac{2R_{eq}}{V_{max}} \end{cases}$$

siendo la función de distribución de T_h:

$$F_{T_h}(t) = \int_{-\infty}^{t} f_{T_h}(x) dx$$
$$= \begin{cases} 0, \text{para}, t < 0 \\ \frac{2}{\pi} \text{arcsen}\left(\frac{V_{max} t}{2R_{eq}} \right) - \frac{2}{\pi} \tan\left[\frac{1}{2} \text{arcsen}\left(\frac{V_{max}}{2R_{eq}} \right) \right], \text{para}, 0 \le t \le \frac{2R_{eq}}{V_{max}} \\ 1 - \frac{4R_{eq}}{\pi V_{max}} \frac{1}{t}, \text{para}, t > \frac{2R_{eq}}{V_{max}} \end{cases}$$

Puede obtenerse una mejor aproximación de la expresión (*) si se tiene únicamente en cuenta la velocidad en los terminales móviles que realizan handover, puesto que el resto son cuasi

estáticos [HX1]. De esta forma, se tiene una función de densidad para la velocidad diferente, ya que ésta alcanza valores más altos:

$$f_v^*(v) = \frac{v f_v(v)}{E[v]}$$

obteniendo una probabilidades P_N y P_H más correctas.

3.9 Probabilidades de evolución de las llamadas

Los valores de la movilidad, funciones de densidad, etc, obtenidos anteriormente permiten calcular de forma adecuada distintas probabilidades de evolución de las llamadas en la red. Se pueden definir los siguientes términos:

P_B: Probabilidad de bloqueo. Probabilidad de que una llamada no entre en servicio a causa de la no disponibilidad de canales.
P_F: Probabilidad de que una llamada sea forzada a finalizar
P_{fh}: Probabilidad de que un intento de handover falle.
P_N: Probabilidad de que una nueva llamada que no sea bloqueada requiera al menos un handover antes de su finalización debido al movimiento del móvil.
P_H: Probabilidad de que una llamada haya hecho un handover y requiera de otro handover antes de la finalización.
K: Es el número de veces que una llamada no bloqueada se traspasa satisfactoriamente durante su tiempo de vida.

$$P_N = Pr\{T_M > T_N\} = \int_0^{\infty} \left[1 - F_{T_M}(t)\right] f_{T_n}(t)dt = \int_0^{\infty} e^{-\mu_M t} f_{T_n}(t)dt$$

$$P_H = Pr\{T_M > T_h\} = \int_0^{\infty} \left[1 - F_{T_M}(t)\right] f_{T_h}(t)dt = \int_0^{\infty} e^{-\mu_M t} f_{T_h}(t)dt$$

P_{nc}: Probabilidad de que se produzcan intentos de llamada nuevos que no serán completados a causa de bloqueo o handover no satisfactorio.

$$P_F = \sum_{l=1}^{\infty} P_{fh}\left[P_N(1 - P_{fh})^{l-1} P_H^{l-1}\right] = \frac{P_{fh} P_N}{1 - P_H(1 - P_{fh})}$$

$$P_{nc} = P_B + P_F(1 - P_B) = P_B + \frac{P_{fh} P_N (1 - P_B)}{1 - P_H(1 - P_{fh})}$$

Probabilidad de no realizar ningún handover satisfactorio:

$$\Pr\{K=0\} = (1-P_N) + P_N P_{fh}$$

Para realizar K handovers satisfactorios han de cumplirse todas las siguientes condiciones:
a) La llamada no es completada en la celda en la cual se origina primeramente.
b) El primer handover es satisfactorio.
c) Requiere y son satisfactorios k-1 handovers adicionales.
d) La llamada se completa antes de requerir otro handover o no se completa pero falla en el intento de handover k+1.
Probabilidad de realizar K handovers satisfactorios:

$$\Pr\{K=k\} = P_N(1-P_{fh}) + (1-P_H+P_H P_{fh})\{P_H(1-P_{fh})\}^{k-1}, \text{con}, k = 1,2,\ldots$$

De aquí, se obtiene el número medio de handovers K como:

$$\bar{K} = \sum_{k=0}^{\infty} k \Pr\{K=k\} = \frac{P_N(1-P_{fh})}{1-P_H(1-P_{fh})}$$

Por continuidad, además se tiene que:

$$\Lambda_{Rh} = \Lambda_R(1-P_B)P_N + \Lambda_{Rh}(1-P_{fh})P_H$$

suponiendo iguales las velocidades de los móviles al entrar y al salir de las celdas, y siendo P_N y P_H conocidas.

Se define una probabilidad general P_{ncg}, que se define tal como los intentos de llamada nuevos que no serán completados a causa de bloqueo, handover no satisfactorio o corte.

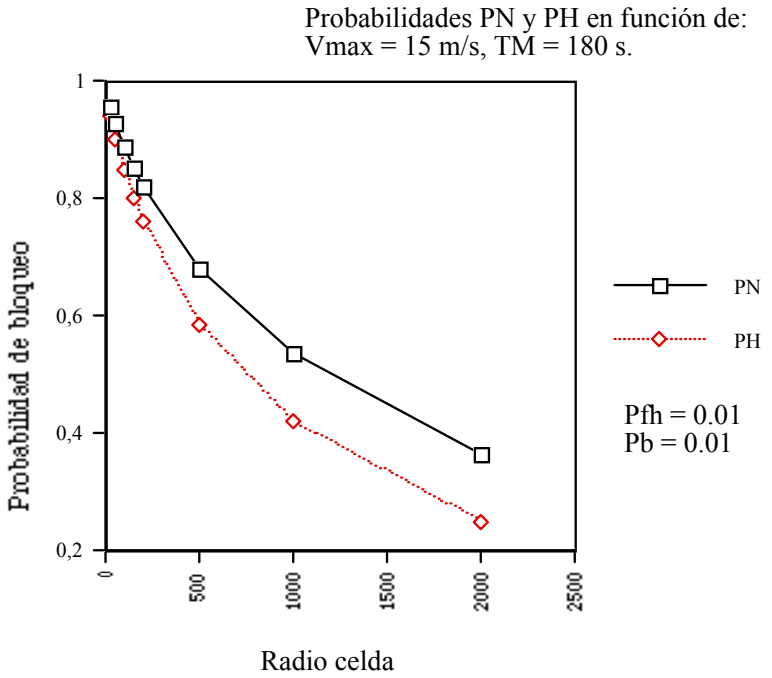
$$P_{ncg} = P_B + P_F(1-P_B) + P_C(1-P_B)(1-P_F)$$

P_{ncg} depende de K y P_c (probabilidad de corte).

3.9.1 Determinación de K1. Conclusiones

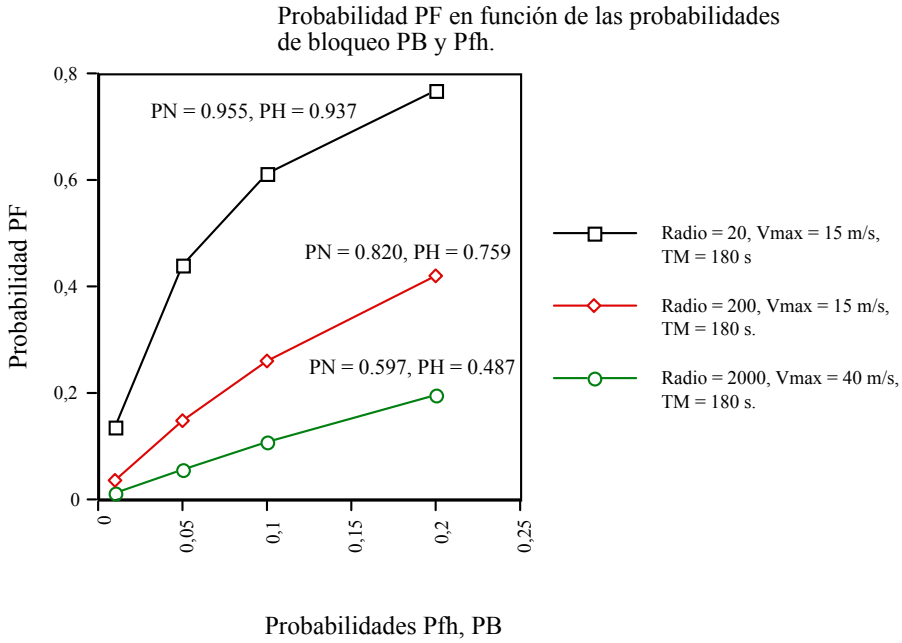
En este apartado, se pretenden hallar los parámetros que definan a la variable K1. Para ello, a continuación, se presentan diversas gráficas en donde se muestra la evolución de los términos especificados anteriormente. Sean:

P_N: Probabilidad de que una nueva llamada que no sea bloqueada requiera al menos un handover antes de su finalización debido al movimiento del móvil.
P_H: Probabilidad de que una llamada haya hecho un handover y requiera de otro handover antes de la finalización.



Gráfica 3.8. Probabilidades P_N y P_H en función del radio de las celdas

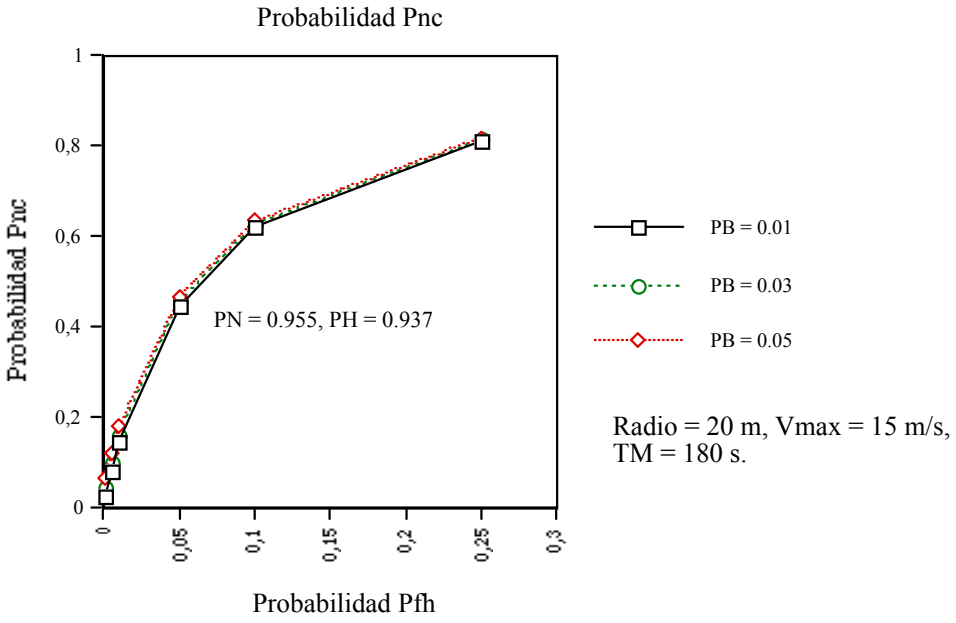
En este caso (gráfica 3.8), se observa que en entornos de microceldas, las probabilidades P_N y P_H crecen conforme el radio de la celda se va reduciendo.



Gráfica 3.9. Probabilidad P_F, en función de P_{fh} y P_B.

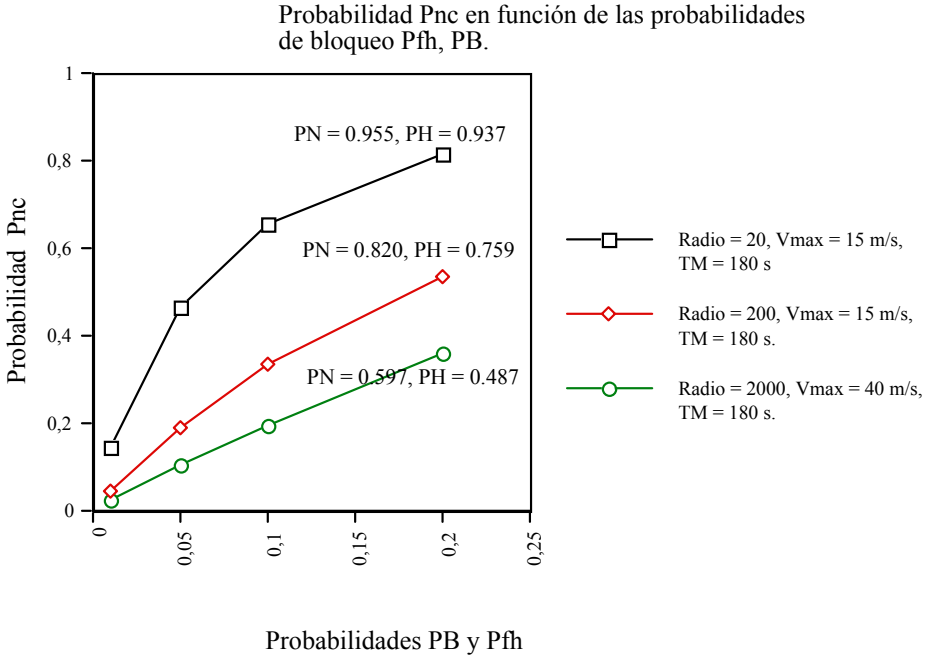
A continuación, se representa a la probabilidad P_F de que una llamada sea forzada a finalizar bajo diferentes parámetros. En la gráfica 3.9 se observa como a menor P_N y P_H, se obtiene una probabilidad P_F más pequeña. Posteriormente se representa a P_{nc} como intentos de

llamada nuevos que no serán completados a causa de bloqueo o handover no satisfactorio en función de otros parámetros.

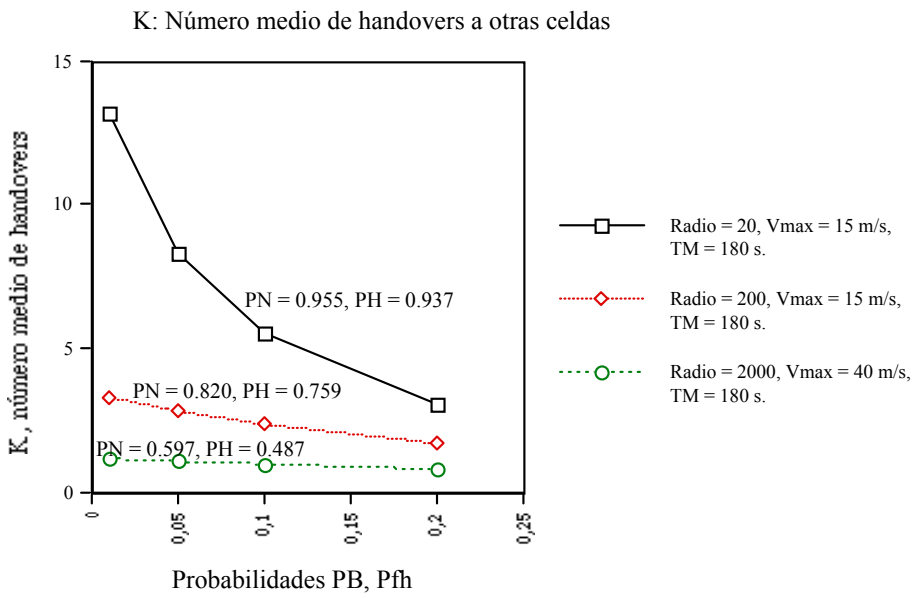


Gráfica 3.10 Probabilidad P_{nc} en función de P_{fh}.

De la gráfica 3.10 se observa que P_{nc} varía mucho con P_{fh} si P_N y P_H son grandes. En este caso, también se concluye que P_B apenas afecta. Si P_N y P_H son pequeños, lógicamente P_B afectaría más y P_{fh} menos.

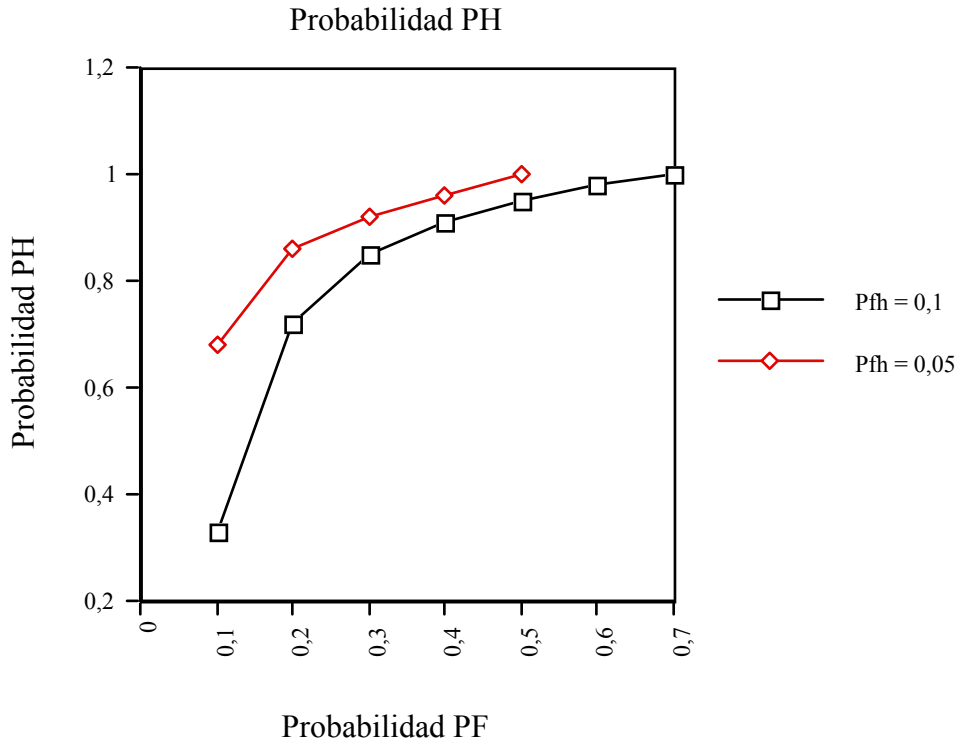


Gráfica 3.11 Probabilidad P_{nc} en función de P_{fh} y P_B.



Gráfica 3.12 Número de handovers K en función de la probabilidad P_{fh} y P_B.

En la gráfica 3.12, se observa que K apenas depende de P_B y P_{fh} si P_N y P_H son bajos.



Gráfica 3.13 P_H en función de P_F

A la vista de las gráficas anteriores, se puede determinar K1 como P_F siendo un buen estimador de P_{fh} para terminales móviles mientras que P_{nc} lo es de P_B para terminales móviles que son fijos. Además, se asocian los terminales móviles en movimiento a

macroceldas mientras que los móviles estáticos suelen estar registrados a microceldas y picoceldas. Esto es:

Si f1 = (1 - Pfh) ya que el terminal móvil está moviéndose, ha realizado handovers previamente o la celda candidata dispone de un tratamiento prioritario para peticiones de handover entonces, $K1 = P_F$

Si f1 = (1 - PB) ya que el terminal móvil está estático o no ha realizado handovers previamente, entonces $K1 = P_{nc}$

El sistema actua a efectos de congestion para priorizar el handover teniendo en cuenta la trayectoria anterior o entorno respecto de la celda actual. En este caso, K1 sería alto en el caso de estar en una celda próxima a la congestión denotando por tanto una mayor sensibilidad al handover a otras celdas (debido más por los efectos del tráfico que sobre las pérdidas de señal).

Finalmente, se incluyen las probabilidades que afectan directamente a la congestión de la red y que sirven para evaluar la función f1 en el algoritmo para la elección de celdas candidatas en el handover.

En primer lugar se procederá a realizar el cálculo de la probabilidad de bloqueo en una determinada celda. Ésta se obtiene de la información obtenida a través de las mediciones efectuadas sobre el número de canales ocupados por establecimientos de llamada o causas de handover registradas. El cálculo obtenido se compara con la capacidad asignada para cada celda.

3.10 Probabilidad de bloqueo en celdas

En este apartado se incide sobre la importancia de la estructura de la celda con el objetivo de mejorar las prestaciones de la red. Se realiza un estudio comparativo con distintos esquemas de tratamiento de las peticiones de llamada y de handover hallando las probabilidades de bloqueo.

Las celdas tienen en consideración la posibilidad de un tratamiento diferente en la asignación de canales según sean peticiones de establecimiento de llamada o handovers. Se consideran además los siguientes aspectos: colas según tipo de petición; reserva exclusiva de canales según tipo de petición; prioridades en cola diferentes según condiciones de propagación o tráfico y técnicas mixtas.

A partir del análisis obtenido, se plantea un escenario que sirve como modelo y que permite interaccionar de forma óptima a la hora de determinar f1 y K1 en el algoritmo de decisión de celdas candidatas propuesto. Los tipos de celda estudiados son los siguientes:

a) Probabilidad de bloqueo en celdas.
b) Probabilidad de bloqueo en celdas con cola
c) Probabilidad de bloqueo en celdas con prioridad
d) Probabilidad de bloqueo en celdas con cola y con prioridad
e) Probabilidad de bloqueo en celdas con cola, sin prioridad
f) Probabilidad de bloqueo en celdas con diferentes disciplinas de cola y sin prioridad.

Notación utilizada:
C: Número total de canales disponibles en el sistema
CM: Tamaño del cluster de macrocelda
CU: Tamaño del cluster de microcelda
AM: Area de macrocelda
AU: Area de microcelda
TO: Distribución de tráfico ofrecido uniforme
a*TO: Pico de tráfico
C*x: Fracción de canales asignados a microceldas
C*(1 - x): Fracción de canales asignados a macroceldas
BM: Probabilidad de bloqueo en macroceldas
BMll: Probabilidad de bloqueo a llamadas originantes en macroceldas
BMha: Probabilidad de bloqueo a handover en macroceldas
BU: Probabilidad de bloqueo en microceldas
BUll: Probabilidad de bloqueo a llamadas originantes en microceldas
BUha: Probabilidad de bloqueo a handover en microceldas
TOM: Trafico ofrecido a macrocelda
TOU: Trafico ofrecido a microcelda
TOM = AM * TO
TOU = AU * a * TO
TPM: Trafico perdido a macrocelda
TPU: Trafico perdido a microcelda
TPM = TOM * BM
TPU = TOU * BU

siendo:
TOM = TOMll + TOMha
TPM = TPMll + TPMha = TOMll * BMll + TOMha * BMha

TPU = TPUll + TPUha = TOUll * BUll + TOUha * BUha

3.10.1 Probabilidad de bloqueo en celdas

En este primer caso, se considera el caso general de peticiones a una macrocelda. La expresión general de bloqueo se halla mediante la función Erlang B.

$$BM = Erlb\left(\frac{C*(1-x)}{CM}, TOM\right)$$

siendo:

TOM = TO * AM

TOM = TOMll + TOMha

CSM: Canales disponibles en la macrocelda (sin paraguas)

$$CSM = \frac{C*(1-x)}{CM}$$

Tráfico perdido definitivo

TPM = TPMll + TPMha

Se presentan resultados de las probabilidades de bloqueo en establecimiento de llamada y handover para tamaños de picocelda con distinto número de canales.

Parámetros utilizados en los cálculos:

Tamaño cluster macrocelda CM = 7

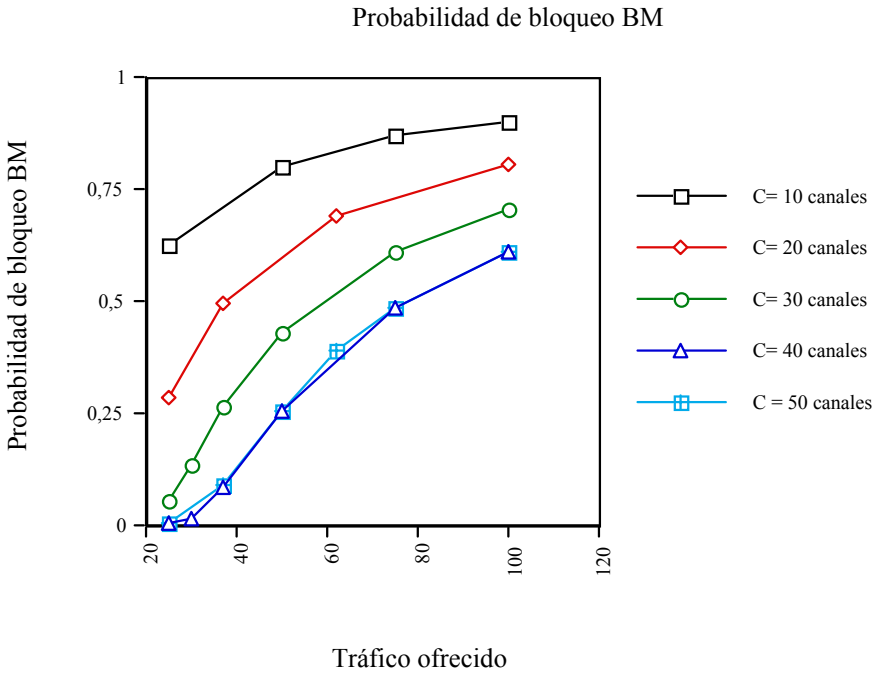
Tamaño cluster microceldas CU = 3

Número de canales total C = 295

Distribución de tráfico ofrecido uniforme TO = 1

Radio celda actual = 20

Radio celda adyacente = 2000



Gráfica 3.14 Probabilidades de bloqueo en establecimiento de llamada y handover para tamaños de picocelda con distinto número de canales

De la gráfica se puede deducir que la probabilidad de bloqueo aumenta conforme lo hace el tráfico ofrecido. El número de canales atenua esa pérdida de llamadas si bien existe un límite en el número de canales disponibles, tanto estática como dinámicamente asignados por el sistema.

3.10.2 Probabilidad de bloqueo en celdas con cola

En este caso, se utilizan primero los N canales para cursar indistintamente llamadas o handovers. Una vez se han ocupado los canales, si existen peticiones de handover, se dejan en espera mediante el buffer de M2 registros. Por tanto, la probabilidad de bloqueo es menor por el efecto de la disposición de un buffer para tratar las peticiones de handover. Así se tiene:

$N = \frac{C}{CM}$: Número de canales en la macrocelda

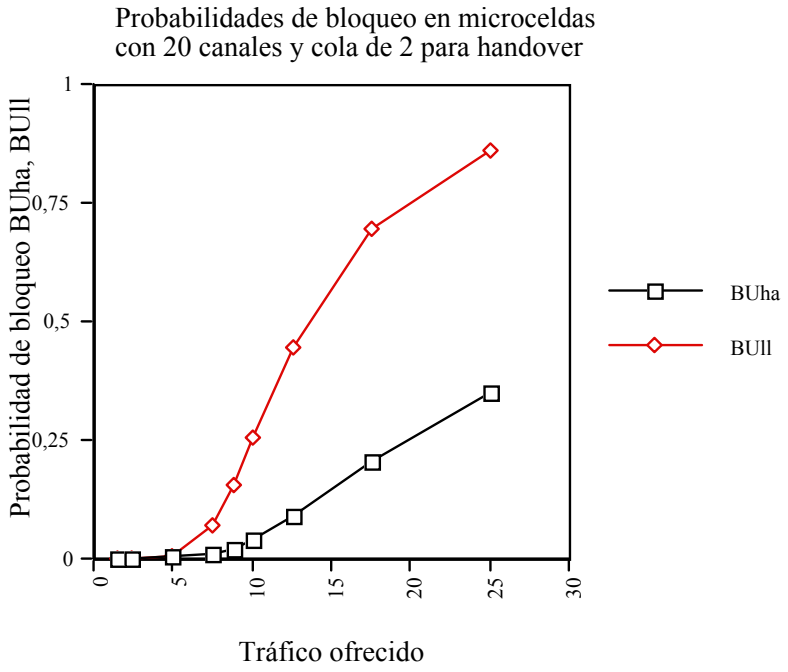
Las expresiones que se obtienen son las siguientes:

$$BMll = \left(\frac{1 - \left(\frac{TOMha}{N}\right)^{M2+1}}{1 - \left(\frac{TOMha}{N}\right)} \right) * \left[N! * \sum_{n=0}^{N-1} \frac{TOM^{n-N}}{n!} + \frac{1 - \left(\frac{TOMha}{N}\right)^{M2+1}}{1 - \left(\frac{TOMha}{N}\right)} \right]^{-1}$$

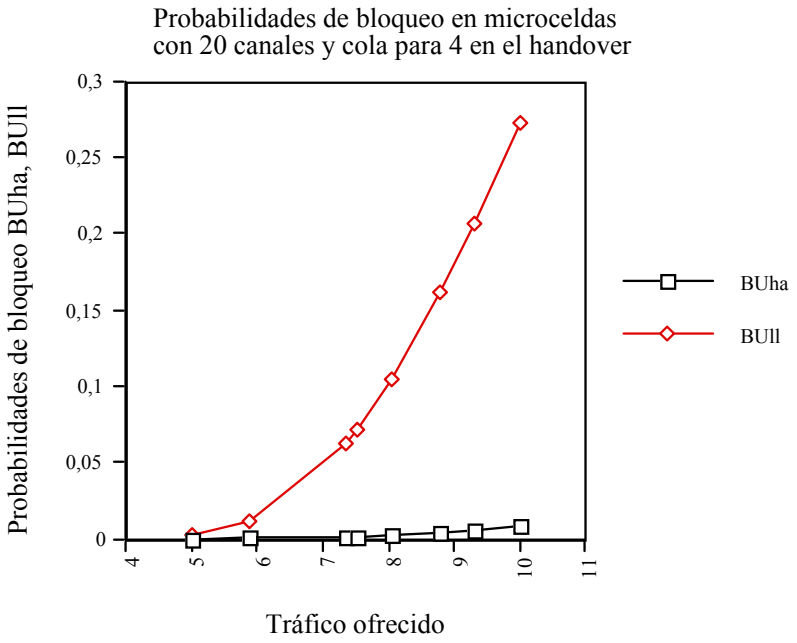
$$BMha = \left(\left(\frac{TOMha}{N}\right)^{M2}\right) * \left[N! * \sum_{n=0}^{N-1} \frac{TOM^{n-N}}{n!} + \frac{1-\left(\frac{TOMha}{N}\right)^{M2+1}}{1-\left(\frac{TOMha}{N}\right)} \right]^{-1}$$

Se presentan resultados de las probabilidades de bloqueo en establecimiento de llamada y handover. Se utilizan colas en el handover para M2 = 2, 4 y 8. Se aplican al caso especial de microceldas.

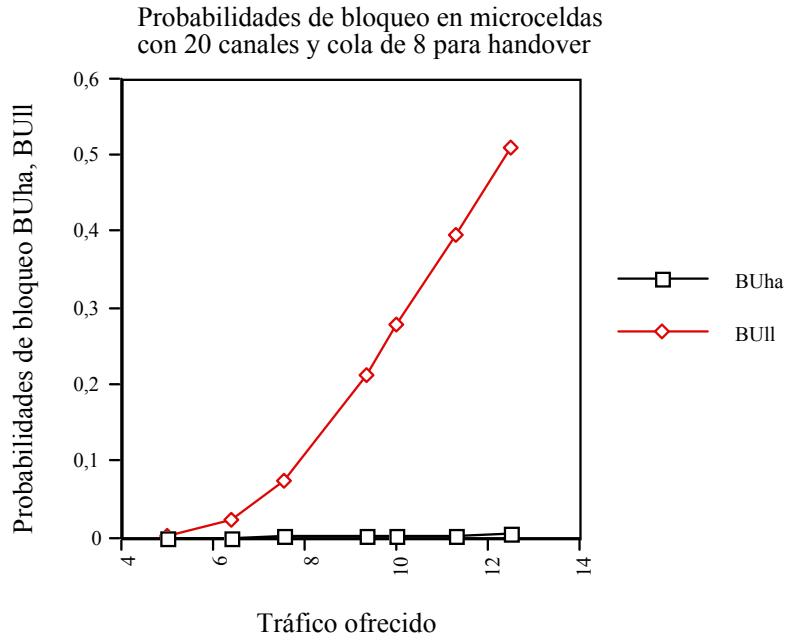
Parámetros utilizados en los cálculos:
Tamaño cluster macrocelda, CM = 7
Tamaño cluster microceldas, CU = 10
Número de canales total, C = 295
Número de canales microcelda = 20
Distribución de tráfico ofrecido uniforme, TO = 1
Radio celda actual = 125
Radio celda adyacente = 2000



Gráfica 3.15 Probabilidades de bloqueo en una microcelda con cola para handover de longitud M2 = 2.



Gráfica 3.16 Probabilidades de bloqueo en una microcelda con cola para handover de longitud M2 = 4.



Gráfica 3.17 Probabilidades de bloqueo en una microcelda con cola para handover de longitud M2 = 8.

De las anteriores gráficas, se puede concluir que el efecto de la cola para peticiones de handover es importante para la probabilidad de bloqueo tanto en los establecimientos de llamada como para los handover. En el caso de una cola con M2 = 2 su efecto es manifiesto pero no decisivo. Sólo a partir de M2 = 4 se obtienen probabilidades de bloqueo en handover realmente bajas.

Es de notar que en esta configuración no se considera todavía el efecto de pérdidas de handover por retardo excesivo en cola.

3.10.3 Probabilidad de bloqueo en celdas con prioridad

En este caso, el esquema de ocupación de canales de la celda es con prioridad para las peticiones de handover sobre las llamadas. Sean N los canales asignados a la celda, N_h los canales reservados a cursar handover y (N - Nh) los canales compartidos para peticiones de nuevas llamadas y handover. Se utilizan primero (N - Nh) canales para cursar indistintamente llamadas o handovers, dejando los N_h canales restantes para uso exclusivo de handovers cuando los anteriores están todos ocupados [DM1].

N: Número de canales en macrocelda
Nh: Número de canales reservados a handover en macrocelda
TOM: Tráfico ofrecido a macrocelda.
TOM = TOMll + TOMha

Probabilidad de Bloqueo en el establecimiento de llamada:

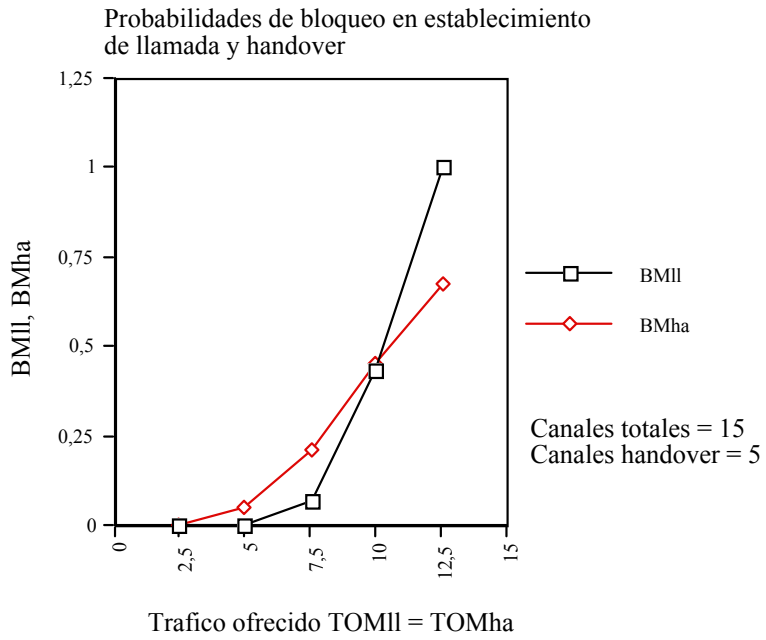
$$BMll = \left(\frac{(TOMll + TOMha)^{N-Nh} * (TOMha)^{Nh}}{N!} \right) * P_0$$

Probabilidad de Bloqueo en el handover:

$$BMha = \left((TOMll + TOMha)^{N-Nh} \sum_{n=N-Nh}^{N} \frac{(TOMha)^{n-N+Nh}}{n!} \right) * P_0$$

siendo:

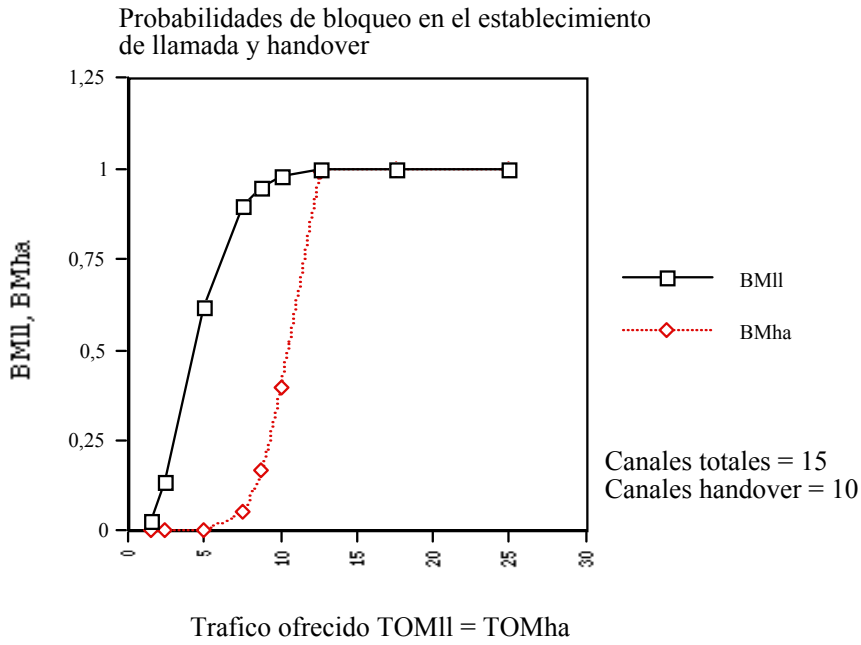
$$P_0 = \left[\sum_{n=0}^{N-Nh-1} \frac{(TOMll + TOMha)^n}{n!} + (TOMll + TOMha)^{N-Nh} \sum_{n=N-Nh}^{N} \frac{(TOMha)^{n-N+Nh}}{n!} \right]^{-1}$$



Gráfica 3.18 Probabilidades de bloqueo en establecimiento de llamada y handover para el handover con Nh = 5 y un número total de canales en la celda N = 15

Se presentan resultados de las probabilidades de bloqueo en establecimiento de llamada y handover para el handover con Nh = 5 y 10 para un número total de canales en la celda N = 15. Se aplican al caso especial de microceldas.

Parámetros utilizados en los cálculos:
Tamaño cluster macrocelda, CM = 7
Tamaño cluster microceldas, CU = 10
Número de canales total, C = 295
Número de canales microcelda = 20
Distribución de tráfico ofrecido uniforme, TO = 1
Radio celda actual = 125
Radio celda adyacente = 2000



Gráfica 3.19 Probabilidades de bloqueo en establecimiento de llamada y handover para el handover con Nh = 10 y un número total de canales en la celda N = 15

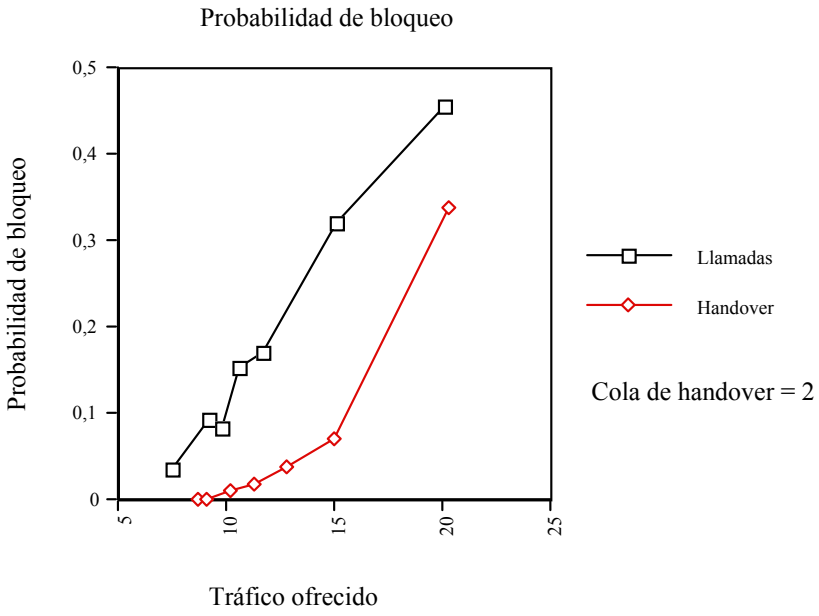
En este escenario, se valoran los efectos de la reserva de canales para peticiones de handover. Se constata que se mejora el tratamiento del bloqueo en las peticiones de handover a costa de empeorar la situación de los establecimientos de llamada, que disponen de menos canales. Una configuración de este tipo sólo se justifica en el caso de una demanda importante de handovers respecto a llamadas y a un tratamiento claramente prioritario para los handovers con la idea de reducir al mínimo su bloqueo.

3.10.4 Probabilidad de bloqueo en celdas con cola y con prioridad

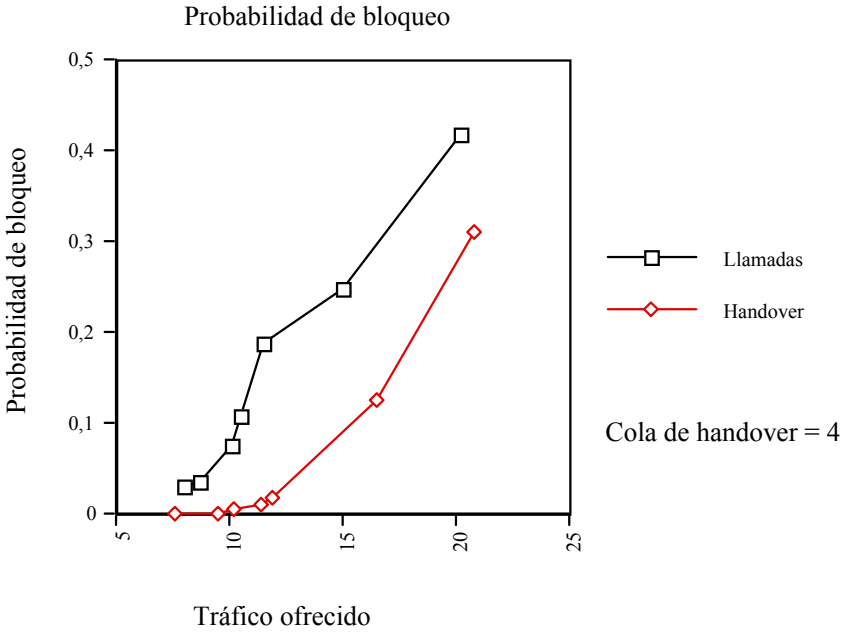
Esta configuración es parecida a la anterior (3.10.3) sólo que se han añadido buffers diferentes para el tratamiento de las peticiones de establecimiento de llamada y handover. Los resultados obtenidos son mejores, pero sigue adoleciendo de los problemas que supone un posible retardo excesivo para las peticiones de handover retenidas en cola provocando terminaciones forzadas.

Mediante simulaciones, se han obtenido los siguientes resultados en forma de gráficas:

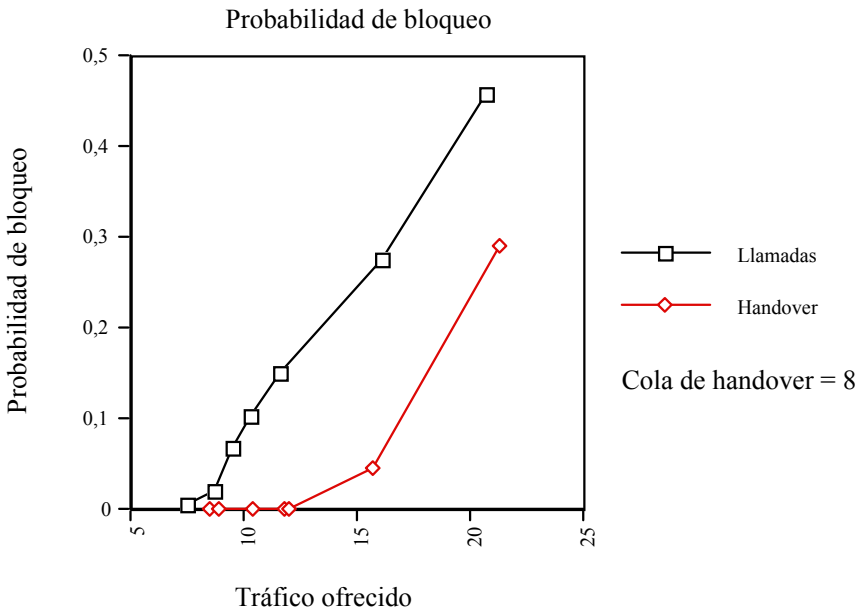
Estructura de celda utilizada:
Número de canales para establecimientos de llamada y handover: 20
Número de canales reservados para handover: 5



Gráfica 3.20 Probabilidad de bloqueo para el caso de tamaño de buffer igual a 2 para tratamiento de peticiones de establecimiento de llamada y handover.

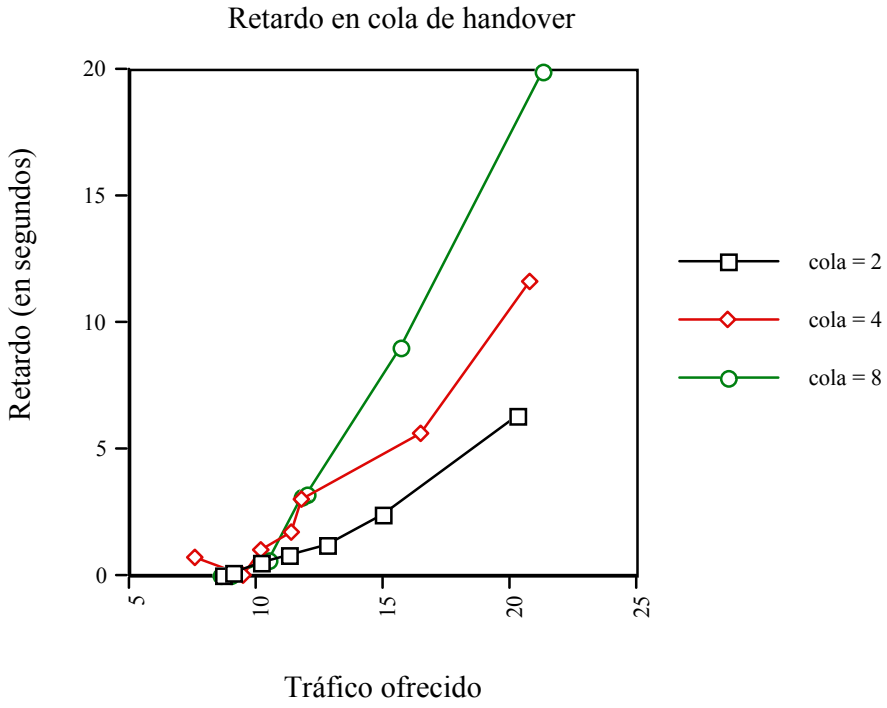


Gráfica 3.21 Probabilidad de bloqueo para el caso de tamaño de buffer igual a 4 para tratamiento de peticiones de establecimiento de llamada y handover.

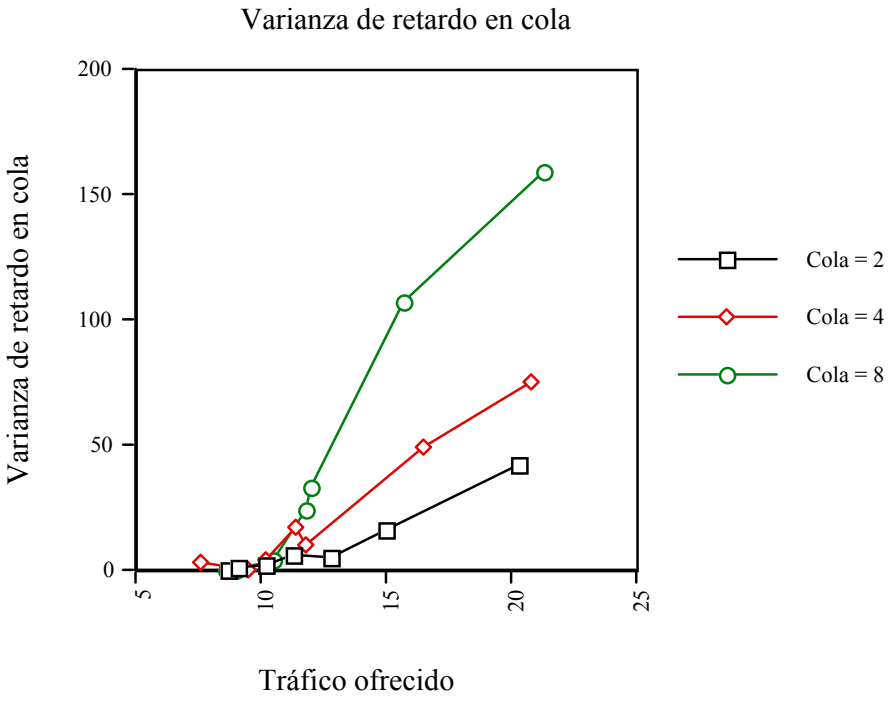


Gráfica 3.22 Probabilidad de bloqueo para el caso de tamaño de buffer igual a 8 para tratamiento de peticiones de establecimiento de llamada y handover.

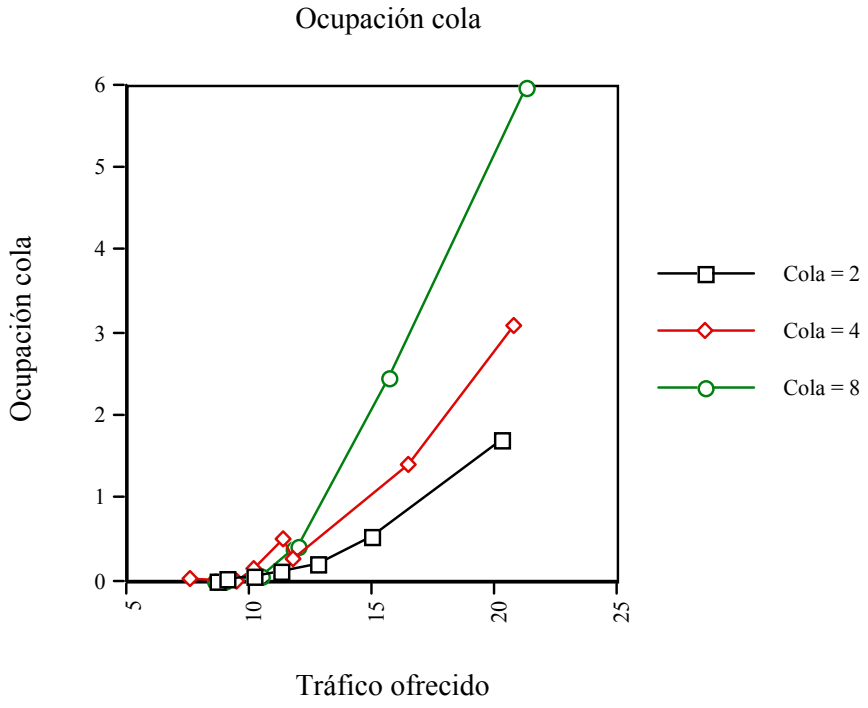
En las gráficas anteriores, se puede constatar el efecto que se obtiene en las probabilidades de bloqueo por el establecimiento de llamada y por pérdida forzada en el handover al compartir un número deerminado de canales en celda e ir variando las longitudes de los buffers para un mismo tráfico ofrecido para los dos tipos de peticiones.



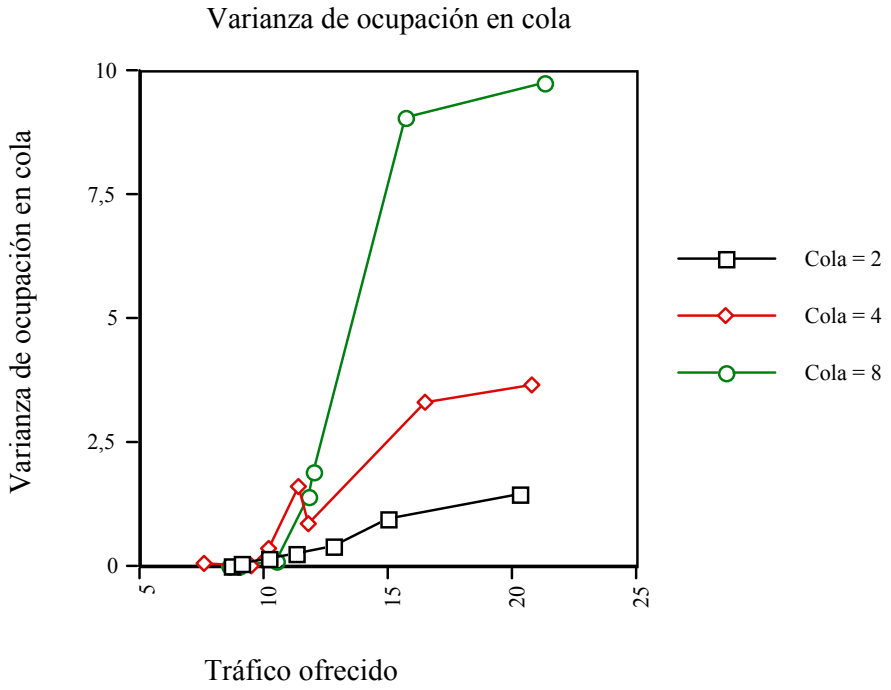
Gráfica 3.23 Retardo medio de la petición en el buffer de handovers.



Gráfica 3.24 Varianza del retardo de la petición en el buffer de handovers.



Gráfica 3.25 Ocupación media del buffer de handovers.



Gráfica 3.26 Varianza de la ocupación del buffer de handovers.

De las gráficas anteriores, se puede deducir que el tamaño óptimo de los buffers de la celda sería de hasta 8 registros. Sin embargo, dada la ocupación media de los buffers y el tiempo medio de las peticiones hacen pensar que eso no fuede funcionar. De hecho, como se observará más adelante, el tamaño óptimo de los buffers se estima de 3 ó 4 registros. Un tamaño mayor es poco aprovechado debido en parte a las pérdidas que se producirían por una espera excesiva de las peticiones en el buffer.

3.10.5 Probabilidad de bloqueo en celdas con cola, sin prioridad

En esta configuración, se utiliza una cola para el tratamiento de las peticiones de handover y se tiene en cuenta la posibilidad de pérdidas por excesivo retardo de la petición en cola. Además no hay prioridad o reserva de canales para el establecimiento de llamada.

La expresión para la probabilidad de bloqueo en establecimiento de llamada es la misma que en (3.10.4). Para el caso del handover, la probabilidad de terminación forzada, es decir, fallo en el handover, es la probabilidad de que el tiempo de espera en cola exceda el intervalo de degradación máximo tolerable para un terminal móvil. Así se tiene:

Sea N el número de canales disponibles.
Longitud de cola media: L_q

$$L_q = \sum_{n=N}^{\infty} (n - N) p_n$$

Probabilidad de terminación forzada: P_F

$$P_F = 1 - \int_0^{\square} W_q(t) f_{Td}(t) dt$$

Se obtiene:

$$W_q(t) = P_0(TOMll + TOMha)^N \frac{1}{(N-1)!} \frac{\left(1 - e^{-(N - TOMha)\mu t}\right)}{(N - TOMha)} + W_q(0)$$

$$W_q(0) = 1 - P_0(TOMll + TOMha)^N \frac{1}{(N)!} \frac{N}{(N - TOMha)}$$

siendo $W_q(t)$ la distribución del tiempo de espera en cola, T_d el intervalo de degradación distribuido normalmente y $f_{Td}(t)$ una función N(.,.).

Por simulaciones, se ha podido constatar, que para un tamaño de cola adecuado (p.e. 3 ó 4 registros) la probabilidad de terminación forzada por excesiva duración de la petición en cola es similar al caso anterior y es muy pequeña.

3.10.6 Probabilidad de bloqueo en celdas con diferentes disciplinas de cola y sin prioridad

En este caso, las peticiones de handover son puestas en cola de espera. Así que un canal está disponible, se ofrece al terminal móvil con parámetros de mediciones más cercanos al nivel mínimo de potencia aceptable para comunicación. La cola se reordena dinámicamente cuando se tienen en cuenta nuevos resultados de mediciones. Este sistema es el que obtiene en general, los mejores resultados en cuanto a prestaciones, sin embargo su implementación es muy compleja y no se ha tenido en cuenta en nuestro modelo final.

3.10.7 Resultados comparativos entre las distintas estructuras de celda definidas

Como consecuencia del estudio realizado con distintos esquemas de tratamiento de las peticiones de llamada y de handover, donde se han considerado colas, reserva de canales y distintos tipos de prioridades en las peticiones se han obtenido los siguientes resultados comparativos.

De entrada, se ha tratado de optimizar los siguientes parámetros:

- Minimizar el número de pérdidas de señal por caida o desvanecimiento frente al handover.
- Minimizar los efectos de bloqueo en el establecimiento de nuevas llamadas afectando lo menos posible el compromiso entre pérdidas de señal por desvanecimientos y nuevas llamadas.
- Minimizar el número de handovers.
- Tratar de realizar el handover lo más cerca posible de los límites de la celda.
- Minimizar el deterioro de la calidad de señal durante el proceso de handover.

Algunos compromisos importantes detectados en el diseño de estas configuraciones han sido los siguientes [GS1-4]:

- El número de handovers puede reducirse a costa de aumentar el número de caidas o desvanecimientos de señal. El número de cortes puede minimizarse permitiendo más peticiones de handover.
- El número de cortes se puede minimizar manteniendo un gran número de canales exclusivamente para handover (que incrementa el bloqueo de nuevas llamadas) o encolando las peticiones de handover (que comporta un mayor tiempo de procesado e incrementa el retardo en el procedimiento de handover).
- El promediado de muestras de señal en el radioenlace permite obtener valores más correctos, sin embargo, tambien incrementa el procesado en el terminal y el retardo en el sistema.
- La minimización en el número de handovers puede realizarse según los siguientes métodos:
a) Incorporar un margen de histeresis a la decision
b) Incorporar un contador o reloj a las BTS y terminales para que las peticiones de handover sean consistentes.
c) Usar algoritmos de predicción que hagan predicciones a largo plazo sobre la intensidad de la señal, respecto a predicciones cercanas basadas en un diferente periodo de muestreo.
Todos estos métodos comportan retardos en la decisión de invocar peticiones de handover.

Resultados que se han obtenido para los siguientes parámetros de entrada:
- Velocidad del móvil: 15 m/s y constante
- Dirección del móvil fija

Valores obtenidos considerados como óptimos:
- Para el caso de la mejora en el sistema respecto de la probabilidad de corte
    Es preferible un sistema con colas al caso de reserva de canales de handover.
    Celdas sin cola: 0 dB de margen de histéresis
    Celdas con cola: 1 dB de margen de histéresis
    Celdas con cola: Longitud de cola: 3 ó 4 registros
- Para el caso de la mejora en el sistema respecto de la probabilidad de corte y número de handovers innecesarios
    Celdas con cola: 3 dB de margen de histéresis.
    Reserva de canales: 2 canales para handover.

3.10.8 Conclusiones

En general, se opta por mecanismos de buffer frente a la reserva de canales en el handover ya que en un contexto más amplio, los DCA (algoritmos de control dinámico de canales) ya se encargan de gestionar los canales sobrantes entre las celdas.

Los algoritmos que presentan resultados más óptimos respecto a esta serie de parámetros son los que se basan en el uso de colas diferenciadas según handover o establecimiento de llamada y con diferentes niveles de prioridad según las condiciones de recepción de señal minimizando el número de handovers. Sin embargo, el número de handovers innecesarios cambia solo ligeramente entre los varios algoritmos de asignación de canales siendo las estrategias de propagación y los esquemas de predicción de tráfico los elementos más importantes en el balance final de prestaciones.

El uso variable de parámetros de propagación, como márgenes de histéresis o niveles de disparo son ventajosos para el balance entre número de handovers necesario y probabilidad de corte en la señal. Este aspecto se trata más en detalle en la fase de ejecución del handover, en este caso se trata de un resultado colateral al estudio realizado.

Se observa también que determinados esquemas de predicción de tráfico son útiles en la mejora de la probabilidad de corte en la señal al mejorar el tratamiento de las peticiones de handover, pero no lo son tanto en la prevención del número de handovers innecesarios.

Por último, es de notar pues, que las soluciones más óptimas son las más complejas de implementar por cuanto contienen un mayor grado de procesamiento.

3.11 Probabilidad de bloqueo en un escenario de macro/microceldas

El estudio de la probabilidad de bloqueo en el handover se realiza en un escenario formado por clusters de microceldas que son integradas en una macrocelda paraguas. La agrupación de diversas macroceldas da lugar a su vez a clusters de macroceldas [MF1]. Las peticiones de establecimientos de llamada y handovers forman un tráfico ofrecido que mayoritariamente es cursado por microceldas y que sus desbordamientos son enrutados a las macroceldas paraguas. Por sencillez, las microceldas están modeladas con una cola para cursar las peticiones de handover mientras que para los establecimientos de llamada el acceso a los canales es libre. Para nuestro análisis, se pueden distinguir las siguientes situaciones:

a) Probabilidad de bloqueo en macrocelda paraguas sin colas
b) Probabilidad de bloqueo en microcelda con cola en el handover

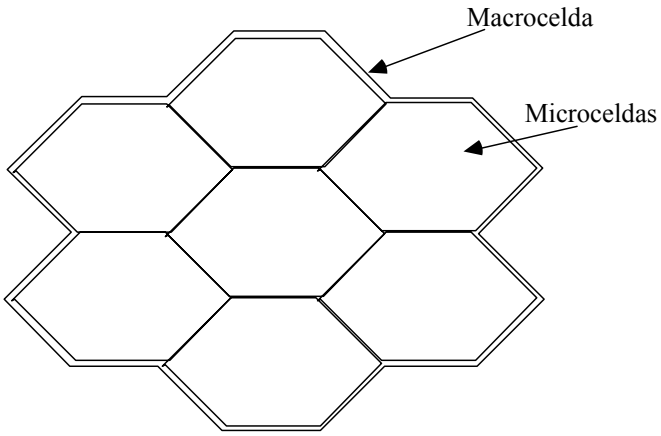


Fig. 3.16 Ejemplo de estructura de cluster de microceldas dentro de una macrocelda paraguas.

La notación ha utilizar en los cálculos será la siguiente:

C: Número total de canales disponibles en el sistema
CM: Tamaño del cluster de macrocelda
CU: Tamaño del cluster de microcelda
AM: Area de macrocelda
AU: Area de microcelda
C*x: Fracción de canales asignados a microceldas
C*(1 - x): Fracción de canales asignados a macroceldas
Bm: Probabilidad de bloqueo en macroceldas
BU: Probabilidad de bloqueo en microceldas
BUll: Probabilidad de bloqueo en microceldas a llamadas originantes
BUha: Probabilidad de bloqueo en microceldas a handover
TOM: Trafico ofrecido a macrocelda
TOU: Trafico ofrecido a microcelda
TOM = AM * TO
TOU = AU * a * TO
TPM: Trafico perdido a macrocelda
TPU: Trafico perdido a microcelda
TPM = TOM * Bm
TPU = TOU * BU

Siendo:
TOM = TOMll + TOMha
TPM = TPMll + TPMha = TOMll * BMll + TOMha * BMha
TPU = TPUll + TPUha = TOUll * BUll + TOUha * BUha

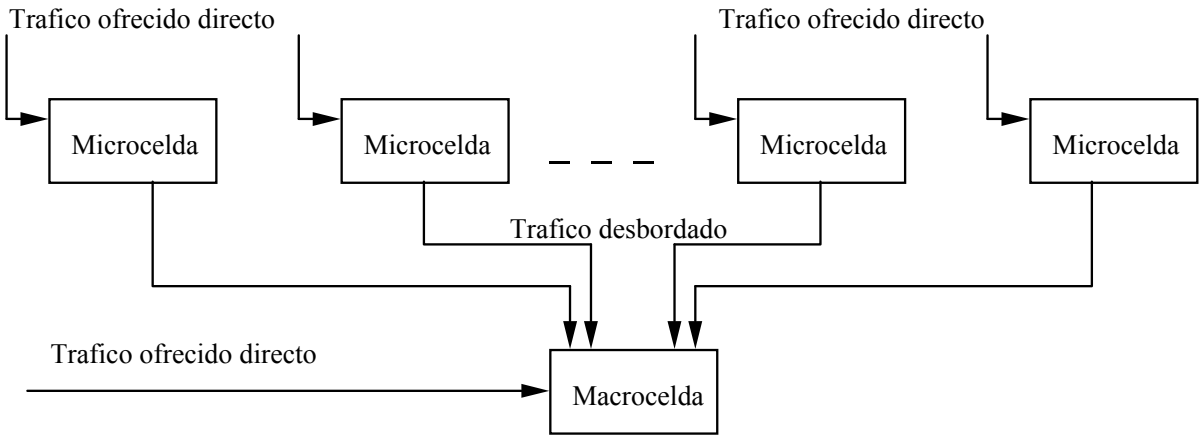


Fig. 3.17 Distribución de los tráficos desbordados de las microceldas sobre la macrocelda paraguas.

3.11.1 Probabilidad de bloqueo en macrocelda paraguas sin colas

La configuración en estudio consiste en un cluster formado por macroceldas donde cada macrocelda está formado de un cluster de microceldas. Cada macrocelda paraguas (a) recoge los tráficos desbordados de las microceldas (picoceldas), las cuales pueden presentar distintas estructuras de canales (b), para ser cursados por el resto de canales disponibles en la macrocelda. Se tiene que el tráfico perdido de microceldas desborda a macroceldas puede expresarse como:

TPU = TPUll + TPUha (Tráfico perdido por microceldas que no es de Poisson)

medll = TOUll * BUll

$$varll = medll\left[1 - medll + \frac{TOUll}{\frac{C^{*}x}{CU} - TOUll + medll + 1}\right]$$

medha = TOUha * BUha

$$var\,ha = med\,ha\left[1 - med\,ha + \frac{TOU\,ha}{\frac{C^{*}x}{CU} - TOU\,ha + med\,ha + 1}\right]$$

b: Porcentaje de area de macrocelda cubierta por microceldas

NU: Número de microceldas contenidas en una macrocelda paraguas

Suma de tráficos ofrecidos a la macrocelda:

medt: Suma de las medias de tráficos desbordados de microceldas

vart: Suma de varianzas de tráficos desbordados de microceldas

medt = NU * (medll + medha) + (1 - b) * TOM

vart = NU * (varll + varha) + (1 - b) * TOM

TOM = TOMll + TOMha

Aproximación de la probabilidad de bloqueo en macrocelda paraguas sin colas [AF1]:

$$Bm = Erlb\left(\frac{C(1-x)}{CM} * \frac{1}{z}, \frac{medt}{z}\right)$$
$$z = \frac{vart}{medt}$$

3.11.2 Probabilidad de bloqueo en microceldas con cola

En este caso, la cola existe en los handover pero no en las llamadas originantes. Sean pues:

M2: Tamaño de la cola para handover
M1: Tamaño de cola para llamadas originantes (igual a cero)
N: Número de canales por microcelda

$$N = \frac{C*x}{CU}$$

$\frac{1}{\mu}$: Tiempo medio de llamada incluyendo llamadas originantes y handover (en seg)
$\lambda 1$: Tasa de llamadas originantes (llamadas/seg)
$\lambda 2$: Tasa de handovers (han/seg)

$$TOUll = \frac{\lambda 1}{\mu}$$
$$TOUha = \frac{\lambda 2}{\mu}$$
$$TOU = TOUll + TOUha$$

Las probabilidades de bloqueo en microceldas con cola en handover que se obtienen son las siguientes:

$$BUll = \left(\frac{1-\left(\frac{TOUha}{N}\right)^{M2+1}}{1-\left(\frac{TOUha}{N}\right)}\right) * \left[N! * \sum_{n=0}^{N-1} \frac{TOU^{n-N}}{n!} + \frac{1-\left(\frac{TOUha}{N}\right)^{M2+1}}{1-\left(\frac{TOUha}{N}\right)}\right]^{-1}$$

$$BUha = \left(\left(\frac{TOUha}{N}\right)^{M2}\right) * \left[N! * \sum_{n=0}^{N-1} \frac{TOU^{n-N}}{n!} + \frac{1-\left(\frac{TOUha}{N}\right)^{M2+1}}{1-\left(\frac{TOUha}{N}\right)}\right]^{-1}$$

3.11.3 Resultados

Finalmente, se muestra mediante gráficas, la probabilidad de bloqueo (Bm) en función del desbordamiento de tráfico en microceldas con cola de handover con sus correspondientes probabilidades de bloqueo. Dado que alrededor del 70 a 80% (Tokyo) de usuarios de terminales móviles son estáticos y el restante tanto por ciento son móviles de alta velocidad (p.e. coches), se ha adoptado un x = 70, el resto de parámetros utilizados en el modelo son los siguientes.

Tráfico ofrecido para establecimiento de llamada, TOUll = 25

Tráfico ofrecido para handover, TOUha = 200

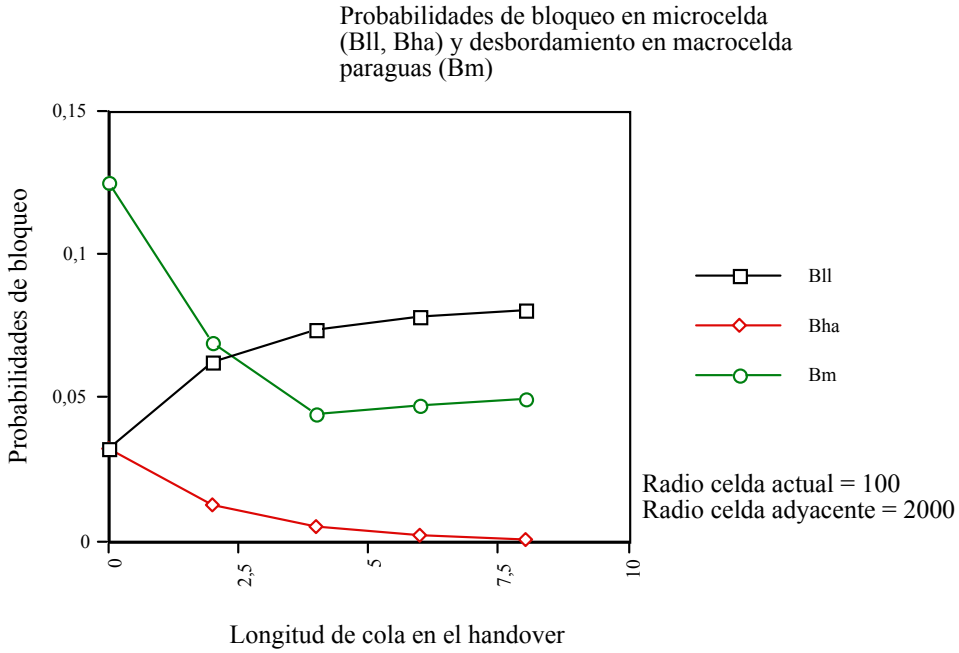
Tamaño cluster macrocelda, CM = 7

Tamaño cluster microceldas, CU = 10

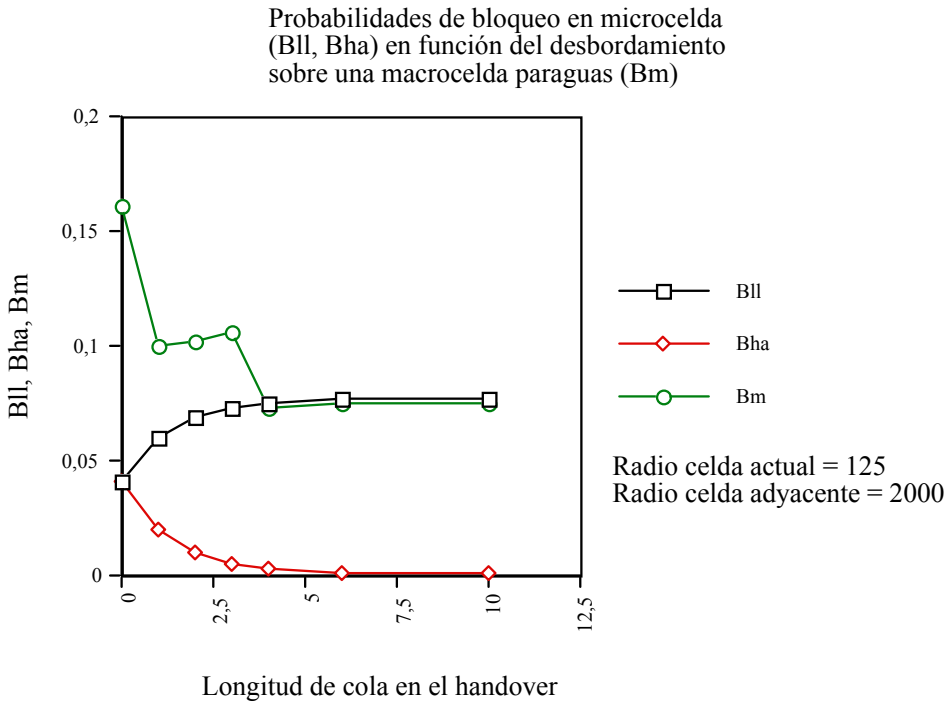
Tanto por ciento de canales en microceldas, x = 70

Número de canales total, C = 295

Distribución de tráfico ofrecido uniforme, TO = 1



Gráfica 3.27 Probabilidad de bloqueo en macrocelda paraguas en función del bloqueo en microceldas (100m).



Gráfica 3.28 Probabilidad de bloqueo en macrocelda paraguas en función del bloqueo en microceldas (125m) para un tráfico ofrecido mayor.

3.11.4 Conclusiones

A la vista de los resultados obtenidos en forma de gráficas, se puede considerar que en general, la probabilidad de bloqueo del sistema crece según aumenta el tráfico ofrecido. Sin embargo, es de notar que el efecto de utilizar microceldas con buffer en las peticiones de handover mejora esa probabilidad de bloqueo para un determinado margen de peticiones antes de la saturación del buffer.

De los resultados obtenidos en otros apartados, también se deduce que las peticiones originadas por usuarios de alta movilidad (p.e. terminales en coches) serían servidas por las macroceldas, mientras que las peticiones originadas por usuarios peatones serían procesadas por las microceldas. El uso de un buffer de tres o cuatro registros para peticiones de handover en las microceldas (e incluso en las macroceldas) mejora notablemente la probabilidad de bloqueo forzada. Las restricciones lógicas en este caso, son que un móvil a determinada velocidad no deja apenas tiempo de procesamiento a la microcelda para determinar los parámetros de handover o renovación de posición por lo que su servicio es redireccionado a macroceldas. Por otra parte, las microceldas permiten dar servicio a zonas de tráfico más intenso, que en su mayor parte son usuarios estáticos.

Es de notar además, que si se aumenta la superficie de solape entre celdas limítrofes también aumenta el margen que se tiene de tiempo de espera de peticiones en cola, con lo que el

tamaño de los buffers de las celdas puede ser mayor al disponer el sistema de más tiempo. Sin embargo, este tipo de situaciones repercuten en un mayor coste del sistema al aumentar el número de celdas para una determinada área.

3.12 Análisis y conclusiones de la función de selección de celdas candidatas

Por último, en este apartado se muestran los resultados correspondientes a las subfunciones que forman la función FHAi que representa la función de selección de celdas candidatas para el handover. Se plantean diversos casos, como el de handover entre celdas del mismo tipo (microceldas) para pasar posteriormente al análisis de handover entre celdas de distinto tipo (picoceldas a microceldas). El caso de macroceldas es en cualquier caso más sencillo de implementar al presentar menores restricciones de tiempo.

Como ya se especificado anteriormente, la función FHAi que describe la selección de celdas candidatas en el handover puede definirse de la siguiente forma:

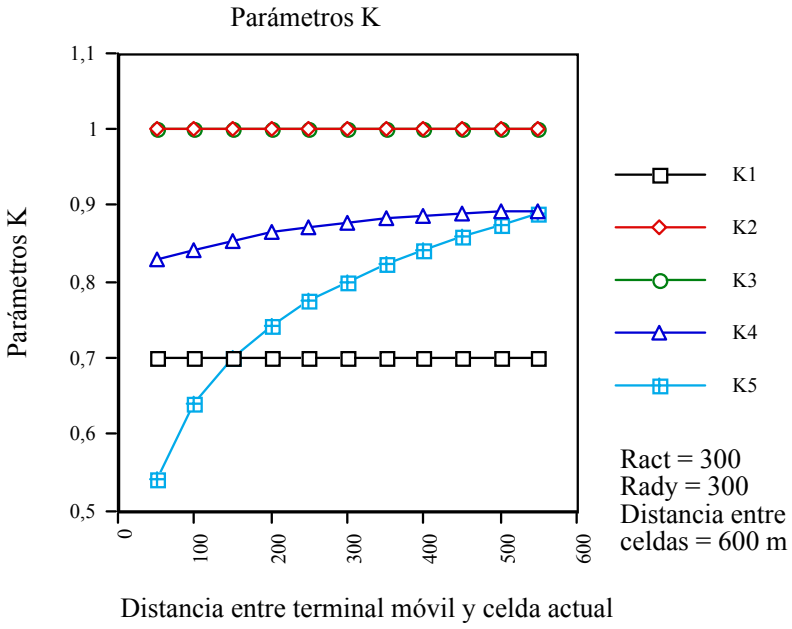
$$FHAi = (f1*K1 + f2*K2 + f3*K3 + f4*K4 + f5*K5)(1 + f6*K6 + f7*K7)$$

Siendo:
K1: Peso correspondiente al número de canales disponibles de la celda.
K2: Peso correspondiente a la distancia entre el terminal móvil y las celdas candidatas.
K3: Peso correspondiente al control de acceso o condición de mismo tipo de celda por parte de la red.
K4: Peso correspondiente a las pérdidas debidas a la señal recibida.
K5: Peso correspondiente a balances de potencia en el terminal móvil o MCPN.
K6: Peso correspondiente a la gestión del handover por acción manual en el terminal móvil.
K7: Peso correspondiente a la importancia de la gestión del handover por parte de la red.

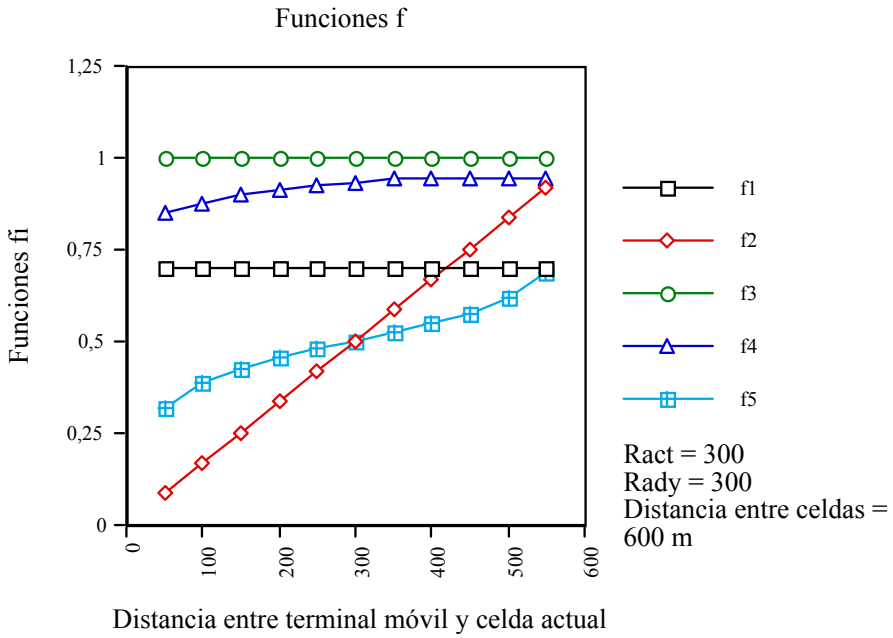
A continuación, se representan mediante gráficas, los parámetros K y las funciones fi correspondientes a la expresión de la función objetivo FHAi.

En las gráficas correspondientes a los parámetros K y fi , se está tratando un escenario formado por dos celdas separadas una distancia de 600 m. Se puede observar un valor de f1 elevado, que indica que la celda candidata tiene una buena disponibilidad de canales y no está congestionada. En cambio, un valor de K1 alto indica que la celda actual está muy congestionada. Todo ello condiciona una contribución alta a la función FHAi beneficiando el handover a esa celda. Por otra parte, un f3 = K2 = K3 = 1 indican que se está haciendo un handover entre celdas en las que la distancia es importante (p.e. como acceso, con lo que K2 = 1) de tipo macroceldas (f3 = 1) y por parte de un terminal de alta movilidad (p.e. vehiculo)

(K3 = 1). Unos valores altos de f4 y K4 indican también que la probabilidad de corte por desvanecimiento es pequeña lo cual es razonable dada la corta distancia entre celdas.

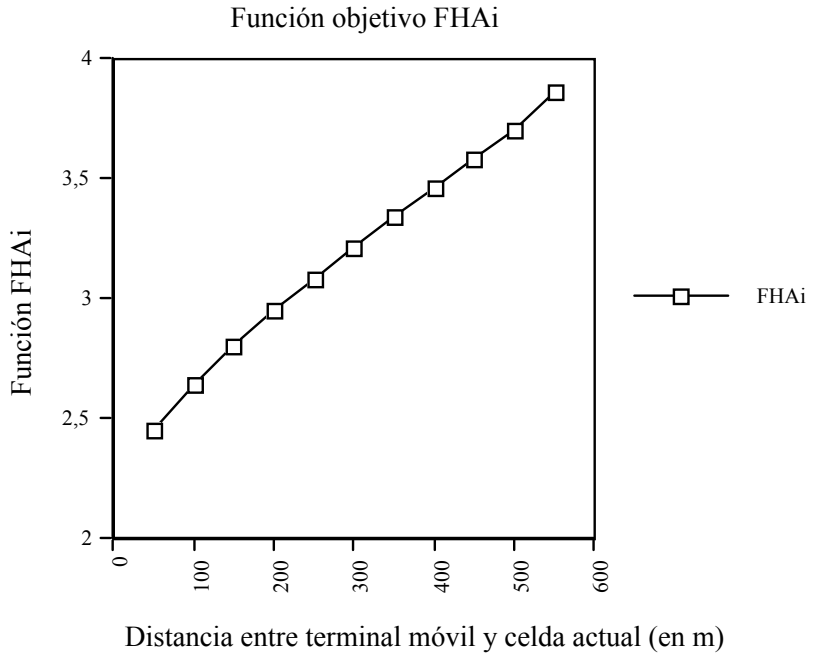


Gráfica 3.29 Parámetros Ki.



Gráfica 3.30 Funciones fi.

La función FHAi, una vez tiene fijados los parámetros relativos al grado de congestión y al control de acceso, crece según aumenta la distancia desde el terminal móvil a la celda actual, teniendo en cuenta el efecto de la atenuación. Ver gráfica.



Gráfica 3.31 Función FHAi según el mismo entorno.

Efectos del tráfico en el handover:

- Caso de un terminal móvil que haya realizado varios handovers en entornos congestionados y encuentra una celda candidata no congestionada respecto a la celda actual. En esta situación, tanto K1 como f1 tendrán valores altos favoreciendo la ejecución del handover a esa celda.

- Caso de un terminal móvil que transita por entornos con poco tráfico y sintoniza una celda congestionada. En esta situación, K1 y f1 son valores muy bajos con lo que se evita que esa celda pueda seleccionarse como candidata para el handover.

Efectos de la distancia y velocidad en el handover:

- El escenario de handover entre macroceldas presenta unas características respecto a tiempo disponible para la selección de celda candidata y ejecución de handover que lo hace muy apropiado para la movilidad de equipos terminales situados en vehiculos, trenes, ... que requieren de un handover muy rápido. Las matrices de parámetros para K2, K3, f2 y f3 reflejan este hecho, donde se potencia el handover de terminales móviles a celdas del mismo tipo cuando la distancia, tiempo o velocidad son parámetros relevantes.

- Se reserva el uso de handovers entre picoceldas y microceldas a los terminales móviles utilizados por peatones o en zonas de alta densidad de usuarios.

Efectos de la atenuación de la señal en el handover:

- K4 y f4 recogen el efecto de los desvanecimientos en la señal, sean de tipo lognormal o de Rayleigh. En general, el parámetro K4 tomará valores elevados cuando se trate la señal recibida en el terminal móvil en puntos alejados de la estación base actual mientras que f4 considera el efecto de la probabilidad de corte respecto la celda adyacente candidata.

- K5 y f5 estiman el efecto de la atenuación de la señal según la distancia entre el terminal móvil y la celda. K5 lo hace de forma relativa entre la celda actual y la celda adyacente considerada mientras que f5 hace una valoración absoluta respecto a un nivel de señal prefijado mínimo de recepción en la celda actual.

Efectos conjuntos:

- Si la potencia recibida en el terminal móvil es alta y se está en un entorno de solapamientos de muchas celdas, por ejemplo, microceldas o picoceldas en centros de ciudades o en determinados edificios de empresas, donde se podría dar macrodiversidad, entonces, las distancias de los móviles a las estaciones base de las celdas no adquieren tanta importancia y por tanto, la determinación de la celda candidata se hace casi exclusivamente por criterios de tráfico o control de acceso.

- Cuando el móvil se encuentra en entornos de mucha atenuación, interesa que los respectivos coeficientes (K4, K5) sean elevados para una correcta selección de celdas. Los parámetros K1, K2 y K3 son menos relevantes.

- En entornos de macroceldas donde la distancia suele ser un factor importante, K2, K3, K4 y K5 configuran la selección de las celdas candidatas.

- Si las probabilidades P_F, P_{nc} o K (número de handovers) registradas en los centros de control de la red fija son elevadas, entonces es que la red se encuentra muy congestionada. PF, Pnc o K también pueden ser elevados si la velocidad del terminal móvil es alta o la duración de la llamada es grande. Estos parámetros afectan en general a K1 y f1, que son obtenidos por las entidades de gestión de red.

- El parámetro K3 relaciona la preferencia de los handovers por un determinado tipo de celda. Es decir, puede actuar a modo de control de acceso a otros dominios o operadores de redes distintas haciendo K3 elevado o nulo. También cobra un especial significado en casos especiales como en la gestión de handovers sobre entornos muy congestionados donde se prima un determinado tipo de celda.

- f6*K6 y f7*k7 tomarán valores elevados o nulos según interese priorizar una determinada celda debida a una selección manual por parte del usuario o priorizar un control de acceso a una determinada celda por parte de la red.

3.13 Fase de ejecución

Una vez se han determinado las celdas candidatas para ejecutar el handover, y obtenido una celda objetivo del handover, procedimiento que se realiza periódicamente, tan sólo resta determinar cuando se ejecuta el handover propiamente dicho. Para ello basta que se produzca cualquiera de las condiciones siguientes:

1. Calidad del enlace
Calidad asegurada para el enlace i > Calidad requerida

2. Pérdidas del radioenlace
Pérdidas del radioenlace (celda actual) - Pérdidas del radioenlace (celda adyacente candidata) > Margen handover;

RSSI(celda actual) < RSSI mínimo.

Las pérdidas del radioenlace son la diferencia de señal transmitida en la estación base respecto de la señal recibida en el terminal móvil.

En carácter especial, el handover también podría ejecutarse por parte de la red por cuestiones de mantenimiento o a petición del terminal móvil por razones derivadas de las características del servicio demandado.

3.14 Fase de ejecución del handover

En este apartado se introduce el protocolo correspondiente a la fase de ejecución, que va a ser la base sobre la cual en los capitulos posteriores va a introducirse una gestión de claves y determinados servicios de seguridad. En la fase de ejecución es donde se realiza el relevo de canales entre celdas propiamente dicho, más exactamente, el control de decisión del handover, que reside en el terminal móvil (MHDC) selecciona el procedimiento (backward o forward) tal como se describe en el proceso P6 de la fase de decisión, y llama a la ejecución del handover (HE), subfunción del RC descrita en el proceso P10 [RACE30].

3.14.1 Forward handover

En este apartado, se describen las funciones y mensajes utilizados en un protocolo de forward handover.

Función P1:

La MHE pide al MLC para establecer un canal DCCH asc/desc para transmisión de señalización durante la ejecución del handover. Mensaje generado:

M1: Comando de creación de portadores enviado desde MRC a MLC para crear DCCH entre MT y la actual BTS2 (nueva BTS).

Tipo de canal: MT interno.

Función P2:

El portador DCCH será establecido usando un procedimiento similar al acceso PRMA++. El MLC y BLC2 (nuevo enlace) son informados que se ha establecido un canal. En la otra cara de la red también se informa a NRC. Mensajes generados:

M2a: Reconocimiento de creación de portadores enviado desde MLC a MRC.

Tipo de canal: MT interno.

M2b: Información de creación de portadores enviado desde BLC2 a NRC.

Tipo de canal: Dentro de la red fija.

M2c: Reconocimiento de creación de portadores enviado desde MRC a MTC.

Tipo de canal: MT interno.

M2d: Información de creación de portadores enviado desde NRC a NTC.

Tipo de canal: Dentro de la red fija.

Función P3:

La subfunción HE de MRC envia la petición de conexión a la nueva BTS (BTS2) ya que el MT conoce el tipo de enlaces. El mensaje se envia via el canal DCCH abierto en P2. Mensajes generados:

M3a: Petición de conexión desde MRC a MRA.

Tipo de canal: MT interno.

M3b: Petición de conexión desde MRA a BRA de BTS2.

Tipo de canal: DCCHu.

Función P4:
La BTS2 envia una confirmación de conexión al MT en la cual se dan las descripciones del nuevo enlace. Se generan los siguientes mensajes:

M4a: Reconocimiento de la confirmación de conexión. Respuesta a M3b.
Tipo de canal: DCCHd.

M4b: Reconocimiento de la confirmación de conexión. El RA informa al MHE que los portadores han sido asignados.
Tipo de canal: MT interno.

Función P5:
Liberación del DCCH entre MT y BTS1.

Función P6:
Se crean nuevos controladores de portadores en MT y en BTS2. Los nuevos canales lógicos (TCH, ACCH, LCCH) son asignados entre el MT y la nueva BTS.

Función P7:
Se informa a la red del nuevo portador asignado. Mensajes generados:

M7a: Información de conexión requerida enviada desde BRA2 a NRA.
Tipo de canal: Dentro de la red fija.

M7b: Información de conexión requerida enviada desde NRA a NRC.
Tipo de canal: Dentro de la red fija.

Función P8:
El MHE enruta la información de usuario a los nuevos enlaces.

Función P9:
Periodo de macrodiversidad.

Entonces, el proceso de liberación de recursos comienza siendo el proceso igual que el procedimiento de backward handover.

Si no se asume macrodiversidad durante el handover, la activación de la subfunción MHT se realiza antes que el proceso P9.

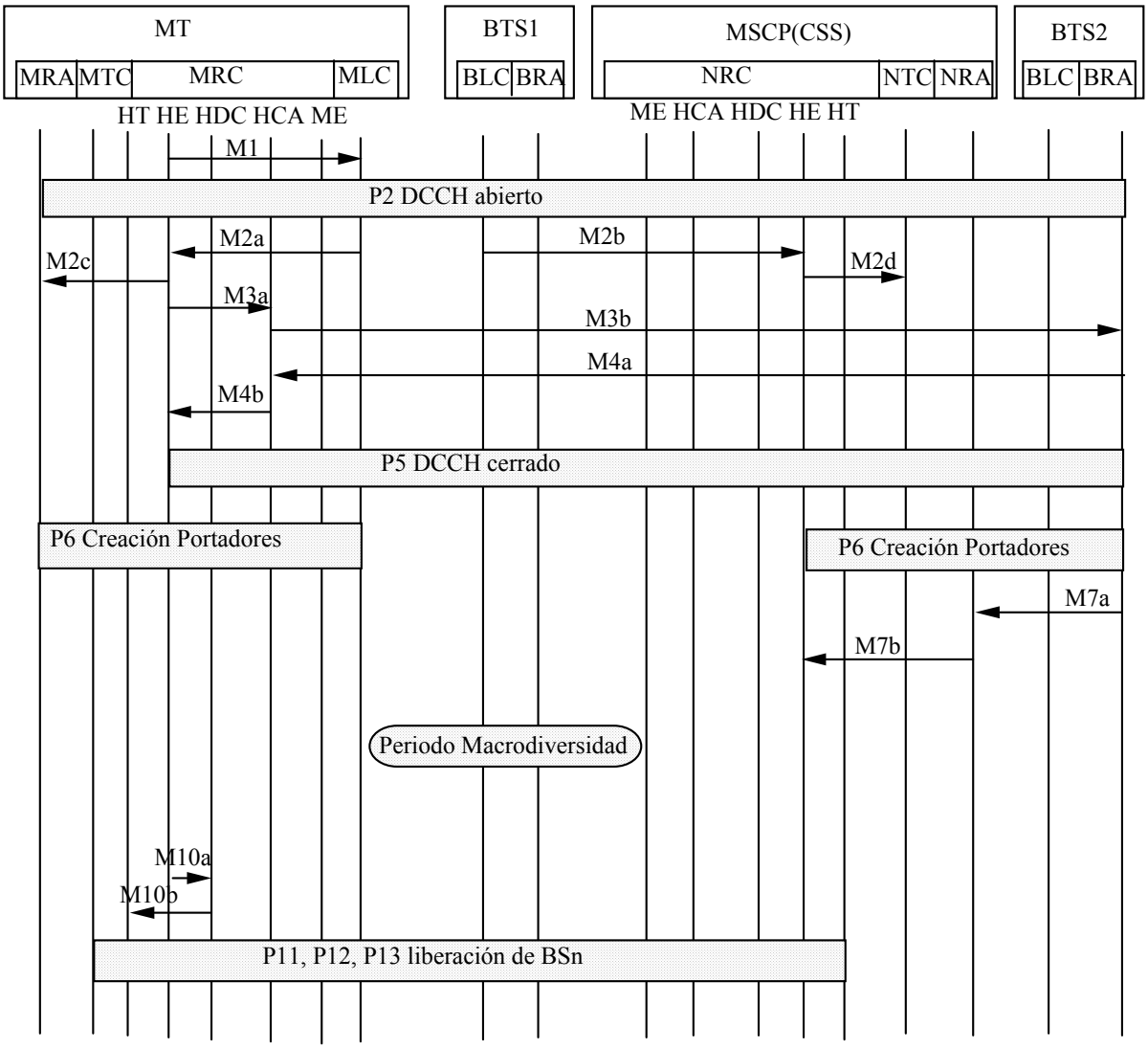


Fig. 3.18 Fase de ejecución del forward handover.

3.14.2 Backward handover

A continuación, se describen las funciones y mensajes utilizados en un protocolo de backward handover.

Función P1:

El MHE pide al MLC para establecer un canal DCCH asc/desc para transmisión de señalización durante la fase de ejecución del HA (el uso del DCCH es temporal). Se genera el siguiente mensaje:

M1: El mensaje es enviado desde el MHE al MLC para crear un DCCH entre el MT y la actual BTS.

Tipo de canal: MT interno

Función P2:

El canal portador DCCH se establece usando el mismo procedimiento que para el acceso PRMA++. El BLC1 es informado de que se establece un canal por el RA y crea el BC. Entonces, se informan RCs y TCs. Se generan los siguientes mensajes:

M2a: Creador de portadores. Es enviado desde MLC a MRC.

Tipo de canal: MT interno

M2b: Creador de portadores. Es enviado desde BLC1 a NRC.

Tipo de canal: Dentro de la red fija

M2c: Creador de portadores. Es enviado desde MRC a MTC.

Tipo de canal: MT interno

M2d: Creador de portadores. Es enviado desde NRC a NTC.

Tipo de canal: Dentro de la red fija.

Función P3:

La subfunción HE de MRC envia la petición de HA a la NRC. La NRC se encarga de la adquisición de recursos en la BTS2 así que pide a la NRA para seleccionar, entre los enlaces objetivos, el nuevo enlace. Mensajes generados:

M3a: Petición de handover de MHE a NHE

Tipo de canal: DCCHu

M3b: Petición de handover de NHE a NRA. La NRA conocería la capacidad necesaria para el nuevo enlace, como la misma de la anterior que es almacenada en NRA.

Tipo de canal: DCCHu

Función P4:

La NRA determina la capacidad necesaria y la información relevante concerniente a los nuevos enlaces y pide éstas al RA de la BTS2 objetivo. Se generan los siguientes mensajes:

M4a: Petición de disponibilidad de recursos enviada desde NRA a BRA2.

Tipo de canal: Dentro de la red fija.

M4b: Reconocimiento a la disponibilidad de recursos enviada desde NRA a BRA2. Proporciona información del nuevo enlace.

Tipo de canal: Dentro de la red fija.

Función P5:

La red envia al MT un mensaje de reconocimiento positivo o negativo. Si es positivo, el MT recibe la descripción del nuevo enlace objetivo con BTS2. Mensajes generados:

M5a: Reconocimiento del handover requerido. Respuesta al mensaje M3b, es enviada a NHE.

Tipo de canal: Dentro de la red fija.

M5b: Reconocimiento a la confirmación de handover. Respuesta a M3a, va desde NHE a MHE.

Tipo de canal: DCCHd.

Función P6:

Liberación del DCCH entre el MT y la BTS1.

Función P7:

Nuevos controladores de portadores se crean en MT y en BTS2. Los nuevos canales lógicos (TCH, ACCH y LCCH) se disponen entre MT y la nueva BTS.

Función P8:

El MHE enruta la información de usuario a los nuevos enlaces. Mensajes generados:

M8a: Comando de acceso al handover.

Tipo de canal: Interno al MT.

M8b: Comando de acceso al handover.
Tipo de canal: Nuevo TCHu.

M8a y M8b muestran la confirmación del nuevo enlace. La información es enviada desde el MT a la BTS2.

M8c: Detección de handover. El mensaje muestra la información previamente enviada a NRC via la BTS2
Tipo de canal: Dentro de la red fija.

Función P9:
Periodo de macrodiversidad

Función P10:
El MHE transmite un mensaje tipo de reconocimiento a la subfunción MHDC, que decide que enlaces han de ser liberados por la activación de la subfunción MHT. La determinación de qué enlaces han de ser liberados está basada en el criterio de los enlaces objetivos. Mensajes generados:

M10a: Es el reconocimiento del tipo de mensajes enviados por MHE a MHDC
Tipo de canal: MRC interno.

M10b: Es el comando de activación enviado por MHDC a MHT
Tipo de canal: MRC interno.

Si no se asume macrodiversidad durante el HA, el mensaje M10b y el proceso P11 se envian justo después del proceso P8 y el mensaje correspondiente M8c.

Función P11:
El MHT se empieza por el MHDC y interactua con el grupo funcional LC.
- Si hay macrodiversidad, MHT se activa después del periodo de macrodiversidad y determina que enlaces liberar.
- Si no hay macrodiversidad, MHT se activa antes del periodo de macrodiversidad y no determina que enlaces liberar (es tarea del MHDC).
En cualquier caso, una vez que se determina el enlace liberado, el MHT envia el comando de liberación a NHT via LC de BTS1 ó BTS2 usando respectivamente los enlaces anteriores o nuevos. Mensajes generados:

M11: Comando de liberación de BTS enviado por MHT a MLC.
Tipo de canal: MT interno.

En este punto se presentan dos procesos P12 y P13 que son alternativos.

Función P12:
En este caso, el MLC envia la liberación de recursos usando el interfaz aire que podría ser liberado. Mensajes generados:

M12a: Comando de liberación de BTS enviado desde MLC a BLC de la anterior BTS (BTS que controla el enlace liberado).
Tipo de canal: En señalización de banda.

M12b: Comando de liberación de BTS enviado desde BLC de la anterior BTS a NHT para informar al NRC acerca del enlace liberado.
Tipo de canal: Dentro de la red fija.

Función P13:
Se ejecuta en el caso de que el MLC envie la liberación de recursos usando el interfaz aire que es mantenido (o no liberado). Mensajes generados:

M13a: Comando de liberación de BTS enviado desde MLC a BLC de la nueva BTS (BTS que controla el enlace mantenido).
Tipo de canal: En señalización de banda.

M13b: Comando de liberación de BTS enviado desde BLC de la nueva BTS a NHT para informar al NRC acerca del enlace liberado y enrutar el comando liberado al BLC de la anterior BTS.
Tipo de canal: Dentro de la red fija.

M13c: Comando de liberación de BTS enviado a la BLC de la anterior BTS.
Tipo de canal: Dentro de la red fija.

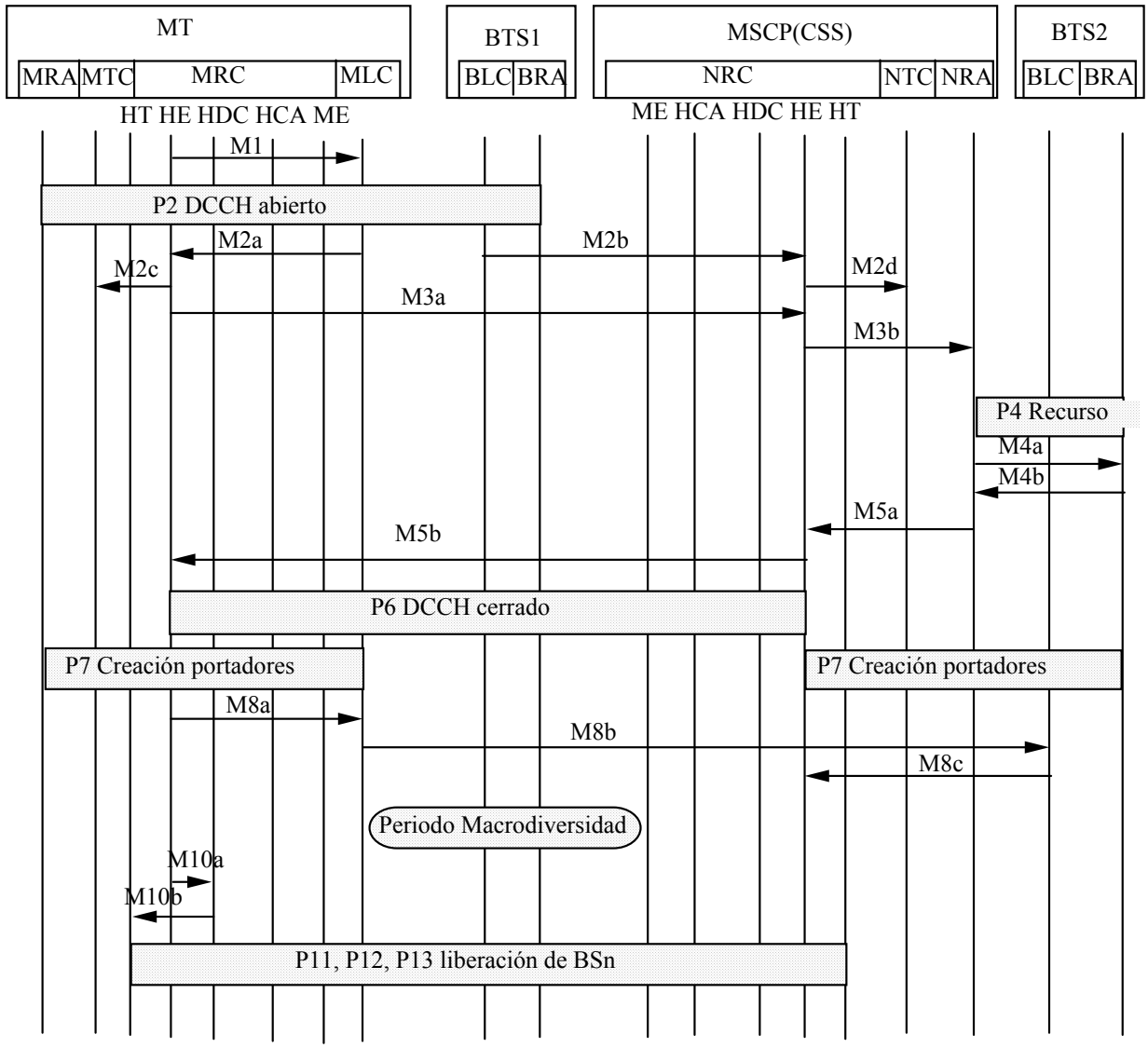


Fig. 3.19 Fase de ejecución del backward handover.

3.15 Contribuciones al capitulo

En este capitulo, se propone un algoritmo de decisión para el handover entre celdas, donde se integra un procedimiento de selección previa de celdas candidatas para el handover [AB11-12].

Se especifican los parámetros y su distribución sobre el radioenlace, se incorpora una gestión de claves y se estudian los periodos de medición para una adecuada respuesta dados unos determinados requerimientos temporales (p.e. frecuencia de fadings o tramas).

Se utiliza una arquitectura de control del handover UMTS a la que se incorporan funcionalidades de seguridad. Este soporte permite implementar el algoritmo de selección de celdas candidatas (función FHAi) donde se especifican los parámetros fi y Ki.

Se presentan diversos análisis para la determinación de estos parámetros fi, Ki donde destaca especialmente la definición de K1 y f1 al tener en cuenta sistemáticamente los niveles de tráfico y congestión en la red. Estos parámetros hacen uso de un entorno de gestión de red inteligente [AB3] donde se plantea un escenario basado en clusters de macroceldas donde se integran microceldas con buffers para evitar pérdidas debidas al establecimiento de llamada o al handover. Se realizan diversas simulaciones para la determinación de escenarios y situaciones de tráfico óptimas [AB10-12].

3.16 Referencias

[AB10] A. Barba y J. L. Melús. *Cell management in the handover.* International Conference on Personal Wireless Communications (ICPWC´95), Sidney (Canada), Junio 1995.

[AB11] A. Barba y J. L. Melús. *Decision phase of a forward handover in an intelligent mobile network.* Wireless ´95, p. 489-499, Calgary, Julio 1995.

[AB12] A. Barba y J. L. Melús. *Traffic evaluation in the decision phase of a handover.* Fourth IEEE International Conference on Universal Communications (ICUPC´95) p. 354-358. Tokyo, Noviembre 1995.

[AF1] A. A. Fredericks. *Congestion in blocking systems- A simple approximation technique.* p. 805-827. The Bell System Technical Journal (AT&T). Julio-Agosto 1980.

[AV2] Andrew Viterbi, Audrey Viterbi, Klein S. Gilhousen and Ephraim Zehavi. *Soft handoff extends CDMA cell coverage and increases reverse link capacity.* International Zurich Seminar on Digital Communications *,* Zurich 1994.

[BG1] Bjorn Gudmundson and Olle Grimlund. *Handoff microcellular based personal telephone systems.* Third Generation Wireless Information Networks. Editores Nanda/Goodman. Ed. Kluwer 1992.

[CL1] C. Lau, W. C. Chan. *A new handoff algorithm for indoor cellular systems using outage probability.* p. 627-631. Wireless´94. Calgary, 1994.

[DA1] D. K. Anvekar, P. Agrawal, B. Narendran. *A traffic-driven channel reservation scheme for handovers in mobile cellular networks.* p. 422-434, Wireless´94, Calgary, 1994.

[DM1] David McMillan. *Traffic modelling and analysis for cellular mobile networks.* p. 627-632. Teletraffic and Datatraffic ITC-13. 1991.

[DP1] David Parsons. *The mobile radio propagation channel.* Ed Pentech Press. Londres, 1992.

[EM1] E. D. Murray, P. Blanc, F. de Ryck and U. Dropmann. *The ATDMA global simulation testbed.* p. 221-225. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[GS1] Gamini N. Senarath and David Everitt. *Combined analysis of transmission and traffic characteristics in micro-cellular mobile communication systems.* p. 577-580. 43th VTC Secaucus NJ, 1993.

[GS2] Gamini N. Senarath and David Everitt. *Comparison of alternative handoff strategies for micro-cellular mobile communication systems.* p. 1465-1469, 44th VTC Estocolmo, 1994.

[GS3] Gamini N. Senarath and David Everitt. *Performance of handover priority and queueing systems under different handover request strategies for microcellular mobile communication systems.* p. 897-901. 45th VTC Chicago, 1995.

[GS4] Gamini N. Senarath and David Everitt. *Handover performance; Propagation and traffic issues.* p. 87-100. Winlab 95. New Jersey. 1995.

[HX1] Hai Xie y Simon Kuek. *Priority handoff analysis.* p. 855-858. 43th VTC . 1993.

[JD1] John N. Daigle, Nikhil Jain. *A queueing system with two arrival streams and reserved servers with application to cellular telephone.* p. 2161-2167, INFOCOM´92.

[KB1] K. J. Bye. *Handover criteria and control in cellular and microcellular systems*. p. 94-98. 5º IEE Mobile radio and personal communications. 1989.

[KI1] Kolio Ivanov, Gustav Spring. *Mobile speed sensitive handover in a mixed cell environment.* p. 892-896. 45th VTC Chicago, 1995.

[KL1] Kwan L. Yeung, Sanjiv Nanda. *Optimal Mobile-determined micro-macro cell selection.* PIMRC´95, Toronto, 1995.

[KM1] K. Madani, A. H. Aghvami. *Investigation of handover in distributed control channel allocation (DCCA) for microcellular radio systems.* PIMRC´94. p. 160-163.

[KS1] Kevin W. Soerby and Allan G. Williamson. *Outage probabilities in mobile radio systems suffering cochannel interference.* IEEE Journal on selected areas in communications. p. 516-522. Abril 1992.

[KW1] Kenneth Wallstedt, Magnus Almgren, Hakan Andersson and Olle Grimlund. *Micro cellular performance in a TDMA system.* p. 293-296. 43th VTC Secaucus NJ. 1993.

[LE1] W. C. Y. Lee. Mobile Cellular Telecommunications Systems. New York. Ed. McGraw-Hill, 1989.

[MF1] M. Frullone, G. Riva, P. Grazioso, C. Carciofi. *Analysis of optimum resource management strategies in layered cellular structures.* p. 371-375. ICUPC´94.

[MZ1] Mahmood M. Zonoozi, Prem Dassanayake and Michael Faulkner. *Effect of mobility on the traffic analysis in cellular mobile networks.* p.407-410. SICON/ICIE ´95 Singapur.

[PA1] P. Agrawal, D. K. Anvekar, B. Narendran. *Optimal prioritization of handovers in mobile cellular networks.* p. 1393-1398. PIMRC´94.

[PB1] Patrick Blanc, Sami Tabbane, Eric Murray. *Handover procedure evaluation in the G-STB*. p. 467-471. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[PE1] Per-Erik-Ostling. Implications of cell planning on handoff performance in Manhattan environments. p. 625-629. PIMRC´94.

[QZ1] Qing-An Zeng, Kaiji Mukumoto and Akira Fukuda. *Performance analysis of mobile cellular radio system with priority reservation handoff procedures.* p. 1829-1833. 44th VTC Estocolmo, 1994.

[QZ2] Qing-An Zeng, Kaiji Mukumoto and Akira Fukuda. *Influence of cell radius, moving speed and duration of calls on handoff rate in cellular mobile radio systems.* p. 511-520. Wireless´95, Calgary, 1995.

[RACE27] RACE 2084/CNET/TS3/DN/I/021/a1. Handover and macrodiversity section of CEC Deliverable number 27. Febrero 1994.

[RACE28] RACE 2084/ART/PM2/DS/R/016/a1. ATDMA System definition. Julio 1993.

[RACE29] RACE 2084/CNET/TS3/DN/I/011/a1. Routing controller section of the functional groups. Definition document. Febrero 1994.

[RACE30] RACE 2084/FACE/TS3/DN/I/012/a1. Annex 5. Handover procedures. Enero 1994.

[RG1] Roch A. Guérin. *Channel occupancy time distribution in a cellular radio system.* IEEE Transactions on Vehicular Technology. p. 89-99. Agosto 1987.

[SC1] S. T. S. Chia. *A handover protocol for a mixed cell system.* p. 225-232. 6º IEE Mobile radio and personal communications.

[SC2] S. T. Stanley Chia, William Johnston. *Performance of outdoor to indoor handover.* p. 1836-1839. ICC´92.

[SD1] Szalajski D. *Handover optimisation within ATDMA*. RACE Mobile Telecommunications Summit. p. 212-217. Cascais (Portugal) 1995.

[SF1] Satoru Fukumoto, Duk-Kyu Park et al. *Dynamic channel assignment using a channel framework for traffic congestion in a highway micro cellular system.* p.164-168. PIMRC´94.

[SK1] P. Sarath Kumar, Jack Holtzman. *Analysis of handoff algorithms using both bit error rate (BER) and relative signal strength.* p. 1-5, ICUPC´94, San Diego.

[SN1] Sanjiv Nanda. *Teletraffic models for urban and suburban microcells: cell sites and handoff rates.* p. 251-260.

[SS1] Daehyoung Hong and Stephen S. Rappaport. *Traffic model and performance analysis for cellular mobile radio telephone systems with prioritized and nonprioritized handoff procedures.* IEEE Transactions on Vehicular Technology. p. 77-92. Agosto 1986.

[SS2] Lon-Rong Hu y Stephen S. Rappaport. *Micro-cellular communication systems with hierarchical macrocells overlays: Traffic performance models and analysis.* p. 143- 174. Winlab Workshop 1993. New Jersey.

[SS3] Cezary Purzynski and Stephen S. Rappaport. *Traffic performance analysis for cellular communication systems with mixed platform types and queued hand-offs.* p. 172-175. 43th VTC. 1993.

[SS4] Tai-Po Chu and Stephen S. Rappaport. *Generalized fixed channel assignment with hand-off priority in micro-cellular communication systems.* p.607-610. 43th VTC. 1993.

[SS5] Hua Jiang and Stephen S. Rappaport. *Hand-off analysis for CBWL schemes in cellular communications.* p. 496-500. ICUPC´94, San Diego, 1994.

[ST1] Sirin Tekinay and Bijan Jabbari. *Handover and channel assignment in mobile cellular networks.* IEEE Communications Magazine. p. 42-46. Noviembre 1991.

[ST2] Sirin Tekinay and Bijan Jabbari. *A measurement-based prioritization scheme for handovers in mobile cellular networks.* IEEE Journal on selected areas in communications. p. 1343-1350. Octubre 1992.

[ST3] Sirin Tekinay. *A new mobility model for estimating channel holding times in wireless systems.* PIMRC´95. Toronto, 1995.

[TF1] Teruya Fujii y Seiji Nishioka. *Selective handover for traffic balance in mobile radio communications.* ICC´92, p. 1840-1846. 1992.

[XL1] X. Lagrange, P. Godlewski. *Control channel structures in a third generation ATDMA system.* p. 190-192. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[XL2] X. Lagrange and P. Godlewski. *Teletraffic analysis of a hierarchical cellular network.* p. 882-886. 45 th VTC Chicago, 1995.

[YB1] Yi-Bing Lin, Anthony Noerpel and Daniel Harasty. *A non blocking channel assignment stategy for hand-offs.* p. 558-562, ICUPC´94, San Diego, 1994.

[YB2] Yi-Bing Lin, Seshadri Mohan and Anthony Noerpel. *Queueing channel assignment strategies for PCS hand-off and initial access.* p. 365-369. ICUPC´94, San Diego, 1994.

[YB3] Yi-Bing Lin, Seshadri Mohan and Anthony Noerpel. *PCS channel assignment strategies for hand-off and initial access.* IEEE Personal Communications. p. 47-56. 3º trim. 1994.

[ZH1] Zygmunt J. Haas, Jack H. Winters and David S. Johnson. *Simulation study of the capacity bounds in cellular systems.* PIMRC´94. p.1114-1120.

Capitulo 4

Aplicación de seguridad en el handover

4.1 Introducción

En este capítulo, se definen unos requerimientos generales que permitan acometer la adecuada provisión de seguridad en el sistema UMTS y en particular, en el handover tal como se planteó en el primer capitulo. Desde este punto de vista se hace una breve descripción de como se han implementado previamente los mecanismos de seguridad en el handover en redes digitales como GSM o DECT.

Se estudian las amenazas, servicios y mecanismos de seguridad requeridos en el handover para que éste sea seguro sobre una arquitectura de red móvil avanzada. Posteriormente, se hace un análisis de los mecanismos propuestos, enumerando las ventajas que supone el uso de mecanismos de clave pública frente a clave secreta. También se muestran las alternativas con una serie de escenarios propuestos.

Se contrasta la estructura de red fija en UMTS con la red jerárquica distribuida de la recomendación X.500. A raíz de las similitudes detectadas a nivel de arquitectura y protocolos utilizados, se propone el uso de una determinada arquitectura de seguridad basada en una solución híbrida. Por un lado, se propone el uso de algoritmos de clave pública para la protección de la señalización en el sistema móvil celular UMTS y por el otro lado, se usan algoritmos de clave secreta para la protección de información a nivel de usuario [AB5].

El uso de algoritmos de clave pública en redes móviles es claramente innovador puesto que hasta la fecha ninguna red los está empleando para protección de la información transmitida [DB2].

Aparte de las consideraciones estrictamente de seguridad que puede plantear el uso de algoritmos de clave pública para protección de la señalización, se plantea su validación a nivel de prestaciones en un procedimiento de movilidad crítico como es el handover. Posteriormente se determina la disposición de las claves en las entidades funcionales y en los componentes del sistema. En los siguientes capitulos se analizará con más detalle como se realiza la gestión de claves para proporcionar los servicios de seguridad y tener un handover óptimo.

4.2 Amenazas en el handover

A continuación, se especifica una relación detallada de amenazas que afectan directamente al mecanismo del handover. Posteriormente, se especificarán los servicios de seguridad en el protocolo de handover para poder disponer de un sistema seguro integralmente como en el sistema UMTS [RACE2, 6].

La siguiente lista trata de reunir los casos de amenazas más importantes que afectan al handover en UMTS.

Pérdida de confidencialidad:
- Escucha no autorizada de identificadores de terminal y de usuario
- Escucha no autorizada de información de perfil de servicio
- Escucha no autorizada de información de localización
- Escucha no autorizada de datos de seguridad relacionados con la autentificación
- Escucha no autorizada de claves de cifrado

Pérdida de integridad
- Manipulación de identificadores de terminal, usuario y/o información de localización
- Manipulación de información de perfil de servicio (caso de control de acceso)
- Manipulación de datos de seguridad relacionados con la autentificación

Suplantación y acceso no autorizado
- Suplantación como un terminal diferente
- Suplantación como una entidad de red diferente en el radioenlace
- Acceso no autorizado a subredes
- Suplantación como una estación base móvil hacia la red fija
- Suplantación de una estación base fija hacia una estación base móvil
- Suplantación como una entidad de red diferente en la misma subred
- Suplantación como una entidad de red diferente entre subredes diferentes

- Acceso no autorizado a datos concerniendo a derechos de acceso o a datos de seguridad
- Acceso no autorizado a datos en la base de datos distribuida
- Suplantación o acceso no autorizado a información de seguridad relacionada con gestión de seguridad residiendo en el SID, MSCP o MSDP.
- Modificación no autorizada de información de perfil de servicio.

4.3 Mecanismos de seguridad en el handover en redes de la segunda generación

Dentro de las redes móviles de la segunda generación [TIA1, MM2, JB1, DW1, UPT1-2], se expondrán únicamente los casos de las redes GSM y DECT por ser las más importantes en cuanto a integración de seguridad y formar parte de las iniciativas desarrolladas en el entorno europeo [AB7-8].

El sistema GSM

GSM, en principio, no soporta servicios de integridad ni de tarificación incontestable. Por tanto, se tratarán únicamente los servicios de confidencialidad y autentificación [ETSI1-8].

Confidencialidad:

GSM utiliza algoritmos de clave secreta en todos sus procedimientos de movilidad. Los datos se encriptan solamente en el radioenlace, entre el terminal móvil y la BTS. La información que se protege es la de usuario y determinado tipo de señalización.

La clave de cifrado para la conexión se puede obtener de dos formas, usando la última clave de cifrado adquirida en el radioenlace a través del número de secuencia o bien, creando una nueva clave.

Para comenzar el cifrado, la red envia un comando de cifrado al terminal. El terminal al recibir el comando activa tanto el cifrado como el descifrado respondiendo a la BTS que a partir de ese momento puede comenzar con el cifrado. El algoritmo de cifrado utilizado es del tipo de cifrado en flujo (A5), idéntico en toda la red GSM.

En cuanto a la gestión de claves, es obligatorio cambiar la clave de cifrado en:

- Cada registro
- En algunos establecimientos de conexión, donde la frecuencia es responsabilidad del operador de red.
- En algunos servicios suplementarios, por ejemplo en activaciones y desactivaciones.
- Cierto tipo de renovación de localización (location updating), como cuando se cambia de identificadores.

La confidencialidad de la identidad del abonado así como de otras identidades se realiza en la mayor parte de las ocasiones mediante identificadores temporales. La identificación completa no se usa a menos que los identificadores temporales no sean accesibles, esto es, debido en general, a malfuncionamiento de la red o a que no se encuentra en el terminal o en la red. Los identificadores temporales suelen cambiarse con las renovaciones en los registros ('location updating').

Las siguientes identidades sólo se transmiten en modo cifrado sobre el radioenlace: identidad del equipo, identidad del usuario, identidad del abonado, números del llamante y llamado, mientras que algunos datos de señalización se envian a veces por el radioenlace en modo no cifrado (identidad real).

En el caso de almacenar las claves master en los VLR, en lugar del centro de autentificación hace aumentar los riesgos para el sistema.

Autentificación:
En principio, no se activa la autentificación del abonado en el handover cuando la conexión se controla todavía por la MSC/VLR anterior.

Aplicación al handover:
Las claves de cifrado, no se cambian en los handover. La clave de cifrado y los datos de inicialización se envian desde la anterior BTS a la nueva BTS, no necesariamente desde la red en la que se está abonado. La sincronización se mantiene a través del número de trama.

Por otra parte, al no haber handover entre redes diferentes, tampoco se requiere la invocación de autentificación.

El sistema DECT
En principio, el estándar DECT no soporta servicios de integridad ni de tarificación incontestable. En el handover únicamente es relevante el servicio de confidencialidad [PO1, DECT1-2].

Confidencialidad:
Se proporciona confidencialidad de datos de usuario y de ciertos datos de control. El servicio es pedido a nivel de red y ofrecido a nivel de MAC.

La confidencialidad se proporciona a través de un algoritmo de cifrado simétrico entre la terminación de radio fija y la terminación de radio portable. La clave de cifrado puede

obtenerse a través de la terminación de radio fija y la terminación de radio portable como parte de la autentificación, o bien estáticamente, como por ejemplo, manualmente (no recomendable).

El cifrado puede habilitarse o no según ciertas circunstancias como en el handover.

Autentificación:
En principio, no se invocan autentificaciones en el handover.

Aplicación al handover:
En DECT se pueden distinguir tres tipos de handover: Handover intra-celda, handover inter-celda interno y handover inter-celda externo.

El handover intra-celda es un cambio de canales físicos dentro de una celda, comportando un handover de un servicio portador.

El handover inter-celda interno es un cambio de estaciones base (celdas) perteneciendo a la misma terminación fija. Constituye un handover de un servicio portador y un handover de conexión.

El handover inter-celda externo es un cambio de estaciones base (celdas) perteneciendo a diferentes terminaciones fijas. Sólo es posible si los sistemas DECT están conectadas a una misma entidad de gestión. Constituye un handover externo.

En principio, el handover entre diferentes entornos (por ejemplo, negocios a público) no es posible. A continuación, se exponen estos tres tipos de handover desde el punto de vista de seguridad:

a) Handover de un servicio portador
Un portador MAC es un elemento de servicio correspondiente a una única instancia de servicio en el nivel físico. En este caso, el cifrado no es interrumpido. La conmutación de un canal físico a otro es completamente interno a una terminación de radio fija.

b) Handover de conexión
Una conexión MAC es una asociación entre una entidad fuente y destino MAC MBC, esto proporciona un conjunto de canales lógicos, y comporta uno o más portadores MAC. En este caso, el cifrado no se interrumpe.

El handover se realiza asignando una segunda y nueva conexión, mientras se mantiene la anterior. La comunicación en la nueva conexión es primero en modo deshabilitado, usando los comandos de nivel MAC, posteriormente se habilita el cifrado a la vez que se libera la conexión anterior. Es responsabilidad de la terminación fija asegurarse que ninguna información sensible sea transmitida durante el modo deshabilitado.

c) Handover externo
Es el proceso de conmutar una llamada en progreso desde una terminación fija a otra fija. El cifrado es interrumpido y el handover se realiza en modo deshabilitado. La conmutación se realiza usando los comandos del procedimiento de conmutación a nivel MAC. Una vez el handover es completado, la terminación fija vuelve a conmutar al modo cifrado.

Si la clave de cifrado puede transferirse a través de la red fija entonces se considera un handover 'seamless' como un handover de conexión usando la misma clave. Si esa transferencia no es posible, entonces el servicio de confidencialidad debe ser reinvocado y establecerse una nueva clave de cifrado. Si se usa una misma clave de cifrado dinámica, se requiere una reautentificación.

4.4 Requerimientos de seguridad en la red UMTS

A continuación, se especifican una serie de afirmaciones, válidas para toda subred UMTS y que constituyen unos requerimientos generales de seguridad para todo el sistema. Estas especificaciones de definieron primero en el programa marco MONET del RACE sobre la red UMTS y se considera que siguen siendo válidas para nuestros propósitos [AB2-4, RACE2-6].

- El nivel de seguridad de UMTS no debe ser menor que el nivel de seguridad de la red fija.
- Las medidas de seguridad deben garantizar un alto nivel de confidencialidad, integridad y disponibilidad de información sensible y recursos relacionados con UMTS.
- Las medidas de seguridad deben prevenir o detectar la aparición de fallos en seguridad o minimizar las consecuencias de fallos de seguridad relacionados con información sensible y de recursos en UMTS.
- El nivel de seguridad debe ser mantenible y adaptable sobre un largo periodo de tiempo.

Obsérvese el alto grado de dificultad que entraña el mantener tan sólo la primera especificación a un nivel razonable de validación. Por tanto, se requiere primero de un estudio de la red fija para un acercamiento adecuado a la solución del problema.

4.5 Seguridad en X.509 y en UMTS

Se van a definir las funcionalidades de seguridad desarrolladas en X.509 para posteriormente compararlas con la especificaciones proporcionadas en UMTS. Las áreas de seguridad definidas en X.500 (X.509) son la autentificación y la autorización o control de acceso. Asimismo, muchas de las operaciones de directorio pueden ser opcionalmente firmadas por un mecanismo de firma digital para identificación del originador [ITUT3] (Ver anexo 5).

Autentificación

Si bien existen operaciones en X.500 que permiten identificar la identidad de usuarios/entidades, como 'Directory Bind' o la operación 'read', no imponen restricciones en los tipos de acceso permitidos.

La recomendación X.509 define un marco de trabajo para la provisión de servicios de autentificación por el directorio a sus usuarios y describe cómo el directorio puede almacenar y obtener información de autentificación. Se describen dos niveles en la Autentificación.

- Autentificación Simple:

Utiliza un "password" y el "distinguished name" del usuario como una verificación de la identidad reclamada. Ámbos se envian al directorio donde se comparan con los valores almacenados en éste.

- Autentificación Fuerte:

Este tipo de autentificación está basada en criptosistemas de clave pública, pero no dependientes de un algoritmo criptográfico en particular. Una autoridad de certificación (que es una entidad separada del DSA) genera certificados de usuario y se mantienen como atributos en el directorio. No existen requerimientos especiales a tener en cuenta en los proveedores de directorios para almacenar o comunicar certificados de usuario en una forma segura. Sin embargo, los protocolos de intercambio requeridos para soportar la distribución y gestión de la información de autentificación están actualmente fuera del ámbito del estándar.

Autorización

La autorización proporciona un método para restringir el ámbito de cuestiones y operaciones sobre datos almacenados en el directorio. Previene la detección no autorizada, examen, y modificación de información mantenida en un subarbol entero del DIT, una entrada individual, un atributo entero dentro una entrada o instancias seleccionadas de valores de atributos.

Respecto a la autorización, los protocolos DAP y DSP soportan la obtención de información que indican los derechos de acceso sobre un bloque de datos. Sin embargo, los protocolos X.500 no soportan la gestión del control de acceso. Las categorias de control de acceso soportadas por X.500 son las siguientes:

- Detect: Permite al item protegido ser detectado.
- Compare: Permite al valor presentado ser comparado con el item protegido.
- Read: Permite al item protegido ser leido
- Modify: Permite al item protegido ser renovado.
- Add/Delete: Permite la creación y borrado de nuevos componentes (atributos o grupos de atributos) dentro del item protegido.
- Naming: Permite la modificación del RDN, y la creación y borrado de entradas inmediatamente subordinadas a la entrada protegida.

Aplicación a UMTS

Existen diversas opciones para realizar funcionalidades en UMTS de forma segura según las características de los protocolos X.500. A continuación. se describen algunas de las características distintivas que pueden aprovecharse:

- Las operaciones de 'Directory Binding' podrían ser utilizadas para autentificación de los nodos DDB en UMTS antes de una asociación de establecimiento.
- La información de autentificación llevada en la operación Read podría soportar un mecanismo para la verificación de la identidad de usuario UMTS.
- Cada operación en el protocolo DAP puede ser opcionalmente firmada por su iniciador. De forma que la firma digital podría prevenir el acceso no autorizado a las DDB UMTS y comunicaciones no autorizadas entre diversos operadores de red.
- Existen mecanismos de control de acceso incluidos en X.500 que pueden operar entre las DDB (diferentes dominios) en UMTS, en cambio, no está definida la gestión del servicio.

Por tanto, se puede concluir que dada la similitud entre ambas arquitecturas, parece factible a priori, el utilizar una estructura de directorios de certificados que permita el uso de algoritmos de clave pública para la protección de la señalización del sistema. A continuación, pues, se procederá a detallar más esta arquitectura de seguridad para UMTS.

4.6 Arquitectura de seguridad UMTS

En las secciones previas se ha analizado la arquitectura, componentes y otras características que definen UMTS. En esta parte se proponen una serie de componentes especiales que permiten formar una arquitectura de seguridad en la red [AB2-5].

Existen componentes como centros de conmutación, estaciones base, terminales móviles, etc donde determinada información de seguridad, por ejemplo claves de cifrado, se emplea para proporcionar servicios de seguridad. Por otra parte, existen entidades especiales que permiten desarrollar exclusivamente las funcionalidades específicas de seguridad y que sirven de apoyo a las primeras. Entre ellas se puede destacar:

- Dispositivo de identidad de abonado (Subscription Identity Device (SID))
- Centro de autentificación
- Centro de seguridad
- Autoridad de certificación
- Directorios de certificados

Existen otras entidades menores que suelen estar integradas con las anteriores, tales como: centro de notarizacion, centro de generación de claves, autoridad de personalización, autoridad de registro y centro de listas de revocación.

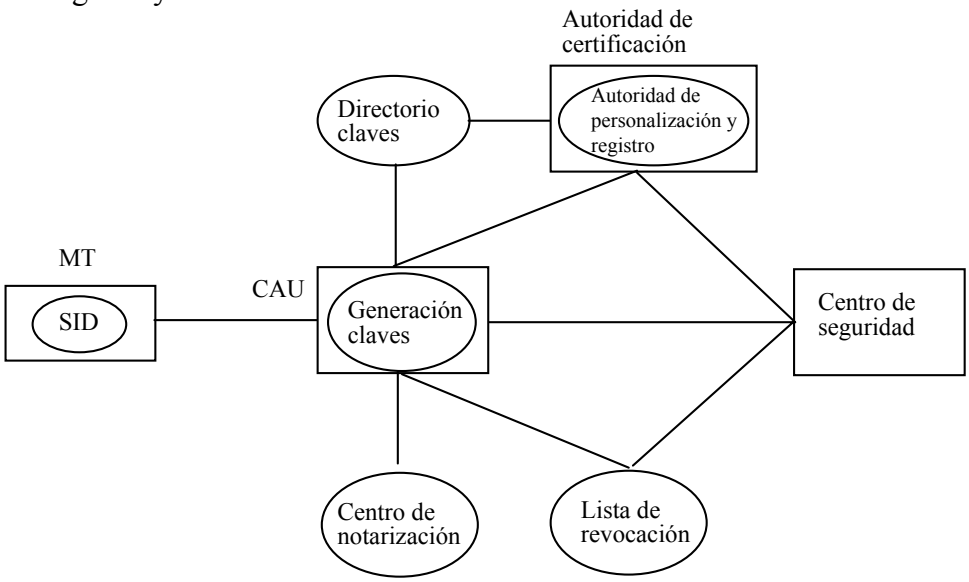


Fig. 4.1 Disposición de entidades en la arquitectura de seguridad propuesta para UMTS

Dispositivo de identidad de abonado (Subscription Identity Device (SID))

El SID (Subscriber Identity Device, p.e. tarjeta inteligente), es un dispositivo que contiene datos muy sensibles, como por ejemplo, la identidad del usuario, clave pública y privada del usuario, claves publicas de las autoridades de certificación, claves secretas de cifrado o información de tarificación. Además, el SID (tarjeta inteligente) debe ser capaz de manipular un PIN como requerimiento de autentificación de usuario por el terminal. De esta forma, el SID proporciona funciones de seguridad tales como autentificación o control de acceso a servicios UMTS y también dispone de las funciones lógicas requeridas por las tarjetas como leer, guardar y borrar,...información.

Centro de autentificación

La gestión del centro de autentificación contempla la distribución de información descriptiva, tales como passwords o claves, usando gestión de claves, a las entidades requeridas para realizar la autentificación de usuarios. El centro tendría funcionalidades en relación a gestión de claves como: determinada generación de claves de cifrado, back up, distribución, instalación, renovación y destrucción de claves.

Centro de seguridad

Las tareas más importantes desarrolladas en el entorno de seguridad serían: La gestión de seguridad del sistema, la gestión de los servicios, y la gestión de los mecanismos de seguridad.

En relación a los servicios de seguridad, contiene las funciones de gestión para el centro de autentificación, centro de notarización, centro de gestión y demás entidades de seguridad en la red UMTS. Además, contribuye a proporcionar funciones de seguridad más complejas a la red como podrían ser la funcionalidad de entidades de confianza, etiquetas de seguridad, gestión de eventos especiales, gestión de auditabilidad de seguridad y gestión de restablecimiento de seguridad.

Autoridad de certificación

Se trata de un centro para crear y asignar certificados a determinadas entidades de la red.

Directorios de certificados

Es la entidad responsable para mantener los certificados preparados para el uso por las entidades de usuario o de red. Puede tratarse de un almacenamiento de certificados de usuarios, estar integrado en entidades de red o bien en autoridades de certificación.

Centro de notarizacion

Este componente actua como entidad de confianza para asegurar ciertas propiedades acerca de la información intercambiada entre el operador de red UMTS y el terminal móvil, tales como su origen, su integridad, el tiempo transcurrido entre el envío y recepción del mensaje o el tiempo ocupado en una llamada. Se utiliza también en relación con servicios de seguridad como no repudiación o tarificación incontestable.

Centro de generación de claves

Es la entidad responsable para la generación de un par de claves asimétrico. Suele integrarse con los centros de autentificación.

Autoridad de personalización
Este centro proporciona información específica del proveedor de servicios y del usuario en el SID. Suele integrarse con las autoridades de certificación.

Autoridad de registro
Este centro es necesario para el registro de usuarios. Suele integrarse con las autoridades de certificación.

Centro de listas de revocación
Centro donde se almacenan las listas de entidades, sean usuarios, terminales, etc que tienen sus certificados revocados.

4.7 Consideraciones acerca de la seguridad en el handover

El procesado debido a la incorporación de seguridad probablemente decrementará la calidad de servicio induciendo retardo por una parte, e incrementando adicionalmente las amenazas sobre la seguridad del sistema. Se requiere de un adecuado compromiso que permita un servicio óptimo al usuario. Estos efectos serán analizados en los capítulos posteriores.

Entre los aspectos directamente afectados en la red se pueden destacar los siguientes: Servicios de seguridad a ser usados y activados durante el handover; sincronización e integración de servicios de seguridad con el procedimiento de handover; prioridades en las acciones a realizar en el handover; gestión de claves y gestión de mecanismos de seguridad junto con otros parámetros de control.

En cuanto a los aspectos más generales en relación con la seguridad en el handover pueden destacarse: el retardo adicional inducido en el handover debido a diferentes mecanismos de seguridad; la complejidad adicional inducida en el control del handover debida a los servicios de seguridad soportados y el impacto de la localización de las entidades funcionales de servicios de seguridad en la red.

La introducción de seguridad en el sistema ha de aprovechar las características intrínsecas de la red a fin de optimizar el funcionamiento de los mecanismos propuestos. Como consecuencia de la distribución de información en la estructura de bases de datos descrita anteriormente formando la red fija, se plantea la integración de una arquitectura de seguridad que permita la máxima sinergia posible. En base a un estudio de las características de los protocolos y de la distribución de esta información en las bases de datos especificadas, se propone en esta tesis la adopción de la recomendación X.509 de la ITU como soporte sobre el

que se desarrollarán las distintas entidades que forman parte de la arquitectura de seguridad en la red UMTS.

Se propone el uso de mecanismos de clave pública (basados en X.509) para la protección de la señalización en la red (a diferencia de propuestas como las de [MB1-3]), mientras que los algoritmos de clave secreta se reservan para la confidencialidad de la información de usuario. La adopción de una estructura híbrida se debe a que la tasa de la información de usuario puede llegar a ser de hasta 2 Mbps y comporta una carga de procesado enorme dificultando una interactividad de funcionamiento en tiempo real entre las dos partes.

A continuación, se proporciona más información para soportar la propuesta anterior. En primer lugar, se enumerarán las ventajas más importantes del uso de mecanismos de clave pública frente a mecanismos de clave secreta:

- Para la autentificación de un usuario no hay necesidad de transmitir datos secretos a través de la red fija permitiendo utilizar unos protocolos más simples. Al mismo tiempo, los operadores de red no reciben información secreta de manera que no pueden suplantar a un usuario. Eso es importante en entornos como UMTS donde podrán coexistir diversos operadores públicos y privados en una misma zona que no necesariamente son de confianza.
- Se puede realizar una autentificación local frente al caso de usar claves secretas que requieren de una autentificación con el proveedor de servicio del abonado (aut. remota).
- Se protege la confidencialidad de la identidad del usuario sin necesidad de ningún mecanismo adicional.
- No hay necesidad de almacenar permanentemente claves secretas de usuario en la red fija. Por tanto, no se requieren centros de autentificación tan protegidos como en GSM.
- Los mecanismos de clave pública podrían usarse para proporcionar mecanismos de no repudiación para soportar tarificación incontestable. Muy útil en entornos multioperador tipo UMTS.
- Los continuos avances en tecnologia permiten afirmar que para el tiempo en que UMTS entre en servicio, no habrá problemas en la implementación de algoritmos de clave pública, siendo los retardos incluso inferiores a otros mecanismos más convencionales.

Por otra parte, el protocolo basado en clave pública presenta las siguientes ventajas:

- Posibilita la autentificación mutua explicita entre usuario y red
- Se establece una clave secreta entre usuario y red, donde ambas entidades saben que sólo la entidad identificada puede estar en posesión de la clave correcta.
- Permite la confidencialidad de la identidad del usuario respecto a terceras entidades.
- Permite el intercambio de claves públicas certificadas entre usuario y red.

Además, mediante el uso de un esquema de firma digital pueden proveerse servicios como tarificación incontestable, integridad o bien transporte de claves secretas para confidencialidad de la información de usuario.

El uso de otros mecanismos de seguridad como los basados en la identidad o "zero-knowledge" si bien son útiles para autentificación no son suficientemente flexibles para proporcionar el resto de servicios de seguridad propuestos. En cualquier caso, no responden a los requerimientos de rapidez explicitados en el handover que en el caso general no requiere de autentificación [CG1, MI1].

Llegados a este punto, se expone la aplicación de estos mecanismos de seguridad definidos a un procedimiento de movilidad como es el handover. Desde un punto de vista de seguridad, en el handover se realizan los siguientes pasos:

a) Conocimiento de la clave pública del nuevo dominio de control seguridad en la parte de usuario/terminal.
b) Conocimiento de las claves públicas de usuario y de las claves de autentificación del terminal en el dominio del nuevo control de seguridad.
c) Conocimiento de una clave de cifrado (para confidencialidad e integridad de información de usuario) compartida entre el usuario/terminal y el nuevo dominio de control de seguridad.

En general, el proceso del handover puede dividirse en dos fases: la fase de decisión cuando la red y/o el terminal móvil deciden que es necesario ejecutar el handover, donde puede disponerse una gestión de claves inteligente (paso a), y la fase de ejecución para encontrar y establecer las nuevas conexiones via red y radio y proceder a posibles autentificaciones (pasos b y c).

Los factores determinantes en las prestaciones del handover son el retardo, complejidad e integración. Para obtener unas buenas prestaciones, existe la posibilidad de integración del control de seguridad en el control del handover. Esto permitiría dependiendo de la política de seguridad establecida, involucrar determinados servicios de seguridad en la fase de ejecución del handover. Eso puede suponer el iniciar el handover con retardo debido a la gestión de claves previa en la fase de decisión para tener un ahorro de procesamiento posterior obteniendo una ejecución de handover rápida.

Por otra parte, los handover y los servicios de seguridad aplicados dependen de unos escenarios de políticas de seguridad que se basan en el concepto de dominios de seguridad. En general, sería aceptable una política de confianza dentro de entidades de red situadas en el

mismo dominio de seguridad [NA1, TH1]. En consecuencia, cabe identificar dos tipos de escenarios:

- Dominados por la seguridad con políticas de seguridad fuertes. Util para entornos de usuarios de negocios o del gobierno y para accesos a redes privadas.
- Dominados por la calidad de servicio con políticas de seguridad suaves. Util para entornos de usuarios domésticos y para accesos a redes públicas.

4.8 Gestión de la seguridad en el handover

Seguidamente, se especifican los distintos servicios y mecanismos de seguridad de usuario que se proponen para una red móvil avanzada UMTS [AB2-5, RACE3-5]. Los servicios definidos son la confidencialidad, integridad, autentificación, control de acceso y la provisión de servicios de tarificación segura. Se estudian diversas de sus características para el caso de su aplicación al handover.

Si se valora el impacto de los servicios de seguridad sobre los procedimientos de movilidad que se definen en UMTS, se compueba que el handover es el que más restricciones impone a los servicios de seguridad. Se tratan pues las alternativas que pueden proponerse.

4.8.1 Autentificación

La autentificación en el handover se realiza sólo en determinados casos de cambios de dominios de seguridad que se especificarán más adelante y que dependen en gran parte de la política de seguridad del proveedor de servicio u operador de red. En esos casos, se realiza una autentificación mutua entre el terminal móvil y el nuevo punto de conexión a la red, para ello se utilizan o toman parte los siguientes servicios de seguridad:

- Autentificación de Terminal por Operador de red.
- Autentificación de Operador de Red por terminal.
- Autentificación de BTS por Operador de Red.
- Autentificación de Operador de Red por BTS.
- Autentificación entre entidades de la red fija.

Los servicios de autentificación se establecen entre el nuevo punto de conexión y el terminal móvil. En general, un usuario podría usar recursos de la red UMTS siempre que pudiera estar seguro de que su identidad es auténtica. La entidad de red encargada del control de autentificación se denomina CAU existiendo diversas alternativas posibles:

a) Handover entre elementos de red que están debajo del elemento CAU en la jerarquía.

No se invocaría autentificación ni control de acceso.

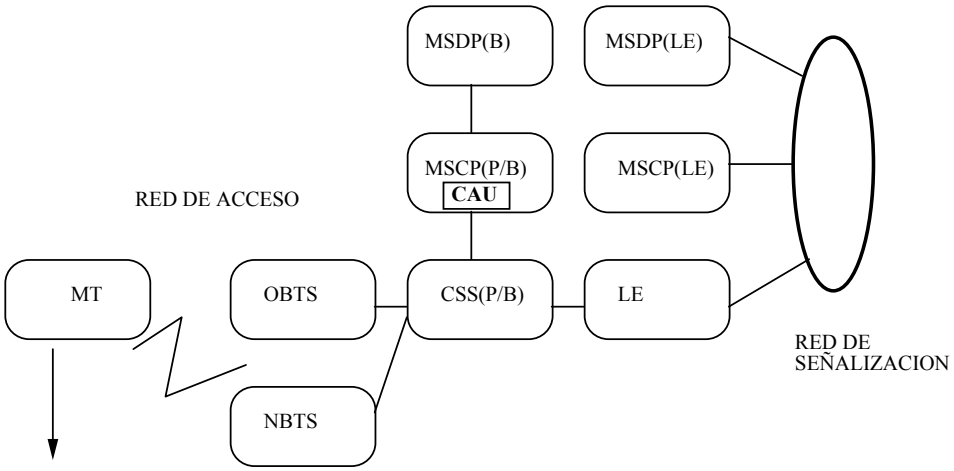


Fig. 4.2 Handover entre BTS´s pertenecientes a la misma CSS (entre elementos de red que están debajo del elemento CAU en la jerarquía).

b) Handover entre diferentes elementos CAU

En esta situación, el tipo de realización del handover en la red podría influir en la decisión de si invocar autentificación o no. En el caso de que el handover pueda realizarse con reenrutado inmediato de la conexión en la red, se encontraría una ruta optimizada y se dispondría de la red al mismo tiempo que el radiocanal es traspasado (forward handover). Sin embargo, la búsqueda y disposición de ese nuevo punto de conexión en la red podría repercutir con un gran retardo.

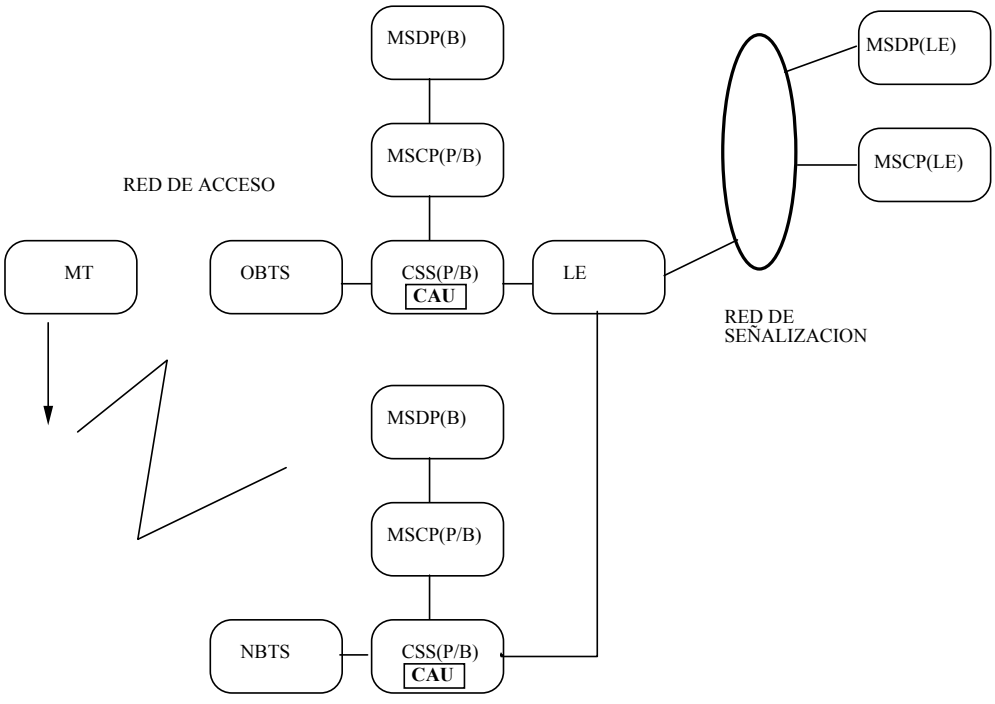


Fig. 4.3 Handover entre BTS´s pertenecientes a CSS controladas por la misma LE (entre diferentes elementos CAU).

Por ello, se definen tres alternativas para la autentificación:

- Autentificación inmediata a coste del retardo introducido: Política de seguridad fuerte.
- En el curso del handover de control se traspasarían los parámetros de autentificación relevantes. Si el nuevo punto de control CAU considera a la anterior CAU de confianza, no se invocaría ninguna autentificación. Se tendría una política de seguridad suave.
- La autentificación se retarda en el tiempo, mientras se traspasan parámetros de autentificación. Es tolerable desde un punto de vista de seguridad sólo temporalmente. Puede resultar crítico en el caso de requerir enviar según que tipo de datos. Se tendría una política de seguridad suave.

Mecanismos de autentificación y gestión de claves

Se proponen técnicas de clave pública basadas en el estándar X.509 para la protección de cierto tipo de señalización dejando las técnicas de clave secreta para la especificación de la protección de información de usuario, la cual puede transmitirse a velocidades de hasta 2 Mbps.

4.8.2 Control de acceso

Las políticas de seguridad definidas en UMTS requieren en general la invocación de control de acceso en los handover que incorporen cambios en dominios de operadores de red, dominios de servicios o dominios de seguridad.

Mecanismos de control de acceso

Básicamente se proponen dos técnicas, el uso de listas de control de acceso y el uso de esquemas de capacidad. Para el esquema de listas de control de acceso, el perfil de servicios del usuario es almacenado en la red, para el esquema de control de acceso por capacidad, el perfil de servicios o parte de él estarían almacenados en el SID. El uso de listas es el más extendido pero en este caso, el menor retardo que supone el uso del SID requiere un mayor estudio.

4.8.3 Confidencialidad

Se requiere de la confidencialidad de cierto tipo de señalización y datos de control de seguridad (p.e. claves de cifrado, identificadores, etc). Además se requiere de la confidencialidad de datos de usuario.

La información usualmente a proteger en el radioenlace, bien sea entre MT y BTS o bien entre MCPN y la red pública, suele ser del tipo de identidad del usuario, perfil de servicio y claves de cifrado. El modo de cifrado a utilizar debe tener en cuenta la incorporación de información de sincronización en los datos transmitidos, cuestiones de retardos y de propagación de errores. Dentro de los algoritmos simétricos, sólo el mecanismo de cifrado en flujo parece ser aceptable. Sin embargo, no pueden precisarse más las características de este servicio ya que el tipo de sincronismo en el radioenlace todavía no ha sido definido en UMTS.

Mecanismos de confidencialidad

Se recomiendan cifradores en flujo para la encriptación de datos de usuario. Los algoritmos asimétricos son descartados por razones de velocidad. Los cifradores de bloques simétricos ECB, CBC o modos CFB no se recomiendan por razones de prestaciones de retardos o errores. La elección del mecanismo final no es posible dado que el tipo de radioenlace a utilizar no se ha definido todavía.

4.8.4 Integridad

Se requiere de la integridad de cierto tipo de información de control así como de la información de usuario por lo que se debe evitar cualquier manipulación en el radioenlace o en el handover.

Si el algoritmo de cifrado permite ofrecer este servicio de integridad con ciertas modificaciones, se podrán asumir algunas de las características proporcionadas por el servicio de integridad. Sin embargo, en caso contrario siempre se pueden utilizar mecanismos tipicos de integridad como los ofrecidos por las funciones Hash. Por otra parte, será necesario disponer de la adecuada sincronización con el servicio de autentificación.

Mecanismos de integridad

Se pueden utilizar los siguientes tipos de mecanismos de integridad: integridad a través de un control de acceso (caso de bases de datos); integridad a través de mensajes redundantes mediante el cifrado; integridad a través de MACs e integridad a través de firma digital. Por otra parte, el uso de la firma digital está reservado únicamente a información de señalización, ya que la información de usuario a 2 Mbps exigiría retardos que esta técnica no permite fácilmente.

4.9 Gestión de claves

Se propone una distribución permanente de pares de claves asimétricas en forma de certificados que se realiza sobre determinadas entidades de la red (p. e. directorios de

certificados) en base a una gestión de claves regida por una autoridad de certificación y/o centro de seguridad. Asimismo, como consecuencia del registro (sesión) de un usuario en un terminal, se produce un nuevo intercambio de claves públicas y secretas con la red con el objetivo de proporcionar los adecuados servicios de seguridad al usuario en el establecimiento posterior de la llamada [AB5, 9].

Respecto a los componentes en la red de acceso, los centros de control de estaciones base (CSS) se hallan conectadas a un centro de conmutación local (LE) y a varias estaciones base (BTS) con las que pueden distribuir los certificados periódicamente. Disponen también de otras funciones de seguridad como son una adecuada gestión de claves para posibilitar servicios de autentificación, confidencialidad e integridad. Las BTS interaccionan a su vez con el usuario sobre un radioenlace cifrado.

En general, se requiere de autentificaciones entre entidades UMTS para realizar el establecimiento de llamada, precisándose de caminos de certificación entre CSS's y LE's en la red de acceso y también con las MSCPs y MSDPs en la red fija. Es decir, se facilitan caminos seguros entre entidades fijas que forman una red inteligente para la adecuada protección de determinada señalización que circula por los enlaces. Para ello, se dota a cada nodo de los certificados de las demás entidades a las que está conectado.

La protección de los canales de información de usuario (servicios portadores), que interconectan los diferentes nodos de la red CSS, LE y TX, se puede hacer mediante cifrado con algoritmos simétricos, requiriendo de autentificación en el establecimiento de llamada y en determinados handover.

Se estudiará a continuación el caso del handover, como un mecanismo determinante a la hora de validar esta arquitectura de seguridad propuesta.

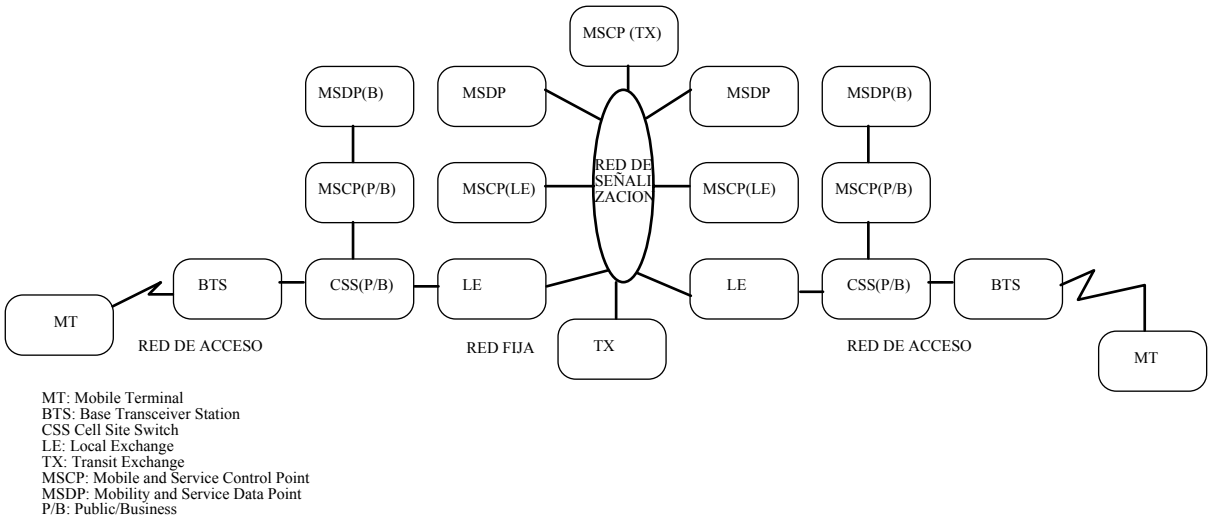


Fig. 4.4 Distribución de los componentes en la red en el establecimiento de llamada entre dos terminales móviles.

En el caso general del handover, no se requiere autentificación entre MT y/o la nueva BTS, siendo responsabilidad de la política de seguridad del sistema su activación. Las técnicas utilizables para la gestión de claves son de tipo asimétrico y se basan en el establecimiento de claves por transporte.

Las posibilidades de conexión a UMTS con radioenlace pueden realizarse en base a radioenlaces entre el terminal móvil y las estaciones base BTS o bien, radioenlaces entre redes privadas móviles (MCPN) y la red fija.

Puede darse el caso de ser los radioenlaces funcionalmente separados en cuanto a claves de cifrado, o bien unidos en ambos sentidos, ascendente y/o descendente. Los criterios para una de las dos opciones pasan por el análisis de los servicios involucrados (punto a punto, broadcasting, y en qué sentidos) y también el tipo de información a proteger, de usuario, o de señalización. Las claves de cifrado pueden ser de los siguientes tipos:

- Claves de sesión originadas en un proceso de autentificación inicial.
- Claves secretas creadas por el SID en cada activación del handover para protección de la información del usuario.
- Pares de claves públicas y privadas certificadas en el caso de la señalización.

El periodo de validez de las claves puede ser:
- Durante un tiempo predefinido (p.e. clave pública según politica del operador de red)
- Durante una llamada o sesión (p.e. clave secreta según politica del operador de red)
- Entre handovers (p.e. claves secretas de protección de información de usuario)

4.9.1 Opciones en la generación de claves secretas

En principio, se configura el diseño del SID para posibilitar la generación de claves secretas para la confidencialidad e integridad de información del usuario. Por ello, a continuación, se especifican las opciones posibles de generación y/o gestión de claves secretas en el handover.

• Generación de la nueva clave por el MT (o SID)

Este es el sistema elegido para la gestión de claves de handover en nuestro estudio. Presenta la ventaja de que el usuario tiene cierto control del sistema. Sin embargo, en este caso el SID requiere de la capacidad de generar claves, lo cual no suele ser complicado para claves secretas.

Otras opciones que se consideraron fueron las siguientes:

• Generación o introducción de una nueva clave por la BTS.

Presenta la ventaja de que no se requiere la capacidad de generación por parte del terminal, si bien entonces, el usuario no tiene control del sistema y la nueva BTS ha de ser de confianza para aceptar la nueva clave.

• Generación de claves por un centro de distribución de claves.

En este caso, el principal inconveniente es que el usuario tiene que tener confianza en el nuevo centro. La clave tiene que ser certificada para probar su origen, por lo que el MT (o BTS) necesita conocer la clave pública auténtica de la entidad de confianza requiriendo por tanto un tiempo mayor que en los casos anteriores.

La generación o introducción de una nueva clave por parte de la BTS es especialmente interesante en el caso del backward handover, sin embargo, como se verá más adelante, el forward handover es más rápido y ello se basa en parte en la generación de una nueva clave por parte del SID en cada handover.

4.9.2 Gestión de claves públicas

En este apartado, se especifica la propuesta de distribución de claves en la red de acceso como resultado de la gestión de claves en la arquitectura de seguridad definida para el sistema [AB5]. Inicialmente y mediante una renovación periódica, los siguientes elementos de red almacenarán las siguientes claves:

MT:

(Xp, Xs)

BTS:

(BTSp, BTSs), (CSSp)

CSS:

(CSSp, CSSs), (LEp) y (BTSp)

LE:

(LEp, LEs), (CSSp)

TX:

(TXp, TXs).

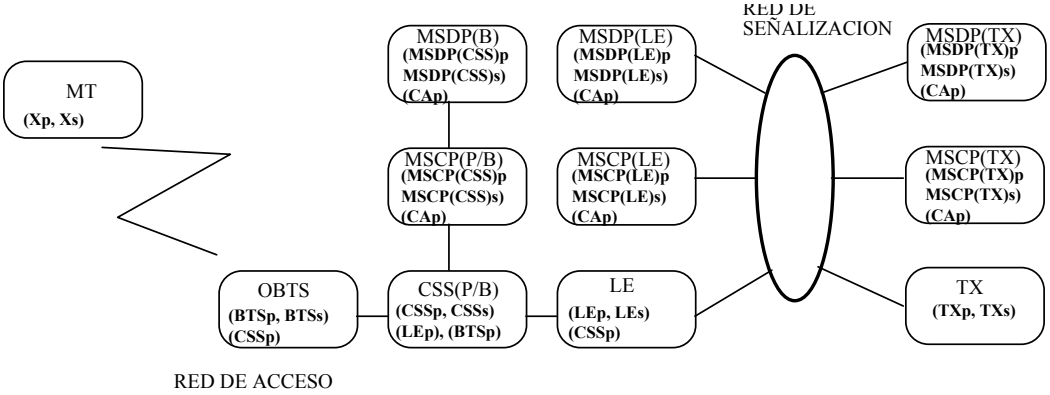


Fig. 4.5. Distribución de claves en los diferentes elementos de la red.

Las distintas configuraciones y entornos admiten la posibilidad de que las MSCP y MSDP puedan existir opcionalmente en los componentes CSS, LE y TX de la arquitectura de la red y estar integradas en un mismo componente físico. Es decir, por ejemplo, la CSS, MSCP(CSS) y la MSDP(CSS) podrían formar una misma entidad física. Por ello, opcionalmente se definen unos pares de claves de claves (pública y privada) para el resto de componentes.

MSDP(CSS):

(MSDP(CSS)p, MSDP(CSS)s), MSCP(CSS)p y dispone también de un directorio con los certificados de los usuarios registrados y del resto de las entidades de red del mismo dominio, así como de las CAp.

MSCP(CSS):

(MSCP(CSS)p, MSCP(CSS)s), MSDP(CSS)p, CSSp y las CAp de las autoridades de certificación de la red. Puede constituir además un centro de autentificación (CAu).

MSCP(LE):

(MSCP(LE)p, MSCP(LE)s), LEp, y las CAp de las autoridades de certificación de la red. Puede constituir además un centro de autentificación (CAu) y/o una autoridad de certificación..

MSDP(LE) o ISN_S:

(MSDP(LE)p, MSDP(LE)s) y dispone también de un directorio con los certificados de los usuarios registrados, y del resto de entidades de red del mismo dominio así como de las CAp.

MSCP(TX):

(MSCP(TX)p, MSCP(TX)s) y las CAp de las autoridades de certificación de la red. Puede constituir además un centro de autentificación (CAu) y/o una autoridad de certificación..

MSDP(TX) o ISN_I:

(MSDP(TX)p, MSDP(TX)s) y dispone también de los certificados del resto de entidades de la red así como de las CAp de otras redes. En general, se integra con una autoridad de certificación para una más efectiva gestión de claves.

A pesar de la opcionalidad de distribución de los diferentes elementos de seguridad, es conveniente situar al menos autoridades de certificación (CAs) en las entidades MSCP(LE), para forman dominios de seguridad en la red de acceso.

En la red fija, sólo se consideran CA en algunos tipos de bases de datos en centros de control y en las MSCP(TX). El resto de entidades (p.e. LEs) obtienen los certificados que no son de su propio dominio a través de los directorios de claves, siendo necesario el uso de caminos de certificación para la adecuada autentificación entre las diferentes entidades de red.

En relación a la necesidad de ubicar claves en las bases de datos distribuidas DDBs de la red fija (ISN), puede hacerse la siguiente clasificación:

ISN_{DN}:

Contiene las claves públicas (certificados) de toda la red. Requiere de CA para la gestión de claves en casos de emergencia o imprevistos. En general, se integra con el centro de seguridad y otras diversas entidades de gestión y/o seguridad según el operador de red o provedor de servicio.

ISN_{Dn}:

Forma parte de la estructura de bases de datos de directorios de la red fija. No se consideran funcionalidades específicas en seguridad.

4.10 Opciones en la ejecución del handover

Se parte de los siguientes supuestos para la gestión de seguridad en el handover. Cada componente de la red tiene su par de claves privada/pública que les han sido enviadas

previamente "off-line" por las autoridades de certificación correspondientes. En el caso del terminal móvil, estas claves se almacenan en el SID.

Las autoridades de certificación usan el algoritmo de clave pública para certificar las claves públicas, produciendo certificados según la recomendación X.509. Para obtener unas prestaciones adecuadas de la red, las MSCP(CSS) han de disponer de las claves públicas CAp del resto de autoridades de certificación del operador de red (dentro un mismo dominio administrativo).

Las claves secretas de cifrado (para confidencialidad e integridad) se generan nuevamente en cada handover por el terminal móvil (SID) y pueden renovarse por sesión/llamada u otros según la política de seguridad del operador de red.

Entre la CSS y cada BTS asociada, se disponen las claves públicas correspondientes de forma que la macrodiversidad sólo es recomendable en BTSs que pertenezcan a un sólo dominio de seguridad (CSS), es decir, que no requieran autentificaciones.

En la fase de decisión, previa a la ejecución del handover, se envian certificados a todos los terminales móviles de todas las BTS monitorizadas. Estos certificados no serán utilizados hasta que el MT o BTS decida la ejecución del handover a la celda o celdas (caso de macrodiversidad) candidatas elegidas.

En la realización del handover, se pueden distinguir los siguientes casos para la gestión de claves.
- Gestión de claves mientras el MT está conectado a la anterior BTS (backward handover)
- Gestión de claves mientras el MT está conectado a la nueva BTS (forward handover)
- Gestión de claves mientras el MT está conectado a la anterior BTS y a la nueva BTS (macrodiversidad)

A partir de aquí, se definen dos procedimientos de handover: forward y backward en los que la gestión de claves se plantea de forma diferente.

Forward handover

En el forward handover, el terminal móvil cambia su punto de conexión antes de que la red haya enrutado la llamada al nuevo punto de conexión. En una situación de política de seguridad fuerte, el forward handover se inicia con el envio previo de la clave pública de la nueva BTS al terminal móvil en la fase de decisión. El móvil debe proporcionar su clave pública así como las claves secretas de cifrado para la decodificación por parte de la red. Posteriormente la información puede ser transmitida cifrada a través del terminal que tiene

acceso a la clave pública de la red. El uso de autoridades de certificación permite la distribución de las claves públicas en los correspondientes directorios, donde deben ubicarse los certificados para el móvil y los diversos componentes de la red.

Backward handover

En este caso, el terminal móvil cambia su punto de conexión despues de que la red haya enrutado la llamada al nuevo punto de conexión.

En los backward handover, la anterior BTS está en posesión de la información de seguridad apropiada (p.e. claves de sesión). En el caso de handover entre dos subredes, si hay coordinación entre la anterior BTS de la anterior subred, puede enviarse información cifrada por el nuevo radioenlace. Diversas opciones son posibles, si bien sólo se desarrolla el primer caso:

1) La anterior red pide la clave pública de la nueva red y la proporciona al móvil en un comando handover. Esta clave puede utilizarse durante la llamada en la nueva red según la política de seguridad utilizada.
2) La anterior red proporciona la clave pública usada en el antiguo enlace a la nueva red antes de que se active un comando handover. Esta situación sería temporal, a la espera de una nueva clave pública enviada por la NBTS. En este caso, el MT y la BTS anterior tienen una clave comun anterior que puede ser usada (inicialmente).

Por otra parte, el uso de centros de distribución o traslación de claves secretas ralentizan el proceso de handover ya que la gestión no puede hacerse "off-line" y los centros necesitan conocer los grupos involucrados para encriptar la nueva clave y poder transmitirla. Se requiere como posible solución un algoritmo de broadcast de claves secretas, solución compleja y más lenta que el uso de clave pública.

Para los mecanismos de establecimiento de claves punto a punto. El envio de la anterior clave (por la anterior BTS o MT) a la nueva BTS, se realiza a través de una clave pública conocida con anterioridad y mediante firma digital (transporte).

4.11 Contribuciones al capitulo

En este capitulo, se proponen los mecanismos de seguridad que van a ser empleados en el procedimiento de handover y por extensión al resto de los procedimientos de movilidad y llamada establecidos en una red móvil avanzada.

Se parte de unos trabajos previos por parte del autor [RACE2-6] en donde se introdujeron los aspectos relacionados con los requerimientos de la red, estudio de las amenazas más importantes y la aplicación de los servicios de seguridad en UMTS. Posteriormente, y en relación a nuestro trabajo, se propuso una arquitectura de seguridad basada en la estructura de la red UMTS [AB2-4, AB9] donde se aprovechó el hecho de presentar una estructura de bases de datos distribuidas jerárquicamente para plantear unos mecanismos de seguridad basados en X.509. Se plantea pues, en un sistema móvil específico y por primera vez, el uso de algoritmos de clave pública (en señalización) con su correspondiente gestión de claves [AB5] basada en certificados X.509.

Se propone el uso de algoritmos de clave pública para la introducción de servicios de seguridad a un determinado tipo de información de señalización en una red de tercera generación como es UMTS. Se hace uso también, de una gestión de claves mediante certificados (X.509) y de firmas digitales para proporcionar el cifrado a señalización y proporcionar autentificación implícita entre entidades de red [AB13-15].

Se plantea también el uso de algoritmos de clave secreta para la confidencialidad de la información de usuario debido a su elevado bit-rate (< 2 Mbps).

Se propone una distribución de claves en determinadas entidades de seguridad, como bases de datos estructuradas en forma de directorios y en nodos específicos de la red.

4.12 Referencias

[AB2] A. Barba, J. L. Melús. *Security architecture in the UMTS network.* Second IEEE Network Management and Control Workshop, p. 55-66, New York, 1993.
[AB3] A. Barba, F. Recacha, J. L. Melús. *Security architecture in the UMTS network. A comparison with the FPLMTS network.* International II Conference on Universal Personal Communications, p. 854-860, Ottawa, 1993.
[AB4] A. Barba, F. Recacha, J. L. Melús. *Security architecture in the third generation networks.* SICON/ICIE '93. p. 421-425, Singapur, 1993.
[AB5] A. Barba y J. L. Melús. *Directory services for UMTS. Security aspects.* 44th VTC Vehicular Technology Conference. p. 1606-1610. Estocolmo, 1994.
[AB6] E. Cruselles, F. Recacha, A. Barba, J. L. Melús. *Seguridad en comunicaciones móviles. Mecanismos y servicios.* Mundo Electrónico, p. 22-31. Abril 1994.
[AB7] F. Recacha, A. Barba, E. Cruselles y J. L. Melús. *Comunicaciones móviles. Seguridad en redes GSM.* Mundo Electrónico, p. 42-51. Octubre 1994.
[AB8] J. L. Melús, A. Barba, F. Recacha y E. Cruselles. *Seguridad en comunicaciones móviles. El estándar DECT*. Mundo Electrónico, p. 58-63, Jun-Julio 1995

[AB9] A. Barba, J. L. Melús, F. Recacha y E. Cruselles. *Comunicaciones móviles. Seguridad en sistemas de 3ª generación UMTS.* Mundo Electrónico, p. 62-69, Septiembre 1995.

[AP1] Anton Prins. *Flexibility for authentication functions in UMTS.* p. 369-374. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[AR1] Akiyama Ryota, Sasaki Susumu. *Authentication and encryption in a mobile communication system*. p. 927- 930. 43 VTC Estocolmo, 1994.

[AS1] Ashar Aziz, Whitfield Diffie. *Privacy and authentication for wireless local area networks*. p. 25-31. IEEE Personal Communications 1994.

[CB1] Carl Bedingfield, *Understanding personal mobility and terminal mobility in PCS.* p 1688-1692. Globecom '93 Houston. 1993.

[CG1] Christoph G. Günther. *An identity-based key-exchange protocol.* p. 29-37. Eurocrypt '89.

[DB1] Dan Brown, *Security planning for personal communications.* p 107-111. 1st Conf. Computer&Communication Security. 1993.

[DB2] Dan Brown. *Techniques for privacy and authentication in personal communications systems.* IEEE Personal Communications. p. 6-10. Agosto 1995.

[DD1] Danny Dolev and Andrew C. Yao. *On the security of public key protocols. IEEE Transactions on information theory*. p.198-210. 1983.

[DECT1] DECT CI: Part 7. Security Features.

[DECT2] DECT. Services and facilities requirements specification.

[DW1] David R. Wilson. *Signaling system nº7, IS-41 and cellular telephony networking.* p. 644-652. Proceedings of the IEEE. Abril 1992.

[ETSI1] Framework of network architecture, interworking and integration for the UMTS. Special Mobile Group (SMG). 14/1/93.

[ETSI2] Recommendation GSM 02.09. Security aspects. ETSI PT12.

[ETSI3] Recommendation GSM 02.17. Subscriber identity modules, functional characterstics. ETSI PT12.

[ETSI4] Recommendation GSM 03.09. Handover procedures. ETSI/PT12. 1992.

[ETSI5] Recommendation GSM 03.20. Security related network functions.

[ETSI6] Recommendation GSM 05.08. Radio sub-system link control. Feb. 1992.

[ETSI7] Recommendation GSM 11.11. Specification of internal logical organization of the subscriber Identity Module (SIM) and its interfaces.

[ETSI8] Recommendation GSM 12.03. Security Management.

[GC1] Gnanesh Coomaraswamy and Srikanta P. R. Kumar. *A novel method for key exchange and authentication with cellular network applications*. p. 186-190. ICUPC '93.

[GC2] Gnanesh Coomaraswamy and Srikanta P. R. Kumar. *Keeping authentication and key exchange alive in communication networks.* Second IEEE Network Management and Control Workshop, New York, 1993.

[GH1] Günther Horn, *Security aspects of new UMTS features. Requirements and solutions*. p. 350-354. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[GR1] Gert Roelofsen. *Security principles for the PSCS.* p. 355-362. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[HY1] Hung-Yu, Lein Harn. *Authentication in wireless communications.* p 550-554. Globecom IEEE. Houston, 1993.

[ISO1] International standard ISO 7498 - 2. Security Architecture.

[ISO9] OSI Upper layers Security Model. SC 21 N 5001 rev.

[ISO15] International standard ISO 7498 - 4. Management framework.

[ITUT3] The Directory: Authentication Framework. X.509. 04-1992.

[JW1] Joseph E. Wilkes. *Privacy and authentication needs of PCS.* IEEE Personal Communications. p. 11-15. Agosto 1995.

[LF1] L. Frey. *The possible use of public key cryptosystems for UMTS.* p. 364-368. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[LF2] Frey L., Horn G., Müller K. *Security protocols for UMTS*. RACE Mobile Telecommunications Summit. p. 404-410. Cascais (Portugal) 1995.

[MB1] Michael J. Beller, Li-Fung Chang, Yacov Yacobi, *Privacy and Authentication on a portable communication system.* p 1922-1927. Globecom 1991.

[MB2] Michael J. Beller, Li-Fung Chang, Yacov Yacobi. *Security for personal communications services: public key vs. private key approaches.* p. 26-31. PIRMC´92. Boston. 1992.

[MB3] Michael J. Beller, Li-Fung Chang, Yacov Yacobi. *Privacy and Authentication on a Portable Communications System*, IEEE Journal on Selected Areas in Communications, p.821-829, August 1993.

[MI1] Mihir Bellare, Shafi Goldwasser. *New Paradigms for digital signatures and message authentication based on non-interactive zero knowledge proffs.* p. 194-211. Crypto '89.

[MT1] Makoto Tatebayashi, Natsume Matsuzaki, David B. Newman. *Key distribution protocol for digital mobile communication systems.* p. 324-334.

[NA1] Nazim Agoulmine, José Neuman de Souza, Mauro De Oliveira. *Distribution of management over multi-domains network management systems*. p. 1217-1221. Globecom '93 Houston 1993.

[NJ1] Nigel Jefferies, Gert Roelofsen. *PSCS Authentication management*. p. 409-411. RACE Mobile Telecommunications workshop. Metz. 1993.

[RACE2] RACE 2066/ASCOM/MF3/DS/P/04/b1 Scenarios of threats for the UMTS network (draft). 1992.

[RACE3] RACE 2066/ASCOM/MF3/DS/P/010/b1, Specification of security services and service levels (draft). 1992.

[RACE4] RACE 2066/ASCOM/MF3/DS/P/011/b1, Allocation of security services to network components (draft). 1992.

[RACE5] RACE 2066/ASCOM/MF3/DS/P/046/b1, Specification of security services and service levels (final). 1993.

[RACE6] RACE 2066/ASCOM/MF3/DS/P/047/b1, Scenarios of threats for the UMTS network (final). 1993.

[RH1] Rolf Hager, Peter Hermesmann, Michael Portz. *Security management. Overview to reliable authentication procedures for automatic debiting systems in RTI/IVHS environments.* Second IEEE Network Management and Control Workshop, New York, 1993.

[RK1] Rola Krayem-Nevoux, Gérald Mazziotto, Philippe Hiolle. *Payphone service for third generation mobile systems.* p. 1708-1712. Globecom´93 Houston, 1993.

[RM1] Refik Molva, Didier Samfat and Gene Tsudik. *Authentication of mobile users.* p. 26-34. IEEE Network. Marzo/Abril 1994.

[RM2] Refik Molva, Pierre-Alain Etique y Jean_Pierre Hubaux. *Strong authentication in intelligent networks.* p. 629-634. ICUPC´94, San Diego, 1994.

[SC1] Santosh Chokhani. *Toward a national public key infrastructure.* IEEE Communications Magazine. p. 70-74. Sept. 1994.

[SM1] Seshadri Mohan. *Network impacts of privacy and authentication protocols for PCS.* p. 1557- 1561. ICC´95, Seattle, 1995.

[TH1] Thomas Hardjono, Tetsuya Chikaraishi, Tadashi Ohta. *An approach to key management and inter-domain authentication in the Telecommunications Management Network.* p. 171-176. Globecom '93.

[TIA1] TIA/EIA/IS-95. Mobile syation-base station compatibility standard for dual-mode wideband spread spectrum cellular system. Julio 1993.

[UPT1] Service requirements on security features. UPT, ETSI DTR NA-70203.

[UPT2] General UPT Security Architecture. ETSI DTR/NA- 70401.

[WB1] Wouter van den Broek, Maurizio Montagna. *User mobility in UMTS. Operational aspects and the implications for user and terminal identifiers.* p. 543-546. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[WF1] Walter Fumy and Peter Landrock. *Principles of key management.* IEEE Journal on selected areas in communication. p. 785-793. Junio 1993.

Capitulo 5

Evaluación de una gestión de claves en la fase de ejecución del handover

5.1 Introducción

Uno de los mayores problemas que plantea el handover desde un punto de vista de seguridad es el conocimiento de las claves públicas del nuevo dominio de control de seguridad por parte del usuario/terminal móvil que realiza el handover. En este diseño que se propone, esta clave pública de la nueva estación base (NBTSp) será utilizada por el terminal móvil para enviar las claves secretas de cifrado via firma digital a la nueva BTS en la fase de ejecución del forward handover y así poder empezar a intercambiar información de forma segura [AB11, 12].

El envio de esta NBTSp de forma adelantada en la fase de decisión reduce en buena parte el retardo en el uso de los servicios de seguridad y por tanto, el envio de información de usuario protegida.

El empleo de una fase de búsqueda de celdas candidatas para una decisión óptima en el handover resuelve el problema de la gestión de claves en el caso especial del forward handover permitiendo minimizar el impacto del retardo en el servicio. Una vez se ha definido esta fase y partiendo de la arquitectura de seguridad especificada previamente, se estudia el protocolo que rige el proceso de ejecución o invocación de handover.

Primero se describe la fase de ejecución con sus mensajes, posteriormente los handover se clasifican según el origen de activación, en forward handover, activado por terminal y

backward handover, activado por la red. A su vez, se estudian tres tipos de handover según se ha especificado en la arquitectura del sistema:

a) Handover entre celdas pertenecientes a la misma CSS o entre elementos de red que están debajo del elemento CAU en la jerarquía.
b) Handover entre celdas pertenecientes a diferentes elementos CAU (en distintos dominios de seguridad y en el mismo dominio administrativo).
c) Handover entre celdas pertenecientes a diferentes elementos CAU (en distintos dominios de seguridad y distinto dominio administrativo).

En cada uno de los handovers especificados se estudian los mecanismos y servicios de seguridad requeridos. En esta fase de ejecución, por medio de mecanismos de firma digital se realiza una gestión de claves secretas previa al cifrado de la información de usuario. También se invocan autentificaciones entre terminal y red según cada situación.

Finalmente, mediante programación se obtienen una serie de gráficas que permiten determinar las prestaciones de cada procedimiento de movilidad así como su frecuencia de invocación. Eso permite valorar con mayor precisión el alcance y bondad de los algoritmos y protocolos propuestos.

5.2 Gestión de claves en la fase de decisión

Tal como se expuso en el capitulo anterior, el terminal móvil (o el MCPN) correspondiente dispone de un sistema de gestión interno que les permite obtener información para la determinación de las celdas candidatas. Eso les permite desarrollar un método que posibilita una gestión de claves de seguridad por anticipado (fig. 5.1).

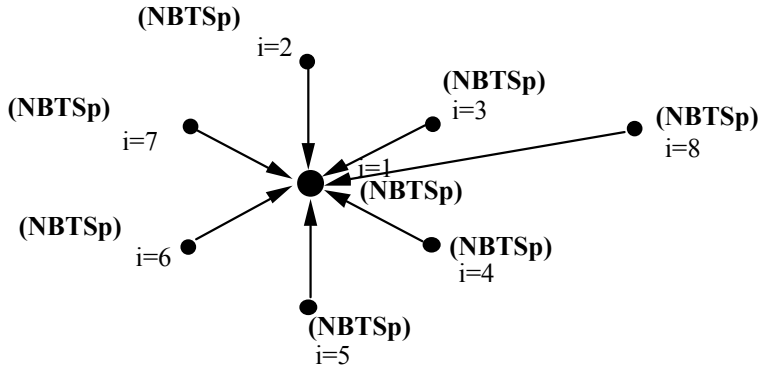


Fig. 5.1. Distribución de las NBTSp por parte de las estaciones base de las celdas candidatas a cada terminal móvil situado en la celda i=1.

Esta distribución de claves se realiza sobre una zona correspondiente al mismo dominio de seguridad y aprovecha el intercambio de parámetros descrito en 3.2.3 para el envio de la clave pública desde la nueva estación base (NBTSp).

5.3 Gestión de claves en el forward handover

En este tipo de handover, se considera que la invocación es efectuada por el terminal móvil.

Se propone como solución a la gestión de claves la distribución previa de claves públicas por parte de cada CSS a las BTS a las que está conectado y éstas a su vez la distribución a los terminales móviles a los que se tiene cobertura [AB13-15, ISO2].

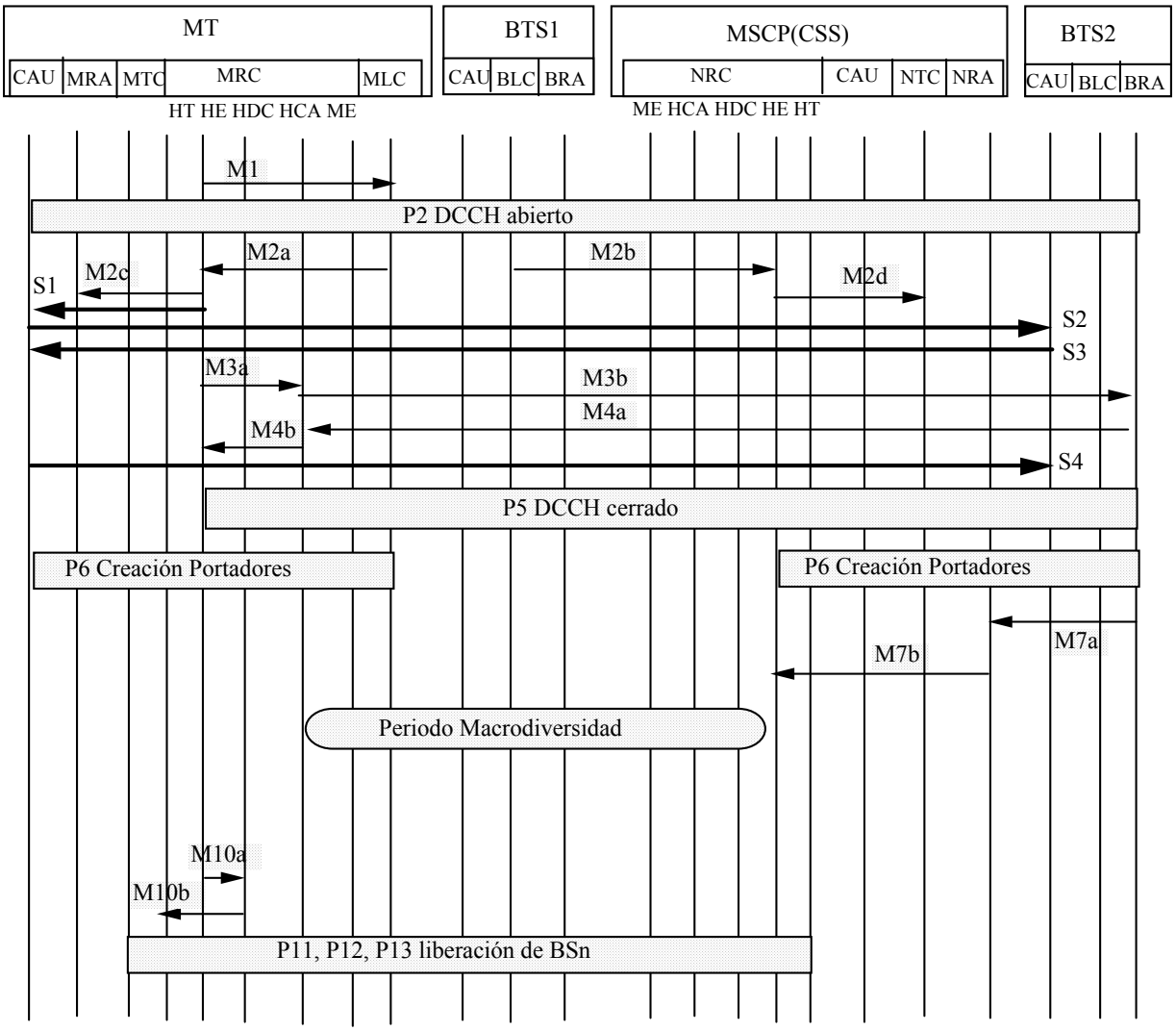


Fig. 5.2 Protocolo de un forward handover con mecanismos de seguridad incorporados.

Básicamente, se pueden presentar dos situaciones posibles:

1) Handover en la misma estación base.
Se trata del caso de handover entre canales de la misma BTS. En este caso, no se requiere autentificación ni control de acceso por ser la misma entidad de red la que realiza el handover. Sin embargo, debe situarse algun mecanismo para evitar pérdidas por desincronización y/o pérdidas de datos.

2) Handover entre estaciones base controladas por la misma CSS (en el mismo dominio de seguridad).
En este caso, la invocación de autentificación vendría impuesta por requerimientos de la política de seguridad vigente en el dominio, sin embargo, normalmente no será necesaria.

En general, se requiere invocación de control de acceso en los handover que incorporan cambios en dominios de servicios, seguridad u operadores de red.

Notación:
La notación utilizada en los mensajes descritos posteriormente va a ser la siguiente:

Xp: Clave pública del terminal móvil
Xs: Clave privada del terminal móvil
Xc: Clave secreta para confidencialidad de la información de usuario
Xi: Clave secreta para integridad de la información de usuario
Xp[I]: I cifrada por Xp
Xs[I]: I cifrada por Xs
CAp: Clave pública de la Autoridad de Certificación
CAs: Clave privada de la Autoridad de Certificación
OBTSp: Clave pública de la estación base anterior
OBTSs: Clave privada de la estación base anterior
NBTSp: Clave pública de la nueva estación base
NBTSs: Clave privada de la nueva estación base
CAH: Autoridad de Certificación de la cual el terminal móvil está abonado
CCA: Autoridad de Certificación común entre CAH y NCAV
OCAV: Autoridad de Certificación del anterior dominio visitado por el terminal móvil
NCAV: Autoridad de Certificación del nuevo dominio visitado por el terminal móvil

X{I}: Firma digital de I por el usuario X (con el uso de una función Hash)
CA(X): Autoridad de Certificación de X
Fir (a; b): Mensaje resultante (b, a{b}) siendo a{b} la firma digital de b con la clave procedente de a.
X1<<X2>>: Certificado de usuario X2 enviado por la autoridad de certificación X1

Certificado: Fir (CAs; Contenido del certificado)
Contenido de un certificado:
- Número de serie
- Periodo validez
- Nombre del componente (terminal o entidad de red)
- Clave pública del componente
- Nombre de la autoridad de certificación
- Firma digital de la información anterior por la clave secreta de la autoridad de certificación

A -> B: Camino de certificación formada por una cadena de certificados de A a B.

5.3.1 Handover entre elementos de red que están debajo del elemento CAU en la jerarquía

En este apartado se describe el protocolo utilizado para la gestión de claves y servicios de seguridad en la ejecución del handover. En la figura se muestra el tipo de handover al que se hace referencia.

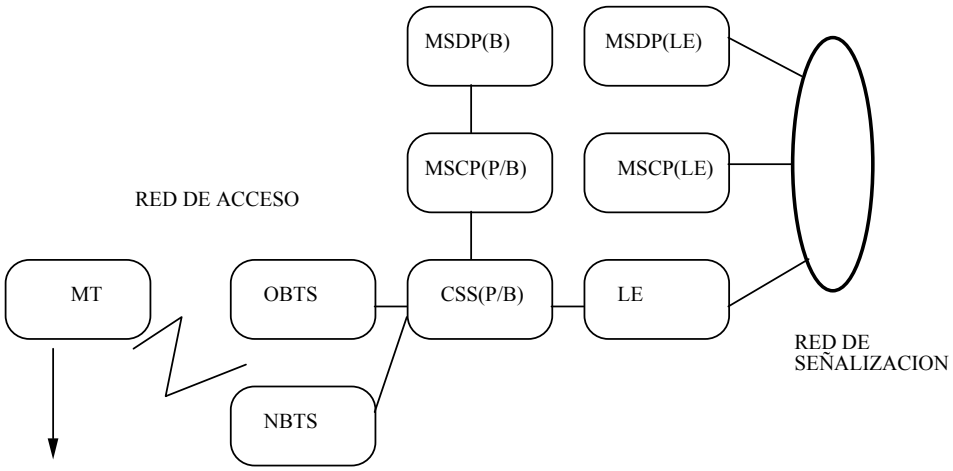


Fig. 5.3 Handover entre BTS´s pertenecientes a la misma CSS.

La secuencia de mensajes de seguridad enviados es la siguiente:
Mensaje S1: Intercambio interno de información en el terminal móvil.

La entidad funcional de ejecución del handover del terminal móvil informa a la entidad de seguridad (entidad de autentificación) acerca de la necesidad de enviar las claves de confidencialidad, integridad y demás parámetros de seguridad a la nueva estación base.

Mensaje S2: Terminal móvil -> Nueva BTS

NBTSp[CCA<<X>>, lista de algoritmos, CH1, Fir(Xs; Xc, Xi, lista de algoritmos, CH1)]

Este mensaje S2, puede presentarse en dos versiones, una en la que el mensaje se cifra con la NBTSp obtenida por el terminal móvil en la fase de distribución previa (fase de decisión), donde se envian las claves secretas para los servicios de confidencialidad e integridad mediante un mecanismo de firma digital. En este caso, la CCAp también se supone conocida por la nueva BTS ya que es accesible al nuevo dominio mediante la distribución previa que se realiza en la fase de decisión del handover. En la otra versión, se puede prescindir de NBTSp, pero requiere de una autentificación aparte (handover tipos 5.3.2 y 5.3.3).

Se supone que cada BTS y CSS tiene las claves públicas de los demás nodos a los que está conectado, dentro de un mismo dominio. En el caso de no disponerse y que sean diferentes, (handover tipos 5.3.2 y 5.3.3) se requerirá de más mensajes.

Mensaje S3: Nueva BTS -> Terminal móvil.

(Xp [NCAV<<NBTS>>, RN1, algoritmo escogido, lista de revocación de certificados, Fir(NBTSs; Xp[RN1], algoritmo escogido, lista de algoritmos, lista de revocación de certificados, CH1)])

En este caso, se envia el mensaje S3 por la nueva BTS al terminal móvil y se procede a una autentificación de la estación base por el terminal móvil. El procesado de este mensaje puede posponerse en el tiempo según las restricciones ya expuestas en el capitulo 4.

Es necesario el envio de S3 para confirmación y para información de identificación de la nueva BTS al terminal móvil. La NCAVp se halla por el terminal móvil con el camino de certificación proporcionado y su comprobación se realiza posteriormente.

En el caso general es necesario el envío de un número aleatorio RN1 por si se requiere de una autentificación del terminal móvil por la estación base retardada (casos de handovers 5.3.2 y 5.3.3).

5.3.2 Gestión de claves en el handover entre diferentes elementos CAU (en distintos dominios de seguridad y en el mismo dominio administrativo)

Este tipo de handover se realiza entre dominios de seguridad distintos, en general precisa de autentificación, aunque depende de la política de seguridad vigente entre los dominios. Pueden darse las siguientes situaciones: que el handover sea entre CSS controladas por la misma LE o bien controladas por diferentes LEs. Para ambos casos se va a suponer que las CSS (MSCP(CSS), MSDP(CSS)) disponen de las CAp del resto de autoridades de certificación del operador de red (dentro un mismo dominio administrativo).

Se va a proponer la siguiente politica de seguridad para el caso de un handover que se realice entre distintos dominios de seguridad, se tienen las siguientes situaciones:

1) Handover entre CSS controladas por la misma LE (figura):

- Caso general: autentificación simple
- Opción: autentificación mutua (según política de seguridad)

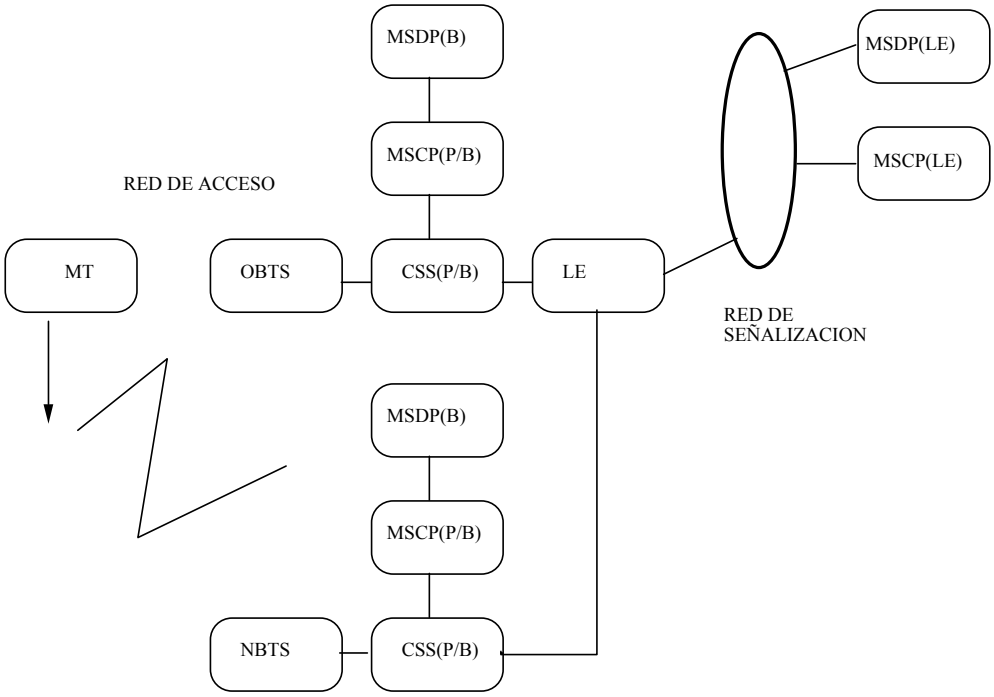


Fig. 5.4 Handover entre BTS´s pertenecientes a CSS controladas por la misma LE

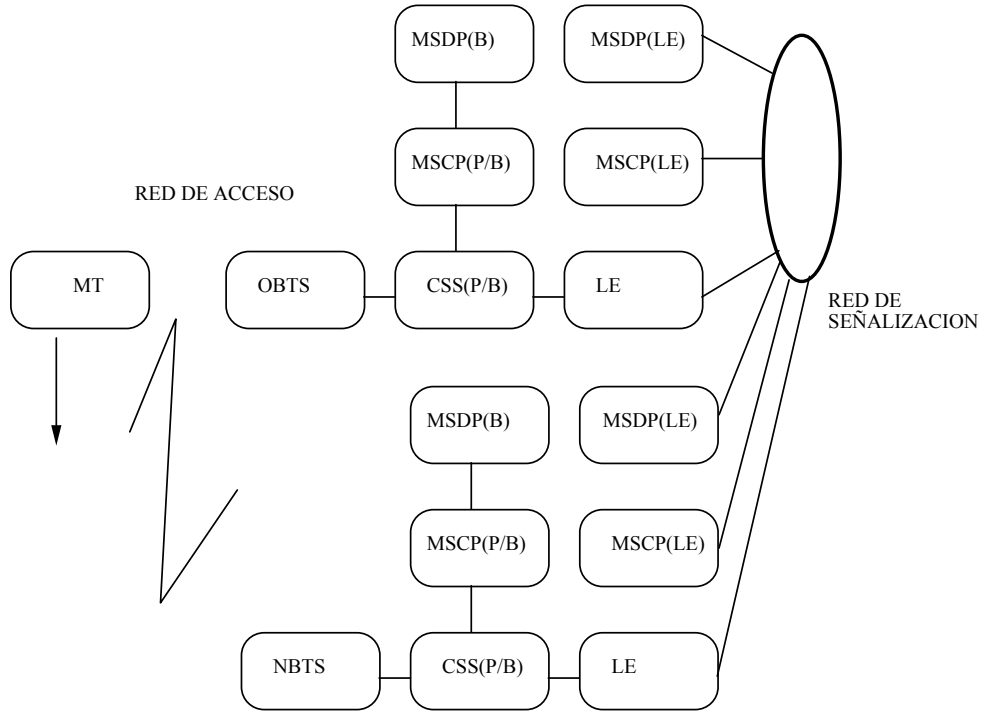


Fig. 5.5 Handover entre BTS´s pertenecientes a CSS controladas por distinta LE

2) Handover entre CSS controladas por diferentes LEs (figura) . Caso de autentificación mutua. Opciones:

- Handover con reenrutado inmediato: autentificación sin retardo.
- Handover con reenrutado retardado: autentificación retardada.

En el caso de no haber obtenido previamente por parte del terminal móvil la NBTSp de la nueva estación base, la MSCP(LE) obtiene los certificados (claves públicas) de las nuevas BTS del nuevo dominio de seguridad off-line. En este caso de forward handover, se realiza un pase de la clave NBTSp de la MSCP(LE) a la CSS y a la nueva BTS. Seguidamente, la nueva BTS pasa su clave pública al MT.

El modo de proceder es semejante al seguido en el apartado anterior en los primeros mensajes. Es decir:

Mensaje S1: Intercambio interno de información en el terminal móvil.

Caso análogo a 5.3.1.

Mensaje S2: Terminal móvil -> Nueva BTS

NBTSp [CCA<<X>>, lista de algoritmos, CH1, Fir(Xs; Xc, Xi, lista de algoritmos, CH1)]

En este mensaje, siguen siendo válidas las consideraciones efectuadas en 5.3.1. Además, es de suponer que la CCAp se conoce por el nuevo MSCP(CSS) ya que se envia (o es accesible) al nuevo dominio a través de la distribución efectuada en la fase de decisión.

En el caso de no haberse obtenido previamente la CCAp, en este tipo de handover se supone que los nodos CSS son lo suficientemente inteligentes para obtener la información concerniente a las CCAp y tener el control de acceso del nuevo dominio. Por tanto, se va a suponer un único camino de búsqueda de esa información independientemente de si las CSS son controladas o no por la misma LE.

Es decir, el camino correspondiente a seguir para la búsqueda de la CCAp sería el siguiente: Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) ida y vuelta.

Respecto al control de acceso, tanto la búsqueda de CCAp como la lista de revocación de certificados podrían integrarse en un único camino. Este camino a seguir para la búsqueda de la la lista de revocación de certificados sería:

Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva MSDP(CSS) ida y vuelta.

En el caso general, las claves públicas de las BTS serán diferentes, (handover tipos 5.3.2 ó 5.3.3) y se requerirá de más mensajes (según la politica de seguridad vigente). Pasándose a enviar S3.

Mensaje S3: Nueva BTS -> Terminal móvil.

(Xp [NCAV<<NBTS>>, RN1, algoritmo escogido, lista de revocación de certificados, Fir(NBTSs; Xp[RN1], algoritmo escogido, lista de algoritmos, lista de revocación de certificados, CH1)])

En este caso, se procede a una autentificación de la estación base por el terminal móvil. Se requiere el envío de RN1 junto a Xc, en el caso general, por si se requiere de una autentificación retardada del terminal móvil por la estación base mediante algoritmos de clave secreta (casos de handovers 5.3.2 y 5.3.3).

Opción: Autentificación del terminal móvil por la estación base (retardada).

Mensaje S4: Terminal móvil -> Nueva BTS

(NBTSp [RN2, Fir(Xs; NBTSp[RN2], lista de revocación de certificados)])

En este mensaje S4, la NCAVp es hallada por el terminal móvil, reenviada a la estación base y su comprobación se realiza posteriormente mediante la lista de revocación de certificados.

Por otra parte, sería posible para un usuario tener un handover activado por un cambio de ruta iniciado en la red fija. Un usuario podría tener un enlace a cualquier estación base, podrían haber situaciones en que la optimización de la ruta a través de la red implicara que el usuario se sometiera a un handover desde una BTS asociada a un conmutador LE a otro que estuviera asociado con una ruta completa más conveniente.

Este handover sería similar en el caso de producirse internamente en redes privadas (Customer Premises Networks (CPNs) o MCPNs).

5.3.3 Gestión de claves en el handover entre diferentes dominios de seguridad y entre diferentes entornos administrativos

En este tipo de handover, la invocación de autentificación vendría impuesta por requerimientos de la política de seguridad vigente, sin embargo, en el caso normal será

necesaria la invocación de autentificación mutua debido a que las redes pertenecen a entornos administrativos distintos. Además, se requerirá de la invocación de un control de acceso, junto con una adecuada gestión de claves para soportar confidencialidad e integridad en el radioenlace.

En un contexto de centros de seguridad estructurados jerárquicamente, se podrían dar cambios en las estrategias de seguridad que podrían requerir interacciones con el centro de gestión del sistema aumentando los retardos.

Entre los diversos entornos administrativos a tratar estarían CPNs, MCPNs, diversos operadores de red (privados o públicos) y la red pública. Un caso especial, lo forman los handover de conexiones múltiples, donde se requeriría un gran trasiego de señalización. Se pueden establecer dos situaciones, es el caso de una CPN (usualmente MCPN) que tiene que ser traspasada ('handover') o bien, el terminal móvil es envuelto en una llamada de conexión múltiple (llamada multiparty) y tiene que ser traspasada ('handover').

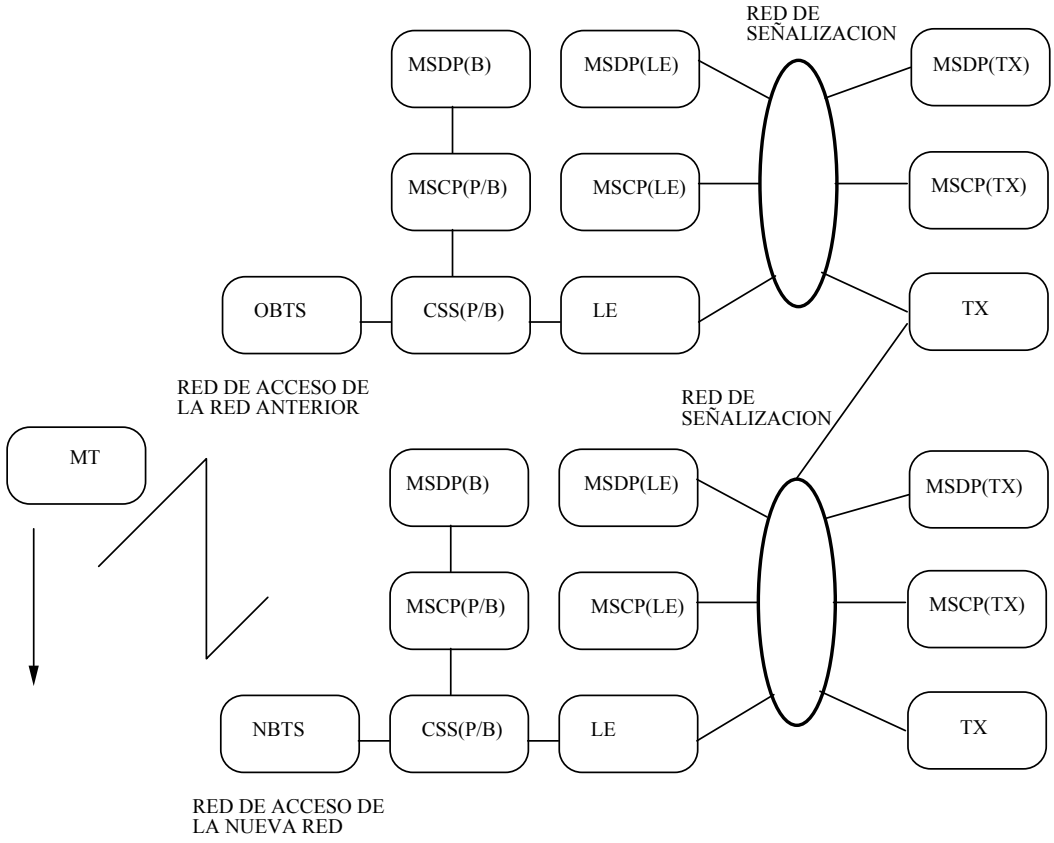


Fig. 5.6 Handover entre BTS´s pertenecientes a diferentes dominios de seguridad y entre diferentes entornos administrativos

Se va a suponer que el nodo CSS (MSCP(CSS), MSDP(CSS)) no dispone de las CAp del resto de autoridades de certificación de distintos operadores de red (en distintos dominios

administrativos). Ya que en el procedimiento de handover se cambia el punto de conexión, en el caso de handover originado por terminal, se pueden distinguir dos autoridades de certificación. Cualquiera, la red antigua o la nueva podría proporcionar las nuevas claves públicas visitadas (ser de confianza). En este caso, la ISN_I dispone de una CA desde la cual, el MSCP(TX) obtiene certificados del resto de entidades de red con las que realiza autentificaciones mutuas de manera unilateral en cada red (off line). Por tanto, la MSCP(TX) obtiene del ISN_I los certificados (claves públicas) de las nuevas BTS del nuevo dominio de seguridad (y administrativo) off-line. Los pasos realizados a continuación tanto en el forward como en el backward handover son análogos al caso 5.3.2.

En el forward handover, independientemente de la distribución realizada en la fase de decisión, se realiza un pase de la clave NBTSp de la MSCP(TX) a la CSS y a la nueva BTS. La nueva BTS pasa su clave pública al MT.

Opciones que pueden darse:
c1) Handover con reenrutado inmediato: Requiere de autentificación mutua inmediata
c2) Handover con reenrutado retardado: Requiere de autentificación mutua retardada

Mensaje S1: Intercambio interno de información en el terminal móvil.

Análogo a 5.3.1

Mensaje S2: Terminal móvil -> Nueva BTS

NBTSp[CCA<<X>>, lista de algoritmos, CH1, Fir(Xs; Xc, Xi, lista de algoritmos, CH1)]

En este tipo de handover, el camino correspondiente para la búsqueda de la CCAp sería el siguiente:
Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva CSS -> Nueva LE -> Nueva MSDP(TX) ida y vuelta.

Es de suponer que la CCAp se conoce por la nueva MSDP(TX) ya que se envia (o es accesible) al nuevo dominio por ejemplo, con los location updating (modo retardado).

El camino correspondiente a seguir para la búsqueda de la lista de revocación de certificados sería:
Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva CSS -> Nueva LE -> Nueva MSDP(TX) ida y vuelta.

Ambos procesos, para hallar la CCAp y la lista de revocación de certificados podrían integrarse.

También se requiere el envio de un mensaje S3 para confirmación y para información de identificación de la nueva BTS al terminal móvil.

Mensaje S3: Nueva BTS -> Terminal móvil.

(Xp [NCAV<<NBTS>>, RN1, algoritmo escogido, lista de revocación de certificados, Fir(NBTSs; Xp[RN1], algoritmo escogido, lista de algoritmos, lista de revocación de certificados, CH1)])

En este caso, se procede a una autentificación de la estación base por el terminal móvil. En el caso general, se requiere el envío de RN1 y Xc, por si es necesaria una autentificación retardada del terminal móvil por la estación base mediante algoritmos de clave secreta (caso de handovers 5.3.2 y 5.3.3).

Al requerirse también de una autentificación del terminal móvil por la estación base (retardada), se envia un mensaje S4:

Mensaje S4: Terminal móvil -> Nueva BTS

(NBTSp [RN2, Fir(Xs; NBTSp[RN2], lista de revocación de certificados)])

Donde puede realizarse una autentificación mutua entre terminal móvil y estación base.

5.4 Gestion de claves en el backward handover

En el backward handover, se parte de la idea de que el handover se invoca por parte de la red hacia el terminal móvil y el nodo que toma la iniciativa es la estación base anterior.

Al igual que en el caso de forward handover, la politica de seguridad más general, requiere invocación de control de acceso en los handover que incorporan cambios en dominios de servicios, seguridad u operadores de red.

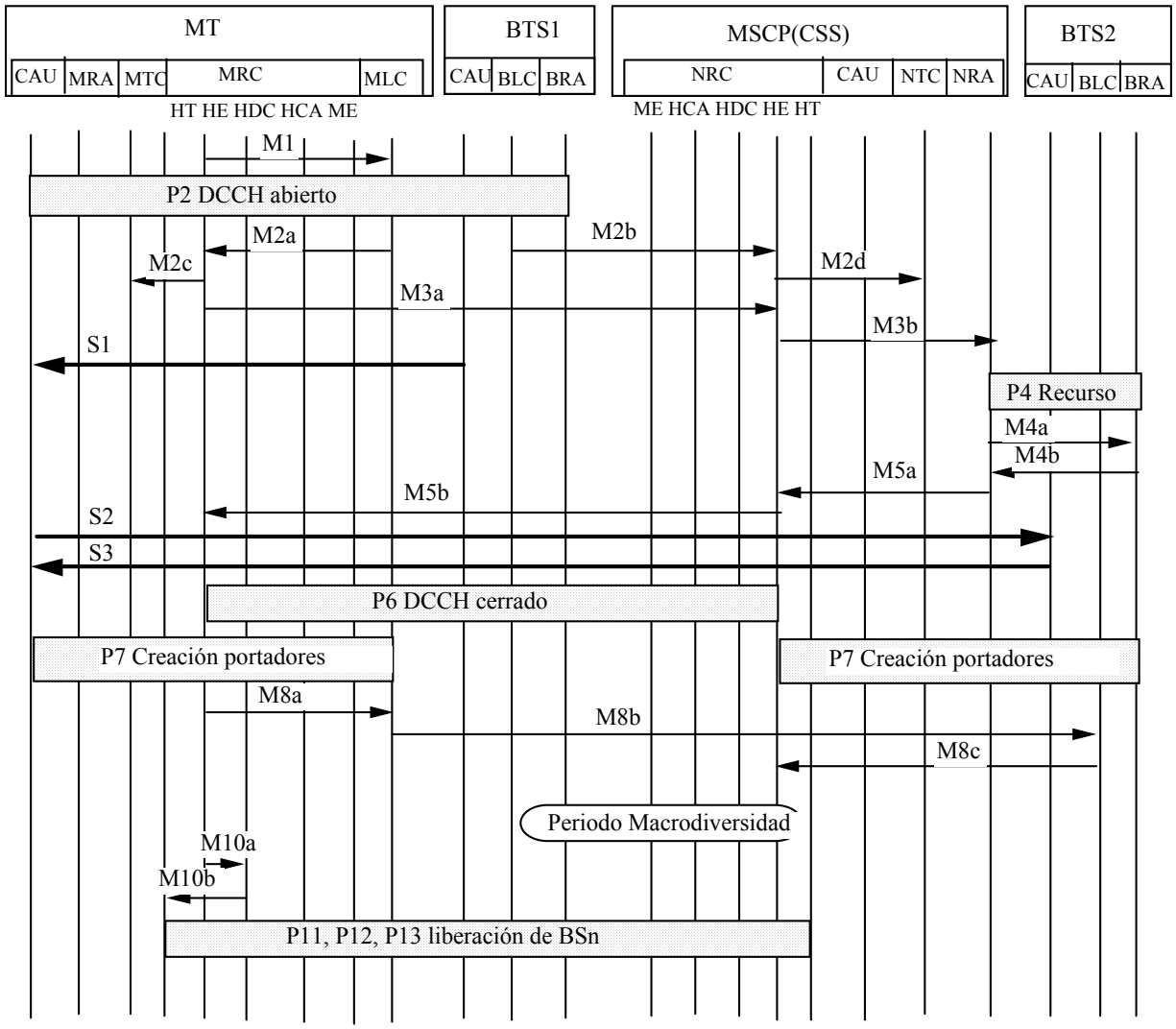


Fig. 5.7 Protocolo de un backward handover con protocolo de seguridad incorporado.

5.4.1 Entre elementos de red que están debajo del elemento CAU en la jerarquía

En este procedimiento, mediante la clave pública del terminal móvil, la OBTS envía la clave pública de la NBTS al terminal a través de un certificado proporcionado por el nuevo dominio. En general, OBTSp y NBTSp pueden ser similares, lo cual se comprueba posteriormente por el terminal móvil. Es decir, se tiene la siguiente secuencia de mensajes:

Mensaje S1: Anterior BTS -> Terminal móvil

(Xp[NCAV<<NBTS>>, lista de algoritmos, CH1, Fir(OBTSs; CH1, lista de algoritmos)])

El terminal móvil en este momento, puede usar la NBTSp proporcionada por la anterior BTS, si bien no está completamente seguro de su autenticidad al carecer de NCAVp.

Mensaje S2: Terminal móvil -> Nueva BTS.

(NBTSp[CCA<<X>>, RN1, algoritmo escogido, Fir(Xs; Xc, Xi, NBTSp[RN1], algoritmo escogido)])

En este paso, se realiza un cambio en el procedimiento general, este mensaje S2 se envia a la nueva estación base, variando la estrategia de un backward handover puro, sin embargo, los resultados que se obtienen son más óptimos ya que pueden en un futuro posibilitar mejor la integración de los dos tipos de handover.

En este paso, se puede hacer una autentificación del terminal móvil por la estación base a través de CH1 y una clave secreta (p.e.Xc) mediante un algoritmo de clave secreta. También es necesario el envío de RN1, en el caso general, por si se requiere de una autentificación de la estación base por el terminal móvil retardada (casos de handovers 5.4.2 y 5.4.3).

Además, se supone que cada BTS y CSS tiene las claves públicas de las demás, dentro de un mismo dominio. En el caso de no disponerse y que sean diferentes, (handover tipos 5.4.2 y 5.4.3) se requerirá de los correspondientes mensajes internos. En el caso de macrodiversidad, el procedimiento sería similar.

Por otra parte, la clave de verificación CCAp puede obtenerse de la nueva MSCP(CSS) con la que enlaza el handover.

5.4.2 Gestión de claves en el handover entre diferentes elementos CAU (en distintos dominios de seguridad y en el mismo dominio administrativo)

En general, también precisa de autentificación, aunque depende de la política de seguridad. Pueden darse las siguientes opciones: que el handover sea entre CSS controladas por la misma LE o bien controladas por diferentes LEs.

En este caso, se supone que las CSS (MSCP(CSS), MSDP(CSS)) disponen de las CAp del resto de autoridades de certificación del operador de red (dentro un mismo dominio administrativo) y la MSCP(LE) obtiene los certificados (claves públicas) de las nuevas BTS del nuevo dominio de seguridad off-line.

En el backward handover se realiza el pase de las claves públicas del nuevo dominio, de la MSDP(LE) anterior a la CSS y a la anterior BTS y de ésta se pasa la clave pública al MT.

Los pasos a realizar antes del envío del primer mensaje al terminal móvil, para ambos tipos de handover pasan por localizar la NBTSp: El camino correspondiente a seguir para la búsqueda de la NBTSp sería:

Anterior MSDP(LE) -> Anterior LE -> Anterior CSS -> Anterior MSCP(CSS) -> Anterior CSS -> Anterior BTS ida y vuelta.

Con la clave pública del terminal móvil, la OBTS envía la clave pública de la NBTS al terminal móvil a través de un certificado proporcionado por el nuevo dominio. En general, OBTSp y NBTSp serán diferentes, lo cual es comprobado por el terminal móvil. Esto es:

Mensaje S1: Anterior BTS -> Terminal móvil

(Xp[NCAV<<NBTS>>, lista de algoritmos, CH1, Fir(OBTSs; CH1, lista de algoritmos)])

El terminal móvil en este momento, puede usar la NBTSp proporcionada por la anterior BTS, si bien no está completamente seguro de su autenticidad al carecer de NCAVp.

Mensaje S2: Terminal móvil -> Nueva BTS.

(NBTSp [CCA<<X>>, RN1, algoritmo escogido, Fir(Xs; Xc, Xi, NBTSp[RN1], algoritmo escogido)])

Paralelamente, se realiza una autentificación del terminal móvil por la estación base a través de CH1.

Una vez recibido este segundo mensaje, se tiene que comprobar la veracidad del certificado enviado por el terminal móvil, para ello, se requiere de la CCAp. El camino correspondiente para la búsqueda de la CCAp sería el siguiente:
Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) ida y vuelta.

El envío de RN1, es necesario en el caso general, por si se requiere de una autentificación de la estación base por el terminal móvil retardada (casos de handovers 5.4.2 y 5.4.3).

No se considera macrodiversidad con estaciones base correspondientes a diferentes CSS por diversos problemas de sincronización y seguridad.

En el caso de requerir de autentificación de la estación base por el terminal móvil (retardada), se requiere el envio de un tercer mensaje.

Se considera que no es necesario un control de acceso en el caso de la opción 1 (CSS controlada por la misma LE), sin embargo, en la opción 2 (CSS controlada por distinta LE),

dependerá de la política de seguridad vigente y para ello habrá que hacer un acceso a la base de datos para obtener la lista de revocación de certificados. Es decir:

Opción: 1. Handover entre CSS controladas por la misma LE:
El camino correspondiente a seguir para la búsqueda de la lista de revocación de certificados sería:
Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva MSDP(CSS) ida y vuelta.

Opción: 2. Handover entre CSS controladas por diferentes LE:
El camino correspondiente a seguir para la búsqueda de la la lista de revocación de certificados sería:
Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva MSDP(CSS) ida y vuelta.

Ambas búsquedas de información (CCAp y la lista de revocación de certificados) a la MSDP(CSS) podrían integrarse en un único camino.

Mensaje S3: Nueva BTS -> Terminal móvil

(Xp [RN2, Fir(NBTSs; Xp[RN2], lista de revocación de certificados)])

Caso de requerirse una autentificación de la nueva estación base por parte del terminal móvil.

5.4.3 Gestión de claves en el handover entre diferentes dominios de seguridad y entre diferentes entornos administrativos

En este caso, la invocación de autentificación vendría impuesta por requerimientos de la política de seguridad vigente, sin embargo, en el caso normal será necesaria la invocación de autentificación mutua debido a que las redes pertenecen a entornos administrativos distintos. Además, se requerirá la invocación de un control de acceso.

Debido a la distribución jerárquica de centros de seguridad y a los diferentes tipos de operadores de red (públicos y privados), se podrían dar cambios en las estrategias de seguridad que podrían requerir interacciones con el centro de gestión del sistema aumentando los retardos.

Entre los diversos entornos administrativos a tratar estarían CPNs, MCPNs, diversos operadores de red (privados o públicos) y la red pública.

En principio, se supone que las CSS (MSCP(CSS), MSDP(CSS)) no disponen de las CAp del resto de autoridades de certificación de distintos operadores de red (en distintos dominios administrativos).

Ya que en el procedimiento de handover se cambia el punto de conexión, en el caso de handover originado por terminal, se pueden distinguir dos autoridades de certificación. Cualquiera, la red antigua o la nueva podría proporcionar las nuevas claves públicas visitadas (ser de confianza).

En este caso, al igual que en el apartado 5.3, la ISN_I dispone de una CA desde la cual, el MSCP(TX) obtiene certificados del resto de entidades de red con las que realiza autentificaciones mutuas de manera unilateral en cada red (off line). El MSCP(TX) obtiene de ISN_I los certificados (claves públicas) de las nuevas BTS del nuevo dominio de seguridad (y administrativo) off-line. Los pasos realizados a continuación tanto en el forward como en el backward handover son análogos a los casos 5.4.2 y 5.4.3).

En el backward handover se realiza el pase de las claves públicas del nuevo dominio, de la MSCP(TX) anterior a la CSS y a la anterior BTS y de ésta se pasa la clave pública al MT.

El camino correspondiente a seguir para la búsqueda de la NBTSp sería:
Anterior MSDP(TX) -> Anterior LE -> Anterior CSS -> Anterior MSCP(CSS) -> Anterior CSS -> Anterior BTS ida y vuelta.

Con la clave pública del terminal móvil, la OBTS envía la clave pública de la NBTS al terminal móvil a través de un certificado proporcionado por el nuevo dominio. En general, OBTSp y NBTSp serán diferentes, lo cual es comprobado por el terminal móvil. Pueden darse las siguientes opciones:

c1) Handover con reenrutado inmediato: Requiere de autentificación mutua inmediata
c2) Handover con reenrutado retardado: Requiere de autentificación mutua retardada

Mensaje S1: Anterior BTS -> Terminal móvil

(Xp[NCAV<<NBTS>>, lista de algoritmos, CH1, Fir(OBTSs; CH1, lista de algoritmos)])

Se requiere de un segundo mensaje para el paso de las claves de sesión a la estación base. Para ello, se supone que la nueva BTS tiene la CCAp que puede adquirirse de la anterior MSDP(TX) para autentificación (retardada) del certificado del terminal móvil.

Mensaje S2: Terminal móvil -> Nueva BTS.

(NBTSp[CCA<<X>>, RN1, algoritmo escogido, Fir(Xs; Xc, Xi, NBTSp[RN1], algoritmo escogido)])

Se realiza una autentificación del terminal móvil por la estación base a través de CH1 y alguna clave secreta.

En este caso, el camino correspondiente a seguir para la búsqueda de la CCAp sería:
Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva CSS -> Nueva LE -> Nueva MSDP(TX) ida y vuelta.

El envío de RN1 es necesario ya que se requiere de una autentificación de la estación base por el terminal móvil retardada (casos de handovers 5.4.2 y 5.4.3).

Por otra parte, no se considera macrodiversidad con estaciones base correspondientes a diferentes CSS por diversos problemas de sincronización y seguridad.

Tanto la búsqueda de CCAp como la de la lista de revocación de certificados podrían integrarse en un único camino. El camino correspondiente para la búsqueda de la la lista de revocación de certificados sería el siguiente:

Nueva BTS -> Nueva CSS -> Nueva MSCP(CSS) -> Nueva CSS -> Nueva LE -> Nueva MSDP(TX) ida y vuelta.

En este caso se requiere de autentificación de la estación base por el terminal móvil (retardada) y se envia un tercer mensaje.

Mensaje S3: Nueva BTS -> Terminal móvil

(Xp [RN2, Fir(NBTSs; Xp[RN2], lista de revocación de certificados)])

Con este mensaje, se realiza una autentificación de la estación base por el terminal móvil (retardada).

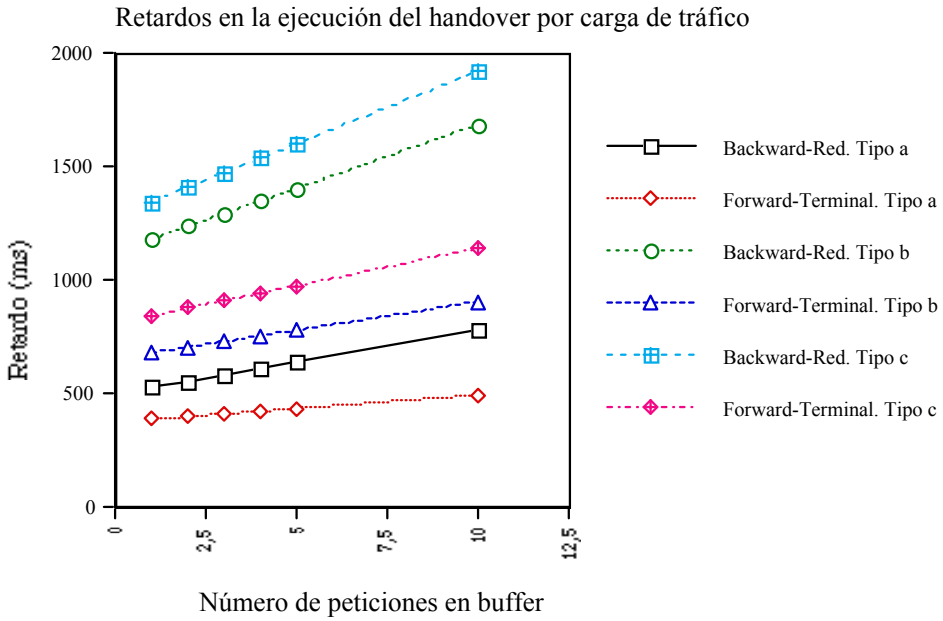
5.5 Comparación de resultados

Con el motivo de poder analizar las prestaciones de los procedimientos de handover definidos en los apartados anteriores, se ha construido un modelo de arquitectura de red en el cual se han especificado los parámetros de funcionamiento que se recogen con detalle en el anexo A.4.

A raíz de los programas realizados basados en la arquitectura de red [RACE25] y los procedimientos descritos anteriormente, se han obtenido los siguientes resultados en forma de gráficas.

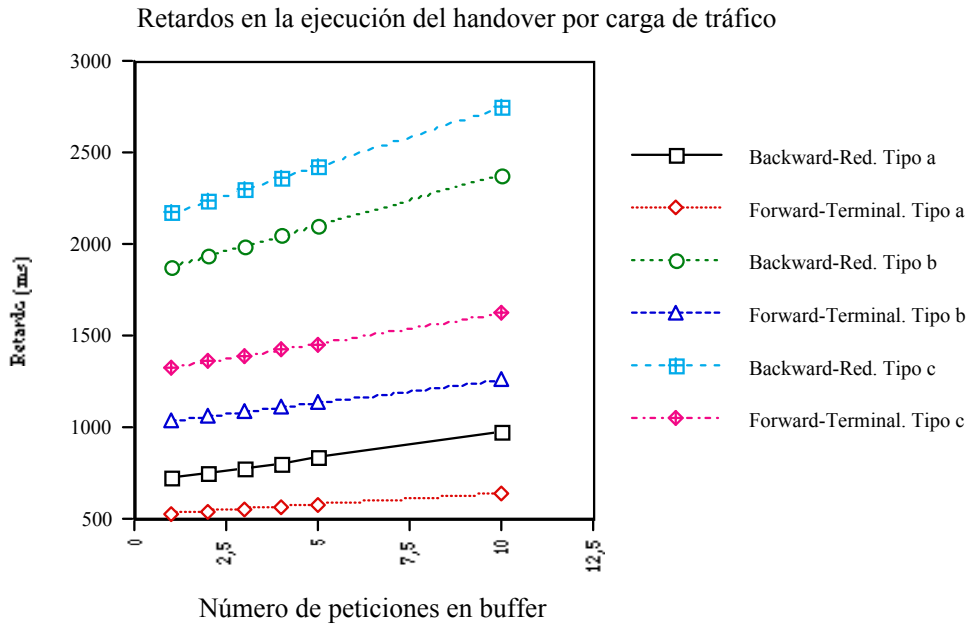
En esta primera gráfica 5.1 se pretende mostrar el efecto del retardo en los distintos tipos de handover definidos conforme aumenta el tráfico ofrecido, descrito en forma de registros de buffer ocupados.

Nota:
El handover tipo a corresponde al realizado en el apartado 5.3.1 ó 5.4.1. El handover tipo b corresponde al realizado en el apartado 5.3.2 ó 5.4.2. Finalmente, el handover tipo c corresponde al realizado en el apartado 5.3.3 ó 5.4.3.

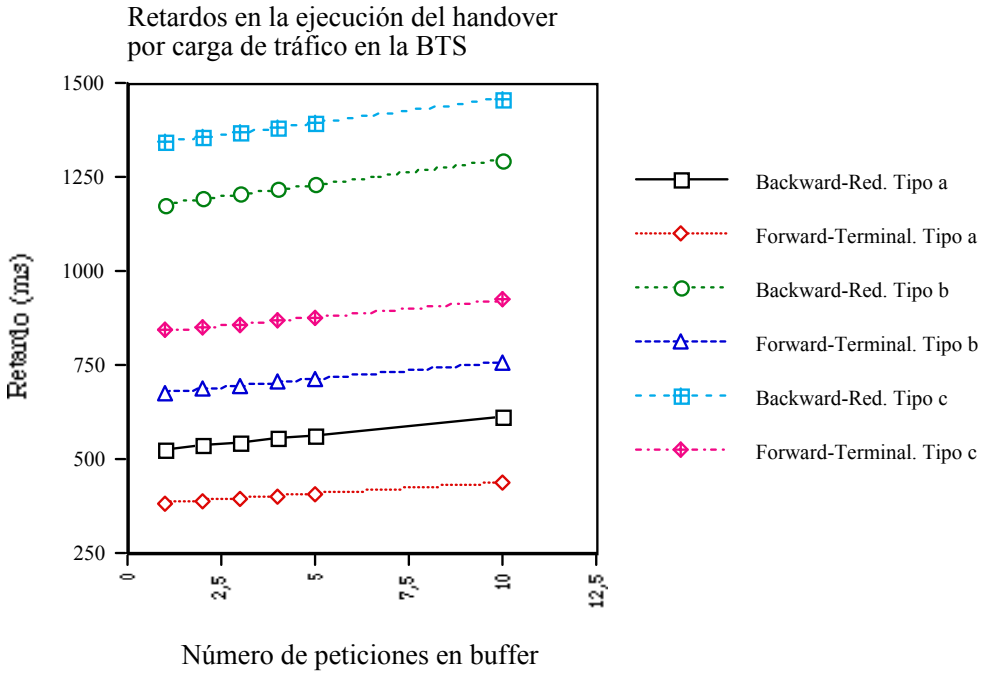


Gráfica 5.1 Retardos en la ejecución del handover para cargas crecientes de tráfico en la red con cifrado de señalización a 64 Kbps.

La gráfica 5.2 respecto de la anterior muestra el efecto de ralentizar a la mitad (32 Kbps) el flujo de información de señalización por el radioenlace al mismo tiempo que la velocidad de cifrado y descifrado.

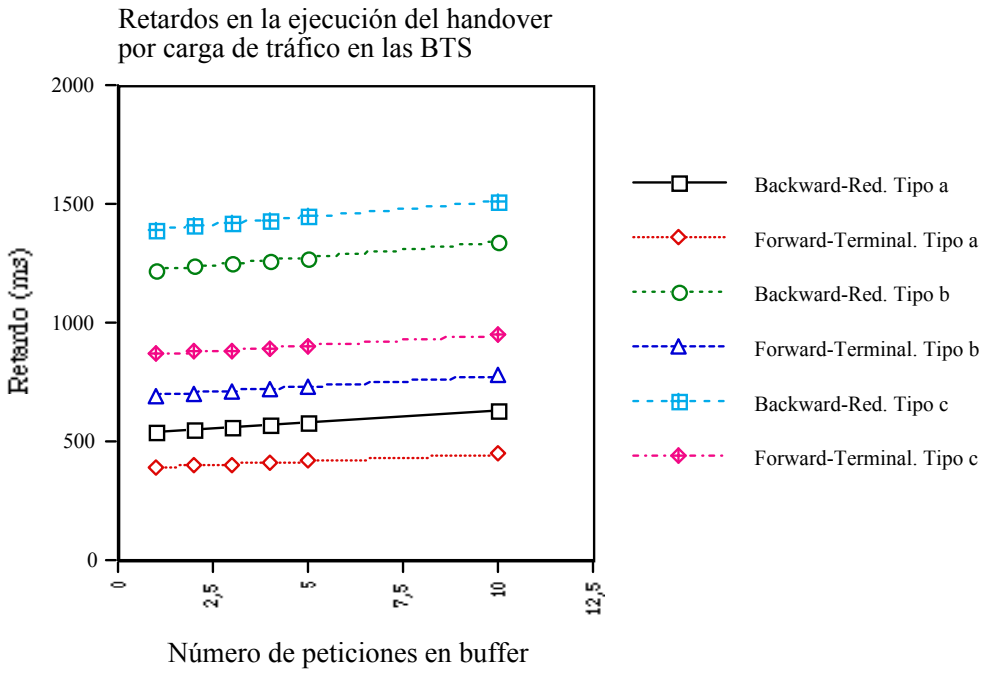


Gráfica 5.2 Retardos en la ejecución del handover para cargas crecientes de tráfico en la red con cifrado de señalización a 32 Kbps.



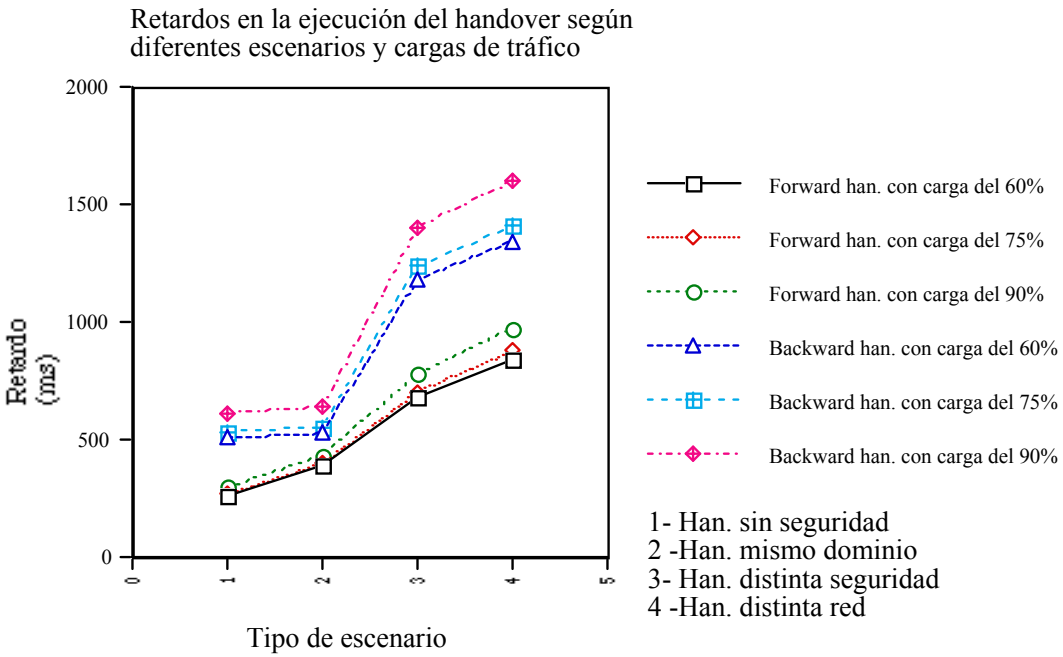
Gráfica 5.3 Retardos en la ejecución del handover para cargas crecientes de tráfico en las BTS con cifrado de señalización a 64 Kbps.

En las gráficas 5.3 y 5.4 se muestra como afecta la congestión producida en la estación base respecto de un tráfico del 60% y del 75% en el resto de los nodos de la red sobre los procedimientos de handover.



Gráfica 5.4 Retardos en la ejecución del handover para cargas crecientes de tráfico en las BTS con cifrado de señalización a 64 Kbps y red fija con tráfico intenso (carga del 75%).

Por último, en la gráfica 5.5, se tiene una representación de los retardos en cuatro tipos de escenarios de los procedimientos de handover según cargas de tráfico variables.



Gráfica 5.5. Retardos en la ejecución del handover para cargas crecientes de tráfico según diferentes escenarios.

5.5.1 Conclusiones

- A raíz de los resultados obtenidos en las gráficas, se constata una mayor rapidez del handover en el caso del procedimiento forward con respecto al backward para los tres tipos definidos a), b), c).

- Como consecuencia de la mayor rapidez estimada por el procedimiento del forward handover, el inicio del handover por parte del terminal es preferible al inicio por parte de la red.

- A pesar de que el forward handover en los casos b) y c) es más rápido que en el caso backward, presenta posibles problemas por motivos de seguridad al enviar información sensible previa a un control de acceso.

- Como se muestra en las gráficas 1 y 2, los efectos de ralentizar la velocidad de la información de señalización y/o velocidad de cifrado en el radioenlace provocan importantes retardos en la ejecución del handover.

- Como consecuencia de las gráficas 3, 4 y 5 puede decirse que los efectos de congestión en la red también afectan pero en menor medida ya que se parte de una arquitectura distribuida.

- Los handovers definidos para los casos b) y c), aunque poco frecuentes, incorporan considerable retardo. Estos casos dependen bastante de la arquitectura de la red fija. Aquí se ha utilizado la arquitectura UMTS definida en [RACE25] RACE, sin embargo, continuamente se estan realizando modificaciones para la incorporación de fibra óptica hasta las mismas BTS alterando los protocolos de señalización por sus canales buscando su interconexión via técnicas ATM a la red fija BISDN. También se está avanzando en el diseño de arquitecturas en las que se interconectan BTS mediante redes de area metropolitana (MAN) o ATM para el adecuado soporte de comunicaciones (o handovers) en terminales móviles a gran velocidad, o bien en celdas de tamaño pequeño (micro, picoceldas). Todo eso exige protocolos nuevos y readaptaciones de parámetros en los modelos, que si bien están en fase de estudio, no son incluidos en la presente tesis.

- Por otra parte, el avance continuo de la tecnología en circuitos integrados, permite integrar funciones complejas en cada vez menos espacio. El uso masivo de tarjetas inteligentes, procesadores en paralelo en los nodos de la red, terminales más pequeños, etc, permitirá mejorar continuamente las prestaciones del sistema. De esta forma, si bien las diferencias relativas en prestaciones entre procedimientos variarán poco, si que pueden hacerlo sus magnitudes absolutas.

- La deseable interconexión (integración) de UMTS con redes preexistentes, tipo GSM, DECT o redes con modulación CDMA hace suponer que los terminales móviles, a pesar de todo, podrían invocar distintos procedimientos de handover en un futuro. Actualmente, diversos estudios persiguen una compatibilidad de funcionamiento sobre un único terminal móvil inteligente con un sistema multiacceso a diferentes redes móviles avanzadas.

5.6 Movilidad y generación de handover

Se puede modelar el comportamiento del tráfico en un sistema de telefonía móvil formado con celdas hexagonales a partir de la movilidad de sus terminales. Seguidamente, se plantean los términos que definen las frecuencias de cruce, y por tanto, de handover en una celda, en un cluster de celdas y por último entre redes. Eso permitirá tener una referencia sobre la carga de señalización que deberá afrontar el sistema desde un punto de vista teórico. Se puede determinar el número de handover entre celdas distintas, dominios distintos (clusters) o bien el número de handover entre redes de operadores distintos.

Por otra parte, se han realizado pruebas de tipo experimental en entornos de población reales en diferentes ciudades europeas (p.e. Londres, Amsterdam, Helsinki) donde se han obtenido medidas de la movilidad de los terminales y que ha permitido evaluar la bondad de los modelos teóricos. (Ver anexo A.4).

Para el análisis del modelo se utilizará la siguiente notación:

R_{HA} : Número de handovers entre celdas del mismo dominio
R_{LU} : Tasa de handover entre distintos dominios
R_{RED} : Número de handovers cruzando el área de una red
M_{celda} : Número de usuarios cruzando una celda de un mismo dominio por seg
M_{LU} : Número de usuarios cruzando un área de distinto dominio por seg.
ρ : Densidad de terminales (usuarios/Km^2)
v: Velocidad media de los usuarios (Km/seg)
L: Longitud perímetro (Km)
Pter: Probabilidad de cruzar estando llamando

Sea la movilidad de los usuarios en direcciones aleatorias y con velocidad media v en las celdas:

$$M_{celda} = \frac{\rho * v * L}{\pi}$$

$$R_{HA} = M_{celda} * Pter$$

y la movilidad entre dominios:

$$R_{LU} = M_{LU} * Pter$$

$$M_{LU} = \frac{2}{\sqrt{3}}\sqrt{N} * M_{celda}$$

Si se define:
N: Número de celdas por dominio
K: Número de dominios en cada red
$N_s(N)$: Número de caras expuestas limítrofes con N celdas hexagonales
Fracción del dominio dentro del área considerada que genera tráfico.

$$\frac{N_s(KN)}{K * N_s(N)} = \frac{1}{\sqrt{K}}$$
$$N_s(KN) = 4\sqrt{3N}$$

Movilidad entre redes:

$$R_{RED} = M_{RED} * Pter$$
Donde M_{RED} es una agrupación de dominios en una red.
$$M_{RED} = \sqrt{K} * M_{LU}$$

Además puede hacerse una estimación del coste, por ejemplo retardo, que supone para la red la movilidad especificada en cada caso por el terminal.

Sea el coste por celda:
$S_{HA} = R_{HA} * C_{HA}$
R_{HA} : Número de handovers por celda.
C_{HA} : Coste: Retardos o número de paquetes (bits de información) para cada procedimiento.

Coste por dominios:
$S_{LU} = R_{LU} * C_{LU}$
R_{LU} Proporcional a la tasa de handovers de las celdas limítrofes,no interiores.
C_{LU} : Coste por dominio

Coste por redes:

$S_{RED} = R_{RED} * C_{RED}$

R_{RED} : Número de handovers por red

C_{RED} : Coste: Retardos o número de paquetes (bits de información) para cada red.

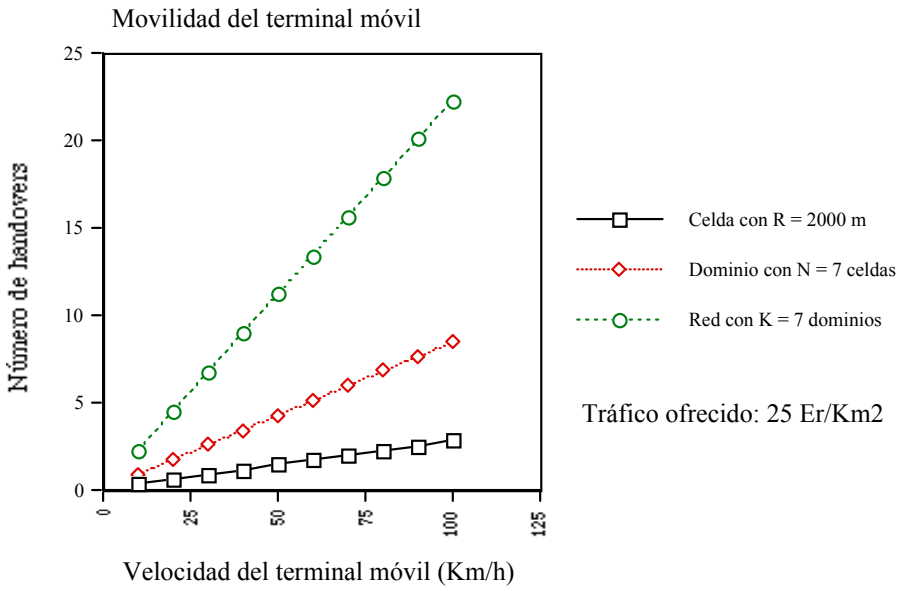
Como consecuencia de aplicar la información obtenida en pruebas experimentales sobre entornos de Londres y Randstad sobre tráfico en diversas situaciones, se puede establecer un retardo medio de handover con la siguiente expresión:

$$Tmedio = 0,626 * T_A + 0,271 * T_B + 0,102 * T_C$$

siendo T_A el retardo medio en el handover entre celdas pertenecientes a la misma CSS, T_B el retardo medio en el handover entre celdas pertenecientes a distintos dominios y T_C el retardo medio en el handover entre celdas pertenecientes a distintas redes. Aplicando los valores de retardos obtenidos en el apartado anterior, y conociendo la proporción de tipos de handover para una estructura de red con N = K = 7, se obtiene un Tmedio = 0,505 s, que puede considerarse aceptable y está dentro de los requerimientos exigidos por los servicios propuestos en la red.

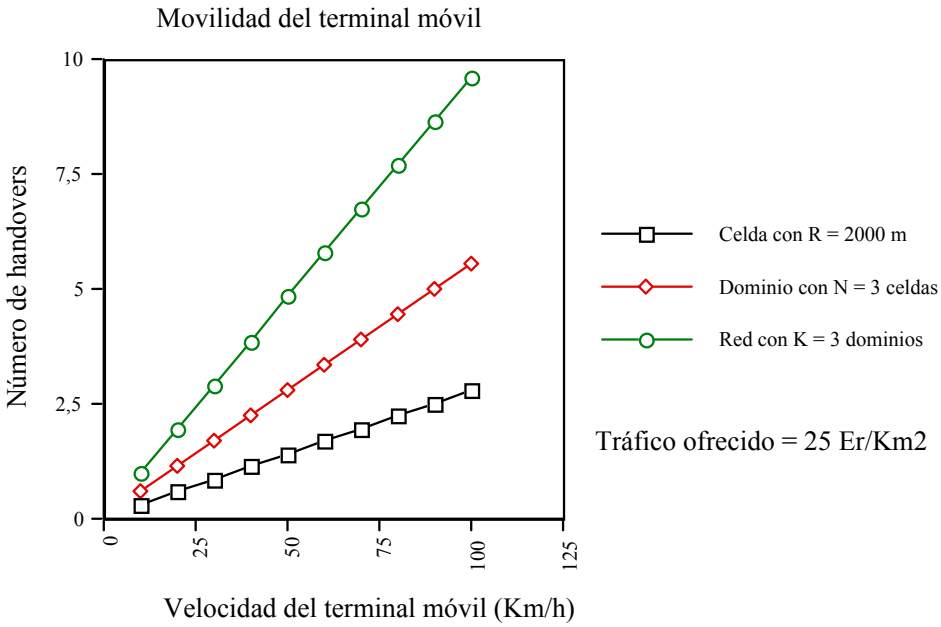
A continuación, se presentarán por medio de gráficas los resultados relativos al número de handovers para un conjunto de diferentes configuraciones obtenidos a través de las expresiones definidas en este apartado .

La gráfica 5.6 muestra el número de handovers que se producen de los tres tipos definidos para un escenario formado con macroceldas de radio 2 Km con una estructura de N = 3 celdas por dominio y K = 3 dominios por red en función de la velocidad del terminal móvil.



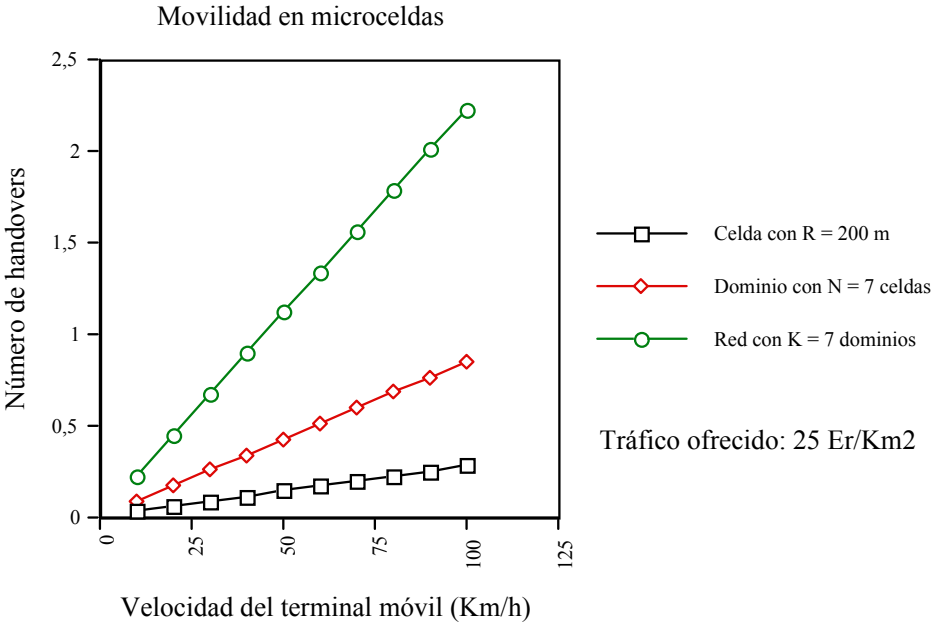
Gráfica 5.6 Número de handovers en un entorno de macroceldas en función de la velocidad del terminal móvil.

La gráfica 5.7 muestra los efectos de tener una estructura de N = 7 celdas por dominio y K = 7 dominios por red con el fin de comparar los resultados con la gráfica anterior.

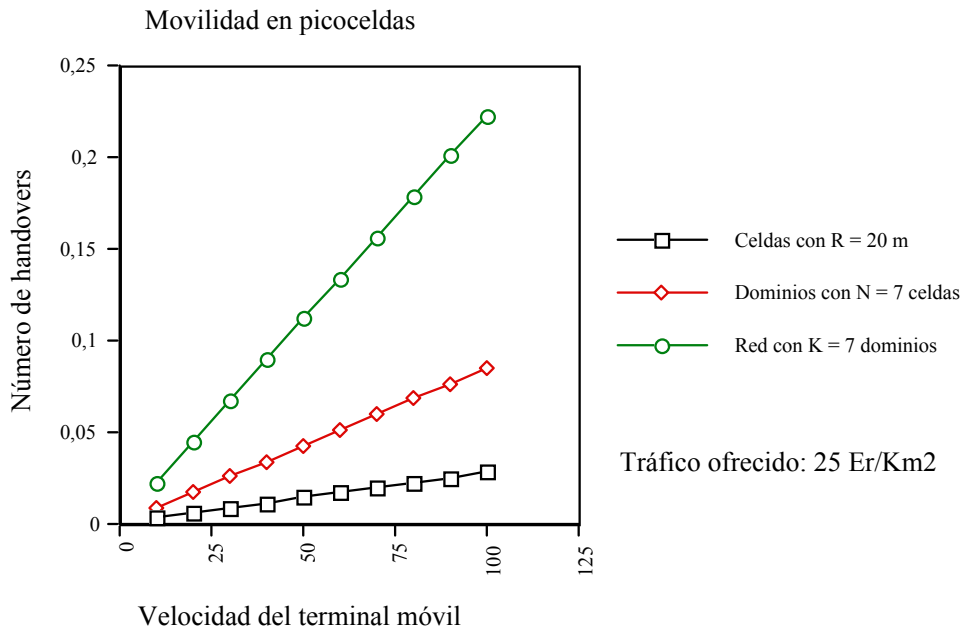


Gráfica 5.7. Número de handovers en un entorno de macroceldas menor en función de la velocidad del terminal móvil.

Las gráficas 5.8 y 5.9 muestran el efecto del número de handovers registrados en el caso de utilizar escenarios con microceldas de R = 200 m y picoceldas con R = 20 m en función de la velocidad del terminal móvil.

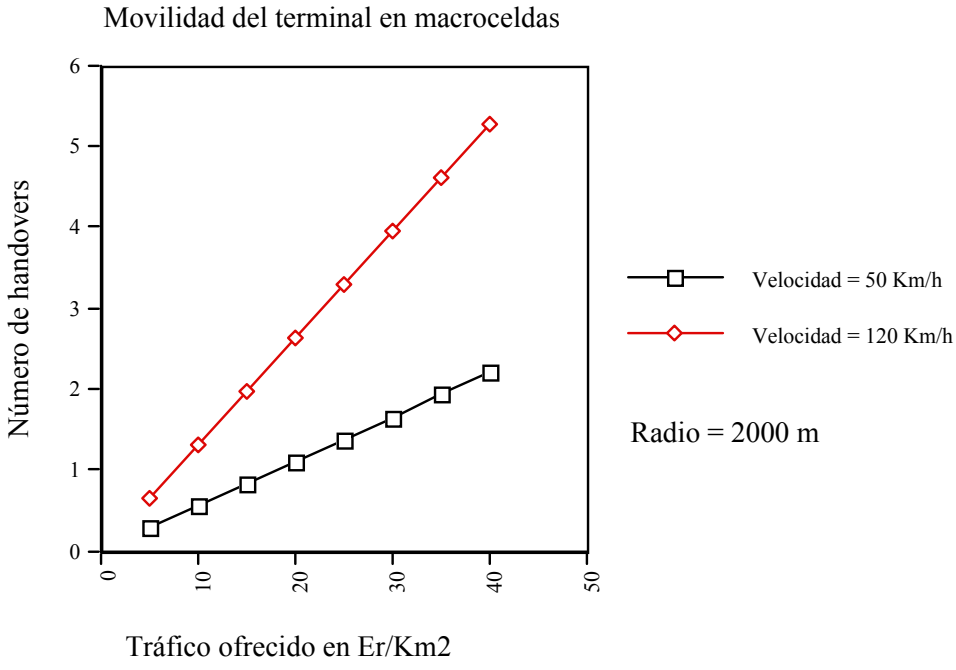


Gráfica 5.8 Número de handovers en un entorno de microceldas en función de la velocidad del terminal móvil.



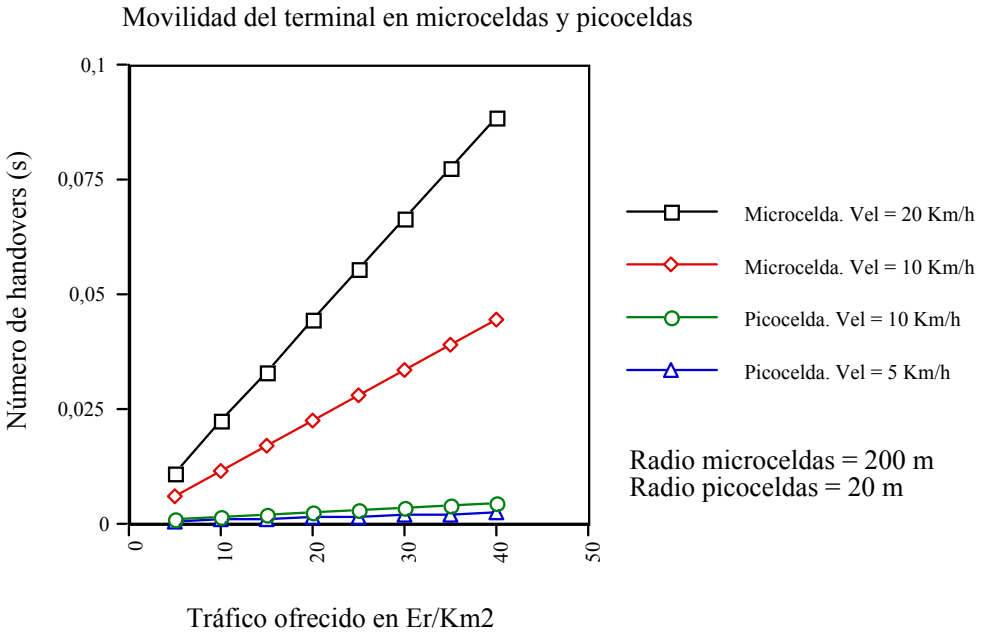
Gráfica 5.9 Número de handovers en un entorno de picoceldas en función de la velocidad del terminal móvil.

En la gráfica 5.10 se muestran los efectos estadísticos en el número de handovers registrados por el paso de un terminal móvil sobre macroceldas de R = 2 Km a distintas velocidades según la carga de tráfico ofrecido.



Gráfica 5.10 Número de handovers en un entorno de macroceldas en función del tráfico ofrecido en la celda.

Finalmente, en la gráfica 5.11, se muestran los efectos descritos en la gráfica anterior para el caso de escenarios formados con microceldas o bien picoceldas.



Gráfica 5.11 Número de handovers en un entorno de microceldas y picoceldas en función del tráfico ofrecido en la celda.

5.6.1 Conclusiones

- De las gráficas 5.6 y 5.7 se puede determinar que el número de handovers entre dominios o bien entre redes distintas aumenta conforme la estructura de la red se hace más compleja. En este caso, se pasa de N = 3 celdas por dominio y K = 3 dominios por red a N = 7 celdas por dominio y K = 7 dominios por red. Eso se debe a la mayor longitud de la linea de cobertura de los clusters formados por un mayor número de macroceldas.

- Respecto a las gráficas 5.6, 5.8 y 5.9 se vuelve a constatar un mayor número de handovers conforme aumenta la velocidad del terminal móvil en los casos de entornos formados por macroceldas respecto a entornos con microceldas o picoceldas.

- De la gráfica 5.10 se puede deducir que conforme el tráfico ofrecido a la celda es mayor, la probabilidad de que se produzca un handover aumenta. También contribuye a ese efecto la velocidad del mismo terminal móvil.

- A partir de las gráficas 5.10 y 5.11 se contrasta el numero de handovers realizados según el tamaño de las celdas. Se observa que la mayor longitud de circunferencia de las celdas contribuye en general a una mayor probabilidad de handover.

- Como resultado de aplicar la información obtenida en pruebas experimentales sobre entornos de diversas ciudades así como de contrastar esas mediciones con las formulaciones estadísticas anteriores sobre tráfico en diversas situaciones, se puede establecer un retardo medio de handover de 0,505 s, que puede considerarse aceptable y que está dentro de los requerimientos exigidos por los servicios propuestos en redes avanzadas.

5.7 Contribuciones al capitulo

En este capitulo, se propone un algoritmo de ejecución al que se integran unos mensajes para soportar servicios de seguridad. También se detalla una gestión de claves a fin de proporcionar los servicios de forma óptima en el handover [AB13-15].

Se realizan diversas simulaciones en donde se define una arquitectura de red semejante a la UMTS y en donde se incorporan las funcionalidades de seguridad propuestas.

Se consideran diversos tipos de handover según la procedencia de las entidades funcionales que son involucradas, se analiza el impacto de la seguridad en los diferentes tipos de escenarios de handover según las redes involucradas [AB1]. Después de un determinado análisis previo, se proponen dos algoritmos de ejecución seguros: *forward* y *backward* donde se analizan las prestaciones. Se complementan los resultados mediante estimaciones teóricas y experimentales de los niveles de tráfico así como de los requerimientos a soportar por el sistema proporcionando al final las debidas conclusiones.

5.8 Referencias

[AA2] Anthony S. Acampora, Mahmoud Naghshineh. *An architecture and methodology for mobile executed handoff in cellular ATM networks.* IEEE Journal on selected areas in communications. p. 1365-1375. Octubre 1994.

[AB13] A. Barba y J. L. Melús. *Gestión de claves en un handover avanzado según una arquitectura de seguridad UMTS.* III Reunión española sobre Criptología, Barcelona, Nov. 1994.

[AB14] A. Barba y J. L. Melús. *The key management mechanism in the handover. performances related to an advanced mobile network.* IEEE SICON/ICIE´95 p. 411-415. Singapur, Julio 1995.

[AB15] A. Barba y J. L. Melús. *Key management in the handover. Application to third generation mobile systems.* Personal, Indoor and mobile radio communications (PIMRC´95) p. 300-305. Toronto, Septiembre 1995.

[AD1] Andrew D. Malyan, Leslie J. Ng, Victor C. M. Leung, Robert W. Donaldson. *Network architecture and signaling for wireless personal communications.* p. 830-841. IEEE Journal on selected areas in communications. Agosto 1993.

[AS1] Ashar Aziz, Whitfield Diffie. *Privacy and authentication for wireless local area networks*. p. 25-31. IEEE Personal Communications 1994.

[GP1] Gregory P. Pollini, Sami Tabbane. *The intelligent network signalling and switching costs of an alternate location strategy using memory*. 43rd VTC. p.931-934. 1993.

[GP2] Gregory P. Pollini. *Capacity of an IEEE 802.6 based cellular packet switch*. p. 1264-1268. ICC'93 Geneve. 1993.

[GP3] Gregory P. Pollini, Kathleen S. Meier-Hellstern, and David J. Goodman. *Signalling traffic volume generated by mobile and personal communications.* IEEE Communications Magazine, p.60-65, Junio 1995.

[IJ1] Immonen Jukka, Romann Jean-Marc, Plassmann Dieter. *Requirements and protocol architecture for MBS access to ATM network.* p. 324-328. Portugal, 1995.

[IS1] Ivan Seskar, Svetislav V. Marie, Jack Holtzman and Jack Wasserman. *Rate of location area updates in cellular systems.* VTC´92, p.694-697, Denver, 1992.

[ISO2] ISO/IEC CD 11770-3 Key management mechanisms using asymmetric cryptographic techniques. June 1993.

[ISO3] Information Technology - Security Frameworks for Open Systems- Part 2: Authentication Framework (DIS 10181-2).

[ISO4] Revised working Draft: Key management, Part 1: Framework. SC27 N 602.

[ISO12] Banking - Key management (wholesale). ISO 8732.

[ISO13] WD: Key management, Part 2: key management mechanisms using symmetric cryptographic techniques. SC27 N 486.

[KM1] Kathleen S. Meier-Hellstern, Gregory P. Pollini and David J. Goodman. *A wireless service for the IEEE 802.6 metropolitan area network.* p. 1964-1968. Globecom '91.

[KM2] Kathleen S. Meier-Hellstern, Eduardo Alonso. *The use of SS7 and GSM to support high density personal communications.* p. 1698-1702. ICC 1992.

[KM3] Kathleen S. Meier-Hellstern, Gregory P. Pollini, David J. Goodman. *Network protocols for the cellular packet switch.* p. 705-710. 42nd IEEE Vehicular Technology. 1992.

[KM4] Eduardo Alonso, Kathleen S. Meier-Hellstern. *Influence of cell geometry on handover and registration rates in cellular and universal personal telecommunications networks.* Proc. 8th International Teletraffic seminar, Santa Margherita Ligure (Genova), p.261-270, Octubre 1992.

[LF2] Frey L., Horn G., Müller K. *Security protocols for UMTS*. RACE Mobile Telecommunications Summit. p. 404-410. Cascais (Portugal) 1995.

[MH1] Mitts Hakan. *Universal wireless accesss to ATM.* p. 329-333. Portugal, 1995

[RACE7] RACE 2066/ASCOM/MF3/DS/P/064/b1. Implementation of security services by security mechanisms. 1994.

[RACE8] RACE 2066/ASCOM/MF3/DS/P/077/b1, Specification of protocols for security services (final). Dic. 1994.

[RACE9] RACE 2066/ASCOM/MF3/DS/P/085/b1, Integration of security services and definition of interfaces. Dic. 1994.

[RACE25] RACE 2066/FACE/GA3/DS/P/033, UMTS Network Architecture Draft. July 1993.

[RACE30] RACE 2084/FACE/TS3/DN/I/012/a1. Annex 5. Handover procedures. Enero 1994.

[RACE31] RACE 2066/CSELT/MF2/DS/P/071/b1. BSS Architecture and interconnection schemes. Junio 1994.

[RM1] Refik Molva, Didier Samfat and Gene Tsudik. *Authentication of mobile users.* p. 26-34. IEEE Network. Marzo/Abril 1994.

[SN2] Sanjiv Nanda, Subra dravida, Behrokh Samadi. *Handoff management and performance for wireless access using metropolitan area networks.* p. 839-845. 43th VTC. 1993.

[TH1] Thomas Hardjono, Tetsuya Chikaraishi, Tadashi Ohta. *An approach to key management and inter-domain authentication in the Telecommunications Management Network.* p. 171-176. Globecom '93.

[WIN1] Technical report WINLAB-TR-24. The use of SS7 and GSM to support high density personal communications. 1991.

Capitulo 6

Conclusiones

6. Conclusiones

Las redes de comunicaciones, en definitiva, se diseñan para servir a los usuarios, bien sea a través de entornos de empresas o bien para zonas residenciales. Estas nuevas redes cada vez más, tratan de dar solución a un mayor número de necesidades que plantean las sociedades modernas. Entre estas necesidades destaca últimamente la de satisfacer una mayor movilidad de los usuarios, así como una mayor necesidad de mantenerse informado en cualquier escenario, es decir, el usuario precisa cada vez más de redes que proporcionen cobertura mundialmente.

La globalización es una de las influencias más importantes para este fin de siglo y para bien entrado el próximo milenio. Estas fuerzas económicas afectan tanto a gobiernos, grandes corporaciones como a usuarios. Los procesos que caracterizan mejor estas nuevas tendencias son:
a) Incremento de la movilidad, asociada a gente, ideas, en general a transmisión de la información financiera, científica, etc...
b) Simultaneidad: Todo el mundo ha de estar disponible en cualquier lugar en cualquier momento. Información y productos de las grandes corporaciones han de estar disponibles en todos los países para los usuarios.
c) La posibilidad de que esta globalización permita la competitividad entre fronteras y permita diversas alternativas en la selección de múltiples operadores de red por parte de los usuarios.
d) Pluralismo y dispersión de expertos e influencias desde centros corporativos centralizados a jerarquías distribuidas formadas por centros filiales.

Es en este contexto donde debe ubicarse nuestra propuesta de diseño de funciones en algoritmos para el procedimiento de handover que permita una movilidad óptima de terminales en un sistema de comunicaciones móviles avanzado.

Por otra parte, los crecientes avances tecnológicos permiten diseñar escenarios de redes inteligentes con sistemas de gestión distribuidos basados en equipos informáticos de altas prestaciones capaces de soportar los altos requerimientos de cálculo de estas nuevas redes. En este trabajo se utiliza un escenario de este tipo, mediante el diseño de entidades de control MSCP(CSS) inteligentes que se apoyan en centros de gestión integrados en una red fija formada por bases de datos.

Los centros de gestión proporcionan información acerca del 'status' y del estado de congestión de la red, las bases de datos almacenan los certificados de clave pública y los terminales inteligentes permiten soportar la gestión de claves y servicios de seguridad especificados por los requerimientos del sistema.

Se definen los servicios y mecanismos para proporcionar seguridad al procedimiento de handover. Para ello se especifica una arquitectura de seguridad para redes móviles avanzadas basada en una distribución de bases de datos distribuidas jerárquicamente ya especificada para estos tipos de sistemas. Por otra parte, asumible dentro de la iniciativa europea que afronta este reto mediante el sistema UMTS.

Se constata además que la integración de algoritmos de clave pública y algoritmos de clave secreta en un sistema híbrido es una solución suficientemente flexible y óptima técnicamente que posibilita un buen entendimiento al mismo tiempo que garantiza la protección de la información entre operadores de red de múltiples países.

Concretamente, y a modo de resumen, en esta tesis se ha presentado:

- Un diseño basado en la idoneidad de determinados parámetros para su empleo en la fase de decisión de selección de celdas en el handover.

- Un algoritmo de decisión para la selección de celdas candidatas (FHAi) en el handover junto con un modelo de escenario formado por estructuras de macro-microceldas dispuestas de manera óptima para un sistema de comunicaciones móviles.

- Los análisis teóricos, mediante modelos y por medio de programas de simulación que permiten determinar las prestaciones de parámetros de diseño y los algoritmos más adecuados en cada entorno de handover.

- La definición de una arquitectura de seguridad basada en requerimientos de amenazas y servicios planteados previamente en el sistema UMTS.

- La introducción de un sistema de gestión de claves integrado en la fase de decisión del handover.

- Un protocolo para la gestión de claves y servicios de seguridad para la fase de ejecución del handover.

- La introducción de un método híbrido basado en el uso de certificados y algoritmos de clave pública para la protección de los canales de señalización y el uso de algoritmos de clave secreta para la protección de la información de usuario.

- Proponer un sistema de gestión de tráfico y congestión en la red que integre los algoritmos DCA (Asignación Dinámica de Canales) con la gestión debida al handover.

- Optimizar el modelo de tráfico y el escenario de celdas empleados, por ejemplo, para una gestión de red inteligente que integre además una cobertura con satélites artificiales.

- Plantear una nueva arquitectura de red que permita afrontar mejor el retardo ocasionado en el handover para el caso de terminales móviles de alta movilidad en entornos de microceldas.

- El planteamiento del uso de agentes itinerantes para la operatividad de los terminales móviles en los procedimientos de movilidad y de establecimiento de llamada.

- Sistema de gestión de red orientado al soporte de un servicio de directorios distribuido.

- Ubicación óptima de entidades de seguridad en la red. Por ejemplo, puede requerir de un estudio más preciso si se cambia la arquitectura de la red o si el factor coste económico es muy importante.

- Avanzar en la definición de firmas digitales y certificados. Por ejemplo, valorar el impacto de las curvas elípticas en la longitud de los certificados.

Anexo 1

Parámetros utilizados en modelos y simulaciones

En este anexo se describen las características de los programas, modelos y simulaciones, usados para la realización de los cálculos requeridos en el presente trabajo.

A1.1 Modelo de red utilizado para el protocolo de ejecución del handover

En este apartado se introducirán el modelo de red y los parámetros utilizados en la definición del protocolo de ejecución del handover. Por ello, se analizan a continuación con más detalle los requerimientos a tener en cuenta en el modelo de los nodos, enlace, buffers, etc.

A1.1.1 Modelo de un nodo

Los nodos de la red física son definidos con una misma estructura básica. La operación de los nodos está representada por modelos cola - servidor para representar el buffer y el procesado de los mensajes de información respectivamente. Cada cola podría establecerse para el acceso a un proceso, por ejemplo, control de llamada, control de servicios portadores, etc .

Cada proceso podría ejecutarse en uno o más procesadores estando disponible una compartición de carga. Un nivel de complejidad superior consistiría en que cada procesador podría compartir temporalmente entre un número de tareas simultáneamente o podría ser interrumpido por algún proceso interno relacionado del nodo. Para un multiprocesador con compartición de carga, el retardo de cola podría ser muy pequeño. Una solución sería modelar los procesadores centrales con un retardo fijo para cada tipo de función por el uso del procesador (M/D/1).

Los nodos se comportan de la siguiente forma:

1) Los mensajes No. 7 del sistema de señalización entrantes al nivel físico 1 son colocados inicialmente en cola. Todos ellos se configuran en múltiplos de 64 bytes.

2) Los mensajes SS7 son desenpaquetados por el preprocesador hasta el nivel 3 para determinar si el mensaje requiere ser procesado por el nodo. En caso contrario, el mensaje es enrutado directamente al correspondiente buffer del puerto de salida con un retardo dt3, usando el nodo como un STP (Signalling Transfer Point). El desempaquetado del mensaje dentro del procesador desde el nivel 1 al 3 toma un tiempo tu independiente de la talla del mensaje.

Tiempo completo medio para desempaquetar un mensaje, Tu = (Qav + 1) * tu
donde Qav es la longitud de la cola media en buffer del puerto de entrada.

3) Un tiempo de retardo fijo dt1 se asigna en el enrutado del mensaje a nivel 3 desde el preprocesador al procesador principal. Esto se debe al retardo del bus interno y debido al método de acceso usado por el procesador.

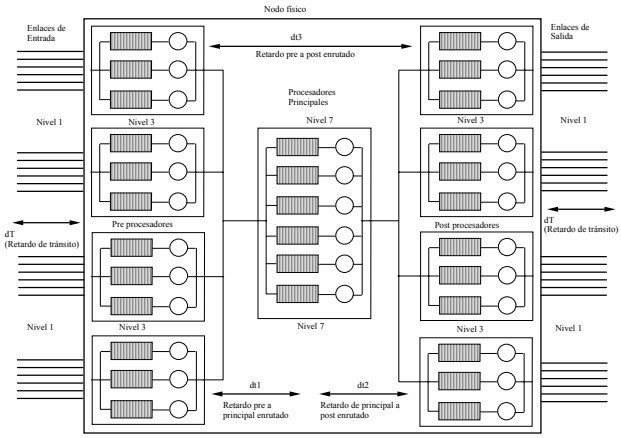


Fig. A1.1 Esquema genérico que muestra la estructura de buffers y servidores de un nodo de la red.

4) Los mensajes a ser procesados por el nodo son aleatoriamente asignados a uno de los buffers del procesador principal del nodo.

5) El tiempo de procesamiento principal incluye la conversión del mensaje de señalización entre el nivel 3 de red y el nivel 7 de aplicación y depende de:

- La subfunción UMTS realizada en particular.
- El mensaje UMTS en particular.

6) Retardo fijo dt2 asignado al enrutado del mensaje de nivel 3 desde el procesador principal al postprocesador. De nuevo, esto se debe al retardo del bus interno y debido al método usado de acceso al procesador.

7) Los mensajes de nivel 3 son enrutados a los buffers de los puertos de salida apropiados. Siendo asignado a un postprocesador, el mensaje es enpaquetado desde el nivel 3 al nivel físico 1. El empaquetamiento del mensaje dentro del procesador tiene un retardo fijo tp independiente del tamaño del mensaje.

Tiempo total medio de desempaquetado de un mensaje, Tp = (Qav + 1) * tp
donde Qav es la longitud de la cola media a la cola del puerto de salida.

A1.1.2 Parámetros de un nodo

A continuación, se especifican los valores asignados a los distintos retardos que parametrizan el funcionamiento de los nodos que conforman la red.

- Tiempo de desempaquetado (tu):
Cada nodo de red tiene un número de preprocesadores dentro de cada enlace que desempaquetan del nivel 1 de señalización SS7 al nivel 3 para determinar si necesitan ser procesados por el propio nodo. Este retardo se ha estimado para todo tipo de nodo como:
tu = 1 ms

- Retardo temporal de preprocesador a procesador principal (dt1):
Este es un retardo fijo que representa el enrutado del mensaje de nivel 3 a la cola del procesador principal. Se asigna:
dt1 = 5 ms.

- Tiempo de retardo de procesador principal:
Se aplica a los siguientes tipos de nodos, BTS, CSS, LE, TX, MSCP, MSDP.
Puede realizarse la siguiente división:

- Tiempo de procesamiento del controlador de servicios en MT: 5 ms.
- Tiempo de procesamiento de control de handover en BTS: 3 ms.
- Tiempo de procesamiento del controlador de servicios en CSS: 3 ms.
- Tiempo de procesamiento de control de handover en LE: 3 ms.
- Tiempo de procesamiento de control de servicios en TX: 3 ms.
- Tiempo de procesamiento de control de servicio en MSCP: 1 ms.
- Tiempo de procesamiento para acceso de datos/renovación en MSDP: 5 ms.

- Tiempo de procesamiento de transferencia/renovación de ficheros en MSDP: 100 ms.

El tiempo de procesamiento para leer/escribir ficheros como perfiles de usuario puede ser de unos 100 ms frente a elementos particulares de información de unos 5 ms.

- Tiempo de retardo de procesador principal a postprocesador (dt2):
Este es un retardo fijo que representa el enrutado del mensaje de señal de nivel 3 desde el procesador principal a la cola apropiada del post procesador para el requerido puerto de salida:
dt2 = 5 ms.

- Tiempo de empaquetamiento (tp):
Cada puerto de salida tiene un número de post procesadores que empaquetan los mensajes desde el nivel 3 al nivel 1 antes de enviar la señal por el apropiado enlace de señalización de salida:
tp: 1 ms.

- Tiempo de retardo pre a post procesador (dt3):
Este es un retardo fijo que representa el enrutado del mensaje de la señal desde el preprocesador a la cola del post procesador adecuado después de que el preprocesador identifique que el mensaje no es para procesar en ese nodo particular. Esto es, el nodo es usado como STP (Signalling Transfer Point).
dt3 = 5 ms.

- Retardos de procesos especificados en los algoritmos de ejecución:
Forward handover:
PF[2] = 25 ms (acceso PRMA++)
PF[5] = 5 ms (acceso PRMA++)
PF[6] = 5 ms (creación portadores)
PF[9] = 50 ms (macrodiversidad)

Backward handover:
PB[2] = 25 ms (acceso PRMA++)
PB[4] = 25 ms (capacidad)
PB[6] = 5 ms (acceso PRMA++)
PB[7] = 5 ms (establecimiento de llamada, portadores)
PB[9] = 50 ms (macrodiversidad)

A1.1.3 Parámetros de la red de acceso

La red de acceso incluye funcionalidad localizada tanto en terminal móvil UMTS como en la estación base (BTS). Los retardos a tener en cuenta sobre el radioenlace son modelados de la siguiente forma:

1) Empaquetamiento y cola de mensajes en la estación base
2) Retardo de la comunicación en el enlace descendente
3) Procesado en el terminal UMTS
4) Retardo de la comunicación en el enlace ascendente
5) Desenpaquetamiento de los mensajes en la estación base

A1.1.4 Modelo de un enlace

El modelo de simulación de un enlace se reduce a considerar un retardo debido al tránsito (dT) que es fijo y que depende de:

- La longitud del mensaje UMTS (N bits)
- El ancho de banda del enlace de señalización (B bps)

Esto es, para el caso de un mensaje de 50 bytes en un enlace de señalización de 64 kbps, se tendrá un retardo de 6.25 ms.

A1.1.5 Parámetros de un enlace

Se consideran dos tipos de enlaces para la información de señalización:
- Enlace de de 64 Kbps.
- Enlace de 2Mbps.

Los enlaces de señalización entre nodos suelen ser de 64 Kbps, aunque podrían considerarse agrupaciones de canales (n * 64 Kbps) como los anteriores si fuera necesario.

Por otro lado, se asumen las siguientes suposiciones para los cálculos:

a) El retardo de propagación se considera despreciable frente al retardo de tránsito.
b) Se considera que no hay retransmisiones de los mensajes de señalización entre los nodos.

Otros parámetros relativos a la propagación en el radioenlace tomados en cálculos son los siguientes:

Pot_max = 30; (dBm por canal máximo)
Ermin = -97; (RSSI min en dBm)

Nivel_per = 120; (Nivel de disparo de pérdidas)
Hist = 5; (Histéresis de pérdidas)
HA = 15; (HO_margin o margen de handover)
CImin = 18; (Relación señal a ruido, C/I mínima)

A1.1.6 Longitudes de claves y certificados tomados en los cálculos realizados

Para el cálculo de los retardos ocasionados en el sistema, se han utilizado claves públicas de 768 bits, siendo las firmas digitales de longitud similar. Las longitudes de los parámetros temporales (p.e. timestamps) son de 16 bits y las identidades de 64 bits.

Una de las causas importantes de los retardos está en la misma longitud de los certificados, debido a que el bit-rate en el radioenlace suele ser lento en el caso de la señalización. Por tanto, uno de los mayores esfuerzos en su optimización pasa por reducir la longitud de las claves, podrían utilizarse claves de longitud menor (p.e. 256 ó 512 bits) pero reducen el nivel de seguridad del sistema. Otra solución pasa por el empleo de curvas elipticas, con longitudes de clave pública de 256 bits.

A1.2 Modelos utilizados para la obtención de las probabilidades de bloqueo en las celdas

Para obtener las expresiones cerradas que permiten modelar las probabilidades de bloqueo para el establecimiento de llamada y de handover se utilizan cadenas de Markov. En este caso, se va a mostrar a modo de ejemplo, el caso de una celda con prioridad (apartado 5.11.3), es decir, con canales de reserva diferenciados para el tratamiento de peticiones de establecimiento de llamadas y handover.

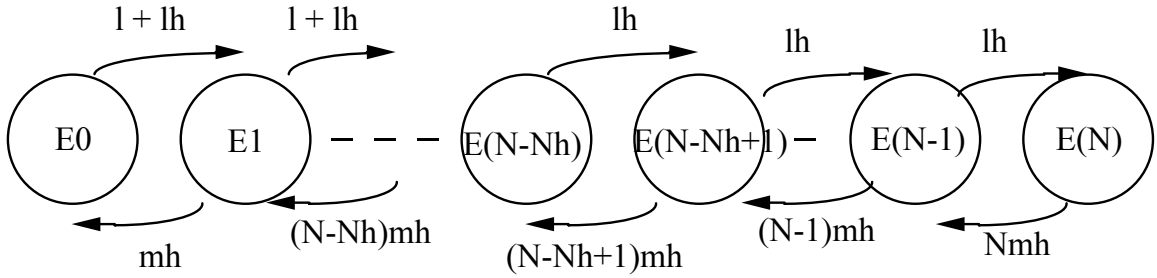


Fig. A1.3 Esquema de la cadena de Markov utilizada para el caso de celda con canales de reserva.

Sean:
l: Tasa de peticiones de establecimientos de llamada
lh: Tasa de peticiones de handover
N: Número de canales totales
Nh: Número de canales de handover.

mh: Inverso del tiempo de mantenimiento del canal (considerado igual para establecimientos de llamada y handover).

$$Pj = \begin{cases} \frac{l + lh}{mh} P_{j-1} \\ \frac{lh}{mh} P_{j-1} \end{cases}$$ para j = 1, 2, , N - Nh en el primer caso y j = N - Nh + 1, ... , N. para el segundo caso.

Se obtiene de esta forma:

$$Pj = \begin{cases} \frac{(1 + lh)^{j}}{j!\,(mh)^{j}} P_0 \\ \frac{(1 + lh)^{N-Nh} (lh)^{j-(N-Nh)}}{j!\,(mh)^{j}} P_0 \end{cases}$$ para j = 1, 2, , N - Nh en el primer caso y j = N - Nh + 1, ... , N. para el segundo caso.

Siendo:

$$TOMha = \frac{lh}{mh} \text{ y } TOMll = \frac{l}{mh}$$

$$P_0 = \left[\sum_{n=0}^{N-Nh-1} \frac{(TOMll + TOMha)^{n}}{n!} + (TOMll + TOMha)^{N-Nh} \sum_{n=N-Nh}^{N} \frac{(TOMha)^{n-N+Nh}}{n!} \right]^{-1}$$

Se obtiene finalmente:

$$BMll = \sum_{j=N-Nh}^{N} P_j \text{ con } BMha = P_c$$

Probabilidad de Bloqueo en el establecimiento de llamada:

$$BMll = \left(\frac{(TOMll + TOMha)^{N-Nh} * (TOMha)^{Nh}}{N!} \right) * P_0$$

Probabilidad de Bloqueo en el handover:

$$BMha = \left((TOMll + TOMha)^{N-Nh} \sum_{n=N-Nh}^{N} \frac{(TOMha)^{n-N+Nh}}{n!} \right) * P_0$$

A1.3 Modelos utilizados para la simulación del tráfico en las celdas

Para la simulación de los distintos tipos de celdas definidos en el apartado 5.11 se ha utilizado un programa simulador denominado SES. Con la ayuda de este simulador se han podido realizar diversas comparaciones con los resultados obtenidos mediante modelos.

En las hojas adjuntas, a modo de ejemplo, se muestra el esquema del diseño utilizado para la simulación de los sistemas correspondientes a los apartados:

Celdas con cola de handover (5.11.2): simple1
Celdas con cola y con prioridad (5.11.4): Colasres

El intervalo de confianza y el nivel de confianza alcanzados en los resultados dependen en cada caso del objetivo que se persigue con cada simulación en concreto. Sin embargo, de modo orientativo, para un nivel de confianza del 90 por 100 se obtienen intervalos de confianza con $p = 0,7$ de $0,7 - 0,069 \leq p \leq 0,7 + 0,069$.

A1.4 Referencias

[BG1] Brian G. Marchent, Phil T. Wright. *Simulation of signalling in ATM networks for 3rd generation mobile systems*. Roke Manor Reserch (documento interno). 1994

[BG2] Marchent Brian G. *Performance evaluation of network architectures and signalling procedures for integration of UMTS into BISDN IN.* p.377-381. Portugal, 1995.

[DM1] David McMillan. *Traffic modelling and analysis for cellular mobile networks.* p. 627-632. Teletraffic and Datatraffic ITC-13. 1991.

[JD1] Johan Dahlström, Jonas Ericsson, Damian Lawniczak. *Evaluation of directory node architectures for the DDB network in UMTS.* p. 459-461. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[PW1] P. T. Wright, B. G. Marchent. *Simulation of the UMTS core network.* p. 435-440. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[RACE15] RACE 2066/RMR/NESSY1/DS/P/066/b1, Performance evaluation of the mobile network and load figures for the BSS/FN. Dic. 1994.

[RACE17] RACE 2066/ERA/NESSY2/DS/P/050/b1. First results on evaluation of network architectures and mobility.

[RACE18] RACE 2066/RMR/NESSY2/DS/P/051/b1. First results on evaluation of roaming and interconnection concepts.

[RACE19] RACE 2066/ERA/NESSY2/DS/P/075/b1, Evaluation of network architectures and UMTS procedures. Dic. 1994.

[RACE20] RACE 2066/SEL/NESSY3/084, Simulation results. Dic. 1994.

[RACE22] RACE 2066/SESA/GA2/DS/P/054/b1, Signalling traffic requirements for UMTS. 1993.

[SES1] SES/Workbench. Introductory trainning course. 1992.

[SES2] SES/Workbench. User´s manual. 1992.

[SES3] SES/Workbench. Reference manual. 1992.

Anexo 2

Estructuras de canales de control para sistemas de la tercera generación

En este anexo se describen los diversos tipos de canales de control utilizados en GSM y que se diseñan para sistemas como UMTS. En primer lugar, se requiere de una clasificación de los canales lógicos:

Canales de acceso común:
- BCCH (Broadcast Control Channel)
- CCCH (Common Control Channel)
    - PCH (Paging channel)
    - RACH (Random Access Control Channel)
    - AGCH (Access Grant Control Channel)

Canales asociados:
- ACCH (Associated Control Channels)
- LCCH (Leash Control Channel)

Canales dedicados:
- DCCH (Dedicated Control Channel)
- TCH (Traffic Channel)

A continuación, se relacionan diversos grupos funcionales con canales de control y señalización.

- Controlador de enlace
    ACCH: Control de potencia adaptativo y adaptación al transporte.
    LCCH: Avance del tiempo y mediciones en celdas adyacentes.

- Controlador de enrutado
    LCCH: Establecimiento de portadores no urgente
    DCCH: Ejecución del handover
    CCCH: Establecimiento de portadores
    BCCH: 'status' de celda

- Asignador de recursos
    ACCH: Cambio de ancho de banda
    LCCH: Acceso
    CCCH: Acceso y derechos de acceso
    BCCH: Estructura de trama

- Controlador de tráfico
    DCCH: Señalización de establecimiento de llamada
    CCCH: Acceso inicial

- Plano de transporte
    BCCH: Sincronización

En el caso relativo al handover, se hace referencia al canal DCCH. El DCCH soporta principalmente transmisión de señalización para establecimiento de llamada, ejecución de backward o forward handover y renovación de localización. Esta transmisión de señalización requiere alta fiabilidad y que sea rápida. Los DCCH son básicamente bidireccionales y están soportados por un par de canales físicos (un canal físico se define como un sólo slot por trama TDMA).

El LCCH es un canal de control permanente para gestión de conexiones. El LCCH existe tan pronto como la conexión de radio es establecida entre un terminal móvil y una estación base.

A2.1 Canales para el handover en GSM

A modo de comparación, en GSM se utiliza el canal SACCH para el envio hacia la BTS de mediciones del radioenlace efectuadas por el terminal móvil. Se trata de un flujo de

950 bps que se envía en la trama 13 cada 120 ms. Los intervalos de la multitrama SACCH son de 480 ms que teniendo en cuenta un promediado de 32 muestras obtienen valores aproximadamente cada 15 s. Como se puede ver, es extremadamente lento para los requerimientos de redes como UMTS.

Existe un canal de broadcast BCCH, que envia información de gestión y parámetros de mediciones entre la estación base al terminal móvil con una duración de multitrama de 235 ms (51 tramas * 4,615 ms por trama).

Para la ejecución del handover se utiliza el canal FACCH que puede enviar información de hasta 22,8 Kbps cada 57 ms entre el terminal móvil y la estación base.

A2.2 Referencias

[LH1] L. Hanzo, R. Steele. *The Pan-European mobile radio system.* Part I y II. BT. Marzo-Abril 1994.
[XL1] X. Lagrange, P. Godlewski. *Control channel structures in a third generation ATDMA system.* p. 190-192. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

Anexo 3

Control de acceso PRMA++

El mecanismo de control de acceso considerado aquí es un desarrollo del PRMA conocido como PRMA++. El PRMA++ es utilizado ampliamente en simulaciones por el proyecto ATDMA así como otros grupos de diseñadores de sistemas de comunicaciones móviles avanzados. Constituye un punto de referencia válido para el diseño de protocolo handover tanto a nivel de retardos como para otros tipos de prestaciones.

Cada terminal móvil con reserva tiene uso exclusivo de un slot en cada trama, los terminales con reserva comparten el canal como en TDMA. Con terminales accediendo autónomamente al canal, el PRMA opera con detectores de actividad de voz. Un detector de actividad de voz clasifica una señal de audio en cada instante como 'hablando' y 'silencio' de forma que el detector genera ráfagas de paquetes correspondientes a los intervalos de voz.

Al comienzo de un intervalo de voz ('talkspurt'), un terminal móvil intentará el acceso al primer slot R en la actual trama de transmisión. Si no es satisfactoria entonces el móvil retransmitirá con una probabilidad de retransmisión en el próximo slot R disponible hasta que el acceso es válido o el paquete rebasa el período máximo de retardo y es descartado. El anterior proceso se repite para cada paquete que esté preparado para transmisión. Es de notar que una vez que el móvil ha tenido acceso satisfactorio al slot R y ha sido informado de una asignación de slot via el slot par A, lo antes que el móvil puede usar ese slot es en la próxima trama de transmisión. Ya que esto ocurre 5 ms más tarde, se deduce que si el acceso satisfactorio a un slot R no se produce en 5 ms, entonces no es posible para ese paquete ser transmitido dentro del nivel de retardo de 10 ms, pudiendo descartarse.

Para una carga de tráfico [JD1] dada, hay un valor óptimo para el número de slots R en la trama TDMA, para el tiempo establecido de retransmisión. Para R = 16 slots por trama y asumiendo que un retardo de 20 ms es aceptable, entonces podrían soportarse 128 slots, con una ganancia de 1,78 sobre el caso de conmutación de circuitos. Sin embargo, a este retardo de acceso evaluado sería añadido el tiempo de sincronización (menor de 0,2 ms) y un período de trama adicional (unos 5 ms). Esto es porque una importante diferencia entre el PRMA++ y el convencional PRMA, es que el vehículo para realizar el proceso de contención de acceso, la ráfaga ACI, no contiene una trama de codificación de audio, así que no es hasta que el canal físico ha sido reservado, que la trama de voz puede ser enviada.

A3.1 Referencias

[DG3] D. J. Goodman, R. A. Valenzuela, K. T. Gayliard and B. Ramamurthi. *Packet reservation multiple access for local wireless communications.* p. 885-890. IEEE transactions on communications. Agosto 1989.

[DG4] Wai-Choong Wong and David J. Goodman. *Integrated data and speech transmission using packet reservation multiple access.* p. 172-176. ICC'93 Geneve. 1993.

[DR1] D. Robertson, P. Cosimini and J. Dunlop. *Use of a simulator to optimise the performance of the ATDMA packet access mechanism.* p. 80-84. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

[JD1] Jonathan DeVile. *A reservation multiple access scheme for an adaptive TDMA air interface.* p. 217-225. WINLAB Workshop on Third Generation Wireless Information Networks. New Jersey, 1993.

[SL1] Simon S. Lam. *Packet broadcast networks. A performance analysis of the R-ALOHA protocol.* p. 596-603. IEEE Transactions on computers. Julio 1980.

[SN2] Sanjiv Nanda. *Analysis of packet reservation multiple access: voice data integration for wireless networks.* p. 1984-1988. IEEE 1990.

[ST1] Shuji Tasaka. *Stability and performance of the R-ALOHA packet broadcast system.* p. 717-726. IEEE Transactions on computers. Agosto 1983.

[VC1] V. Casares, J. Paradells. *Variable voice service rate in wireless access packet networks.* p. 609-623. Wireless '93.

Anexo 4

Estadística de handovers y establecimientos de llamada realizados en un entorno real

A continuación, se especifican las tasas de generación de llamadas y handover encontradas experimentalmente para evaluar los resultados acerca de la idoneidad de los procedimientos descritos basados en el handover.

A4.1 Tasas de establecimiento de llamada

Tasas de generación de llamadas expresadas en forma de tablas correspondientes a entornos de Randstad (Holanda).

Area geográfica	**Coche**	**Transporte público**	**Peatón**	**Inmóviles**
Centro ciudad	0.102	0.067	0.050	-
Urbano	0.102	0.067	0.050	-
Suburbano	0.068	0.050	0.033	-
Rural	0.067	0.033	0.033	-
Alto tráfico	-	-	0.050	-
Autopista	0.066	0.033	-	-
CPN móvil	-	0.033	-	-
CPN negocios	-	-	-	0.229
Doméstico	-	-	-	0.167

Tabla A4.1 Requerimientos de tráfico de diferentes clases de usuario (Tráfico ofrecido/área/usuario).

Area geográfica	**Coche**	**Transporte público**	**Peatón**	**Inmóviles**
Centro ciudad	3.48	2.00	1.50	-
Urbano	3.48	2.00	1.50	-
Suburbano	2.34	1.50	1.00	-
Rural	2.26	1.00	1.00	-
Alto tráfico	-	-	1.50	-
Autopista	2.26	1.00	-	-
CPN móvil	-	1.00	-	-
CPN negocios	-	-	-	8.03
Doméstico	-	-	-	3.80

Tabla A4.2 Número medio de llamadas por usuario durante la hora cargada.

Area Geográfica	**Usuarios**	**Radio celda**	**Penetración**	**Tráfico ofr./Km2**	**Area cobertura**	**Radio (Kms)**
Centro ciudad	coches/publico	Macro	25%	26.0	1.9	0.8
Urbano	coches/publico/tran.	Macro	25%	10.7	4.7	1.2
Suburbano	coches/publico/tran.	Macro	25%	2.1	24.3	2.8
Rural	coches/publico/tran.	Macro	25%	0.5	110.3	5.9

Tabla A4.3. Area de cobertura media y radio de las macroceldas.

Estas tablas proporcionan información relativa al tráfico ofrecido esperado en los diferentes tipos de celdas y por kilómetro cuadrado, lo cual es decisivo para tener una referencia de las capacidades en canales de las celdas a través de sus probabilidades de bloqueo.

Asimismo, se proporciona información relativa al porcentaje de terminales móviles que son estáticos y los que pueden admitir una cierta movilidad, lo cual es importante de cara al modelado de los handover.

A4.2 Tasas de handover

Se van a suponer tres tipos de handover; según sean entre celdas dentro un mismo dominio de seguridad, entre dominios de seguridad diferentes o bien entre redes distintas

Caso de un area de intercambio local (mismo dominio de seguridad)
Suponer que un móvil que está con una llamada desde un área de intercambio local a otra área, comportando en ciertos casos un cambio de entorno administrativo. Se han estudiado diversos casos referidos a Londres y al flujo de pasajeros en una determinada área de dominio local.

La situación de handover entre picoceldas y microceldas para usuarios entrantes y salientes en entornos densos como las estaciones de metro en horas punta en el área del centro de Londres ha constituido uno de los casos restricciones más severas por la gran densidad de comunicaciones y señalización. En la figura se muestra un esquema.

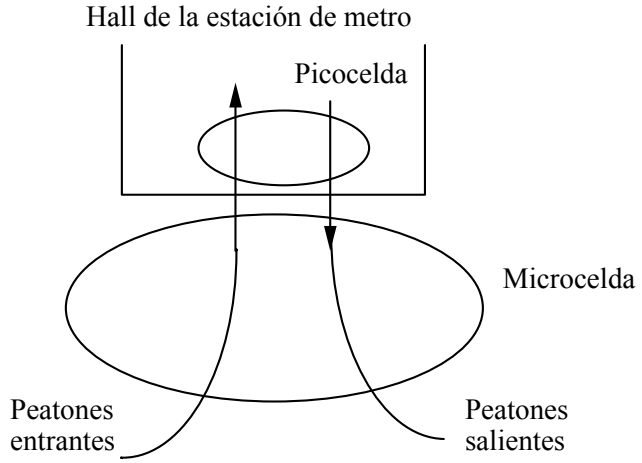


Fig. A4.1 Flujos de usuarios en el intercambio de celdas dentro de una misma red.

Abajo se estudia una fórmula para el cálculo de la tasa de handovers en un área de intercambio local.

$peaton_{in}$	Número de peatones entrando al área.
$peaton_{out}$	Número de peatones saliendo del área.
$pmetro_{in}$	Número de pasajeros entrando al área desde el metro.
$pmetro_{out}$	Número de pasajeros saliendo del área desde el metro.
$ptren_{in}$	Número de pasajeros entrando al área desde el tren.
$ptren_{out}$	Número de pasajeros saliendo del área desde el tren.
$pbus_{in}$	Número de pasajeros entrando al área por bus.
$pbus_{out}$	Número de pasajeros saliendo del área por bus.

$pcoche_{in}$	Número de pasajeros entrando al área con el coche.
$pcoche_{out}$	Número de pasajeros saliendo del área con el coche.
$pBCPN_{out}$	Número de pasajeros saliendo del área pública UMTS a la BCPN.
$pllamada_{peaton}$	Probabilidad de que un peatón esté en una llamada.
$pllamada_{foco}$	Prob. de que un peatón de un foco de llamadas esté con una llamada.
$pllamada_{bus}$	Probabilidad de que un pasajero de bus esté en una llamada.
$pllamada_{coche}$	Prob. de que un pasajero o conductor de coche esté en una llamada.
penetr	Penetración de terminales UMTS.
penetrw	Penetración de terminales UMTS de gente trabajando.

$$LE_{handovers} = penetr(pllamada_{peaton}(peaton_{in} + peaton_{out}) + pllamada_{foco}(pmetro_{in} + pmetro_{out} + ptren_{in} + ptren_{out}) + pllamada_{bus}(pbus_{in} + pbus_{out}) + pllamada_{coche}(pcoche_{in} + pcoche_{out})) + penetrw pllamada_{foco} pBCPN_{out}$$

Los valores de penetración así como los parámetros de probabilidad de una llamada se presentan en la siguiente tabla:

penetr	0,5
penetrw	0,7
$pllamada_{peaton}$	0,05
$pllamada_{foco}$	0,05
$pllamada_{bus}$	0,07
$pllamada_{coche}$	0,1

A modo de orientación, se han obtenido para microceldas de alta densidad (focos) (p. e. enfrente de estaciones de metro), unos rangos de 900 handovers/h a 1500 handovers/h. La mitad de estos handovers son handovers entre microceldas y picoceldas que requieren técnicas de handover muy avanzadas.

Estudio de los cambios de red producidos en Londres:

Sea el caso de determinar el número de handovers ente dos redes distintas. Se utiliza la siguiente notación.

ptrin: Número de desplazamientos en transporte público debidos al trabajo durante la hora punta dirigidos a un área.

ptrout: Número de desplazamientos en transporte público debidos al trabajo durante la hora punta saliendo de un área.

ptrdentro: Número de desplazamientos en transporte público debidos al trabajo durante la hora punta dentro un área.

ppunta: Porción de desplazamientos por trabajo durante la hora punta dentro un área.

pinpunta: Porción de desplazamientos por trabajo dirigidos a un área durante la hora punta.

poutpunta: Porción de desplazamientos por trabajo de salida de un área durante la hora punta.

pdentromcpn: Porción de desplazamientos en transporte público realizados en metro o tren con respecto al tráfico total dentro del área considerada.

trcochein: Número de personas haciendo un desplazamiento en coche debido al trabajo dirigidas a un área durante el dia.

trcocheout: Número de personas haciendo un desplazamiento en coche debido al trabajo saliendo de un área durante el dia.

trcochedentro: Número de personas haciendo un desplazamiento en coche debido al trabajo dentro un área durante el dia.

despin: Número de desplazamientos dirigidos al área durante la hora punta.

despout: Número de desplazamientos saliendo del área durante la hora punta.

pdesp: Porción de viajes de trabajo de todos los viajes durante la hora cargada.

Los correspondientes parámetros **trcicloin, trcicloout, trciclodentro, trpeatin, trpeatout, trpeatdentro** para bicicletas y peatones en desplazamientos de trabajo se definen de forma análoga.

En los desplazamientos en MCPN se desprecian los efectos de cambios en los vehiculos y se asume que el desplazamiento entero es realizado por un único MCPN. En el caso de un viaje en mcpn ocurren tres cambios de red:

(1) Accediendo al vehiculo: Cambio de red desde UMTS pública a mcpn.

(2) Saliendo del vehiculo: Cambio de red desde mcpn a UMTS pública.

(3) Entrando a la oficina: Cambio de red desde UMTS pública a BCPN.

Número de cambios de red/h por Km^2 =

ppunta ((2*pdentromcpn + 1) ptrdentro + trcochedentro + trciclodentro + trpeatdentro) + 2*pinpunta (ptrin + trcochein + trpeatin + trcicloin) + poutpunta (ptrout + trcocheout + trpeatout + trcicloout) + (1 - pdesp)(despin + despout).

Para la ciudad de Helsinki (area sur) el valor de números de cambios entre redes/h por Km^2 es de 8250.

Tipos de vehiculos en desplazamientos para compras en el área del Gran Londres:

Coche: 30%
Autobus: 15%
A pie : 50%
Otros: 5%

	Londres Central	**Londres interior**	**Londres exterior**
ppunta	0.25	0.25	0.25
pinpunta	0.30	0.25	0.25
poutpunta	0.06	0.25	0.25
pdentromcpn	0.44	0.27	0.21
ptrdentro	18.000	213.000	337.000
trcochedentro	8.000	233.000	1.147.000
trciclodentro	3.000	34.000	146.000
trpeatdentro	31.000	230.000	434.000
ptrin	454.000	264.000	315.000
ptrout	403.000	284.000	346.000
trcochein	109.000	216.000	200.000
trcocheout	95.000	206.000	223.000
trcicloin	25.000	27.000	21.000
trcicloout	23.000	30.000	20.000
trpeatin	13.000	20.000	10.000
trpeatout	12.000	21.000	10.000
despin	446.341	321.341	332.927
despout	78.000	329.878	365.244
pdesp	0.4	0.4	0.4
area (Km^2)	28.6	299.9	1849.6
Cambios de red/h /Km^2	25.339	3.301	743

Tabla A4.4 Valores numéricos para los parámetros descritos en el caso de la zona del Gran Londres.

Otras mediciones de handovers realizadas

De [RACE22] se obtienen datos acerca del número de handovers en macroceldas debido a movimientos de usuarios entrantes y salientes en la hora punta según diferentes entornos.

Centro ciudad	400 a 500 handover/h
Urbano	500 handover/h
Suburbano	300 a 400 handover/h
Rural	300 handover/h.

El hecho que la tasa de handover de las macroceldas en el centro de la ciudad sea más baja que en el entorno urbano se explica por el hecho de que los peatones son servidos por microceldas en el centro de la ciudad. La tasa de peatones entrando o saliendo de microceldas durante la hora punta se estima en 130 handover/h.

De la ciudad de Amsterdam [JN1] se han obtenido las siguientes tasas de handover (miles/h) para los diferentes entornos de operación:

Entorno	**Tamaño (Km)**	**Total**	**Entre dominios**	**Entre celdas**	**Intra CSS (9)**	**Intra CSS (3)**
Foco de alta densidad	0.12	39.0	13.0	36.0	16.0	2.6
Negocios	0.05	10.1	2.6	7.5	3.2	0.53
Doméstico	0.25	2.3	0.6	1.7	0.72	0.12
Autopista	3	88.6	4.6	84.0	37.0	9.4

Nota: El número de CSS's por LE es de 3 y 9.

Tabla A4.5 Tasas de handover registradas en Amsterdam entre diferentes tipos de entornos

En la última tabla, se observa una gran tasa de handovers en pequeños focos de alta densidad y en carreteras en donde hay mayoritariamente IntraLE handovers. Ambos entornos sugieren una descentralización de las funciones de control de movilidad a las BSCs para una mejora de las prestaciones. Los demás casos no presentan restricciones importantes de funcionamiento.

Medición del número de handovers, obtenidas en el área de Randstad (Holanda):

	Nº medio de coches salientes	**Nº medio de coches entrantes**	**Nº medio de transp. públ. entr.**	**Nº medio de transp. públ. sal.**	**Nº medio de peatones entrantes**

Centro ciudad	6.925	5.871	5.513	5.068	10.438
Urbano	5.448	5.520	3.083	3.096	6.046
Suburbano	5.370	5.550	2.803	2.883	3.181
Rural	3.613	3.776	1.429	1.487	987

Tabla A4.6 Tasas de coches y transportes públicos entrantes y salientes durante la hora cargada.

	Area cubierta (Km2)	**Pasajeros coche/Km2**	**Pasajeros transporte publico/Km2**	**Peatones/Km2**
Centro ciudad	29	743	429	37.000
Urbano	56	261	104	190
Suburbano	227	79	28	45
Rural	1105	21	5	7
Area total	1406	54	22	35

Tabla A4.7 Densidad de usuarios potenciales.

Area geogr.	**Entradas coche**	**Salidas coche**	**Velocidad coche (Km/h)**	**Entradas transporte público**	**Salidas transp. público**	**Velocidad transporte público (Km/h)**
Centro ciudad	723	1.919	10	375	944	10
Urbano	1.345	1.365	20	563	533	20
Sub-urbano	1.461	1.197	40	507	388	40
Rural	659	570	70	146	115	70

Tabla A4.8 Entradas, salidas y velocidad media de los pasajeros para coche y transporte público.

A4.3 Referencias

[JN1] J.A.M. Nijholf, I.S.Dewantara, R. Prasad, A.J.M. Roovers. *Base station system configurations for third generation mobile telecommunication systems.* 43rd VTC, p.621-624. 1993.

[RACE22] RACE 2066/SESA/GA2/DS/P/054/b1, Signalling traffic requirements for UMTS. 1993.

[RACE23] RACE 2066/NOKIA/GA2/141. The work load case study of the London area. 1994.

[SG1] Seppo Granlund. *Two examples on how to analyse signalling load of UMTS network by using real measurements.* p. 425-429. RACE Mobile Telecommunications workshop. Amsterdam. 1994.

Anexo 5

Operaciones con bases de datos distribuidas en UMTS

En este anexo se describen los protocolos utilizados en la red fija por UMTS y X.500, también se introducen aspectos relacionados con la secuencia que se sigue en la invocación de peticiones para la búsqueda de información en la jerarquia distribuida de bases de datos definida en UMTS. De forma alternativa, en X.500 se siguen procesos similares que se describen con más detalle en [ITUT]. Además en el capitulo 1 se realiza un análisis comparativo.

A5.1 Protocolos de directorios

En este apartado se plantean los mecanismos de protocolos de directorios en X500. En este caso, X.500 define el Directory Access Protocol (DAP) y el Directory System Protocol (DSP) como protocolos que soportan todos los servicios de directorio, excepto la réplica que se regula por el Directory Operational binding management Protocol (DOP) y el Directory Information Shadowing Protocol (DISP). Posteriormente, se planteará una valoración comparativa.

Directory Access Protocol (DAP)

Es la situación de un DUA estando en un sistema abierto diferente del DSA con el cual está interactuando, en este caso, las interacciones son soportadas por el DAP. El DAP proporciona el acceso al directorio para obtener y modificar información de directorio. Por otra parte, utilizando operaciones remotas con ROSE, el DSA no puede invocar operaciones con el DUA. Las operaciones con ASEs permitidas con el DAP son las siguientes:

- SearchASE:
  List : Obtiene los nombres de un grupo de entradas.
  Search: Busca por entradas satisfaciendo algunos criterios y devuelve los nombres y alguna o toda la información contenida en esas entradas.
- ModifyASE:
  RemoveEntry: Borra una entrada del Directorio.
  AddEntry: Añade una entrada conteniendo información acerca un objeto al Directorio.
  ModifyDN: Modifica una entrada de RDN o mueve una entrada a una nueva superior en el DIT.
  ModifyEntry: Modifica la información contenida en una entrada.
- ReadASE:
  Read: Devuelve alguna o toda la información contenida en una entrada a Directorio.
  Abandon: Abandona el procesado de cualquiera de los servicios anteriores.
  Compare: Determina si una entrada contiene una pieza particular de información.

DAP también proporciona operaciones extra con el directorio para establecer y liberar (DirectoryBind, DirectoryUnBind) asociaciones entre DUAs y DSAs.

Directory System Protocol (DSP)

En el caso de un par de DSAs interaccionan entre ellos y están en diferentes sistemas abiertos, estas interacciones son soportadas por DSP. El DSP proporciona el 'chaining' de peticiones para obtener o modificar información de directorio en otras partes del directorio distribuido. También utiliza operaciones remotas mediante ROSE , p.e. el DSA que responde puede invocar operaciones en el DSA inicial y viceversa. El protocolo DSP soporta el siguiente conjunto de operaciones:

- ChainedSearchASE:
  ChainedList
  ChainedSearch
- ChainedModifyASE:
  ChainedRemoveEntry
  ChainedAddEntry
  ChainedModifyDN
  ChainedModifyEntry
- ChainedReadASE:
  ChainedRead
  ChainedAbandon
  ChainedCompare

Obsérvese que consisten básicamente en proporcionar mecanismos de 'chaining' al protocolo DAP.

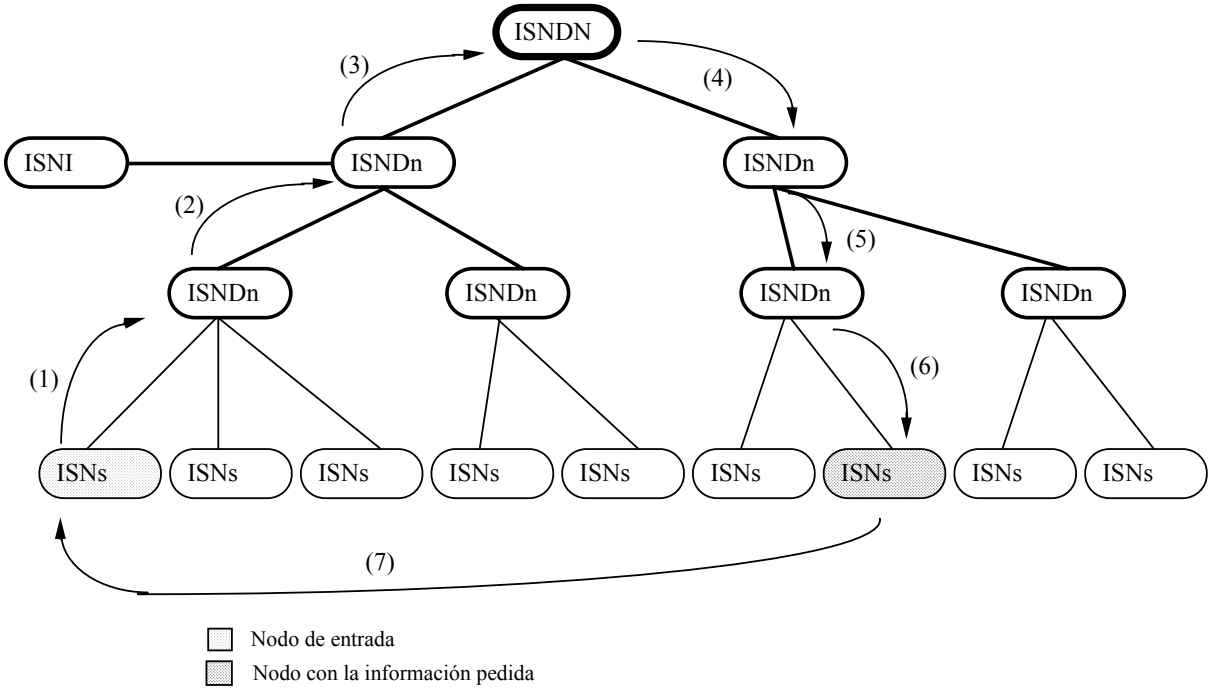


Fig. A5.1 Mecanismo de passing, utilizado en UMTS.

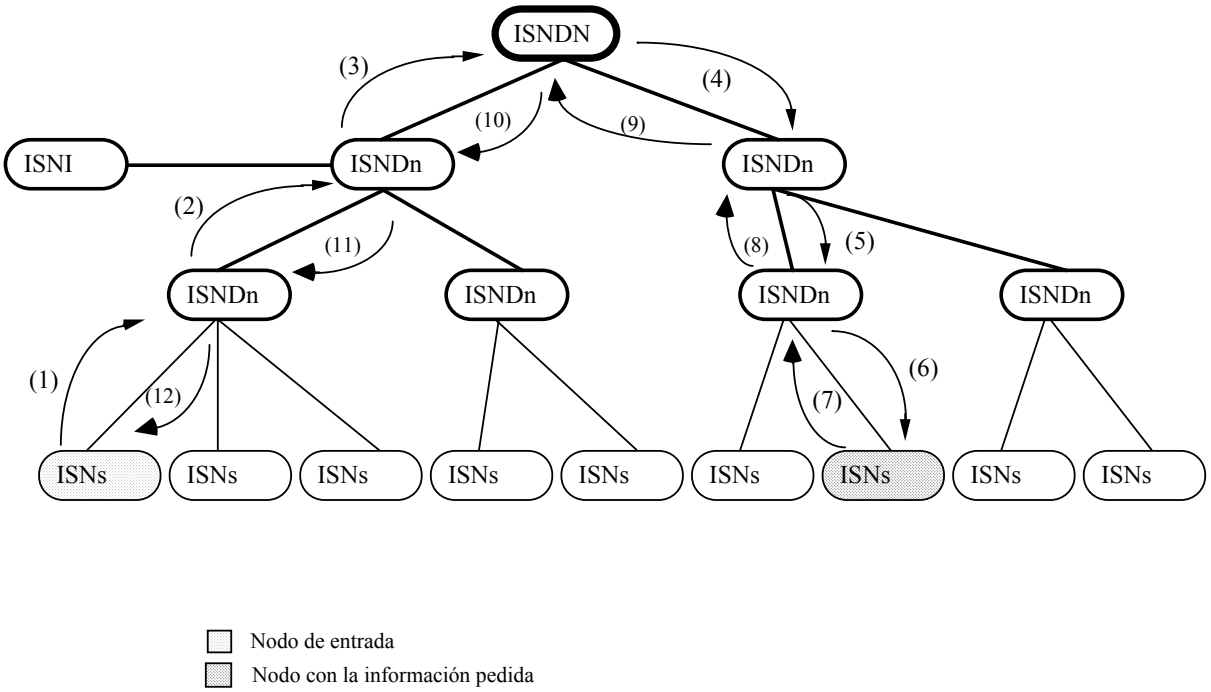


Fig. A5.2 Búsqueda de información mediante la técnica chaining.

Comparación de protocolos de acceso DAP y UMTS

En general, el protocolo DAP proporciona funcionalidades equivalentes para ambos sistemas, X.500 y UMTS, como son operaciones de acceso y operaciones de gestión adicionales. Incluso DAP puede soportar las operaciones UMTS potenciales (p.e. compare, list, search,...).

Por otra parte, se puede decir que hay un gran número de argumentos asociados con cada operación permitiendo al usuario tener un alto grado de control sobre los mecanismos de cuestión (query) dentro de la DDB. A continuación, se comparan las operaciones proporcionadas por UMTS y DAP.

Operaciones UMTS	*Operaciones DAP*
Operaciones de acceso:	
Retrieve	Read
Update	ModifyEntry
Modify	ModifyDN
Operaciones de gestión adicionales:	
Create	AddEntry
Delete	RemoveEntry
Operaciones potenciales:	
List	List
Compare	Compare
Abandon	Abandon
Search	Search

Uno de los inconvenientes importantes del protocolo DAP es que no es usado por los sistemas de redes inteligentes actuales. Por otra parte, en las operaciones maneja muchos parámetros que son innecesarios y que contribuyen a incrementar la carga de señalización y procesado.

A pesar de que el protocolo DAP permite todas las posibles operaciones UMTS, no provee la eficiencia y simplicidad requerida por UMTS. Sin embargo, como se verá más adelante, en el aspecto de seguridad sí que proporciona un marco de trabajo idóneo para desarrollar una arquitectura de seguridad en UMTS.

A5.2 Mecanismos de cuestiones (queries) de directorio en X.500

En principio, un DUA sólo necesita tener acceso a un DSA para tener conocimiento de los servicios de directorio. El Directorio proporciona dos mecanismos para gestionar las peticiones entre DUAs y DSAs, éstas son: chaining y multicasting. Ámbos son asumibles por la arquitectura UMTS.

Réplicas (Replication)

En UMTS existe un mecanismo de réplicas que permite transferir la información de una base de datos a otra. En el caso de renovación de áreas de localización (location updating), este mecanismo se cubre de forma parecida por X.525.

El estándar X.525 define un mecanismo conocido como réplica que permite el "shadowing' (copia y mantenimiento) de información entre un DSA y otro. La réplica requiere un acuerdo entre un 'shadow supplier' DSA (fuente de información) y un 'shadow consumer' (recipiente de la información). Este acuerdo se establece usando el Directory Operational binding management Protocol (DOP).

La información se transmite usando las operaciones 'shadow' del directorio según un Directory Information Shadowing Protocol (DISP). En general, se contemplan dos formas de renovación de la información, renovación total o bien renovación 'incremental' en la que sólo son transmitidos cambios en la información 'shadowed'.

A5.3 Propagación descendente de las cuestiones (queries)

Se estudian los casos de peticiones que son presentadas a una ISN y de como esta ISN conoce que otra ISN_S más abajo en la jerarquía tiene la información demandada.

Buscando datos
Para la localización de información relativa al handover en el cambio de operador de red así como información que pueda ser sensible a la seguridad y/o gestión del sistema se pueden definir diversas estrategias para localizar los datos de los usuarios (sin obtenerlos): R, V y RV [RACE13].

En general la búsqueda de información será diferente según el origen de la petición. En el caso de una petición con origen en otra red, la cuestión irá dirigida a un nodo ISN_{DN} que a continuación distribuirá la petición hacia abajo a otros nodos directorios. En el caso de una cuestión originada en la propia red, la propagación empezará a un nivel más bajo en la jerarquía, p.e. ISN_{Dn}.

Moviendo datos
Los diferentes procedimientos de movilidad de usuarios permiten definir diferentes técnicas de mover datos. Es el caso de cuando la información de usuario (p.e. perfil de usuario) tiene que ser relevada de un nodo a otro, que puede renovarse el puntero del nodo directorio correspondiente ISN_{Dn} o bien, borrar y crear nuevos punteros en los nuevos dominios.

Datos internos requeridos por ISN_S

Para que la estructura de DDB UMTS sea eficiente, cada nodo de la jerarquía de directorios ha de tener conocimiento de los nodos a los que está conectado, creando una estructura de caminos de 'padres a hijos', así como una lista de entidades de confianza para posteriores intercambios de claves o gestión de servicios de seguridad.

A5.4 Propagación ascendente de las cuestiones (queries)

En principio, el ISN_{DN} mantiene la información de todos los ISN_S de la red. Si la petición es externa a la red, ha de pasar primero por un nodo ISN_I y luego ser redireccionada a un nodo ISN_{DN} interno.

Si es una petición interna, procederá de una entidad SCF hacia una base de datos directorio ISN_{Dn} , que a su vez le indicará la ISN_S pertinente.

A5.5 Técnicas de petición internas

En este apartado se describen varias de las técnicas utilizadas en las peticiones internas.

Técnica chaining
En este caso, la cuestión fluye de nodo en nodo, manteniendo junto a su progresión la información del nodo previamente cruzado. Esta técnica es particularmente util en estructuras jerárquicas, ya que los caminos entre los nodos están perfectamente definidos.

Técnica referral
En esta técnica, la cuestión va de un nodo al próximo y entonces retorna al primero, que escoge el próximo nodo según el último puntero recibido. Así que la cuestión es centralizada y controlada por el nodo inicial todo el tiempo hasta su finalización. Eso hace la técnica muy segura.

Técnica multicasting
Para resolver los problemas de velocidad de la técnica anterior, se utiliza esta otra técnica de multicasting en la cual, la cuestión se envia simultáneamente a varios nodos que devuelven sus respuestas. El problema en este caso, es la gran cantidad de señalización empleada, si bien es muy util cuando el nodo demandante no tiene idea de donde obtener la información solicitada.

Técnica passing
Esta técnica es particularmente útil en UMTS requiriéndose un protocolo especial para ella. El método es bastante similar a la técnica chaining sólo que las respuestas son manipuladas

de manera diferente. Si la información no se encuentra en un determinado nodo, la petición interna se pasa al próximo nodo en la DDB. Cuando se localiza la información, los resultados se pasan directamente al nodo inicial. No se requieren respuestas parciales entre nodos. Podrían existir problemas en el caso de la pérdida de información en la cuestión, requiriéndose "timeouts" especiales y/o otras medidas.

X.509 no soporta esta técnica, desde un punto de vista de seguridad, únicamente es factible la comunicación en un sentido, al igual que el intercambio de certificados o la autentificación.

Operaciones internas con respuestas parciales

El conjunto de operaciones internas asociadas a una petición externa (en general, procedente de un ISN_I), puede ser ordenado o no. En un caso, se denomina metodo 'restart' en donde se utiliza una técnica passing una y otra vez (restarting) al nodo inicial para obtener la información solicitada.

En otros casos, se utilizan métodos parcialmente continuos donde después de aplicar la técnica passing, se envia una respuesta parcial al nodo inicial originante y no hay un reinicio de la petición sino que el último nodo direccionado se encarga de redireccionar la próxima cuestión al nodo correspondiente.

En otros métodos, denominados continuos, la petición circula por los nodos (como en la técnica passing) aun a pesar de otener informaciones parciales en su recorrido.

A5.6 Referencias

[ITUT1] The Directory: Overview of concepts, Models and Services. X.500. 04-1992.
[ITUT2] The Directory: The Models. X.501. 04-1992.
[ITUT3] The Directory: Authentication Framework. X.509. 04-1992.
[ITUT4] The Directory: Abstract Service Definition. X.511. 04-1992.
[ITUT5] The Directory: Procedures for Distributed Operation. X.518. 05-1992.
[ITUT6] The Directory: Protocol Specifications. X.519. 05-1992.
[ITUT7] The Directory: Selected Attribute Types. X.520. 05-1992.
[ITUT8] The Directory: Selected Object Classes. X.521. 05-1992.
[ITUT9] The Directory: Replication. X.525. 05-1992.
[ITUT10] Directory Access Protocol: Protocol Implementation Conformance Statements PICS. X.581. 05-1992.
[ITUT11] Directory Systems Protocol: Protocol Implementation Conformance Statements PICS. X.582. 05-1992.

[RACE11] RACE 2066/PTTNL/MF1/DS/P/014/a1, Stage 2 (draft) specification of communications between databases. October 1992.
[RACE12] RACE 2066/PTTNL/MF1/DS/P/032/a1, UMTS Distributed Database functionalities. June 1993.
[RACE13] RACE 2066/PTTNL/MF1/DS/P/061/b1, Implementation aspects of the UMTS database. Dic. 1994.
[RACE26] RACE 2066/VTT/GA4/DS/P/044/b1, Relevance of other application parts. September 1993.