Movilidad IP.
Macromovilidad, micromovilidad, calidad de servicio y seguridad.*

Autores: Josep Mangues Bafalluy[1], Albert Cabellos Aparicio[2], René Serral Gracià[2], Jordi Domingo Pascual[2], Antonio Gómez Skarmeta[3], Tomás P. de Miguel[4], Marcelo Bagnulo[5], Alberto García Martínez[5]

[1] Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), [2] Universitat Politècnica de Catalunya (UPC), [3] Universidad de Murcia (UMU), [4] Universidad Politécnica de Madrid (UPM), [5] Universidad Carlos III de Madrid (UC3M)

Resumen. La actual tendencia hacia la provisión de conectividad ubicua independientemente del lugar, instante, aplicación utilizada o tecnología de acceso ha contribuido a acuñar la expresión *Always Best Connected (ABC)* para describir este entorno. Un requisito fundamental a cumplir hacia este objetivo consiste en ofrecer mecanismos de soporte a la movilidad de usuarios y/o terminales. En el presente artículo se revisan algunas de las soluciones para ofrecer movilidad en la capa de red, así como los puntos a salvar hacia este objetivo, como son la calidad de servicio y la seguridad. Ambos puntos generan interesantes temas de investigación debido a la variabilidad de las condiciones asociadas a un entorno móvil y al potencial aumento de las amenazas de seguridad.

Palabras clave: Movilidad IP, QoS, Seguridad, AAA

1. Introducción

La actual tendencia hacia la provisión de conectividad ubicua independientemente del lugar, instante, aplicación utilizada o tecnología de acceso ha contribuido a acuñar la expresión *Always Best Connected (ABC)* [GuJo03] para describir este entorno en el cual se le ofrece al usuario el mejor acceso mediante el mejor dispositivo en cada momento. La definición de *mejor* depende de múltiples parámetros. Algunos de ellos son: preferencias personales, tamaño y capacidad del dispositivo, requisitos de la aplicación, recursos de red disponibles o seguridad. Un requisito fundamental a cumplir hacia el objetivo de ABC consiste en ofrecer mecanismos de soporte a la movilidad de usuarios y/o terminales. Sin embargo, la movilidad puede ser entendida de diversas maneras, y soluciones para ofrecer movilidad a nivel de subred, red, transporte y aplicación pueden encontrarse en la literatura técnica. Habitualmente, movilidad se diferencia de portabilidad. Mientras que en la primera la conexión no se pierde cuando se cambia de punto de acceso a la red, no sucede lo mismo en lo respecta a portabilidad, que sólo garantiza que la comunicación se puede establecer, pero no necesariamente usando la misma dirección IP, lo que comporta la interrupción de las comunicaciones en curso. Este artículo se centra principalmente en la movilidad ofrecida en la capa de red al terminal, que es el tipo de movilidad que ha recibido mayor atención de la comunidad investigadora, especialmente con el desarrollo de MobileIP por parte del IETF.

* Este trabajo ha sido financiado en parte por el Ministerio de Ciencia y Tecnología (MCYT) y por el Fondo Europeo de Desarrollo Regional (FEDER) bajo el contrato TIC2002-04531-C04 (Proyecto: Servicios Avanzados con Movilidad (SAM)).

El soporte a la movilidad ha sido desarrollado para IPv4 y también para IPv6. Sin embargo, desde el punto de vista del diseño, la situación de ambos protocolos no es la misma. Como IPv4 fue desarrollado mucho antes de que se concibieran escenarios de movilidad, los mecanismos de movilidad fueron incorporados a modo de extensiones al protocolo. Como consecuencia de esto, algunas extensiones, aunque presentan sustanciales ventajas desde el punto de vista técnico, son difíciles de desplegar a gran escala. Por otro lado, el soporte a la movilidad se consideró desde el inicio en el diseño de IPv6. Y lo mismo sucedió con otros aspectos de interés en escenarios ABC, como por ejemplo la calidad de servicio (QoS) y la seguridad.

En relación a la QoS, los mismos servicios disponibles para el usuario fijo deberían poder ofrecerse al usuario móvil. Pero, como la movilidad habitualmente va de la mano de los enlaces inalámbricos, su variabilidad hace difícil cumplir este requisito. Además, el movimiento del terminal móvil implica cambios frecuentes de punto de acceso a la red, un proceso potencialmente perjudicial para la comunicación en curso.

La seguridad es también un campo que ha suscitado mucho interés en entornos móviles debido a que las amenazas potenciales aumentan por el hecho de que habitualmente se utilizan canales inalámbricos, pero también debido a que los esquemas de movilidad requieren interacciones entre nodos que en una red fija son, en general, considerados no habituales. Además, en un entorno ABC, existe la necesidad de una infraestructura coordinada para Autenticar, Autorizar y Contabilizar (AAA) debido a la variedad de tecnologías de acceso y los usuarios potenciales con exigencias diversas sobre la red.

En este artículo, se tratarán todos los temas mencionados anteriormente explicando brevemente los aspectos operativos más relevantes y revisando algunas de las opciones que se pueden encontrar en la literatura para ofrecer macromovilidad y micromovilidad (sección 2), QoS (sección 3) y seguridad (sección 4) en entornos móviles.

2. Movilidad

Las arquitecturas de gestión de la movilidad se dividen en dos partes principales, la gestión de la localización y la gestión del handoff. La primera consiste en el mantenimiento de un registro de los cambios de posición del nodo móvil (MN) y también la localización de un MN inactivo cuando un nodo externo quiere comunicarse con éste. El otro punto importante es la gestión de handoff, el objetivo del cual es mantener todas las conexiones del MN activas aunque éste cambie frecuentemente de punto de acceso a la red. El proceso mediante el que este cambio tiene lugar se denomina handoff, durante el cual se produce una reconexión, la comunicación puede ser interrumpida y el retardo puede aumentar. Dependiendo del tipo de handoff, dicho proceso es más o menos complejo, debido a que puede comportar cambios en el punto de acceso, el encaminador (router) de acceso, la tecnología de acceso y/o el dominio administrativo.

Desde el punto de vista de la red, la gestión de la movilidad se aborda desde dos perspectivas. En este sentido se diferencia entre los movimientos que se producen dentro de un dominio administrativo confinado dentro de una zona geográfica concreta, denominada micromovilidad, y por otra parte, la macromovilidad se encarga de gestionar los movimientos en áreas más extensas, que generalmente contienen redes distintas, que pueden utilizar tecnologías de acceso diferentes y pertenecer a dominios administrativos distintos. Los protocolos de micromovilidad intentan solucionar la sobrecarga, pérdida de paquetes y la latencia en el reestablecimiento del camino experimentado por los protocolos de macromovilidad durante el handoff. En general, las soluciones adoptadas confinan los intercambios de mensajes de control a una área reducida y configuran agentes móviles que actúan de representantes de ese área y permiten la interoperabilidad con esquemas de macromovilidad. El objetivo final de ambas soluciones es ofrecer al usuario una red funcional, capaz de mantener las conexiones activas todo el tiempo, independientemente de la posición del nodo, dentro de un único dominio (micromovilidad) o incluso dentro de toda Internet (macromovilidad). Las siguientes subsecciones intentan ofrecer un breve repaso de algunas de las soluciones que se pueden encontrar en la literatura.

2.1 Macromovilidad (Mobile IP)

Mobile IP es un protocolo de capa de red concebido para proporcionar macromovilidad a terminales móviles. Mobile IP está siendo diseñado por la Internet Engineering Task Force (IETF) en dos versiones, IPv4 e IPv6. Después de varias mejoras, el último estándar propuesto para Mobile IPv4 está descrito en el RFC 3344 [PeAl02]. Sin embargo, Mobile IPv6 es aún un borrador de IETF [JoPe03]. El objetivo de ambos protocolos es permitir que usuarios que se mueven en áreas extensas mantengan sus conexiones mientras cambian de punto de acceso a la red.

Funcionamiento de Mobile IPv4

Mobile IPv4 introduce cuatro entidades funcionales:

- Mobile Node (MN): Un dispositivo móvil
- Home Agent (HA): Un encaminador de la red propia que gestiona la localización del MN.
- Foreign Agent (FA): Un encaminador de la red visitada que coopera con el HA para proporcionar movilidad.
- Correspondent Node (CN): Un nodo fijo o móvil con el que el MN se comunica.

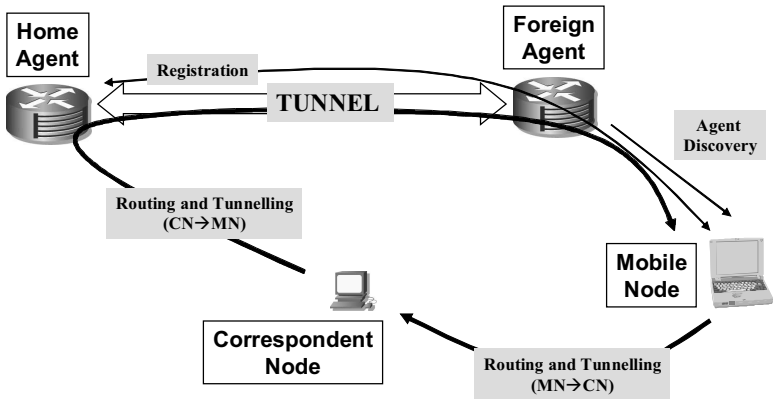

Figure 1. Funcionamiento de Mobile IPv4

El protocolo establece cuatro fases (figura 1). En la primera (*Agent Discovery*), el MN debe ser capaz de detectar si está conectado a su red propia o a una visitada. Para ello, el HA y el FA envían periódicamente mensajes de Agent Advertisements (una extensión del ICMP Router Discovery). Cuando el MN recibe este mensaje, es capaz de determinar en qué red está conectado, y si es una visitada, obtiene una Care-of Address (CoA). La CoA es la dirección IP asignada temporalmente al MN mientras está en una red visitada. El MN puede también solicitar un Agent Advertisement enviando un mensaje de Agent Solicitation para acelerar el proceso.

En la fase de *Registration*, el MN registra su CoA en el HA. El MN envía un Registration Request al FA, que, a su vez, lo reenvía al HA. El HA responde con un mensaje Registration Reply aceptando la solicitud. A partir de este punto, el HA conoce la localización del MN y la comunicación con los CN puede empezar, o continuar en caso de handoff.

En la tercera fase, denominada *Routing and Tunnelling*, el CN se comunica con el MN (y viceversa). Cuando un CN envía un paquete IP al MN, la dirección destino es la dirección asignada al MN en la red propia (home address). Cuando este paquete llega a la red propia del MN, éste es interceptado, encapsulado y reenviado por el HA al FA, que, a su vez, lo desencapsula y lo entrega al MN. Por otro lado, cuando el MN envía un paquete al CN, lo envía directamente utilizando su home address como dirección origen. Los paquetes enviados por el CN al MN son encaminados a través del HA. Este encaminamiento asimétrico, que no suele ser el óptimo, se conoce como triangle routing (ver figura 1). Esto genera una serie de ineficiencias, como un mayor retardo o un aumento en la carga de la red. A pesar de que existen mejoras para solucionar este problema (Route Optimization), éstas requieren modificaciones en los CN (que pueden ser cualquier nodo de Internet) y, por lo tanto, su despliegue es bastante costoso.

En la cuarta fase, conocida como *Handoff Management*, el MN cambia de subred asociando a un nuevo punto de acceso. El MN debe obtener una nueva CoA, registrarla en el HA y, una vez aceptada, vuelve a ser capaz de continuar la comunicación con los CN. Durante el proceso de *Handoff Management*, el HA puede no ser capaz de localizar el MN y algunos paquetes pueden perderse entre el CN y el MN.

Funcionamiento de Mobile IPv6

Mobile IPv6 es muy similar a Mobile IPv4. Sin embargo, la movilidad en IPv4 no fue considerada durante la fase de diseño del protocolo, sino que es un añadido posterior. En cambio, en IPv6, la movilidad se tuvo en cuenta desde el diseño inicial, y está totalmente integrada. Por este motivo, Mobile IPv6 es más eficiente y evita algunos problemas sufridos por Mobile IPv4. Entre otros, Mobile IPv6 (figura 2) no requiere FA, puesto que la autoconfiguración de direcciones de IPv6 proporciona la funcionalidad requerida en la fase de *Agent Advertisement*. Durante las fases de *Registration* y *Routing and Tunnelling*, los paquetes se encapsulan directamente desde el HA a la CoA del MN.

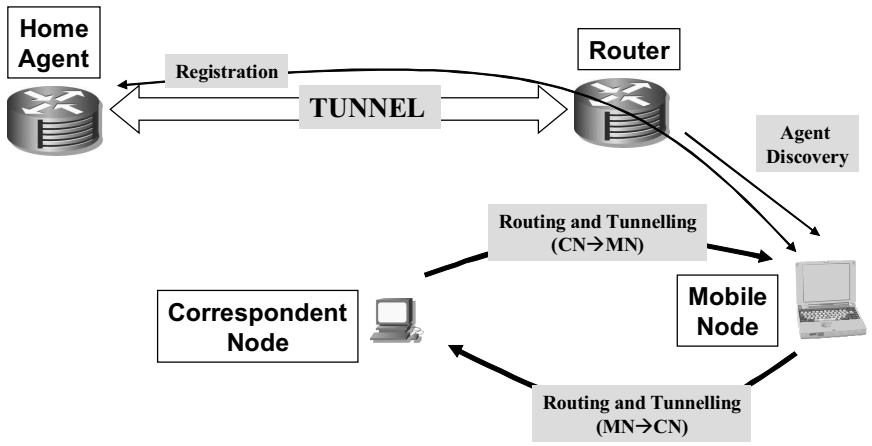

Figure 2. Mobile IPv6 overview

Mobile IPv6 también evita el triangle routing, porque cuando un CN envía un paquete a la home address del MN, el HA lo intercepta, encapsula y reenvía al MN. Sin embargo, el MN también puede enviar un mensaje de Binding Update (BU) al CN. Este mensaje incluye la CoA del MN, que se almacena en la Binding Cache del CN. Entonces, cualquier CN que quiera enviar un paquete, primero consulta su Binding Cache buscando la dirección IP destino. Si encuentra la entrada correspondiente en la cache, el paquete se envía directamente al MN usando la CoA asociada a la home address de éste. Esta funcionalidad es inherente a IPv6 y no requiere modificar los CN.

2.2 Micromovilidad

Hay muchos entornos donde determinadas aplicaciones que se ejecutan en equipos móviles pueden ser inservibles si éstos cambian frecuentemente de punto de acceso a la red. Por ejemplo, muchas aplicaciones de tiempo real, como la voz sobre IP (VoIP), experimentan una alta degradación del servicio si las reconexiones (handoffs) son frecuentes. Este problema es especialmente grave cuando se debe soportar un número de usuarios elevado.

El protocolo básico de movilidad IP basado en el mecanismo de túneles introduce sobrecarga en la red en términos de retardo creciente, pérdida de paquetes y señalización. El establecimiento de nuevos túneles puede introducir retardos

adicionales durante el proceso de handoff, produciendo pérdidas de paquetes y retrasando la entrega de datos a las aplicaciones. Este retardo es inherente al bucle introducido por la Movilidad IP al enviar la petición del registro al HA y enviar este la respuesta de vuelta al MN (o algunas veces al FA).

Los protocolos de micromovilidad [CaGo02] persiguen manejar el movimiento dentro de un dominio de equipos móviles, con mínima o nula pérdida de paquetes, mínima señalización, reducido consumo de potencia y sólo interaccionan con Mobile IP en el gateway de la red de acceso (ANG), es decir el nodo a través del cual el dominio se conecta a Internet. Esto tiene la ventaja de reducir el retardo y la pérdida de paquetes durante la reconexión al eliminar el registro entre los MNs y los posiblemente distantes HAs cuando los MNs permanecen dentro de áreas locales de cobertura. Todos los protocolos de micromovilidad IP comparten los mismos principios operacionales relacionados con fast handoff (reconexión rápida), la actualización de localización reducida, la seguridad rápida o incluso la calidad de servicio.

El soporte de fast handoff es una característica importante de los protocolos de micromovilidad. La reconexión está influenciada por la gestión de reconexión, las técnicas de envío (forwarding) y retención (buffering), el comportamiento del enlace radio, la predicción y detección de movimiento y el acoplamiento y la sincronización entre las capas radio e IP.

Típicamente, los equipos fijos conectados a Internet permanecen en línea durante largos periodos de tiempo, aunque no se comuniquen durante la mayor parte de ese tiempo. Los suscriptores móviles esperan un servicio similar. En el caso de MNs que mantienen la información de localización para soportar la alcanzabilidad continua, requieren actualizaciones de localización frecuentes que consumen recursos preciosos de ancho de banda y energía de la batería. Esta sobrecarga de señalización y consumo de potencia del equipo se pueden reducir con la introducción de *paginación (paging)*. Los MNs inactivos no se tienen que registrar si se mueven dentro de una misma área de búsqueda (*paging area*), y por tanto, sólo se registran si cambian de área de búsqueda.

Funciones de red como seguridad o tarificación invocadas durante la reconexión, se deben diseñar para ayudar a realizar la operación rápidamente. Mientras la autenticación de los mensajes de actualización de localización parece necesaria en muchos casos, la encriptación en la interfaz aire o en redes fijas no siempre es necesaria. La identificación de usuario para autorización y contabilidad se puede necesitar en algunos casos, mientras que el acceso anónimo es suficiente en otros.

Los protocolos de micromovilidad tratan de asegurar la llegada de paquetes y la señalización reducida ocultando las migraciones locales a los HAs. Los protocolos de movilidad jerárquicos registran en el HA la dirección del gateway en vez de la dirección asignada al MN en el dominio visitado. De esta manera, cuando el nodo móvil se desplaza de un

punto de acceso a otro (alcanzable desde el mismo gateway) el HA no necesita ser informado. El objetivo de los protocolos de micromovilidad es asegurar que los paquetes que llegan al gateway se envían al punto de acceso adecuado. Para encaminar los paquetes al punto de acceso actual del móvil, los protocolos mantienen una base de datos de localización para relacionar identificadores de nodo con información de localización. Hay dos estilos de micromovilidad: la jerarquización de túneles y el encaminamiento específico a móvil.

En la jerarquización de túneles, la base de datos de localización se mantiene de forma distribuida en el conjunto de agentes de movilidad. Cada agente lee la dirección de destino original de los paquetes entrantes y busca en su lista de visitantes la entrada correspondiente. La entrada contiene la dirección del agente de siguiente nivel por abajo o bien directamente la dirección asignada al MN en la red visitada. Las entradas se crean y se mantienen transmitiendo mensajes de registro desde los MNs. Algunas de estas propuestas desembocan en una estructura en árbol de agentes de movilidad. Sin embargo, en la versión más reciente de HMIP (Mobile IP jerárquico) [SoCa03], una de las propuestas principales de túneles jerárquicos, los agentes de movilidad interaccionan directamente con el MN sin tener necesidad de establecer una estructura de agentes en forma de árbol.

Las propuestas de encaminamiento específico de móvil eliminan la sobrecarga introducida por la desencapsulación y reencapsulación de las propuestas basadas en túneles. Estos esquemas introducen señalización implícita o explícita para actualizar las rutas específicas a móvil. En el caso de Cellular IP [CaGo00] los MNs conectados a una red de acceso usan la dirección IP del gateway como su CoA. El gateway desencapsula los paquetes y los envía al punto de acceso. Dentro de la red de acceso, el MN se identifica por su home address y los paquetes de datos se encaminan directamente sin necesidad de túnel o conversión de direcciones. El protocolo de encaminamiento asegura que los paquetes se entregan en la ubicación actual del nodo.

3. Calidad de servicio (QoS)

La movilidad va habitualmente asociada con enlaces inalámbricos. Estos enlaces presentan características (p.e. fading o interferencias) que pueden variar sustancialmente dependiendo del entorno, y por tanto, afectan la comunicación. Además, la movilidad de los nodos está implícitamente asociada con nodos relativamente simples que pueden tener características muy diferentes en cuanto a capacidad de procesado, interfaz de usuario o consumo de potencia. Asimismo, la movilidad también implica la existencia potencial de handoffs cuando el nodo se mueve. En este entorno, el objetivo de la gestión de handoff con QoS es resolver tanto el encaminamiento de paquetes a través del nuevo camino como los aspectos relacionados con el reestablecimiento del estado de QoS en este camino. En este marco tan cambiante, se producen efectos menores que se pueden ocultar mediante adaptación a nivel de aplicación. Sin embargo,

también se producen variaciones severas que requieren la intervención de la red, particularmente en presencia de handoffs. Esta sección se centra en los problemas que aparecen y las posibles soluciones propuestas para gestionar los handoffs teniendo en cuenta la QoS.

El objetivo de las arquitecturas de movilidad que tienen en cuenta la QoS es el de mantener, no sólo la comunicación en caso de handoff, sino también la QoS requerida por el MN. El RFC 3583 [ChAl03] señala como requisitos principales impuestos sobre una solución que ofrezca QoS para mobile IP: minimización de la interrupción de QoS durante handoff, reestablecimiento en las partes afectadas del camino de QoS, liberación del estado de QoS a lo largo del camino anterior, interoperabilidad con protocolos de movilidad, soporte a caminos con QoS heterogénea (debido a filosofías de QoS diferentes), capacidad de ofrecer QoS a través de multiples caminos e interacción con el soporte de QoS ofrecido en las capas bajas en el enlace inalámbrico.

Tal como se ha comentado más arriba, la profundidad del handoff, es decir, la magnitud de los cambios asociados (p.e. cambios de punto de acceso y/o de tecnología y/o de dominio) determinan la complejidad a la hora de ofrecer QoS. Es decir, si sólo se cambia de punto de acceso y se mantiene la subred, el handoff es más simple que si además se cambia de subred o de dominio (mayor profundidad de handoff). Por tanto, el retardo de reconexión con QoS es previsible que aumente con la profundidad del handoff. Los protocolos de macromovilidad han sido rediseñados desde su concepción inicial para ofrecer mejor procesado de los paquetes, particularmente en Mobile IPv6. Sin embargo, estas soluciones, incluso cuando se combinan con señalización de QoS (p.e. RSVP), no escalan en áreas extensas debido a la sobrecarga de señalización y la latencia de reestablecimiento del estado. Por otro lado, las soluciones de micromovilidad confinan la gestión de la movilidad a áreas locales, ofreciendo latencias menores y menos sobrecarga en la red. Pero estas soluciones sólo son de aplicación dentro de un dominio administrativo. En conclusión, todavía no existe una solución global integrada [MaLo 02].

A nivel del ofrecimiento de QoS a agregados de tráfico, apropiado para aplicar la filosofía diffserv, algún tipo de control de admisiones estadístico puede realizarse en el borde de la red. Ésta puede ser una tarea asignada a los ANGs y encaminadores de acceso (ARs). Los primeros para el tráfico destinado a los MNs del dominio y los segundos para el generado por los MNs. ANGs y ARs, cuando reciben una petición de comunicación contactan con un agente de QoS (QoS broker), que es el encargado de gestionar los recursos de un dominio determinado. A su vez, para QoS con una granularidad mayor dentro de un dominio, se suelen considerar soluciones que integren los protocolos de micromovilidad y de QoS a nivel de flujo (Intserv). La intensidad de esta integración puede variar desde utilizar eventos de handoff para iniciar mensajes de reserva de QoS hasta diseñar conjuntamente e integrar los protocolos de micromovilidad y reserva de QoS. En este último caso, los objetos de QoS se transportan en los mensajes de registro,

estableciendo así el estado de QoS al mismo tiempo que se establece el camino después del handoff. Modificaciones en los nodos de red también permiten confinar los mensajes de seguimiento de los cambios en las reservas de QoS a un área local, evitando de esta forma la necesidad del reestablecimiento del camino extremo a extremo. Esto minimiza la latencia de reestablecimiento de la QoS y la sobrecarga de señalización a costa de incrementar la complejidad de la red y la dependencia de las soluciones de QoS del protocolo de micromovilidad.

Aparte de mejorar la latencia y la sobrecarga de la arquitectura de QoS, la provisión de garantías de QoS a una sesión determinada de un MN requiere la existencia de mecanismos para el control de admisiones y para realizar reservas anticipadas en todas las células que pudieran ser visitadas durante la sesión. El control de admisiones se encarga de dar mayor prioridad a las conexiones que entran en una célula después de un handoff frente a las nuevas. La idea básica es la reserva anticipada de recursos en las células vecinas en vistas a potenciales handoffs. Los mecanismos de reserva anticipada se encargan de señalizar explícitamente las necesidades de QoS a aquellas células que puedan ser visitadas por el MN durante la sesión. Ejemplos de este tipo de mecanismos son Mobile Resource Reservation Protocol (MRSVP), que sigue una filosofía Intserv, e ITSUMO, que sigue una filosofía Diffserv [MaLo 02].

Alternativamente, mecanismos para realizar negociaciones pre-handoff, como por ejemplo el protocolo de transferencia de contexto que se está desarrollando en el grupo de trabajo Seamoby de IETF, pueden ayudar a determinar qué célula colindante es capaz de ofrecer la QoS demandada y transferir el estado de QoS a fin de que cuando el handoff se produzca, todo esté disponible para ofrecer la QoS al MN sin tener que iniciar una nueva petición de reserva [KeAl02]. De esta forma, el desperdicio potencial de recursos debido a las reservas anticipadas se podría minimizar a riesgo de aumentar la tasa de conexiones rechazadas.

4. Seguridad

Para preservar la seguridad de Internet, debemos proveer a los entornos móviles con el mismo nivel de seguridad disponible en los entornos fijos. Sin embargo, la complejidad es mayor debido a las implicaciones que la movilidad de los nodos conlleva. Algunos aspectos a considerar son: implicaciones del nodo móvil sobre una red visitada, implicaciones sobre la red propia cuando el MN está fuera e implicaciones sobre el MN cuando visita una red [MiPä00]. Estos aspectos son los que se pretenden resolver mediante los mecanismos explicados en esta sección.

Seguridad en MobileIP

Para cumplir los objetivos de seguridad, el nodo que recibe un mensaje relacionando una Home Address y una Care-of Address debe verificar que éstas corresponden al mismo nodo. En MIP4 [PeAl02], solamente el HA procesa dichos mensajes. Dado que es razonable asumir que existe alguna relación de confianza previa entre el nodo móvil (MN) y el

HA, la seguridad en este caso se obtiene a través de una asociación de seguridad preestablecida entre ambos para proteger los paquetes de BU enviados por el MN al HA.

En MIP6 [JoPe03], tanto el HA como el nodo correspondiente (CN) son capaces de procesar dichos mensajes, llamados Binding Update (BU). Los mensajes de BU desde el MN al HA son protegidos mediante un mecanismo similar al usado en MIP4 basado en una asociación de seguridad preestablecida y el uso de IPSec.

Para proteger los mensajes BU desde el MN al CN no es posible utilizar el método anterior ya que no es razonable asumir que el MN tiene una relación previa de confianza con todos los potenciales CN existentes en Internet, por lo que es necesario un método alternativo. El método utilizado se basa en verificar que el nodo alcanzable a través de la home address es el mismo que el nodo alcanzable a través de la CoA. Para ello, cuando un MN desea enviar un mensaje de BU a un CN, debe primero obtener información de validación de dicho BU de la siguiente forma:

El MN solicita que el CN le envíe una clave a la home address.

Asimismo, el MN solicita al CN que le envíe otra clave a la CoA.

Una vez dispone de ambas claves, el MN utiliza una función de hash sobre ambas e información adicional para generar la información de autorización del mensaje BU.

Cuando el CN recibe el mensaje BU, verifica la información de autorización antes de procesarlo. A partir de dicha información de validación, el nodo CN puede verificar que el mismo MN es accesible a través de la home address y de la CoA (ya que la información de validación contiene tanto la clave enviada a la CoA como la clave enviada a la home address).

Mediante los mecanismos de seguridad anteriormente descritos, los protocolos de soporte de movilidad en IPv4 y en IPv6 garantizan que las comunicaciones móviles poseen un nivel de seguridad equivalente al de las comunicaciones con nodos fijos. Para mayor información sobre el diseño de la arquitectura de seguridad de MIP, el lector es referido a [NiAr03].

Integración de IPv6 Móvil e Infraestructura AAA

Igualmente importante para el marco de seguridad de soporte a la movilidad es la integración con una infraestructura de Autenticación, Autorización y Contabilidad (AAA). En IPv6 Móvil (*Mobile IPv6*), tal y como ocurría en el protocolo MIPv4, no se consideran entornos de redes multidominio, entendiendo como dominio una entidad lógica que tiene sus propias reglas y políticas y que puede establecer acuerdos de negocio con otros dominios. Además de permitir a un nodo moverse entre distintos dominios, son necesarios ciertos acuerdos de negocio y un nivel de servicio entre los distintos operadores. Alguna de estas cuestiones deben ser tratadas mediante una infraestructura complementaria: AAA

[DIAM] permite autenticar usuarios, procesos y dispositivos (el acto de verificar la identidad de una entidad), autorizarlos (el acto de determinar cuando una entidad tendrá acceso a un recurso que solicite, por ejemplo, la propia red puede considerarse un recurso) y llevar la cuenta de las operaciones de los usuarios sobre la red (por ejemplo, controlar cargos, facturas..). Por consiguiente, la integración de ambos elementos, esto es, *Mobile IPv6* y AAA, permitirá el movimiento de usuarios en un escenario multidominio.

Un aspecto importante en este contexto es el protocolo para llevar la información de AAA entre los nodos móviles y los equipos de la infraestructura, estos equipos llamados *attendant,* que también toman parte en el despliegue de la infraestructura AAA (de hecho, son los responsables de recibir las peticiones de acceso de los usuarios de *Mobile IPv6* y reenviarlo a un punto AAA de la infraestructura, por medio del *Diameter Protocol*). Una de las propuestas más interesantes es el protocolo definido por el grupo de trabajo de IETF PANA [PANA]. El objetivo de PANA (*Protocol for carrying Authentication for Network Acces)* es permitir a los clientes autenticarse a través de protocolos IP. Dicho protocolo permite a un cliente interactuar con un punto de la infraestructura AAA para obtener acceso sin necesidad de conocer el protocolo específico de la infraestructura AAA utilizado.

Por otro lado, uno de los objetivos del proceso de autenticación y autorización es el establecimiento de una asociación de seguridad (SA) entre los nodos móviles (MN) y el equipo de servicio (SE). Se supone que los *attendant* tiene una serie de relaciones de confianza preestablecidas con la infraestructura AAA. Para obtener la asociación de seguridad de MN-SE debe establecerse un esquema de distribución de claves (i.e. [LeFa02]) entre los nodos móviles y el equipo de servicio o *attendant*. La idea más generalizada es que el servidor AAA del usuario debe distribuir dichas claves [FaLe02].

Para concluir, el protocolo *Mobile IPv6* puede beneficiarse de la interacción con AAA. MIPv6 necesita autenticar alguno de sus paquetes de gestión (*binding updates, bindings acknoledgments)* [JoPe03] para evitar problemas de seguridad.

5. Referencias

[CaGo00] A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, C.-Y. Wan, and A. Valkó. "Design, Implementation and Evaluation of Cellular IP." *IEEE Personal Communications* 7 (4): 42-49, August 2000.

[CaGo02] A. T. Campbell, J. Gomez, S. Kim, A. Valkó, C.-Y Wan, and Z. Turanyi, "Comparison of IP Micromobility Protocols." IEEE Wireless Communications Magazine, 9(1): 72-82, February 2002

[GuJo03] E. Gustafsson, A. Johnson. “Always Best Connected”. IEEE Wireless Communications 10(1): 49-55, February 2003.

[ChAl03] Chaskar H., ed. “Requirements of a Quality of Service (QoS) Solution for Mobile IP,” IETF RFC 3583, September 2003.

[DIAM] Open Source Diameter Server http://sourceforge.net/projects/diameter

[FaLe02] Stefano M. Faccin, Franck Le “Mobile IPv6 Authentication, Authorization, and Accounting Requirements”, November 2002. http://www.ietf.org/internet-drafts/draft-le-aaa-mipv6-requirements-01.txt

[JoPe03] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6.” Internet Draft, draft-ietf-mobileip-ipv6-24, June 2003.

[KeAl02] Kempf J. ed. ”Problem description: reasons for performing context transfers between nodes in an Ip access network.” IETF RFC 3374, September 2002.

[LeFa02] F.Le, S.M. Faccin “Dynamic Diffie Hellman based Key Distribution for Mobile IPv6”, Internet Draft, April 2002.

[MaLo 02] Manner J., López A., Mihailovic A. et al. "Evaluation of mobility and quality of service interaction." Computer Networks 30: 137-163, 2002.

[MiPä00] Mink S., Pählke F., Schäfer G., and Schiller J. “Towards secure mobility support for IP networks.” IFIP International Conference on Communication Technologies (ICCT): 555-562, August 2000.

[NiAr03] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, “Mobile IP version 6 Route Optimization Security Design Background”, Internet-Draft, draft-nikander-mobileip-v6-ro-sec-02, December 2003.

[PANA] Protocol for carrying Authentication for Network Access (PANA) http://www.ietf.org/html.charters/pana-charter.html

[PeAl02] C. Perkins, ed. “IP Mobility Support for IPv4.” IETF RFC 3344, August 2002

[SoCa03] H. Soliman, C. Castelluccia, K. Malki, L. Bellier, "Hierarchical Mobile IPv6", Internet Draft, draft-ietf-mipshop-hmipv6-00, October 2003.