

**EVALUACIÓN DEL EFECTO DEL HANDOVER EN UN CONTEXTO DE
MICROMOVILIDAD IPV6 SOBRE UN SERVICIO DE TIEMPO REAL**



**Laura Beatriz Terán Ramírez
Maicol Alberto Cuastuza**

**Universidad del Cauca
Facultad de Ingeniería en Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Nuevas Tecnologías en Telecomunicaciones GNTT
Popayán, Octubre 2011**

**EVALUACIÓN DEL EFECTO DEL HANDOVER EN UN CONTEXTO DE
MICROMOVILIDAD IPV6 SOBRE UN SERVICIO DE TIEMPO REAL**



**Trabajo de grado como requisito para optar al título de Ingeniero en Electrónica y
Telecomunicaciones**

**Laura Beatriz Terán Ramírez
Maicol Alberto Cuastuza**

Director: Ing. Oscar Josué Calderón Cortés

**Universidad del Cauca
Facultad de Ingeniería en Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de Nuevas Tecnologías en Telecomunicaciones GNTT
Popayán, Octubre 2011**

TABLA DE CONTENIDO

CAPÍTULO I. MOVILIDAD IP	3
1.1 INTRODUCCIÓN.....	3
1.1.1 Gestión de Movilidad	5
1.2 ESCENARIOS DE MOVILIDAD IP.....	6
1.2.1 Macromovilidad.....	7
1.2.2 Micromovilidad	8
1.3 HANDOVER.....	9
CAPÍTULO II. FACTORES QUE INCIDEN EN LA CALIDAD DE UN SERVICIO DE TIEMPO REAL	11
2.1 INTRODUCCIÓN.....	11
2.2 CALIDAD DEL SERVICIO - QoS	12
2.2.1 Calidad de Servicio Según los Organismos de Regulación ITU/ETSI	12
2.3 TRÁFICO EN LA RED	14
2.3.1 Tráfico Elástico.....	14
2.3.2 Tráfico Inelástico.....	14
2.4 FACTORES QUE AFECTAN EL DESEMPEÑO DE SERVICIOS PRESTADOS EN TIEMPO REAL	17
2.4.1 Movimiento del Móvil	19
2.4.2 Medio de Transmisión.....	20
2.4.3 Configuración de la Red	21
2.4.4 Aplicación.....	24
2.5 PARÁMETROS DE QoS PARA SERVICIOS EN TIEMPO REAL.....	25
2.5.1 Variación de Retardo (Jitter).....	27
2.5.2 Pérdida de Paquetes	27
2.5.3 Ancho de Banda.....	28
2.5.4 Throughput.....	28
2.5.5 Disponibilidad de Servicios.....	29
2.5.6 Latencia Extremo a Extremo	29
2.5.6.1 <i>Latencia de Handover</i>	30
2.5.6.2 <i>Pérdida de Paquetes Durante el Handover</i>	30

CAPÍTULO III. PROTOCOLOS DE MOVILIDAD IPv6	32
3.1 INTRODUCCIÓN	32
3.2 MOBILE IPv6 (MIPv6)	33
3.2.1 Antecedentes	33
3.2.2 Términos Utilizados en Mobile IPv6	33
3.2.3 Operación de Mobile IPv6	35
3.3 HIERARCHICAL MOBILE IPv6 (HMIPv6)	37
3.3.1 Antecedentes	37
3.3.2 Términos Utilizados en Hierarchical Mobile IPv6	38
3.3.3 Operación de Hierarchical Mobile IPv6	38
3.4 PROXY MOBILE IPv6 (PMIP)	40
3.4.1 Antecedentes	40
3.4.2 Términos Utilizados en Proxy Mobile IPv6	40
3.4.3 Operación de Proxy Mobile IPv6	41
3.5 SÍNTESIS DE PROTOCOLOS DE MOVILIDAD	43
CAPÍTULO IV. SIMULACIÓN, PRUEBAS Y RESULTADOS	45
4.1 SELECCIÓN DEL PROTOCOLO DE MICROMOVILIDAD IPv6 Y DE LA HERRAMIENTA DE SIMULACIÓN	45
4.1.1 Selección del Protocolo de Micromovilidad IPv6	45
4.1.2 Herramientas de Simulación	45
4.1.2.1 OPNET	46
4.1.2.2 OMNet ++	47
4.1.2.3 NS2	47
4.1.3 Elección de la Herramienta de Simulación	48
4.2 METODOLOGÍA DE SIMULACIÓN	49
4.2.1 Planteamiento General de los Escenarios y Casos de Simulación	50
4.2.1.1 Generalidades de los Escenarios de Simulación	50
4.2.2 Definición de las Características Técnicas de los Escenarios de Simulación ..	53
4.2.3 Ejecución de las Pruebas de Simulación	53
4.2.4 Análisis de los Resultados	54
4.2.4.1 Escenario 1	54
4.2.4.1.1 Caso 1a: Un Nodo Móvil con Movimiento Controlado	54
4.2.4.1.2 Caso 1b: Un Nodo Móvil con Movimiento Aleatorio	66
4.2.4.2 Escenario 2	71

4.2.4.2.1 Caso 2a: <i>Un Nodo Móvil con Movimiento Controlado</i>	71
4.2.4.2.2 Caso 2b: <i>Un Nodo Móvil con Movimiento Aleatorio</i>	79
4.2 OBSERVACIONES DE LOS RESULTADOS OBTENIDOS.....	88
CAPÍTULO V. CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS	91
5.1 CONCLUSIONES	92
5.1.1 Respecto a la Movilidad	92
5.1.2 Respecto al Desarrollo de la Simulación	93
5.1.3 Respecto a los Resultados de la Simulación	94
5.2 RECOMENDACIONES.....	94
5.3 TRABAJOS FUTUROS.....	95
REFERENCIAS	96

LISTA DE FIGURAS

Figura 1.1. Jerarquía e Interconexiones en Internet	7
Figura 1.2. Escenarios de Movilidad IP. Macromovilidad IP y Micromovilidad IP	9
Figura 2.1. Relación entre las diferentes perspectivas de QoS	13
Figura 2.2. Clasificación de las aplicaciones según la tolerancia a pérdida de paquetes .	16
Figura 2.3. Clasificación de las aplicaciones según la tolerancia a retardos	16
Figura 2.4. Marco conceptual de los factores que afectan el desempeño de un servicio en tiempo real	18
Figura 2.5. Parámetros de QoS para servicios en tiempo real	26
Figura 3.1. Funciones de los elementos de Mobile IPv6	34
Figura 3.2. Diagrama de Tiempo MIPv6	36
Figura 3.3. Funciones de los elementos de Hierarchical Mobile IPv6	38
Figura 3.4. Diagrama de Tiempo HMIPv6	39
Figura 3.5. Funciones de los elementos de PMIPv6	41
Figura 3.6. Diagrama de Tiempo PMIPv6	42
Figura 3.7. Principales Características de los Protocolos de Movilidad	44
Figura 4.1. Escenario de Simulación No. 1	51
Figura 4.2. Escenario de Simulación No. 2	52
Figura 4.3. Trayectoria del nodo móvil para el caso 1a	54
Figura 4.4. Ocurrencia de los Handover en una Línea de Tiempo	54
Figura 4.5. Ocurrencia del primer Handover para el caso 1a	55
Figura 4.6. Histograma de Paquetes para el caso 1a	57
Figura 4.7. Tasa de Pérdida de Paquetes durante los Handover 1, 3 y 5 realizados por el MN para el caso 1a	58
Figura 4.8. Comportamiento del Throughput durante los Handover 1, 3 y 5 realizados por el MN para el caso 1a	60
Figura 4.9. Comportamiento del Retardo durante los Handover 1, 3 y 5 realizados por el MN para el caso 1a	62
Figura 4.10. Comportamiento del Jitter durante los Handover 1, 3 y 5 realizados por el MN para el caso 1a	64
Figura 4.11. Ocurrencia de los Handover en una Línea de Tiempo para el caso 1b	65
Figura 4.12. Tasa de Pérdida de Paquetes para los Handover 1 y 3 realizados por MN para el caso 1b	67
Figura 4.13. Comportamiento del Throughput durante los Handover 1 y 3 realizados por el MN para el caso 1b	68

Figura 4.14. Comportamiento del Retardo durante los handover 1 y 3, realizados por el MN para el caso 1b.....	69
Figura 4.15. Comportamiento del Jitter durante los Handover 1 y 3 realizados por MN para el caso 1b	70
Figura 4.16. Trayectoria del nodo móvil para el caso 2a.....	70
Figura 4.17. Ocurrencia de los Handover en una Línea de Tiempo para el caso 2a	71
Figura 4.18. Tasa de Perdida de Paquetes durante los Handover 1, 3 y 5 realizados por el MN para el caso 2a.....	73
Figura 4.19. Comportamiento del Throughput durante los Handover 1, 3 y 5 realizados por el MN para el caso 2a	75
Figura 4.20. Comportamiento del Retardo durante los Handover 1, 3 y 5 realizados por el MN para el caso 2a.....	77
Figura 4.21. Comportamiento del Jitter durante los Handover 1, 3 y 5 realizados por el MN para el caso 2a	78
Figura 4.22. Ocurrencia de los Handover en una Línea de Tiempo para el caso 2b	79
Figura 4.23. Tasa de Perdida de Paquetes durante los Handover 2, 5 y 8 realizados por MN para el caso 2b.....	81
Figura 4.24 Comportamiento del Throughput durante los Handover 2, 5 y 8 realizados por el MN para el caso 2b.....	83
Figura 4.25 Comportamiento del Retardo durante los Handover 2, 5 y 8 realizados por el MN para el caso 2b.....	85
Figura 4.26 Comportamiento del Jitter durante los Handover 2, 5 y 8 realizados por el MN para el caso 2b	86

LISTA DE TABLAS

Tabla 2.1. Tipos de Tráfico y Aplicaciones Relacionadas	15
Tabla 3.1. Síntesis de Protocolos de Movilidad IPv6	43
Tabla 4.1. Comparación de las características de las herramientas de simulación	48
Tabla 4.2. Distribución de las MAGs en los canales de transmisión disponibles	52
Tabla 4.3. Características Generales de Simulación	54
Tabla 4.4. Características de los Enlaces	54
Tabla 4.5. Momento aproximado en el que se realizó cada handover	55
Tabla 4.6. Eventos importantes durante un handover para el caso 1a	56
Tabla 4.7. Duración de los Handover y No. de Paquetes Perdidos para el caso 1a	56
Tabla 4.8. Instante aproximado en el que se realizó cada Handover para el caso 1b	65
Tabla 4.9. Duración de los Handover y No. de Paquetes Perdidos para el caso 1b	66
Tabla 4.10. Instante aproximado en el que se realizó cada Handover para el caso 2.....	71
Tabla 4.11. Duración de los Handover y No. de Paquetes Perdidos para el caso 2a	71
Tabla 4.12. Instante aproximado en el que se realizó cada Handover para el caso 2b.....	79
Tabla 4.13. Duración de los Handover y No. de Paquetes Perdidos para el caso 2b	80
Tabla 4.14. Parámetros de QoS durante los Handover presentados en la comunicación	87

LISTA DE ECUACIONES

Ecuación 2.1. Velocidad del Nodo Móvil.....	19
Ecuación 2.2. Función del <i>Jitter</i>	27
Ecuación 2.3. Latencia Total de <i>Handover</i>	30

LISTA DE ACRÓNIMOS

- AD:** *Administrative Domain* (Dominio Administrativo).
- AP:** *Access Point* (Punto de Acceso).
- BA:** *Binding Acknowledgement* (Confirmación de Asociación).
- BE:** *Best Effort* (Mejor Esfuerzo).
- BU:** *Binding Update* (Actualización de Asociación).
- CN:** *Correspondent Node* (Nodo Corresponsal).
- CoA:** *Care of Address* (Dirección del MN en una red visitada).
- ETSI:** *European Telecommunications Standards Institute* (Instituto Europeo de Normas de Telecomunicaciones).
- FN:** *Foreing Network* (Red Visitada).
- HA:** *Home Agent* (Agente Local).
- HMIP:** *Hierarchical Mobile IP* (IP Móvil Jerárquico).
- HN:** *Home Network* (Red Local).
- HO:** *Handover* (Traspaso).
- IP:** *Internet Protocol* (Protocolo de Internet).
- ITU:** *International Telecommunication Union* (Unión Internacional de Telecomunicaciones).
- LMA:** *Local Mobility Anchor* (Anclaje de Movilidad Local).
- MAG:** *Mobility Access Gateway* (Compuerta Móvil de Acceso).
- MAP:** *Mobility Anchor Point* (Punto de Anclaje de Movilidad).
- MIP:** *Mobile IP* (IP Móvil)
- MM:** *Management Mobility* (Gestión de Movilidad).
- MN:** *Mobile Node* (Nodo Móvil).
- PBA:** *Proxy Binding Acknowledgement* (Confirmación de Asociación de Proxy).
- PBU:** *Proxy Binding Update* (Actualización de Asociación de Proxy).
- PDV:** *Packet Delay Variation* (Variación de Retardo de Paquete).
- PMIP:** *Proxy Mobile IP*.
- QoS:** *Quality of Service* (Calidad de Servicio).
- QoS_D:** *Quality of Service Delivered* (Calidad de Servicio Proporcionada).
- QoS_O:** *Quality of Service Offered* (Calidad de Servicio Ofrecida).
- QoS_P:** *Quality of Service Perceived* (Calidad de Servicio Percibida).
- QoS_R:** *Quality of Service Required* (Calidad de Servicio Requerida).
- RTP:** *Real Time Protocol* (Protocolo de Tiempo Real).
- TCP:** *Transmission Control Protocol* (Protocolo de Control de Transmisión).
- UDP:** *User Datagram Protocol* (Protocolo de Datagrama de Usuario).

INTRODUCCIÓN

En la última década el crecimiento de las redes de comunicaciones ha sido acelerado y cambiante, debido en gran medida a la cantidad y variedad de aplicaciones y servicios que soportan y al incremento en el número de usuarios que hacen uso de éstas.

La masificación que ha tenido Internet a nivel global, ha llevado a los proveedores de red y servicios a establecer nuevas metas y estrategias en la prestación de sus servicios con el fin de garantizar a las características de calidad de servicio (QoS – Quality of Service) que las diferentes aplicaciones demandan, las cuales son requeridas para la adecuada satisfacción del usuario final al recibir un servicio particular.

A esto se suma el auge que en la actualidad tienen las comunicaciones inalámbricas, las cuales permiten y facilitan el establecimiento de una comunicación sin la necesidad de depender de un punto fijo de conexión y además brinda la capacidad de movilidad y desplazamiento que los usuarios requieren. Sin embargo, esto puede conllevar algunos problemas en la prestación de los servicios con la calidad deseada, debido entre otros a la variabilidad inherente que presentan los canales inalámbricos, y más aun a los diferentes procesos que están involucrados en el desplazamiento y la movilidad del usuario: señalización, autenticación, cambio de zonas de cobertura (Proceso de Traspaso o *Handover*), etc.

Un nodo móvil conectado a un punto de acceso a la red al desplazarse dentro de un dominio particular, puede realizar un cambio de zona de cobertura, lo que implica que éste debe ser hecho con rapidez, coordinadamente y de forma transparente para que el servicio no sufra ningún tipo de degradación que pueda ser percibido por el usuario final; de la efectividad con que se realice este proceso, depende el mantenimiento continuo de la conexión y la minimización de los errores que se presentan en la comunicación. Adicionalmente, en un contexto de movilidad basado en IP, es necesario conservar la continuidad de la conexión lógica previamente establecida, y esto se logra con los protocolos de movilidad IP adecuados.

A partir de lo anterior, este trabajo de grado realiza mediante simulación, un análisis y evaluación del impacto del proceso de *handover* en un servicio de tiempo real en un contexto de micromovilidad basado en un protocolo de movilidad IPv6, con el fin de determinar cómo se afecta la prestación de dicho servicio durante el proceso de *handover*.

Este documento se divide en cinco capítulos estructurados de la siguiente manera:

Capítulo I. Presenta los conceptos relacionados con ambientes y comunicaciones móviles basadas en IP, resaltando al final del mismo el concepto de *handover*, dada su incidencia en la continuidad de la prestación de un servicio.

Capítulo II. Define conceptos referentes a la calidad de servicio y al tráfico que cursa la red. Posteriormente describe detalladamente los factores generales que pueden afectar cualquier comunicación en un ambiente móvil IP, generando degradaciones en la misma.

Capítulo III. Describe antecedentes, definiciones y funcionamiento de 3 protocolos de movilidad adecuados para el desarrollo de este proyecto.

Capítulo IV. Describe la herramienta software seleccionada, el escenario de red y sus características. Además se especifican y describen las pruebas, los parámetros a evaluar, los resultados obtenidos y se analizan los mismos. Finalmente se realiza una Tabla comparativa de los resultados y algunas observaciones de los mismos.

Capítulo V. Se exponen las conclusiones del desarrollo de todo proyecto y se presentan una serie de recomendaciones para el desarrollo de futuros trabajos e investigaciones en este campo.

CAPÍTULO I. MOVILIDAD IP

1.1 INTRODUCCIÓN

En la actualidad, en el contexto de las redes móviles es necesario brindar a los usuarios un ambiente en el que puedan estar siempre conectados, independientemente del lugar, momento o dispositivo utilizado, permitiéndoles acceder sin inconvenientes a los servicios deseados. Las soluciones para facilitar la conectividad móvil se han planteado desde hace tiempo, sin embargo hoy en día, aún se siguen definiendo nuevos modelos y estrategias que satisfagan los requerimientos y tendencias que imponen las nuevas aplicaciones y servicios.

La movilidad describe a un objeto capaz de moverse o que puede ser movido habitual u ocasionalmente. Como tal, la movilidad no representa un servicio, sino que mejora la disponibilidad de los servicios de red. Por lo tanto, se ve reflejada en la capacidad que tiene un usuario para acceder a sus servicios independientemente de los cambios de entorno que debe realizar, producto de las actividades que desarrolla. Si no va acompañada por algún servicio, la movilidad no tiene ningún valor [1][2]. Por otro lado, la gestión de movilidad (*MM – Mobility Management*) se define como un conjunto de funciones utilizadas para proporcionar la movilidad al usuario, al servicio y al terminal. Estas funciones abarcan desde la comunicación con la red local hasta los procesos de autenticación, autorización, actualización de ubicación y descarga de información de usuario [3].

En redes de telecomunicaciones, la movilidad puede ser definida y aplicada según la gestión que se realice, como: movilidad personal, movilidad de servicios y movilidad de terminal [4].

- La movilidad personal es la facilidad de un usuario para acceder a servicios de telecomunicaciones desde cualquier terminal, manteniendo siempre una única identidad independientemente de cuál sea su punto de conexión en la red [5].
- La movilidad de servicios permite a un usuario mantener acceso a sus servicios, sin importar la ubicación del mismo ni del terminal empleado para ese fin [6].
- La movilidad de terminal se define como la capacidad que tiene un terminal para acceder a servicios de telecomunicaciones desde diferentes ubicaciones y mientras se encuentra en movimiento. La red debe ser capaz de identificar y localizar a dicho terminal [7].

El soporte para la movilidad se desarrolló en las 2 versiones manejadas por el protocolo Internet (*IP – Internet Protocol*). Inicialmente, este tipo de soporte se adecuó por medio de actualizaciones correctivas en IPv4, y aunque trajo consigo muchas ventajas desde un punto de vista técnico, no fue suficiente para cumplir con las demandas de los usuarios que cada vez eran más complejas, lo que llevo a considerar que esto generaría inconvenientes en caso de que se quisiera implementar a gran escala. Por otro lado, en IPv6 el soporte para la movilidad, entre otras cosas, se tuvo en cuenta desde que se inició su diseño, lo que resolvió el problema que presentaba el protocolo *Mobile IPv4*, y convirtió a *Mobile IPv6* en una importante técnica para realizar comunicaciones personales, lo que trajo ventajas en cuanto a movilidad se refiere [8].

Las soluciones para el soporte y gestión de la movilidad se encuentran disponibles en diferentes capas acorde al modelo de referencia OSI.

- Gestión de movilidad en la capa de aplicación: En esta capa se elimina la necesidad de contar con protocolos de movilidad de las capas inferiores por lo que las mismas no se tienen en cuenta. Aunque resulta apropiado para algunos servicios, la movilidad en este nivel puede tomar más tiempo del adecuado, dado el lento procesamiento de información que se tiene. En la actualidad se soporta movilidad en esta capa para aplicaciones basadas en el Protocolo de Inicio de Sesión (*SIP - Session Initiation Protocol*¹) [4][9][10].
- Gestión de movilidad en la capa de transporte: En esta capa, una comunicación extremo a extremo puede mezclar tanto conexiones cableadas como inalámbricas, por lo que el control de congestión se convierte en una tarea compleja dadas las diferentes características de la red. Para el soporte de movilidad a este nivel, se presentan 2 soluciones: el Protocolo de control de transmisión de flujo (*SCTP - Stream Control Transmission Protocol*) y la arquitectura MSOCKS (del esquema SOCKS, abreviación de "SOCKeT S"). El primero, un protocolo orientado a conexión, extremo a extremo, es el encargado de soportar transporte de datos en una secuencia de flujos independientes. Provee confiabilidad, control de flujo y secuenciación como TCP y utiliza la orientación a datagrama de UDP. El segundo, es una arquitectura para la gestión de movilidad en la capa de transporte, que permite a las aplicaciones cliente-servidor usar de manera transparente los servicios de un firewall por medio de servidores proxy [4][11].

Debido al enfoque de este proyecto, se presenta una breve descripción de las soluciones empleadas para la gestión de movilidad en la capa de aplicación y de transporte, pero se centrará el estudio en la movilidad que se desarrolla en la capa de red, ya que es la que permite a los usuarios establecer una comunicación inalámbrica y mantener la conexión aún cuando su terminal este cambiando de punto de acceso constantemente.

¹ SIP es un protocolo extremo a extremo (*end-to-end*), diseñado para iniciar, mantener y terminar sesiones en Internet que

1.1.1 Gestión de Movilidad

La movilidad a nivel de red, o movilidad IP se conoce como la capacidad que tiene un nodo de moverse de una red a otra, manteniendo siempre una misma dirección IP, con el fin de que los paquetes enviados a dicho nodo, lleguen a su destino a pesar de que éste se encuentre alejado de su red principal. Se considera un beneficio para los usuarios poder realizar un desplazamiento sin ningún tipo de conexión física, pero más aún tener la capacidad de moverse hacia redes diferentes, que manejan direcciones de red distintas, manteniendo la comunicación en curso.

En los tipos de movilidad descritos anteriormente: usuario, servicios y terminal, se distinguen dos aspectos fundamentales: la movilidad continua y la movilidad discreta o nomádica. La primera asegura que una conexión activa no se va a interrumpir aún si el nodo cambia de punto de conexión en la red; la segunda le permite a un usuario realizar desplazamientos discretos, es decir, cambiar de ubicación cuando no se tiene ninguna comunicación activa [2][12]. Se considera muy importante ofrecerle a los usuarios movilidad continua, garantizándoles una comunicación sin interrupciones y por lo tanto una conexión más segura, sin limitaciones geográficas y sin problemas con la diversidad de tecnologías de red que se pueden encontrar en la actualidad [13].

La gestión de movilidad consiste en dos operaciones fundamentales: la gestión de localización y la gestión de *handover* [4][11][14].

- Gestión de localización: es una operación utilizada para localizar a un nodo móvil o a un usuario con el fin de iniciar y establecer una comunicación, aún cuando su ubicación pueda estar en continuo cambio. Los mecanismos incluidos en la gestión de localización son: Registro de Localización (*Location registration*) y Búsqueda de Localización (*Location paging*). La primera, es el procedimiento en el que el nodo móvil informa a la red y a otros nodos de su nueva localización a través de mensajes especiales, actualizando la información correspondiente a la localización y almacenándola en bases de datos de la red. La segunda, también conocida como búsqueda de la ubicación, intenta encontrar la posición exacta del dispositivo móvil. Esto debido a que en muchas ocasiones, la información de localización almacenada en las bases de datos solo corresponde a una posición aproximada del dispositivo.

La gestión de localización incluye entre otros direccionamiento, estructuras de bases de datos y esquemas de búsqueda (*paging*).

- Gestión de *Handover* (*Handover* - Traspaso): esta operación se encarga de controlar el cambio que puede realizar un dispositivo móvil desde un punto de acceso a otro, con el fin de mantener sus conexiones activas funcionando correctamente. Se realizan 3 funciones básicas en la gestión de *handover*: Activación del *Handover* (*Handover Triggering*), Restablecimiento de la Conexión

(*Connection re-establishing*) y Enrutamiento de Paquete (*Packet Routing*). La primera, se encarga de iniciar el proceso de *Handover* dependiendo de algunas condiciones como: deterioro de la intensidad de la señal, sobrecarga de trabajo, disminución del ancho de banda, disponibilidad de nuevas y mejores conexiones, características del flujo de datos, cambios en la topología de la red, entre otros. La segunda, es la encargada de generar una nueva conexión entre el nodo móvil y el nuevo punto de acceso. Su principal tarea está en encontrar y asignar recursos para la nueva conexión. La tercera, hace el cambio de ruta hacia la nueva posición del nodo para la entrega de paquetes, antes de que esta conexión se haya establecido exitosamente.

Dadas las operaciones fundamentales para la correcta gestión de movilidad en un contexto basado en IP, se definen diferentes tipos de escenarios donde se puede llevar a cabo dicha gestión. Estos escenarios se describen a continuación.

1.2 ESCENARIOS DE MOVILIDAD IP

La topología de red que tiene actualmente Internet es muy compleja. En sus inicios, las redes se diseñaban con una topología jerárquica, ahora, también se interconectan lateralmente (dentro de un mismo nivel de la jerarquía). Las redes privadas contribuyen a esta complejidad cuando se conectan a Internet de diversas formas, ya sea jerárquicamente con un proveedor de servicios, lateralmente con otras organizaciones, e incluso cuando dichas redes privadas abarcan todos los niveles jerárquicos al tratarse de organizaciones grandes establecidas en varios países. Este último caso es posible gracias al uso de Redes Privadas Virtuales. La Figura 1.1 muestra de forma simple estas características.

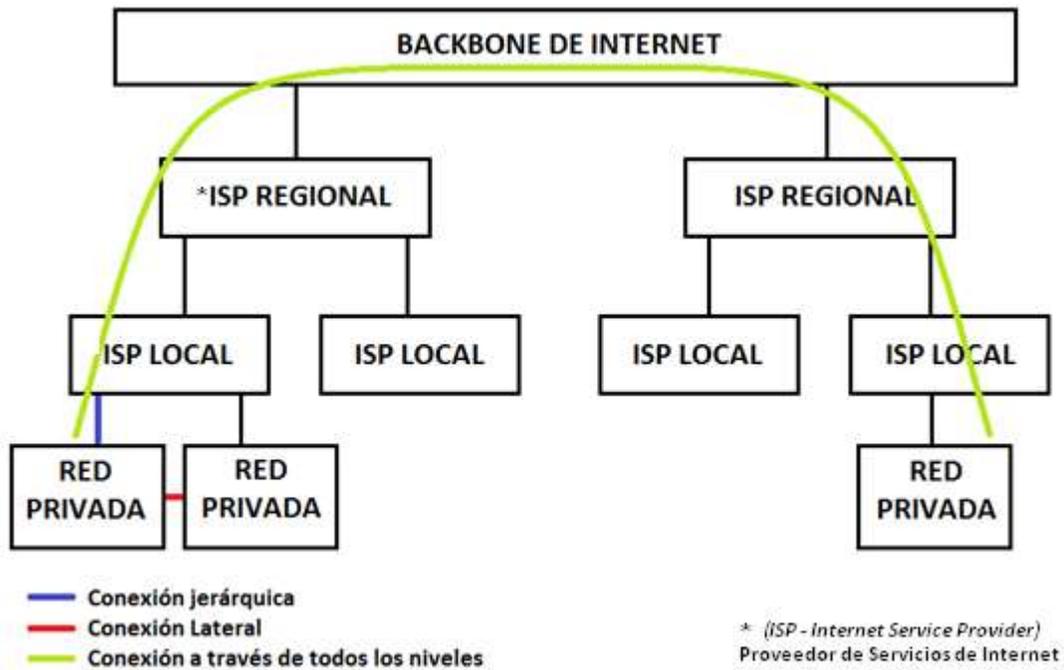


Figura 1.1 Jerarquía e interconexiones en Internet. Adaptado de [15]

Definir un conjunto de escenarios de movilidad con la complejidad actual de las redes no es una tarea simple. No es posible especificar las condiciones que determinan un escenario y que esas condiciones se apliquen de igual forma en cualquier lugar. Por el contrario, las fronteras que delimitan a un escenario de movilidad de otro, están sujetas al contexto de estudio del escenario. En la literatura de movilidad se definen dos escenarios o tipos de movilidad: macromovilidad y micromovilidad [16][17]. Para establecer los límites entre éstos se define lo que es un Dominio Administrativo.

Un Dominio Administrativo (*AD - Administrative Domain*) “es un grupo de hosts, enrutadores, y redes que se operan y gestionan por una sola organización. El enrutamiento dentro de un Dominio Administrativo se basa en un plan técnico consistente. Un Dominio Administrativo se percibe desde el exterior, para propósitos de enrutamiento, como una entidad unificada cuya estructura interna no tiene importancia. La información proveniente de otro Dominio Administrativo es de menor confianza que la del propio dominio [18]”.

1.2.1 Macromovilidad

Es un escenario de movilidad donde un nodo se mueve entre redes que se encuentran en distintos Dominios Administrativos.

Este tipo de movilidad generalmente está relacionado con movilidad en áreas extensas, sin embargo, la compleja topología de Internet y las diferentes tecnologías de acceso, permiten que se presente macromovilidad en áreas geográficas pequeñas. Un mejor enfoque, diferente al de la distancia geográfica, es la distancia topológica en la infraestructura de red entre los enrutadores de acceso involucrados en el movimiento del nodo [19]. De esta forma, un número considerable de saltos entre dichos enrutadores puede considerarse un escenario de macromovilidad, aun cuando se encuentren en la misma área geográfica.

Ejemplos de macromovilidad se presentan cuando un móvil realiza un traspaso entre dos operadores de red diferentes o cuando se realiza movimiento de una red cableada a una red de área local inalámbrica (*LAN – Local Area Network*) de distintos Proveedores de Servicio a Internet (*ISP – Internet Service Provider*).

Las soluciones que se brindan para macromovilidad se encuentran en diferentes esquemas. En cuanto a la capa de red los protocolos propuestos para Macromovilidad IP son *Mobile IPv4* y *Mobile IPv6*.

1.2.2 Micromovilidad

Es un escenario de movilidad donde un nodo se mueve entre subredes de un solo Dominio Administrativo.

Un escenario de micromovilidad generalmente se relaciona con áreas geográficas pequeñas, sin embargo, al igual que en macromovilidad, la compleja topología de las redes actuales, permite que este tipo de movilidad se presente en áreas extensas. Ejemplo de esto es un Dominio Administrativo que se extiende por varios países. El número de saltos entre enrutadores en este escenario es menor que en el de macromovilidad.

Los movimientos del nodo móvil son más frecuentes en un escenario de micromovilidad, por lo tanto las soluciones propuestas para macromovilidad (*Mobile IP*), se vuelven incompatibles aquí [20]. En su reemplazo, se proponen otros protocolos, muchos de ellos derivados de *Mobile IP*, por ejemplo *Proxy Mobile IP*, *Hierarchical Mobile IP*, más apropiados para ambientes de micromovilidad.

En la Figura 1.2 se muestra un ejemplo básico de los dos escenarios de movilidad IP.

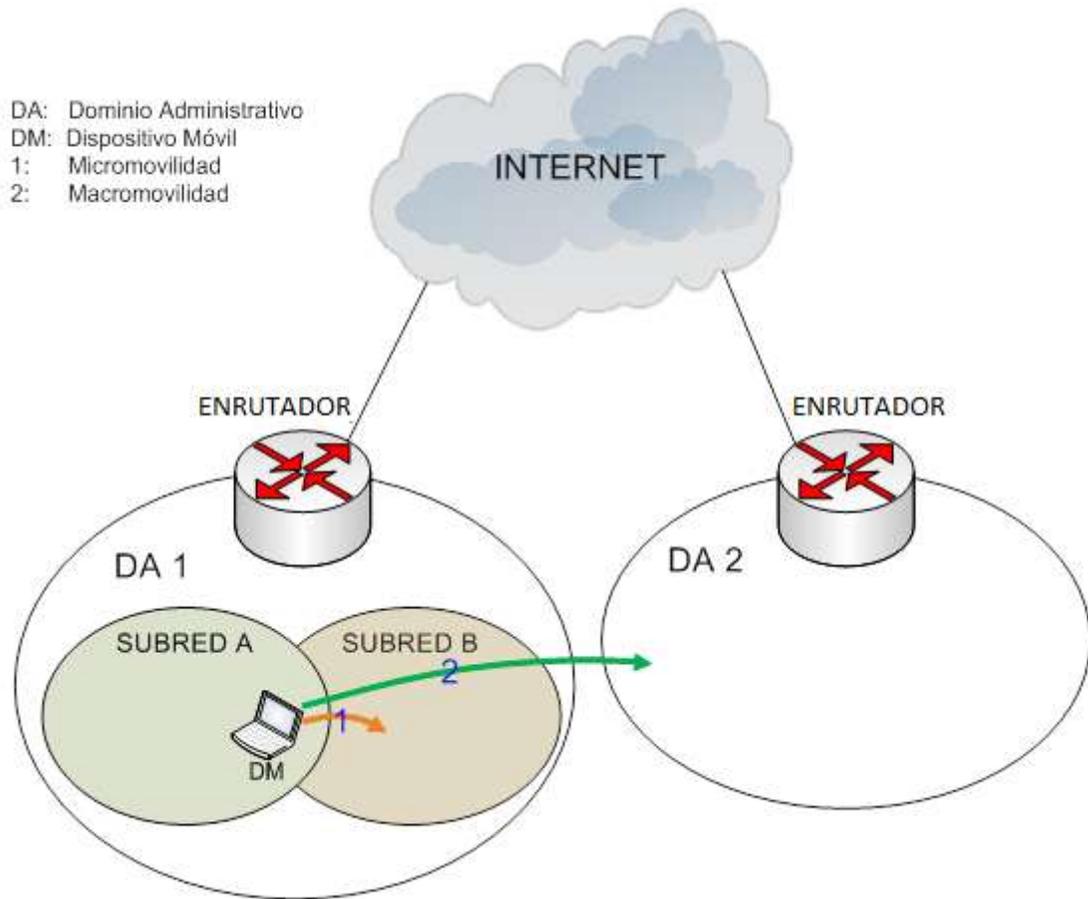


Figura 1.2. Escenarios de movilidad IP: Macromovilidad IP y Micromovilidad IP.
Adaptado de [15].

1.3 HANDOVER

Un ambiente de movilidad se caracteriza porque los nodos móviles realizan cambios de punto de acceso. Es probable que si no se tienen buenos mecanismos que controlen este tipo de cambios se presenten retardos, pérdidas de paquetes e inclusive una desconexión total de la comunicación, afectando así la calidad del servicio prestado.

El proceso en el cual estos cambios tienen lugar se denomina *handover*.

El *handover* es el proceso que permite mantener continuidad en una comunicación establecida por un nodo, mientras que este cambia de punto de acceso a la red.

Existen diferentes tipos de *handover* y se clasifican según diferentes aspectos.

Acorde al nivel del modelo OSI en que opera, el *handover* puede ser de capa dos (L2, *Layer 2*) y de capa tres (L3, *Layer 3*):

- Un *handover* L2 se realiza cuando el nodo móvil cambia de un punto de acceso a otro, pero éstos están conectados a un mismo enrutador de acceso. Debido a que este tipo de *handover* ocurre en la capa de enlace, es transparente a la capa de red (la dirección IP del nodo no cambia), y por lo tanto no se necesita utilizar ningún mecanismo de movilidad [21][22].
- Un *handover* L3 implica un *handover* L2 y además un cambio de enrutador de acceso. A diferencia del caso anterior, en este traspaso se produce un cambio de subred por lo que está involucrada la capa de red (hay un cambio de dirección IP en la interfaz del nodo), así como los protocolos y mecanismos de movilidad [17][22].

Desde el punto de vista de tecnologías de acceso a la red el *handover* puede ser horizontal o vertical. En ambos casos se puede presentar en las capas L2 o L3 [17]:

- *Handover Horizontal*, se presenta cuando un nodo móvil realiza un cambio de punto de acceso entre dos redes que utilizan la misma tecnología de acceso, por ejemplo entre dos Puntos de Acceso (*Access Point*) 802.11g. Es llamado también *Handover Intra-Tecnología*.
- *Handover Vertical*, se presenta cuando un nodo móvil realiza un cambio de punto de acceso entre redes que utilizan diferentes tipos de tecnologías de acceso, por ejemplo entre una red Wi-Fi y una UMTS. Es llamado también *Handover Inter-Tecnología*.

El *handover* constituye un proceso de importancia en la gestión de la movilidad, es por eso que este trabajo se centra en el estudio de las soluciones propuestas que giran en torno a él. Con el objetivo de determinar cuál es el rendimiento de esas soluciones y realizar una comparación entre ellas, se deben definir parámetros de medida y factores que intervienen para que una comunicación tenga buena calidad de servicio. Este es el objetivo del siguiente capítulo.

CAPITULO II. FACTORES QUE INCIDEN EN LA CALIDAD DE UN SERVICIO DE TIEMPO REAL

2.1 INTRODUCCIÓN

Anteriormente, la Calidad de Servicio (QoS – *Quality of Service*) no era una prioridad en la prestación de servicios de datos, ya que estos correspondían a lo que se denomina tráfico de “mejor esfuerzo” (*BE – Best Effort*). Para este tipo de tráfico no se requería garantía alguna de calidad de servicio ya que no demandaba valores críticos respecto al retardo y variación de retardo, aunque sí respecto a la integridad de los mismos. Servicios tales como el correo electrónico y las descargas de audio y vídeo almacenado no requerían tradicionalmente el suministro de información en tiempo real, lo que quiere decir que el tamaño del canal, flujo de paquetes, consistencia del servicio y retardo no estaban especificados o no eran necesarios.

En la actualidad y gracias al avance de la tecnología, la información digitalizada se transporta por medio de paquetes IP. Esto obliga a los proveedores de servicios a satisfacer los estrictos requerimientos de cada uno de los servicios que demandan los usuarios finales, garantizando la prestación de los mismos con los niveles de calidad exigidos. De esta manera se establece el concepto de Calidad de Servicio – QoS, que aunque definido y entendido de diversas maneras, converge hacia el establecimiento de parámetros o condiciones mínimas con las cuales la red debe cumplir para que un servicio se ejecute sin ningún tipo de falencia (pérdidas, mala calidad de audio, mala calidad de video, etc.). Una red con QoS prioriza los recursos disponibles (ancho de banda, capacidad de procesamiento, encolado, etc.), asignándolos a cada conjunto de paquetes de acuerdo a sus requerimientos [23].

Los servicios ofrecidos y desplegados en redes fijas empiezan a ser implementados sobre redes inalámbricas, sin embargo, debido a la variabilidad que presenta un ambiente de este tipo, algunas veces se hace complejo cumplir con las exigencias de calidad que requieren. Generalmente esto se debe a que un terminal móvil realiza cambios frecuentes de punto de acceso, lo que puede perjudicar la calidad percibida de cualquier servicio prestado en un ambiente inalámbrico. Problemas de este tipo son menos frecuentes cuando las comunicaciones se desarrollan en ambientes de micromovilidad ya que la conexión se desenvuelve solamente en un dominio de red. A pesar de esto, la tendencia actual a la utilización masiva de servicios de tiempo real, hacen de la prestación de los mismos un proceso complejo exponiéndolos así a pérdidas de paquetes y retardos, entre otros problemas.

Con el fin de tener claridad en los aspectos mencionados, en este capítulo se abarcan las definiciones de algunos de ellos, así como los factores y parámetros a tener en cuenta para la correcta prestación de un servicio de tiempo real.

2.2 CALIDAD DEL SERVICIO – QoS

La calidad en un contexto general se define como “*todas las características de una entidad que inciden en su capacidad de satisfacer las necesidades indicadas e implícitas*” (ISO 8402) [24].

Por consiguiente, el concepto de Calidad de Servicio o QoS, es el que establece una serie de condiciones que deben cumplirse con el fin de que la calidad de funcionamiento de un servicio de telecomunicaciones satisfaga los requerimientos y necesidades del usuario final. Este concepto es abordado de distintas maneras dependiendo del punto de vista con el que se mire. Sin embargo, en este proyecto se considera el enfoque de QoS propuesto por los organismos de regulación ITU y ETSI.

2.2.1. Calidad de Servicio según los organismos de regulación ITU/ETSI

Los organismos de regulación ITU y ETSI, basados en la recomendación E. 800 [25], definen a la QoS como: “*La totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio*” [24][26].

Para la definición anterior se establecen criterios utilizados para evaluar la calidad de las funciones que todo servicio debe soportar. De esta manera, se hace una extensión del concepto de QoS analizándolo desde 4 perspectivas diferentes [24][27].

- **QoS Requerida por el Usuario/Cliente (QoSR – Quality of Service Required):** define el nivel de calidad que requiere un usuario para estar satisfecho con un servicio en particular. Estos requerimientos generalmente se expresan en un lenguaje corriente que facilite su entendimiento por parte de un usuario final. Posteriormente el proveedor de servicio deberá traducirlos a terminología técnica de desempeño de red.
- **QoS Ofrecida/Planificada por el Proveedor del Servicio (QoSO – Quality of Service Offered):** es el nivel de calidad que el proveedor espera ofrecer a sus usuarios finales. Esta forma de QoS es útil para la planificación, la definición y especificación de los acuerdos de nivel de servicio. Cada servicio tendrá su propio conjunto de parámetros a partir de los cuales se estimará el funcionamiento del mismo.
- **QoS Proporcionada/Lograda por el Proveedor de Servicio (QoSD – Quality of Service Delivered):** es el nivel de calidad real alcanzado y entregado al usuario final. Se estima mediante valores que son asignados a parámetros que deben ser

idénticos a los especificados para la QoS ofrecida, con el fin de compararlos y evaluar el nivel de calidad de funcionamiento logrado.

- **QoS Experimentada/Percibida por el Cliente/Usuario (QoSP – Quality of Service Perceived):** es una declaración en la que se expresa por parte de los usuarios finales el nivel de calidad que ellos consideran haber experimentado y que se expresa en función del grado de satisfacción de los mismos.

Para garantizar los mejores niveles de QoS en los servicios entregados a los usuarios es necesario que el concepto de Calidad de Servicio se complemente siempre desde las cuatro perspectivas nombradas anteriormente y que se encuentren en una continua realimentación para lograr los objetivos propuestos. Dado esto, se hace necesario agregar una consideración complementaria propuesta por la ETSI [26], en la que se plantea una relación de las 4 perspectivas expresadas por la ITU-T con el desempeño de la red, de manera que la QoS ofrecida y la QoS lograda por el proveedor tienen dependencia directa con los factores del mismo.

La Figura 2.1 ilustra la relación existente entre los diferentes contextos de la calidad de servicio.

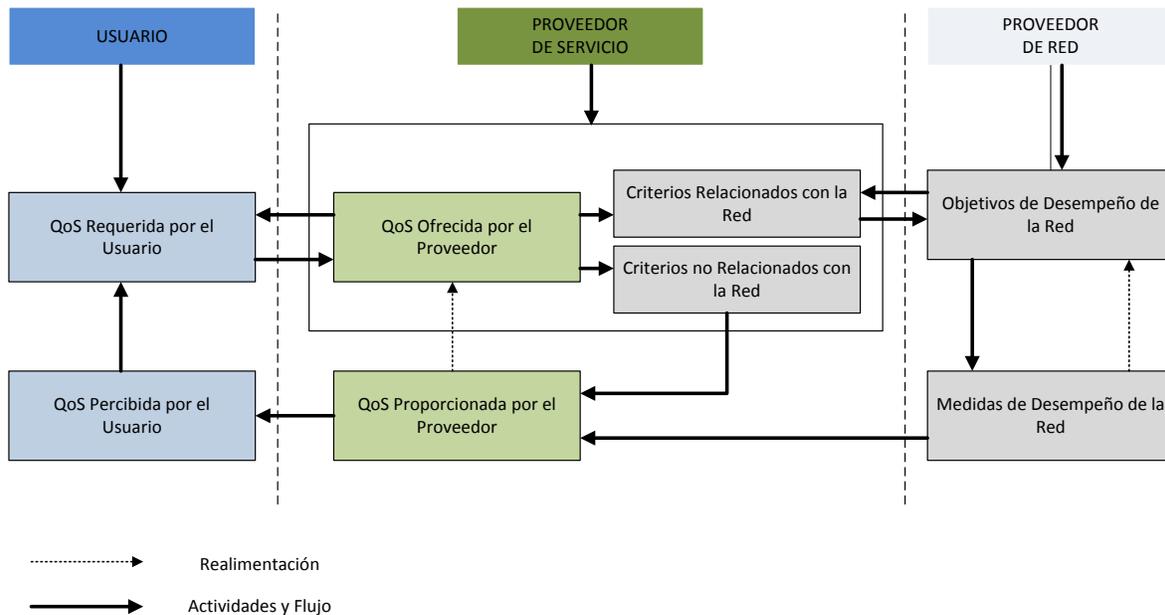


Figura 2.1. Relación entre diferentes perspectivas de QoS. Adaptado de [26]

La QoS es asunto tanto del usuario quien la requiere y la percibe, como del proveedor de servicio quien la ofrece y la proporciona. El proveedor de servicios en la mayoría de los casos, es a su vez el proveedor de red, por lo que tiene responsabilidad por la QoS. En la

Figura 2.1, se observa la separación entre proveedor de servicios y el proveedor de red y las relaciones existentes entre ellos.

2.3 TRÁFICO EN LA RED

Actualmente con la diversidad de servicios y aplicaciones ofrecidas por los proveedores, los requerimientos de los usuarios son cada vez más exigentes en cuanto a la prestación de los mismos se refiere y más aún cuando se trata de servicios que se prestan en tiempo real, por lo que se debe brindar un nivel de calidad adecuado para los mismos. Por lo tanto, es importante conocer los 2 tipos de tráfico que debe soportar una red basada en IP y las aplicaciones basadas en los mismos [28][29][30].

2.3.1. Tráfico elástico

Este tipo de tráfico es capaz de ajustarse a variaciones de retardo y rendimiento, de tal manera que se satisfagan las necesidades que exigen las aplicaciones. Sin embargo, es necesario definir mecanismos de control de calidad que respondan a las necesidades requeridas por la aplicación.

Este tráfico es el admitido por las redes TCP/IP, usando como protocolos de transporte a UDP y TCP. Para el primero, una aplicación utiliza tanta capacidad como haya disponible, compatible con la velocidad de la aplicación que genera los datos. En el segundo, una aplicación utiliza tanta capacidad como haya disponible hasta la máxima velocidad de datos que el receptor pueda aceptar. El tráfico elástico no admite pérdidas.

Los protocolos que generan tráfico elástico son FTP, SMTP, SSH, SNMP y HTTP.

2.3.2 Tráfico inelástico

El tráfico inelástico difícilmente se adapta a los cambios en el retardo y el rendimiento a través de un conjunto de redes. Requiere un trato preferencial y en muchas ocasiones es difícil ajustar las necesidades demandadas por una aplicación, por lo que generalmente estas deben especificarse antes de iniciar alguna transmisión. Esto es posible utilizando los campos de la cabecera IP ó un protocolo de reservación de recursos. Admite pérdidas moderadas de paquetes.

El principal ejemplo del tráfico inelástico corresponde a las aplicaciones en tiempo real. Estas demandan de ciertos requerimientos que las hacen complejas, sin embargo, se utilizan técnicas para su tratamiento con el fin de que sea prestado siempre con las

mejores condiciones. Estas generalmente tienen que ver con: rendimiento, retardo, variación de retardo, pérdida de paquetes, entre otros [28].

Las aplicaciones que generan tráfico inelástico son: voz conversacional, audio en tiempo real, videotelefonía, entre otros.

La prestación de este tipo de servicios está ligada a satisfacer requisitos de telecomunicaciones específicos que presentan en la actualidad los clientes de los mismos [31].

Sin embargo, y dados los dos conceptos anteriores, en [32] se destaca que desde el punto de vista de aplicación se generan las siguientes clasificaciones dependiendo de las aplicaciones y el tipo de tráfico: elástico o inelástico, e interactivo y no interactivo. Por lo tanto resultan 4 tipos:

- Elástico no Interactivo.
- Elástico Interactivo.
- Inelástico no Interactivo (*streaming*).
- Inelástico Interactivo (también llamado conversacional o tiempo real).

La Tabla 2.1 indica algunos ejemplos de aplicaciones que clasifican dentro de estas 4 categorías.

Elástico		Inelástico	
No Interactivo	Interactivo	No Interactivo	Interactivo
Descarga de Archivos.	Navegación por la Web.	Radio Difusión.	VoIP.
Copia de Seguridad Remota.	Telnet/SSH.	Video sobre Demanda.	Telefonía.
Compartir Archivos P2P.	Grid Computing.	Televisión en Vivo.	Videoconferencia.
E-mail.	Control de Red.		Video-Chat.
Almacenamiento de Datos Médicos.			Juegos en Línea.
Distribución Digital.			Cirugía Remota.
			Comunicaciones de Emergencia.

Tabla 2.1. Tipos de tráfico y aplicaciones relacionadas. Tomada de [32].

Consecuente con lo anterior, la recomendación G.1010 de la ITU, brinda una organización general acerca de las aplicaciones de comunicación existentes según la tolerancia que tengan las mismas a las pérdidas de paquetes y al retardo, como se observa en las Figuras 2.2 y 2.3 respectivamente.

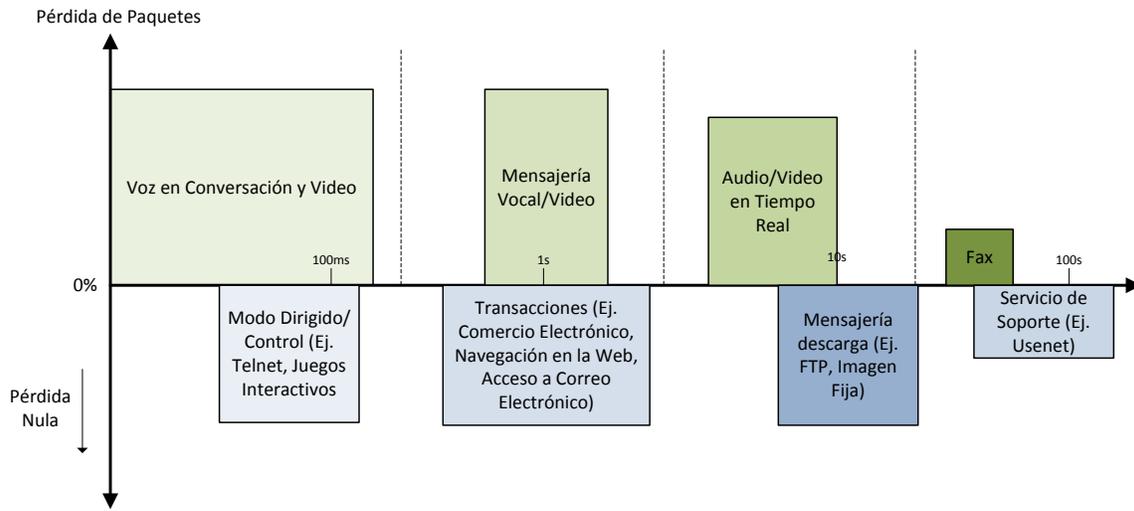


Figura 2.2. Clasificación de las aplicaciones según la tolerancia a pérdida de paquetes. Tomada de [33].

Tolera Errores	Voz en Conversación y Video	Mensajería Vocal/Video	Audio/Video en Tiempo Real	Fax
No Tolera Errores	Modo Dirigido/Control (Ej. Telnet, Juegos Interactivos)	Transacciones (Ej. Comercio Electrónico, Navegación en la Web, Acceso a Correo Electrónico)	Mensajería descarga (Ej. FTP, Imagen Fija)	Servicio de Soporte (Ej. Usenet)
	Interactivo (Retardo << 1s)	Pronta Respuesta (Retardo ~ 2s)	Oportuno (Retardo ~ 10s)	Oportuno (Retardo >> 10s)

Figura 2.3. Clasificación de las aplicaciones según la tolerancia a retardos. Tomada de [33].

2.4 FACTORES QUE AFECTAN EL DESEMPEÑO DE SERVICIOS PRESTADOS EN TIEMPO REAL

Con el fin de examinar los aspectos de Calidad de un servicio en tiempo real, en un ambiente móvil e inalámbrico, basado en IP, es necesario conocer los factores que en algún momento podrían afectar una comunicación, produciendo fallas y errores e incluso la desconexión de la misma.

Producto del análisis realizado en el presente proyecto, la Figura 2.4, presenta un diagrama conceptual que describe las diferentes categorías en las que se propone la clasificación de los factores que pueden influir en la prestación exitosa de un servicio en tiempo real durante una comunicación en un ambiente de micromovilidad IPv6.

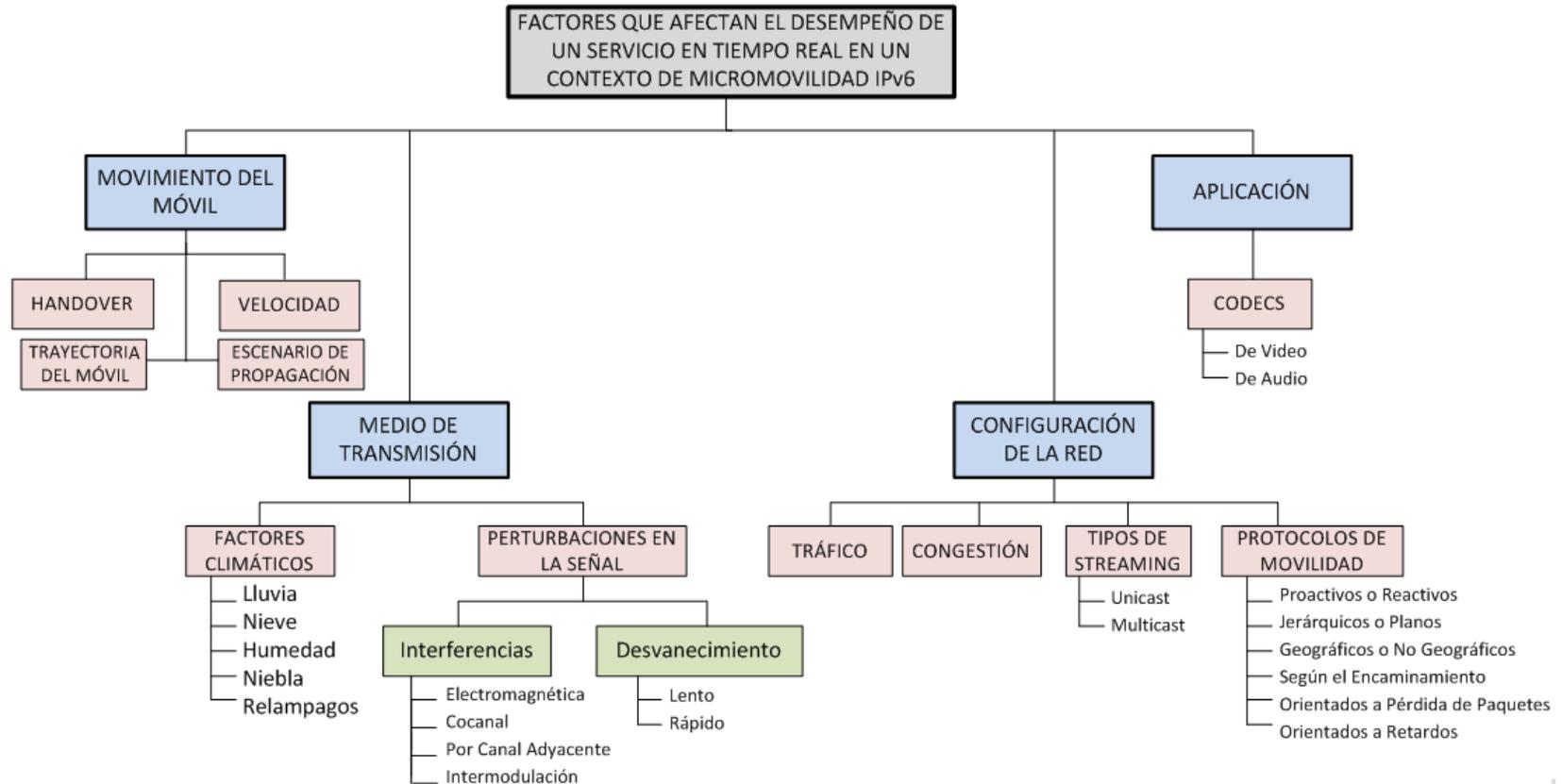


Figura 2.4. Diagrama conceptual de los factores que afectan el desempeño de un servicio en tiempo real. Fuente: los autores.

A continuación se definen cada uno de los factores y de los elementos que lo componen.

2.4.1. Movimiento del móvil

Los siguientes factores están relacionados exclusivamente con las características del movimiento del móvil. Estos son:

- **Handover:** es el proceso por el cual el móvil realiza un cambio de punto de acceso sin perder la continuidad en la conexión previamente establecida. Durante el recorrido del dispositivo móvil este puede atravesar grandes distancias y por lo tanto hacer cambio de punto de acceso varias veces.
- **Trayectoria del móvil:** la trayectoria se refiere al camino que sigue el móvil durante su recorrido. Es importante tener en cuenta este factor ya que de la trayectoria seguida dependerá el número de *handover* que el móvil efectuará. Un móvil puede seguir una trayectoria circular alrededor de un punto de acceso sin necesidad de efectuar ningún *handover*, o puede tener una trayectoria de vaivén en el límite de las áreas de cobertura de dos puntos de acceso, haciendo que efectúe una gran cantidad de *handover*. Si el proceso de *handover* se presenta pocas veces durante una comunicación ocasionará una breve interrupción de la misma, mientras que si la frecuencia en la que estos se presentan es considerable, la comunicación se puede tornar inestable o se puede perder por completo.
- **Velocidad:** debido a la velocidad del móvil se produce un desplazamiento de frecuencia en la portadora de la señal. Esto se conoce como Efecto Doppler. El desplazamiento está dado por:

$$f' = \pm \frac{v}{c} f_0$$

Ecuación 2.1. Velocidad del Nodo Móvil (*MN – Mobile Node*)

Donde:

f' : Desplazamiento Doppler

v : Velocidad del móvil.

c : Velocidad de la luz

f_0 : frecuencia de la portadora.

El efecto Doppler y por lo tanto la velocidad del móvil afectan de forma diferente a las diferentes tecnologías inalámbricas existentes para la transmisión de datos

(802.11g, 802.16e, etc.). Para algunas el efecto es despreciable, mientras que en otras es una limitación importante.

- **Escenario de Propagación:** es importante tener en cuenta el escenario en el cual se está propagando la onda, debido a que entre el emisor y el receptor la misma puede propagarse por múltiples caminos (Propagación Multitrayecto), lo que puede causar desvanecimiento de la misma debido a los fenómenos de difracción y reflexión.

2.4.2. Medio de transmisión

En el medio de transmisión se producen perturbaciones que pueden alterar la calidad de la señal de información que circula por la red y por ende pueden afectar la calidad del servicio y más aún si se trata de uno en tiempo real.

- **Factores climáticos:** los fenómenos climáticos-ambientales son factores que si se presentan de manera continua y/o severa pueden afectar cualquier tipo de comunicación y más aún si se trata de una comunicación inalámbrica en un ambiente de micromovilidad. Esto es debido a que en este tipo de ambientes, las señales viajan como ondas de radio por el aire.

Entre los factores que más afectan las comunicaciones móviles se encuentran: la lluvia, la nieve, la humedad, la niebla y los relámpagos.

- **Perturbaciones en la Señal:** existen diferentes tipos de perturbaciones que pueden afectar una señal durante la comunicación. Estas se caracterizan por degradar la misma, reflejándose esto en la señal recibida en el destino. Las perturbaciones más importantes son:
 - **Electromagnética (*EMI – Electromagnetic Interference*):** es cualquier señal o emisión que degrada, obstruye o interrumpe de forma repetida un servicio de comunicación por radio. La interferencia electromagnética que más afecta a los sistemas de telecomunicaciones es el ruido. Este es una perturbación que degrada la señal original transmitida comprometiendo la calidad de funcionamiento del sistema. Es imposible eliminarlo totalmente de los canales radioeléctricos debido a que los componentes del mismo no son perfectos, sin embargo se puede reducir lo suficiente para que la calidad de la comunicación sea aceptable. Múltiples causas lo ocasionan, entre ellas están los componentes electrónicos, el ruido térmico de las resistencias, las interferencias de señales externas, entre otras.

- Interferencia cocanal: son señales interferentes causadas por un transmisor que emite en el mismo canal que la señal útil, resultando particularmente perjudiciales cuando se planifica erróneamente el re-uso de canal.
- Interferencia por canal adyacente: es causada por niveles de potencia no deseados provenientes de transmisores que emiten en canales adyacentes a la de la señal útil y que no son eliminados por los filtros del receptor.
- Intermodulación: se refiere a la modulación de amplitud de la señal transmitida, por la presencia de señales no deseadas en un sistema de telecomunicaciones con comportamiento no lineal. Es causada por fuentes de naturaleza, localización y comportamiento desconocido. Generalmente entre sus causantes se encuentran contactos entre metales diferentes, elección de los materiales conductores, corrosión, suciedad, entre otros.
- ✓ Desvanecimiento: es la atenuación que sufre la señal en ciertos medios de propagación. Este puede variar según el tiempo y la posición geográfica, entre otros. Existen 2 tipos de desvanecimiento.
 - Desvanecimiento Lento o por sombra: es aquel causado por obstáculos presentes en el camino de la señal, que ocultan la trayectoria de la misma entre el transmisor y el receptor, afectando su correcta propagación.
 - Desvanecimiento Rápido: es causado por la propagación multi-trayecto. Se puede dar debido a la presencia de reflectores en el camino entre el transmisor y el receptor, creando múltiples caminos que la señal puede seguir.

2.4.3. Configuración de la red

Es muy importante tener en cuenta la configuración de red ya que de esto depende el correcto funcionamiento que realice la misma durante la transmisión de unidades de información, y más aún cuando éstas presentan requerimientos en tiempo real. Una incorrecta configuración de la red puede provocar pérdidas de paquetes afectando la calidad del servicio prestado a los usuarios. En este apartado se tratarán los factores más influyentes en la configuración y el desempeño de la red.

- **Tráfico:** hace referencia a todas las unidades de información que circulan por la red. Es fundamental que éstas no sean tratadas de la misma manera, debido a los requerimientos de algunos servicios, como los de tiempo real. Esto permite aplicar los mecanismos de control apropiados para cada unidad de información con el fin

de que el servicio resulte satisfactorio para el usuario final. La recomendación Y.1221 de ITU-T [34], explica diferentes procedimientos y funciones para el control del tráfico en redes basadas en IP.

- **Congestión:** según [34][35], la congestión se define como un estado de los elementos de red durante el cual la misma no es capaz de satisfacer los objetivos de calidad de un servicio y cumplir los compromisos de la QoS establecida para el tráfico cursante en ese momento. Generalmente esta situación se presenta debido a que diferentes fuentes de información inyectan continuamente tráfico a la red con diferentes tasas, provocando más tráfico del que sus elementos son capaces de soportar.

En un periodo de congestión de la red se pueden perder paquetes, lo que influye en la adecuada prestación de un servicio. Para esto, existen métodos para el control de la congestión, explicados en la recomendación Y.1221 de la ITU-T [34].

- ✓ Control de Tráfico y de Congestión: la función principal de estos métodos de control es proteger la red y el tráfico que accede a la misma con el fin de alcanzar los objetivos de funcionamiento de la red y cumplir con los compromisos de QoS para el tráfico establecido. Además, estos controles optimizan el uso de recursos de la red.
 - Control de Tráfico: hace referencia a un conjunto de funciones como el control de admisión, la gestión de recursos de red, el control de parámetros de tráfico, entre otros, que permiten el control del flujo de los paquetes. Lo que se pretende con el control de tráfico es atender los requerimientos de calidad de servicio de los usuarios, asegurando la utilización eficiente de la red.
 - Control de Congestión: en el momento en que las funciones de control de tráfico no se comporten de la manera adecuada, se puede producir congestión. Es en ese instante donde las funciones de control de congestión reaccionan a la congestión de la red, con el fin de minimizar su intensidad, dispersión y duración.
- **Tipo de *streaming*:** es importante conocer el tipo de *streaming* que se va a utilizar con el fin de saber si el servicio va a ser prestado a un solo usuario o a varios al mismo tiempo.
 - ✓ Unicast: en este tipo de *streaming*, cada usuario inicia su propio *stream*, independientemente de si el servicio es demandado por más de uno de ellos. En ese caso se crean muchas conexiones entre el servidor y los usuarios (una

conexión por cada usuario), requiriendo el servidor un ancho de banda mucho mayor para poder soportar la cantidad de conexiones uno a uno. Además, esto genera mucho más tráfico en red, dando paso a la posibilidad de que se cree congestión, lo que podría afectar la prestación de cualquier servicio de tiempo real.

- ✓ Multicast: esta técnica de *stream* es mucho mejor ya que reduce en gran cantidad el tráfico en la red y evita la congestión en los enrutadores, esto gracias a que se utiliza una única conexión entre el servidor y un grupo específico de usuarios (grupo multicast) que han demandado el servicio, lo que quiere decir que un único *stream* se comparte entre diferentes usuarios. De esta manera, el ancho de banda requerido en la red para prestar los servicios es menor.
- ✓ Broadcast: aunque utiliza la misma técnica que multicast, se diferencia de éste, en que cualquier usuario puede recibir el servicio, sin necesidad de pertenecer a un grupo específico, como lo requiere el caso anterior.
- **Protocolos de movilidad:** debido al ambiente cambiante en el que se desarrollan las comunicaciones móviles, es necesario conocer qué tipo de protocolos existen y cuáles se adaptan mejor al medio en un momento dado, de esta manera se pueden escoger el o los protocolos que lo favorezcan, haciendo la prestación de cualquier servicio por este medio más eficiente. Dependiendo de sus características, los protocolos se pueden clasificar de la siguiente manera [36]:
 - ✓ Proactivo o Reactivo: en los primeros se envía información de encaminamiento periódicamente, de tal manera que un nodo pueda comunicarse con cualquier otro nodo de la red en un momento dado. Esto, aunque proporciona una rápida respuesta ante solicitudes de ruta, introduce sobrecarga en la red con información de control. Por otro lado, los reactivos solo crean rutas cuando es necesario. De esta manera aunque la sobrecarga es mucho menor, los retardos en el establecimiento de rutas son mayores.
 - ✓ Jerárquico o Plano: en los protocolos jerárquicos los nodos pertenecen a diferentes niveles y su función en la retransmisión depende del nivel en el que se encuentre. En los planos, los nodos se encuentran en el mismo nivel por lo que tienen las mismas funciones y responsabilidades.
 - ✓ Geográficos o No geográficos: en este tipo de protocolos es necesario tener en cuenta la posición geográfica exacta de cada nodo para poder realizar el encaminamiento.

- ✓ Encaminamiento en el origen o encaminamiento salto a salto: en los protocolos con encaminamiento en el origen, cada paquete sabe el camino que debe seguir hasta llegar a su destino. Por otro lado, en el encaminamiento salto a salto, la decisión de qué camino seguir se toma en cada nodo.
- ✓ Orientados a la pérdida de paquetes: estos protocolos fueron diseñados con el fin de minimizar la pérdida de paquetes durante el *handover*. Esto es posible mediante un almacenamiento temporal de los paquetes (*buffering*) en el momento en el que se está realizando el cambio de red.
- ✓ Orientados a los retardos: existen protocolos de movilidad que reducen los tiempos de señalización, disminuyendo de esta manera el retardo presentado durante el *handover*. Sin embargo, la reducción del retardo no implica que durante el *handover* se evite la pérdida de paquetes.

2.4.4. Aplicación

Para un servicio de tiempo real, una característica muy importante a tener en cuenta es la codificación y decodificación. Por este motivo la escogencia del códec se convierte en un factor determinante al momento de transmitir señales por la red.

- **Códecs:** son los encargados de codificar y decodificar la información que transita por la red para la reproducción en un formato apropiado para el usuario del servicio. Generalmente son usados para servicios con requerimientos en tiempo real como por ejemplo una videoconferencia, o para la transmisión de voz sobre IP. El códec determina la tasa de bits necesaria y junto con esto la calidad tanto del video como de la voz.
 - ✓ Códec de Video: este determina la forma en la que una señal de video analógica debe ser convertida a un formato digital comprimido, utilizando el mínimo número de datos posibles (tasa de bits) con el fin de mantener la calidad del contenido. Su objetivo es obtener un almacenamiento mucho menor de la información de video. Entre los códecs más utilizados para video basado en IP están: H.261, H.263, MJPEG, MPEG-1, MPEG-2, MPEG-4 [37].
 - ✓ Códec de Audio: al igual que un códec de video, lo que se busca es convertir la señal de audio analógica a un formato digital comprimido, con fin de ocupar un menor espacio, además de mantener la calidad del contenido. Se puede implementar en software, en hardware o en una combinación de ambos. Los códecs más utilizados para audio basado en IP se dividen en 3 categorías: códecs de forma de onda (PCM, DPCM, ADPCM), códecs vocales y códecs híbridos (G.723 CELP, GSM RPEKTP, VAD) [38].

2.5 PARÁMETROS DE QoS PARA SERVICIOS EN TIEMPO REAL

La provisión de QoS durante una comunicación basada en IP en un ambiente móvil, adquiere la misma importancia que la provisión de la misma en redes fijas. La variabilidad presentada por los ambientes inalámbricos y los exigentes requerimientos en los servicios que se prestan al usuario hacen de este un requisito difícil de cumplir. Sin embargo, los proveedores de servicio se han concentrado en brindar niveles de calidad adecuados para los usuarios, cumpliendo con los requerimientos expresados en el RFC 3583 de la IETF [39][40], para la calidad del servicio.

En este orden de ideas los requerimientos planteados son:

- **Requerimientos de Comportamiento:**
 - Minimizar la Interrupción de la QoS durante un *handover*: en el momento en que ocurre el *handover*, la interrupción en la QoS se puede dar si los paquetes enviados o recibidos por el nodo móvil, llegan al nodo intermedio sin que este conozca los requerimientos de QoS para su correcto envío. Por lo tanto, estos paquetes recibirán un tratamiento por defecto, que puede no resultar beneficioso para la comunicación.
 - Localizar el re-establecimiento de la QoS en el segmento del camino afectado: en algunos casos el *handover* cambia solo un pequeño segmento próximo a un extremo del camino. En estos casos, el mecanismo de QoS debe limitar el alcance del re-establecimiento de la misma, solo al segmento afectado.
 - Liberar el estado de QoS a lo largo del camino antiguo del paquete después del *handover*: el mecanismo de QoS debe proveer algunos medios para liberar cualquier estado de QoS a lo largo del antiguo camino de los paquetes que no se requiera después del *handover*.
- **Requerimientos de Interoperabilidad:**
 - Interoperabilidad con otros protocolos de movilidad: algunos protocolos que son complementarios de *Mobile IP*, han sido o serán definidos en un futuro por la IETF. Los mecanismos de QoS para *Mobile IP* deben tomar ventaja de estos protocolos para optimizar su operación.
 - Interoperabilidad con caminos heterogéneos respecto a mecanismos de QoS: el nuevo camino por el que cursa el flujo del nodo móvil después del *handover* puede atravesar diferentes dominios de red que emplean distintos mecanismos de QoS comparados con aquellos utilizados a lo largo del antiguo camino. Los mecanismos de QoS para *Mobile IP* deben ejecutar un adecuado tratamiento

de los paquetes enviados por o hacia el nodo móvil, a través de los diferentes caminos que los utilizan.

- **Otros Requerimientos:**

- Soporte de QoS a través de múltiples caminos: después de que el nodo móvil realiza el proceso de *Handover*, existen múltiples caminos por los cuales los paquetes pueden ser dirigidos. Es importante que éstos soporten QoS para el debido tratamiento de los paquetes.
- Interacción con el nivel de enlace inalámbrico para el soporte de la QoS: debido a que un gran número de dispositivos móviles que usan *Mobile IP* se conectan a Internet por enlaces inalámbricos, los mecanismos de QoS para *Mobile IP* deben proveer alguna información a las capas de enlace inalámbrico para que soporten la QoS requerida.

Después de describir los requisitos de Calidad que plantea el RFC 3583, para ser considerados en ambientes de micromovilidad IP, la Figura 2.5 muestra los parámetros de QoS que ocasionan que la prestación de un servicio en tiempo real pueda verse afectada en el momento en que se está realizando un *handover* desde un punto de acceso a otro o desde una red hacia otra.

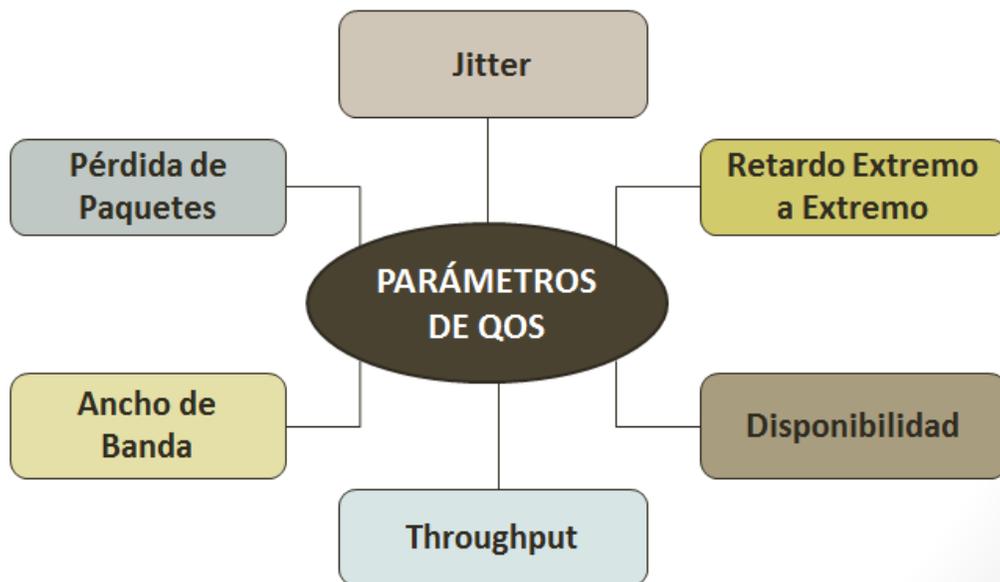


Figura 2.5. Parámetros de QoS para Servicios en Tiempo Real. Fuente: los autores

A continuación se describen los parámetros que encierran los problemas más críticos de desempeño de cualquier servicio en tiempo real. Generalmente estos, se encuentran a nivel de red.

2.5.1. Variación de Retardo (*Jitter*)

. El *Jitter* se conoce como la variación de retardo presentado entre paquetes de datos consecutivos que forman parte de un mismo tráfico, se incluye como parámetro de calidad de funcionamiento, debido a la importancia que tiene para los sistemas de datos empaquetados en la capa de transporte.

Dado que todos los sistemas de transporte presentan *Jitter* es necesario e importante conocer que tipos de servicios son poco tolerantes a estas variaciones de retardo, especialmente aquellos que manejan tráfico con requerimientos en tiempo real. Para estos servicios, generalmente se toman medidas para eliminar o reducir significativamente la variación de retardo percibida por el usuario mediante la implementación de un almacenamiento temporal de paquetes en el receptor, con el fin de enviar sincronizadamente hacia el decodificador los bloques de información que fueron codificados en el emisor, a pesar de que de esta manera se añadan algunos retardos de tiempo fijos [33][41][42].

La ecuación que define el *jitter* está dada por:

$$PDV_i = D_i - D(\min)$$

Ecuación 2.2. Función del *Jitter* [43]

Donde:

PDV(i): Packet Delay Variation – Variación de Retardo (*Jitter*).

D(i): Retardo en un camino del i-ésimo paquete de un flujo.

D(min): Retardo del Paquete con el menor valor de retardo (Mínimo).

Esta ecuación, a diferencia de otras formas de calcular el *jitter* de los paquetes, es la adecuada, según las demostraciones realizadas en [43], para su uso en escenarios donde se presenten continuos cambios de la trayectoria de los paquetes. En este caso, el cambio de trayectoria ocurre después de un *handover*.

2.5.2. Pérdida de Paquetes

Debido a que IP no es un protocolo 100% confiable, puede suceder que en ciertas circunstancias la información transmitida se vea afectada a causa del descarte o pérdida de paquetes por parte de la red. Esta pérdida de información tiene un efecto negativo en

la calidad de la información presentada al usuario final, ya sean datos, imagen, voz o video. Para servicios con requerimientos en tiempo real, el tráfico se implementa sobre UDP (RTP sobre UDP), por lo que el único control que se puede realizar sobre este parámetro es en los extremos de la transmisión. De esta manera, en los códecs se implementan técnicas de corrección de errores para hacer los mismos transparentes al usuario. Sin embargo, hay que tener en cuenta que cuando estas pérdidas superan el umbral establecido (del orden del 3%) o cuando se presentan en ráfagas, este tipo de técnicas deja de ser útil.

Durante la transmisión pueden ocurrir otros errores, por lo que este parámetro también corrige efectos que se puedan presentar debido a la degradación introducida por la codificación del medio. Esto con el fin de conseguir una transmisión más eficaz.

La pérdida de paquetes se asocia a la congestión de la red, al fallo de la conexión, insuficiencia en ancho de banda, entre otros [33][41][42].

2.5.3. Ancho de Banda

Se define como la cantidad de flujo de datos que se puede enviar a través de un elemento de red en un periodo de tiempo dado. Cuando el ancho de banda no es suficiente para soportar la cantidad de datos enviados, se pueden presentar retardos y pérdidas de paquetes.

En una comunicación, los datos viajan a través de una sucesión de conexiones las cuales pueden emplear diferentes anchos de banda. Cuando una de estas conexiones no tiene el suficiente ancho de banda se vuelve más lenta que las demás y actúa como cuello de botella, perjudicando la entrega de los paquetes a su destino.

Para un correcto envío de información, los servicios de tiempo real requieren un mayor ancho de banda, para mejorar la velocidad de transferencia de datos por unidad de tiempo. Esto con el fin de que los paquetes enviados lleguen a su destino correctamente de manera que el usuario se sienta satisfecho con el servicio prestado. Dependiendo de la aplicación o servicio que se brinde, el proveedor del servicio debería proporcionar el ancho de banda requerido.

2.5.4. Throughput

Este parámetro se define como la tasa de transferencia de datos de usuario, esto quiere decir la capacidad de datos que un elemento de red puede transmitir en un periodo de tiempo, lo que se traduce como un rendimiento de procesamiento.

El *throughput* puede depender de factores como la información adicional de encabezados, impuesta por el protocolo de comunicación utilizado, la capacidad del sistema de utilizar completamente el ancho de banda proporcionado por el canal de comunicaciones, limitaciones impuestas por el elemento de comunicación de datos, el enlace de comunicación, el retardo entre dos puntos, entre otros.

Se puede concluir entonces que el ancho de banda en teoría es la capacidad que tiene un elemento de red para el transporte de datos y el *throughput* es la utilización real que se puede lograr de dicho elemento.

2.5.5. Disponibilidad de Servicios

Se refiere al tiempo programado por un proveedor de servicios para que un servicio se encuentre disponible para los usuarios. Según la ITU-T en [41], a menos que el proveedor de servicio indique otra cosa, el tiempo de servicio programado para un servicio es de 24 horas al día, 7 días a la semana.

La ITU-T define una función de disponibilidad que especifica la tasa de pérdida de paquetes, como único parámetro de decisión de disponibilidad, para establecer si la sección de red observada está o no disponible. Además, define dos parámetros de disponibilidad.

- **Porcentaje de Indisponibilidad de Servicio de Protocolo Internet (PIU, *Percent IP Service Unavailability*):** según la función de disponibilidad definida por la ITU-T, se establece como el periodo (%) de indisponibilidad, del tiempo total de servicio programado.
- **Porcentaje de Disponibilidad de Servicio de Protocolo Internet (PIA, *Percent IP Service Availability*):** según la función de disponibilidad definida por la ITU-T, se establece como el periodo (%) de disponibilidad, del tiempo total de servicio programado.

2.5.6 Retardo extremo a extremo

Es el tiempo que le toma a un paquete viajar de un nodo origen a un nodo destino. Este tiempo, es la suma de todos los retardos que sufre el paquete al transitar por la red y en los enlaces que debe atravesar.

Los retardos pueden ser clasificados en:

- Fijos: son retardos que se pueden cuantificar y se añaden directamente al retardo total. Entre estos se encuentran el retardo por codificación, el retardo de empaquetado, el retardo por serialización, el retardo de propagación, entre otros.
- Variables: son retardos difíciles de cuantificar debido a que provienen de fuentes aleatorias. Entre estos se encuentran el retardo de encolamiento, el retardo de almacenamiento, entre otros.

Fundamentalmente el retardo extremo a extremo está compuesto por:

- Retardo de la red.
- Retardo del códec.
- Retardo del *buffer* receptor

El retardo tiene un impacto directo sobre la satisfacción del usuario según el servicio prestado por el proveedor [33][41][42].

2.5.6.1 Retardo de Handover

Hace referencia a la duración del proceso de *Handover*, definido como el tiempo desde que el nodo móvil inicia y finaliza el cambio desde un punto de acceso de la red a otro, perdiendo en este tiempo la capacidad momentánea de enviar o recibir paquetes, hasta que las tareas involucradas en este proceso se hayan totalizado.

Esta latencia está compuesta por diferentes tipos de retardos que se dan en el momento en que se realiza el proceso de *Handover*. De esta manera, el retardo de *handover* se puede definir de acuerdo a la Ecuación 2.3:

$$T_{HO}: T_{L2HO} + T_{MD} + T_{L3HO} [44]$$

Ecuación 2.3. Retardo Total de Handover

Donde:

T_{HO} : Retardo Total de *Handover*.

T_{L2HO} : Retardo de *Handover* en capa 2.

T_{MD} : Retardo de detección de movilidad. Esta generalmente es cero debido a que el movimiento realizado de L2 a L3 pasa desapercibido de acuerdo a los mecanismos utilizados.

T_{L3HO} : Retardo de *Handover* en capa 3.

Estos retardos, a su vez están compuestos por pequeñas latencias cuya sumatoria resulta en el retardo de *Handover* total. Sin embargo, estas latencias no se tendrán en cuenta en el presente proyecto.

2.5.6.2. Pérdida de paquetes durante el Handover

Esta pérdida de paquetes tiene lugar durante el tiempo en que se demore el nodo móvil en realizar el proceso de *Handover*. Se produce por la desconexión momentánea de la red que puede sufrir el nodo móvil en el momento en que hace el traspaso de una red a otra. Este parámetro se define como la suma de los paquetes perdidos durante un *Handover* [44].

Los conceptos, factores y parámetros descritos anteriormente, dan una visión general acerca de las afectaciones que puede presentar un servicio de tiempo real cuando se desenvuelve en un contexto de movilidad IP.

Conocidos estos, es importante darle prioridad a los mismos en el análisis que se realice para la correcta prestación de este tipo de servicios, con el fin de que los usuarios finales se sientan satisfechos con el servicio que están percibiendo.

En los siguientes capítulos se definirán los protocolos a utilizar, los escenarios de trabajo y el plan de pruebas a seguir, dándole inicio a la simulación con el fin de evaluar el impacto del proceso de *handover* sobre un servicio de tiempo real.

CAPÍTULO III. PROTOCOLOS DE MICROMOVILIDAD IPv6

3.1 INTRODUCCIÓN

Para soportar movilidad IP en los terminales de red se han especificado un conjunto de protocolos que facilitan que un nodo móvil pueda desplazarse y mantener una comunicación estable, en tanto cambia de punto de acceso a la red, reduciendo al máximo los efectos que pueda traer este cambio sobre la información que se transmite.

Los protocolos de movilidad IP hacen uso de mensajes de señalización que determinan la ubicación actual del nodo móvil y que permiten establecer (o continuar) una comunicación cuando se cambia de ubicación. Los protocolos se pueden desplegar en ambientes de macromovilidad, micromovilidad o ambos, según lo definido en la sección 1.2 de este documento. Existen dos características importantes que indican si un protocolo puede aplicarse en esos ambientes [45]:

- Cantidad de mensajes de señalización: un protocolo puede desplegarse en ambientes de micromovilidad IP cuando el número de mensajes de señalización sea bajo, esto es debido a que la alta cantidad de traspasos que se efectúan allí requiere un buen uso de los recursos red. En un ambiente de macromovilidad no es obligatoria esta característica ya que el número de traspasos que se realizan allí es bajo.
- Cantidad de saltos de red: se refiere al número de enrutadores que atraviesa un paquete para llegar de un punto de la red a otro. En un ambiente de micromovilidad IP, regularmente, los saltos de red entre los dispositivos que participan en la señalización es pequeño en consideración con el ambiente de macromovilidad, esto se establece con el fin de introducir retardos pequeños.

Mobile IPv4 y *Mobile IPv6* surgen como protocolos de macromovilidad [46] a partir de los protocolos IPv4 e IPv6 respectivamente. Para micromovilidad IP, se hicieron adaptaciones de los dos anteriores, con el fin de reducir las limitaciones que tenían dichos protocolos y poder ser implementados en este tipo de ambiente.

En este capítulo se describe el funcionamiento de *Mobile IPv6*, un protocolo de macromovilidad, base de otros protocolos que se emplean en micromovilidad. Posteriormente se describe el funcionamiento de dos protocolos de micromovilidad IPv6 que surgen como extensiones de *Mobile IPv6*: *Hierarchical Mobile IPv6* y *Proxy Mobile IPv6*. Finalmente se hace una síntesis comparativa entre los tres protocolos.

3.2 MOBILE IPv6 (MIPv6)

3.2.1 Antecedentes

Mobile IPv6 se propone como estándar en el año 2004 y está definido en el RFC 3775² [21]. Este protocolo se especifica para la gestión de movilidad en el nivel de red acorde al modelo OSI. Las ventajas que proporciona este protocolo surgen de las características propias del protocolo IPv6, que fue concebido originalmente con el fin de hacerlo extensible, esto significa, que nuevas funcionalidades se agregan al protocolo de forma sencilla y dinámica, en la medida que se necesiten. Una de estas funcionalidades es el soporte de movilidad IPv6, y es de aquí de donde se deriva *Mobile* IPv6 (MIPv6).

Mobile IPv6 fue diseñado como un protocolo de macromovilidad y por lo tanto se espera que en el escenario donde se despliegue, los *handover* que realicen los móviles no sean tan frecuentes. El rendimiento de este protocolo disminuye si la frecuencia de los *handover* aumenta [46].

3.2.2 Términos utilizados en *Mobile* IPv6

A continuación se describen los términos que son usados por *Mobile* IPv6 separados en cuatro grupos: general, elementos de red, mensajes y acciones.

- ❖ Términos generales: hacen referencia entre otros, a direcciones IPv6 y Tablas de cache (Tablas para guardar información temporal), estos son:
 - *Red Local* del Nodo Móvil (*Home Network*): red de donde proviene originalmente el nodo móvil.
 - *Red Visitada* (*Foreign Network*): cualquier red diferente a la red local del nodo móvil.
 - *Dirección Local* (*Home Address*): dirección IPv6 asignada a un nodo móvil en su red local, que se usa como dirección permanente del nodo.
 - *Care-of Address*, *CoA*: dirección IPv6 asociada a un nodo móvil mientras está en una *Red Visitada*.
 - *Asociación* (*Binding*): la relación que se establece entre la *Care-of Address* actual del nodo móvil y su *Home Address*.

² Durante el desarrollo de este proyecto de grado el RFC 3775 se vuelve obsoleto y es reemplazado por el RFC 6275. Los cambios realizados (Apéndice B) no influyen en la descripción que se hace de *Mobile* IPv6 en este documento.

- *Caché de Asociación (Binding Cache)*: Tabla de registros donde se guarda una asociación y el tiempo de vida (*lifetime*) de la misma. El tiempo de vida indica el tiempo restante para el vencimiento de la asociación antes de que sea eliminada. Cada registro de esta caché se denomina *Registro de en la Caché de Asociación (Binding Cache Entry - BCE)*.
- ❖ Elementos de red: por ejemplo enrutadores, terminales de red, que cumplen funciones específicas. Estos elementos se muestran en la Figura 3.1:

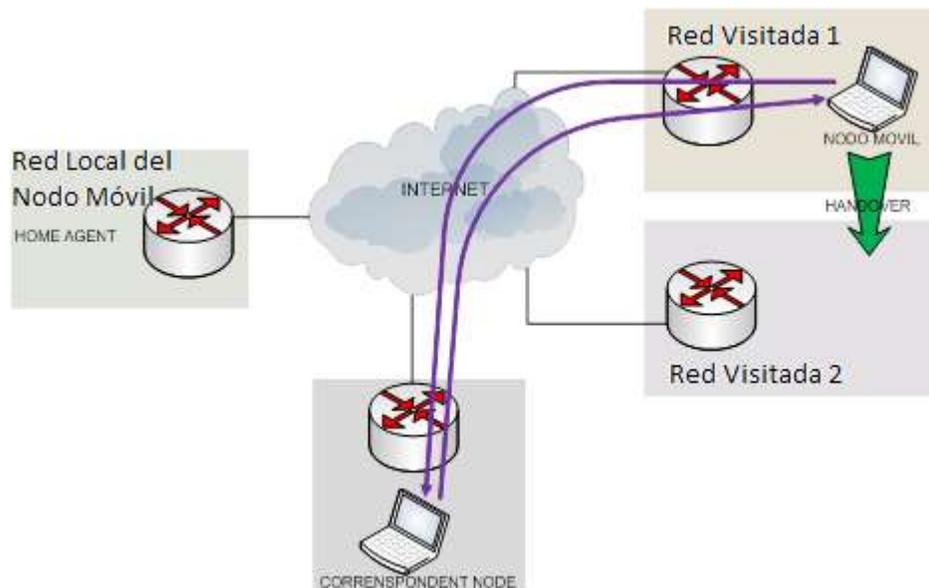


Figura 3.1. Elementos de red de *Mobile IPv6*. Por los autores.

- *Nodo Móvil (Mobile Node - MN)*: el nodo que cambia de punto de acceso a la red.
 - *Correspondent Node, CN*: nodo con el que el nodo móvil se está comunicando.
 - *Agente Local (Home Agent)*: es “un enrutador ubicado en la red local del nodo móvil con el que ha registrado su actual Care-of Address. Mientras el nodo móvil esté lejos de casa, el Agente Local intercepta los paquetes en el enlace inicial que van destinados a la Dirección Local (Home Address) del nodo móvil, los encapsula, y los envía mediante un túnel a la Care-of Address registrada por el nodo” [21].
- ❖ Mensajes de señalización:
- *Binding Update, BU*: es un mensaje que es enviado por el nodo móvil al *Correspondent Node* o a su *Agente Local (Home Agent)*, indicándole su actual

Care-of Address. Este se envía cuando el nodo adquiere una nueva *Care-of Address* o cuando el tiempo de vida de la *asociación* expira, de esta forma un *Binding Update* puede ser enviado después de un *handover* cuando ha cambiado la *Care-of Address*, o simplemente cuando se requiera actualizar la *Binding Cache*, sin que la *Care-of Address* haya cambiado.

- *Binding Acknowledgement, BA*: este mensaje es enviado por el *Correspondent Node* o el *Agente Local*, como respuesta a un *Binding Update* indicando el resultado de la actualización de la *asociación*.
 - *Home Test Init, HoTI* y *Home Test, HoT*: mensajes usados para verificar que el CN puede alcanzar al nodo móvil a través del *Agente Local*.
 - *Care-of Test Init, CoT* y *Care-of Test, CoT*: mensajes usados para verificar que el CN puede alcanzar directamente al nodo móvil.
- ❖ Acciones: haciendo uso de los anteriores mensajes de señalización, MIPv6 describe las siguientes acciones realizadas por los elementos de red:
- Procedimiento de Retorno de Ruta: “*permite al Correspondent Node obtener una garantía suficiente de que el nodo móvil es direccionable en la Care-of Address que anuncia, así como también en su Home Address. Solo con esta garantía el Correspondent Node es capaz de aceptar Binding Updates del nodo móvil*” [21].
 - Registro con el *Correspondent Node*: proceso en el que se envía un *Binding Update* al CN con el fin de registrar una *asociación* para el nodo móvil. Para realizar este registro, previamente se debe haber realizado un Procedimiento de Retorno de Ruta.
 - Registro con el *Agente Local*: proceso en el que se envía un BU al *Agente Local* con el fin de registrar una *asociación* para el nodo móvil.

3.2.3 Operación de MIPv6

Existen dos modos posibles para las comunicaciones entre el nodo móvil y el *Correspondent Node*:

- Túnel bidireccional: no requiere que el *Correspondent Node* soporte *Mobile IPv6*. Todos los paquetes enviados desde y hacia el *Correspondent Node* son enrutados a través del *Agente Local*.
- Optimización de ruta: requiere el soporte de *Mobile IPv6* en el *Correspondent Node*. Con este modo se logra que todos los paquetes se envíen directamente a la *Care-of Address* del nodo móvil [21].

Para describir el funcionamiento de MIPv6 se usa el escenario de la Figura 3.1 nombrada anteriormente. Este escenario usa el modo de optimización de ruta donde es necesario que todos los dispositivos soporten *Mobile IPv6*. El estado actual de los elementos mostrados, justo antes de realizar un *handover*, es el siguiente:

Existe un nodo móvil ubicado fuera de su red local, asociado a un Punto de Acceso (*Access Point* - AP) en una Red Visitada 1 y con una *Care-of Address* asociada, CoA 1. El nodo móvil tiene establecida una comunicación con un CN con esa dirección IPv6, y se dispone a realizar un *handover* hacia una Red Visitada 2.

Los sucesos que ocurren durante el *handover* se observan en el diagrama de tiempo de la Figura 3.2 y se describen a continuación:

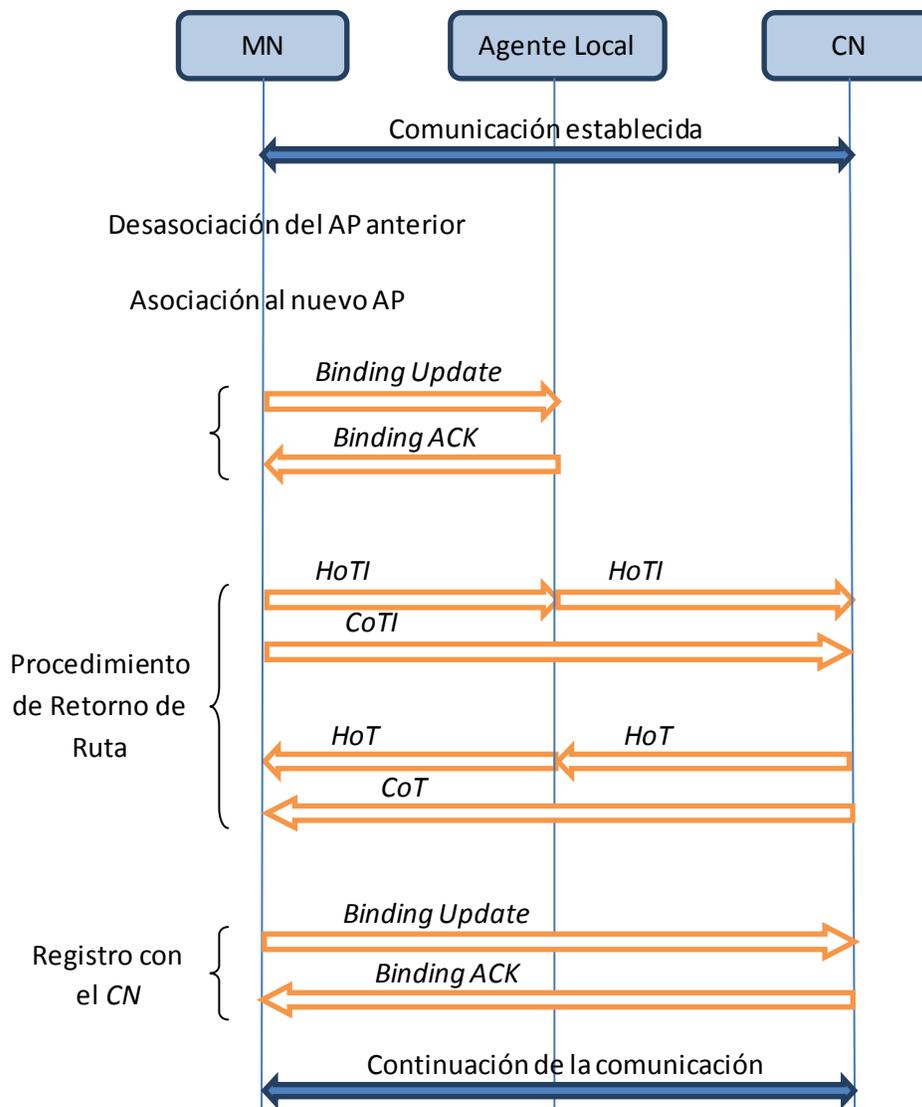


Figura 3.2. Diagrama de tiempo MIPv6. Fuente: los autores.

1. El nodo móvil pierde el enlace con la primera red y establece un nuevo enlace con la segunda red. Allí conFIGura su dirección IPv6 y obtiene una CoA 2. El nodo móvil no puede continuar con la comunicación mantenida hasta ese momento, después de haber perdido el enlace con la primera red, ya que dicha comunicación se estableció haciendo uso de la CoA 1.
2. El nodo móvil envía un *Binding Update* a su *Agente Local* para registrar su nueva *Care-of Address (CoA 2)*.
3. El *Agente Local* envía un *Binding Acknowledgement* a la CoA 2 del nodo móvil indicando el resultado del registro.
4. El nodo utiliza el procedimiento de retorno de ruta con cada uno de los *Correspondent Node* con los que tenía establecida una comunicación. Esto con el fin de determinar si la nueva *Care-of Address* es una dirección enrutable y válida para mantener la comunicación.
5. Si el procedimiento de retorno de ruta es exitoso con un *Correspondent Node*, el nodo móvil le envía un *Binding Update* para registrar su CoA 2.
6. El *Correspondent Node* puede enviar un *Binding Acknowledgement* al nodo móvil indicando el resultado del registro.

El nodo móvil, una vez ha conFIGurado su CoA 2 y ha actualizado las *asociaciones* en el *Agente Local* y los *Correspondent Node* exitosamente, ya puede restablecer su comunicación con ellos. “*Mobile IP no almacena los paquetes enviados al nodo móvil durante el Handover. Por lo tanto, estos paquetes se pueden perder y deben ser retransmitidos*” [47].

Se observa que el proceso para realizar un *handover* con *Mobile IPv6*, requiere del intercambio de varios paquetes. Debido a esto, este protocolo no tiene buen rendimiento en ambientes de micromovilidad, en los que su despliegue haría un mal uso de los recursos de red, cuando se presenten frecuentes *handovers* [48].

3.3 HIERARCHICAL MOBILE IPv6 (HMIPv6)

3.3.1 Antecedentes

HMIPv6 es un protocolo creado con base en MIPv6. En su especificación, en el RFC 5380 [49], se introducen extensiones a MIPv6 y a IPv6 *Neighbour Discovery*, y se describen nuevas funciones para los elementos de red. El objetivo es reducir la cantidad de mensajes de señalización y mejorar la velocidad del *handover*. La primera de estas dos

características es propia de protocolos que se despliegan en un ambiente de micromovilidad.

3.3.2 Términos utilizados en HMIPv6

HMIPv6 describe una nueva funcionalidad que extiende MIPv6 y es agregada a un elemento de red (el enrutador):

- *Punto de Anclaje de Movilidad (Mobility Anchor Point - MAP)*: es un enrutador que esencialmente se comporta similar a un *Agente Local*, pero en este caso no se encuentra en la red de origen del nodo móvil sino en la red que esté visitando.

También define las siguientes direcciones IPv6:

- *Regional Care-of Address, RCoA*: dirección IPv6 que identificará al nodo en toda red ajena al dominio del MAP
- *On-Link Care-of Address, LCoA*: anteriormente, en MIPv6, denominada *CoA*, es la dirección IPv6 del nodo móvil dentro de la red local donde esté ubicado.

El MAP y las direcciones IPv6 definidas se muestran en la Figura 3.3.

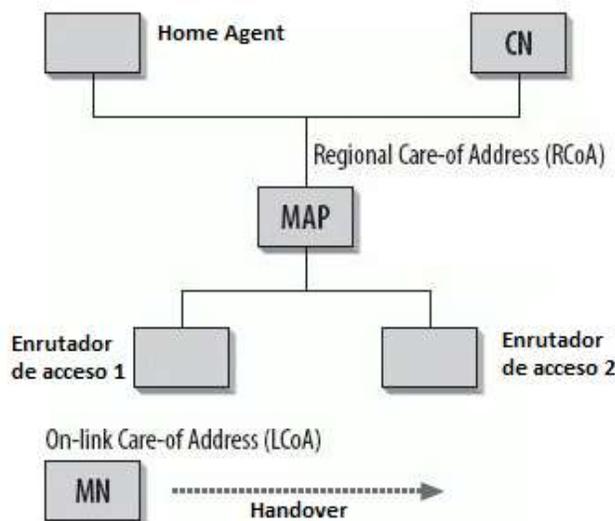


Figura 3.3. Funciones de los elementos de HMIPv6. Adaptado de [49].

La *asociación*, en HMIPv6, enlaza la RCoA con la verdadera dirección del nodo móvil en la red local donde se encuentra, la LCoA. De esta forma el MAP actúa en representación del nodo móvil para recibir todos los paquetes que vayan dirigidos a éste (a su RCoA) y los encapsula y reenvía directamente al nodo móvil (a su LCoA).

3.3.3 Operación de HMIPv6

A continuación se detalla el procedimiento que se realiza cuando el nodo móvil efectúa un *handover* dentro del dominio del MAP. Se asume que el nodo móvil soporta HMIPv6 (y por lo tanto también MIPv6). La Figura 3.4 muestra el diagrama de tiempo de los mensajes:

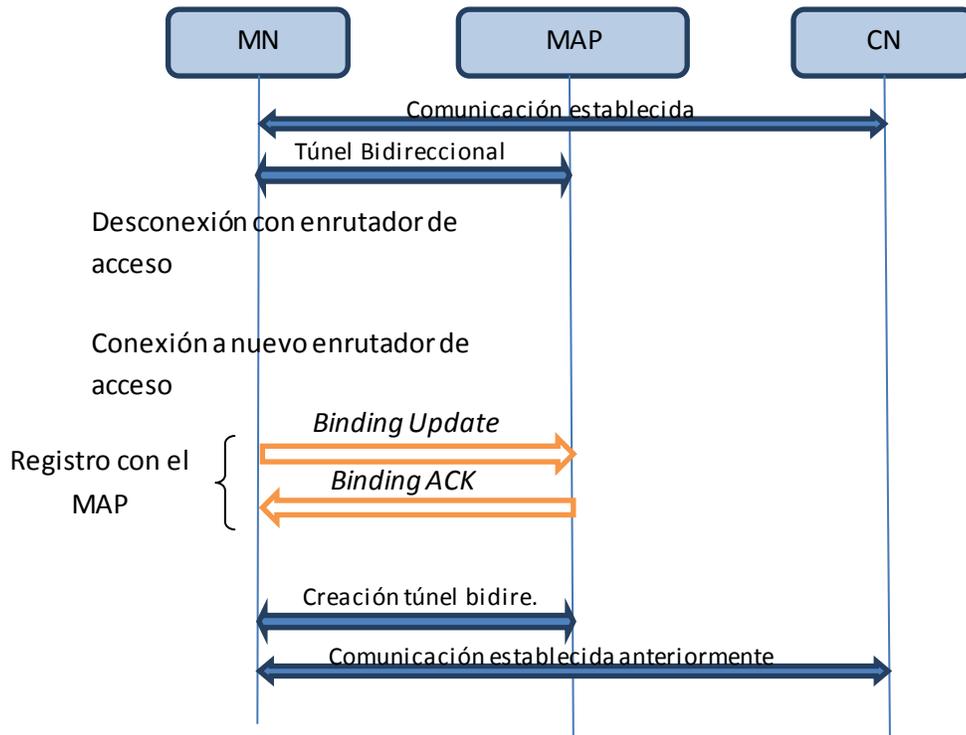


Figura 3.4. Diagrama de tiempo HMIPv6. Por los autores.

1. El nodo móvil está conectado al enrutador de acceso 1, posee una LCoA 1, una *Home Address*, y tiene establecida la comunicación con el *Correspondent Node*. Inicia el movimiento hacia el área de cobertura del enrutador de acceso 2.
2. El nodo móvil sale del área de cobertura del enrutador de acceso 1, se desconecta de éste, y se conecta al enrutador de acceso 2. Allí obtiene una LCoA 2. Al igual que en MIPv6, el nodo pierde comunicación ya que ésta se realizaba anteriormente con la LCoA 1.
3. El nodo envía un *Binding Update* al MAP para registrar su nueva *On-Link Care-of Address* (LCoA 2).
4. El MAP envía un *Binding Acknowledgement* a la LCoA 2 del nodo móvil indicando el resultado del registro. El *handover* es transparente para el CN y el *Agente Local* del nodo móvil.

5. Después de un registro exitoso se establece un túnel bidireccional entre el nodo móvil y el MAP. Los paquetes enviados por y hacia el nodo móvil son interceptados por el MAP, que a su vez los envía hacia la red externa o al nodo móvil respectivamente.

En el proceso descrito anteriormente no hay mensajes de señalización entre el nodo móvil y el CN o el *Agente Local*, ni tampoco entre el MAP y el CN o el *Agente Local*. Dichos mensajes solo se producen cuando el nodo móvil sale del dominio del MAP y solo se intercambian entre el MAP y el *Agente Local*. En este caso ya se habla de un ambiente de macromovilidad y los mensajes son los definidos en el RFC 3775 excepto que no son procesados por el nodo móvil sino por el MAP, (el MAP reemplaza al nodo móvil).

3.4 PROXY MOBILE IPv6 (PMIPv6)

3.4.1 Antecedentes

PMIPv6 se define en el RFC 5213 [50]. Es un protocolo especificado para brindar gestión de movilidad IPv6 a un nodo móvil, sin que este participe en el proceso de señalización. Esto significa que el nodo móvil no requiere soportar ningún protocolo de movilidad y es suficiente con que trabaje con IPv6. Esta característica es importante desde dos puntos de vista:

- Al no participar el nodo móvil en el proceso de señalización, se reducen los mensajes de dicho proceso y por lo tanto se hace un buen uso de los recursos de red. Esto es una ventaja cuando se trabaja con escenarios de micromovilidad.
- Al no necesitar el nodo móvil de protocolos de movilidad, el despliegue de este protocolo se vuelve relativamente fácil, ya que los cambios necesarios para soportarlo solo se deben realizar por parte de los proveedores de servicio, los inconvenientes que se presenten solo estarían del lado del proveedor.

3.4.2 Términos utilizados en PMIPv6

PMIPv6 introduce las siguientes funciones en los elementos de red que participen en el proceso de gestión de movilidad IPv6. La Figura 3.5 ilustra estas funciones:

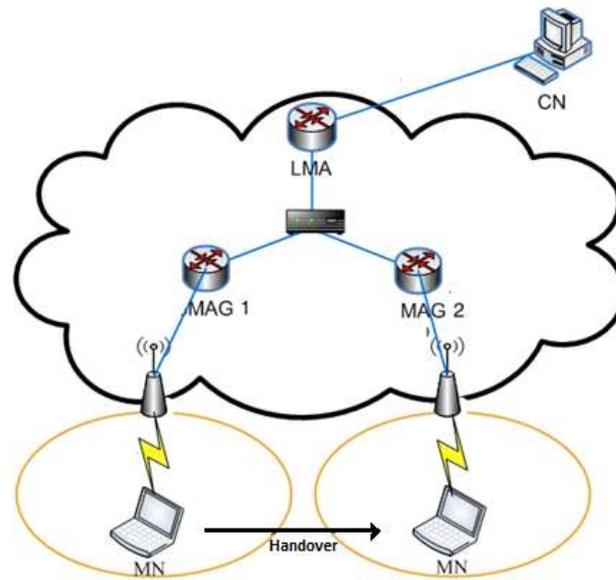


Figura 3.5. Funciones de los elementos de PMIPv6. Adaptado de [51].

- *Local Mobility Anchor, LMA:* se comporta como el *Agente Local* del nodo móvil dentro del dominio donde PMIPv6 está siendo usado. Sus funciones están definidas en el RFC 3775 como *Agente Local (Home Agent)*, y se agregan algunas características para soportar PMIPv6 en el RFC 5213.
- *Mobile Access Gateway, MAG:* se encarga de la gestión de los mensajes de señalización de movilidad en representación de los nodos que están conectados a su enlace de acceso. Debe ser capaz de determinar cuándo un nodo se ha conectado o desconectado de dicho enlace para informar dicho evento al LMA.

Define la siguiente dirección IPv6:

- *Proxy Care-of Address, Proxy-CoA:* configurada en la interfaz de salida del MAG, en el enlace con el LMA. Esta es la dirección que se usa como CoA del nodo móvil en los registros del LMA

PMIPv6 también define los siguientes mensajes de señalización:

- *Proxy Binding Update, PBU:* es un mensaje enviado por la MAG al LMA indicándole la *Care-of Address* (denominada Proxy-CoA en esta especificación) del nodo móvil asociado. Las características de este mensaje están especificadas en el RFC 3775 como *Binding Update* y se agregan otras en el RFC 5213 para soportar PMIPv6.
- *Proxy Binding Acknowledgement, PBA:* es el mensaje de respuesta a un PBU indicando el resultado de la actualización de la *asociación*.

3.4.3 Operación del protocolo

El procedimiento que se realiza durante un *handover* en un dominio PMIPv6 se detalla de forma simplificada en la Figura 3.6.

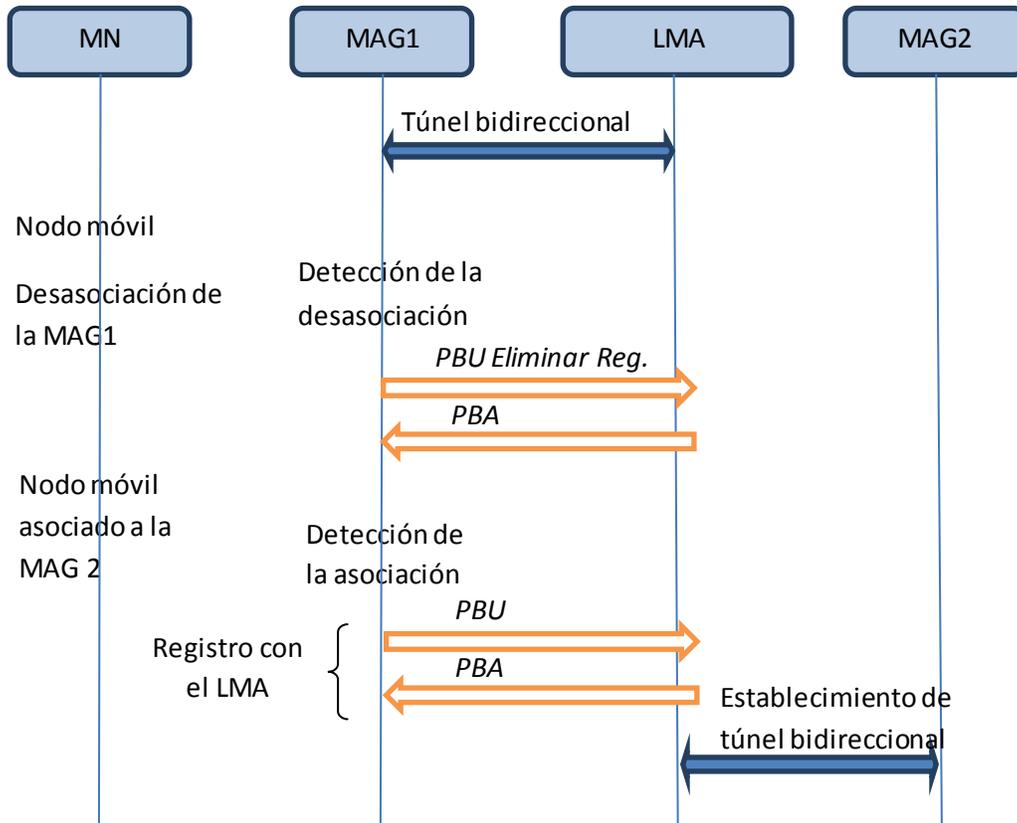


Figura 3.6. Diagrama de tiempo PMIPv6. Adaptado de [50].

1. El nodo móvil está conectado a la MAG 1 y tiene establecida una comunicación con el CN, (en el diagrama de tiempo no se muestra tal comunicación), a través de un túnel entre la MAG 1 y el LMA. El nodo móvil inicia el movimiento hacia el área de cobertura del punto de acceso de la MAG 2 (o hacia la MAG 2 directamente, si se comporta como punto de acceso).
2. El nodo móvil pierde el enlace con la MAG 1, que detecta este evento y envía un PBU al LMA con el fin de eliminar el registro del nodo móvil. El LMA una vez recibido este mensaje, esperará un tiempo antes de eliminar el BCE de la cache. Esto permite que la MAG 2 actualice esa *asociación* cuando el nodo móvil se haya conectado, si este no es el caso, la *asociación* se eliminará después de dicho tiempo.

3. El LMA envía un PBA a la MAG 1 en respuesta al PBU de cancelación de registro enviado por la MAG 1.
4. El nodo móvil se conecta al enlace de la MAG 2, que detecta el evento y notifica al LMA mediante un mensaje PBU. En este mensaje le indica su dirección de red (la del MAG 2) que será registrada como la *Proxy-CoA* asociada al nodo móvil.
5. El LMA envía un PBA a la MAG 2 en respuesta al PBU de registro enviado por la MAG 2. Si el proceso fue exitoso se establece un túnel bidireccional entre el LMA y la MAG 2 que será usado para la comunicación del LMA con el nodo móvil.

Cuando el proceso termina (con éxito) el nodo móvil conserva su dirección de red local, la *Home Address*, y continua con las comunicaciones que haya tenido establecidas. El *handover* es transparente para el CN, que no participó en la señalización y no requiere ninguna actualización de información para continuar la comunicación.

3.5 SÍNTESIS DE PROTOCOLOS DE MOVILIDAD

De los protocolos descritos en este capítulo, se resaltan sus características más importantes con el fin de realizar comparaciones entre los mismos (Tabla 3.1 y Figura 3.7). Una comparación más profunda y con otros protocolos se encuentra en [52]. El objetivo es identificar las ventajas y desventajas que tiene un protocolo al momento de seleccionarlo.

Característica del protocolo	Protocolos de movilidad IPv6		
	MIPv6	HMIPv6	PMIPv6
Escenario donde desplegarlo	Macromovilidad	Micro/Macromovilidad	Micromovilidad
Funciones de elementos de red	Nodo Móvil <i>Agente Local</i> CN	Micromovilidad: Nodo Móvil MAP CN Macromovilidad: Nodo Móvil <i>Agente Local</i> MAP CN	LMA MAG
Funciones de elementos involucradas en un <i>handover</i>	Nodo móvil <i>Agente Local</i> CN	Micromovilidad: Nodo móvil MAP Macromovilidad:	LMA MAG

		Nodo Móvil <i>Agente Local</i> MAP CN	
Modificación del nodo móvil	Si	Si	No
Retardo de <i>handover</i>	Bajo	Medio	Alto
Túneles	Depende de si todos los nodos soportan MIPv6	SI	SI

Tabla 3.1. Síntesis de protocolos de movilidad IPv6. Fuente: Los autores.

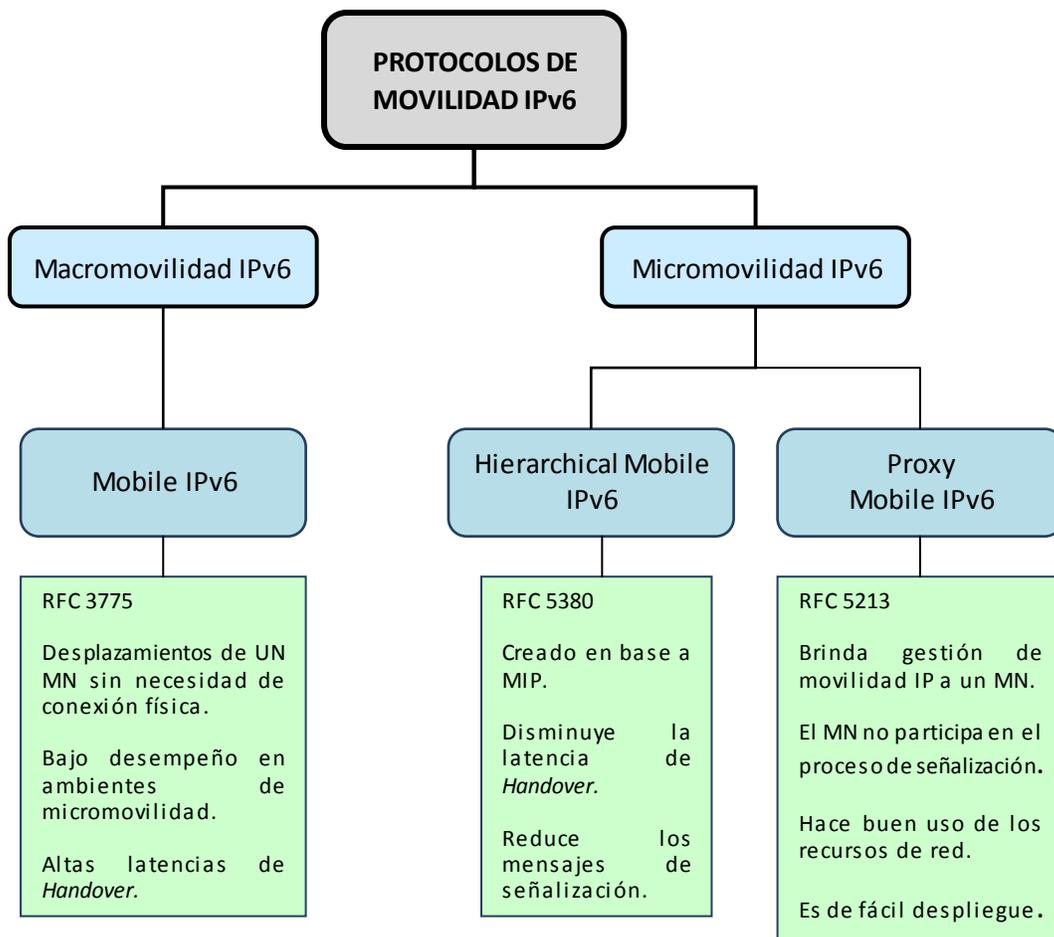


Figura 3.7. Principales Características de los Protocolos de Movilidad.

Fuente: Los Autores.

En este capítulo se mostraron las características, el funcionamiento y las diferencias de tres protocolos de movilidad. Se observa como un protocolo de macromovilidad como lo es MIPv6 puede ser extendido con facilidad para dar soporte a ambientes de micromovilidad y cuáles son los requerimientos para que esto se cumpla. La información que aquí se da sobre los protocolos de movilidad, sirve de base en el siguiente capítulo para elegir un protocolo con el que se harán las pruebas de simulación y los análisis de los resultados.

CAPITULO IV. SIMULACIÓN, PRUEBAS Y RESULTADOS

Este capítulo, presenta inicialmente la herramienta de simulación adoptada para el desarrollo del proyecto en cuestión. Se definen dos escenarios para realizar las pruebas con el fin de evaluar el efecto que tiene el proceso de *handover* en un contexto de micromovilidad IPv6 sobre un tráfico de tiempo real que fluye en una comunicación. Para la realización de pruebas, se definen 2 casos por escenario, se utiliza uno de los protocolos de movilidad descrito en el capítulo anterior, se caracteriza el servicio en tiempo real a utilizar en la simulación y se analizan los resultados en términos de pérdidas de paquetes, *throughput*, *jitter* y retardo.

Finalmente se presenta una Tabla comparativa, que permita concluir que tan afectada resulta la comunicación por la ocurrencia de los procesos de *handover*, en cada uno de los casos analizados.

4.1 SELECCIÓN DEL PROTOCOLO DE MICROMOVILIDAD IPv6 Y DE LA HERRAMIENTA DE SIMULACIÓN

4.1.1 Selección del protocolo de micromovilidad IPv6

Para la elección del protocolo de micromovilidad se tiene en cuenta la síntesis mostrada en la Tabla 3.1 del anterior capítulo. De acuerdo con ella se muestran dos candidatos para protocolo de micromovilidad IPv6: HMIPv6 y PMIPv6. Se selecciona el protocolo PMIPv6 para ser usado en los escenarios de simulación por las siguientes razones [52][53]:

- El número de funciones de elementos de red usados en un ambiente de micromovilidad IPv6 es menor que el de HMIPv6 en una proporción de 2 a 3 respectivamente. La ventaja se refleja directamente en el número de dispositivos que deben soportar este protocolo y en los costos que esto conlleva.
- El nodo móvil no participa en la señalización establecida por el protocolo y por lo tanto no necesita soportar PMIPv6. La ventaja se refleja en que cualquier dispositivo que soporte IPv6 es compatible con este protocolo y en los costos para los consumidores.
- El bajo retardo de *handover*, que es importante para los objetivos de este trabajo y que es uno de los inconvenientes que se quiere superar en cualquier protocolo de movilidad al igual que la pérdida de paquetes.

4.1.2 Herramientas de simulación

Las herramientas de simulación candidatas deben cumplir con los siguientes requerimientos mínimos:

- Soporte para comunicaciones inalámbricas.
- Soporte del protocolo IPv6.
- Soporte de protocolos de movilidad IPv6.
- Soporte de protocolos de tráfico de información.
- Generación de resultados que permitan obtener información para estadísticas.

Se realizó una evaluación de 3 herramientas de simulación que cumplen con los anteriores requisitos: Opnet, Omnet++ y NS2. Estas serán descritas brevemente a continuación:

4.1.2.1 OPNET (OPTimized Network Engineering Tools) [54]

Es una herramienta de simulación que usa un lenguaje de programación orientado a comunicaciones. Permite la creación de modelos para extender su funcionalidad. Dispone de herramientas que permiten analizar los resultados de simulación. OPNET cuenta con un modelo para IPv6 que incluye las siguientes características:

- Direccionamiento Expandido.
- Implementación de doble pila, IPv4 e IPv6.
- Protocolos de enrutamiento IPv6: RIPng, OSFv3, y enrutamiento estático.
- *Mobile* IPv6.
- Túneles IPv6.
- ICMPv6.
- *Neighbor Discovery*.
- *Stateless Address AutoconFiguration*.

La creación de escenarios se hace de forma gráfica y reproduce de forma animada el proceso de simulación. Además, dispone del *Modeler Wireless*, que permite la simulación en escenarios inalámbricos, con condiciones de movilidad y da soporte a diferentes protocolos de la misma.

La obtención de resultados, el análisis y graficación de estos, vienen incorporados en la herramienta, que se destaca por tener una amplia lista de estadísticas predefinidas, que se pueden escoger de acuerdo a lo que se desee medir para cada escenario en particular. Entre ellas se incluyen *throughput*, *jitter*, retardo extremo a extremo, retardo de permanencia en cola, uso de ancho de banda, pérdida de paquetes y calidad de la transmisión [55].

La ventaja de este simulador está en que es un sistema robusto con el que se puede simular en varias áreas incluyendo, las aplicaciones y las redes de telecomunicaciones. Sin embargo, aunque brinde soporte para *Mobile* IPv6, no lo hace para *Proxy Mobile* IPv6, y es necesario crear un modelo que le permita a OPNET agregar esta funcionalidad. Otra desventaja es el licenciamiento de esta herramienta, ya que las licencias tienen un costo elevado.

4.1.2.2 OMNeT++ (Objective Modular Network Testbed in C++) [56]

Es un entorno de simulación orientado a objetos y de código abierto. Su área de aplicación es la simulación de redes de comunicaciones, pero puede ser utilizado en otras áreas más complejas, debido a su arquitectura genérica y flexible.

OMNeT++ proporciona una arquitectura basada en componentes para la creación de modelos. Los componentes básicos son programados en C++ para luego ensamblarse en otros componentes más grandes o en modelos, usando un lenguaje de alto nivel (*NED – Network Descriptor*). El uso de componentes y modelos permite la reusabilidad de los mismos.

Para el soporte de protocolos de redes de comunicaciones, tiene un conjunto de librerías denominado *INET Framework*, el cual contiene modelos para varios protocolos de redes cableadas e inalámbricas, incluyendo UDP, TCP, SCTP, IP, IPv6, Ethernet, PPP, 802.11, MPLS, OSPF, entre otros.

Cuenta con un excelente conjunto de herramientas para el análisis de resultados que incluye gráficas, estadísticas, diagramas de tiempo, filtros, entre otros. A diferencia de OPNET, no tiene una lista de estadísticas predefinida para obtención de datos, que facilite el análisis. La obtención de estos datos se realiza en el código de la simulación y su análisis gráfico con las herramientas mencionadas.

Esta herramienta es gratis para uso académico y sin ánimo de lucro. Para uso comercial es necesario obtener una licencia con la que se obtiene soporte técnico. La versión licenciada se denomina OMNeST.

En cuanto al soporte de movilidad, OMNeT++ cuenta con un modelo de simulación denominado *Extensible Mobile IPv6 (xMIPv6) Simulation framework*, diseñado conforme al RFC 3775, en el cual se especifica a *Mobile IPv6* [57]. Uno de los objetivos del modelo xMIPv6 es ser extensible, de tal forma que a partir de él se puedan crear modelos de simulación, los cuales funcionen con otros protocolos de movilidad que tengan como base a MIPv6, por ejemplo FMIPv6, HMIPv6, PMIPv6, etc.

4.1.2.3 NS2 (Network Simulator 2) [58][59]

Es una herramienta de simulación orientada a objetos y de código libre, utilizada principalmente en ambientes académicos que cuenta con una abundante documentación en línea. Permite realizar validaciones de pruebas de protocolos y aplicaciones de red, simulación para TCP/UDP, enrutamiento y multicast sobre redes cableadas o inalámbricas, interacciones multiprotocolo tales como protocolos de transporte, sesión, aplicación, algoritmos de enrutamiento y control de congestión, redes satelitales, entre otros.

NS2 está implementado en lenguaje C++ y usa otro lenguaje interpretado llamado OTcl. La mayoría de los scripts utilizados en simulaciones están desarrollados en lenguaje Tcl y sirven para definir la topología de red, los elementos que la componen, su configuración y funcionamiento.

El análisis de resultados que entrega el simulador es limitado, la mayor parte debe realizarse de forma manual o con herramientas de terceros ya que este simulador solo entrega archivos de texto que contienen los eventos que ocurren durante la simulación.

Esta herramienta cuenta con extensiones que permiten agregarle funciones. Una de esas extensiones añade el soporte para *Proxy Mobile* IPv6 en concordancia al RFC 5213 [50]. Se resalta que el soporte para este protocolo, para IPv6 o IPv4 y para otros protocolos basados en IPv6 o IPv4, no incluye el formato de direcciones IP estándar. Debido a esto una dirección IP, en cualquiera de sus versiones, se representa por un único número entero.

La Tabla 4.1, muestra un resumen de las características de las anteriores herramientas de simulación. Esta Tabla será usada en la siguiente sección para la elección del simulador.

	OPNET	OMNET++	NS2
Soporta MIPv6	Si	Si	Si
Soporta PMIPv6	No	No	Si
Dificultad para implementar PMIPv6	Desconocido	Fácil	-
Extensible mediante módulos	Si	Si	Si
Creación de escenarios gráficamente	Si	Si	Funcionalidad básica mediante la herramienta externa <i>Network Animator</i> , NAM
Licencia	De pago	Código libre	Código libre
Análisis de resultados	Si	Si	No

Tabla 4.1. Tabla comparativa con las características de las herramientas de simulación.

Fuente: Los Autores.

4.1.3 Elección de la herramienta de simulación

Aunque de las tres herramientas de simulación solo NS2 soporta PMIPv6, se consideró que esto no era impedimento para la elección ya que en las otras dos, era posible la creación del módulo que implemente este protocolo. Omnet++, gracias a las características del módulo xMIPv6, permitía la implementación de PMIPv6.

OPNET no fue tomada en cuenta en la elección principalmente porque su licencia solo puede ser adquirida por medios de pago. Las dos herramientas restantes permanecieron como candidatas y particularmente hubo interés en OMNET++ por las siguientes razones:

- A diferencia de NS2, es una herramienta creada recientemente, con pocos años en el campo de la investigación académica, pero muy completa para la simulación de redes y organizada en cuanto al desarrollo de sus versiones.
- PMIPv6 puede extenderse con facilidad gracias al módulo xMIPv6.
- La creación de los escenarios no tiene dificultad ya que el lenguaje NED es sencillo y solo es usado para describir algunos detalles avanzados, todo lo demás se hace de forma gráfica.
- Las herramientas que trae OMNET para el análisis de resultados son potentes, lo que permite que el análisis de los resultados se realice en profundidad.

Con base en lo anterior, inicialmente se trabajó con la herramienta OMNeT++, teniendo como propósito extender el módulo xMIPv6 para darle soporte al protocolo *Proxy Mobile* IPv6, sin embargo debido a inconvenientes causados por la implementación incompleta de xMIPv6 y por el tiempo requerido para darle solución a esto, se decidió cambiar al simulador NS2. Este cambio no ocasionaría ningún problema, y al contrario, sería ventajoso ya que PMIPv6 se encuentra implementado en este simulador.

4.2 METODOLOGÍA DE SIMULACIÓN

La metodología de simulación adoptada para llevar a cabo el plan de pruebas se basa en [60][61], y consta de los pasos descritos a continuación:

- a) Planteamiento general de los escenarios y casos de simulación: se definen los escenarios, según la herramienta de simulación seleccionada, y se plantean los casos con los cuales se ejecutarán las pruebas de simulación como lo muestra el ítem c).
- b) Definición de las características técnicas de los escenarios de simulación: es necesario definir cómo se caracterizaran los enlaces y cuál será el tráfico con el que se va a simular, con el fin de poner la simulación en marcha.
- c) Ejecución de las pruebas de simulación: planteados los escenarios y caracterizados los enlaces y el tráfico de simulación, se empiezan a ejecutar la pruebas de la misma dependiendo de los casos planteados según el ítem a).
- d) Análisis de resultados: según los parámetros de QoS a evaluar y después de la ejecución de la pruebas de simulación, se procede a realizar un análisis de los resultados arrojados por el simulador.

4.2.1 Planteamiento General de los Escenarios y Casos de Simulación

4.2.1.1 Generalidades de los Escenarios de Simulación

Para analizar el efecto que tiene el proceso de *handover* en un servicio de tiempo real en un ambiente de micromovilidad IPv6, se proponen 2 escenarios de simulación y 2 casos (o condiciones) de simulación por cada escenario.

Para todos los escenarios y casos se hace uso de la tecnología de red inalámbrica 802.11g y de las funciones definidas por el protocolo de micromovilidad *Proxy Mobile IPv6*, en los que existirá un nodo móvil en movimiento.

- Escenario de simulación No. 1: éste consta de 6 nodos: CN, LMA, Enrutador, MAG1, MAG2, MN, como se observa en la Figura 4.1. El MN se conecta inalámbricamente a una MAG, la cual actúa como un Punto de Acceso (Access Point - AP). En este capítulo MAG y AP hacen referencia al mismo elemento de red y se habla indistintamente entre ellos. El CN es el encargado de enviar los datos, el MN de recibirlos y los nodos LMA y MAG son representativos del protocolo a evaluar. Además se muestran las áreas de cobertura de las MAG y como se distribuyen los dos canales en este escenario.

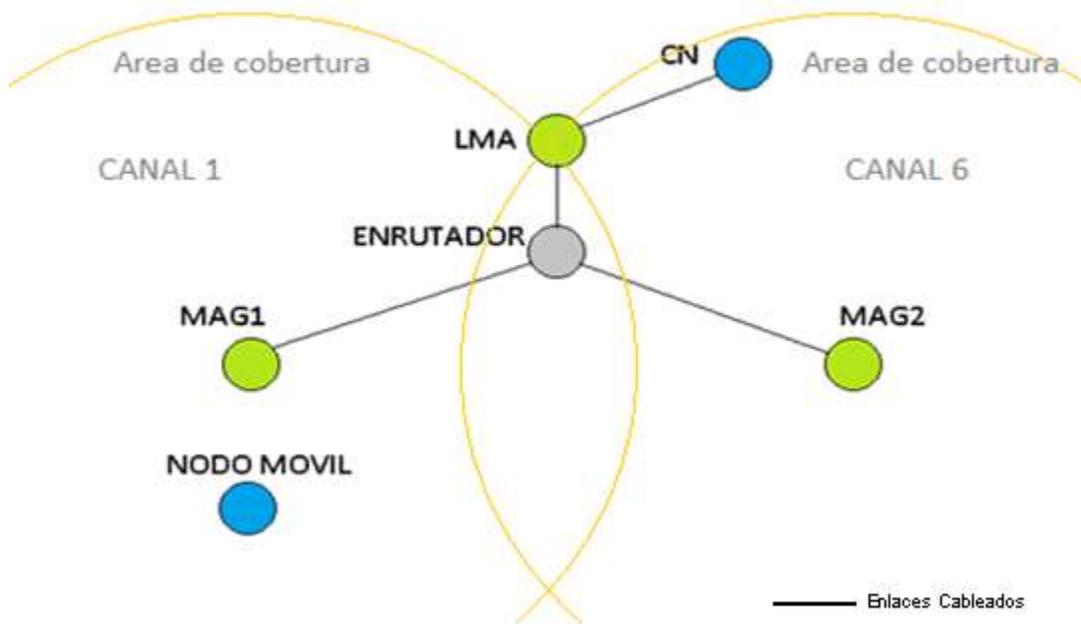


Figura 4.1. Escenario de Simulación No.1.

- Escenario de Simulación No. 2: Este consta de 10 nodos: CN, LMA, Enrutador, MAG1, MAG2, MAG3, MAG4, MAG5, MAG6 y el MN, como se observa en la Figura 4.2.

Además muestra las áreas de cobertura de las MAG, y como están distribuidos los canales en este escenario.

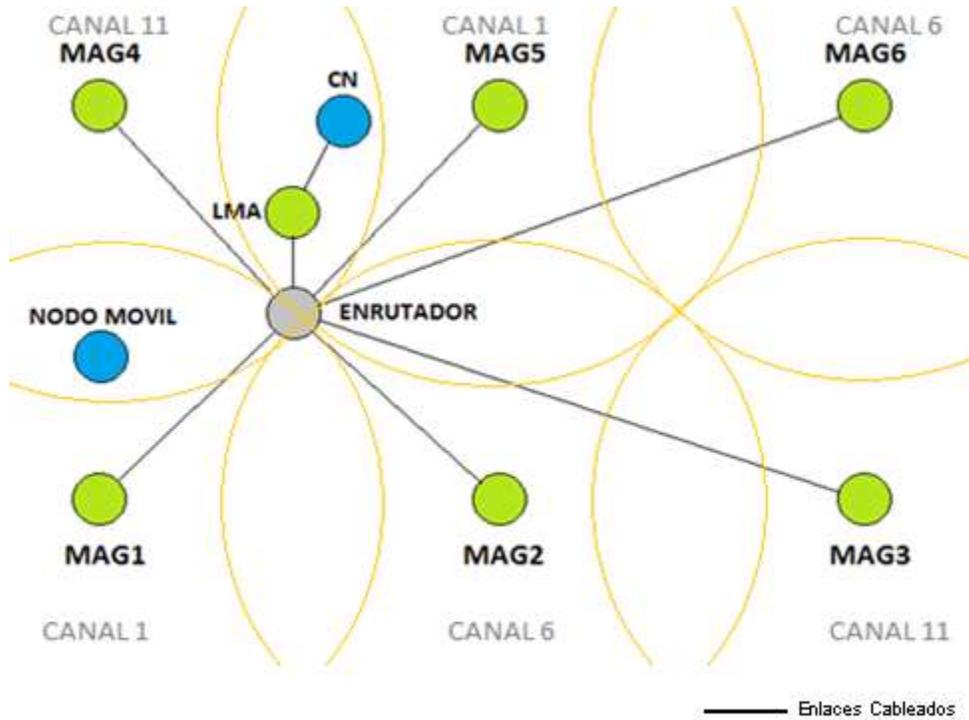


Figura 4.2. Escenario de Simulación No. 2.

Para la asignación de canales se tienen en cuenta dos aspectos:

- Con el fin de reducir al máximo la interferencia por canal adyacente se seleccionan los canales 1, 6 y 11, que no se traslapan entre sí [62].
- Al existir seis puntos de acceso ubicados como se muestra en la gráfica 4.1c, se necesita distribuir los 3 canales seleccionados entre éstos. Así, en cada canal habrán dos APs transmitiendo (Tabla 4.2). La distribución se realiza de forma que las áreas de cobertura de los APs que transmiten en el mismo canal no se intersecten (Figura 4.2b). Esto reduce aún más la interferencia por canal adyacente.

CANAL 1	CANAL 6	CANAL 11
MAG1	MAG2	MAG3
MAG5	MAG6	MAG4

Tabla 4.2. Distribución de las MAGs en los canales de transmisión disponibles.

4.2.2 Definición de las Características Técnicas de los Escenarios de Simulación.

Las características técnicas generales de los escenarios y los casos propuestos, se presentan en la Tabla 4.3. La Tabla 4.4 muestra las características de los enlaces inalámbricos.

Características	ESCENARIO No. 1		ESCENARIO No. 2	
	Caso 1a	Caso 1b	Caso 2 ^a	Caso 2b
Movimiento del nodo móvil	Controlado	Aleatorio	Controlado	Aleatorio
Velocidad del nodo móvil	1.5 m/s	Aleatorio	1.5 m/s	Aleatorio
Número de MAGs	2		6	
Canales de Transmisión (802.11g)	1, 6		1, 6, 11	
Radio área de cobertura de las Bases	200 m			
Potencia de Transmisión	25mw			
Umbral de Recepción (R_x)	-72 dBm			
Modelo de Propagación	Two Ray Ground			
Tiempo de simulación	750ms			
Tipos de antena	Omnidireccionales			

Tabla 4.3. Características Generales de Simulación.

Enlaces	Ancho de Banda	Retardo
CN – LMA	100Mb	20ms
LMA – ENRUTADOR	1000Mb	1.5ms
ENRUTADOR – MAGs	1000Mb	1.5ms

Tabla 4.4. Características de los enlaces cableados.

Para la ejecución de las pruebas de simulación se consideraron diferentes servicios con requerimientos en tiempo real, como lo son: voz sobre IP, videoconferencia y transmisión de video en tiempo real. Teniendo en cuenta esto, y después de ciertos análisis se escogió la transmisión de video en tiempo real por las características que posee (Tráfico inelástico, unidireccional, sensible al retardo y a la pérdida de paquetes, etc.).

En los escenarios de simulación descritos anteriormente, para la fuente de tráfico primero se analizó la transmisión de un video codificado con H.264+AAC (TS). Posteriormente luego de monitorear el tráfico anterior, se determinó que con esta codificación se envía un promedio de 1316 bytes a un intervalo de 0.01 segundos. Los anteriores datos se usan para caracterizar en la simulación, una fuente de tráfico de Tasa de Bits Constante (*Constant Bit Rate, CBR*). Esta fuente será utilizada en todos los escenarios de simulación propuestos. La principal característica de una fuente CBR frente a una de Tasa de Bits Variable (*Variable Bit Rate, VBR*), es que permite que se reserve un ancho de banda fijo,

el cual puede ser usado durante toda la comunicación. VBR por el contrario varía sus requerimientos de ancho de banda durante la comunicación lo cual puede afectar negativamente la QoS del servicio si no existe ancho de banda disponible en un momento dado.

4.2.3 Ejecución de las Pruebas de Simulación.

Los escenarios de simulación definidos anteriormente, son implementados en NS2. El tiempo para cada simulación se define en 700s. Terminado el tiempo de simulación y según la información guardada en los archivos de traza, NS2 graficará los parámetros a evaluar dependiendo del filtro que se le aplique al archivo. Las pruebas se realizan para los dos escenarios descritos y los cuatro casos definidos.

4.2.4 Análisis de los Resultados.

4.2.4.1 Escenario 1

4.2.4.1.1 Caso 1a: Un Nodo Móvil con Movimiento Controlado.

En el caso 1a, se realizaron 5 procesos de *handover* durante el tiempo de simulación. El nodo móvil se mueve controladamente como se indica a continuación:

- a) El nodo móvil parte del punto 1 y se dirige al punto 3.
- b) El nodo móvil parte del punto 3 y se dirige al punto 2.
- c) El nodo móvil parte del punto 2 y se dirige al punto 3.
- d) Se repite la trayectoria de los puntos b y c.

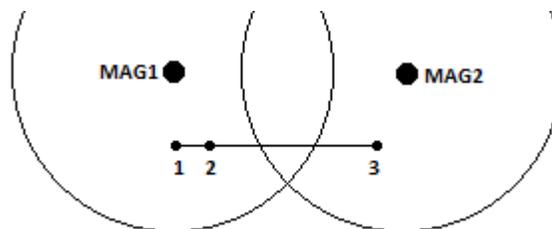


Figura 4.3. Trayectoria del nodo móvil para el caso 1a. Escenario 1.

- **Ocurrencia de los *Handover***

En la Figura 4.4, se muestra en una línea de tiempo, la ocurrencia de cada uno de los 5 *handover*.

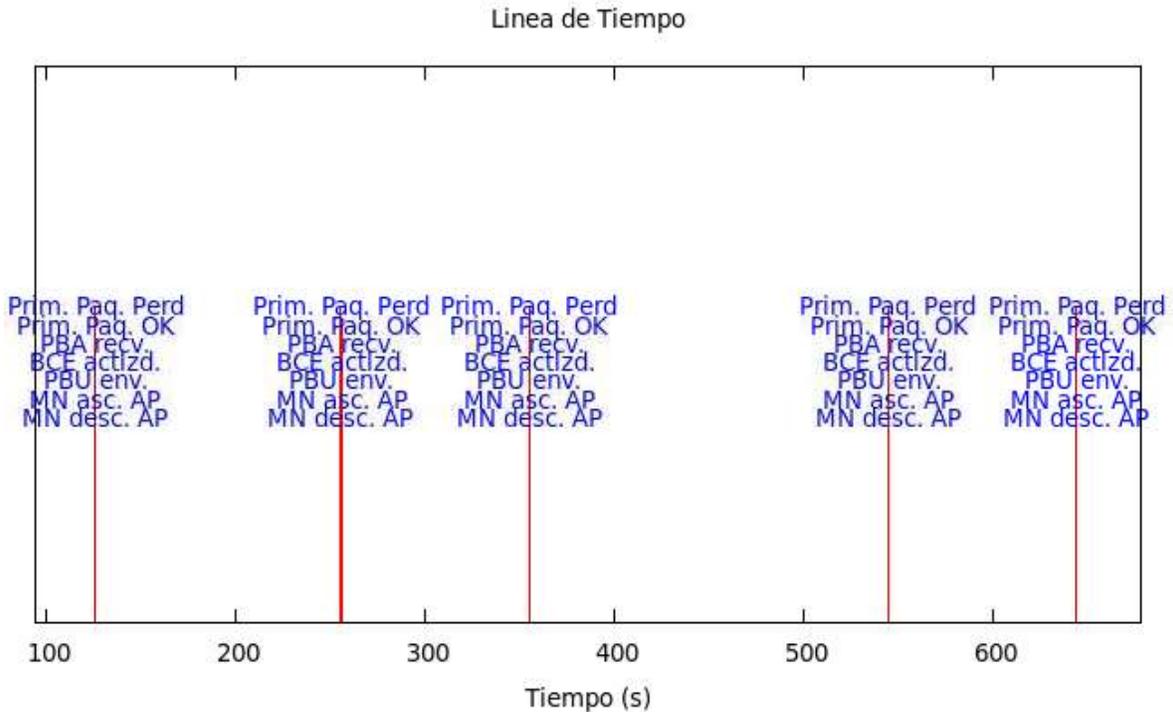


Figura 4.4. Ocurrencia de los *Handover* en una Línea de Tiempo para el caso 1a.

Con la Figura 4.4, se pueden determinar los instantes de tiempo aproximados en los que se realizaron los *handover* generados en la simulación, como lo muestra la Tabla 4.5.

No. de <i>Handover</i>	Tiempo aproximado en que se realizó
<i>Handover 1</i>	125.9s
<i>Handover 2</i>	255.5s
<i>Handover 3</i>	354.9s
<i>Handover 4</i>	544.6s
<i>Handover 5</i>	643.9s

Tabla 4.5. Momento aproximado en el que se realizó cada *handover* para el caso 1a.

La Figura 4.5, muestra con detalle la ocurrencia del primer *Handover*, con el fin de conocer los eventos y el instante en el que se llevan a cabo.

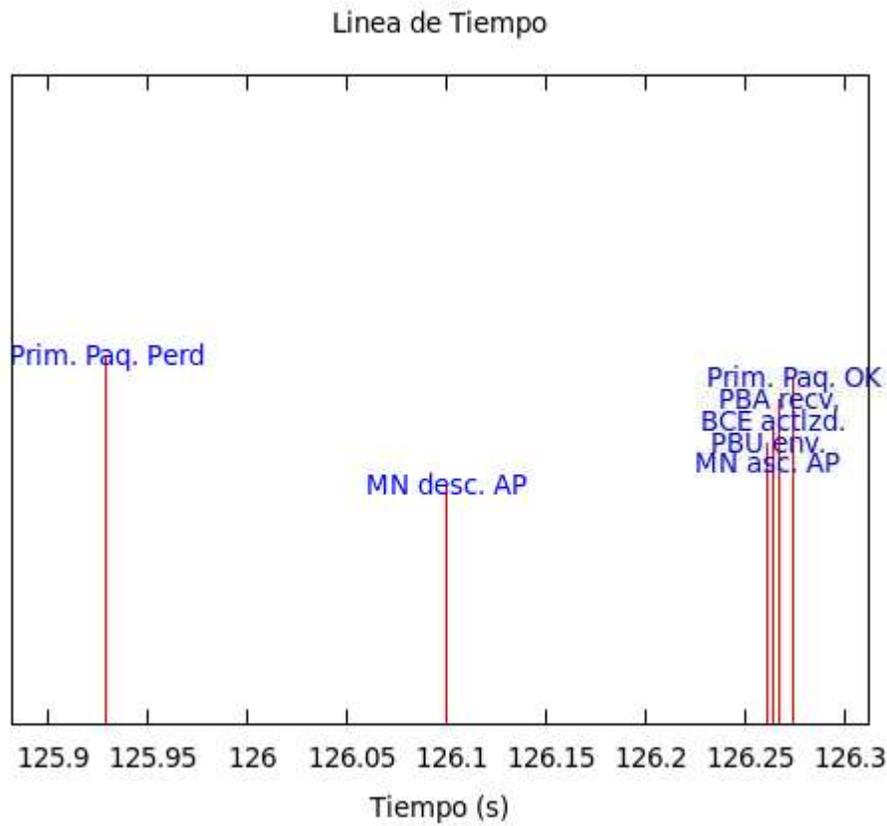


Figura 4.5. Ocurrencia del primer *Handover* para el caso 1a.

En la Tabla 4.6 indican los diferentes eventos ocurridos durante el *handover*, y el instante preciso en el que se realizó cada uno. El *handover* (HO) tuvo una duración de 0.344774569 segundos y en él se perdieron 37 paquetes como lo muestra más adelante la Tabla 4.7.

Eventos ocurridos durante el HO	Tiempo del evento
1) Primer Paquete Perdido	125.929s
2) Desconexión del MN del AP	126.100s
3) Asociación del MN al nuevo AP	126.261s
4) PBU enviado	126.261s
5) BCE Actualizada	126.267s
6) PBA Recibido	126.270s
7) Primer Paquete Recibido después del HO	126.274s

Tabla 4.6. Eventos importantes durante un *handover* para el caso 1a.

- **Pérdida de Paquetes**

Durante cada *handover*, se generó una leve pérdida de paquetes. Según los datos arrojados por el simulador, durante el tiempo de simulación, se enviaron 74851 paquetes hacia el MN de los cuales se recibieron 74676, dándose por perdidos 175 paquetes, distribuidos como lo muestra la Tabla 4.7. Además, muestra los tiempos utilizados por el nodo móvil en cada traspaso.

No. de <i>Handover</i>	Tiempo Utilizado	No. de Paquetes Perdidos
<i>Handover 1</i>	0.344774569s	37
<i>Handover 2</i>	0.308148073s	32
<i>Handover 3</i>	0.355608066s	37
<i>Handover 4</i>	0.308308074s	32
<i>Handover 5</i>	0.337648067s	37

Tabla 4.7. Duración de los *Handover* y No. de Paquetes Perdidos para el caso 1a.

De la Tabla anterior se concluye que el tiempo promedio para realizar un *Handover* es aproximadamente 0,3308973698 segundos y los paquetes perdidos en promedio durante este tiempo son 35.

En la Figura 4.6, se puede observar el histograma de los paquetes en la comunicación, donde la barra azul representa los paquetes enviados, la barra verde los recibidos y la pequeña barra roja representa a los paquetes que no pudieron ser entregados en recepción.

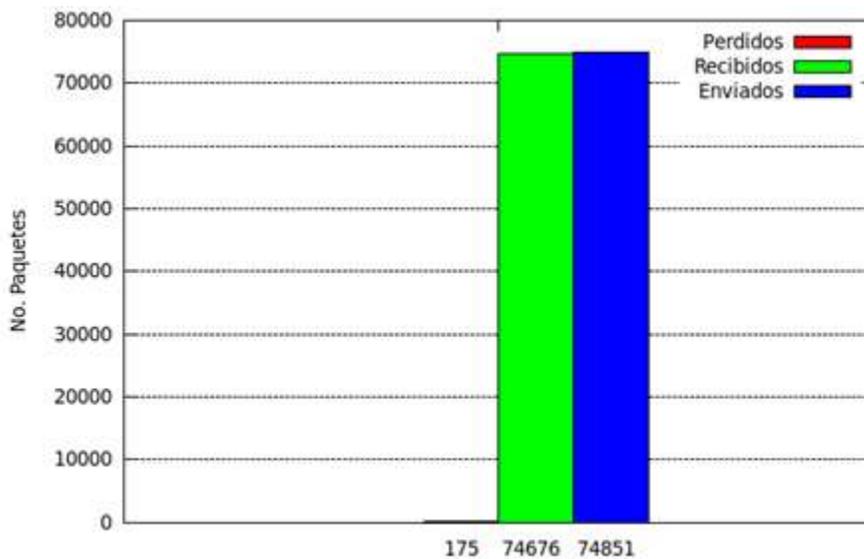


Figura 4.6. Histograma de Paquetes para el caso 1a.

La Figura 4.7, muestra la tasa de pérdidas de paquetes generada durante cada uno de los *handover* presentados en la simulación de este caso. Las gráficas b, c, d, representan los *handover* 1, 3 y 5 respectivamente (se abstraen las gráficas de estos tres *handover* con el fin de realizar un análisis para las mismas y teniendo en cuenta que todas son muy parecidas). Haciendo una comparación entre estas y la Tabla 4.7 donde se presenta el tiempo de duración de cada *handover*, se observa que el tiempo de duración de la tasa de pérdidas, es un poco más largo que la duración del *handover* en sí. Esto debido a que en el momento preciso en que se inicia el traspaso, el antiguo AP mantiene a los paquetes en cola para ser retransmitidos. Las retransmisiones se realizan 7 veces por cada paquete, acumulando un tiempo en cola antes de que los mismos sean descartados por el nodo. De esta manera cuando el nodo móvil se conecta al nuevo AP, todavía existen paquetes a la espera de ser retransmitidos y por último descartados, por lo que la duración del tiempo en el que se genera pérdida de paquetes es mayor a la duración del proceso de *handover* en sí.

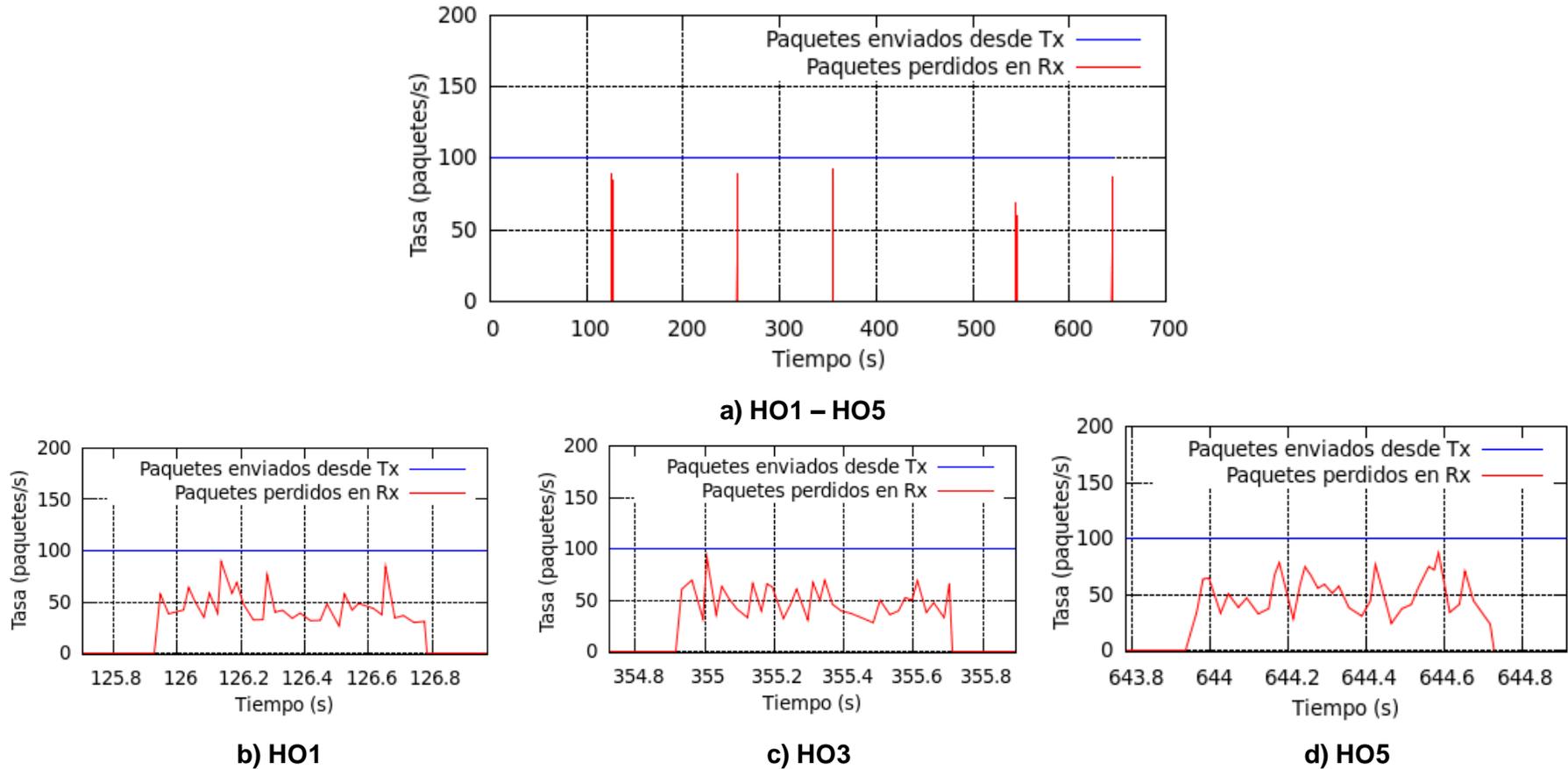


Figura 4.7. Tasa de Pérdida de Paquetes durante los Handover 1, 3 y 5 realizados por el MN para el caso 1a.

- **Throughput**

Como se mencionó en el capítulo 2, el *throughput* permite conocer la tasa de transferencia de datos en una comunicación. De esta manera, en la Figura 4.8 a), se puede observar la gráfica arrojada por el simulador, donde se aprecia que antes y después de los *handover*, la tasa de transmisión es relativamente constante, mientras que durante los lapsos en los cuales se presentan los *handover*, la capacidad del enlace es nula. Esto debido a que la desconexión que sufre el MN durante los mismos, no permite que todos los paquetes transmitidos sean entregados correctamente al receptor.

Las Figuras 4.8 b), c), y d), muestra el *throughput* de cada uno de los *handover* ocurridos durante la comunicación. Las caídas observadas en las gráficas, concuerdan con el momento aproximado en el cual se realiza la desconexión (Ver Tabla 4.5).

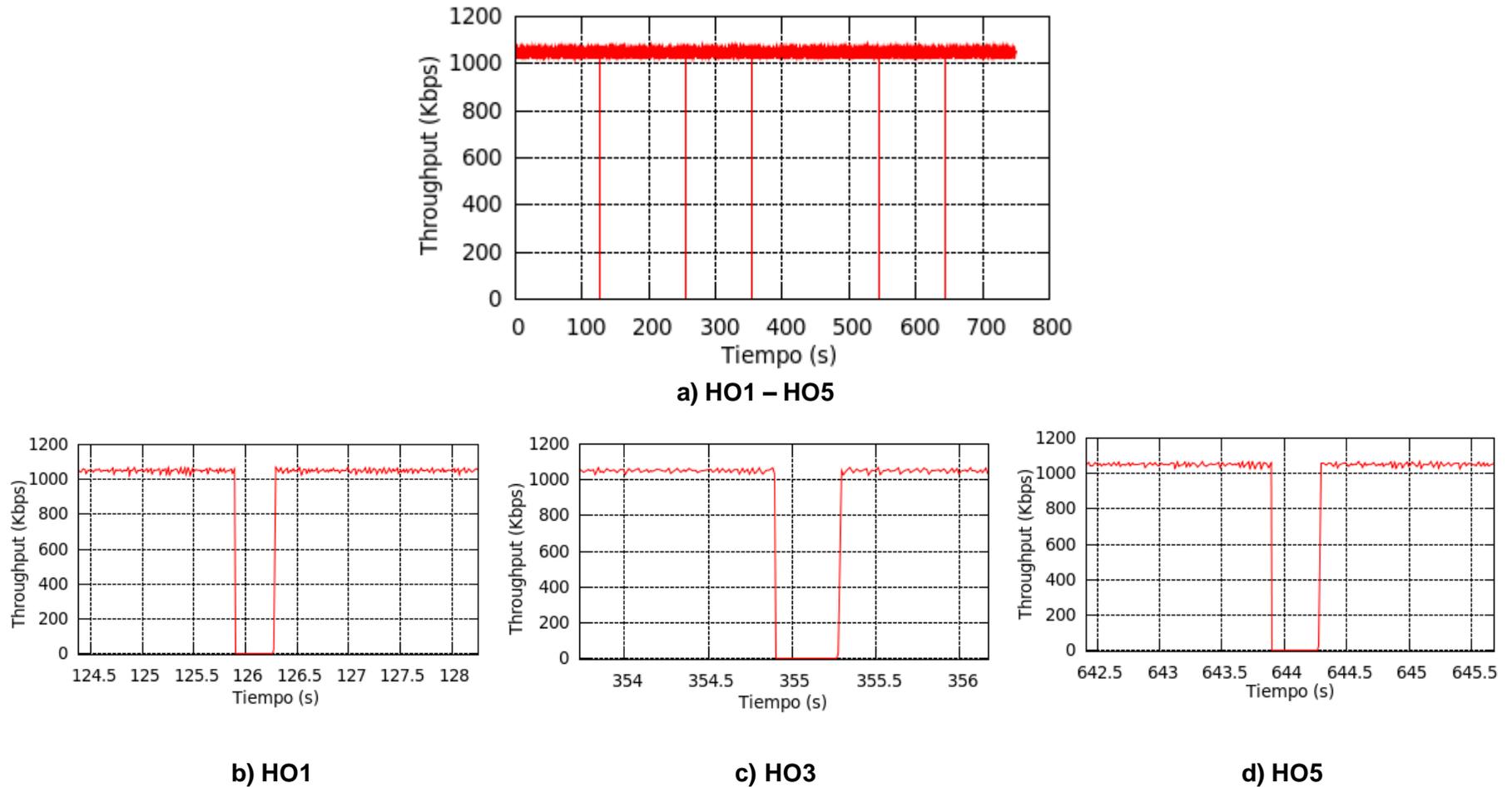


Figura 4.8. Comportamiento del *Throughput* durante los *Handover* 1, 3 y 5 realizados por el MN para el caso 1a.

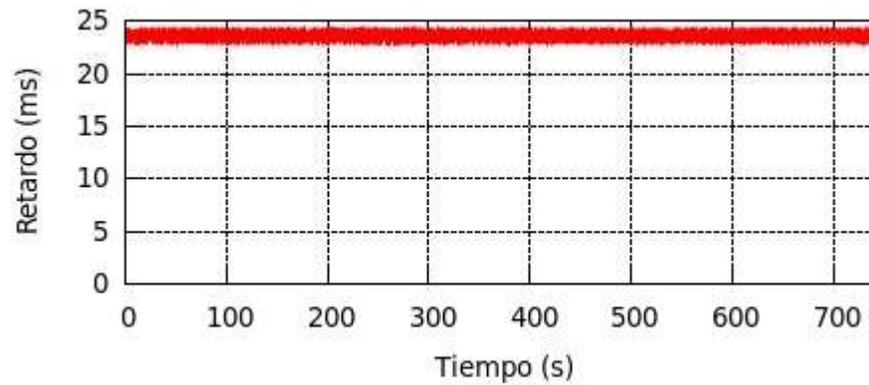
- **Retardo y Jitter**

La recomendación G.1010 de la ITU-T [33], expresa que el retardo máximo admitido en aplicaciones que requieran la transmisión de audio y video en tiempo real para asegurar las condiciones óptimas de QoS es de 150 ms, característica realmente estricta para servicios de voz de dos vías y videotelefonía, enmarcados dentro de un entorno conversacional. Sin embargo, para aplicaciones como el *streaming* de audio y video en una sola vía no son tan restrictivas respecto al retardo, tolerando valores de hasta 10 s, como se muestra en la Figura 2.3, referenciada en el capítulo 2.

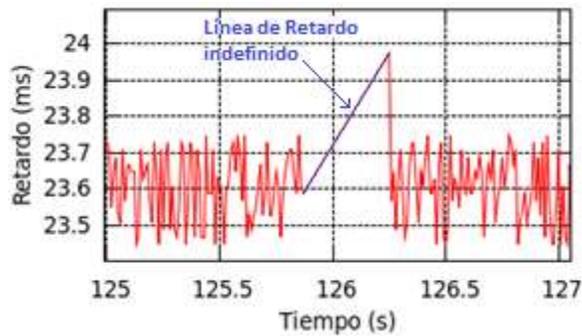
Las gráficas 4.9. a), b), c) y d), muestran que antes y después del proceso de *handover* realizado por el MN, el retardo es relativamente constante. El retardo siempre está variando entre 23.45ms y 23.75ms. Esto debido a que se está trabajando en un ambiente de simulación perfecto. Sin embargo, si se realizaran las mismas pruebas en un ambiente real, los resultados serían diferentes tal y como se indica en [63], en el que las gráficas muestran una variación en el retardo justo antes de iniciar y justo después de terminar el proceso de *handover* respectivamente.

Cuando los paquetes se pierden durante un *handover*, el retardo de los mismos se hace indefinido dado que se tiene información de su tiempo de salida, más no se puede verificar su tiempo de llegada. En las gráficas, lo anterior está representado por la línea recta más larga (Figura 4.9 b). Se debe tener cuidado al interpretar dicha línea ya que no representa ningún valor de retardo y solo existe porque la herramienta de graficación la usa para unir sus dos puntos extremos (que si representan valores de retardo).

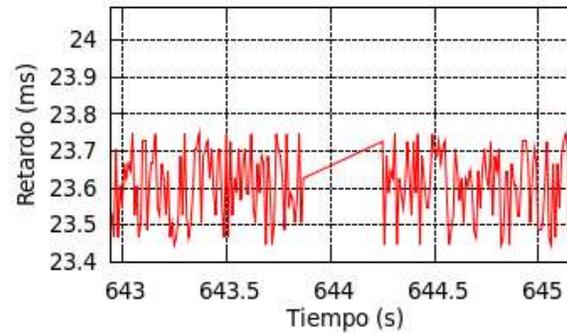
Se destaca que de las gráficas b), c), y d) solo la segunda muestra una elevación en forma de pico, la cual sobrepasa el valor de 23.9 ms. Esto se debe a que en el primer *handover* realizado, cuando el nodo se conecta al segundo AP por primera vez durante toda la simulación, aun no se ha establecido una ruta que permita alcanzar al nodo en ese AP. El establecimiento o cálculo de una ruta hacia un dispositivo, requiere que los dispositivos de red (que funcionen en la capa 3 del modelo OSI), se comuniquen entre si informando de las redes que se pueden alcanzar a través de ellos. La señalización utilizada en este proceso es la que introduce retardos adicionales. El pico en las gráficas restantes, correspondientes a los *handover* 3 y 5 respectivamente, desaparece debido a que las rutas ya se han establecido y no es necesario recalcularlas.



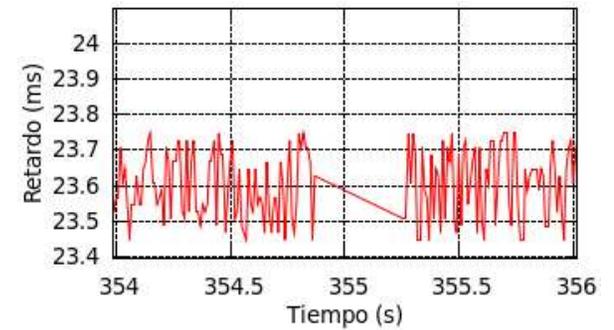
a) HO1 – HO5



b) HO1



c) HO3



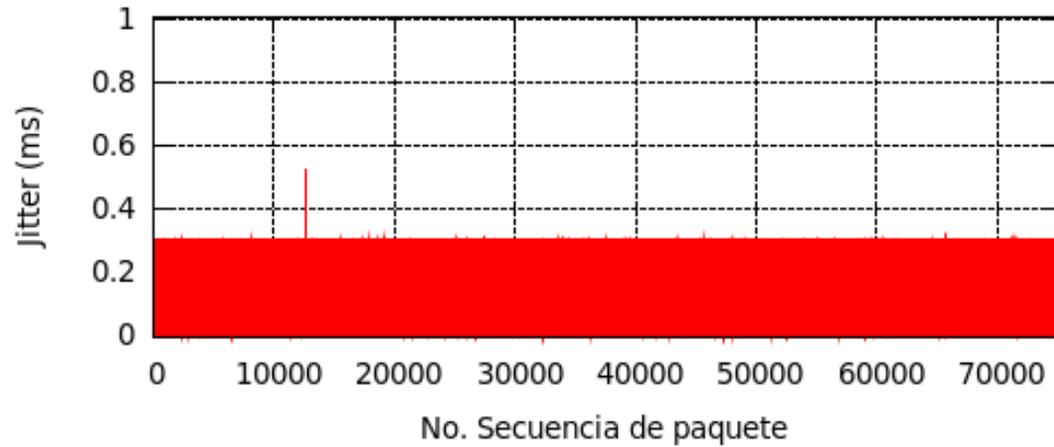
d) HO5

Figura 4.9. Comportamiento del Retardo durante los *Handover* 1, 3 y 5 realizados por el MN para el caso 1a.

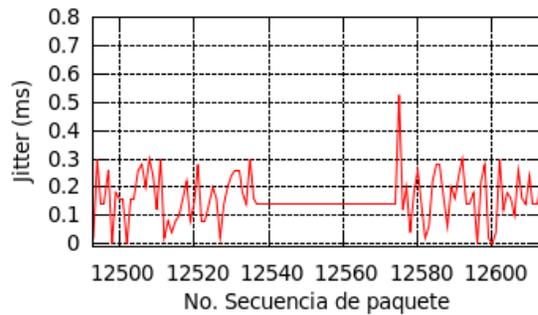
Otro parámetro importante para servicios prestados en tiempo real, y que se mencionó en el capítulo 2, es el *jitter*. Este es un parámetro capaz de alterar la fluidez de las aplicaciones de audio y video dependiendo de su valor. Según [33], el valor requerido de *jitter* para el servicio de voz en dos vías es de 1ms, debido a la sensibilidad del oído humano ante la variación del retardo en la voz. El *streaming* de audio requiere un *jitter* mucho menor a 1 ms esperando que la calidad ofrecida por este servicio sea mejor que la ofrecida por el servicio de telefonía convencional. Sin embargo, para servicios como video en un solo sentido, la recomendación G.1010 [33], no especifica valor alguno. El *jitter* no impacta de manera notable el tráfico de datos, ya que su efecto generalmente no es apreciable por el usuario. Por esta razón, este tipo de tráfico no recibe especial consideración respecto a este parámetro.

La Figura 4.10 a), presenta el tiempo de simulación total y el comportamiento del *jitter* durante este. Las Figuras restantes b), c), y d) presentan el mismo comportamiento para los *handover* 1, 3 y 5 respectivamente. De esta manera se observa que la variación de retardo permanece casi constante durante la simulación, viéndose afectada en los instantes en los que se presentan los *handover*, debido a la pérdida de paquetes durante los mismos. Al igual que en el retardo, la línea más larga no representa ningún valor de *jitter*, (*jitter* indefinido), y solo es usada por la herramienta de graficación para unir dos puntos extremos que si representan valores de *jitter*.

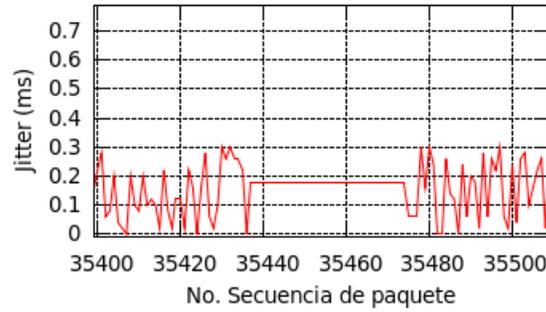
El pico que existe en la primera gráfica se debe al retardo adicional generado por el cálculo de ruta, como se explicó anteriormente para el retardo.



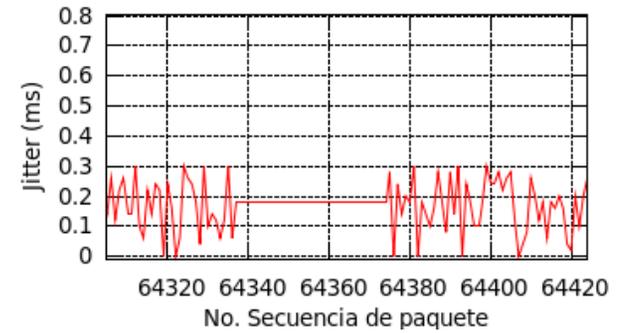
a) HO1 – HO5



b) HO2



c) HO3



d) HO5

Figura 4.10. Comportamiento del *Jitter* durante los *Handover* 1, 3 y 5 realizados por el MN para el caso 1a.

4.2.4.1.2 Caso 1b: Un MN con movimiento aleatorio.

En este caso, durante el tiempo de simulación se realizaron 4 procesos de *handover*. El nodo móvil se mueve aleatoriamente.

- **Ocurrencia de los Handover**

En la Figura 4.11, se observa en una línea de tiempo, la ocurrencia de cada uno de los 4 *handover*.

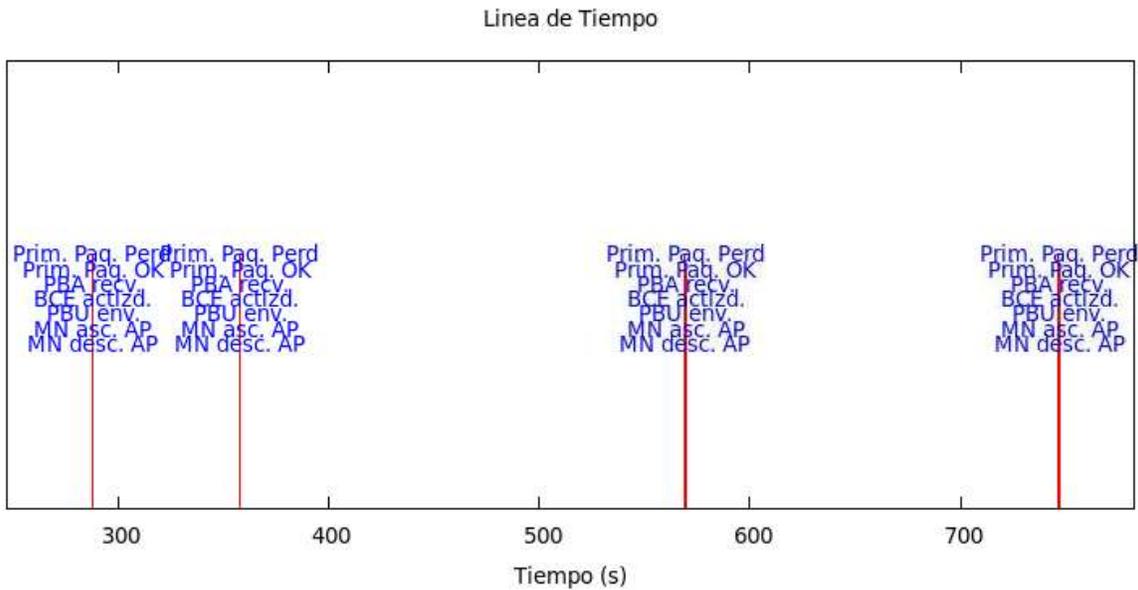


Figura 4.11. Ocurrencia de los *Handover* en una Línea de Tiempo para el caso 1b.

El instante en el que se realizó cada proceso de *handover* se puede observar en la Tabla 4.8.

No. de <i>Handover</i>	Tiempo aproximado en que se realizó
<i>Handover 1</i>	287.7s
<i>Handover 2</i>	357.742s
<i>Handover 3</i>	569.1s
<i>Handover 4</i>	746.721s

Tabla 4.8. Instante aproximado en el que se realizó cada *handover* para el caso 1b.

- **Pérdida de Paquetes**

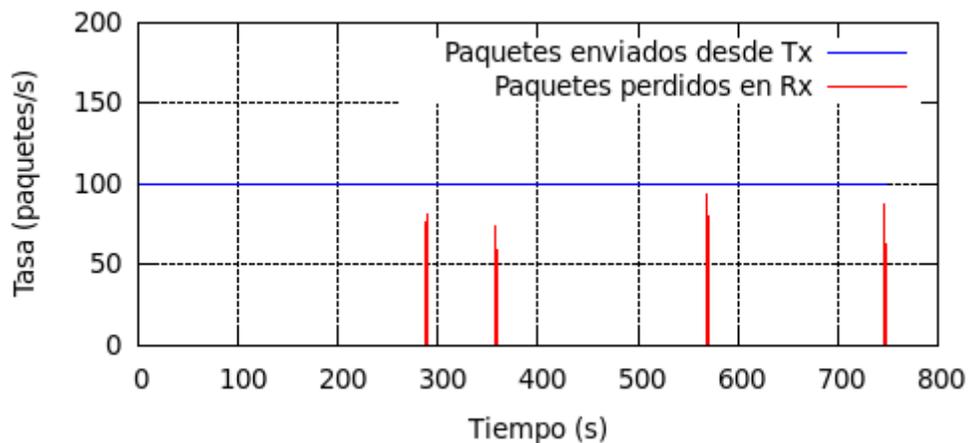
Durante el proceso de simulación se enviaron 74851 paquetes hacia el MN de los cuales se recibieron 74716, resultando 135 paquetes perdidos, distribuidos como lo muestra la Tabla 4.9. Además, la misma muestra los tiempos utilizados por el MN en cada traspaso.

No. de Handover	Tiempo Utilizado	No. de Paquetes Perdidos
Handover 1	0.339734000s	37
Handover 2	0.252851502s	29
Handover 3	0.354409014s	39
Handover 4	0.271948052s	30

Tabla 4.9. Duración de los *Handover* y No. de Paquetes Perdidos para el caso 1b.

De la Tabla anterior se concluye que el tiempo promedio para realizar un *handover* es aproximadamente 0,304735642s y los paquetes perdidos en promedio durante este tiempo son 33.75. Comparando estos resultados con la Tabla 4.6 del caso 1a, se alcanza a notar una disminución en los tiempos de *handover* y por lo tanto en la pérdida de paquetes en cuyo caso su promedio fue de 35. La causa de esto es que en el primer caso en el cual el MN se movía controladamente se realizaron 5 HO, mientras que durante el mismo tiempo para el segundo caso en el que el MN se movía aleatoriamente se realizaron solo 4 HO, disminuyendo de esta manera el número de paquetes perdidos.

En la Figura 4.12 a), se muestran los *handover* ocurridos durante el tiempo de simulación, y las Figuras b) y c), muestran la tasa de pérdidas de paquetes que se generó durante los *handover* 1 y 3 respectivamente (al igual que en el caso anterior de seleccionan solo algunas gráficas para los respectivos análisis). Se puede observar, que respecto al primer caso, este caso no presenta muchas diferencias, ya que el tiempo de duración de la tasa de pérdida de paquetes sigue siendo mayor al tiempo que dura el *handover*, análisis que se realizó para el caso 1a.



a) HO1 – HO5

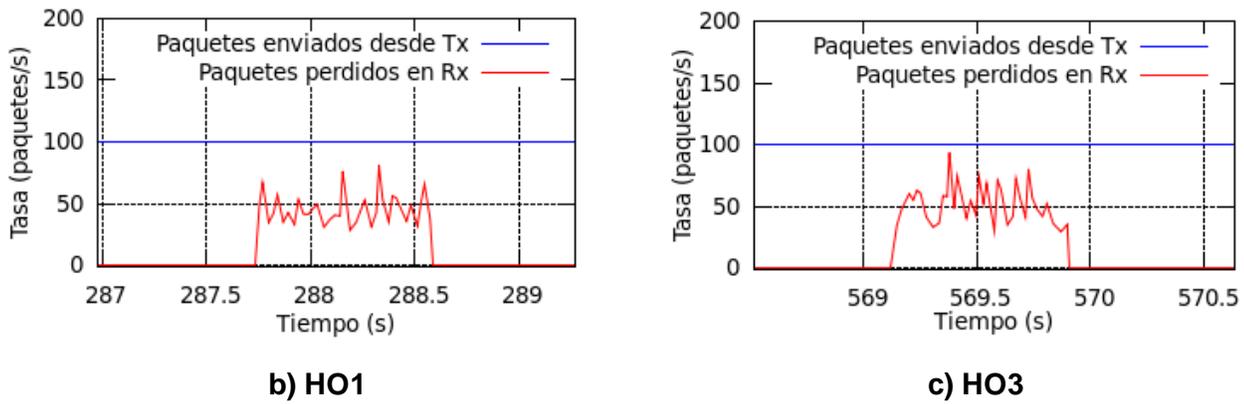
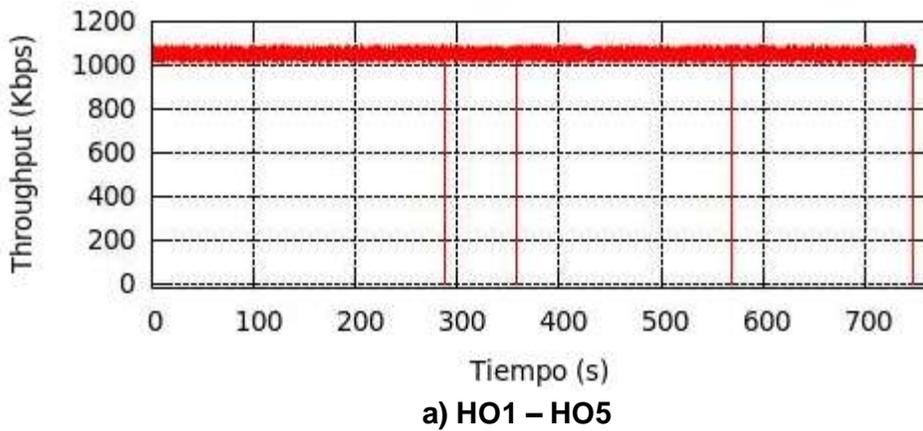


Figura 4.12. Tasa de Pérdida de Paquetes para los *Handover* 1 y 3 realizados por MN para el caso 1b.

- **Throughput**

En la Figura 4.13 a), b), y c) se destaca que la tasa de transmisión de datos durante el tiempo que dura cada uno de los *handover* es nula, como paso para el caso 1a. Las caídas observadas en las gráficas concuerdan con el momento en el cual se realiza la desconexión (Ver Tabla 4.8).



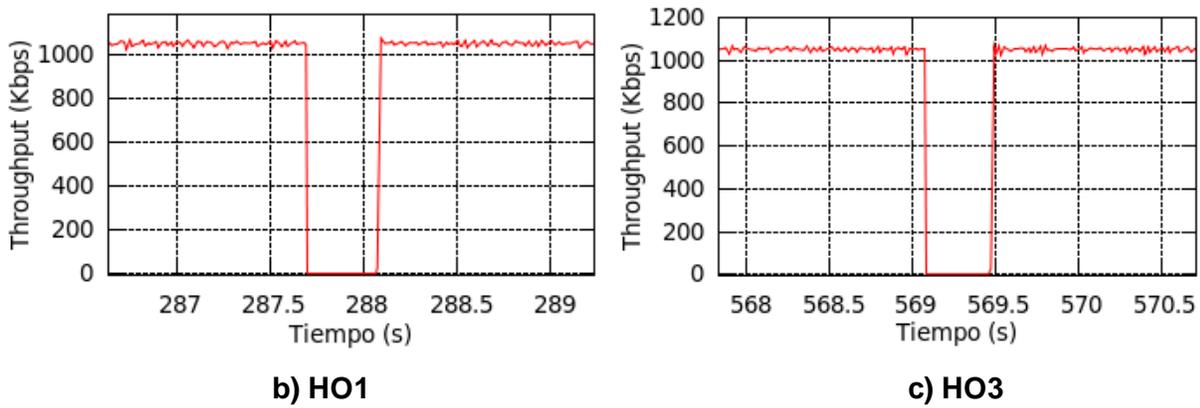
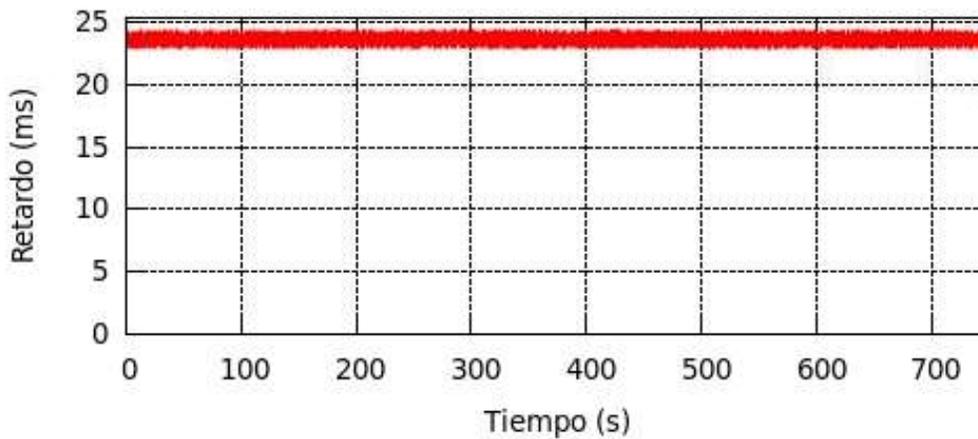


Figura 4.13. Comportamiento del *Throughput* durante los *Handover* 1 y 3 realizados por el MN para el caso 1b.

- **Retardo y Jitter**

La Figura 4.14 a), b), c), y d) muestran que el retardo varía constantemente entre 23.45 ms y 23.75 ms. En comparación con el caso 1a, el retardo varía entre los mismos valores, por lo cual la diferencia es casi nula. El análisis para estas gráficas concuerda con lo expresado para el caso 1a.



a) HO1 – HO5

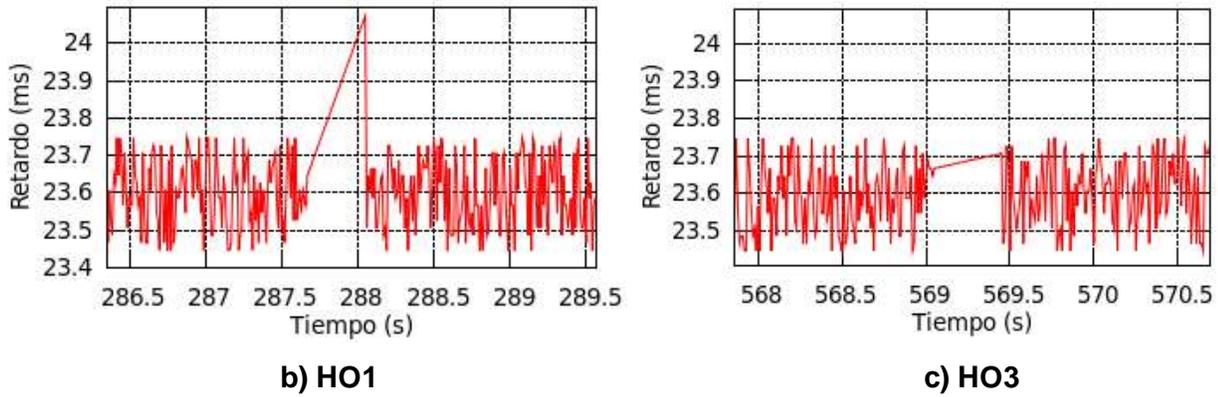
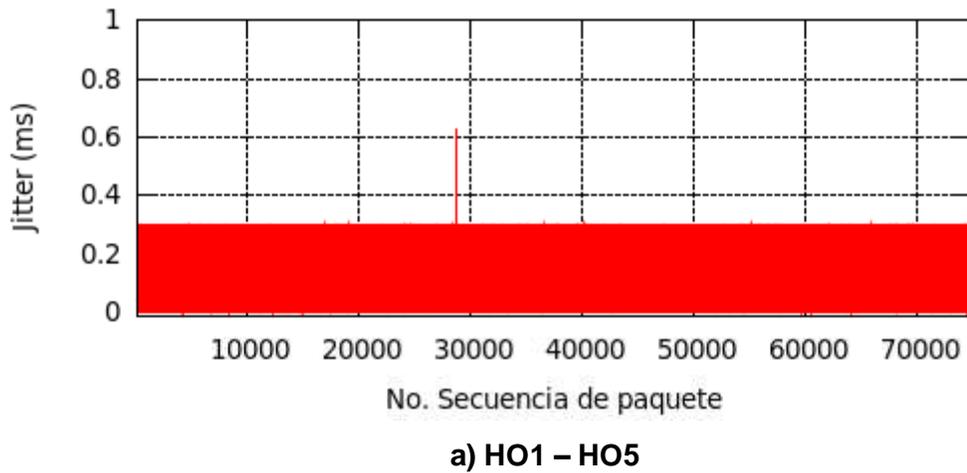


Figura 4.14. Comportamiento del Retardo durante los *handover* 1 y 3, realizados por el MN para el caso 1b.

La Figura 4.15 a), b), y c) presenta el comportamiento del *jitter* durante la comunicación. Al igual que en el caso 1a, este parámetro permanece casi constante antes y después de cada *handover*. Durante estos procesos el valor del *jitter* es indefinido como se expresó anteriormente para el caso 1a.



a) HO1 – HO5

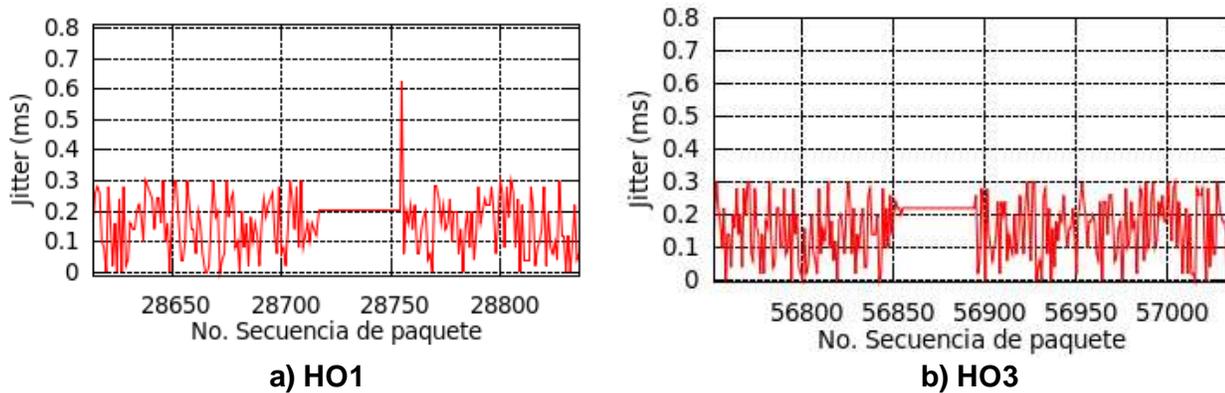


Figura 4.15. Comportamiento del *Jitter* durante los *Handover* 1 y 3 realizados por MN para el caso 1b.

4.2.4.2 Escenario 2.

4.2.4.2.1 Caso 2a: Un Nodo Móvil con Movimiento Controlado.

Para el caso en mención, se realizaron 5 procesos de *handover* durante el tiempo de simulación. El nodo móvil se mueve del punto 1 al punto 2 por la trayectoria rectangular indicada en la Figura 4.16.

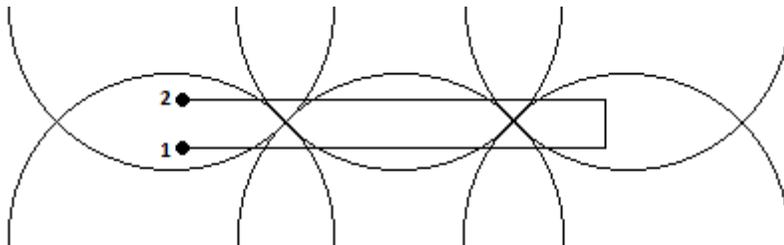


Figura 4.16. Trayectoria del nodo móvil para el caso 2a.

- **Ocurrencia de los *Handover***

En la Figura 4.17, se observa en una línea de tiempo, la ocurrencia de cada uno de los 5 *handover*.

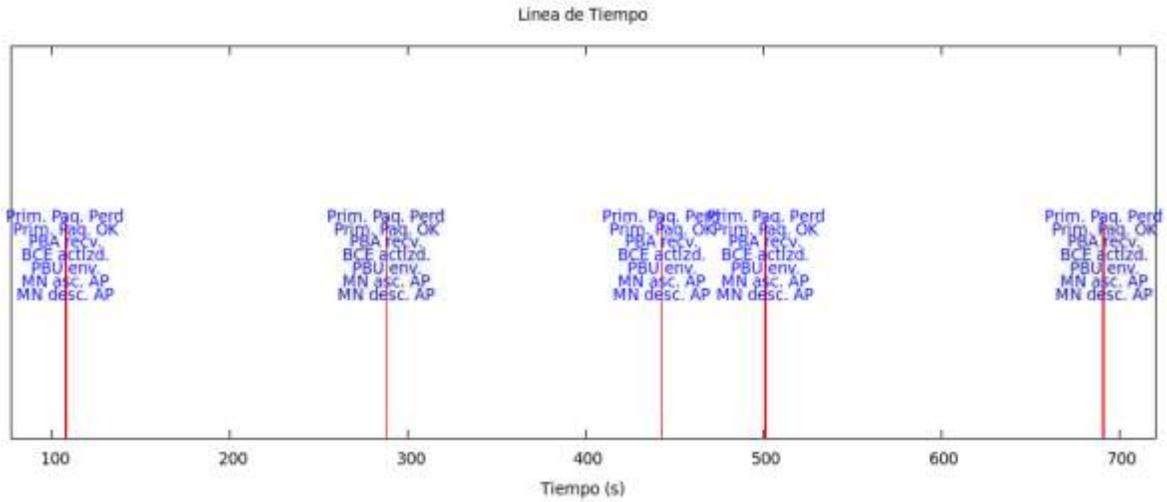


Figura 4.17. Ocurrencia de los *Handover* en una Línea de Tiempo para el caso 2a.

Con la Figura anterior se puede determinar el instante aproximado en el que se dio lugar cada *handover*, como lo muestra la Tabla 4.10.

No. de <i>Handover</i>	Tiempo aproximado en que se realizó
<i>Handover 1</i>	107.2s
<i>Handover 2</i>	287.5s
<i>Handover 3</i>	442.3s
<i>Handover 4</i>	500.7s
<i>Handover 5</i>	690.9s

Tabla 4.10. Instante aproximado en el que se realizó cada *handover* para el caso 2a.

- **Pérdida de Paquetes**

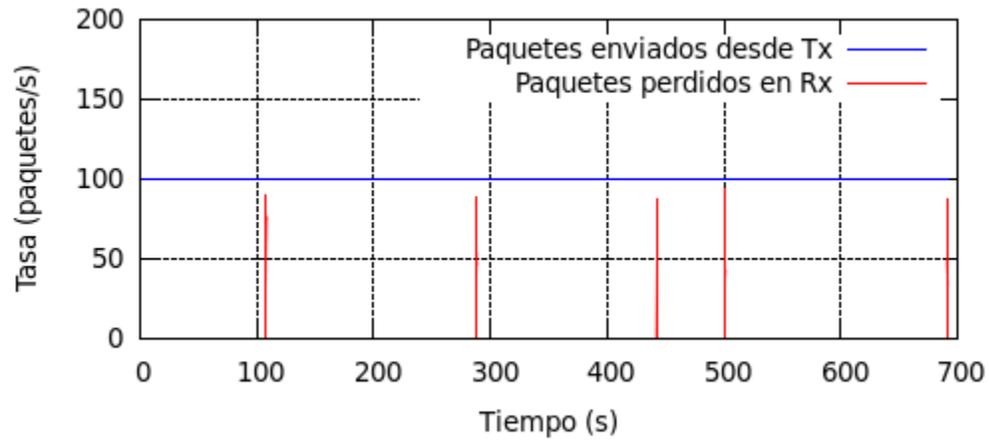
Según los datos arrojados por el simulador, durante el tiempo de simulación, se enviaron 74851 paquetes hacia el MN de los cuales se recibieron 74643, perdiéndose 208 paquetes, distribuidos como lo muestra la Tabla 4.11. Además, la misma muestra los tiempos utilizados por el MN en cada traspaso.

No. De <i>Handover</i>	Tiempo Utilizado	No. De Paquetes Perdidos
<i>Handover 1</i>	0,394754542	42
<i>Handover 2</i>	0,481214630	50
<i>Handover 3</i>	0,399254359	42
<i>Handover 4</i>	0,260234584	27
<i>Handover 5</i>	0,457207759	47

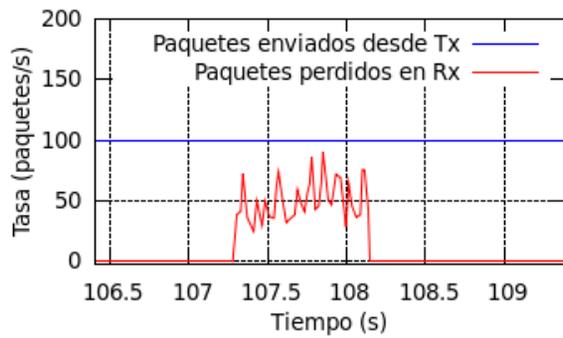
Tabla 4.11. Duración de los *Handover* y No. de Paquetes Perdidos para el caso 2a.

De la Tabla anterior se concluye que el tiempo promedio para realizar un *handover* es aproximadamente 0.39853317s y los paquetes perdidos en promedio son 41.6. Comparada con las Tablas anteriores (4.6 y 4.8), en este escenario tanto el tiempo de duración del *handover* como la pérdida de paquetes es mayor. Esto debido a que el escenario de simulación para este caso es más grande y en cada *handover* el MN establece conexión con un AP diferente, haciendo que los tiempos de traspaso sean más largos y por lo tanto que las pérdidas de paquetes aumenten.

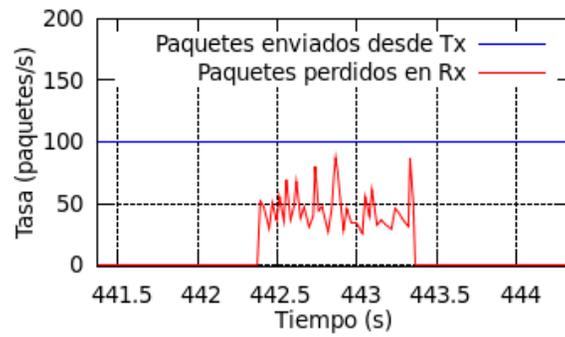
La Figura 4.18 a), muestra a nivel general la tasa de pérdidas generadas durante el tiempo de simulación, mientras que las Figuras restantes b), c) y d) muestran la tasa de pérdidas de paquetes durante los *handover* 1, 3 y 5 (como se planteó para los casos anteriores) que realizó el MN durante la simulación. Al igual que en los casos anteriores el tiempo de pérdida es mayor al que dura el proceso de *handover*, como se explicó para el caso 1a.



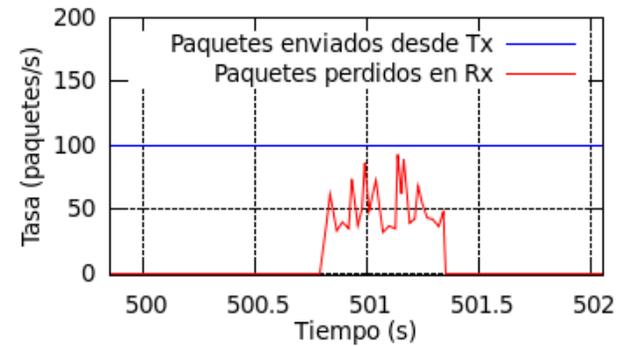
a) HO1 – HO5



b) HO1



c) HO3

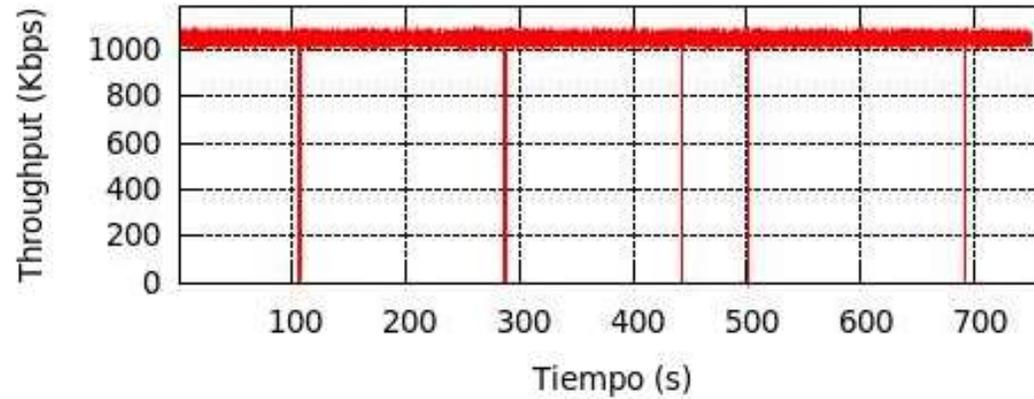


d) HO5

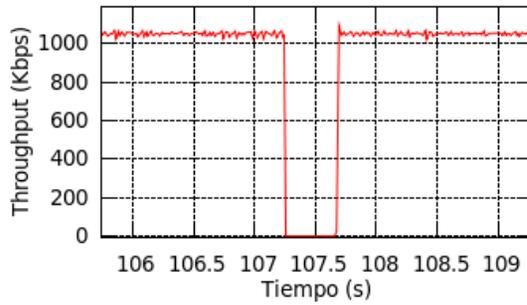
Figura 4.18. Tasa de Perdida de Paquetes durante los Handover 1, 3 y 5 realizados por el MN para el caso 2a.

- **Throughput**

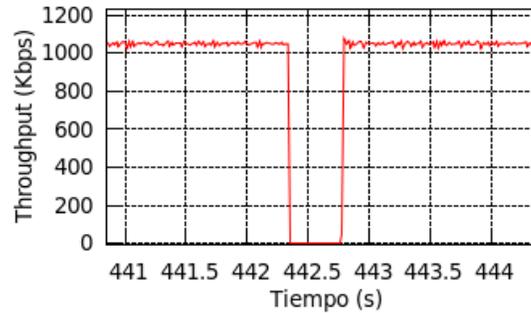
La Figura 4.19 a), b), c) y d), muestran que el *throughput* de cada uno de los *handover* ocurridos durante la comunicación se reduce a cero. Las caídas observadas en las gráficas, concuerdan con el instante en el cual se realiza la desconexión (Ver Tabla 4.9).



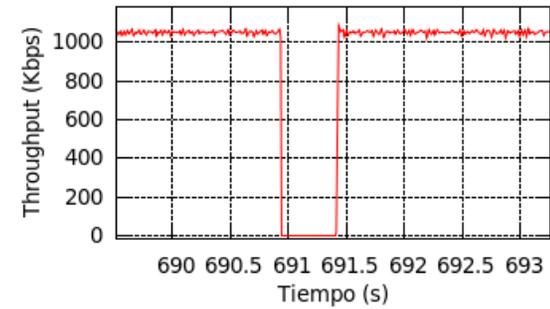
a) HO1 – HO5



a) HO1



b) HO3



c) HO5

Figura 4.19. Comportamiento del *Throughput* durante los *Handover* 1, 3 y 5 realizados por el MN para el caso 2a.

- **Retardo y Jitter**

La Figura 4.20. a), muestra el comportamiento del retardo durante el tiempo de simulación. Las Figuras b), c) y d) muestran que el retardo en los *handover* 1, 3 y 5 respectivamente. El mismo, varía constantemente entre 23.3ms y 23.75ms, valores mencionados en los casos anteriores para este mismo apartado. La diferencia para este caso se presenta en los picos mostrados en las 3 Figuras y no únicamente en la primera, como en los casos anteriores. Este comportamiento es normal ya que en cada uno de los *handover* generados, el nodo móvil se conecta a un nuevo AP y por lo tanto siempre es necesario el cálculo de una nueva ruta.

La Figura 4.21 a), muestra el comportamiento del *jitter* durante el tiempo de simulación, mientras que las Figuras b), c) y d) presentan el comportamiento del *jitter* durante los *handover* 1, 3 y 5 respectivamente. Al igual que en el caso 1a, este parámetro permanece casi constante antes y después de cada *handover*. Los picos de las gráficas se deben al cálculo de nuevas rutas como se explicó anteriormente. El análisis restante concuerda con lo expresado para el caso 1a.

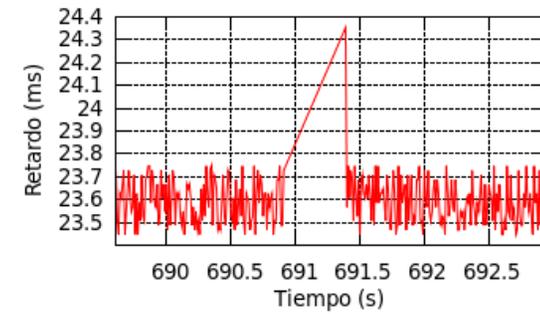
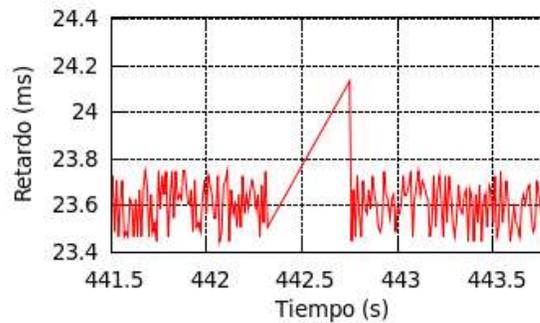
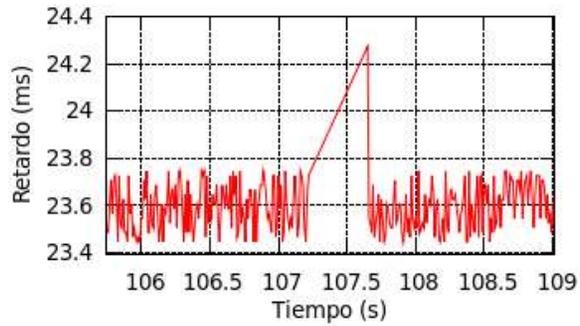
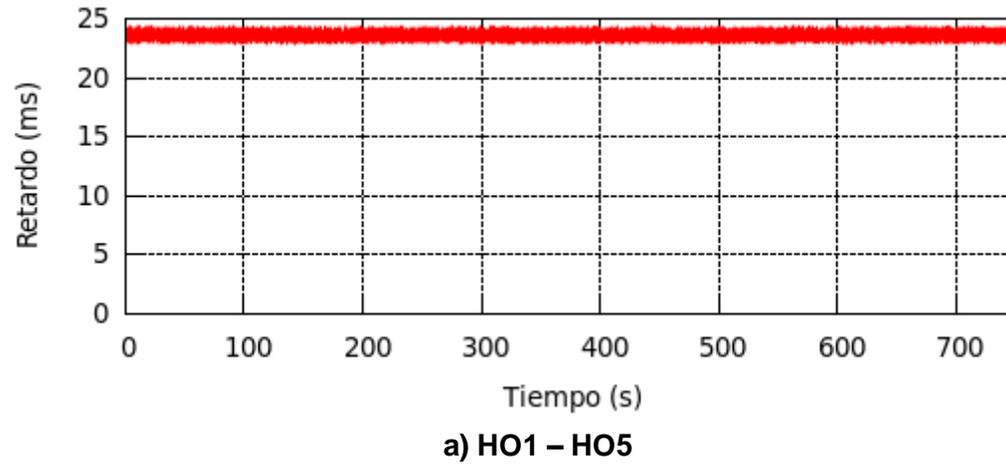
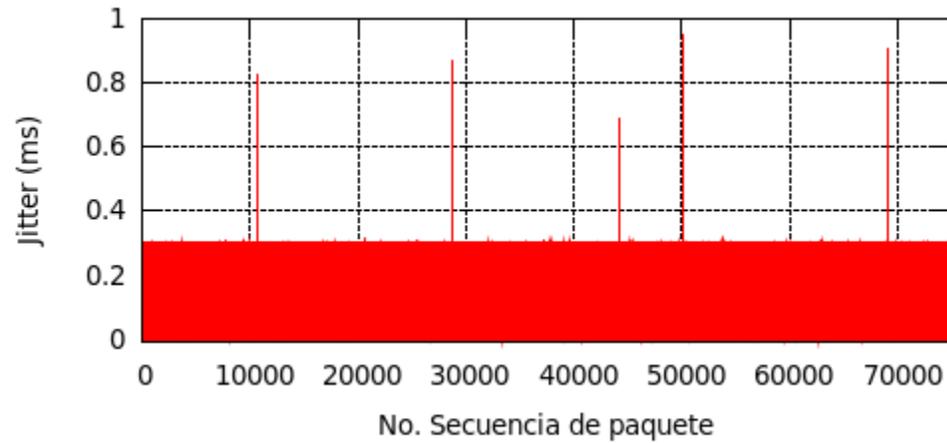
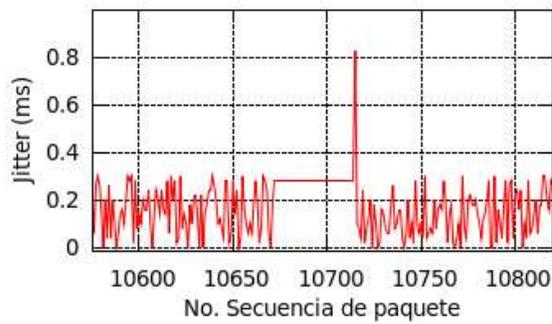


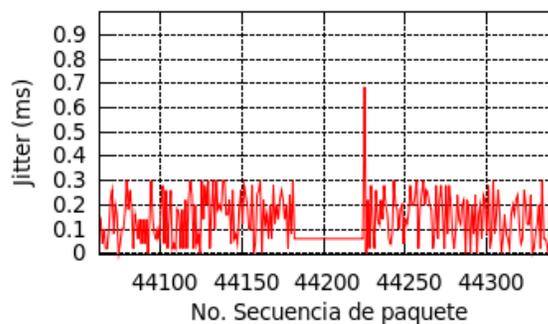
Figura 4.20. Comportamiento del Retardo durante los *Handover* 1, 3 y 5 realizados por el MN para el caso 2a.



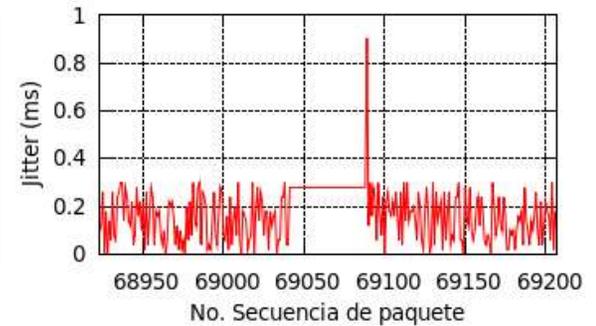
a) HO1 – HO5



a) HO1



b) HO3



c) HO5

Figura 4.21. Comportamiento del *Jitter* durante los *Handover* 1, 3 y 5 realizados por el MN para el caso 2a.

4.2.4.2.2 Caso 2b: Un MN con movimiento aleatorio.

Durante el tiempo de simulación se realizaron 8 procesos de *handover*. Hay que tener en cuenta que el nodo tiene un movimiento aleatorio en el escenario planteado.

- **Ocurrencia de los Handover**

En la Figura 4.22, se observa en una línea de tiempo, la ocurrencia de cada uno de los 8 *handover*.

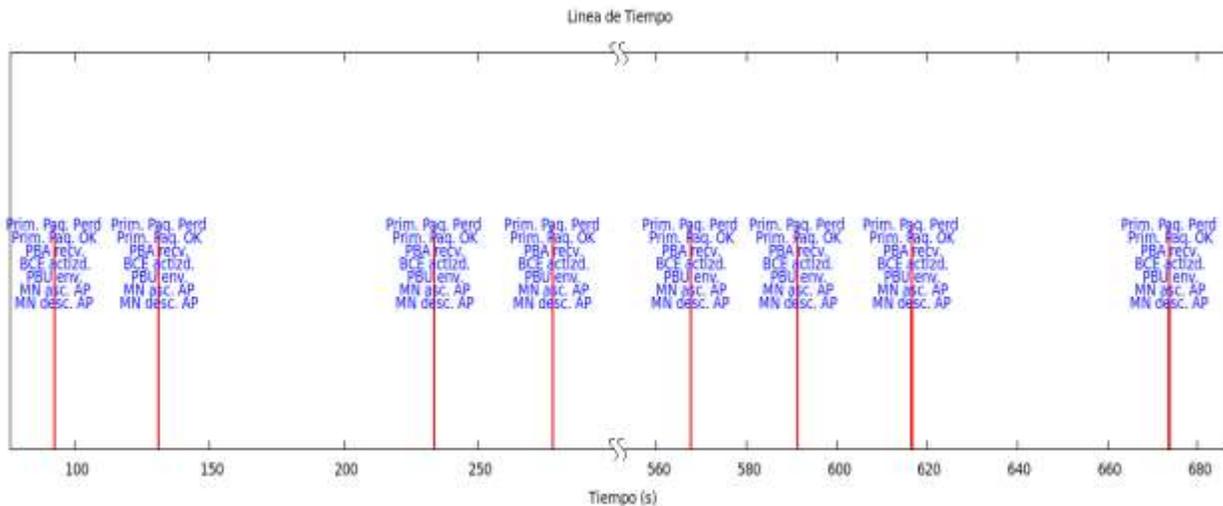


Figura 4.22. Ocurrencia de los *Handover* en una Línea de Tiempo para el caso 2b.

La Tabla 4.12 muestra los instantes de tiempo en los que tuvieron lugar los *handover* ocurridos durante el tiempo de simulación.

No. de <i>Handover</i>	Tiempo aproximado en que se realizó
Handover 1	91.9s
Handover 2	130.8s
Handover 3	233.3s
Handover 4	277.4s
Handover 5	567.3s
Handover 6	591.1s
Handover 7	616.3s
Handover 8	673.4s

Tabla 4.12. Instante aproximado en el que se realizó cada *handover* para el caso 2b.

- **Pérdida de Paquetes**

Durante la simulación se enviaron 74851 paquetes hacia el MN de los cuales se recibieron 74547, ocurriendo una pérdida de 304 paquetes, distribuidos como lo muestra

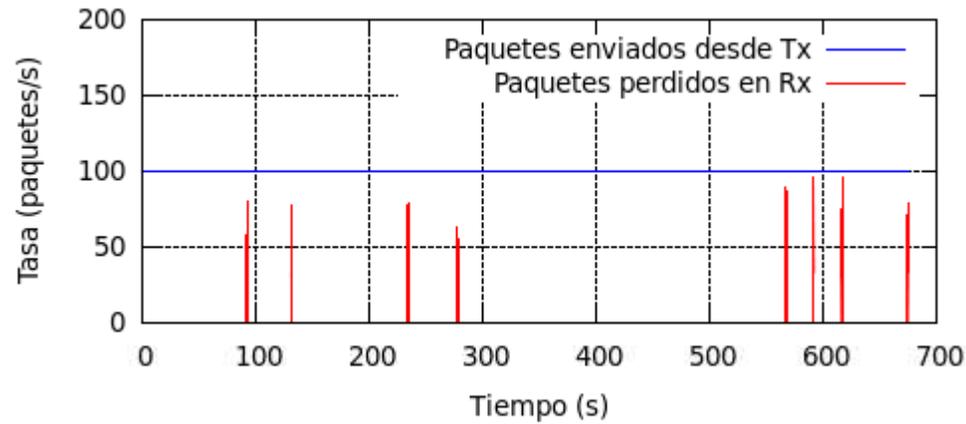
la Tabla 4.13 a continuación. Además, la misma muestra los tiempos utilizados por el MN en cada traspaso.

No. De Handover	Tiempo Utilizado	No. De Paquetes Perdidos
Handover 1	0.308614986s	34
Handover 2	0.319754971s	34
Handover 3	0.441874633s	46
Handover 4	0.276487865	31
Handover 5	0.359166094	38
Handover 6	0.315248075	33
Handover 7	0.360066170	39
Handover 8	0.454693981	49

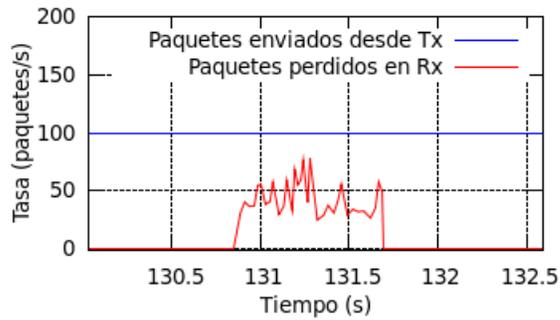
Tabla 4.13. Duración de los *Handover* y No. de Paquetes Perdidos para el caso 2b.

De la Tabla anterior se concluye que el tiempo promedio para realizar un *handover* es aproximadamente 0,354488347s y los paquetes perdidos en promedio son 38. Comparando estos resultados con la Tabla 4.9 del caso 2a, aunque los tiempos tomados por cada *handover* y los paquetes perdidos durante los mismos sean menores, hay que tener en cuenta que para este caso, se realizaron 3 *handover* más que para el caso anterior por lo que la pérdida de paquetes total resulta mayor que en el caso anterior.

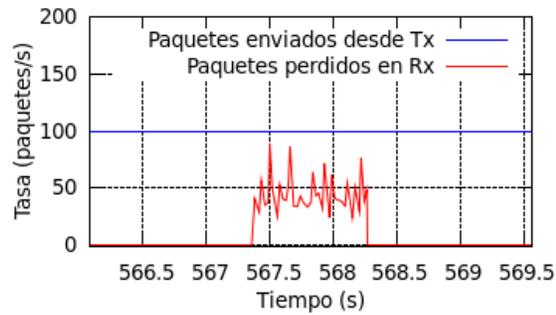
La Figura 4.23 a), muestra la tasa de pérdidas ocasionada durante el tiempo de simulación. En las Figuras restantes, b), c) y d), se muestra la tasa de pérdidas de paquetes que se generó para los *handover* 2, 5 y 8 respectivamente (Figuras seleccionadas para el análisis de este caso). Se observa, que respecto a los casos anteriormente analizados, este caso no presenta muchas diferencias, ya que el tiempo durante la pérdida de paquetes sigue siendo mayor al tiempo que dura el *handover*, análisis que se realizó para el caso 1a.



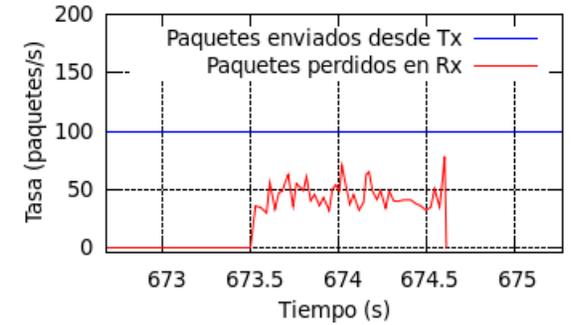
a) HO1 – HO8



b) HO2



c) HO5

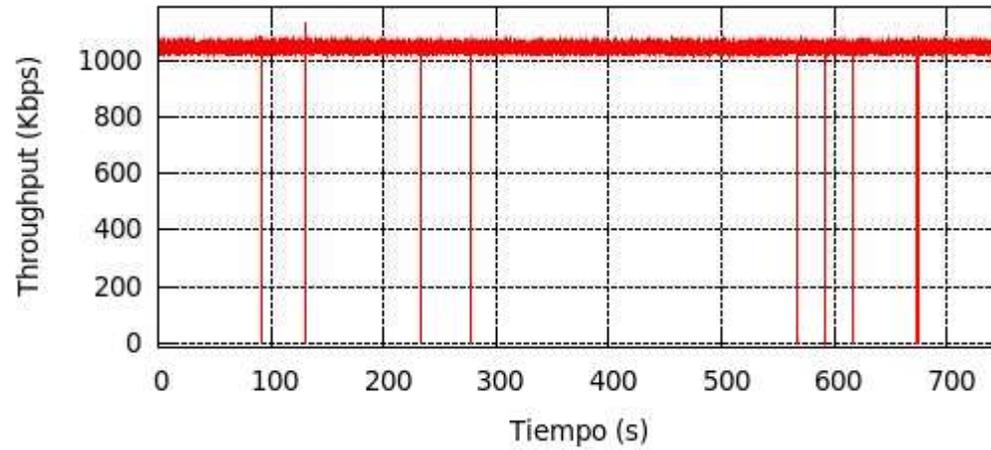


d) HO8

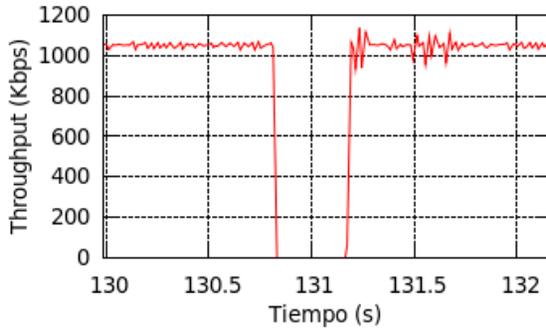
Figura 4.23. Tasa de Perdida de Paquetes durante los *Handover* 2, 5 y 8 realizados por MN para el caso 2b.

- **Throughput**

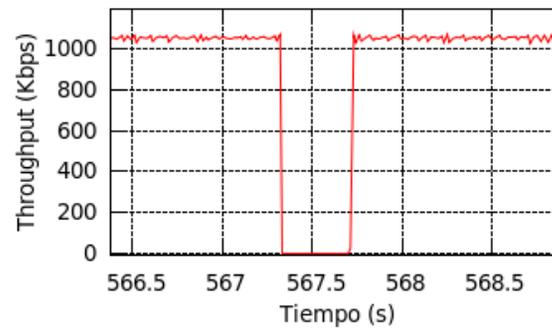
En las Figuras 4.24 a), b), c) y d), al igual que en los casos analizados anteriormente, se observa que la capacidad durante el tiempo que dura cada uno de los *handover* es nula. Las caídas observadas en las gráficas, concuerdan con momento en el cual se realiza la desconexión (Ver Tabla 4.11). De las 8 gráficas de *throughput* arrojadas por el simulador, solo en la segunda se resaltan picos de inestabilidad justo después del *handover*. Pruebas aisladas y análisis se realizaron para determinar el origen de dicha inestabilidad y se concluyó que se presenta cuando el nodo móvil realiza un *handover* entre dos APs que transmiten en un mismo canal. La gráfica con inestabilidad mostrada corresponde al *handover* realizado entre las MAGs 1 y 5, las cuales transmiten en el canal 1.



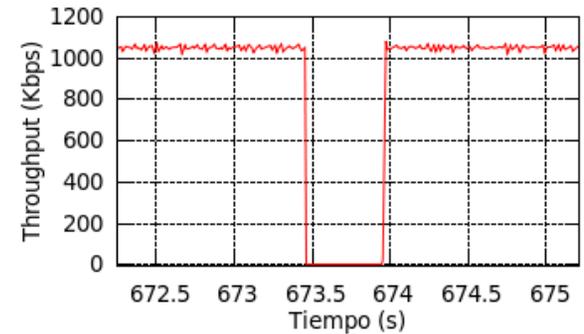
a) HO1 – HO8



b) HO2



c) HO5



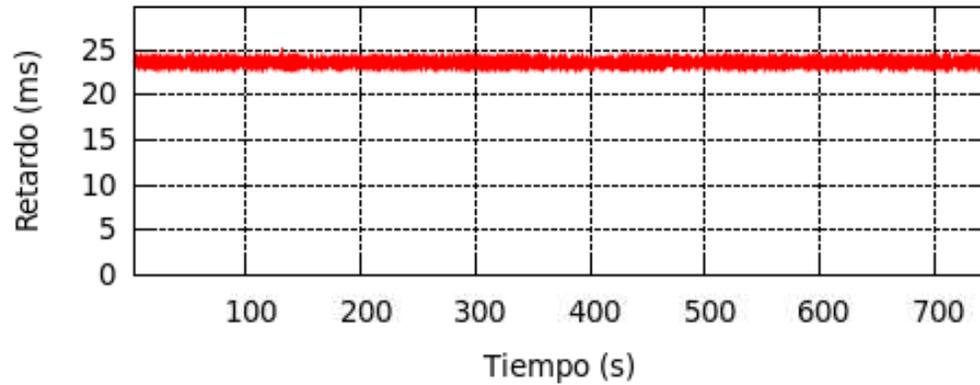
d) HO8

Figura 4.24. Comportamiento del *Throughput* durante los *Handover* 2, 5 y 8 realizados por el MN para el caso 2b.

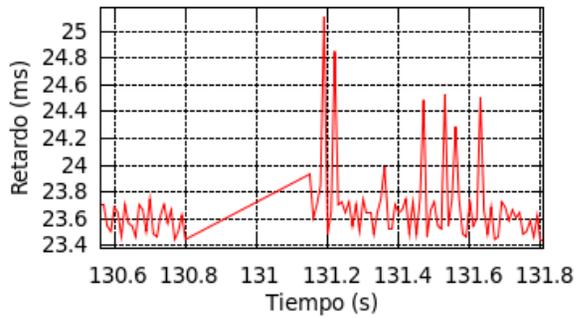
- **Retardo y Jitter**

La gráfica 4.25. a), muestra el comportamiento del retardo durante la simulación. Las gráficas restantes b), c) y d), representan los *handover* 2, 5 y 8 respectivamente. Se observa que la variación del retardo es casi constante antes y después del proceso de *handover*, como sucede en los casos 1, 2 y 3. Su variación se encuentra generalmente entre los 23.45ms y 23.75ms, al igual que en los casos mencionados, por lo que el análisis para estas gráficas concuerda con lo expresado para el caso 1a. Como sucedió con el *throughput*, la Figura b) HO2 presenta inestabilidad después del realizar el proceso. La explicación para esto está dada en el apartado anterior.

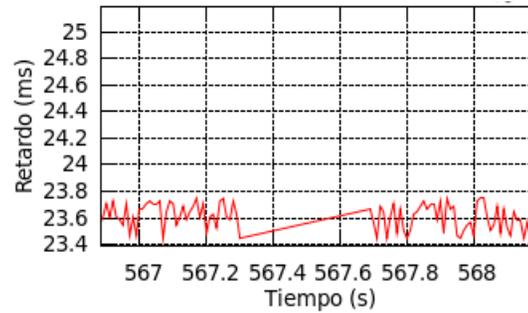
La Figura 4.26 a), presenta el comportamiento del *jitter* durante el tiempo de simulación. Las Figuras b), c) y d) representan los *handover* 2, 5 y 8 respectivamente. Al igual que en el caso 1a, este parámetro permanece casi constante antes y después de cada *handover*. La inestabilidad que se observa en la segunda gráfica se presenta por la misma razón explicada anteriormente para el *throughput*.



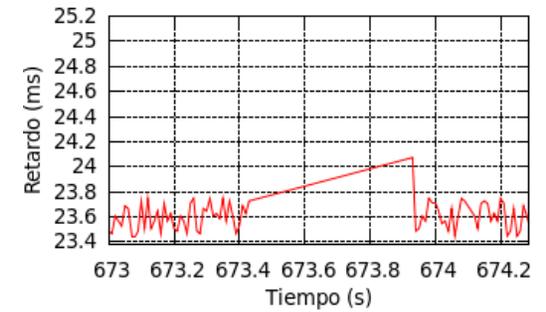
a) HO1 – HO8



b) HO2

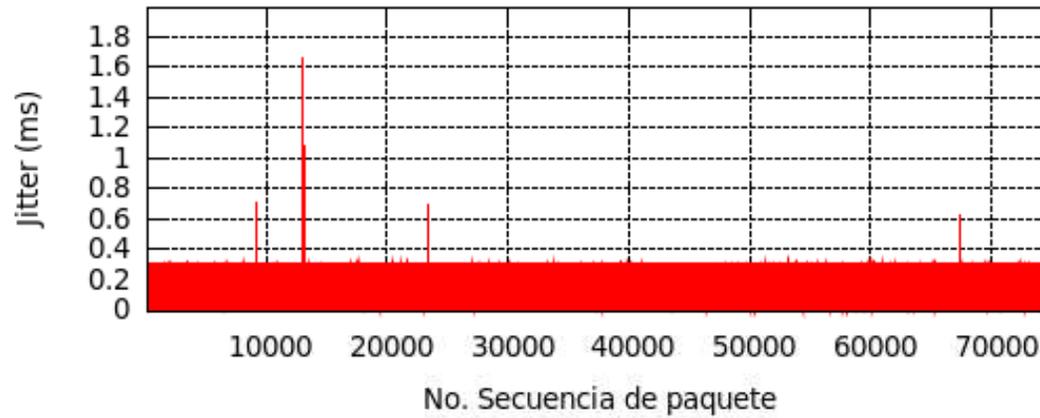


c) HO5

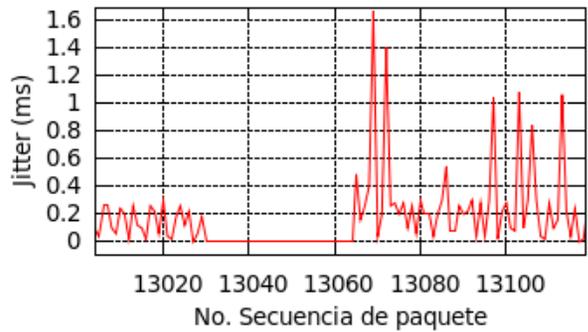


d) HO8

Figura 4.25. Comportamiento del Retardo durante los *Handover* 2, 5 y 8 realizados por el MN para el caso 2b.



a) HO1 – HO8



b) HO2



c) HO5



d) HO8

Figura 4.26. Comportamiento del *Jitter* durante los *Handover* 2, 5 y 8 realizados por el MN para el caso 2b.

Después de realizar los respectivos análisis para cada caso descrito, la Tabla 4.14, presenta una comparación en los resultados de los parámetros de QoS para los mismos, con el fin de llegar a una conclusión general en la que se visualice cuál de los casos arroja mejores resultados. Sin embargo, se observa que estos parámetros presentan resultados constantes en los casos analizados. La diferencia radica en el número de paquetes perdidos que mantiene una relación directamente proporcional con el número de *handover* presentados durante la simulación en cada caso. De esta manera entre mayor sea el número de HOs, será mayor el número de paquetes perdidos y por lo tanto la comunicación podrá presentar más fallas y/o verse más afectada por los mismos efectos. Esta situación se hace más crítica cuando el MN se mueve por un dominio que contiene un mayor número de MAGs, ya que éste podrá conectarse a un nuevo AP en cada *handover*, extendiendo el tiempo de duración del proceso y por lo tanto generando una mayor pérdida de paquetes.

Además, se observa en la Tabla 4.14, que mientras el MN mantenga un movimiento aleatorio va a realizar un número de *handover* variable según el tiempo de simulación y el recorrido que haga. Sin embargo, la variación del mismo MN cuando se mueve controladamente, puede ser nula, debido a que el mismo mantiene un recorrido específico definido por los autores del proyecto.

	Movimiento del MN	# de HOs	# de Paquetes Perdidos	Throughput	Retardo	Jitter
ESCENARIO 1						
CASO 1a	Controlado	5	175	0 Kbps	Indefinido	Indefinido
CASO 1b	Aleatorio	4	135	0 Kbps	Indefinido	Indefinido
ESCENARIO 2						
CASO 2a	Controlado	5	208	0 Kbps	Indefinido	Indefinido
CASO 2b	Aleatorio	8	304	0 Kbps	Indefinido	Indefinido

Tabla 4.14. Parámetros de QoS durante los HOs presentados en la comunicación.

4.3 RECOMENDACIONES DE MOVILIDAD SEGÚN LOS RESULTADOS OBTENIDOS

Con las simulaciones ejecutadas se puede observar que es necesario realizar mejoras en el proceso de *handover* con el fin de reducir su retardo y por lo tanto la pérdida de paquetes durante el mismo, problema comúnmente presentado en las redes móviles.

A continuación se presentan algunas recomendaciones para esto:

- Debido a las deficiencias e incompatibilidad presentadas por los protocolos de movilidad, se hace necesario que en un futuro se realice una integración de los mismos para permitir la utilización de tecnologías que puedan aprovechar las ventajas que ofrecen las redes móviles, con el fin de que durante las

comunicaciones se realice el proceso de *handover* de una formas transparente al usuario, permitiendo que servicios con requerimientos en tiempo real puedan ser ofrecidos con altos niveles de calidad.

- Debido a la dependencia que existe entre el cambio de conexión físico y lógico durante el *handover* y que no es suficiente un mecanismo de *handover* en capa física que funcione a la perfección, si el reingreso a la red no es lo suficientemente óptimo para evitar las afectaciones presentadas durante este proceso, es necesario una asociación entre estas capas, L2 y L3 (*Cross-layer*), para que el mecanismo funcione óptimamente, quizá negociando una dirección IP antes de comenzar el proceso de *handover* con el fin de que la conexión a la red se realice de una manera más rápida, como lo plantea [64]. Por lo tanto es importante, acoplar las capas involucradas durante el proceso de *handover* con el fin de lograr un mejor comportamiento del mismo, y así evitar degradación en la calidad de servicio ofrecida a los usuarios.
- Se plantea el desarrollo de propuestas, donde se integren los protocolos de movilidad con diversas técnicas o mecanismos para que los retardos presentados durante el proceso de *handover* sean minimizados al máximo con el fin de evitar una pérdida de paquetes muy grande, de tal manera que la calidad del servicio prestado no se vea afectado en gran medida. Aunque hay muchas propuestas por ser desarrolladas, algunas de ellas ya existen y están siendo implementadas. Por ejemplo [65], propone una tunelización multicast para el protocolo HMIPv6-BI (*Hierarchical Mobile IPv6 with Bandwidth Improvement*), que con los resultados muestra que se reducen los tiempos de *handover*, mejorando este proceso en redes móviles.
- Se propone establecer estrategias que realicen un mejor control de tráfico y de congestión, para optimizar el uso de recursos de la red y por lo tanto asegurarle un trato adecuado al tráfico que circula por la misma, cumpliendo con los requerimientos de QoS establecidos.

Este capítulo presentó un análisis detallado de una comunicación móvil, antes, durante y después de la ocurrencia de los *handover*, para lo cual se tuvieron en cuenta algunos parámetros de QoS (pérdida de paquetes, *throughput*, retardo y *jitter*), utilizados para valorar el efecto que produce este proceso en una comunicación en un contexto de micromovilidad IPv6 con base a los resultados arrojados por la simulación en los 4 casos que componen el plan de pruebas.

El capítulo 5 presenta las conclusiones a las que se llegaron después del desarrollo del proyecto, recomendaciones y trabajos futuros que se pueden implementar con referencia a esta temática.

CAPITULO V. CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En este capítulo se presentan las conclusiones, recomendaciones y los trabajos futuros, resultado de la realización de este trabajo de grado. Las conclusiones se basan en los objetivos propuestos y en su desarrollo, lo que ha sido registrado en este documento. Las recomendaciones se dan acerca de la metodología de trabajo y los trabajos futuros con respecto a herramientas de simulación, protocolos de movilidad, y escenarios de simulación.

5.1 CONCLUSIONES

5.1.1 Respecto a la movilidad IPv6

- La extensión geográfica no está relacionada con el escenario de movilidad utilizado, pero sí con la topología de red propuesta. Se identifican dos escenarios de movilidad IP en los que se aplican diferentes protocolos de gestión: macromovilidad y micromovilidad IP. En el primer escenario los *handover* se presentan entre diferentes dominios administrativos mientras que en el segundo solo se presentan dentro de un único dominio.
- En un ambiente de comunicaciones móviles, es de suma importancia tener en cuenta los factores y parámetros que en cualquier momento pueden afectar un servicio de comunicaciones, con el fin de contrarrestar sus efectos y evitar una mala prestación de los mismos, ofreciendo a los usuarios una calidad adecuada para cualquier servicio.
- *Mobile IPv6* es un protocolo para ser usado en escenarios de macromovilidad, la señalización usada por este protocolo disminuiría su rendimiento si es usado en micromovilidad.
- Muchos protocolos de micromovilidad IPv6 se definen con base en *Mobile IPv6*, mediante extensiones realizadas a ese protocolo. *Hierarchical Mobile IPv6* y *Proxy Mobile IPv6* son dos de ellos.
- Las características de *Proxy Mobile IPv6* lo convierten un buen candidato para usarse en las redes que requieran soporte de movilidad. Este protocolo presenta bajo retardo de *handover* y especifica un número reducido de elementos de red que necesitan soportarlo.

5.1.2 Respecto al desarrollo de la simulación

- NS2 es una herramienta robusta para ser usada en pruebas con redes de telecomunicaciones. Cuenta con una amplia documentación y un gran soporte, y

permite la simulación de varios escenarios de movilidad IP. *Proxy Mobile IPv6* es soportado por esta herramienta.

- Los escenarios de simulación definidos caracterizan ambientes de micromovilidad IP. Para esto se establecieron topologías que cuentan con conexiones cableadas, tecnologías de acceso inalámbricas y áreas de cobertura, entre otros aspectos, de forma que tengan un gran parecido a un ambiente real pero conservando los límites que permiten obtener resultados que se puedan analizar.
- NS2 no cuenta con herramientas propias para realizar análisis de resultados, existen desarrollos de terceros que sirven para tal fin. Sin embargo los análisis con este simulador generalmente se realizan desarrollando utilidades propias y si es necesario con ayuda de herramientas de graficación de terceros.

5.1.3 Respecto a los resultados de la simulación

- En ambientes de micromovilidad IP, donde los *handover* se realizan entre un número limitado de puntos de acceso, es probable que el MN haga conexión dos o más veces con un mismo AP reduciendo la duración del proceso de *handover* y por lo tanto la pérdida de paquetes, ya que no es necesario realizar de nuevo el cálculo de rutas.
- En ambientes de micromovilidad IP donde exista un número considerable de puntos de acceso, el rendimiento del protocolo usado disminuye y la pérdida de paquetes y retardo de *handover* aumentan. Dependiendo del número de puntos de acceso el nodo móvil podrá asociarse a uno nuevo en cada *handover* presentado durante la comunicación lo que extenderá el tiempo de duración de los mismos, poniendo en riesgo la comunicación en curso.
- En un ambiente simulado no se observa ninguna variación del retardo de paquetes en los instantes justo antes de realizar un *handover*, mientras que un ambiente real el retardo aumenta en esos instantes. Dependiendo de la medida en la que el retardo aumente, los paquetes durante este tiempo pueden ser considerados o no como perdidos, aumentando el retardo de *handover*.
- En un ambiente de simulación, en los instantes justo después de un *handover* se puede presentar inestabilidad en cualquiera de los parámetros evaluados. Esto ocurre cuando el *handover* se realiza entre dos puntos de acceso que transmiten en un mismo canal.
- En un ambiente real, el retardo de *handover* y la pérdida de paquetes se reflejan en la calidad de imagen y audio que se reciben por el usuario. El video se puede ver afectado por pérdida de píxeles, de *cuadros de imagen* y de audio, saltos abruptos en la reproducción y desincronización entre video y audio.

- La fórmula matemática para obtener el *jitter* de los paquetes no es única, existen varias que pueden usarse dependiendo del escenario al que van dirigidas. Cuando en el escenario se presentan continuos cambios en la trayectoria de los paquetes, como es el caso en ambientes de movilidad, la mejor fórmula está definida en [43] bajo el nombre de *PDV*.

5.2 RECOMENDACIONES

- Para seleccionar una herramienta de simulación particular, es necesario hacer un estudio previo y profundo sobre las características de la misma, que permitan determinar si cumple con todos los requisitos que se planteen para los escenarios y condiciones a simular. Esto evita que se presenten inconvenientes al no obtener los datos útiles para un análisis valedero.
- Cuando se trabaje con herramientas de simulación libres, es recomendable que se conozcan todas las versiones existentes, y se seleccione la que mejor se adapte a los requisitos, tal como ocurre con NS-2, la cual tiene muchas versiones producto de las diferentes modificaciones o adiciones que se han hecho, y no todas funcionan de igual forma, así sea en el mismo contexto de uso.
- Cuando se trabaje con alguna de las versiones de NS2 es recomendable tener el código modificado o desarrollado bien organizado y con comentarios que describan el objetivo de cada línea del código. Si se tienen varios escenarios de simulación que comparten características en común es posible tener un escenario que sirve de plantilla, lo cual permitirá hacer pruebas y cambios mucho más rápido.
- Para realizar un análisis adecuado de los datos obtenidos en la simulación, particularmente en NS-2, se debe tener cuidado de realizar análisis con herramientas (scripts) creadas por terceros, pues en muchas ocasiones están no procesan los datos conforme a lo establece la teoría. Se debe analizar en profundidad si esta herramienta se puede aplicar para realizar el análisis en los escenarios propios, de lo contrario siempre es mejor desarrollar herramientas propias.
- De ser posible, es recomendable trabajar con programas licenciados, dado que estos poseen muchas herramientas útiles, que permiten el análisis de muchos más parámetros de red y de aplicación, y poseen muchos módulos de tecnologías, además de brindar soporte técnico.

5.3 TRABAJOS FUTUROS

- La herramienta de simulación OMNET++ es muy potente y cuenta con características que NS2 no posee. A diferencia de este, con OMNET++ se pueden realizar simulaciones más cercanas a lo real sin necesidad de hacer modificaciones a la herramienta, como es el caso de los parches aplicados a NS2. Se propone que en trabajos posteriores se haga uso de esta herramienta de simulación y se desarrolle el módulo del protocolo PMIPv6.
- Los protocolos de micromovilidad IP son actualizados con frecuencia y nuevas propuestas también aparecen. Se plantea realizar comparaciones entre *Proxy Mobile* IPv6 y alguna de sus extensiones o nuevos protocolos, verificando características importantes como retardo de *handover* y pérdida de paquetes.
- NS2 cuenta con la característica de emulación, que permite enviar información real a un ambiente simulado y obtenerla nuevamente en el entorno real. El uso de esta característica permite observar directamente y no con estadísticas, cuales son los efectos que tiene el *handover* o algún otro proceso que se simule. Se propone hacer uso de esta característica en trabajos posteriores para evidenciar los efectos del *handover* u otro efecto de la red sobre un servicio en tiempo real.
- Se pueden realizar un sinnúmero de simulaciones dependiendo de la topología que se implemente en los escenarios. En este trabajo de grado se trabajó con un único nodo móvil y en escenarios inalámbricos ideales, sin tener en cuenta atenuación o desvanecimiento de la señal causados por factores externos. Se plantea que en trabajos posteriores se tengan en cuenta estas características con el fin de que los escenarios simulados se parezcan más a los reales.
- Con el fin de mejorar el desempeño durante el proceso de *handover* en un ambiente de micromovilidad o macromovilidad IP, se propone desarrollar un proyecto que analice y desarrolle una aproximación multi-nivel (cross-layer) del proceso de *handover* y su forma de activación, para reducir los retardos en el mismo.

REFERENCIAS

- [1] ITU-T Rec. Q.1761, “Principles and requirements for convergence of fixed and existing IMT-2000 systems”, 2004.
- [2] T. Robles Valladares, “Movilidad en redes IP”, DIT Universidad Politécnica de Madrid, 2007.
- [3] ITU-T Rec. Q.1741.6, “IMT-2000 references to Release 8 of GSM-evolved UMTS core network”, 2009.
- [4] K. Anderson, “*Always Best Served and Managed: Research Challenges in Future Mobile Multimedia Application Architectures*”, Department of Computer Science and Electrical Engineering, Lulea University of Technology, 2007.
- [5] ITU-T Rec. Q.1742, “IMT-2000 references to ANSI-41 evolved core network with cdma2000 access network”, 2008.
- [6] ITU-T Rec. H.510, “Mobility for H.323 multimedia systems and services”, 2002.
- [7] ITU-T Rec. M.1224 “Vocabulary of Terms for International *Mobile* Telecommunications-2000 (IMT-2000)”, 2000.
- [8] Z. Yi, Z. Xuefeng, J. Jia, “*Mobile IP Protocol Research and Development*” Computer College, Beijing University of Science and Technology, China Unites Telecommunications Corporation Beijing Branch, 2009
- [9] T. Chiba, H. Yokota, Akiraldoue, “Mobility Mangement Schemes for Heterogeneity Support in Next Generation Wireless Networks”, Columbia University, 2007.
- [10] A. Polidoro, “Mobility Management in Next Generation Networks”, Universidad de Roma – TorVergata, Tesis Doctoral, 2009.
- [11] J. Sun, J. Sauvola, “Mobility and Mobility Mangement: A conceptual Framework”, University of Oulu, 2007.
- [12] ITU-T Rec. Q.1703 “Service and network capabilities framework of network aspects for systems beyond IMT-2000”, 2004.
- [13] M. Díaz, C. Olvera, P. García, “Despegando con movilidad IPv6 (MIPv6)”, CONSULINTEL, Universidad de Murcia, 2007.
- [14] M. Alnas, I. Awan, D.R Holton, “A Survey of Handoff Performance in *Mobile IP*”, 2009.
- [15] M. Boban, “An Overview of Macro-Mobility Management in Next Generation All-IP Based Wireless Network Infrastructures”, University of Zagreb, 2005.
- [16] C. Perkins, “RFC 5944: IP Mobility Support for IPv4, Revised”, IETF, 2010.

- [17] J. Manner, "RFC 3753: Mobility Related Terminology", Network Working Group, 2004.
- [18] S. Hares, "RFC 1136: Administrative Domains and Routing Domains, A Model for Routing in the Internet", Network Working Group, 1989.
- [19] P. Roberts, J. Kempf, "Mobility Architecture for the Global Internet", Motorola Labs, DoCoMo USA Labs, 2007.
- [20] N. Kara, "Mobility Management Approaches for *Mobile* IP Networks: Performance Comparison and Use Recommendations", IEEE, 2009.
- [21] D. Johnson, C. Perkins, J. Arkko "RFC 3775: Mobility Support in IPv6", Network Working Group, 2004.
- [22] K. Ray, K. Pawlikowski, H. Sirisena, "*Handover in Mobile WiMAX Networks: The State of Art and Research Issues*", Department of Computer Science and Software Engineering, Department of Electrical and Computer Engineering, University of Canterbury, 2009.
- [23] L. Gyalog, M. Weldon, M. Scott, "El Reto de la QoS Garantizada", Revista Interactiva Enriching Communications de ALCATEL-LUCENT, 2009
- [24] ITU T Rec. G.1000, "Communications Quality of Service: A framework and definitions", 2002
- [25] CCITT Rec. E.800, "Quality of service and dependability vocabulary", Third Edition, 1988 ; ITU-T Rec. E.800, "Terms and definitions related to quality of service and network performance including dependability", Fourth Edition, 1994.
- [26] ETSI TECHNICAL REPORT 003, "General aspects of Quality of Service (QoS) and Network Performance (NP)" Second Edition, 1994.
- [27] ITU-T Rec. E.800 "Definitions of terms related to quality of service" Fifth edition, 2008
- [28] "Funcionamiento de la Interconexión de Redes", Área de Ingeniería Telemática, Universidad de Oviedo, España, 2007
- [29] "Servicios Integrados", Departamento de Sistemas Informáticos, Universidad de Castilla – La Mancha, 2009
- [30] J. Caballano, "Tecnología de las Infraestructuras de las Comunicaciones", Infraestructura de la Comunicaciones, 2009.
- [31] ITU-T Rec. T.174 "Application programming interface (API) for MHEG-5", 2002
- [32] R. Stankiewicz, P. Cholda, A. Andrzej, "QoX: What is It Really?" AGH University of Science and Technology, Communication Magazine, 2011
- [33] ITU-T Rec. G.1010, "End – User Multimedia QoS Categories", 2002.

- [34] ITU-T Rec. Y. 1221, "Traffic control and congestion control in IP-based Networks", 2010.
- [35] ITU-T Rec. E.416 "Network management principles and functions for B-ISDN traffic", 2000.
- [36] R. Subiela, A. León, "Simulación de Protocolos de encaminamiento en redes móviles Ad Hoc con NS-2", Departamento de Comunicaciones, Universidad Politécnica de Valencia, 2007.
- [37] ITU-T FG On IPTV, "Quality of Experience Requirements for IPTV Services", 2007.
- [38] Telchemy, "Managing IPTV Performance. IP Video Performance Management", 2008.
- [39] H. Chaskar, "RFC 3583: Requirements of a Quality of Service (QoS) Solution for *Mobile IP*", Nokia Research Center, Network Working Group, 2003
- [40] J. Padilla, "Contribución al soporte de Calidad de Servicio en Redes Móviles", Tesis Doctoral, Universidad Politécnica de Cataluña, 2007
- [41] ITU-T Rec. Y. 1540, "Internet protocol data communication service – IP packet transfer and availability performance parameters", 2007.
- [42] P. Casas, D. Guerra, I. Irigaray, "Calidad de Servicio Percibida en Servicios de Voz y Video sobre IP", Universidad de la Republica, 2007.
- [43] A. Morton, B. Claise, "RFC 5481: Packet Delay Variation Applicability Statement", Network Working Group, Cisco Systems, 2009.
- [44] Astudillo, C.A.; Calderón, O.J.; Ortiz, J.H.; "PMPLS: Integrating Proxy Mobile IPv6 and MPLS in Wireless Access Networks," *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, vol., no., pp.1-5, 7-10 Feb. 2011.
- [45] J. Nolivos, "Estudio comparativo de los protocolos de movilidad y micromovilidad IP, servicios y aplicaciones para los sistemas de comunicaciones móviles", Escuela Politécnica Nacional, 2006.
- [46] R.Gunasundari, S.Shanmugavel, "Macro/micro-mobility fast *handover* in *Hierarchical Mobile IPv6*", Pondicherry Engineering College, Anna University-Chennai, 2011.
- [47] M. Alnas, I. Awan, D.R Holton, "A Cross-Layer Decision for *Mobile IP Handover*", 2009
- [48] A. Campbell, J. Gomez, Columbia University, "IP Micro-Mobility Protocols", 2000
- [49] H. Soliman, C. Castelluccia, K. Elmaki, L. Bellier, "RFC 5380: *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management*", Network Working Group, 2008.

- [50] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "RFC 5213: *Proxy Mobile IPv6*", Network Working Group, 2008.
- [51] "Proxy Mobile IPv6", Open Air Interface, 2008.
<http://www.openairinterface.org/components/page1095.en.htm>
- [52] K. Kong, W. Lee, Y. Han, M. Shin, H. You, "Mobility Management for all-IP *Mobile Networks: Mobile IPv6 vs. Proxy Mobile IPv6*", Korea University, Korea University of Technology and Education, Electronics and Telecommunications Research Institute, Korea Telecommunication, 2007.
- [53] R. Koodli, "RFC 5568: Mobile IPv6 Fast Handover, Apendice B" Network Working Group, 2009.
- [54] www.opnet.com
- [55] V. García, "Transmisión de VoIP en redes de cable", Universidad de Oviedo, 2003.
- [56] <http://www.omnetpp.org/home/what-is-omnet>
- [57] F. Zarrar, C. Bauer, C. Wietfed, "An Accurate and Extensible *Mobile IPv6 (xMIPv6)* Simulation Model for OMNeT++", Communication Networks Institute, Institute of Communications and Navigation, 2008.
- [58] C. Mellon, "NS Tutorial", Computer Science Department, 2007
- [59] Fall, K., "The NS Manual". VINT Project. URL: <http://www.isi.edu/nsnam/ns/ns-documentation>, 2003.
- [60] M. Ulgen, J. Black, B. Johnsonbaugh, R. Klungle, "Simulation Methodolgy – A Practitioner's Perspective", Michigan Simulation User Group, Technical Committee on Simulation Methodology, 2006
- [61] V. Wojcik, "Steps in Simulation and Model Building", Simulation Methodology – Discrete Event Simulation, 2003
- [62] E. Garcia, E. López, R. Vidal, J. Paradells, "Effect of adjacent-channel interference in IEEE 802.11 WLANs", University of Catalonia, 2007.
- [63] A. M. Avelar, L.L Marques, T. Bemerguy, K.L, " QoE Provisioning and Seamless Mobility Management base don PMIPv6 Protocol", IEEE Latinamerican Transactions, Vol 9, No 2, Abril, 2011.
- [64] V. Toledo, "Análisis y Diseño de Mecanismos de Handoff en Redes Inalámbricas de Banda Ancha *IEEE802.16e*", Tesis de Maestría, Universidad Nacional Autónoma de México, 2009.

[65] Y. Becerra, J. Padilla, "Multicast Tunneling Proposal for the HMIPv6-BI Protocol", Grupos de Investigación TICS y GITEL, 2010.