TESIS DEFENDIDA POR

Elizabeth Ramírez Mondragón

Y APROBADA POR EL SIGUIENTE COMITÉ

Dr. Luis Armando Villaseñor González
Director del Comité

Dr. José Rosario Gallardo López
Miembro del Comité

MC. Raúl Rivera Rodríguez
Miembro del Comité

Dr. José Antonio García Macías
Miembro del Comité

Dr. Luis Alejandro Márquez Martínez
Coordinador del programa de posgrado en Electrónica y Telecomunicaciones

Dr. David Hilario Covarrubias Rosales
Encargado del despacho de la Dirección de Estudios de Posgrado

3 de diciembre del 2007

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR DE ENSENADA

PROGRAMA DE POSGRADO EN CIENCIAS
EN ELECTRÓNICA Y TELECOMUNICACIONES

MECANISMO DE ENRUTAMIENTO PARA REDES HÍBRIDAS INALÁMBRICAS (INFRAESTRUCTURA - AD HOC)

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de
MAESTRO EN CIENCIAS

Presenta:

ELIZABETH RAMÍREZ MONDRAGÓN

Ensenada, Baja California, México, diciembre del 2007.

RESUMEN de la tesis de **Elizabeth Ramírez Mondragón**, presentada como requisito parcial para la obtención del grado de MAESTRO EN CIENCIAS en ELECTRÓNICA Y TELECOMUNICACIONES. Ensenada, Baja California, México. Diciembre del 2007.

MECANISMO DE ENRUTAMIENTO PARA REDES HÍBRIDAS INALÁMBRICAS (INFRAESTRUCTURA – AD HOC)

Resumen aprobado por:

_____

Dr. Luis Armando Villaseñor González
Director de Tesis

En los últimos años se ha observado un gran avance en el área de las redes inalámbricas. Las arquitecturas de red inalámbrica, en general, se pueden clasificar como redes inalámbricas de infraestructura y redes inalámbricas ad hoc. Las redes inalámbricas de infraestructura se caracterizan por estar constituidas por un dispositivo de coordinación central (punto de acceso o estación base). Por otro lado, las redes inalámbricas ad hoc se caracterizan por utilizar estrategias de coordinación distribuida entre los dispositivos inalámbricos que la conforman.

Existen diversas ventajas al considerar arquitecturas que implementan la coexistencia de una red de infraestructura cableada y una red inalámbrica ad hoc. Algunos de estos beneficios incluyen: incremento de robustez, mayor escalabilidad, soporte de topologías dinámicas, balanceo de carga, aumento del área de cobertura, entre otras. En este trabajo se propone un mecanismo de enrutamiento para integrar una red de infraestructura cableada y una red inalámbrica ad hoc para formar una red híbrida; este protocolo de enrutamiento se basa en el protocolo de micromovilidad HAWAII y el protocolo de enrutamiento AODV. El protocolo HAWAII se utiliza para proporcionar conectividad hacia Internet a los nodos móviles; de igual forma, éste se emplea para manejar los traspasos de capa 3 relacionados con la movilidad de los nodos inalámbricos ad hoc dentro del dominio administrativo. Por otro lado, el protocolo AODV se utiliza para la comunicación de los nodos móviles dentro de la red ad hoc. La red híbrida se compone de nodos móviles ad hoc y enrutadores de acceso, estos últimos implementan el protocolo de enrutamiento AODV en la interfaz de red inalámbrica para permitir la interoperabilidad de la red de infraestructura cableada y la red inalámbrica ad hoc. El mecanismo propuesto se evalúa bajo diferentes escenarios con alta y baja carga de tráfico.

Palabras clave: Redes híbridas inalámbricas, HAWAII, AODV, Enrutamiento.

ABSTRACT of the thesis presented by **Elizabeth Ramírez Mondragón** as a partial requirement to obtain the MASTER OF SCIENCE degree in ELECTRONICS AND TELECOMMUNICATIONS. Ensenada, Baja California, Mexico. December 2007.

ROUTING MECHANISM FOR HYBRID WIRELESS NETWORKS (INFRASTRUCTURE-AD HOC)

Abstract approved by:

_____

Dr. Luis Armando Villaseñor González
Thesis Supervisor

In recent years there has been a great advance within the area of the wireless networks. Wireless network architectures, in general, can be classified as wireless infrastructure networks and wireless ad hoc networks. Wireless infrastructure networks are characterized by the use of a central coordination device (access point or base station). On the other hand, wireless ad hoc networks are characterized by the implementation of distributed coordination strategies between the wireless devices.

There are several advantages to considering architectures that implement the coexistence of a wired infrastructure network and a wireless ad hoc network. Some of these benefits include: increased robustness, greater scalability, support of dynamic topologies, load balancing, extending the coverage area, among others. In this work a proposal of a routing mechanism is made to integrate a wired infrastructure network and a wireless ad hoc network to form a hybrid network; this routing protocol is based on the HAWAII micromobility protocol and the AODV routing protocol. The HAWAII protocol is used to provide Internet connectivity to the mobiles nodes; similarly, it is used to handle handoffs at the layer 3 which are related to the mobility of the wireless ad hoc nodes within the administrative domain. On the other hand, the AODV protocol is used for the communication between the mobiles nodes in the ad hoc network. The hybrid network is composed of ad hoc mobile nodes and access routers, where the access routers implement the AODV routing protocol in the wireless network interface to allow the interoperability of the wired infrastructure network and the wireless ad hoc network. The proposed mechanism is evaluated under different scenarios with high and low traffic load.

Keywords: Hybrid Wireless Networks, HAWAII, AODV, Routing.

Contenido

Página

Contenido (continuación)

Lista de Figuras

Página

Lista de Figuras (continuación)

Página

Lista de Figuras (continuación)

Página

Lista de Tablas

Capítulo I.

Introducción

Desde su surgimiento en 1970, las redes inalámbricas han ido incrementando su popularidad en la industria y han sido ampliamente utilizadas para proveer acceso a Internet de alta velocidad a usuarios móviles [Royer y Toh, 1999]. Las arquitecturas de red inalámbrica, en general, se pueden clasificar como redes inalámbricas de infraestructura y redes inalámbricas ad hoc.

I.1 Redes Inalámbricas

Redes Inalámbricas de Infraestructura

Este tipo de redes se caracterizan por estar constituidas por un dispositivo de coordinación central (punto de acceso o estación base), el cual se utiliza para todas las comunicaciones en la red de infraestructura, incluyendo la comunicación entre nodos móviles dentro del área de cobertura. Esto implica que la comunicación entre dos nodos móviles se lleve a cabo en dos saltos y requiera de una mayor capacidad de transmisión [Gast, 2002]. Hoy en día, los puntos de acceso han sido reemplazados por dispositivos que incorporan la funcionalidad de enrutamiento, por lo que resulta común encontrar un enrutador

inalámbrico (o enrutador de acceso) como dispositivo de coordinación de una red de infraestructura.

Los nodos móviles se comunican con el enrutador de acceso más cercano que está dentro de su área de cobertura; conforme el nodo móvil se mueve fuera del rango de transmisión del enrutador de acceso y entra al rango de otro, se debe realizar un traspaso, entonces el nodo es capaz de continuar la comunicación transparente a través de la red. Este procedimiento de traspaso requiere de la implementación de un protocolo de movilidad. En la figura 1 se muestran algunas aplicaciones típicas de este tipo de red, las cuales son redes de área local inalámbrica (WLANs) y las redes celulares [Royer y Toh, 1999].

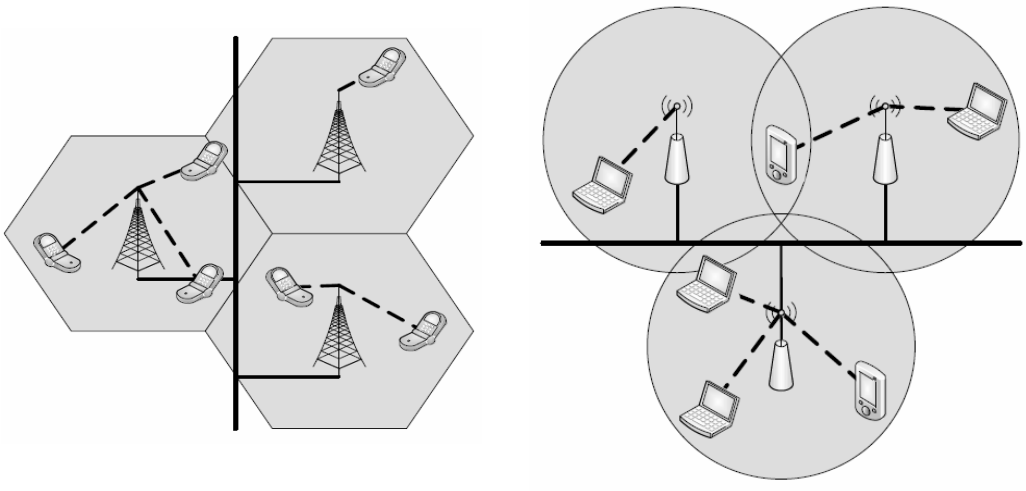


Figura 1. Red Inalámbrica de Infraestructura.

Redes Inalámbricas Ad hoc

Una red ad hoc se caracteriza por estar formada de una colección de nodos que forman una red temporal y arbitraria sin una administración centralizada. Debido al rango de

transmisión limitado de los dispositivos inalámbricos usados existe la posibilidad de que los nodos no tengan comunicación directa entre ellos, por lo tanto, los nodos móviles deben ser capaces de comportarse como nodos enrutadores para poder establecer comunicación multisalto dentro de la red. Las estaciones o nodos que forman una red ad hoc pueden ser fijos o móviles, en el caso de redes ad hoc donde los nodos tienen movilidad se denominan redes móviles ad hoc (Manets). Algunos ejemplos de aplicaciones en que las redes ad hoc pueden ser de gran utilidad son escenarios como operaciones de rescate de emergencia, reuniones o convenciones en donde las personas desean compartir rápidamente información y operaciones de adquisición de datos en terrenos inhabitables, entre otros.

Entre las ventajas de las redes móviles ad hoc se puede mencionar su fácil instalación, bajo costo y mantenimiento, mayor flexibilidad y habilidad para emplear nuevos y eficientes protocolos de enrutamiento para la comunicación inalámbrica [Gast, 2002]. En la figura 2 se ilustra un ejemplo de una red móvil ad hoc.

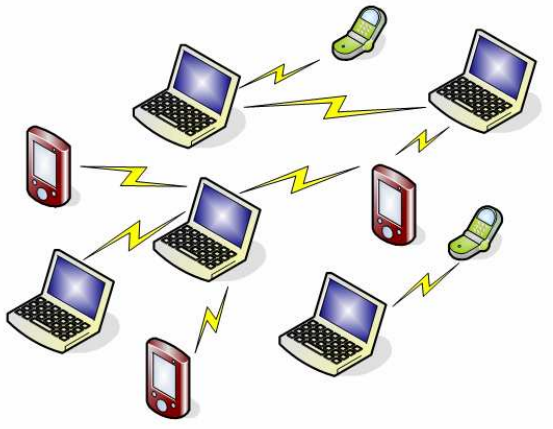


Figura 2. Red Inalámbrica Ad hoc.

I.2 Planteamiento del problema

Las redes inalámbricas de infraestructura y ad hoc tienen muchas limitaciones. Por un lado, en las redes de infraestructura todos los usuarios se conectan directamente hacia un enrutador de acceso y todos los paquetes son enviados por el mismo, ocasionando que la capacidad de la red y el área de cobertura sea limitada, y cuando se necesita instalar una red de este tipo se deben de evitar las zonas muertas, es decir, las zonas sin área de cobertura. En situaciones donde no hay infraestructura fija, las redes inalámbricas ad hoc llegan a ser alternativas valiosas como en el caso de redes celulares inalámbricas o LANs inalámbricas donde se requiere que los nodos puedan comunicarse entre sí, por otro lado, debido a la carencia de infraestructura y el rango de transmisión limitado de cada nodo, los datos necesitan ser enrutados hacia su destino utilizando nodos intermedios por lo que se requiere implementar la comunicación multisaltos.

Las redes inalámbricas de infraestructura y las redes inalámbricas ad hoc pueden combinarse para satisfacer mejor las necesidades del usuario. A la integración de una red cableada (o de infraestructura cableada) con una red ad hoc se le considera una *red híbrida.* Las redes híbridas inalámbricas son una solución viable para combatir las limitaciones de las redes inalámbricas de infraestructura y proveer conexión de Internet a redes ad hoc, de esta manera se puede ampliar el uso de las redes inalámbricas, ya que las trayectorias multisaltos entre nodos móviles y enrutadores de acceso pueden extender el área de cobertura de una red, además los usuarios pueden tomar ventaja de las conexiones ad hoc para enviar datos locales y por lo tanto disminuir la carga de tráfico a través del enrutador

de acceso e incrementar la capacidad de la red [Sun y Belding-Royer, 2003]. En la figura 3 se muestran ejemplos de redes híbridas inalámbricas.

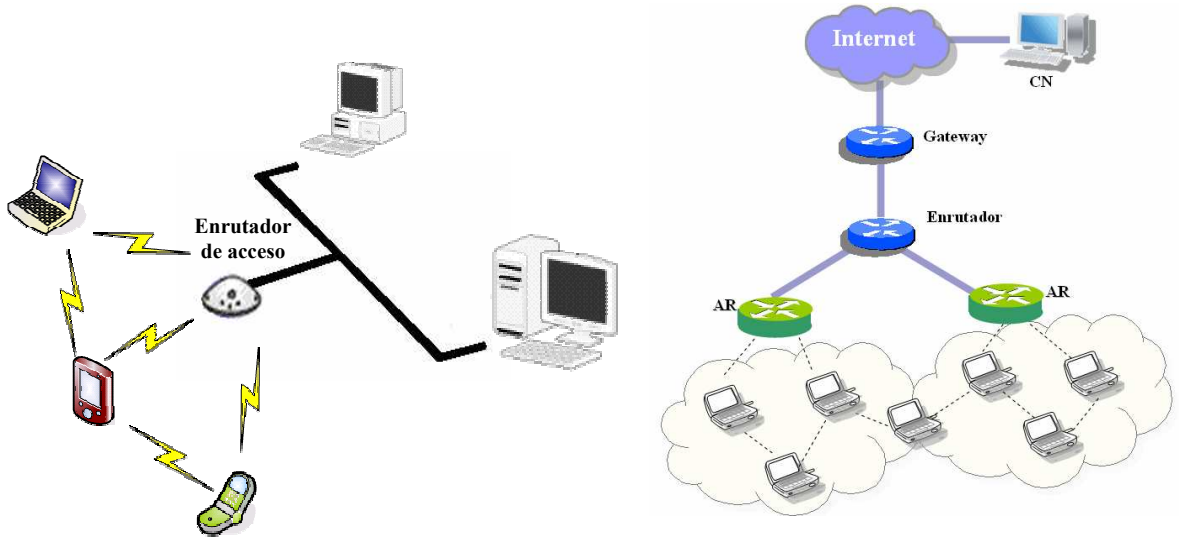


Figura 3. Red Híbrida Inalámbrica.

Otras ventajas de las redes híbridas inalámbricas pueden ser el incremento de robustez, mayor escalabilidad, soporte de topologías dinámicas, balanceo de carga, aumento del área de cobertura [Hui, *et al*., 2003], además las redes híbridas inalámbricas disfrutan de las ventajas de ambos tipos de redes, ofrece la flexibilidad local de las redes ad hoc con eficientes estrategias de enrutamiento de las redes de infraestructura cableada.

Mientras las redes inalámbricas ad hoc y de infraestructura cableada han sido extensamente estudiadas individualmente, las redes híbridas inalámbricas brindan nuevos retos en el diseño de protocolos y evaluación de desempeño. El patrón de tráfico en estos escenarios variará, porque las aplicaciones tienen diferentes configuraciones y diferentes

requerimientos de desempeño. Además, como los protocolos de enrutamiento para redes de infraestructura cableada están basados sobre un rango de transmisión directa al enrutador de acceso, no se pueden aplicar directamente en comunicación multisaltos. Es importante investigar nuevos esquemas de enrutamiento que puedan adaptarse mejor a las redes híbridas con diferente composición de tráfico y requerimientos de aplicaciones [Sun y Belding-Royer, 2003].

Hay muchas propuestas en la literatura para integrar una red ad hoc con una red de infraestructura cableada, por ejemplo, hay propuestas basadas en la integración de IP Móvil y una red ad hoc empleando un protocolo de enrutamiento, por ejemplo Broch*, et al*., [1999]; Ammari y El-Rewini, [2004]. En Jonsson, *et al*., [2000] y Sun y Belding-Royer, [2003] siguen un enfoque similar basado en el protocolo AODV, pero sólo trabajan con IPv4 porque requieren agentes foráneos, estas propuestas utilizan IP Móvil para servir a los nodos más allá de un salto de distancia de los enrutadores de acceso y para darles conectividad hacia Internet, proveen buena conectividad, pero imponen alta sobrecarga, especialmente cuando los nodos en la red ad hoc no requieren conectividad externa (i.e. Internet). En algunos trabajos como Miller, *et al*., [2003]; Boppana, *et al*., [2004] proponen nuevos algoritmos de enrutamiento, basándose en el protocolo reactivo AODV. En Chelius y Fleury, [2003] dividen la red híbrida en varias subredes en las cuales pueden ser aplicados diferentes protocolos de enrutamiento, en otros trabajos como Benzaid, *et al*., [2002], Wu, *et al*., [2001] aplican un protocolo de enrutamiento a toda la red híbrida, considerando a la red de infraestructura como una red ad hoc estática y en trabajos como Sessinghaus*, et al*., [2003]; Typpo*, et al*., [2003]; Nilsson*, et al*., [2004] utilizan una solución de

micromovilidad con un protocolo de enrutamiento reactivo, dividen a la red híbrida en dos partes: una parte la comprende la red ad hoc y otra parte la red de infraestructura cableada, y se enfocan en evitar la ruptura de una ruta ad hoc mientras un nodo móvil realiza un traspaso [Typpo*, et al*., 2003]. Esta solución podría ser adecuada porque los esquemas sin soporte de micromovilidad carecen de la ventaja de traspaso suave en las redes de acceso inalámbricas. Cuando IP Móvil se extiende dentro de la red ad hoc, el número de traspasos ocurridos aumenta con el tamaño de la red, ya que cualquier nodo intermedio puede realizar un traspaso entre enrutadores de acceso, no sólo los nodos más cercanos a los ARs; por otro lado, el uso de protocolos de micromovilidad introducen diversas ventajas como manejar eficientemente el enrutamiento intradominio, habilitar a los nodos a realizar traspasos rápidos entre enrutadores de acceso, así como servicio de voceo.

Este trabajo de tesis considera una arquitectura de red híbrida que tiene enlaces cableados e inalámbricos para incorporar los elementos de una red de infraestructura cableada y de una red inalámbrica ad hoc. Los enrutadores de acceso de esta red, a pesar de ser similares a los puntos de acceso de una red inalámbrica de infraestructura porque cuentan con dos interfases (una alambrada y una inalámbrica), no funcionan igual, porque en la parte inalámbrica se deben desempeñar como un nodo más de la red ad hoc.

I.3 Objetivo de la tesis

El objetivo general de este trabajo de tesis es diseñar y proponer un mecanismo de enrutamiento para redes híbridas inalámbricas. Para realizar esto se propone utilizar el

protocolo de micromovilidad HAWAII y el protocolo de enrutamiento AODV. El protocolo HAWAII manejará los traspasos que realicen los nodos móviles y les dará conectividad hacia Internet, mientras que el protocolo de enrutamiento AODV se encargará de la comunicación de los nodos móviles dentro de la red ad hoc.

El protocolo de enrutamiento AODV fue elegido como protocolo base para la parte ad hoc de este trabajo de tesis porque existe mucha información sobre su funcionamiento en la literatura de las redes ad hoc y es uno de los protocolos reactivos que ha tenido mejor desempeño y mayor aceptación dentro de la IETF (Internet Engineering Task Force) [Broch, *et al*., 1998],[Lee, *et al*., 1999], [Johansson, *et al*., 1999]. Entre sus ventajas se encuentra que reacciona muy rápido a los cambios topológicos de la red y actualiza sólo a los nodos afectados por estos cambios. Funciona mejor que otros protocolos cuando se utiliza en redes con baja movilidad, porque la sobrecarga de este protocolo está relacionada con el descubrimiento de ruta, el cual se inicia cuando una ruta se rompe y en las redes de este tipo, la ruptura de enlace ocurre con menos frecuencia [Perkins, *et al*., 2003]. Además, este protocolo ha sido extendido y modificado para brindarle conectividad hacia Internet a los nodos móviles de la red ad hoc [Hamidian, *et al*., 2004].

Por otro lado, el protocolo HAWAII fue elegido porque es uno de los protocolos de micromovilidad más populares que existen en la literatura. Tiene muchas similitudes con IP Celular, como dividir a la red en dominios y el enrutamiento salto a salto, pero HAWAII ofrece una solución más completa para reducir el número de mensajes enviados al agente de casa. Además, los nodos móviles mantienen su dirección de red mientras se mueven

dentro del mismo dominio, simplificando el soporte de calidad de servicio. Este protocolo tiene menor retardo de traspaso y menor pérdida de paquetes en comparación con IP Celular e IP Móvil Jerárquico, porque la pérdida de paquetes solamente ocurre durante los procesos de traspasos. HAWAII soporta dos esquemas de traspasos dependiendo de las capacidades del nodo móvil, estos esquemas realizan un excelente desempeño reduciendo la interrupción de las aplicaciones de los usuarios y a diferencia de IP Celular e IP Móvil Jerárquico, el nodo móvil no necesita tener implementado el protocolo HAWAII. [Campbell, *et al*., 2002].

Objetivos particulares:

- Los nodos móviles deberán ser capaces de encontrar la mejor ruta para enviar los paquetes de datos hacia su destino, eligiendo enviarlos sobre la infraestructura de red cableada o utilizando sólo los enlaces inalámbricos de la red ad hoc.
- Los nodos deberán ser capaces de asociarse al enrutador de acceso más cercano.
- Los nodos móviles deberán ser capaces de comunicarse con un nodo correspondiente y viceversa.
- Cuando un nodo correspondiente se comunique con un nodo móvil de la red ad hoc, y este realice un traspaso, estos movimientos deberán ser transparentes para el nodo correspondiente.

I.4 Estructura del trabajo

El presente trabajo de tesis está dividido en un total de seis capítulos, los cuales están organizados de la siguiente manera:

- en el capítulo 2, se describe el funcionamiento de los diferentes protocolos de enrutamiento ad hoc, pero principalmente el protocolo AODV ;
- en el capítulo 3, se explican las principales características de IP Móvil, así como de los conceptos básicos de macromovilidad y micromovilidad; se describen los diferentes protocolos de micromovilidad, centrándose en el protocolo de micromovilidad HAWAII ;
- en el capítulo 4, se describe la integración del protocolo de micromovilidad HAWAII con el protocolo de enrutamiento AODV y el funcionamiento del mecanismo propuesto.
- el capítulo 5, hace referencia al simulador de redes NS-2, y a la extensión CIMS (Columbia IP Micromobility Software) utilizada para implementar el protocolo de micromovilidad HAWAII ; se definen los diferentes parámetros y escenarios utilizados en las simulaciones, y se analizan los resultados obtenidos;
- finalmente, en el capítulo 6, se presentan las conclusiones de este trabajo de investigación.

Capítulo II.

AODV (Ad hoc On-demand Distance Vector)

II.1 Introducción

Los protocolos de enrutamiento se utilizan para facilitar la comunicación dentro de una red ad hoc y descubrir rutas entre los nodos. El objetivo principal de dichos protocolos es establecer eficientemente una ruta entre un par de nodos para que los datos puedan ser enviados de una manera oportuna.

Se han desarrollado muchos protocolos de enrutamiento para las redes móviles ad hoc. Tales protocolos deben tratar con las limitaciones típicas de estas redes, las cuales incluyen alto consumo de potencia, bajo ancho de banda, y altas tasas de error. Como se muestra en la figura 4, los protocolos de enrutamiento pueden clasificarse como protocolos proactivos, protocolos reactivos y protocolos híbridos [Royer y Toh, 1999].

En este capítulo se explican los diferentes algoritmos de enrutamiento usados en las redes móviles ad hoc, centrándose en el protocolo AODV, el cual es usado en este trabajo de tesis.

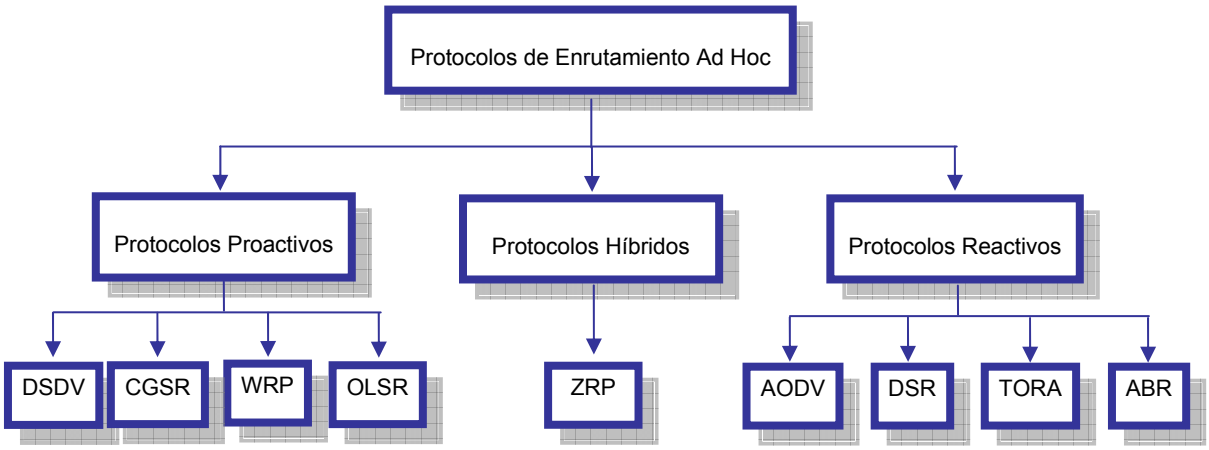


Figura 4. Protocolos de Enrutamiento Ad Hoc

II.2 Protocolos de Enrutamiento

II.2.1 Protocolos Proactivos

Los protocolos proactivos tratan de mantener actualizada la información de enrutamiento de cada nodo en la red. Estos protocolos requieren que cada nodo mantenga una o más tablas para almacenar información de enrutamiento, entonces el retardo para enviar un paquete es mínimo. Estas tablas de enrutamiento son intercambiadas entre los nodos vecinos cada vez que ocurre un cambio en la topología de la red, esto hace que se consuma un mayor ancho de banda y energía. Los diferentes protocolos proactivos difieren entre sí en base al número de tablas que requieren y en base al método por medio del cual los cambios en la estructura de la red se difunden [Royer y Toh, 1999].

Dentro de los protocolos proactivos se encuentran:

DSDV (Destination Sequenced Distance Vector): Este protocolo está basado en el algoritmo *Bellman-Ford* y utiliza números de secuencia para evitar el problema de *conteo infinito*, ocasionado por usar dicho algoritmo. Además, cada nodo mantiene una lista de todos los nodos destinos, el número de saltos hacia cada destino y cada entrada está marcada con un número de secuencia. DSDV es adecuado para redes pequeñas.

CGSR (Clusterhead Gateway Switch Routing): Este protocolo se basa en DSDV pero usa un esquema de enrutamiento jerárquico. Se considera que este protocolo es diferente de los demás porque organiza la red en clusters y por el tipo de direccionamiento que utiliza, además selecciona un nodo para que sea la cabeza del cluster.

WRP (Wireless Routing Protocol): Este protocolo mantiene la información de enrutamiento de todos los nodos en la red, para lograrlo cada nodo en la red mantiene varias tablas: una tabla de distancia, una tabla de enrutamiento, una tabla de costo-enlace y una tabla de lista de retransmisión de mensajes.

OLSR (Optimized Link State Routing): Este protocolo se diseñó para reducir la cantidad de mensajes de control que se difunden en la red. La clave de este protocolo es el uso de MPRs (*multipoint relays*), los cuales son nodos seleccionados que se encargan de retransmitir los mensajes de control que se difunden en la red. Cada nodo envía periódicamente mensajes *hola* a nodos específicos para intercambiar información de enrutamiento y con esta información el nodo construye una tabla de enrutamiento. Este protocolo es adecuado para redes grandes.

II.2.2 Protocolos Reactivos

Los protocolos reactivos crean rutas sólo cuando son necesarias por el nodo fuente. Cuando un nodo requiere una ruta hacia un destino, este inicia un proceso de *descubrimiento de ruta* dentro de la red. Este proceso termina cuando se encuentra una ruta o se han examinado todas las rutas posibles. Una vez que se ha establecido una ruta, se realiza un proceso de *mantenimiento de ruta* hasta que el destino sea inaccesible a lo largo de cada ruta o hasta que la ruta ya no sea deseada [Royer y Toh, 1999]. En contraste a los protocolos proactivos se reduce drásticamente la sobrecarga [Stojmenovic, 2002].

Dentro de los protocolos reactivos para redes ad hoc se encuentran:

AODV (Ad Hoc On-demand Distance Vector): Protocolo de enrutamiento reactivo para manets. Se presentan mayores detalles en la sección II.3.

DSR (Dynamic Source Routing): Este protocolo se basa en el concepto de enrutamiento fuente, tiene dos fases: *descubrimiento de ruta* y *mantenimiento de ruta*, permite múltiples rutas hacia un destino y le permite a los nodos fuente seleccionar y controlar las rutas usadas en el envío de paquetes. Funciona bien para redes pequeñas con baja movilidad.

TORA (Temporally Ordered Routing Algorithm): Este protocolo es considerado un protocolo de enrutamiento distribuido basado en el concepto de enlaces en reversa, es altamente adaptativo y libre de lazos. Provee múltiples rutas para cualquier par de nodos

fuente/destino y tiene tres funciones básicas: creación de rutas, mantenimiento de rutas y borrado de rutas.

ABR (Associativity-Based Routing): En este protocolo las rutas se seleccionan en base a una métrica llamada *grado de estabilidad de asociación*, cuando el grado de estabilidad es alto indica que el nodo casi no se mueve y si es bajo significa que el nodo tiene mucha movilidad. Tiene 3 funciones: descubrimiento de rutas, reconstrucción de rutas y borrado de rutas. Además, cada nodo envía mensajes para identificar su existencia.

SSR (Signal Stability Routing): Este protocolo se basa en el nivel de potencia de la señal de los nodos y en la estabilidad de la posición, por lo tanto, las rutas que tengan mayor estabilidad serán seleccionadas.

II.2.3 Protocolos Híbridos

La idea básica de estos protocolos es usar mecanismos de enrutamiento proactivo en algunas áreas de la red por cierto tiempo y usar enrutamiento reactivo en el resto de la red. Las operaciones proactivas están restringidas a un pequeño dominio, llamado *zone radius*, para reducir la sobrecarga de control y los retardos. Los protocolos de enrutamiento reactivos son usados para localizar nodos fuera de este dominio.

ZRP es un protocolo híbrido donde cada nodo móvil proactivamente mantiene rutas dentro de una región local (referido como la zona de enrutamiento). Los nodos móviles que están

fuera de la zona pueden ser alcanzados con el enrutamiento reactivo [Mukherjee, *et al*., 2003].

II.3 AODV

AODV (*Ad Hoc On Demand Distance Vector*) es un protocolo de enrutamiento reactivo que se diseñó a partir de los protocolos de enrutamiento DSDV y DSR. Reduce la difusión de mensajes comparado con DSDV, porque el proceso está basado en un mecanismo por *demanda*, además, comparte algunas características con el protocolo DSR porque descubre rutas conforme son necesarias, similar a un proceso de *descubrimiento de ruta*. Sin embargo, AODV adopta un mecanismo muy diferente para mantener información de enrutamiento porque usa tablas de enrutamiento tradicionales, en donde se utiliza una entrada por cada destino [Mukherjee, *et al*., 2003]. En la figura 5 se muestra el funcionamiento del protocolo AODV.

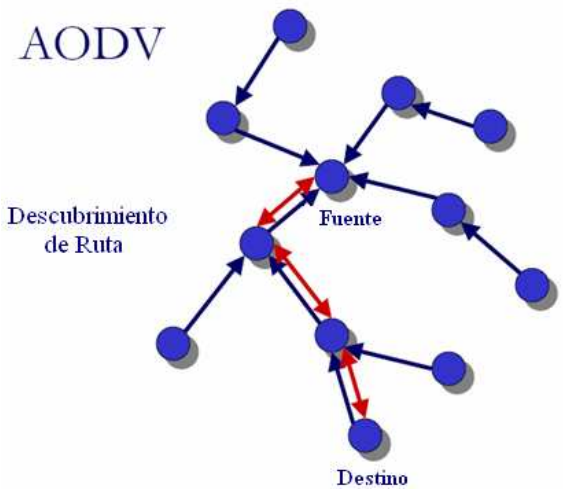


Figura 5. Protocolo de Enrutamiento AODV.

AODV le permite a los nodos móviles obtener rutas rápidamente para nuevos destinos, y no requiere que los nodos mantengan rutas hacia destinos que no se estén comunicando, está diseñado para redes ad hoc móviles pequeñas, puede manejar diferentes tasas de movilidad, así como una variedad de niveles de tráfico de datos, reduce la diseminación de tráfico de control y elimina la sobrecarga en el tráfico de datos, para mejorar su desempeño y escalabilidad [Perkins, *et al*., 2003].

II.3.1 Formato de los mensajes

AODV utiliza tres diferentes tipos de mensajes

a) Mensaje petición de ruta (RREQ)

El formato del mensaje de petición de ruta se muestra en la figura 6, y contiene los siguientes campos:

Figura 6. Mensaje de petición de ruta (RREQ)**.**

Tipo	Indica el tipo de mensaje que se está enviando. 1 indica un mensaje de petición de ruta (RREQ).
J	Bandera de Unión; reservado para multicast.
R	Bandera de Reparación; reservado para multicast.
G	Bandera RREP Gratuito; indica si un RREP gratuito debe ser enviado hacia la dirección IP destino.
D	Bandera Sólo destino; Indica que sólo el destino puede responder a este mensaje RREQ.
U	Número de secuencia no conocido; indica que el número de secuencia no es conocido.
Reservado	Bits reservados para uso futuro, se ignora en recepción si es cero.
Conteo de saltos	El número de saltos desde la dirección IP origen hasta el nodo que maneja la petición.
RREQ ID	Un número de secuencia único para identificar una petición de ruta, junto con la dirección IP del nodo fuente.
Dirección IP destino	Indica la dirección IP del destino deseado.
No. de secuencia destino	Es el último número de secuencia recibido por el originador de cualquier ruta hacia el destino.
Dirección IP Origen	Indica la dirección IP del nodo que originó la petición de ruta.
No. de secuencia Origen	Es el número de secuencia actual del nodo origen.

b) Mensaje Respuesta de Ruta (RREP)

El formato del mensaje de respuesta de ruta se muestra en la figura 7, y contiene los siguientes campos:

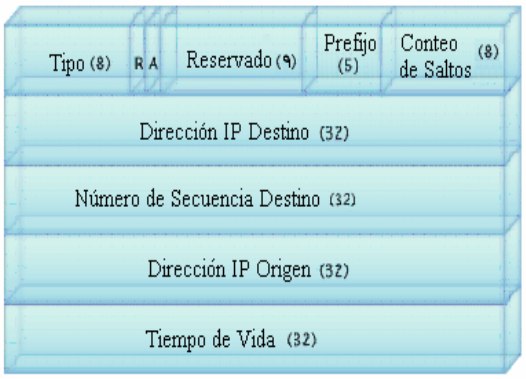


Figura 7. Mensaje de respuesta de ruta (RREP).

Tipo	Indica el tipo de mensaje que se está enviando. 2 indica un mensaje de respuesta de ruta (RREP).
R	Bandera de reparación; usado para multicast.
A	Reconocimiento requerido. Se activa cuando se quiere comprobar si un enlace es unidireccional.
Reservado	Bits reservados para uso futuro, se ignora en recepción si es cero.
Tamaño del prefijo	Si no es cero, el tamaño de prefijo 5 bits especifica que el siguiente salto indicado puede ser usado por cualquier nodo con el mismo prefijo de enrutamiento que el destino pedido.

Conteo de saltos El número de saltos desde la dirección IP origen hasta la dirección IP destino.

Dirección IP destino La dirección IP destino para la cual es proveída la ruta.

No. de secuencia destino El número de secuencia destino asociado a la ruta.

Dirección IP Origen La dirección IP del nodo que originó el mensaje RREQ para la cual es proveída la ruta.

Tiempo de vida El tiempo en milisegundos durante el cual los nodos que han recibido un mensaje RREP deben considerar válida la ruta.

c) Mensaje de error de ruta (RERR)

El formato del mensaje de error de ruta se muestra en la figura 8, y contiene los siguientes campos:

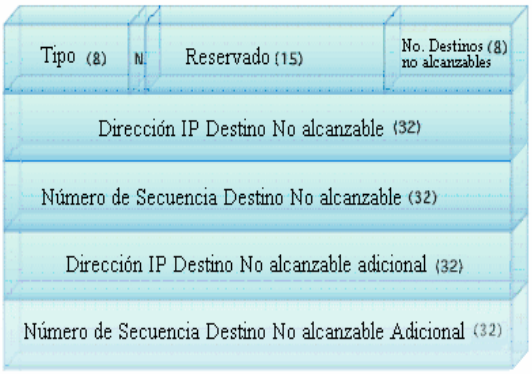


Figura 8. Mensaje de error de ruta (RERR)**.**

Tipo Indica el tipo de mensaje que se está enviando. 3 indica un mensaje de error de ruta.

N	Bandera No borrado; Se establece cuando un nodo realiza una reparación local de un enlace.
Reservado	Bits reservados para uso futuro.
No. Destinos no alcanzables (descount)	El número de destinos no alcanzables incluidos en el mensaje; debe ser al menos 1.
Dirección IP destino no alcanzable	La dirección IP del destino que llega a ser inalcanzable debido a una ruptura de enlace.
No. de secuencia destino no alcanzable	El último número de secuencia conocido del destino que se encuentra en el campo dirección IP destino no alcanzable.

II.3.2 Operación de AODV

II.3.2.1 Números de Secuencia

Los números de secuencia son usados para mantener rutas actualizadas y permiten a los nodos comparar que tan nueva es su información. Un nodo destino incrementa su propio número de secuencia:

- Antes de que un nodo realice un *descubrimiento de ruta*, debe incrementar su propio número de secuencia. Esto previene conflictos con rutas en reversa establecidas anteriormente hacia el originador del mensaje RREQ.

- Antes de que un nodo destino origine un mensaje RREP en respuesta a un mensaje RREQ, debe actualizar su propio número de secuencia al máximo de su número de secuencia actual y el número de secuencia destino en el mensaje RREQ.

Otra razón por la que un nodo puede cambiar el número de secuencia destino en su tabla de enrutamiento es porque un enlace hacia ese destino se perdió o expiró. El nodo determina cuales destinos usan el siguiente salto consultando su tabla de enrutamiento y por cada destino que usa el siguiente salto, el nodo incrementa el número de secuencia y marca la ruta como inválida. En el ejemplo de la figura 9, el nodo 1 envía un mensaje de respuesta de ruta (RREP) al nodo 4 y compara el número de secuencia actual que tiene almacenado en su tabla de enrutamiento con el número de secuencia del mensaje, entonces como el mensaje tiene un número de secuencia mayor (#Sec 128 < 136), el nodo 1 actualiza el número de secuencia en su tabla de enrutamiento.

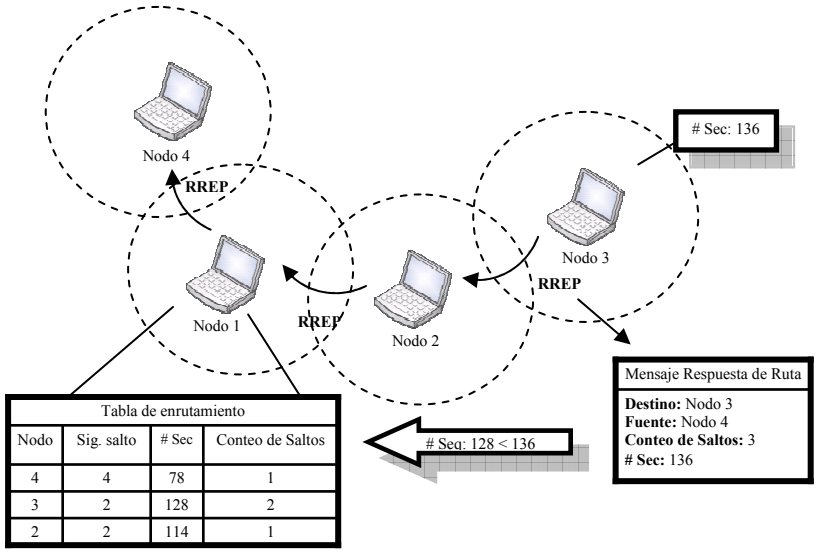


Figura 9. Números de Secuencia.

Un nodo puede cambiar el número de secuencia de un nodo destino sólo si:

- Es el nodo destino, y ofrece una nueva ruta hacia el mismo.
- Si recibe un mensaje AODV con información nueva sobre el número de secuencia para un nodo destino.
- La ruta hacia el nodo destino expira o se rompe.

II.3.2.2 Tabla de enrutamiento y Listas Precursor

AODV requiere que cada nodo mantenga una tabla de enrutamiento por cada destino con el nodo que se está comunicando. La información de la tabla de enrutamiento debe mantenerse aún para rutas de corto tiempo, las cuales son creadas para almacenar temporalmente rutas en reversa hacia los nodos que originaron los mensajes RREQs. Una tabla de enrutamiento contiene los siguientes campos:

- **Dirección IP destino**: La dirección IP del nodo destino para el cual la ruta es proporcionada.
- **Número de Secuencia Destino**: El número de secuencia destino asociado a la ruta.
- **Conteo de Saltos**: Número de saltos necesarios para alcanzar el destino.
- **Siguiente salto**: La dirección del nodo destino o nodo intermedio designado para enviar paquetes hacia el destino.

- **Lista de precursores**: Cada nodo guarda una lista que contiene las direcciones IP de cada uno de sus vecinos que posiblemente se usarán como siguiente salto hacia el destino.
- **Tiempo de vida**: Para una ruta activa este campo representa el tiempo de expiración y para una ruta inválida representa el tiempo de borrado de la ruta.
- **Bandera de enrutamiento:** El estado de la ruta: up (válida), down (no válida) o en reparación [Perkins, *et al*., 2003].

AODV no usa almacenamiento de rutas. En su lugar, cada nodo mantiene sólo la dirección del siguiente salto en la tabla de enrutamiento [Milanovic, *et al*., 2004]. En la figura 10 se muestra las tablas de enrutamiento que almacena cada nodo.

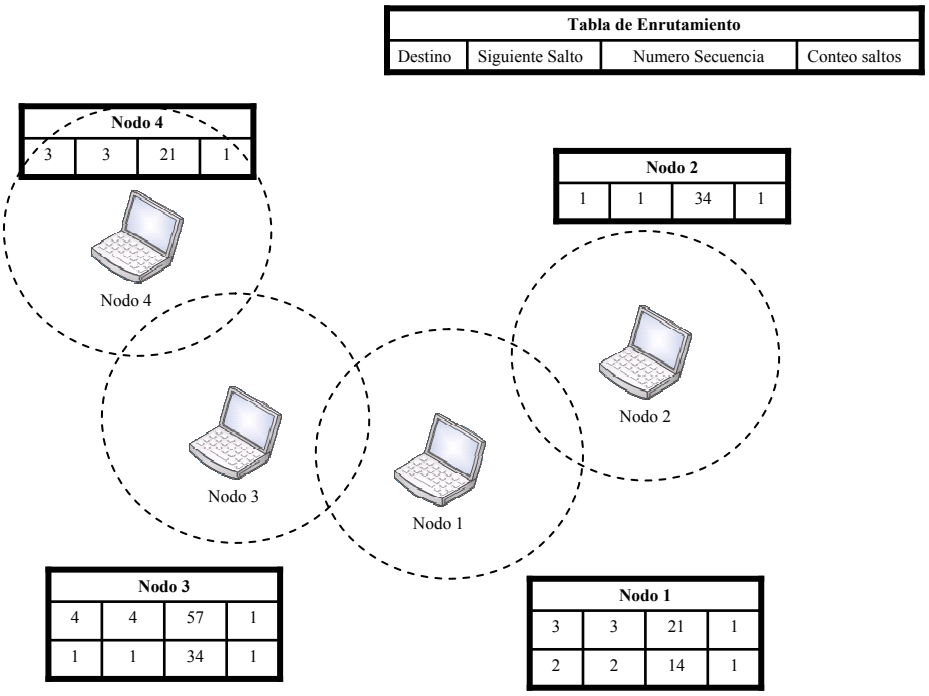


Figura 10. Tablas de Enrutamiento.

Cuando un nodo recibe un mensaje de control, AODV crea o actualiza una ruta para un destino en particular. Si no hay una entrada para ese destino, se crea una entrada. El número de secuencia se determina con la información contenida en el mensaje de control, o bien, el campo *número de secuencia válido* se coloca como falso. La ruta sólo se actualiza si el nuevo número de secuencia es:

1. Más alto que el número de secuencia destino en su tabla de enrutamiento.
2. Los números de secuencia son iguales, pero el conteo de saltos es más pequeño que el conteo de saltos existente en la tabla de enrutamiento.
3. El número de secuencia es desconocido.

El campo *tiempo de vida* de la tabla de enrutamiento inicia con el valor ACTIVE_ROUTE_TIMEOUT y cada vez que la ruta es usada se actualiza con el valor *tiempo actual* + *active_route_time*. Por cada ruta válida que mantiene un nodo en la tabla de enrutamiento, también se mantiene una *lista de precursores* que pueden estar enviando paquetes en esta ruta. La *lista de precursores* en una tabla de enrutamiento contiene las direcciones de los nodos vecinos que se les envió una respuesta de ruta. Estos nodos recibirán mensajes RERR, si el nodo que está al siguiente salto en la ruta llega a ser inalcanzable.

II.3.2.3 Generación de peticiones de ruta

Cuando un nodo fuente necesita enviar información hacia un nodo destino y no tiene una ruta válida para ese destino en sus tablas de enrutamiento, inicia un proceso de *descubrimiento de ruta* para localizar al nodo destino. El descubrimiento de ruta inicia cuando el nodo fuente envía un *mensaje de petición de ruta* (RREQ) hacia sus nodos vecinos, este mensaje contiene la siguiente información:

- *Número de secuencia destino* es el último número de secuencia destino conocido para el destino, si no existe debe colocarse la bandera de número de secuencia desconocido.
- *Número de secuencia origen* es el número de secuencia del nodo, el cual se incrementa antes de insertarlo en el mensaje RREQ.
- *Conteo de saltos* se pone a cero.
- *ID RREQ* le permite al nodo descartar peticiones que hayan sido vistas antes, y es incrementado por el nodo fuente antes de cada nuevo RREQ.
- *Dirección IP fuente y destino.*

Antes de enviar el mensaje RREQ, el nodo fuente almacena el ID RREQ y la dirección IP origen del mensaje RREQ para PATH_DISCOVERY_TIME. De esta forma, cuando el nodo reciba el mensaje otra vez de sus vecinos, este no reprocesará y reenviará el mensaje. Por otro lado un nodo no debe originar más de RREQ_RATELIMIT mensajes RREQ por segundo.

II.3.2.4 Procesado y envío de peticiones de rutas (RREQ)

La figura 11 ilustra la propagación de los mensajes RREQs a través de la red. En este ejemplo, el nodo “s” quiere comunicarse con el nodo “t”.

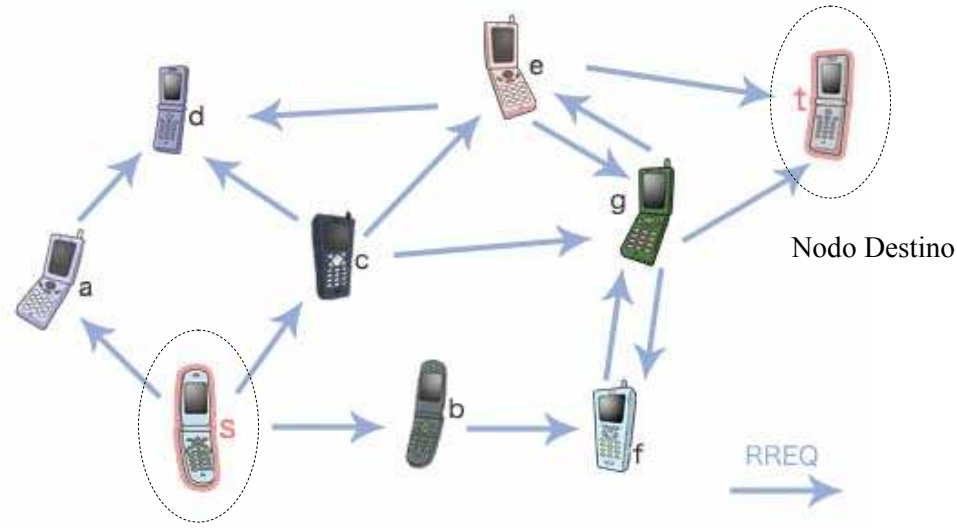


Figura 11. Distribución de los mensajes RREQ por toda la red.

Cada nodo que recibe el mensaje RREQ debe revisar si es el nodo destino, si el nodo que recibe el mensaje RREQ es el destino o es un nodo que tiene una ruta para ese destino debe enviar un *mensaje de respuesta de ruta* (RREP) hacia el nodo fuente, si no es así, el nodo debe incrementar el conteo de saltos del mensaje RREQ y enviarlo hacia sus nodos vecinos [Ilyas, 2003]. Además debe revisar si ha recibido un mensaje RREQ con la misma dirección IP que originó el mensaje RREQ y el ID del RREQ dentro del último PATH_DISCOVERY_TIME. Si ya se había recibido ese mensaje RREQ, el nodo simplemente lo descarta, para prevenir que sean enviados y evitar mensajes RREQs duplicados. Los nodos graban en sus *tablas de enrutamiento* la dirección fuente y el ID

RREQ del nodo vecino del cual se recibió la primera copia del mensaje RREQ, de esta forma se establece una ruta en reversa.

Cuando la ruta en reversa es creada o actualizada, puede ocurrir lo siguiente:

1. El número de secuencia origen del mensaje RREQ es comparado con el *número de secuencia destino* de la tabla de enrutamiento y copiado si es más grande que el valor existente.
2. El campo *número de secuencia* válido se coloca como verdadero
3. El siguiente salto en la tabla de enrutamiento es el nodo del cual se recibió el mensaje RREQ (se obtiene de la *dirección IP fuente* en el encabezado IP y algunas veces no es igual al campo *dirección IP origen* en el mensaje RREQ).
4. El *conteo de saltos* es copiado del mensaje RREQ.

El nodo actual puede usar la ruta en reversa para enviar paquetes de datos de la misma forma como cualquier ruta en la tabla de enrutamiento.

Si un nodo no genera un mensaje RREP, y el encabezado IP recibido tiene un TTL más grande que 1, el nodo actualiza y envía el mensaje RREQ hacia la dirección 255.255.255.255, es decir, envía el mensaje RREQ a sus nodos vecinos. Para actualizar el mensaje RREQ, el campo *TTL* en el encabezado IP es decrementado por uno, y el campo *conteo de saltos* en el mensaje RREQ es incrementado por uno. Finalmente, el *número de secuencia destino* se coloca al máximo valor recibido en el mensaje RREQ.

Este proceso continúa hasta que el mensaje RREQ llega al nodo destino o se encuentre algún nodo intermedio con una ruta para ese destino cuyo número de secuencia destino sea más grande o igual al que tiene el mensaje RREQ [Perkins, *et al*., 2003].

II.3.2.5 Generación de Respuestas de Ruta

Una vez que el mensaje RREQ llega al nodo destino o a un nodo intermedio que tiene una ruta más actual, el nodo destino/intermedio responde con un mensaje RREP "unicast" de regreso al nodo vecino del cual se recibió el primer mensaje RREQ [Royer y Toh, 1999].

El mensaje RREP contiene la siguiente información:

- El número de secuencia destino y el conteo de saltos es copiado de su tabla de enrutamiento.
- La dirección IP destino, la dirección IP origen y el número de secuencia origen es extraído del mensaje RREQ.

Si el nodo que genera el mensaje RREP es el *destino*, debe incrementar su propio número de secuencia por uno si el número de secuencia en el mensaje RREQ es igual a ese valor. De otra manera, el destino no cambia su número de secuencia antes de generar el mensaje RREP. El nodo destino pone su número de secuencia dentro del campo *número secuencia destino*, introduce el valor cero en el campo *conteo de saltos* y copia el valor de MY_ROUTE_TIMEOUT dentro del campo *tiempo de vida* del mensaje RREP.

Si el nodo que genera el mensaje RREP no es el nodo destino, pero hay un nodo intermedio con una ruta nueva hacia el destino, copia su número de secuencia dentro del campo *número de secuencia destino*, pone su distancia en saltos hacia el destino en el campo *conteo de saltos* del mensaje RREP y calcula el valor del campo *tiempo de vida* del mensaje RREP restando el *tiempo actual* del *tiempo de expiración* en la tabla de enrutamiento.

En cualquier caso, el mensaje RREP es enviado al siguiente salto hacia el originador del mensaje RREQ. Conforme el mensaje RREP viaja hacia el nodo que originó el mensaje RREQ, el campo *conteo de saltos* es incrementado por uno en cada salto. Entonces, cuando el mensaje RREP alcanza al nodo fuente, el campo *conteo de saltos* representa la distancia, en saltos, del nodo destino al nodo fuente.

II.3.2.6 Recibiendo y enviando respuestas de ruta (RREP)

Cada vez que un nodo recibe un mensaje RREP incrementa el valor del campo *conteo de saltos*, entonces, puede ser actualizada o creada una entrada para el nodo destino o cualquier otro nodo en la tabla de enrutamiento. En la figura 12 se ilustra la propagación de los mensajes RREP.

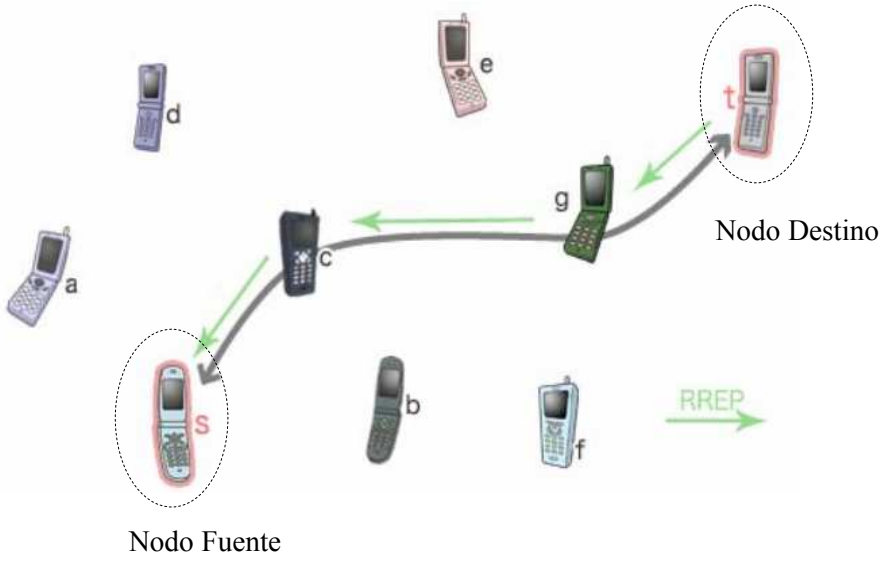


Figura 12. Generación de mensajes RREP.

La ruta existente es actualizada si:

1. El número de secuencia en la tabla de enrutamiento está marcada como inválida.
2. El *número de secuencia destino* en el mensaje RREP es más grande que el número de secuencia destino de la tabla de enrutamiento y el valor conocido es válido.
3. Los números de secuencia son los mismos, pero la ruta está marcada como inactiva, o
4. Los números de secuencia son los mismos, y el nuevo conteo de salto es más pequeño que el conteo de saltos en la tabla de enrutamiento.

Si la entrada de la tabla de enrutamiento hacia el destino es creada o actualizada:

- La ruta es marcada como activa.

- El número de secuencia destino es marcado como válido.
- El siguiente salto en la entrada de ruta es el nodo del cual se recibió el mensaje RREP, indicado en el campo *dirección IP fuente* del encabezado IP.
- El conteo de salto se pone al valor del nuevo *conteo de saltos*.
- El tiempo de expiración se pone como el *tiempo actual* más el valor del *tiempo de vida* en el mensaje RREP.

Si el nodo que recibe el mensaje RREP no es el destino y una ruta de envío ha sido creada o actualizada, el nodo tiene que consultar su tabla de enrutamiento para determinar el siguiente salto, y enviar el mensaje RREP hacia el nodo fuente usando la información de la tabla de enrutamiento.

Conforme el mensaje RREP se propaga a lo largo de la ruta en reversa, los nodos actualizan las entradas hacia el destino en sus tablas de enrutamiento [Milanovic, *et al*., 2004]. Cada entrada de ruta tiene asociado un temporizador de ruta, el cual es usado para borrar rutas que no están activas. Finalmente, una vez que el mensaje RREP llega al nodo fuente, se puede usar esta ruta para enviar paquetes de datos hacia el destino.

Debido a que el mensaje RREP se envía utilizando la ruta establecida por el mensaje RREQ, AODV sólo soporta enlaces simétricos [Royer y Toh, 1999].

Por otro lado, si no se establece una ruta dentro de NET_TRANSVERSAL_TIME milisegundos, el nodo puede tratar otra vez de descubrir una ruta enviando otro mensaje

RREQ, arriba de un máximo de RREQ_RETRIES veces en el máximo valor de TTL. Cada nuevo intento debe incrementar y actualizar el ID de RREQ. Si un descubrimiento de ruta ha sido intentado RREQ_RETRIES veces en el máximo TTL sin recibir un mensaje RREP, todos los paquetes de datos almacenados deben ser tirados del buffer y debe ser enviado un *mensaje de destino no alcanzable*.

II.3.2.7 Control de envío de los mensajes de petición de ruta (RREQ)

Para prevenir un envío innecesario de mensajes RREQs en toda la red, el nodo fuente debe usar una técnica llamada *búsqueda expansiva en anillo*. En una *búsqueda expansiva en anillo*, se controla el valor del campo *tiempo de vida* (TTL) en el encabezado IP. El primer mensaje RREQ enviado por la fuente tiene un TTL = TTL_START. El valor del TTL define el máximo número de saltos que un mensaje RREQ puede moverse a través de la red ad hoc móvil. También se establece el *tiempo de expiración* para recibir un mensaje RREP en RING_TRANSVERSAL_TIME milisegundos. El TTL_VALUE usado en el cálculo de RING_TRANSVERSAL_TIME es igual al valor del campo TTL en el encabezado IP. Si el mensaje RREQ expira sin recibir un mensaje RREP, la fuente envía otra vez el mensaje RREQ. Esta vez el TTL se incrementa a *TTL_START* + *TTL_INCREMENT*. Este proceso continúa hasta que se recibe un mensaje RREP o hasta que el campo TTL alcanza TTL_THRESHOLD. Si el campo TTL alcanza TTL_THRESHOLD, se envía un mensaje RREQ con TTL=NET_DIAMETER, el cual difunde el mensaje RREQ por toda la red. Una vez que el campo TTL es igual a NET_DIAMETER, el tiempo para esperar un mensaje RREP se pone a NET_TRANSVERSAL_TIME. Si un nodo fuente hace una búsqueda en

toda la red y todavía no recibe un mensaje RREP, puede tratar de encontrar una ruta hacia el nodo destino un máximo de RREQ_RETRIES veces.

La entrada de una tabla de enrutamiento que ya expiró no debe ser eliminada antes de *tiempo actual* + *DELETE_PERIOD*. Cualquier entrada de la tabla de enrutamiento que espera un mensaje RREP no debe ser borrada antes de *tiempo actual* + *2* * *NET_TRANSVERSAL_TIME* [Perkins, *et al*., 2003].

II.3.2.8 Mensajes HOLA

Un aspecto adicional del protocolo es el uso de mensajes *hola* (este requerimiento no es obligatorio), estos mensajes se difunden periódicamente para informar a cada nodo móvil de otros nodos en su vecindario. Los mensajes *hola* pueden ser usados para mantener la conectividad local de un nodo. Sin embargo, no se requiere el uso de mensajes *hola*. Los nodos escuchan la retransmisión de paquetes de datos para asegurar que el siguiente salto está todavía dentro de su alcance. Si tal retransmisión no es escuchada, el nodo puede usar la recepción de mensajes *hola*, para determinar si el siguiente salto está dentro del rango de comunicación [Royer y Toh, 1999]. Cada vez que un nodo recibe un mensaje *hola* de su nodo vecino, éste actualiza la información asociada con ese nodo en su tabla de enrutamiento [Ilyas, 2003].

Cada HELLO_INTERVAL milisegundos, el nodo revisa si ha enviado un mensaje *broadcast* dentro del último HELLO_INTERVAL. Si no es así, difunde un mensaje RREP con TTL = 1, llamado mensaje *hola*, con los campos del mensaje RREP como sigue:

Dirección IP destino: Dirección IP del nodo

Número de secuencia destino: El último número de secuencia del nodo

Conteo de salto 0

Tiempo de vida ALLOWED_HELLO_LOSS * HELLO_INTERVAL

Un nodo puede determinar conectividad escuchando los mensajes de su conjunto de vecinos. Si dentro del último DELETE_PERIOD, ha recibido un mensaje *hola* de un nodo vecino, y ese vecino no recibe un mensaje por más de ALLOWD_HELLO_LOSS * HELLO_INTERVAL milisegundos, el nodo debe asumir que el enlace se perdió.

Si un nodo recibe un mensaje *hola* de un nodo vecino, el nodo debe asegurarse que tenga una ruta activa hacia ese nodo vecino, y crear una si es necesario. Si ya existe una ruta, entonces el tiempo de vida de la ruta debe ser incrementada, al menos ALLOWED_HELLO_LOSS * HELLO_INTERVAL. La ruta hacia el nodo vecino debe contener el último *número de secuencia destino* del mensaje *hola*. El nodo actual puede empezar a usar esta ruta para enviar paquetes de datos. Las rutas que son creadas por los mensajes *hola* y que no son usadas por otras rutas activas tendrán listas precursor vacías y no activarán mensajes RERR si el vecino se mueve lejos.

II.3.2.9 Mensajes de error de ruta, expiración de ruta y borrado de ruta

El error de ruta y el proceso de ruptura de enlace requieren los siguientes pasos:

- Invalidación de rutas existentes.
- Escuchar destinos afectados.
- Determinar cuales vecinos pueden ser afectados.
- Enviar un mensaje RRER apropiado a tales vecinos.

Los mensajes de error (RERR) le permiten a AODV ajustar rutas cuando los nodos se mueven. Un nodo no debe generar más de RERR_RATELIMIT mensajes RERR por segundo.

Un nodo envía un mensaje RERR en 3 situaciones:

1. El nodo detecta una ruptura de enlace para el siguiente salto de una ruta activa en su tabla de enrutamiento mientras se están transmitiendo datos (y la reparación de ruta no fue exitosa), o
2. El nodo recibe un paquete de datos para una ruta inválida o para un destino no conocido.
3. El nodo recibe un mensaje RERR de un vecino de una o más rutas activas.

El mensaje RERR contendrá una lista de los destinos no alcanzables e invalidará cualquier ruta donde el destino esté presente. El mensaje RERR es enviado hacia la dirección broadcast local (IP DESTINO ==255.255.255.255, TTL=1) con los destinos no alcanzables, y sus correspondientes números de secuencia destino. El campo *descount* del mensaje RRER indica el número de destinos no alcanzables.

En la figura 13 se muestra la propagación de los mensajes RERR por toda la red cuando se pierde la ruta hacia el destino.

Figura 13. Envío de mensajes RERRs a través de la red.

Antes de transmitir el mensaje RERR, se realizan algunas actualizaciones en la tabla de enrutamiento que pueden afectar a los *números de secuencia destino* para los destinos no alcanzables. Para cada uno de estos destinos, la entrada de la tabla de enrutamiento correspondiente se actualiza como sigue:

- El número de secuencia destino de esta entrada de enrutamiento, si existe y es válida, se incrementa para los casos 1 y 2, y es copiado del mensaje RERR que llega en el caso 3.
- La entrada es invalidada marcando la entrada de ruta como inválida.
- El campo *tiempo de vida* es actualizado al tiempo actual más DELETE_PERIOD, antes de este tiempo, la entrada no debe ser borrada.

II.3.2.10 Reparación Local

Cuando un enlace se rompe a lo largo de una ruta activa, hay varios destinos que se convierten inalcanzables. El nodo que está arriba del enlace (i.e. en dirección al nodo fuente) puede elegir hacer una *reparación local* si el destino no está más allá de MAX_REPAIR_TTL saltos. Para realizar una *reparación local*, el nodo incrementa el número de secuencia destino y entonces envía un mensaje RREQ hacia ese destino. El nodo que inicia la reparación espera un tiempo para recibir mensajes RREPs en respuesta al mensaje RREQ. Si después de un tiempo, este nodo no recibe un mensaje RREP, transmite un mensaje RERR hacia ese destino. El mensaje de error contiene la dirección IP del destino que es inalcanzable debido a la ruptura del enlace. Después de recibir el mensaje RERR, el nodo busca en su tabla de enrutamiento alguna ruta hacia el destino no alcanzable el cual usa el originador del mensaje RERR como el siguiente salto. Si tales rutas existen, son invalidadas y el nodo difunde un nuevo mensaje RERR hacia sus vecinos. Este proceso continúa hasta que el nodo fuente recibe el mensaje de error. El nodo fuente invalida las rutas enlistadas y reinicia el proceso de descubrimiento de ruta si es necesario.

Por el otro lado, si el nodo recibe uno o más RREPs, compara el *conteo de saltos* de la nueva ruta con el *conteo de saltos* de la tabla de enrutamiento inválida para ese destino. Si el conteo de saltos de la nueva ruta hacia el destino es más grande que el conteo de saltos de la ruta anterior, el nodo debe enviar un mensaje RERR para ese destino, con la bandera "N" puesta y actualizar la tabla de enrutamiento para ese destino. La bandera "N" indica que se realizó una *reparación local* y debe inicializarse cuando la ruta expire.

La *reparación local* de una ruta antes de que se reciba un paquete de datos ocasiona el riesgo de reparar rutas que no se estén usando. Entonces dependiendo del tráfico local en la red, el nodo puede escoger entre reparar las rutas antes de que los paquetes sean recibidos o esperar hasta que un dato sea recibido para comenzar el proceso de *reparación de ruta*.

II.3.2.11 Configuración de Parámetros

A continuación se muestran algunos parámetros importantes asociados con las operaciones del protocolo AODV. La información que se presenta indica los valores utilizados por omisión.

Nombre del parámetro	*Valor*
ACTIVE_ROUTE_TIMEOUT	3,000 MILISEGUNDOS
ALLOWED_HELLO_LOSS	2
BLACKLIST_TIMEOUT	RREQ_RETRIES*NET_TRANSVERSAL_TIME
DELETE_PERIOD	Si se usan los mensajes *hola*, debe ser al menos ALLOWED_HELLO_LOSS * HELLO_INTERVAL.

HELLO_INTERVAL	1,000 MILISEGUNDOS
LOCAL_ADD_TTL	2
MAX_REAPIR_TTL	0.3 * NETWORK_DIAMETER
MIN_REPAIR_TTL	Último conteo de saltos conocido hacia el destino.
MY_ROUTE_TIMEOUT	2 * ACTIVE_ROUTE_TIMEOUT
NET_DIAMETER	35
NET_TRANVERSAL_TIME	2*NODE_TRANSVERSAL_TIME*NET_DIAMETER
NEXT_HOP_WAIT	NODE_TRANSVERSAL_TIME + 10
NODE_TRANSVERSAL_TIME	40 MILISEGUNDOS
PATH_DISCOVERY_TIME	2*NET_TRANSVERSAL_TIME
RERR_RATELIMIT	10
RING_TRANSVERSAL_TIME	2*NODE_TRANSVERSAL_TIME* (TTL_VALUE+TIMEOUT_BUFFER)
RREQ_RETRIES	2
RREQ_RATELIMIT	10
TIMEOUT_BUFFER	2
TTL_START	1
TTL_INCREMENT	2
TTL_THESHOLD	7
TTL_VALUE	Valor del campo TTL en el encabezado IP mientras se realiza una *búsqueda expansiva en anillo*.

- Si se usan los mensajes *hola*, el valor del parámetro ACTIVE_ROUTE_TIMEOUT debe ser mayor que el valor ALLOWED_HELLO_LOSS *HELLO_INTERVAL.

- TIMEOUT_BUFFER provee un buffer para la expiración, si el mensaje RREP se retrasa debido a la congestión, es menos probable que expire mientras el mensaje RREP esté todavía en la ruta de regreso a la fuente. Para omitir este buffer, se coloca TIMEOUT_BUFFER = 0.
- DELETE_RATIO determina el tiempo de disponibilidad de los enlaces hacia los nodos del siguiente salto. Más allá de este tiempo los nodos vecinos pueden borrar la ruta hacia el destino.
- NET_DIAMETER mide el máximo número posible de saltos entre dos nodos en la red.
- NODE_TRANSVERSAL_TIME es el tiempo promedio de un salto y debe incluir retardos de cola, tiempos de procesamiento interrumpido y tiempos de transferencia.
- TTL_START debe estar colocado al menos a 2 si los mensajes *hola* son usados para información de conectividad local.
- BLACKLIST_TIMEOUT debe ser incrementado si se usa una *búsqueda expansiva en anillo*. En tales casos, debería ser {[(TTL_THRESHOLD -TTL_START) / TTT_INCREMENT] + 1+ RREQ_RETRIES}* NET_TRANSVERSAL_TIME. Esto es para contar todos los intentos adicionales de descubrimiento de ruta posibles.

El desempeño del protocolo AODV es sensitivo a los valores escogidos de estas constantes, las cuales algunas veces dependen de las características del protocolo de capa de enlace, tecnologías radio, etc [Perkins, *et al*., 2003].

Capítulo III.

PROTOCOLOS DE MACRO Y MICROMOVILIDAD EN REDES CABLEADAS

III.1 Introducción

La movilidad de un nodo móvil en una red puede ser clasificada dentro de dos categorías. Por un lado, está la movilidad dentro de un sólo dominio administrativo limitado a una región geográfica, la cual es llamada *micromovilidad* y por el otro lado está la *macromovilidad*, la cual trata con la movilidad a través de regiones más grandes, algunas veces comprende varias redes, con tecnologías de acceso potencialmente diferentes, las cuales pueden pertenecer a diferentes dominios administrativos [Manges, *et al.*, 2004]. La figura 14 presenta dos redes de acceso inalámbricas conectadas a través de gateways hacia Internet. En general, el objetivo principal del manejo de movilidad de un nodo es asegurar conectividad continua y transparente entre la micromovilidad y macromovilidad, la cual ocurre en un período corto de tiempo [Saha, *et al*., 2004].

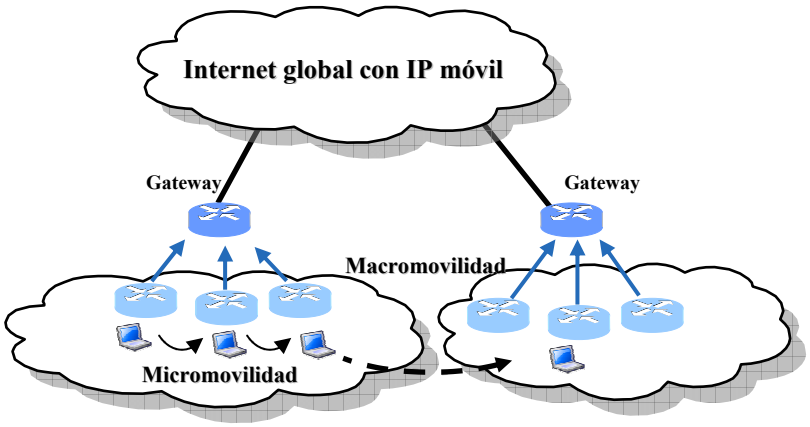


Figura 14. Macromovilidad **y** Micromovilidad.

Para el soporte de movilidad global en una red, IP Móvil es una solución apropiada para manejar los traspasos de un nodo móvil [Vena, *et al*., 2002]. Sin embargo, IP Móvil introduce sobrecarga significativa en la red, lo que se traduce en un incremento de retardo, pérdida de paquetes y señalización cuando el nodo móvil realiza traspasos frecuentes dentro de un área geográfica muy pequeña [Saha, *et al*., 2004]. Para mejorar el desempeño de IP Móvil en un ambiente con traspasos frecuentes dentro de un sólo dominio IP, se han desarrollado varios *protocolos de micromovilidad*. Entre los protocolos de micromovilidad más populares se encuentran IP Celular, IP Móvil jerárquico y HAWAII.

En este capítulo se describen estos protocolos de micromovilidad, dándole mayor enfoque al protocolo de micromovilidad HAWAII, el cual es usado en este trabajo de tesis. Además, como los protocolos de micromovilidad trabajan con IP Móvil, también se da una breve explicación de este protocolo.

III.2 IP Móvil

En IP Móvil (MIP), un nodo pertenece a una red de casa y la dirección IP asignada a ese nodo móvil es llamada *dirección de casa (Home Address)*. El nodo móvil siempre se identifica con esta dirección, independientemente de su punto actual de unión hacia Internet. Además, define dos entidades para proveer soporte de movilidad transparente: un *agente de casa* (Home Agent - HA) y un *agente foráneo* (Foreign Agent - FA) en el caso de IPv4. El agente de casa se asigna estáticamente al nodo móvil basado en su dirección de casa y el agente foráneo se asigna basado en su localización actual [Ramjee, *et al*., 1999]. El nodo móvil también tendrá otra dirección, llamada *asistente de dirección* (Care-Of-Address – COA) y se usará para localizar al móvil cuando éste se encuentre en una red foránea, es decir, el CoA estará asociado con la posición actual del nodo móvil. De esta manera, la dirección de casa actúa como su identificador permanente y el CoA como su localizador temporal. [Wisely, *et al*., 2002].

El agente de casa y el agente foráneo envían periódicamente *mensajes de aviso de agente* en la red de casa y en la red foránea respectivamente para notificar al nodo móvil de su existencia. Los agentes también envían *mensajes de aviso de agente* en respuesta al *mensaje de solicitud* de los nodos móviles activos. El nodo móvil considera si está en su red de casa o en una red foránea de acuerdo al mensaje de aviso de agente [Yu, *et al*., 2003].

En el envío de paquetes hacia un nodo móvil, un nodo correspondiente siempre envía el paquete hacia la dirección de casa del nodo móvil, independientemente de la posición actual del nodo móvil; este procedimiento se ilustra en el paso 1 de la figura 15. En la red

de casa, el agente de casa del nodo móvil intercepta los paquetes y los encapsula dentro de un nuevo paquete IP, es decir, el agente de casa crea un nuevo paquete, con un nuevo encabezado que contiene el CoA como dirección destino y la dirección fuente es la dirección del HA, además la nueva parte de datos consiste del paquete original completo. El HA envía estos nuevos paquetes hacia la red foránea (paso 2). En la red foránea, el FA hace la función de gateway del nodo móvil, desencapsula los paquetes (el paquete original se extrae removiendo el encabezado IP exterior) y los envía a su nodo móvil (paso 3). Esta operación algunas veces es llamada *tunelaje*, porque los paquetes son encapsulados en un extremo del túnel y desencapsulados cuando alcanzan el otro extremo. En la dirección inversa, los paquetes enviados por el nodo móvil pueden ser enrutados directamente hacia su destino usando los mecanismos de enrutamiento IP estándar (Paso 4) [Yu, *et al*., 2003].

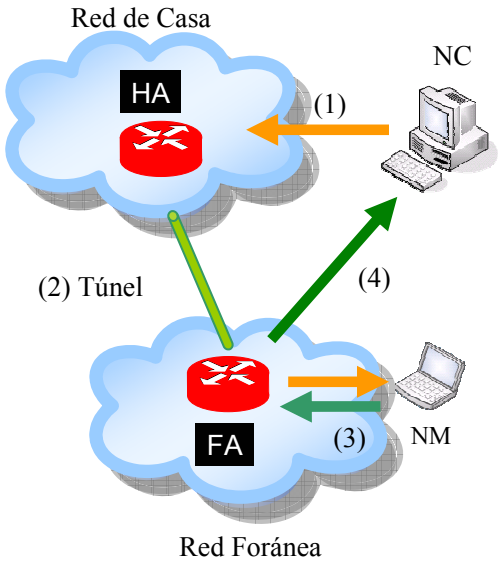


Figura 15. IP Móvil

Como se ve en la figura 15, los paquetes hacia el nodo móvil deben viajar por medio del agente de casa, pero los paquetes originados por el nodo móvil pueden ser enviados directamente hacia el nodo correspondiente (NC). Esta característica de IP Móvil, es llamada *enrutamiento triangular*. Para evitar este problema se utiliza una extensión de MIP llamada *optimización de ruta* que le permite al nodo correspondiente enviar paquetes directamente hacia el nodo móvil [Wisely, *et al*., 2002].

El nodo móvil requiere registrarse con su agente de casa cada vez que cambia su CoA. Si la distancia entre la red foránea y la red de casa del nodo móvil es grande, el retardo de señalización para estas registraciones puede ser largo y provocar una interrupción para el tráfico de usuario durante cada traspaso [Ramjee, *et al*., 1999]. Para aliviar este problema se puede hacer uso de un protocolo de micromovilidad.

III.3 Protocolos de Micromovilidad

Como se mencionó anteriormente, para mejorar el funcionamiento de IP Móvil dentro de un sólo dominio, se han desarrollado varios *protocolos de micromovilidad*. Estos protocolos soportan movimientos locales del nodo móvil en un sólo dominio IP sin informar al agente de casa sobre los traspasos frecuentes. Con esto se reduce la latencia y la pérdida de paquetes durante el traspaso y se eliminan los mensajes de registro entre nodos móviles y agentes de casa distantes cuando el nodo móvil permanece dentro de su área de

cobertura local. La eliminación de los mensajes de registro reduce la carga de señalización de la red en el soporte de movilidad [Jaiswal, *et al*., 2004], [Manges, *et al.*, 2004].

El objetivo principal de los *protocolos de micromovilidad* es asegurar que los paquetes que llegan de Internet, destinados hacia los nodos móviles, sean enviados al enrutador de acceso de manera eficiente [Manges, *et al.*, 2004]. La mayoría de estos protocolos dividen a la red dentro de dominios y trabajan en un escenario donde el nodo móvil se está moviendo y cambiando su punto de unión a la red. La comunicación con el punto de unión (enrutador de acceso) es siempre directo, es decir, a un sólo salto [Michalak, *et al*., 2005]. Entre los protocolos de micromovilidad se encuentran IP Celular, IP Móvil jerárquico y HAWAII.

III.3.1 IP Celular

El protocolo de micromovilidad *IP Celular* (CIP) fue propuesto por la universidad de Columbia y el centro de investigación Ericsson, utiliza IP Móvil para proveer soporte de movilidad de área amplia, además soporta voceo y un número de técnicas de traspaso.

El principal componente de las redes CIP son los enrutadores de acceso, los cuales son llamado nodos CIP, estos enrutadores implementan IP Celular en lugar de enrutamiento IP estándar, son usados por los nodos móviles para enviar y recibir datos a través de la interfaz inalámbrica y enrutar los paquetes dentro de la red CIP [Jaiswal, *et al*., 2004].

Los principales procedimientos de IP Celular son enrutamiento, traspaso y voceo (paging).

a) **Enrutamiento :** Los enrutadores de acceso en la red CIP emiten periódicamente avisos (beacons). Los nodos móviles usan estos mensajes para localizar al enrutador de acceso más cercano y pueden enviar un paquete a cualquier destino transmitiéndolo a ese enrutador de acceso. Todos los paquetes transmitidos por los nodos móviles dentro de un dominio CIP son enviados salto a salto hacia el gateway independientemente de la dirección destino y los envía hacia su destino de acuerdo a los mecanismos de enrutamiento IP [Campbell, *et al*., 2000]. Para enviar paquetes destinados hacia el nodo móvil, los nodos CIP usan la ruta en reversa usada recientemente para transmitir paquetes del nodo móvil al gateway, la cual está presente en el almacenamiento de ruta (*route cache*) [Jaiswal, *et al*., 2004]. Si el nodo móvil se mueve dentro de la red CIP siempre hay una ruta en reversa válida del gateway al nodo móvil, entonces los paquetes que llegan de Internet pueden ser correctamente enviados hacia el nodo móvil [Valko, *et al*., 1999].

b) **Traspaso:** Cuando un nodo móvil se mueve del rango de un enrutador de acceso a otro, ocurre un *proceso de traspaso*, en el cual, siempre se envía un paquete de actualización de ruta (RU - *Route Update*) hacia el gateway, para informarle sobre su posición actual de unión [Jaiswal, *et al*., 2004].

En las figuras 16 y 17 se muestran los dos tipos de esquemas de traspaso que soporta IP Celular.

Traspaso duro: En este esquema, un nodo móvil sintoniza su radio hacia el nuevo enrutador de acceso (Paso 1) y envía un paquete RU hacia el gateway, estableciendo nuevas entradas de almacenamiento de ruta. (Paso 2) [Campbell, *et al*., 2000]. Cuando el RU alcanza al enrutador de cruce, donde la nueva ruta coincide con la ruta anterior, la entrada de almacenamiento de ruta es reemplazada con una nueva apuntando hacia el nuevo enrutador de acceso, es decir, el enrutador de cruce redirecciona todos los paquetes que anteriormente se enviaban al enrutador de acceso anterior para enviarlos hacia el nuevo enrutador de acceso actualizando todas las rutas de almacenamiento que van hacia el gateway (Paso 3). Una vez que la ruta anterior expira, los paquetes destinados al nodo móvil son enviados sólo hacia la nueva ruta. Después de que se establece la nueva ruta, el nodo móvil recibe los paquetes de datos por medio del nuevo enrutador de acceso (Paso 4). Si el nodo no tiene paquetes que enviar durante un traspaso, este debe generar mensajes de actualización de ruta para permitir la correcta actualización de las rutas almacenadas [Ilyas, 2003].

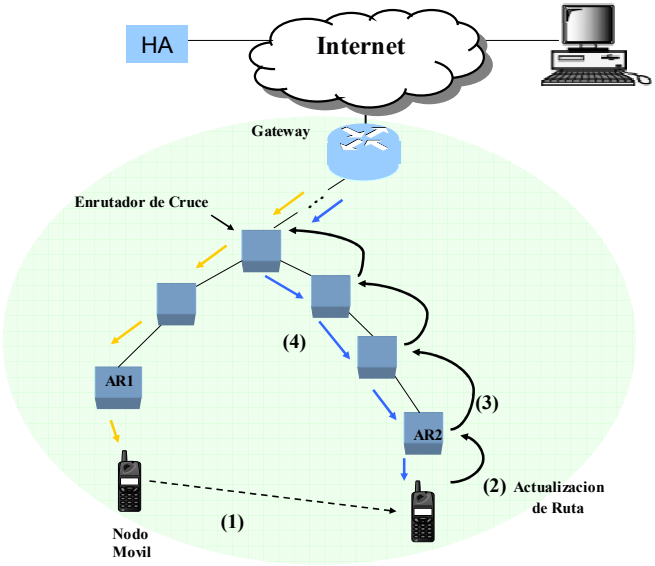


Figura 16. Esquema de Traspaso Duro.

Traspaso Semisuave: Para iniciar este traspaso, el nodo móvil envía un paquete RU con una bandera "S" hacia el nuevo enrutador de acceso AR2 (Paso 1) y continúa escuchando al enrutador de acceso anterior AR1 (Paso 2). Usualmente, el paquete RU establece una nueva ruta, pero cuando llega al enrutador de cruce, la entrada de almacenamiento de la ruta anterior apunta hacia el enrutador de acceso anterior, y esta ruta no es reemplazada con una nueva (Paso 3). En lugar de eso, la nueva entrada es añadida dentro del almacenamiento de ruta y a la entrada anterior se le permite existir. Ahora el enrutador de cruce envía los paquetes dirigidos al nodo móvil hacia ambos enrutadores de acceso (Paso 4). Después que el nodo móvil se mueve al nuevo enrutador de acceso, le envía un paquete RU sin la bandera 'S' borrada. Este paquete borra la entrada de almacenamiento de la ruta anterior en el enrutador de cruce y sólo se mantiene válida la nueva ruta (Paso 5) [Campbell, *et al*., 1999], [Valko, *et al*., 1999]. El *traspaso semisuave* minimiza la pérdida de paquetes sobre el *traspaso duro*. Independientemente del método elegido, el procedimiento de traspaso es iniciado por el nodo móvil [Campbell, *et al*., 1999].

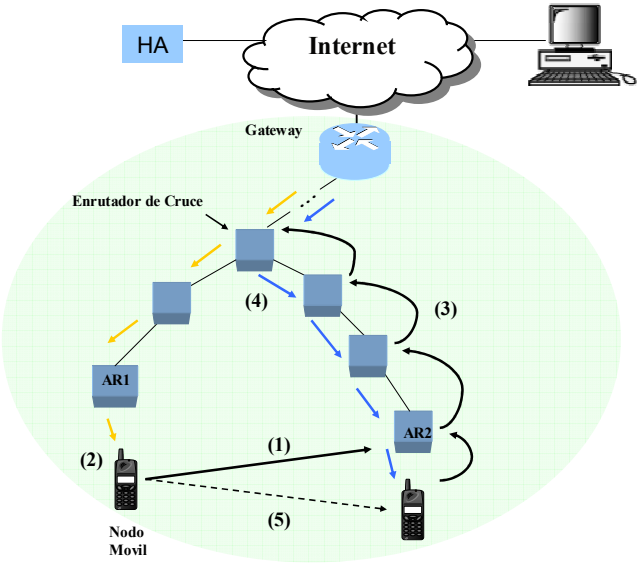


Figura 17. Esquema de Traspaso Semisuave.

c) Voceo (*Paging*): El *proceso de voceo* ocurre cuando un paquete es dirigido hacia un nodo móvil inactivo, y el gateway o enrutador de acceso no encuentra una ruta válida para ese destino. Debido a la falta de mensajes de actualización, el almacenamiento de rutas de un nodo móvil inactivo expirará completamente, entonces, para mantenerse alcanzable, los nodos móviles transmiten *paquetes de actualización de voceo* en intervalos regulares hacia el gateway y hacia los enrutadores de acceso. Los paquetes de actualización de voceo no pueden actualizar el almacenamiento de rutas, lo que da como resultado que los nodos móviles inactivos tengan almacenamiento de voceo pero no almacenamiento de ruta. En contraste, los nodos móviles activos mantienen ambos, enrutamiento y almacenamiento de voceo. Los enrutadores de acceso pueden opcionalmente mantener un almacenamiento de voceo. [Campbell, Gomez, Kim, 2002].

El operador de la red IP celular puede dividir la red en *áreas de voceo*, las cuales típicamente comprenden unos cuantos enrutadores de acceso adyacentes. Los nodos móviles inactivos sólo transmitirán *paquetes de actualización de voceo* cuando se muevan entre áreas de voceo. Cada área de voceo tiene un identificador, el cual está incluido en los avisos transmitidos por los enrutadores de acceso [Campbell, *et al*., 2000].

III.3.2 IP Móvil Jerárquico (HMIP Hierarchical Mobile IP)

IP Móvil Jerárquico es una arquitectura propuesta por los centros de investigación de Ericsson y Nokia, usa una jerarquía basada en la organización física de los agentes foráneos

(FA) para manejar registros IP móvil localmente, asumiendo que el nodo móvil está en una red foránea [Ilyas, 2003]. Con esto, el nodo móvil puede evitar registrarse con el HA (el cual puede estar muy lejos) cada vez que cambia su punto de unión.

III.3.2.1 IPv4 Móvil Jerárquico

Un dominio está asignado al FA más alto en la jerarquía para esta región, el cual es llamado *agente foráneo gateway* (GFA). El dominio está divido en subdominios, cada uno es asignado a FAs que están en niveles menores en la jerarquía. Los FAs en el nivel más bajo de la jerarquía, por ejemplo, en el salto más cercano hacia los nodos móviles, están definidos como los *enrutadores de acceso* (ARs) y cualquier FA entre los GFAs y los ARs están definidos como los agentes foráneos regionales (RFAs)**.** En un dominio IP, los enrutadores que no tienen las funciones de un GFA o un RFA, corren el estándar de enrutamiento IP. Los nodos móviles envían mensajes de registro IP Móvil (con extensiones apropiadas) para actualizar su respectiva información de posición. Con el uso de una jerarquía de agentes foráneos, un nodo móvil puede registrarse localmente dentro de un dominio foráneo. Esto reduce el número de mensajes de señalización que tienen que ser enviados a la red de casa del nodo y también mejora el desempeño de traspasos, ya que minimiza el retardo transcurrido en el proceso de registro cuando la red foránea está muy lejos de la red de casa [Campbell, Gomez, Kim, 2002], [Ilyas, 2003].

Cuando un nodo se mueve dentro del mismo dominio IP, el cambio de FA debe ser notificado al GFA. Entonces se inicia un proceso de *registro regional*, el nodo móvil envía

un mensaje de *petición de registro regional* al GFA por medio del FA y cuando el GFA lo recibe, este envía un mensaje de *respuesta de registro regional* hacia el nodo móvil.

Cuando un nodo móvil llega a un dominio foráneo, se registra con su red de casa. En este proceso, el HA registra la dirección del GFA como su CoA, entonces, cuando el nodo móvil se mueve entre FAs bajo el mismo GFA, la CoA se mantiene igual y el HA no necesita estar informado de los movimientos de los nodos dentro del dominio foráneo. El GFA mantiene una lista de todos los nodos móviles que actualmente están registrados con él [Tewari, *et al*., 2003]. El tráfico destinado hacia el nodo móvil es interceptado por el HA y enviado al GFA. El GFA desencapsula el paquete, lee la dirección destino y lo busca en su lista de nodos. Si la entrada existe, reencapsula el paquete y lo envía al FA del siguiente nivel hasta que el nodo móvil reciba el paquete.

III.3.2.2 IPv6 Móvil Jerárquico

HMIPv6 sigue el mismo principio de HMIPV4, pero introduce un agente de movilidad local llamado "Punto de Anclaje de Movilidad" (MAP – *Mobility Anchor Point*). El MAP difunde avisos de enrutador en toda la red hasta que llegan a los enrutadores de acceso y cuando un nodo móvil entra a un dominio MAP, recibe estos avisos. El nodo móvil registra una dirección que pertenece al prefijo MAP (llamada CoA regional (RCoA) y obtiene una segunda COA, denominada LCOA, para definir su nuevo enrutador de acceso. Además, el nodo móvil envía mensajes al MAP para informarle de traspasos entre enrutadores de acceso. Por otra parte, el MAP actúa como un agente de casa local, y recibe todos los

paquetes en representación del nodo, los encapsula y los envía directamente hacia la dirección actual del nodo móvil. Si el nodo cambia su dirección actual dentro de un dominio local MAP, sólo necesita registrar la nueva dirección con el MAP. Así, sólo el RCoA necesita estar registrado con los nodos correspondientes y el agente de casa. El RCoA no cambia si el nodo móvil se mueve dentro del mismo dominio MAP. Esto hace que la movilidad del nodo móvil sea transparente al nodo correspondiente con el que se está comunicando [Pack y Choi, 2004]. En la figura 18 se muestra una red de acceso de *IP móvil jerárquico*.

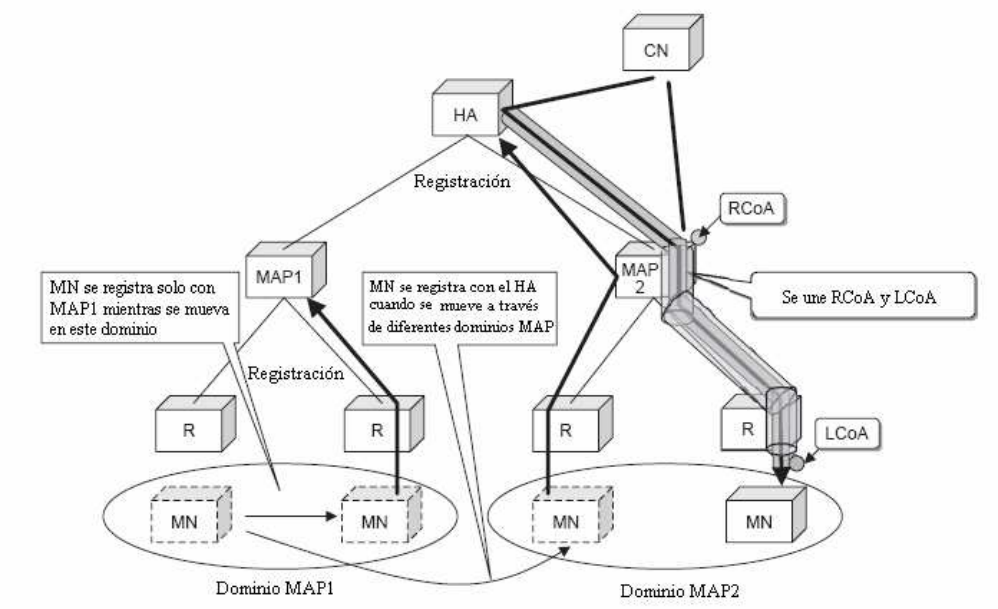


Figura 18. IP Móvil Jerárquico

Las extensiones de voceo para IP Móvil jerárquico son definidas en Haverinen y Malinen, [2000] permitiendo que los nodos móviles inactivos operen en modo de salvar potencia mientras estén dentro de un área de voceo. La posición de nodos móviles es conocida por

los HA y es representada por áreas de voceo. Después de recibir un paquete destinado hacia un nodo móvil inactivo localizado en una red foránea, el HA envía el paquete hacia el FA, el cual entonces vocea al nodo móvil para reestablecer una ruta hacia el punto actual de unión [Campbell, et al., 2002].

III.4 HAWAII (Handoff-Aware Wireless Access Internet Infrastructure)

HAWAII es un protocolo de micromovilidad propuesto por la IETF (Internet Engineering Task Force) y por investigadores de los laboratorios Lucent Bell para mejorar la calidad de servicio y reducir la ineficiencia de MIP [Ilyas, 2003]. HAWAII utiliza IP Móvil tradicional; esta combinación de usar el protocolo HAWAII para micromovilidad dentro de un dominio e IP Móvil para macromovilidad entre dominios, provee movilidad transparente y escalable en todos los niveles [Ramjee, *et al*., 1999].

Los objetivos de diseño de HAWAII son:

1. Escalabilidad
2. Enrutamiento eficiente
3. Interrupción limitada para tráfico de usuario
4. Soporte de QoS
5. Confiabilidad

Esencialmente, HAWAII realiza estos objetivos suponiendo que la mayoría de la movilidad está dentro de un sólo dominio administrativo. Un enfoque común para proveer movilidad transparente hacia nodos correspondientes es dividir la red dentro de jerarquías. HAWAII usa una estrategia similar, separando la red dentro de jerarquías de dominios, como en la jerarquía de sistema autónomo de Internet, además propone usar identificadores de acceso de red (NAI) para identificar a los diferentes dominios HAWAII.

Un *dominio* HAWAII comprende varios enrutadores de acceso corriendo el protocolo HAWAII, así como de nodos móviles. Cada dominio tiene su propio gateway llamado *enrutador raíz de dominio* (DRR *domain root router*), el cual toma el papel de HA. Cada nodo tiene una dirección IP y un dominio casa, esta dirección se mantiene mientras el nodo se mueva dentro de su dominio casa. Además, el agente de casa y cualquier nodo correspondiente ignoran la movilidad del nodo dentro de ese dominio [Ramjee, *et al*., 1999]. La arquitectura de una red HAWAII se ilustra en la figura 19.

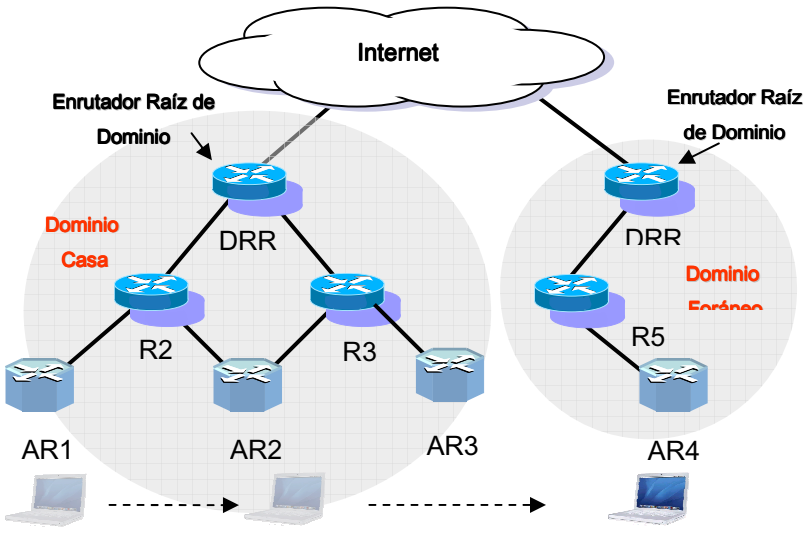


Figura 19. Arquitectura de red HAWAII

En la arquitectura tradicional de IP Móvil, no hay noción de un dominio y el nodo móvil está directamente unido a cualquier enrutador raíz dominio casa (llamado agente de casa) o al enrutador raíz de dominio foráneo (llamado agente foráneo). Entonces, cada traspaso causa un cambio de dirección IP para el nodo móvil, resultando en dificultad en el soporte de escalabilidad, eficiencia y QoS [Ramjee, *et al*., 1999].

III.4.1 Procesamiento de los enrutadores de acceso

Los enrutadores de acceso de la red HAWAII tienen que implementar la funcionalidad de FA (sin la función de desencapsulación), originar *mensajes HAWAII* para procesarse dentro del dominio, enviar *avisos de agentes* periódicamente y responder a los *mensajes de solicitud de agente* enviados por los nodos. Los *mensajes de aviso de agente* deben incluir la extensión de agente foráneo (foreign-agent-challenge) y el NAI del dominio administrativo al cual pertenece el enrutador de acceso.

Cuando se recibe una *petición de registro*, el enrutador de acceso debe revisar si el NAI del nodo móvil presente en la petición corresponde al NAI del dominio al cual pertenece. Si los dos corresponden, el enrutador de acceso debe rechazar cualquier petición que esté registrando al nodo móvil con un CoA colocado. Si el registro es válido, el enrutador de acceso genera *mensajes HAWAII de actualización de traspaso* (handoff update) o *power up* basado si el campo PFANE (Previous Foreign Agent Notification Extension - *Extensión de Notificación de Agente Foráneo Anterior*) está presente o no [Ramjee, *et al*., 2000].

III.4.2 Procesamiento del nodo móvil

El nodo móvil en el dominio HAWAII intercambia sólo mensajes de control MIP con la red, mientras que el enrutamiento dentro del dominio HAWAII es realizado con *mensajes HAWAII* basados en UDP (User Datagram Protocol). Los *mensajes HAWAII* nunca se envían fuera del dominio, ni hacia el nodo móvil. El objetivo es que la operación de HAWAII sea oculta para el nodo móvil [Wisely, *et al*., 2002]. Los paquetes destinados hacia el nodo móvil serán enviados hacia el DRR casa usando la dirección de subred del dominio y entonces serán enviados hacia el nodo móvil usando rutas establecidas dinámicamente [Ilyas, 2003].

Cuando un nodo móvil se mueve hacia un dominio foráneo, se usan los procedimientos usuales de MIP y el protocolo HAWAII compara el NAI avisado por el enrutador de acceso con el NAI del nodo móvil para distinguir si un nodo móvil está en su dominio casa HAWAII o en un dominio foráneo HAWAII. Si el nodo está en un dominio foráneo, el enrutador raíz de ese dominio es el FA, es responsable de asignar un CoA y de enviar paquetes hacia el nodo móvil. Mientras el nodo móvil se esté moviendo dentro del dominio foráneo, mantiene su CoA sin cambiarla, entonces, el HA no necesita estar involucrado a menos que el nodo móvil se mueva hacia un nuevo dominio [Campbell, *et al*., 2002].

Por otro lado, cuando el nodo móvil detecta un cambio de enrutador de acceso debe enviar una petición de registro MIP hacia el nuevo enrutador de acceso. El protocolo usa estos

mensajes de registro MIP para activar esquemas de establecimiento de ruta dentro del dominio HAWAII y de esta manera crear rutas hacia el nodo móvil [Ramjee, *et al*., 1999].

El protocolo contiene dos tipos de mensajes para establecer rutas:

a) Mensajes HAWAII Update

b) Mensajes HAWAII Refresh

III.4.3 Establecimiento de ruta del proceso Power Up

En la figura 20 se ilustra la secuencia de los *mensajes HAWAII update* de establecimiento de ruta durante el proceso *power up*. Cuando un nodo móvil se une por primera vez a un dominio se realiza un procedimiento llamado *power up*, en donde el nodo móvil envía una *petición de registro MIP* al enrutador de acceso más cercano (mensaje 1). Cuando el enrutador de acceso recibe el mensaje de petición de registro MIP, este envía un mensaje HAWAII *update* de establecimiento de ruta al enrutador que está al siguiente salto, para establecer y actualizar entradas de enrutamiento (mensaje 2), además, añade una entrada de envío para la dirección IP del nodo móvil con la interfaz de salida colocada con la interfaz que recibió el mensaje (la interfaz inalámbrica en este caso). Entonces, cada enrutador que está en la ruta entre el enrutador de acceso y el DRR añade una entrada de envío para este nodo en particular (mensaje 3). Finalmente, el DRR responde enviando un *mensaje HAWAII update acknowledgement* (mensaje de reconocimiento) al enrutador de acceso

(mensaje 4), el cual envía un *mensaje de respuesta de registro MIP* hacia el nodo móvil (mensaje 5).

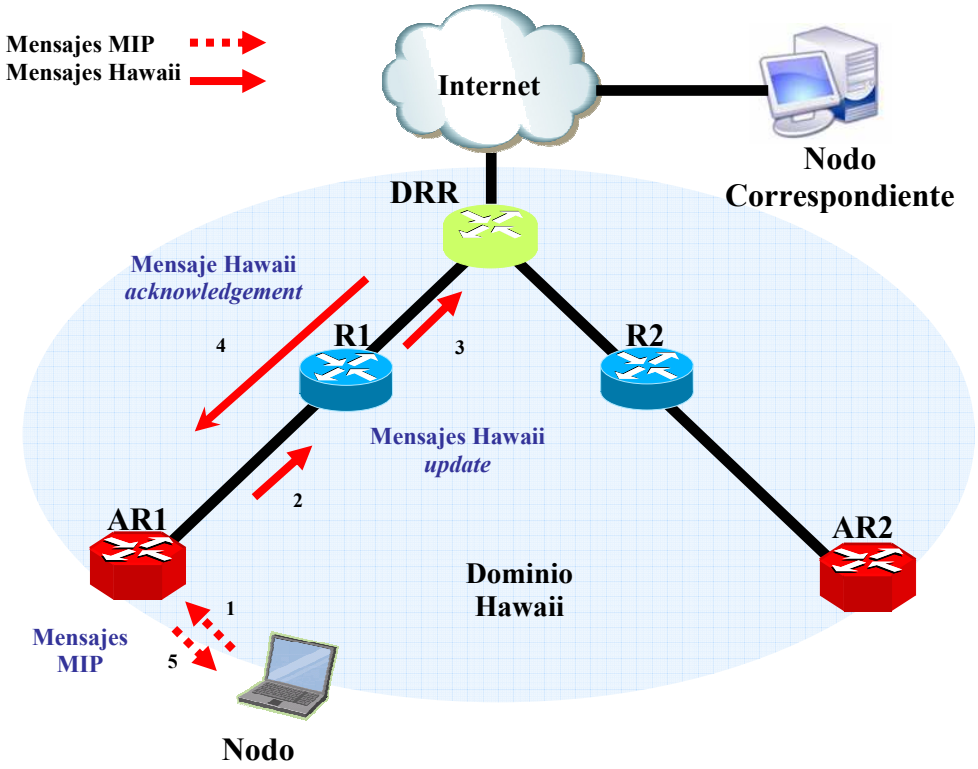


Figura 20. Proceso Power Up.

Este procedimiento crea una ruta de estado suave, la cual provee al nodo móvil conectividad hacia Internet a través del DRR. Una ruta de estado suave significa que es válida durante un período de tiempo mientras los enrutadores de acceso envíen regularmente *mensajes HAWAII refresh* hacia los enrutadores superiores, estos mensajes actualizan los temporizadores asociados con la ruta de ese nodo móvil en particular. De otra manera, la ruta se borrará automáticamente cuando un temporizador asociado con ese enrutador expire. Una ruta de estado suave dentro de los enrutadores incrementa la robustez

del protocolo bajo condiciones de fallas del enrutador o fallas de enlace [Ramjee, *et al*., 2000].

III.4.4 Esquemas de Establecimiento de ruta HAWAII

Hawaii define cuatro alternativas de esquemas de establecimiento de rutas que controlan el traspaso entre enrutadores de acceso y pueden ser clasificados dentro de dos tipos: esquemas de envío (*Forwarding)* y esquemas de no envío (*Non-Forwarding*), basado en la forma en la que los paquetes son enviados al nodo móvil durante un traspaso.

El esquema de establecimiento de ruta apropiado es seleccionado dependiendo de las prioridades del operador entre eliminar pérdida de paquetes, minimizar la latencia de traspaso y mantener el orden de los paquetes [Campbell, Gomez, Kim, 2002].

III.4.4.1 Esquemas de Envío

Los esquemas de envío están diseñados para redes donde los nodos móviles son capaces de escuchar/ transmitir datos de un sólo enrutador de acceso, como en el caso de una red TDMA (Acceso múltiple por división de tiempo) [Ramjee, *et al*., 2000]. En este tipo de esquemas, la idea es enviar todos los paquetes de datos del enrutador de acceso anterior al nuevo enrutador de acceso antes de que se desvíen en el enrutador de cruce, después de que un traspaso ha ocurrido. Un *enrutador de cruce* es el enrutador que está en la intersección de dos rutas, una entre el DRR y el enrutador de acceso anterior, y la segunda entre el DRR

y el nuevo enrutador de acceso. Este envío es necesario sólo hasta que los paquetes de datos cesen de llegar del enrutador de acceso anterior debido a las tablas de enrutamiento actualizadas en enrutadores de niveles más altos, además estos esquemas son independientes del enlace inalámbrico y se basan en la red cableada para almacenar paquetes y enviarlos al nuevo enrutador de acceso de forma transparente [Ramjee, *et al*., 1999].

Existen dos variantes de esquemas de envío, una que trabaja con tablas de enrutamiento IP estándar para actualizar las entradas basadas en nodos, y otro esquema en el cual se extienden las tablas de enrutamiento IP para acomodar la información basada en interfases. Estos esquemas se llaman *Multiple Stream Forwarding* (MSF) y *Single Stream Forwarding* (SSF). En las figuras 21 y 22 se presentan los *esquemas de envío MSF y SSF*. Las flechas denotan la propagación de los mensajes entre los nodos, y las entradas de envío se muestran a un lado de los enrutadores. El número en el paréntesis a un lado de cada entrada indica el número del mensaje, el cual establece que mensaje fue responsable de establecer la entrada en particular (un mensaje con número cero indica una entrada preexistente). Las letras denotan las diferentes interfases.

a) Multiple Stream Forwarding (MSF)

El procedimiento de establecimiento de ruta es iniciado por el nodo móvil, cuando se mueve de un enrutador de acceso a otro. El nodo móvil envía un *mensaje de registro MIP* (mensaje 1) con la dirección del enrutador de acceso anterior como parte de la *Extensión de*

Notificación de Agente Foráneo Anterior (PFANE - Previous Foreign Agent Notification Extension) hacia el nuevo AR. Entonces, el nuevo enrutador de acceso envía un *mensaje HAWAII update* de establecimiento de ruta (mensaje 2) hacia el enrutador de acceso anterior (este mensaje contiene la dirección del nuevo enrutador de acceso). El enrutador de acceso anterior busca en su tabla de enrutamiento al nuevo enrutador de acceso y añade una entrada de envío para el nodo móvil en su tabla de enrutamiento con la dirección IP, la interfaz por donde sale el paquete (interfaz A) y el enrutador que está al siguiente salto (enrutador R1). Después, el enrutador de acceso anterior envía el *mensaje HAWAII update* de establecimiento de ruta (mensaje 3) al siguiente enrutador (enrutador 1). El enrutador 1 realiza acciones similares y envía el mensaje al enrutador 0 (mensaje 4). El enrutador 0, el enrutador de cruce en este caso, añade una entrada de envío para que los nuevos paquetes se desvíen hacia el nodo móvil en el nuevo enrutador de acceso. Salto a salto el mensaje es enviado hacia el nuevo enrutador de acceso, y cada enrutador a lo largo de la ruta modifica su tabla de enrutamiento para tener una entrada actualizada para el nodo móvil (mensaje 5,6). Eventualmente el mensaje 6 alcanza al nuevo enrutador de acceso. Finalmente, el nuevo enrutador de acceso cambia su entrada de envío y envía un *mensaje de respuesta de registro MIP* hacia el nodo móvil para completar el procedimiento de traspaso (mensaje 7). El principal beneficio de este sistema es que es simple y no hay pérdida de paquetes.

Note que sólo los enrutadores de acceso (anterior y nuevo), y los enrutadores conectados a ellos, están involucrados en el proceso de *mensajes HAWAII update* de establecimiento de ruta. También, sólo los enrutadores en la ruta entre el nuevo enrutador de acceso y el DRR recibirán los *mensajes HAWAII refresh* periódicamente. Así que, las entradas en el

enrutador 1 y el enrutador de acceso, las cuales no pertenecen a esta ruta, expirarán, mientras que las entradas en los enrutadores 0 y 2, y el nuevo enrutador de acceso serán actualizadas.

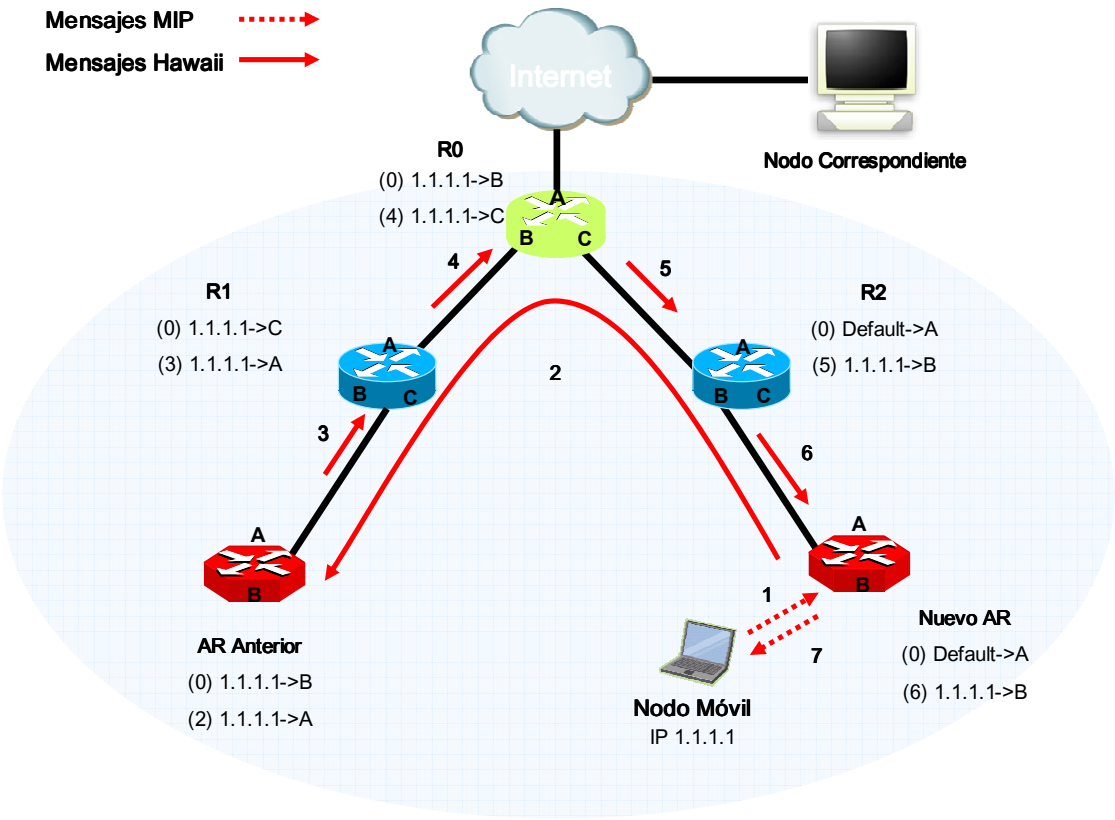


Figura 21. Esquema de Envío MSF.

Los ARs en este esquema de envío usan un *buffer de envío* por cada nodo para almacenar los paquetes enviados en el *proceso de traspaso*. Todos los paquetes destinados hacia el nodo móvil son almacenados en el buffer (aún después de ser transmitidos hacia el nodo móvil). Esto permite que los paquetes sean enviados al nodo móvil y no se pierdan porque el nodo móvil se mueva fuera del área de cobertura, de esta forma los paquetes tendrán la oportunidad de alcanzar al nodo móvil cuando se envíen al nuevo AR. Además, el buffer de

envío tiene un mecanismo de expiración que mantiene a los paquetes por un período de tiempo limitado [Vena, *et al*., 2002].

b) *Single Stream Forwarding* (SSF)

El esquema *Single Stream Forwarding* (SSF) actualiza las entradas de envío utilizando un método similar al que se usa en el esquema de *Optimización de Ruta de IP móvil*, en el cual, los paquetes son enviados del enrutador de acceso anterior al nuevo enrutador de acceso en un sólo flujo. Para lograr esto sin usar *tunelaje*, se utiliza una técnica que se llama *envío basado en interfaz*. Esto requiere entradas de tablas de enrutamiento más descriptivas. Una tabla de enrutamiento típicamente tiene una entrada de la forma (Dirección IP -> Interfaz de salida). En este esquema, el enrutador debe ser capaz de enviar los mensajes basándose en un campo adicional, la interfaz por donde llega el paquete. La entrada de enrutamiento resultante, es de la forma (Interfaz por donde llega el paquete, dirección IP -> Interfaz por donde sale el paquete). En la figura 22, los mensajes del 1-5 establecen estas entradas dando como resultado paquetes que llegan al enrutador de acceso anterior y empiezan a desviarse al nuevo enrutador de acceso en un sólo flujo. El enrutador de acceso anterior envía el mensaje 6 al enrutador 0 para desviar el flujo en el enrutador de cruce. Después de procesar el mensaje 6, el enrutador 0 envía un *mensaje HAWAII update acknowledgement* de establecimiento de ruta para desviar los nuevos paquetes de datos directamente hacia el nuevo enrutador de acceso (mensaje 7). Por último, el nuevo enrutador de acceso envía una *respuesta de registro MIP* hacia el nodo móvil (mensaje 8). Este esquema tiene menos pérdida de paquetes, mantiene un sólo flujo de envío de paquetes

hasta que la desviación es realizada en el enrutador de cruce (hasta el mensaje 6) y es más complejo de implementar.

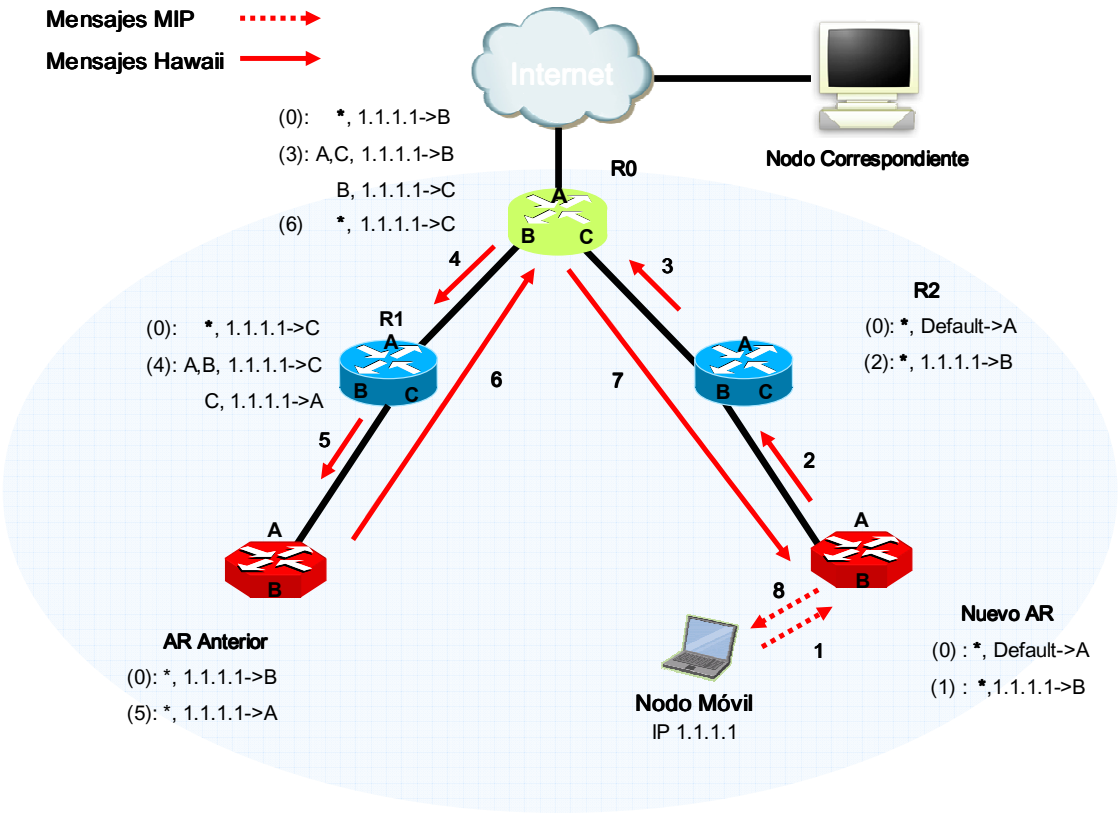


Figura 22. Esquema de Envío SSF.

III.4.4.2 Esquemas de No envío

En una red donde los nodos móviles pueden al menos temporalmente recibir datos de dos enrutadores de acceso simultáneamente, el esquema de envío no es una solución óptima. En su lugar, el flujo de datos puede ser redireccionado en el enrutador de cruce antes de que la información sobre un traspaso alcance al enrutador de acceso anterior.

Los esquemas de no envío se usan para redes con nodos móviles capaces de escuchar / transmitir a dos o más enrutadores de acceso simultáneamente por corto tiempo, como en el caso de una red CDMA (Acceso múltiple por división de código) o WaveLAN [Ramjee, *et al*., 2000]. En estos esquemas de establecimiento de ruta, conforme el *mensaje HAWAII update* de establecimiento de ruta viaja del nuevo enrutador de acceso hacia el enrutador de acceso anterior, los paquetes de datos son desviados en el enrutador de cruce hacia el nuevo enrutador de acceso, dando como resultado un no envío de paquetes hacia el enrutador de acceso anterior, además toman ventaja de las propiedades de ciertos enlaces inalámbricos donde ambos enrutadores de acceso (anterior y nuevo) pueden mantener conectividad con el nodo móvil para un envío transparente durante un traspaso [Ramjee, *et al*., 1999].

Hay dos variantes del esquema de No envío, el esquema *Unicast Non-Forwarding* (UNF) y el esquema *Multicast Non-Forwarding* (MNF).

En la figura 23 se muestra el esquema UNF, después de que un nuevo enrutador de acceso recibe un *mensaje de registro MIP* del nodo móvil (mensaje 1), con el campo PFANE, este añade una entrada de envío para la dirección IP del nodo móvil con la interfaz de salida colocada con la interfaz que recibió este mensaje, busca en su tabla de enrutamiento al enrutador de acceso anterior (identificado usando el campo PFANE en el *mensaje de registro MIP*) y determina al enrutador que está al siguiente salto, enrutador 2. El nuevo enrutador de acceso entonces envía un *mensaje HAWAII update* de establecimiento de ruta hacia el enrutador 2 (mensaje 2). Este enrutador realiza acciones similares y envía el mensaje hacia el enrutador 0 (mensaje 3). En el enrutador 0, el enrutador de cruce en este

caso, las entradas de envío son añadidas para que los nuevos paquetes sean desviados directamente hacia el nodo móvil en el nuevo enrutador de acceso, es decir, el flujo de datos hacia el nodo móvil es redireccionado hacia el nuevo enrutador de acceso tan pronto como el mensaje de establecimiento de ruta alcance al enrutador de cruce. Eventualmente el mensaje alcanza al enrutador de acceso anterior (mensaje 5). El enrutador de acceso anterior cambia su entrada de envío y envía un *mensaje HAWAII update acknowledgement* de establecimiento de ruta de regreso al nuevo enrutador de acceso (mensaje 6), el cual entonces envía una *respuesta de registro MIP* hacia el nodo móvil (mensaje 7).

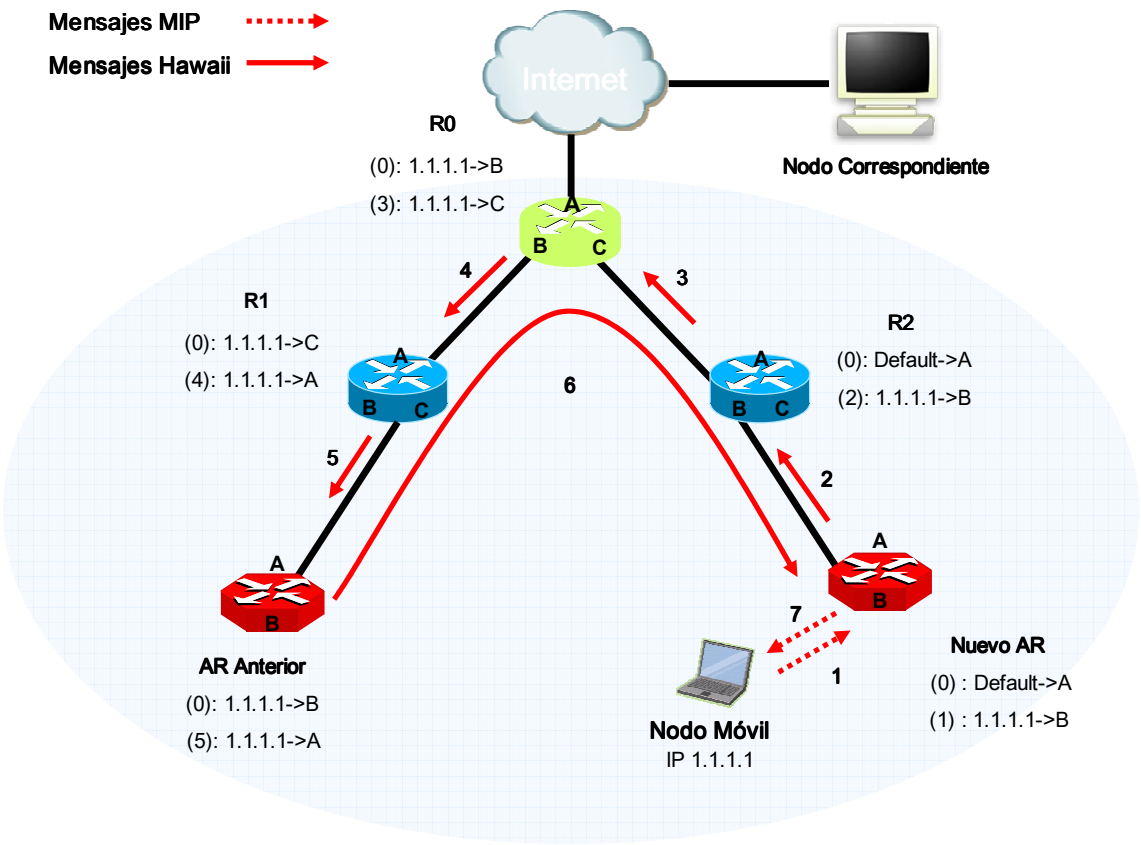


Figura 23. Esquema de No envío UNF.

El esquema MNF es muy similar al esquema UNF. La principal diferencia es que el enrutador de cruce, el enrutador 0, envía los paquetes de datos durante un periodo de tiempo muy corto. En la figura 24 se muestra el esquema MNF, el enrutador 0 envía los paquetes de datos de la interfaz A hacia ambos enrutadores de acceso (anterior y nuevo) después de recibir el mensaje 3, hasta que reciba el mensaje 6. Esto ayuda a disminuir la pérdida de paquetes en las redes donde el nodo móvil puede escuchar sólo a un enrutador de acceso [Ramjee, *et al*., 1999].

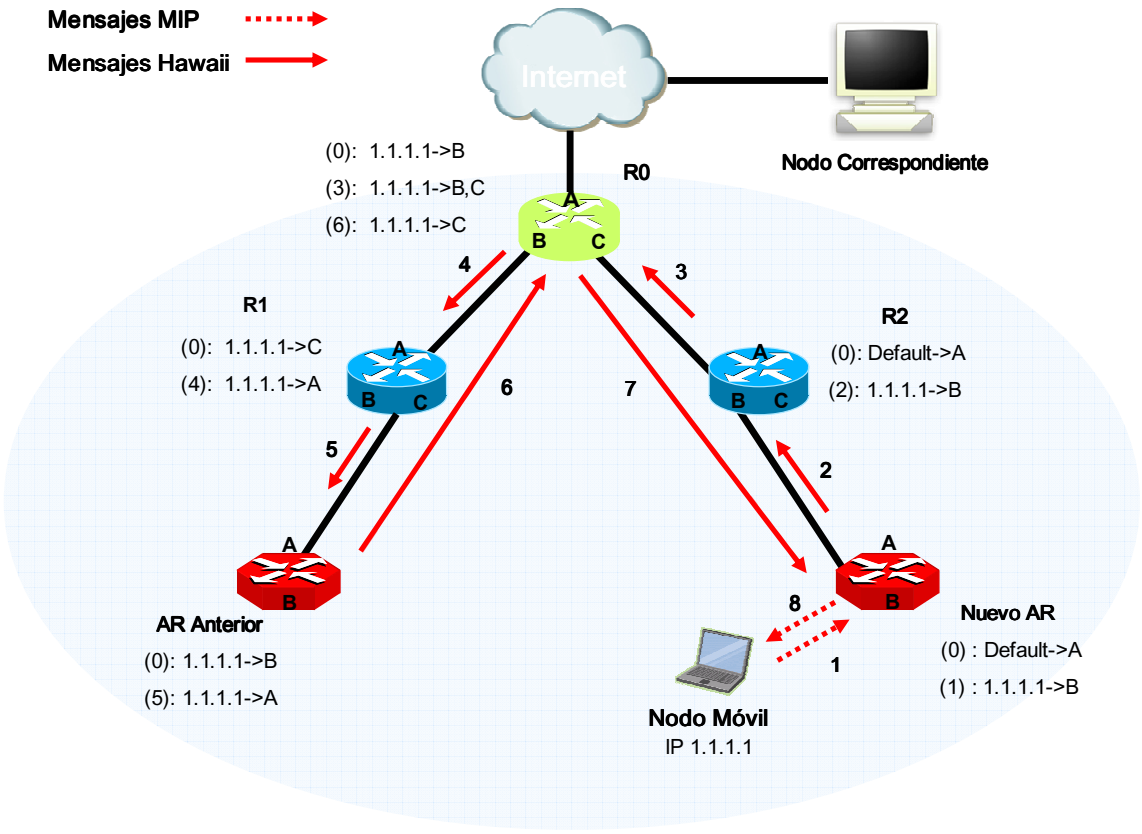


Figura 24. Esquema de No envío MNF.

Note que otros enrutadores en el dominio no tienen un conocimiento específico de estas direcciones IP del nodo móvil.

III.4.5 Formato de los mensajes

a) Mensaje HAWAII update

El formato de los mensajes HAWAII *update* de establecimiento de ruta enviado por los enrutadores de acceso y los enrutadores superiores dentro de un dominio es el siguiente:

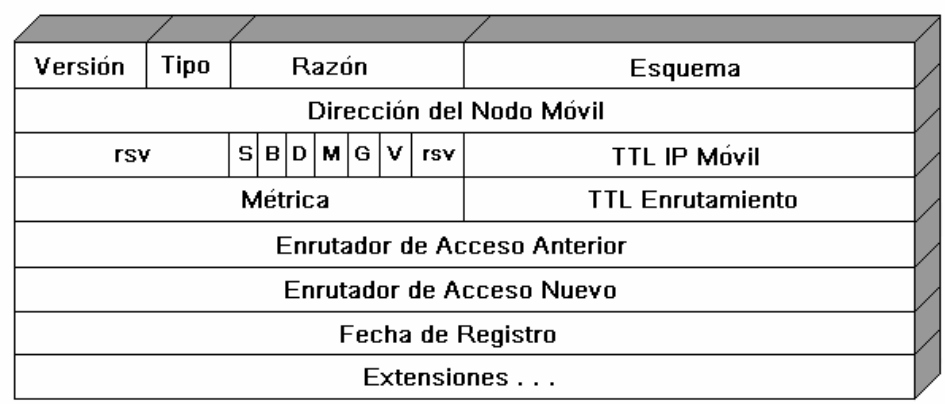


Figura 25. Mensaje HAWAII Update.

El mensaje es enviado usando el protocolo UDP hacia un puerto reservado. Cuando el campo tipo del *mensaje HAWAII update* indica que es un *mensaje power up* (tipo 1), el mensaje es enviado hacia el enrutador de acceso actual. Si el campo tipo del mensaje indica que es un *mensaje handoff* (tipo 2), el mensaje es enviado hacia el enrutador de acceso anterior en el caso de *esquemas de envío*, y hacia el nuevo enrutador de acceso en caso de *esquemas de no envío*.

Versión (4 bits) Este campo especifica la versión que se está utilizando.

Tipo (4 bits) Este campo indica el tipo de mensaje de control que se envía.

1 Mensaje *power up update.*

2 Mensaje de actualización de traspaso (*handoff update*).

3 Mensaje de reconocimiento (*acknowledgement*).

Razón (8 bits) Este campo indica la razón del por qué se envía un mensaje de reconocimiento (*acknowledgement*) y sólo lo utilizan los mensajes tipo 3.

0 Mensaje aceptado

1 Mensaje formateado pobremente

2 Falla de autentificación

3 Esquema no soportado

4 Recurso no disponible.

Esquema (16 bits). Este campo define el tipo de esquema de establecimiento de ruta utilizado.

1 Esquema de Envío (*Forwarding*)

2 Esquema de No envío (*Non-Forwarding*).

Dirección de nodo móvil (32 bits). Este campo indica la dirección de casa en el dominio casa y el CoA en el dominio foráneo.

rsv (8 bits). Este campo se reserva para uso futuro y es enviado con un valor de 0.

S, B, D, M, G, V (1 bit c/u). Estos campos especifican banderas de registro IP móvil.

Tiempo de vida de IP móvil (16 bits). Este campo indica el tiempo de vida en el registro IP Móvil.

Métrica (16 bits). Este campo indica la distancia hacia el nodo móvil en saltos.

Tiempo de vida de enrutamiento (16 bits). Este campo especifica el valor del temporizador de estado suave.

Enrutador de Acceso Anterior (32 bits). Este campo contiene la dirección IP del enrutador de acceso anterior cuando se usa un mensaje tipo 2 (*handoff update)* y la dirección IP 0.0.0.0 cuando se usa un mensaje tipo 1 (*power up update*).

Nuevo Enrutador de Acceso (32 bits). Este campo contiene la dirección IP del nuevo enrutador de acceso cuando se usa un mensaje tipo 2 (*handoff update)* y la dirección IP del enrutador de acceso actual cuando se usa un mensaje tipo 1 (*power up update*).

Fecha de Registro (Timestamp) (32 bits). Este campo define la hora y la fecha que fue enviado el mensaje. El formato del campo es el que se usa en el Protocolo de Tiempo de

Red (Network Time Protocol), el cual, es un protocolo que sirve para sincronizar los relojes de los nodos y los enrutadores en Internet.

Extensiones (variable). Es un campo de autentificación.

b) Mensaje Hawaii Refresh

El formato de un mensaje *refresh* se muestra a continuación. El mensaje puede contener múltiples entradas cuando es enviado por los enrutadores de acceso hacia enrutadores superiores. Sin embargo, el tamaño del mensaje no debe exceder 4 KB.

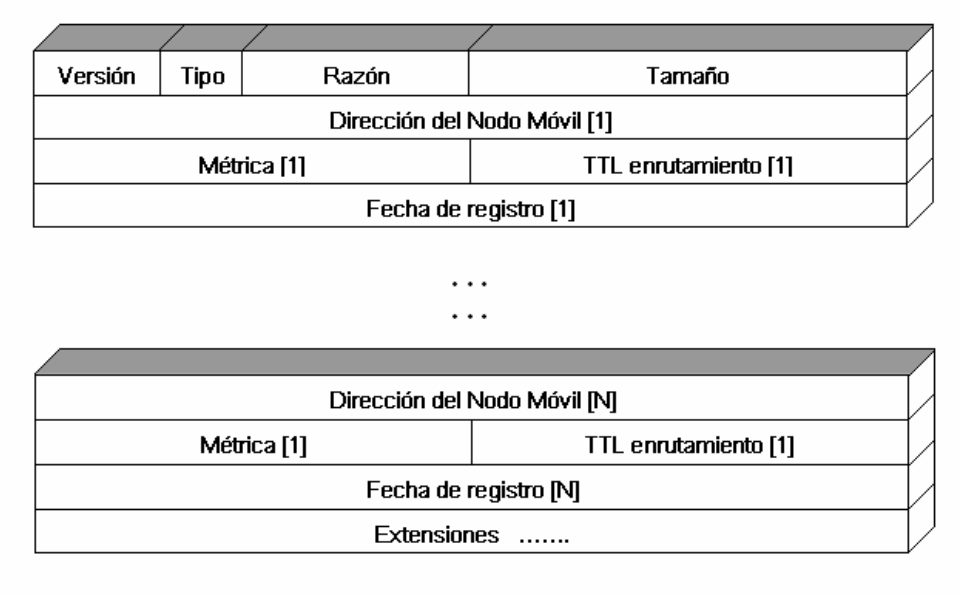


Figura 26. Mensaje HAWAII Refresh.

Versión (4 bits). Este campo especifica la versión que se está utilizando.

Tipo **(**4 bits). Este campo indica el tipo de mensaje de control que se envía.

4 Indica un mensaje tipo *Refresh*

Razón (8 bits). Este campo indica la razón del por qué se envía un mensaje tipo *refresh*.

0 Normal

1 Activado debido a falla de enlace/nodo.

Tamaño (16 bits). Este campo indica el número de entradas del nodo móvil.

Dirección del nodo móvil (32 bits). Este campo especifica la dirección de entrada del nodo móvil.

Métrica (16 bits). Este campo indica la distancia hacia el nodo móvil en saltos.

Tiempo de vida de enrutamiento (16 bits). Este campo contiene el valor del temporizador de estado suave.

Fecha de Registro (Timestamp) (32 bits). Este campo indica la fecha y hora de la entrada del nodo.

Extensiones (variable)**.** Es un campo de autentificación.

El formato para los mensajes enviados entre los nodos móviles y los enrutadores de acceso sigue el estándar IP Móvil y se muestra en las figuras 27 y 28.

a) *Mensaje de Petición de Registro IP Móvil*

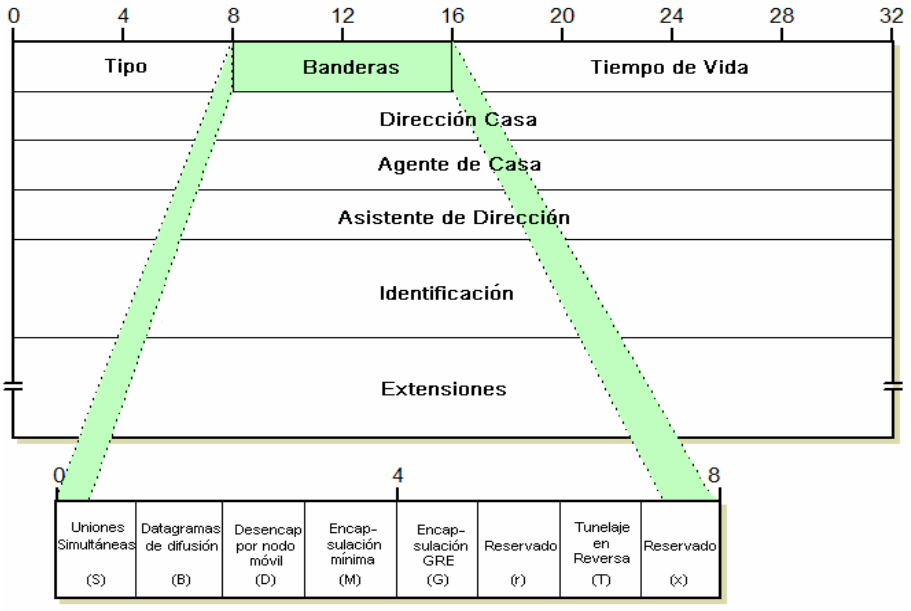


Figura 27. Mensaje de Petición de Registro IP Móvil

Tipo *(8 bits)*. Identifica el tipo de mensaje, para un mensaje de petición, este campo se coloca a 1.

Banderas *(1 bit c/u*). Contiene varias banderas de información de peticiones hechas por el nodo móvil al HA.

Tiempo de Vida *(16 bits)*. Tiempo de vida en segundos, que el nodo móvil pide al agente de casa para registrarse.

Dirección Casa *(32 bits)*. La dirección IP del nodo móvil cuando está en su red casa.

Agente de Casa *(32 bits).* La dirección IP del agente de casa del nodo móvil.

Asistente de dirección (CoA) (*32 bits*). La dirección IP que está siendo usada por el nodo móvil como su CoA.

Identificación *(32 bits).* Este campo identifica la petición de registro y es usada para relacionar las peticiones con las respuestas, también provee protección contra posibles ataques.

Extensiones (Variable) En estos campos se incluye información de autentificación de la petición.

b) *Mensaje de Respuesta de registro IP Móvil*

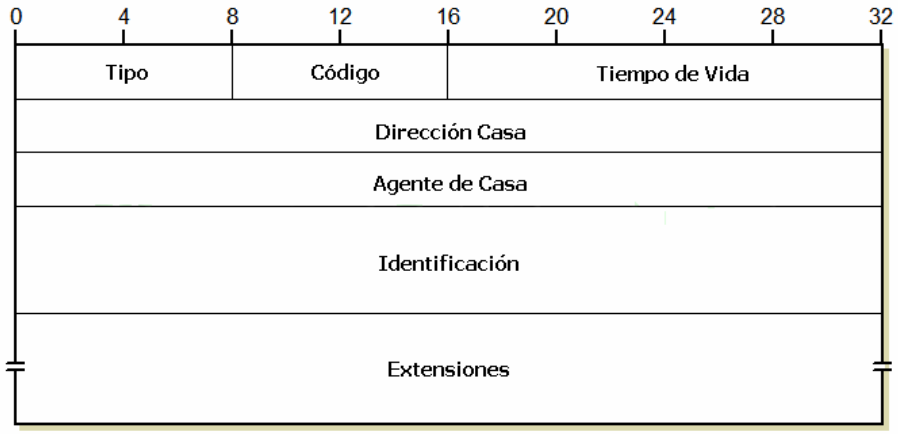


Figura 28. Mensaje de Respuesta de registro IP Móvil.

Tipo *(8 bits).* Identifica el tipo de mensaje de registro. Para una respuesta, el campo se coloca a 3.

Código *(8 bits).* Indica el resultado de la petición de registro. Este campo es colocado a 0 si la petición de registro fue aceptada. Si la petición fue negada, un código de razón diferente es proveído para indicar la razón de la negación.

Tiempo de Vida *(16 bits).* Si la petición de registro fue aceptada, indica el tiempo en segundos hasta que la petición de registro expira.

Dirección de Casa *(32 bits).* La dirección IP del nodo móvil cuando está en su red de casa.

Agente de Casa *(32 bits).* La dirección IP del agente foráneo del nodo móvil.

Identificación *(32 bits)*. Este campo identifica la respuesta de registro y es relacionada con el campo de identificación de la petición.

Extensiones (Variable). Estos campos son incluidos para autentificación de la respuesta.

III.4.6 Voceo (Paging)

La sobrecarga de señalización y consumo de potencia del nodo móvil puede ser disminuido a través de la introducción del *proceso de voceo*. HAWAII también soporta voceo y es capaz de distinguir nodos móviles activos o inactivos. Similarmente a IP Celular, un nodo móvil inactivo envía *peticiones de voceo* periódicamente, los cuales actualizan las entradas de voceo de los enrutadores. Un dominio HAWAII comprende de una o más *áreas de voceo*, las cuales están definidas como conjuntos de enrutadores de acceso. Cada área de voceo tiene asignada una dirección de grupo multicast y todos los enrutadores de acceso que pertenecen a la misma área de voceo forman un grupo multicast [Vena, *et al*., 2002]. HAWAII usa IP Multicast para vocear a los nodos móviles cuando llegan paquetes a la red de acceso y no hay información de enrutamiento disponible. Dependiendo de la forma como está organizada el área de voceo, los paquetes son almacenados en los enrutadores de acceso o en los enrutadores superiores. El nodo inicia una petición de voceo, la cual es enviada al nodo móvil que está en algún lugar del área de voceo. Después de recibir la petición de voceo, el nodo móvil se activa y envía al enrutador de acceso una *respuesta de voceo*, la cual establece una entrada de enrutamiento válida. Después que la respuesta de voceo ha alcanzado al nodo que inició la petición de voceo, los datos almacenados pueden ser enviados al nodo móvil [Typpö, 2001].

Capítulo IV.

MECANISMO DE ENRUTAMIENTO PARA REDES HÍBRIDAS

IV.1 Introducción

El mecanismo de enrutamiento propuesto integra la funcionalidad del protocolo de enrutamiento AODV con la del protocolo de micromovilidad HAWAII. Uno de los objetivos principales del mecanismo propuesto es elegir la mejor ruta para enviar los datos, ya sea por la parte cableada o por la parte inalámbrica y lograr que los nodos móviles se asocien al enrutador de acceso más cercano. El proceso de selección de un enrutador de acceso se puede realizar en base a dos métricas: midiendo la distancia en metros o en número de saltos, dependiendo de la elección del usuario.

El mecanismo propuesto utiliza el protocolo de enrutamiento AODV para encontrar una ruta hacia el destino, cuando dos nodos se quieren comunicar dentro de la red ad hoc, y utiliza el protocolo de micromovilidad HAWAII para controlar los traspasos que realiza un nodo cuando se cambia de un enrutador de acceso a otro, de esta forma es posible proporcionar conectividad hacia Internet a los nodos móviles.

Para describir el principio de operación del mecanismo propuesto, primero se explica la integración del protocolo de enrutamiento AODV con el protocolo de micromovilidad

HAWAII, después como funciona el mecanismo en la parte de IP Móvil y por último como funciona en la parte de AODV.

IV.2 Integración del protocolo de micromovilidad HAWAII y el protocolo de enrutamiento AODV

Debido a que el protocolo de enrutamiento AODV no funciona para redes híbridas, ya que éste fue diseñado para redes inalámbricas ad hoc, se tuvieron que hacer algunas modificaciones en la implementación de AODV para integrar el protocolo de micromovilidad HAWAII y el protocolo de enrutamiento AODV y de esta manera simular el mecanismo propuesto.

En este mecanismo, los enrutadores de acceso tienen implementado el protocolo de micromovilidad HAWAII y el protocolo de enrutamiento AODV, también conocen la existencia de los demás enrutadores de acceso que están presentes en la red híbrida y del enrutador de dominio.

Por su parte, los nodos móviles utilizan el protocolo de enrutamiento AODV, intercambian mensajes de IP Móvil con los enrutadores de acceso, pero nunca mensajes HAWAII, porque estos mensajes son transparentes para los nodos móviles y sólo se envían entre enrutadores HAWAII, es decir, no tienen implementado el protocolo de HAWAII, pero también deben de estar informados de quien es el enrutador de dominio. Por otro lado,

cuando un nodo móvil se mueve dentro de un mismo dominio HAWAII, la dirección IP del nodo móvil se mantiene.

La implementación de AODV sólo utiliza nodos inalámbricos, no toma en cuenta a los enrutadores de acceso (estaciones base). En los escenarios con redes híbridas hay nodos fijos, nodos inalámbricos y estaciones base. Cada nodo inalámbrico está asociado a una estación base, entonces para realizar simulaciones donde los nodos móviles cambian de estación base es necesario añadir una referencia al objeto nodo móvil, el cual representa el nodo al cual está unido el agente de enrutamiento [Ros y Ruiz, 2004].

De acuerdo al protocolo AODV, los nodos móviles pueden recibir diferentes tipos de mensajes AODV (RREQ, RREP, RERR), con el soporte de HAWAII se debe considerar que los nodos además de recibir los mensajes de AODV también pueden recibir mensajes de *aviso de enrutador* que envían los enrutadores de acceso o recibir *peticiones de registro MIP* si es un enrutador de acceso. Cuando un nodo recibe un mensaje de *aviso de enrutador* debe enviar un mensaje de *petición de registro* hacia el enrutador que le envió dicho mensaje, entonces se tiene que agregar la condición de que cuando el nodo móvil envíe un mensaje de *petición de registro* dirigido a un enrutador de acceso o al enrutador de domino y se encuentre a un sólo salto del enrutador (esté dentro del área de cobertura del enrutador de acceso: 250 metros) , el campo *siguiente salto* del encabezado común se colocará como la dirección del enrutador de acceso que envió el aviso, y si el enrutador de acceso está a más de un salto del nodo móvil, el nodo móvil debe realizar un proceso de descubrimiento

de ruta para encontrar una ruta hacia el enrutador de acceso que envió el mensaje de *aviso de enrutador*.

IV.3 Funcionamiento del mecanismo de enrutamiento para redes híbridas

IV.3.1 IP Móvil

Como se describió en la sección III.2, los enrutadores de acceso envían periódicamente (cada segundo) *mensajes de aviso de enrutador* hacia los nodos móviles que están en la red ad hoc, para que estos conozcan de su existencia y se asocien a ellos, sin embargo la implementación estándar de MIP define que los mensajes de aviso de enrutador se envíen con un TTL=1, por lo tanto, estos mensajes los reciben sólo los nodos que están a un salto de los enrutadores, dando como resultado que los nodos móviles que están fuera del área de cobertura de los enrutadores de acceso no reciban estos avisos. Para solucionar este problema, se propone que los nodos móviles que reciban los avisos, los retransmitan hacia sus nodos vecinos, para que todos los nodos móviles que estén fuera del área de cobertura del enrutador de acceso los reciban y se puedan asociar a ellos. En la figura 29 se muestra la transmisión de los avisos de enrutador por toda la red.

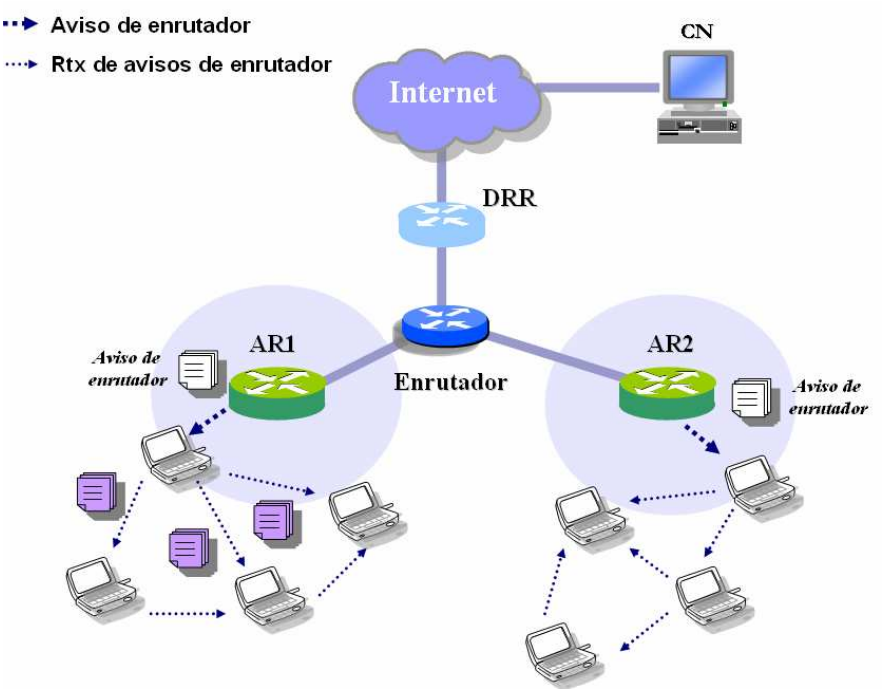


Figura 29. Transmisión de los avisos de enrutador.

Los *mensajes de aviso de enrutador* tienen los siguientes campos:

a) Tiempo de vida

b) Número de Secuencia

c) Enrutador de Acceso

d) Tiempo de Expiración

e) Número de Saltos

f) Distancia

Cuando un nodo móvil recibe un aviso de enrutador por primera vez o no está asociado a ningún enrutador de acceso, el nodo se asocia a ese enrutador independientemente de la

distancia que haya entre ellos. El proceso de asociación se ilustra en la figura 30 y es el siguiente: después de que el nodo móvil recibe el aviso de enrutador (paso 1), envía un mensaje de *petición de registro MIP* al enrutador de acceso del cual recibió el aviso de enrutador (paso 2), entonces cuando el enrutador de acceso recibe el *mensaje de petición de registro MIP*, este envía un mensaje HAWAII de actualización de ruta (HAWAII update) al enrutador que está al siguiente salto (paso 3), y cuando el mensaje llega al enrutador de dominio (paso 4), este envía un mensaje HAWAII de reconocimiento (HAWAII acknowledgement) al enrutador de acceso (paso 5), el cual envía un *mensaje de respuesta de registro MIP* al nodo móvil (paso 6), de esta manera el nodo móvil se asocia a un enrutador de acceso y registra en una lista (*lista de agente*) al enrutador de acceso con el que se asoció, también guarda el tiempo de vida, el tiempo de expiración del aviso y la distancia. Una vez que el nodo móvil se ha asociado a un enrutador de acceso, éste procede a retransmitir los avisos de enrutador que reciba de dicho enrutador de acceso, de esta forma los avisos de enrutador se propagan hacia los nodos vecinos en la red ad hoc (paso 7).

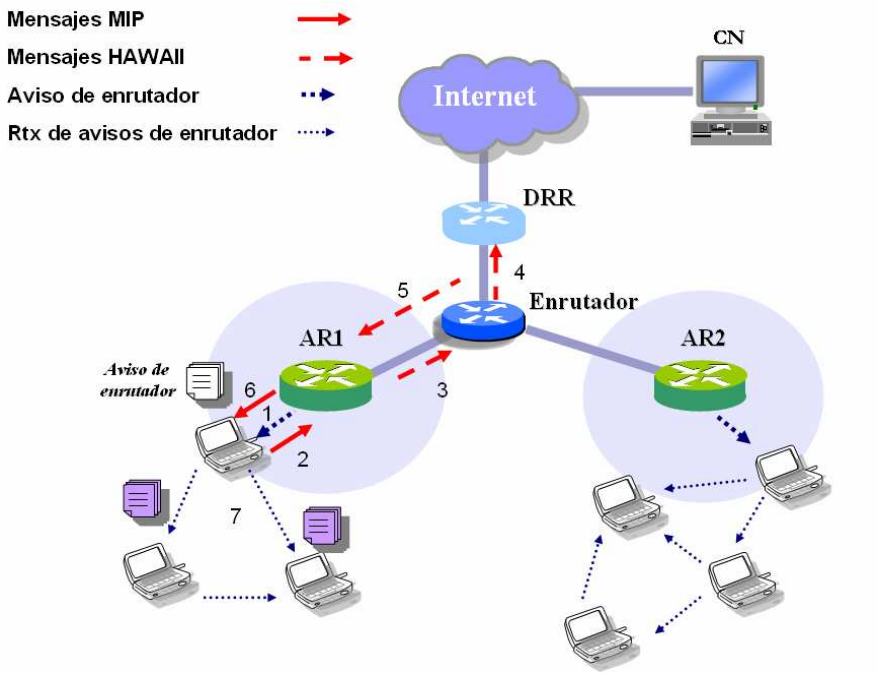


Figura 30. Proceso de asociación de los nodos móviles.

Para evitar sobrecarga de *mensajes de avisos* por toda la red, los nodos móviles retransmiten los avisos de enrutador hacia sus nodos vecinos sólo si se asocian al enrutador de acceso y se descartan los avisos que ya recibieron con anterioridad, para lograr esto, los nodos móviles además de tener una *lista de agente* en donde registran a los enrutadores de acceso con los que se asocian, guardan otra lista en donde almacenan el número de secuencia y el enrutador de acceso de los avisos que reciben, entonces cuando un nodo móvil recibe un aviso y se encuentra asociado a un enrutador de acceso, tiene que revisar su lista para saber si ya había recibido ese aviso antes, comparando el número de secuencia y el enrutador de acceso del mensaje actual con los que ya había recibido antes. Si el nodo descubre que ya había recibido el mensaje antes, lo descarta y no lo retransmite. Si por el contrario, el aviso que recibe el nodo móvil es nuevo y es del enrutador de acceso al que se

encuentra actualmente asociado, actualiza la información del aviso: el tiempo de vida, el tiempo de expiración y la distancia, envía un *mensaje de petición de registro IP Móvil* al enrutador de acceso, después este le contesta con un *mensaje de respuesta de registro IP Móvil* y el nodo retransmite el aviso de enrutador a sus nodos vecinos.

Cuando un nodo móvil recibe un aviso de un enrutador de acceso diferente al que se encuentra asociado actualmente, el nodo móvil tiene que comparar la distancia (en metros o en número de saltos) que hay entre él y el enrutador de acceso al que se encuentra asociado y la distancia que hay entre el enrutador de acceso desconocido y el nodo móvil, para asociarse al enrutador de acceso más cercano. Si la distancia actual (i.e. la que se reporta en el mensaje) es mayor que la distancia anterior (i.e. la distancia hacia el enrutador de acceso asociado), entonces el nodo móvil descarta el aviso y no lo retransmite. Pero si la distancia actual es menor que la distancia anterior, entonces el nodo móvil realiza un traspaso y se asocia al nuevo enrutador, es decir, se asocia al enrutador de acceso más cercano. Entonces, el nodo móvil almacena en su *lista de agente* al enrutador de acceso con el que se asoció, la distancia actual, el tiempo de expiración y el tiempo de vida del aviso, después, el nodo retransmite el aviso a sus nodos vecinos.

Si un nodo móvil se asocia a un enrutador (AR1) y después se asocia a otro enrutador (AR2), cuando el nodo móvil reciba otra vez un aviso del AR1, descartará el aviso y no lo retransmitirá porque el primer aviso que envió el AR1 no ha expirado y aún se encuentra registrado en la lista de agente del nodo móvil.

El AR1 se borrará de la lista sólo cuando el tiempo actual sea mayor al tiempo de expiración del aviso. Una vez que se borre de la lista al AR1 y el nodo móvil reciba otro aviso de ese enrutador (AR1), lo procesará como si fuera un aviso de un enrutador desconocido. En la figura 31 se ilustra que el nodo móvil recibe el segundo aviso del AR1 a los 1.01 seg y que el primer aviso que recibió del AR1 expira a los 2.01 seg, entonces, el nodo móvil descarta al segundo aviso porque el primero no ha expirado todavía. Después de un tiempo, el nodo móvil recibe otro aviso del AR1 y se da cuenta que es de un enrutador que ya no conoce, entonces, lo procesa y lo retransmite a sus nodos vecinos, esto se debe a que el AR1 ya no se encuentra en la lista de agente.

Figura 31. Lista de Agente.

Cuando un nodo móvil no tiene registrado a ningún enrutador de acceso en su lista, quiere decir que no ha recibido un aviso de enrutador en determinado tiempo, entonces, el nodo móvil envía un mensaje de *solicitud de agente* a los enrutadores de acceso cada 3 segundos y cuando un enrutador de acceso lo recibe, este envía un *mensaje de aviso de enrutador* al nodo móvil que le envió el mensaje de *solicitud de agente*. El nodo móvil, entonces, se

asocia a ese enrutador de acceso independientemente de la distancia que haya entre él y el enrutador de acceso.

IV.3.2 AODV

Si un nodo quiere comunicarse con un nodo que está en la red ad hoc y no hay una ruta disponible, se inicia un *proceso de descubrimiento de ruta*, en el cual, el nodo fuente envía un mensaje RREQ hacia sus nodos vecinos para encontrar una ruta, este mensaje funciona como un mensaje de AODV normal, entonces, cuando un nodo o enrutador de acceso recibe el mensaje RREQ tiene las siguientes opciones:

a) Si el nodo móvil o enrutador de acceso que recibe el mensaje RREQ es el nodo destino, entonces envía un mensaje RREP.
b) Si el nodo móvil o enrutador de acceso que recibe el mensaje RREQ no es el nodo destino, pero tiene una ruta hacia ese destino, entonces envía un mensaje RREP.
c) Si el nodo móvil o enrutador de acceso que recibe el mensaje RREQ no es el destino y no tiene una ruta hacia ese destino, entonces, retransmite el mensaje RREQ hacia sus nodos vecinos.

Con este mecanismo, los enrutadores de acceso también realizan estas funciones porque tienen implementado el protocolo AODV. Por otro lado, cuando un enrutador de acceso recibe un mensaje RREQ, y no es el destino, este procede a generar una copia de ese mensaje y lo envía hacia los demás enrutadores de acceso que existen en la red de manera

"unicast" (i.e. se genera una nueva copia del mensaje RREQ para ser enviado a cada uno de los enrutadores de acceso), una vez que los enrutadores reciben la copia del mensaje RREQ, estos retransmiten el mensaje RREQ dentro de la red ad hoc, es decir, tiene que enviar el mensaje RREQ de manera "broadcast" hacia sus nodos móviles vecinos en la red inalámbrica ad hoc.

De esta manera, se pretende que los mensajes RREQ se difundan más rápido por toda la red inalámbrica y se pueda encontrar rápidamente la mejor ruta para enviar los datos.

IV.3.3 Comunicación de un nodo móvil con un nodo correspondiente

La implementación de AODV también fue modificada para que un nodo móvil se pudiera comunicar con un nodo correspondiente en la red cableada (suponiendo que sólo exista un nodo correspondiente fijo en la arquitectura), como se muestra en la figura 32.

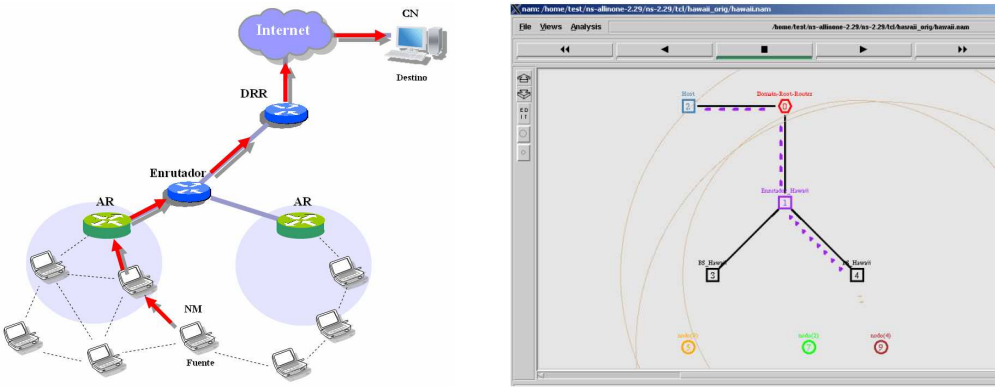


Figura 32. Comunicación de un nodo móvil con un nodo correspondiente.

En AODV normal, si el mensaje que recibe un nodo móvil no va dirigido a otro nodo dentro de la red ad hoc, se considera que el destino del mensaje es un nodo correspondiente en la red cableada. En este mecanismo, la dirección del nodo correspondiente es conocida en la red híbrida, por eso cuando un nodo móvil envía un mensaje dirigido al nodo correspondiente, no tiene que realizar una búsqueda mediante algún procedimiento de AODV para saber si el mensaje es para un nodo correspondiente en la red cableada. Entonces, para lograr la comunicación de un nodo móvil con un nodo correspondiente se realiza lo siguiente:

Si un nodo móvil se quiere comunicar con un nodo que está en Internet, éste debe buscar una ruta hacia algún enrutador de acceso en su tabla de enrutamiento, y no la dirección del nodo correspondiente en Internet, si hay una ruta disponible, se envía el mensaje; esto se hace así, porque el enrutador de acceso conoce una ruta hacia el nodo correspondiente por el protocolo de micromovilidad HAWAII (sólo si éste se encuentra en el mismo dominio administrativo). Si no hay una ruta disponible hacia el AR, entonces se añade la dirección destino del nodo correspondiente en la tabla de enrutamiento y se hace un *proceso de descubrimiento de ruta*; el mensaje RREQ que envía el nodo que se quiere comunicar con el nodo correspondiente en Internet debe tener como dirección destino al enrutador de acceso al cual está asociado el nodo móvil.

Si hay una ruta válida que ya expiró hacia el enrutador de acceso y hay paquetes almacenados en el buffer dirigidos al nodo correspondiente, se envían y después se invalida la ruta.

Capítulo V.

SIMULACIÓN Y RESULTADOS

V.1 Introducción

Para evaluar el mecanismo de enrutamiento propuesto se utilizó el simulador de redes ns-2 (Network Simulator), fue escogido como herramienta de simulación para este trabajo de tesis porque tiene una arquitectura abierta que puede ser modificada, extendida y es muy usado para la investigación de redes.

V.2 Simulador de redes ns-2

Network Simulator (ns) es un simulador que maneja eventos discretos orientados a la investigación de redes de computadoras y protocolos de redes [Chung y Claypool, 1999].

Entre otras cosas, ns soporta las siguientes tecnologías:

- Conexiones punto a punto, redes de área local, enlaces satelitales, enlaces inalámbricos.
- Modelos de tráfico y aplicaciones (web, FTP, telnet, CBR)
- Protocolos de transporte: TCP (Tahoe, Reno, Vegas,..),UDP, SRM

- Enrutamiento (Enrutamiento cableado unicast, multicast), enrutamiento ad hoc, IP Móvil
- Modelos de Colas : Drop Tail, RED, FIFO
- Medio Físico
- Calidad de Servicio (IntServ, DiffServ)
- Protocolos MAC (control de acceso al medio) del tipo CSMA/CD (acceso múltiple por sensado de portadora y detección de colisiones)
- Soporte matemático (generación de números aleatorios, integrales, etc.)

El simulador de redes ns está basado en dos lenguajes de programación: C++ y OTcl. OTcl es una versión orientada a objetos de Tcl, la cual es usada para el control de la estructura y la descripción de los escenarios de simulación. También se encarga de la organización de los eventos y la configuración dinámica de los componentes de red durante la simulación. La base del simulador está escrita en C++ para permitir una rápida simulación de escenarios grandes. Mientras este enfoque es muy flexible, también añade complejidad [Altman y Jiménez, 2003].

El ns-2 posee además una herramienta llamada animador de redes (NAM, *the network Animator*) la cual tiene como utilidad el representar gráficamente la red que se haya construido y compilado por ns-2. Pueden visualizarse dinámicamente los resultados de la simulación que ns-2 haya producido en un archivo junto con la topología de la red. Estos

resultados dependerán de la topología, protocolos, parámetros, etc. que en ellos se definan [Sosa, 2005]. En la figura 33 se muestra al simulador de redes ns-2.

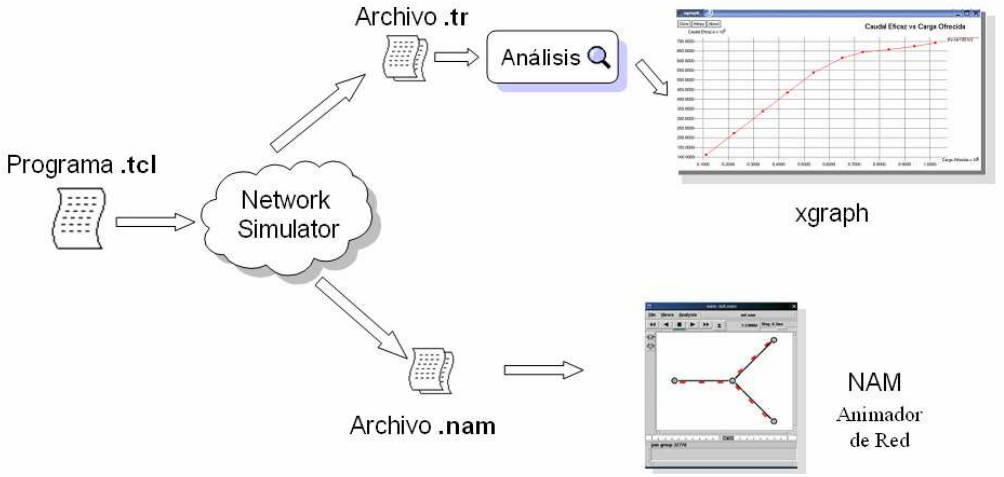


Figura 33. Simulador de redes NS-2.

V.2.1 El modelo inalámbrico de ns-2

Los nodos inalámbricos implementados en ns tienen características adicionales en comparación con los nodos cableados. La diferencia más importante es que los nodos móviles están conectados a canales inalámbricos para su comunicación. Tienen información acerca de su localización y pueden moverse con una velocidad específica. La figura 34 muestra el esquema de un nodo móvil, el cual consiste de los siguientes componentes:

- *El Clasificador de dirección* se usa para manejar paquetes hacia el clasificador de puerto o agente de enrutamiento.

- *El* C*lasificador de puerto* es usado para enviar paquetes hacia los agentes unidos al nodo móvil.

- *El Agente de enrutamiento* es usado para el manejo de tablas de enrutamiento y envío de paquetes. El agente de enrutamiento debe colocar en el campo *next_hop_* de los paquetes el destino que está al siguiente salto.

- *La Capa de enlace* (LL) es responsable de convertir una dirección de red a una dirección hardware (con la ayuda del modulo ARP) y preparar los paquetes para ponerlos dentro del canal inalámbrico.

- *El Modulo ARP* mapea la dirección de red a la dirección MAC.

- *La* C*ola de interfaz* (IfQ) es usada para almacenar paquetes que deben ser enviados.

- *La Capa MAC* maneja el acceso al canal inalámbrico.

- *La Interfaz de red* envía y recibe paquetes sobre el canal inalámbrico.

- *El Modelo de propagación radio* determina la potencia de la señal de los paquetes recibidos, para que el paquete puede ser recibido por una interfaz de red o no.

- *El Canal inalámbrico* en el cual son distribuidos los paquetes.

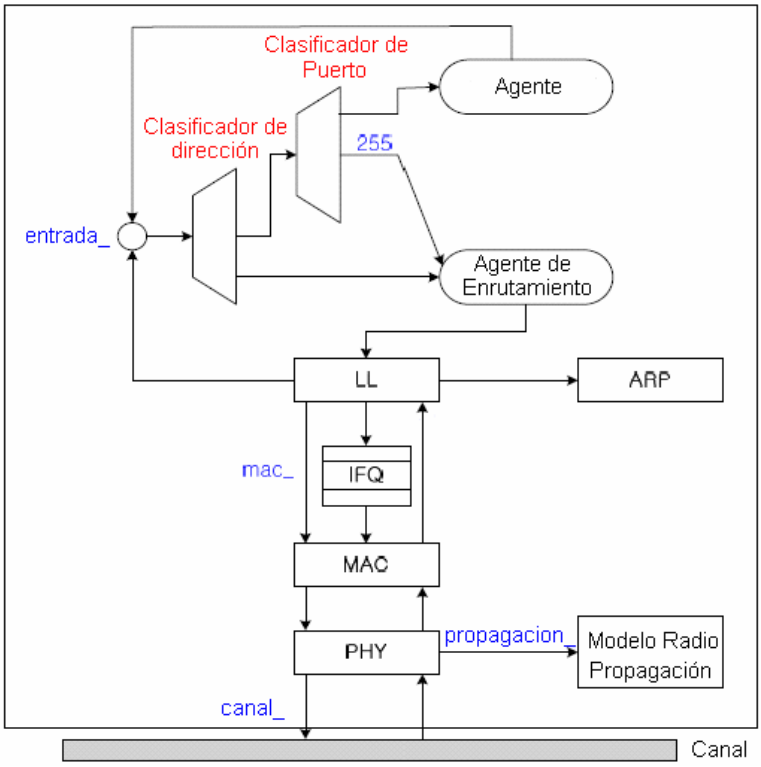


Figura 34. Modelo de un nodo inalámbrico en ns-2.

Al comienzo de una simulación inalámbrica se necesita definir el tipo de cada uno de estos componentes. Adicionalmente, se necesitan definir otros parámetros como el tipo de antena, el modelo de radio propagación, el tipo de protocolo de enrutamiento usado por los nodos móviles, etc. [Wiberg, 2002].

V.2.2 Enrutamiento en redes móviles

Los nodos móviles usan un agente de enrutamiento para calcular rutas hacia otros nodos dentro de la red, es decir, toma toda la responsabilidad de enrutar y enviar paquetes. Los nodos móviles no mantienen tablas de enrutamiento, en lugar de eso el agente de enrutamiento tiene que mantener tal tabla de enrutamiento internamente. No hay una lógica de ruta disponible para realizar cálculo de rutas; esto lo realiza el agente de enrutamiento. También calcula las rutas que no están instaladas modificando la dirección del clasificador. En su lugar, el clasificador de dirección usualmente tiene el agente de enrutamiento colocado como su objetivo, y el agente de enrutamiento tiene que realizar el envío de paquetes. Finalmente, este envío ocurre sobre el canal inalámbrico. Es responsabilidad del agente de enrutamiento llenar el campo *next_hop_* de cada paquete que debe ser enviado, antes de enviarlo a la capa de enlace del nodo móvil.

Actualmente ns soporta los protocolos de enrutamiento DSDV, DSR, TORA y AODV [Wiberg, 2002].

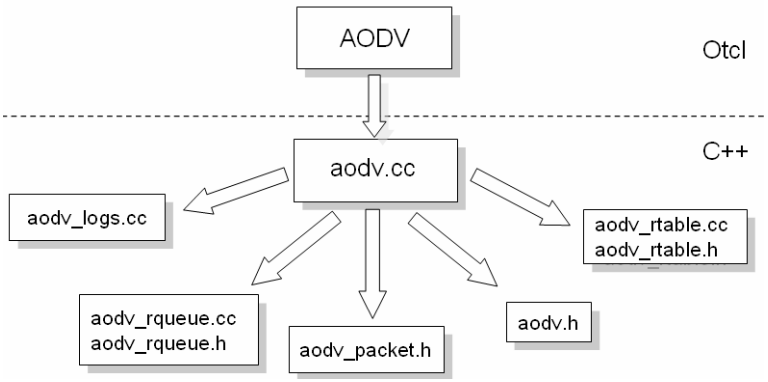


Figura 35. Implementación del protocolo AODV en ns.

V.2.2.1 AODV en ns

La implementación del protocolo de enrutamiento AODV en ns-2 está basada en el RFC 3561. Están definidos los formatos de los mensajes RREQ, RREP, RERR y los mensajes HOLA; el agente de AODV tiene una tabla de enrutamiento que mantiene y actualiza las rutas de los nodos, una lista de nodos vecinos de cada entrada de enrutamiento y tiene implementado las funciones más importantes del protocolo como el proceso de *descubrimiento de ruta*, el cual funciona de la siguiente manera: cuando un nodo fuente quiere comunicarse con un nodo destino trata de encontrar una ruta hacia ese destino (función *rt_rsolve*). Si el nodo móvil no tiene una ruta válida hacia ese destino difunde un mensaje RREQ (función *SendRequest*). Cuando los mensajes RREQ son recibidos por el nodo destino u otro nodo que conoce una ruta hacia el destino (función *recvRequest*), este envía mensajes de regreso al nodo fuente (función *SendReply*) y cuando el originador del mensaje recibe el mensaje RREP (función *recvReply*) , empieza a enviar paquetes hacia el nodo destino. En la figura 35 se muestra como está implementado el protocolo AODV en ns-2.

Para este trabajo fue necesario modificar el código de AODV para poder integrarlo con el protocolo de micromovilidad HAWAII.

V.2.2.2 Protocolo de micromovilidad HAWAII en ns-2

Por otro lado, debido a que el protocolo de micromovilidad HAWAII no está implementado en el simulador, fue necesario agregarle la extensión CIMS v1.0 (Columbia IP Micromobility Software), la cual es una extensión para el simulador de redes ns-2 basado en la versión ns-2.1b6 que soporta diferentes protocolos de micromovilidad como HAWAII, IP Celular e IP Móvil jerárquico [Campbell, *et al*., 2002].

La implementación de HAWAII soporta dos esquemas de traspaso: esquemas de envío (MSF) y esquemas de no envío (UNF). De acuerdo al protocolo de micromovilidad HAWAII, los enrutadores de acceso HAWAII necesitan implementar la funcionalidad de agente foráneo IP móvil sin la capacidad de desencapsulación y son responsables de generar mensajes de actualización HAWAII; los creadores de CIMS modificaron el objeto **BaseStationNode** de *ns-2* para incluir estas características. Además, extendieron el objeto *nodo móvil* para incluir las funciones **PFANE** requeridas por el protocolo HAWAII. Los enrutadores HAWAII son implementados en objetos especiales llamados *HawaiiAgent* que pueden procesar mensajes HAWAII y realizar operaciones específicas del protocolo. Por otro lado, las capacidades de voceo no están soportadas en la extensión CIMS [Campbell, *et al*., 2002].

Todos los protocolos de micromovilidad implementados en esta extensión tienen la topología de red mostrada en la figura 36.

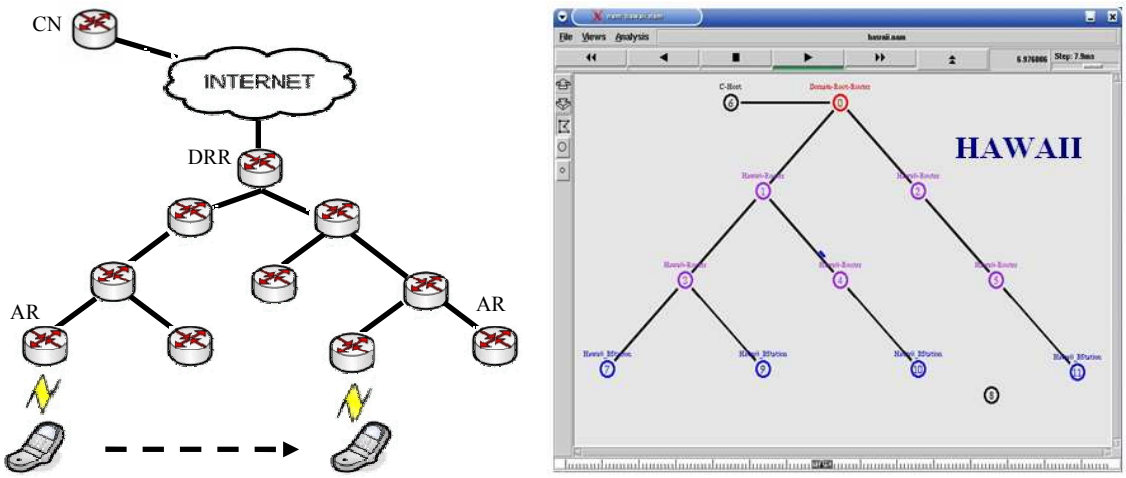


Figura 36. Topología de red usada en la extensión CIMS.

Como se mencionó en otros capítulos, el protocolo de micromovilidad HAWAII trabaja junto con IP Móvil, por eso es importante mencionar la implementación de IP Móvil en ns.

V.2.2.3 IP Móvil en ns

Además de los nodos inalámbricos, existen otros nodos llamados nodos *estación base* que pueden ser conectados a los enlaces cableados y a los canales inalámbricos. Actúan como puentes entre la parte cableada e inalámbrica de la red y son una parte importante de la simulación de IP Móvil. En la figura 37 se muestra el modelo de un nodo *estación base* o *enrutador de acceso*.

La implementación de IP Móvil para ns-2 incluye los componentes básicos (Agentes de casa, nodos móviles, agentes foráneos) y la funcionalidad básica como el proceso de registro con un nuevo agente foráneo.

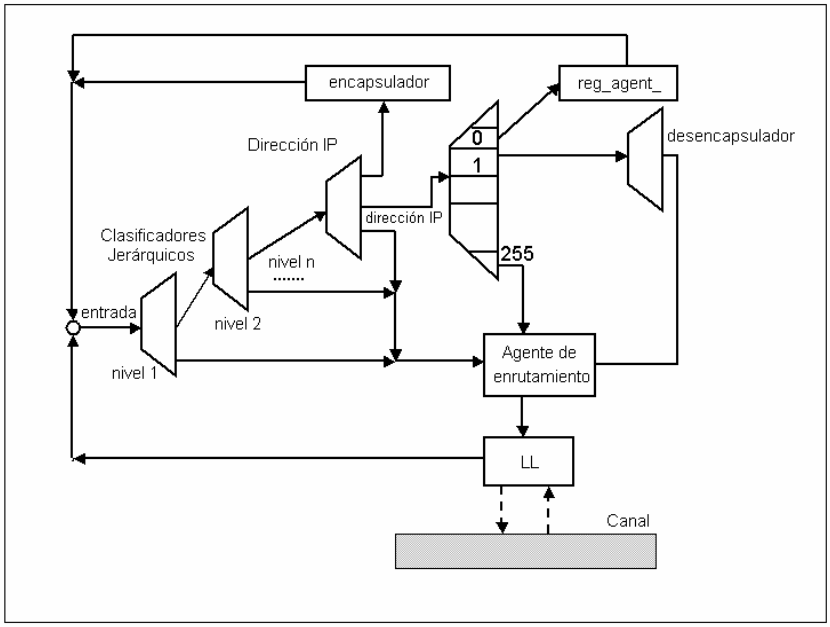


Figura 37. Modelo de un nodo enrutador de acceso.

Todos los ARs anuncian su presencia enviando mensajes de aviso de enrutador en un intervalo de tiempo. Los nodos móviles almacenan en una lista la dirección de los ARs que están en el rango. Cuando no se recibe un mensaje de aviso de enrutador de un enrutador de acceso registrado en cierto tiempo, la lista de entradas expira y es borrada. Cuando los nodos móviles tienen que realizar un traspaso, escogen un enrutador de acceso de su lista como su nuevo agente foráneo. Si la lista no contiene entradas, el nodo móvil envía un mensaje de solicitud de agente. Los enrutadores de acceso que reciben este mensaje tienen que enviarle un mensaje de aviso de enrutador, lo cual le permite al nodo móvil registrarse con ellos. El traspaso es iniciado con una petición de registro del nodo móvil. El enrutador de acceso, entonces, envía la petición hacia el agente de casa del nodo móvil. El agente de casa actualiza la CoA del nodo móvil e instala un encapsulador para enviar los paquetes IP

hacia el nodo móvil por medio del enrutador de acceso. El agente de casa entonces envía un mensaje de respuesta de registro al enrutador de acceso y este informa al nodo móvil que el traspaso fue un éxito. De ahí en adelante, el enrutador de acceso actúa como el agente foráneo del nodo móvil.

Sin embargo, el algoritmo de traspaso se mantiene muy simple. Si el nodo móvil recibe un mensaje de aviso de enrutador de un enrutador de acceso, este envía un mensaje de petición de registro y de ahí en adelante usa el enrutador de acceso como agente foráneo. Esto da como resultado interrupciones hasta que la nueva conexión se establece aunque el nodo móvil podría seguir comunicándose con el resto de la red sobre su agente foráneo actual. Tan pronto como las áreas de los enrutadores de acceso se traslapan, el nodo móvil constantemente cambia de enrutador de acceso [Fall y Varadhan, 2007].

V.3 Métricas de desempeño

Para evaluar el desempeño del algoritmo propuesto se utilizaron las siguientes métricas:

- Pérdida de paquetes
- Retardo de paquetes
- Jitter (variaciones en el retardo)
- Caudal Eficaz (Throughput)
- Número de traspasos

V.3.1 Pérdida de paquetes

La pérdida de paquetes está definida en función del número de paquetes recibidos por el destino y los generados por la fuente; esta métrica proporciona información relacionada con la cantidad de paquetes que no llegaron a su destino o que se perdieron en una transmisión.

La pérdida de paquetes se calculó de la siguiente forma:

$$Paquetes\ Perdidos = Paquetes\ Enviados - Paquetes\ Recibidos \quad (1)$$

V.3.2 Retardo de paquetes

El retardo de paquetes está definido como la diferencia que existe entre el tiempo en el que un paquete es recibido por el destino y el tiempo en el que dicho paquete fue generado por la fuente.

Para calcular el retardo de paquetes se utilizó una herramienta creada por Ke, [2005], la cual consiste de un agente que monitorea el envío/recepción de los paquetes y crea dos archivos de salida, uno para el transmisor y otro para el receptor, es decir, cuando inicia una sesión CBR entre dos nodos móviles y se empiezan a enviar paquetes, el identificador del paquete y el tiempo de envío son grabados en un archivo y cuando los paquetes son recibidos por el destino, el identificador del paquete y el tiempo en el que se recibieron son grabados en otro archivo.

Para medir el retardo promedio de los paquetes recibidos sólo se usó el archivo que se genera para el receptor. Este archivo consiste de cuatro columnas, la primera columna es el identificador del paquete, la segunda columna es el tiempo de envío del paquete, la tercera columna es el tiempo en que se recibe el paquete, y la cuarta columna es el retardo extremo a extremo, es decir la resta de la segunda y tercer columna. En la figura 38 se muestra un ejemplo de este archivo.

Id. pte	Tiempo tx	Tiempo rx	Retardo
1	301.200000	301.219731	0.019731
2	301.400000	301.419751	0.019751
3	301.600000	301.619251	0.019251
4	301.800000	301.819871	0.019871
5	302.000000	302.019171	0.019171
6	302.200000	302.219411	0.019411
.....	.....	.....	.....
1495	598.600000	598.619271	0.019271
1496	598.800000	598.819531	0.019531
1497	598.000000	598.019711	0.019711

Figura 38. Salida de archivo.

Entonces, para obtener el retardo promedio de una simulación se suman los retardos de cada paquete (la columna 4) y se divide entre el número de paquetes recibidos.

V.3.3 Jitter (variaciones en el retardo)

El jitter es la variación del tiempo de llegada de paquetes consecutivos, debido a que no todos los paquetes tienen el mismo retardo, y por tanto se produce una espera que varía durante la recepción de un paquete y otro.

De acuerdo a Elarag y Bassiouni, [2000], Aad y Castelluccia, [2001] el jitter se puede definir como la desviación estándar del retardo de paquetes.

$$Jitter = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(x_i - \bar{x}\right)^2} \qquad (2)$$

donde N es el número de paquetes recibidos, x_i es el retardo de cada paquete y $\bar{x}$ es el promedio de todos los retardos. Utilizando el mismo archivo que se usa para calcular el retardo de los paquetes nos permite obtener el *jitter* en el proceso de recepción durante una simulación.

V.3.4 Caudal Eficaz (Throughput)

El caudal eficaz, o throughput, se define como la relación entre el número de paquetes que se reciben durante un intervalo de tiempo [Lee, et al., 2002].

De acuerdo a Talipo, [2005] el throughput se calcula:

$$Throughput = \frac{Paquetes\ \mathrm{Re}cibidos}{Intervalo\ de\ tiempo\ (seg)}\ x\ Tamaño\ del\ paquete\ (bytes)\ x\ 8\ bits \qquad (3)$$

El tamaño del paquete es un parámetro de configuración de *ns-2* dado en bytes, y el intervalo de tiempo es el tiempo que dura la conexión CBR en una simulación.

V.4 Entorno de simulación

Como se mencionó en el capítulo anterior, las simulaciones fueron realizadas con el simulador de redes ns-2 y con la extensión CIMS. Para evaluar el desempeño del algoritmo propuesto se tomaron en cuenta las siguientes consideraciones:

- *Los nodos móviles se muevan a diferentes velocidades*

Para lograr esto se crearon movimientos aleatorios con una herramienta de ns-2 llamada *setdest*, la cual genera los movimientos usando el algoritmo *random waypoint*, y funciona de la siguiente manera, cada nodo empieza la simulación con una posición inicial, después selecciona un destino aleatorio y se mueve hacia ese destino con una velocidad que se obtiene del rango de una variable aleatoria uniformemente distribuida entre 0 y un valor de velocidad máxima. Después de alcanzar al destino, el nodo se detiene y hace una pausa de algunos segundos, selecciona otro destino y repite el mismo comportamiento durante toda la simulación. Entonces, para crear los movimientos aleatorios de las simulaciones se generaron varios archivos en donde se establecieron los parámetros de la tabla I.

Tabla I. Parámetros de Simulación.

Parámetro	Valor
Número de nodos	10, 30 nodos
Tipo de velocidad	Uniforme
Velocidad promedio	1 , 2 y 4 m/s
Tipo de pausa	Constante
Tiempo de pausa	0 segundos
Área de simulación	1000 x 1000 m
Tiempo de simulación	600 segundos

Como era necesario que los nodos se movieran a diferentes velocidades promedio, se tuvo que especificar una velocidad mínima (velocidad inicial) y una velocidad máxima (velocidad final), donde la velocidad mínima tenía que ser diferente de cero, porque de acuerdo a Yoo, *et al*., [2003] la velocidad promedio decae después de un tiempo de simulación si la velocidad inicial es 0, es decir, si se desea una velocidad promedio de 10 m/s y la velocidad inicial se establece a 0 m/s, la velocidad promedio después de un tiempo será de 4 m/s y tenderá a cero conforme aumenta el tiempo de simulación. Entonces, para mantener una velocidad promedio de 10 m/s durante toda la simulación, la velocidad mínima puede ser de 1 m/s y la velocidad máxima de 19 m/s. Por otro lado, un tiempo de pausa de 0 significa que todos los nodos se mueven continuamente.

- *Los nodos móviles generen tráfico CBR con enlaces independientes*

En este trabajo se le llama *enlace independiente* cuando un nodo móvil participa en un sólo enlace durante toda la simulación. Entonces, las conexiones con tráfico CBR fueron creadas aleatoriamente con enlaces independientes para que un nodo móvil no participara en dos enlaces diferentes durante una simulación y de esta manera evitar que se repitiera un nodo transmisor o un nodo receptor. Además, como se muestra en la tabla II para calcular el número de conexiones se consideró que fueran generadas dependiendo de la carga de la red (alta carga de tráfico cuando el 80% de los nodos móviles se comunica y baja carga cuando el 10% de los nodos móviles se comunica) y del número de nodos móviles.

Tabla II. Número de Conexiones con enlaces independientes.

Número de nodos	Número de conexiones	
10 nodos móviles	10%	1 conexión (2 nodos)
	80%	4 conexiones (8 nodos)
30 nodos móviles	10%	2 conexiones (4 nodos)
	80%	12 conexiones (24 nodos)

Por ejemplo, si tenemos una red con 10 nodos móviles y se necesita que se comuniquen el 80% de los nodos móviles, es decir, que se comuniquen 8 nodos, entonces habrá cuatro conexiones, en donde los nodos transmisores y receptores no se repetirán, como en la figura 39.

En el ejemplo de la figura 40 se ilustra una red con 10 nodos móviles, de los cuales 8 nodos se están comunicando, dando como resultado cuatro conexiones, se puede observar que el nodo 6 participa como nodo receptor y transmisor en dos enlaces diferentes (conexión 1 y 4) , y el nodo 8 participa como nodo receptor en dos enlaces (conexión 2 y 3), entonces se considera que estos enlaces son dependientes porque los nodos se repiten en una misma simulación.

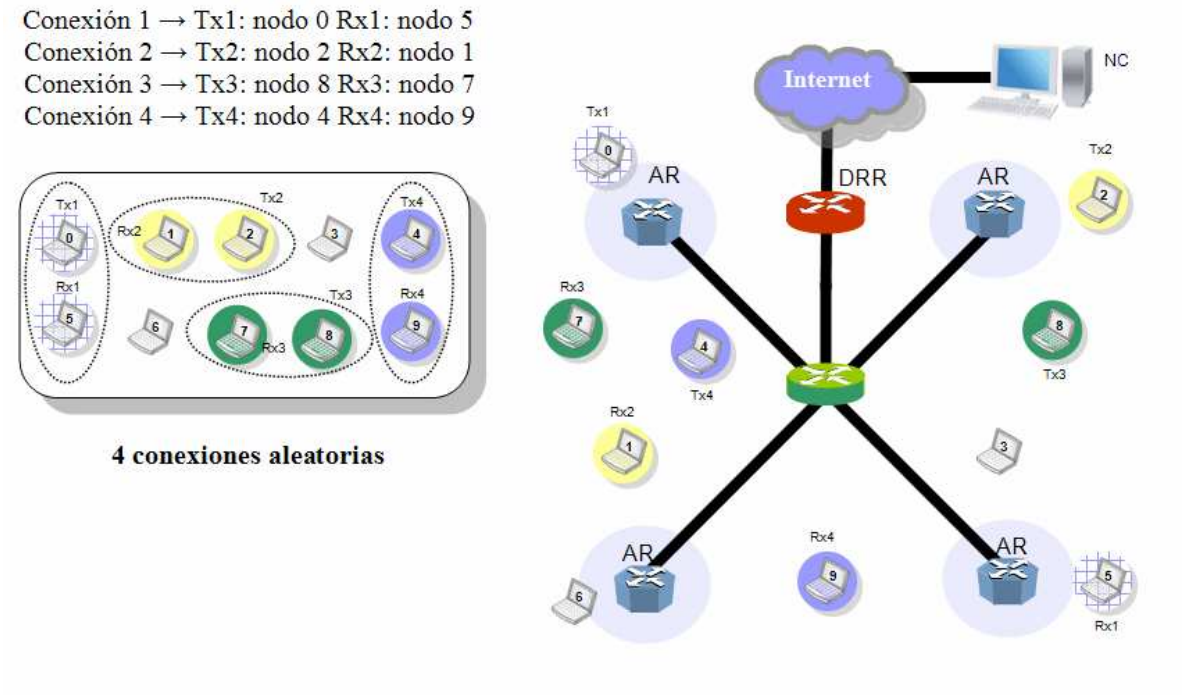


Figura 39. Generación de conexiones aleatorias con enlaces independientes.

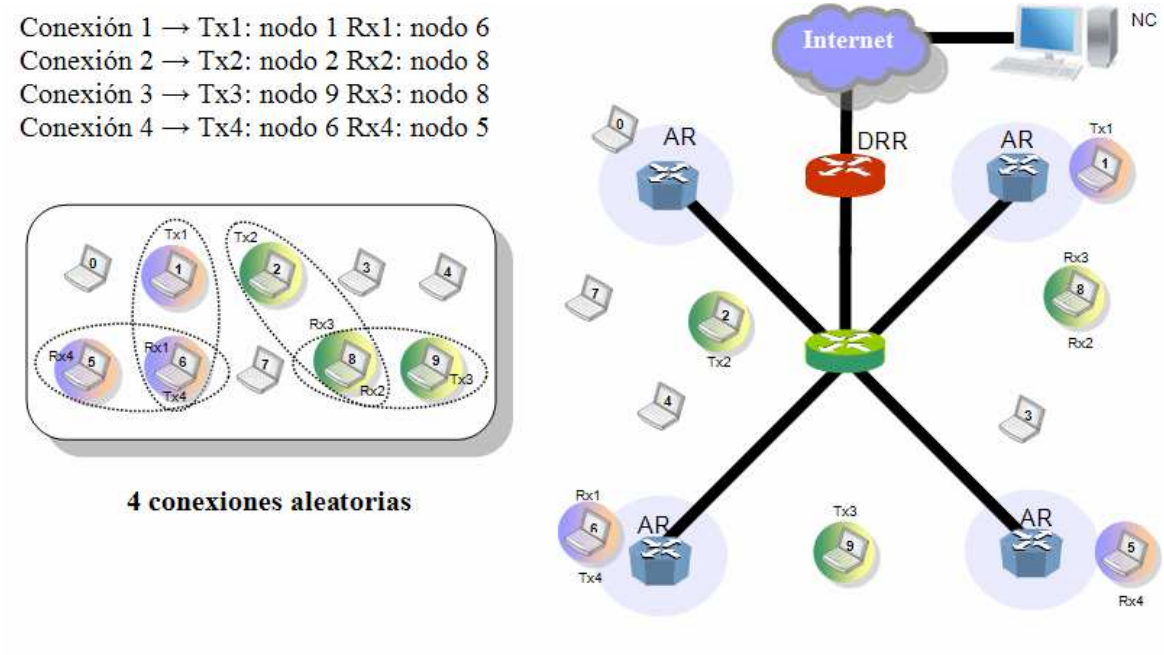


Figura 40. Generación de conexiones aleatorias con enlaces dependientes.

Entonces, para generar conexiones de tráfico aleatorias en las simulaciones, se establecieron los parámetros de la tabla III.

Tabla III. Parámetros para generar tráfico CBR.

Parámetro	Valor
Número de conexiones para 10 nodos	1, 4
Número de conexiones para 30 nodos	2, 12
Tipo de conexión de tráfico	CBR
Tamaño del paquete	1000 bytes
Generador CBR tiempo de envío de paquetes	0.2 seg (5 ptes/seg)
Tasa de Transmisión	40 Kbps
Tiempo de inicio de la conexión	300 segundos
Fin de la conexión	599.5 segundos

Las conexiones de tráfico CBR inician después de 300 segundos de simulación porque de acuerdo a Yoo, *et al*., [2003], cuando se utiliza un modelo de movilidad como *random waypoint* se debe esperar a que la red alcance un nivel de estabilidad, es decir, que la velocidad promedio de los nodos de la red se estabilice y ya no cambie, entonces, esto se logra después de que transcurre aproximadamente 300 segundos de simulación. La idea es que la sesión de CBR inicie cuando ya se haya estabilizado la velocidad promedio de los nodos.

Todas las simulaciones fueron realizadas con el mismo escenario de simulación con una duración de 600 segundos, variando la carga de tráfico de la red y el número de nodos móviles , además, las simulaciones se realizaron 100 veces para sacar un valor promedio y así tener un comportamiento más acertado del algoritmo propuesto.

V.4.1 Escenario 1

El primer escenario de simulación utiliza los parámetros mostrados en la tabla IV, se encuentra en un área rectangular de 1000 m x 1000 m, está formado por un enrutador de cruce, 10 nodos móviles, cuatro enrutadores de acceso, un gateway (enrutador dominio) y un nodo correspondiente. Los nodos móviles están situados aleatoriamente como se ilustra en la figura 41, y se mueven a una velocidad promedio de 1,2 y 4 m/s.

Tabla IV. Parámetros de simulación del escenario 1.

Parámetro	*Valor*
Protocolo de transporte	UDP
Tipo de Tráfico	CBR
Control de Acceso al medio	CSMA/CA
Modelo de Canal Radio	Dos Rayos
Modelo de Movilidad	Random Waypoint
Modulación	DSSS
Tasa máxima de transmisión	2 Mbps
Número de simulaciones realizadas	100
Área de Simulación	1000 x 1000 m
Número de nodos móviles	**10 nodos**
Velocidad Promedio	1,2 y 4 m/s
Tiempo de Simulación	600 seg
Número de conexiones para 10 nodos	**1,4**
Tamaño del paquete	1000 bytes
Generador CBR intervalo de envío de ptes	0.2 seg (5 ptes/s)
Tasa de transmisión	40 Kbps
Tiempo de conexión CBR	299.5 seg

Los enlaces cableados de la red de acceso son enlaces duplex con un retardo fijo de 2 ms y tienen un ancho de banda de 10 Mbps. Los enlaces inalámbricos son de 2 Mbps. La

distancia entre los enrutadores de acceso es de 500 m y la interfaz inalámbrica de los enrutadores de acceso tienen un rango de transmisión de 250 m. Las conexiones CBR tienen una duración de 299.5 seg porque empiezan a los 300 seg y terminan a los 599.5 seg y la tasa de transmisión de paquetes utilizada es de 40 Kbps porque se envían 5 ptes/s de 1000 bytes, entonces

$$\text{CBR Throughput} = 5 \text{ ptes/s} \times 1000 \text{ bytes} \times 8 \text{ bits} = 40 \text{ Kbps}$$

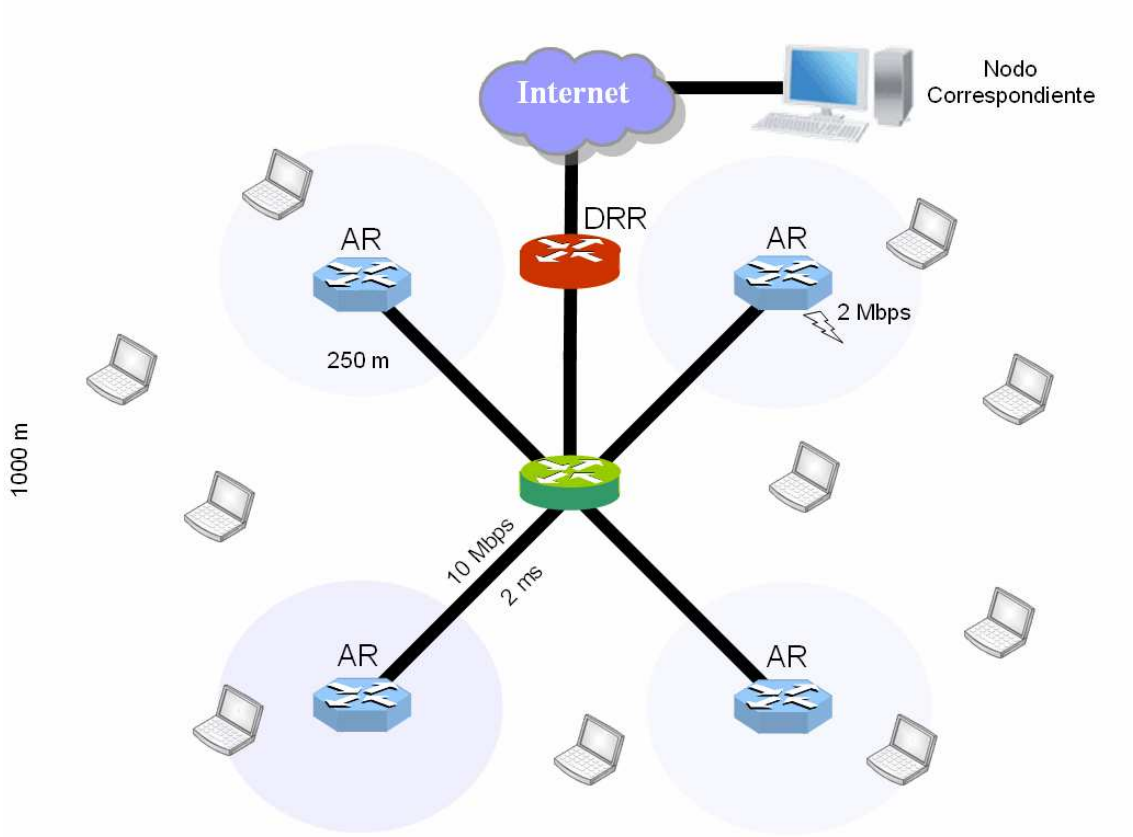


Figura 41. Escenario de simulación con 10 nodos móviles.

Se varió la carga de tráfico de la red, considerando alta carga cuando el 80% de los nodos móviles de la red se comuniquen y baja carga cuando sólo el 10% de los nodos móviles se comuniquen. El mecanismo de enrutamiento propuesto tiene dos modos de operación, donde los nodos se asocian al enrutador de acceso más cercano midiendo la distancia en metros o en número de saltos. Cuando los nodos se asocian a los enrutadores midiendo la distancia en metros se le llama *aodv+hawaii+metros* y cuando los nodos se asocian a los enrutadores midiendo la distancia en número de saltos se le llama *aodv+hawaii+saltos*.

V.4.2 Resultados de Simulación

a) Simulación con 10 nodos móviles y baja carga de tráfico (10% de los nodos comunicándose)

En esta simulación se comunican dos nodos móviles de la red ad hoc (i.e. una sola conexión) y el número de paquetes enviados durante una simulación es de 1498.

Paquetes Transmitidos = 5 ptes/s x 299.5 seg x 1 conexión CBR = 1498 paquetes

Las etiquetas utilizadas en las figuras tienen el siguiente significado:

- *aodv+hawaii+metros* : los nodos móviles se asocian al enrutador de acceso más cercano midiendo la distancia en metros.
- *aodv+hawaii+saltos:* los nodos móviles se asocian al enrutador de acceso más cercano midiendo la distancia en número de saltos.

- *aodv+hawaii:* los nodos móviles se asocian a cualquier enrutador de acceso sin tomar en cuenta la distancia, no hay retransmisión de avisos de enrutador, y los enrutadores de acceso no envían los mensajes de petición (i.e RREQ) hacia otros enrutadores de acceso, para que estos los envíen a los nodos móviles.

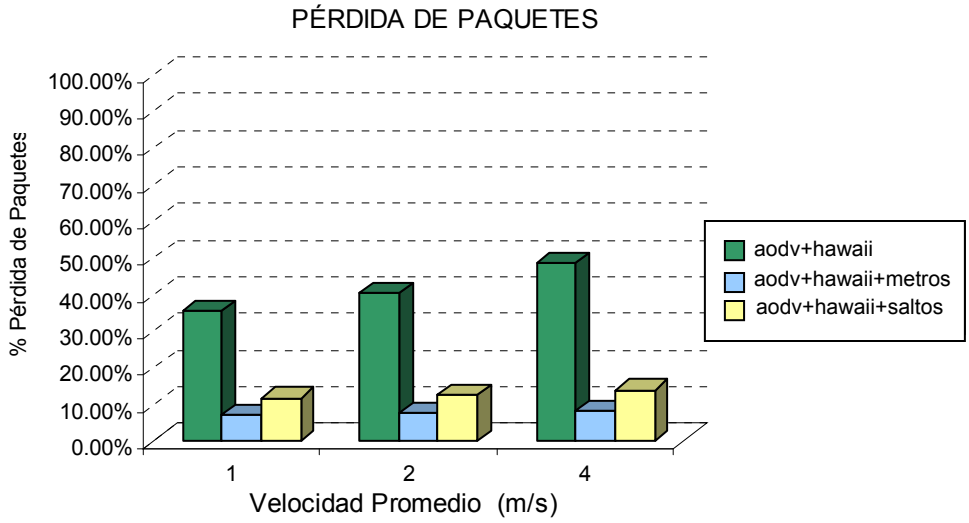


Figura 42. Gráfica de la pérdida de paquetes con baja carga de tráfico.

En la figura 42 se muestra el porcentaje de pérdida de paquetes de una conexión CBR en función de la velocidad promedio con que se mueven los nodos móviles. Se puede observar que conforme aumenta la velocidad promedio de los nodos móviles, la pérdida de paquetes es mayor en todos los casos, esto se debe a que cuando el nodo móvil se mueve más rápido, las rutas establecidas entre los nodos se rompen, provocando que haya fallas de enlaces y entonces, se tengan que crear nuevas rutas. Por el contrario, cuando los nodos móviles se mueven a una velocidad menor, no se realizan actualizaciones de rutas frecuentemente y por lo tanto hay menos fallas de enlaces. También se observa que de los tres casos, los que

tienen menor pérdida de paquetes es aodv+hawaii+metros y aodv+hawaii+saltos, esto puede ser porque los enrutadores de acceso también envían los mensajes de petición (i.e RREQ) hacia los demás enrutadores de acceso que existen en la red y hacia los nodos móviles haciendo que se encuentre más rápido la ruta deseada, y otra razón es que se asocian al enrutador de acceso más cercano. En particular aodv+hawaii+metros tiene mejor desempeño debido a que tiene una mayor exactitud de donde se encuentra el enrutador de acceso más cercano en comparación con aodv+hawaii+saltos.

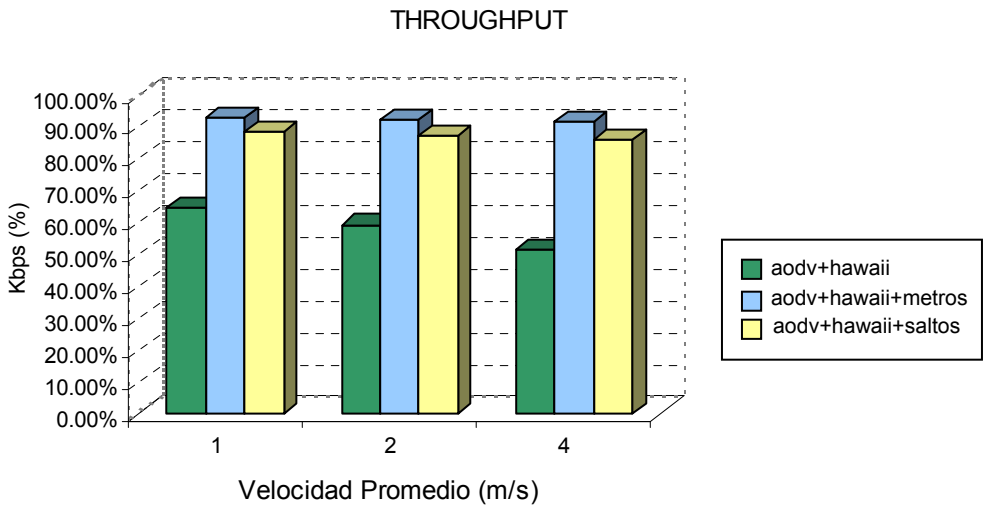


Figura 43. Gráfica del throughput con baja carga de tráfico.

En la figura 43 se muestra la gráfica del caudal eficaz (throughput) normalizado de una conexión CBR en función de la velocidad promedio con que se mueven los nodos móviles. Se observa que el caudal eficaz disminuye conforme aumenta la velocidad promedio de los nodos móviles. Esto es porque a velocidades mayores se presenta una mayor pérdida de paquetes y por lo tanto se reciben menos paquetes. De los tres casos simulados, el que tiene

menor throughput es aodv+hawaii porque es el que tiene mayor pérdida de paquetes, por otro lado, aodv+hawaii+metros es el que tiene mayor throughput; este último resultado es una consecuencia del número de paquetes perdidos, como se ilustra en la figura 42.

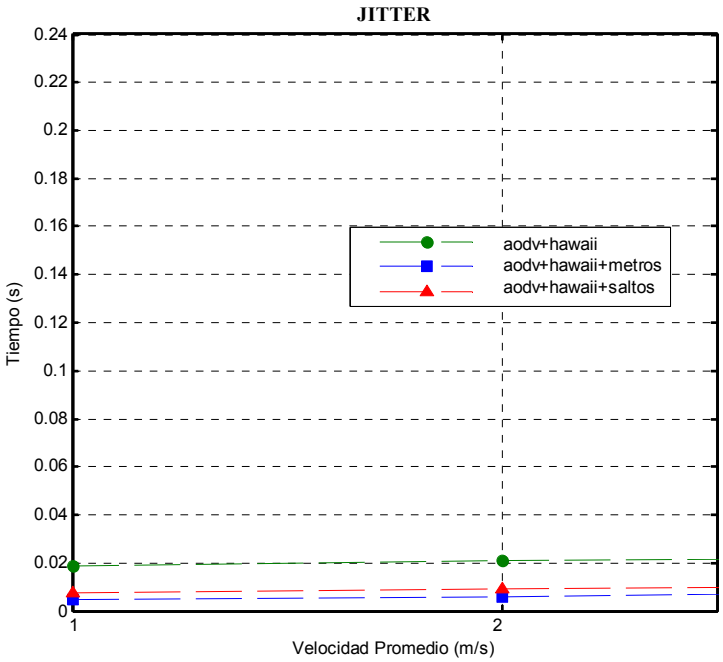


Figura 44. Gráfica del jitter con baja carga de tráfico.

En las figuras 44 y 45 se muestra la gráfica del jitter y el retardo, respectivamente, de una conexión CBR en función de la velocidad promedio de los nodos. Se observa que en cualquier caso, el jitter y el retardo se incrementan conforme la velocidad promedio de los nodos móviles aumenta, esto se debe a que cuando los nodos móviles se mueven más rápido hay fallas de rutas, y se tienen que crear nuevas rutas para reestablecer los enlaces de comunicación y continuar enviado los datos; como resultado se presenta un retardo aleatorio mientras se establecen las nuevas rutas. Por otro lado, el retardo también se ve afectado por el número de saltos que hay en la ruta establecida, es decir, entre mayor

número de saltos tenga una ruta, mayor será el retardo y el jitter. De los tres casos simulados, los que tienen menor retardo y jitter son aodv+hawaii+metros y aodv+hawaii+saltos, esto puede ser porque las rutas son creadas en menor tiempo por la rápida difusión de los mensajes RREQ, y las rutas pueden consistir de enlaces cableados e inalámbricos con menor número de saltos.

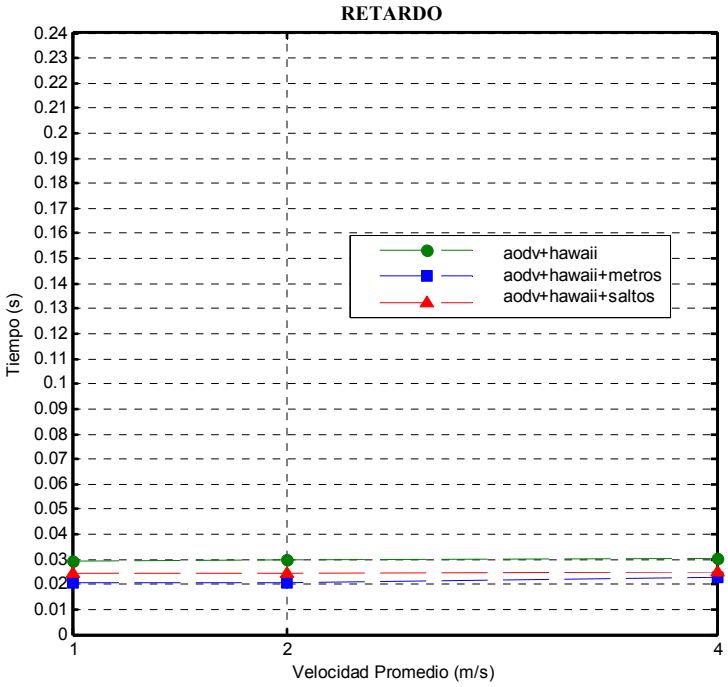


Figura 45. Gráfica del retardo con baja carga de tráfico.

b) Simulación con 10 nodos móviles y alta carga de tráfico (80% de los nodos comunicándose)

En esta simulación se comunican aleatoriamente ocho nodos móviles de la red ad hoc (4 conexiones) y el número de paquetes enviados por todas las conexiones durante una simulación es de 5990.

Paquetes transmitidos = 5 ptes/s x 299.5 seg x 4 conexiones CBR = 5990 paquetes

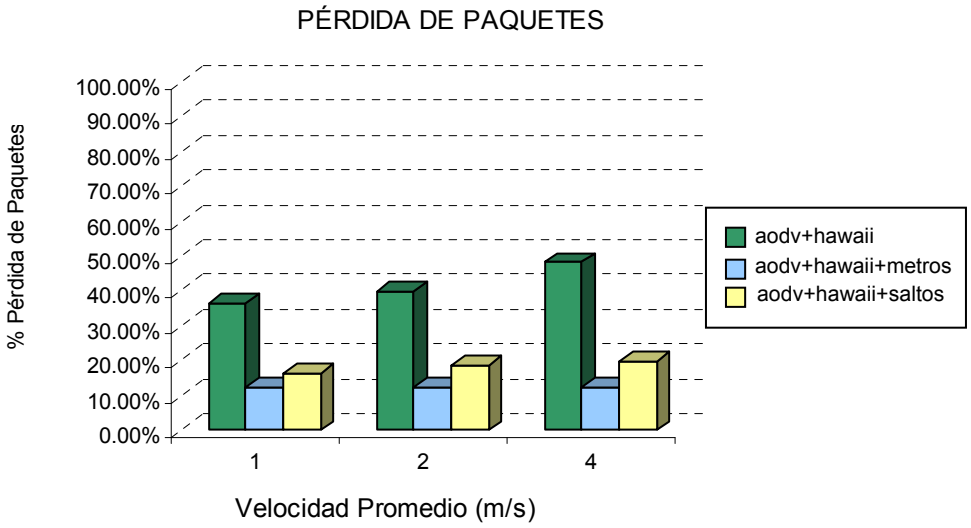


Figura 46. Gráfica de la pérdida de paquetes con alta carga de tráfico.

En la figura 46 se muestra la pérdida de paquetes de cuatro conexiones CBR en función de la velocidad promedio con que se mueven los nodos móviles. Al aumentar el número de conexiones, aumenta el número de paquetes enviados, entonces, es muy probable que haya mayor pérdida de paquetes que cuando se usa una sola conexión CBR. De la gráfica se puede observar que el comportamiento es igual al que sucede cuando se usa una sola conexión, esto es al aumentar la velocidad promedio de los nodos móviles, aumenta la pérdida de paquetes. Por otro lado, al tener un mayor número de conexiones en una simulación provoca que aumente mucho más las fallas de enlace y se tengan que crear nuevas rutas. Comparado los resultados de la gráfica 42 con los que se muestran en esta gráfica, se puede observar que el porcentaje de pérdida de paquetes es mayor para cuatro

conexiones que para una sola conexión porque se suma la pérdida de paquetes promedio de las cuatro conexiones. En particular aodv+hawaii+metros y aodv+hawaii+saltos tienen menor pérdida de paquetes en comparación con aodv+hawaii.

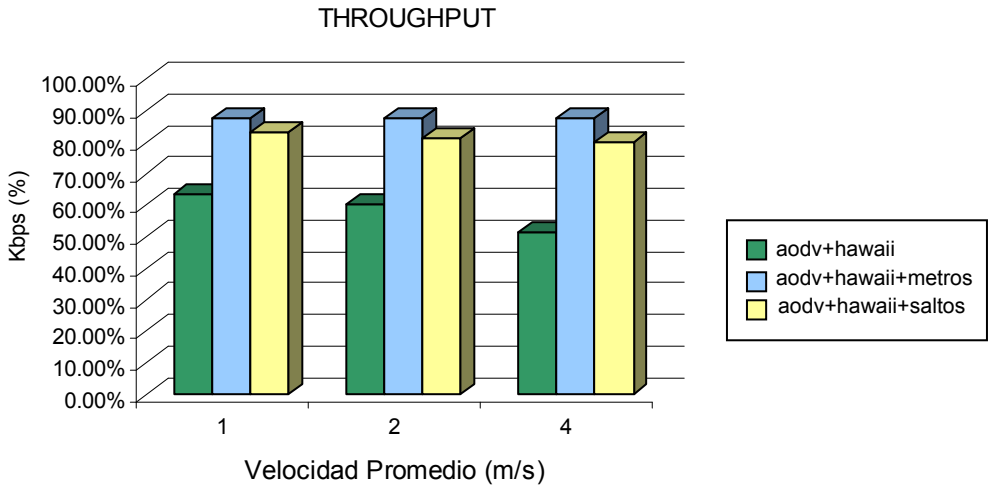


Figura 47. Gráfica del throughput con alta carga de tráfico.

En la figura 47 se muestra la gráfica promedio del caudal eficaz (throughput) normalizado de cuatro conexiones CBR en función de la velocidad promedio con que se mueven los nodos móviles. Se observa un comportamiento similar que en el escenario con una sola conexión CBR, el throughput disminuye conforme aumenta la velocidad promedio de los nodos móviles; esto se debe a que cuando los nodos móviles se mueven a una velocidad mayor provoca que se pierdan más paquetes. Comparando los resultados de la gráfica 43 con los que se muestran en esta gráfica, se puede observar que el porcentaje de caudal eficaz es mayor en comparación a los resultados obtenidos con una sola conexión, esto se debe a que se reciben menos paquetes. Se observa que el throughput es mayor en

aodv+hawaii+metros y en aodv+hawaii+saltos en comparación a aodv+hawaii; este resultado es una consecuencia del número de paquetes perdidos, como se muestra en la figura 46.

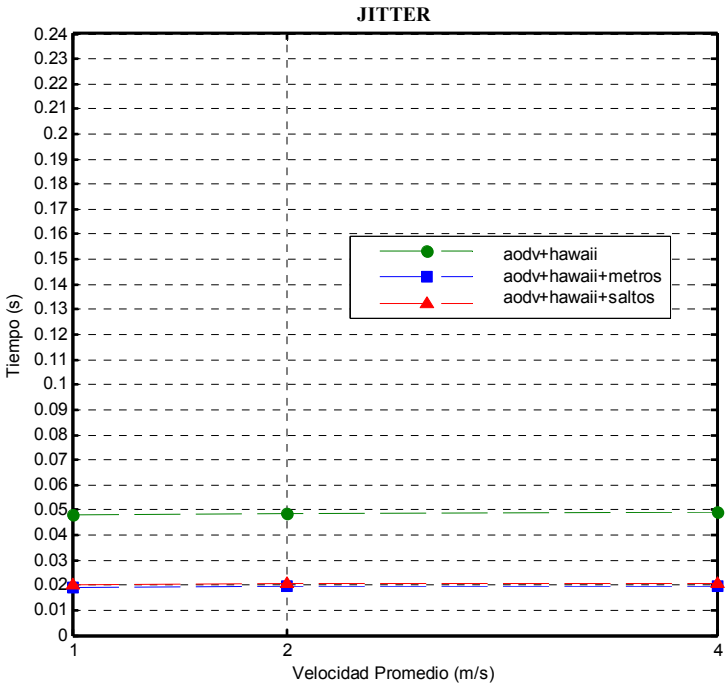


Figura 48. Gráfica del jitter con alta carga de tráfico.

En las figuras 48 y 49 se muestran las gráficas del jitter y el retardo de cuatro conexiones CBR, respectivamente, en función de la velocidad promedio con que se mueven los nodos móviles. Se observa que el comportamiento es similar al que tiene con una sola conexión CBR, conforme aumenta la velocidad de los nodos móviles, se incrementa el jitter y el retardo, esto se debe al tiempo de establecimiento de nuevas rutas cuando se rompen los enlaces debido al movimiento de los nodos y al número de saltos que tenga la ruta seleccionada. Los valores obtenidos de jitter y retardo con cuatro conexiones es mayor en

comparación a los obtenidos con una sola conexión, porque se suman los retardos promedio de las cuatro conexiones CBR.

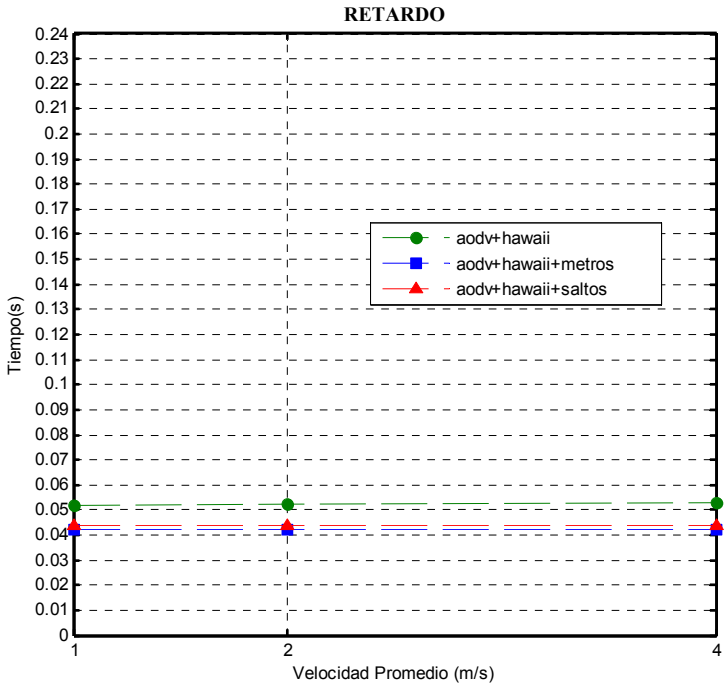


Figura 49. Gráfica del retardo con alta carga de tráfico.

En la tabla V se muestran los valores obtenidos de este escenario de simulación y se observa que en cualquier esquema de simulación (aodv+hawaii+metros, aodv+hawaii+saltos y aodv+hawaii) tanto en baja carga como en alta carga, conforme aumenta la velocidad promedio de los nodos móviles, la pérdida de paquetes, el jitter y el retardo incrementa y el throughput disminuye. Además, cuando aumenta la carga de tráfico, es decir el número de conexiones, también aumenta la pérdida de paquetes, esto se debe a que se consideran todos los paquetes que envían los nodos que participan en las conexiones.

Se observa que de los tres casos simulados en alta y baja carga de tráfico, los que tienen menor pérdida de paquetes son los que se asocian al enrutador de acceso más cercano (midiendo la distancia en metros y en número de saltos), esto se debe a que en el mecanismo propuesto, los enrutadores de acceso también difunden el mensaje de petición de ruta AODV haciendo que se difunda más rápido este mensaje para encontrar una ruta hacia el destino. Además de que las rutas pueden consistir de enlaces cableados y de enlaces inalámbricos con un número de saltos menor. También se tiene menor pérdida de paquetes, retardo y jitter porque los nodos móviles tienen una mayor exactitud de donde se encuentran los enrutadores de acceso, para asociarse al más cercano.

También, de los tres casos simulados, el que tiene mayor throughput es el que mide la distancia en metros para asociarse al AR más cercano, porque es el que tiene menor número de paquetes perdidos, por el contrario se tiene menor throughput cuando solamente se usa aodv+hawaii. En la figura 50 se muestra el escenario de simulación utilizado en ns-2 para obtener los resultados.

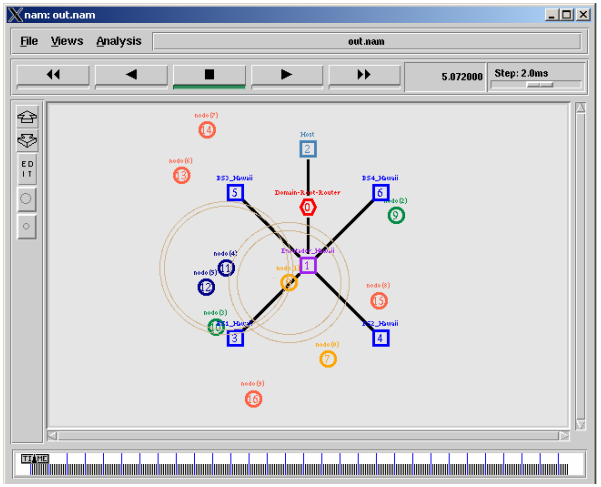
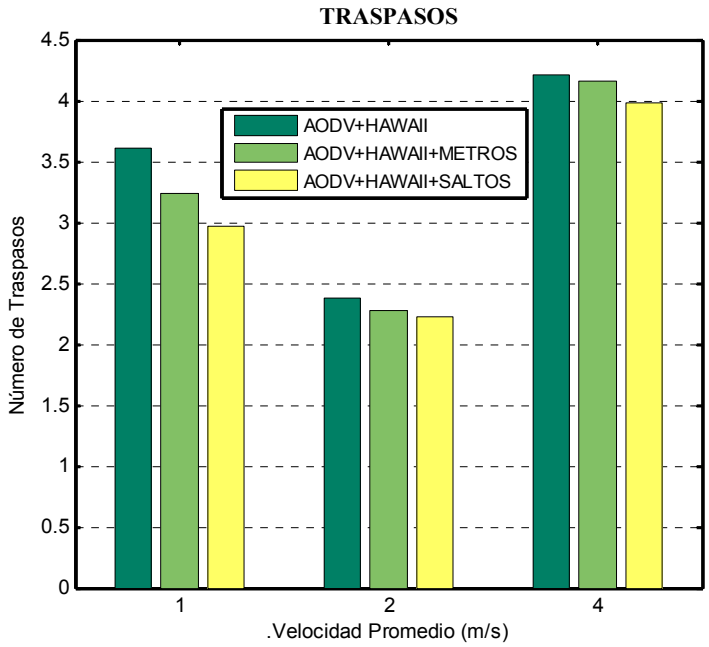


Figura 50. Escenario de simulación con 10 nodos móviles.

Tabla V. Comparación de los parámetros de desempeño con alta y baja carga de tráfico para 10 nodos móviles.

10 nodos		aodv+hawaii+metros			aodv+hawaii+saltos			aodv+hawaii		
Velocidad (m/s)		1	2	4	1	2	4	1	2	4
Baja Carga (10%)	Pérdida de ptes	104.81 (6.9%)	113.1 (7.5501%)	126.33 (8.4332%)	175.67 (11.72%)	191.96 (12.81%)	208.84 (13.941%)	532.33 (35.5%)	608.4 (40.614%)	730.3 (48.752%)
	Throughput	37.21 (93.03%)	37.003 (92.51%)	36.66 (91.66%)	35.32 (88.30%)	34.88 (87.21%)	34.43 (86.09%)	25.79 (64.49%)	23.76 (59.41%)	20.50 (51.27%)
	Retardo	0.020666	0.020846	0.022746	0.024502	0.024658	0.024702	0.029036	0.029903	0.030557
	Jitter	0.004747	0.006026	0.009243	0.007753	0.009369	0.009982	0.01889	0.020992	0.022251
Alta Carga (80%)	Pérdida de ptes	731.15 (12.20%)	738.9 (12.33%)	753.44 (12.57%)	994.37 (16.59%)	1108.84 (18.51%)	1178.97 (19.68%)	2192.06 (36.58%)	2387.37 (39.84%)	2892.68 (48.28%)
	Throughput	140.523 (87.83%)	140.316 (87.70%)	139.928 (87.46%)	133.492 (83.43%)	130.434 (81.52%)	128.561 (80.35%)	101.500 (63.44%)	96.283 (60.18%)	82.786 (51.74%)
	Retardo	0.042065	0.042126	0.042163	0.043603	0.043657	0.043692	0.051909	0.052221	0.052967
	Jitter	0.019309	0.019546	0.019736	0.019945	0.020456	0.0205	0.04781	0.048624	0.049296



	Aodv+Hawaii			Aodv+Hawaii+Metros			Aodv+Hawaii+Saltos		
Velocidad (m/s)	1	2	4	1	2	4	1	2	4
10 nodos	3.60	2.37	4.21	3.24	2.27	4.16	2.97	2.21	3.98

Figura 51. Número de traspasos promedio de 10 nodos móviles.

En la figura 51 se muestra el número de traspasos promedio de 10 nodos móviles en función de la velocidad con que se mueven los nodos. Se puede observar de la gráfica y de los valores obtenidos que el número de traspasos entre aodv+hawaii, aodv+hawaii+metros y aodv+hawaii+saltos es casi la misma, esto se debe a que las simulaciones fueron realizadas con los mismos escenarios, los cuales tienen el mismo patrón de movilidad, entonces no importa cual escenario se utilice, ya que los nodos siempre van a realizar los mismos movimientos. En otras palabras, la métrica relacionada con el número de traspasos es independiente del protocolo de enrutamiento, pero si está relacionada con el algoritmo utilizado para la selección del enrutador de acceso con el que se asocia cada uno de los nodos móviles.

V.4.3 Escenario 2

Este escenario de simulación consiste de 30 nodos móviles moviéndose a diferentes velocidades: 1,2,4 m/s con un tiempo de pausa de 0 segundos en un área de 100 x 100 metros. Este escenario de simulación tiene las mismas características que el escenario anterior como se muestra en la figura 52, pero se evalúa el desempeño del algoritmo con 30 nodos móviles y también se varía la carga de la red (2 y 12 conexiones CBR). Los parámetros utilizados en esta simulación se muestran en la tabla VI. El desempeño de la red es medida en función a la velocidad a la que se mueven los nodos móviles.

Tabla VI. Parámetros de simulación del escenario 2.

Parámetro	*Valor*
Protocolo de transporte	UDP
Tipo de Tráfico	CBR
Control de Acceso al medio	CSMA/CA
Modelo de Canal Radio	Dos Rayos
Modelo de Movilidad	Random Waypoint
Modulación	DSSS
Tasa máxima de transmisión	2 Mbps
Número de simulaciones realizadas	100
Area de Simulación	1000 x 1000 m
Número de nodos móviles	**30 nodos**
Velocidad Promedio	1,2 y 4 m/s
Tiempo de Simulación	600 seg
Número de conexiones para 30 nodos	**2,12**
Tamaño del paquete	1000 bytes
Generador CBR intervalo de envío de ptes	0.2 seg (5 ptes/s)
Tasa de transmisión	40 Kbps
Tiempo de conexión CBR	299.5 seg

Se puede observar que el número de conexiones cambia porque el número de nodos móviles aumentó.

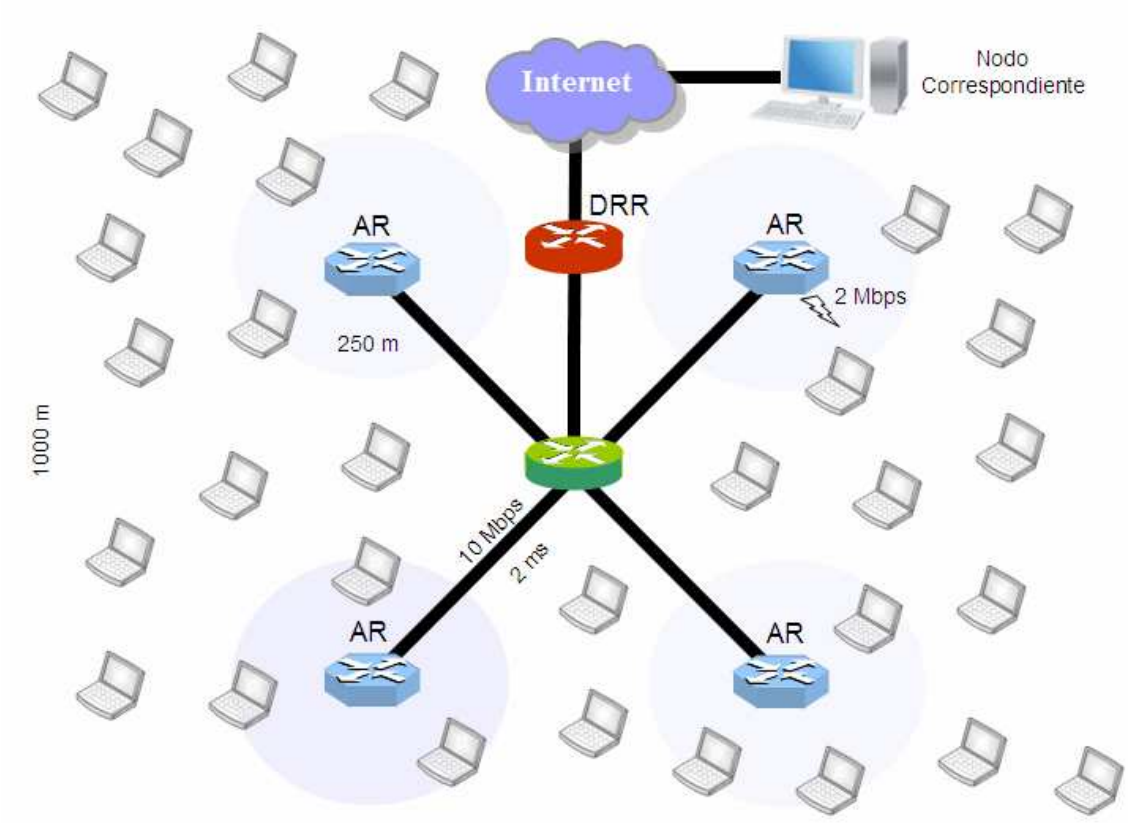


Figura 52. Escenario de simulación con 30 nodos móviles**.**

V.4.4 Resultados de Simulación

a) Simulación con 30 nodos móviles y baja carga de tráfico (10% de los nodos comunicándose)

En esta simulación se comunican aleatoriamente cuatro nodos móviles de la red ad hoc (dos conexiones) y el número de paquetes enviados durante una simulación es de 2995.

Paquetes transmitidos = 5 ptes/s x 299.5 seg x 2 conexiones CBR = 2995 paquetes

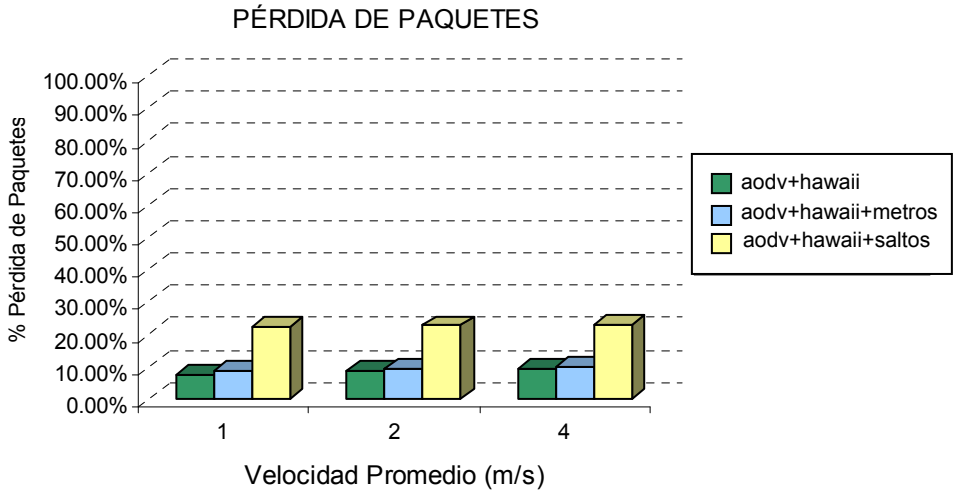


Figura 53. Gráfica de la pérdida de paquetes con baja carga de tráfico.

En la figura 53 se muestra el porcentaje de pérdida de paquetes de dos conexiones CBR en función de la velocidad promedio de los nodos móviles. Se puede observar que conforme aumenta la velocidad de los nodos, la pérdida de paquetes aumenta, en este caso, aodv+hawaii tiene un ligero mejor desempeño que aodv+hawaii+metros, esto se debe a que al haber mayor número de nodos, hay mayor probabilidad de encontrar una ruta por medio de enlaces inalámbricos, por otro lado, el que tiene mayor pérdida de los tres casos es aodv+hawaii+saltos. Comparando los resultados de pérdida de paquetes que se muestran en la figura 42 con los obtenidos en esta gráfica, se puede observar que aodv+hawaii tiene menor pérdida de paquetes que cuando se utiliza una sola conexión, por su parte aodv+hawaii+saltos y aodv+hawaii+metros tiene una mayor pérdida de paquetes. En particular aodv+hawaii+saltos puede tener el peor desempeño debido a que no se asocia al

enrutador de acceso más cercano, porque no distingue con exactitud en donde se encuentran los enrutadores de acceso.

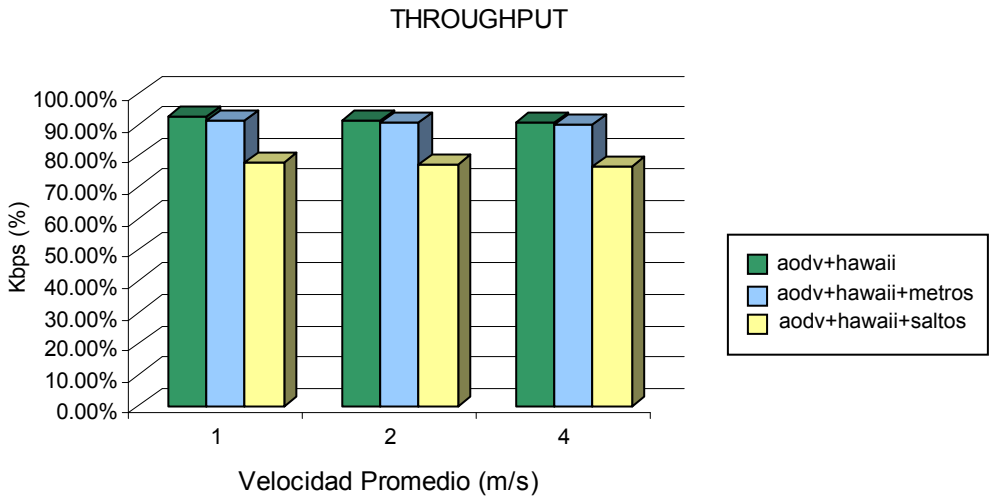


Figura 54. Gráfica del throughput con baja carga de tráfico.

En la figura 54 se muestra la gráfica del promedio del caudal eficaz (throughput) normalizado de dos conexiones CBR en función de la velocidad promedio de los nodos móviles. Se observa que en cualquiera de los tres casos, el throughput disminuye conforme aumenta la velocidad de los nodos, esto es porque a velocidades mayores hay mayor pérdida de paquetes, por lo tanto se reciben menos paquetes. También se puede ver que aodv+hawaii y aodv+hawaii+metros tienen mayor throughput que aodv+hawaii+saltos porque tienen menor pérdida de paquetes. Comparando los resultados obtenidos en la gráfica 43, se puede ver que el caudal eficaz para aodv+hawaii, aodv+hawaii+metros y aodv+hawaii+saltos aumenta.

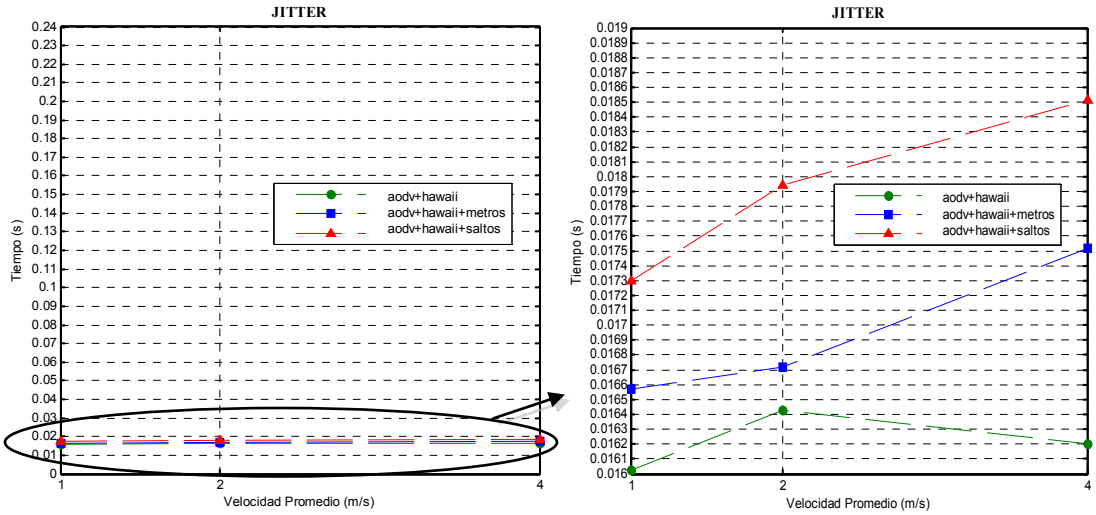


Figura 55. Gráfica del jitter con baja carga de tráfico.

En las figuras 55 y 56 se muestra la gráfica del jitter y retardo, respectivamente, de dos conexiones CBR en función de la velocidad promedio de los nodos móviles. Estas figuras tienen un acercamiento para observar mejor su comportamiento. Se puede observar que en los tres casos simulados, el jitter y el retardo se incrementan conforme aumenta la velocidad de los nodos móviles. El retardo y jitter de aodv+hawaii+saltos es mayor que en aodv+hawaii+metros y en aodv+hawaii. Se puede ver que aodv+hawaii es el que tiene menor jitter y retardo pero los valores obtenidos en la simulación son ligeramente menores en comparación a aodv+hawaii+metros, esto se debe a que los nodos móviles que se encuentran a más de un salto de un enrutador de acceso y se quieren asociar a él, necesitan realizar un proceso de descubrimiento de ruta para encontrar una ruta hacia ese enrutador de acceso, provocando un retardo. Comparando los resultados obtenidos con la gráfica 44, se observa que el retardo y jitter aumenta en todos los casos.

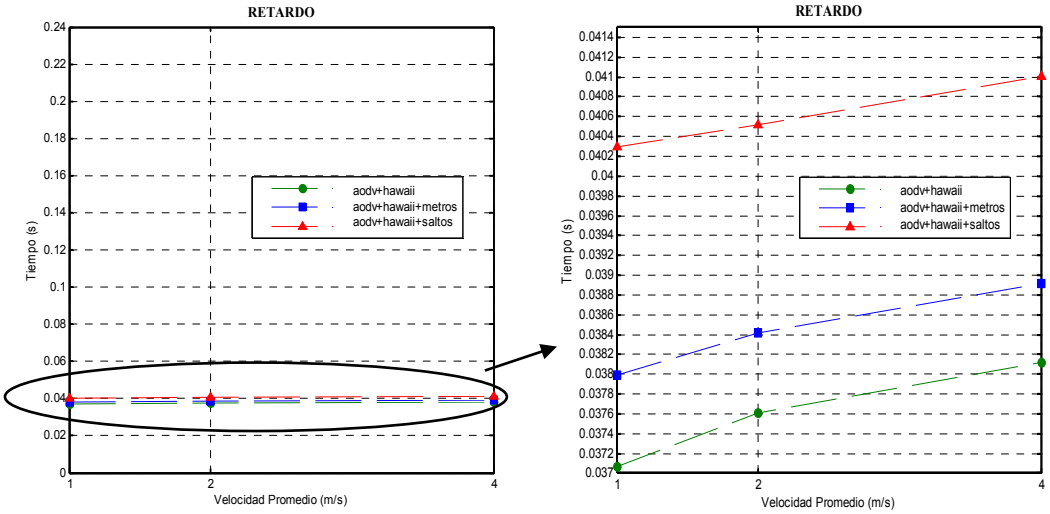


Figura 56. Gráfica del retardo con baja carga de tráfico.

b) Simulación con 30 nodos móviles y alta carga de tráfico (80% de los nodos comunicándose)

En esta simulación se comunican aleatoriamente veinticuatro nodos móviles de la red ad hoc (doce conexiones) y el número de paquetes enviados durante una simulación es de 17970.

Paquetes transmitidos = 5 ptes/s x 299.5 seg x 12 conexiones CBR = 17970 paquetes

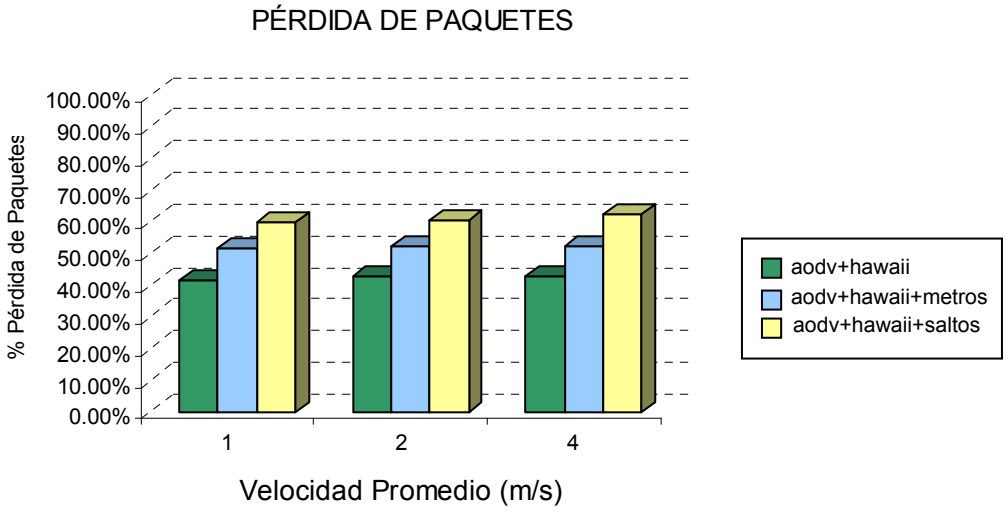


Figura 57. Gráfica de la pérdida de paquetes con alta carga de tráfico.

En la figura 57 se muestra la pérdida de paquetes de doce conexiones CBR en función de la velocidad promedio con que se mueven los nodos móviles. En esta simulación la diferencia de pérdida de paquetes entre aodv+hawaii y aodv+hawaii+metros es mayor que cuando se utilizan sólo dos conexiones, como se mostró en la figura 53. De los tres casos simulados, el que presenta el mejor desempeño es el de aodv+hawaii, esto se debe a que al aumentar el número de nodos, existe la probabilidad de encontrar rutas más rápido por la parte inalámbrica y tiene mayor número de posibles rutas para elegir la mejor para enviar datos.

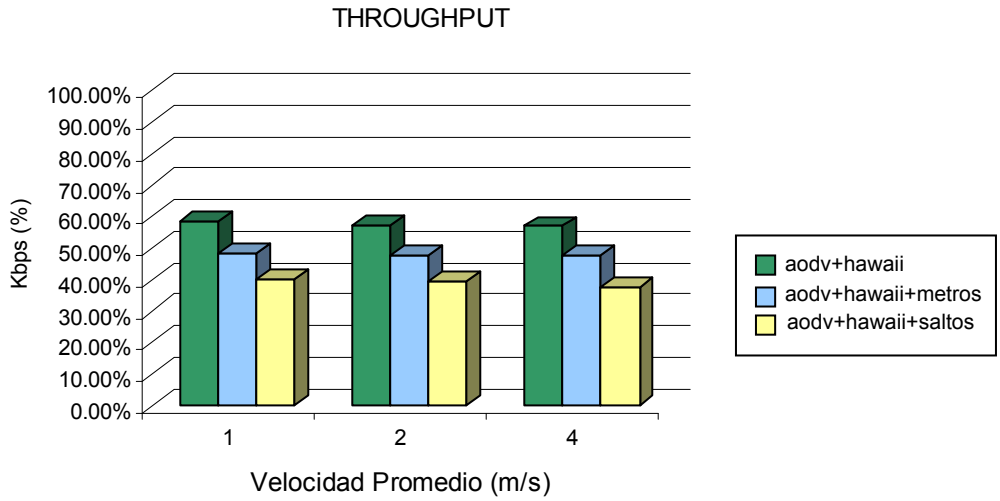


Figura 58. Gráfica del throughput con alta carga de tráfico.

En la figura 58 se muestra la gráfica del promedio del caudal eficaz (throughput) de doce conexiones CBR en función de la velocidad promedio de los nodos móviles. Se observa que en cualquier caso, conforme aumenta la velocidad promedio de los nodos, el throughput disminuye. En este escenario, aodv+hawaii tiene el mayor caudal eficaz porque es el que tiene menor pérdida de paquetes, sin embargo, el caudal eficaz no era tan bueno para el escenario donde se usan dos conexiones. Por su parte aodv+hawaii+metros tiene mayor throughput que aodv+hawaii+saltos porque se pierden menos paquetes.

Cuando se usa aodv+hawaii+metros y aodv+hawaii+saltos, los nodos móviles pueden depender de otros nodos intermedios para asociarse a un enrutador de acceso, entonces si se mueve un nodo intermedio se puede romper la ruta entre el nodo móvil y su enrutador de acceso lo que provoca que se tenga que realizar otro proceso de descubrimiento de ruta, en

cambio, cuando se utiliza, aodv+hawaii, los nodos móviles siempre se encuentran a un sólo salto del enrutador de acceso, es decir, se encuentran dentro del área de cobertura, entonces se asocian directamente al enrutador de acceso, sin utilizar nodos intermedios que se estén moviendo y que provoquen que las rutas se rompan.

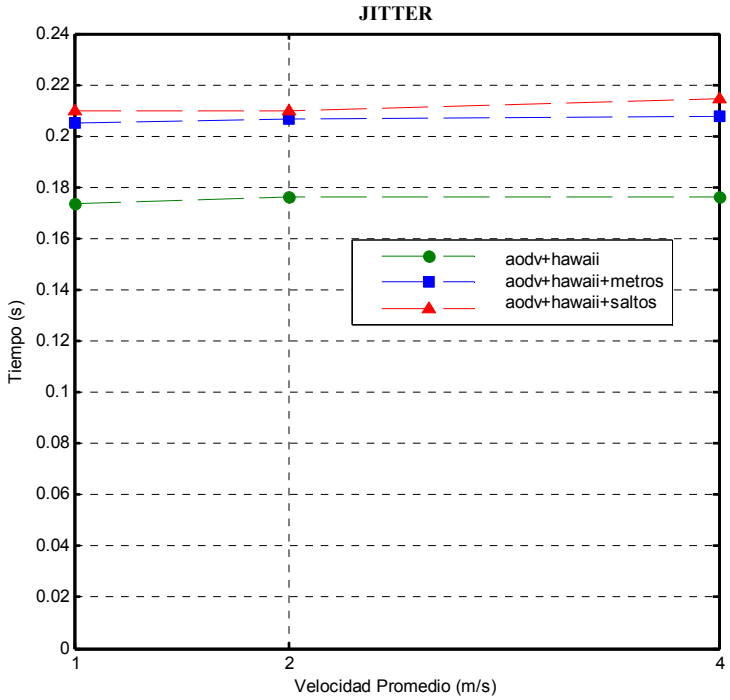


Figura 59. Gráfica del jitter con alta carga de tráfico.

En las figuras 59 y 60 se muestran las gráficas del jitter y retardo de doce conexiones CBR, respectivamente. Se observa que el jitter y el retardo aumentan conforme aumenta la velocidad de los nodos móviles. Los valores de jitter y retardo son mayores que los obtenidos cuando se usan dos conexiones, porque se suman los retardos de todas las conexiones CBR que participan en la simulación. El caso de aodv+hawaii es el que tiene menor jitter y retardo en comparación a los otros dos casos; Por otro lado,

aodv+hawaii+saltos es el que presenta el mayor retardo y jitter. Cuando se toma en cuenta la distancia en metros y en número de saltos para asociarse al enrutador de acceso más cercano, se tiene mayor pérdida de paquetes, jitter y retardo que con aodv+hawaii, esto se debe a que al aumentar el número de nodos, también aumenta el número de retransmisiones de mensajes de control de aodv y mayor retransmisión de avisos de enrutador (los nodos móviles que están a un salto retransmiten los avisos de enrutador a los nodos vecinos), esto provoca que los nodos procesen más mensajes y se tarden, haciendo que la red se sature de mensajes. Además, cuando los nodos móviles que están a más de un salto reciben los avisos de enrutador porque se los retransmitieron los nodos vecinos, envían un mensaje de petición de registro al enrutador de acceso que envió el aviso, para hacerlo, los nodos tienen que realizar un proceso de descubrimiento de ruta AODV para encontrar una ruta hacia ese enrutador de acceso, esto provoca que se envíen más peticiones de ruta. Por otro lado, como se mencionó anteriormente, cuando un nodo móvil que se encuentra a más de un salto de un enrutador de acceso y se quiere asociar a ese enrutador, necesita realizar un proceso de descubrimiento de ruta, para encontrar una ruta hacia ese enrutador , entonces, esto provoca un mayor retardo.

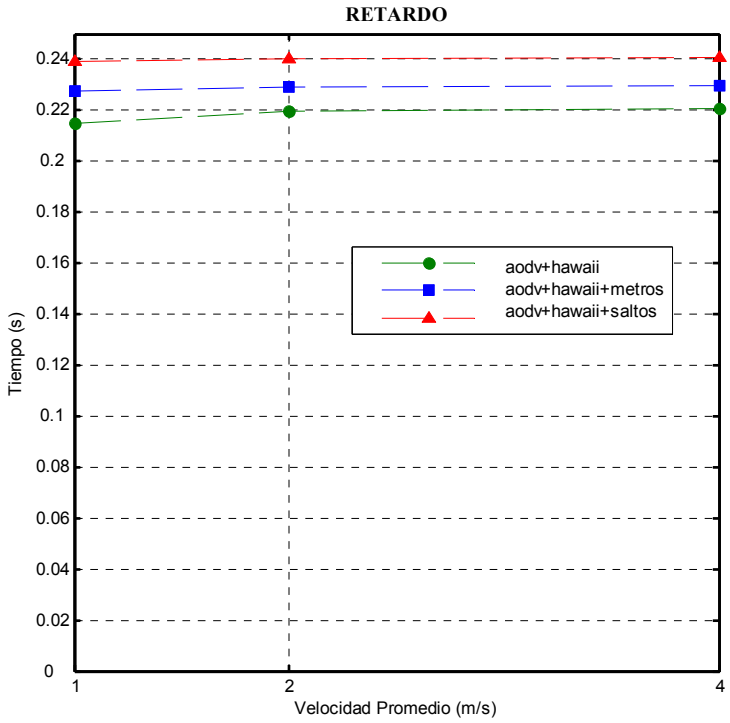


Figura 60. Gráfica del retardo con alta carga de tráfico.

En la tabla VII se muestran los valores obtenidos en los escenarios de simulación que se presentan en esta sección y se observa que en cualquier esquema de simulación (aodv+hawaii+metros, aodv+hawaii+saltos y aodv+hawaii) tanto en baja carga como en alta carga, conforme aumenta la velocidad promedio de los nodos móviles, la pérdida de paquetes, el jitter y el retardo incrementa, mientras que el throughput disminuye. Además, cuando aumenta la carga de tráfico, es decir cuando se incrementa el número de sesiones de comunicación activas, también aumenta la pérdida de paquetes.

En general se observa que al aumentar el número de nodos, y la carga de tráfico, se pierde un mayor número de paquetes, pero se observa que el mecanismo que tiene mayor pérdida es aodv+hawaii+saltos, esto se puede deber a que cuando los nodos se asocian al enrutador tomando en cuenta sólo el número de saltos, se tiene una menor exactitud de donde se encuentra el enrutador de acceso más cercano, porque el área de cobertura de un enrutador es de 250 m y mientras el nodo esté dentro de esa área se considera que está a 1 salto, entonces cuando el nodo tenga que elegir asociarse entre dos enrutadores que están a un salto, por ejemplo un AR ubicado a 30 m y otro a 200 m del nodo móvil , el nodo podría asociarse a un enrutador más lejano pensando que los dos tienen la misma distancia en número de saltos. En este último ejemplo, si el nodo se asocia al enrutador de acceso que se encuentra a 200 m puede suceder que pierda rápidamente la comunicación con éste si el nodo móvil se aleja del AR. En la figura 61 se muestra el escenario de simulación utilizado en ns-2 para obtener los resultados con 30 nodos móviles.

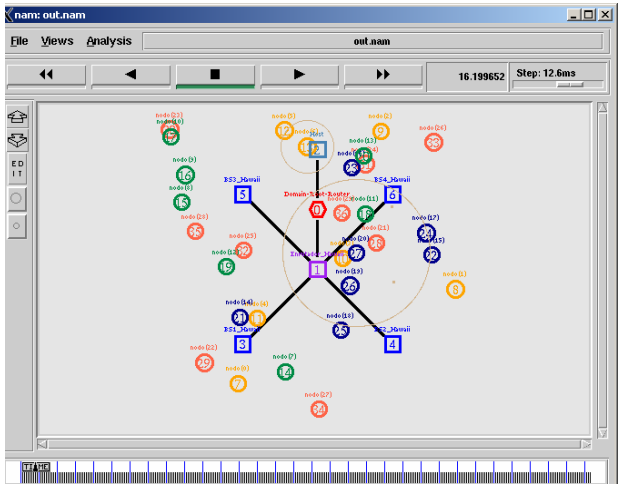
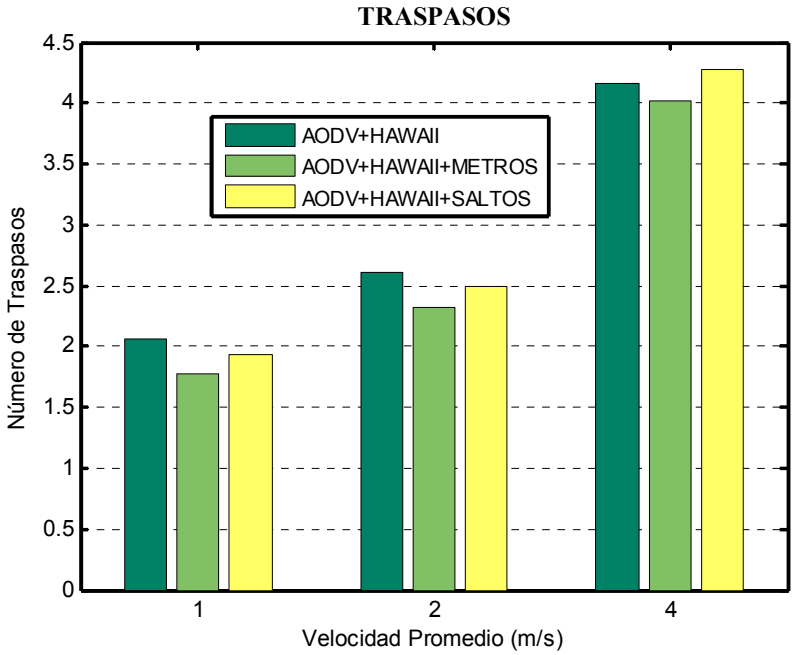


Figura 61. Escenario de simulación con 30 nodos móviles.

Tabla VII. Comparación de los parámetros de desempeño con alta y baja carga de tráfico para 30 nodos móviles.

30 Nodos		aodv+hawaii			aodv+hawaii+metros			aodv+hawaii+saltos		
Velocidad (m/s)		1	2	4	1	2	4	1	2	4
Baja Carga (10%)	Pérdida de ptes	233.47 (7.79%)	260.09 (8.68%)	291.04 (9.71%)	258.59 (8.63%)	280.9 (9.38%)	305.07 (10.18%)	670.17 (22.3%)	682.56 (22.78%)	698.11 (23.30%)
	Throughput	73.79 (92.24%)	73.079 (91.35%)	72.25 (90.32%)	73.1194 (91.40%)	72.52 (90.65%)	71.87 (89.85%)	62.12 (77.6%)	61.78 (77.23%)	61.36 (76.70%)
	Retardo	0.037068	0.03761	0.03812	0.037989	0.038413	0.038915	0.04029	0.040513	0.04101
	Jitter	0.016026	0.016425	0.016201	0.01657	0.016718	0.017518	0.01729	0.017945	0.018513
Alta Carga (80%)	Pérdida de ptes	7481.83 (41.62%)	7644.25 (42.52%)	7738.94 (43.05%)	9252.45 (51.47%)	9354.14 (52.04%)	9411.27 (52.35%)	10749.3 (59.8%)	10900.79 (60.64%)	11198 (62.30%)
	Throughput	280.3117 (58.40%)	275.97 (57.49%)	273.444 (56.97%)	233.0163 (48.55%)	230.7544 (48.07%)	228.8456 (47.68%)	193.03(40 .2%)	188.9872 (39.37%)	181.0270 (37.71%)
	Retardo	0.215108	0.219709	0.220739	0.227411	0.22901	0.229573	0.2391	0.24002	0.2408
	Jitter	0.173655	0.175952	0.176284	0.205096	0.20657	0.207768	0.20989	0.210037	0.214335



	Aodv+Hawaii			Aodv+Hawaii+Metros			Aodv+Hawaii+Saltos		
Velocidad (m/s)	1	2	4	1	2	4	1	2	4
30 nodos	2.05	2.60	4.15	1.77	2.31	4.01	1.927	2.49	4.274

Figura 62. Número de traspasos promedio de 30 nodos móviles.

En la figura 62 se muestra el número de traspasos promedio de 30 nodos móviles en función de la velocidad con que se mueven los nodos móviles. Se puede observar que en cualquiera de los casos, el número de traspasos incrementa conforme la velocidad promedio del nodo aumenta, esto se debe a que cuando los nodos se mueven más rápido tienen mayor probabilidad de desasociarse y volverse a asociar con otros enrutadores. Además, la diferencia entre el número de traspasos para cualquier caso en todas las velocidades es muy baja, por ejemplo, para 1 m/s, el número de traspasos es 2.05, 1.77 y 1.9227, esto se debe a que los escenarios usados en las simulaciones tienen el mismo patrón de movilidad, provocando que los nodos realicen los mismos movimientos.

Capítulo VI.

CONCLUSIONES

VI.1 Conclusiones

Para combatir las limitaciones de las redes inalámbricas de infraestructura y proveer conectividad hacia Internet a las redes ad hoc, se pueden utilizar redes híbridas que permitan soportar diferentes tipos de aplicaciones. Para tal efecto, es importante lograr la interoperabilidad entre los protocolos de capa 3 que son comúnmente utilizados en redes cableadas e inalámbricas.

En relación a los protocolos de micromovilidad y los protocolos de enrutamiento ad hoc, estos pueden trabajar juntos en las redes híbridas inalámbricas para encontrar una ruta disponible por medio de nodos móviles vecinos, establecer rutas multisaltos hacia enrutadores de acceso, y lograr la conectividad hacia Internet.

Este trabajo de tesis se basa en la integración de una red de infraestructura cableada y una red ad hoc para formar una red híbrida inalámbrica. Para lograr dicha integración se utiliza el protocolo de micromovilidad HAWAII para darle conectividad a los nodos móviles hacia Internet y manejar los traspasos que realicen de un enrutador a otro en un mismo dominio administrativo, por otro lado, el protocolo de enrutamiento AODV se utiliza para la comunicación de los nodos móviles dentro de la red ad hoc. La red híbrida inalámbrica está

compuesta de nodos móviles y enrutadores de acceso que trabajan como terminales móviles (i.e. implementan el protocolo AODV en la interfaz de red inalámbrica), para incrementar la flexibilidad y la movilidad de los usuarios.

El protocolo HAWAII puede trabajar con IP Móvil para soportar la movilidad de los usuarios en un área amplia. Tiene la ventaja de tener menor sobrecarga de señalización que otros protocolos debido a la eliminación de registros necesarios entre nodos móviles y agentes de casa posiblemente distantes, mientras los nodos móviles se mantienen realizando traspasos dentro de un dominio administrativo foráneo. Además, los esquemas de actualización dentro del dominio administrativo local mantienen mensajes de actualización de ruta de los enrutadores de acceso cercanos pero no del gateway, y esto también contribuye a una menor sobrecarga de señalización.

Por su parte, el protocolo AODV tiene la ventaja de crear rutas sólo en demanda, lo cual reduce en gran medida la sobrecarga asociada con los mensajes de control que se envían periódicamente en comparación a los protocolos de enrutamiento proactivos, pero su desventaja es que tiene un retardo en el establecimiento de rutas cuando se necesita una, porque AODV almacena los paquetes mientras se descubren nuevas rutas y estos paquetes son enviados sólo cuando se establece la ruta deseada. Esto provoca que haya menor caudal eficaz (throughput) en escenarios con alta movilidad, porque los paquetes se pierden rápidamente debido a la selección de rutas inestable.

El algoritmo propuesto en este trabajo de tesis comprende la integración de los protocolos AODV y HAWAII (aodv+hawaii) con dos modos de operación diferente:

1. Los nodos móviles se pueden asociar al enrutador de acceso más cercano midiendo la distancia en metros.
2. Los nodos móviles se pueden asociar al enrutador de acceso más cercano midiendo la distancia en número de saltos.

Estos modos de operación fueron comparados con la integración de AODV y HAWAII sin retransmisión de avisos, ni transmisión de mensajes AODV realizado por los enrutadores y sin que los nodos móviles se asociaran al enrutador de acceso más cercano. El desempeño del algoritmo fue comparado en términos de caudal eficaz, pérdida de paquetes, jitter, retardo y número de traspasos.

Se simularon y evaluaron dos escenarios con baja y alta carga de tráfico, en donde se utilizaron 10 y 30 nodos móviles. Los resultados demuestran que el algoritmo propuesto funciona mejor en alta y baja carga de tráfico utilizando los dos modos de operación, en escenarios donde se tiene una baja densidad de nodos en la red inalámbrica.

También se demuestra que el desempeño es mejor cuando los nodos móviles se asocian al enrutador de acceso más cercano midiendo la distancia en metros que cuando se mide la distancia que hay entre ellos en número de saltos. Cuando se aumenta el número de nodos, funciona mejor AODV+HAWAII que el algoritmo propuesto en sus dos modos de

operación (saltos y metros), esto se debe a que se envía un menor número de mensajes de petición porque los avisos de enrutador no se retransmiten y los nodos móviles siempre se encuentran a un salto para asociarse a los enrutadores de acceso, es decir, no dependen de nodos móviles intermedios que se puedan mover, para asociarse a los enrutadores de acceso. Para el caso de *aodv+hawaii+metros*, si se contara con información geográfica se podría utilizar algún algoritmo de enrutamiento geográfico como LAR (Location-Aided Routing), en el cual la información de localización puede ser obtenida usando un GPS (Sistema de Posicionamiento Global).

VI.2 Aportaciones

La mayoría de los trabajos que están relacionados con el enrutamiento en redes híbridas tienen el objetivo de darle conectividad a los nodos móviles hacia Internet y no le dan mucha importancia a la comunicación entre los nodos móviles de la red ad hoc, la cual es realizada utilizando un protocolo de enrutamiento.

Este trabajo se enfoca en proporcionar a los nodos móviles la mejor ruta considerando enlaces en la parte cableada y la parte inalámbrica. Esto fue posible al realizar ligeras modificaciones en el protocolo de enrutamiento AODV, por ejemplo, los enrutadores de acceso mandan los mensajes de petición utilizados en AODV (i.e. RREQ) en la parte cableada, acelerando la difusión de estos mensajes para encontrar una ruta, considerando la mejor ruta la que tiene el menor número de saltos.

Una de las aportaciones de este trabajo de tesis es el mecanismo de enrutamiento propuesto que integra el protocolo AODV con el protocolo HAWAII, para lograr dicha integración fue necesario modificar el protocolo AODV, con el fin de que los nodos móviles entendieran los mensajes MIP. Por otro lado, también se modificó este protocolo para que los enrutadores de acceso fueran capaces de entender los mensajes de AODV y los retransmitan a los demás enrutadores de acceso que se encuentren en la red para acelerar la difusión de dichos mensajes. También, se modificó el protocolo IP Móvil para que los nodos móviles se asocien al enrutador de acceso más cercano y además retransmitan los avisos de enrutador a los nodos móviles que se encuentren a más de un salto.

Otra aportación es la implementación del mecanismo propuesto dentro del simulador ns-2, para lograrlo fue necesario modificar la extensión del protocolo HAWAII en ns-2 para que trabajara con una versión más actual del simulador. Además, se realizó un programa en lenguaje tcl para generar conexiones aleatorias en donde no se repitiera el nodo receptor o el nodo transmisor, tomando en cuenta el número de nodos móviles y si se requiere alta o baja carga de tráfico. También, otra aportación sería la evaluación del desempeño del mecanismo propuesto bajo diferentes escenarios, con alta y baja carga de tráfico, demostrando sus ventajas y desventajas.

VI.3 Trabajo Futuro

Como trabajo futuro se pretende mejorar el algoritmo de enrutamiento propuesto para mejorar su desempeño y los resultados obtenidos. Por ejemplo, cuando los nodos móviles

de la red ad hoc están a más de un salto del enrutador de acceso y reciben un *aviso de enrutador* transmitido por otro nodo móvil, el algoritmo actual procede a realizar un proceso de *descubrimiento de ruta* para encontrar una ruta hacia el enrutador de acceso que generó el aviso. Una posible mejora sería considerar como siguiente salto hacia el enrutador de acceso al nodo móvil que retransmite el mensaje, de esta forma se enviará la petición de registro MIP al nodo móvil que está al siguiente salto o al nodo móvil que le retransmitió el aviso, reduciendo de esta forma la latencia asociada con el procedimiento de descubrimiento de ruta hacia el enrutador de acceso.

También se propone incluir el uso de algún protocolo multicast para enviar los mensajes RREQ a los diferentes AR, ya que enviar el mensaje de manera "unicast" a cada uno de ellos puede resultar ineficiente y costoso, implementar el balanceo de carga en los enrutadores de acceso para que no se saturen cuando haya muchos nodos móviles asociados a ellos, así como realizar pruebas con diferentes protocolos de micromovilidad como IP Móvil jerárquico e IP Celular y diferentes protocolos de enrutamiento como DSDV, cambiar la topología de la red, el número de fuentes de tráfico, el número de paquetes enviados por segundo, el tamaño de paquetes de datos, el número de enrutadores de acceso y la distancia que hay entre ellos, realizar sesiones de tráfico hacia Internet mezcladas con sesiones entre nodos móviles dentro de la red ad hoc y utilizar otras métricas para evaluar el desempeño del algoritmo como *conteo de saltos* para medir el número de saltos que hay en los enlaces cableados e inalámbricos.

Referencias

Aad, I., Castellucia, C. 2001. **"Differentiation mechanisms for IEEE 802.11"**. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. 1: 209-218 p.

Altman, E., y Jimenez, T. 2003. **"NS Simulator for beginners"**. Lecture Notes. 142 p.

Ammari, H. y El-Rewini, H. 2004. ***"Performance evaluation of hybrid environments with mobile gateways"***. Proceedings ISCC Ninth International Symposium. Texas, USA. Julio, 2004. 1: 152 - 157 p.

Benzaid, M., Minet, P., y Agha, K. Al. 2002. **"Integrating fast mobility in the OLSR routing protocol"**. IEEE Communications Society. 217-221 p.

Boppana, R.V., Zheng, Zhi. 2004. **"Designing Ad Hoc Networks with Limited Infrastructure Support"**. IEEE 2: 7-12 p.

Broch, J., Maltz, D., Johnson, D., Hu, Y., Jetcheva, J. 1998.**"A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols"**.Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking. Texas, USA. Octubre, 1998. 85-97 p.

Broch, J., Maltz, D.A., Johnson, D.B. 1999. **"Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks"**. Proceedings of the Workshop on Mobile Computing held in conjunction with the International Symposium on Parallel Architectures, Algorithms, and Networks, IEEE. Australia. Junio, 1999. 370–375 p.

Campbell, A.T, Gomez, J. y Valko, A.G. 1999. **"An Overview of Cellular IP "**. IEEE WCNC. LA, USA. Septiembre, 1999. 2: 606-610 p.

Campbell, A., Castellanos, J.G, Kim, S., Valko, A., Wan, C.Y, Turanyi, Z. 2000. **"Design, implementation, and evaluation of cellular IP"**. IEEE Personal Communications. 7(4):42-49 p.

Campbell, A.T., Gomez, J., Kim, S., Turanyi, Z., Wan, C-Y., Valko A. 2002. **"Comparison of IP Micro-Mobility Protocols"**. IEEE Wireless Communications Magazine, 9(1):72-82 p.

Campbell, A.T., Gomez, J., Kim, S., Turanyi, Z., Valko, A. G, Wan, C. Y. 2002. **"Internet micromobility"**. Journal of High Speed Networks, Special Issue on Multimedia in Wired and Wireless Environment. 11 (3-4): 177-198 p.

Chelius, G., y Fleury, E. 2003. **"Design of a hybrid routing architecture"**. IEEE International Conference on Mobile and Wireless Communications Networks. Singapur. Noviembre, 2003. 1-6 p.

Chung J., y Claypool, M. 1999. **"NS by Examples"**. WPI Worcester Polytechnic Institute. 48 p.

Elarag, H., Bassiouni, M. 2000. **"Simulation of transport protocols over wireless communication networks"**. Simulation Conference Proceedings. Orlando, Florida. Diciembre, 2000. 2: 1235-1241 p.

Fall, K. y Varadhan K. 2007. **"The ns manual"**. The VINT Project. http://www.isi.edu/nsnam/ns/. Octubre 2007. 417 p.

Gast, Matthew S. 2002. **"802.11 Wireless Networks: The Definitive Guide"**. Ed. O'Reilly & Associates Inc. USA. Segunda Edicion. 464 p.

Hamidian, A., Körner, U., Nilsson, A. 2004. **"Performance of Internet Access Solutions in Mobile Ad Hoc Networks"**. EuroNGI Workshop. Dagstuhl Castle, Alemania. Junio, 2004. 189-209 p.

Haverinen, H., Malinen, J. 2000. **"Mobile IP Regional Paging"**. draft-haverinen-mobileip-reg-paging-00.txt. Octubre, 2007. 16 p.

Hui, Tian., Fang, Xie., JianDong, Hu., Ping, Zhang. 2003. **"The channel adaptive routing for hybrid networks"**. ICCT International Conference on Communication Technology Proceedings. China. Abril, 2003. 2: 1266 – 1269 p.

Ilyas, Mohammad. 2003. **"The handbook of ad hoc wireless networks"**. Ed. CRC Press, Inc. Florida, USA. 560 p.

Jaiswal, S., Orvalho, J., Boavida, F. 2004. **"Handoff Mechanisms in Cellular IP: Enhancement into the Indirect Handoff Mechanism"**. The 5th European Wireless Conference, Mobile and Wireless Systems beyond 3G. Barcelona, España. Febrero, 2004. 1-7 p.

Johansson, P., Larsson, T., Hedman, N., Mielczarek, B., Degermark, M. 1999.**"Scenario-Based Performance Analysis of Routing Protocols for Mobile Ad-Hoc Networks"** *Proc. ACM/IEEE MOBICOM Conf*. Seattle, Washington. Agosto, 1999. 195-206 p.

Jonsson, U., Alriksson, F., Larsson, T., Johansson, P., Maguire, G. **"MIPMANET Mobile IP for Mobile Ad Hoc Networks"**. 2000. Mobile and Ad Hoc Networking and Computing (MobiHOC. 2000). Boston, USA. Agosto, 2000. 75 – 85 p.

Ke, Chih-Heng. 2005. **"How to measure packet loss rate, jitter, and end to end delay for UDP based applications"**. http://140.116.72.80/ ~smallko/ ns2/ tool_en.htm. Octubre 2007.

Kozat, Ulaş C., Tassiulas, Leandros. 2003. **"Throughput capacity of random ad hoc networks with infrastructure support"**. 9na. Conferencia Internacional anual de redes y computación. San Diego, CA. Septiembre, 2003. 55 – 65 p.

Lee, J., Toh, C.K., Gerla, M. 1999. **"Performance Evaluation of Table-Driven and On-Demand Ad Hoc Routing Protocols"** *Proc. IEEE Symp. Personal, Indoor and Mobile Radio Comm.* Osaka, Japón. Sept. 1999. 297-301 p,

Lee, J., Kim, G.Y., Park, S. 2002. **"Optimum UDP packet sizes in ad hoc networks"**. IEICE TRANSACTIONS on communications. E88-B (2): 815-820 p.

Mangues, Josep Bafalluy. 2004. **"IP Mobility: Macromobility**, **Micromobility, Quality of Service and Security"**. Upgrade Magazine. (The European Journal for the Informatics Professional). 5(1): 1-49 p.

Michalak, M., Braun, T. 2005. **"Common gateway architecture for mobile ad-hoc networks"**. Telscom Wireless On demand Network Systems and Services. Washington, DC. Enero, 2005. 70- 75 p.

Milanovic, N., Miroslaw M., Davidson, A., Milutinovic, V. 2004. **"Routing and Security in Mobile Ad Hoc Networks"**. IEEE Computer Society, 37(2): 61-65 p.

Miller, Matthew J., List, William D., Vaidya, Nitin H. 2003. ``**A Hybrid Network Implementation to Extend Infrastructure Reach"**. Reporte Técnico. 1-12 p.

Mukherjee, A., Bandyopadhyay, S., Saha, D. 2003. **"Location Management and Routing in Mobile Wireless Networks"**. Artech House. Norwood, Massachusetts. 69-113 p.

Nilsson, A., Hamidian, A. y Körner, U. 2004. **"Micro Mobility and Internet Access Performance for TCP connections in Ad hoc Networks"**. Nordic Teletraffic Seminar 17. Noruega. Agosto, 2004. 1-6 p.

Pack, S., Choi, Y. 2004. **"A Study on Performance of Hierarchical Mobile IPv6 in IP-based Cellular Networks"**. IEICE Transactions on Communications, E87-B. Japón. Marzo, 2004. (3): 462-469 p.

Perkins, C.E., Belding-Royer, E y Das, S.R. 2003. **"Ad hoc On-demand Distance Vector (AODV) routing"**. IETF RFC 3561. http://www.ietf.org/rfc/rfc3561.txt. Octubre 2007. 37 p.

Ramjee, R., La Porta, T., Thuel, S., Varadhan, K., Wang, S. 1999. **"HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks"**. IEEE International Conference on Network Protocols. USA. Noviembre, 1999. 10(3): 396-410 p.

Ramjee, R., La Porta, T., Thuel, S., Varadhan, K. 2000. **"IP Micromobility Support using HAWAII"**. IETF draft "draft-ietf-mobileip-hawaii-00.txt". Octubre 2007. 30 p.

Ros, F. y Ruiz P. 2004. **"Implementing a New Manet Unicast Routing"**. Dept. of Information and Communications Engineering. 35 p.

Royer E. y Toh C.K. 1999. **"A review of current routing protocols for ad hoc mobile wireless networks"**. IEEE Pers. Commun. 6(2): 46–55 p.

Saha, D. Mukherjee, A. Misra, I.S. Chakraborty, M. Subhash, N., 2004. **"Mobility support in IP: a survey of related protocols"**. IEEE Network. 18(6). 34-40 p.

Sessinghaus, M., Aust, S., Fikouras, N.A., Görg, C., Pampu, C. 2003. **"Hierarchical Mobile IP ns-2 Extensions for Mobile Ad Hoc Networks"**. Wireless Networks and Emerging Technologies. Canada. Julio, 2004.1-6 p.

Sosa, M. 2005. **"Simulación de fuentes TCP-RED en Ns-2"**. Tesis. Universidad de Los Andes, Venezuela. 42 p.

Stojmenovic, Ivan. 2002. **"Handbook of wireless networks and mobile computing"**. Capítulo 15 Mobile Ad hoc Networks. Ed. John Wiley & Sons, Inc., New York. 664 p.

Sun, Yuan y Belding-Royer Elizabeth M. 2003 **"Application-Oriented Routing in Hybrid Wireless Networks"**. IEEE ICC. USA. Mayo, 2003. 1: 502–506 p.

Talipo, E.A. 2005. **"Network Simulator Metrics"**. http://www-public.intevry.fr/~gauthier/ns2/doc/Metrics.pdf. Octubre 2007.

Tewari, H. O., Mahony, D., 2003. **"Real-time payments for mobile IP"**. Communications Magazine, IEEE. 41 (2): 126 – 136 p.

Typpo, V., Sukuvaara, T., Jurvansuu, M y Mahonen,P. 2003. **"Extending IP Micro-mobility to AODV based ad hoc networks"**. VTT Electronics and Univeristy of Oulu. 53-60 p.

Typpö, V. 2001. **"Micro-Mobility within Wireless Ad Hoc Networks: Towards Hybrid Wireless Multihop Networks"**. Tesis. Department of Electrical Engineering, University of Oulu, Finland. 73 p.

Valkó, A., Campbell, A.T., Gomez, J., Wan, C-Y., Kim, S., Turanyi, Z. 1999. **"Cellular IP"** Internet draft "draft-ietf-mobileip-cellularip-00.txt". Octubre 2007. 22 pp.

Vena, F., Cerdà, L., y Casals O. 2002. **"Study of the TCP Dynamics over Wireless Networks with Micromobility Support Using the Simulator"**. European Wireless. Italia. Febrero, 2002. 10 (1): 17-27 p.

Wiberg, B. 2002. **"Porting AODV-UU Implementation to ns-2"**. Tesis de maestría. Uppsala University. 95 p.

Wisely, D., Eardley, P., Burness, L. 2002. **"IP for 3G Networking Technologies for Mobile Communications"**. Ed. John Wiley & Sons, Inc., Inglaterra. 304 p.

Wu, E. H., Huang, Y., Chiang, J. 2001. **"Dynamic adaptive routing for heterogeneous wireless network"**. IEEE Conference on Global Telecommunications. USA. Noviembre, 2001. 6: 3608-3612 p.

Yoon, J., Liu, M., Noble, B. 2003. **"Random waypoint considered harmful"**. 21 Annual Joint Conference of IEEE Computer and Communications Societies. USA. Abril, 2003. 2: 1312-1321 p.

Yu, L., Min-hua, Y., Hui-min, Z. 2003. **"The handoff schemes in mobile IP"**. IEEE Vehicular Technology Conference. China. Abril, 2003.1:485- 489 p.