

# Router solar autoconfigurable para redes Mesh IEEE 802.11 de telemedicina rural en América Latina

Javier Simó<sup>1 y 4</sup>, Pablo Osuna<sup>1 y 2</sup>, Joaquín Seoane<sup>1 y 3</sup>, Andrés Martínez<sup>1 y 4</sup>

<sup>1</sup>Fundación EHAS. [jsimo@ehas.org](mailto:jsimo@ehas.org)

<sup>2</sup>Fundación Rafael Escolá. [pog@rafaelescola-fund.org](mailto:pog@rafaelescola-fund.org)

<sup>3</sup>Departamento de Ingeniería Telemática. Universidad Politécnica de Madrid. [jsp@dit.upm.es](mailto:jsp@dit.upm.es)

<sup>4</sup>Departamento de Teoría de la Señal y Comunicaciones. Universidad Rey Juan Carlos. [andres.martinez@urjc.es](mailto:andres.martinez@urjc.es)

## RESUMEN

La provisión de diferentes servicios de telemedicina (teleformación, teleconsulta, vigilancia epidemiológica, etc) en entornos rurales aislados requiere de la adaptación de las tecnologías existentes para lograr una solución de bajo costo. La Fundación EHAS, en colaboración con la Fundación Rafael Escolá, está desarrollando un router inalámbrico solar de bajo coste, autoconfigurable y de alta mantenibilidad, con soporte de QoS y capacidad para crear redes inalámbricas Wi-Fi de larga distancia y alta velocidad. Estas redes permiten el acceso a Internet y comunicación con la red telefónica básica a través de centralitas software de VoIP implementadas en los propios routers. El artículo presenta los trabajos de desarrollo del primer prototipo, su aplicación a la red Wi-Fi de Perú, y las fases de investigación actuales y futuras para un segundo prototipo.

## 1. INTRODUCCIÓN

La atención sanitaria en establecimientos de salud rurales de países en desarrollo suele ser muy deficiente debido a la falta de medios materiales, la insuficiente cualificación de los técnicos de salud y la incomunicación con el resto de la red de salud; todo ello da lugar a serias dificultades para prevenir las enfermedades, realizar diagnósticos y tratamientos adecuados o atender de forma debida las emergencias médicas.

Ante esta situación el Programa EHAS [1] apuesta por introducir sistemas de comunicación y telemedicina para el personal sanitario rural, de forma que permitan un mejor uso de los recursos ya existentes y una mejor coordinación del sistema completo de atención de salud. Las condiciones particulares de las regiones rurales suelen condicionar grandemente las tecnologías de comunicación que se pueden usar: la falta de recursos hace inapropiadas las redes de operador tales como la telefonía móvil, las infraestructuras cableadas y las redes satelitales; la inaccesibilidad de muchos lugares y la dispersión de la población sugiere el uso de tecnologías inalámbricas de largo alcance, y la falta de energía eléctrica y de técnicos cualificados también incide en qué tipo de tecnologías se pueden usar de forma sostenible. En EHAS se han empleado con éxito redes radio operando en las bandas HF y VHF, ampliamente utilizadas para las comunicaciones de voz semi-dúplex, y que pueden ser

aprovechadas también para comunicaciones de datos. No obstante, esta solución presenta algunos inconvenientes como la lentitud en la comunicación de datos, el alto consumo de los equipos, el alto coste de las instalaciones, la difícil adaptación a la red telefónica y el uso de frecuencias con licencia.

Una nueva línea de investigación abierta recientemente en EHAS se basa en la tecnología inalámbrica 802.11b. Dentro de esta tecnología, nuestro trabajo se ha centrado en las redes Mesh Wi-Fi, cuya popularidad cada vez es mayor. Este tipo de redes pueden definirse como redes que se forman de forma espontánea sin ninguna infraestructura, constituyendo mallas que conectan un cierto número de nodos entre sí, y en que cada nodo puede ser al mismo tiempo estación de trabajo de un usuario, servidor o encaminador.

Hemos evaluado este tipo de redes como una solución al contexto planteado por algunas de sus características:

- Basadas en una tecnología ampliamente conocida y popular: IEEE 802.11.
- Bajo coste, debido al uso de una tecnología popular y a la existencia del estándar Wi-Fi.
- Estructura descentralizada autoconfigurable. En zonas rurales aisladas, donde gran parte del tiempo puede emplearse en desplazamientos, resulta fundamental que la tecnología minimice la instalación, administración y el mantenimiento de la red.
- Alimentación e integración: a diferencia de otras tecnologías inalámbricas donde sus nodos exigen ingentes cantidades de energía, los nodos Mesh sólo necesitan de una mínima energía, dotándoles de autonomía con una energía natural como pueda ser la solar. Además el hardware Mesh es fácilmente integrable en un sistema impermeable que soporte condiciones meteorológicas adversas.
- Flexibilidad: un nodo puede adherirse a la red si puede ver a uno de los nodos vecinos. Las zonas rurales aisladas normalmente no siguen una distribución geométrica ordenada alrededor de un punto central.

La popularidad de este tipo de redes y el creciente interés suscitado por las comunicaciones móviles dieron lugar a la creación del grupo MANET (Mobile Ad-hoc

NETwork) por parte del IETF (Internet Engineering Task Force). Sin embargo nuestra área de trabajo se centra en estos momentos en las redes Mesh estáticas. Como veremos más adelante, muchas de las investigaciones que actualmente tienen lugar sobre las MANETs serán fácilmente aplicables a nuestro caso. En este artículo presentaremos el trabajo que nuestro grupo está realizando en el diseño de un router Mesh Wi-Fi que permita crear una red Mesh como sistema óptimo de telecomunicación para el entorno planteado anteriormente. Primero describiremos brevemente las componentes actuales del router que ya se está instalando en nuestra red. A continuación recogeremos algunas de las conclusiones técnicas que obtuvimos a partir de nuestra experiencia en la instalación de la red de Perú, con especial énfasis en los enlaces de larga distancia. Por último entraremos a valorar de forma más detallada aquellas mejoras funcionales de las que está siendo objeto nuestro router para adaptarse a un escenario rural aislado de un país en desarrollo.

Aunque existen trabajos similares, como la red Roofnet del MIT [2], el desarrollado por el grupo TIER de la Universidad de Berkeley [3] o el grupo Inveneo [4], ninguno ofrece una solución completa en cuanto a bajo consumo, autoconfigurabilidad, calidad de servicio y enrutamiento dinámico multisalto.

## 2. COMPONENTES DEL ROUTER ACTUAL

En un escenario rural aislado de un país en desarrollo encontramos las siguientes variables de contorno:

- Distancias largas de varias decenas de kilómetros.
- Inexistencia de una infraestructura de comunicaciones que permita desplazarse de forma rápida y accesible a los distintos puntos de la red.
- Ausencia de una instalación eléctrica en aquellas zonas rurales más aisladas, e inestabilidad de la misma en caso de existir.
- Escasez y alto coste de personal técnico cualificado.

Como solución de comunicaciones al entorno planteado el grupo EHAS ha trabajado en un router Mesh Wi-Fi, actualmente en su primera versión. Este router está siendo instalado en las redes Wi-Fi de Perú, Cuba y Colombia en el marco del Programa @LIS de la Unión Europea. En este apartado estudiaremos por separado el hardware y software de esta primera versión, dando cuenta de cuáles son las líneas de investigación que nos han llevado a seleccionar cada componente.

### 2.1. Hardware

- Subsistema informático, que por imperativos de consumo y tamaño se trata de un ordenador empotrado. Cuenta con los elementos mínimos para un sistema de comunicaciones y las interfaces apropiadas para su interconexión a los otros subsistemas. Además tiene un watchdog hardware que

le permite reiniciarse en situaciones inestables o de bloqueo. Para nuestro primer prototipo evaluamos dos posibilidades: WRAP y Soekris net4521, ambas de arquitectura x86. De prestaciones similares en potencia, finalmente se decidió escoger la placa Soekris por un doble motivo: disponibilidad de tres interfaces inalámbricas (frente a las dos de WRAP), y mejor robustez ante condiciones climáticas adversas.

- Subsistema wireless, responsable de la comunicación con el resto de la red y que consta de varios interfaces Wi-Fi, pigtailes, cables de baja atenuación y antenas de gran potencia y directividad. Estamos trabajando con tarjetas de dos chipsets diferentes, Intersil Prism II y Atheros, con modelos que transmiten desde 80mW hasta 400mW.

### 2.2. Software

El Sistema Operativo que hemos diseñado, pebble-EHAS, está basado en la minidistro Pebble y ocupa unos 77 MB. Cuenta con las herramientas de red necesarias para realizar enrutamiento (estático en la primera versión del prototipo), así como con servidores DHCP, DNS y NTP, y un watchdog software. Además al sistema operativo se le ha añadido la centralita software Asterisk de VoIP que posibilitará posteriormente en nuestras redes la descentralización de la conmutación de voz. Los controladores de las interfaces inalámbricas, Hostap y Madwifi, son los más que cuentan con una mayor estabilidad y madurez, además de permitir modificar ciertos parámetros que mejorarán las prestaciones en los enlaces de larga distancia.

## 3. PRUEBAS EN ENLACES DE LARGA DISTANCIA EN LA RED DE PERÚ

La familia de estándares IEEE 802.11 se diseñó con objeto de lograr redes de área local inalámbricas (WLAN), por lo que los protocolos están pensados para distancias de decenas o centenas de metros. No obstante, en EHAS hemos conseguido establecer enlaces Wi-Fi de varias decenas de kilómetros con un throughput aceptable. En redes para zonas rurales aisladas de países en desarrollo nos interesa especialmente sacar el máximo partido de esta tecnología en cuanto a mayor alcance y mejores prestaciones posibles, ya que esto redundaría directamente en una reducción del número de nodos que hacen falta para atravesar zonas deshabitadas y, frecuentemente, poco accesibles. Sin embargo, no hay trabajos de investigación que hayan permitido determinar con rigor cuáles son los límites de distancia de 802.11, ni cómo evolucionan las prestaciones de los enlaces en función de la distancia. De forma paralela a la instalación del primer prototipo del router en Perú pudimos realizar una serie de pruebas en enlaces de larga distancia 802.11 que nos permitieron aprender ciertas técnicas prácticas al mismo tiempo que corroborar algunos resultados teóricos. Abordaremos este tema desde tres niveles: el PHY (capa física de 802.11), el MAC (capa de enlace y control de acceso al medio de 802.11), y la arquitectura de red.



Figura 1: Instalación Wi-Fi en Josojahuarina (Perú)

### 3.1. Nivel físico

- Velocidad. El protocolo IEEE 802.11 recoge distintas velocidades según el modo de funcionamiento: 1, 2, 5.5 y 11 Mbps para 802.11b; 6, 9, 12, 18, 24, 36, 48 y 54 Mbps para 802.11a, y el conjunto de todas las anteriores para el modo 802.11g. Estos modos usan diferentes tipos de modulación y codificación, de forma que cuanto mayor sea la velocidad, mayor es la potencia necesaria en recepción para mantener un enlace con una BER (Bit Error Rate) baja. Esta potencia, llamada sensibilidad, va a obligarnos a usar velocidades bajas si queremos lograr enlaces de larga distancia con una cierta estabilidad. En una de las tarjetas que hemos empleado en estas pruebas, Ubiquity SR2 802.11b/g de 400mW, la diferencia de sensibilidad entre el modo b en 1 Mbps y el modo g en 6 Mbps es de sólo 3dB. Así, en los enlaces de 40km decidimos apostar por el modo g logrando unos resultados muy prometedores que se mostrarán después. Añadir también que en términos de estabilidad y prestaciones resulta mejor configurar la velocidad del canal a un valor fijo.
- Diversidad. Este concepto hace referencia a la existencia de más de una antena para mejorar la calidad de recepción/transmisión. Muchas tarjetas inalámbricas tienen dos conectores para antena exterior. Aunque una antena transmita por sólo uno de los conectores puede ocurrir perderse una pequeña potencia por el otro. En estas ocasiones resulta conveniente desactivar la diversidad y activar una única antena para transmisión/recepción. En las pruebas realizadas en laboratorio comprobamos pérdidas de hasta 2dBs en el caso de tarjetas de chipset Atheros, no observándose ninguna diferencia aparente en el caso de las de chipset Intersil Prism II.
- Potencia. Previa abstracción de otros factores, el caso de los enlaces de larga distancia en Wi-Fi se resume a conseguir un balance de enlace en que la potencia recibida sea suficientemente superior a la sensibilidad del receptor, teniendo en cuenta la potencia transmitida, las ganancias y las pérdidas del enlace. El problema es precisamente estimar las pérdidas de propagación, ya que las medidas reales no se ajustan

a la ecuación de Friis de pérdidas de propagación en el espacio libre. En las pruebas de campo hemos observado un desequilibrio claro (entre 15 y 25 dB) entre el nivel de potencia medido y el teórico. El modelo Longley-Rice, empleado por el software RadioMobile, también muestra unos resultados diferentes a los medidos. Actualmente estamos trabajando en el diseño de un modelo que a partir de los resultados prácticos obtenidos nos permita ajustar un modelo teórico y parametrizar el Longley-Rice para las distancias y terrenos en los que trabajamos.

- Otros aspectos que será necesario revisar en pruebas futuras son la influencia de los fenómenos meteorológicos, la polarización de las antenas y la influencia de la interferencia intersimbólica.

### 3.2. Nivel MAC

En el protocolo 802.11 todas las transmisiones de datos unicast son confirmadas por el receptor mediante ACKs; el transmisor esperará un tiempo máximo ACKTimeout después de transmitir para recibir la confirmación. Si la confirmación no llega, el transmisor tratará de realizar un determinado número de retransmisiones. Estos ACKs influyen de manera decisiva sobre los enlaces de larga distancia. Si el ACKTimeout es configurado con un valor demasiado pequeño, el transmisor nunca recibirá confirmaciones, realiza siempre el máximo número de retransmisiones, y en consecuencia el caudal se reduce de manera considerable. En el caso contrario, cuando el ACKTimeout es configurado con un valor demasiado alto, el transmisor esperará un tiempo demasiado largo antes de retransmitir en el caso de que el paquete o el ACK se hubieran perdido, revistiendo de nuevo sobre el throughput final.

Se han realizado varios trabajos de investigación [5][6] que tratan de modificar el nivel MAC de 802.11 para el caso particular de enlaces Wi-Fi de larga distancia. Muchos sólo han llegado a implementarse de manera comercial, siendo el protocolo nstreme de Mikrotik uno de los más destacados actualmente. Muchos de estos trabajos se basan en la idea de que determinados drivers pueden modificar parámetros como el ACKTimeout (no especificado por el estándar 802.11), la deshabilitación de ACKs o el ajuste o deshabilitación de retransmisiones.

Los dos drivers que utilizamos en Linux permiten modificar parámetros distintos.

- Madwifi. Este driver permite modificar el valor de ACKTimeout, CTTimeout y SLOT Time. Las tarjetas de chipset Atheros suelen contar con un ACKTimeout por defecto de 48µs, deficiente para distancias mayores a los 3km. En las pruebas que hemos realizado en campo hemos comprobado cómo mejorábamos sensiblemente las prestaciones del enlace al modificar estos parámetros.
- Hostap. En este caso no es posible modificar los valores anteriores. Sin embargo, las tarjetas de chipset Intersil Prism II tienen un ACKTimeout por defecto mayor que las de Atheros, de manera que

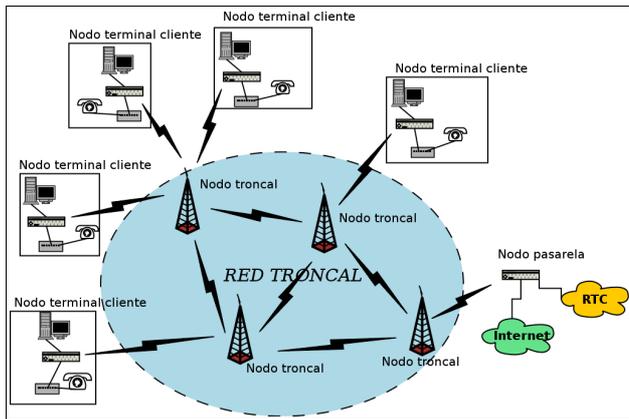


Figura 2: Arquitectura de la red Mesh

pueden ser usadas con prestaciones aceptables en enlaces largos de hasta 30km. Este driver permite un modo Ad-Hoc llamado Pseudo-Ibss en el que los ACKs han sido eliminados. En las pruebas que hemos realizado no hemos encontrado diferencias significativas con el modo Ad-Hoc tradicional en términos de throughput.

### 3.3. Arquitectura de red

La arquitectura propuesta consiste en una red Mesh en la que todos los nodos conmutan paquetes a nivel IP. Funcionalmente nos encontramos con tres tipos de nodos: el nodo pasarela, encargado de la conectividad externa con Internet y la RTC, el nodo troncal o repetidor, encargado de conmutar comunicaciones con otros nodos, y el nodo terminal o cliente, típicamente instalado en el Puesto de Salud al que da servicio. Aunque varían los equipos conectados a estos nodos, el diseño hardware/software que subyace debajo de ellos el mismo. Ver Figura 2.

Como se dijo en la introducción, es muy deseable usar redes Mesh en que los nodos puedan ser lo más autoconfigurables que se pueda, de forma que el personal para instalación y mantenimiento no tenga que hacer virtualmente ninguna operación de administración de redes. Esto supone que los nodos puedan descubrirse y enlazar adecuadamente de forma automática en cualquier situación. Claramente, esto es difícilmente conseguible con BSS (modo "infraestructura"), resultando en cambio teóricamente sencillo con IBSS (modo Ad-Hoc). No obstante, el cada vez más implementado modo WDS (Wireless Distribution System), que permite constituir por vía inalámbrica ESS (Extended Service Sets), está siendo usado por investigaciones muy recientes [7] para poder establecer enlaces AP-AP en redes mesh, lo cual rompería esta barrera.

En los drivers que estamos manejando en Linux, el funcionamiento del modo Ad-Hoc todavía no se puede considerar del todo estable. Así, mientras que en Hostap el funcionamiento de Ad-Hoc ha resultado satisfactorio en las pruebas realizadas, en Madwifi encontramos ciertos problemas relacionados la propia implementación del código y el particionado de red (dos nodos con idéntica configuración crean dos células distintas que no pueden

Rate	Cusco - Josojahuarina	Josojahuarina - Don Juan
1M	68.5	69.7
2M	119	110
5.5M	205	197
11M	368	350

Tabla 1: Throughput (Kbytes/s) en 802.11b con la SR2

Rate	Cusco - Josojahuarina	Josojahuarina - Don Juan
6M	275	266
9M	440	425
12M	500	499
18M	602	585
24M	759	721
36M	833	810
48M	184	-
54M	-	-

Tabla 2: Throughput (Kbytes/s) en 802.11g con la SR2

Rate	Master - Managed	Ad-Hoc	Pseudo - Ibss
1M	79.5	74	80.1
2M	159	152	153
5.5M	360	334	331
11M	553	341	506

Tabla 3: Throughput (Kbytes/s) en 802.11b con la Senao

verse) En las primeras instalaciones hemos usado la solución más estable, el modo infraestructura, a la espera de que el modo Ad-Hoc adquiera la suficiente madurez.

### 3.4. Resultados

Entre todas las pruebas en enlaces de larga distancia que realizamos en Perú nos interesa destacar dos escenarios diferentes según la longitud del enlace.

- Enlaces de 40km: Cusco – Josojahuarina y Josojahuarina – Don Juan. Realizamos pruebas en dos enlaces de 40km obteniendo resultados muy similares. La tarjeta que se empleó fue la Ubiquity SR2 b/g de 400mW. Se trataba de la primera vez que

establecíamos un enlace de larga distancia en modo g. Obtuvimos unas cifras bastante prometedoras (más de 6.5 Mbps) Será interesante realizar pruebas con mayor seguimiento en este modo y en 802.11a, a pesar de que ambos modos presentan sensibilidades peores que las de 802.11b. Los resultados mostrados en las tablas fueron obtenidos después de modificar algunos parámetros de la capa MAC. Sin estas modificaciones los resultados fueron muy deficientes. Comentar que el modo Ad-Hoc no funcionó en ninguna de las pruebas, por lo que todos los resultados recogidos aquí hacen referencia al modo infraestructura. Ver *Tabla 1* y *Tabla 2*.

- Enlace de 11km: Josojahuarina – Urpay. En esta ocasión la tarjeta empleada fue el modelo Senao 2511CD PLUS EXT2 200mW de driver Hostap. En la *Tabla 3* quedan recogidos los resultados para el modo infraestructura, Ad-Hoc y Ad-Hoc sin ACKs (Pseudo-Ibss). Los números muestran un comportamiento muy similar en los tres modos, ligeramente mejor en el modo infraestructura. El modo Ad-Hoc presentó un comportamiento estable, aunque será necesario realizar pruebas en un marco temporal mayor que permitan afianzar este resultado.

#### **4. MEJORAS FUNCIONALES: SEGUNDA VERSIÓN DEL ROUTER**

Las primeras pruebas realizadas en campo sobre la red de Perú han mostrado unos resultados satisfactorios en cuanto a estabilidad y prestaciones del primer prototipo del router. Sin embargo, aún existen ciertas mejoras funcionales que nuestro router deberá alcanzar si queremos que se adapte de forma completa a un escenario rural aislado. En los apartados siguientes desarrollaremos cuáles son estas mejoras, dando cuenta del trabajo desarrollado hasta ahora y de las tareas futuras.

##### **4.1. Autoconfiguración**

Para participar en una red IP cada nodo necesita ser configurado con una dirección IP, ya sea manualmente o de forma automática a través de un servidor DHCP. Sin embargo, el carácter dinámico y autoconfigurable de las redes Mesh convierten a estos mecanismos en una solución poco adecuada. Al no haber una infraestructura de red preexistente ni una jerarquía, cada nodo se tiene que atribuir una dirección IP autónomamente, normalmente de rango privado; esto supone que esa dirección IP no tiene porque tener una relación determinada con las de los nodos vecinos, por lo que no es modo alguno evidente asegurar su unicidad.

En IPv6 existen soluciones [8][9][10] que permiten obtener una dirección IP de forma automática en el ámbito de un único dominio multicast. Ese carácter local las hace inservibles para los nodos de una red Ad-Hoc, cuyas direcciones no guardan una relación determinada, y por tanto no comparten el mismo dominio. En IPv4 el grupo de trabajo Zeroconf ha implementado una solución similar a la de IPv6. A través de este proyecto, y de su

implementación en Linux zeip, un nodo se configura automáticamente con una dirección IPv4 de prefijo 169.254/16. Por razones similares a las de IPv6 estas direcciones son sólo válidas para la comunicación con otros nodos en el mismo enlace físico (o lógico).

El draft [11] presenta una panorámica de las soluciones que se han propuesto para el problema de la autoconfiguración en MANETs. Estas soluciones están siendo estudiadas por el grupo AUTOCONF, responsable de la estandarización de los mecanismos de autoconfiguración. Sin embargo aún nos encontramos lejos en el tiempo de una solución que venga a implementar el estándar que finalmente sea propuesto.

Algunas de las soluciones que se han planteado y estudiado para abordar el problema de la autoconfiguración a nivel IP son:

- En IPv4, aunque los nodos disponen de direcciones MAC de 48 bits, no se produce una relación de unicidad directa con una dirección IP de 32 bits. Una solución parcial pasaría por usar tarjetas del mismo fabricante, ya que estas cuentan con una parte variable que nos podría permitir establecer una dirección IP única. También podrían usarse direcciones privadas de forma secuencial a partir de un conjunto previamente definido.
- PACMAN [12], NOA-OLSR [13], LUNARng [14]. Son soluciones nacidas de investigaciones o proyectos puntuales que no tienen la suficiente madurez y estabilidad para ser usadas en nuestra red. Además están integradas en protocolos de enrutamiento dinámico que no incluyen una métrica basada en calidad de servicio o tienen otras limitaciones como el número de interfaces por nodo.
- Servidor DHCP. Haciendo uso de un servidor DHCP centralizado en un nodo de la red, se envían peticiones DHCP desde cualquier punto de la red a través de cadenas de repetidores DHCP (DHCP relays) o encapsuladas en un protocolo de encaminamiento. Esta solución es fuertemente dependiente de una estructura centralizada lo cual choca de frente con la filosofía de una red Ad-Hoc. Además exige que todos los enlaces al nodo DHCP se encuentren activos en todo momento.

##### **4.2. Encaminamiento dinámico multisalto**

Para la primera versión del router hemos configurado rutas estáticas a través del comando "route" de Linux. Esta solución resulta estable, sencilla de configurar y no añade tráfico de control de enrutamiento entre los nodos que componen la red. Sin embargo, se trata de una solución no autoconfigurable, lo cual obliga a disponer de un personal cualificado para realizar la administración de redes en su diseño inicial y posterior mantenimiento. Si queremos evitar esta situación deberemos optar por un protocolo dinámico multisalto. En las redes Mesh se han desarrollado muchos protocolos específicos que son capaces de encaminar paquetes entre nodos contiguos o no contiguos de la red, o entre cualquier nodo de la red y

el exterior a través de un nodo pasarela, y ello sin importar que cada nodo tenga una dirección IP completamente independiente de los otros. Algunos de estos protocolos han dado lugar a RFCs o a internet-drafts del IETF; otros surgen de artículos de investigación publicados o de desarrollos de la industria. Abundan los artículos de investigación que analizan y comparan las prestaciones de los distintos protocolos, entre ellos el más famoso es [15]. Una clasificación tradicional de estos protocolos los divide en: 1) Reactivos, en los que un nodo sólo intercambia información de control cuando quiere iniciar una comunicación con otro nodo. AODV [16] y DSR [17] son los más extendidos en esta categoría. 2) Proactivos, en los que los nodos intercambian información de forma periódica para aprender la topología de la red. OLSR [18] y TBRPF son los más populares.

Algunos de los aspectos críticos en estos protocolos que hacen a unos mejor que otros en determinadas circunstancias son la convergencia rápida ante cambios en la topología de la red, los mecanismos que eviten los bucles, el correcto establecimiento de rutas a las pasarelas, y la mayor eficiencia posible para no cargar innecesariamente la red con tráfico de control. La mayoría de los problemas desaparecen en redes estáticas y esos protocolos son mayoritariamente aptos desde el punto de vista de la estabilidad, si bien en redes móviles hay estudios que identifican problemas de inestabilidad importante en varios de ellos. Nuestro trabajo [19] hace mención a algunas pruebas de laboratorio que nos permitieron usar con éxito tanto AODV (implementación de la Universidad de Upsala) como OLSR (versión Qolyster) en cadenas estáticas ad-hoc.

Además, hay un problema concreto que sólo recientemente ha sido abordado por algunos grupos de investigación y por muy escasos proyectos de desarrollo: la QoS. Como demostró un grupo del MIT en [20], los protocolos anteriormente citados establecen rutas que no siempre son óptimas debido a que usan como métrica el número de saltos. Con frecuencia en redes Mesh, cuando hay más de una ruta alternativa para unir dos nodos no contiguos, el camino con menor número de saltos usa algún enlace más lento e inestable; los protocolos anteriores escogen con frecuencia este tipo de rutas. Algunos, como AODV, son en este sentido algo mejores que el resto por definir un umbral de nivel de señal para considerar que un enlace existe. Los trabajos de De Couto et al., a parte de demostrar que "el camino más corto no es suficiente" como métrica, han propuesto una métrica llamada ETX [21], que tiene en cuenta el número medio de retransmisiones en cada enlace. Esta fue una de las primeras propuestas de encaminamiento ad-hoc que rompe la regla de independencia entre capas, ya que usa información de la capa MAC para alimentar la métrica del encaminamiento en capa IP. Un proyecto de desarrollo de Urbana-Champaign ha usado esta métrica para desarrollar un protocolo nuevo. Es fácil ver que esta métrica tiene fundamento: si una ruta tiene menos saltos pero alguno es muy débil, los paquetes tendrán que ser retransmitidos

muchas veces debido a los errores de bit frecuentes, con lo que las rutas que pasan por ese enlace serán penalizadas. El proyecto QOLSR [22] también se ha centrado en introducir QoS en OLSR, de forma que se tengan en cuenta informaciones de la capa MAC para determinar las rutas con mayor ancho de banda y menores retardo y jitter. Su implementación, Qolyester, todavía se encuentra en una primera fase de desarrollo pero merece la pena ser seguida de cerca en el futuro.

Nuestro equipo ha seleccionado "olsrd" [23], la implementación de OLSR de Andreas Tønnesen, como la mejor solución actual para nuestra red. A diferencia de otros proyectos ha alcanzado una madurez y estabilidad destacables y a día de hoy sigue siendo mantenido por una comunidad extensa. "olsrd" es un protocolo estructurado de forma modular a través de plugins, en constante creación y evolución. Así podríamos destacar los siguientes:

- Pasarela dinámica de Internet. Permite añadir pasarelas a Internet de forma dinámica y sin necesidad de configuraciones manuales en el resto de la red.
- Seguridad. Permite añadir una firma a los paquetes OLSR de forma que sólo los nodos que estén en posesión de esa clave podrán formar parte del dominio de la red.
- HTTP. Implementa un servidor HTTP que muestra distintos tipos de información sobre el demonio olsrd.
- Información de topología. Genera gráficas de la topología actual de la red.

Además este protocolo incorpora desde sus últimas versiones la métrica de calidad de servicio, ETX.

### 4.3. Calidad de Servicio

El planteamiento de este trabajo es que las redes 802.11 pueden ofrecer una solución robusta, apropiada y de bajo coste para distribuir comunicaciones de voz y datos en zonas rurales apartadas. Lo visto hasta ahora puede resolver más o menos bien el problema de las comunicaciones de datos elásticos, ya que se ha visto cómo sacar lo mejor posible de esta tecnología para comunicaciones de muy largo alcance robustas y sostenibles, pero si queremos también proponer comunicaciones de tiempo real, es necesario asegurar una calidad de servicio en determinadas condiciones. En nuestro caso, las comunicaciones de telefonía son imperativas, ya que la telefonía es el servicio más demandado y prioritario para comunicar zonas rurales incomunicadas, y así se ha demostrado en la evaluación de impacto de los proyectos demostrativos previos del grupo EHAS [24]. Si adicionalmente se pueden proponer otros servicios de tiempo real como la videoconferencia, también podría ser de interés para algunas aplicaciones de telemedicina y tele-educación entre otras. El mayor problema asociado a la calidad de servicio en una torre de protocolos es que todas las capas deben contemplar el soporte de QoS. En 802.11 no se tiene este soporte. No obstante, el uso de ciertos procedimientos técnicos de control avanzado del tráfico en la capa IP puede permitir

que al menos se de un tratamiento diferenciado a los distintos tipos de tráfico. La arquitectura de QoS de la que haremos uso es una adaptación de DiffServ [25] [26], basada en la prioridad relativa de una determinada clase de servicio. Una limitación importante que nos encontraremos para repartir los recursos de una red 802.11 entre tráficos con distintas prioridades es que el caudal y el retardo de los enlaces inalámbricos deben ser estimados a priori, y sin embargo no se puede tener la certeza de que las prestaciones estimadas se vayan a conservar. Además, como hemos visto anteriormente, las prestaciones dependen incluso de la intensidad del tráfico ofrecido a medida que nos aproximamos a la saturación, por lo que la necesidad de estimar las prestaciones del enlace es doblemente importante, ya que necesitaremos conformar el tráfico para garantizar que trabajamos en la zona cuasi-lineal de la curva caudal-carga ofrecida.

Algunos experimentos realizados por nuestro grupo han permitido demostrar en cadenas de nodos Mesh que se puede garantizar una calidad de servicio diferenciada a voz, vídeo y datos elásticos si se pueden acotar las prestaciones de los enlaces [19]. Resultaría de interés para trabajos futuros que las prestaciones de los enlaces de la red se estimaran de forma dinámica y que el reparto de los recursos se adaptara a lo largo del tiempo a los cambios, ofreciéndose incluso un control de admisión adaptativo. De momento, es plausible hacer una previsión estática conservadora de las prestaciones de los enlaces en redes estáticas, y una configuración estática del control del tráfico para implementar servicios diferenciados adaptados a redes Mesh según se ha dicho. En este caso, un deterioro de los enlaces de la red por debajo de las prestaciones estimadas supondría un riesgo para la calidad de servicio de las comunicaciones de tiempo real.

#### 4.4. Sistema solar y diseño de bajo consumo

Nuestro router será instalado en zonas rurales aisladas de carácter montañoso y selvático, en su mayoría desprovistas de toda instalación eléctrica. Se impone por tanto una solución basada en un sistema de energía solar diseñado para proporcionar la suficiente energía de forma continuada. Este sistema deberá tener todos los elementos para alimentar en DC nuestro equipo de comunicaciones: panel solar, baterías, cargador/regulador y cableado de interconexión. Un sistema típico para un escenario de una región tropical y calculado para proveer una potencia de 3W durante las 24 horas del día sería el constituido por un panel solar de 22 Wp, un regulador de 3A y una batería de 17Ah. Es importante remarcar que el coste y tamaño del sistema solar es directamente proporcional a la potencia consumida por nuestro router, resultando por tanto fundamental un diseño de bajo consumo. Podemos plantear esta estrategia desde dos perspectivas:

- Placa hardware. Según mediciones realizadas en nuestro laboratorio la placa Soekris presenta un consumo medio de 4W en reposo. Migrando a una arquitectura de bajo consumo como ARM o MIPS podemos reducir esta cifra a valores cercanos a 1W. Con objeto de realizar un estudio comparativo en potencia hemos seleccionado las siguientes placas:

- Arquitectura ARM: Peplink, Compulab, Inhand

- Arquitectura MIPS: RouterBoard, MeshCube

Además de un diseño enfocado hacia el bajo consumo, en la anterior selección hemos seguido teniendo en cuenta otros criterios como el número y tipo de interfaces inalámbricas, el bajo coste de los equipos, y su compatibilidad con un Sistema Operativo Linux. Otra posibilidad relacionada con el ahorro de energía en una placa hardware tiene que ver con el modo de ahorro de energía que la mayoría de placas incluyen entre sus características. Es un campo que aún se encuentra inmaduro en Linux pero al que cada vez se le dedican más esfuerzos.

- Tarjetas wireless. Según medidas realizadas en laboratorio sabemos que las tarjetas inalámbricas son el elemento de mayor consumo en nuestro sistema. Esto se acentúa de forma especial en tarjetas del tipo SR2 Ubiquity de 400mW que actualmente usamos en nuestros enlaces de larga distancia. Estas tarjetas llegan a consumir valores cercanos a los 4W en sus velocidades más bajas. Y hay que tener en cuenta que nuestros nodos tendrán al menos dos interfaces, siendo también probable el caso de tres. Es imperativo por tanto buscar un diseño que minimice el consumo de las interfaces inalámbricas. El estándar 802.11 recoge en su especificación un modo de ahorro de energía, Powersaving mode (PS), que permite a las estaciones dormir sus tarjetas inalámbricas y despertarlas de forma periódica gracias a un circuito de temporización. Cuando son despertadas comprueban a través de tramas beacon si existen datos esperando a ser transmitidos para ellas. De no ser así, la estación vuelve a dormir entrando en un ciclo periódico. Resulta difícil determinar de manera exacta el ahorro de energía que introduce este modo en el consumo de una tarjeta inalámbrica. Según las hojas de fabricantes de diversas tarjetas inalámbricas, podemos considerar el consumo medio de transmisión en unos 250mA. Cuando la estación se duerme este número se reduce hasta los 30mA. Debido a que la tarjeta se despertará de forma periódica, la corriente variará entre los 30 y los 250mA, dependiendo de la duración de los intervalos beacon que hayamos configurado en el punto de acceso. Es importante destacar que cuánto más alto sea el throughput que queramos conseguir mayor será la frecuencia de estos intervalos, y por tanto menor será el ahorro energético conseguido. El modo Powersaving no termina de ser una solución válida para nuestro escenario por los siguientes motivos:

- El ahorro conseguido es parcial, ya que las interfaces siguen activas incluso cuando están durmiendo debido al circuito de temporización.

- Aunque el estándar 802.11 recoge ambas arquitecturas en la especificación de este modo, en una arquitectura Ad-Hoc no resulta tan eficiente por su carácter descentralizado.

- En una arquitectura tipo infraestructura el ahorro que este modo introduce es sólo efectivo para el lado del cliente. El punto de acceso permanece siempre despierto, transmitiendo tramas beacon y almacenando en un buffer tramas de datos para aquellos clientes que permanezcan dormidos.

- El driver actual de Hostap implementa este modo en su funcionamiento por defecto. En el caso del driver Madwifi no parece haber sido implementado aún.

Además de las dos estrategias descritas sería interesante tratar esta problemática con un ámbito más global, esto es, con un protocolo de bajo consumo enfocado a toda la red. Es importante establecer en este punto algunas de las variables que definen nuestros escenarios:

- La utilización de la red no es estrictamente 24x7. Además durante el periodo nocturno se puede prever un uso mucho menor.
- Según estudios que hemos realizado la mayoría de las comunicaciones que se producen en nuestras redes tienen carácter local, sin salida al exterior, y sin implicar a todos los Puestos a la vez.
- Existe un modelo de uso compartido. Un sólo PC o teléfono por Puesto de Salud obliga a su compartición en el caso de que se quieran realizar varias comunicaciones a la vez.
- En los escenarios en los que trabajamos las comunicaciones más importantes son las de voz, por encima de las de datos.

Estas características nos llevan al diseño de un modelo de red en el que no es necesario que todas las partes de la misma se encuentren funcionando a la vez, y en el que de forma excepcional y durante determinados periodos, típicamente nocturnos, se pueda tolerar un retraso de hasta varios minutos en el establecimiento de la comunicación. Así, se podría desarrollar un protocolo que durmiese las interfaces inalámbricas y las despertará en un ciclo periódico o ante la presencia de tráfico.

#### 4.5. Sistema estructural outdoor y PoE

En las instalaciones realizadas hasta ahora los componentes hardware han sido instalados de forma separada. Así, antenas y placa fotovoltaica se encuentran instalados en la torre de comunicaciones o mástil mientras que la placa Soekris se encuentra instalada en el interior de la caseta o Puesto de Salud. Para la segunda versión del prototipo estamos diseñando un único sistema estructural compacto, compuesto fundamentalmente de una caja estanca donde habrá de montarse el panel solar, con un mecanismo para girarlo y fijarlo en la orientación apropiada, y las antenas. También harán falta elementos de fijación a la torre o mástil. En su interior situaremos la placa hardware con sus correspondientes tarjetas inalámbricas y pigtails. Esta caja estanca deberá ser impermeable, así como incluir un sistema de protección adecuado ante condiciones extremas de temperatura y humedad. De forma complementaria a un montaje

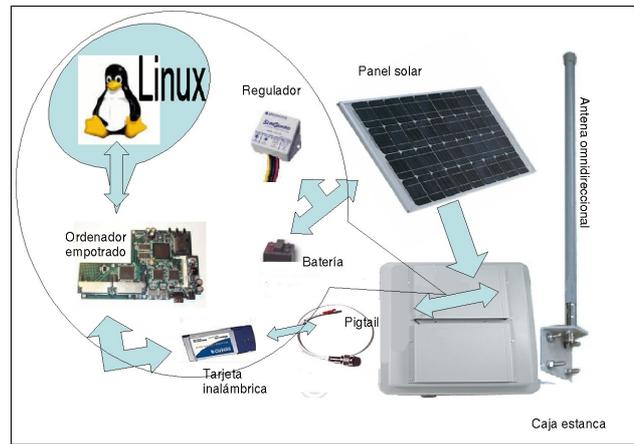


Figura 3: Diseño hardware del router solar

outdoor se hará uso de un sistema PoE (Power over Ethernet), de acuerdo al estándar 802.3af, consiguiendo de este modo llevar en un único cable datos y energía.

La Figura 3 recoge de forma esquemática el diseño hardware del futuro router inalámbrico solar.

#### 4.6. Nueva distribución software

El Sistema Operativo Pebble que hemos usado en nuestra primera versión ocupa alrededor de 77 MB en su versión más sencilla, y 98 MB en el caso de incorporar la centralita de VoIP Asterisk. Este tamaño no resultó ser un factor crítico en el primer prototipo ya que el sistema de almacenamiento empleado, una tarjeta Compact Flash, puede ser ampliado hasta tamaños de 512 GB sin grandes diferencias de coste. Sin embargo para el resto de placas que estamos considerando el sistema de almacenamiento se basa en memoria Flash. Debido al alto coste de este tipo de memoria, la elección de un tamaño adecuado resulta un factor de diseño más crítico que en el caso de la CF. De este modo será necesario optimizar en la medida de lo posible el tamaño final del Sistema Operativo que vamos a usar, no siendo mayor de 32 MB. A diferencia de Pebble, que fue construido a partir un sistema Debian Woody, hemos diseñado nuestro propio sistema operativo desde cero con aplicaciones como busybox y tinylogin. Por último remarcar que el uso de arquitecturas diferentes a x86 nos obliga a realizar una compilación en cruzado de cualquier software que queramos instalar. Proyectos como Scratchbox [27] ayudan a facilitar esta tarea, ya que permiten compilar en cruzado paquetes Debian de forma automática en vez de modificar ficheros del tipo .configure.

#### 4.7. Sistema de Gestión de red

Las redes desplegadas dentro del programa EHAS en zonas rurales de América Latina empiezan a tener un tamaño considerable, lo que hace que surjan nuevas necesidades a partir de la experiencia que vamos adquiriendo con ellas. Entre otras se ha detectado de forma especial la necesidad de una aplicación de Gestión de red. Gracias a ella podremos conocer con detalle la disponibilidad y estado en tiempo real de los nodos, así como prevenir posibles problemas o averías con la antelación suficiente. La arquitectura de Gestión en la que

trabaja EHAS se un nodo que gestiona (nodo gestor) al resto de nodos (nodos gestionados). En los nodos gestionados diferentes tipos de datos son obtenidos a través de las MIBs 802.11 de SNMP, y almacenados y procesados en forma de gráficas por las RRDTool. De forma periódica y haciendo uso del correo electrónico se envían en forma de logs al nodo gestor. En este nodo se hace uso de la aplicación Zabbix, la cual permite realizar a través de un interfaz Web diferentes funciones como servicio de alarmas, mapas de red, envío de alertas, etc. Está prevista la instalación inminente de este sistema en nuestra red.

#### 4.8. Sistema de seguridad de red

A diferencia de lo que ocurre con una red cableada no es necesario el acceso físico a una red inalámbrica para poder vulnerar su seguridad en diferentes aspectos. Así se hace especialmente importante la búsqueda de sistemas de seguridad que garanticen la autenticidad y confidencialidad de los datos que van a viajar por nuestra red. De forma histórica estos han sido algunos de los mecanismos de seguridad desarrollados a nivel wireless:

- WEP (Wireless Encryption key) estático. Una única clave es usada para cifrar las comunicaciones entre dos nodos, tanto en modo infraestructura como Ad-Hoc. En la mayoría de las implementaciones, la misma clave es usada por cada estación lo que reduce drásticamente la seguridad. Sigue siendo el método de seguridad más usado a pesar de que en 2001 se demostró que el mecanismo de encriptación usado resultaba fácilmente vulnerable [28].
- WEP dinámico basado en 802.1X. Añade una mejoría respecto a WEP estático ya que la clave se envía de forma dinámica a los clientes haciendo uso de 802.1X.
- TKIP y CCMP. Creados a partir de 802.11i, grupo responsable de la seguridad Wi-Fi. TKIP ofrece un sistema de cifrado e encriptación basado en WEP aunque con sustanciales mejoras. Además, y gracias al estándar WPA de Wi-Fi Alliance, es totalmente compatible con las tarjetas inalámbricas que hacen uso de WEP. Sin embargo CCMP sólo es válido para las tarjetas inalámbricas más recientes debido a su sistema de cifrado totalmente distinto a los anteriores.

Es importante señalar que todos estos mecanismos de red, a excepción de WEP, han sido diseñados con vistas a una arquitectura centralizada. Por eso en una red Mesh Ad-Hoc sólo podremos implementar seguridad a nivel 2 a través de WEP y no del reciente WPA. Será necesario entonces buscar otros mecanismos adicionales que añadan seguridad a niveles superiores: IPSec - VPN (nivel 3), SSL (nivel 4), SSH, NoCat (nivel 7).

### 5. RESULTADOS

Hemos obtenido un primer prototipo basado en la placa Soekris de arquitectura x86 al que se ha instalado pebble-EHAS, una distribución Linux mantenida por nuestro

grupo. Cuenta además con una centralita de VoIP Asterisk que confiere una solución de voz al sistema. Este primer prototipo actualmente está siendo instalado con éxito en nuestras redes de comunicación en Colombia y Perú. Además hemos realizado diversas pruebas de campo en enlaces de larga distancia con unos resultados muy prometedores, llegando a enlazar 40 km con un throughput de más de 6.5 Mbps. A partir de las variables de contorno que definen un entorno rural aislado de un país en desarrollo se han identificado las mejoras funcionales hacia un segundo prototipo. Especialmente se ha hecho énfasis en la autoconfigurabilidad y el bajo consumo.

### 6. DISCUSIÓN Y FUTURO TRABAJO

En este artículo hemos presentado la línea de investigación que el grupo EHAS está desarrollando en el área de las redes Mesh Wi-Fi. Este tipo de redes cuentan con una serie de características que las hacen muy adecuadas como red de comunicaciones para los sistemas de telemedicina rural en los países en desarrollo, tanto desde el punto de vista de la conectividad de datos y voz, como de los servicios que soportarían. El mismo sistema de comunicación podría permitir la formación remota del personal sanitario rural y el acceso del mismo a fuentes de información actualizada de salud, rompiendo en alguna medida la sensación de aislamiento profesional. Se podría además utilizar el mismo sistema de comunicación de voz y datos para realizar consultas remotas sobre dudas diagnósticas o de tratamiento, mejorando así los procesos de atención médica. Además un sistema de envío de datos informatizado podría acabar con los dos graves problemas de los actuales sistemas de vigilancia epidemiológica, su lentitud y sus errores, permitiendo a su vez la rápida realimentación de la información a la zona rural. También los mismos sistemas pueden servir para coordinar adecuadamente la evacuación y atención de emergencias.

Algunas de las líneas de investigación que siguen abiertas y deberán ser continuadas por nuestro equipo en el futuro son:

- Estudio del problema de la larga distancia en Wi-Fi: Estudio de un modelo de propagación en frecuencias Wi-Fi ajustado a las distancias y terrenos en los que instalamos. Cuantificación de los efectos meteorológicos en el modelo anterior.
- Seguimiento al funcionamiento del modo Ad-Hoc en los drivers Hostap y Madwifi.
- Evaluación de las distintas alternativas para la implementación de la autoconfiguración de red.
- Estudio comparativo de diferentes protocolos de encaminamiento dinámico multisalto para el caso concreto de redes Mesh estáticas.
- Soporte de QoS a nuestra red y cálculo de prestaciones de enlaces de red de forma dinámica.

- Evaluación comparativa en potencia de las placas hardware seleccionadas.
- Aplicación a nuestra red del Sistema de Gestión de Red desarrollado por EHAS.

## REFERENCIAS

- [1] A. Martínez, V. Villarroel, J. Seoane, F. del Pozo, "Rural Telemedicine for Primary Healthcare in Developing Countries", *IEEE Technology and Society Magazine*, Volume 23, Number 2, Summer 2004.
- [2] John Bicket, Daniel Aguayo, Sanjit Biswas, and Robert Morris, "Architecture and Evaluation of an Unplanned 802.11b Mesh Network", *Mobicom 2005*, Aug 2005.
- [3] Eric Brewer, Michael Demmer, Bowei Du, Kevin Fall, Melissa Ho, Matthew Kam, Sergiu Nedeveschi, Joyojeet Pal, Rabin Patra, and Sonesh Surana, "The Case for Technology for Developing Regions", *IEEE Computer*, Volume 38, Number 6, pp. 25-38, June 2.
- [4] Sitio web del Grupo Inveneo, URL: <http://www.inveneo.org/>.
- [5] R. Draves et al, "Routing in Multi-Radio. Multi-Hop Wireless Mesh Networks", *In Proc. of MobiCom04*, Philadelphia, September 2004.
- [6] P. Kyasanur, N. H. Vaidya, "Routing and Interface Assignment in Multi Channel Multi-Interface Wireless Networks", *UIUC Technical Report*, October 2004.
- [7] V. Navda, A. Kashyap, S. R. Das, "Design and Evaluation of iMesh: An Infrastructure Mode Wireless Mesh Network", *In Proc. in WoWMoM'05*, Jun 2005.
- [8] RFC 2461, "Neighbor Discovery for IP Version 6 (Ipv6)"
- [9] RFC 2462, "IPv6 Stateless Address Autoconfiguration"
- [10] RFC 3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"
- [11] Carlos J. Bernardos, María Calderón, "Survey of IP address autoconfiguration mechanisms for MANETs, draft-bernardos-manet-autoconf-survey-00", Work-in-progress, 2005-07-11.
- [12] K. Weniger, "PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks", to appear in *IEEE Journal on Selected Areas in Communications (JSAC)* Special Issue 'Wireless Ad hoc Networks', March 2005.
- [13] Pr. Kenichi Mase, NOA OLSR specifications, "draft-mase-manet-autoconf-noalsr".
- [14] Christian Tschudin, Richard Gold, Olof Rensfelt and Oskar Wibling, "LUNAR: a Lightweight Underlay Network Ad-hoc Routing Protocol and Implementation", Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN'04), St. Petersburg, Feb 2004.
- [15] J. Broch et al., "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", *Proc. Mobicom '98*.
- [16] C. Perkins. E. Belding-Royer. S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing" *IETF-RFC3561(experimental)*, July 2003.
- [17] D. B. Johnson, D. A. Maltz, Y.C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)" *Internet-Draft manetdsr- 10.txt*, July 2004.
- [18] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", *IETF-RFC3626(experimental)*, October 2003.
- [19] J. Simó, J. Seoane, R. Salazar, "A QoS-aware Ad-Hoc Wireless Network for Isolated Rural Environments", *In Proc. EUNICE 2005*, July 2005.
- [20] D. S. J. de Couto et al, « Performance of Multihop Wireless Networks: Shortest Path is Not Enough" *ACM SIGCOMM Computer Communication Review*, Vol. 33, N. 1, January 2003. architecture for sparse sensor networks. 2003 IEEE International Workshop on Sensor Network Protocols.
- [21] Douglas S.J. De Couto, Daniel Aguayo, John Bicket, Robert Morris, "A high-throughput path metric for multi-hop wireless routing" *In Proc. ACM/IEEE Mobicom '03*. September 2003.
- [22] H. Badis, K. Al Agha, "QOLSR, QoS routing for Ad Hoc Wireless Networks Using OLSR", *European Transactions on Telecommunications*, Vol. 15, No. 4, 2005.
- [23] Andreas Tønnesen, Master thesis: "Implementing and extending the Optimized Link State Routing protocol".
- [24] A. Martínez, V. Villarroel, J. Seoane, F. del Pozo, "Analysis of information and communication needs in rural primary healthcare in developing countries IEEE transactions on Information Technology in Biomedicine", Vol. 9, N. 1, March 2005.
- [25] S. Blake, D. Black, M. Carlson, E. Davies, Zh. Wang, W. Weiss, "RFC2475: An architecture for Differentiated Services", *IETF RFC*, 1998.
- [26] B. Hubert, "Linux Advanced Routing and Traffic Control", Julio de 2003. URL: <http://www.lartc.org>
- [27] Sitio web del Proyecto Scratchbox, URL: <http://scratchbox.org>
- [28] Nikita Borisov, Ian Goldberg, David Wagner, "Intercepting Mobile Communications: The insecurity of 802.11".