## CAPÍTULO CUARTO

# LAS REDES *AD HOC* Y SU USO EN COMUNICACIONES MILITARES

# LAS REDES *AD HOC* Y SU USO EN COMUNICACIONES MILITARES

Por Francisco Javier Ramos López
y Carlos Alberich Landáburu

**Resumen**

En este capítulo, se revisan los últimos desarrollos en redes *ad hoc* desde una perspectiva eminentemente tecnológica, evaluando las ventajas e inconvenientes de su uso para comunicaciones militares.

## Definición y clasificación de redes *ad hoc*

Introducimos en este apartado el concepto de red *ad hoc*, analizando las diferencias con el otro gran grupo de redes inalámbricas, las redes celulares. También se menciona y aclara el concepto de red *mesh* y su relación con el concepto de red *ad hoc*. En el segundo apartado se mencionan los principales retos que debe abordar esta tecnología y las ventajas que representa. Se mencionan también las aplicaciones más destacadas de forma breve, ya que más adelante se desarrollarán aquellas que tienen un ámbito militar. En el apartado siguiente se describen los distintos tipos de redes *ad hoc* o redes *mesh* existentes, atendiendo a diversos criterios. Por último, se describen algunos de estos tipos de redes, con redes propuestas como alternativas para las comunicaciones militares.

### *Definición y caracterización*

En las redes de comunicaciones tradicionales los usuarios se comunican dos a dos a través de una infraestructura común. En el caso de las comu-

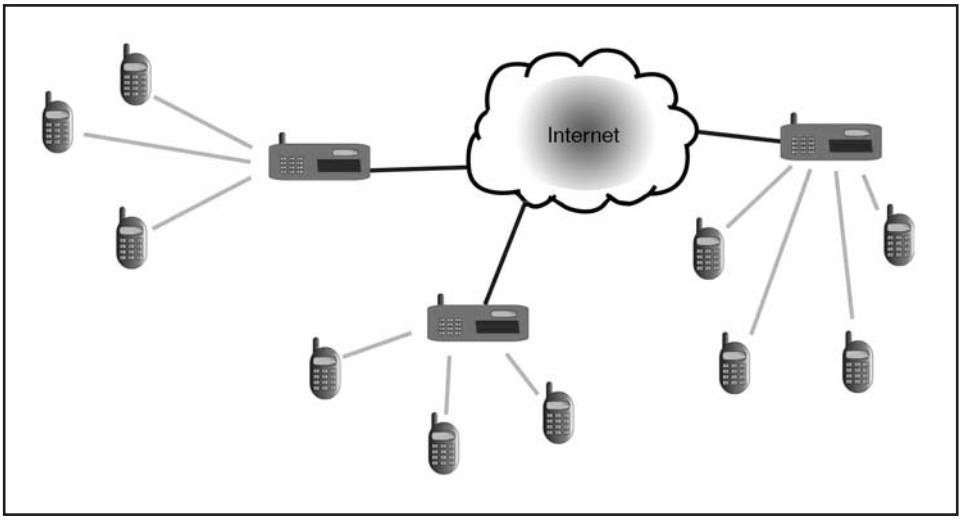


**Figura 1.** *Topología de red tradicional con infraestructura.*

nicaciones inalámbricas, cada usuario, que representa un nodo de la red, se comunica únicamente con una estación base cercana. El resto de la red, denominada troncal, suele no ser inalámbrica, y es la que realiza la mayor parte del trabajo. Este tipo de redes se denominan redes celulares, y el esquema típico de su topología se representa en la figura 1.

Las redes *ad hoc* se definen en contraposición a estas redes celulares como aquellas en las que los usuarios pueden interconectarse entre ellos sin necesidad de la existencia de una estación base u otra infraestructura. En realidad, el término *ad hoc* se refiere en este caso al concepto «creado a partir de lo disponible de forma inmediata, improvisado», es decir, a una red generada de forma espontánea a partir de los usuarios que eventualmente se incorporan a la misma, y que no cuenta con una infraestructura previamente diseñada, jerarquizada y establecida. Una forma clásica de una red *ad hoc* se puede observar en la figura 2 (1, 2, 3 y 4).

Muchos autores también denominan a estas redes como redes *mesh*. El término *mesh* se traduce literalmente por malla, y por tanto este tipo de redes se denominan redes malladas. En efecto, la definición de redes *mesh* es un concepto íntimamente ligado a la topología de la red, que en el caso puro es aquella en la que los nodos están comunicados directamente todos con todos. En la figura 3 se representa un ejemplo típico de esta topología.

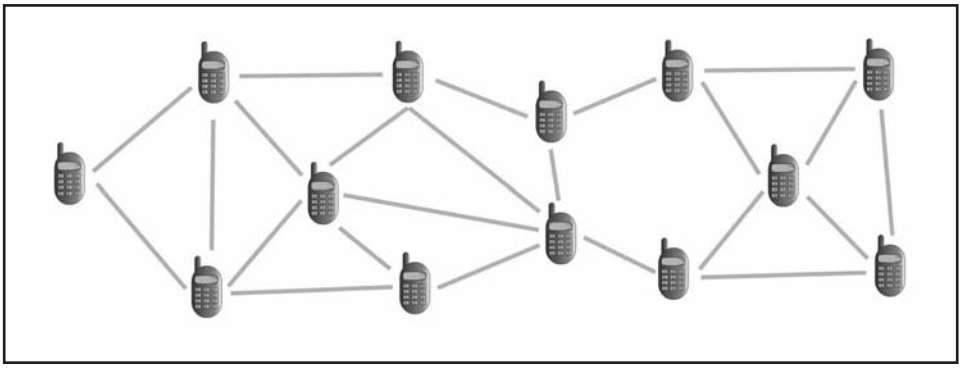

**Figura 2.** *Topología de red* ad hoc.

Como se puede observar, ambos conceptos, redes *ad hoc* y redes *mesh*, parecen no ser idénticos, y sin embargo, ambos se usan a menuda de forma indistinta. Esto es debido a que ambos conceptos, aparte de ser similares, se suelen dar de manera simultánea. El hecho de que todos los nodos estén interconectados entre sí sin el uso de infraestructura, como en las redes *ad hoc*, lleva a una topología en la que o bien todos los nodos están en el radio de cobertura de todos los demás, o bien se utilizan otros nodos similares (no jerarquizados) para realizar la conexión, por lo que

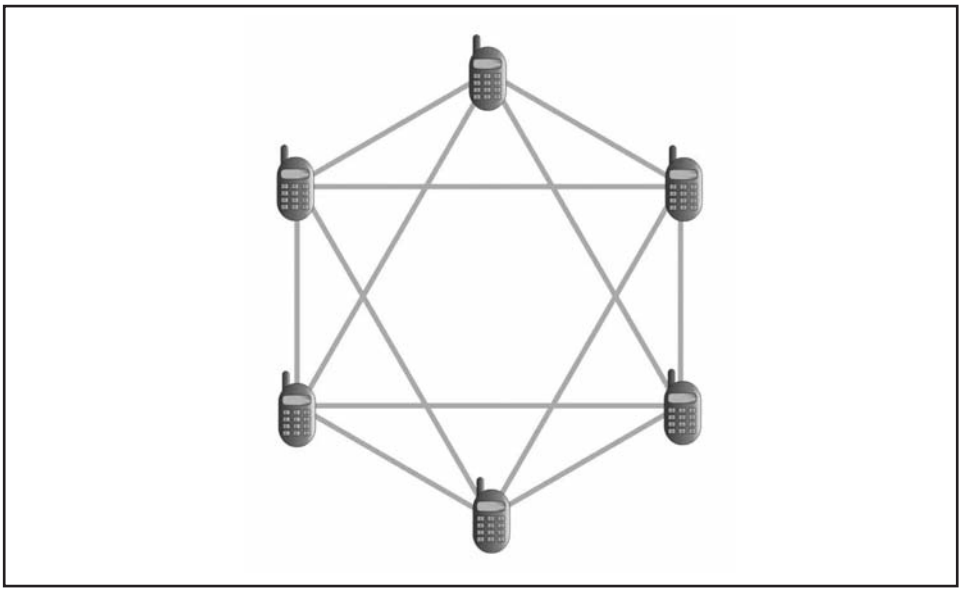

**Figura 3.** *Topología de red* mesh.

ambos conceptos tienen mucho en común. En este trabajo utilizaremos indistintamente ambos términos.

*Retos y ventajas*

El uso de redes inalámbricas *ad hoc* es un reto tecnológico importante. Existen dificultades intrínsecas a la propia definición de estas redes (1).

El hecho de que no exista una infraestructura común, implica que todos los procesos que la red debe llevar a cabo (enrutamiento, control de tráfico y seguridad) tienen que ser realizados de forma distribuida, lo cual genera una complejidad alta en los diseños de procesos y algoritmos.

Por otra parte, cada nodo debe realizar un descubrimiento de la red cuando entra en ella, pues ésta tampoco es una información que se encuentre centralizada. Además los nodos deben ser reconfigurables pues es inherente a las redes *ad hoc* una gran variabilidad de sus componentes. De esta manera las redes deben ser autoconfigurables, lo cual produce que la implantación sea automática y sencilla, pues basta con desplegar los nodos por la zona de cobertura deseada.

Al ser la red inalámbrica, y no existir un control centralizado de los nodos que existen o pueden entrar en la red, la seguridad frente a nodos no deseados o frente a interferencias externas es otro de los grandes retos de estas redes.

Por último, es necesario que estas redes den soporte a los servicios de última generación para que su desarrollo sea factible y tenga utilidad (8). Algunos de estos servicios son tráfico de datos de alta velocidad, aplicaciones en tiempo real o comunicaciones de vídeo y voz, que a su vez necesitan de un sistema que controle la calidad de servicio y el caudal disponible.

A pesar de todos los retos que se le plantean a estas redes existen importantes ventajas que han promovido un fuerte desarrollo de la investigación en este campo (1 y 2).

En primer lugar es obvio que la primera ventaja es la no necesidad de una infraestructura previa. Esto tiene múltiples efectos positivos, entre los que destacan el abaratamiento de la red, la velocidad y facilidad de implantación o la disponibilidad para situaciones adversas, como conflictos bélicos o desastres naturales. Allí donde es inconcebible o extremadamente cara la implantación de una infraestructura, una red cuyos nodos finales

establezcan de forma automática y autónoma una malla entre ellos que permita la comunicación de todos se convierte en una alternativa clara y potente.

En segundo lugar, la no existencia de una jerarquía entre los nodos hace que ningún nodo sea imprescindible. Por ello estas redes son denominadas también redes robustas frente a fallos, ya que la eliminación de un nodo no supone en ningún caso la caída de la red, o de una parte de ella.

Estas dos ventajas conforman las dos características más importantes de las redes *ad hoc*: la flexibilidad y facilidad de implantación y la robustez. Finalmente, otra ventaja importante es la capacidad teórica de usar más eficientemente los recursos disponibles (ancho de banda, principalmente).

*Aplicaciones*

Algunas de las aplicaciones típicas donde el uso de estas redes se hace más aconsejable son las que se enumeran a continuación (2):

— Comunicaciones militares, donde la rapidez de la implantación y la robustez sean más críticos.
— Operaciones de búsqueda y rescate, por las mismas razones.
— Comunicaciones en edificios históricos, donde instalar cables no es posible.
— Redes inalámbricas en conferencias, o allí donde el número de nodos sea elevado.
— Comunicaciones entre vehículos.
— Comunicaciones entre satélites.

*Clasificación de las redes* ad hoc

A la hora de clasificar las redes *ad hoc* podemos hacerlo en función de varios criterios, de los que destacamos: la topología, el ancho de banda y la tecnología de los nodos.

En cuanto a la topología, en apartados anteriores denominábamos redes *ad hoc* o *mesh* puras a aquellas cuya topología consta de nodos sin jerarquizar conectados todos con todos. Sin embargo, desde un punto de vista más amplio, es conveniente mencionar aquí topologías híbridas o jerarquizadas, ya que algunas de las redes *ad hoc* desarrolladas hasta hoy cuentan con estas características. Mencionamos también un tipo de red especial, denominada redes celulares de rápido despliegue, por tener objetivos comunes con el tipo de red tratado en este capítulo, así como

interés en algunos tipos de comunicaciones militares. Centrándonos únicamente en enumerar y diferenciar las distintas categorías, sin entrar en más detalle, la clasificación de redes *ad hoc* según su topología sería la siguiente (7):

— Redes malladas puras. Son las descritas hasta el momento en este documento. En ellas todos los nodos tienen la misma categoría, y sirven tanto de punto final como de repetidor. Son muy robustas y su despliegue es sencillo. La complejidad tecnológica es elevada.
— Redes malladas con posibilidad de infraestructura. La mayoría de las redes *mesh* de la actualidad son aquellas que conforman Redes Inalámbricas de Ordenadores de Área Local (WLAN, de sus siglas en inglés), que disponen también de la posibilidad de añadir un modo infraestructura, en el que algunos nodos realizan funciones de red tales como enrutado, sirviendo así de punto de acceso a los demás nodos. Estos nodos principales se conectarán entre sí con la misma filosofía que una red mallada pura, sin ninguna jerarquía. Se trata por tanto de una situación híbrida.
— Redes jerárquicas auto-organizadas. Recoge el tipo de redes en el que sí existe una jerarquía, si bien ésta no es rígida y se genera de una forma autónoma (auto-organización). Algunos nodos, semejantes a los demás, son elegidos de alguna manera como cabezas de un *cluster*. Todos los nodos pertenecientes a ese *cluster* les utilizarán para que realicen funciones de enrutado y de comunicaciones troncales. Este modo no nos permite ahorrar complejidad *hardware* debido a que cualquier nodo se puede convertir en algún momento en cabeza de *cluster,* pero sí simplifica enormemente las tareas de encaminamiento.
— Redes celulares de rápido despliegue. Se caracterizan por el uso de telefonía celular con estaciones base portátiles que se organizan entre ellas de manera rápida y flexible, tal y como lo harían los nodos principales en una red mallada con infraestructura. Existen numerosos inconvenientes en el uso de este tipo de redes, que se analizarán más adelante. Otra posible clasificación que podemos realizar es la que se refiere al ancho de banda o velocidad de la red. Según este parámetro las redes *ad hoc* se pueden clasificar en redes de banda ancha y de banda estrecha.
— Redes *ad hoc* de banda ancha. Cuando la aplicación requiere la transmisión de datos de alta velocidad y con latencia reducida es necesario que la red pueda soportar una velocidad de transmisión alta. La complejidad es alta en estas redes, ya que deben soportar

diferentes servicios, cada uno de ellos con sus requerimientos de calidad de servicio.

— Redes *ad hoc* de banda estrecha. A veces la principal función de la red no es el transporte masivo de una gran cantidad de datos, sino la transmisión rápida de pequeñas cantidades de información. El caso más típico de estas redes son las Redes Inalámbricas de Sensores WSN *(Wireless Sensor Networks)*. Están formados por nodos cuya función, aparte de la propia de comunicaciones, es la de sensar el medio que le rodea. Cuando un evento se produce el nodo lo detecta y desea enviar esa información a un punto concreto de la red. Este tipo de redes han despertado un enorme interés por su amplia gama de aplicaciones, entre ellas militares, y serán descritas con más profundidad en apartados posteriores. Otra clasificación de las redes *ad hoc* que resulta interesante es la que divide a las redes según la tecnología utilizada como infraestructura para los nodos o los repetidores (7). Sin entrar en detalles, podemos destacar:
  — Redes inalámbricas terrestres. Los nodos son iguales y están situados a nivel de tierra.
  — Redes con estaciones base móviles. Algunos nodos son más complejos, y en el despliegue se elije su posición de forma estratégica, como en el caso de las estaciones base portátiles.
  — Redes con repetidor en una aeronave. Los nodos son terrestres pero se apoyan en una red troncal aérea, formada por aeronaves.

Por último mencionamos otras dos clasificaciones interesantes. La primera de ellas se refiere a la movilidad de los nodos. Las redes pueden ser móviles o no. Si bien las redes inalámbricas están preparadas para que los nodos puedan desplazarse libremente por la zona de cobertura, la movilidad y el tipo de movilidad (esporádica, continuada, rápida y lenta) afecta al diseño de la red, sin olvidar que algunas redes inalámbricas muy comunes, como las redes de ordenadores, no son inherentemente móviles, sino que los terminales permanecen fijos la mayor parte del tiempo. La última clasificación que mencionamos es aquella que divide a las redes por su cobertura. Dentro de las redes *ad hoc* es común encontrar WPAN (*Wireless Personal Area Network*) con unos pocos metros de cobertura y WLAN con unos cientos de metros de cobertura. Asimismo, también podemos señalar redes más extensas, que cubren una zona de decenas de kilómetros, denominadas Redes de Área Metropolitana (WMAN). Finalmente, uno de los objetivos de las redes *ad hoc*, en especial en las comunicaciones militares, es proporcionar una infraestructura robusta, flexible y heterogénea que dote a la red de una cobertura global.

*Descripción de algunos tipos de redes* ad hoc

REDES CELULARES DE RÁPIDO DESPLIEGUE

Existe un interés considerable por parte de los militares estadounidenses en el uso de telefonía celular con estaciones base modificadas que sean transportables. Ericson desarrolló un sistema de estas características en el año 1997. Operaciones en zonas catastróficas también se podrían beneficiar de estos sistemas.

Sin embargo, existen muchos inconvenientes a tener en cuenta en el uso de este tipo de redes para comunicaciones tácticas. En primer lugar, las estaciones bases deben ser cuidadosamente colocadas, según una planificación previa, para que den una cobertura global y sin agujeros, y para que las interferencias entre células sean pequeñas. Esta planificación necesita un tiempo para llevarse a cabo, y además es necesario la colaboración de personal muy especializado. Además, se necesita una planificación de frecuencias para que células adyacentes no reutilicen la misma. Por otra parte, la red troncal que une y coordina las antenas en las situaciones en las que una única antena no dé suficiente cobertura es compleja y debe instalarse en cable o con enlaces de muy alta velocidad.

Por último, otro problema de las redes GSM es que en cada país utilizan diferentes frecuencias, por lo que sería necesario equipos especiales que pudieran adaptarse a esta situación. Si unimos esto al hecho de que una vez puestas las antenas es complicado cambiarlas, y a que toda la instalación se debe hacer con rapidez y celeridad observamos que el uso en comunicaciones tácticas en zonas en conflicto es poco recomendable.

En realidad, únicamente se contempla la posibilidad de uso de estas tecnologías en centros de operaciones, áreas de retaguardia, o zonas urbanas en las que se realizan misiones de paz, donde las circunstancias permiten la instalación más detenida del sistema, que puede sustituir a las comunicaciones telefónicas con cable.

REDES MÓVILES CON TOPOLOGÍA MALLADA

Las redes móviles con topología mallada son las que hemos denominado redes *mesh* puras, y sus características se han explicado ya. Aquí analizamos las ventajas más importantes para las comunicaciones militares.

Mientras que en áreas de retaguardia las comunicaciones pueden ser sostenidas mediante redes celulares de despliegue rápido u otras alternativas

híbridas que necesiten infraestructura, en el frente, o en acciones ofensivas de avance rápido, las condiciones del campo de batalla son aparentemente y en ocasiones realmente caóticas. Unidades ligeras de alta movilidad, como vehículos de combate ligeros, abandonan rápidamente agrupamientos tácticos para unirse y dar respaldo a otros. Entre estos agrupamientos, con toda esta movilidad, la tecnología de red que dé soporte a las comunicaciones debe ser de inmediato reconfigurable, completamente descentralizada y debe ofrecer redundancia en los enlaces para dar robustez. Todas estas características son las propias de una red móvil con topología mallada. Un grupo de aeronaves y barcos en una operación naval también pueden formar una red *mesh*. En operaciones anfibias este grupo también puede comunicarse con unidades móviles de tierra.

A pesar de que se puede concebir una red *mesh* con diferentes tipos de nodos, que no tengan la misma potencia de transmisión, el mismo número de antenas ni la misma capacidad de almacenamiento o procesado, el diseño de la red sería realmente muy complicado si se intenta utilizar las ventajas de cada característica especial de cada nodo. Sin embargo, debido a la «maldición» de la herencia histórica de equipos, éstos serán, inevitablemente, diferentes, y las redes *mesh* militares deberán aprovechar esta diversidad en su diseño.

Todos estos argumentos nos llevan a pensar que la elección de redes móviles puramente malladas es una alternativa adecuada para soluciones en situaciones críticas. Sin embargo, es importante destacar las dificultades que esta opción conlleva y que se explican a continuación.

El principal inconveniente de las redes móviles malladas puras es la complejidad extra que cada nodo debe tener para poder almacenar el estado de la red, participar en el encaminamiento de la información o almacenar paquetes de otros nodos para su reenvío. De hecho, el coste de una red *mesh* puede ser más alto que el de una red jerarquizada con una zona de red troncal móvil, porque en el caso de la red *mesh* todos los nodos deben poder realizar las funciones que en el caso de la red jerarquizada sólo realizan los nodos troncales.

Para situaciones donde el coste del equipo de comunicaciones sea bajo en relación con el de la plataforma que lo soporta, como por ejemplo una red naval, el concepto de red móvil mallada parece apropiado en términos económicos.

Si nos fijamos ahora en otro aspecto, el tamaño y portabilidad de los componentes, hay que plantearse si un equipo con múltiples receptores,

capacidad de enrutamiento y almacenamiento y otros servicios necesarios es transportable por un soldado. Esta discusión es, sin embargo, una cuestión de tiempo, ya que durante esta década los equipos que se desarrollen pueden llegar a ser realmente minúsculos.

Por otro lado, las comunicaciones inalámbricas que un solo salto conectan al terminal móvil con una infraestructura fija son apropiadas para muchas situaciones, tanto civiles como militares, y son tecnologías conocidas y probadas. En el mundo civil, y en bases militares o en zonas de retaguardia, los usuarios siempre operan en las cercanías de una red cableada.

En este punto de la discusión aparece una nueva problemática de las redes *mesh* utilizadas en comunicaciones tácticas: la necesidad de alcanzar una buena cobertura y conectividad. Para conseguirla es necesario que todos los equipos estén continuamente transmitiendo. Aparte del problema de duración de baterías, en el que existe una intensa investigación, otro problema aparece, ya que el soldado se ve amenazado por el hecho de que al tener una radio con él que está todo el tiempo transmitiendo, puede estar delatando su posición al enemigo. Este nuevo reto tecnológico deberá ser tenido en cuenta en el diseño de estas redes.

Todo lo dicho parece indicar que las redes con tecnología mallada pura son solamente apropiadas para zonas conflictivas, en el frente, o en operaciones en zonas catastróficas donde no existe ninguna infraestructura, y aún así existen problemas asociados que hace falta resolver.

### REDES MÓVILES JERÁRQUICAS TERRESTRES

Una alternativa a las redes *mesh* puras y sus inconvenientes asociados son las redes totalmente móviles jerárquicas terrestres. Si bien son menos ambiciosas en términos de diseño de protocolos y complejidad *hardware*, el esquema jerárquico puede ofrecer una funcionalidad comparable con las redes *mesh*.

En una red móvil jerárquica la mayoría de los nodos son relativamente simples, pues tienen un procesado sencillo y una capacidad de almacenamiento mínima. Únicamente un conjunto pequeño de los nodos tendrían el *hardware* necesario para realizar funciones de enrutado, conmutación, almacenamiento, etc. Estos nodos son también móviles, y se denominan estaciones base móviles.

Hace pocos años las Fuerzas Armadas de Estados Unidos desarrollaron un punto de acceso radio que en muchos aspectos es similar al concep-

to de estaciones base móviles. Estos puntos unían equipos de transmisión y conmutación de datos para dar servicios de voz, datos y vídeo para comunicaciones tácticas. Soportaba movilidad y conectaba a los usuarios a una red troncal ATM. Este tipo de solución no cubre, sin embargo, situaciones de operaciones de unidades infiltradas en el territorio enemigo o de pequeñas unidades aisladas.

En la arquitectura analizada en este apartado, una estación base móvil, como una fija de telefonía convencional, proporcional conectividad a los usuarios que están próximos a ella. Además estas estaciones base deberán estar conectadas de alguna manera. El sistema de comunicaciones terrestres y espaciales que el Centro de Comunicaciones ha desarrollado pretende dar capacidad de 1 a 100 megabits por segundo con coberturas de hasta 40 kilómetros, y sirve de ejemplo de la infraestructura que sería necesaria para unir las estaciones base móviles.

Existen casos en los que la conectividad es más compleja. En terrenos montañosos resulta inviable el establecimiento de enlaces en los que sea necesaria la línea de visión directa, en especial porque las estaciones base móviles están a nivel de tierra. En estas zonas, o en zonas controladas por el enemigo o cercadas por éste una salida a la conectividad de la zona es necesaria. Para ello existen dos alternativas, las comunicaciones por satélite y las comunicaciones con una aeronave, que se explica en el siguiente apartado.

### REDES CON REPETIDOR EN UNA AERONAVE

Una solución al problema de la conectividad de las redes móviles jerárquicas terrestres es poner alguna o todas las estaciones base en plataformas aéreas. Previamente a desarrollar el concepto, presentamos el JTIDS (*Joint Tactical Information Distribution System*), que nos proporciona un importante punto de referencia.

El JTIDS es una red *mesh* pura, desarrollada para comunicaciones aire-aire o aire-tierra. Está basada en redes de radio. Cada 30 redes usan un patrón distinto para la modulación *frequency hopping*. Dentro de cada red, todos los nodos se comunican por todos transmitiendo en difusión. El punto más interesante de esta arquitectura es que no existen nodos críticos, con lo que la pérdida de un nodo no implica la pérdida de conectividad.

La mayor ineficiencia de una red de este tipo viene dada porque la reutilización de frecuencias no existe y porque no se puede realizar correccio-

nes de frecuencia y fase en el transmisor, ya que los receptores son muchos y un mismo transmisor observa diversos canales hasta los receptores. Además, en un Sistema TDMA como el JTIDS los tiempos de guarda deben ser grandes, para evitar que dos estaciones lejanas empiecen a transmitir a la vez. En resumen, la distancia variable y la diversidad de receptores para una misma transmisión implican dificultades que no permiten utilizar algunas técnicas típicas de comunicaciones inalámbricas que mejora el rendimiento del sistema.

Si usamos un repetidor en una aeronave los tiempos de guarda pueden ser pequeños y conocidos, y se puede realizar una corrección de tiempo y frecuencia tanto en el transmisor como en el receptor porque cada nodo transmite únicamente hacia un nodo, el repetidor, y por tanto el canal es único y se pueden usar diversas técnicas de estimación de canal, control de potencia o estimación del tiempo de guarda.

La primera opción posible es colocar el repetidor en un avión pilotado, de manera que no se necesitan nuevas plataformas, sino sólo modificar las existentes. Hay, sin embargo, un inconveniente muy importante: en el caso de terrenos montañosos será necesario que los aviones sobrevuelen la zona de conflicto, con lo que pondríamos en peligro el avión pilotado.

Si colocamos el repetidor en un Avión No Pilotado UAV (*Unmanned Air Vehicle*) solventamos este problema. Además se pueden aprovechar los protocolos existentes para comunicaciones por satélite. El UAV puede transmitir su posición por un canal seguro de manera que los transmisores puedan corregir el efecto doppler y el sincronismo. Según la banda utilizada, se pueden alcanzar anchos de banda de 500 MHz (*X-band*). Para solventar la vulnerabilidad del sistema sería necesario tener repetidores dispersos o un nodo de respaldo para comunicaciones directas sin repetidor.

Aunque esta arquitectura simplifica enormemente el diseño de protocolos y la complejidad *hardware*, tiene aún limitaciones que sugieren alguna mejora a la idea básica.

La primera mejora es un sistema de doble banda que añada al sistema la posibilidad de establecer enlaces directos que no pasen por el repetidor para nodos cercanos entre sí. Esta opción le quita tráfico al repetidor, que queda sólo para comunicaciones de más largo alcance, y permite a los nodos ahorra energía. Otra mejora es el uso de un anillo de UAV en el cielo que permita cubrir un área grande y además no tener que realizar enlaces excesivamente largos. Los UAV estarían comunicados entre ellos, aumen-

tando su complejidad, pero disminuyendo la de los nodos. Estas dos mejoras se pueden combinar para dar un sistema altamente flexible y robusto.

## REDES INALÁMBRICAS DE SENSORES

Las investigaciones iniciales en el campo de las WSN surgieron para aplicaciones militares, con la Agencia DARPA (*Defense Advanced Research Projects Agency*), que ha financiado proyectos importantes de investigación (como *Smart Dust* o NEST). Las líneas de investigación comunes han derivado en una definición *de facto* de las redes de sensores como un conjunto de muchos nodos con capacidad de sensar el medio (miles, cubriendo zonas geográficas amplias), inalámbricos, con topología *ad hoc*, encaminamiento multisalto. Los nodos son pequeños, prácticamente inmóviles después de su colocación, todos homogéneos y esparcidos de forma aleatoria por la zona de cobertura (9 y 30).

Estas redes tienen dos objetivos, sensar el medio y transportar de forma eficaz y eficiente la información a algún punto determinado. Además de las ventajas en cuanto a cobertura, flexibilidad y robustez, las redes de sensores mejoran el sensado en sí ya que permiten una gran redundancia en la información que puede utilizarse para depurarla convenientemente.

Por todos estos motivos en la actualidad las redes de sensores inalámbricas copan gran parte del interés de los investigadores, en especial dentro del campo de las redes *ad hoc*.

De forma más reciente se han considerado otras aplicaciones civiles, como monitorización de especies, agricultura, producción industrial o cuidado de la salud. Estudios y proyectos concretos en todas estas áreas y también en las propias aplicaciones militares demuestran que la definición dada *de facto* inicialmente no cubre todas las características necesarias. Actualmente el debate sobre lo que son o dejan de ser las redes de sensores sigue abierto, y por ello a continuación describimos brevemente algunas dimensiones del espacio de diseño de estas redes, que permiten hacernos una idea de la utilidad de las mismas y del rango de aplicaciones tan heterogéneas que pueden cubrir.

Según la manera en que estas redes son desplegadas en el medio físico podemos encontrar distintos tipos. Los nodos pueden ser desplegados de forma aleatoria (definición clásica) o instalados de forma deliberada en ciertos puntos estratégicos. El despliegue puede ser de una vez, en la ins-

talación de la red, o bien un proceso continuo en el tiempo de uso de la red para, por ejemplo, relevar a los nodos con baterías agotadas. El tipo de despliegue afecta a muchas propiedades de la red, como la densidad de nodos esperada, la localización de los mismos o la evolución en el tiempo de la conectividad.

También se puede dar la posibilidad de que los nodos cambien de posición después del despliegue inicial. Esta movilidad puede ser accidental (viento, mareas, etc.) o bien porque los nodos estén en infraestructuras móviles (un vehículo, un ser humano) o porque los propios nodos tengan movilidad. Ésta puede afectar a todos los nodos o a algunos, y ser esporádica o continua. Todo ello tiene un impacto importante sobre el tipo de dinámica que tendrá la red o el tiempo que un nodo está conectado con otro nodo.

Otros factores importantes son el coste, el tamaño y la energía. Respecto al coste, es significativo diferenciar aquellas redes con pocos nodos todos ellos importantes (estaciones meteorológicas, por ejemplo) en el que la complejidad de cada nodo puede ser alta, o aquellas redes con muchos nodos que deben ser sencillos y barato (como los *Smart Dust* para las aplicaciones militares). También el tamaño se puede analizar en los mismos términos. Existirán redes con nodos muy pequeños (los mismos *Smart Dust*) y otras en los que el tamaño no sea tan crítico (un sensor en un avión).

La energía también es un factor importante en estas redes. Gran parte de la investigación realizada sobre ellas se centra en conseguir protocolos, *software* y *hardware* que maximicen el tiempo de vida de las baterías. En algunos casos es posible que las baterías puedan recargarse (con paneles solares, porque están enchufadas a la red) y en otros ser irreemplazables, con lo que el nodo muere cuando la batería se acaba.

Por último la homogeneidad o heterogeneidad de los nodos, como ya se ha expuesto anteriormente en las redes *ad hoc* genéricas es un elemento muy importante que puede cambiar totalmente la topología y la arquitectura de la red.

Como se puede observar, el ámbito de aplicación y la flexibilidad de estas redes es amplio. En concreto, dentro de las aplicaciones militares las más destacadas son monitorización de campo de batalla, vigilancia, reconocimiento, adquisición de objetivos, vigilancia de ataques Nucleares, Biológicos o Químicos (NBQ), detección de intrusos, detección de francotiradores, radares o sónares distribuidos y otras muchas.

## Estado del arte en redes *ad hoc*

### *Tecnologías implicadas*

#### UWB *(Ultra Wide Band)*

Las comunicaciones UWB se caracterizan por la transmisión de pulsos electromagnético de muy corta duración (1 nanosegundo o menos) y por no usar frecuencias portadora. El ancho de banda ocupado por esos pulsos es inversamente proporcional a su duración, y por tanto ocupan desde bajas frecuencias a frecuencias del orden de gigaherzios. Es por tanto una señal en banda base con un espectro muy amplio, y poca densidad espectral de potencia (poca potencia en una banda de frecuencias determinada) (10).

Sus propiedades más importantes es que debido a lo ancho del espectro es extremadamente difícil de detectar por usuarios externos, por lo que representa una gran oportunidad para comunicaciones seguras. La baja probabilidad de intercepción LPD (*Low Probability of Detection*) es una demanda clave de todas aquellas aplicaciones con requerimientos de seguridad, como lo son todas las militares.

Además al tener poca potencia en cada banda de frecuencias no interfiere con otros sistemas, ya que frente a ellos aparece como ruido de baja potencia. Otra característica es que puede operar en situaciones de línea de visión directa o en situaciones en las que no la hay, ya que atraviesa muros y puertas con facilidad. La inmunidad a la dispersión multitrayecto es una ventaja también muy importante de estos sistemas.

Otras ventajas son su bajo coste, el bajo consumo, que es plenamente digital y que los equipos pueden estar integrados en un solo chip.

De entre las aplicaciones más importantes se pueden destacar las que tienen que ver con posicionamiento, las de comunicaciones y las de imagen (en realidad detección de objetivos).

Respecto a las primeras, UWB permite detectar tanto la posición como la distancia y permite seguimiento y navegación en tiempo real tanto en interior como en exterior. Como ejemplo, con un sistema de pruebas de 400 MHz de ancho de banda y 2,5 nanosegundos de pulso, se consiguen precisiones en localización de 30 cm en interiores y 10 cm en exteriores.

En cuanto a las aplicaciones en comunicaciones se investiga en utilizar estos sistemas para comunicaciones personales de corto alcance, redes

inalámbricas de ámbito local, comunicaciones entre vehículos y comunicaciones móviles con alta capacidad de envío de datos.

Para aplicaciones de radar se puede utilizar para detección de objetos subterráneos (minas antipersonales), localización de personas escondidas, localización de canalizaciones metálicas en muros o seguridad en la automoción con detección de colisiones.

Resulta evidente que todas estas aplicaciones son realmente útiles en el ámbito militar, tanto para comunicaciones tácticas como estratégicas y operacionales, pues ofrecen un alto nivel de seguridad y son difícilmente interceptables, a lo que hay que sumar el alto ancho de banda que ofrecen para, por ejemplo, vídeo en tiempo real. La detección de objetos y personas detrás de muros o la capacidad de localización precisa son también claros ejemplos de utilidad en el ámbito militar.

Por tanto, los Sistemas UWB permiten comunicaciones inalámbricas de gran ancho de banda. El precio que hay que pagar es, sin duda, el corto alcance de los equipos. Esto conduce a los diseñadores de UWB a buscar una alianza tecnológica con un tipo de redes que permita la coexistencia de muchos nodos y la aproveche para disminuir el alcance necesario de los enlaces: las redes *mesh*. Las redes *mesh* en general acortan la distancia de enlace ya que implican que los nodos existentes puedan comunicarse entre ellos en lugar de comunicarse con una estación base que puede estar lejos. Por ello, ambas tecnologías se complementan muy bien y la industria está apostando claramente por esta unión, que aporta gran ancho de banda y alcances más altos.

El reto está, evidentemente, en que la red *mesh* pueda hacer uso de ese potencial ancho de banda que puede llegar al medio gigabit por segundo en la actualidad. Para ello la retransmisión de los datos en cada nodo, las funciones de encaminamiento, el control de tráfico y la calidad de servicio se deben realizar de una manera muy optimizada, lo cual supone un reto tecnológico claro para este tipo de redes.

Por último, cabe destacar que debido al corto alcance que esta tecnología permite, al menos en el ámbito de las comunicaciones, queda claro que una topología de red diseñada correctamente es necesaria para su implantación. Evidentemente, para un gran número de nodos, situados a poca distancia, una configuración *ad hoc* podría permitir explotar las ventajas de esta tecnología que en estos años comienza a explotar y que en breve se convertirá en la más potente de las tecnologías inalámbricas.

WiFi *(Wireless Fidelity)*

El término WiFi hace referencia al estándar del IEEE 802.11, en sus modalidades *a*, *b* y *g*. El estándar define los niveles de enlace y físico para la interconexión inalámbrica de estaciones (11).

Las versiones más usadas son la *b* y la *g*. La velocidad de transmisión máxima que soporta la versión 802.11*b* es de 11 Mbps, si bien la velocidad se adapta a las condiciones del canal y puede ser también de 1, 2 o 5 Mbps. La versión *g* posibilita los 54 Mbps como máximo.

Las distancias típicas de cobertura son de pocos centenares de metros como máximo, aunque depende del tipo de antes que se utilicen. En cualquier caso para las distancias largas es necesario hacer modificaciones sobre el estándar.

El estándar define dos tipos de arquitectura. La primera es el habitual modo de infraestructura, en el que los nodos se conectan a la red a través de un punto de acceso. Los distintos puntos de acceso se conectan entre sí y con el resto de la red por medio de una red cableada. La segunda arquitectura se corresponde con el modo *ad hoc*, en el que los nodos se pueden interconectar entre ellos sin necesidad de punto de acceso, creando así entre todos una red *mesh*.

La importancia de esta tecnología viene dada por su amplia difusión en el mercado, tanto empresarial como doméstico. Las enormes economías de escala basadas en la popularidad de estas redes han permitido un abaratamiento de los productos muy importante. La mayor parte de las redes son redes de ordenadores, en las que los habituales cables *ethernet* se sustituyen por conexiones inalámbricas.

Las ventajas más importantes de esta tecnología son su amplio uso, el conocimiento extenso que existe sobre ella y que además está estandarizada. Las desventajas son su corto alcance, que se puede solucionar contando con una red *mesh*, y la falta de seguridad que tiene.

Desde el comienzo de la existencia de WiFi ha existido un interés militar por esta tecnología, y algunas empresas como Texel han modificado las tarjetas para cumplir con los requisitos de seguridad militares en Estados Unidos.

El uso de esta tecnología en su formato *ad hoc* tiene aplicaciones de comunicaciones de media distancia básicamente, y para la interconexión en bases militares y puestos de retaguardia.

WiMAX *(Wordwide Interoperability for Microwave Access)*

WiMAX es el nombre de una tecnología radio de acceso muy reciente, que corresponde a un nuevo estándar del IEEE, el 802.16*x*, y que es una especificación para redes metropolitanas promovida por algunas de las empresas más destacadas del sector (como Intel y Nokia) (13).

WiMAX no es aún una tecnología de consumo, y eso de momento ha permitido que el estándar se desarrolle conforme a un ciclo bien establecido, lo cual garantizará con el tiempo la estabilidad e interoperabilidad de los componentes.

Esta tecnología está pensada para dar coberturas mucho mayores que WiFi y con velocidades de transmisión que lleguen hasta los 100 Mbps. Podrían situarse como tecnología paraguas que permita a los proveedores de Internet dará acceso inalámbrico en la última milla, ya que puede coexistir con WiFi. En la figura 4 se muestra el alcance pretendido de esta tecnología y su situación respecto a WiFi.

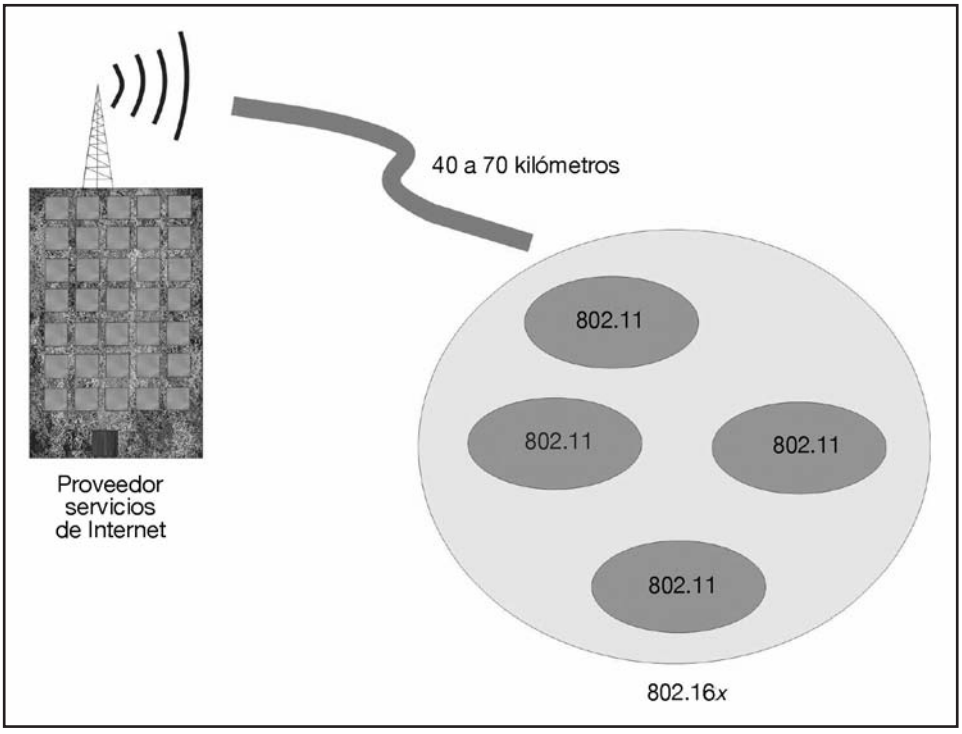


**Figura 4.** *WiMAX. Alcance y compatibilidad con WiFi.*

En marzo de 2003, se ratificó una nueva versión del estándar, el 802.16*a*, y fue entonces cuando WiMAX, como una tecnología de banda ancha inalámbrica, empezó a cobrar relevancia. También se pensó para enlaces fijos, pero llega a extender el rango alcanzado desde 40 a 70 km, operando en la banda de 2 a 11 GHz, parte del cual es de uso común y no requiere licencia para su operación. Es válido para topologías punto a multipunto y, opcionalmente, para redes en malla, y no requiere línea de visión directa. Emplea las bandas de 3,5 GHz y 10,5 GHZ, válidas internacionalmente, que requieren licencia (2,5-2,7 en Estados Unidos), y las de 2,4 GHz y 5,725-5,825 GHz que son de uso común y no requieren disponer de licencia alguna.

El estándar 802.16 puede alcanzar una velocidad de comunicación de más de 100 Mbit/s en un canal con un ancho de banda de 28 MHz (en la banda de 10 a 66 GHz), mientras que el 802.16*a* puede llegar a los 70 Mbit/s, operando en un rango de frecuencias más bajo (<11 GHz).

En el cuadro 1 se muestra una comparativa entre algunas tecnologías de acceso de última generación. Se muestran las velocidades, coberturas, ventajas e inconvenientes, así como la necesidad de licencias.

WiMAX soporta varios cientos de usuarios por canal, con un gran ancho de banda y es adecuada tanto para tráfico continuo como a ráfagas, siendo independiente de protocolo; así, transporta IP *(Internet Protocol)*, Ethernet, ATM, etc. y soporta múltiples servicios simultáneamente ofreciendo Calidad de Servicio (QoS) en 802.16*e*, por lo cual resulta adecuado para voz sobre IP (VoIP), datos y vídeo. Por ejemplo, la voz y el vídeo

**Cuadro 1.** *Comparativa entre tecnologías inalámbricas.*

| Conceptos | WiMAX 802.16 | WiFi 802.11 | Mobile-Fi 802.20 | UMTS y cdma2000 |
|---|---|---|---|---|
| Velocidad | 124 Mbit/s | 11-54 Mbit/s | 16 Mbit/s | 2 Mbit/s |
| Cobertura | 40-70 km | 300 m | 20 km | 10 km |
| Licencia | Sí/No | No | Sí | Sí |
| Ventajas | Velocidad y alcance | Velocidad y precio | Velocidad y movilidad | Rango y movilidad |
| Desventajas | ¿Interferencias? | Bajo alcance | Precio alto | Lento y caro |

requieren baja latencia pero soportan bien la pérdida de algún bit, mientras que las aplicaciones de datos deben estar libres de errores, pero toleran bien el retardo.

Otra característica de WiMAX es que soporta las llamadas antenas inteligentes (*smart antenas*), propias de las redes celulares de 3G, lo cual mejora la eficiencia espectral, llegando a conseguir 5 bps/Hz, el doble que 802.11*a*. Estas antenas inteligentes emiten un haz muy estrecho que se puede ir moviendo, electrónicamente, para enfocar siempre al receptor, con lo que se evitan las interferencias entre canales adyacentes y se consume menos potencia al ser un haz más concentrado.

Una de las principales limitaciones en los enlaces a larga distancia vía radio es la limitación de potencia, para prever interferencias con otros sistemas, y el alto consumo de batería que se requiere. Sin embargo, los más recientes avances en los procesadores digitales de señal hacen que señales muy débiles (llegan con poca potencia al receptor) puedan ser interpretadas sin errores, un hecho del que se aprovecha WiMAX. Con los avances que se logren en el diseño de baterías podrá haber terminales móviles WiMAX, compitiendo con los tradicionales de GSM, GPRS y de UMTS.

Finalmente, es importante destacar que el estándar contempla la posibilidad de formar redes malladas (*mesh networks*) para que los distintos usuarios se puedan comunicar entres sí, sin necesidad de tener visión directa entre ellos. Ello permite, por ejemplo, la comunicación entre una comunidad de usuarios dispersos a un coste muy bajo y con una gran seguridad al disponerse de rutas alternativas entre ellos. En cuanto a seguridad, incluye medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos Triple DES (128 bits) y RSA (1.024 bits).

El Ejército de los Estados Unidos está probando el estándar WiMAX implementado por la empresa Telos Corp. en bases como el fuerte Carson (Colorado) para enlaces punto a punto y punto a multipunto. La idea es extender la red cableada a zonas de difícil acceso (14). En el fuerte Dix (Nueva Jersey), se está extendiendo el acceso de banda ancha a Internet a las zonas de entrenamiento. El resultado es un despliegue rápido que abarata enormemente los costes de la red (a menos de la mitad). Por ello, el desarrollo actual de las redes WiMAX en usos militares se dirigen a la posibilidad de implantar redes troncales de banda ancha con rapidez, flexibilidad y de forma económica. Si a estas carac-

terísticas les añadimos la posibilidad de formar redes *mesh*, queda claro que el siguiente paso será el de proporcionar comunicaciones móviles a un conjunto de nodos dispersos, siendo estas comunicaciones de alta velocidad.

*ZigBee*

La alianza de empresas ZigBee presentó el pasado diciembre la especificación v1.0 del protocolo radio para transmisión de datos a baja velocidad para aplicaciones de automatización de viviendas y edificios, fábricas y otras aplicaciones de monitorización en diferentes sectores (15).

ZigBee es una nueva tecnología inalámbrica de corto alcance y bajo consumo que tiene su origen en la antigua alianza HomeRF. A esta iniciativa de la conocía con nombres como: PURLnet, RF-Lite, Firefly y HomeRF Lite, finalmente se escogió el término ZigBee.

ZigBee pretende ser la base sobre la que crear productos y sistemas para diversidad de sectores como la domótica (automatización en viviendas), la inmótica (automatización en edificios), la automatización en fábricas y en otros sectores con necesidad de usar diversidad de sensores repartidos en un área acotada.

De la diversidad de miembros que forman parte de esta alianza, destacan empresas como Invensys, Mitsubishi, Philips y Motorola que trabajan para crear dispositivos de domótica, automatización de edificios (inmótica), control industrial, periféricos de PC y sensores médicos.

Las empresas que han desarrollado el ZigBee han formado el «ZigBee Working Group» (16) el cual también participa en el grupo de trabajo 4 del Comité de Estandarización IEEE 802.15. Este grupo está enfocado en el desarrollo de especificaciones para productos WPAN en las bandas de frecuencia de uso sin licencia. De esta manera, el ZigBee está ratificado como estándar el IEEE, al igual que por ejemplo la tecnología Bluetooth (IEEE 802.15.1).

El estándar IEEE 802.15.4 tiene como objetivo especificar los niveles físicos y de acceso al medio (MAC) de redes inalámbricas con dispositivos de muy bajo consumo y baja velocidad. Colaboran con el ZigBee Working Group con el objetivo de publicar un único estándar. La tecnología ZigBee será la responsable de implementar las funciones de la aplicación del dispositivo en cuestión, de la gestión de la red y de la seguridad.

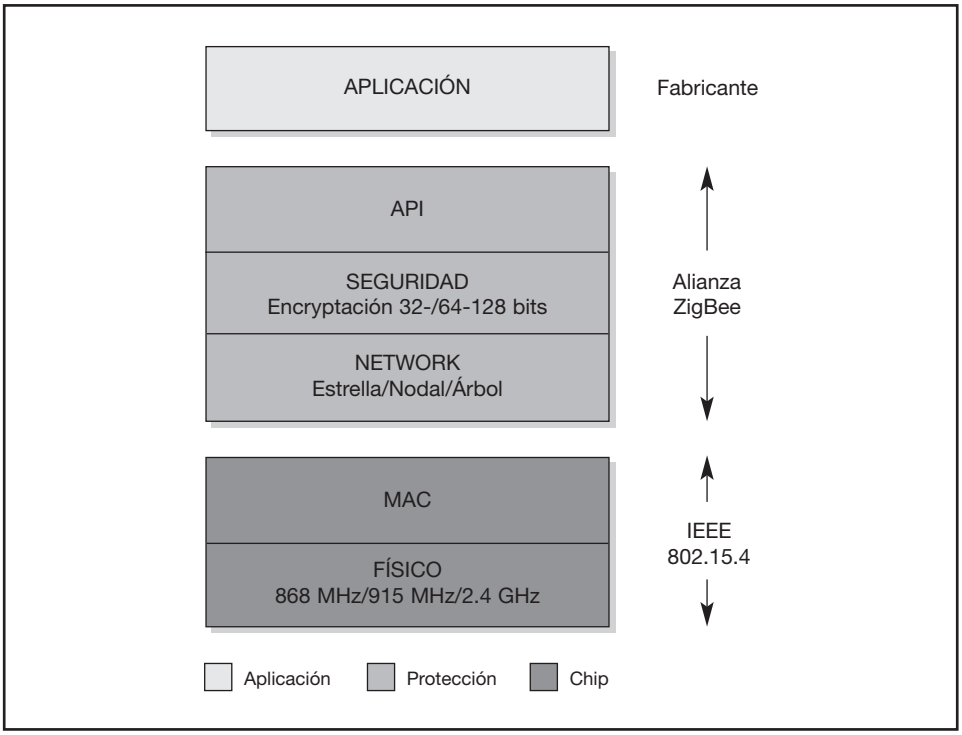


**Figura 5.** *Torre de protocolos asociada a ZigBee.*

En la figura 5 se recoge la torre de protocolos de ZigBee. Se observa la flexibilidad del nivel físico y una capa especial dedicada a seguridad.

Con velocidades comprendidas entre 20 kB/s y 250 kB/s y rangos de 10 m a 75 m, ZigBee puede funcionar en las bandas de 2,4 GHz, 868 MHz y 915 MHz, aunque la mayoría de fabricantes optarán por la primera ya que puede ser usada en todo el mundo, mientras que las dos últimas sólo se pueden usar en Europa y Estados Unidos, respectivamente.

Una red ZigBee puede estar formada por 65.000 nodos, agrupados en subredes de hasta 255 nodos, los cuales tienen la mayor parte del tiempo el transceptor ZigBee dormido con objeto de reducir el consumo al mínimo. El objetivo es que un sensor equipado con tecnología ZigBee pueda ser alimentado con dos pilas AA durante al menos seis meses y hasta dos años, aunque en la práctica se ha verificado que se podrán conseguir más de cinco años de duración de batería en aplicaciones de domótica y seguridad.

Hay tres topologías: estrella, árbol y en red mallada (*mesh network*). Siempre hay un nodo de red que asume el papel de coordinador central encargado de centralizar la adquisición y las rutas de comunicación entre dispositivos. Además, si se aplica el concepto de *mesh network*, pueden existir coordinadores o *routers*, alimentados permanentemente en espera de recibir/repetir las tramas de los dispositivos o sensores. Ambos dispositivos son del tipo FFD (*Full Functionality Device*), debido a que exigen empotrar la mayoría de primitivas definidas por el *stack* ZigBee.

Sin lugar a dudas, una de las mayores aportaciones del ZigBee y el que mayor interés está despertando a las empresas desarrolladoras de productos, es el concepto de red nodal o *mesh network* por el que cualquier dispositivo ZigBee puede conectarse con otro dispositivo usando a varios de sus compañeros como repetidores. De esta manera cualquier nodo ZigBee puede hacer llegar los datos a cualquier parte de la red inalámbrica siempre y cuando todos los dispositivos tengan un vecino dentro de su rango de cobertura.

La aplicación del concepto de *mesh networks*, hará viable muchas aplicaciones, de distintas áreas, como domótica vía radio en viviendas construidas, o aplicaciones industriales o militares, allí donde las tecnologías radio de generaciones anteriores estaban limitadas en cuanto a la cobertura o alcance entre dispositivos. Gracias a esto la instalación y puesta en marcha de dispositivos en cualquier situación será una tarea muy sencilla e independiente de la tipología y tamaño de la red.

Las dos limitaciones clave de esta tecnología son la distancia máxima entre nodos (unos 75 m) y la velocidad. Por ello, su uso en aplicaciones militares puede centrarse en dos vías. La primera de ellas las comunicaciones entre dispositivos de seguridad, por ejemplo, en bases militares. La otra, actuando como redes de sensores, con sus múltiples aplicaciones, incluso en el campo de batalla. El tamaño de los elementos es muy reducido y su larga vida y bajo coste permitirían un despliegue rápido de una red de sensores por el área requerida.

*Enrutado dinámico y robusto*

En las redes de comunicaciones de datos raramente el transmisor y el receptor de la información se encuentran directamente enlazados. Normalmente necesitan nodos intermedios para realizar la comunicación. En una red normal, será preciso que el transmisor conozca la ruta por la que sus paquetes de datos puedan alcanzar el receptor. Éste es el cometido de los protocolos de enrutado.

En las redes *ad hoc* no existe un nodo central que gestione las rutas, y el enrutado debe realizarse de forma eficiente para evitar que el mismo protocolo añade un tráfico a la red desmesurado. Además, el número de nodos suele ser grande, y a esto se le puede añadir la componente de la movilidad de nodos. En resumen, la tarea de enrutar paquetes en una red *ad hoc* es realmente compleja, y existen numerosas líneas de investigación que tratan de solventar los problemas asociados (17, 18 y 19).

Aún quedan más dificultades por añadir en el momento en que consideramos el escenario de las comunicaciones militares. Un enrutado dinámico que soporte cambios en la topología, que sea flexible según las circunstancias es imprescindible. También es fundamental que sea robusto, y no se produzca la pérdida de rutas al desaparecer nodos.

En general, se puede hablar de dos tipos de enrutado básicos. Los protocolos proactivos y los reactivos. En los primeros, la ruta se descubre en cuanto la red se despliega, y se va modificando cada vez que sea necesaria una actualización. Se añade una cantidad de tráfico de control a la red bastante grande, pero una vez que tenemos las rutas diseñadas, cada vez que un nodo tenga que transmitir un paquete lo hará de forma inmediata, por lo que son protocolos de baja latencia. Los protocolos reactivos, sin embargo, no realizan el descubrimiento de la ruta hasta que tienen un paquete que transmitir. Conocerán solamente, por tanto, las rutas que necesiten. Se malgastan muchos menos recursos, ya que el tráfico de control asociado es mucho menor, pero la latencia es mucho mayor porque cada vez que llega un paquete debemos redescubrir la ruta antes de mandarlo. Existen protocolos híbridos intermedios que intentan recoger lo mejor de ambas aproximaciones.

Otras aproximaciones, como el enrutado geográfico, implican conocer la posición, al menos aproximada, del nodo receptor. Siendo así, múltiples protocolos explotan ese conocimiento para optimizar el enrutado.

En redes *ad hoc*, múltiples investigadores tratan de realizar protocolos de enrutado robusto. Algunos de ellos presentan modificaciones robustas de protocolos conocidos, como *Robust* AODV, que es un protocolo reactivo que utiliza actualizaciones locales para dar robustez a las rutas, ya que las rutas son capaces de adaptarse rápidamente a los cambios de la topología. Otros protocolos están diseñados para redes móviles.

En los cuadros 2 y 3 se muestran listas resumidas de los protocolos actuales más destacados. Se añaden solamente para mostrar la gran

**Cuadro 2.** *Resumen de protocolos proactivos.*

| Protocol | RS | Number of tables | Frequency of updares | MH | Critical nodes | Characteristic feature |
|---|---|---|---|---|---|---|
| DSDV | F | 2 | Periodic and as required | Yes | No | Loop free |
| WRP | F | 4 | Periodic | Yes | No | Loop freedom using predecessor info |
| GSR | F | 3 and a list *(a)* | Periodic and local *(b)* | No | No | Localised updates |
| FSR | F | Same as GSR | Periodic and local *(b)* | No | No | Controlled frequency of updates |
| STAR | H | 1 and a 5 lists | Conditional *(c)* | No | No | Employes LORA and/or ORA. Minimize CO |
| DREAM | F | 1 | Mobility based | No | No | Controlled rate of updates by mobility and distance |
| MMWN | H | Maintains a detabase | Conditional | No | Yes, LM | LORA and minimized CO |
| CGSR | H | 2 | Periodic | No | Yes, Clusterhead | Clusterheads exchange routing information |
| HSR | H | 2 (link-state table and location management) *(d)* | Periodic, within each subnet | No | Yes, Clusterhead | Low CO and Hierarchical structure |
| OLSR | F | 3 (routing, neighbour and topology table) | Periodic | Yes | No | Reduces CO using MPR |
| TBRPF | F | 1 table, 4 lists | Periodic and differential | Yes | Yes, Parent node | Broadcasting topology updates over a spanning tree |

RS = Routing Structure; HM = Hello Message; H = Hierarchical; F = Fiat; CO = Control Overhead; LORA = Least Overhead Routing Approach; ORA = Optimum Routing Approach; LM = Location Manager.

*a)* GSR also has a list of all available neighbours. *b)* In GSR and FSR link-state is periodically axchanged with neighbouring nodes.

*c)* In conditional update methods, the updates occur if a particular event occurs. *d)* Number of link-state tables may vary according to the number of logical levels.

**Cuadro 3.** *Resumen de protocolos reactivos.*

| Protocol | RS | Multiple routes | Beacons | Route metric method | Route maintained in | Route reconfiguration strategy |
|---|---|---|---|---|---|---|
| AODV | F | No | Yes, hell messages | Freshest & SP | RT | Erase route then SN or local route repair |
| DSR | F | Yes | No | SP, or next available in RC | RC | Erase route the SN |
| ROAM | F | Yes | No | SP | RT | Erase route & *(a)* |
| LMR | F | Yes | No | SP, or next available | RT | Link reversal & route repair |
| TORA | F | Yes | No | SP, or next available | RT | Link reversal & route repair |
| ABR | F | No | Yes | Strongest Associativity & SP & *(b)* | RT | LBQ |
| SSA | F | No | Yes | Strongest signal strength & stability | RT | Erase route then SN |
| RDMAR | F | No | No | Shortest relative distance or SP | RT | Erase route then SN |
| LAR | F | Yes | No | SP | RC | Erase route then SN |
| ARA | F | Yes | No | SP | RT | Use alternate route or back track until a route is found |
| FORP | F | No | No | RET & stability | RT | A Flow_HANDOFF used to use alternate route |
| CBRP | H | No | No | First available route (first fit) | RT at cluster head | Erase route then SN & local route repair |

RS = Routing Structure; H = Hierarchical; F = Fiat; RT = Route Table; RC = Route Cache; RET = Route Expiration Time; SP = Shortest Path; SN = Source Notification; LBQ = Lacalised Broadcast Query.
*a)* Start a diffusing search if a successor is available, else send a query with infinite metric. *b)* Route relaying load and cumulative forwarding delay.

variedad de protocolos existentes, y la complejidad de este campo. En los protocolos proactivos, se observa que muchos no tienen nodos críticos, lo que evidentemente les proporciona robustez.

Existen pocos protocolos de enrutado comerciales especializados en redes *mesh*. Un caso interesante es el protocolo de *mesh networks*. Una vez analizadas las necesidades especiales de las redes *mesh* han desarrollado un protocolo dinámico, que permite autoconfiguración de los nodos, y que está a caballo entre los protocolos reactivos y proactivos. Además permite configuraciones *mesh* y con jerarquía. Implementa también un sistema para aumentar la vida de los nodos, teniendo en cuenta el nivel de batería de cada uno a la hora de establecer las rutas. Sirva este protocolo de ejemplo práctico, aún con muchas limitaciones, de las posibilidades que las redes *ad hoc* pueden tener si la tecnología es capaz de resolver las dificultades asociadas a esta topología.

*Sensores*

Dentro de las redes *ad hoc*, destacan, como se ha expuesto anteriormente, las redes inalámbricas de sensores. Hemos analizado sus características más destacables, en todo lo que a su dimensión de red de comunicaciones se refiere. Aquí nos referimos a los sensores en sí mismos.

Algunos tipos de sensores son: los sensores de movimiento, sensores de presión, de temperatura, de humedad, de detección de gases, de detección de componentes bioquímicos, sensores magnéticos, sensores de radiación, sensores de movimiento, sensores de aceleración, etc.

Destacan los sensores de infrarrojos que se emplean para localizar y seguir objetivos, para la guía de misiles y para recopilar información. Las imágenes infrarrojas se utilizan también para detectar minas escondidas y para desarrollar sistemas de alarma preventivos.

Las aplicaciones típicas de todos estos sensores son la vigilancia, establecimiento de perímetros de seguridad, detección de personas, localización, seguimiento de objetivos, detección de ataques NBQ.

Tanto en la localización y seguimiento como en la recopilación de información, así como en la detección de ataques químicos o biológicos resulta especialmente conveniente el despliegue de los sensores como una red inalámbrica, que permita la distribución de la información y la mejora del procesamiento de la misma.

Todas estas tecnologías están enormemente avanzadas, y comercialmente se encuentran multitud de opciones tecnológicas diferentes para la misma aplicación (20).

*Confidencialidad*

El rápido crecimiento de los sistemas de comunicaciones inalámbricos ha puesto de manifiesto un problema común a todos ellos: la seguridad. Muchos de estos sistemas nacieron sin la preocupación primordial de proporcionar seguridad a los usuarios. Según pasan los años el uso de este tipo de comunicaciones está más extendido en las comunicaciones entre empresas, particulares o el ejército. A la vez, diferentes y tipos de ataques amenazan la seguridad de los sistemas creados. Hoy en día, los investigadores están muy ocupados desarrollando nuevas tecnologías de seguridad y tapando los agujeros de las ya creadas (21).

De forma clásica, las comunicaciones por cable también han necesitado protegerse de ataques. Sin embargo, las características propias de los sistemas inalámbricos ofrecen un mayor reto a los diseñadores de sistemas de seguridad. En las comunicaciones por cable, para acceder a una red, es necesario en primer lugar tener una conexión física con esa red. En las conexiones inalámbricas esta conexión física es mucho más vulnerable, ya que cualquier persona dentro de la zona de cobertura de la red está conectado físicamente. Ello supone una diferencia básica tanto en el tipo de ataques como en la filosofía a aplicar para los diseños de sistemas de seguridad.

Analizamos brevemente los tipos de amenazas que una red inalámbrica puede tener. La taxonomía de las amenazas ha sido analizada en diversos documentos científicos, pero se puede resumir en algunas líneas generales.

En primer lugar, diferenciamos entre amenazas desde fuera (*outsiders*) o desde el interior de la red (*insiders*). Los *outsiders* tienen acceso a la red inalámbrica y el *software* y *hardware* que utilizan no es interno a la red, sino comercial. Los *insiders* son usuarios legales de la red cuyo objetivo es obtener datos de la red a los cuales no tienen acceso de forma legítima. Utiliza por tanto *software* y *hardware* propio de la red, totalmente válido (22).

En general, existen tres tipos de ataques genéricos. El primero es un ataque de disponibilidad. Se trata de impedir la conexión física en la red (el equivalente a cortar un cable) normalmente introduciendo interferencias

potentes en la red, para que ningún receptor pueda detectar información útil. El segundo de los tipos genéricos es el ataque contra la confidencialidad y el tercero son ataques que violan la integridad de los datos.

De forma más concreta diferenciamos siete tipos de ataques. Tres de ellos únicamente violan la confidencialidad o privacidad de la sesión y son: análisis del tráfico, escucha pasiva y escucha activa. Otros tres violan la integridad y otro se sitúa a caballo entre estas dos situaciones. Los siete casos son:

1. *Análisis de tráfico:* el atacante únicamente es capaz de leer la cantidad de paquetes y el tipo de paquetes que se están enviando, pero no es capaz de leer la información que los paquetes contienen. Puede hacerlo con cualquier antena situada dentro de la red y una tarjeta que incluya el nivel físico y el nivel de enlace la red espiada. Le permite tres cosas: detectar que existe actividad (detectar la red), detectar la posición de los puntos de acceso, *routers*, nodos, y así poder detectar zonas más vulnerables; y el tipo de protocolo que la red utiliza, basándose en el tipo, tamaño y número de paquetes que detecta.
2. *Escucha pasiva:* el atacante escucha de forma pasiva los paquetes y los datos contenidos en los paquetes. Si los datos están encriptados debe desencriptarlos para leer contenido. El peligro no es sólo que el atacante lee la información, y por tanto rompe la privacidad, sino que se puede hacer con datos que luego le faciliten un ataque mucho más peligroso.
3. *Escucha activa:* el atacante escucha la transmisión de paquetes, es capaz de leer su carga, y además puede incluir paquetes de datos en la transmisión con el propósito de facilitar la escucha. Por tanto, no modifica los datos, pero sí se asegura mediante pequeñas transmisiones que tendrá todas las claves necesarias para la escucha.
4. *Atacante en el medio:* el atacante rompe una sesión establecida entre un nodo y un punto de acceso, y cuando el nodo intenta volverse a conectar, el atacante suplanta al punto de acceso, consigue información, y se conecta también al punto de acceso, con lo que el nodo cree estar conectado como siempre, pero en realidad sus datos pasan por el atacante. Cuando sólo existe encriptación a nivel de red o nivel tres (en una red privada virtual, por ejemplo) este ataque permite obtener y modificar la información a nivel dos. Es un ataque que viola la confidencialidad y tiene potencial para violar la integridad de los datos.
5. *Acceso no autorizado:* un atacante externo intenta acceder a la red en su conjunto, consiguiendo identificarse de alguna manera en un punto de acceso. Una vez conseguido puede lanzar otros ataques.

6. *Suplantación de sesión:* el atacante corta una sesión y suplanta al nodo que se ha identificado correctamente, obteniendo así privilegios y permisos para hacer lo que quiera dentro de la red.
7. *Ataque por réplica:* el atacante saca información de una sesión actual para más tarde poder identificarse y entrar en la red, replicando las claves y mecanismos de acceso que el objetivo utilizó.

¿Cómo actuar frente a estos ataques? Depende de la aplicación y de las posibles consecuencias del ataque. En general, las técnicas para proporcionar seguridad utilizan la modulación, codificación, encriptación, *interleaving* (entrelazado de datos) y autenticación. Un esquema lógico de estas técnicas es el representado en la figura 6 (23).

El encriptado es una capa que modifica los datos enviados con algún algoritmo. Los más complejos sólo se pueden decodificar con una inspección continuada y analítica de los datos, y mediante procesado intensivo. Las agencias de seguridad de Estados Unidos utilizan un código de encriptado con una clave de 64 bits, lo que haría necesario $1.27 \times 10^{89}$ operaciones matemáticas para poder decodificar los datos «por la fuerza bruta».

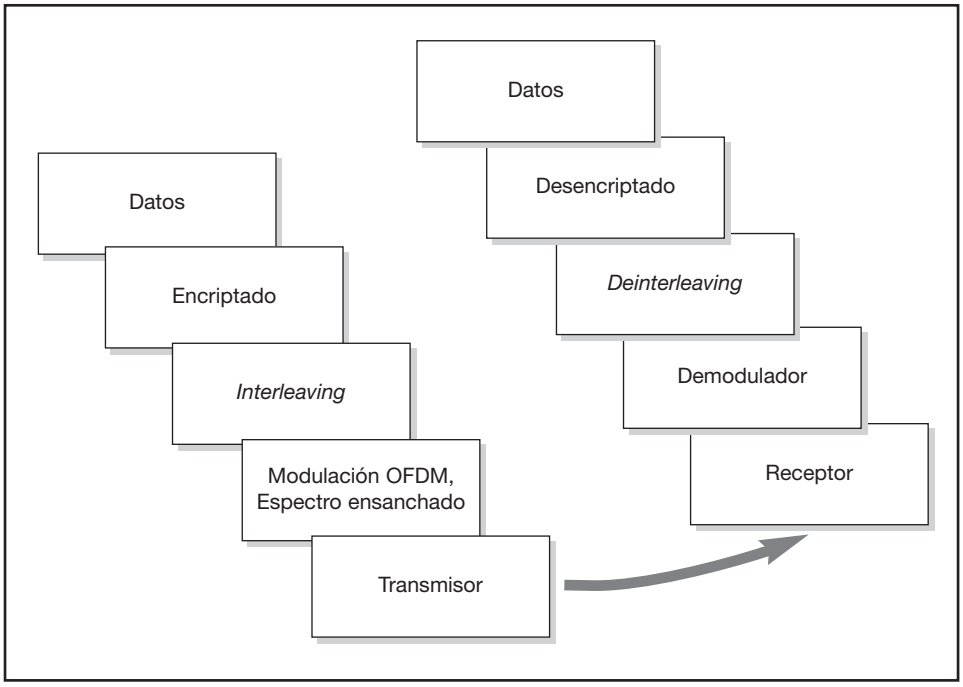


**Figura 6.** *Esquema lógico de técnicas de seguridad.*

El *interleaving* consiste en desordenar de forma pseudoaleatoria los datos. Unida a la codificación del encriptado, resulta complejo su intercepción, ya que los datos aparecen como ruido en el receptor que no conoce el algoritmo.

La modulación también puede ser una parte muy importante del sistema para proporcionar seguridad. En general, las técnicas de espectro ensanchado permiten enviar la información abarcando un espectro muy amplio pero sin enviar mucha potencia en cada banda de frecuencia, lo que las hace difícilmente detectables. Por otra parte, la codificación con la que se ensancha el espectro CDMA (*Frequency Hopping*) tienen siempre un carácter de aleatoriedad que genera robustez frente a aquellos intrusos que no conocen el código. Cambiar la frecuencia central de emisión cada cierto tiempo es también una técnica muy utilizada para dar mayor seguridad a las transmisiones FH (*Frequency Hopping*). Cabe destacar en este punto las redes de baja probabilidad de intercepción LPD. Se trata simplemente de utilizar las características mencionadas del espectro ensanchado llevándolas al extremo, de forma que se transmita una potencia tan baja que la señal quede por debajo de la potencia de ruido. Para cualquier receptor de banda estrecha o que no tenga el código de ensanchado la señal se recibe como ruido indetectable.

*Equipos disponibles en el mercado*

A estas alturas existen numerosos productos en el mercado relacionados con las redes *ad hoc*. En general, podemos encontrar empresas que ofrecen soluciones basadas en ZigBee, WiFi, UWB o en menor medida, WiMAX. Señalamos aquí las más destacadas, que ofrecen soluciones *ad hoc* o *mesh* independientemente de la tecnología de enlace que utilicen. En el cuadro 4, pp. 132-133, se resume la información más relevante de cada compañía y sus productos, señalando una pequeña descripción de cada uno.

*Temas abiertos de investigación*

BATERÍAS/CONSUMO/VIDA ÚTIL

El concepto de redes *ad hoc* o redes *mesh* es relativamente amplio. Se pueden incluir aquí desde redes de una decena de ordenadores personales conectados sin punto de acceso hasta redes de decenas de miles de pequeños sensores distribuidos aleatoriamente por un campo de cultivo con el objetivo de tener medidas de humedad precisas en todos los puntos.

**Cuadro 4.** *Productos* ad hoc *en el mercado.*

| Compañía | Producto | Descripción/Comentarios |
|---|---|---|
| Ascentry | Instantly Deployable Interoperable Communications | Una plataforma *ad hoc* de propósito general que proporciona conectividad. Aplicaciones: seguridad, defensa, redes instantáneas, etc. |
| BTNode | BTNode | Plataforma *hardware* y *software* basada en tecnología Bluetooth como demostración de redes *ad hoc* móviles. |
| Colligo | Conexión *ad hoc* | *Software* para gestionar redes *ad hoc* entre ordenadores personales y portátiles. |
| Dust Networks | Dust Networks' SmartMesh™ | Proporciona una red *mesh* para sensores y sistemas de control de forma totalmente inalámbrica. |
| Firetide | HotPort™ High Performance Mesh Network | Proporciona redes *mesh* que funcionan a 4.0 GHz para situaciones de emergencia. |
| BelAir Networks | BelAir Mesh | Ofrecen redes *mesh* de gran cobertura que soportan movilidad. |
| Kiyon Inc | Kiyon Autonomic Networks | Redes *ad hoc* que no necesitan gestión externa y que soportan cualquier aplicación con cualquier calidad de servicio. |
| LocustWorld | LocustWorld MeshAP | Diseñan redes *mesh* con funcionalidades extras y ofrecen el núcleo del *software* de su diseño en su *web.* |
| Strix Systems | Access/One Network | Desarrollan redes *mesh* empleando sistemas multiradio y multicanal para ofrecer soluciones escalables y flexibles basadas en redes *mesh.* |
| MeshDynamics | Hybrid Mesh™ Networks for Public Safety Network and the Battlefield | Desarrollan redes *mesh* híbridas para uso militar. |

**Cuadro 4.** *(Continuación).*

| Compañía | Producto | Descripción/Comentarios |
|---|---|---|
| AutoNet | AutoNet | Una red *ad hoc* punto a punto para redes de tráfico. |
| Millenial Net | MeshScape™ | Redes *mesh* para comunicaciones en grandes edificios de negocios y entornos difíciles. |
| NovaRoam | Tactical, Practical Meshed Networks™ | Redes robustas y de largo alcance para situaciones de alta movilidad. |
| OrderOne | OrderOne Network | Redes para miles de nodos, con alta movilidad, autoconfigurables. |
| AeroComm | MeshRF™ Protocol | Redes *mesh* de corto alcance a 900 MHz. |
| Sarnoff Corp. | | Redes inalámbricas *ad hoc* para acceso a Internet y en general, comunicaciones corporativas. |
| MobileRoute | Wireless *ad hoc* Routing Protocol | Protocolo de enrutamiento para redes *ad hoc.* |
| Tropos Networks | MetroMesh | Tecnologías de acceso con redes *mesh* para comunicaciones empresariales o urbanas en general. |
| MeshNetworks (ahora Motorola) | Varios | Gran distribuidor y pionero de redes *mesh* y protocolos asociados. Ahora comprada por Motorola. |
| | | |

Sin embargo, prácticamente en todos los casos el concepto de red *mesh* va unido al concepto de autonomía. Autonomía para que la red se configure automáticamente, autonomía para que no se produzcan fallos, o para que se recalculen las rutas si un nodo cae. Pero, evidentemente, también autonomía energética. En algunos la energía será un bien escaso a cuidar (PC portátil) y en otros un recurso limitado que no se puede reponer (nodo en medio del campo, una vez que se queda sin batería, muere).

Por ello un porcentaje altísimo de la investigación en redes *ad hoc* se ha desarrollado entorno al concepto de eficiencia energética. Recortar el gasto de batería en cada una de las tareas que realiza un nodo permite alargar la vida del nodo en la mayoría de los casos, o bien simplemente darle más autonomía, que en ocasiones puede ser vital para que una red tenga utilidad práctica. Será necesario, por lo tanto, analizar dónde se produce el gasto energético y cuál es la mejor manera de limitarlo. En este tipo de redes, el problema energético tiene a veces una dimensión peculiar, ya que muchas veces no se trata de minimizar el consumo en un nodo, sino de maximizar la vida de la red, ya que la existencia o no de un nodo concreto no es importante para muchas aplicaciones.

Mirando la literatura existente se pueden encontrar cientos de artículos que tratan el tema desde aproximaciones muy diversas (24). Desde el punto de vista del nodo, diferentes trabajos desarrollan arquitecturas *hardware* de bajo coste, computación limitada por la energía del nodo, *software* eficiente energéticamente y radios que realizan gestión de potencia. También se han tenido usado modelos no ideales de baterías, que tienen en cuenta las características no lineales de las baterías reales.

Desde el punto de vista de la red, las aproximaciones más importantes son el enrutado eficiente y el protocolo de acceso al medio eficiente. Al hablar de enrutado eficiente energéticamente, cambiamos la perspectiva habitual del enrutado, que es lograr el transporte de los datos en el menor tiempo posible, y migramos a una orientación distinta, que es encontrar las rutas actuales y futuras que maximicen el tiempo de vida de la red. En los protocolos de acceso al medio, encontramos numerosos artículos que intentan discernir qué método de acceso es óptimo, analizando Sistemas CDMA, TDMA, etc., y viendo la mejor manera de no incrementar el tráfico con las gestiones propias de estos protocolos.

### SEGURIDAD

Como hemos mencionado antes el tema de seguridad es crítico en comunicaciones inalámbricas, tanto militares como civiles. Hasta la fecha se han

desarrollado multitud de algoritmos en todos los niveles que pretenden proporcionar un nivel de seguridad determinado a una red concreta.

El desarrollo más conocido es el relacionado con redes inalámbricas 802.11. En este estándar se incluye el protocolo WEP (*Wire Equivalent Protocol*) como intento de simular la seguridad de redes cableadas, utilizando claves cifradas para cada usuario registrado.

Un aspecto muy importante y que aún representa un reto es la habilidad de autentificar las fuentes de información de una manera fiable. En entornos militares, o en aplicaciones de transacciones comerciales es una cuestión crítica. Hay diversas maneras de llevar a cabo, todas ellos englobadas bajo el acrónimo PKI (*Public Key Infrastucture*), y son actualmente uno de los puntos calientes en la investigación.

Otro aspecto en desarrollo actualmente es el proporcionar seguridad en las redes inalámbricas mediante la conexión a través de redes privadas virtuales. El gran problema que esto representa es que es una seguridad a nivel tres o superiores, y necesita ser acompañada por otros mecanismos de niveles inferiores.

En esta misma línea, el uso de Firewalls especializados en comunicaciones inalámbricas es otra línea de investigación importante en estos momentos para aplicaciones como WAP (21).

La criptografía utilizada en el 802.11 es conocida y presenta ya dificultades, por lo que nuevos algoritmos son necesarios. Hasta ahora, otros protocolos utilizaban técnicas que incluían el uso de certificados y técnicas de gestión de claves simétricas. En cualquier caso, todos estos tipos de técnicas asumen el conocimiento previo de algún tipo de semilla con el que generar la clave. En una red *ad hoc* las dificultades que esto implica son grandes, debido a la gran movilidad de los nodos y la variabilidad de la topología (25).

La autenticación de los nodos es otro problema en el que sigue habiendo muchos puntos oscuros. En WiFi se utiliza un protocolo basado en claves encriptadas compartidas, que utilizan la dirección de la tarjeta MAC. Si un atacante escucha la conversación y es capaz de leer la dirección de la tarjeta la seguridad de la red estará comprometida.

Frente a todos estos problemas una serie de nuevos estándares están siendo desarrollados. De ellos destacamos PIC (*Pre-IKE Credential*), en el que existe un servidor de licencias donde cada usuario debe solicitar una clave que luego utilizará en sus otras comunicaciones. También en desa-

rrollo está OMAP, un protocolo de Texas Instruments que implementa una librería de *software* que se usará en terminales y nodos inalámbricos utilizados para transacciones comerciales. MeT es un consorcio de grandes productores de teléfonos móviles para afrontar estos temas de seguridad. Por último la utilización técnicas biométricas conforma el estado del arte de las tecnologías de seguridad inalámbrica.

## Análisis de prestaciones y limitaciones en campo militar de las redes *ad hoc*

*Seguridad*

Una vez analizadas las técnicas generales de seguridad para redes inalámbricas, analizamos los requerimientos típicos de las comunicaciones militares (26, 27 y 28). En este escenario, surge el concepto de seguridad multinivel. En este concepto las entidades no son simplemente seguras o inseguras, sino que tienen diversos grados de sensibilidad (como difusión limitada, confidencial, reservado o secreto) que origina la coexistencia simultáneamente de distintas redes en el teatro de operaciones o zona de crisis. Los esquemas deben, por tanto, proporcionar comunicaciones que puedan soportar estas clasificaciones. Evidentemente, en redes *ad hoc*, esto debe ser conseguido por protocolos de enrutado complejos.

Para ello, se deben asegurar los siguientes requerimientos:

— Todos los nodos participantes en un protocolo deben tener un determinado nivel de privilegio de lectura y transmisión. Cada entidad leerá o transmitirá sólo aquellos mensajes que tiene permitido por ese nivel.
— Todos los mensajes intercambiados por el canal deben tener un nivel en la clasificación anterior.
— Todos los nodos deben ser autenticados correctamente antes de poder participar en la comunicación.
— El origen de los datos puede ser cualquier participante, siempre y cuando transmita mensajes que estén dentro de sus limitaciones de seguridad.
— Los nodos de mayor nivel pueden leer todos los mensajes y tomar todas las decisiones, y pueden transmitir en cualquier nivel.
— Es necesario disponer de mecanismos para echar a un miembro del grupo.
— Los datos deben ser totalmente secretos de cara a agentes externos a la red.

— Es necesario que la identidad de los miembros legítimos del grupo permanezca también en secreto, para evitar intrusos suplantadores.

Dentro del genérico mundo de las redes *ad hoc* móviles existen protocolos que tratan de ofrecer seguridad en sus transmisiones, dando solución al problema que conlleva la seguridad multinivel en un escenario de difusión multisalto. Algunos de ellos son:

— ARAN (*Authenticated Routing for Ad hoc Networks*). Es un protocolo de enrutado reactivo, que usa certificados encriptados para asegurar la seguridad en el enrutado. El problema que tiene es que usa criptografía asimétrica, que no es adecuada para una red *ad hoc* en la que todos los nodos son parecidos en complejidad.
— Ariadne: basado en MAC (*Messae Authentication Code*) y TESLA, un protocolo de gestión de claves. Necesita que el transmisor sea consciente de la topología de la red y no permite que el receptor autentifique un paquete inmediatamente a su llegada. Además no proporciona confidencialidad en los mensajes.
— LHAP (*Lightwight Hop-by-hop Authentication Protocol*). Está diseñado para una red genérica. Requiere un gran número de operaciones por nodo para asegurar la seguridad.
— SAR (*Security-aware Ad hoc Routing*). Asigna distintos niveles de seguridad a cada nodo y los paquetes sólo pueden ir enrutados por nodos de igual nivel de seguridad. Esta restricción en el camino que puede tomar el paquete es excesiva para una red *ad hoc*.

Finalmente, algunos trabajos tratan de cubrir todos los requerimientos, como el de (M. Choudhary), que integran todas las características permitiendo diferenciar cada individuo o paquete según distintos niveles de seguridad.

En resumen, observamos como el tema de seguridad en comunicaciones inalámbricas, especialmente militares donde los requerimientos son más estrictos, es un tema abierto tanto en investigación, como en desarrollo, como a nivel de mercado. Existen soluciones probadas y robustas pero que no ofrecen toda seguridad requerida. Los protocolos más avanzados están todavía en sus primeras fases de desarrollo. Representa por tanto un aspecto clave de este tipo de comunicaciones, en especial en las basadas en redes *ad hoc*.

*Robustez*

Al describir los distintos tipos de redes *ad hoc* utilizables en entornos militares hemos hecho mención a los problemas y ventajas de robustez que

las redes *ad hoc* representan. En este apartado, se resumen los aspectos más importantes teniendo en cuenta las distintas opciones (7).

En primer lugar, cabe destacar que el uso de las redes *ad hoc* se considera apropiado para aplicaciones militares por dos motivos fundamentales: rapidez de despliegue y flexibilidad y por la robustez de esta solución. Como ya hemos mencionado, la gran ventaja de una topología mallada pura es que ningún nodo es imprescindible, y por tanto, si el diseño de la red está bien realizado, y se dan las condiciones de conectividad necesarias, no existe ninguna otra configuración más segura frente a pérdidas de nodos o ataques externos.

Sin embargo, este primer análisis debe puntualizarse brevemente. En primer lugar porque las condiciones de conectividad necesarias implican que cada nodo tenga en su rango de cobertura a varios nodos, cuantos más mejor, y que la red no se disgregue en ningún momento en pequeñas redes, es decir, que exista una continuidad en la malla formada por los nodos. Esto no siempre será posible, en especial en situaciones conflictivas o en zonas controladas o cercadas por el enemigo, o en zonas montañosas.

Existen además casos especiales como unidades aisladas o soldados en campo enemigo que no deberían o no querrían delatar su posición con una transmisión continua necesaria para actuar como repetidores en una red *mesh*.

Por tanto para asegurar la conectividad y la robustez es necesario, bien de asegurar la existencia de una densidad de nodos suficiente, bien dotar a la red de puntos de acceso visibles por todos los nodos, a modo de eje troncal, con algunas de las soluciones indicadas en el primer apartado.

Por supuesto, estas soluciones por sí mismas son menos robustas que una red mallada pura, a no ser que se disponga de una redundancia suficiente de nodos troncales. Uniendo ambas aproximaciones, la red mallada pura y la red, se obtendría, desde el punto de vista de la estructura de la red y la conectividad, un sistema robusto resistente a fallos y ataques.

Queda sin embargo, el análisis de robustez en capas superiores, íntimamente ligado al de la seguridad. El uso de sistemas de espectro ensanchado, por ejemplo, proporciona robustez en el nivel físico, ya que hace más difícil producir una interferencia malintencionada. Otros sistemas, como los de encriptación y autenticación proporcionan robustez en las comunicaciones a niveles superiores.

Por todo lo expuesto, se puede concluir que aunque la robustez en las redes *ad hoc* es aún tema abierto, con mucho camino de investigación por delante, con el diseño adecuado y conjuntamente con soluciones híbridas, las redes *mesh* representan una opción que mejora la robustez de los sistemas en comunicaciones tácticas, que es donde su uso es más indicado.

*Utilización en comunicaciones*
*de nivel estratégico y nivel operacional*

A lo largo de los primeros apartados hemos analizado los tipos de redes *mesh* y sus características, así como el estado del arte de las tecnologías implicadas y los productos existentes. Este apartado recoge las ideas desarrolladas para concluir con la viabilidad del uso de las redes *ah hoc* en comunicaciones de nivel estratégico y operacional. El siguiente apartado lo hará con las comunicaciones tácticas.

De entre las características exigibles en una red de este tipo destacan la fiabilidad y robustez de la red, una facilidad relativa de despliegue, un alcance amplio, y una seguridad de muy alto nivel.

Si bien todas estas características se pueden alcanzar con una red *ad hoc* con tipología mallada pura, no existe en la práctica ninguna necesidad de recurrir a estos sistemas novedosos que añaden tanta complejidad a los nodos.

Como se ha explicado anteriormente, la fiabilidad y robustez de la red se pueden alcanzar con redes híbridas, o redes celulares de rápido despliegue, que utilicen un único salto inalámbrico y luego encaminen los datos por canales más robustos. El despliegue, que no tiene que ser tan ágil como en el campo de batalla, se adapta perfectamente a las características de las redes híbridas o a las soluciones basadas en telefonía celular de rápido despliegue. La seguridad, incluso, mejora si optamos por redes con menos saltos inalámbricos.

Por tanto, en comunicaciones de nivel estratégico y nivel operacional resulta conveniente el uso de redes *ad hoc* que utilicen algún tipo de jerarquía, o soluciones híbridas en los que la zona mallada o *ad hoc* sea sólo el salto final hacia el posible usuario móvil. Estos tipos de redes se han descrito en el primer apartado, y representan las alternativas más claras para las comunicaciones mencionadas, como así los atestiguan los numerosos casos prácticos llevados a cabo.

*Utilización en comunicaciones de nivel táctico*

Las comunicaciones de nivel táctico deben ser robustas, seguras y permitir rapidez en el despliegue. Además, el número de nodos a comunicar puede ser elevado, y la topología muy cambiante.

Para la realización práctica de una red de estas características resulta conveniente el tipo de red *ad hoc* mallada pura. Una estructura *mesh* permite, siempre y cuando la densidad de nodos sea suficiente, una red de comunicaciones muy robusta y de despliegue inmediato.

Reforzar estas redes con enlaces de reserva que usen nodos troncales, es una buena táctica que asegura la comunicación en situaciones especiales en las que la densidad de nodos no es suficiente o las circunstancias así lo aconsejan.

Para ello, cada soldado, vehículo móvil, elemento de artillería, etc., puede representar un candidato ideal para soportar un nodo. Un despliegue masivo de centenares o incluso miles de nodos pequeños y difícilmente detectables asegura una conectividad total, y es otra de las alternativas en investigación en la actualidad.

De todo lo descrito se desprende que las redes *mesh* puras representan potencialmente el núcleo futuro de las comunicaciones de nivel táctico, siempre y cuando los retos tecnológicos a los que se enfrentan estas complejas redes sean soluciones, y siempre y cuando los diseños se vean reforzados por otras redes clásicas para situaciones especiales.

## Aplicaciones avanzadas de redes *ad hoc*

Existen muchas aplicaciones específicas de este tipo de redes en el entorno militar. En primer lugar están las de comunicaciones que se han comentado ya. También existen muchas basadas en redes de sensores. Describimos las líneas generales de los grandes grupos de aplicaciones, algunas de ellas en desarrollo (2 y 29).

*Comunicaciones*

Como se han comentado hasta ahora, una aplicación importante de las redes *ad hoc* en campo militar es su capacidad para proporcionar redes de comunicación de rápido despliegue, flexible, móviles y robustas frente a ataques, en especial para comunicaciones tácticas.

*Monitorización de fuerzas amigas, equipamiento y munición*

En una situación de conflicto el equipo de mando puede monitorizar constantemente el estado de sus tropas, las condiciones y disponibilidad del equipamiento y la munición en el campo de batalla. Cada tropa, vehículo, equipamiento y munición crítica puede llevar un nodo que informe sobre su estado. La información se envía a nodos con capacidad de transmisión de gran ancho de banda que lo reenvían al centro de mando.

*Vigilancia en campo de batalla*

Terrenos críticos, rutas de acceso y caminos importantes pueden ser objeto de un despliegue de redes de sensores que permitan monitorizarlas. De esta manera, en todo momento se puede recopilar información sobre la actividad en esos puntos.

*Reconocimiento de las fuerzas enemigas y los terrenos ocupados*

Pequeños nodos, casi indetectables, pueden ser dispuestos en el terreno enemigo para obtener información valiosa y detallada sobre su posición y otros parámetros importantes.

*Información sobre daños*

Antes y después de un ataque se pueden desplegar redes de sensores que cuantifiquen los daños y realicen un informe de la situación.

*Detección precoz de ataques NBQ*

La detección precoz de un ataque de estos tipos es muy importante, pero muy complicada sin poner en peligro a seres humanos. Desplegar una red por toda la zona de interés permite avisar de ataques NBQ, y además determinar la naturaleza del ataque.

*Localización*

Las redes *mesh* tienen la capacidad de ofrecer un sistema de posicionamiento 3D de alta precisión. También permiten realizar el seguimiento del objetivo y todo ello sin la necesidad de usar satélites. Extraer información de localización mediante el Sistema de Posicionamiento Global (GPS)

siempre es más complicado que cuadrar la posición de un objetivo con nodos situados a escasos cientos de metros entre sí. Los sistemas actuales basados en esta tecnología (*mesh netoworks position system*) permiten precisiones de menos de 10 m a velocidades mayores de 250 km/h.

*Seguimiento de vehículos militares*

Cada vehículo militar amigo puede llevar incorporado un nodo que le permita dar su posición a los nodos más cercanos, que, formando una red *ad hoc* envían la información al centro de mando.

*Despliegue de minas inteligentes*

Las minas antitanque son equipadas con equipos de comunicaciones y sensado que aseguran que una determinada zona está cubierta. Si se detecta el fallo de una mina en una zona se envía el mensaje para que sea sustituida.

*Localización de francotiradores*

Detectar y localizar de forma precisa francotiradores es una tarea complicada para la que no existe hasta ahora una solución fiable. Existen múltiples aproximaciones a este problema, algunas de ellas basadas en redes *ad hoc*. La más actual y más potente consiste en una red *ad hoc* compuesta de sensores inalámbricos de bajo coste. Después del despliegue los sensores sincronizan sus relojes, se auto-organizan y esperan eventos acústicos. Los sensores pueden compartir la información que detectan y conseguir así detectar un sonido de bala, calcular su velocidad y su dirección, de manera que pueden estimar la posición donde se generó el disparo.

**Bibliografía**


(1) Ramanathan, R. y Redi, J. (2002): «A brief overview of ad hoc networks: Challenges and directions», IEEE *Commun. Mag.,* vol. 40, n.º 5, pp. 20-22, mayo de 2002.

(2) Akyildiz, I. F.; Su, W.; Sankarasubramanian, Y. y Cacyirci, E. (2002): «Wireless sensor networks: a survey», Computer Networks (Elsevier) *Journal,* vol. 38, n.º 4, pp. 393-422, marzo de 2002.

(3) Akyildiz, I. F.; Wang, X. y Wang, W.: «Wireless mesh networks: a survey», to appear, *Computer Networks Journal* (Elsevier).

(4) MeshNetworks, «Mesh Networks Technologies», Now Wireless Limited, en: *http://mesh.nowwireless.com/technology.htm*

(5) Buckner, M. A. y Batsell, S. (2001): «Mobile Ad Hoc Networking», Sensors Magazine Online, enero de 2001 en: *http://www.sensorsmag.com*

(6) Poor, R. (2003): «Wireless Mesh Networks», Sensors Magazine Online, Intelligent Systems, febrero de 2003 en: *http://www.sensorsmag.com*

(7) Feldman, P. M. (1998): «Emerging Commercial Mobile Technology and Standars: Suitable for the Army?», RAND Documents, ref. MR-960-A, pp. xvii-80, RAND Corporation, 1998.

(8) Nilsson, J.; Hansson, A. y Sterner, U. (2000): *The ability to provide services in military radio networks-A feasibility study,* IEEE, 2000.

(9) Chong, C. Y. y Kumar, S. P. (2003): «Sensor Networks: Evolution, Opportunities and Challenges», Proc. Of the IEEE, *Invited Paper,* agosto de 2003.

(10) Kolic, R. (2004): «An introduction to Ultra Wideband (UWB) wireless», Technology@Intel Magazine en: *http://www.intel.com/technology/magazine/* Intel Corp. 2004.

(11) Breeze Wireless Communications Ltd. «IEEE 802.11 Technical Tutorial», Wireless Communication en: *http://www.breezecom.com*

(12) IEEE Standard, (1997): «802.11. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications», 1997.

(13) Huidrobo, J. M.: «WiMAX. ¿El sustituto de WiFi?» en: *http://www.monografías.com*

(14) Hawk, J. (2005): «WiMAX Paln Aims To Cut Army Costs» Signal AFCEA's en *International Journal,* septiembre de 2005.

(15) Vázquez, D. (2005): «Homeplug y ZigBee» en: *http://www.casadomo.es* mayo de 2005.

(16) ZigBee Alliance: «ZigBee Specification» en: *http://www.zigbee.org/*

(17) Jones, C.; Sivalingam, K. M.; Agrawal, P. y Chen, J. C. (2001): «A survey of Energy Efficient Networks Protocols for Wireless Networks» en *Wireless Networks,* n.º 7, pp. 343-358, Kluwer Academic Publishers, 2001.

(18) Al-Karaki, J. N. y Kamal, A. E. (2004): *Routing techniques in wireless sensor networks: a survey,* Wireless Sensor Networks, IEEE, 2004.

(19) Jiang, Q. y Manivannan, D. (2004): *Routing protocols for Sensor Networks,* IEEE, 2004.

(20) Sensors Magazine Online en: *http://www.sensorsmag.com*

(21) Miller, S. K. (2001): «Facing the challenge of wireless security» en *Technology News,* Computer Mag., julio de 2001.

(22) Welch, D. y Lathrop, S. (2003): *Wireless Security Threat Taxonomy,* Proc. Of the 2003 IEEE Workshop on Information Assurance. West Point, USA, junio de 2003.

(23) Manges, W. W. y Allgood, G. O. (2002): «How Secure Is Secure?», Sensors Magazine Online, Intelligent Systems, febrero de 2002 en: *http://www.sensorsmag.com*

(24) Raghunathan, V.; Schurgers, C.; Park, S. y Srivastava, M. B. (2002): «Energy-aware wireless microsensor networks«, IEE Signal Processing Magazine, IEEE, marzo de 2002.

(25) Balakrishnan, V. y Varadharajan, Vijay (2005): «Designing Secure Wireless Mobile Ad hoc Networks», Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05), IEEE, 2005.

(26) HARRINGTON, J. J. y PRITCHARD, D. A. (1997): «Concepts and Applications of Wireless Security Systems for Tactical, Portable, and Fixed Sites», IEEE, 1997.

(27) CHOUDHARY, M.; SHARMA, P. y SHANGI, D. (2004): «Secure Multicast model for ad hoc military networks», IEEE, 2004.

(28) NIRANJAN, A. GANZ (2004): «Adaptative Link Layer Security for wireless networks, (ALL-SEC)», 2004 IEEE Military Communications Conference, IEEE, 2004.

(29) MAROTI, M.; SIMON, G.; LEDECZI, A. y SZTIPANOVIT, J. (2004): «Shooter Localization in Urban Terrain» en *Computer Magazine,* agosto de 2004.

(30) RÖMER, K. y MATTERN, F. (2004): «The design space of wireless sensor networks», IEEE Wireless Comm. Magazine, IEEE, diciembre de 2004.

## COMPOSICIÓN DEL GRUPO DE TRABAJO

D. DAVID RÍOS INSUA
*Catedrático de Estadística e Investigación Operativa. Vicerrector de Nuevas Tecnologías de la Universidad Rey Juan Carlos. Numerario (electo) de la Real Academia de Ciencias Exactas, Físicas y Naturales.*

D. JOSÉ ANTONIO VALDIVIESO DUMONT
*Coronel (DEM). Profesor del CESEDEN.*

D. CARLOS ALBERICH LANDÁBURU
*Teniente coronel. Jefe de Redes y Servicios de Red del CCEA del Ministerio de Defensa.*

D. FRANCISCO JAVIER RAMOS LÓPEZ
*Director de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Rey Juan Carlos.*

D. JOSÉ MIGUEL CASTILLO CHAMORRO
*Teniente coronel. Secretario de Estudios de la Escuela de Informática del Ejército.*

D. LUIS PASTOR PÉREZ
*Catedrático de Arquitectura y Tecnología de Computadores. Director del Departamento de Arquitectura y Tecnología de Computadores y Ciencia de la Computación e Inteligencia Artificial de la Universidad Rey Juan Carlos.*

D. EUGENIO FERNÁNDEZ VICENTE
*Profesor Titular EU. Director Académico del Servicio de Informática de la Universidad Rey Juan Carlos.*

D. ISAÍAS PERAL PUEBLA
*Coronel de Transmisiones. Jefe de Comunicaciones e Informática de la Casa de Su Majestad el Rey.*