

# DARP – Protocolo de radio adaptativo y dinámico

Francisco José Estévez<sup>1</sup>, Alejandro Fernández<sup>2</sup>, Jesús González<sup>3</sup>, José Manuel Palomares<sup>4</sup> y Miguel Damas<sup>5</sup>

*Resumen*— El protocolo de red DARP, posee una serie de características únicas como son, nodos con roles dinámicos, gestión de la inteligencia de red de forma externa a la propia red o estructuración en subredes virtuales. Tal y como se discute a lo largo del presente artículo, estas características resultan de especial interés para el desarrollo de redes inalámbricas ubicuas. Destacar que un gran número de necesidades de este tipo de redes no se encuentran cubiertas actualmente por los principales protocolos de comunicaciones inalámbricas existentes. Esta carencia hace necesaria una propuesta que cubra ese déficit y para ello presentamos DARP.

*Palabras clave*— Redes inalámbricas de sensores, ZigBee, 6LoWPAN.

## I. INTRODUCCIÓN

**W**IRELESS SENSOR NETWORKS O WSN, es un término que hace referencia a las redes inalámbricas de sensores. Estas redes se encuentran actualmente en un momento de gran importancia dado el auge en proyectos de computación ubicua y a las acuciantes necesidades de gestión distribuida de las sociedades modernas. En estas áreas, es donde estas redes son especialmente útiles y, donde gracias a su rápida expansión y a sus particulares características se ha acuñado el término *Ubiquitous Sensor Networks* o USN.

Las redes anteriormente comentadas, son consideradas ubicuas cuando se componen de un amplio número de dispositivos, siendo esta la esencia del *Internet of Things* (IoT) o Internet de las cosas. El Internet de las cosas, es un concepto en el que todos los objetos que conforman nuestro entorno poseen un mínimo de inteligencia y se encuentran conectados mediante una red común. Como se puede deducir, estos conceptos están estrechamente relacionados dada la necesidad de un medio de comunicación ágil que permita la interconexión de dispositivos, siendo esta la base de las redes ubicuas o USN.

En el campo de las USN existen diversos protocolos de comunicaciones que permiten su aplicación práctica. Cada uno de estos protocolos cuenta con sus propias características definidas vía estándares. La popularidad de las WSN ha propiciado la aparición de múltiples protocolos como *ZigBee* [1], *6LoWPAN* [7], *WirelessHART* o *Isa 100.11a*. Actualmente son

los más utilizados y han sido ampliamente probados y verificados, arrojando interesantes resultados en el ámbito de las redes inalámbricas de sensores, aunque también presentan numerosos problemas en su aplicación a redes ubicuas.

Desde hace un par de años las características requeridas para la aplicación y el desarrollo de las USN vienen cambiando, esto ha llevado a unos resultados no muy buenos para los protocolos de comunicaciones existentes actualmente, y en concreto para *ZigBee* y *6LoWPAN*. Los nuevos escenarios de aplicación surgidos con las USN y los cambios en las necesidades de la sociedad [13] [11], han provocado que estas redes adquieran especial interés de cara a resolver problemas asociados con la adaptabilidad y dinamismo de las topologías de red, robustez, sencillez, bajo consumo o bajas tasas de comunicaciones. Además de estas características, los nuevos escenarios de aplicación, presentan entornos hostiles y amplios problemas de saturación y coexistencia en las bandas de frecuencia típicamente utilizadas por estos protocolos.

Dadas estas nuevas características [15], en este artículo se presenta un nuevo protocolo de comunicaciones para USN, basado en la adaptabilidad, sencillez, dinamismo y en el funcionamiento en diversas bandas de frecuencia, características imprescindibles en los escenarios actuales. Para proporcionar una visión general se presentan las principales características de los protocolos para WSN disponibles actualmente. Se realiza a continuación una discusión de sus carencias y fortalezas para, en el siguiente capítulo especificar en profundidad nuestra propuesta. Se discuten después, los detalles de implementación acerca de nuestra propuesta, se muestran las pruebas y los resultados obtenidos, y finalmente se presentan una serie de conclusiones y se discute acerca de las mismas.

## II. ESTADO DEL ARTE

Las redes inalámbricas de sensores se han asentado como un importante área de trabajo en los últimos años. Actualmente se están llevando a cabo numerosas investigaciones en todos los ámbitos que abarcan las WSN. Estos estudios se están centrando en necesidades como el número de dispositivos que pueden soportar estas redes, aspecto muy importante para evolucionar hacia redes ubicuas del tipo USN. También se estudian aspectos de eficiencia energética que permitan aumentar el tiempo de vida útil de los dispositivos. Se buscan además, mejoras en la capacidad de transmisión de los canales de comunicación utili-

<sup>1</sup>Dpto. Arquitectura y Tecnología de Computadores, Univ. Granada, e-mail: fjestevez@ieee.org.

<sup>2</sup>e-mail: alexfcabezas@gmail.com.

<sup>3</sup>Dpto. Arquitectura y Tecnología de Computadores, Univ. Granada, e-mail: jesus@atc.ugr.es.

<sup>4</sup>Dpto. de Arquitectura de Computadores, Univ. Córdoba, e-mail: jmpalomares@uco.es.

<sup>5</sup>Dpto. Arquitectura y Tecnología de Computadores, Univ. Granada, e-mail: mdamas@atc.ugr.es.

zados, interoperabilidad entre diferentes tecnologías e incluso se están iniciando investigaciones acerca de la necesidad de gestionar eficientemente millones de dispositivos con independencia de los protocolos de comunicaciones que utilicen.

Estas necesidades que ahora son objeto de investigación se encuentran recogidas en su mayoría en el estándar *IEEE 802.15.4* [10], siendo éste el estándar en el que se basan las principales WSN. Este estándar recoge una serie de características que son comunes a la práctica totalidad de protocolos de comunicaciones disponibles en este área. Concretamente, comprende las capas física (PHY) y de acceso al medio (MAC) y opera en las bandas de frecuencia de 868 MHz y 2.4 GHz. Las bandas de frecuencia tienen ciertas características especiales, para comenzar, la frecuencia de 868 MHz tiene un único canal disponible y el máximo ancho de banda que permite es de 100 kb/s, en cambio, su propagación y alcance son mucho mayores, del orden de varios cientos de metros. Por otro lado, la frecuencia de 2.4 GHz, posee 10 canales, y permite llegar a transmitir a 1 Mb/s, en cambio su alcance es muy limitado, normalmente de decenas de metros. Además, la frecuencia de 2.4 GHz se ve muy afectada por los factores ambientales y el entorno. En el estándar se encuentran definidas también, dos topologías de red: en estrella y punto a punto, así como dos tipos de nodos: *Full Function Device* (FFD) o *Reduce Function Device* (RFD). La topología y los nodos deben ser prefijados antes del inicio de la red, de forma muy rígida. Se debe destacar también que este tipo de redes dependen completamente de un nodo FFD que mantiene el control sobre toda la red.

En este sentido se han desarrollado nuevas topologías de red como son en árbol y en malla. La topología en malla es una topología que permite la interconexión de todos los nodos en la red. Este tipo de topología presenta ciertas ventajas sobre las básicas que ofrece el estándar 802.15.4, aunque conlleva un considerable aumento en la complejidad y del tráfico en la red dada la cantidad de enlaces entre nodos que deben ser mantenidos. Presenta además, la necesidad de dispositivos más potentes y perjudica el ahorro energético, lo cuál es una característica indispensable de estas redes. La topología en árbol es ligeramente diferente de la topología en malla. Esta topología aunque permite la comunicación entre diferentes nodos a lo largo del árbol, obliga a realizar un recorrido con un mayor número de saltos. En este tipo de estructuras es posible minimizar el número de enlaces entre nodos a mantener, se puede jerarquizar la toma de decisiones en la red y la gestión energética es más eficiente.

Al respecto de todos estos detalles, se debe destacar que el estándar *IEEE 802.15.4* posee una serie de fortalezas y debilidades que deben ser comentadas antes de proseguir. Estas fortalezas y debilidades son heredadas por todos los protocolos de comunicaciones que son utilizados para WSN. Las principales fortalezas radican en su escalabilidad, robustez y configuración. Es decir, el estándar permite escalar

diversos niveles de redes y cada una de ellas puede componerse de cientos de dispositivos. Permite además utilizar una dirección especial una vez un nodo se ha conectado a la red, evitando propagar su dirección MAC y liberando espacio para aumentar la carga útil de las tramas. Otra fortaleza de este estándar es la robustez, ésta se puede observar en la forma en que se controlan los enlaces entre nodos. Esta tarea se realiza de forma periódica, permitiendo un alto grado de control de los elementos disponibles en la red y una buena gestión energética. Por último, el estándar *IEEE 802.15.4* ofrece, un alto grado de configuración, lo cual queda demostrado con los diversos protocolos de red que lo utilizan como base.

En cuanto a sus debilidades, la principal es la necesidad de mantener un nodo FFD con conocimiento de todos los elementos que conforman la red [3]. Esto representa una importante amenaza en redes del tipo USN, dada la densidad y la masificación de los canales de comunicaciones, lo que puede derivar en la incapacidad del nodo coordinador para gestionar la red correctamente. Destacar también la limitación que existe con respecto al número de nodos que permite manejar. Esta limitación es muy importante, dado que cuanto mayor es el número de nodos disponibles, peor es el desempeño del nodo que gestiona el enrutamiento y que debe enrutar los mensajes hacia el resto de dispositivos que componen la red. Otra potencial debilidad es la no limitación en la adición de nodos a la red. Esto provoca que cualquier técnica de suplantación de identidad permita a un nodo introducirse en la red, o que las redes queden desbalanceadas con el perjuicio en el desempeño de las comunicaciones que este hecho supone.

Dentro de los protocolos que se basan en el estándar 802.15.4 se encuentra el protocolo de red *ZigBee*. Este se utiliza en una amplia gama de productos y aplicaciones en todo el mundo, siendo como se comentó anteriormente el más utilizado actualmente. *ZigBee* se basa en el estándar *IEEE 802.15.4*, y define las especificaciones de la capa de red para topologías en malla y árbol. *ZigBee* proporciona además un marco bien definido para la programación en la capa de aplicación, así como una capa de seguridad adicional. *ZigBee* permite redes con hasta 65535 nodos estructurados en subredes de 255 elementos. Posee tres tipos de nodos: coordinador, *router* (se corresponden con FFDs en el estándar) y nodo final (se corresponde con un RFD en el estándar). La principal característica de *ZigBee* es la eficiencia energética, que en este protocolo es llevada al extremo.

*ZigBee* además de las características anteriormente citadas, posee una serie de problemas, cuya importancia varía en función de la aplicación.

- El problema de los nodos huérfanos: No se garantiza que un dispositivo se una a una red aunque haya posiciones libres en el espacio de direcciones de la red [12].
- Si se quiere mantener un tiempo de servicio de paquetes medio por debajo de la duración de la supertrama, el tamaño de la red debe man-

tenerse muy pequeño, hasta 40 nodos, incluso para tamaños de paquetes pequeños/moderados y para tasas de llegada de paquetes pequeñas/moderadas [9].

- La media de retrasos en los accesos a búfer es alta, incluso para tamaños de red pequeños. Esto puede afectar seriamente a las aplicaciones con límites estrictos de tiempo [8], por lo que conlleva trabajar con un hardware más específico elevando el coste de los dispositivos.
- Cuello de botella en el nodo coordinador a la hora de gestionar la red. Este problema es probablemente el problema más serio al que se enfrentan las redes *ZigBee*. Se manifiesta en redes muy densas, y conlleva problemas de *Quality of Service* (QoS) y denegación de servicio, provocando la imposibilidad de gestionar la red y de desempeñar las tareas de comunicación para la que ha sido diseñado.

Otro de los protocolos más utilizados y que también utiliza como base el estándar 802.15.4 es *6LoWPAN*. En este se definen los mecanismos para realizar la compresión y fragmentación de cabeceras y permitir la comunicación IPv6 [5] [6] sobre el estándar *IEEE 802.15.4*. En la especificación se describen los elementos clave de la capa de adaptación que se sitúa por encima del nivel de acceso al medio. *6LoWPAN* está compuesto de tres elementos principales:

*Compresión de la cabecera* Los campos de cabecera IPv6 se eliminan de un paquete cuando la capa de adaptación puede derivarla de la información transportada por el nivel de enlace en la trama 802.15.4.

*Fragmentación* Los paquetes IPv6 se fragmentan en múltiples tramas a nivel de enlace para cumplir con el requerimiento mínimo de tamaño de trama (MTU) que establece IPv6.

*Reenvío de mensajes* Para soportar el envío de paquetes IPv6 la capa de adaptación puede resolver las direcciones de la capa de enlace a la finalización de un salto IPv6.

El concepto clave de aplicar la capa de adaptación *6LoWPAN*, es la utilización de compresión estática para proveer de un método de adaptación que se pueda aplicar a los campos de cabecera, a la red y a la capa de transporte. Se puede observar que es posible comprimir los campos de cabecera en unos pocos bits cuando observamos que a menudo se imponen valores comunes, reservando un valor de escape para cuando otros valores menos comunes aparezcan. Los valores más comunes se producen debido al uso frecuente de un subconjunto de funcionalidades IPv6 (como UDP, TCP e ICMPv6 como valores de la siguiente cabecera) y los supuestos simples de contexto compartido (por ejemplo, un prefijo común de enrutamiento global para una red de área personal). *6LoWPAN* también evita mantener información redundante de los encabezamientos a lo largo de las capas que tiene el protocolo (por ejemplo, los campos de longitud y las direcciones IPv6 son eliminadas

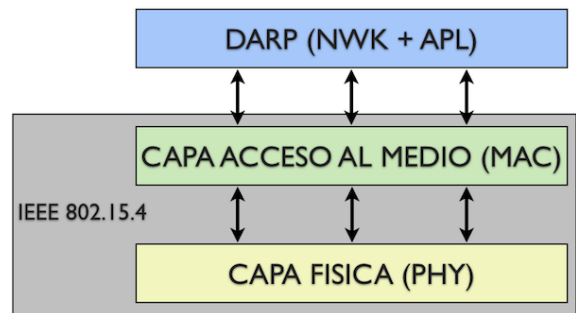


Fig. 1. Pila del protocolo DARP.

de los encabezamientos de las capas inferiores).

Además de las fortalezas derivadas del estándar *IEEE 802.15.4*, y de compatibilidad con IPv6, *6LoWPAN* posee diversos inconvenientes que se describen a continuación [4].

- El protocolo de enrutado RPL (*Routing Protocol for Low Power and Lossy Networks*) permite tener un nodo que realiza las funciones de coordinador pero que es seleccionado de forma dinámica. Esta característica busca minimizar el impacto de problemas con el nodo coordinador de la red, pero a su vez conlleva un elevado tráfico y caídas constantes para rearmar la propia red, con todos los inconvenientes de trazabilidad que esto representa. En una red ubicua de tipo USN, este planteamiento conllevaría una sobrecarga que dejaría fuera de servicio a determinadas partes de la red dado el numeroso tráfico que conlleva este método de selección de nodos.
- *6LoWPAN* presenta muchos más problemas a nivel energético, al tener los dispositivos mayores necesidades de comunicación para mantener constantemente las redes activas y poder modificar dinámicamente el nodo coordinador de la red.

### III. PROPUESTA DE PROTOCOLO DE RED

Tal y como se ha descrito en las secciones anteriores, existen diversas carencias en los protocolos de comunicaciones actuales. Para solventar este hecho, se ha desarrollado un protocolo al que hemos denominado DARP, *Protocolo de Radio Adaptativo y Dinámico*. Este protocolo, también basado en el estándar 802.15.4, presenta una arquitectura de red flexible y dinámica, con una topología en árbol y que utiliza una nueva propuesta de subredes virtuales para la gestión de los nodos. Otra de las características más importantes está asociada a la inteligencia que posee la propia red y que se encuentra en una pasarela [16] conectada directamente con el nodo raíz del árbol, simplificando las operaciones y la complejidad de la red, mediante un enlace de comunicaciones robusto y de mayor capacidad que la propia red.

Como se ha descrito en la sección anterior, las redes en árbol proporcionan un importante grado de estructuración lo que mejora la organización de la red y minimiza el tráfico en circulación. Es por este motivo, por el que nuestra propuesta se basa en una

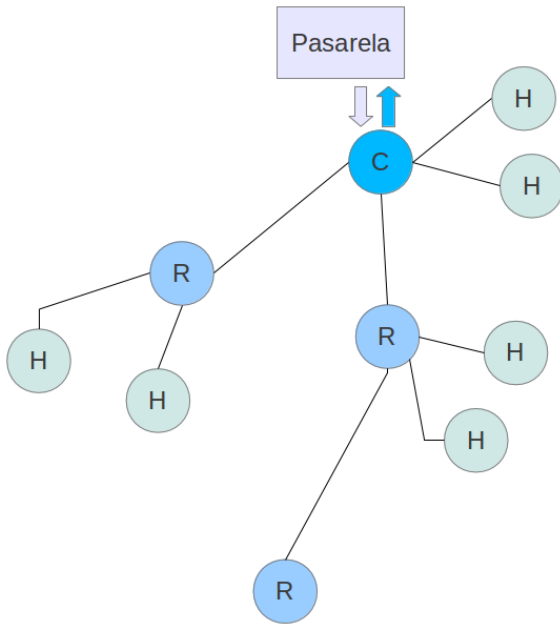


Fig. 2. Topología de red en árbol típica.

topología de red en árbol.

Es interesante detallar en profundidad algunas de las propiedades de la propuesta aquí presentada. Para comenzar se debe apuntar que existen tres tipos de rol para los nodos: rol de raíz, rol de enrutador y rol de hoja. Todos los nodos se basan en la especificación FFD del *IEEE 802.15.4*. Los roles de los nodos no se fijan antes del despliegue de la red, como en los protocolos actuales, lo que supone una arquitectura rígida y estática, además de conllevar un importante estudio del área de despliegue de dicha red.

En nuestra propuesta, el rol se auto-configura en base a un valor de LQI (*Link Quality Indicator*). Este parámetro es transmitido en todas las tramas 802.15.4 y está basado en un proceso de detección de la energía que realizan los dispositivos de la red de forma autónoma. Esta detección de la energía (*Energy Detection* o ED) es parte del proceso de escaneo pasivo de canales que se detalla en el estándar *IEEE 802.15.4* y que genera el valor de LQI a nivel de capa de acceso al medio (MAC). Mediante este valor se establece el rol de los nodos, en base a la siguiente expresión.

$$Rol = \begin{cases} Enrutador & \text{Si } 25 \leq LQI < 200 \\ Hoja & \text{Si } 200 \leq LQI < 250 \end{cases} \quad (1)$$

Esta propiedad es muy interesante, dadas las necesidades de los nuevos escenarios propuestos para estas redes. En estos escenarios se necesitan mecanismos que garanticen una topología robusta y dinámica, capaz de adaptarse a cambios en el entorno. Es por este motivo, por el que se ha desarrollado este mecanismo, que en el caso de necesitar un cambio en la topología, permite desconectar uno o toda una serie de dispositivos y reconectarlos con otro rol diferente, aumentando el desempeño final de toda la red.

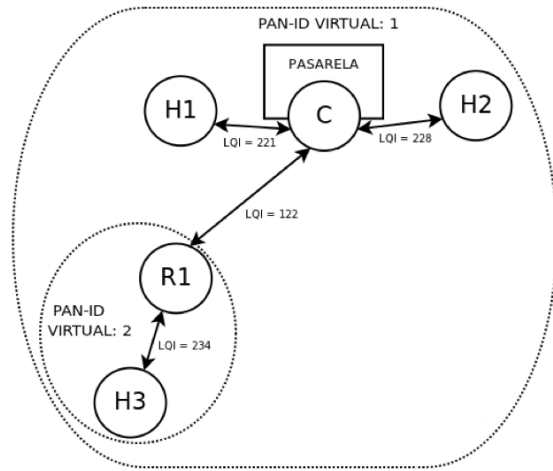


Fig. 3. Organización en subredes virtuales utilizada en DARF.

Otra importante propiedad es la utilización de una nueva propuesta que permite gestionar la red en base a subredes virtuales. Actualmente, no existe esta posibilidad, ya que en los protocolos disponibles, las comunicaciones se gestionan en base a una dirección de red que un FFD se auto-asigna en el momento de inicio de la red y que mantiene durante toda el tiempo de vida de la red. Al no existir estas subredes, el dispositivo que gestiona la red, necesita un mayor espacio de memoria para mantener las tablas de enrutamiento, haciendo pesadas las tareas de búsqueda en el espacio de direcciones de la red.

La estructuración que se propone aquí, se realiza siempre que un nuevo nodo con rol de enrutador se incorpora a la red. Este enrutador, obtiene la asignación de una nueva dirección de subred virtual y los nodos con rol de hoja que se incorporen a la red a través de él, pertenecerán a esa subred virtual. Esta aplicación provee una importante mejora y una mayor abstracción en los flujos de mensajes dado el menor número de entradas en las tablas de enrutamiento, lo que permite aumentar el número de nodos en la red y mejorar la eficiencia en las tareas de enrutamiento que desempeña el nodo raíz. Este método permite también realizar difusión de mensajes por grupos e incluso aislar zonas problemáticas de una red, mejorando la respuesta y la reconfiguración de la red.

Entre estas propiedades, es también necesario destacar qué representa la extracción de la inteligencia hacia el exterior de la red. Esta propiedad presenta una dupla compuesta por un nodo raíz que es la interfaz de salida de la red hacia el exterior y por la pasarela con la que se conecta el nodo raíz y que puede comunicar con uno o varios protocolos de comunicaciones diferentes. Esta pasarela es un elemento importante, ya que además de realizar una traducción entre protocolos y permitir la comunicación con otras redes, con independencia del protocolo o la tecnología que utilicen, permite la gestión de las tablas de enrutamiento y de las subredes virtuales, permitiendo aplicar eficientes algoritmos ya existentes a estas redes y aumentando

así el desempeño en redes ubicuas. La utilización de una pasarela está asociada con la necesidad de redundancia y la aplicación de numerosas técnicas de gestión ya existentes para Internet. Resulta de amplio interés que sea la pasarela la que posea las tablas de enrutamiento completas de la red y que conozca que dispositivos se encuentran en ella con el objetivo de solventar problemas surgidos de caídas o malfuncionamiento del nodo raíz y a desarrollar técnicas de gestión eficiente tanto en los modos de enrutamiento como en el campo de la seguridad de la red. En nuestra propuesta, el nodo raíz actúa como un enrutador más, lo que permite su sustitución con un mínimo impacto en el caso de que sea necesario. Esto proporciona un grado de redundancia adicional, dado que las tablas de enrutamiento pueden recomponer toda la red en muy poco tiempo, minimizando así el impacto de un fallo global en el nodo raíz y acortando el tiempo durante el que la red se encuentra no disponible.

#### IV. PRUEBAS Y RESULTADOS

En esta sección, se presentan las pruebas que hemos realizado de cara a comparar nuestra propuesta de protocolo con las dos principales alternativas en el marco de las WSN. Las pruebas aquí realizadas se corresponden con una comparación del tiempo medio de formación de la red en dos escenarios diferentes. Los dispositivos utilizados en ambas pruebas han sido:

- Implementación *DARP*: *AT91SAM3S* con radio *AT86RF212* a 868 MHz.
- Implementación *ZigBee* de Atmel (Bitcloud Stack): *AT91SAM3S* con radio *AT86RF212* a 868 MHz.
- Implementación *6LoWPAN* en Contiki: Freescale *MC1322x* con radio a 2.4GHz.

La arquitectura que se propone utilizar para la correcta realización de las pruebas y en la que se ha centrado el desarrollo del presente protocolo de red, es una arquitectura ARM de 32 bits. Las comunicaciones, están basadas en un chip de radio que opera en la banda de frecuencia de 868 MHz, aunque el desarrollo se presenta con una marcada independencia de la plataforma hardware utilizada. El dispositivo que se ha utilizado en concreto, es un microcontrolador ATMEL, *AT91SAM3S* y un chip de radio *AT86RF212*. Destacar que la comparativa con *6LoWPAN*, se realiza de forma desigual, dadas las necesidades de tamaño de trama mínima que tiene este protocolo. Estas necesidades obligan a la utilización de transmisores que operan en la frecuencia de 2.4 GHz. Esta frecuencia provee un mayor ancho de banda y permite la transmisión de tramas mayores, tal y como se ha comentado anteriormente.

Es necesario apuntar que el uso de una arquitectura de 32 bits viene marcado por el propósito multi-tarea del presente protocolo. Esto se debe a que está pensado para que sea ligero y eficiente, de forma que

TABLA I  
RESULTADOS DE LAS PRUEBAS ENTRE ZIGBEE, 6LOWPAN  
Y DARP EN LOS DOS ESCENARIOS PROPUESTOS.

Esc.	DARP	ZigBee	6LoWPAN
1	0.9-1.1 secs	2-3 secs	1-1.2 secs
2	5 - 5.8 secs	12-17 secs	6-8 secs

los dispositivos en los que opere puedan realizar múltiples tareas simultáneamente. Adicionalmente, esta elección, permite su utilización en otro tipo de dispositivos basados en arquitecturas de 32 bits, con mínimos cambios, dada la independencia arquitectónica con la que se ha desarrollado *DARP*.

La principal prueba que se ha realizado es el cálculo del tiempo medio de formación de la red. Para esta prueba se han realizado mediciones del tiempo medio de conexión en nodos individuales y se han realizado pruebas a pequeña escala en el laboratorio. Esta prueba se ha planteado en dos escenarios específicos en un entorno controlado.

1. El primer escenario representa el tiempo medio que un nodo con independencia de su rol en la red, ha tardado en conectarse de forma efectiva.
2. El segundo escenario representa el tiempo medio que una red de 5 nodos ha tardado en conectarse completamente y encontrarse preparada para la transmisión de información.

Estas pruebas se han basado en redes de pequeño tamaño, compuestas por entre 5 dispositivos. En todas las pruebas el dispositivo raíz o coordinador se encontraba directamente conectado a una máquina de mayor capacidad tipo pasarela o pc mediante conexión cableada.

#### V. CONCLUSIONES Y TRABAJO FUTURO

Las redes que se han abordado a lo largo del presente artículo están centrando en gran medida el esfuerzo en la investigación en el área de las comunicaciones inalámbricas de sensores. Es acertado contemplar también, los grandes esfuerzos que se están realizando de cara a llevar IPv6 a este tipo de redes, así como a conseguir una interoperabilidad a nivel de capa MAC entre diversos protocolos de comunicaciones. Otro aspecto importante que está centrando numerosos esfuerzos en la investigación en este campo, es en el área de gestión de estas redes, en la que se están adaptando y probando nuevas y cada vez más eficientes técnicas de direccionamiento, seguridad y gestión energética.

Los resultados arrojan unos prometedores valores en la media de tiempo necesario para la conexión [2] [14]. Los dos escenarios planteados han presentado mejores tiempos en la operación de conexión a la red. Destacar además que nuestra propuesta está pensada para grandes despliegues de dispositivos en ambientes altamente cambiantes y en los que la velocidad de conexión, un tráfico significativamente bajo y un alto grado de interoperabilidad son requisitos imprescindibles. Con el presente protocolo, estos

requisitos son cubiertos en gran medida, dadas las propiedades que posee, como por ejemplo, los roles dinámicos que pueden desempeñar los nodos, la gestión de la inteligencia de la red que realizan las pasarelas o la estructuración en subredes virtuales. Tal y como se ha expuesto en el presente artículo, resultan de especial interés para el desarrollo de las WSN, una serie de características que no se encuentran cubiertas actualmente por ninguno de los protocolos de red existentes. Esta carencia hace necesaria una propuesta que cubra ese déficit y como se puede observar en los resultados de las pruebas realizadas, esta primera versión presenta datos esperanzadores.

Además de continuar con el desarrollo y la mejora de *DARP*, aumentando el rango de pruebas y desarrollando nuevas e interesantes iniciativas dentro del protocolo como por ejemplo, una comparativa de la media de mensajes necesarios para el establecimiento y mantenimiento de la red con diferentes protocolos. Existen otras líneas de investigación con gran interés en este área. Una de estas líneas es la investigación orientada al ámbito de la eficiencia energética en este tipo de redes. Resulta de especial interés comparar el rendimiento en términos energéticos que tienen estas redes, así como desarrollar nuevas propuestas que puedan ser recogidas e implementadas en *DARP*.

Para finalizar destacar otra interesante propuesta, como es la integración de este trabajo dentro de un marco más amplio de sistema de control y desarrollo de una plataforma de gestión de grandes redes ubicuas del tipo USN, dentro de la cuál el desarrollo de este protocolo de red puede jugar un importante papel en un marco de integración e interoperabilidad tanto a nivel hardware como a nivel tecnológico.

#### AGRADECIMIENTOS

Trabajo desarrollado en el marco del proyecto TASA (Técnicas Avanzadas para Sistemas Activos), TSI-020100-2010-484, financiado por el Ministerio de Industria, Turismo y Comercio: Subprograma Avanzada Competitividad I+D+I.

#### REFERENCIAS

- [1] P. Baronti, P. Pillai, V. W. C. Chook, A. Gotta S. Chessa, and Y. Fun Hu. Wireless Sensor Networks: A Survey on the State of the Art and the 802.15.4 and ZigBee Standards. *Computer Communications*, 30(7):1655–1695, Mayo 2007.
- [2] E. Casilari, J. Cano-García, and G. Campos-Garrido. Modeling of current consumption in 802.15.4/ZigBee sensor motes. *Sensors*, 10(6):5443–5468, 2010.
- [3] Z. Cheng, M. Perillo, and W. B. Heinzelmann. General network lifetime and cost models for evaluating sensor network deployment strategies. *IEEE Transactions on Mobile Computing*, 7(4):484–497, 2008.
- [4] A. A. Hasbollah, S. H. S. Ariffin, and M. I. A. Hamini. Performance Analysis For 6LoWPAN IEEE 802.15.4 with IPv6 Network. In *TENCON 2009*, pages 23–26, IEEE Region 10, Jan. 2009.
- [5] J. W. Hui and D. E. Culler. Extending IP to Low-Power, Wireless Personal Area Networks. *Internet Computing*, 12(4):37–45, 2008.
- [6] J. W. Hui and D. E. Culler. IPv6 in low-power wireless networks. *Proceedings of the IEEE*, 98(11):1865–1878, 2010.
- [7] N. Kushalnagar, G. Montenegro, and C. Schumacher. IPv6 over Low-Power Wireless Personal Area Networks

(6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. Network Working Group, Agosto 2007. Disponible en <http://www.ietf.org/rfc/rfc4919.txt>.

- [8] J. Misić and V. B. Misić. Access delay for nodes with finite buffers in IEEE 802.15.4 beacon enabled PAN with uplink transmissions. *Computer Communications*, 28(10):1152–1166, 2005.
- [9] J. Misić, S. Shafi, and V. B. Misić. The impact of MAC parameters on the performance of 802.15.4 PAN. *Ad Hoc Networks*, 3(5):509–528, 2005.
- [10] Institute of Electrical, Electronics Engineers, and Inc. IEEE Std. 802.15.4-2006 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs). In *IEEE Press*, New York, United States of America, Oct. 2003.
- [11] S. N. Pakzad, G. L. Fenves, S. Kim, and D. E. Culler. Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring. *Journal of Infrastructure Systems*, 14(1):89–101, 2008.
- [12] M. S. Pan, C. H. Tsai, and Y. C. Tseng. The Orphan Problem in ZigBee Wireless Networks. *IEEE Transactions on Mobile Computing*, 8(7):1573–1584, 2009.
- [13] R. Roman and C. Alcaraz. Applicability of Public Key Infrastructures in Wireless Sensor Networks. In *Proceedings of the 2000 Asia and South Pacific Design Automation Conference*, pages 635–640, Yokohama, Japan, Jan. 2000.
- [14] D. Singh, U. S. Tiwary, H. J. Lee, and W. Y. Chung. Global Healthcare Monitoring System using 6LoWPAN Networks. In *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference*, pages 113–117, Busan, South Korea, Feb. 2009.
- [15] R. Verdonesi and C. Burattini. Modelling for wireless sensor network protocol design. In *International Workshop on Wireless Ad-hoc Networks (IWVAN)*, pages 23–26, London, United Kingdom, May. 2005.
- [16] M. M. Wang, J. N. Cao, J. Li, and S. K. Dasi. Middleware for wireless sensor networks: A survey. *Journal of Computer Science and Technology*, 23(3):305–326, 2008.