Gestión de redes inteligentes domésticas mediante *ZigBee Smart Energy*

Carlos Rodríguez-Morcillo

Doctor Ingeniero del ICAI (2007) y Máster en Tecnologías y Sistemas de Comunicaciones (UPM). Investigador del IIT y coordinador del Grupo de Electrónica y Automática del IIT.

José Daniel Muñoz

Doctor Ingeniero del ICAI (2002). Profesor del Departamento de Electrónica y Automática del ICAI e investigador en el IIT.

Javier Juárez

Ingeniero Industrial del ICAI (2009). Investigador en Formación del IIT.

David Contreras

Doctor Ingeniero del ICAI (2010). Profesor del Departamento de Sistemas Informáticos del ICAI e investigador en el IIT.

Sadot Alexandres

Doctor Ingeniero de Telecomunicación (UPM). Profesor del Departamento de Electrónica y Automática del ICAI e investigador en el IIT.

Palabras clave: Redes inteligentes, ZigBee, perfil Smart Energy, IEEE 802.15.4.

Resumen

A raíz del compromiso adoptado por la Unión Europea en 2008 sobre las emisiones de CO_2, la eficiencia energética y la generación de energía con fuentes renovables, se ha cambiado el modelo energético de Europa, lo que ha dado lugar a las Redes Inteligentes (*Smart Grids*). Para otorgar de "inteligencia" a las redes eléctricas, es necesario desarrollar e instalar una infraestructura de comunicaciones que permita conocer el estado de la red en tiempo real y actuar sobre ella lo más rápidamente posible. A nivel doméstico, en el Instituto de Investigación Tecnológica (IIT) se está trabajando con *ZigBee Smart Energy* como solución para la monitorización, control y automatización del reparto y uso de la electricidad, el gas y el agua en el hogar. *ZigBee Smart Energy* es una solución estandarizada desarrollada por la alianza ZigBee (*ZigBee Alliance*).

Key words: *Smart Grids, ZigBee, Smart Energy Profile, IEEE 802.15.4.*

Abstract:

Adapting to the commitment made by the European Union in 2008 discussing key issues such as: CO_2 emissions, energy efficiency as well as energy generation from renewable sources, the energy model of Europe has changed, which has led to the development of Smart Grids. To provide "intelligence" to power grids, it is necessary to develop and install a communications infrastructure that allows us to know the network status in real time, and to act on it as quickly as possible. The Institute for Research in Technology (IIT) is working with ZigBee Smart Energy as a solution for monitoring, control and automation of distribution and use of electricity, gas and water in-home. ZigBee Smart Energy is a standardized solution developed by ZigBee Alliance

Introducción

A finales del año 2008, en Estrasburgo, la Unión Europea (UE) alcanzó un acuerdo por el que se compromete a reducir un 20% las emisiones de CO_2, a aumentar un 20% la eficiencia energética y a generar el 20% de la energía de la UE con fuentes renovables (el conocido plan 20-20-20). Esto ha obligado a elaborar un nuevo modelo energético que, además de cumplir con los objetivos establecidos, asegure la economía del suministro, garantice la fiabilidad del servicio y sea sostenible. Por este motivo surgen las Redes Inteligentes (*Smart Grids*), que permiten gestionar de forma eficiente y segura la energía, mediante la Gestión Activa de la Demanda.

Por otra parte, el rápido crecimiento de la demanda, el rechazo social a la construcción de infraestructuras eléctricas y el incremento de la generación distribuida, entre otras razones, hacen que sea necesario el empleo de las tecnologías de la información y las comunicaciones más avanzadas. Esto permitirá en un futuro disponer de redes de distribución controladas en tiempo real para gestionarlas de forma eficiente, sostenible y segura.

Desde el punto de vista del consumidor, es fundamental impulsar la Eficiencia Energética y promover la Gestión Activa de la Demanda, para lo cual es necesario que los clientes se integren en la Red con equipos de medida y control comunicados en red.

Por todos estos motivos, desde hace varios años, se han dispuesto fondos para realizar grandes proyectos de I+D en los que se investiguen y desarrollen los equipos y sistemas necesarios que permitan gestionar la demanda de forma segura, eficiente y sostenible, y que, por tanto, permitan avanzar en la implantación de las Redes Inteligentes. En muchos de esos proyectos, como por ejemplo ENERGOS [1], DENISE [2] y ADDRESS [3], está involucrado activamente el Instituto de Investigación Tecnológica (IIT) de la Escuela Técnica Superior de Ingeniería (ICAI).

Fruto de estas actividades, en el IIT se está trabajando con *ZigBee Smart Energy,* que es una solución estandarizada de la alianza ZigBee (*ZigBee Alliance*), el cual se ha consolidado, a lo largo de estos años, como solución para la monitorización, control y automatización del reparto y uso de la energía, el gas y el agua en el hogar. Está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (*Wireless Personal Area Network* - WPAN), el cual tiene como objetivo desarrollar aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos, maximizando la vida útil de las baterías. Esta tecnología, por tanto, ayuda a crear hogares más ecológicos, informando a los consumidores y automatizando los sistemas para reducir el consumo y ahorrar dinero.

Desde el punto de vista de las Redes Inteligentes, con ZigBee se puede crear una HAN (*Home Area Network*) que permita monitorizar el estado de cada dispositivo del hogar y gestionar la energía de manera inteligente. Además, la implantación de HAN en todos los hogares va a permitir a las compañías distribuidoras conocer el estado de generación y demanda a nivel de núcleo urbano, facilitando así la gestión de la energía.

ZigBee

ZigBee es una tecnología de red inalámbrica, especificada por *ZigBee Alliance,* desarrollada para cubrir las necesidades de bajo coste, seguridad, fiabilidad, flexibilidad y bajo consumo eléctrico en áreas de control. Utiliza una pila de comunicaciones (como la mostrada en la Figura 1), similar al modelo de referencia OSI (*Open System Interconnection*), formada por varias capas independientes entre sí y con funciones específicas.

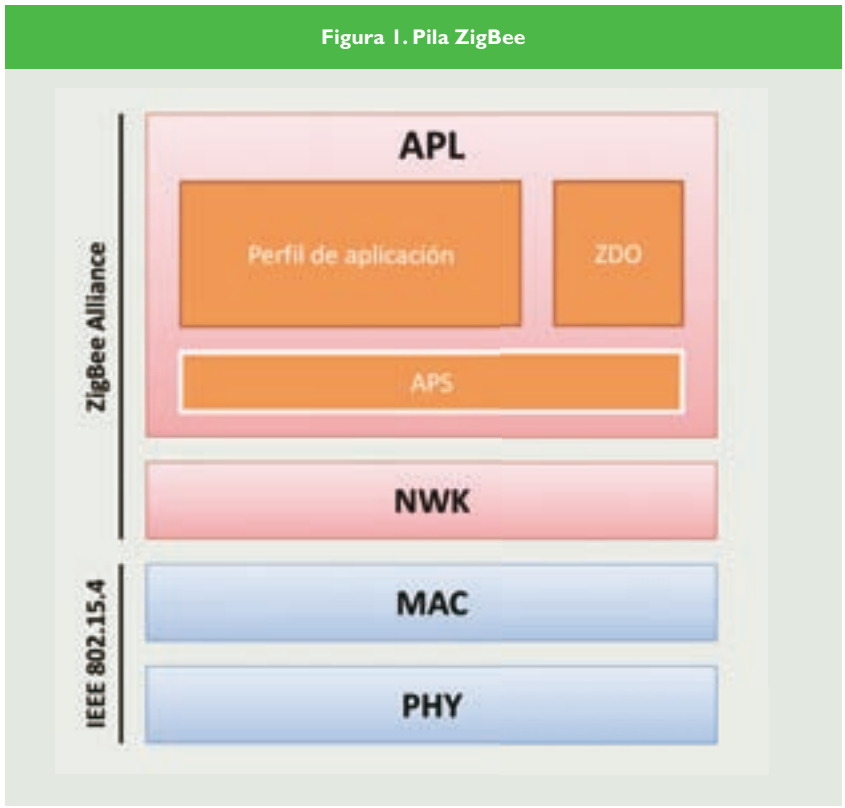
Como se puede comprobar en la figura, las capas más bajas de dicha pila (PHY y MAC) están definidas en el estándar IEEE 802.15.4; mientras que el resto de capas (NWK y APL), las define la alianza ZigBee. Dentro de la capa de aplicación se configura la solución o el perfil ZigBee que se desee. Para abordar una solución en el contexto de las redes inteligentes se deberá hacer uso del perfil *ZigBee Smart Energy.*

A continuación se detallan cada una de las capas de la pila ZigBee.

Capas PHY y MAC: IEEE 802.15.4

El estándar IEEE 802.15.4 define las capas de nivel físico (PHY) y de nivel

Figura 1. Pila ZigBee



de enlace (MAC) de la pila empleada por ZigBee.

La capa de nivel físico se encarga de transmitir y recibir tramas de bits sobre el medio físico (el aire), modulando los bits a transmitir y demodulando la señal recibida. El dispositivo puede funcionar en distintas bandas de frecuencia con distinta tasa binaria de transmisión de información y distinto número de canales, con un alcance global entre 10 y 75 metros. En la Tabla 1 se muestran los valores especificados en la versión de la IEEE 802.15.4 del año 2003, que es la que utiliza ZigBee.

La modulación empleada en la comunicación es DSSS (*Direct Sequence Spread Spectrum*) la cual apenas interfiere con sistemas que trabajan en la misma banda de frecuencias, y es robusta ante las distintas recepciones por multi-trayecto.

Según el grado de funcionalidad del dispositivo, el estándar define:

- Los **FFD** (*Full-Function Device*), que son dispositivos que implementan un modelo de comunicaciones completo, que le permite comunicarse con cualquier otro dispositivo de la Red; y
- Los **RFD** (*Reduced-Function Device*), que son dispositivos con unas prestaciones limitadas para la comunicación, que sólo le permiten comunicarse con un FFD.

Las redes que se pueden formar albergan tres tipos de nodos:

- **Coordinador.** Es un dispositivo FFD que se encarga de crear la red de nodos y de gestionar su comunicación. En cada red existe un único coordinador.

Tabla 1. Valores de la capa PHY

Banda de frecuencias	Tasa binaria	Nº canales
868 – 868,8 MHz	20 kbps	1
902 – 928 MHz	40 kbps	10
2.400 – 2.483,5 MHz	250 kbps	16

- **Router.** Es un dispositivo FFD que se encarga de encaminar la información entre nodos que están muy separados en la red.
- **Dispositivo final.** Es un dispositivo RFD que puede transmitir o recibir información pero que no puede realizar labores de enrutamiento. Necesariamente debe estar comunicado con un Coordinador o con un Router.

Cada red ZigBee tiene un identificador de red único, lo que permite que varias redes ZigBee puedan compartir un mismo canal de comunicaciones, y pueden configurarse según distintas topologías: estrella, árbol o malla (ver Figura 2). En todas hay un Coordinador y uno o varios dispositivos Routers y/o finales.

Estas topologías permiten la comunicación entre dos dispositivos que se encuentran fuera de su rango de transmisión, siempre y cuando se encuentren conectados por nodos intermedios.

Respecto a la capa de nivel de enlace (MAC) definida en el estándar IEEE 802.15.4, su finalidad es controlar y gestionar el acceso al medio, para lo que utiliza un protocolo CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*); así como sincronizar tramas y controlar el flujo. También es el encargado de reducir al máximo el gasto energético del dispositivo, para alargar la vida útil de la batería.

El ahorro energético en ZigBee se realiza gracias a que los dispositivos entran en un periodo de inactividad (*sleep*) después del tiempo de transmisión o recepción. Este estado de *sleep* puede afectar a todos los dispositivos de la red ZigBee o sólo a los Dispositivos Finales, en función del modo en el que trabajan.

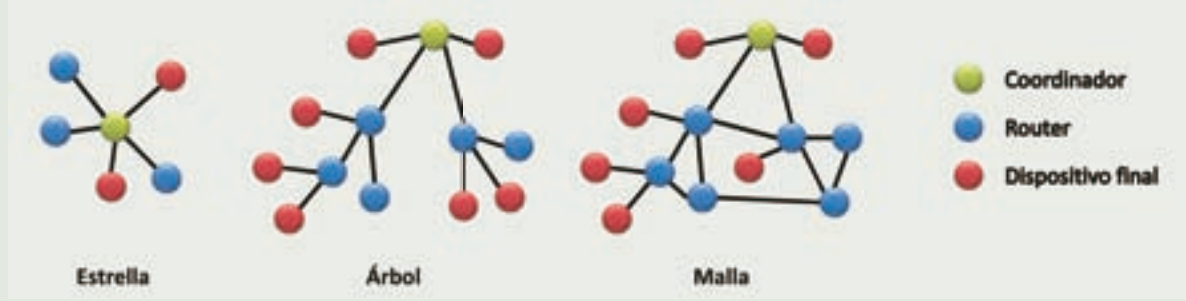
Capas NWK y APL: ZigBee

La capa de nivel de red (NWK) se encarga de la topología de la red, añadiendo o eliminado dispositivos de la misma; asignando direcciones de red a los dispositivos; y redireccionando las tramas de información hacia el destinatario por el camino más adecuado.

También se encarga de garantizar la fiabilidad y calidad de los datos recibidos en el nodo, mediante el control y la corrección de los errores. Éstos pueden ser provocados por una mala comunicación radio, la congestión de la red, colisión entre paquetes transmitidos, o fallos propios del nodo.

Por último, la capa del nivel de aplicación (APL) es la responsable de ejecutar las aplicaciones del sistema, y se subdivide en tres partes (ver Figura 1):

Figura 2. Topologías de la Red.[4]



• La **subcapa ZDO** (*ZigBee Device Object*), que define el papel que desempeña el dispositivo en la red (Coordinador, Router o Dispositivo Final);

• Los **objetos de aplicación,** definidos por cada fabricante, que se emplean para definir diferentes perfiles ZigBee, como puede ser el *ZigBee Smart Energy;* y

• La **subcapa de soporte** (APS), que es una interfaz entre la capa del nivel de red (NWK) y la capa del nivel de aplicación (APL), mediante el uso de un conjunto de servicios que se utilizan colectivamente con la subcapa ZDO y los objetos de aplicación.

El perfil *ZigBee Smart Energy*

Tal como se ha comentado en la introducción, ZigBee dispone de un perfil diseñado para dar soporte a las redes inteligentes [5]. Este perfil contempla tanto las redes de vecindario, propiedad de la compañía distribuidora con objeto de realizar telemedida de contadores, como redes individuales de vivienda, conectadas con la distribuidora para realizar una gestión eficaz de la energía. Mientras que en el primer tipo de redes sólo tiene sentido hablar de contadores, en el segundo existen distintos tipos de dispositivos definidos por el estándar.

Tipos de dispositivos *ZigBee Smart Energy*

Estos tipos de dispositivos son elementos lógicos, de forma que un mismo dispositivo físico puede albergar varios dispositivos lógicos. Si se da esta circunstancia, cada uno de los dispositivos lógicos utiliza un distinto "end point" de forma que la comunicación entre dispositivos es transparente, siendo gestionada por la capa de red (NWK) de ZigBee.

Los tipos de dispositivos definidos en el perfil son:

• ***Energy Service Interface.*** Este dispositivo es el puente entre la red ZigBee y la red de datos de la compañía suministradora. Obviamente, además del interfaz de la red ZigBee necesita otra interfaz para comunicarse con la compañía, como por ejemplo GPRS (*General Packet Radio Service*)

para comunicaciones vía telefonía móvil, IP (*Internet Protocol*) para comunicaciones por Internet, PLC (*Power Line Communication*) para comunicaciones por el cable eléctrico, etc. Mediante este dispositivo, la compañía distribuidora puede enviar actualizaciones de precios, eventos de gestión de la demanda que permitan desconectar cargas no críticas de la casa, o mensajes al usuario que serán visualizados en el display, entre otros servicios. También mediante este puente la compañía puede tener acceso a las medidas de los contadores.

• ***Metering Device***. El estándar permite conectar a la red *ZigBee Smart Energy* contadores de electricidad, agua y gas. Para alargar la vida de las baterías de los contadores no conectados al suministro eléctrico, éstos envían periódicamente las medidas, estando el resto del tiempo en reposo y con la radio apagada. En el caso de los contadores eléctricos también es posible leer en cualquier momento las medidas, ya que suelen estar conectados permanentemente a alimentación. Por último destacar que junto con la medida, estos contadores pueden enviar información del estado del contador, como por ejemplo que la batería está baja o que lo han intentado abrir para manipularlo.

• ***In Premises Display Device.*** Este dispositivo consiste en una pantalla situada en la vivienda del usuario, a través de la cual éste puede ver el consumo actual de energía o históricos de consumo, precios, etc. Está demostrado [6] que una información en tiempo real sobre el consumo de energía hace que el usuario consuma menos. Por otro lado, la compañía puede enviar mensajes a través de esta pantalla para informar, por ejemplo, de cambios en los precios, franjas horarias, etc. Esto permite al usuario hacer un consumo más racional de la energía, como por ejemplo, poner la lavadora a la hora que la energía sea más barata.

• ***Programmable Communicating Thermostat.*** Este dispositivo es capaz de controlar la climatización del hogar (frío y/o calor) recibiendo órdenes de

gestión de demanda para modificar las consignas de temperatura o incluso apagarse completamente en caso de sobrecarga en la red. También es posible que estos dispositivos actúen en función de los precios para modificar su consigna si el precio sube, por ejemplo. Incluso el estándar contempla que estos dispositivos puedan enviar a la pantalla de gestión energética información sobre su consumo energético para que el usuario sea consciente del coste de subir un grado la consigna de temperatura en la calefacción.

• ***Load Control Device.*** Son dispositivos similares a los anteriores salvo que usados para controlar otro tipo de cargas, como por ejemplo termos eléctricos. Pueden recibir eventos de gestión de demanda para desconectarse en caso se sobrecarga de la red.

• ***Smart Appliance Device.*** Estos dispositivos están pensados para estar integrados en los electrodomésticos, permitiendo a éstos recibir información del precio de la energía o eventos de gestión de la demanda. Esto permitiría a una lavadora "inteligente", por ejemplo, cambiar el programa de lavado a agua fría si el precio de la energía sube. Por otro lado es posible enviar mensajes al display para indicar anomalías. Así un frigorífico "inteligente" podría enviar una alarma de temperatura elevada en el interior.

• ***Prepayment Terminal.*** Aunque no es usado en nuestro país, en ciertos países se están aprobando normativas para poder usar terminales de prepago para la energía. En este caso el contador ha de disponer de un sistema para aceptar el pago de un bloque de energía mediante, por ejemplo, una tarjeta y debe de informar del saldo restante, dar una alarma cuando el saldo se aproxima a cero, etc. En este caso los mensajes pueden ser canalizados en el display.

Seguridad

Obviamente la seguridad es un tema fundamental en una red de comunicaciones como la descrita en este artículo. Por un lado es fundamental validar la identidad de los dispositivos conectados a la red, para que, por ejemplo, no pueda conectarse un contador que envíe información falsa sobre el consumo; y por otro lado es preciso asegurar la integridad y confidencialidad de los mensajes para evitar que alguien los manipule, por ejemplo, para falsear datos de consumo o de precios.

Para conseguir la integridad y la confidencialidad de los datos, la alianza ZigBee adopta el cifrado AES-CCM* (*Advanced Encryption Standard – CCM Star*), el cual está orientado a dispositivos con baja potencia de cálculo, como son los microcontroladores usados en los dispositivos ZigBee. Este cifrado está basado en una clave simétrica de 128 bits, que han de conocer todos los dispositivos que deban compartir información.

Dentro de ZigBee existen dos modos de seguridad, el estándar, usado por aplicaciones no críticas como la domótica; y el de alta seguridad, definido en el estándar ZigBee PRO, que es el usado por el perfil Smart Energy. En el primer nivel todos los dispositivos de la red comparten una misma clave, denominada clave de red (*Network Key*), por lo que cualquier dispositivo puede acceder a la información transmitida. En el segundo nivel, se establecen claves privadas a nivel de aplicación (*Application Link Key*) entre cada dos dispositivos que quieren compartir información.

La gestión de claves la realiza un dispositivo denominado "Trust Center", que ha de coincidir con el "Energy Service Interface" en una red Smart Energy. Dicho Trust Center se encarga de distribuir las claves simétricas al resto de dispositivos que forman la red. No obstante, dicha clave no puede distribuirse en claro (sin cifrar), por lo que es necesario un mecanismo para distribuir la clave de red de forma segura. Para ello se usa una segunda clave, denominada clave de enlace (*Link Key*), para cifrar la clave de red. Esta segunda clave es única para cada dispositivo que quiere unirse a la red y se preconfigura durante su fabricación. El problema ahora consiste en cómo hacer llegar dicha clave al *Trust Center.*

El método consiste en generar un código de instalación aleatorio en el proceso de fabricación para cada

dispositivo ZigBee. Mediante una función Hash *Matyas-Meyer-Oseas* se genera una clave de enlace a partir de este código de instalación y se graba en el dispositivo. Cuando se quiere instalar el dispositivo en una red, dicho código de instalación ha de hacerse llegar a la compañía distribuidora por algún método distinto de la red ZigBee (página web, servicio de atención telefónico, etc.). La compañía entonces vuelve a aplicar la misma función *Hash* al código para obtener la clave de enlace y ésta se envía a la red ZigBee a través del *"Energy Service Interface"*. De esta forma el *Trust Center* y el dispositivo disponen de una clave común con la que realizar una primera comunicación. En ésta, el *Trust Center* reconoce el dispositivo y le envía la clave de red cifrada para que pueda comunicarse con el resto de dispositivos.

Como se ha mencionado anteriormente, cuando se usa en nivel de seguridad alto, además de la clave de red, usada para las comunicaciones no críticas, cada dos dispositivos que deseen intercambiar información crítica necesitan una clave de enlace de aplicación. En este caso, una vez que un dispositivo se ha unido a la red mediante su clave de enlace preconfigurada, ha de establecer una clave de enlace de aplicación con el *Trust Center.* Esta clave se establece "al vuelo" usando certificados. De esta forma la clave no se transporta por la red, sino que se establece de común acuerdo entre ambos dispositivos intercambiando una serie de información.

En este caso es necesario que el *Trust Center* pueda saber si el dispositivo que está intentando entrar en la red es quien dice ser (por ejemplo, un contador de un fabricante autorizado por la compañía) o es un "impostor". Para ello se utilizan certificados implícitos [7], los cuales son similares a los certificados X.509 usados en Internet, pero adaptados a dispositivos con menos recursos. Así, mientras un certificado X.509 ocupa 8.000 bits, un certificado implícito ocupa 160 bits. Estos certificados implícitos permiten por un lado conocer la dirección MAC del dispositivo y por otro el código del fabricante. Para garantizar la integridad, el certificado va firmado por una autoridad certificadora.[1] Una vez establecida la nueva clave de enlace de aplicación con el *Trust Center,* cuando dos dispositivos deseen comunicarse con nivel de seguridad alto, el *Trust Center* generará una clave de enlace de aplicación privada para ambos y se la enviará cifrada usando la clave de enlace de aplicación entre cada dispositivo y el *Trust Center.*

Costes de licencias

Lamentablemente el desarrollo de dispositivos *ZigBee Smart Energy* tiene un coste de entrada algo elevado para una empresa pequeña. Por un lado, antes de poder poner un producto en el mercado, es necesario pertenecer a la alianza ZigBee, lo cual tiene unos costes dependiendo del grado de participación. El más económico, denominado "adopter" cuesta anualmente 3.500 $, a lo que hay que sumar el coste de certificación del producto más 1.000 $ por gastos de "administración del logo" para el primer producto certificado. Por otro lado, es necesario obtener un certificado de Certicom para cada producto fabricado. En este caso los certificados han de pedirse por lotes, teniendo cada lote un coste fijo de 1.000 $ y un coste por certificado variable que oscila entre 1,00 $ para lotes de menos de 500 certificados y 0,21 $ para lotes de más de 100.000 certificados.

Conclusiones

En este artículo se han introducido las redes inteligentes domésticas y se ha justificado la necesidad de que sean seguras, eficientes y sostenibles. Dentro de este marco de actuación, en el IIT se ha trabajado con ZigBee, que es una tecnología de red inalámbrica, especificada por ZigBee Alliance, desarrollada para cubrir las necesidades de bajo coste, seguridad, fiabilidad, flexibilidad y bajo consumo.

Más concretamente, en este artículo se ha descrito el perfil *ZigBee Smart Energy.* Se ha mostrado que soporta todos los posibles dispositivos de gestión de la energía que se pueden integrar dentro de un hogar "inteligente" y se ha mostrado que el estándar utiliza métodos de cifrado lo suficientemente seguros como para que pueda circular información crítica por la red inalámbrica.

No obstante, también se ha mostrado que el coste de entrada para los fabricantes es relativamente alto. Esto ha provocado que existan estándares alternativos de código abierto como 6LoWPAN o MBus. El primero está orientado a la red doméstica y el segundo a la red de vecindario para realizar telemedida de contadores.

Agradecimientos

Las actividades y trabajos descritos en este artículo han sido soportados en parte por el proyecto ENERGOS, proyecto financiado por el Centro para el Desarrollo Tecnológico Industrial (CDTI) del Ministerio de Economía y Competitividad, a través del contrato con la empresa Sistemas Avanzados de Control (SAC). ▮

Referencias

[1] «ENERGOS». [Online]. Available: http://innovationenergy.org/energos/index.php. [Accessed: 28-sep-2012].

[2] «DENISE». [Online]. Available: http://www.cenit-denise.org/.

[3] «ADDRESS Project - FP7 ENERGY». [Online]. Available: http://www.addressfp7.org/. [Accessed: 28-sep-2012].

[4] «Node Types». [Online]. Available: http://www.jennic.com/elearning/zigbee/files/html/module2/module2-3.htm. [Accessed: 28-sep-2012].

[5] ZigBee Alliance, «ZigBee Smart Energy Profile Specification», ZigBee Alliance, 075356r16ZB, mar. 2011.

[6] Jessica Stromback, Christophe Dromacque, y Mazin H. Yassin, «The potential of smart meter enabled programs to increase energy and systems efficiency: a mass pilot comparison», VaasaETT Global Energy Think Tank, Helsinki, Finland, 2011.

[7] «Implicit certificate». [Online]. Available: http://en.wikipedia.org/wiki/Implicit_certificate. [Accessed: 03-oct-2012].

[8] «Certicom». [Online]. Available: http://www.certicom.com/. [Accessed: 28-sep-2012].

(1) De momento la única autoridad certificadora autorizada para generar estos certificados es Certicom [8].