

# REVISIÓN ESTADO DEL ARTE DE LA TECNOLOGIA ZIGBEE

## REVIEW STATE OF THE ART TECHNOLOGY ZIGBEE

Henry Montaña Quintero\* Jaime Alberto Zipamocha Camargo\*\*  
Franklin Johvany Caina López\*\*\*

**Resumen:** Esta revisión comienza ubicando a Zigbee dentro del contexto de redes. Para esto, se clasifican las mismas según su cobertura en: redes de área geográfica o WAN (Wide Area Network), redes de área local o LAN (Local Area Network) y redes de área personal o PAN (Personal Area Network). También se clasifican de acuerdo a su rango de cobertura.

Se hace una comparación general de estándares inalámbricos en cuanto a consumo de potencia, capacidad de transmisión de datos y alcance. Con esto se ubica al estándar IEEE 802.15.4 destinado a cubrir con ventajas las aplicaciones de muy bajo consumo y baja velocidad de transmisión de datos. Se introduce el estándar Zigbee como una extensión del IEEE 802.15.4.

El trabajo continúa describiendo las capas de ZigBee comenzando con la capa física hasta la capa aplicación. Se mencionan algunos aspectos de seguridad informática implementados en este protocolo y luego algunos de los muchos anuncios que publica la página oficial de Alliance ZigBee.

---

\* M.Sc. Universidad Distrital Francisco Jose de Caldas, Bogota, Colombia. Contacto: [hmontana@gmail.com](mailto:hmontana@gmail.com)

\*\* Tecnólogo en Electrónica, Universidad Distrital Francisco José de Caldas Facultad Tecnológica, Bogotá, Colombia. Contacto: [jaimewizamoch@hotmail.com](mailto:jaimewizamoch@hotmail.com)

\*\*\* Tecnólogo en Electrónica, Universidad Distrital Francisco José de Caldas Facultad Tecnológica, Bogotá, Colombia. Contacto: [frankaina@gmail.com](mailto:frankaina@gmail.com)

**Palabras clave:** Zigbee, inalámbrico, redes, **IEEE802.15.4**

Summary: This review begins placing within the context of Zigbee networks. For this, they are classified according to their coverage: geographical area network or WAN (Wide Area Network), local area network or LAN (Local Area Network) and Personal Area Network or PAN (Personal Area Network). They are also classified according to their range of coverage. A general comparison of wireless standards in terms of power consumption, data transmission capacity is made and scope. With this being located to the IEEE 802.15.4 standard intended to cover benefits applications with very low power consumption and low speed data transmission. The Zigbee standard is introduced as an extension of IEEE 802.15.4.

The work continues describing the layers of ZigBee starting with the physical layer to the application layer. Some aspects of security implemented in this protocol and then some of the many advertisements published by the official website of ZigBee Alliance are mentioned

**Key Words:** Zigbee, wireless, networks, IEEE 802.15.4

## **1. Introducción**

El avance tecnológico en las dos últimas décadas en el área comunicaciones ha permitido el desarrollo de nuevos circuitos integrados de muy pequeño tamaño, alta eficiencia energética y bajo costo. Esto llevó a disponer de transmisores/receptores que operan en frecuencias de GHz. Aparece la explosión de redes inalámbricas (Wireless) para aplicaciones con requerimientos disímiles en cuanto a transferencia de datos, alcance y costos.

Las redes inalámbricas se obtienen al unir 2 o más nodos sin utilizar cables para la conexión y se logra un intercambio de información mediante la utilización de protocolos. Estos protocolos son originados por organismos internacionales como IEEE y UIT. [2]

El IEEE ha creado varios estándares dentro de la familia de 802.x que se han adoptado para las comunicaciones de datos inalámbricas. En oficinas y casas la implementación de redes de área local inalámbricas (WLAN) basadas en el estándar IEEE 802.11.

La utilización de teléfonos celulares para transmisión de datos prueba que las redes inalámbricas son aplicables a un costo relativamente bajo.

Hay muchas aplicaciones que requieren establecer una red de bajo alcance con baja tasa de transmisión. Ver Figura 1. Estas redes se denominan LR-WPAN. (Low Rate Wireless Personal Area Network). Hay muchas soluciones propietarias para este tipo de redes, pero son caras, orientadas a un problema en particular e incompatibles entre ellas. El IEEE 802.15.4 es un estándar para las LR-WPAN que provee una solución simple y de bajo costo [2]. El ámbito de aplicación, entre otros, es el manejo de redes de sensores y activación de actuadores en domótica, monitoreo ambiental, industria, hospitales y hoteles. [1].

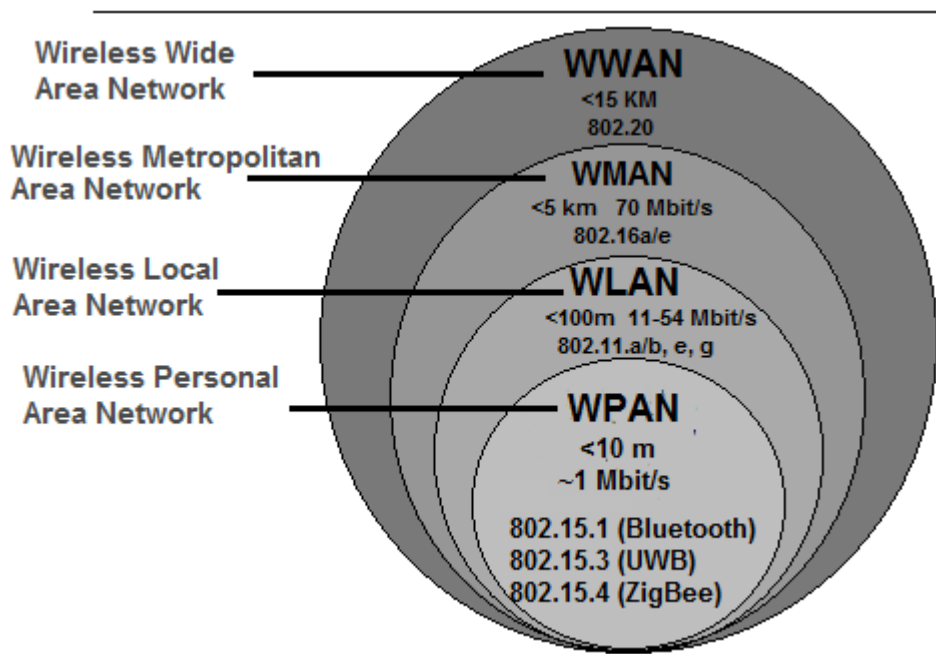


Figura 1. Tipos de Redes de Comunicación. Fuente: Elaboración propia de los autores

En el protocolo IEEE 802.15.4 se definen solo las 2 primeras capas ISO. (la capa física y la de enlace). Fue especialmente definido para estandarizar las redes de sensores WSN (wireless sensor network). [4].

Cada vez más se irán conectando sensores y actuadores en casas, industrias y hospitales. ZigBee es uno de los protocolos dominantes en redes WPAN y es fundamental tener un conocimiento cabal del mismo para implementar redes de sensores y actuadores. La tendencia es que en un futuro cercano se tendrá la "Internet of things" en donde todas las cosas estarán conectadas. Más aún se habla hoy de BAN (Body Area Network), en donde hay una red de sensores dentro del cuerpo de una persona. Así, por ejemplo, un paciente puede medir su nivel de glucosa, ritmo cardíaco, temperatura y enviar los datos a un servidor, o alertar en una red por una situación de emergencia médica.

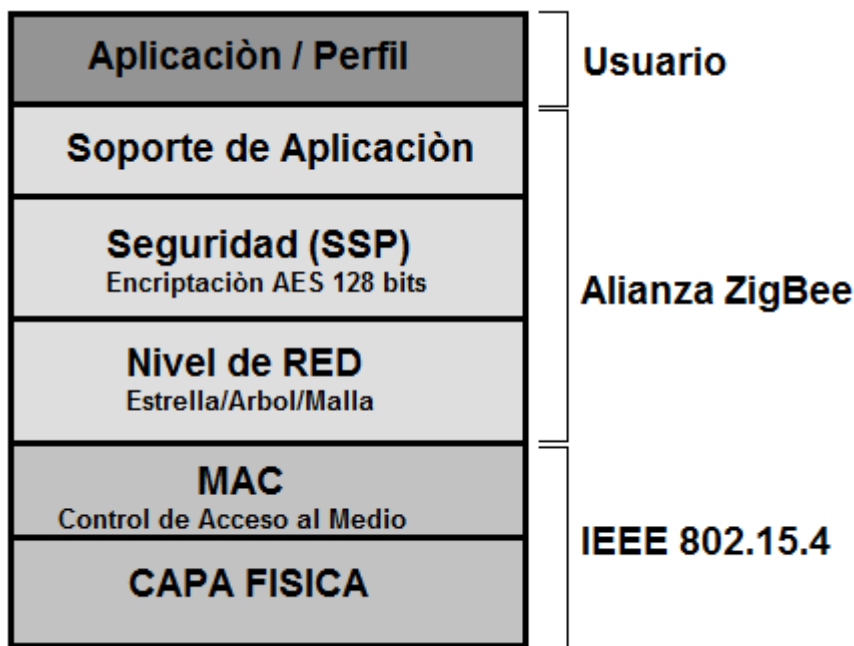
## **1. ¿Qué es Zigbee?**

El nombre "Zigbee" se deriva de los patrones erráticos comunicativos que hacen muchas abejas entre las flores durante la recogida de polen. Esto es evocador de las redes invisibles de las conexiones existentes en un entorno totalmente inalámbrico.

Zigbee se ha desarrollado para satisfacer la creciente demanda de capacidad de red inalámbrica entre varios dispositivos de baja potencia. En la industria Zigbee se está utilizando para la próxima generación de fabricación automatizada, con pequeños transmisores en cada dispositivo, lo que permite la comunicación entre dispositivos a un ordenador central [6]. Para llevar a cabo este sistema, un grupo de trabajo llamado Alianza Zigbee (Zigbee Alliance) formado por varias industrias, sin ánimo de lucro, la mayoría de ellas fabricantes de semiconductores, está desarrollando el estándar. La alianza de

empresas está trabajando codo con codo con IEEE para asegurar una integración, completa y operativa.

Zigbee se basa en el nivel físico y el control de acceso al medio (MAC) definidos en la versión de 2003 del estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal area network, WPAN) Figura 2.



**Figura 2. Relación IEEE 802.15.4/ZigBee. Fuente: Elaboración propia de los autores**

Esta alianza en las cuales destacan empresas como Invensys, Mitsubishi, Philips y Motorola trabajan para crear un sistema estándar de comunicaciones, vía radio y bidireccional, para usarlo dentro de dispositivos de automatización hogareña (domótica), de edificios (inmótica), control industrial, periféricos de PC y sensores médicos. Los miembros de esta alianza justifican el desarrollo de este estándar para cubrir el vacío que se produce por debajo del Bluetooth [5].. Ver en la Tabla 1.

<b>CARACTERISTICAS DE REDES INALAMBRICAS</b>			
	<b>ZigBee</b>	<b>Bluetooth</b>	<b>Wi-Fi</b>
<b>Estándar</b>	IEEE 802.15.4	802.15.1	IEEE 802.11a, b, g
<b>Organización</b>	ZigBee Alliance	Bluetooth SIG	Wi-Fi Alliance
<b>Topología</b>	Estrella, Árbol, malla	Estrella	Estrella
<b>Frecuencia RF</b>	868/915 MHz, 2.4 GHz	2.4 GHz	2.4 GHz, 5.8 GHz
<b>Tasa de transmisión</b>	250 kbits/s	723 kbits/s	11 a 105 Mbits/s
<b>Rango</b>	10 a 300 m	10 m	10 a 100 m
<b>Consumo de energía</b>	Muy baja	Baja	Alto
<b>Operación con baterías</b>	Baterías Alcalinas (meses o años)	Baterías Recargables	Baterías recargables (Horas)
<b>Nodos</b>	65.000	8	32

**Tabla 1. Comparación general de estándares inalámbricos.  
Fuente: elaboración propia de los autores.**

Esta nueva aplicación, definida por la propia Zigbee Alliance como el nuevo estándar global para la automatización del hogar, permite que las aplicaciones domóticas desarrolladas por los fabricantes sean completamente interoperables entre sí, garantizando así al cliente final fiabilidad, control, seguridad y comodidad [7].

Además la Zigbee Alliance también deja disponible para su acceso la Zigbee Cluster Library, ofreciendo de este modo a los ingenieros y demás integradores, deseosos de trabajar bajo este estándar mundial idóneo para los servicios domóticos, bloques de construcción para aplicaciones con necesidades bajo el denominador común de la automatización residencial, reduciendo de este modo las labores de desarrollo y permitiendo implementaciones más precisas.

La especificación 1.0 de Zigbee se aprobó el 14 de diciembre de 2004 y está disponible a miembros del grupo de desarrollo (Zigbee Alliance). Un primer nivel de suscripción, denominado adopter, permite la creación de productos para su comercialización adoptando la especificación por 3500 dólares anuales. Esta especificación está disponible al público para fines no comerciales en la petición de descarga, Esta primera versión ahora se le denomina ZigBee 2004.

La segunda versión y actual a junio de 2006 se denomina ZigBee 2006, y reemplaza la estructura MSG/KVP con una biblioteca de clusters, dejando obsoleta a la anterior versión. Finalmente ZigBee Alliance ha presentado la versión de 2007 . También se incluyen algunos perfiles de aplicación nuevos, como lectura automática, automatización de edificios comerciales y automatización de hogares basados en el principio de uso de la biblioteca de clusters.

En ocasiones ZigBee 2007 se denomina Pro, pero Pro es en realidad un perfil de aplicación que define ciertas características.

El nivel de red de ZigBee 2007 no es compatible con el de ZigBee 2004 o 2006, aunque un nodo RFD puede unirse a una red 2007 y viceversa. No pueden combinarse routers de las versiones antiguas con un coordinador 2007 [8].

## **2. Características de redes ZigBee [9].**

### **2.1 Dispositivos que conforman una red Zigbee**

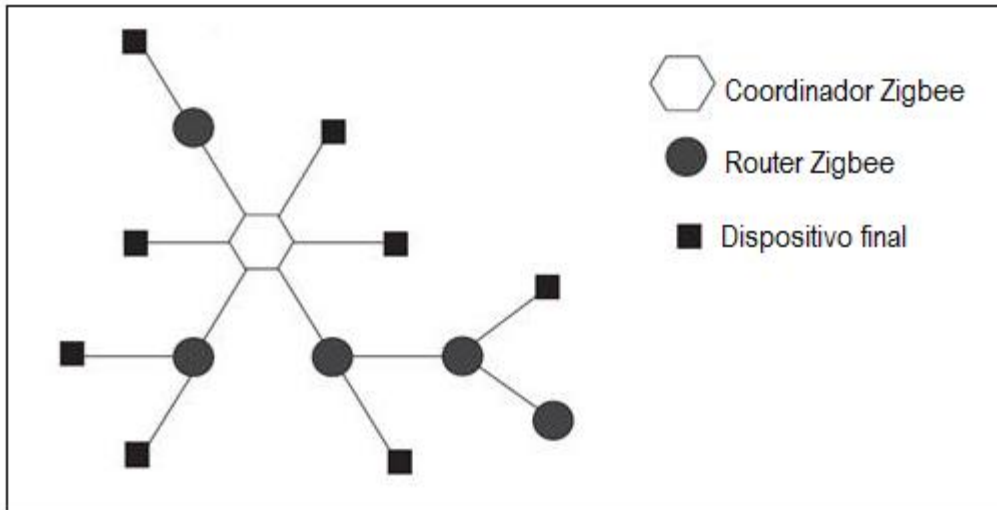
**2.1.1 Coordinador de Red (Zigbee Coordinator, ZC).** El tipo de dispositivo más completo. Debe existir uno por red. Sus funciones son las de encargarse de

controlan la red y los caminos que deben seguir los dispositivos para conectarse entre ellos. Recoge los datos de la red, sirve como punto de unión con la red LAN o con Internet. Ver Figura 2.

**2.1.2 El dispositivo de función completa (FFD):** (Full Function Device) dispositivo capaz de recibir mensajes del estándar 802.15.4. Este puede funcionar como un coordinador de red. La memoria adicional y la capacidad de computar, lo hacen ideal para hacer las funciones de **Router** (Zigbee Router, ZR). o para ser usado en dispositivos de red que actúen de interface con los usuarios. Interconecta dispositivos separados en la topología de la red, además de ofrecer un nivel de aplicación para la ejecución de código de usuario, Permiten evadir obstáculos, resolver problemas de congestión en la emisión de la información y posibles fallos en alguno de los aparatos creando nuevas rutas para redes más extensas.

**2.1.3 Dispositivo de funcionalidad reducida (RFD):** (Reduced Function Device): También conocido como nodo pasivo o **Dispositivo final** (Zigbee End Device, ZED). Tiene capacidad y funcionalidad limitadas (especificada en el estándar) con el objetivo de conseguir un bajo coste y una gran simplicidad. Posee la funcionalidad necesaria para comunicarse con su nodo padre (el coordinador o un router), pero no puede transmitir información destinada a otros dispositivos. De esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías. Un ZED tiene requerimientos mínimos de memoria y es por tanto significativamente más barato. Compuesto por sensores y actuadores donde se capturan los datos. Ver Figura 3.





**Figura 3. Dispositivos que conforman una red ZigBee.**  
**Fuente: Elaboración propia de los autores**

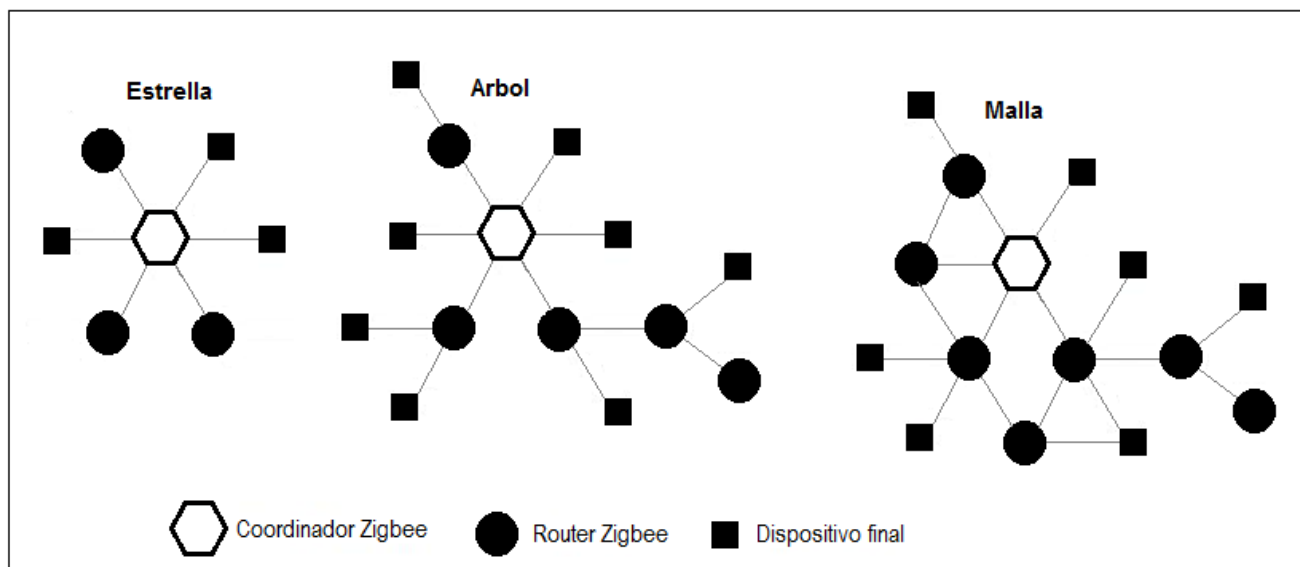
#### 2.1.4 Otras consideraciones:

Un nodo Zigbee, tanto activo como pasivo, reduce su consumo gracias a que puede permanecer “dormido” la mayor parte del tiempo, incluso muchos días seguidos. Cuando se requiere su uso, el nodo Zigbee es capaz de “despertar” en un tiempo muy corto y volverse a dormir cuando deje de ser requerido. Un nodo cualquiera “despierta” en aproximadamente 15 ms. Además de este tiempo, se muestran otras medidas de tiempo de funciones comunes:

- Nueva enumeración de los nodos esclavo (por parte del coordinador):  
aproximadamente 30 ms.
- Acceso al canal entre un nodo activo y uno pasivo: aproximadamente 15 ms.

## 2.2 Topologías [10].

Dependiendo de la aplicación que se esté desarrollando, se pueden configurar tres tipos de topología: Estrella, Árbol, Malla. A continuación se definen cada una de ellas: Ver Figura 4



**Figura 4. Topología de una red ZigBee. Fuente: Elaboración propia de los autores**

### 2.3.1 Topología en estrella

En la topología en estrella la comunicación se establece entre los nodos (RFD o FFD) y el nodo central llamado Coordinador. Una vez se conectan los nodos en una red en estrella, se elige cual va a ser el nodo coordinador de dicha red, el nodo elegido proporciona un identificador de red que no puede ser igual al identificador de otra red dentro del radio de acción de este nodo coordinador (área de cobertura o huella). El nodo coordinador será el que autorice la transmisión a los demás nodos debido a que será este el controlador de la red. Las aplicaciones más comunes que utilizan este tipo de topología son la conexión entre el ordenador personal y los periféricos, domótica o juguetes. Ver Figura 4.

### 2.3.2 Topología de Árbol

En este tipo de topología existen varios nodos coordinadores en una determinada zona y luego existe el papel del *PAN coordinator* que es el coordinador de toda la red que está en un nivel superior. Ver Figura 4.

### 2.3.3 Topología en Malla

En la topología en malla cualquier dispositivo puede comunicarse con cualquier otro mientras ambos estén en la misma área de cobertura o utilizando otros nodos para llegar al destino (topología mesh) debido a que tienen la misma prioridad a la hora de transmitir. Este tipo de topología es utilizada en redes ad hoc y se implementa en distintas aplicaciones como pueden ser control industrial, control de incendios o aplicaciones de inventario. Esta topología permite múltiples saltos entre el nodo origen y destino con lo que conlleva la utilización de protocolos de enrutamiento en este tipo de topología [11].. Ver Figura 4.

## 3. Relación IEEE 802.15.4 / ZigBee

La capa de más bajo nivel es la **capa física** (PHY), que en conjunto con la **capa de acceso al medio** (MAC), brindan los servicios de transmisión de datos por el aire, punto a punto. Estas dos capas esta descritas en el estándar IEEE 802.15.4–2003. Ver Figura 5.

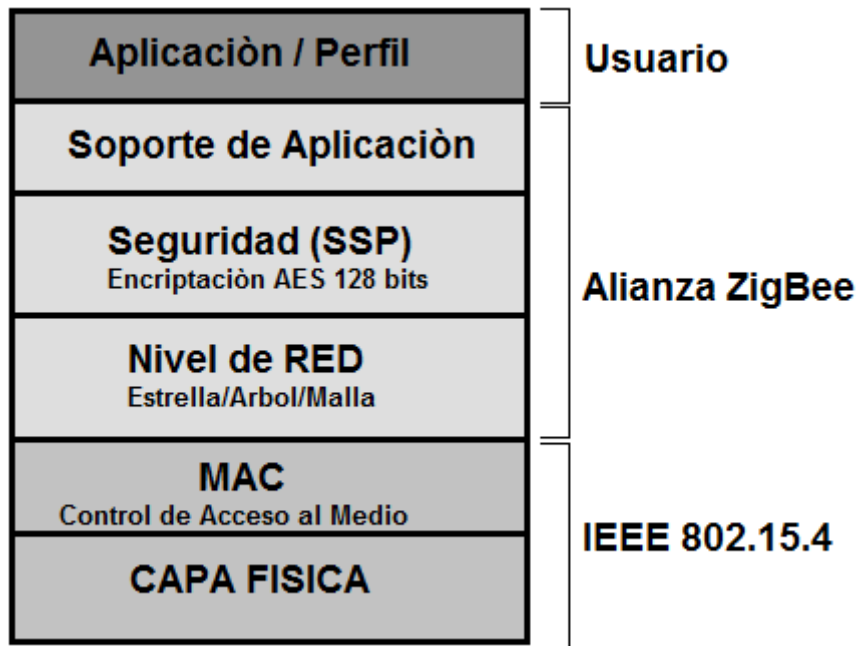


Figura 5. Relación IEEE 802.15.4/ZigBee.

Fuente: Elaboración propia de los autores

La **capa de red** (NWK) tiene como objetivo principal permitir el correcto uso del subnivel MAC y ofrecer una interfaz adecuada para su uso por parte de la capa de aplicación. En esta capa se brindan los métodos necesarios para: iniciar la red, unirse a la red, enrutar paquetes dirigidos a otros nodos en la red, proporcionar los medios para garantizar la entrega del paquete al destinatario final, filtrar paquetes recibidos, cifrarlos y autentificarlos.

**Capa de soporte a la aplicación** que es el responsable de mantener el rol que el nodo juega en la red, filtrar paquetes a nivel de aplicación, mantener la relación de grupos y dispositivos con los que la aplicación interactúa y simplificar el envío de datos a los diferentes nodos de la red. [12].

#### 4. Capa de Seguridad

AES (Advanced Encryption Standard), de acuerdo con la Comisión de Seguridad Nacional de Sistemas, el diseño y la fuerza del algoritmo AES es suficiente para proteger incluso

información clasificada considerada como de nivel secreto [15] y desde el 2003 se convirtió en uno de los algoritmos más utilizados hasta la actualidad.

Basado en el algoritmo de cifrado simétrico desarrollado por los estudiantes Vincent Rijmen y Joan Daemen de la Katholieke Universiteit Leuven en Bélgica, bajo el nombre "Rijndael" fue presentado en 1997 al concurso organizado por el Instituto Nacional de Normas y Tecnologías (NIST) para elegir el mejor algoritmo de cifrado; el algoritmo ganó el concurso transformándose en un estándar en el año 2002, con algunos cambios fue posteriormente renombrado AES (Advanced Encryption Standard).

El algoritmo AES en sí es una serie de pasos bien definidos que utilizan una clave proporcionada para la modificación de un mensaje por medio de la sustitución y permutación.

En AES el tamaño del bloque de datos es siempre 128 bits. Pero la clave puede ser de 128, 196, o 256 bits. El estándar ZigBee utiliza la opción de clave de 128 bits. El número de bits en una clave determinará el nivel de seguridad. Si la clave es sólo un 8 los bits, el intruso tiene que tratar un máximo de  $2^8 = (256)$  claves diferentes para recuperar el mensaje original. ZigBee es compatible con el uso de claves de 128 bits, lo que significa que hay  $2^{128} = (3.4) \times 10^{38}$  claves posibles. Es computacionalmente imposible probar  $2^{128}$  llaves diferentes.

En AES, cada algoritmo de cifrado está asociado con una llave. El algoritmo en sí es público conocimiento y al alcance de todos, pero el valor de la clave en cada transmisión es secreto. Existen diferentes métodos para adquirir una garantía llave. Por ejemplo, la clave puede ser embebido en el propio dispositivo por el fabricante.

Entre las principales limitaciones en la implementación de las funciones de seguridad en una red inalámbrica ZigBee son los recursos limitados. Los nodos son principalmente con pilas y han limitado potencia de cálculo y capacidad de memoria. ZigBee se apunta para aplicaciones de bajo costo, y el hardware de los nodos no puede ser resistente a las manipulaciones. Si un intruso adquiere un nodo de una red operativa no tiene resistencia a la manipulación, la clave real podría obtenerse simplemente de la memoria del dispositivo. Un nodo resistente a la manipulación puede borrar la información sensible incluyendo las claves de seguridad si se detecta la manipulación. [14].

## **5. Zigbee el día de hoy**

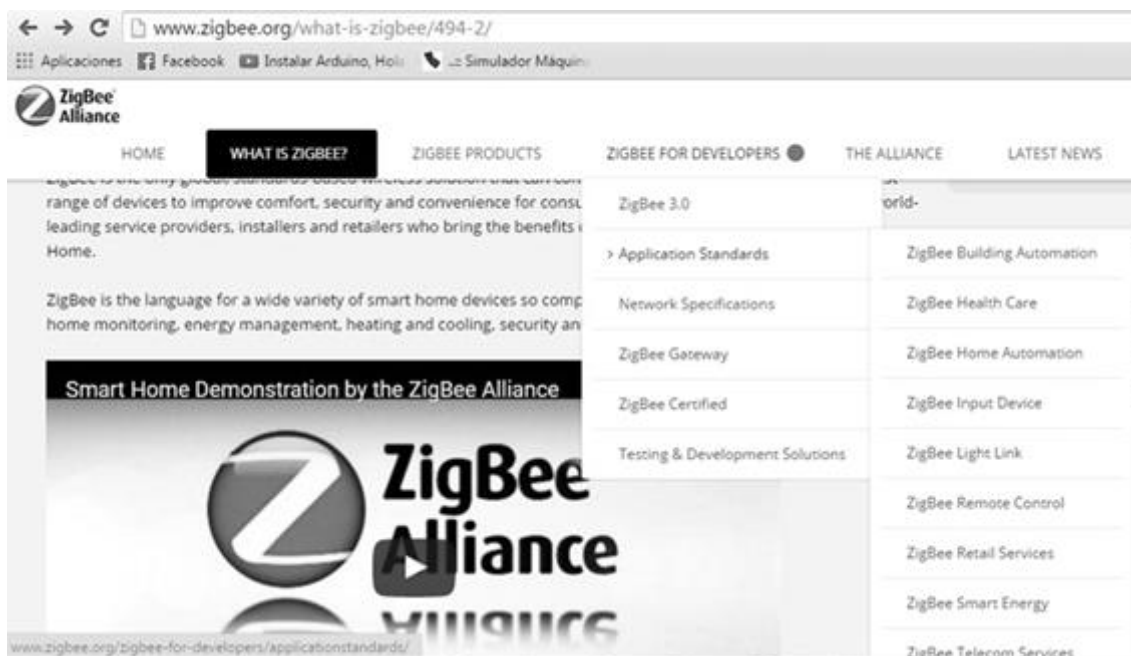
ZigBee 3.0: El fundamento para el Internet de las cosas ya está disponible [13].

ZigBee 3.0 es la unificación de los estándares inalámbricos líderes en el mercado de la Alianza en una sola norma. Esta norma proporciona interoperabilidad sin fisuras entre la más amplia gama de dispositivos inteligentes y ofrece a los consumidores y las empresas el acceso a productos y servicios innovadores que van a trabajar juntos sin problemas para mejorar la vida cotidiana.

ZigBee certificación 3.0 ya está disponible. Muchos miembros de la Alianza, incluyendo Atmel, Freescale, The Kroger Co., Legrand, NXP, Philips, Schneider Electric, Silicon Labs, Texas Instruments, Wincor Nixdorf, y V-Mark participaban activamente en el proceso de desarrollo y pruebas.

ZigBee es global y se basa en 2,4 GHz, que está disponible para su uso sin licencia en cualquier lugar del mundo. Esto significa que un desarrollador de productos puede vender el mismo producto en cualquier parte del planeta.

ZigBee 3.0 define más de 130 dispositivos y la más amplia gama de tipos de dispositivos incluyendo domótica, iluminación, gestión de energía, electrodomésticos inteligentes, seguridad, sensores y control de los productos de cuidado de la salud. Es compatible tanto con instalaciones prototipo de fácil de uso, así como los sistemas instalados profesionalmente. Todos los actuales tipos de dispositivo, comandos, y la funcionalidad se define en las normas basadas en ZigBee PRO actuales están disponibles en el ZigBee 3.0.



**Figura 6. ZigBee para desarrolladores.**

**Fuente:** <http://www.zigbee.org/zigbee-for-developers/zigbee3-0/>

La versión inicial de ZigBee 3.0 incluye ZigBee Home Automation, ZigBee Light Link, ZigBee Building Automation, ZigBee Retail Services, ZigBee Health Care, y los servicios de telecomunicaciones ZigBee. Ver Figura 6. Esto significa una gran variedad de dispositivos inteligentes puede interoperar sin problemas dando lugar a nuevas e innovadoras soluciones de IO.

## **6. Abreviaturas y Acrónimos**

AES Advance Encryption Standard

FFD Full Function Device

LR-WPAN Low-Rate Wireless Personal Area Network

MAC Medium Access Control

NWK Network Layer

PAN Personal Area Network

PHY Physical Layer

RFD Reduced Function Device

WLAN Wireless Personal Area Network

WPAN Wireless Personal Area Network

## **7. Conclusiones**

Durante la revisión del estado del arte acerca de ZigBee se amplió los conocimientos acerca de las tecnologías inalámbricas existentes y con mayor futuro dentro de las comunicaciones, las redes de nueva generación y la convergencia al Internet de las cosas, le dan a ZigBee un papel protagónico, esta tecnología se perfila como la que interconecte todo con todos, la Alianza ZigBee en este año está impulsando 6 normas de aplicación que abarcan la automatización de edificios, cuidado de la salud, domótica, energía inteligente, monitoreo del ambiente y otras aplicaciones de control básico.

Después de casi 15 años de su creación y 2 revisiones que al día de hoy son obsoletas, la Alianza ZigBee y sus desarrolladores han llegado a comunicar que están listos para que el



público y los integradores de tecnología le den la bienvenida a la era del Internet de las cosas.

## Referencias

- [1] 802.15.4 - IEEE Standard for Local and metropolitan area networks, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), 2011.
- [2] J. P. Dignani, "Análisis Del Protocolo Zigbee", tesis M. Sc., Facultad de Informática, Universidad Nacional de La Plata, La Plata, Argentina, 2012.  
[http://www.cib.espol.edu.ec/Digipath/D\\_Tesis\\_PDF/D-99539.pdf](http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-99539.pdf)
- [3] O. O. Jazmin, "Desarrollo De Un Prototipo De Adquisición De Variables Ambientales En Cultivos Hidropónicos De Lechuga, Mediante Una Red De Sensores, Utilizando Un Sistema Embebido", tesis M. Sc., Facultad De Ingeniería, Universidad De San Buenaventura, Bogotá D.C., Colombia, 2014.
- [4] 802.15.4 - IEEE Standard for Air Interface for Broadband Wireless Access Systems, Sección uno, 2012.
- [5] 802.15.1 – IEEE Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN's ), Sección uno, 2005
- [6] A. Sikora; V. F. Groza, "Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band", IEEE Conference Publications, 2005, pp. 1786 - 1791
- [7] C. Evans-Pughe, "Is the ZigBee wireless standard, promoted by an alliance of 25 firms, a big threat to Bluetooth?", IEE Reviews, vol. 49, no. 3, pp. 28-31, Marzo 2003.
- [8] C. G. Arano, "Impacto De La Seguridad En Redes Inalámbricas De Sensores IEEE 802.15.4", tesis M. Sc, Facultad de Informática, Universidad Complutense de Madrid, Madrid, España, 2010.
- [9] J. L. Burbank; J. Andrusenko; J. S. Everett; W. T. M. Kasch, "Wireless Networking: Understanding Internetworking Challenges", Wiley-IEEE Press, 2013, cap.3, pp. 41-99.

- [10] R. Schneiderman, "Modern Standardization:Case Studies at the Crossroads of Technology, Economics, and Politics", Wiley-IEEE Standards Association, 2015, cap.2, pp. 56-78.
- [11] T. Elarabi; V. Deep; C. K. Rai, "Design and simulation of state-of-art ZigBee transmitter for IoT wireless devices", 2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 2015, pp. 297-300.
- [12] E. D. Pinedo-Frausto; J. A. Garcia-Macias, "An experimental analysis of Zigbee networks", 2008 33rd IEEE Conference on Local Computer Networks (LCN), 2008, pp. 723 – 729.
- [13] "ZigBee 3.0: The Foundation for the Internet of Things is now Available", <http://www.zigbee.org/zigbee-for-developers/zigbee3-0/> , 2016
- [14] F. Rao; J. Tan, "Energy consumption research of AES encryption algorithm in ZigBee", Cyberspace Technology (CCT 2014), International Conference on, 2014, pp. 1 –6.
- [15] Announcing the ADVANCED ENCRYPTION STANDARD (AES), <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>, November 2001.