



# Tecnologías inalámbricas para recintos inteligentes

Iván Cabrera Altamirano, *Seguridad en Sistemas de Información.*

*Dr. Francisco Rodríguez Henríquez, CINVESTAV-IPN. Departamento de Computación*

**Resumen—** El presente documento presenta diversas tecnologías inalámbricas para la captura automática de información, haciendo especial énfasis en redes inalámbricas de sensores con protocolo IEEE 802.15.4 y Zigbee. También presenta la tecnología de identificación por radio frecuencia – RFID –. Se describirán los principios básicos de funcionamiento, sus principales ventajas y desventajas, así como sus áreas de futuro desarrollo. Finalmente aborda el diseño de espacios inteligentes haciendo uso de estas tecnologías.

## I. INTRODUCCIÓN

Una red inalámbrica de sensores es una infraestructura compuesta de elementos de sensado, elementos de cómputo y elementos de comunicaciones que proporcionan al administrador la habilidad para instrumentar, observar y reaccionar a eventos y fenómenos en un medio ambiente determinado.

El administrador típicamente es una entidad civil, gubernamental, comercial o industrial. El medio ambiente puede ser el mundo físico, un sistema biológico, o un sistema de información.

Las redes inalámbricas de sensores son vistas como una tecnología importante que experimentara un mayor desarrollo en los años siguientes.

Las aplicaciones típicas incluyen, pero no están limitadas a, recolección de datos, monitoreo, vigilancia, telemetría médica.

Adicionalmente al sensado, otras áreas de interés en las redes inalámbricas de sensores, son el control y activación de procesos.

En un contexto amplio, cualquier transmisión de radio que contenga algún tipo de información que permita identificación, es considerada como Identificación por Radio Frecuencia – RFID – (de su significado en inglés Radio Frequency Identification).

El termino RFID es usualmente utilizado para dispositivos y tecnología que utiliza señales de radio para intercambiar datos de identificación. En un contexto usual, esto implica un pequeño identificador o etiqueta que identifica a un objeto en específico.

El objeto recibe una señal de radio, interpreta esta, y entonces regresa un identificador o cualquier otra información que sirva para identificar al objeto. (e.g., ¿Quién eres tú? Contestando con, “Soy el objeto con identificador 0123456789”).

Alternativamente, el identificador puede ser tan complejo como una serie de retos y respuestas codificados mediante algún algoritmo de cifrado, que son interpretados con el apoyo de una base de datos, enviados a algún sistema de comunicación, o tomando parte de un sistema de pago.

Algunos de los usos actuales de la tecnología de identificación por radio frecuencia incluyen:

- Puntos de venta
- Identificación automática de vehículos.
- Control de acceso para inmuebles.
- Identificación de ganado.
- Seguimiento de activos.
- Identificación de mascotas.
- Manejo de almacenes y logística.
- Seguimiento de productos en la cadena de suministro.
- Seguimiento de partes y materiales en fábricas.
- Préstamo de libros en bibliotecas.
- Seguimiento de equipaje en aeropuertos.
- Cronometraje de eventos deportivos.
- Autenticación de objetos y prendas.

Se entiende por recintos inteligentes a aquellas construcciones que tienen integradas un conjunto de sistemas capaces de automatizar el recinto, aportando servicios de gestión energética, seguridad, bienestar y comunicación, y que pueden estar integrados por medio de redes interiores y exteriores de comunicación, cableadas o inalámbricas, y cuyo control goza de cierta ubicuidad, desde dentro y fuera del hogar.

Un recinto inteligente simultáneamente usa la electricidad, la electrónica y la informática, para crear un diseño arquitectónico propio, de tal manera que las personas que la habitan disfruten de mayores comodidades.

La tecnología avanzada, uno de los elementos que las caracterizan se puede aplicar tanto a casas habitación, departamentos, edificios, salones de eventos, escuelas, hospitales, entre otros.

## II. PRESENTACIÓN

### Zigbee

Zigbee es una especificación para un conjunto de protocolos de alto nivel, utilizando pequeños radios digitales de bajo consumo de energía, basados en el estándar IEEE 802.15.4 para redes inalámbricas de área personal, como pueden ser auriculares inalámbricos conectando con un teléfono celular vía un radio de corto alcance. La tecnología definida por Zigbee, es pensada para ser más simple y menos costosa que otras tecnologías de redes inalámbricas de área personal, como Bluetooth. Zigbee se enfoca a las aplicaciones de radio frecuencia que requieren una baja tasa de transferencia, larga duración de la batería y un entorno de red seguro.

Zigbee es oficialmente un protocolo para redes inalámbricas de sensores que fue diseñado para usarse en sensores con baja transferencia de datos y en redes de control. Si un sensor no necesita reportar constantemente su estado, el sensor puede mandar a un estado de bajo consumo de energía a la mayoría de sus componentes electrónicos (incluyendo el radio) la mayor parte del tiempo. Zigbee también puede eliminar la necesidad de instalar cables en el lugar donde instale la red.

Zigbee puede fácilmente alcanzar tasas de transferencia comparables con estándares cableados como RS232 y RS485. Aun cuando estas redes de sensores pueden fácilmente alcanzar las tasas de transferencia de RS232, no será común ver aplicaciones alimentadas a baterías haciendo reemplazo de un enlace RS232, especialmente si el tráfico en el enlace es pesado.

Cabe aclarar que Zigbee no es IEEE 802.15.4, y que IEEE 802.15.4 no es Zigbee. Zigbee es un protocolo de red basado en estándares soportados por la alianza Zigbee, que usan los servicios de transporte de la especificación de red en IEEE 802.15.4. La alianza Zigbee es responsable del estándar Zigbee, mientras que la IEEE es responsable de la especificación IEEE 802.15.4.

El estándar IEEE 802.15.4 actualmente define 2 capas físicas (abreviadas en inglés como PHY), las cuales operan en 3 bandas de frecuencia libres de licencia. La primera capa física, opera en la banda de frecuencias de 868 a 915 Mhz y la otra capa física es dedicada a la banda de frecuencias de 2.4 Ghz.

La banda de frecuencias ubicada en 2.4 Ghz, soporta un total de 16 canales, numerados del 11 al 26. Diez canales, numerados del 1 al 10, pueden ser encontrados en el rango de frecuencias de 902 Mhz a 928 Mhz. El tercer canal, el canal 0 puede ser encontrado entre 868 Mhz y 870 Mhz.

La tasa de transferencia de datos también difiere para cada banda, para la banda ubicada en 2.4 Ghz la máxima transferencia de datos es de 250 kbps, para la banda de 902 Mhz a 928 Mhz, la máxima transferencia de datos es de 40 kbps, mientras que para el canal 0, ubicado en 868 Mhz, su máxima transferencia de datos es de 20 kbps.

En cualquier parte del mundo es posible hacer uso de la banda de 2.4 Ghz, mientras que la banda por debajo de 1 Ghz, sólo puede ser usada en Norteamérica, Australia, Nueva Zelanda, Israel y Europa.

### Tipos de dispositivo:

Existen 3 tipos de dispositivos Zigbee:

- **Coordinador Zigbee (Zigbee Coordinator – ZC):** El dispositivo más capaz, el coordinador forma la raíz de la topología de red y también puede funcionar como puente entre otras redes. Hay exactamente sólo un coordinador Zigbee en cada red, siendo este el dispositivo que inicia la red. Es capaz de almacenar información acerca de la red, incluyendo un rol como centro de confianza y repositorio para llaves.
- **Ruteador Zigbee (Zigbee Router – ZR):** Así como puede ejecutar una aplicación común, un ruteador puede actuar como un ruteador intermediario, pasando data desde otros dispositivos.
- **Dispositivo Final Zigbee (Zigbee End Device – ZED):** Contiene solo funcionalidad limitada para hablar con los nodos padres (ya sea coordinadores o ruteadores), este dispositivo no puede retransmitir datos de otros dispositivos. Esta relación permite que el nodo esté dormido una cantidad significativa del tiempo, de tal modo que de una larga vida de batería. Un dispositivo final Zigbee requiere la menor cantidad de memoria, y por lo tanto puede ser menos costoso de fabricar que un ruteador o coordinador Zigbee.

### Seguridad en Zigbee

Uno de los aspectos más importantes ZigBee son los servicios de seguridad que ofrece para el soporte de comunicaciones. Se protege el establecimiento y transporte de claves, el cifrado de tramas y el control de dispositivos.

Se apoya en el marco definido por IEEE 802.15.4; la seguridad depende de la correcta gestión de las claves simétricas y la adecuada implementación de los métodos y políticas de seguridad.

### Modelo básico de seguridad

Las llaves son la base de la arquitectura de seguridad y, como tal, su protección es fundamental para la integridad del sistema.

Las claves nunca deben transportarse utilizando un canal inseguro, si bien existe una excepción momentánea que se da en la fase inicial de la unión de un dispositivo desconfigurado a una red.

La red ZigBee debe tener particular cuidado, pues una red ad hoc puede ser accesible físicamente a cualquier dispositivo externo y el entorno de trabajo no se puede conocer de antemano.

Las aplicaciones que se ejecutan en concurrencia utilizando el mismo transceptor deben, así mismo, confiar entre sí, ya que por motivos de costo no se asume la existencia de un cortafuegos entre las distintas entidades del nivel de aplicación.

Los distintos niveles definidos dentro de la pila de protocolos no están separados criptográficamente, por lo se necesitan políticas de acceso, que se asumen correctas en su diseño. Este modelo de confianza abierta posibilita la compartición de claves disminuyendo el costo de forma significativa.

No obstante, el nivel que genera una trama es siempre el responsable de su seguridad. Todos los datos de las tramas del nivel de red han de estar cifradas, ya que podría haber dispositivos maliciosos, de forma que el tráfico no autorizado se previene de raíz.

De nuevo, la excepción es la transmisión de la clave de red a un dispositivo nuevo, lo que dota a toda la red de un nivel de seguridad único. También se posible utilizar criptografía en enlaces punto a punto.

### Arquitectura de seguridad

ZigBee utiliza llaves de 128 bits en sus mecanismos de seguridad. Una llave puede asociarse a una red (utilizable por los niveles de ZigBee y el subnivel MAC) o a un enlace (en tal caso, adquirida por preinstalación, acuerdo o transporte). Las llaves de enlace se establecen en base a una llave maestra que controla la correspondencia entre claves de enlace.

Como mínimo la llave maestra inicial debe obtenerse por medios seguros (transporte o preinstalación), ya que la seguridad de toda la red depende de ella en última instancia. Los distintos servicios usarán variaciones en una sola dirección de la llave de enlace para evitar riesgos de seguridad.

Es claro que la distribución de llaves es una de las funciones de seguridad más importantes. Una red segura encarga a un dispositivo especial la distribución de llaves: el denominado centro de confianza (*trust center*).

En un caso ideal los dispositivos llevarán precargados de fábrica la dirección del centro de confianza y la llave maestra inicial. Si se permiten vulnerabilidades momentáneas, se puede realizar el transporte como se ha descrito.

Las aplicaciones que no requieran un nivel especialmente alto de seguridad utilizarán una llave enviada por el centro de confianza a través del canal inseguro transitorio.

Por lo tanto, el centro de confianza controla la llave de red y la seguridad punto a punto. Un dispositivo sólo aceptará conexiones que se originen con una llave enviada por el centro de confianza, salvo en el caso de la llave maestra inicial. La arquitectura de seguridad está distribuida entre los distintos niveles de la siguiente manera:

- El subnivel MAC puede llevar a cabo comunicaciones fiables de un solo salto. En general, utiliza el nivel de seguridad indicado por los niveles superiores.
- El nivel de red gestiona el ruteo, procesando los mensajes recibidos y pudiendo hacer difusión de peticiones. Las tramas salientes usarán la llave de enlace correspondiente al ruteo realizado, si está disponible; en otro caso, se usará la llave de red.
- El nivel de aplicación ofrece servicios de establecimiento de claves al dispositivo de objeto Zigbee y las aplicaciones, y es responsable de la difusión de los cambios que se produzcan en sus dispositivos a la red. Estos cambios podrían estar provocados por los propios dispositivos (un cambio de estado sencillo) o en el centro de confianza, que puede ordenar la eliminación de un dispositivo de la red, por ejemplo. También encamina peticiones de los dispositivos al centro de seguridad y propaga a todos los dispositivos las renovaciones de la llave de red realizadas por el centro. El dispositivo de objeto Zigbee mantiene las políticas de seguridad del dispositivo.

La estructura de niveles de seguridad se basa en CCM, una variante de CCM que añade servicios de sólo-cifrado y sólo-integridad.

### RFID

Un sistema RFID se compone básicamente de los siguientes elementos:

- Lector
- Antenas
- Identificadores

### Lector

Es un dispositivo electrónico que permite leer y escribir diversos tipos de etiquetas, autenticar una etiqueta en caso de que cuente con capacidades de cifrado. Comúnmente se conecta a una PC, PDA o también se encuentra disponible como un dispositivo independiente.

En el caso de etiquetas con capacidad de escritura, el lector tiene la capacidad de guardar información en las localidades asignadas con tal fin.

Como parte del sistema se puede conectar con una base de datos en la cual se pueden consultar o modificar registros de acuerdo a la operación seleccionada.

## Antena

Una antena es un dispositivo capaz de emitir o recibir ondas de radio. Está constituida por un conjunto de conductores diseñados para radiar un campo electromagnético cuando se le aplica una fuerza electromotriz alterna.

De manera inversa, en recepción, si una antena se coloca en el alcance de un campo electromagnético, genera como respuesta a este campo, una fuerza electromotriz alterna.

El tamaño de las antenas está relacionado con la longitud de onda de la señal de radiofrecuencia transmitida o recibida, debiendo ser, en general, un múltiplo o submúltiplo exacto de esta longitud de onda.

Por eso, a medida que se van utilizando frecuencias mayores, las antenas disminuyen su tamaño.

La antena deberá ser seleccionada de acuerdo a la frecuencia de operación de las etiquetas RFID disponibles.

## Identificadores

Los identificadores son los dispositivos RFID que se adherirán al producto que se desee identificar, existen 3 tipos de identificadores: pasivos, semi-activos y activos.

Las identificadores pasivos no tienen una fuente de alimentación interna, la corriente eléctrica inducida por el campo electromagnético es suficiente para hacer que el identificador responda a la solicitud de información requerida por un sistema RFID.

Típicamente un identificador pasivo tendrá menos alcance y menos capacidad de almacenamiento que un identificador activo.

Al contrario de los identificadores pasivos, un identificador activo tiene una batería como fuente de alimentación, proporcionando un mayor rango de alcance y una mayor capacidad de almacenamiento, una batería puede durar varios años en un dispositivo activo.

Un identificador activo tiene un costo más alto de fabricación; sin embargo tiene ventajas sobre un identificador pasivo, todo depende del uso que se le desee dar.

Actualmente la mayoría de los identificadores son pasivos debido a su bajo costo e independencia de una fuente de alimentación.

Un identificador semi-activo es aquel que utiliza la corriente eléctrica inducida por el campo electromagnético para poner en un estado de listo al identificador, pero que para responder con la información solicitada al lector, lo hace utilizando como fuente de alimentación las baterías conectadas al sistema.

Este esquema amplia la distancia a la cual un identificador puede ser detectado, la razón principal es que en un identificador pasivo puede recibir energía de un lector aún encontrándose muy lejos de él, sin embargo la energía que recibe no es suficiente para contestar estando a esa distancia, por lo tanto, agregando baterías al sistema este es capaz de emitir su respuesta.

Además las etiquetas también pueden clasificarse por sus rangos de frecuencias de operación:

Categoría	Frecuencias
<b>Baja frecuencia</b>	125 – 134 KHz
<b>Alta frecuencia</b>	13.56 Mhz
<b>Ultra elevada frecuencia</b>	868 – 956 Mhz
<b>Microondas</b>	2.45 Ghz

A continuación se describe el funcionamiento de un identificador de baja frecuencia. Figura 1.

### Baja Frecuencia

1. Un circuito integrado envía una señal a un oscilador, el cual produce una fuerza electromotriz alterna en la bobina del lector.
2. La corriente en la bobina genera un campo magnético que sirve de fuente de alimentación para la etiqueta.
3. El campo producido interactúa con la bobina en la etiqueta, la cual induce una corriente que produce que un condensador se cargue.
4. El voltaje en el condensador debido a su carga, activa el circuito integrado de la etiqueta el cual transmite su identificador.
5. El identificador se expresa como señales digitales bajas y altas que polarizan a un transistor para que este se encuentre apagado o encendido.
6. Variaciones en la resistencia del circuito como consecuencia del encendido o apagado del transistor causan que se genere un campo magnético, el cual interactúa con el campo magnético del lector.

En esta técnica llamada modulación de carga, los cambios en las fluctuaciones en el campo magnético causan cambios en el flujo de corriente desde el lector a la bobina en el mismo patrón de unos y ceros transmitidos por la etiqueta.

7. Las variaciones en el flujo de corriente en la bobina del lector son captadas por un dispositivo que convierte ese patrón en una señal digital la cual es enviada a un circuito integrado que determina el identificador.

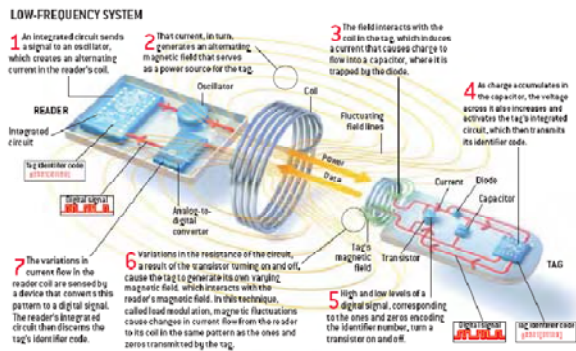


Figura 1. Funcionamiento de un sistema RFID en baja frecuencia.

## Seguridad en sistemas RFID

La seguridad a menudo se considera como secundaria e ciertas tecnologías. RFID está siendo utilizado en múltiples áreas donde poca o nula consideración se realiza acerca de los problemas de seguridad.

Aun cuando RFID es una tecnología joven, la seguridad de algunos sistemas RFID ha sido comprometida. En Enero de 2005, el cifrado del dispositivo SpeedPass de Mobil fue rota por un equipo de estudiantes de la universidad John Hopkins.

En Febrero de 2006, Adi Shamir, profesor del departamento de ciencias computacionales del Instituto Weizmann, reportó que pudo monitorear los niveles de potencia en identificadores RFID utilizando una antena direccional y un osciloscopio.

Él dijo, que los patrones en los niveles de potencia pueden ser usados para determinar cuando los bits de una contraseña son correctamente o incorrectamente recibidos por un dispositivo RFID.

Usando esta información, un atacante puede comprometer la aplicación del algoritmo SHA-1, el cual es usado para criptográficamente asegurar algunos identificadores RFID.

Un grupo de investigadores, de la universidad de Ámsterdam, crearon virus y gusanos para dispositivos RFID, como una prueba de concepto.

Este grupo logró ajustar un programa malicioso "malware", en un área de memoria de un identificador RFID. Cuando el identificador es interrogado por un lector, el código malicioso pasa del identificador a la base de datos, desde donde el código malicioso puede pasar a otros identificadores, o usado para llevar a cabo acciones malévolas.

El código malicioso empleado, incluye sentencias en lenguaje SQL las cuales generalmente son usados contra servidores.

Sin llegar a entender los errores del pasado, la gente comete los mismos errores, dado que RFID está basado en ondas de radio, siempre existe la posibilidad de que existan entidades que escuchan sin autorización.

## Recintos Inteligentes

Se entiende por recinto inteligente a toda instalación que integra servicios con el fin de automatizar y eficientar al máximo un conjunto de actividades.

Entre los aspectos más importantes a manipular encontramos:

- **Ahorro de energía:** No es necesario sustituir la mayoría de los aparatos del hogar con similares que consuman menos energía, sino ejecutar un plan energético de manera eficiente, el cual contempla, apagar aparatos cuando no son utilizados, zonificación y programación de climas, uso de energías alternas.
- **Comodidad:** Implica todas las acciones que se puedan llevar a cabo para mejorar la comodidad del recinto, donde destaca la iluminación, control vía Internet, facilidad de uso, integración de tecnologías, entre otros.
- **Seguridad:** Consiste en una red de seguridad encargada de proteger tanto los bienes patrimoniales y la seguridad de los habitantes, haciendo uso de los siguientes recursos: alarmas de incendio, sensores de gas, control de acceso, alerta médica, acceso a cámaras de seguridad.
- **Comunicaciones:** Son los sistemas e infraestructuras de comunicaciones que posee el hogar. Acceso al sistema desde Internet, una computadora personal, un celular, PDA, entre otros.
- **Accesibilidad:** Diseño para todos, un diseño accesible para la diversidad humana, la inclusión social y la igualdad. Este enfoque constituye un reto ético y creativo. Donde las personas con capacidades diferentes puedan acceder a estas tecnologías sin temor a un obstáculo del tipo tecnológico.

## Arquitectura de Recintos Inteligentes

La arquitectura de un sistema inteligente está conformada básicamente por 3 entidades:

- **Controlador:** Es el principal componente del sistema, este se encarga de recoger las señales de los sensores, analizarlas, procesarlas y producir una señal a ser llevada a cabo por los actuadores.

Debe tener capacidad de comunicación con dispositivos tanto internos como externos al sistema, así como de llevar un registro de todas las operaciones efectuadas.

- Sensores: Estos dispositivos se encargan de recoger el valor de variables físicas y convertirlos a señales eléctricas de voltaje y/o corriente que serán interpretadas por el controlador.

La etapa de conversión de una variable física a una señal eléctrica de corriente y/o voltaje, se le denomina transducción, en este proceso actúan diversos componentes electrónicos como filtros, amplificadores, convertidores análogo/digital.

- Actuadores: Estos dispositivos se encargan de recibir órdenes por parte de un controlador para efectuar una cierta acción física en el sistema, como por ejemplo, abrir y cerrar una válvula, una puerta, levantar o bajar las persianas, encender y apagar el aire acondicionado.

Todas estas acciones las realiza mediante componentes electromecánicos, entre los cuales destacan: relevadores, contactores, triacs, entre otros.

Dependiendo del recinto donde se vaya a instalar la aplicación inteligente, podemos tener las siguientes arquitecturas:

- Centralizada: Un controlador recibe información de múltiples sensores, y una vez procesada genera las órdenes apropiadas para los actuadores.
- Distribuida: Toda la inteligencia está distribuida por los módulos sensores o módulos actuadores.
- Mixta: sistemas con arquitectura descentralizada en cuanto a que disponen de varios pequeños dispositivos capaces de adquirir y procesar la información de múltiples sensores y transmitirlos al resto de dispositivos distribuidos en el recinto.

### III. CONCLUSIONES

El desarrollo de tecnologías de captura automática de información e identificación se ha desarrollado bastante en las últimas décadas, crean algunas tecnologías muy interesantes como las presentadas en este trabajo.

Sin embargo muchas de estas tecnologías aún se encuentran en desarrollo, con áreas de oportunidad de mejora bastante amplias.

Una de esas áreas con bastante oportunidad de mejora, es la seguridad, donde hemos visto que muchas de las limitantes actuales de seguridad en dispositivos inalámbricos, son debido a las altas restricciones en poder de cómputo, memoria y energía que estos dispositivos poseen.

La estandarización de protocolos como lo es por parte de IEEE para las redes inalámbricas de sensores o como lo es por parte de ISO para los identificadores RFID ha contribuido bastante al crecimiento de forma organizada de estas tecnologías, dándole al integrador de aplicaciones más de una opción para elegir los dispositivos con los cuales construirá su aplicación.

Por último, pero no menos importante, es la polémica respecto a la privacidad de los usuarios de estas tecnologías, dado a que es posible con infraestructura adicional, llevar registro de las actividades del usuario, lo cual constituye una grave violación a la privacidad de las personas – en cuanto a sus preferencias, actividades y costumbres –.

Para que estos sistemas puedan ser implementados de forma eficiente, los usuarios finales deben estar absolutamente seguros de que los datos proporcionados o recabados a través de dispositivos inalámbricos solamente serán usados para el fin que fueron diseñados (e.g. en una tienda, para la transacción de compra – venta, movimientos en inventarios, etc).

### IV. REFERENCIAS

- Thorton, Frank - RFID Security
- Sohrawy, Kazem - Wireless Sensor Networks
- Security Analysis of a Cryptographically-Enabled RFID Device.  
Bono Steve, Juels Ari, Rubin Avi.  
<http://www.rfidanalysis.org>
- RFID: The Promise and Perils of Talkative Chips  
Scientific American – January 2004
- <http://es.wikipedia.org/wiki/Domótica>
- <http://es.wikipedia.org/wiki/Zigbee>