Comunicaciones Wi-Fi de bajo consumo e inmunes a ataques de denegación de servicio (DoS) para redes de sensores inalámbricos

Berná Galiano, José Ángel[1,*].

[1,*] Dpto. Física, Ingeniería de Sistemas y Teoría de la Señal. Universidad de Alicante. Apartado de Correos 99 E-03080 (Alicante). Correo electrónico: jberna@ua.es

---

Resumen: La transformación digital del control y monitorización de los sistemas físicos se ha denominado paradigma IoT (Internet of Things), donde la conectividad de cualquier tipo de dispositivo es uno de los elementos principales. Uno de sus campos de aplicación es la sensorización de sistemas físicos (domóticos, industriales, vehículos de transporte, etc.) donde se establecen unos requisitos de comunicaciones de bajo consumo y gran alcance. Estas tecnologías de comunicación LPWAN se han extendido fundamentalmente en tres modelos: Sigfox, LoRaWAN y NB-IoT. Su uso está limitado al coste económico del servicio de datos (cuota por sensor conectado) y la cobertura de estaciones base. Este trabajo presenta un nuevo sistema de comunicaciones patentado aplicable a chipsets Wi-Fi (IEEE 802.11), proporcionando un bajo consumo en los sensores, cobertura de varios kilómetros y coste de comunicaciones por sensor nulo. El sistema consta de una estación base que recibe paquetes IEEE 802.11 emitidos desde los sensores con unas características que permiten superar los problemas de seguridad del estándar WPA2 actual (ataques de desautenticación Wi-Fi, cracking de contraseñas WPA2-PSK, etc.). Para ello se emplean enlaces Wi-Fi no asociados y cifrado de los datos (AES) con claves preinstaladas y reconfigurables para cada escenario de uso. Como prueba de concepto, se presenta una prueba piloto consistente en el despliegue de un prototipo de estación base en un entorno forestal de montaña que obtiene medidas de temperatura y humedad de una serie de sensores desplegados en la zona. La estación base prototipo recibe las transmisiones de los sensores a distancias de 3 km con visión directa (sin obstáculos opacos a la banda de 2.4 GHz). Los sensores presentan un bajo consumo de energía en la transmisión de datos al combinar el sistema de comunicaciones patentando y el uso del chipset Wi-Fi del SoC (*System on Chip)* ESP8266.

Palabras clave: IoT LPWAN WiFi Seguridad Redes Sensores

---

1. Introducción

El desarrollo del paradigma IoT (Internet de las Cosas) en la década de 2010 se ha fundamentado en el desarrollo tecnológico de las redes de sensores. La sensorización es un proceso clave del desarrollo de sistemas automáticos digitales, donde un bajo consumo del sensor y un sistema de comunicaciones inalámbrico son sus elementos clave.

Los sistemas de comunicaciones inalámbricos para redes de sensores han sufrido una evolución tecnológica pasando de las redes inalámbricas propietarias a redes inalámbricas de uso generalizado en el entorno LAN y WAN. En estas redes inalámbricas estándares, distinguimos entre las que emplean un espectro de radiofrecuencia público (Wi-Fi [1], Bluetooth, Sigfox, LoRaWAN) o espectro privado (NB-IoT, LTE-M) [2].

En la actualidad, el auge de las redes de sensores se encuentra en el desarrollo de los entornos inteligentes (*smart cities, smart buildings, smart rural areas,* etc.) donde la solución de comunicación son redes inalámbricas de gran cobertura y bajo consumo (*Low Power Wide Area Network*). Así, sistemas como NB-IoT, LTE-M, Sigfox o LoRaWAN son los más extendidos. Estas redes presentan la característica de ser ofrecidos por algún operador de telecomunicaciones, lo que implica unos costes de explotación (cuota de datos por sensor) que no existen en otras como las redes Wi-Fi. La tecnología Wi-Fi puede ser desplegada por el propio usuario de la red y emplea un espectro de radiofrecuencia de libre uso (2.4/5 GHz), por lo que su coste económico de despliegue es muy bajo, así como el coste de explotación (cuota de datos por sensor nulo).

El uso de la tecnología Wi-Fi como sistema de comunicaciones en redes de sensores implica un funcionamiento basado en el modo de infraestructura [1]. Las redes de infraestructura con puntos de acceso (APs) permiten una mayor cobertura para redes de sensores, donde no es necesaria cobertura solapada entre todos los sensores de la red. Así, es posible establecer redes de sensores basados en puntos de acceso Wi-Fi que gestionan la conectividad entre los sensores y la seguridad de la comunicación (cifrado y autenticación).

Sin embargo, el uso de la tecnología Wi-Fi en redes de sensores es poco eficiente y segura, debido a las siguientes características:

1) Los enlaces Wi-Fi asociados entre APs y dispositivos (sensores) precisan de un nivel mínimo de señal adecuado para mantener activo el enlace. Las atenuaciones en la señal provocan conexiones/desconexiones continuas y por tanto, una distancia efectiva de comunicación de pocos cientos de metros.
2) Los procesos de conexión/desconexión del AP y la monitorización del estado del enlace (paquetes *Probe Request*) provocan un consumo energético elevado en el sensor, lo que reduce su autonomía.
3) La seguridad de las redes Wi-Fi actuales basadas en WPA2-PSK [7], es totalmente insuficiente debido a los problemas de seguridad ya conocidos [2] [4]. Además todos los sistemas WPA2 son víctimas sencillas de los ataques de denegación de servicio (DoS) por desautenticación [5] [6], al no emplear en su gran mayoría el mecanismo IEEE 802.11w que los evita. Aunque el recién publicado sistema WPA3 [7] solventará estos problemas en el futuro, existen millones de chipsets Wi-Fi en el mercado que seguirán operativos y no lo soportarán.

Las limitaciones indicadas anteriormente han impulsado el uso y desarrollo de redes LPWAN específicas para la conectividad de sensores, descartando la tecnología Wi-Fi en gran cantidad de campos de aplicación.

Sin embargo, es posible solventar las limitaciones anteriores empleando una tecnología de comunicación Wi-Fi patentada [8] que se presenta en este trabajo.

2. Comunicaciones Wi-Fi de bajo consumo y gran alcance

2.1 Esquema de funcionamiento

Se presenta un nuevo sistema de comunicaciones Wi-Fi que, empleando la misma arquitectura que una red Wi-Fi de infraestructura, proporciona mejoras prestaciones en cuanto a área de cobertura, consumo de energía y seguridad de las comunicaciones. En la Figura 1 se muestran los elementos del sistema de comunicaciones, consistente en una estación base (EB) con cobertura para un conjunto de sensores en un entorno de varios kilómetros de distancia.

Figura 1. Elementos de la tecnología de comunicación Wi-Fi patentada

Este sistema de comunicaciones tiene las características de:

1) No emplea enlaces asociados Wi-Fi, transmitiendo la información directamente entre una estación base (EB) y los sensores que se encuentren en la cobertura de la EB. Este procedimiento, detallado en [8], permite encapsular los datos dentro de paquetes de control *Beacon Frame*, identificados todos con el mismo valor del campo SSID. Así, no emplea el protocolo IP como transporte de los datos transmitidos por los sensores.
2) El uso de una EB que no emplea WPA2 proporciona una inmunidad a ataques DoS de desautenticación. La seguridad de las comunicaciones entre EB y sensores se realiza con cifrado AES de 128 bits con claves preinstaladas en los sensores y la EB.
3) El sistema permite la transmisión de datos al nivel de la sensibilidad del chipset Wi-Fi de la EB y los sensores, lo que permite distancias de comunicación de varios kilómetros.
4) El sistema puede implementarse en cualquier chipset Wi-Fi, pues emplea paquetes recogidos en la norma IEEE 802.11.

2.2 Consumo energético

Una de las características de las redes de sensores es que éstos deben disponer en general de una autonomía de batería elevada (de días a meses) pues su acceso estará muchas veces restringido, o bien la renovación de las fuentes de alimentación supone un coste elevado.

Existen chipsets Wi-Fi diseñados para su empleo en sensores. Uno de ellos es el módulo ESP8266, un SoC que incorpora un chipset Wi-Fi con consumos reducidos. Además, permite la

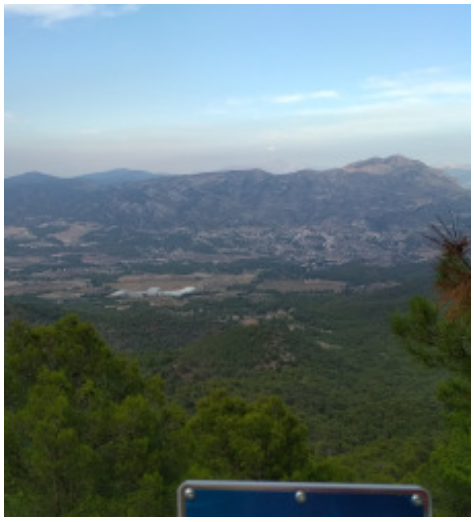
programación de paquetes *Beacon Frame* a medida (proporciona el modo monitor para el chipset Wi-Fi) y dispone de un modo de consumo muy bajo (*Deep Sleep)* para mantener el módulo en reposo cuando no hay transmisiones Wi-Fi.

3. Escenario de prueba de concepto

3.1 Red de sensores en zonas forestales

Como escenario de pruebas de evaluación del sistema de comunicaciones Wi-Fi descrito en el apartado 2, se escogerá una zona forestal en la que se desplegará un conjunto de 4 sensores de temperatura y humedad, y una Estación Base (EB) que almacenará la información transmitida por los sensores.

La EB se emplazará en un punto elevado de la zona forestal, disponiendo de visual a la localización de los diferentes sensores, que se distribuirán a diferentes distancias de la EB según se indica en la Figura 2.

a) 

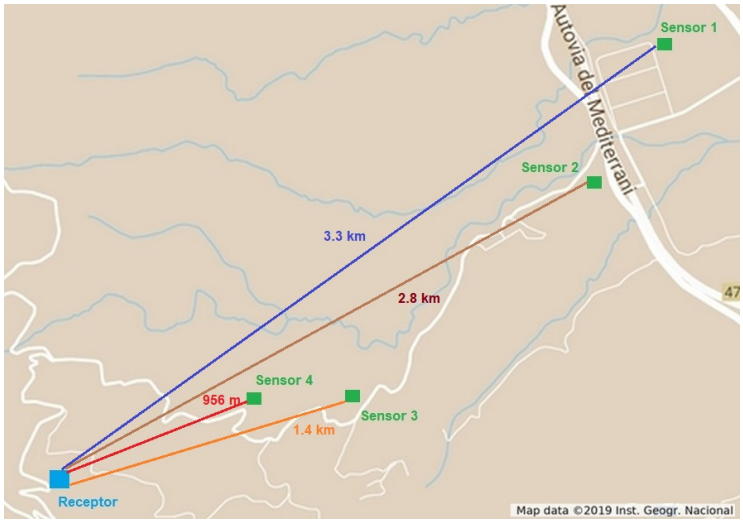
b) 

Figura 2. Emplazamiento de la EB a) y los sensores b).

Así, se podrá evaluar la transmisión de datos por parte de los sensores según las características de su emplazamiento, como se indica en la Tabla 1.

Sensor	Distancia a la EB	Altura sobre el terreno	Visual de la EB
Sensor 1	3.3 km	2 m	Total
Sensor 2	2.8 km	1.80 m	Total
Sensor 3	1.4 km	0.60 m	Parcial
Sensor 4	0.956 km	0.60 m	Total

Tabla 1. Emplazamientos de los sensores.

El emplazamiento de los diferentes sensores permite una visual sin obstáculos entre sensor y EB (Visión Total) o con obstáculos de la masa forestal (Visión Parcial) como se observa en la Figura 3.

a) 

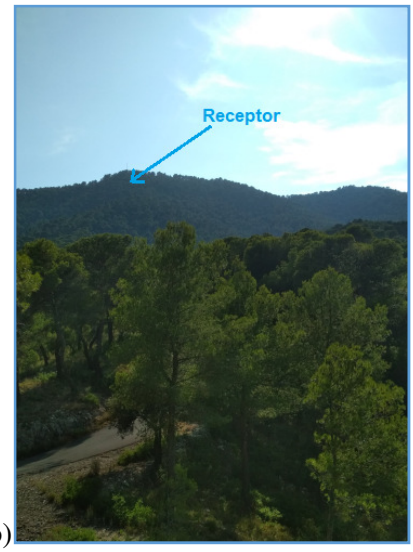
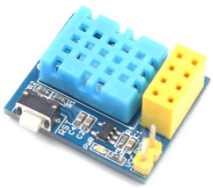
b) 

Figura 3. Visual Parcial a), o Total b), desde el sensor a la EB.

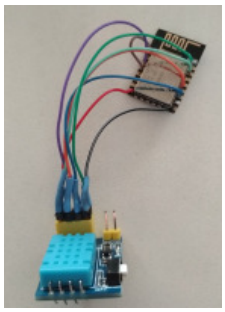
3.2 Sensores de temperatura y humedad

Los dispositivos sensores empleados constan de dos elementos: el sistema de comunicaciones basado en el SoC ESP8266 y el elemento de sensorización de temperatura y humedad, el sensor DHT11.

La elección del sensor DHT11 se ha hecho para una fácil integración electrónica con el ESP8266. Así, es posible emplear el módulo ESP01-S DHT11, que permite lecturas de temperatura y humedad por parte del ESP8266. Sin embargo, este módulo está pensado para el módulo ESP01 de la familia ESP8266, que no permite el acceso al modo de ahorro de energía *Deep Sleep*. Por ello, se empleará el módulo ESP12 que permite acceso al modo de ahorro de energía *Deep Sleep* y se integrará con el módulo ESP01-S DHT11, como se indica en la figura Figura 4.

a) 

b) 

c) 

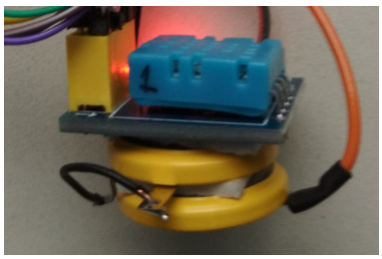
d) 

Figura 4. Módulo ESP01-S DHT11 a), ESP12 b), conexión entre ambos c), y alimentación d).

Para evaluar las prestaciones de transmisión en diferentes localizaciones, cada sensor se programará para transmitir cada 30 segundos **2** paquetes Wi-Fi (duplicados) con los datos obtenidos de temperatura y humedad. Estos datos estarán cifrados empleando una clave AES de 128 bits común para los sensores y la EB. La transmisión duplicada tiene como objetivo una mayor tolerancia a atenuaciones o interferencias de la señal transmitida. Se empleará además la banda de transmisión de 2.4 GHz, pues proporciona una menor atenuación con la distancia.

La alimentación del sensor es muy variada en cuanto a tipos de batería y debe estar comprendida en el rango de 3.7V a 12V. En este despliegue se ha optado por una alimentación con el tamaño más

reducido posible. Esta selección son pilas de litio modelo CR2032 por lo que, al proporcionar 3V de tensión, será necesario emplear 2 unidades en serie proporcionando 6V. El reducido tamaño de las baterías tipo *cell coin* permite una adaptación al módulo minimizando el volumen, como se muestra en la Figura 4.

La autonomía de los sensores permite un despliegue de hasta 40 horas de funcionamiento. Las principales limitaciones en la autonomía del sensor está en la baja capacidad de las baterías CR2032 (150 - 200 mAh, según proveedor), el consumo continuo del módulo DHT11 de 1.5 mA, y el consumo importante del ESP12 en la transmisión Wi-Fi (aproximadamente de 150 mA). Aunque el consumo del módulo ESP12 se minimiza al emplear el modo *Deep Sleep*, las 2 transmisiones Wi-Fi tienen un consumo importante en un periodo muy corto (pocos milisegundos).

3.3 Estación Base

La Estación Base se ha desarrollado empleando un microPC con procesador Broadcom de 1GHz, 512 MB RAM y Sistema Operativo Linux. En esta arquitectura se ha programado un software en lenguaje C que, empleando la librería libpcap [9], permite la monitorización de señales detectadas en un interfaz Wi-Fi con chipset Ralink 3070. Este interfaz está conectado a una antena direccional comercial de gran ganancia y diseño de tipo *patch*.

Todo el conjunto tiene unas reducidas dimensiones (antena Wi-Fi de 20cm x 18cm) y reducido peso que puede ser alimentado con baterías tipo PowerBank, como se muestra en la Figura 5.

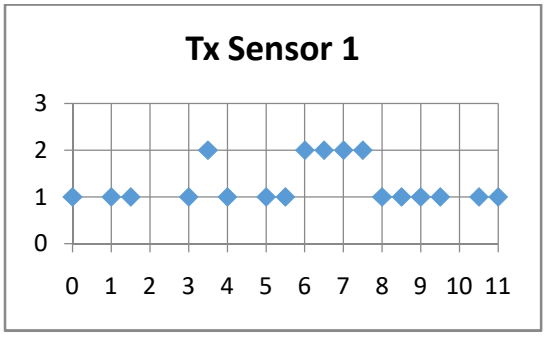
a)  b) 

Figura 5. Componentes de la Estación Base a) y emplazamiento en la prueba b).

4. Resultados y discusión

La prueba de concepto del funcionamiento del sistema de comunicaciones Wi-Fi desarrollado ha obtenido unos resultados satisfactorios para los diferentes emplazamientos de los sensores.

Se describirá a continuación el éxito de las transmisiones Wi-Fi de los sensores, donde se mostrará el número de transmisiones recibidas por la Estación Base (1 o 2) en cada periodo de 30 segundos, para cada uno de los sensores.

a) 

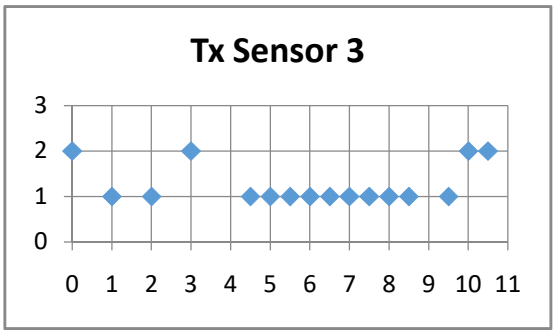
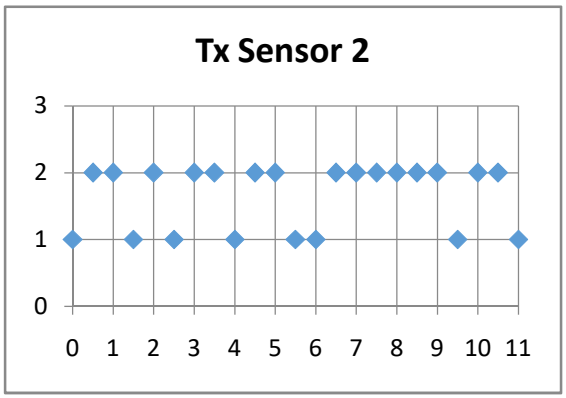
b) 

Figura 6. Transmisiones con éxito del sensor 1 y sensor 3 en un periodo de 11 minutos.

a) 

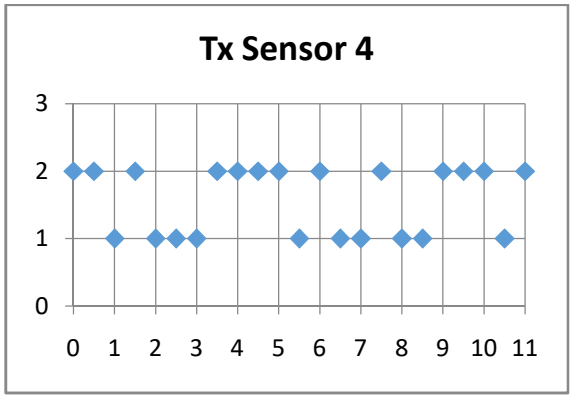
b) 

Figura 7. Transmisiones con éxito del sensor 2 y sensor 4 en un periodo de 11 minutos.

En la Figura 6 puede comprobarse que, aunque existe una gran continuidad en la recepción de datos de los sensores 1 y 3 por parte de la Estación Base (EB), existen periodos donde la información no se recibe. El valor medio de potencia de señal medido en la EB es de -75,22 dBm para el sensor 1 y de -75,69 dBm para el sensor 3. La sensibilidad del chipset Wi-Fi Ralink 3070 está en unos -80 dBm, y por tanto estos emplazamientos están en el límite de distancia alcanzable por parte de la EB (sensor 1) y visión parcial por parte de la EB (sensor 3).

En la Figura 7 puede comprobarse como, en el caso de los sensores 2 y 4, existe continuidad en la recepción de datos por parte de la EB (debido a la duplicación de la transmisión Wi-Fi por parte del sensor), no existiendo pérdida de datos en ninguno de los periodos de 30 segundos. Las ubicaciones de los sensores 2 y 4 se caracterizan por una atenuación adecuada para el chipset Wi-Fi Ralink 3070, pues el valor medio de potencia de señal medida en la EB es de -69,68 dBm para el sensor 2 y de -72,31 dBm para el sensor 4.

5. Conclusiones

El sistema de comunicaciones Wi-Fi presentado en este trabajo ha sido verificado para su funcionamiento en redes de sensores. Sus prestaciones son una alternativa a otros tipos de redes de sensores existentes, destacando:

1) Reducción del consumo energético y aumento de las distancias de comunicación de los chipsets Wi-Fi actuales.
2) Inmunidad a los ataques dirigidos a las redes de sensores que emplean IP como protocolo de transporte de datos (IP/ARP spoofing) y a los ataques de Denegación de Servicio (DoS) propios de redes Wi-Fi WPA2.

3) Uso de espectro de radiocomunicación no reservado (2.4 GHz), lo que implica independencia de un operador de telecomunicaciones y libertad de despliegue en cualquier emplazamiento. Así como coste de datos cero en la transmisión de información.

El empleo de esta red de sensores puede tener un especial interés en aplicaciones en el campo militar y de emergencias, como pueden ser:

1) Despliegue de redes de sensores para la Unidad Militar de Emergencias en atención a desastres naturales donde las redes de sensores basadas en operadores de telecomunicaciones quedan inutilizadas: incendios forestales, terremotos, etc.
2) Despliegue de redes de sensores en vehículos y edificios con un coste económico reducido, inmunidad a ataques DoS y bajo consumo.

Este sistema, además, tiene una gran capacidad de mejora: Es posible reducir el consumo de los sensores con un diseño electrónico específico y aumentar las distancias de comunicación con un diseño de antena en la EB con mejores prestaciones que el sistema comercial empleado.

Referencias

1. Stallings W. Comunicaciones y Redes de Computadores. *Madrid: Prentice Hall;* **2004**.
2. Gobierno de España. Cuadro Nacional de Atribución de Frecuencias. Disponible en: https://avancedigital.gob.es/espectro/Paginas/cnaf.aspx
3. Martín A, Alonso C. Crackear WPA/WPA2 PSK. Disponible en: http://www.elladodelmal.com/2009/01/crackear-wpawpa2-psk-i-de-ii.html
4. Vanhoef M. Key Reinstallation Attacks. Disponible en: https://www.krackattacks.com/
5. Bicakci K, Tavli B. Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces*. **2009**; 31(5): 931-941.
6. Singh R, Sharma T.P. On the IEEE 802.11i security: a denial-of-service perspective. *Security and Communication Networks*. **2015**; 8(7): 1378-1407.
7. Wi-Fi Alliance. Documentos normativos de las redes Wi-Fi WPA2, WPA3. Disponible en: https://www.wi-fi.org/
8. Berná J.A. Procedimiento de difusión y obtención de información, dispositivo emisor, dispositivo receptor y sistema de difusión y obtención de información. Patente ES2608506. *Oficina Española de Patentes y Marcas*. **2016**.
9. PCAP – Packet Capture Library. Disponible en: https://www.tcpdump.org.