SISTEMA DE DETECCIÓN DE PUNTOS DE ACCESO WIFI EN UN CENTRO DE DATOS

José Ignacio Vega Luna

Universidad Autónoma Metropolitana, Unidad Azcapotzalco

vlji@correo.azc.uam.mx

Mario Alberto Lagos Acosta

Universidad Autónoma Metropolitana, Unidad Azcapotzalco

Gerardo Salgado Guzmán

Universidad Autónoma Metropolitana, Unidad Azcapotzalco

Víctor Noé Tapia Vargas

Universidad Autónoma Metropolitana, Unidad Azcapotzalco

Francisco Javier Sánchez Rangel

Universidad Autónoma Metropolitana, Unidad Azcapotzalco

Resumen

Se presenta la implantación de un sistema que detecta puntos de acceso WiFi no autorizados en un centro de datos que puedan vulnerar la seguridad de la información. El sistema consiste de tres módulos: el módulo de detección WiFi, el módulo supervisor y la interface de usuario. Se construyeron cinco módulos de detección WiFi instalados en diferentes puntos del centro de datos los cuales se comunican inalámbricamente con el módulo supervisor conectado a una computadora donde se ubica la interface de usuario. La computadora se localiza en una oficina de control y monitoreo. Periódicamente la interface de usuario solicita al módulo supervisor, conectado al puerto USB de la computadora, transmitir la orden de exploración de señal WiFi a cada módulo de detección, al recibir esta orden los módulos envían el nombre de los puntos de acceso detectados. La interface de usuario muestra el nombre de los puntos de acceso

detectados no autorizados, registrándolos con fecha y hora en un archivo diario. La comunicación entre los módulos de detección y el módulo supervisor se realiza usando transceptores ZigBee. El alcance entre los módulos de detección y la oficina de control fue 95 metros y el alcance de detección fue 50 metros.
Palabra(s) Clave(s): centro de datos, microcontrolador, USB, WiFi, ZigBee.

1. Introducción

En el ámbito de comunicaciones inalámbricas, un punto de acceso WiFi (hotspot) es un lugar desde el cual se puede acceder a la Internet usando una red inalámbrica y un router. Un hotspot contiene uno o varios routers para cubrir un área donde la demanda de tráfico es alta [1]. El acceso a un hotspot es mediante una computadora, teléfono móvil, tableta u otro router. En algunas empresas existen hotspots en lugares específicos y bajo control. La red WiFi de un hotspot usa transceptores que trabajan a 2.4 GHz (802.11b y 802.11g) o 5 GHz (802.11a) con alcance de 30 a 300 metros dependiendo del tipo de antena y potencia de transmisión [2].

Un centro de datos es un espacio donde empresas e instituciones instalan, mantienen y operan su infraestructura de TIC (Tecnologías de Información y Comunicaciones) usada para realizar las actividades de su negocio y giro. En este espacio se alojan servidores, sistemas de almacenamiento y equipo de comunicaciones para la ejecución y acceso de aplicaciones. Existen empresas con grandes instalaciones que proporcionan servicios de un centro de datos a clientes que necesitan centrar su atención en las actividades propias de su negocio olvidándose del funcionamiento de un centro de datos. Estos centros de datos cuentan con instalaciones de alta tecnología redundantes en lo que respecta a piso falso, enfriamiento, ventilación, energía eléctrica, cableado, detección y extinción de incendios, detección de fugas de agua, controles de seguridad y acceso, así como facilidades de comunicación de datos. Los clientes, usuarios, administradores y operadores de los centros de datos acceden los sistemas de cómputo de forma remota o local, los usuarios que lo hacen localmente usan redes alambradas o inalámbricas. Dada la extrema seguridad requerida en el

acceso a la información, la cantidad de redes inalámbricas WiFi y hotspots en un centro de datos debe ser limitada y bajo control de los administradores del mismo [3]. Los clientes y usuarios externos pueden instalar y usar routers WiFi temporalmente cuando sea estrictamente necesario para realizar sus actividades con previa autorización. Estas medidas de seguridad son certificadas por instituciones y organismos que auditan el funcionamiento, operación y calidad de servicios de centros de datos. Cada punto de acceso WiFi permanente o temporal en el centro de datos es registrado. Una necesidad actual, simple y existente es detectar puntos de acceso no autorizados, los cuales en ocasiones son instalados sin malas intenciones o por error y representan riesgo en la seguridad de datos o pueden interferir con redes WiFi existentes. El objetivo de este trabajo fue diseñar y construir un sistema confiable, de bajo costo, compacto y de fácil instalación que detecte puntos de acceso WiFi en diferentes áreas de un centro de datos, y transmita inalámbricamente su nombre a una interface de usuario para su registro. El desarrollo del trabajo fue a solicitud de una empresa que tiene centros de datos y ofrece sus servicios a una diversidad de clientes. Para diseñar el sistema se identificaron dos necesidades básicas: la detección de puntos de acceso y la transmisión inalámbrica con alcance de 75 metros donde se ubica la interface de usuario.

Existen soluciones que monitorean, configuran y operan puntos de acceso WiFi. Algunas soluciones sirven para monitorear puntos de acceso y determinar los servicios más utilizados por los usuarios [4, 5], otras determinan la calidad de servicio (tiempo de respuesta y cantidad de información transferida) de puntos acceso [6] o realizan estadísticas de tiempo de permanencia de usuarios [7]. Se han desarrollado también trabajos que analizan el tráfico de redes WiFi y asignan canales de frecuencia a dispositivos terminales para mejorar la calidad de servicio [8, 9]. Respecto a aplicaciones del circuito ESP8266, usado en el trabajo aquí presentado, los trabajos realizados se han enfocado a utilizarlo para automatización de hogares y oficinas desde dispositivos móviles [10, 11, 12]. Aunque realmente es sencilla, no existe ninguna solución para detectar puntos de

acceso y mejorar la seguridad en centros de datos, como la aquí presentada, que cumpla con los requerimientos y tareas solicitadas en este trabajo.

Para la implantación de este trabajo se usó un circuito integrado del tipo SoC (System on Chip) de reciente tecnología para explorar el ambiente y detectar puntos de acceso WiFi. El SoC seleccionado fue el circuito ESP8266 [13]. El ESP8266 es un adaptador de Serie a WiFi de bajo consumo de energía que proporciona acceso a Internet para aplicaciones de dispositivos móviles e Internet de las cosas (IoT-Internet of Things), entre las cuales se incluyen: electrodomésticos, automatización de hogares y oficinas, cámaras IP, redes de sensores y dispositivos para acceso a redes WiFi. Las principales características del ESP8266 son las siguientes: tamaño compacto, económico, fácil de usar e incorpora diferentes funcionalidades que pueden configurarse y accederse desde un controlador.

El circuito ESP8266 proporciona conectividad WiFi de bajo costo a un microcontrolador liberándolo de realizar funciones de red WiFi o puede funcionar como procesador que ejecuta una aplicación, como por ejemplo un servidor web. Cuenta con memoria interna ROM para almacenar el firmware y se le puede conectar memoria externa flash de programa cuando funciona como procesador. El firmware implanta las siguientes funcionalidades: WiFi 802.11 b/g/n de 2.4 GHz, soporte de protocolos de red IPv4, TCP/UDP/HTTP/FTP, así como funciones de protocolos de bajo nivel RTS/CTS, reconocimiento, encapsulamiento y fragmentación de tramas (802.11h/RFC 1042). La figura 1 muestra el diagrama de bloques funcionales del ESP8266 entre los cuales se pueden distinguir los siguientes: adaptador de antena, transceptor de RF, CPU, memoria SRAM, reloj de tiempo real, watchdog, convertidor analógico-digital (ADC) de 10 bits, 17 terminales de entrada/salida, interfaces serie: UART (dos), I2C (Inter-integrated Circuit Interface), SPI (Serial Peripheral Interface), I2S (Integrated Interchip Sound, para transmisión de audio de alta fidelidad) y salida PWM. Todos estos bloques permiten conectar el ESP8266 a un controlador con mínima circuitería externa.

La CPU del circuito ESP8266 es un procesador de 32 bits que se puede programar usando el kit de desarrollo suministrado por el fabricante del circuito. La

CPU puede usarse para implantar funcionalidades adicionales como por ejemplo algoritmos de seguridad, pre-autenticación y prioridad de tráfico.

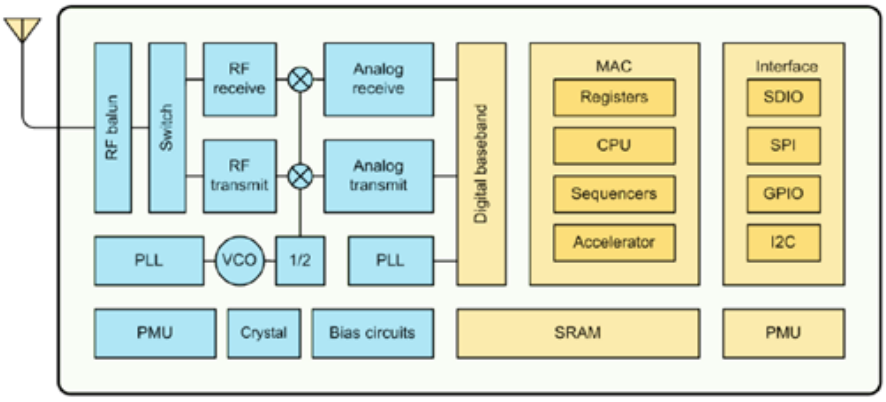

Figura 1 Diagrama de bloques del ESP8266.

El ESP8266 se alimenta con una fuente de 3.0 a 3.6 V y puede configurarse en uno de tres modos de operación: modo activo, modo suspendido (sleep) o modo suspendido profundo (deep sleep). En modo activo consume 50 mA. En modo sleep solo se encuentran activos el watchdog y el reloj de tiempo real y consume 0.9 mA, el circuito puede mantener la conexión a un punto de acceso. En modo deep sleep solo se encuentra activo el reloj de tiempo real y consume 60 µA. El circuito puede programarse para despertar después de un tiempo configurado en el reloj de tiempo real o al suceder alguna condición específica. Además, puede configurarse en uno de tres modos de funcionamiento: estación, punto de acceso o mixto (estación y punto de acceso). En el modo estación, el ESP8266 proporciona acceso a una red WiFi al controlador conectado a una de sus interfaces serie. En modo punto de acceso proporciona acceso a una red WiFi a dispositivos conectados a él por RF.

Las características operacionales del ESP8266 se establecen enviando comandos AT desde un microcontrolador conectado a la interface UART0 del ESP8266 o desde una computadora conectando el UART0 al puerto USB de la computadora. En la computadora debe ejecutarse un programa emulador de terminal, como por ejemplo hyperterminal o Putty, para suministrar los comandos y mostrar la respuesta del circuito. El puerto UART0 puede configurarse a una velocidad entre

9.6 Kbps y 115.2 Kbps. Algunas características operacionales que pueden seleccionarse con comandos AT son las siguientes: inicializar el circuito (reset), listar puntos de acceso WiFi disponibles, mostrar versión de firmware, mostrar direcciones IP, establecer velocidad de interfaces serie, establecer modo de operación y establecer modo de funcionamiento.

En la implantación de este trabajo, para transmitir la información de puntos de acceso detectados por el ESP8266 a la interface de usuario, ubicada en la oficina de control y monitoreo del centro de datos, se usaron transceptores XBee-PRO (S2). Estos transceptores son compatibles con el estándar ZigBee. ZigBee es un estándar que define un conjunto de protocolos de comunicación para redes inalámbricas de corto alcance y baja velocidad de datos [14]. ZigBee está basado en el estándar IEEE 802.15.4 de WPAN ya que usa la capa física y protocolos de control de acceso medio (MAC) de este estándar. ZigBee fue desarrollado para aplicaciones inalámbricas de bajo costo y ultra-bajo consumo de energía. En muchas aplicaciones de ZigBee, el tiempo que el dispositivo inalámbrico está involucrado en la actividad es limitado y se mantiene la mayor parte de tiempo en modo de ahorro de energía, conocido como modo de suspensión o reposo. Como resultado, los dispositivos ZigBee pueden trabajar varios años antes de reemplazar su batería. Inicialmente ZigBee se usó en aplicaciones domóticas y en años recientes se ha utilizado en diversas aplicaciones en los campos de control y monitoreo de procesos, industrial, medicina, agricultura, automotriz, entre otros, ya que se pueden configurar redes de malla con transceptores ZigBee. La relación entre IEEE 802.15.4-2003 y ZigBee es similar a la existente entre IEEE 802.11 y WiFi Alliance. ZigBee utiliza la banda ISM de uso industrial, científico y médico, la cual incluye: 868 MHz en Europa, 915 en Estados Unidos y 2.4 GHz en el resto del mundo y transmite a una velocidad máxima es 250 Kbps [15]. Sin embargo, la mayoría de dispositivos de este tipo usan de 2.4 GHz, por ser libre en todo el mundo. Las redes ZigBee pueden tener hasta 65,535 nodos distribuidos en subredes de 255 nodos. Las principales características operacionales de un nodo o transceptor ZigBee son las siguientes: consume aproximadamente 30 mA transmitiendo y 3 µA en reposo, permanece la mayor parte del tiempo suspendido

o en reposo y su velocidad máxima es 250 Kbps. Los transceptores ZigBee se utilizan en aplicaciones sensibles al uso de energía en las cuales la transferencia de datos es menor que otras tecnologías inalámbricas como por ejemplo Bluetooth. Algunas de estas aplicaciones son para monitoreo de variables y procesos y control de actuadores [16].

Dependiendo de la función en la red, un nodo ZigBee puede ser uno de tres tipos siguientes:

- Coordinador. Es el modo más completo de un transceptor ZigBee. En una red ZigBee debe existir al menos un coordinador, ya que su función es el control de la red y las rutas que deben seguir los dispositivos para conectarse entre sí.
- Router. Su función es conectar dispositivos separados en la topología de la red y ofrecer un nivel de aplicación para la ejecución de código de usuario.
- Dispositivo final. Realiza la función de comunicarse con su nodo padre (coordinador o router), pero no puede transmitir información a otros dispositivos. Este tipo de nodo puede estar suspendido la mayor parte del tiempo para aumentar la vida útil de sus baterías. Tiene requerimientos mínimos de memoria y es más económico que los dos tipos anteriores.

2. Desarrollo

El primer paso de la metodología usada en el diseño de este trabajo fue dividirlo en tres módulos: el módulo remoto de detección WiFi, el módulo supervisor y la interface de usuario. En la figura 2 se indica el diagrama de bloques del sistema construido. El segundo paso fue especificar las funciones de los componentes de cada módulo.

El tercer paso fue seleccionar los componentes de acuerdo a las características indicadas en el objetivo del sistema y su función en cada módulo, y el último paso fue conectar y configurar los componentes del sistema. La función de cada módulo, características y componentes se explican a continuación.

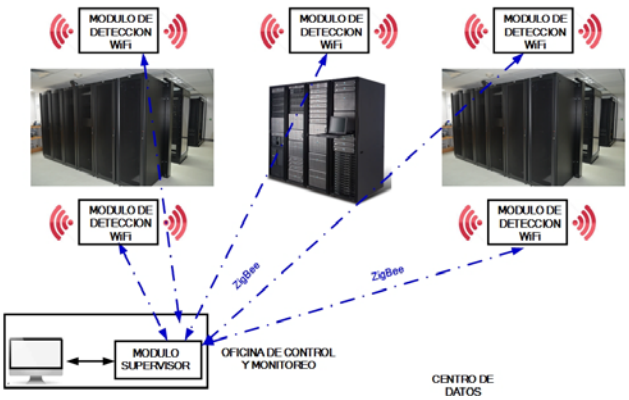

Figura 2 Diagrama de bloques del sistema.

El módulo remoto de detección WiFi

Este módulo está compuesto por tres elementos como se indica en el diagrama de bloques de la figura 3: el circuito detector y de acceso a WiFi, el adaptador de niveles, el microcontrolador y el transceptor ZigBee.

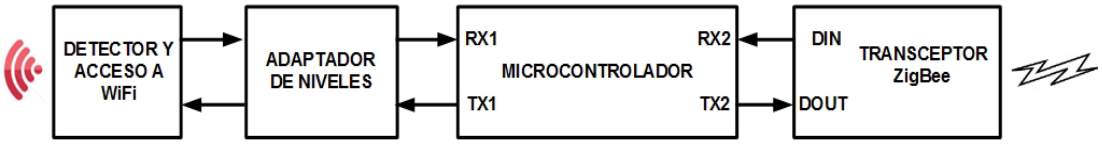

Figura 3 Diagrama de bloques del módulo de detección WiFi.

La función de detección de redes WiFi la realiza el circuito ESP8266. Para acceder y configurar el ESP8266 desde el microcontrolador, se usó el puerto EUSART1 del microcontrolador conectado al puerto UART0 del ESP8266. No se conectaron directamente ambos puertos, ya que el ESP8266 se alimenta con 3.3 V y el nivel de voltaje de las terminales de su puerto UART0 son también de 3.3 V, mientras que el nivel de voltaje de las terminales del EUSART1 del microcontrolador son 5 V. Para adaptar los niveles de voltaje, se utilizó el circuito bidireccional BP1. El circuito BP1 se alimenta con 5 V y sus terminales A1 y A2 se conectaron a las terminales RX1 y TX1, respectivamente, del puerto EUSART 1 del microcontrolador como se indica en la figura 4.

El circuito ESP8266 se configuró desde el programa que se ejecuta en el microcontrolador enviando comandos AT. La configuración establece las

siguientes funciones: modo activo, como estación y velocidad de 9.6 Kbps. Se configuró como estación porque la tarea del circuito es solo explorar el ambiente e indicar el nombre de las redes WiFi detectadas en su vecindad. Se estableció velocidad de 9.6 Kbps porque la cantidad de información que envía el ESP8266 a la interface de usuario no es grande.

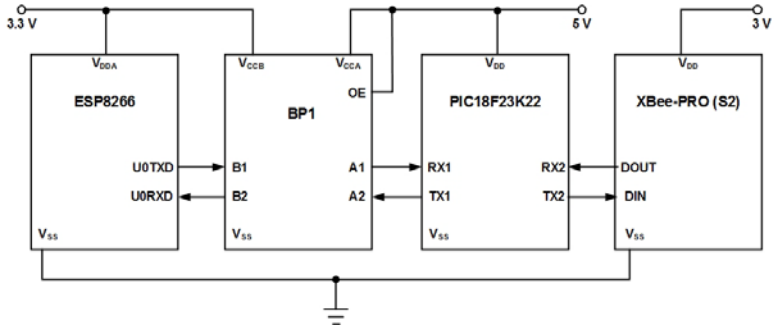

Figura 4 Diagrama de conexión de componentes del módulo de detección WiFi.

El microcontrolador usado en este módulo es el PIC18F23K22, este dispositivo cuenta con los siguientes recursos: CPU de 8 bits, memoria de programa flash de 8 kBytes, memoria RAM de 512 Bytes, tres puertos paralelo, dos puertos serie EUSART, convertidor analógico/digital (ADC) de 30 canales y 10 bits, siete temporizadores y dos puertos serie síncronos (Master Synchronous Serial Port-MSSP). La programación que se ejecuta en el microcontrolador inicializa los puertos EUSART, inicializa los temporizadores 1 y 2 (para generar el baud rate de los EUSART), configura el circuito ESP8266 y a continuación entra a un ciclo donde espera la orden de detección de WiFi enviada por el módulo supervisor. Al recibir la orden, el microcontrolador envía, por medio del puerto EUSART1 el comando AT+CWLAP al circuito ESP8266 para indicarle que explore los puntos de acceso WiFi existentes en su periferia. Cuando el ESP8266 responde con el nombre de las redes detectadas, el microcontrolador transmite, por medio del puerto EUSART2, esta información al transceptor ZigBee. Esta programación se implantó usando lenguaje mikroC PRO FOR PIC siguiendo el diagrama de flujo de la figura 5. La secuencia de comandos enviados por el microcontrolador para configurar el circuito ESP8266 se muestra en la figura 6.

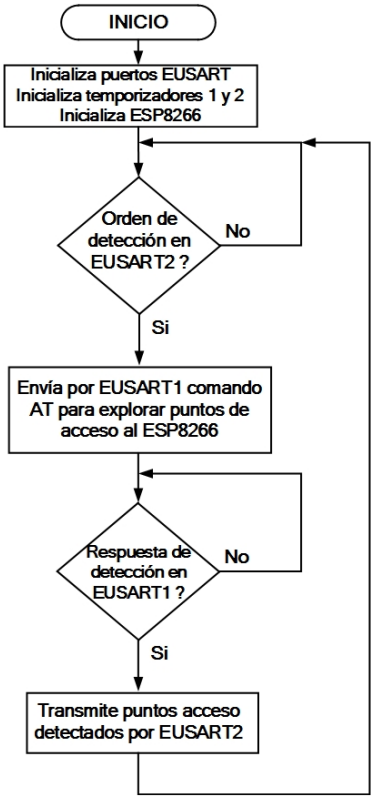

Figura 5 Diagrama de flujo de la programación del módulo de detección WiFi.

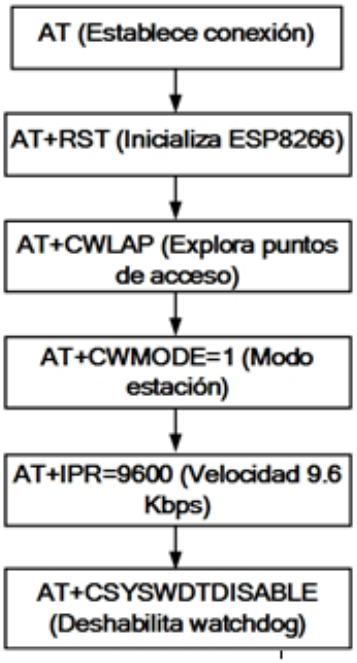

Figura 6 Secuencia de comandos AT enviados para inicializar el circuito ESP8266.

Para comunicarse con el módulo supervisor, cada módulo de detección tiene un transceptor ZigBee. El puerto EUSART2 del microcontrolador se conectó al puerto UART del transceptor ZigBee para transmitir al módulo supervisor el nombre de las redes detectadas y el identificador del módulo de detección (número de serie del transceptor XBee). Se seleccionaron transceptores ZigBee porque son de tecnología inalámbrica que no requieren instalar cableado adicional ni modificar la infraestructura de comunicaciones actual del centro de datos y además su señal no interfiere con las redes WiFi usadas.

El transceptor usado fue el circuito XBee-PRO (S2), este circuito es un dispositivo compatible con el protocolo ZigBee 802.15.2, cuenta con antena integrada que puede transmitir información inalámbrica a una distancia máxima de 300 pies (90 m) en interiores, se alimenta con una fuente de 3.3 V y puede configurarse para trabajar en una red de malla, lo que le permite extender su rango de transmisión usando routers ZigBee. El circuito XBee-PRO (S2) del módulo de detección WiFi se configuró como router y se estableció una velocidad de 9.6 kbps bps para comunicarse con el puerto EUSART2 del microcontrolador. De esta manera, se pueden instalar uno o varios módulos de detección WiFi en diferentes ubicaciones del centro de datos reportando al módulo supervisor conectado al puerto USB de una computadora localizada en la oficina de monitoreo y control.

El módulo supervisor

Este módulo está compuesto por el transceptor ZigBee y el microcontrolador, como se puede ver en el diagrama de bloques de la figura 7.

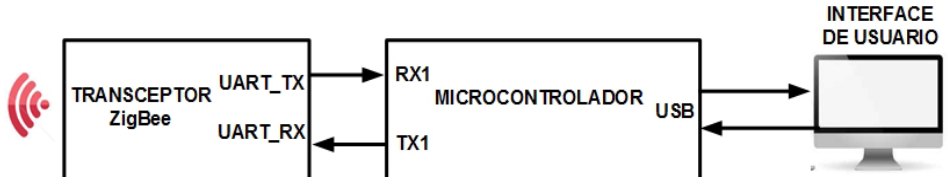

Figura 7 Diagrama de bloques del módulo supervisor.

En este módulo también se usó el transceptor XBee-PRO (S2), el cual se configuró como coordinador para comunicarse con el puerto EUSART del

microcontrolador a una velocidad de 9.6 Kbps. Se utilizó un PIC18F4550 porque cuenta con los siguientes recursos, suficientes para la función del módulo supervisor: CPU de 8 bits, memoria de programa flash de 32 kBytes, memoria RAM de 2,048 Bytes, cuatro puertos paralelo, puerto serie EUSART, puerto USB, cuatro temporizadores y puerto serie síncrono (Master Synchronous Serial Port-MSSP). El puerto EUSART del PIC18F4550 se conectó al puerto UART del XBee-PRO (S2). Las terminales RX1 y TX1 del EUSART se conectaron, respectivamente, a las terminales UART_TX y UART_RX del UART. El puerto USB del microcontrolador de este módulo se conectó al puerto USB de la computadora donde reside la interface de usuario.

La programación que se ejecuta en el PIC18F4550 realiza las siguientes tareas: inicializa el puerto EUSART, inicializa el puerto USB, inicializa el temporizador 1 (para generar el baud rate del EUSART) y a continuación entra a un ciclo donde espera, por el puerto USB, la orden de detección de WiFi enviada por la interface de usuario y transmitirla a cada módulo de detección. Finalmente, espera la respuesta de la orden en el puerto EUSART para entregarla a la interface de usuario. La información contenida en la respuesta es el identificador, nombre y nivel de la señal del punto de acceso y el número de serie del transceptor ZigBee del módulo de detección. En la figura 8 se indica el diagrama de flujo usado realizar la programación del PIC18F4550 la cual se implantó usando lenguaje mikroC PRO FOR PIC.

La interface de usuario

La interface de usuario se realizó en lenguaje Visual C++. La interface solicita cada 30 segundos al módulo supervisor enviar la orden de detección a cada módulo. Este periodo de tiempo es configurable. A continuación, espera que los módulos de detección transmitan el nombre de las redes WiFi detectadas por su correspondiente circuito ESP8266. La interface realiza adicionalmente las siguientes tareas: permite al usuario almacenar en un archivo el nombre de los puntos de acceso autorizados, muestra en pantalla el nombre los puntos de acceso detectados no autorizados, el identificador del módulo que la detectó y la

fecha y hora de detección, y registra además esta información histórica en un archivo de texto. El propósito de este archivo es que su contenido pueda ser usado por herramientas de monitoreo y auditoria del centro de datos. En la figura 9 se muestra la ventana principal de la interface de usuario donde indica la información de redes detectadas no autorizadas.

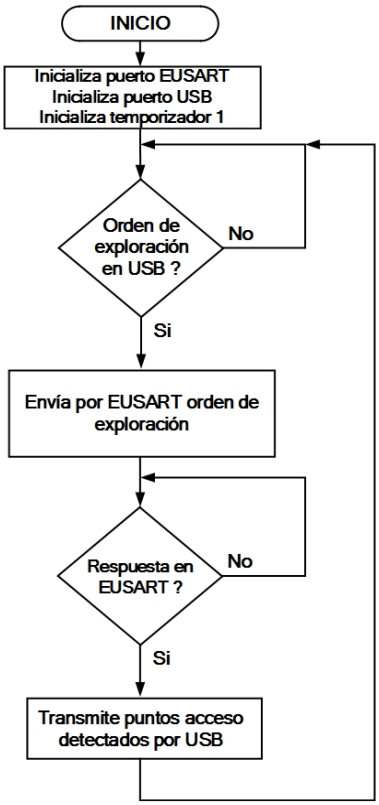

Figura 8 Diagrama de flujo de la programación del módulo supervisor.

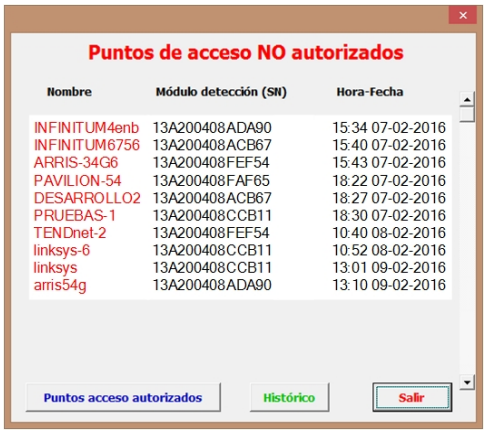

Figura 9 Interface de usuario del sistema.

3. Resultados

La elección del circuito ESP8266, permitió la construcción de un sistema sencillo, compacto y fácil de instalar. El centro de datos donde se instaló y probó el sistema está dividido en zonas llamadas bunkers. Los cinco módulos de detección WiFi se ubicaron en diferentes puntos de un bunker y realizaron dos conjuntos de pruebas: uno para medir el alcance del circuito ESP8266 y otro para medir el alcance de los transceptores ZigBee. En el primer conjunto de pruebas se instalaron diez routers WiFi adicionales a los ya existentes en el bunker. Estos routers no se registraron como autorizados en la interface de usuario y se ubicaron a diferentes distancias de los módulos de detección. El resultado obtenido fue que cada módulo detectó los puntos de acceso que estuvieron a distancia menor o igual a 50 metros de él. Los diez puntos de acceso no autorizados se mostraron en la interface de usuario. Algunos puntos de acceso fueron detectados por uno o varios módulos y otros puntos por otros módulos. Esto se comprobó conectando el puerto USB de una computadora portátil al puerto UART0 del circuito ESP8266 de cada módulo de detección (figura 10), para enviarle por medio del programa hyperterminal, el comando AT+CWLAP para determinar los puntos de acceso que detecta cada módulo. En la Fig. 10 se muestra en la ventana de hyperterminal el resultado del comando AT+CWLAP entregado por el circuito ESP8266 de dos módulos de detección. Puede notarse que cada módulo detecta puntos de acceso que están a su alcance y la información de cada punto de acceso (identificador, nombre y nivel de la señal). El alcance de 50 metros se determinó usando está conexión y moviendo los módulos de detección con respecto al router del punto de acceso. Para el bunker donde se hicieron las pruebas, son necesarios al menos cinco módulos para cubrir el área del bunker (500 m^2) y detectar todos puntos de acceso. En lo que respecta a la distancia entre los módulos de detección y el módulo supervisor, el resultado del segundo conjunto de pruebas consistió en variar la distancia de un módulo de detección respecto a la oficina de control y monitoreo. El resultado obtenido fue que el alcance del módulo de detección es de 95 metros aproximadamente con línea de vista. Esta distancia es un poco mayor a los 75 metros solicitados en el diseño del sistema.

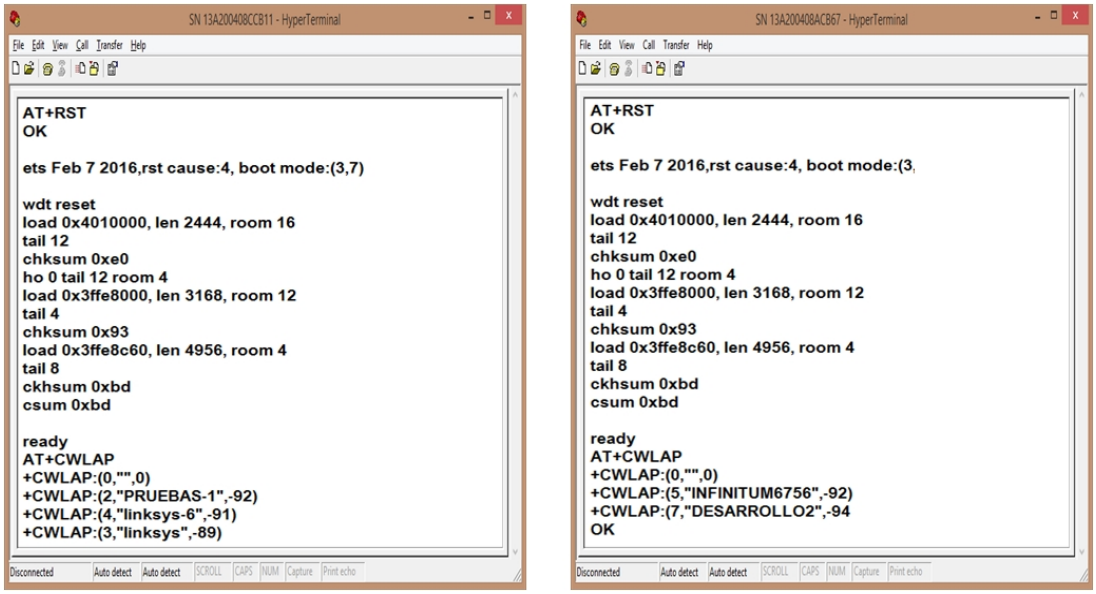

Figura 10 Conexión al circuito ESP8266 de dos módulos de detección.

4. Discusión

A pesar de que la función del sistema construido es sencilla, fue desarrollado para satisfacer una necesidad real, destacando que el sistema debe ser confiable. Es un sistema que está en operación, no es un prototipo de laboratorio y puede servir para mantener y crecer la relación de investigación con la industria. El diseño del sistema se realizó considerando también su escalabilidad. Esto es, se pueden adicionar funciones al trabajo desarrollado sin modificar el hardware de los módulos. Por ejemplo, la interface de usuario puede determinar y graficar la ubicación aproximada de un hotspot por triangulación, sabiendo donde están localizados los módulos que han detectado la red WiFi. Si la distancia entre la oficina de control y monitoreo y el bunker más lejano es mayor a 95 metros basta con adicionar al menos un módulo de detección ya que el transceptor ZigBee de estos módulos está configurado como router siendo parte de una red de malla y repitiendo tramas enviadas por otros transceptores. En el trabajo desarrollado solo se usó una función del circuito ESP8266 y quedan aún por aun las restantes, pero si no se utilizara este circuito en el diseño, el sistema resultante sería más grande y complejo. Es importante considerar el alcance de cada módulo de detección, ya que esto indicará la cantidad de módulos necesarios para cubrir el área de trabajo.

5. Conclusiones

Se obtuvo como resultado un sistema que detecta puntos de acceso ubicados a una distancia máxima de 50 metros y transmite su identificador, nombre y nivel de señal de RF, por medio de un transceptor ZigBee a una interface de usuario ubicada a una distancia máxima de 95 metros. Una mejora al sistema construido es eliminar el microcontrolador del módulo de detección y usar la CPU del circuito ESP8266. Esto implica usar el kit de desarrollo del circuito ESP8266 para programar la CPU e implantar una aplicación como sería un servidor web. Con esto, el módulo de detección podría conectarse a la interface de usuario ubicada en cualquier punto de la Internet. O bien, otra mejora sería que el microcontrolador de los módulos de detección envíe la información de puntos de acceso a través de la Internet usando el circuito ESP8266 configurado como punto de acceso. Independientemente de las mejoras que sea necesario realizar al sistema, todas indicarán que lo único a modificar será la programación del microcontrolador y/o del circuito ESP8266, lo cual es relativamente sencillo aun sin conocer a detalle el ESP8266, basta que se tenga experiencia en el uso de los conocidos módulos Bluetooth HC-06 y HC-05 usados en muchos sistemas de comunicación cuya configuración es similar al ESP8266. Ambas tecnologías de comunicación son inalámbricas pero una ventaja del módulo ESP8266 es que contiene la pila de protocolos TCP/IP que permite realizar sistemas de control y monitoreo con mayor alcance y ancho de banda accediendo a redes WiFi las cuales pueden encontrarse en muchos lugares de trabajo. Otro trabajo a futuro es usar el circuito ESP8266 con una antena externa lo cual proporcionará mayor alcance a los módulos de detección WiFi.

6. Bibliografía y Referencias

[1] L. K. Raju, R. Nair, "Secure Hotspot a novel approach to secure public Wi-Fi hotspot". 2015 International Conference on Control Communication & Computing India (ICCC). Trivandrum. 19-21 Nov. 2015. Pp. 642-646.

[2] D. Ding, A. J. Torres, F. G. Pikus, "High performance lithographic hotspot detection using hierarchically refined machine learning". 16th Asia and

South Pacific Design Automation Conference (ASP-DAC 2011). Yokohama. 25-28 Jan. 2011. Pp. 775-780.

[3] S. R. Talpur, S. Abdalla, T. Kechadi, "Towards middleware security framework for next generation data centers connectivity". 2015 Science and Information Conference (SAI). London. 28-30 July. 2015. Pp. 1277-1283.

[4] G. Vanderhulst, L. Trappeniers, "Public WiFi hotspots at your service". 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). Lugano. 19-23 March. 2012. Pp. 411-414.

[5] M. Seufert, T. Griepentrog, V. Burger, "A Simple WiFi Hotspot Model for Cities". IEEE Communications Letters. Volume 20. Issue 2. 2015. Pp. 384-387.

[6] M. A. Ertürk, L. Vollero, M. A. Aydin, "A framework for modeling and implementing QoS-aware load balancing solutions in WiFi hotspots". 2014 11th International Symposium on Wireless Communications Systems (ISWCS). Barcelona. 26-29 Aug. 2014. Pp. 33-38.

[7] J. Manweiler, N. Santhapuri, R. R. Choudhury, "Predicting length of stay at WiFi hotspots". 2013 Proceedings IEEE INFOCOM. Turin. 14-19 April 2013. Pp 3102-3110.

[8] J. Choi, K. G. Shin, "Out-of-band sensing with ZigBee for dynamic channel assignment in on-the-move hotspots". 2011 19th IEEE International Conference on Network Protocols. Vancouver. 17-20 Oct. 2011. Pp. 216-225.

[9] L. Qiu, H. Rui, A. Whinston,"When Cellular Capacity Meets WiFi Hotspots: A Smart Auction System for Mobile Data Offloading". 2015 48th Hawaii International Conference on System Sciences (HICSS). Kauai. 5-8 Jan. 2015. Pp. 4898-4907.

[10] N. K. Walia, P. Kalra, D. Mehrotra, "An IOT by information retrieval approach: Smart lights controlled using WiFi". 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence). Noida. 14-15 Jan. 20156. Pp. 708-712.

[11] Y. P. Zhang, T. Liu, Z. X. Yang, "Design of remote control plug". 2015 IEEE International Conference on Applied Superconductivity and Electromagnetic Devices (ASEMD). Shanghai. 20-23 Nov. 2015. Pp. 29-30.

[12] Q. M. Ashraf, M. I. Yusoff, A. A. Azman, "Energy monitoring prototype for Internet of Things: Preliminary results". 2015 IEEE 2nd World Forum on Milan Internet of Things (WF-IoT). Milan. 16-18 Dec. 2015. Pp. 1-5.

[13] ESP8266EX Datasheet, Version 4.3. Espressif Systems IOT Team. http://bbs.espressif.com/. 2015.

[14] E. Nugroho, A. Sahroni, "ZigBee and wifi network interface on Wireless Sensor Networks". 2014 Makassar International Conference on Electrical Engineering and Informatics (MICEEI). Makassar. 26-30 Nov. 2014. Pp. 54-58.

[15] J. H. Biddut, N. Islam, R. S. Sultana, "A new approach of ZigBee MAC layer design based on security enhancement". 2015 IEEE International Conference on Telecommunications and Photonics (ICTP). Dhaka. 26-28 Dec. 2015. Pp. 1-5.

[16] R. Akbar, E. Nugroho, "Wireless Sensor Networks for microclimate telemonitoring using ZigBee and WiFi". 2014 IEEE International Conference on Aerospace Electronics and Remote Sensing Technology (ICARES). Yogyakarta. 13-14 Nov. 2014. Pp. 200-204.

7. Autores

M.C. José Ignacio Vega Luna obtuvo su título de Maestría en Ciencias de la Computación en la UAM-Azcapotzalco. Sus áreas de especialización y trabajo son: aplicaciones de microcontroladores, UNIX y sistemas de alta disponibilidad. Desde 1985 es Profesor Titular de carrera en la UAM-Azcapotzalco.

Ing. Mario Alberto Lagos Acosta es Ingeniero en Electrónica por la UAM-Azcapotzalco. Sus áreas de especialización y trabajo son: aplicaciones con microprocesadores y microcontroladores. Actualmente es Profesor Asociado en la UAM-Azcapotzalco.

Ing. Gerardo Salgado es Ingeniero en Electrónica por la UAM-Azcapotzalco. Sus áreas de especialización y trabajo son: aplicaciones con microprocesadores y microcontroladores. Actualmente es Profesor Titular en la UAM-Azcapotzalco.

Ing. Víctor Noé Tapia Vargas es Ingeniero en Electrónica por la UAM-Azcapotzalco, cuenta con el 100% de créditos de la Maestría en Ciencias de la Computación en la UAM-Azcapotzalco. Sus áreas de especialización y trabajo son: aplicaciones con microprocesadores, microcontroladores y robótica. Actualmente es Profesor Titular en la UAM-Azcapotzalco.

M.C. Francisco Javier Sánchez Rangel. Sus áreas de especialización y trabajo son: aplicaciones con microprocesadores, microcontroladores y robótica. Actualmente es Profesor Titular en la UAM-Azcapotzalco.