Sistema de acceso a áreas restringidas con detección de intrusos

José Ignacio Vega Luna

Universidad Autónoma Metropolitana-Azcapotzalco, Av. San pablo 180, Col. Reynosa Tamaulipas, México, D.F., Teléfono: 55-53189552

vlji@correo.azc.uam.mx

Mario Alberto Lagos Acosta

Universidad Autónoma Metropolitana-Azcapotzalco, Av. San pablo 180, Col. Reynosa Tamaulipas, México, D.F., Teléfono: 55-53189552

vlji@correo.azc.uam.mx

Gerardo Salgado, Víctor Noé Tapia Vargas

Universidad Autónoma Metropolitana-Azcapotzalco, Av. San pablo 180, Col. Reynosa Tamaulipas, México, D.F., Teléfono: 55-53189552

vlji@correo.azc.uam.mx

Resumen

En este trabajo se presenta el desarrollo e implantación de un sistema electrónico usado en el acceso a áreas importantes y reservadas en un centro de datos. El usuario debe proporcionar, por medio de un botón o switch, el código Morse de cada uno de los números de una clave pre-establecida de 4 dígitos para que el sistema le permita el acceso. Cada vez que se proporciona una clave, válida o inválida, el sistema envía de forma inalámbrica una notificación a una computadora personal, ubicada en una oficina central de monitoreo.

Palabra(s) Clave(s): centro de datos, código Morse, inalámbrica.

1. Introducción

Un centro de procesamiento de datos (CPD), también llamado simplemente centro de datos o data center por su equivalente en inglés, es una instalación que concentra recursos o equipos necesarios para el procesamiento y almacenamiento de información de empresas e instituciones, así como equipos de telecomunicaciones para acceder tanto local como remotamente dicha información. Con la rápida evolución de la Internet y la necesidad de estar conectados en todo momento, las empresas se ven obligadas a contar con un alto nivel de confiabilidad y seguridad en el acceso a su información, ubicando sus equipos de cómputo, telecomunicaciones y de almacenamiento en un CPD para garantizar la continuidad de servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras [1]. Es vital que el CPD cuente con mecanismos seguros y eficientes para la protección física del equipo, ya que contienen información con datos críticos y necesarios para las operaciones diarias de la empresa a fin de evitar poner en riesgo la productividad y el negocio mismo. Hoy en día las compañías, sobre todo las medianas y grandes, cuentan con su propio CPD o usan los servicios que ofrecen empresas que se dedican a la instalación, mantenimiento y operación de centros de datos, lo cual les permite centrarse en el desarrollo de su propio negocio y olvidar las complejidades tecnológicas de un CPD, sin necesidad de realizar una elevada inversión en equipamiento e instalaciones. La seguridad en un centro de datos, tanto de equipos, instalaciones e información, es un aspecto tan importante como la operación del mismo. Periódicamente los centros de datos son auditados por organismos y empresas externas, para poder estar certificados y ofrecer servicios garantizados a sus clientes. Un punto importante que consideran estas auditorías es la vulnerabilidad de los sistemas de acceso [2]. En los centros de datos se usa una gran variedad de dispositivos para acceder a las instalaciones incluyendo: cerraduras electromagnéticas, torniquetes, videocámaras, detectores de movimiento, tarjetas de identificación, sistemas biométricos y de teclados para introducir una clave de acceso. Se usa uno o varios de estos dispositivos dependiendo de los siguientes

factores: tipo de área a proteger, cantidad y tipo de usuarios que pueden acceder al área, equipo alojado y confiabilidad del mecanismo de seguridad. Comúnmente, sólo una cantidad pequeña bien identificada de personal del centro de datos puede acceder a las áreas críticas, privilegiadas e importantes del mismo, donde el mecanismo de acceso es con dispositivos biométricos y/o con claves numéricas o alfanuméricas [3]. Este tipo de claves son suministradas por el usuario mediante un teclado de 10 botones similar al de los teléfonos, que aún son un método confiable y complementario de acceso. Cada tecla es push-button normalmente abierto. Estos sistemas son bastante seguros, ya que es muy difícil que un intruso determine la clave correcta. Sin embargo, con el tiempo y el uso, estos sistemas son más vulnerables que útiles, puesto que un intruso puede determinar la clave observando el desgaste por uso de las teclas.

En los centros de datos todos los sistemas de acceso, seguridad y monitoreo de variables, como humedad y temperatura, son controlados y operados remotamente desde una oficina central [4]. La comunicación de estos sistemas con la oficina central utiliza tecnologías alámbricas o inalámbricas. Cuando es necesario instalar un nuevo equipo de acceso y monitoreo, el punto de partida a considerar, es que no debe interrumpirse la operación actual y tanto como se pueda, no cambiar la infraestructura existente. Es decir, si se instala un nuevo equipo o mecanismo de acceso es altamente recomendable que no se modifique o adicione cableado al ya existente, puesto que el cableado de datos de los equipos alojados en el centro de datos cumple con estándares de instalación y operación altamente calificados. Por esta razón fundamental, es indispensable usar una tecnología de comunicación inalámbrica con la oficina central.

WiFi es la tecnología de comunicación inalámbrica con más tiempo en el mercado y que se usa para transmisión de grandes cantidades de datos y de alta velocidad. Existen alternativamente las tecnologías Bluetooth y ZigBee. Los dispositivos y electrónica de WiFi son de mucho mayor costo y consumo de energía que las dos últimas. WiFi se usa principalmente en las aplicaciones multimedia y acceso a la nube y no tanto en la transmisión de información de sensores de variables. La tecnología Bluetooth se usa en

la comunicación entre un par de periféricos o entre una computadora y un periférico previamente vinculados y a corta distancia. La tecnología ZigBee es la más aceptada actualmente para la comunicación con sistemas remotos de control y monitoreo. En la Tabla 1 se resumen las principales diferencias entre las tres tecnologías anteriores.

	ZigBee®	**Bluetooth**	**WiFi™**
Estándar usado	802.15.4	802.15.1	802.11
Aplicación	Monitoreo y control	Periféricos, monitoreo, control, video.	Web, Email, Video
Duración de la batería (días)	100 - 100+	1 – 7	0.5 - 5
Tamaño de la red (nodos)	65,535	7	32
Ancho de banda (Kbps)	250	24,000	300,000
Rango (metros)	100	30	20
Arquitectura de red	Malla	Estrella	Estrella
Optimizado para	Confiabilidad, bajo consumo de energía, bajo costo y crecimiento	Bajo costo y conveniencia	Velocidad y cantidad de información

Tabla 1. Principales características de ZigBee, Bluetooth y WiFi.

La tecnología ZigBee representa un conjunto de protocolos de alto nivel de comunicación inalámbrica de bajo consumo de corriente que se basa en el estándar de redes inalámbricas de área personal (WPAN) IEEE 802.15.4 [5]. Su objetivo son las aplicaciones que requieren comunicaciones seguras de baja velocidad de transmisión y maximización de la vida útil de baterías. ZigBee se ha desarrollado para satisfacer la creciente demanda de capacidad de red inalámbrica entre varios dispositivos de baja

potencia [6]. Se está utilizando en la automatización de procesos, con pequeños transmisores en cada dispositivo, lo que permite la comunicación entre dispositivos a una computadora central. ZigBee es ideal para configurar redes domóticas ya que fue diseñado específicamente para reemplazar la proliferación de sensores y actuadores individuales, presentando las siguientes tres características principales: bajo consumo de energía, se puede usar fácilmente para realizar redes de comunicación de datos con una topología de malla, es de fácil integración con otros dispositivos (se pueden fabricar nodos ZigBee con muy poca electrónica) y es más fácil de usar que otros dispositivos de transmisión inalámbrica como WiFi. ZigBee puede transmitir a una velocidad máxima de 250 Kbps., suficiente para la aplicación aquí diseñada [7].

En este trabajo se presenta el desarrollo e implantación de un sistema electrónico usado en el acceso de áreas importantes y reservadas en un centro de datos, donde el usuario debe proporcionar el código Morse de cada uno de los números de una clave pre-establecida de 4 dígitos.

El Código Morse es un medio de comunicación basado en la transmisión y recepción de mensajes empleando sonidos o luces parpadeantes y un alfabeto alfanumérico compuesto por dos símbolos: puntos y guiones. Debe su nombre a su creador, el pintor y físico estadounidense Samuel F.B. Morse (1791-1872), quien lo desarrolló en 1830 para servir como un medio de comunicación en la telegrafía eléctrica. Este código surgido en el siglo XIX, continúa usándose hoy en día fundamentalmente en ambientes donde las condiciones atmosféricas adversas no permiten el empleo de otros medios más desarrollados como, por ejemplo, la transmisión de la voz [8]. Aun cuando en una transmisión inalámbrica por radiofrecuencia realizada solamente con código Morse y bajo interferencias producidas por tormentas eléctricas, los sonidos de los puntos y los guiones serán siempre reconocibles para el oído humano aunque se escuchen mezclados con el ruido que produce en esos casos la estática atmosférica. El sistema Morse representa las letras del alfabeto, los números y otros signos mediante una combinación de puntos, guiones y espacios. Cada punto representa una unidad, cuyo

tiempo de duración es de aproximadamente 40 ms, y cada guion tres unidades. El espacio entre las letras es de 3 puntos y 5 puntos entre palabras.

2. Desarrollo

Para la implantación del sistema se siguió una metodología que consistió en dividir el trabajo en seis módulos funcionales: un microcontrolador, un módulo de identificación de usuario, un módulo de salida, un transceptor inalámbrico local, un transceptor inalámbrico remoto y una interface de usuario en una computadora personal. La Fig. 1 muestra el diagrama de bloques del sistema completo. A continuación se explicará el funcionamiento de cada módulo y posteriormente la programación del microcontrolador quién es el módulo principal del sistema.

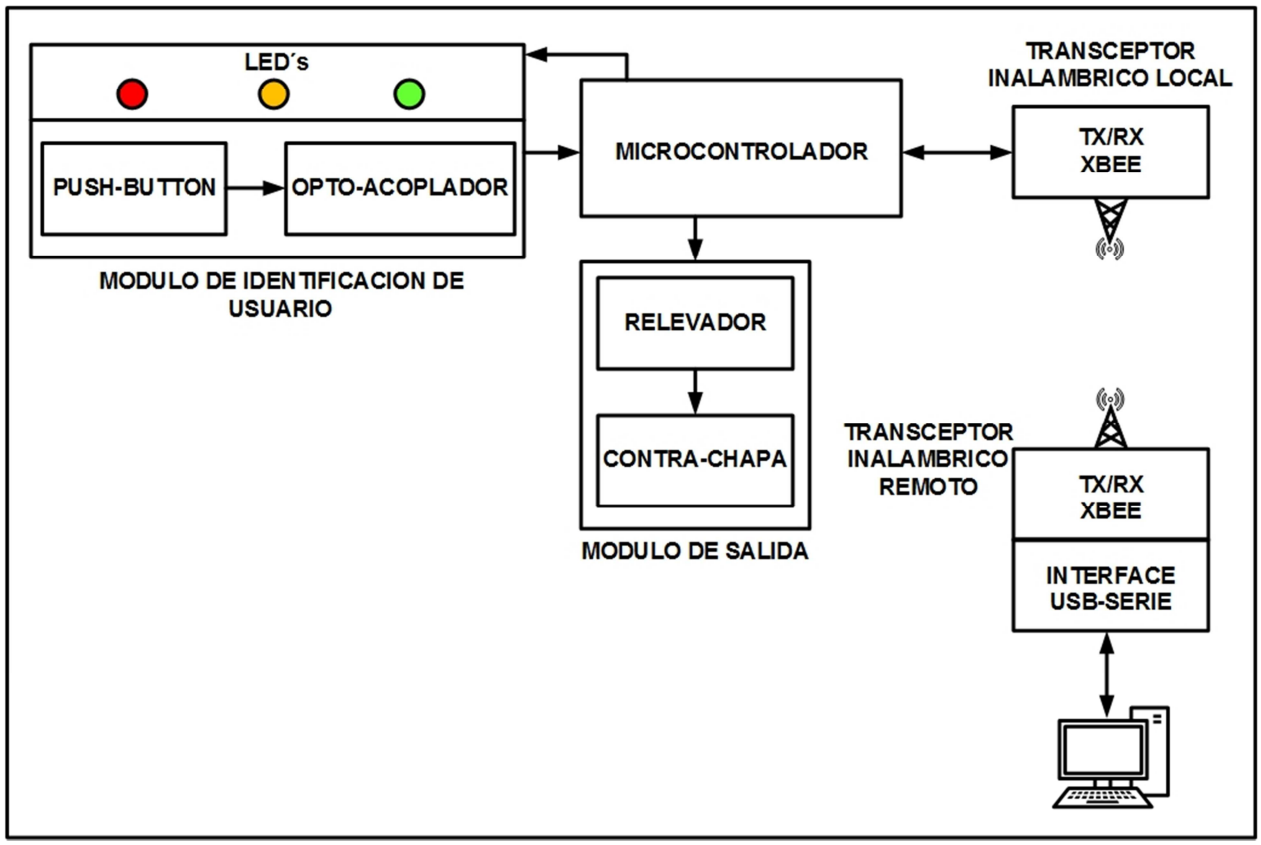

Fig. 1. Diagrama de bloques del sistema completo.

El microcontrolador

Se utilizó un microcontrolador PIC 16F887 ya que cuenta con los siguientes recursos principales necesarios y suficientes para la realización de este trabajo: CPU de 8 bits, memoria de programa FLASH de 8 KB, memoria RAM de 368 bytes, memoria EEPROM de 256 bytes, puerto serie EUSART, cuatro puertos paralelo y tres temporizadores [9]. En la memoria EEPROM del microcontrolador se almacena la clave de 4 números para activar una contra-chapa eléctrica y permitir el acceso al área bajo resguardo. Esta clave es establecida por el administrador del sistema desde una interface de usuario en una computadora personal, localizada en una oficina central de control y monitoreo, la cual es enviada al microcontrolador inalámbricamente usando transceptores ZigBee. La persona que necesite ingresar al área bajo resguardo debe suministrar el código Morse de cada número de la clave. Cada vez que se ingrese una clave correcta o incorrecta, el microcontrolador envía a la interface de usuario una notificación que se registra en un archivo de la computadora personal, indicándole el evento al usuario. Se seleccionó el código Morse porque es relativamente sencillo que un usuario pueda introducirlo al sistema, solo basta con usar un botón y que el usuario aprenda el código de los cuatro números de la clave. El código de cada número es una secuencia de uno hasta cuatro puntos y guiones, a los cuales se les denominará signos de aquí en adelante. Cada vez que se presione o cierre el botón ubicado en el módulo de entrada, potencialmente el usuario estará suministrado un signo. Si la persona presiona el botón durante un intervalo de 50 a 200 ms, se considera un punto, si lo presiona durante un tiempo de 200 a 1500 ms, se considera un guion. Menor a 50 ms y mayor a 1500 ms, se considera un signo inválido. Al proporcionar el código de un número, el usuario tiene máximo 5 segundos para proporcionar el siguiente. Si excede este tiempo, el sistema regresa a su estado inicial. Estos tiempos pueden modificarse y ser ajustados en la programación del microcontrolador, ya que son generados por el Timer 0 del microcontrolador

El módulo de identificación de usuario

Este módulo consiste de un switch del tipo push-button normalmente abierto conectado a la entrada de un opto-aislador 4N28 [10]. La etapa de salida del opto-acoplador se conectó a una línea de entrada del Puerto A del microcontrolador. Cuenta también con tres leds: un rojo, un ámbar y un verde. Inicialmente, cuando el usuario no está suministrando una clave, solo se encontrará prendido el led rojo que indica que la contra-chapa se encuentra cerrada. Al iniciar el suministro de una clave, se apaga el led rojo y se enciende el ámbar. Cuando se ha suministrado la clave correcta se apaga el led ámbar, se enciende el led verde y se activa la contrachapa durante 10 segundos. Si el usuario suministra una clave errónea se apaga el led ámbar y se enciende el rojo, regresando el sistema a su estado inicial. Como ya se indicó, al presionar el switch dentro de un rango de tiempo indicará un punto, un guion o un signo inválido. Un grupo de signos, de uno a cuatro, corresponde al código Morse de un número.

El módulo de salida

Este módulo consiste de un relevador conectado a una línea de salida del Puerto A del microcontrolador, y de una contra-chapa eléctrica conectada a la salida del relevador. Cuando el usuario ha suministrado la clave correcta, el microcontrolador activa la contra-chapa durante 10 segundos. En la Fig. 2 se muestra la contra-chapa eléctrica usada en este módulo.

Fig. 2. Contra-chapa magnética.

El transceptor inalámbrico local

En este módulo del sistema se utilizó un circuito XBee Serie 2, como el mostrado en la Fig. 3, conectado al puerto serie del microcontrolador. Su función es enviar una notificación a la interface de usuario de la computadora personal cada vez que el usuario suministre una clave, valida o invalida, así como recibir desde la interface de usuario de la computadora una clave, que el administrador establezca, y almacenarla en la memoria EEPROM del microcontrolador. El circuito XBee Serie 2 es un dispositivo compatible con el protocolo ZigBee 802.15.2. Se usa la tecnología ZigBee en este trabajo dado que permite ubicar la computadora a una distancia hasta de 90 metros del sistema de acceso, sin necesidad de instalar cableado adicional ni modificar la infraestructura existente, dado que por lo general no es factible realizar o en ocasiones imposible llevar a cabo en un centro de datos [11].

El circuito XBee Serie 2 cuenta con antena integrada, que puede trasmitir información inalámbrica a una distancia máxima de 300 pies en interiores, trabaja a una frecuencia de 2.4 GHz. y usa los protocolos de red y ruteo del estándar ZigBee. Se alimenta con una fuente de voltaje de 3.3 V y puede configurarse para trabajar en una red de malla, lo que le permite extender su rango de transmisión haciendo uso de ruteadores. El circuito XBee Serie 2 se puede configurar en uno de los siguientes dos modos de operación: modo transparente o modo API. En el modo transparente o AT, el circuito XBee funciona como una línea serie simple, de manera que la información que recibe por su entrada serie (en este caso conectada a la salida de datos serie del USART del microcontrolador) la transmite por la antena y de manera similar, la información que recibe por medio de la antena se entrega por medio de la línea de salida serie. En el modo API (Application Programming Interface), el circuito XBee recibe y transmite comandos para realizar diversas actividades. Es en este modo en el que realmente el circuito XBee usa el protocolo ZigBee, aprovechando todas las funciones del protocolo, permitiendo al diseñador implantar redes inalámbricas. Independientemente del modo

transparente y modo API, los circuitos XBee pueden configurarse para funcionar como nodos coordinadores o nodos ruteadores.

Fig. 3. Circuito Xbee Serie2.

Los nodos coordinadores reportan a los nodos ruteadores. Los nodos coordinan la actividad al interior de la red, enviando paquetes de un nodo a otro, actuando, como lo indica el nombre, como ruteadores o intermediarios de la red. Para configurar un circuito XBee Serie 2 en modo transparente o API y para operar como coordinador o ruteador, es necesario cargar o cambiarle el firmware correspondiente [5].

El circuito XBee de este módulo se configuró en modo transparente y coordinador, para lo cual se utilizó el software X CTU proporcionado por el fabricante del circuito. Este software permite conectar el circuito XBee, vía una terminal serie, a una computadora personal y enviarles una serie de comandos para inicializarlos [6]. Para obtener el voltaje de 3.3 V que alimenta al circuito XBee Serie 2, se usa una tarjeta XBee Shield, como la indicada en la Fig. 4., que se alimenta con la misma fuente del microcontrolador, permitiendo una conexión sencilla y rápida del circuito XBee Serie 2. Para poder transmitir y recibir paquetes, la salida DOUT del circuito XBee Serie 2 se conectó a la entrada RX del USART del microcontrolador, y la entrada DIN del circuito XBee Serie 2 se conectó a la salida TX USART del microcontrolador.

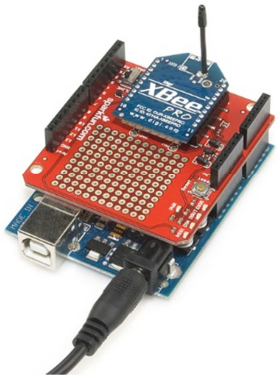

Fig. 4. Tarjeta Xbee Shield.

El transceptor inalámbrico remoto

Este módulo se compone de un dispositivo ZigBee Serie2, como el mostrado en la Fig.5, configurado en modo transparente y como ruteador. Aunque en este trabajo la computadora personal se comunica con un solo sistema de acceso, como el aquí presentado, en el futuro se instalarán sistemas de este tipo en otras áreas del centro de datos, los cuales se comunicaran también con este módulo ruteador, conformando de esta manera una red de circuitos XBee conectada a la computadora. Para conectar el circuito XBee Serie 2 al puerto USB de la computadora y obtener su voltaje de alimentación de 3.3 V, se usó una tarjeta XBee Explorer USB. Esta tarjeta contiene un circuito convertidor USB-Serie FT231X que le permite conectarse directamente a un puerto USB. El FT231X sirve como interface entre el XBee Serie 2 y el puerto USB de la computadora. Con esto se obtiene una base inalámbrica sin necesidad de construir una placa de circuito impreso para el XBee Serie 2, ya que únicamente éste se inserta en un conector específico de la tarjeta XBee Explorer USB.

Fig. 5. Circuito Xbee Serie2 en la tarjeta Explorer USB.

La interface de usuario en la computadora

La computadora personal está localizada en la oficina del administrador o responsable del monitoreo y control del centro de datos. Esta interface se realizó usando leguaje de programación Visual C. La interface tiene tres funciones básicas: la primera, recibir las notificaciones de clave correcta o errónea enviadas por el microcontrolador y registrarlas de manera histórica en un archivo con formato Excel. Este archivo permite al administrador visualizar las notificaciones y entregar un informe del registro a la autoridad certificadora o auditora del centro de datos que así lo requiera. La segunda función es mostrar visualmente al administrador, que se ha suministrado una clave correcta indicando por el led verde o en rojo su es incorrecta. La tercera función es permitir al administrador establecer o cambiar una clave para el sistema de acceso.

La programación del microcontrolador

La programación se realizó usando el leguaje MikroC que permite configurar al microcontrolador usando lenguaje C. Las tareas principales de esta programación son: establecer el ambiente inicial de trabajo, configurar los puertos paralelo y serie, los temporizadores y las variables. Una parte importante de la programación es el uso de los temporizadores, puesto que es base para determinar si se ha suministrado un

código Morse válido. A continuación, el programa enciende el led rojo, apaga los leds ámbar y verde y desactiva la contra-chapa. Posteriormente, entra en un ciclo en el cual el microcontrolador espera que se active el push-button. Al salir de este ciclo se apaga el led rojo y se enciende el amarillo para indicar al usuario que el sistema se encuentra solicitando una clave de acceso, arrancando al mismo tiempo un temporizador de 50 ms que marca el tiempo mínimo de un signo Morse.

3. Resultados

A pesar de que es complicado que una persona memorice la clave Morse de los 4 dígitos y que la introduzca en el tiempo requerido, se realizó un conjunto significativo de pruebas con 50 usuarios para validar el sistema, cuyos resultados y conclusiones se indican a continuación. Se establecieron desde la interface de usuario distintas claves de acceso, la cuales fueron proporcionadas correcta e incorrectamente por un grupo de 50 usuarios. Estas pruebas sirvieron para el ajuste de los temporizadores que el programa del microcontrolador usa tanto para eliminar los rebotes del push-button, como para establecer el tiempo máximo que debe trascurrir entre cada signo y entre cada código Morse suministrado por el usuario. Difícilmente el valor de estos temporizadores tendrá que cambiarse en el futuro, ya que la mayoría de usuarios que participaron en estas pruebas tuvieron características diferentes al usar el push-button. En caso de tener que modificar el valor de los temporizadores, puede realizarse muy fácilmente al inicio del programa principal del microcontrolador.

Con respecto a las pruebas de alcance realizadas en la transmisión inalámbrica, la distancia máxima que se logró fue de 80 metros, de manera tal que el sistema de acceso diseñado puede situarse hasta esta distancia de la oficina de monitoreo y control. En el centro de datos en el cual se trabajó, dicha oficina está situada a una distancia de 30 metros de recinto donde se instaló el sistema de acceso aquí diseñado y a 70 metros del recinto más lejano que aloja equipo de cómputo y en el que posiblemente necesite instalarse un sistema de acceso.

4. Discusión

Como puede observarse en el trabajo aquí presentado, el código Morse no se usa para la transmisión inalámbrica de textos, se aplicó en la codificación, sencilla, segura y flexible, de una clave de acceso. Aunque es complicado el código Morse, el sistema se construyó tal como fue solicitado para ser instalado en un centro de datos, y se puede utilizar en cualquier tipo de instalación donde se requiera un sistema de acceso compacto y fácil de operar y de configurar. Es importante indicar que, aunque el diseño del sistema dio como resultado una circuitería sencilla, lo más significativo fue que se realizó un prototipo que actualmente se encuentra en operación, con el cual se puede iniciar una relación con una empresa que necesita confiar en diseños llevados a cabo por Universidades y que a futuro puede fomentar la continuación de la relación con el desarrollo de distintos sistemas de control y monitoreo de variables.

5. Conclusiones

Si es necesario extender el alcance de la transmisión entre la oficina de monitoreo y control y el sistema de acceso, deberán diseñarse módulos repetidores de la señal y tramas ZigBee. Estos módulos son relativamente sencillos, ya que solamente están compuestos de circuitos XBee Serie 2 como los usados en este trabajo, con su correspondiente fuente de alimentación, configurados como ruteadores, conformando así una red de malla ZigBee. No tendrá que modificarse la configuración actual del sistema de acceso aun en el caso de adicionar otro sistema de acceso para otro recinto del centro de datos, ya que cada circuito XBee envía su identificador único a la computadora personal, lo cual puede ser usado para identificar la ubicación del circuito XBee con el cual se está comunicando la interface de usuario.

Finalmente, una actualización y trabajo futuro que podría ser realizado en este sistema es conectar el transceptor inalámbrico remoto, que actualmente se conecta a un puerto USB de la computadora, a un gateway ZigBee, lo cual le permitiría conectarlo a una red

Ethernet y ubicar la computadora personal fuera del centro de datos e inclusive en cualquier parte de la Internet.

6. Referencias

[1] A multi-tiered model approach for monitoring and control of data center entrance and exit scenarios. 4th International Conference on Interaction Sciences (ICIS). Busan. 16-18 Aug. 2011.

[2] Next Generation Data Center design under Smart Grid. Fourth International Conference on Ubiquitous and Future Networks (ICUFN). Phuket. 4-6 July 2012.

[3] Data center design of optimal reliable systems. IEEE International Conference on Quality and Reliability (ICQR). Bangkok. 14-17 Sept. 2011.

[4] Wireless sensor network for data-center environmental monitoring. 2011 Fifth International Conference on Sensing Technology (ICST). Palmerston North. Nov. 28-Dec. 1 2011.

[5] Multi-sensors Data Fusion Based on Arduino Board and XBee Module Technology. International Symposium on Computer, Consumer and Control (IS3C). Taichung. 10-12 June 2014.

[6] Wireless data acquisition system based on XBee modules for remote sensing and monitoring ions concentration in aqueous solutions. IEEE 9th Ibero-American Congress on Sensors (IBERSENSOR). Bogota. 15-18 Oct. 2014.

[7] Development of a PIC-based wireless sensor node utilizing XBee technology. The 2nd IEEE International Conference on Information Management and Engineering (ICIME). Chengdu. 16-18 April 2010.

[8] Implementation of Morse decoder on the TMS320C6748 DSP development kit. 2014 6th European Embedded Design in Education and Research Conference (EDERC). Milano. 11-12 Sept. 2014.

[9] PIC16F887 Data Sheet. Microchip Technology Inc. En línea en: http://www.microchip.com. Acceso: 2015.

[10] 4N25D Data Sheet. Motorola, Inc. En línea en: http://Design–NET.com. Acceso: 2015.

[11] ZigBee RF Modules Documentation. Digi International Inc. En línea en: http://www.digi.com. Acceso: 2015.

7. Autores

M. en 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.