



PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

**DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO SOBRE
PROTOCOLO ZIGBEE PARA LAS OFICINAS DE UN EDIFICIO
EDUCATIVO**

Tesis para optar el Título de Ingeniero Electrónico, que presenta el bachiller:

José Enrique Maqueira Valencia

ASESOR: Ángelo Velarde

Lima, agosto del 2013

RESUMEN

Los sistemas de control de acceso se usan para permitir o denegar el ingreso de ciertas personas a un área específica en un determinado horario. Estos sistemas se usan ampliamente en hoteles, condominios y todo tipo de empresas, en los que dependiendo del usuario, se le otorga acceso a más o menos áreas. Actualmente, tienen diversas aplicaciones como control de asistencia, control de rondas y exclusas de seguridad.

Los centros educativos también requieren cierto control del acceso a sus instalaciones, tanto al campus, como a áreas específicas donde personal docente o administrativo tienen acceso pero el alumnado no. Existen ciertas políticas de seguridad que cada unidad debe cumplir para garantizar el correcto resguardo de estas zonas. Un adecuado sistema de control de acceso puede facilitar la implementación de estas políticas y su eficiencia, así como proveer de funciones adicionales específicas para cada aplicación.

La propuesta a desarrollar plantea el uso de un sistema de control de acceso inalámbrico de bajo consumo de energía, que pueda ser integrado con otros sistemas para lograr una solución más completa mediante el intercambio de información, como la grabación de las personas al ingreso. Este sistema deberá tener un bajo costo y generará la posibilidad de llevar un registro de los ingresos y salidas y de conocer en qué zona del área restringida se encuentra cada ingresante.

FACULTAD DE
 CIENCIAS E
 INGENIERÍA

 PONTIFICIA
 UNIVERSIDAD
 CATÓLICA
 DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño de un Sistema de Control de Acceso sobre protocolo ZigBee para las Oficinas en un Edificio Educativo
 Área : Comunicaciones # 711
 Asesor : Ingeniero Ángelo Velarde
 Alumno : José Enrique Maqueira Valencia
 Código : 20030255.7.12
 Fecha : 28 de Mayo de 2009


Descripción y Objetivos

Los sistemas de control de acceso se usan para permitir o denegar el ingreso de ciertas personas a un área específica en un determinado horario. Estos sistemas se usan ampliamente en hoteles, condominios y todo tipo de empresas, en los que dependiendo del usuario, se le otorga acceso a más o menos áreas. Actualmente, tienen diversas aplicaciones como control de asistencia, control de rondas y exclusas de seguridad.

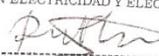
Los centros educativos también requieren cierto control del acceso a sus instalaciones, tanto al campus, como a áreas específicas donde personal docente o administrativo tienen acceso pero el alumnado no. Existen ciertas políticas de seguridad que cada unidad debe cumplir para garantizar el correcto resguardo de estas zonas. Un adecuado sistema de control de acceso puede facilitar la implementación de estas políticas y su eficiencia, así como proveer de funciones adicionales específicas para cada aplicación.

La propuesta a desarrollar plantea el uso de un sistema de control de acceso inalámbrico de bajo consumo de energía, que pueda ser integrado con otros sistemas para lograr una solución más completa mediante el intercambio de información, como la grabación de las personas al ingreso. Este sistema deberá tener un bajo costo y generará la posibilidad de llevar un registro de los ingresos y salidas y de conocer en qué zona del área restringida se encuentra cada ingresante.



MÁXIMO 100 PÁGINAS

 PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
 SECCIÓN ELECTRICIDAD Y ELECTRONICA


 Ing. ANDRÉS FLORES ESPINOZA
 Coordinador de la Especialidad de Ingeniería Electrónica

FACULTAD DE
CIENCIAS E
INGENIERÍA



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño de un Sistema de Control de Acceso sobre protocolo ZigBee para las Oficina de un Edificio Educativo

Índice

Introducción

1. Descripción de Sistemas de Control de Acceso y Definición de la Problemática
2. Tendencias actuales en Seguridad Electrónica y Control de Acceso
3. Análisis de Parámetros a tomar en cuenta en el Diseño del Sistema de Control de Acceso
4. Diseño del Sistema de Control de Acceso

Conclusiones

Recomendaciones

Bibliografía

Anexos

[Handwritten signature]
4

PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
SECCION ELECTRICIDAD Y ELECTRONICA

[Handwritten signature]
Ing. ANDRES FLORES ESPINOZA
Cordinador de la Especialidad de Ingenieria Electrónica

MÁXIMO 100 PÁGINAS

ÍNDICE

INTRODUCCIÓN.....	1
CAPÍTULO 1	2
ANÁLISIS DE LOS SISTEMAS DE SEGURIDAD ELECTRÓNICA	2
1.1 Edificios inteligentes	2
1.2 Seguridad a nivel electrónico.....	4
1.3 Sistemas de Seguridad en Edificios Educativos.....	4
1.4 Planteamiento del problema	5
CAPÍTULO 2	9
SISTEMAS DE SEGURIDAD Y CONTROL DE ACCESO EN LA ACTUALIDAD....	9
2.1 Edificios Inteligentes en la Actualidad.....	9
2.2 Seguridad Electrónica.....	10
2.2.1 Detección de Intrusión.....	10
2.2.2 Circuito Cerrado de Televisión	11
2.2.3 Detección y Alarma de Incendios	14
2.2.4 Control de Accesos	14
2.2.5 Comunicación.....	18
2.3 Síntesis de la investigación y planteamiento de la propuesta.....	21
CAPÍTULO 3	22
ANÁLISIS DE PARÁMETROS A TOMAR EN CUENTA EN EL DISEÑO DEL SISTEMA DE CONTROL DE ACCESO	22
3.1. Hipótesis de la investigación	22
3.1.1. Hipótesis principal	22
3.1.2. Hipótesis secundarias	22
3.2. Objetivos de la investigación	23
3.2.1. Objetivo general	23
3.2.2. Objetivos específicos.....	23

3.3.	Características requeridas del sistema.....	23
3.3.1.	Etapas de adaptación de protocolo Wiegand a UART	23
3.3.2.	Comunicación por Radiofrecuencia.....	25
3.3.3.	Adaptación de protocolo UART a RS-232	25
3.3.4.	Requerimientos de la PC o Servidor	26
3.4.	Esquema general de la Solución Planteada	26
CAPÍTULO 4	29
DISEÑO DEL SISTEMA DE CONTROL DE ACCESO	29
4.1	Justificación de la elección de Componentes y Estándares	29
4.1.1.	Elección del Protocolo de Control de Acceso de entrada.....	29
4.1.2.	Elección del módulo ZigBee	29
4.1.3.	Elección del Microcontrolador	31
4.1.4.	Elección de estándar para interfaz con PC	33
4.1.5.	Elección del MAX232	33
4.2	Esquema del Sistema de Control de Acceso en base a los dispositivos elegidos	34
4.3	Diseño de los circuitos que forman parte del Sistema de Control de Acceso	35
4.3.1	Diseño del circuito de un nodo remoto.....	35
4.3.2	Diseño del circuito del nodo principal	38
4.4	Lógica de comunicación de los Módulos XBee	40
4.4.1	Explicación de la lógica de funcionamiento	40
4.4.2	Configuración de los Módulos XBee.....	41
4.5	Pruebas	44
4.5.1.	Envío de datos por protocolo ZigBee.	45
4.5.2.	Generador de trama Wiegand	48
4.5.3.	Comunicación inalámbrica de la trama Wiegand decodificada.....	51
4.5.4.	Interfaz en el Servidor	53
4.6	Presupuesto	55
CONCLUSIONES	57
RECOMENDACIONES	59
FUENTES	60

LISTA DE FIGURAS

Fig. 1: Edificio Inteligente de Interbank ubicado en San Isidro	3
Fig. 2: Plano modificado del área objetivo.....	6
Fig. 3: Puertas (a) 1, (b) 2 y (c) 3 como señaladas en la Figura 2	7
Fig. 4: (a) Contactos Magnéticos (b) Sensor de movimiento tipo PIR	11
Fig. 5: Cámara Domo PTZ	12
Fig. 6: Detector Fotoeléctrico de Humo	14
Fig. 7: Ejemplos de (a) Lectoras de proximidad y de (b) Credenciales	16
Fig. 8: Composición de Trama en Protocolo Wiegand.....	24
Fig. 9: Cable para estándar RS-232 DB9	25
Fig. 10: Diagrama de Bloques del Funcionamiento del Sistema.....	27
Fig. 11: (a) Módulo XBee (b) Logo de ZigBee Alliance.....	30
Fig. 12: (a) Puerto RS-232 DB9 (b) Cable adaptador RS-232/USB de TrendNet33	35
Fig. 13: Esquema del Sistema de Control de Accesos	35
Fig. 14: Diagrama esquemático de un nodo remoto	37
Fig. 15: Imagen de un nodo remoto implementado.....	38
Fig. 16: Diagrama esquemático del nodo Principal.....	39
Fig. 18: Sección “Modem Configuration” del Programa X-CTU	43
Fig. 19: Datos configurados en el nodo Principal	45
Fig. 20: Datos configurados en el nodo Remoto	46
Fig. 21: Mensaje enviado desde el nodo Principal	47
Fig. 22: Mensaje recibido en el nodo Remoto	47
Fig. 23: Mensaje enviado desde el nodo Remoto.....	48
Fig. 24: Mensaje recibido en el nodo Principal.....	48
Fig. 25: Trama Wiegand generada en VMLab	49
Fig. 26: Longitud de pulso de la Trama Wiegand generada	50
Fig. 27: Periodo entre pulsos de la Trama Wiegand generada.....	51
Fig. 28: Simulación de los datos enviados desde el nodo remoto.....	52
Fig. 29: Datos recibidos en ventana del servidor usando el X-CTU.....	52
Fig. 30: Datos recibidos en ventana del servidor mediante una aplicación de Visual Basic llamada “ControlSerialManual”.....	53
Fig. 31: Interfaz del usuario en nodo Central o Coordinador mediante la aplicación ControlSerialAuto en Visual Basic	54
Fig. 32: Registro de Accesos en la Interfaz del usuario.....	55

LISTA DE TABLAS

Cuadro 1: Comparación de características más importantes entre principales familias de XBee	30
Cuadro 2: Comparación de niveles de voltaje de los puertos E/S del módulo XBee, ATmega8L y ATmega8	32
Cuadro 3: Presupuesto del sistema planteado	56

LISTA DE ANEXOS

ANEXO 1: Encuestas a usuarios del área de oficinas del tercer piso del pabellón V	
ANEXO 2: Plano del Área Objetivo	
ANEXO 3: Códigos de Programación de las Pruebas realizadas al sistema	
ANEXO 4: Esquemáticos de las Tarjetas diseñadas para el sistema	
ANEXO 5: Fotos e imágenes de las Pruebas realizadas al sistema	
ANEXO 6: Hojas de datos de los dispositivos involucrados en el proyecto	
ANEXO 7: Precios y presupuestos recibidos de empresas por sistemas similares al planteado (sin capacidad inalámbrica)	

INTRODUCCIÓN

El objetivo de la presente tesis es presentar el diseño de un Sistema de Control de Acceso inalámbrico que sirva para incrementar la seguridad y monitorear el flujo de personas en el área de oficinas del pabellón de un edificio educativo como una universidad. Se presenta cuatro capítulos.

En el primer capítulo, se busca describir el contexto actual dentro del cual intervienen los edificios inteligentes y la seguridad electrónica, y ahondando en el sector de edificios educativos para explicar la problemática.

En el segundo capítulo, se hace una descripción de las tecnologías actuales aplicadas en los edificios inteligentes, específicamente dentro del rubro de seguridad electrónica, la cual se divide en sistemas de Intrusión, circuito cerrado de televisión, control de acceso y detección y alarma de incendios. También se hace una revisión de los protocolos de comunicación vigentes aplicados a este tipo de sistemas.

En el tercer capítulo, se describe en mayor detalle las hipótesis supuestas, los objetivos y las características requeridas del sistema que se planteará.

Y, finalmente, en el capítulo cuatro, se procede a explicar el diseño y configuración planteado para el sistema, dividido en nodos, y posteriormente en etapas para una descripción más detallada. Además, se justifica la elección de los dispositivos principales y los componentes electrónicos utilizados.

CAPÍTULO 1

ANÁLISIS DE LOS SISTEMAS DE SEGURIDAD ELECTRÓNICA

A continuación, se procederá a explicar el contexto en el que se ubica la problemática de la presente tesis, empezando desde el punto de vista de los edificios inteligentes. Después, como una de las áreas dentro de ese concepto, se dará una breve reseña del avance de la del avance de la seguridad electrónica en el país, para luego centrarse en el sector de edificios educativos y en la problemática en sí.

1.1 Edificios inteligentes

En la actualidad, los avances de la tecnología están siendo aplicados no solamente a nivel industrial, sino que cada vez más para usos domésticos. Hay varios ejemplos de dispositivos que fueron originalmente desarrollados para uso militar, que actualmente se usan diariamente por millones de personas. La globalización y las tendencias de los nuevos estilos de vida dan pie a que confíen cada vez más en las nuevas tecnologías para hacer más fáciles y llevaderas sus vidas y las de sus familias.

Estos nuevos estilos de vida hacen que el desarrollo de sistemas automáticos integrados aplicados al confort, seguridad, ahorro energético y mejor aprovechamiento de las comunicaciones sea una consecuencia natural; y, así como todo producto electrónico en la actualidad, sus costos están siendo cada vez más rápidamente accesibles.

Por el lado del mundo empresarial, también se está implementando diversos sistemas tecnológicos con el fin de facilitar ciertas funciones o procesos, así como para dar mayor comodidad a los trabajadores, y así crear un mejor ambiente de trabajo.

Los edificios inteligentes combinan la inteligencia otorgada a estos dispositivos o sistemas con capacidades de integración [1] con las que pueden generar un funcionamiento más completo; y contando con una correcta configuración de la unidad de control se puede personalizar su uso y llegar a adaptarse a los comportamientos habituales del usuario o a sus necesidades.

Así, los edificios inteligentes suelen combinar sistemas de ventilación e iluminación inteligente que brindan confort, con sistemas de seguridad como controles de acceso y alarmas comunicadas con sistemas de intrusión; todo esto, de una forma completamente automatizada y configurable por y/o para el usuario. Las posibilidades y combinaciones son tantas que se pueden llegar a satisfacer necesidades de usuarios ancianos o discapacitados, o simplemente generar un ambiente más cómodo y seguro en un hogar, una oficina u otro espacio. [2]



**Fig. 1: Edificio Inteligente de Interbank ubicado en San Isidro
(Tomado de memoriainterbank.pe)**

El hecho de poder comunicar estos diferentes sistemas entre sí para lograr respuestas automáticas más eficaces y completas es lo que le da inteligencia al sistema como conjunto, y es lo que debe irse buscando, ya que es mucho más útil tener un sistema integrado que todos los sistemas por separado.

Comparando un sistema de este tipo con otro sistema dependiente de solamente personas, permite valorar las funcionalidades del primero, ya que aparte de ser más confiable y seguro, puede proveer información de utilidad al usuario o al sistema.

Por ejemplo, un sistema de control de acceso puede no solo determinar si una persona tiene o no el permiso para entrar a una zona, sino también identificar cuándo el usuario está presente para comunicárselo al sistema de iluminación inteligente o al de ventilación, generando su activación y un consecuente grado de confort.

1.2 Seguridad a nivel electrónico

El rubro de Seguridad Electrónica es un sector tecnológico que está creciendo cada vez más en el país. Actualmente existen empresas dedicadas a Sistemas de Intrusión, Circuito Cerrado de Televisión, Detección de Incendios y Posicionamiento por Satélite (GPS), entre otros. Algunas de estas empresas son Orus, Siemens, Prosegur, G4S y Cartago.

Por otro lado, más municipalidades están optando por invertir en sistemas electrónicos de seguridad como Circuitos Cerrados de Televisión, ya que estos sistemas facilitan la labor del personal de seguridad e incrementa grandemente la eficiencia del manejo de la seguridad en la zona protegida.

Cabe resaltar que, aunque los sistemas electrónicos de seguridad aumentan la eficiencia de la seguridad en una zona o institución, la labor de las personas en los sistemas no puede ser remplazada por completo aún, ya que gran parte de la eficiencia de los sistemas, se debe a la interpretación de los datos obtenidos de los sistemas electrónicos y a los criterios de seguridad mayormente obtenidos en base a la experiencia de las personas.

1.3 Sistemas de Seguridad en Edificios Educativos

Es importante contar con sistemas de seguridad en todo edificio educativo. Normalmente suele usarse sistemas de Circuito Cerrado de Televisión en muchas empresas, así como hay áreas específicas donde será más importante un sistema de detección de incendios y otras donde será necesario un sistema para controlar el acceso de personas a zonas restringidas.

En este caso, el control de acceso en un área de profesores es necesario porque éstos cuentan con material que no puede ser visto ni manipulado por los alumnos, como las evaluaciones a ser rendidas o los documentos con las calificaciones. Además de esto, los profesores de tiempo completo guardan en esta zona sus pertenencias a lo largo del año, estén presentes o no en sus cubículos, y esto

merece ciertas medidas de seguridad para garantizar la tranquilidad de los docentes.

Según Roberto Ñaupari, Jefe de Seguridad de la Pontificia Universidad Católica del Perú, la mayoría de incidentes de robo o pérdida de objetos en la universidad se debe a situaciones inseguras generadas por las mismas personas y un sistema de seguridad como el control de acceso puede ayudar a disminuir los malos hábitos que causan estas situaciones. También es cierto que si los usuarios no ponen de su parte para contribuir con la seguridad y cumplir ciertas normas básicas, el sistema de seguridad puede perder gran parte de su eficacia.

1.4 Planteamiento del problema

En el tercer piso del Pabellón V de la Pontificia Universidad Católica del Perú se encuentran las oficinas de los profesores de Ingeniería Electrónica y de las Telecomunicaciones. Esta área tiene dos vías de ingreso: una por la parte interior del pabellón (al lado de la secretaría, se indica con un “1” en la Figura 2) y otra por el lado exterior (al lado del estacionamiento, se indica con un “3” en la Figura 2). Debido a las políticas de seguridad de la Universidad, es importante que solo se deje ingresar a esta área al personal docente autorizado, por lo que estas entradas siempre deben mantenerse cerradas.

La entrada “1” es una puerta de vidrio que se puede abrir tanto con llave, como eléctricamente desde la secretaría y da al área bordeada de líneas rojas segmentadas en la Figura 2. Al ingresar por ahí, se puede observar 5 puertas. Dos de ellas llevan a ambientes destinados a reuniones de coordinación de los profesores, asesoría hacia los alumnos, presentaciones, u otras actividades; otra puerta lleva al archivo, normalmente accedido solo por las secretarías; otra lleva a un laboratorio; y la última puerta (indicada como “2” en la Figura 2), lleva al área de oficinas de los profesores (bordeada de azul en la Figura 2) y suele estar cerrada con llave.

En la Figura 2 se muestra el plano del área objetivo del proyecto, aunque así como cuando se inició el desarrollo de la presente tesis hace dos años, se puede apreciar que algunos ambientes internos dentro de estas áreas no se encuentran actualizados. Sin embargo, se optó por usar este mismo plano por ser la versión “oficial” del mismo y debido a que su modificación no alterará el desarrollo del proyecto planteado en el presente documento.

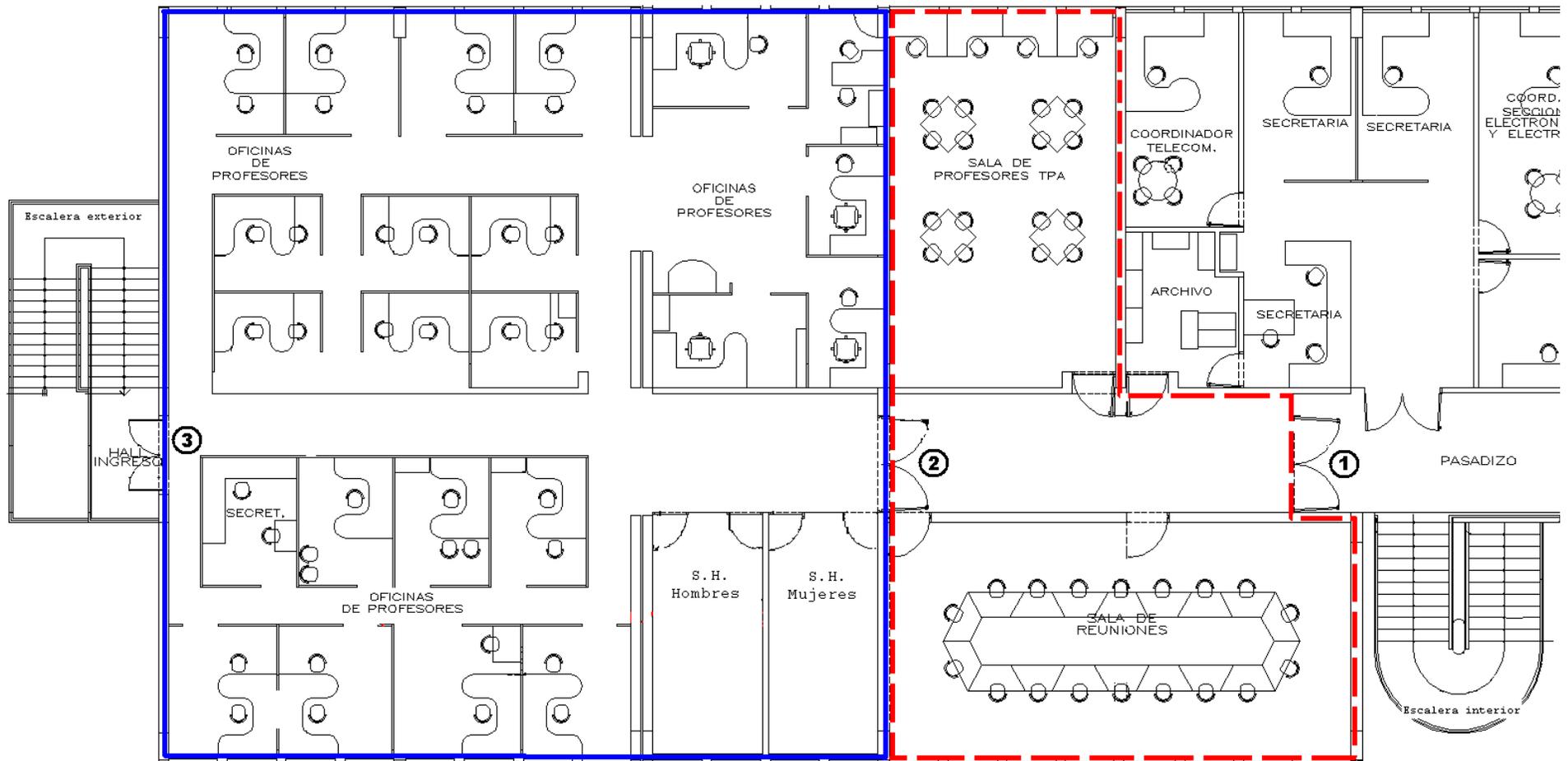


Fig. 2: Plano modificado del área objetivo

La entrada por el exterior del pabellón es una puerta de vidrio que se puede abrir con llave para ingresar y que tiene un sistema anti-pánico de salida, permitiendo a toda persona salir, como una puerta de emergencia. Este sistema hace que la puerta se cierre sola con un sistema de brazo amortiguado, el cual se encuentra defectuoso.



(a)



(b)



(c)

Fig. 3: Puertas (a) 1, (b) 2 y (c) 3 como señaladas en la Figura 2

El problema consiste en que el ingreso al área de profesores es muy fácil, porque no hay un real control de las personas que ingresan a ella. Los usuarios son alrededor de 20 profesores contratados a tiempo completo, otros 25 por horas, más 7 secretarías y asistentes, integrantes de los grupos de investigación presentes en el área, además el personal de limpieza y algún profesor invitado con acceso temporal. Esto suma alrededor de 60 usuarios, la mayoría de los cuales posee llaves de las 3 puertas. El problema con el uso de las llaves es que se les puede dar un uso muy abierto, y es muy fácil sacar copia de un juego. Además, se necesita una llave para ingresar por cada una de las puertas, pero la salida normalmente es libre. A esto se le suma la posibilidad de la existencia de malos hábitos como el hecho de prestarle la llave a otra persona o el simple y cortés (pero a la vez inseguro) hecho de que una persona con acceso mantenga la puerta abierta mientras pasa, a personas que desean entrar detrás de él. No se está afirmando el continuo desarrollo de estos hábitos, sino que se les señala como ejemplos de vacíos en el sistema de seguridad actual que pueden suceder en cualquier momento. Finalmente, según los reportes de seguridad, muchas veces se deja abierta la puerta exterior que da al estacionamiento por problemas con el funcionamiento del sistema de cierre lo cual puede ser motivo de problemas en la seguridad de este ambiente.

En esta tesis se planteará una solución que podrá asegurar un mejor control del acceso a esta área restringida de este pabellón de la Universidad para cumplir con las normas de seguridad que ésta establece, usando herramientas tecnológicas que permitan un uso sencillo, seguro, que cubran los problemas de seguridad existentes actualmente.

Durante el desarrollo de este trabajo de tesis, se realizó una encuesta a ciertos usuarios de la zona objetivo. Este estudio revela que a los usuarios les importa mucho que el sistema de control de acceso a utilizar sea sencillo y práctico y que no dificulte o demore el ingreso de los usuarios. Además, es importante señalar que los usuarios advierten que la mayor inseguridad es causada por malos hábitos de los mismos usuarios, como no cerrar correctamente las puertas y también recomiendan que se lleve un registro de los accesos, especialmente para llevar un control en horas poco comunes, como en las noches. Estas encuestas se encuentran adjuntas en los anexos.

CAPÍTULO 2

SISTEMAS DE SEGURIDAD Y CONTROL DE ACCESO EN LA ACTUALIDAD

2.1 Edificios Inteligentes en la Actualidad

Los Sistemas Domóticos y de Edificios Inteligentes pueden proveer a los usuarios, entornos completos de gran confort y seguridad mediante la manipulación de conjuntos de diferentes variables que se adaptan a las preferencias pre-configuradas. Estas variables incluyen el control de acceso, iluminación, seguridad, monitoreo, acceso compartido a medios, etc. Algunas empresas en el Perú que se especializan en estos campos son Controlmatic, Trazzo, Viditek, Home&Office Technologies y AV Integradores.

Para que el diseño e instalación de un sistema como éste pueda ser más eficaz, debería poseer dos capacidades que brindan gran facilidad en su crecimiento y resultados mucho más eficientes: la integración y la escalabilidad. [3]

- **Integración**

La integración es la capacidad de un sistema inteligente mediante la cual todo el sistema como conjunto puede aprovechar la información compartida desde cada dispositivo parte de cualquiera de sus subsistemas, para mejorar el desempeño de otros. Esto mejora grandemente la funcionalidad del sistema en su totalidad y genera diversidad de posibilidades para beneficio del usuario.

Por ejemplo, el control de acceso que me identifica en la entrada de mi hogar, puede también enviar una señal para que se encienda el aire acondicionado y que se reproduzca mi selección musical preferida; o que cuando una persona sale de su hogar y activa el modo “*all out*” todos los dispositivos y luces deben apagarse, a no ser que estén pre-programados para operar también en esas condiciones.

Con un correcto grado de integración, el uso del sistema se torna más sencillo y es capaz de satisfacer las necesidades del usuario de forma más completa.

- **Escalabilidad**

Un sistema fácilmente escalable es el que no genera problemas cuando se requiere agregarle subsistemas o hacerlo crecer con el uso de más dispositivos que generarán mayores funciones. Esto es algo que ocurre en muchos de los casos, ya que el costo inicial de un sistema inteligente completo puede ser muy elevado, así que el usuario puede adquirir solo los dispositivos básicos y luego ir agregándole más funcionalidades al sistema a medida que compra los dispositivos complementarios.

Esta capacidad tiene mucho que ver con la compatibilidad de marcas o las formas de comunicación entre los dispositivos. En el mercado existen marcas como Siemens que producen sistemas de protocolo cerrado o propietario, es decir, que solo pueden comunicarse con otros productos de la misma marca. Normalmente los “kits básicos” de estos sistemas tienen un menor precio, ya que la mayor ganancia la obtienen con la venta de los dispositivos adicionales.

Sin embargo, hay gran cantidad de marcas que ofrecen productos con protocolos abiertos para que puedan comunicarse con una mayor gama de dispositivos de diversas gamas, compartiendo el mismo protocolo. Esto le da más flexibilidad y capacidad de escalabilidad al sistema, ya que es compatible con más variedad de dispositivos.

2.2 Seguridad Electrónica

La Seguridad Electrónica como campo abarca varias áreas que pueden o no estar integradas. A continuación, se procederá a explicar la función de cada una de ellas y las alternativas con las que se cuenta. Algo a tener siempre en cuenta es que la Seguridad Electrónica no es solamente el hecho de usar coordinadamente ciertos dispositivos y sistemas electrónicos, sino hacerlo con los debidos criterios de seguridad que suelen ser obtenidos con la experiencia en proyectos reales y su mantenimiento y análisis.

2.2.1 Detección de Intrusión

Un sistema de detección de intrusión consiste en detectar cuando una persona no autorizada ha ingresado a un lugar, como una casa o una oficina. Normalmente, el

sistema, al detectar a un intruso, genera una señal de alarma que puede ser audible en el interior, en el exterior o detectada directamente en la empresa de seguridad contratada.

Existen muchos tipos de tecnologías que permiten la detección:

- Barreras fotoeléctricas
- Cables microfónicos
- Contactos Magnéticos
- Detectores de movimiento
 - Tipo Fresnel: Detecta cambios de temperatura. En este grupo están los Receptores Pasivos Infrarrojos (PIR).
 - Óptico: Similar al Fresnel, con tecnología de espejos.
 - Radares de alcance controlado: De mayor precisión costo. Combina la tecnología PIR con la de radar.
- Sensores de choque
- Detectores de rotura de cristal

2.2.2 Circuito Cerrado de Televisión

Un Sistema de Circuito cerrado de televisión consiste en el monitoreo de la actividad en una determinada área o conjunto de áreas de una forma eficaz para poder determinar fácilmente cuando algo fuera de lo normal está ocurriendo. Está comprendido por 3 etapas: captura de imagen, transporte y procesamiento de datos, y, presentación y almacenamiento. [4]



Fig. 4: (a) Contactos Magnéticos (b) Sensor de movimiento tipo PIR
(Tomado de utcssecurityproducts.com)

a) Equipos de captura de imagen

Hay diferentes tipos y tecnologías para cámaras en la actualidad. Para poder seleccionar una cámara adecuada se debe tomar en cuenta algunos factores vinculados a la aplicación y a lo que se necesitará:

- Imagen en blanco y negro o a color
- Mucha o poca definición
- Objetos móviles o inmóviles
- Planos cortos, largos o variables
- En interior o exterior
- Iluminación del ambiente

Con esta información se podrá decidir que características son necesarias para ciertos elementos, como:

- El lente
- El sensor CCD
- La carcasa
- El posicionador
- La iluminación auxiliar

Como se debe suponer, hay una amplia gama de variantes para elegir, pero se puede mostrar un pequeño listado dentro del cual cada tipo tendría más potencial a ser explotado que el anterior.

- Cámaras fijas
- Cámaras Domo
- Cámaras PTZ (Pan-Tilt-Zoom)
- Scanners
- Cámaras IP



Fig. 5: Cámara Domo PTZ
(Tomado de *pelco.com*)

De cada uno de estos se puede variar sus características para cumplir con los requerimientos de cierta aplicación específica.

b) Equipos de Transporte y Procesamiento

Cada señal capturada debe viajar a una central de monitoreo, así que existen dispositivos que se encargan de transmitir la señal y otros de recibirla. Dependiendo del sistema, las cámaras podrán o no recibir órdenes de la central, para lo cual se necesitará equipos de transmisión y recepción que puedan proveer estas funciones de comunicación.

Además, dependiendo de los requerimientos del sistema, se puede elegir un medio de transmisión adecuado:

- Fibra Óptica monomodo o multimodo
- Par trenzado
- Cable Coaxial (RG-11 o RG-59)
- Comunicación Inalámbrica

c) Equipos de Presentación y Almacenamiento

Existe una diversidad de monitores o pantallas donde pueden ser visualizadas las imágenes, ya que no es necesario usar uno de aplicación específica. Sin embargo, la principal característica a tener en cuenta para elegir este elemento es simplemente su tamaño; esto dependerá de la aplicación que se le esté dando al sistema y de la forma en que se esté visualizando.

En cuanto a las tecnologías de grabación usadas, existen dos principales:

- Tarjetas capturadoras.- Requieren ser insertadas en un CPU y pueden manipular 4, 8 o 16 cámaras. Son muy usadas en el país.
- Grabadores independientes.- Son dispositivos de funcionamiento independiente (*Stand-Alone*) que tienen mayores opciones de configuración y suelen ser diez veces más caros que las tarjetas.

Existen tres variantes principales:

- Video Cassette Recorder (VCR)
- Digital Video Recorder (DVR)
- Network Video Recorder (NVR)

También es posible que necesite usarse algún dispositivo para poder visualizar las señales de cierta forma en especial: secuencialmente o a la vez, entre otras opciones. Para esto pueden usarse:

- Secuenciadores
- Divisores de cuadrantes
- Multiplexores Simplex o Dúplex

Adicionalmente, existen otros equipos, como los paneles de control, con los que se puede controlar las cámaras para observar un punto específico en mayor detalle e insertar texto en las imágenes.

2.2.3 Detección y Alarma de Incendios

La NFPA (*National Fire Protection Association*) define a un sistema de detección y alarma de incendios como los componentes y circuitos destinados a monitorear y anunciar el estatus de alarma de un incendio, a supervisar las señales de los dispositivos de detección e iniciar los protocolos de respuesta a aquellas señales.[5] Un sistema de detección de incendios tiene como objetivo descubrir dónde se está iniciando un incendio con precisión de tiempo y espacio y alertar con un eficiente sistema de alarmas. Para esto, una Central monitorea constantemente los detectores automáticos y manuales, y emite alarmas en el panel central cada vez que detecta una irregularidad.

Hay muchas marcas que proveen sistemas de detección y alarma de incendios, como Honeywell, Siemens, Edwards y Simplex.



Fig. 6: Detector Fotoeléctrico de Humo
(Tomado de notifier.com)

2.2.4 Control de Accesos

La idea más básica de un sistema de control de acceso es que controla a qué personas se les permite o deniega el acceso a cierto lugar, en cierto momento. Según esta definición una simple cerradura junto con un juego de llaves también controlan el acceso a un área, y son muy útiles para muchas ocasiones. Sin embargo, cuando se requiere de mayor seguridad o de ciertas funciones específicas, se puede usar una tecnología más avanzada.

Esto consiste en una serie de dispositivos, llamados lectores, colocados cerca a las puertas de zonas restringidas, que están conectados a un servidor principal. Cuando una persona quiere entrar a una zona, se identifica ante el lector asociado a la puerta correspondiente y un controlador decide si se le da acceso o no. Cada vez que alguien trata de ingresar, la información queda guardada en el servidor. El controlador puede encontrarse en el servidor o en cada lector.

Este tipo de sistemas puede proveer información muy útil a otros subsistemas si está integrado a un sistema más grande.

a) Partes de un sistema de control de acceso

Un sistema de control de accesos consta de un lector, una credencial, un controlador, un servidor y un mecanismo para apertura de puerta. Para cada uno de estos existen diversas tecnologías cuya utilidad varía dependiendo de la aplicación específica.

- **Lector**

Es el dispositivo que se comunica con una credencial y envía su información al controlador para determinar el permiso de acceso. Es como una interfaz entre el sistema y el usuario. Existen diversas tecnologías:

- Teclado matricial: Consiste en que el usuario debe ingresar una clave personal (PIN) a través de un teclado.
- Biométrico: El lector tiene la capacidad de identificar algún parámetro personal único de una persona, como la retina del ojo, su voz, sus huellas digitales o la geometría de la mano o su rostro.
- De contacto: Requiere que el usuario pase su credencial a través del lector. Suele ser con tarjetas con código de barras o de cinta magnética.
- De proximidad (RFID): Requiere que el usuario acerque su credencial a cierta distancia del lector para que éste pueda leerla. Suele usarse con tarjetas de proximidad, Wiegand o tarjetas inteligentes. También existen otros dispositivos que usan las mismas tecnologías pero adoptan diferentes formas, como llaveros e incluso teléfonos celulares.[6]

Además, existen lectores que combinan dos o tres de estas opciones para generar un mayor grado de seguridad. Se suele combinar un teclado con un lector de tarjetas o de huellas digitales.

- **Credencial**

Es lo que identifica a una persona y que ésta requiere para obtener el acceso a las zonas permitidas. Puede definirse como algo que una persona posee, sabe o es. Aparte de los códigos de seguridad y los parámetros biométricos (retina, voz, huellas digitales y geometría de la mano) que fueron mencionados anteriormente, se usa una gran variedad de tarjetas u objetos basados en distintos principios físicos. Los principales tipos son los siguientes:

- **Ferrita de Bario**
- **Cinta Magnética**
- **Código de barras**
- **Wiegand**
- **RFID (incluye los de Proximidad)**
- **Inteligentes (*smart cards*)**



Fig. 7: Ejemplos de (a) Lectoras de proximidad y de (b) Credenciales
(Tomado de honeywellaccess.com)

- **Controlador**

Es el encargado de decidir a quiénes se les permite el acceso a qué zonas y en qué momentos. Es consultado en cada intento de ingreso y puede ser parte de las funciones del lector, si es un sistema de control distribuido o del servidor si es un sistema de control centralizado.

- **Servidor**

El servidor normalmente es una PC que se encarga de almacenar la información de cada intento de acceso, sea exitoso o no, para llevar un registro que puede ser utilizado para cumplir con ciertas funciones adicionales o para generar reportes. Además, el sistema también se podría diseñar para que reciba una señal cuando alguien está tratando de forzar uno de los lectores o cuando una puerta es dejada abierta por mucho tiempo.

- **Mecanismo de apertura**

Cuando se determina que el usuario tiene permiso de acceso, se le debe permitir el ingreso, normalmente mediante la apertura de una puerta. Esto suele hacerse mediante la activación de contactos magnéticos o pulsos eléctricos, según la aplicación.

Para algunas de estas tecnologías existen dos medidas de seguridad básicas [7]:

- *Fail safe*: Permite que una puerta se mantenga abierta en caso no contar con energía eléctrica.
- *Fail secure*: Deja la puerta cerrada si no se cuenta con energía eléctrica. Normalmente, en la dirección de salida la puerta si se podría abrir, como medida de seguridad en caso de incendios, sismos u otros.

b) Comunicaciones en Control de Acceso

Existen dos formas principales en que la información es comunicada desde un lector de control de acceso hacia su controlador, independientemente de la tecnología de reconocimiento que use.

La primera es el estándar para control de acceso basado en normas SIA AC-01-1996.10: el protocolo Wiegand. [8] Éste define los niveles de voltaje y otras especificaciones eléctricas de la capa física. También propone la composición de la trama y, en ella, su revisión de errores mediante el chequeo de paridad.

La segunda forma es el uso del estándar RS-485 que define los parámetros de la capa física, como niveles de voltaje, y es ampliamente utilizado para aplicaciones industriales. La composición de la trama, si no es generada con protocolo Wiegand, suele estar formada por protocolos propietarios de los fabricantes de sus propios equipos.

En el mercado existen controladores que permiten entradas de lectoras de su misma marca así como entradas de lectoras Wiegand, como el caso del controlador AR-716Ei de Soyal, cuya hoja de datos se encuentra en los anexos. La mayoría de las soluciones planteadas por las empresas implican varios equipos, como las lectoras, controladores, adaptadores de RS-485 a USB o Ethernet, y otros dispositivos intermedios de adaptación.

c) Aplicaciones

Existen varias aplicaciones para las cuales se puede usar las bases de un Sistema de Control de accesos o que éste puede proveer adicionalmente si está integrado a un sistema más grande. Algunos ejemplos son:

- **Control de asistencia**, sea al trabajo, a clases u otro. En este caso no se requiere de tanta seguridad, así que se puede usar sistemas más sencillos, ya que no hay zonas restringidas que resguardar.
- **Localización del personal**. Se puede determinar donde está o donde estuvo una persona dentro del edificio si se analiza el registro de sus ingresos y salidas en el servidor.
- **Control de parqueo y estacionamiento** para tomar el tiempo que un vehículo se queda en una zona y realizar el cobro adecuado de dinero.
- **Exclusas de Seguridad**. Como medida de seguridad a la entrada de una empresa o planta.
- **Control de rondas**. Se utiliza lectoras distribuidas en diversas partes de un local, como una universidad, banco, museo, etc. El personal de seguridad debe marcar su paso por dichos puntos, y así confirmar que está realizando rondas de seguridad a las horas establecidas.

2.2.5 Comunicación

Los dispositivos pueden comunicarse entre sí por medio de cierto cableado estructurado o a través de ondas de radio; una variante de la alternativa cableada es usar la red eléctrica para comunicar datos. La elección depende del tipo de ciertos factores, como la distancia y el costo.

Además, para que la comunicación se efectúe de forma correcta, es necesario contar con un protocolo de comunicación determinado que es el conjunto de reglas estandarizadas para poder establecer la comunicación entre los dispositivos.

a) Medios de comunicación

Entre los principales medios de comunicación están las siguientes tecnologías:

- Par trenzado: Se usa para conexiones telefónicas y para conexiones de red. Se usa las variantes UTP, FTP y STP, donde la primera es la más usada por ser la más flexible. Diversas categorías de esta misma son ampliamente usadas para redes de área local (LAN) alcanzando una velocidad de 1 Gbit/s.
- Cable coaxial: Usado ampliamente para sistemas de televisión por cable (CATV) y circuitos cerrados de televisión (CCTV). Soporta hasta 300 Mbit/s.
- Fibra Óptica: Es usada por los proveedores de Internet y servidores de alta velocidad y no por usuarios finales debido a razones de costo-beneficio. Puede alcanzar velocidades de hasta 100 Gbit/s.
- Ondas de radio: El uso de las radiofrecuencias depende de la normativa de cada país. La frecuencia libre mundialmente es la de 2,4 Ghz. En el Perú, el Ministerio de Transportes y Comunicaciones (MTC) se encarga de gestionar su uso. La velocidad máxima a alcanzar por esta vía depende del ancho de banda permisible en el área y del protocolo de comunicación a utilizar.

b) Protocolos de comunicación

Un protocolo de comunicación trabaja con ciertos parámetros que definen el tipo de aplicación con el que será más conveniente trabajar, como la topología de red, el ancho de banda disponible y el número de nodos máximo de la red.

Existen protocolos libres y protocolos propietarios. Los libres pueden ser usados para generar redes propias pudiendo éstas ser configuradas para aplicaciones específicas por el usuario; los propietarios solo pueden ser manipulados por el fabricante o proveedor y el usuario final no puede hacer configuraciones, solamente recibe la información resultante. Algunos de los principales protocolos libres son:

- WiFi: Es un protocolo de comunicación inalámbrica, mayormente utilizado para permitir la conexión a Internet de un dispositivo, siempre y cuando se encuentre en el área de alcance de un punto de acceso. También permite conectarse punto a punto (peer-to-peer) a través de una red ad-hoc que permite conectar dos o más dispositivos directamente. Su alto consumo de potencia permite amplios rangos de alcance, normalmente 95 metros en un lugar abierto y 30 metros en uno cerrado. Puede alcanzar una velocidad de

108 Mbit/s. Está basado en el estándar IEEE 802.11 y usa la banda de 2.4 Ghz o de 5 Ghz.

- Bluetooth: Este protocolo de comunicación inalámbrica es usado para redes de área personal que puede ser un máximo de 1, 10 o 100 metros dependiendo de la potencia a usar (1mW, 25mW o 100mW respectivamente). Normalmente se usa para dispositivos de uso personal como teléfonos móviles, audífonos y otros. Usa la banda de 2.4 Ghz y está basado en el estándar IEEE 802.15.1. Comúnmente puede lograr 3 Mbit/s pero su gran desventaja es solo puede haber 8 nodos conectados a una misma red.
- ZigBee: Es un protocolo de comunicación inalámbrica pensado para redes seguras con baja tasa de transferencia de datos (comúnmente con un máximo de 250 Kbits/s) y muy bajo consumo de energía (30 mA en estado activo y 3uA en reposo), por lo cual se usa más en sistemas en los que los nodos no estarán activos la mayor parte del tiempo, pero que requerirán ser atendidos rápidamente, como en los sistemas domóticos. Puede abastecer a un máximo de 65635 nodos distribuidos en 255 subredes.
- X-10: Este es un protocolo de muy baja tasa de transferencia de datos que usa como medio el cableado eléctrico existente en un edificio. Para la comunicación de un comando se requiere aproximadamente 183 milisegundos (cada trama completa toma aproximadamente 750 milisegundos), por lo que su aplicación está restringida mayormente a activación o desactivación de sistemas ON/OFF como luminarias.
- Ethernet: Es un protocolo ampliamente usado para conexión a Internet y entre dispositivos de una red local sobre cable UTP de diferentes categorías dependiendo de la capacidad que se requiera. Puede alcanzar muy altas velocidades, hasta sobrepasar los 10 Gbps.
- LonWorks: Es un protocolo que facilita la interacción de dispositivos que usan diferentes medios de comunicación con diferentes anchos de banda mediante adaptadores estandarizados. Soporta medios como par trenzado, fibra óptica, líneas de tensión y radiofrecuencia. Esta dirigido a diversas aplicaciones de control y automatización en edificios.

2.3 Síntesis de la investigación y planteamiento de la propuesta

Se ha procedido a analizar qué elementos son necesarios para elegir un sistema adecuado de seguridad electrónica [9] y qué características se debe tomar en cuenta para la elección del protocolo y medio de transmisión para nuestro sistema.

Para el presente caso, se recomienda contar con un sistema de control de accesos en todas las puertas de ingreso del área objetivo. El criterio de seguridad contempla el monitoreo de todas las personas que ingresan al área de oficinas objetivo, descrita en el punto 1.4. Para poder asegurar que una persona que ingrese con un visitante tenga responsabilidad sobre su acompañante, se plantea la inclusión de lectoras de acceso también en el lado de egreso de cada puerta.

Con esta disposición también se podrá obtener un valor agregado del sistema: se podrá conocer qué personas se encuentran en cada zona, en cada momento, y así tener un monitoreo más acertado de las personas que como se tiene en la actualidad.

Cada ingreso o intento de ingreso será registrado en una computadora, que determinará si se concede o se deniega el acceso. Esta información podrá ser visualizada en esta computadora a través de una interfaz que muestre la hora y la fecha en las que se produjo cada entrada. A través de esta interfaz también se podrá agregar nuevos usuarios y modificar sus permisos de acceso a las diversas áreas.

Se usará el protocolo ZigBee debido a sus capacidades inalámbricas y de muy bajo consumo de energía [10], que minimizará el mantenimiento requerido por el sistema, especialmente en cuanto a cambio de baterías.

CAPÍTULO 3

ANÁLISIS DE PARÁMETROS A TOMAR EN CUENTA EN EL DISEÑO DEL SISTEMA DE CONTROL DE ACCESO

3.1. Hipótesis de la investigación

3.1.1. Hipótesis principal

Toda oficina o grupo de oficinas requiere que el flujo de personas en ella esté controlado por medidas de seguridad, orden y comodidad de sus ocupantes. Un sistema estructurado de control de acceso como el que se plantea mejorará estas variables en el entorno y brindará utilidades y características de valor agregado como la fácil instalación, el ahorro energético y la apertura a la explotación de más funciones a partir de la integración de esta solución con otros sistemas.

3.1.2. Hipótesis secundarias

- Se plantea un sistema que será de fácil uso para los usuarios e incrementará notablemente la seguridad en el área de oficinas, luego de un corto periodo de tiempo de acondicionamiento de los usuarios.
- El sistema propone, como una función adicional, la posibilidad de conocer la ubicación de las personas que se encuentran dentro del área de oficinas, lo cual puede mejorar, por ejemplo, la labor administrativa.
- La solución planteada está diseñada para generar un bajo consumo de energía, lo cual tendrá como una de sus consecuencias que la labor de mantenimiento no necesite ser muy frecuente.
- La capacidad inalámbrica de los nodos del sistema hace que el sistema sea fácil de instalar y no requiera dejar un rastro de cableado poco estético en las inmediaciones del lugar.

- Este sistema está pensado para que pueda ser integrado a un sistema más grande o con otros sistemas, con los cuales se pueda generar una mayor explotación de los datos para la optimización de ciertos procesos.

3.2. Objetivos de la investigación

3.2.1. Objetivo general

Diseñar un sistema de fácil instalación que permita controlar el acceso de personas a un área de oficinas restringida y que permita integrarse con otros sistemas para el intercambio de información.

3.2.2. Objetivos específicos

- a. Elegir un protocolo de comunicación adecuado que ayude a cumplir con las características deseadas del sistema, como la integración, el bajo consumo de energía y el bajo costo.
- b. Elegir dispositivos que permitan ahorrar espacio y que requieran un bajo consumo de energía.
- c. Diseñar las etapas de adaptación de los protocolos de control de acceso hacia el protocolo de comunicación inalámbrica elegido.
- d. Diseñar la interfaz de comunicación con el servidor que contendrá la base de datos y otorgará los permisos.
- e. Configurar la red inalámbrica.
- f. Implementar los sub-sistemas necesarios que permitan realizar pruebas que ratifiquen la correcta operación del sistema.

3.3. Características requeridas del sistema

El sistema en su totalidad necesita ser de fácil uso para que no se convierta en una carga tediosa para el usuario, ya que si esto ocurre es probable que el mismo usuario “sabotee” el sistema mediante malos hábitos, y así deje de ser útil.

A continuación se describen los requerimientos de cada parte o etapa del sistema.

3.3.1. Etapa de adaptación de protocolo Wiegand a UART

Esta etapa deberá tener como entrada niveles de voltaje frecuentes para protocolo Wiegand, el cual fue creado especialmente para sistemas de control de acceso y se considera como un estándar en la industria. Consiste en señales con niveles de 5 voltios con respecto a la tierra común a una frecuencia típica de 20 KHz –pulsos negativos de 50 microsegundos con un espacio entre ellos de 1 milisegundo, por lo

que esta etapa necesita adaptar los voltajes para que pueda soportarlos el módulo de radiocomunicación, así como reordenar la trama para su retransmisión.

El protocolo consta de 3 líneas: una se puede conocer como D0, la segunda como D1 y la tercera sería la tierra común. El estado estable de D0 y D1 es en alta, es decir, 5 voltios. Cuando se quiera enviar un '0' lógico, la línea D0 se tendrá que poner en nivel bajo, mientras D1 se mantiene en nivel alto; y cuando se quiera enviar un '1' lógico D1 deberá ponerse en nivel bajo, mientras que D0 se mantiene en nivel alto. Si tanto D0 como D1 estuviesen en nivel bajo, el dato sería inválido.

La trama Wiegand más común es la de 26 bits, en la que el primer bit indica el valor de paridad par de la suma de los siguientes 12 bits y el último bit indica el valor de paridad impar de los anteriores 12 bits. Los 8 bits del segundo al noveno indican el código que identificará a la lectora de la cual se está solicitando el acceso, y los 16 bits restantes identifican al usuario que está pidiendo acceso.

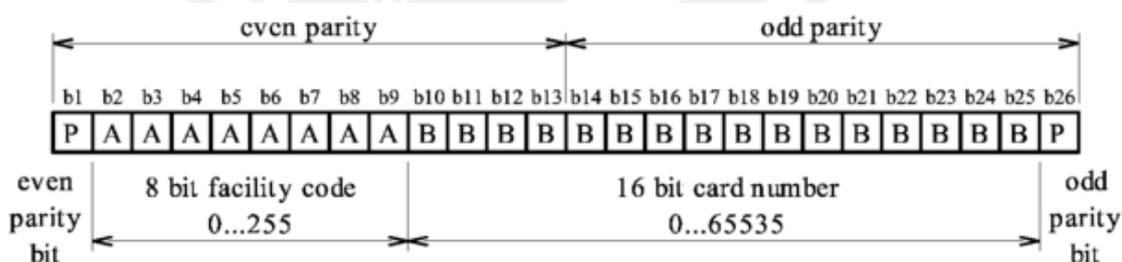


Fig. 8: Composición de Trama en Protocolo Wiegand
(Tomado de <http://courses.cit.cornell.edu>)

La comunicación con el módulo de radiocomunicación, debe ser lo más directa posible para evitar errores por desfase de tiempos y para obtener rápidamente el permiso de acceso, por lo que los niveles de voltaje de los puertos del microcontrolador que hará la descomposición de la trama y de los puertos del módulo de radiocomunicación serán compatibles.

Además, debido a que esta etapa se encuentra en uno de los nodos remotos, ayudaría que el hardware sea lo más pequeño posible por lo que se puede ahorrar en componentes para ahorrar en espacio. Esto también se puede hacer usando la misma fuente de alimentación para todos los circuitos en este nodo.

3.3.2. Comunicación por Radiofrecuencia

Se requiere que los módulos de radiocomunicación conversen a través de una banda libre con cierto nivel máximo de potencia, como lo estipula la ley. Según el Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, publicada en el 2005, “están exceptuados de contar con concesión de la asignación del espectro radioeléctrico, autorización, permiso o licencia, para la prestación de servicios de telecomunicaciones aquellos servicios cuyos equipos, utilizando las bandas de 902-928 MHz, 2400-2483,5 MHz y 5725-5850 MHz transmiten con una potencia no superior a cien milvatios (100mW) en antena (potencia efectiva irradiada), y no sean empleados para efectuar comunicaciones en espacios abiertos. Dichos servicios no deberán causar interferencias a concesionarios de servicios públicos de telecomunicaciones”. [11]



Fig. 9: Cable para estándar RS-232 DB9
(Tomado de www.kellycontroller.com)

Dentro del área de oficinas, el espacio máximo entre lector y nodo central es entre 25 y 30 metros en espacio cerrado y la comunicación necesaria será de punto a punto –de nodo remoto a nodo coordinador- y de punto a multipunto –de nodo coordinador a todos los nodos. La comunicación entre ellos sería mediante protocolo ZigBee, que tiene la ventaja de no interferir con el protocolo WiFi. Por otro lado, se utilizará la capacidad de comunicación serial del nodo coordinador al servidor.

3.3.3. Adaptación de protocolo UART a RS-232

Esta etapa tiene como entrada la comunicación serial proveniente del módulo de radiocomunicación central. Esta etapa no solo debe recibir los datos del módulo de radiocomunicación para reenviarlos a la PC, sino también responder de vuelta de la

PC al módulo para que éste comunique la aceptación o denegación del acceso al nodo remoto. Los niveles de voltaje hacia la PC son simétricos con respecto a la tierra común entre ± 3 y ± 15 voltios, según lo aceptado por el estándar RS-232. Se hará uso de este estándar debido a que para este tipo de aplicaciones tiene alta comercialidad y es fácilmente adaptable con el estándar USB.

3.3.4. Requerimientos de la PC o Servidor

La función de la PC va a ser almacenar la base de datos de los usuarios permitidos para cada área, y en base a ésta, validar o invalidar los permisos de acceso de los usuarios remotamente.

La información que se maneja puede servir para más aplicaciones de las que se propone, pero en base a los requerimientos del sistema planteado, solo se requiere que la PC tenga, como mínimo:

- Sistema Operativo desde Windows 95 a Windows Vista
- 1 puerto serial RS-232 o USB libre
- SQL Server 2000 o posterior
- Espacio libre en el servidor de 1 MB (si se usa el puerto RS-232) o 6 MB (si se usa el puerto USB, para instalar el driver adecuado)
- Espacio de almacenamiento de datos: 45MB para la información de ingresos y salidas por tres meses (considerando 500 accesos por día)

3.4. Esquema general de la Solución Planteada

Finalmente, la solución obtenida se grafica a continuación en la Figura 10. Se contará con un Nodo Central conectado a una PC y con varios Nodos Remotos, cada uno conectado a la entrada o salida de una puerta. Por simplificación, en el gráfico se muestra solo la comunicación entre un nodo remoto y el nodo central. La comunicación será inalámbrica a través de módulos, que usan protocolo ZigBee.

Cada nodo remoto tendrá como entrada principal la data proveniente de la lectora de control de acceso, que se comunicará en protocolo Wiegand. En este nodo se adaptará la información para enviarla serialmente por UART (*Universal Asynchronous Receiver/Transmitter* o *Recepción/Transmisión Asíncrona Universal*) hacia el módulo RF.

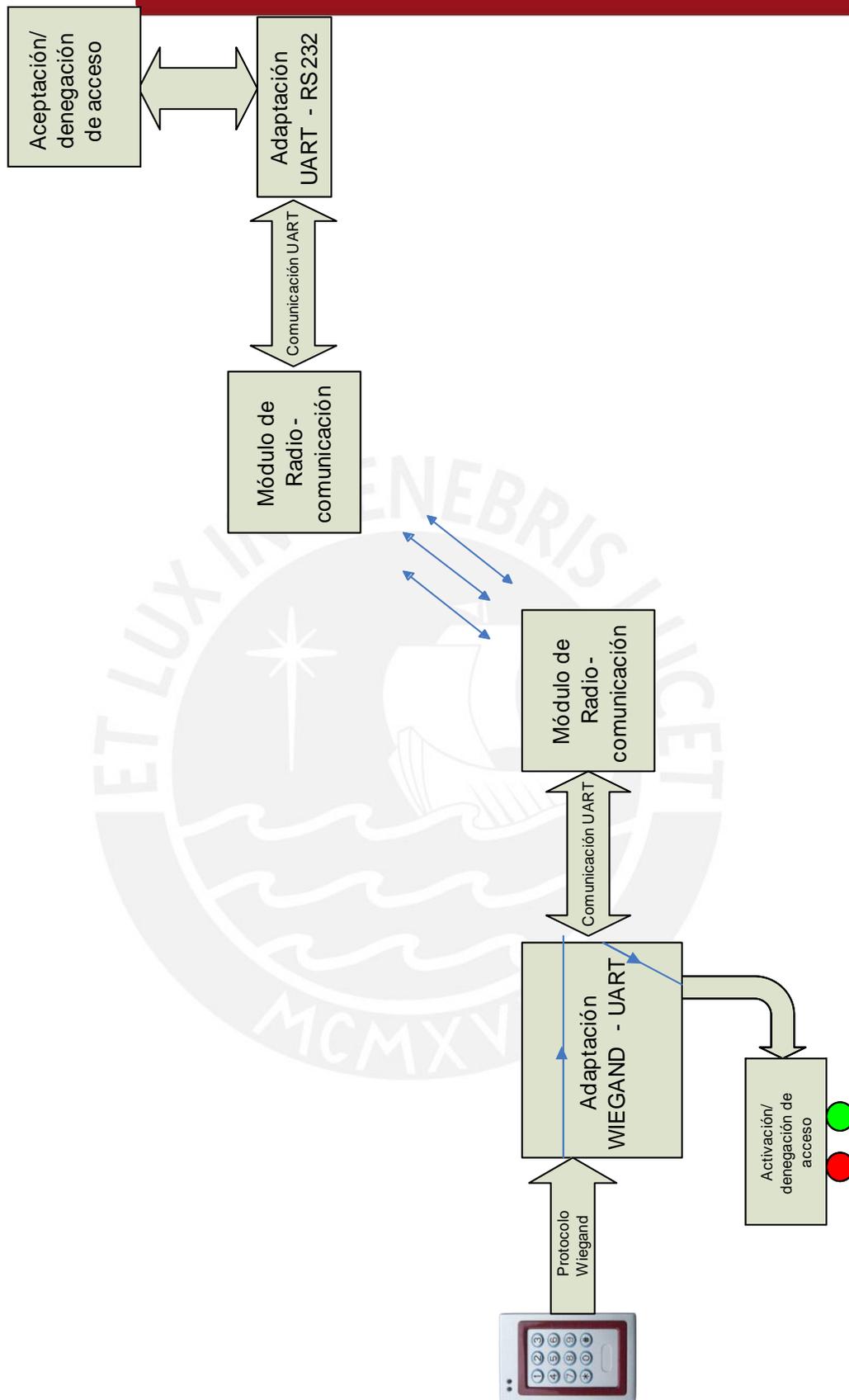


Fig. 10: Diagrama de Bloques del Funcionamiento del Sistema

Luego, los datos pasarán inalámbricamente mediante protocolo ZigBee de un nodo a otro mediante los módulos RF. Esta información se reenviará desde módulo RF mediante UART, y tendrá que ser adaptado a RS-232 para llegar posteriormente al Servidor.

El Servidor analizará la información recibida desde el nodo remoto con su base de datos, y determinará si se otorga o deniega el acceso, y esta respuesta de la petición de acceso será enviada de vuelta por todo el camino, anteriormente explicado, pero a la inversa. Cuando esta información llegue al nodo remoto, se indicará físicamente la aceptación o denegación del acceso.



CAPÍTULO 4

DISEÑO DEL SISTEMA DE CONTROL DE ACCESO

4.1 Justificación de la elección de Componentes y Estándares

4.1.1. Elección del Protocolo de Control de Acceso de entrada

El protocolo Wiegand es un estándar abierto creado especialmente para comunicar los datos de una lectora de control de acceso hacia su controlador o al resto del sistema. La alternativa a Wiegand es el estándar RS-485, el cual suele usarse conjuntamente con protocolos propietario del fabricante de los equipos lectores y controladores.

Existen equipos como controladores que tienen entradas para lectoras que funcionan con el protocolo propietario del fabricante pero que también poseen entradas para lectoras Wiegand.

El sistema planteado en el presente trabajo tomará como entrada una señal en protocolo Wiegand, ya que éste es un estándar ampliamente usado y sí brinda todas las especificaciones necesarias para emular su funcionamiento, analizarlo y descomponerlo, como se describió en el punto 3.3.1.

4.1.2. Elección del módulo ZigBee

El protocolo ZigBee fue diseñado especialmente para aplicaciones domóticas, para equipos que sean accedidos de manera esporádica pero que necesiten una respuesta en tiempo real. Como se ha mencionado anteriormente, este protocolo no permite el uso de un gran ancho de banda pero sus módulos requieren un consumo mínimo de energía, lo cual es muy provechoso para nodos remotos que están alimentados por baterías o pilas. Además, puede coexistir con el protocolo WiFi, comúnmente usado para acceder a Internet inalámbricamente en el hogar u oficina.

[12]

ZigBee es un protocolo abierto para fines no comerciales, pero los principales módulos certificados por *ZigBee Alliance* (grupo de compañías que mantiene y publica este estándar) que engloban todas las funcionalidades del protocolo son los módulos XBee distribuidos por la empresa Digi.

Existen varias familias o variantes de módulos XBee, cada una orientada a una aplicación diferente. En el cuadro 1 se muestra las principales características de cada uno de estos. [13] Algunas de estas familias ofrecen una variante conocida como XBee-PRO. Esta versión permite un mayor alcance al costo de un mayor consumo de energía, y un mayor precio de venta.

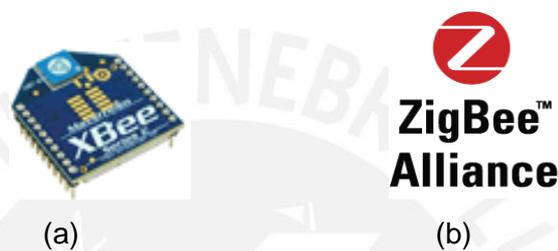


Fig. 11: (a) Módulo XBee (b) Logo de ZigBee Alliance
(Tomados de zigbee.org)

Cuadro 1: Comparación de características más importantes entre principales familias de XBee

Nombre	Frecuencia	Tipo de Red	Rango máximo (Pro)	Convertible a...
XBee 802.15.4	2.4GHz	Punto a multipunto	100m (1,6 Km)	XBee DigiMesh 2.4
XBee DigiMesh 2.4	2.4GHz	Malla	100m (1,6 Km)	XBee 802.15.4
XBee Pro 900	900 MHz	Punto a multipunto	9,6 Km	XBee DigiMesh 900
XBee DigiMesh Pro 900	900 MHz	Malla	9,6 Km	XBee 900
XBee XSC Pro	900 MHz	Punto a multipunto / Malla	24 Km	---
XBee ZNet 2.5 "Series 2"	2.4 GHz	malla	120m (1,6 Km)	XBee ZB
XBee ZB "Series 2"	2.4 GHz	malla	120m (1,6 Km)	XBee ZNet

Los módulos a usar serán los XBee 802.15.4 convencionales, ya que transmiten en la banda libre mundial de 2.4 GHz, son los más baratos y brindan todas las funciones básicas requeridas por el sistema a diseñar: topología de red punto a multipunto, modo transparente, comunicación vía UART y modos de ahorro de energía. Además, se dispone de estos módulos de antemano.

4.1.3. Elección del Microcontrolador

Una de las familias de microcontroladores más populares es la de los PIC, que aunque tiene versiones muy simples, existe también en variedades que contienen cierta variedad de periféricos y capacidades, como temporizadores y Modos de ahorro de energía. Por otro lado, ATmega es una familia de microcontroladores de propósito general que poseen diferentes periféricos, como temporizadores y canales PWM, y memoria Flash, EEPROM y SRAM. Además, tiene capacidades diversas como modos de ahorro de energía (*Sleep Modes*), comunicación serial vía USART (Receptor/Transmisor Síncrono/Asíncrono Universal), sistema de interrupciones internas y externas, entre otros. Algunos de los modelos de estas dos familias pueden llegar a ser parecidas y de similar precio, aunque normalmente los microcontroladores ATmega logran integrar mayor cantidad de periféricos en un mismo modelo. Debido a esto y a la familiarización que se tiene con este dispositivo, se usará una de las variantes de este grupo: el ATmega8, de 8 bits.

Las características de principal utilidad para la presente aplicación son [14]:

- **Comunicación vía UART** (Receptor/Transmisor Asíncrono Universal): El hecho de poseer USART lo hace compatible para comunicarse directamente con los módulos XBee vía UART. Ésta será la forma de comunicación principal que los módulos XBee tendrán con el exterior (no entre sí) en este proyecto.
- **Frecuencia de reloj:** Los pulsos que genera el protocolo Wiegand comúnmente son de 50 microsegundos y entre cada pulso suele haber un espaciamiento de 1 milisegundo. Esto quiere decir que el microcontrolador debe ser capaz de reconocer y procesar estos pulsos a una velocidad mayor a 20 KHz (1/50 us). El Atmega8 puede llegar a una frecuencia de reloj de hasta 16 MHz, así que cumple holgadamente este requisito.
- **Modos de ahorro de energía:** El ATmega8 posee 5 modos en los que apagando algunos módulos del microcontrolador genera un ahorro de

energía. Esta capacidad puede aprovecharse aún más en aplicaciones con nodos remotos que son alimentados con baterías o pilas.

- **Temporizadores e Interrupciones:** Estas características del ATmega8 hacen que la programación para esta aplicación sea más sencilla y se le puede dar un uso más óptimo.

La variante que se usará de este microcontrolador es el ATmega8L, el cual puede recibir un voltaje de alimentación en el rango entre 2.7 a 5.5 voltios DC; a diferencia del ATmega8 ordinario que solo permite un voltaje de alimentación desde 4.5 voltios. Esta capacidad es requerida en este sistema debido a que los niveles de voltaje de las entradas y salidas de los puertos Entrada/Salida (E/S) con los que trabaja el ATmega8 estándar son muy altos para ser compatibles directamente con el módulo XBee; en cambio, el ATmega8L puede ser alimentado con menor voltaje, y así, las características eléctricas de sus puertos E/S se vuelven compatibles con las de los puertos del módulo XBee.

La frecuencia de procesamiento del ATmega8L es de 8 MHz, y posee los mismos periféricos y comunicación USART que el ATmega8 estándar, así que cumple satisfactoriamente con los requerimientos del sistema.

En el cuadro 2 se encuentran resaltadas las características eléctricas de las salidas del XBee y de las entradas de los ATmega: Por un lado, el XBee entrega como salida de valor alto, un mínimo garantizado de 2.5 V; asimismo, se ve que el ATmega8 estándar reconoce como nivel alto en su entrada como mínimo un valor de 3V, en cambio el ATmega8L reconoce como nivel alto valores entre 1.8 y 3.5V.

Cuadro 2: Comparación de niveles de voltaje de los puertos E/S del módulo XBee, ATmega8L y ATmega8

	Vcc (rango máximo)	Vcc (propuesto)	Voltaje de entrada (V)				Voltaje de salida (V)			
			Nivel bajo		Nivel alto		Nivel bajo		Nivel alto	
			Min	Max	Min	Max	Min	Max	Min	Max
Xbee	2.8-3.4V	3 V	-	1.05	2.1	-	-	0.5	2.5	-
ATmega8L	2.7-5.5V	3 V	-0.5	1.2	1.8	3.5	-	0.6	2.2	-
ATmega8	4.5-5.5V	5 V	-0.5	2	3	5.5	-	0.9	4.2	-

Con esta comparación se puede concluir que aunque en algunos aspectos tanto el ATmega8, como el ATmega8L son compatibles con el módulo XBee, el ATmega8

estándar queda descartado como una opción válida para ser interconectado directamente con el módulo XBee, por lo que se optará por utilizar el ATmega8L.

La documentación del módulo XBee [15] no menciona nada acerca del valor máximo de voltaje que soportan los pines de entrada, pero sería recomendable que éste no sea mayor a $V_{cc}+0.5$ voltios (3.5 Voltios, para este caso).

4.1.4. Elección de estándar para interfaz con PC

El estándar RS-232 fue definido por la EIA (*Electronic Industries Alliance*) en 1969 y está ampliamente difundido en la industria de artefactos electrónicos y computacionales.

Aunque cada vez está siendo más desplazado por el estándar USB (*Universal Serial Bus*), el RS-232, especialmente en su versión de 9 pines (DB9), sigue vigente en muchos sectores. Debido a esto y a su facilidad de instalación y comunicación, en este proyecto se usará este estándar.



Fig. 12: (a) Puerto RS-232 DB9 (b) Cable adaptador RS-232/USB de TrendNet (Tomado de trendnet.com)

Actualmente, existen computadoras que ya no tienen incluido el puerto RS-232 D9 pero sí incluyen puertos USB. Para solucionar este problema se puede usar un cable adaptador de RS-232 a USB, el cual puede ser fácilmente encontrado en tiendas de electrónica.

4.1.5. Elección del MAX232

Las familias MAX200 y MAX400 son circuitos integrados que tienen la función de generar niveles de voltaje para estándar RS-232 o RS-485, respectivamente, a partir de una entrada TTL/CMOS (función “*driver*”) y de generar una salida TTL/CMOS a partir de una entrada con los niveles de voltaje de dichos estándares (función “*receiver*”). La familia MAX3000 es similar a la MAX200 pero permite

trabajar con mayor rango de voltajes TTL/CMOS. En todos los casos anteriores al pasar por estos circuitos, la lógica de la señal cambia de nivel, como si pasara por una compuerta negadora.

Debido a que se necesita realizar una comunicación entre XBee (TTL) con la PC (RS-232), se eligió un circuito de la familia MAX3000, el cual posee dos drivers y dos receivers para entablar la comunicación con dos hilos de ida (Dout y RTS - *Request-to-send*) y dos hilos de vuelta (Din y CTS - *Clear-to-send*): el MAX3232. Este circuito puede trabajar con niveles de voltaje TTL/CMOS desde 3 voltios (compatible y recomendable para comunicación con módulos XBee) y niveles de voltaje RS-232 de hasta +/- 12 voltios.

Los circuitos MAX3232 no son muy comerciales, por lo cual en las pruebas se optó por un similar: el MAX232. Éste es prácticamente igual que el MAX3232 pero trabaja con voltajes TTL de 5 voltios. Debido a esto, después de pasar por el MAX232 los niveles de voltaje han sido adaptados para no dañar el módulo XBee. Esta reducción de voltaje puede realizarse mediante el uso de un divisor de voltaje con dos resistencias. Con esto el voltaje de entrada de 5 voltios se verá reducido mediante la siguiente fórmula:

$$V_o = 5 V \times \left(\frac{R_1}{R_1 + R_2} \right)$$

Lo cual deberá resultar en un aproximado entre 2,9 y 3,4 voltios para valores de nivel alto, lo cual sí sería compatible con el módulo XBee.

4.2 Esquema del Sistema de Control de Acceso en base a los dispositivos elegidos

Ya habiendo elegido los componentes principales del sistema, se puede describir más en detalle el diagrama de bloques de la Figura 10, a través del esquema de la Figura 13. En cada nodo remoto, la señal en protocolo Wiegand necesitará ser adaptada eléctricamente, para ser tratada en el ATmega8L, el cual se comunicará vía UART con un módulo XBee. Además, este ATmega8 también emitirá la señal de respuesta recibida del servidor.

En el nodo principal, el módulo XBee administrador recibirá la señal de los nodos remotos y la enviará al servidor mediante un MAX232 y un cable serial RS-232, el cual adaptará los niveles de voltaje. El servidor revisará los permisos en una base de datos y se comunicará de regreso con el módulo XBee, pero en este sentido de

la comunicación, el MAX232 requerirá circuitería adicional, como explicado en el punto 4.1.5.

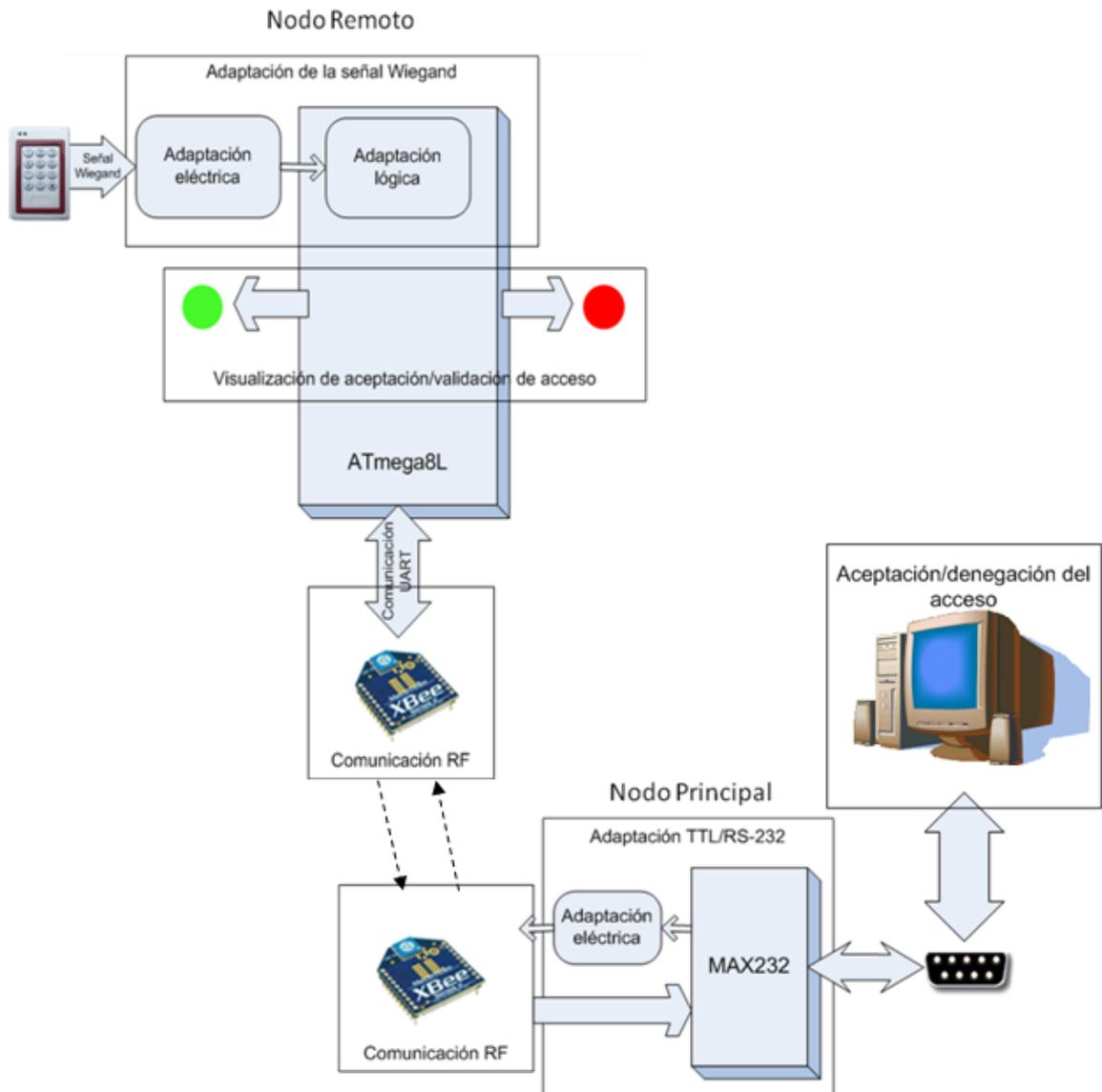


Fig. 13: Esquema del Sistema de Control de Accesos

4.3 Diseño de los circuitos que forman parte del Sistema de Control de Acceso

4.3.1 Diseño del circuito de un nodo remoto

El diseño de este nodo está compuesto por una lógica de tres etapas principales: la etapa de adaptación de la señal en protocolo Wiegand, dada por las compuertas lógicas inversoras 7400 y el Atmega8L; la etapa de comunicación por

Radiofrecuencia dada básicamente por el módulo XBee y su conexión con el ATmega8L; y la etapa de visualización de la aceptación/denegación del acceso, dada por el ATmega8L los diodos LED y las resistencias de 200Ω . La alimentación de este circuito será de $3 V_{DC}$.

a) Etapa de adaptación de la señal en protocolo Wiegand

Esta etapa recibirá de un circuito externo la trama en protocolo Wiegand mediante 3 líneas, D0 (WIEGAND-1), D1 (WIEGAND-2) y la línea de tierra común (WIEGAND-3). Las líneas D0 y D1 tendrán un voltaje de $5 V_{DC}$ por lo cual éste debe ser adaptado para no malograr el microcontrolador. Esto se hará con el uso de las compuertas inversoras 74LS00. Se debe usar específicamente este código de componente porque otros como el 74HC00 se pueden malograr al recibir una entrada con un nivel de voltaje mayor al de su voltaje de alimentación. Sin embargo, el 74LS00 sí puede, y con esto se ahorra el espacio que se necesitaría para usar dos fuentes diferentes de voltaje y más componentes para disminuir el voltaje.

b) Etapa de comunicación por Radiofrecuencia

El módulo XBee estará configurado para transmitir todo lo que le sea enviado desde el ATmega8L vía UART. La conexión entre ambos dispositivos será directa, como ha sido sustentado previamente en el punto 4.1.3. El módulo XBee deberá ser programado previamente para poder enviar y recibir información del XBee del nodo principal y podría ser configurado para operar en bajo consumo de energía cuando el ATmega8L se lo comande.

c) Etapa de visualización de la aceptación/denegación del acceso

Esta etapa se encargará de recibir y expresar la respuesta del nodo principal – transmitida mediante los módulos XBee hacia el ATmega8L- para decidir si se acepta o no la petición de acceso. Esta respuesta se procesará en el microcontrolador, el cual emitirá un nivel de voltaje alto en el pin del LED correspondiente, generando aproximadamente:

$$\frac{2.2 V - 1.5 V}{200 \Omega} = 3.5 mA$$

...lo cual es suficiente para poder apreciar la luminosidad del diodo LED.

La respuesta se expresará mediante la activación de un LED verde, en caso se acepte el acceso o la activación de un LED rojo, en caso de deniegue el acceso. En una implementación real, el pin del LED verde debería ser conectado a un circuito de potencia que accione un receptor eléctrico o un electroimán para la apertura de

la puerta y a una bocina simple que haga sonar el típico zumbido que avisa al usuario de la apertura.

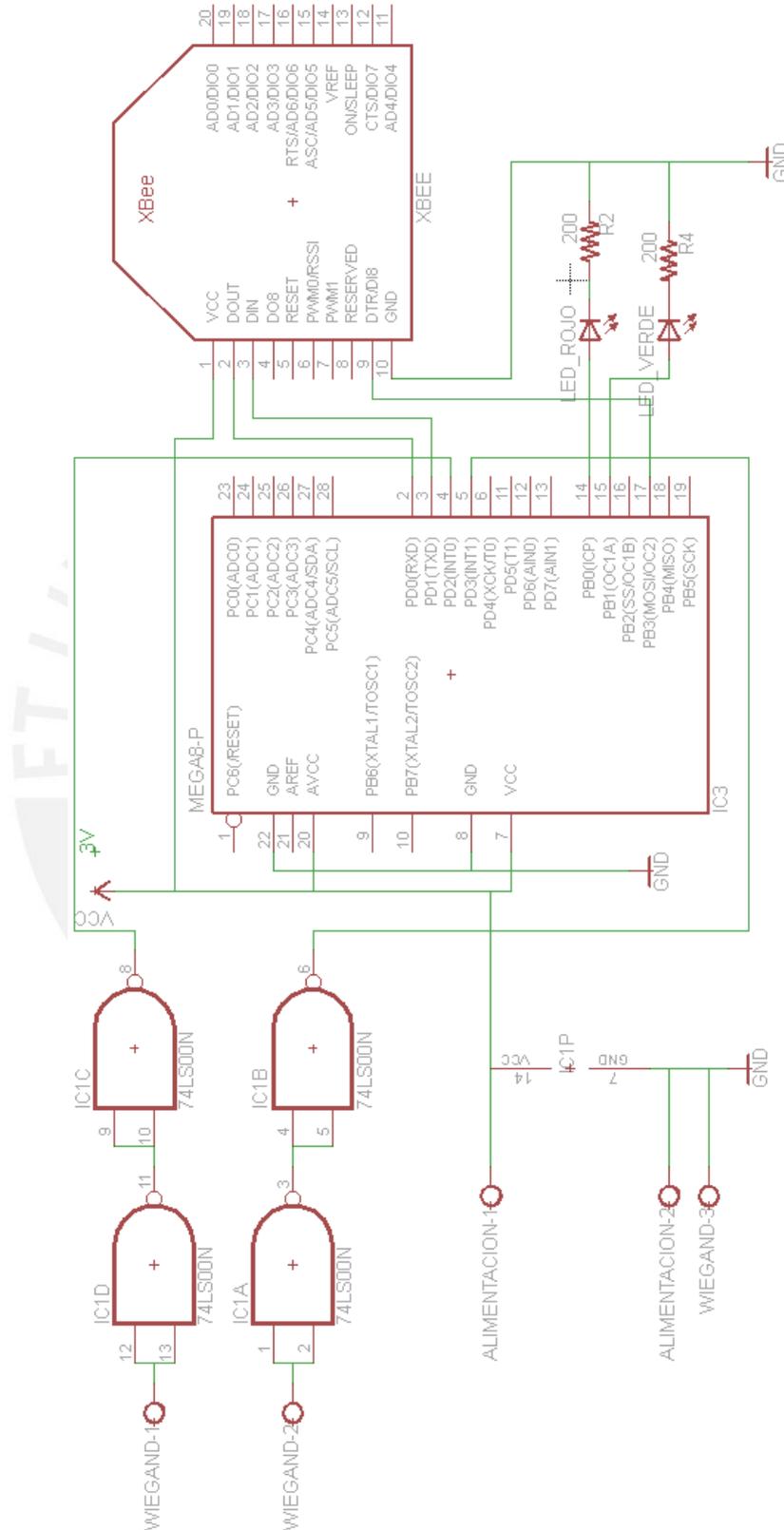


Fig. 14: Diagrama esquemático de un nodo remoto

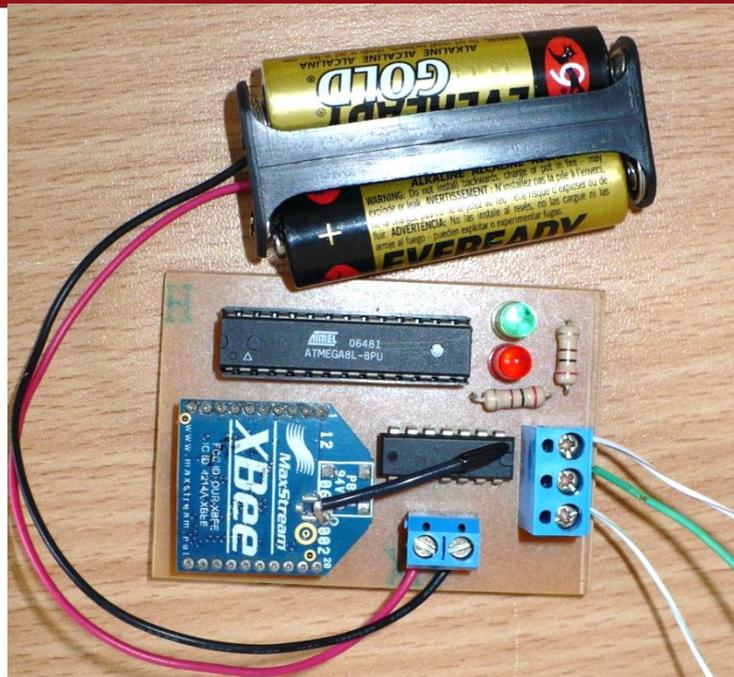


Fig. 15: Imagen de un nodo remoto implementado

4.3.2 Diseño del circuito del nodo principal

El nodo principal está compuesto por dos etapas principales: la etapa de comunicación por radiofrecuencia, dada por el módulo XBee, y la etapa de adaptación de señal de TTL/CMOS a RS-232 DB9 y viceversa, dada por el MAX232 y el resto de componentes. La alimentación a este circuito será de 3V (para el módulo XBee) y de 5V (para el MAX232).

a) Etapa de comunicación por Radiofrecuencia

El módulo XBee será el encargado de generar la comunicación por Radiofrecuencia, similarmente que en los nodos remotos, y también deberá ser programado con anterioridad. La comunicación con el exterior también se hará a través de sus pines 2 y 3, es decir, vía UART. Este módulo XBee no podrá entrar a modo de bajo consumo de energía porque será el módulo principal o administrador.

b) Etapa de Adaptación TTL – RS-232

La adaptación de señales estará a cargo del MAX232, que requerirá de los 4 condensadores electrolíticos de 1 μF , como lo recomienda el fabricante para su óptimo funcionamiento. La comunicación saldrá hacia un conector RS-232 DB9 hembra, por lo que se necesitará un cable serial para conectarse a la PC.

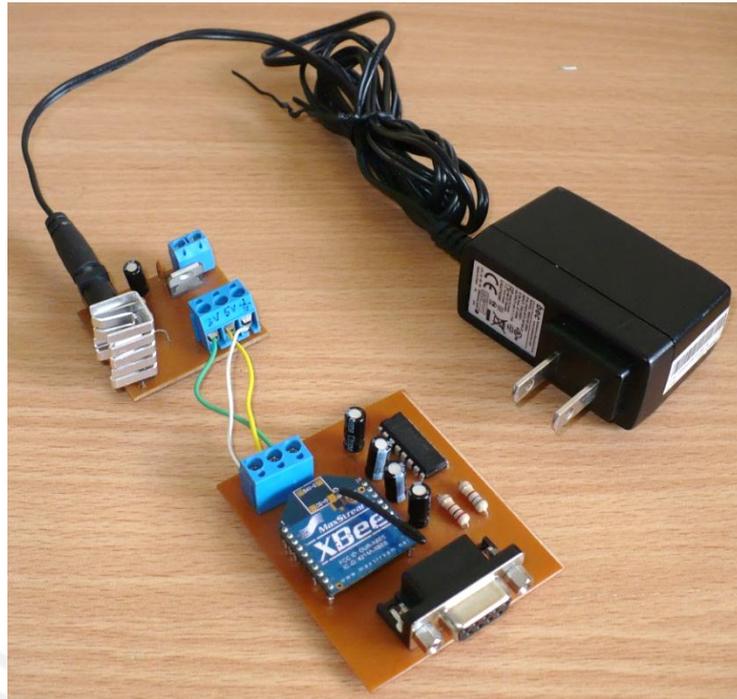


Fig. 17: Imagen del nodo Principal implementado junto con su alimentación

4.4 Lógica de comunicación de los Módulos XBee

4.4.1 Explicación de la lógica de funcionamiento

Los módulos XBee están pre-configurados para operar en Modo Transparente; cuentan con otros modos de comunicación, pero éste es el requerido para esta aplicación. Este modo consiste en que la comunicación entre dos dispositivos pueda realizarse de igual forma conectándolos directamente uno con otro, que inalámbricamente, conectado cada uno a un módulo XBee; es decir, los dispositivos XBee en conjunto actuarían como un cable. Todo dato que ingrese al pin de entrada del módulo XBee transmisor llegará al pin de salida del módulo XBee receptor.

Dentro de este modo existen 2 formas de comunicación:

- *Unicast.*- Permite comunicación punto a punto. La dirección de destino es la dirección “personal” del módulo de destino.
- *Broadcast.*- Permite que un módulo se comunique con todos los módulos de la red, es decir comunicación punto-multipunto.

En este caso, el módulo coordinador, ubicado en el nodo principal, se configurará bajo *Broadcast*, y recibirá la información que le mande cada nodo remoto en todo

momento; mientras que cada módulo en nodo remoto será configurado bajo *Unicast*, teniendo como destino el nodo coordinador.

4.4.2 Configuración de los Módulos XBee

El programa X-CTU es brindado gratuitamente por la compañía Digi, distribuidora de los módulos XBee. Ofrece una fácil visualización del estado del módulo conectado a la computadora, da información acerca de la comunicación que se está realizando en tiempo real y también sirve para reconfigurar o actualizar bajo nuevo Firmware los módulos XBee. En la Figura 18 se muestra la sección de este programa en la que se configuran los módulos, y se puede ver las principales opciones. Algunas de estas opciones deben ser configuradas para este sistema y esto se explicará de forma muy básica en las siguientes páginas. Para mayor detalle se puede revisar el manual de configuración de los módulos XBee. [16]

Se considera que para la configuración del módulo XBee a través de la PC, éste deberá estar conectado a uno de los Kits de Desarrollo distribuidos por Digi o al nodo principal, que tiene conexión con la PC y ofrece las conexiones mínimas necesarias a los pines del módulo XBee para realizar configuraciones. Ambas opciones pueden ser conectadas a la PC a través de un cable serial RS-232 DB9 o, si es un kit adecuado, a través de un cable USB. Si se está usando Windows Vista o Windows 7 con USB, adicionalmente al controlador del adaptador RS232-USB, debe instalarse un controlador localizado en:

>> <http://www.ftdichip.com/Drivers/VCP.htm> [17]

La versión 2.06 de éste se encuentra anexada a este documento.

a) Programación del módulo del Nodo principal

Este nodo será configurado para *Broadcast* hacia los Nodos remotos, y estos son los pasos a seguir para programarlo adecuadamente:

- Conectar el módulo al kit de desarrollo o al nodo principal, y conectar éste a su alimentación eléctrica, y luego a la PC.
- En el X-CTU, ubicarse en la sección “*Modem Configuration*” y hacer *click* en “*Read*” para ver los parámetros y luego en “*Show defaults*”. El modo Transparente estará configurado por defecto.
- Asignar los siguientes valores a los parámetros indicados:
 - MY = 0 – dirección del nodo principal.
 - DH = 0 , DL = 0xFFFF -- dirección de destino serán todos los otros nodos.

- CE = 1 -- se indica que éste es el módulo coordinador.
- SC = 0x0C -- número de canales que se sondearán en las búsquedas de PAN ID (redes inalámbricas locales) y canales. Si se usa módulos XBee estándar, son 16 canales, y para XBee-Pro son 12 canales.
- SD = 4 -- indica que durante $12^* (2 \wedge SD) * 15.36\text{ms}$ el módulo seleccionará el canal de radiofrecuencia con menos energía y un número de red (PAN ID) que no esté siendo usada.
- A1 = 0 -- Siempre es '0' para módulos coordinadores.
- A2 = 7 -- Habilita las búsquedas de canal RF y de PAN ID, y que otros módulos puedan unirse a la red de este coordinador.
- PL = 4 – Highest -- Configura el máximo nivel de energía para que las transmisiones que realice este módulo tengan el mayor alcance posible.
- SM = 0 -- Sirve para elegir un modo de bajo consumo de energía, pero los módulos coordinadores no pueden acceder a ellos.
- ST = 1 -- Tiempo en milisegundos antes de activarse el modo de bajo consumo de energía en los nodos remotos.
- SP = 0x64 -- Tiempo que permanecerán en bajo consumo los nodos remotos (1 seg).
- BD = 2 – 4800 -- Configurado a 4800 baudios para comunicación serial (UART).
- RO = 0 -- El módulo enviará cada byte apenas le llegue a su línea de entrada de UART, sin acumularlos en su buffer.

- Hacer click en “Write” para grabar los parámetros en el módulo

b) Programación del módulo de un Nodo remoto

Será configurado para *Unicast* y tendrán como destino el Nodo principal:

- Conectar el módulo al kit, y conectar éste a alimentación y a la PC
- En X-CTU hacer *click* en “Read” para ver los parámetros y en “Show defaults”.
- Asignar los siguientes valores a los parámetros indicados:
 - MY = cualquiera menos 0 y diferente en cada nodo – dirección propia del nodo. Se le asignará 1 y 2 a los módulos de la puerta ‘1’, 3 y 4 a los de la puerta ‘2’ y, 5 y 6 a los de la puerta 3 (según la Figura 4 del Capítulo 1). Los números impares serán para los módulos de entrada y los pares para los módulos de salida.

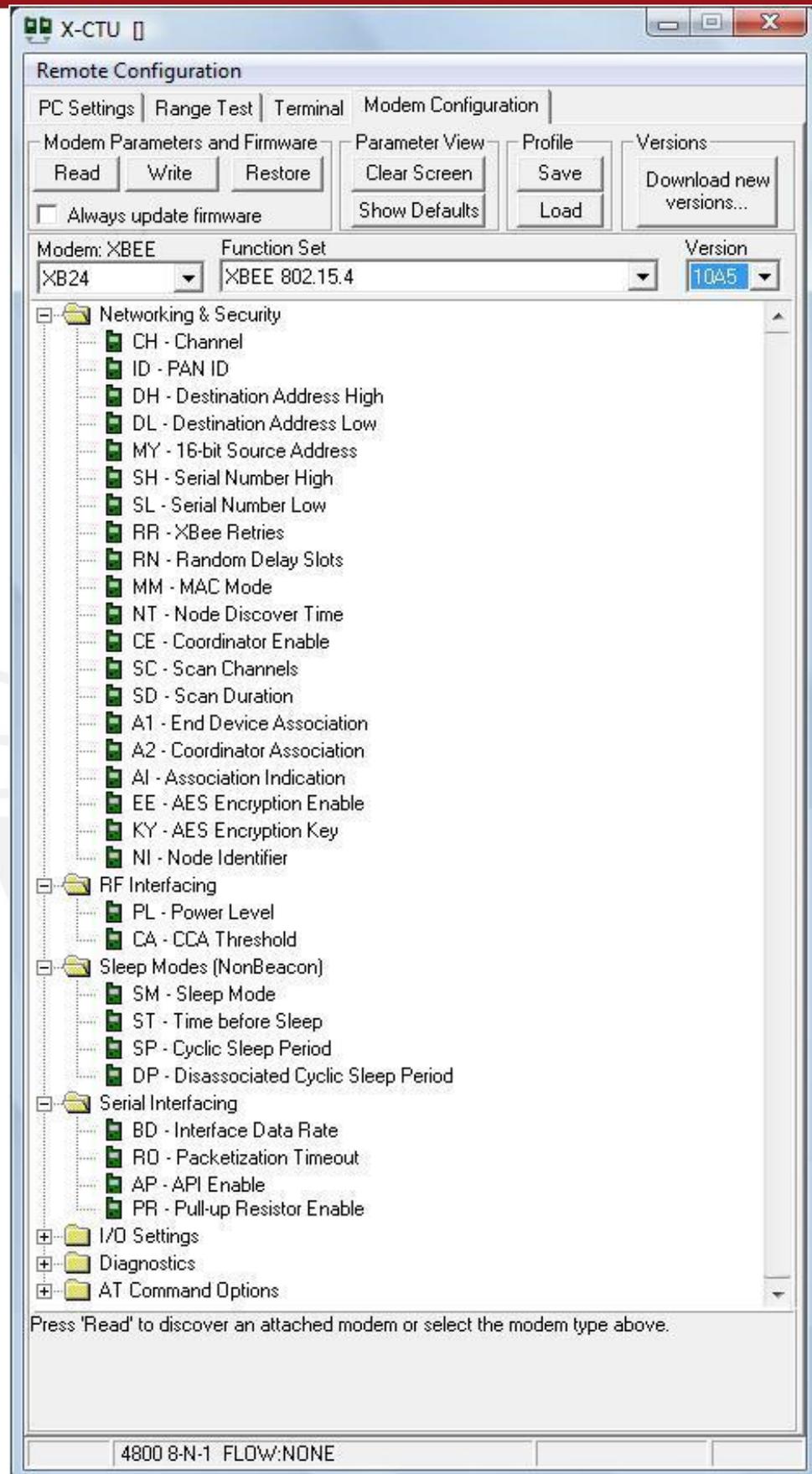


Fig. 18: Sección “Modem Configuration” del Programa X-CTU

- DH = 0 , DL = 0 -- dirección de destino será el nodo principal.
 - CE = 0 -- Estos módulos no son coordinadores.
 - SC = 0x0C -- número de canales que se sondearán en las búsquedas de PAN ID y canales. Si se usa módulos XBee estándar, son 16 canales, y para XBee-Pro son 12 canales.
 - SD = 4 -- Indica que durante un tiempo igual a $SC * (2 \wedge SD) * 15.36ms$ el módulo remoto buscará el módulo coordinador adecuado para asociarse a él.
 - A1 = 15 -- Configura el módulo para que busque una red y un coordinador a los cuales asociarse y, además, que cuando sea activado por hardware, busque datos pendientes en el coordinador.
 - A2 = 0 -- Siempre es '0' para módulos no coordinadores.
 - PL = 4 – Highest -- Configura el máximo nivel de energía para que las transmisiones que realice este módulo tengan el mayor alcance posible.
 - SM = 5 -- Configura cada módulo remoto con el modo de bajo consumo llamado “*Cyclic Sleep Remote with Pin Wake-Up*”, el cual determina que el módulo se “dormirá” ST milisegundos después de dejar de transmitir o recibir data y se “despertará” cada SP centésimas de segundo y cada vez que reciba un pulso negativo por uno su pin 9 (en este caso, a través del ATmega8L).
 - ST = 1 -- Tiempo en milisegundos antes de activarse el modo de bajo consumo de energía en los nodos remotos.
 - SP = 0x64 -- Tiempo que permanecerán en bajo consumo (1 seg)
 - BD = 2 – 4800 -- Configurado a 4800 baudios para comunicación serial (UART).
 - RO = 0 -- El módulo enviará cada byte apenas le llegue a su línea de entrada de UART, sin acumularlos en su buffer.
- Click en “Write” para grabar los parámetros en el módulo.

4.5 Pruebas

A continuación, se muestra una explicación de las principales pruebas a las que se sometió el sistema diseñado, para corroborar el correcto funcionamiento de cada una de sus etapas.

4.5.1. Envío de datos por protocolo ZigBee

El objetivo de esta prueba es la familiarización con el programa X-CTU y probar el envío y recepción de datos de un módulo conectado a una PC y otro módulo conectado a otra PC, por medio de los Kits de desarrollo.

Lo primero será configurar los módulos a través del X-CTU: Primero, se abrirá la sección *PC Settings* para cerciorarse de que ambos nodos están configurados con los mismos parámetros UART. Se tomará los parámetros 4800 baudios, sin paridad (N) y 1 bit de parada.

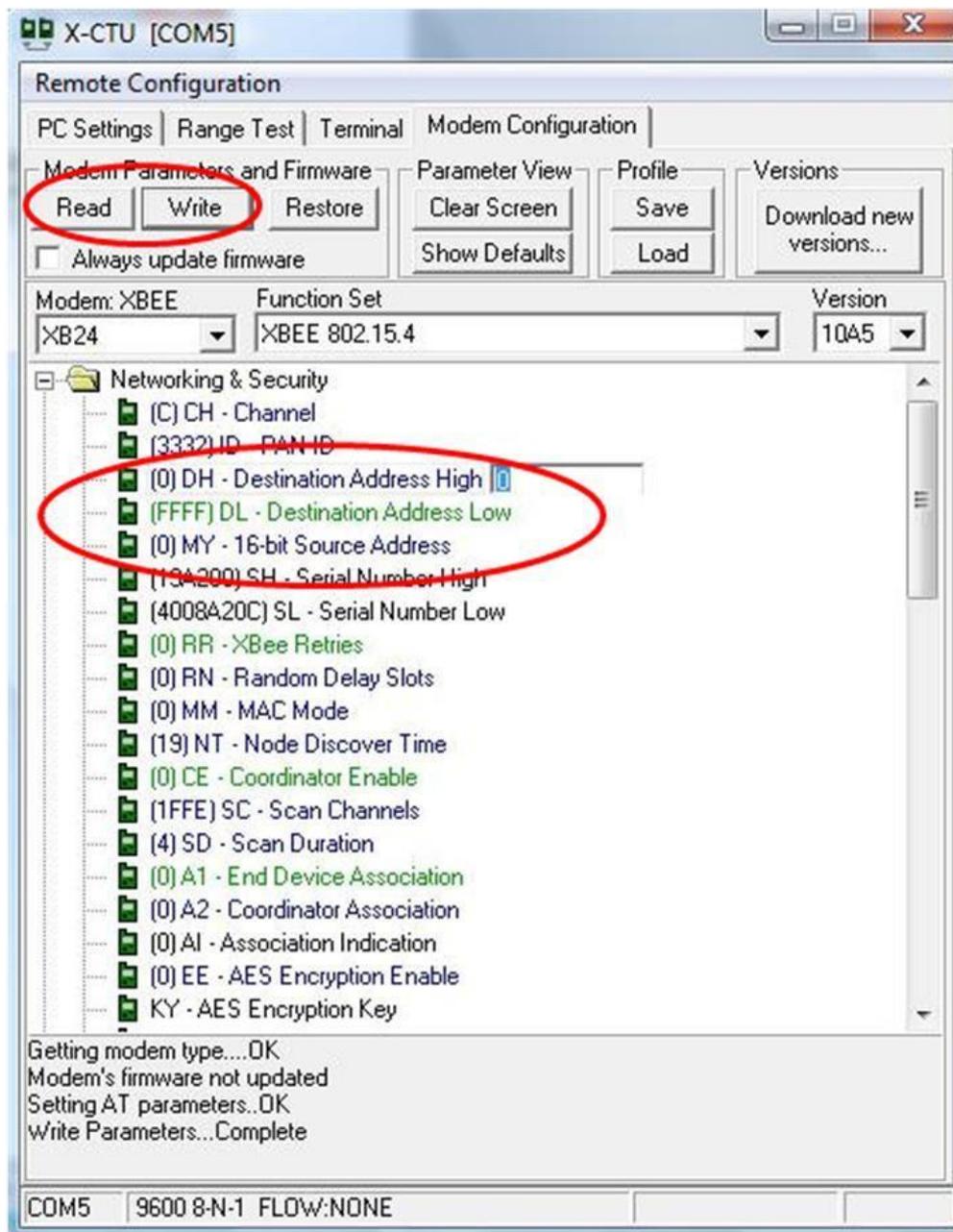


Fig. 19: Datos configurados en el nodo Principal

El nodo “principal”, configurado en *Broadcast*, se observará en la ventana de estilo Windows Vista, color claro; y el nodo remoto, configurado en *Unicast* hacia el nodo “principal”, se le diferenciará en la ventana estilo Windows XP, con bordes azules.

Luego, se procederá a configurar un módulo XBee como nodo principal con los pasos explicados en el punto 4.4.2. Notar, como se muestra en la Figura 19, que el módulo principal será configurado con dirección MY=0 y se comunicará con “todos” los módulos (*Broadcast*).

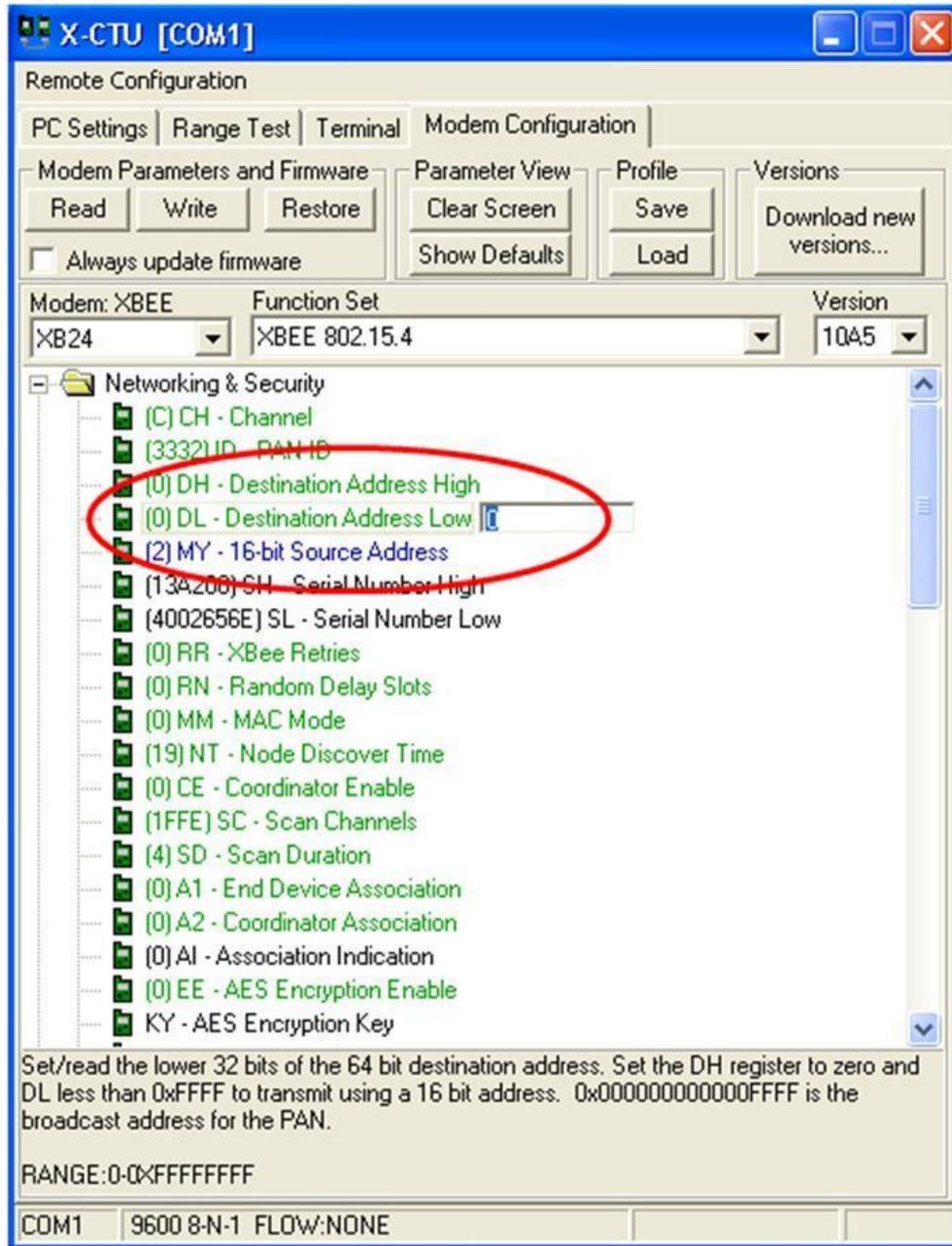


Fig. 20: Datos configurados en el nodo Remoto

Después se configurará un nodo remoto, también según las instrucciones correspondientes en el punto 4.4.2 quedando como resultado lo que se ve en la Figura 20. Notar que este módulo tiene como dirección MY=2 y se comunicará solo con el nodo con MY=0, es decir el módulo principal (*Unicast*).

A continuación se procederá a abrir la sección Terminal en ambos nodos y a transmitir mensajes. Los mensajes transmitidos se ven de color azul y los recibidos de color rojo.

Notar que cuando se configura los valores SD, A1 y A2, como en este caso, primero debe inicializarse el nodo principal, y luego de unos segundos recién los nodos remotos, para dar tiempo al nodo principal para configurar la red, a la que los nodos remotos se asociarán.

Se procede a enviar un mensaje ('*hola*') desde el nodo principal:

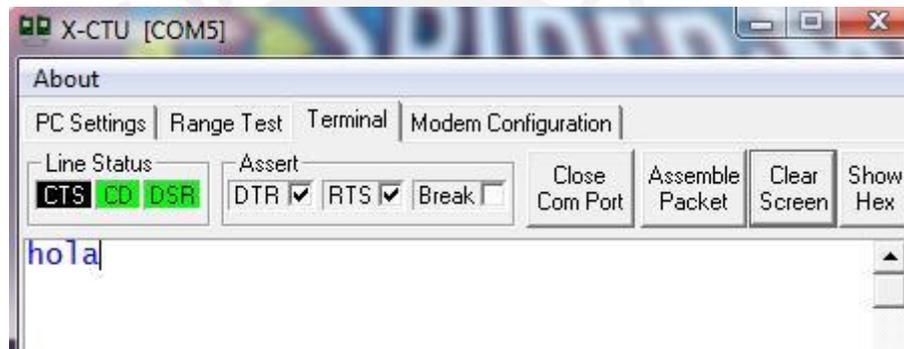


Fig. 21: Mensaje enviado desde el nodo Principal

Se observa que llega a ser recibido desde el nodo remoto:

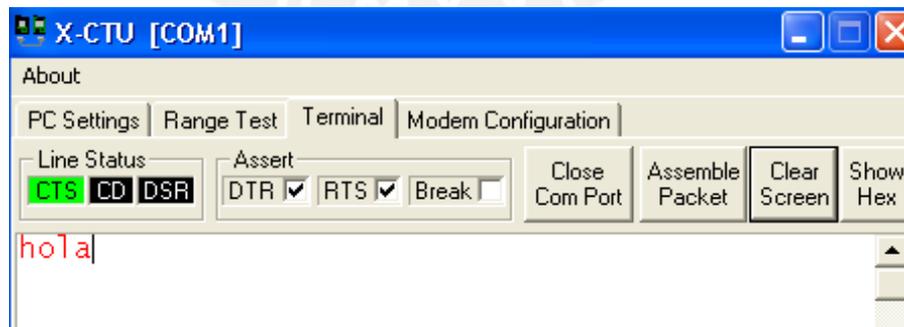


Fig. 22: Mensaje recibido en el nodo Remoto

Con esto se demuestra que la transmisión por *Broadcast* ha sido exitosa. Ahora el nodo remoto responderá al nodo principal por *Unicast*.

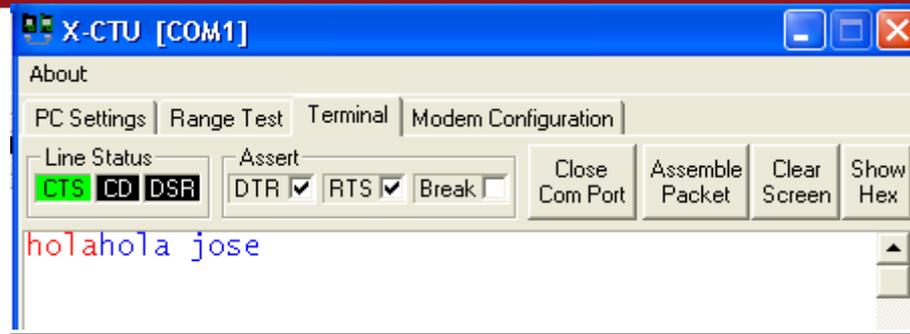


Fig. 23: Mensaje enviado desde el nodo Remoto

Y se observa el mensaje recibido desde el nodo principal:

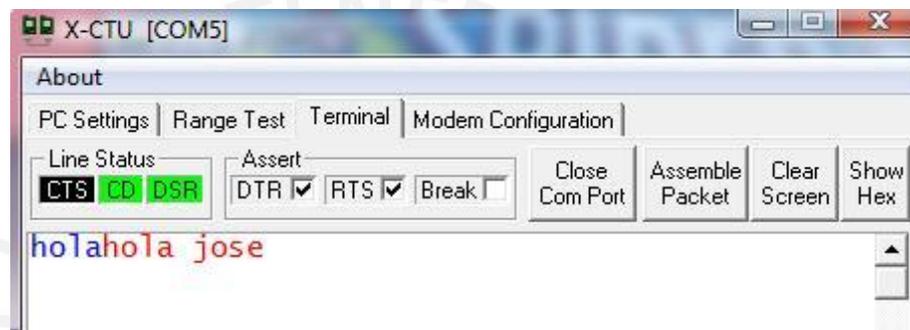


Fig. 24: Mensaje recibido en el nodo Principal

Así, se corrobora el éxito de la comunicación en ambos sentidos vía *Broadcast* y *Unicast*.

4.5.2. Generador de trama Wiegand

El sistema real usaría lectoras Wiegand, pero no se contó con éstas para las pruebas, así que se hizo un circuito que genera tramas en protocolo Wiegand de 26 bits a partir de un teclado matricial, simulando el funcionamiento de una lectora real.

La trama Wiegand que se muestra en la Figura 25 será generada mediante el simulador de señales del programa VMLab. Para este ejemplo, el código identificador de la lectora Wiegand será 151 decimal, el cual se expresa como 10010111 en 8 bits, y en el teclado se ingresará el código del usuario, que en este caso será 1234 hexadecimal (cada número ingresado por el teclado matricial se expresó con 4 bits cada uno), expresado en binario como 0001001000110100 (16 bits). Como se explicó en el punto 3.3.1, el primer y último bits son de paridad.

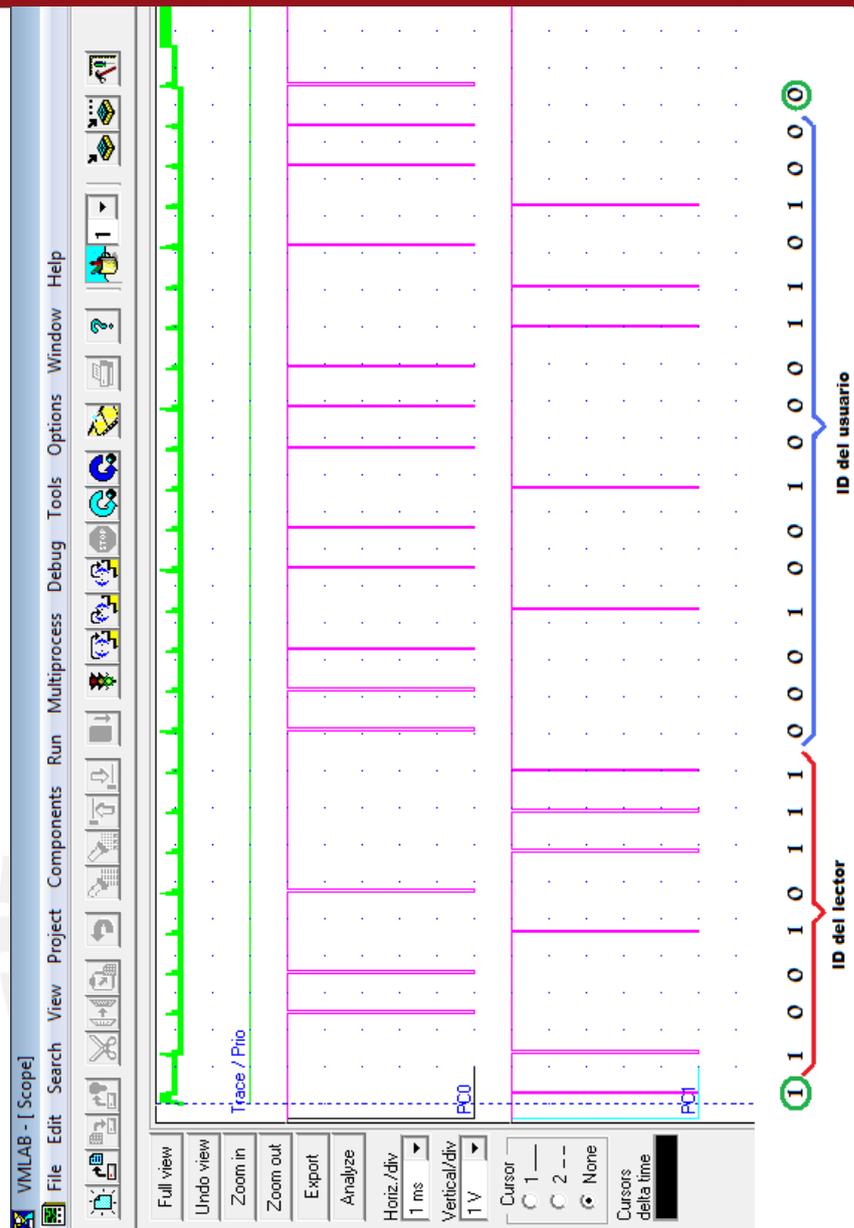


Fig. 25: Trama Wiegand generada en VMLab

El circuito que genera esta señal sería simplemente un ATmega8 alimentado con 5 voltios, que tendría como entrada el teclado matricial y como salidas, dos de sus pines (PC0 y PC1) que funcionarían como las líneas D0 y D1, como también explicado en el punto 3.3.1. La tierra debe ser común. Se puede observar en la Figura 25 que, como en protocolo Wiegand convencional, las líneas están continuamente en nivel alto, y los pulsos negativos en PC0 y PC1 son los que dan la información.

Por otro lado, la longitud mínima de cada pulso debe ser de 50 us y en la Figura 26 esto se cumple, ya que se observa que la diferencia entre los cursores es de 53 us.

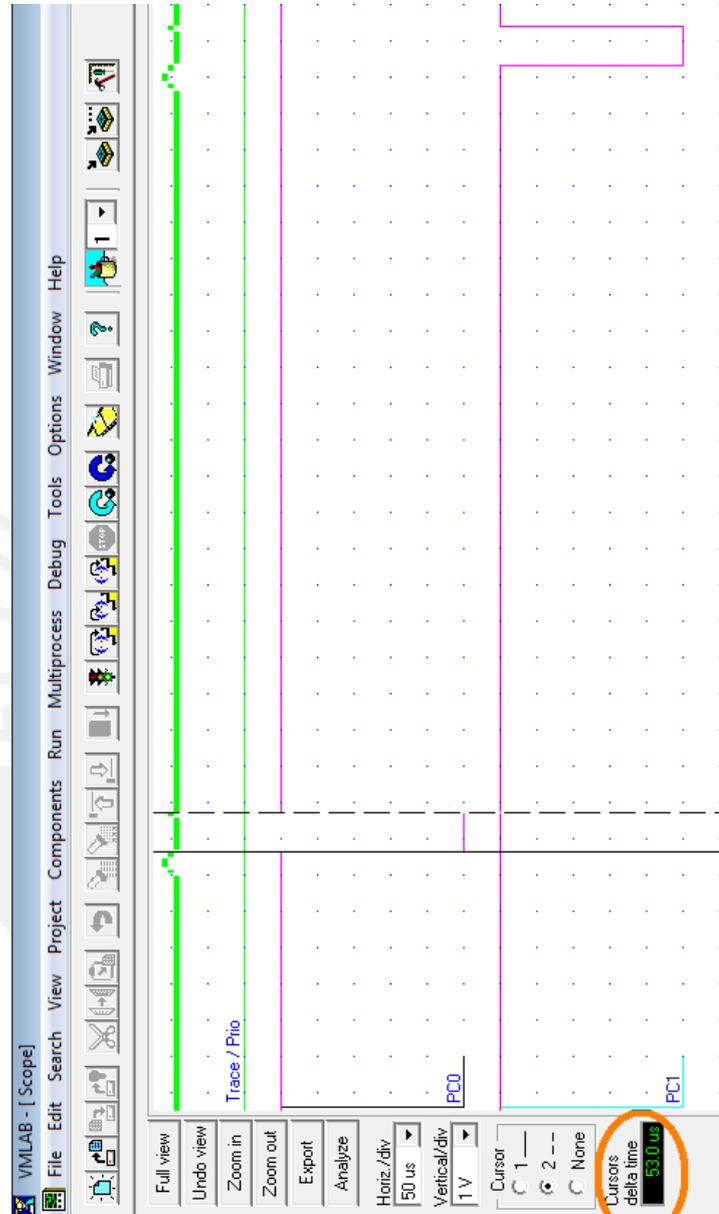


Fig. 26: Longitud de pulso de la Trama Wiegand generada

La separación entre cada pulso debe ser mínimo de 1ms, como se dijo en el punto 3.3.1, y esto se observa en la Figura 27.

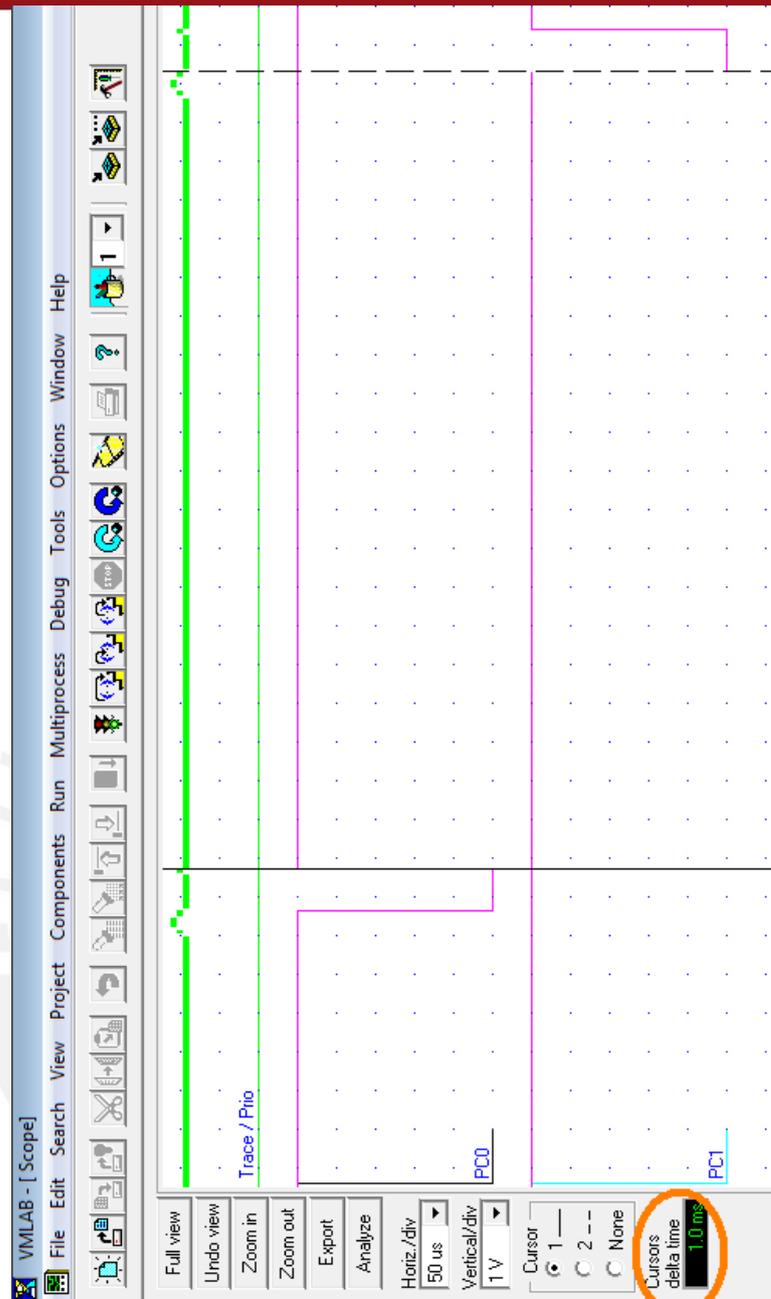


Fig. 27: Periodo entre pulsos de la Trama Wiegand generada

Con lo visto en estos gráficos se demuestra que la trama generada podrá cumplir con la sustitución de un lector Wiegand convencional para efectos de pruebas.

4.5.3. Comunicación inalámbrica de la trama Wiegand *decodificada*

En esta prueba se tomó la misma señal de 26 bits generada en la prueba anterior como entrada del sistema en el nodo remoto configurado en la primera prueba, el microcontrolador extrajo la información, y transmitió la información inalámbricamente hacia el nodo principal. La información extraída que saldría del

nodo remoto se observó simulando el funcionamiento del microcontrolador con el software VMLAB:

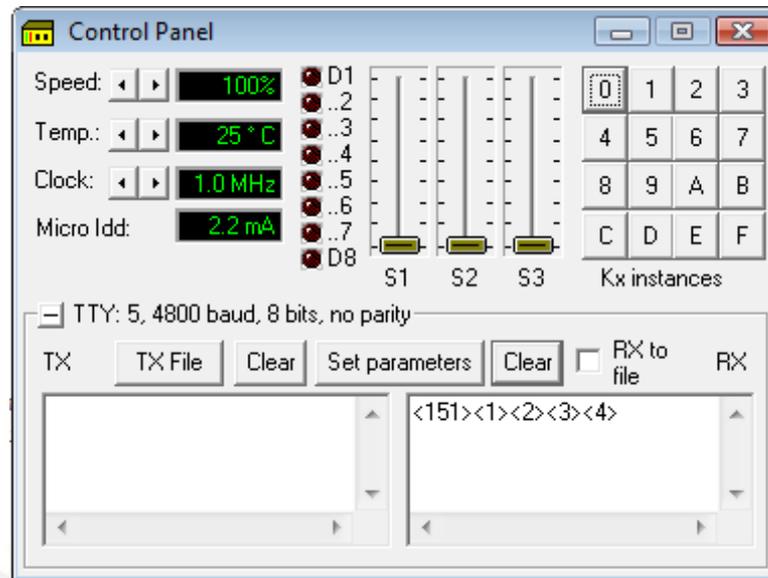


Fig. 28: Simulación de los datos enviados desde el nodo remoto

En la Figura 28 se puede observar que se transmiten 5 bytes. El primer byte nos da el número o código del lector de control de acceso (o nodo remoto), que en este caso es '151'. Los siguientes 4 bytes expresan cada dígito del código que identifica al usuario (UserID) que está solicitando acceso a través de dicha lectora. Los bits de paridad de la trama fueron removidos por el microcontrolador, que recibe la señal Wiegand en el nodo remoto.

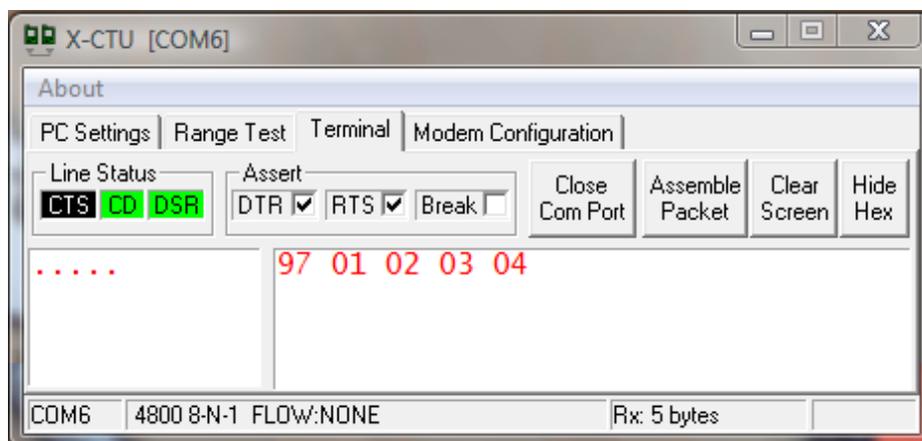


Fig. 29: Datos recibidos en ventana del servidor usando el X-CTU

Estos datos serán recibidos en el nodo principal (o coordinador) y serán usados para consultar una base de datos y determinar si se otorga o deniega el acceso. El resultado se puede ver en la ventana terminal del X-CTU. Además, a través de esta misma ventana, se puede ingresar una trama adecuada por la ventana “Terminal” para activar el led rojo o el led verde en el nodo remoto, como señal de respuesta.

En la imagen de la Figura 29 se observa que el X-CTU ha recibido (en rojo) los 5 bytes de la trama y los muestra en hexadecimal: “97 01 02 03 04”. El número 151 en decimal se representa como 97 en hexadecimal.

En el CD anexo a este documento se incluye un video que permite observar la realización de esta prueba, en la cual el servidor recibe la data y devuelve una respuesta al nodo remoto manualmente a través de una interfaz gráfica diseñada en Visual Basic. Esta interfaz sirvió como herramienta para realizar la prueba, pero no se incluye en el sistema final, ya que éste requiere respuestas generadas automáticamente y son invisibles para el usuario.

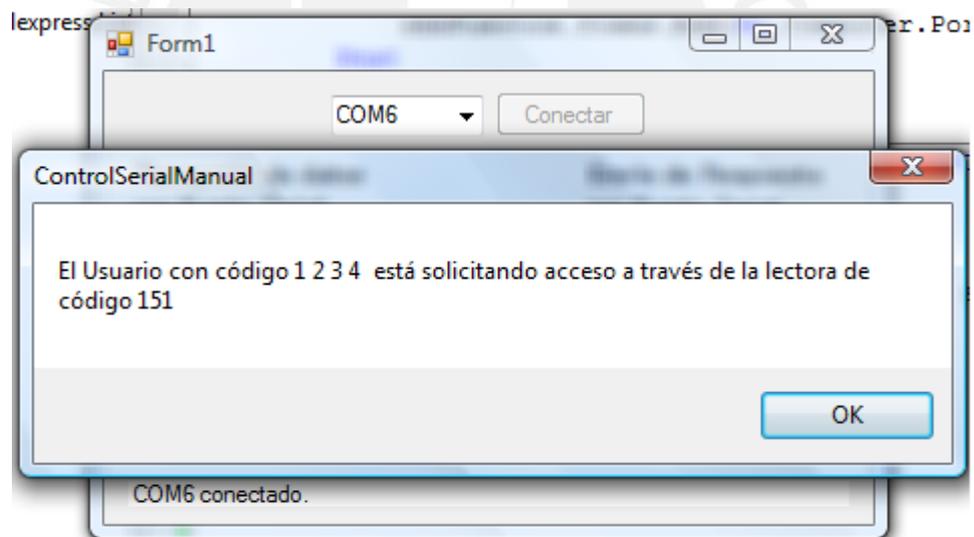


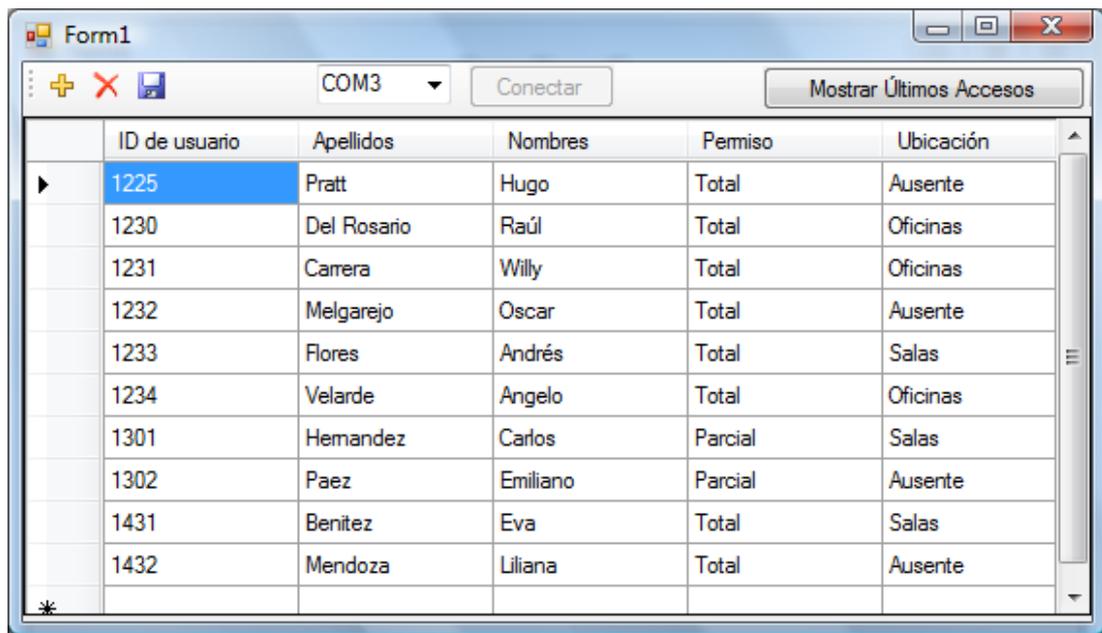
Fig. 30: Datos recibidos en ventana del servidor mediante una aplicación de Visual Basic llamada “ControlSerialManual”

4.5.4. Interfaz en el Servidor

Cada solicitud de ingreso a cualquiera de las puertas, llega al servidor donde una aplicación en Visual Basic procesará la información y a través de una base de datos en SQL, revisará si se otorga o no el ingreso.

Dependiendo de la aplicación y de la información que el usuario o administrador quiera rescatar del sistema, se puede construir una interfaz que le brinde esas facilidades.

El modelo de aplicación en Visual Basic que ha sido creada, ofrece una interfaz que permitirá conocer en qué área se encuentra cada usuario o si no está. También se permitirá ver un historial de las solicitudes de ingreso con las horas y fechas, y modificar la base de datos para ingresar o eliminar usuarios, y para modificar los permisos de ingreso de cada uno.



ID de usuario	Apellidos	Nombres	Permiso	Ubicación
1225	Pratt	Hugo	Total	Ausente
1230	Del Rosario	Raúl	Total	Oficinas
1231	Carrera	Wily	Total	Oficinas
1232	Melgarejo	Oscar	Total	Ausente
1233	Flores	Andrés	Total	Salas
1234	Velarde	Angelo	Total	Oficinas
1301	Hernandez	Carlos	Parcial	Salas
1302	Paez	Emiliano	Parcial	Ausente
1431	Benitez	Eva	Total	Salas
1432	Mendoza	Liliana	Total	Ausente

Fig. 31: Interfaz del usuario en nodo Central o Coordinador mediante la aplicación ControlSerialAuto en Visual Basic

Se plantea que cada usuario tenga una tarjeta que lo identifique en el sistema mediante una “ID de Usuario”. Cada vez que exista un nuevo usuario (por ejemplo, un nuevo profesor o un visitante), la persona encargada con función de Administrador (por ejemplo, la secretaria) le entregará una tarjeta con un código, ingresará este nuevo código al sistema, junto con los datos del nuevo usuario, así como el permiso que tendrá; la ubicación por defecto será “Ausente”. El permiso “Total” le dará acceso a todas las puertas, mientras que el permiso “Parcial” solo le permitirá entrar y salir del ambiente de salas de reuniones, ubicado entre la puerta de vidrio y la puerta de madera (área roja de la Figura 4). Si se extravía una tarjeta, se puede simplemente eliminar a ese usuario de la base de datos, o también se puede otorgar mayor o menor permiso a un usuario en cualquier momento, desde esa misma ventana.

Adicionalmente, se puede observar un cuadro con los últimos ingresos, para que el Administrador del sistema pueda extraer datos diversos (por ejemplo, hace cuánto salió un usuario) y poder informar mejor cuando se le busque o para alguna otra situación administrativa. Esto podemos observarlo en la Figura 32, si en la interfaz se hace *click* en el botón “Mostrar Últimos Accesos”:

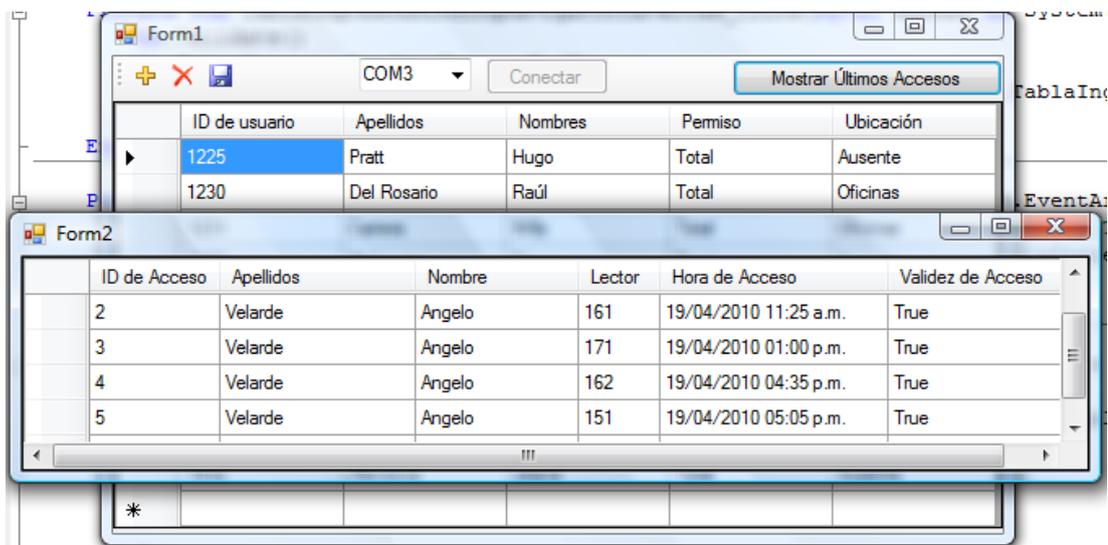


Fig. 32: Registro de Accesos en la Interfaz del usuario

En esta ventana se puede ver a qué hora y fecha cada usuario trató de acceder a cada puerta, y si se le otorgó o no el acceso.

Nótese que se puede agregar mayores capacidades al sistema, como otorgar permisos para solo determinadas horas del día, y que esto solo requiere actualizar el software, sin tener que alterar el hardware de ninguna manera. También se puede agregar nuevos nodos para controlar más puertas sin necesidad de sacar de servicio el sistema por más tiempo que el que toma actualizar el software.

4.6 Presupuesto

A continuación se muestra el costo de la implementación del sistema en el Cuadro 3. Estos costos no incluyen IGV, ni los costos de la circuitería adicional utilizada para pruebas, como en el Generador Wiegand, ni costos de instalación:

Cuadro 3: Presupuesto del sistema planteado

	Costo Unitario (\$)	Cantidad	Costo Total (\$)
Módulos Xbee	19.00	2	38.00
Módulos Xbee Pro	32.00	5	160.00
ATmega8L	3.50	6	21.00
MAX232	1.00	1	1.00
Baterías de Litio para circuitería	3.00	17	51.00
Lectoras Soyal AR-721 U*	45.00	6	270.00
Batería para Lectoras Soyal*	15.00	6	90.00
Tarjetas de Proximidad Soyal*	1.20	50	60.00
Contactos magnéticos para puertas	2.00	3	6.00
Otros componentes	68.00	1	68.00
Total			824.50

El precio de los dispositivos con un asterisco (*) ha sido obtenido de un presupuesto hecho por la empresa Viditek, el cual está incluido en los Anexos.

Haciendo una comparación de los costos de la etapa de control y comunicación entre los nodos del sistema propuesto en el presente trabajo, con los precios de los controladores de sistemas de control de accesos comúnmente instalados, se obtuvo la siguiente información:

- El precio de controladores convencionales de marcas de desempeño promedio es de aproximadamente 1.6 veces el costo del sistema propuesto.
- El precio de controladores de marcas de calidad reconocida internacionalmente, como Honeywell. es de aproximadamente 8 veces el costo del sistema propuesto.

CONCLUSIONES

- Se ha confirmado que el uso del protocolo ZigBee permite grandes facilidades de comunicación para operar distintos tipos de redes dependiendo de su aplicación específica. Se puede optar por aprovechar tanto el bajo consumo de energía, como su capacidad para co-existir con otras redes en la misma banda de frecuencias y sus diversos modos de operación, entre otras opciones.
- El análisis de las necesidades de los usuarios en cuanto al sistema ha permitido concluir que el sistema puede funcionar correctamente de diferentes formas dependiendo de lo que requiera el cliente/usuario y, trabajando sobre la base establecida en este trabajo de tesis, se puede dar cierta flexibilidad al sistema para cumplir con demandas específicas.
- Se ha comprobado la capacidad del protocolo ZigBee, a través de los módulos XBee, para consumir poca potencia. Esta característica puede ser optimizada utilizando los modos de ahorro de energía que ofrecen estos módulos. Estos módulos, junto con dispositivos comunes en el mercado local, pueden componer un sistema que opere correctamente con un nivel de energía y espacio mínimo, el cual puede comunicarse fácilmente a través de interfaces comerciales como el estándar RS-232 o el USB.
- El hecho de diseñar un sistema de control de accesos sobre protocolo ZigBee propone la posibilidad de usar este mismo protocolo para generar muchas otras soluciones en redes inalámbricas para oficinas, casas u otros ambientes.
- Se determinó que el nivel de consumo de energía de la solución planteada

no solo depende de los módulos de radiocomunicación, sino de cada uno de los componentes del circuito. Debido a esto, el consumo actual de energía no es tan bajo como se planteó al comienzo, pero esto puede corregirse con una elección y configuración de los dispositivos aún más minuciosa.

- Se obtuvo un circuito de menos de 4cmx6cm para cada nodo remoto utilizando tecnologías de fabricación sencillas. Esto implica que si se desea tener un circuito aún más pequeño, esto puede lograrse refinando en cierto grado el proceso de fabricación de cada circuito.
- Una trama en cualquier protocolo de comunicación puede retransmitirse sobre protocolo ZigBee para procesar dicha información en cualquier otro nodo de la red.
- Muchas de las aplicaciones de este sistema de control de accesos dependen de la configuración de la aplicación/interfaz de usuario en el servidor, ya que ésta es la que podrá manipular los datos para interpretarlos y generar información útil para cada aplicación específica, y de esta forma explotar los beneficios del sistema.
- Se probó la operación de los nodos, comprobando una correcta comunicación entre ellos.

RECOMENDACIONES

- El sistema puede consumir aún menos energía y espacio si se logra conseguir algunos componentes que ahorren cierta circuitería y funciones, como el MAX3232, que no se ha encontrado aún en mercados locales.
- Se recomienda usar lectoras Wiegand de control de acceso desarrollado por alguna empresa en reemplazo de los generadores Wiegand construidos para las pruebas, para probar la robustez y funcionamiento del sistema.
- Se puede optimizar aún más el uso de la energía con una mayor utilización de las opciones de bajo consumo de energía de los módulos XBee y de los periféricos necesarios en cada microcontrolador ATmega8L.
- Se aconseja instalar brazos mecánicos correctamente mantenidos para el cierre automático de todas las puertas, así como contactos magnéticos de cierre de puertas, los cuales alerten cuando una puerta se quede abierta mucho tiempo, para una mayor eficacia del sistema.
- Luego de instalar el sistema, es recomendable que se instauren normas de “buenos hábitos” y que se brinde una inducción a los usuarios en el uso del sistema. Estas prácticas ayudarán a prevenir el mal uso del sistema, que frecuentemente lleva a provocar vacíos en los sistemas de seguridad.

FUENTES

- [1] TING-PAT SO, Albert
1999 *"Intelligent building systems"*. Massachusetts: Kluwer Academic Publishers.
- [2] FERNANDEZ VALDIVIELSO, Carlos
1999 *"La domótica : esencia de un edificio inteligente"*. *Revista Mundo electrónico*. Madrid, número 298, pp. 56-61.
- [3] CLEMENTS-CROOME, Derek, ed
2004 *"Intelligent buildings: design, management and operation"*. Londres: Thomas Telford Publishing
- [4] NILSSON, Fredrik
2008 *"Intelligent Network Video. Understanding Modern Video Surveillance Systems"*. Florida: CRC Press.
- [5] NATIONAL FIRE PROTECTION ASSOCIATION
2012 *"National Fire Alarm and Signaling Code"*. Edición 2013. Massachusetts: NFPA
- [6] HID GLOBAL
2012 *"HID ASSA ABLOY Mobile Ecosystem Solution Brief"*. Consulta: 3 de diciembre de 2012.
<<http://www.hidglobal.com/documents/hid-assa-abloy-mobile-ecosystem-solutions-brief-en.pdf>>
- [7] KONICEK, Joel; LITTLE, Karen
1997 *"Security, ID Systems and Locks – The Book on Electronic Access Control"*. Massachusetts: Butterworth-Heinemann.
- [8] AMERICAN NATIONAL STANDARDS INSTITUTE
1996 *"Estándar SIA AC-01-1996.10"*. Protocolo Estándar de Control de Acceso para Interface de Lectora Wiegand de 26 bits.

- [9] CUMMING, Neil
1994 “*Security: A guide to security system design and equipment selection and installation*”. Segunda Edición. Massachusetts: Butterworth-Heinemann.
- [10] NAVARRO, María
2004 “*ZigBee: Nuevo Estándar de Tecnología Inalámbrica*”. Revista *Mundo electrónico*. Madrid, número 359, pp. 48-53.
- [11] MINISTERIO DE TTRANSPORTES Y COMUNICACIONES
2005 “*Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones*”
- [12] THONET, Gilles et al.
2008 “*ZigBee - WiFi Coexistence. Schneider Electric White Paper and Test Report*”. Consulta: 3 de diciembre de 2012.
< <http://www.zigbee.org/LearnMore/WhitePapers.aspx> >
- [13] DIGI INTERNATIONAL INC.
2010 “*XBee Wireless RF Modules*”. Consulta: 03 de diciembre de 2012
< <http://www.digi.com/xbee/> >
- [14] ATMEL
2011 “*8-bit AVR with 8KBytes In-System Programmable Flash - ATmega8/ATmega8L*”. Manual del producto Rev.2486Z-AVR-02-11
- [15] DIGI INTERNATIONAL INC.
2012 “*XBee®/XBee-PRO® OEM RF Modules*”. Manual del producto v1.xEx
- [16] DIGI INTERNATIONAL INC.
2008 “*X-CTU - Configuration & Test Utility Software*”. Guía del usuario.
- [17] FUTURE TECHNOLOGY DEVICES INTERNATIONAL LTD.
2012 “*Virtual COM Port Drivers / VCP Drivers*”. Consulta: 3 de diciembre de 2012.
< <http://www.ftdichip.com/Drivers/VCP.htm> >