

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

**DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DOMÓTICO DE
SEGURIDAD INALÁMBRICA PARA UN LABORATORIO DE
TELECOMUNICACIONES**

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

Aldo Carlo Zeballos Chong

ASESOR: Angelo Velarde

Lima, Marzo del 2011

RESUMEN

La presente Tesis está basada en el diseño e implementación de un sistema de seguridad usando sensores comerciales y comunicados inalámbricamente basándose en la tecnología ZigBee y visualizados a través de la pantalla de un computador desde cualquier parte del mundo usando internet.

En una primera etapa se presentará la problemática del asunto de estudio, las razones que justifican la tesis y la coyuntura en la cual se presenta la solución.

En una siguiente etapa se analizará y presentará las distintas tecnologías con las cuales se encuentra uno en el mercado para cada uno de los elementos de la solución, como son los distintos sensores de seguridad, cámaras, protocolos de comunicación y módulos de transmisión-recepción RF.

En la tercera etapa se muestra el diseño de la solución donde se detalla la ubicación, el tipo y el acondicionamiento de cada uno de los sensores, los circuitos a ser implementados, el diseño y conexionado de los módulos de transmisión y receptor inalámbricos. También se diseñará de la interfaz con el usuario a través del puerto serial del computador y creando un programa usando Visual Basic el cual generará alertas en la pantalla de acuerdo a la detección de los sensores.

En la última etapa se mostrará las pruebas realizadas de monitoreo de los sensores, las tramas recibidas, el conexionado de la implementación de la solución, la configuración de la cámara de seguridad y del programa de visualización en la computadora y finalmente el manejo de una página web para la observación del programa en cualquier parte del mundo usando internet.

ÍNDICE

<u>Introducción</u>	1
<u>CAPÍTULO 1: SISTEMA DE SEGURIDAD PARA UN LABORATORIO Y SU PROBLEMÁTICA.</u>	
1.1 Análisis de la coyuntura actual a nivel local	2
1.2 Análisis de la coyuntura actual a nivel global	3
1.3 Condiciones de mercado y normatividad.....	3
1.4 Problemática y causalidad interna.....	4
1.5 Sinopsis de la problemática y situación actual del laboratorio.....	6
<u>CAPÍTULO 2: TECNOLOGÍAS EN SISTEMAS DE SEGURIDAD INALÁMBRICOS PARA EL LABORATORIO V-104.</u>	
2.1 Presentación de la investigación.....	7
2.2 Alternativas Tecnológicas.....	8
2.2.1 Protocolos de Comunicación.....	8
2.2.2 Sensores y Detectores de Seguridad.....	13
2.2.3 Control de Accesos.....	17
2.2.4 Interfaz visual con el usuario.....	19
2.3 Estructuración y política de niveles de seguridad.....	21
2.4 Síntesis sobre la investigación.....	22

CAPÍTULO 3: DISEÑO DE LA ETAPA DE ACONDICIONAMIENTO DE LA SEÑAL, LA COMUNICACIÓN Y LA VISUALIZACIÓN EN LA PC.

3.1 Hipótesis de la investigación.....	23
3.1.1 Hipótesis principal.....	23
3.1.2 Hipótesis secundarias.....	23
3.2 Objetivos de la investigación.....	24
3.2.1 Objetivo general.....	24
3.2.2 Objetivos específicos.....	25
3.3 Diseño de la solución.....	26
3.4 Diseño del acondicionamiento de los sensores.....	28
3.4.1 Conceptos previos.....	28
3.4.2 Sensor de movimiento – Acondicionamiento.....	30
3.4.3 Sensor de humo - Acondicionamiento.....	34
3.4.4 Detector de apertura de puertas y ventanas – Acondicionamiento.....	37
3.4.5 Cámara de seguridad – Implementación.....	40
3.5 Diseño de la Comunicación.....	43
3.5.1 Módulos Xbee.....	43
3.5.2 ¿Por qué Zigbee?.....	45
3.5.3 Receptor – Nodo principal (Coordinador).....	47
3.5.4 Transmisor – Nodo remoto.....	50
3.6 Diseño de la Interfaz con el Usuario.....	53
3.6.1 Funcionamiento del Software.....	54

CAPÍTULO 4: PRUEBAS DE LA RED DE COMUNICACIÓN USANDO XBEE, VISUALIZACIÓN DEL ESTADO DE LOS SENSORES EN LA PC.

4.1	Instalación y uso del programa XCTU.....	56
4.2	Prueba de red – Monitoreo de los sensores.....	60
4.3	Tramas de recepción – Detección y muestra de la información.....	62
4.4	Cámara de Seguridad – Pruebas de resolución y almacenaje.....	63
4.5	Implementación de los sensores y puesta en marcha.....	67
4.5.1	Sensor de Movimiento – Transmisión.....	67
4.5.2	Sensor de Humo – Trasmisión.....	68
4.5.3	Detector de apertura de puertas – Trasmisión.....	69
4.5.4	Cámara de seguridad.....	70
4.5.5	Modulo Receptor.....	71
4.6	Acceso remoto del sistema.....	72
	<u>PRESUPUESTO Y COSTOS DE INSTALACIÓN</u>	75
	<u>CONCLUSIONES</u>	76
	<u>RECOMENDACIONES</u>	77
	<u>BIBLIOGRAFÍA</u>	78

ÍNDICE DE FIGURAS Y TABLAS

CAPÍTULO 1: SISTEMA DE SEGURIDAD PARA UN LABORATORIO Y SU PROBLEMÁTICA.

CAPÍTULO 2: TECNOLOGIAS EN SISTEMAS DE SEGURIDAD INALÁMBRICOS PARA EL LABORATORIO V-104.

Tabla 1: Comparación entre protocolos 12

CAPÍTULO 3: DISEÑO DE LA ETAPA DE ACONDICIONAMIENTO DE LA SEÑAL, LA COMUNICACIÓN Y LA VISUALIZACION EN LA PC.

Figura 3.1: Esquema de la solución 27

Figura 3.2: Negador (símbolo y tabla de verdad) 28

Figura 3.3: Diodo Zener (símbolo y vista real)..... 29

Figura 3.4: Transistor 29

Figura 3.5: Corte – Saturación 30

Figura 3.6: Sensor de movimiento 30

Figura 3.7: Ubicación 30

Figura 3.8: Rango del sensor de movimiento(vista superior) 31

Figura 3.9: Rango del sensor de movimiento (vista lateral) 32

Figura 3.10: Chip sensor de movimiento..... 32

Figura 3.11: Esquemático acondicionamiento del sensor de movimiento 33

Figura 3.12: Diagrama real de conexionado (Board)	33
Figura 3.13: Sensor de humo	34
Figura 3.14: Ubicación	34
Figura 3.15: Chip Sensor de humo	35
Figura 3.16: Esquemático del acondicionamiento	35
Figura 3.17: Diagrama real de conexionado (Board)	36
Figura 3.18: Detector de aperturas	37
Figura 3.19: Ubicación del detector	37
Figura 3.20: Chip del detector	38
Figura 3.21: Esquemático del acondicionamiento	38
Figura 3.22: Diagrama real de conexionado (Board)	39
Figura 3.23: Cámara	40
Figura 3.24: Ubicación	40
Figura 3.25: Conector RCA	41
Figura 3.26: Adaptador RCA – USB	42
Tabla 2. Cuadro comparativo entre módulos Xbee y el Xbee-Pro	44
Figura 3.27: Crecimiento ventas Zigbee	45
Figura 3.28: Diagrama de bloques – Coordinador	47
Figura 3.29: Esquemático de la alimentación	48
Figura 3.30: Esquemático Coordinador	49
Figura 3.31: Board Coordinador	49

Figura 3.32: Diagrama de bloques del Terminal.....	50
Figura 3.33: Esquemático de la alimentación	51
Figura 3.34: Esquemático del Terminal	52
Figura 3.35: Board Transmisor	52
Figura 3.36: Icono de programa	53
Figura 3.37: Vista programa	53
Figura 3.38: Ventana de alerta	53
Figura 3.39: Diagrama de flujo – Programa General	54
Figura 3.40: Diagrama de flujo de la detección	55

CAPÍTULO 4: PRUEBAS DE LA RED DE COMUNICACIÓN USANDO XBEE, VISUALIZACION DEL ESTADO DE LOS SENSORES EN LA PC.

Figura 4.1: Modem Configuration – New versions	56
Figura 4.2: Módulo de programación XBee	57
Figura 4.3: Firmware version	57
Figura 4.4: PC Settings	58
Figura 4.5: Range Test	58
Figura 4.6: Terminal	59
Figura 4.7: Modem Configuration	59
Figura 4.8: Prueba de red – Monitoreo de IO	61
Figura 4.9: Programa Prueba de detección	63
Figura 4.10: Entorno de visualización –Cámara	64

Figura 4.11: Configuración Básica	65
Figura 4.12: Búsqueda y Rebobinado	66
Figura 4.13: Sensor de Movimiento – Transmisión	67
Figura 4.14: Sensor de Humo – Transmisión	68
Figura 4.15: Sensor de Humo – Transmisión	69
Figura 4.16: Implementación Cámara de Seguridad	70
Figura 4.17: Módulo Receptor	71
Figura 4.18: Programa de prueba con todas las tramas	71
Figura 4.19: Pagina Web LogMeIn	72
Figura 4.20: Acceso al computador (registro)	73
Figura 4.21: Menú de opciones de acceso	73
Figura 4.22: Pantalla del servidor- control	74
Tabla 3: Presupuesto y costos de instalación	75

INTRODUCCIÓN

Hoy en día, la seguridad en nuestro país, tanto personal como material, es un tema muy importante que se presenta en todos los niveles socioeconómicos.

En un entorno donde la falta de respeto por lo ajeno prevalece, es importante tomar medidas para contrarrestar estos actos y así brindar una mayor tranquilidad a los propietarios en el tema.

Las escasas precauciones que se toman en tema de seguridad en los locales, ambientes, tiendas y hasta en nuestras propias casas en nuestro país son vulnerables para posibles atentados, es por eso, que se hace necesaria una conciencia de protección de nuestros bienes para evitar futuras pérdidas.

Actualmente en el mundo existen gran variedad de tecnologías y dispositivos, e inclusive hasta sistemas completos y listos para la venta que se adecuan a nuestras particulares necesidades y que brindan un soporte seguro a nuestro hogar con distintos niveles de protección por precios muy variados pero en general elevados.

Esta tesis se basa en la aplicación de estos sistemas visto desde un punto de vista general para brindar seguridad al laboratorio V-104 en el pabellón "V" de la Pontificia Universidad Católica del Perú, pero usando dispositivos simples y económicos que se pueden conseguir en tiendas locales y supermercados sin disminuir en el proceso el grado de confiabilidad necesaria.

CAPÍTULO 1

PROBLEMÁTICA DE LA SEGURIDAD EN EL LABORATORIO

Actualmente en el Perú, la implementación de sistemas de seguridad es muy incipiente y sobretodo escasa en la aplicación a ambientes pequeños tipo laboratorio con costes bajos y usando dispositivos asequibles que contrarresten la inseguridad que representa el tener gran cantidad de equipos costosos en un ambiente relativamente libre y a veces sin ningún tipo de supervisión.

Hay un largo camino por recorrer en lo que respecta a métodos de protección de inmuebles y eso debido al predominio actual del mercado a las ventas de seguros de inmuebles sobre la prevención de siniestros mediante el uso de sistemas confiables de seguridad.

1.1 ANÁLISIS DE LA COYUNTURA ACTUAL A NIVEL LOCAL

El laboratorio V-104 de la Pontificia Universidad Católica del Perú, es un ambiente donde se realizan trabajos de investigación y sesiones de laboratorio correspondientes al campo de telecomunicaciones, por lo que este se encuentra implementado con una amplia gama de equipos y accesorios de alta tecnología, los cuales permiten el desarrollo de experiencias, actividades y simulaciones de sistemas de comunicaciones tanto de tecnologías pasadas como de tecnologías y aplicaciones modernas.

El ambiente y los equipos disponibles son usados por alumnos de ingeniería desde el 7mo ciclo, jefes de práctica de los distintos laboratorios, profesores de los distintos cursos de telecomunicaciones y tesis en la etapa de investigación e implementación.

Para las sesiones de laboratorio cuenta con computadoras, osciloscopios, generadores de señales, generadores de frecuencia, módulos y accesorios, los cuales abastecen a grupos de 16 alumnos por sesión, atendiendo con ello, a las clases prácticas de cursos de carrera de las facultades de ingeniería electrónica e ingeniería de telecomunicaciones.

En la infraestructura general del laboratorio, se cuenta con instrumentos electrónicos de alta tecnología que tienen considerables costos tanto de adquisición como de reparación, que son usados a diario tanto por alumnos inexpertos como por jefes de práctica y profesores.

El laboratorio, en materia de seguridad, cuenta con un seguro simple en las puertas y ventanas con pestillo, sin ningún equipamiento para el control de incendios y sin ningún tipo de vigilancia ni seguridad extra, esto, en confianza de la ética profesional y del alumnado.

1.2 ANÁLISIS DE LA COYUNTURA ACTUAL A NIVEL GLOBAL

Actualmente tanto en las universidades como en el Perú, la implementación de sistemas de seguridad es muy incipiente y sobretodo escasa en la aplicación a ambientes pequeños tipo laboratorio con costes bajos, usando dispositivos asequibles que contrarresten la inseguridad que representa el tener gran cantidad de equipos costosos en un ambiente relativamente libre y a veces sin ningún tipo de supervisión.

Esto genera una alta expectativa y desarrollo en lo que respecta en métodos de protección de inmuebles, eso debido al descuido del gobierno en promocionar mas el uso de seguros y el trabajar en la producción de leyes de castigo contra los siniestros en vez de fomentar una política de prevención mediante el uso de sistemas confiables de seguridad.

1.3 CONDICIONES DE MERCADO Y NORMATIVIDAD

Las tecnologías en sistemas de seguridad que existen actualmente en el mercado trabajan con dispositivos y protocolos propios [1], vendiendo sistemas completos , inclusive con servicios de valor agregado , brindando con ello una protección muy confiable pero con costos muy elevados y por tanto siendo solo accesibles a grandes empresas en oficinas principales o clientes con altos ingresos económicos. Este panorama hace propicia la aparición de nuevas tecnologías y métodos para lograr el mismo nivel de confiabilidad de un sistema de seguridad pero con dispositivos asequibles y de precios comparablemente económicos.

En el mercado peruano existen empresas como Interamsa [2], radioshack [1], orus [3], segurysistem [4], que brindan servicios no solo de instalación de sistemas de vigilancia de perimetrado e interiores sino también servicios de valor agregado como asistencia personal y de la policía ante actos delictivos, rondas de seguridad y aviso telefónico a los propietarios.

Normatividad:

El artículo 28° del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo N° 027-2004-MTC, establece que aquellos servicios cuyos equipos, utilizando las bandas 902-928 MHz, 2400-2483,5 MHz y 5725-5850 MHz que transmiten con una potencia no superior a 100 milivatios (mW) o 20dBm en antena (potencia efectiva irradiada), y no sean empleados para efectuar comunicaciones en espacios abiertos, están exceptuados de contar con concesión, asignación del espectro radioeléctrico, autorización, permiso o licencia, para la prestación o instalación de servicios de telecomunicaciones; mientras que aquellos servicios cuyos equipos utilizando las bandas antes mencionadas transmiten con una potencia no superior a 4 vatios (W) o 36 dBm en antena (potencia efectiva irradiada) en espacio abierto sólo están exceptuados de contar con la asignación del espectro radioeléctrico, autorización, permiso o licencia, para la prestación o instalación de servicios de telecomunicaciones.[5]

1.4 PROBLEMÁTICA Y CAUSALIDAD INTERNA

En el ambiente del laboratorio se presentan distintas situaciones problemáticas causadas por la infraestructura y organización actual en la que se encuentran, como son:

a) Entrada de personal no autorizado

Al ser un laboratorio con horas libres, en la cual los alumnos (sean de ingeniería o no) pueden realizar actividades de investigación o pruebas sobre los temas desarrollados en los cursos, es fácil ingresar con autorización del encargado y manipular los equipos, pero, sin una supervisión adecuada, puede generar problemas como robos o daños en el hardware o software de los equipos.

b) Control de ingreso y salida del personal y alumnado

Actualmente, en los laboratorios, el registro de asistencia es tomado manualmente por el jefe de práctica, pero no hay control sobre la asistencia de los mismos jefes de práctica o profesores, así como tampoco salidas o reingresos del personal a los servicios higiénicos, ni tampoco inventario de equipos al término de las sesiones.

c) Uso adecuado de los equipos del laboratorio

Durante las horas libres o sesiones de laboratorio se utilizan equipos como osciloscopios, generadores de señal, computadoras, multímetros, los cuales al no ser usados correctamente ya sea por desconocimiento de uso, errores casuales o por objetivos malintencionados, estos se averíen y en tales casos es difícil señalar a los culpables.

d) Necesidad de protección contra robos de equipos

Los equipos que se encuentran en el laboratorio tienen un costo alto, y ante la posibilidad de un acto delictivo, con costos sumamente elevados de reinstalación, se justifica el costeo e implementación de un sistema de seguridad que garantice el impedimento del mismo.

e) Fácil acceso por puertas y ventanas

El laboratorio cuenta con ventanas sin rejado (algunas rotas) y con un seguro de puertas simple, lo que advierte la posibilidad de existencia de varias copias de las llaves, garantizando un fácil ingreso en caso de siniestro.

1.5 SINOPSIS DE LA PROBLEMÁTICA Y SITUACIÓN ACTUAL DEL LABORATORIO

Los sistemas de seguridad inalámbrica existentes en el mercado funcionan con sensores de una misma familia en paquetes de venta establecidos con precios algo elevados, lo que dificulta su difusión, en especial su uso en locales o ambientes donde su implementación sería poco rentable debido a esta situación muchos locales, oficinas y laboratorios siguen causando inseguridad y temor de un posible siniestro en los propietarios según estadísticas recientes. [6]

Según el encargado del laboratorio [7], este cuenta con muchos equipos costosos como osciloscopios, multímetros, computadoras, analizadores de espectro, módulos digitales y analógicos entre otras cosas que no solo pueden ser sustraídos, sino también pueden averiarse por malos manejos ya sean casuales o de mala intención, esto en un contexto donde el ambiente está constantemente ocupado ya sea por sesiones de laboratorio o horas de uso libre.

A ello se suma la precaria seguridad que se presenta en el laboratorio debido a que solo cuenta con una cerradura en la puerta con posibles copias no permitidas de las llaves.

La universidad, teniendo en cuenta la posibilidad de ocurrencia de actos delictivos posee personal de seguridad repartido por todo el campus (mayormente en la puertas de la universidad), pero no cerca al laboratorio en cuestión, además de ello no hay un control específico de lo que sale de la universidad a través de vehículos, lo cual propicia un poco más la probabilidad de atentados.

Finalmente, el mercado local ha venido promoviendo el tema de uso de seguros de inmuebles y el gobierno generando nuevas leyes para castigar actos delictivos en vez de promocionar la prevención contra robos mediante la implementación de sistemas de seguridad más eficientes que los que actualmente se usan como son las cerraduras de las puertas y rejas metálicas que son algo volubles y no generan una respuesta ante un acto delictivo.

CAPÍTULO 2

TECNOLOGÍAS EN SISTEMAS DE SEGURIDAD INALÁMBRICOS PARA EL LABORATORIO V-104.

2.1 PRESENTACIÓN DE LA INVESTIGACIÓN

Un sistema domótico de seguridad está fundamentado básicamente en la posibilidad de que mediante un conjunto de sensores y detectores se puede detectar un allanamiento o una irrupción inesperada a un ambiente protegido y por tanto un posible robo y a partir de ello alertar oportunamente a las autoridades competentes del suceso y poder contrarrestar el acto a tiempo.

De la misma forma el sistema también debe ser capaz de alertar la presencia de humo y de un posible incendio a su debido tiempo con el fin de que este pueda ser extinguido antes que se propague más, causando mayores daños a los inmuebles.

El conjunto de sensores y detectores que pueden implementarse son muy diversos y se enfocará más en el uso de los prioritarios como son cámaras y sensores de movimiento, con la particularidad de que estos sean adquiridos en tiendas locales al menor precio posible, lo cual representa la base de esta tesis.

En la etapa de diseño, se investiga y analiza las distintas tecnologías y características que existen para cada uno de los sensores que se usarán con el fin de seleccionar la opción más adecuada para el problema desde un punto de vista de costos, funcionalidades y cumplimiento de los requerimientos, tal es así como la resolución de video, activación de cámara ante abertura de puertas o sensado de movimiento, etc.

En otra etapa de diseño en paralelo se analiza la óptima configuración de ubicación de cada uno de los dispositivos tomando en cuenta la actual infraestructura del laboratorio y con el fin de satisfacer las características de cada uno de los elementos como visibilidad, cercanía a focos de calor y de posible inicio de incendio, prioridad de sensado en ventanas y entradas de fácil acceso, etc.

En el diseño de la transmisión de datos se analizará las distintas tecnologías disponibles para la comunicación entre cada uno de los sensores y el servidor, que es el encargado de mostrar lo sensado además de tomar decisiones al respecto (alarmas), teniendo en cuenta para la selección la simplicidad, viabilidad y por

supuesto el cumplimiento de los requerimientos, teniendo en cuenta para ello la elección correcta del protocolo, tasas de transmisión de información, radios de alcances y configuraciones tanto alámbricas como inalámbricas.

En la etapa de diseño e implementación final se afinará la forma en que se visualizará la información sensada desde el uso de alarmas locales (interiores o exteriores al laboratorio), alerta a la policía, bomberos o seguridad local hasta la comunicación en vivo con el encargado del laboratorio en el caso de transmisión de video y datos en general. Del mismo modo se tomarán decisiones sobre el almacenamiento de la información tanto de video como del historial de eventos.

2.2 ALTERNATIVAS TECNOLÓGICAS

En esta investigación se presentan las distintas alternativas de solución para cada uno de los módulos que conforman el diseño de la solución.

2.2.1 Protocolos de comunicación:

Protocolo de red o también Protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red. A continuación se muestran las tecnologías más económicas y disponibles en el mercado y sus comparaciones.

a) Zigbee

Es la denominación de un conjunto de protocolos de alto nivel de comunicación inalámbrica, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (Wireless Personal Area Network, WPAN). Se define su uso en aplicaciones con requerimientos bajos de velocidad de transmisión de datos y de consumo energéticos. [8], [9].

Características:

- Uso de la banda ISM para usos industriales, científicos y médicos (2.4Ghz de uso mundial).
- Comunicación con baja tasa de envío de datos.
- Larga vida útil de baterías, alrededor de 5 años (bajo consumo).
- Topología de red tipo malla.

- Fácil integración (implementación de nodos con poca electrónica).
- Sencillo y de bajo costo.

Usos:

Para el control industrial, sensores empotrados, recolección de datos, detección de humo, de intrusión y en la domótica, donde no es vital una alta velocidad de transmisión y donde los equipos el 99% del tiempo están “dormidos” (bajo consumo).

b) Bluetooth

Es un protocolo de uso industrial para redes inalámbricas de área personal (WPAN), que permite la transmisión de datos e inclusive voz entre dispositivos usando radiofrecuencia de entre 2.4 y 2.48 GHz. La versión 1.2 usa la técnica de salto de frecuencia adaptativa (Adaptive Frequency Hopping - AFH) que le da seguridad y robustez. [9], [10]

Características:

- Facilita la comunicación entre equipos móviles y fijos sin necesidad de que estén alineados.
- Elimina cables y conectores entre estos con una cobertura de entre 10 y hasta 100 m con repetidoras.
- Bajo consumo.
- Uso de transceptores de bajo costo.
- Velocidades de 1Mbit/s.
- Posibilidad de transmisión full duplex.

Usos:

Se usa mayormente en dispositivos del sector de telecomunicaciones y de informática personal como PDAs, celulares, laptops, impresoras, cámaras digitales, mp4s, auriculares.

c) Wifi

Es un nombre popular de tecnología inalámbrica, usada en redes caseras, teléfonos móviles, videojuegos, mp3, PDAs, que pueden conectarse a Internet siempre y cuando estén dentro del rango de difusión que tenga el punto de acceso. Además, también permite la conectividad punto a punto (peer to peer), es decir la conexión entre cada uno de los dispositivos directamente. [9], [11]

Características:

- Permite la configuración de una Lan (Local Area Network) y comunicación sin cables entre dispositivos.
- Compatibilidad general de los dispositivos, es decir cualquier dispositivo que trabaje con wifi, puede conectarse a cualquier red que trabaje con esta.
- Poder de consumo alto.
- Problemas en la seguridad, fácil penetración a la información.
- El desempeño decrece exponencialmente conforme aumenta el rango de alcance.

Usos:

Su aplicación se extiende básicamente para acceso a Internet, ya sea por cualquiera de los distintos dispositivos, donde a la vez se puede transmitir información entre ellos usando el router.

d) Wireless Usb

Es un protocolo de comunicación inalámbrica por radio con un amplio ancho de banda que combina la simplicidad de manejo de USB con la versatilidad de las redes inalámbricas. [9], [12]

Características:

- Utiliza como base de radio la plataforma Ultra-WideBand.
- Permite la conexión directa de hasta 127 dispositivos a un host único.
- Tasas de transmisión de hasta 480Mbps en rangos de 3m y 110Mbps para rangos de 10 m.
- Trabaja con frecuencias entre 3.1 y 10.6Ghz.

Usos:

Wireless Usb se emplea en mandos de videoconsola, impresoras, escaners, cámaras digitales, reproductores MP3, discos duros y flash, entre otros. También puede usarse para transmisión paralela de video.

e) X10

Es un protocolo abierto e internacional de comunicaciones para el control remoto de dispositivos eléctricos usando la línea eléctrica (110 o 220v) para transmitir señales de control en formato digital y así realizar acciones como prender, apagar, prender todo, apagar todo y en caso de lámparas el DIM y el brillo.

Se basa en la transmisión de ráfagas de pulsos de radiofrecuencia de 120Khz sobre la red eléctrica (60Hz) en los cruces por cero.

Adicionalmente también trabaja con comunicación por radio operando a frecuencias de 310 MHz en USA y 433 MHz en Europa. [9], [13]

Características:

- La trama de información consta de bit de direcciones y de órdenes.
- Cada orden se transmite 2 veces (cuádruple redundancia), involucrando 11 ciclos de red (183.33ms).
- Los dispositivos disponibles que manejan radio incluyen:
 - Controladores por keypad (clikers).
 - Controladores por keychain, que maneja de uno a cuatro dispositivos X10.
 - Módulos de alarma que pueden transmitir datos.
 - Interruptores infrarrojos pasivos que controlan iluminación.
 - Ráfagas de información no pasivas.
- El protocolo es algo lento. Tarda alrededor de $\frac{3}{4}$ de segundo para transmitir la dirección de un dispositivo y un comando.

Usos:

Se utiliza en aplicaciones de control remoto, aplicaciones hogareñas, control de la intensidad de luz, el prendido y apagado de dispositivos como lámparas, alarmas y otros equipos electrónicos que trabajen con ON/OFF.

TABLA COMPARATIVA ENTRE TECNOLOGÍAS:

	ZIGBEE	WIFI	BLUETOOTH	W-USB	X10
Frecuencia	2.4 GHz/868 MHz/915 MHz	2.4 GHz/5 GHz	2.4 GHz	3.1 GHz~10.6 GHz	310 Mhz/ 433Mhz
Ancho de banda	20/40/250 Kbit/s	11-108 Mbit/s	1-3 Mbit/s	480 Mbit/s (3 m),	60bps en USA
Cobertura	1-75 m	20-250 m	1-100 m	3-10 m	max 185m2
Modulación	DQPSK	DSSS-DBPSK-DQPSK-CCK-OFDM	GFSK	MB-OFDM	PLC
Estandar	802.15.4	802.11	802.15.1	-	-
Consumo de potencia	30ma transmitiendo 3ma en reposo	400ma transmitiendo y 20ma en reposo	40ma transmitiendo y 0.2ma en reposo		Menos de 2 W
Ventajas	Batería de larga duración, bajo coste, bajo consumo de energía.	Gran ancho de banda, protección contra interferencias.	Interoperatividad, sustituto del cable. Consumo de bajo de corriente.	Asequible en precios, adecuado para accesorios de PCs.	Uso de la instalación eléctrica, bajo coste de instalación.
Aplicaciones	Control remoto, productos dependientes de la batería, sensores, juguetería.	Navegar por Internet, redes de ordenadores, transferencia de ficheros .	Wireless USB, móviles, informática casera .	Mandos de videoconsola, impresoras, escáners, cámaras digitales, reproductores MP3, discos duros y flash, entre otros.	Control remoto y aplicaciones hogareñas, intensidad de luz, on/off de dispositivos, (lamparas, alarmas, accesorios).
Memoria	32-60KB	+ 100KB	+ 100KB	---	---
Conexión	En malla, punto a punto o punto a multipunto	Punto a multipunto	Punto a multipunto	Punto a punto	Punto a multipunto, punto a punto
Desventajas	Muy baja velocidad, tecnología en fase de lanzamiento.	Interferencias. Dificil configuración.	Dificil configuración y puesta en marcha, costos elevados.	Necesita un host que controle la conexión. Distancia entre dispositivos limitada	Protocolo algo lento, tarda 3/4 seg en, enviar un comando.

CCK	Complementary code keying	EDR	Enhanced data rate
DBPSK	Differential binary phase shift keying	GFSK	Gaussian frequency shift keying
DQPSK	Differential quadrature phase shift keying	MB-OFDM	Multiband-OFDM
DSSS	Direct sequence spread spectrum	OFDM	Orthogonal frequency division multiplexing
PLC	Power Line Carrier		

Tabla 1: Comparación entre protocolos - Elaboración propia, fuentes [8],[9],[10]y[11].

2.2.2 Sensores y detectores de seguridad

En esta investigación se presenta cada uno de los dispositivos de seguridad que conforman la solución y su gama de variedades tecnológicas que existen en el mercado local.

2.2.2.1 Cámaras de seguridad [9]

Existe actualmente en el mercado una amplia gama de equipos de captura de video y cámaras destinadas a cubrir las más diversas necesidades.

Para la elección de la cámara de seguridad adecuada es necesario primero hacer un análisis de las características particulares del ambiente que va a ser protegido y a partir de allí definir el dispositivo que cumpla con los requerimientos.

Las diversas características que se pueden encontrar en el mercado son las siguientes:

- Cámaras tipo Domo (discretas y elegantes).
- Cámaras con infrarrojo para visión nocturna.
- Cámaras ocultas (de menor tamaño y ocultas en otros dispositivos).
- Cámaras para instalación interior o exterior.
- Cámaras con carcasa irrompible anti vandálica.
- Cámaras con óptica intercambiable (zoom).
- Cámaras con señal de vídeo inalámbrica.
- Cámaras con servidor Web de vídeo incorporado.
- Cámaras IP, para ver las imágenes por Internet.
- Cámaras con sensores de movimiento.
- Cámaras con imágenes a color o en blanco y negro.
- Cámaras con o sin captura de sonido.
- Cámaras con o sin alarma.
- Cámaras en circuito cerrado (CCTV) para ver uno o varios ambientes desde todos los ángulos.
- Cámara de captura por fotos de alta resolución (CCDP).

Cabe resaltar que las cámaras que existen en el mercado combinan varias características de las antes mencionadas.

2.2.2.2 Detector de humo y/o incendio [9]

Es un dispositivo de seguridad que detecta la presencia de humo en el ambiente y emite una señal acústica para alertar el peligro de incendio a los habitantes del complejo, además se puede implementar su comunicación con el departamento de bomberos, llamar a un teléfono en particular o mandar alertas vía Internet.

Existen dos tipos de tecnologías de detección:

a) Detector de tipo óptico

Pueden ser de dos tipos, según detecten el humo por oscurecimiento o por dispersión del aire en un ambiente.

Detector con rayo infrarrojo: compuestos por un dispositivo emisor y otro receptor. Cuando se oscurece el espacio entre ellos debido al humo sólo una fracción de la luz emitida alcanza al receptor provocando que la señal eléctrica producida por éste sea más débil y se active la alarma.

Detector de tipo puntual: en los que emisor y receptor se encuentran ubicados en la misma cámara pero no se ven al formar sus ejes un ángulo mayor de 90° y estar separados por una pantalla, de manera que el rayo emitido no alcanza el receptor. Cuando entra humo en la cámara el haz de luz emitido se refracta y puede alcanzar al receptor, activándose la alarma.

b) Detector de tipo iónico.

Este tipo de detector es más económico que el del tipo óptico y puede detectar partículas que son diminutas como para influir en la luz. Está compuesto por una pequeña cantidad del isótopo radioactivo americio-241 que emite radiación alfa.

La radiación pasa a través de una cámara abierta al aire en la que se encuentran dos electrodos, permitiendo una pequeña y constante corriente eléctrica. Si entra humo en esa cámara se reduce la ionización del aire y la corriente disminuye o incluso se interrumpe, con lo que se activa la alarma.

Es importante mencionar el tema del mantenimiento, los detectores normalmente trabajan a pilas o conectados a la red eléctrica, en el caso de las pilas estas se

gastan y vuelven inservible al sensor, algunos emiten una señal de baja batería, lo ideal sería que se revise el estado de las baterías cada 6 meses.

2.2.2.3 Sensores de Movimiento o vibración [9]

Un sensor de movimiento es un equipo electrónico que detecta el movimiento físico en un área dada y lo transforma en una señal eléctrica que puede activar equipos de seguridad, luces, alarmas sonoras entre otros.

Básicamente hay 2 tipos de sensores, los que trabajan con infrarrojo y los que usan microondas.

a) Sensor infrarrojo

Activo: incluye una fuente de radiación y un sensor infrarrojo que es sensible a la variación de radiación sensada. Se activa cuando el intruso interrumpe el camino de luz infrarroja por lo que hay que colocar el sistema en el lugar adecuado.

Pasivo: Es un sistema que detecta la energía calorífica emitida por un objeto o cuerpo que se mueve a través del campo de vista del sensor. Generalmente usan una colección de sistemas ópticos y múltiples elementos de sensado de polaridad alternante para crear un patrón de detección en el ambiente de interés.

El único inconveniente de este tipo de tecnología es el alcance, limitado a la estancia donde se encuentran o con visión directa.

b) Sensor tipo radar

Los sensores basados en un sistema de radar trabajan con una emisión continua de una señal de microondas y comparan la frecuencia emitida con la frecuencia eco para producir una frecuencia patrón proporcional al rango. Cuando el intruso penetra en el área de sensado la frecuencia eco cambia debido al rebote imprevisto y se detecta la intrusión.

Estos sensores disponen de un mayor alcance al traspasar paredes entre ambientes y esto ocasiona que su uso no resulte adecuado en viviendas

(especialmente en edificios) dado que movimientos en viviendas contiguas pueden afectar a la detección en la propia vivienda.

2.2.2.4 Detector de apertura de puertas y ventanas [9]

Son pequeños dispositivos cuya función es detectar cuando una puerta o ventana es abierta que genera una reacción ya sea desde solo enviar la información así como también activar una alarma.

Consta de dos partes: una se coloca en la puerta o ventana misma (transmisor) ya sea con tornillos o con adhesivos y la otra (receptor) en el marco de la puerta o ventana.

El proceso de detección se genera por distintas tecnologías:

- Usando contactos magnéticos, al abrirse la puerta se interrumpe y se activa la detección.
- Usando transmisores y receptores infrarrojos.
- Usando transmisores de láser, para distancias largas.

2.2.2.5 Sistemas de alarma [14]

La alarma está formada generalmente por una sirena, campana o zumbador o algún otro medio alternativo, que advierte de la ocurrencia de una intrusión, presencia de humo, fuego o acción de cualquier otro dispositivo que haya sido configurado a la alarma y es detectado por el sistema usando para ello una señal sonora (tono) de alto nivel.

En algunos casos, también puede incluir algún tipo de señalización visual, como balizas, encendido de luces y destelladores (flash), para aquellas personas que tienen problemas de audición o cuando existe un alto nivel de ruido ambiente.

Normalmente estas sirenas emiten un sonido de unos 120 decibeles (equiparable al sonido de una ambulancia).

Para instalar una alarma debe tenerse en cuenta algunos factores como el nivel de ruido ambiental, el tipo y calidad del sonido ambiental, la duración de la señal requerida, el nivel acústico deseado y la alimentación eléctrica disponible.

Básicamente existen dos sistemas de alarma según el tipo de conexión:

a) **Sistema conectado a una central:** que tras detectar la intrusión, avisará a la empresa de seguridad contratada que a su vez avisará a la policía o ellos mismos se encargaran de atender el problema. Este sistema de seguridad goza de un gran éxito especialmente en viviendas con jardín, en casas que se encuentren aisladas o simplemente para aquellas que están deshabitadas frecuentemente.

b) **Sistema sin conexión:** es el más básico, cubre las necesidades de viviendas habitadas de forma continua ubicadas en un centro urbano. El funcionamiento de este tipo de alarmas es muy simple, consiste principalmente en emitir un sonido cuando se intenta acceder a la vivienda de forma violenta. Con ello se consigue ahuyentar al intruso y atraer la atención de los vecinos y transeúntes para que alerten a la policía.

2.2.3 Control de accesos: [9]

Es la habilidad de permitir o denegar el acceso a un recurso por una entidad en particular. Los mecanismos de control de acceso pueden ser usados en el manejo de recursos físicos, lógicos o digitales. En nuestro caso queremos controlar el acceso del personal al laboratorio.

Tecnologías en el manejo del control de accesos:

2.2.3.1 Credenciales

Cuando la credencial se presenta ante la lectora, esta envía la información (generalmente un número) a un panel de control con procesador. Este controlador compara la credencial con una lista de control de accesos, permitiendo o denegando el acceso mediante el bloqueo o desbloqueo de la puerta.

a) Código de Barras:

El código de barras es una serie de tiras oscuras y claras alternadas que son leídas por una scanner óptico. La ventaja de este tipo de tecnología es que es barato, con facilidad de generar credenciales y son aplicadas en tarjetas u otros ítems.

La desventaja es que debido a lo económico que resulta esta tecnología es propensa al fraude, además el lector óptico es fácilmente confundido con la suciedad y con las credenciales deterioradas.

b) Tecnología de tiras magnéticas:

Llamada así porque se basa en el uso de una cinta de óxido magnético laminada en una tarjeta. Está conformada en tres pistas de datos configuradas de acuerdo al estándar de codificación.

Esta tecnología es más económica que las anteriores y es fácil de programar.

La cinta magnética puede almacenar más información que el código de barras, pero es también muy susceptible a fallos de lectura y datos errados.

c) Tarjetas de proximidad:

Está basado en el uso de una lectora que genera un campo eléctrico alrededor de ella y tarjetas que incluyen un simple circuito LC (capacitor-bobina). Cuando la tarjeta se acerca a la lectora el circuito es excitado por el campo magnético, cargando el capacitor, alimentando el circuito integrado y por tanto enviando el número de acceso.

d) Smart Card:

Existen dos tipos de Smart Card: con contacto y sin contacto. Ambas tienen un microprocesador embebido y memoria. Lo que diferencia a estas tarjetas sobre las de proximidad es que no solo almacenan el número de identificación sino también poseen sistemas de operación que manejan múltiples aplicaciones como tarjeta de débito, tarjetas de membresía prepago, etc.

2.2.3.2 Código de seguridad:

El número de identificación personal consiste normalmente entre 4 y 8 dígitos. Menor a esa cantidad es más fácil de adivinar y más de esta cantidad haría difícil recordar.

La ventaja de este tipo de dispositivos es que una vez que el número es memorizado, la credencial no se puede perder o dejar en algún lado, como sucede con la tecnología de tarjetas.

2.2.3.3 Sistemas biométricos— escaneo de huellas digitales

Está basado en una base de datos donde se manejan las huellas digitales de todo el personal permitido y no permitido al acceso. Previamente formada esta base de datos en formatos no digitales (huellas recopiladas a tinta en papeles), se procede al uso de un software de escaneo, donde se trabaja con algoritmos que registran los puntos minuciosos, núcleos, y deltas (espacios) que conforman cada huella digital, la cual es considerada como única.

El sistema de escaneo posee la capacidad de verificar los patrones de la huella digital de cada individuo que requiere el acceso y compararla contra esta base de datos, de esta manera permite o deniega el acceso del personal.

2.2.4 Interfaz visual con el usuario

La interfaz o comunicación con el usuario se realizará con el uso de una computadora servidor. El servidor es una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes.

Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar, acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. [9]

Existen distintos objetivos que deben cumplir:

Abstracción de la información. Deben ahorrar a los usuarios detalles acerca del almacenamiento físico de los datos. Da lo mismo si una base de datos ocupa uno o cientos de archivos, este hecho se hace transparente al usuario. Así, se definen varios niveles de abstracción.

Redundancia mínima. Un buen diseño de una base de datos logrará evitar la aparición de información repetida o redundante. De entrada, lo ideal es lograr una redundancia nula; no obstante, en algunos casos la complejidad de los cálculos hace necesaria la aparición de redundancias.

Seguridad. La información almacenada en una base de datos puede llegar a tener un gran valor, por lo tanto deben garantizar que esta información se encuentra segura frente a usuarios malintencionados, que intenten leer información privilegiada.

Respaldo y recuperación. Deben proporcionar una forma eficiente de realizar copias de respaldo de la información almacenada en ellos, y de restaurar a partir de estas copias los datos que se hayan podido perder.

Tiempo de respuesta. Lógicamente, es deseable minimizar el tiempo que el servidor tarda en darnos la información solicitada y en almacenar los cambios realizados.

Ventajas:

1. Facilidad de manejo de grandes volúmenes de información.
2. Gran velocidad de procesamiento.
3. Independencia del tratamiento de información.
4. Seguridad de la información (acceso a usuarios autorizados), protección de información, de modificaciones, inclusiones, consulta.
5. No hay duplicidad de información, comprobación de información en el momento de introducir la misma.
6. Integridad referencial al terminar los registros

2.3 ESTRUCTURACIÓN Y POLÍTICA DE NIVELES DE SEGURIDAD

En nuestro sistema de seguridad es importante detectar el ingreso, la salida y todo acto indebido que se puede presentar dentro del ambiente de laboratorio a ser protegido, a partir de allí definir los parámetros, sus características de cada uno de los accesorios que se escogen para este fin, de no hacerlo, el sistema sería imperfecto y por ende ineficaz en cuestiones de seguridad.

Realizando una clasificación de niveles de seguridad propia, basándonos en la confiabilidad que representa cada etapa definimos:

Para un primer nivel de seguridad se requiere el uso de sensores de apertura de puertas, los cuales, dan la primera alerta y para ello se deben conectar vía inalámbrica con el servidor.

Debido a lo accesible que resultan las ventanas se implementan varios sensores de apertura de ventanas las cuales deben también comunicarse inalámbricamente con el servidor para avisar los cambios que pueden presentarse.

Para un segundo nivel de seguridad se implementan sensores de presencia o movimiento los cuales una vez que detectan un cambio en el ambiente envían un aviso al servidor para un respectivo análisis y respuesta.

Para un tercer y último nivel de seguridad se implementa una cámara de video ubicada de tal manera que tenga una visión completa del ambiente. Esta cámara funciona a pedido del encargado y también debe activarse ante el registro de algún cambio proporcionado por el sensor de movimiento, esto para cumplir con un ahorro tanto de energía como de memoria en el disco duro del servidor en comparación a un grabado de información permanente.

Con el mismo criterio, la grabación se hará con baja resolución para lograr un mayor ahorro de memoria.

Por un tema de seguridad ante posibles incendios, ya que, el ambiente está lleno de equipos eléctricos y electrónicos se instalará un sensor de humo adecuadamente ubicado, el cual al detectar la anomalía enviará la información al servidor y además activará una sirena.

Debido a que es un sistema de seguridad, se instalan distintos tipos de alarma desde sonoras (sirenas, pitidos) hasta mensajes en la pantalla del servidor.

La comunicación entre los distintos dispositivos con el servidor se hace de manera inalámbrica por cuestiones de estética, practicidad y conveniencia, usando el protocolo adecuado para cumplir requisitos y tiempos de respuesta óptimos.

Finalmente, como es conocido en el Perú el factor económico es limitante, por tanto se usarán equipos que se pueden conseguir en tiendas electrónicas locales y supermercados a precios relativamente bajos, además se utilizará un servidor existente y protocolos de transmisión inalámbrica de libre uso.

2.4 SÍNTESIS SOBRE LA INVESTIGACIÓN

Un sistema domótico de seguridad debe ser implementado de tal manera que cumpla los requerimientos propios del local, como detección cuando una persona ingresa o sale, grabación de sesiones de laboratorio y en horas libres mediante la instalación de una cámara, sensores de movimiento tales que activen la cámara cuando la puerta esté cerrada así como detección de apertura de ventanas para caso de siniestros y como una medida más de seguridad.

También es necesario implementar un sensor de humo, ya que el laboratorio es propenso a cortocircuitos, esto, debido a la presencia de gran cantidad de equipos eléctricos y electrónicos, con el fin de avisar lo más rápido posible a las autoridades pertinentes para contrarrestar el fuego a tiempo.

Las tecnologías actuales permiten conseguir equipos muy variados y confiables de alta tecnología [1], pero resultan muy costosos, generalmente no resulta rentable el adquirirlos, por lo que tomamos como base para esta tesis la implementación de un sistema más simple y a la vez más económico sin descuidar el grado de protección.

Tanto la elección de los distintos sensores, detectores así como la ubicación de cada uno de ellos y el protocolo de comunicación con el que transmitirán la información deben ser seleccionados de tal manera que cumplan los requisitos que el nivel de protección deseado implica, tales como cobertura de sensado, resolución de cámaras, detecciones magnéticas confiables, duraciones de batería, tiempos de respuesta, velocidades de comunicación y que los precios estén dentro del presupuesto estimado.

CAPÍTULO 3

DISEÑO DE LA ETAPA DE ACONDICIONAMIENTO DE LA SEÑAL, LA COMUNICACIÓN Y LA VISUALIZACIÓN EN LA PC.

3.1 HIPÓTESIS DE LA INVESTIGACIÓN

3.1.1 Hipótesis principal

Dado que en el pabellón “V” de la Pontificia Universidad Católica del Perú , en especial el laboratorio V-104, cuenta con equipamiento costoso que posee mecanismos de seguridad ineficientes y no se toman medidas al respecto debido a la gran inversión que representa la implementación de un sistema domótico de seguridad usando dispositivos que se pueden adquirir localmente y usando un protocolo libre, y que podrían ayudar mucho a contrarrestar posibles siniestros, generando un ambiente seguro y supervisado.[7]

También es posible que en el futuro sea aplicado a otros laboratorios hasta ser extendido en oficinas y otros ambientes que lo ameriten.

3.1.2 Hipótesis secundarias

- 1) Las precarias medidas de seguridad que se presentan en el laboratorio (solo seguros en las puertas) representan un problema latente para no solamente robos, sino también de mal uso de equipos y por tanto posibles averías sin conocer los responsables hace necesario la implementación de un sistema que solucione estos problemas.
- 2) Un sistema conformado por equipos como cámaras, sensores de movimiento y detectores de puerta lograrían un ambiente seguro, siempre en control y supervisión resolviendo los problemas anteriormente mencionados.

- 3) Para el diseño del sistema se requiere de cuatro análisis, la elección de los dispositivos, el análisis de la ubicación, la elección del protocolo de comunicación y la elección del modo de interfase con el usuario, logrando con ello el nivel de seguridad deseado.
- 4) Para la elección de los dispositivos se toma en cuenta la accesibilidad de estos, los costos y el cumplimiento básico de los requerimientos del sistema como coberturas, resolución, etc.
- 5) La ubicación adecuada de los distintos dispositivos garantiza que el sistema no tenga fallas, logrando la cobertura adecuada de los puntos óptimos de sensado así como alerta ante incendios.
- 6) El uso del voltaje en la salida de alarma de los dispositivos pueden usarse como información ON/OFF y el supuesto envío de la trama de cambio de estado (Detección)
- 7) El uso del protocolo Zigbee permite un ahorro en el consumo, así como costos increíblemente bajos en el ámbito de comunicación entre cada uno de los dispositivos y el servidor además de garantizar un bajo consumo de energía lo que reduce costos de mantenimiento.[15]

3.2 OBJETIVOS DE LA INVESTIGACIÓN

3.2.1 Objetivo general

El objetivo principal es diseñar e implementar un sistema de seguridad usando sensores, detectores y cámaras de seguridad, los cuales puedan ser adquiridos en cualquier mercado local a precios cómodos realizando la comunicación inalámbricamente, usando un protocolo con banda de libre uso y con un servidor (computador) para su análisis y visualización.

3.2.2 Objetivos específicos

- 1) Encontrar los dispositivos requeridos para la implementación del sistema tomando en cuenta la comercialidad de los mismos, satisfacción de requisitos mínimos y costos bajos.
- 2) Analizar y ubicar los puntos óptimos donde serán colocados los dispositivos con el fin de proteger cada rincón y punto débil logrando dar una seguridad de alto nivel.
- 3) Diseñar e implementar la red inalámbrica usando el protocolo más adecuado para la seguridad en el laboratorio teniendo en cuenta la cobertura, velocidad de transmisión y posibilidad de implementación en circuitos de transmisión y recepción.
- 4) Optimizar la programación de los módulos de transmisión y recepción con el fin de enviar solo información ON/OFF, logrando que el tiempo de respuesta sea mínimo.
- 5) Acondicionamiento de la señal de los sensores de tal manera que cualquier dispositivo pueda ser usado para el envío de la información.
- 6) Optimizar la eficiencia del uso de la cámara de vigilancia, reduciendo la resolución y lograr facilidad de almacenaje al ocupar poca memoria.
- 7) Visualizar el cambio de estado de los sensores mediante ventanas emergentes en el computador (localmente o grandes distancias) usando algún software o método de análisis de recepción de tramas seriales.
- 8) Control y supervisión del laboratorio mediante registro de entradas y salidas, control de asistencia de alumnado y jefatura de práctica, supervisión en horas libres y control de fallas en los equipos y ubicación de responsables.

3.3 DISEÑO DE LA SOLUCIÓN:

El diseño de la solución será realizada en forma modular, donde cada módulo tiene sus características en particular pero a la vez comunes.

En una primera etapa se realizará el acondicionamiento de cada uno de los sensores. Esto consiste en utilizar alguna variación de voltaje en algún punto del circuito interno, debido al cambio o detección del sensor. Normalmente se usa el voltaje que aparece en la alarma sonora con la que cuenta el dispositivo, algún led que se enciende o la salida de algún integrado.

Esta variación de voltaje será transformado a una señal digital (0 y 1) a través de algunos circuitos integrados, transistores u otros métodos y serán las entradas para la siguiente etapa.

La segunda etapa consiste en el envío y recepción de la información recibida por medio inalámbrico, para ello se utilizará unos módulos de comunicación RF, Xbee, ya que se usará el protocolo Zigbee por sus ventajas y utilidades, tal y como se verá más adelante.

Para una tercera y última etapa se diseñará la visualización por parte del usuario, lo cual consiste en tomar la información recibida por el receptor inalámbrico usando un puerto de la computadora. Luego utilizando un entorno de programación gráfica, crear un programa que genera ventanas de alerta una vez detectada una trama de detección por parte de cualquiera de los sensores.

Cabe resaltar que la investigación y el diseño también incluyen la selección y ubicación de cada uno de los dispositivos de acuerdo a las características y precios de los mismos.

A continuación se muestre el esquema general de la solución: Ver Figura 1.

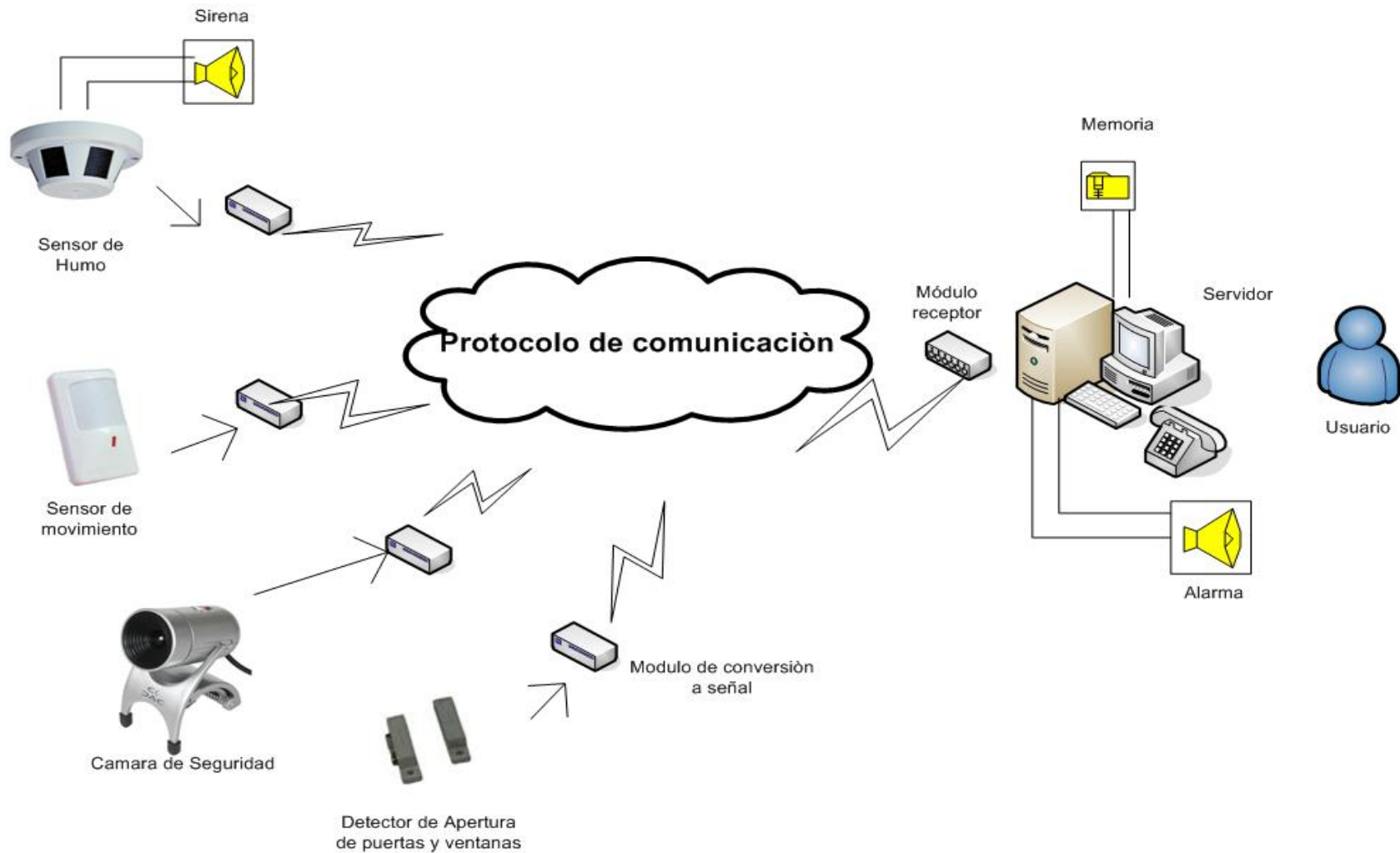


Figura 1 : Esquema de la solución - Elaborado por Aldo Zeballos

3.4 DISEÑO DEL ACONDICIONAMIENTO DE LOS SENSORES

3.4.1 Conceptos previos

Tecnología CMOS

En un circuito CMOS, la función lógica a sintetizar se implementa por duplicado mediante dos circuitos: uno basado exclusivamente en transistores pMOS, y otro basado exclusivamente en transistores nMOS. El circuito pMOS es empleado para propagar el valor binario **1**, y el circuito nMOS para propagar el valor binario **0**. Véase la figura 3.2. Representa una puerta lógica NOT o inversor. [9]

Ventajas

- El bajo consumo de potencia, gracias a la alta impedancia de entrada de los transistores de tipo MOSFET y a que, en estado de reposo, un circuito CMOS sólo experimentará corrientes parásitas.
- Gracias a su carácter regenerativo, los circuitos CMOS son robustos frente a ruido o degradación de señal debido a la impedancia del metal de interconexión.
- Los circuitos CMOS son sencillos de diseñar.
- La tecnología de fabricación está muy desarrollada, y es posible conseguir densidades de integración muy altas a un precio mucho menor que otras tecnologías.
- Permite un amplio rango de entradas de voltaje y en función a eso un amplio rango de voltajes de señales digitales o analógicas.

Circuito Negador:

Se basa en una puerta lógica la cual activa la salida cuando la entrada es cero y desactiva la salida cuando hay voltaje en la entrada. Se usará para invertir el flanco de subida en un flanco de bajada. [9]



Figura 3.2: Negador (símbolo y tabla de verdad)

Diodo Zener:

Un **diodo Zener**, es un diodo de silicio que se ha construido para que funcione en las zonas de rupturas. Llamados a veces diodos de avalancha o de ruptura, el diodo zener es la parte esencial de los reguladores de tensión casi constantes con independencia de que se presenten grandes variaciones de la tensión de red, de la resistencia de carga y temperatura.[9]



Figura 3.3: Diodo Zener (símbolo y vista real)

Transistor (corte –Saturación) [9]

Cuando un **transistor** se utiliza como interruptor o switch la corriente de base debe tener un valor para lograr que el **transistor** entre en corte y otro para que entre en saturación, esto se logra con una resistencia en el colector >10 veces la resistencia de la base. ($R_c > 10R_b$) Ver Figura 3.5

- Un **transistor en corte** tiene una corriente de colector (I_c) mínima (prácticamente igual a cero) y un voltaje colector emisor (V_{CE}) máximo (casi igual al voltaje de alimentación). Ver Figura 3.5-Corte

- Un **transistor en saturación** tiene una corriente de colector (I_c) máxima y un voltaje colector emisor (V_{CE}) casi nulo (cero voltios). Ver Figura 3.5-Saturación

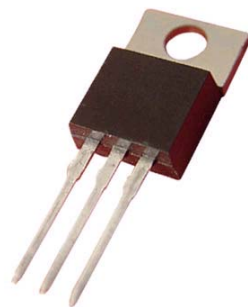


Figura 3.4: Transistor (www.compucanjes.com)

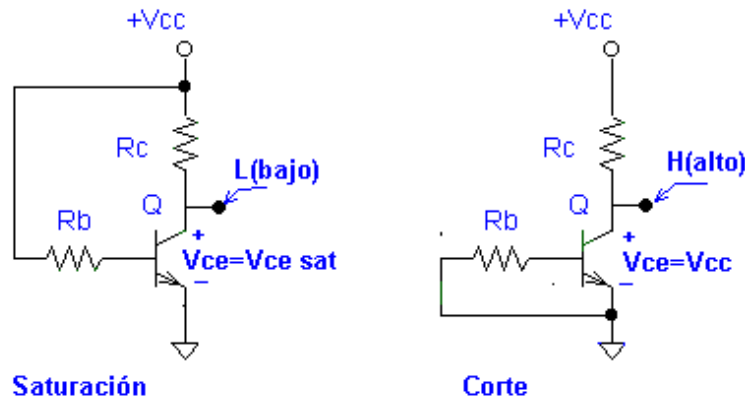


Figura 3.5: Corte - Saturación

3.4.2 Sensor de movimiento - Acondicionamiento

De acuerdo a la infraestructura del laboratorio y a la ubicación del sensor, este debe ser capaz de detectar la presencia de un individuo en el pasillo y la zona de computadoras (Ver figuras 3.8 y 3.9). El sensor debe contar con una alarma la cual se usará como flanco (disparo) para el envío de la información de activación mediante un circuito de acondicionamiento y un modulo de transmisión inalámbrica.



Figura 3.6: Sensor de movimiento



Figura 3.7: Ubicación

Características del sensor a usar [1]:

- Marca Boston Technologies.
- Batería de 9V DC.
- Rango de detección de 60°.
- Distancia de detección de 8m.
- Velocidad de detección de 0.6 – 1.5 m/s.
- Tecnología de rayos infrarrojos.

Diseño de la ubicación:

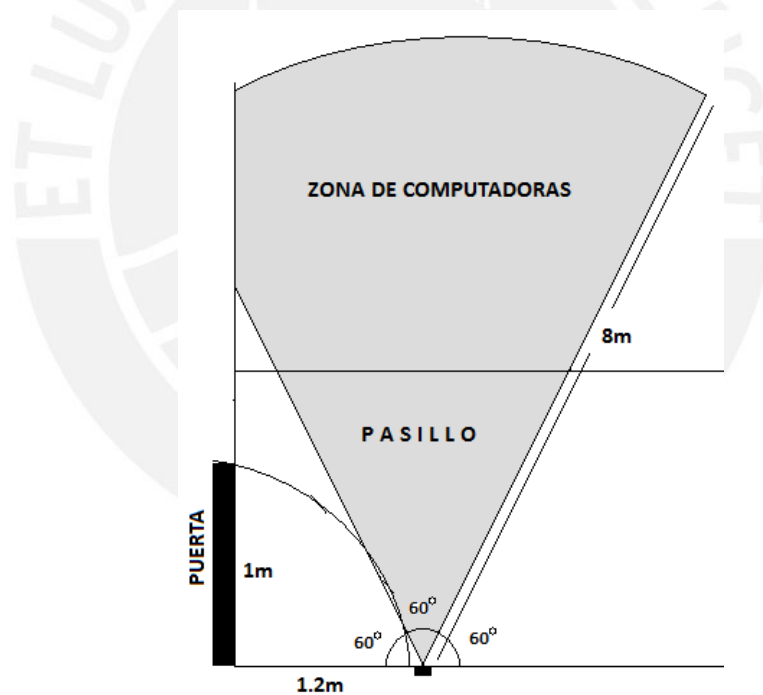


Figura 3.8: Rango del sensor de movimiento (vista superior)

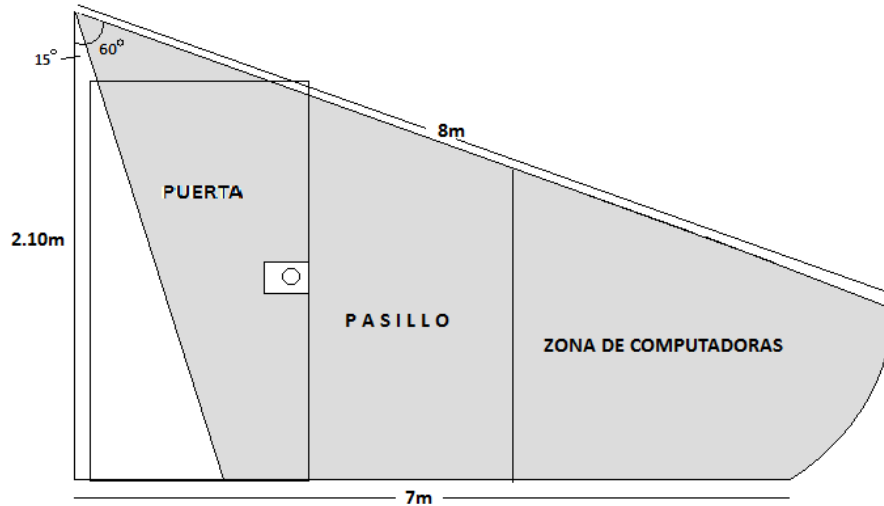


Figura 3.9: Rango del sensor de movimiento (vista lateral)

Diseño del acondicionamiento de la señal de detección:

El sensor cuenta con una salida de 0 voltios cuando no está activado y de 8.5 voltios cuando se detecta movimiento (representado por la alarma), este flanco de subida es acoplado a una compuerta negadora (integrado CMOS 4069) para invertir el flanco. Se usará un Zener con el fin de enclavar el voltaje a 3.3V.

El detalle del conexionado se ve en los diagramas esquemáticos siguientes:

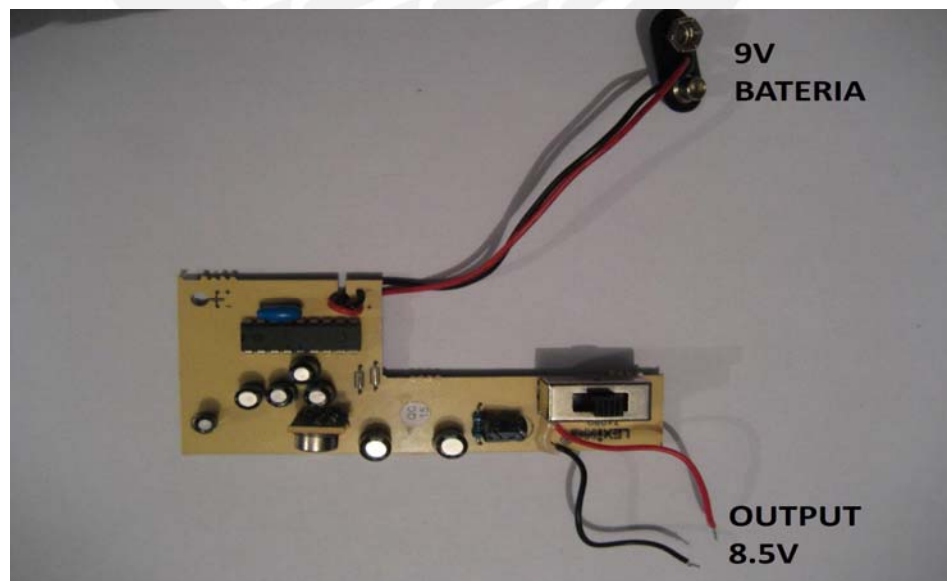


Figura 3.10: Chip sensor de movimiento

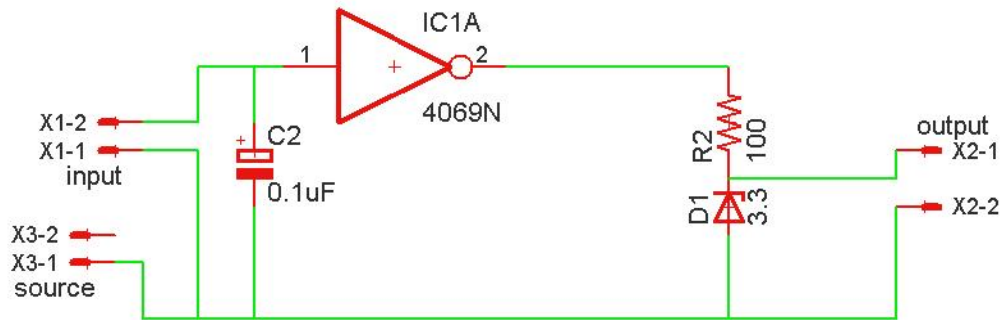


Figura 3.11: Esquemático acondicionamiento del sensor de movimiento

- Las entradas X1-1 y X1-2 representan la entrada de las alarmas (flanco de subida-8.5V).
- Las salidas X2-1 y X2-2 representan las salidas estables a ser enviadas por radiofrecuencia y su referencia a tierra. (3.3V y 0V).
- Las entradas X3-1 y X3-2 representan la alimentación del integrado CMOS, 9V de la fuente de la batería.

El diagrama de conexionado real en el circuito impreso es el siguiente:

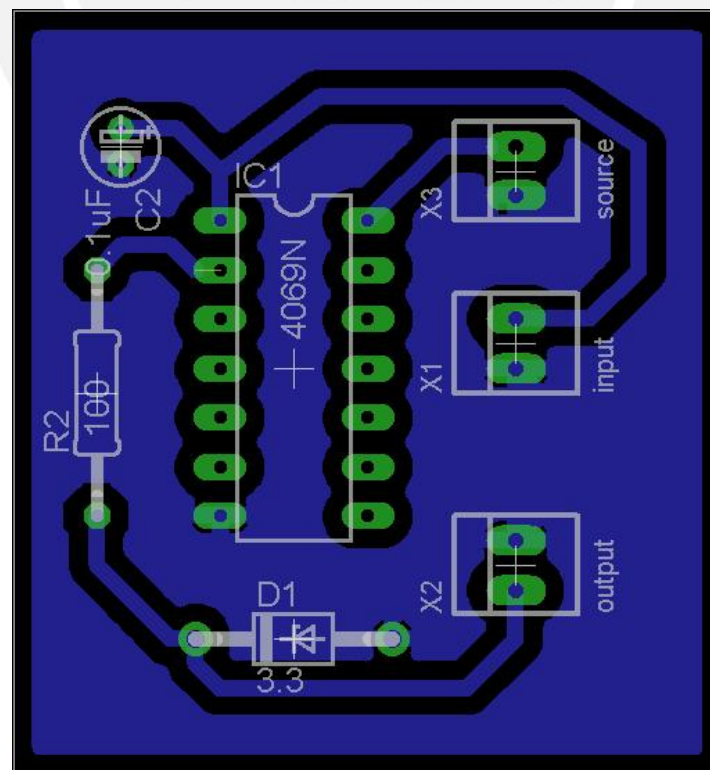


Figura 3.12: Diagrama real de conexionado (Board)

3.4.3 Sensor de humo - Acondicionamiento

De acuerdo a la infraestructura del laboratorio, el sensor debe ser ubicado en la zona mas adecuada del mismo de tal manera que se encuentre lo mas cerca posible del foco mas probable de aparición de humo, y esto es en la zona inmediatamente encima de las computadoras y mesas de pruebas, muy cercana a la zona central del laboratorio, por ello se ubicará aprovechando la columna superior tal como se muestra en la figura 3.14.

El sensor debe contar con una alarma la cual se usara como flanco (disparo) para el envío de la información de activación mediante un circuito de acondicionamiento y un módulo de transmisión inalámbrica.



Figura 3.13: Sensor de humo

Figura 3.14: Ubicación

Características del sensor: [1]

- Marca Boston Technologies.
- Batería de 9V DC.
- Tecnología fotoeléctrica.
- Alarma de 85dB.

Diseño del acondicionamiento de la señal de detección:

El sensor cuenta con un botón de test de funcionamiento, y será usado como disparador para las pruebas de conexión, esto debido a que la cámara de sensado es muy sensible y propensa a averiarse con pruebas seguidas de humo real.

En la salida de la pata 16 (Test), aparecen 0 V cuando el pulsador se encuentra en reposo y 9V cuando se presiona el pulsador.

El detalle del conexionado se ve en los diagramas esquemáticos siguientes:

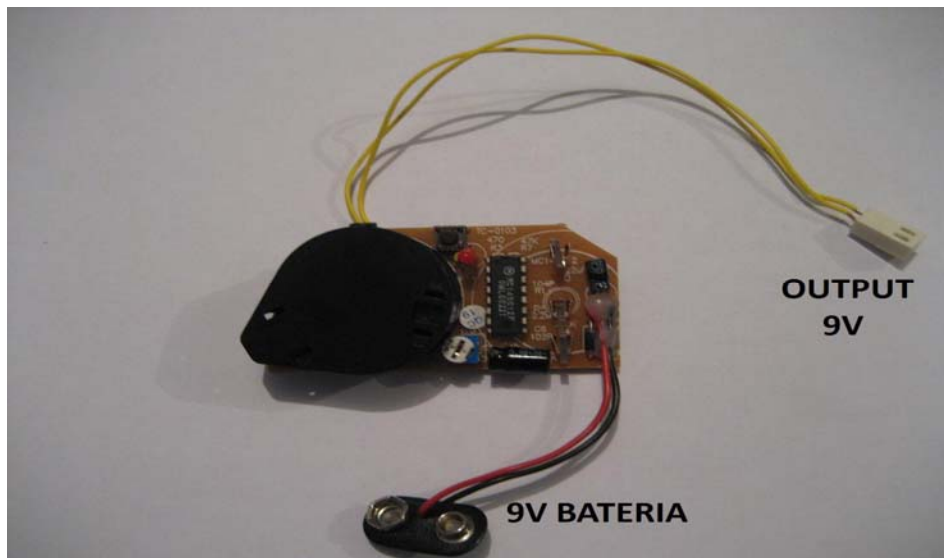


Figura 3.15: Chip Sensor de humo

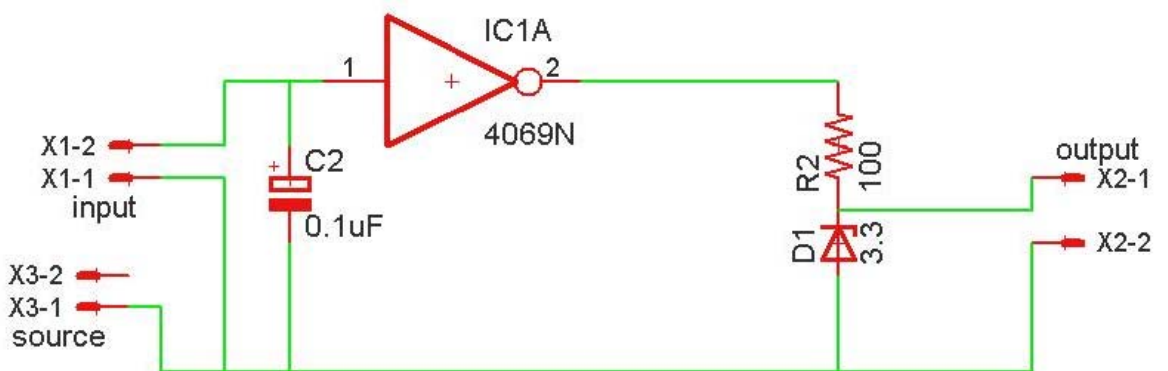


Figura 3.16: Esquemático del acondicionamiento

- Las entradas X1-1 y X1-2 representan la entrada de las alarmas (flanco de subida - 9V).

- Las salidas X2-1 y X2-2 representan las salidas estables a ser enviadas por radiofrecuencia y su referencia a tierra. (3.3V y 0V).
- Las entradas X3-1 y X3-2 representan la alimentación del integrado CMOS, 9V de la fuente de la batería.

El diagrama de conexionado real en el circuito impreso es el siguiente:

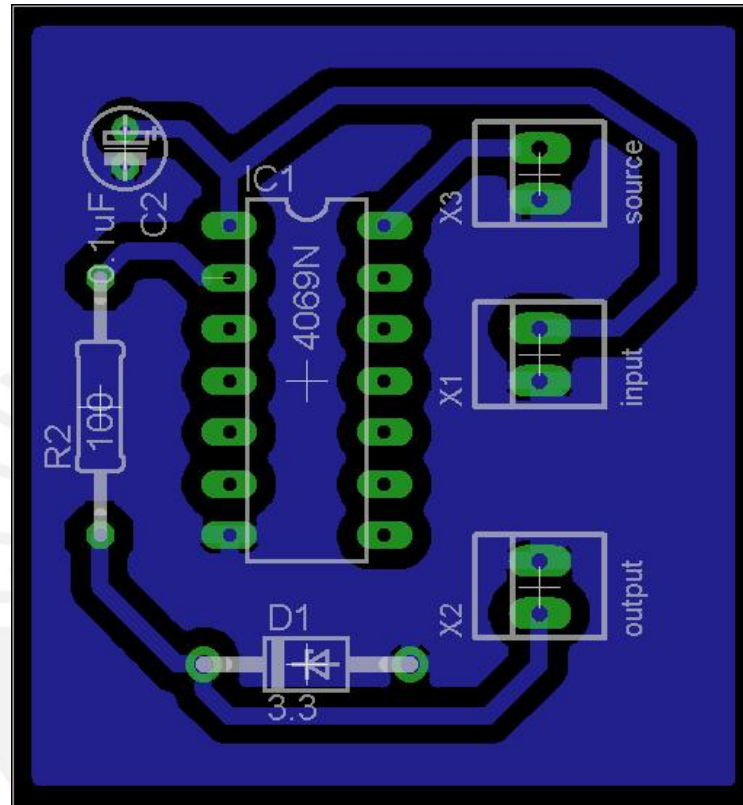


Figura 3.17: Diagrama real de conexionado (Board)

3.4.4 Detector de apertura de puertas y ventanas - Acondicionamiento

De acuerdo a la estructura del laboratorio, se cuenta con 2 puertas, y un panel de ventanas, por lo cual es conveniente la implementación de una serie de detectores de apertura de forma masiva y por tanto de bajo coste. Se ubicará en la parte superior del marco de la puerta.



Figura 3.18: Detector de aperturas

Figura 3.19: Ubicación del detector

Características del Detector a usar: [1]

- Modelo genérico RL-9805
- Fácil de montar en puerta o ventana a través de una pegatina.
- Usa un sensor magnético para la detección. (Bajo costo).
- Uso de 3 pilas tipo botón de 1.5V. (Incluidas).
- Salida de 2.5V.
- Alarma de 90dB.
- Botón de apagado/encendido para mayor comodidad.

Diseño del acondicionamiento de la señal de detección:

Debido a que el sensor cuenta con un voltaje de 2.5V en los extremos del switch, cuando este es activado, se usará el mismo como voltaje de saturación del transistor (Configurado en corte y saturación mediante resistencias de 300Ω y $5K\Omega$).

Cuando el voltaje en la entrada es 0V el transistor se encuentra en corte y el voltaje en la salida es el mismo que en la entrada del colector, 3.3V.

El detalle del conexionado se ve en los diagramas esquemáticos siguientes:

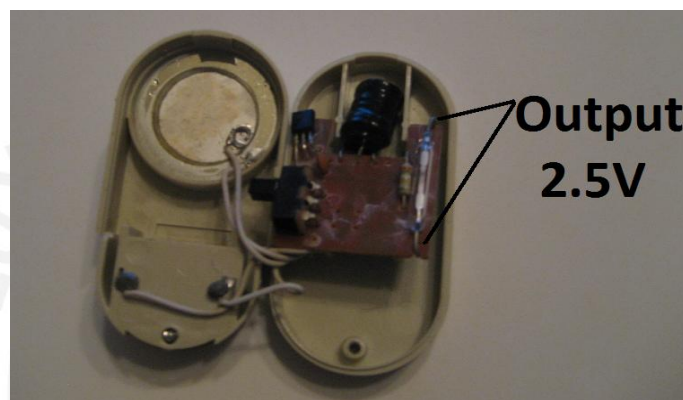


Figura 3.20: Chip del detector

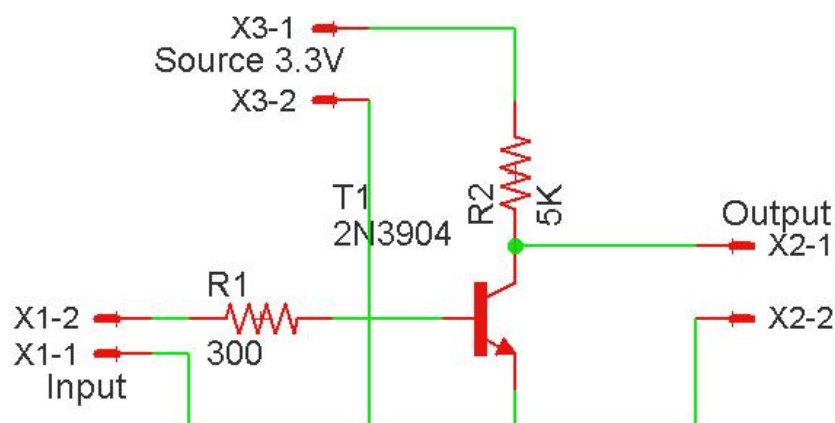


Figura 3.21: Esquemático del acondicionamiento

- Donde las entradas X1-1 y X1-2 son la salida de voltaje del interruptor magnético del chip del detector. (0V y 2.5V).

- Las entradas X3-1 y X3-2 son la fuente de alimentación del colector 3.3V. Este será el voltaje a la salida del circuito de acondicionamiento cuando el transistor se encuentre en corte.
- La Salida X2-1 y X2-2 serán las entradas al circuito transmisor RF (Xbee terminal), con voltajes de 0V y 3.3V.

El diagrama de conexionado real en el circuito impreso es el siguiente:

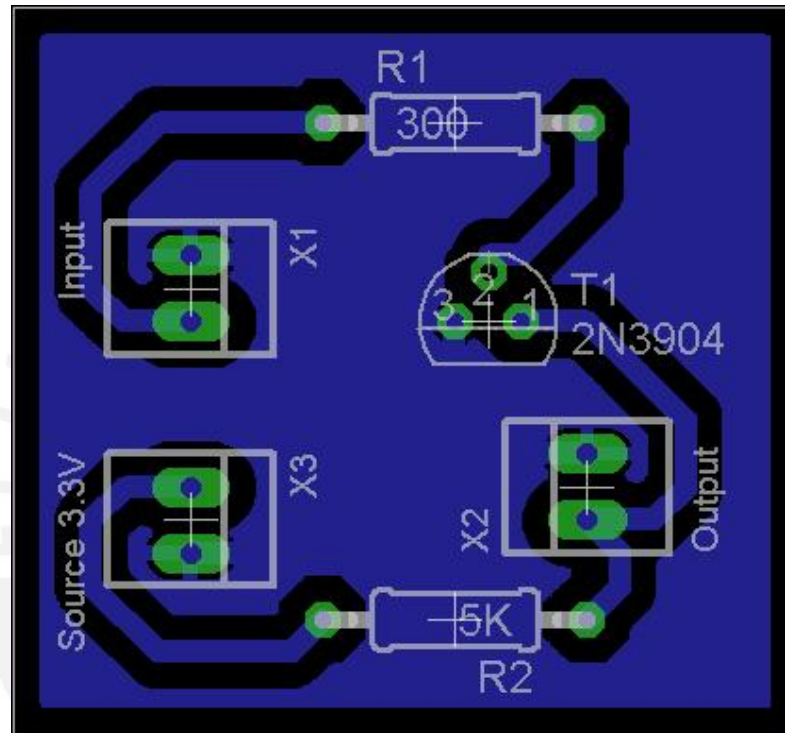


Figura 3.22: Diagrama real de conexionado (Board)

3.4.5 Cámara de seguridad - Implementación

Requisitos:

- Cámara tipo inalámbrica con transmisión RF.
- Rango de visión de 15m.
- Angulo de visibilidad de 60 grados.
- Captura de video – Software de análisis.
- Visión nocturna.



Figura 3.23: Cámara



Figura 3.24: Ubicación

Características de la cámara a utilizar:

- Marca Astak
- Cámara de seguridad CCD inalámbrica en color con visión nocturna apto también para exteriores (Weatherproof).
- 12 LED Infrarrojo integrados para la visión nocturna.
- Calidad profesional y diseño duradero, conexión a VCR o Televisión mediante cables RCA.
- No necesita cables, instalación en 5 minutos.

- Integra micrófono.
- Imagen de alta calidad.

-Rango de 50 a 90 metros con línea directa de visión (se reducirá por obstáculos y paredes)

Será ubicado en la parte superior izquierda del laboratorio (Ver figura 3.24), debido a que combina el rango completo de visibilidad que se consigue desde cualquier esquina y la prioridad que se requiere de visualización de la puerta.

RCA

El conector RCA es un tipo de conector eléctrico común en el mercado automotor. El nombre "RCA" deriva de la Radio Corporation of America, y es el más usado cuando de equipos de audio y video se trata.



Figura 3.25: Conector RCA

Su principal desventaja es que en el sistema RCA cada señal necesita su propio cable, además las computadoras de escritorio normalmente no tienen interfaz para su implementación, por lo que será necesario un adaptador hacia USB para visualizar las imágenes en el monitor. [9]

Adaptador RCA –USB

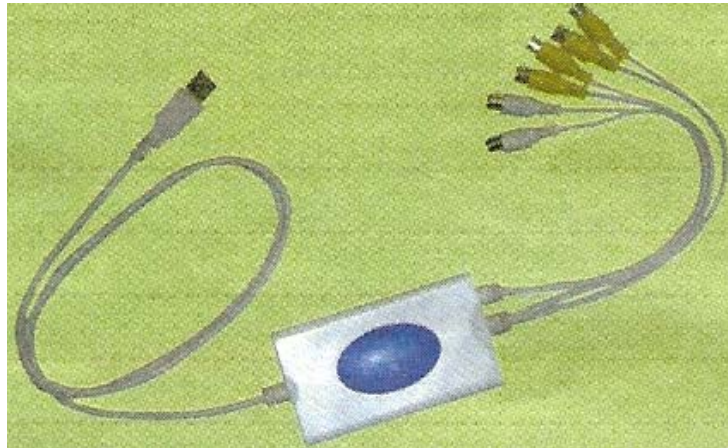


Figura 3.26: Adaptador RCA - USB

Características y Funciones:

- Soporta sistema de vigilancia remota a través de internet.
- Calidad de grabación programable de 1 a 30 cps.
- Función de reproducción remota.
- 4 entradas de video en una tarjeta.
- 4 diferentes modos de visualización.
- Compresión de video MPGE4.

Se utilizará para conectar la salida RCA y a la PC mediante el puerto USB para observar la cámara en la pantalla del computador.

3.5 DISEÑO DE LA COMUNICACIÓN

3.5.1 Módulos Xbee

Los módulos de RF Xbee están basados bajo el estándar Zigbee 802.15.4, esta tecnología garantiza un bajo consumo energético sin disminuir el excelente desenvolvimiento propio de las comunicaciones RF.

Estos módulos permiten la adquisición de los datos o las señales de otros dispositivos (sensores, integrados, señales directas) mediante sus puertos analógicos y digitales y ser enviados inalámbricamente a otros módulos.

Del mismo modo permiten la comunicación con microprocesadores o computadoras por los mismo puertos para analizar, controlar o mostrar la información recibida mediante un software o programación.

Maxstream es una compañía especializada en tecnología inalámbrica en circuitos electrónicos, diseñando y manufacturando tecnología de 900MHz y 2.4GHZ y los módulos Xbee que serán utilizados en esta tesis.

Existen dos tecnologías con distintas prestaciones en lo que a módulos Xbee se refiere, son los módulos Xbee y Xbee pro. A continuación se presenta un cuadro comparativo entre las mismas: [22]



Rendimiento	Ambientes interiores	Hasta 30m	Hasta 100m
	Ambientes exteriores	Hasta 100m	Hasta 1200 m
	Potencia de Salida	1 mW (0 dBm)	60 mW (18 dBm)
	WB	250 Kbps	250 Kbps
Requerimiento de Potencia	Suministro de Voltaje	2.8 – 3.4 V	2.8 – 3.4 V
Información General	Frecuencia	ISM 2.4 GHz	ISM 2.4 GHz
	Dimensiones	2.438 cm * 2.761 cm	2.438 cm * 3.294 cm
	Temperatura de Operación	-40 a 85 C	-40 a 85 C
Trabajo en Red	Topologías permitidas	Punto a Punto, Punto a Multipunto y Mesh	Punto a Punto, Punto a Multipunto y Mesh
	Número de canales	16 canales de secuencia directa	12 canales de secuencia directa

Tabla 2. Cuadro comparativo entre módulos Xbee y el Xbee-Pro [20], [22]

3.5.2 ¿Por qué Zigbee?

ZigBee está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal área Newark, WPAN) y tiene como objetivo las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

ZigBee es un sistema ideal para redes domóticas, específicamente diseñado para reemplazar la proliferación de sensores/actuadores individuales. ZigBee fue creado para cubrir la necesidad del mercado de un sistema a bajo coste, un estándar para redes Wireless de pequeños paquetes de información, bajo consumo, seguro y fiable. [8], [20].

En la siguiente figura se muestra el crecimiento progresivo en ventas y uso de la Tecnología Zigbee a nivel mundial, se espera unos venta de 5 millones de equipos basados en Zigbee para el 2010.

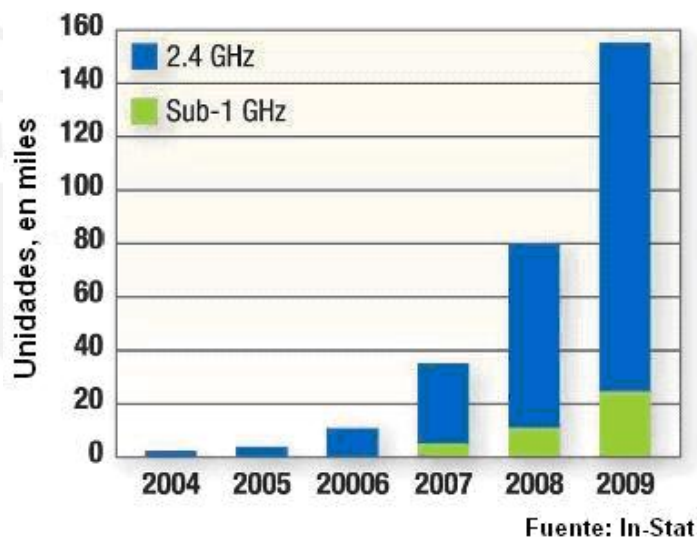


Figura 3.27: Crecimiento ventas Zigbee – (<http://www.eetasia.com>)

Ventajas:

- Ideal para conexiones punto a punto y punto a multipunto.
- Diseñado para el direccionamiento de información y el refrescamiento de la red.
- Opera en la banda libre de ISM 2.4 GHz para conexiones inalámbricas.

- Óptimo para redes de baja tasa de transferencia de datos. (Diferencia con Bluetooth)
- Alojamiento de 16 bits a 64 bits de dirección extendida.
- Reduce tiempos de espera en el envío y recepción de paquetes.
- Detección de Energía (ED).
- Bajo ciclo de trabajo - Proporciona larga duración de la batería. (Ventaja sobre todas las tecnologías)
- Soporte para múltiples topologías de red: Estática, dinámica, estrella y malla.
Hasta 65.000 nodos en una red. (Ventaja sobre todas las tecnologías).
- 128-bit AES de cifrado - Provee conexiones seguras entre dispositivos.
- Son más baratos y de construcción más sencilla.

Desventajas:

- La tasa de transferencia es muy baja. (Sacrifica ancho de banda)
- Solo manipula textos pequeños comparados con otras tecnologías. (Ideal para sensado)
- Zigbee trabaja de manera que no puede ser compatible con Bluetooth en todos sus aspectos porque no llegan a tener las mismas tasas de transferencia, ni la misma capacidad de soporte para nodos.
- Tiene menor cobertura porque pertenece a redes inalámbricas de tipo WPAN. (Pero mayor que Bluetooth)

3.5.3 Receptor – Nodo principal (Coordinador)

Es el tipo de dispositivo más completo. Debe existir uno por red y sus funciones son las de encargarse de controlar la red y los caminos que deben seguir los dispositivos para conectarse entre ellos, requiere memoria y capacidad de computación.

El equipo Coordinador es el encargado de recolectar la información sensada de los equipos terminales y mostrarla en la PC mediante el uso del software XCTU.

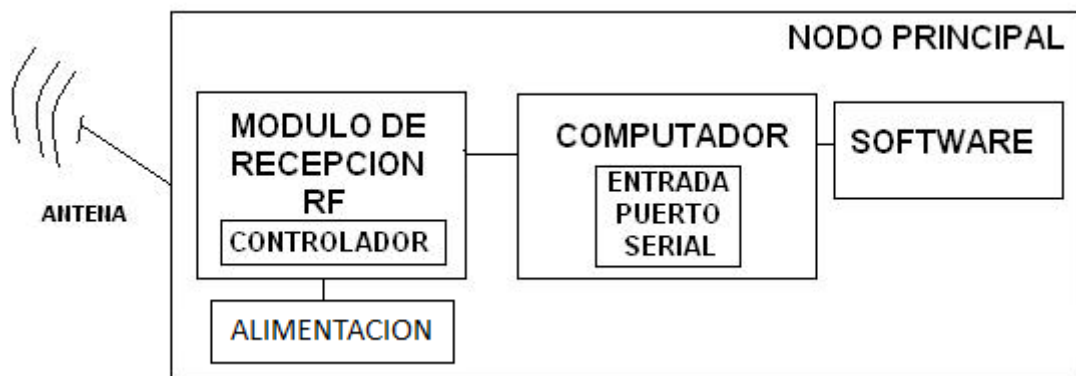


Figura 3.28: Diagrama de bloques - Coordinador

El conexionado del modulo de recepción incluye:

- Modulo Xbee de recepción.
- Circuito de alimentación de 5 y 3.3V.
- Modulo de comunicación serial (Max232).

El diagrama esquemático de la alimentación se muestra a continuación:

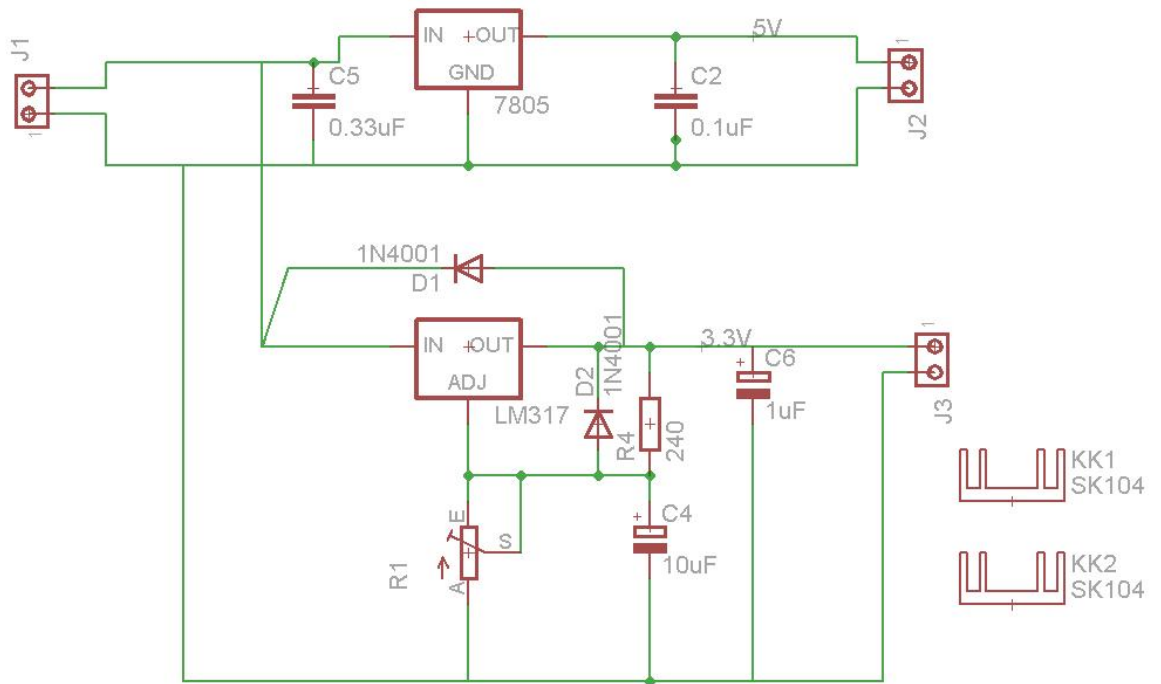


Figura 3.29: Esquemático de la alimentación

Donde:

- J1 son las entradas de la batería de 9V (Alimentación general).
- J2 son las salidas referenciales de 5V (Alimentación del Max232).
- J3 son las salidas referenciales de 3.3V (Alimentación del Xbee).

El integrado 7805 es usado para generar la fuente regulada de voltaje a 5V.

El integrado LM317 es usado para generar la fuente regulada de 3.3V.

Se usará un disipador (SK104) para cada integrado con el fin de evitar sobrecalentamiento de los mismos.

El diagrama esquemático del modulo Xbee de Recepción junto con el del conexionado del Max232 se muestra a continuación:

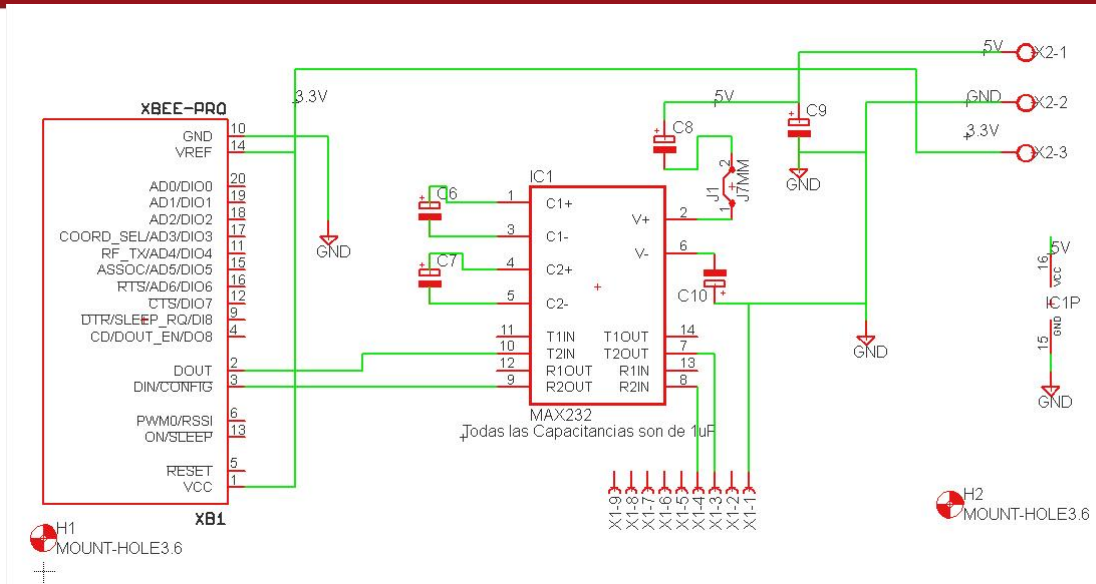


Figura 3.30: Esquemático Coordinador

Donde los pines:

X2-1, X2-2 y X2-3, son las entradas de alimentación en 5, 3.3v y tierra.

X1-1, X1-3 y X1-4 son las líneas de comunicación por cable RS232 al computador.

Solo se usará una salida digital (pin 2) y es el dato que determinará si se detectó algún cambio en el ambiente por alguno de los sensores.

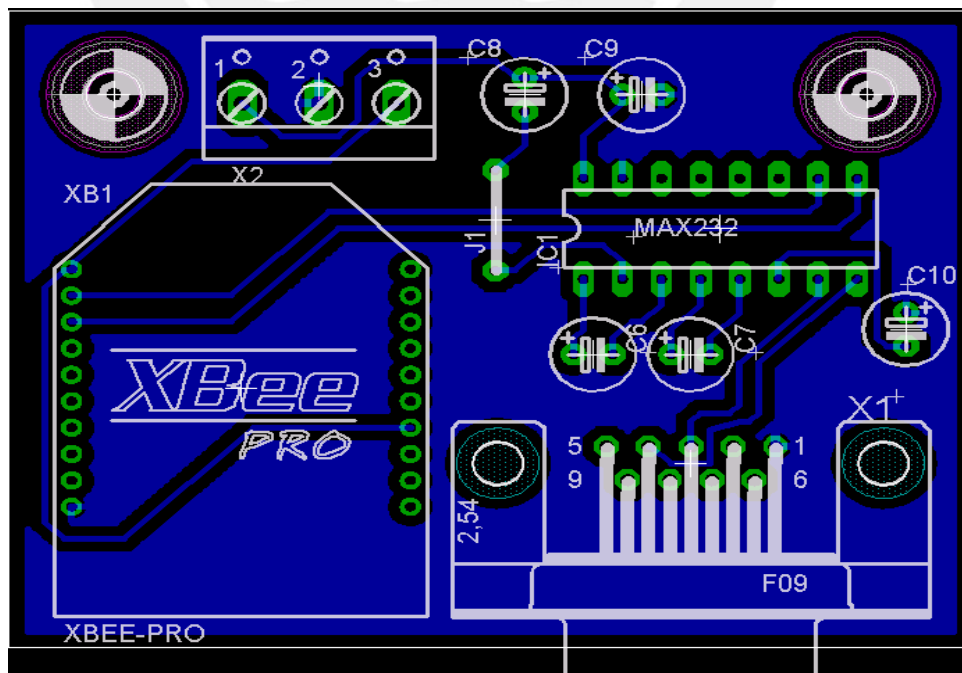


Figura 3.31: Board Coordinador

3.5.4 Transmisor – Nodo remoto

Posee las funciones necesarias para comunicarse y enviar la información proveniente de los sensores al nodo coordinador, pero no puede transmitir información destinada a otros dispositivos. De esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías. Posee requerimientos mínimos de memoria y es por tanto significativamente más barato.

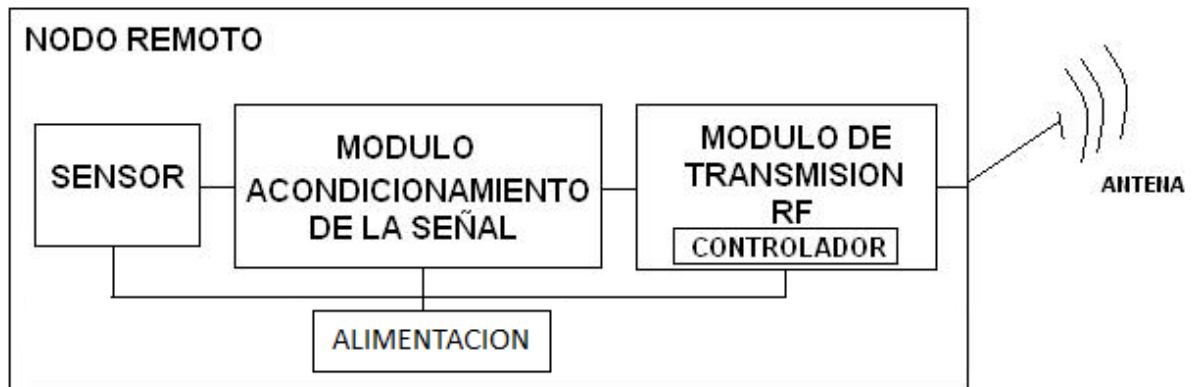


Figura 3.32: Diagrama de bloques del Terminal

El conexionado del modulo de transmisión incluye:

- Modulo Xbee de transmisión
- Circuito de alimentación de 5 y 3.3V
- Modulo de acondicionamiento de la señal

El diagrama esquemático de la alimentación se muestra a continuación:

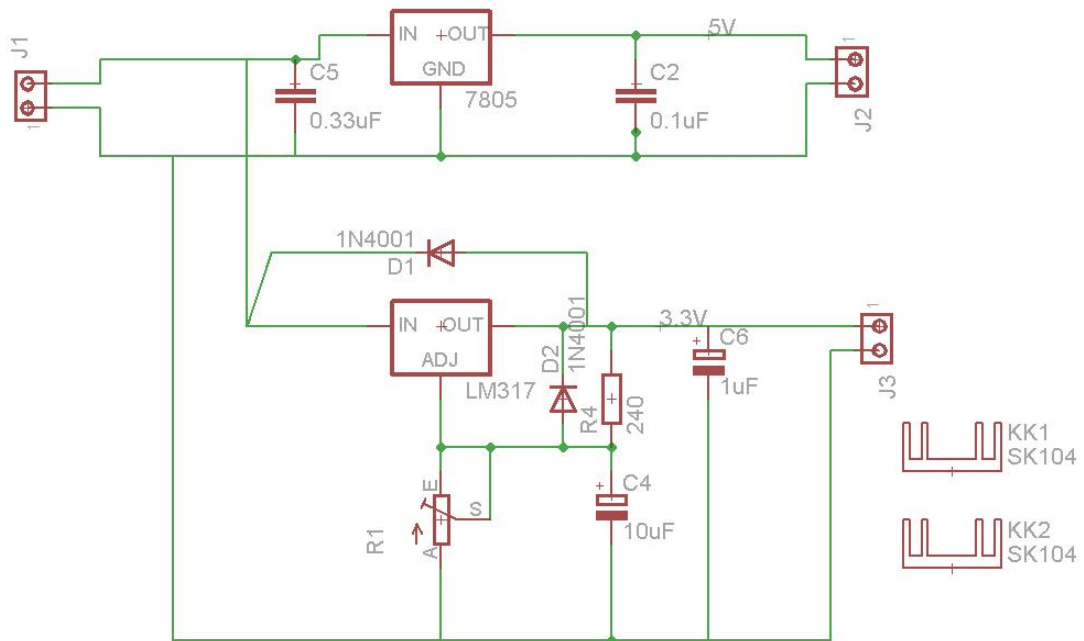


Figura 3.33: Esquemático de la alimentación

Donde:

- J1 son las entradas de la batería de 9V (Alimentación general)
- J2 son las salidas referenciales de 5V (Alimentación del 555)
- J3 son las salidas referenciales de 3.3V (Alimentación del Xbee)

El integrado 7805 es usado para generar la fuente regulada de voltaje a 5V.

El integrado LM317 es usado para generar la fuente regulada de 3.3V.

Se usará un disipador (SK104) para cada integrado con el fin de evitar sobrecalentamiento de los mismos.

El diagrama del modulo de acondicionamiento de la señal se encuentra en el diseño del acondicionamiento de la señal de cada de uno de los sensores. Ver 3.4.2, 3.4.3 y 3.4.4.

El diagrama esquemático del modulo Xbee de Transmisión se muestra a continuación:

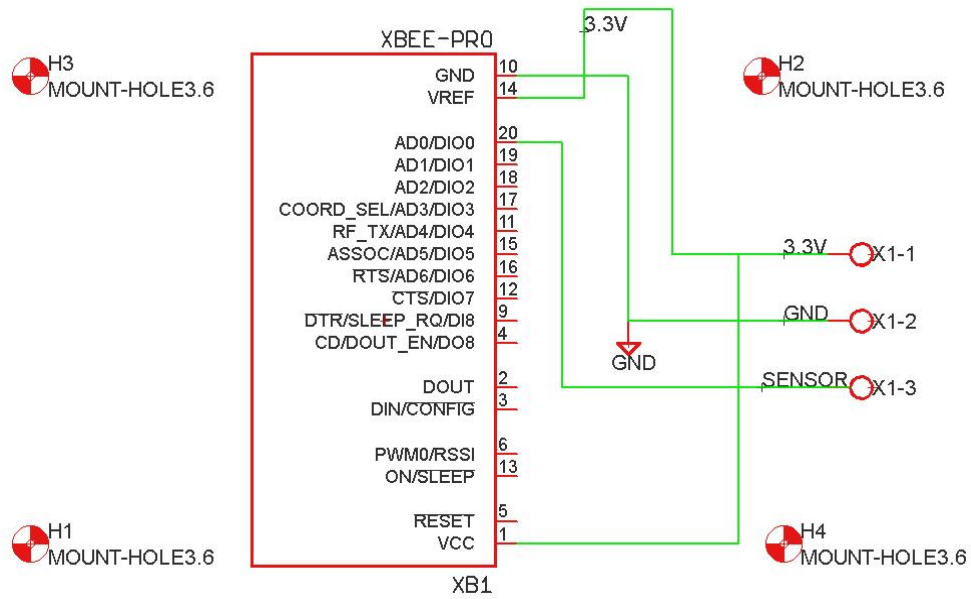


Figura 3.34: Esquemático del Terminal

El mismo circuito será usado para cada uno los sensores, una vez acondicionada la señal de salida de cada uno de los mismos, esta será la entrada digital al pin 20 a través de la entrada X1-3 de su respectivo circuito.

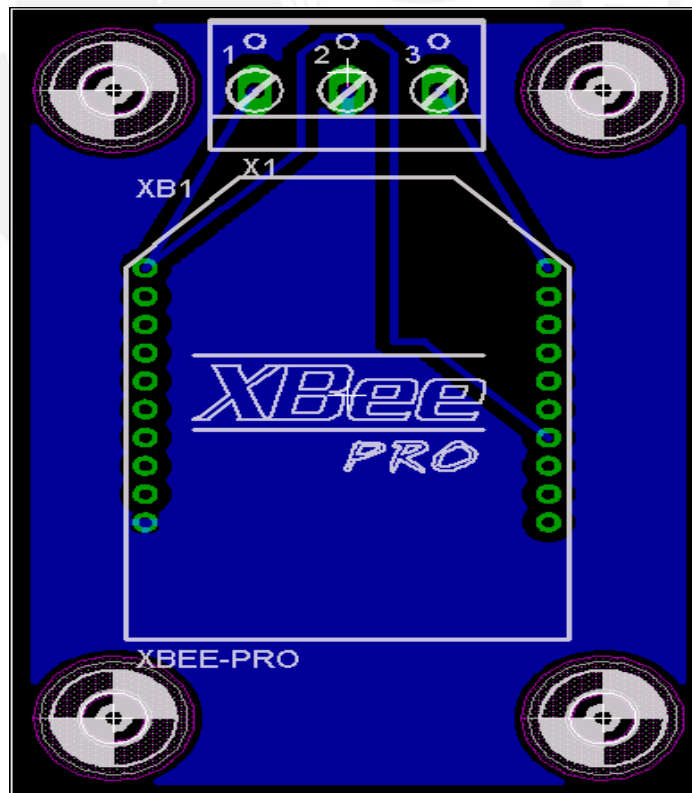


Figura 3.35: Board Transmisor

3.6 DISEÑO DE LA INTERFAZ CON EL USUARIO

Instalación:

El archivo ejecutable así como el código en Visual Basic se encuentran en el CD de contenidos.

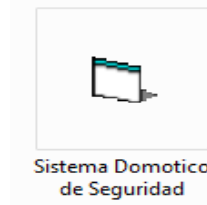


Figura 3.36: Icono de programa

Menú Principal:



Figura 3.37: Vista programa

1. 1. Permite la observación del laboratorio en pantalla de la computadora.
2. 2. Abre un block de notas con el registro de los últimos eventos.

Ventanas de Alerta:



Figura 3.38: Ventana de alerta

- 1.- Abre un block de notas con el registro de los últimos eventos.
- 2.- Cierra la ventana de alerta.

3.6.1 Funcionamiento del Software

Diagrama de flujo del programa principal en Visual Basic 6.0

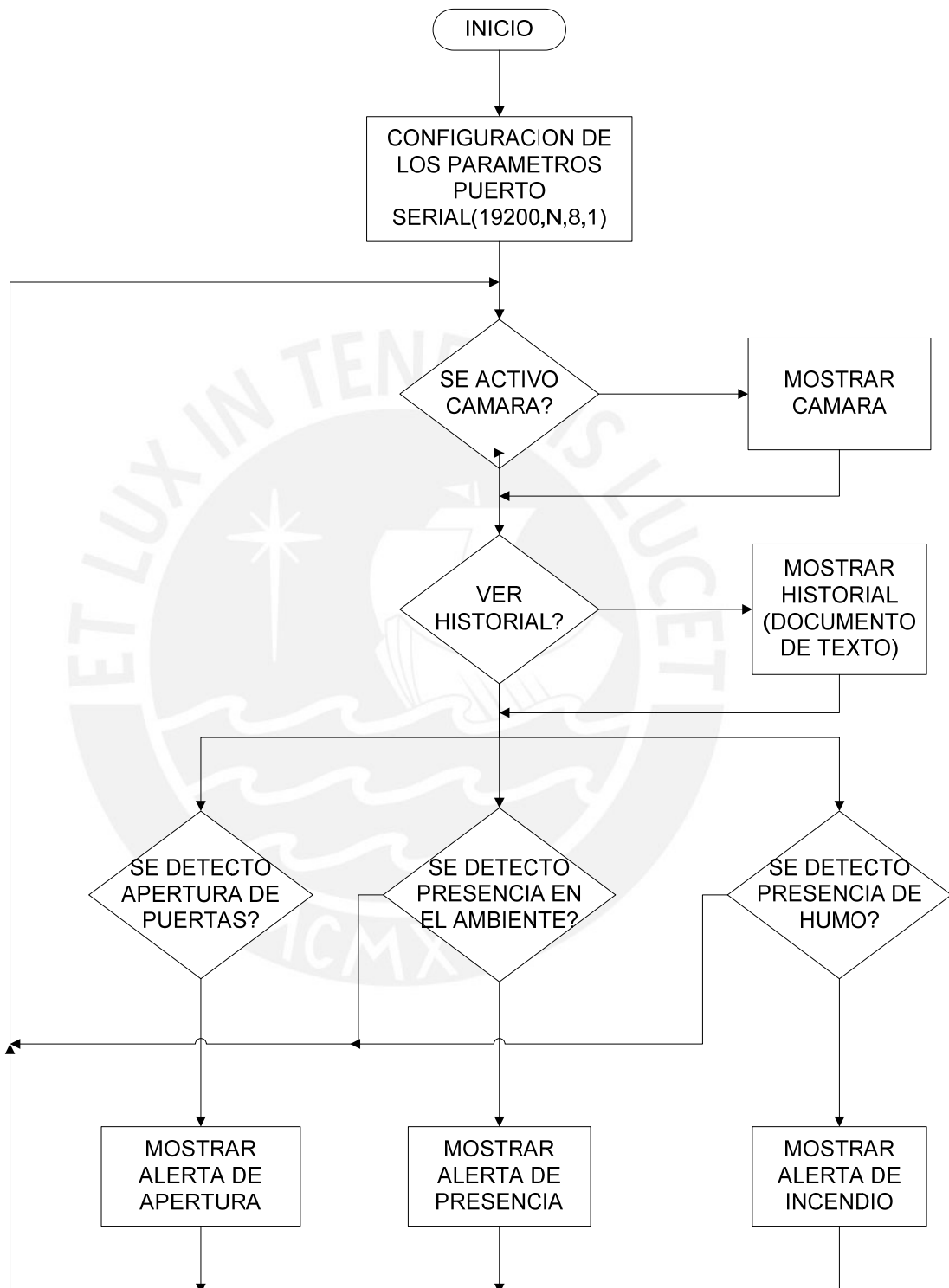


Figura 3.39: Diagrama de flujo – Programa General

Diagrama de flujo - Detección de cambio en los sensores

Usando las tramas de recepción como base, ver capítulos 4.3 y 4.4

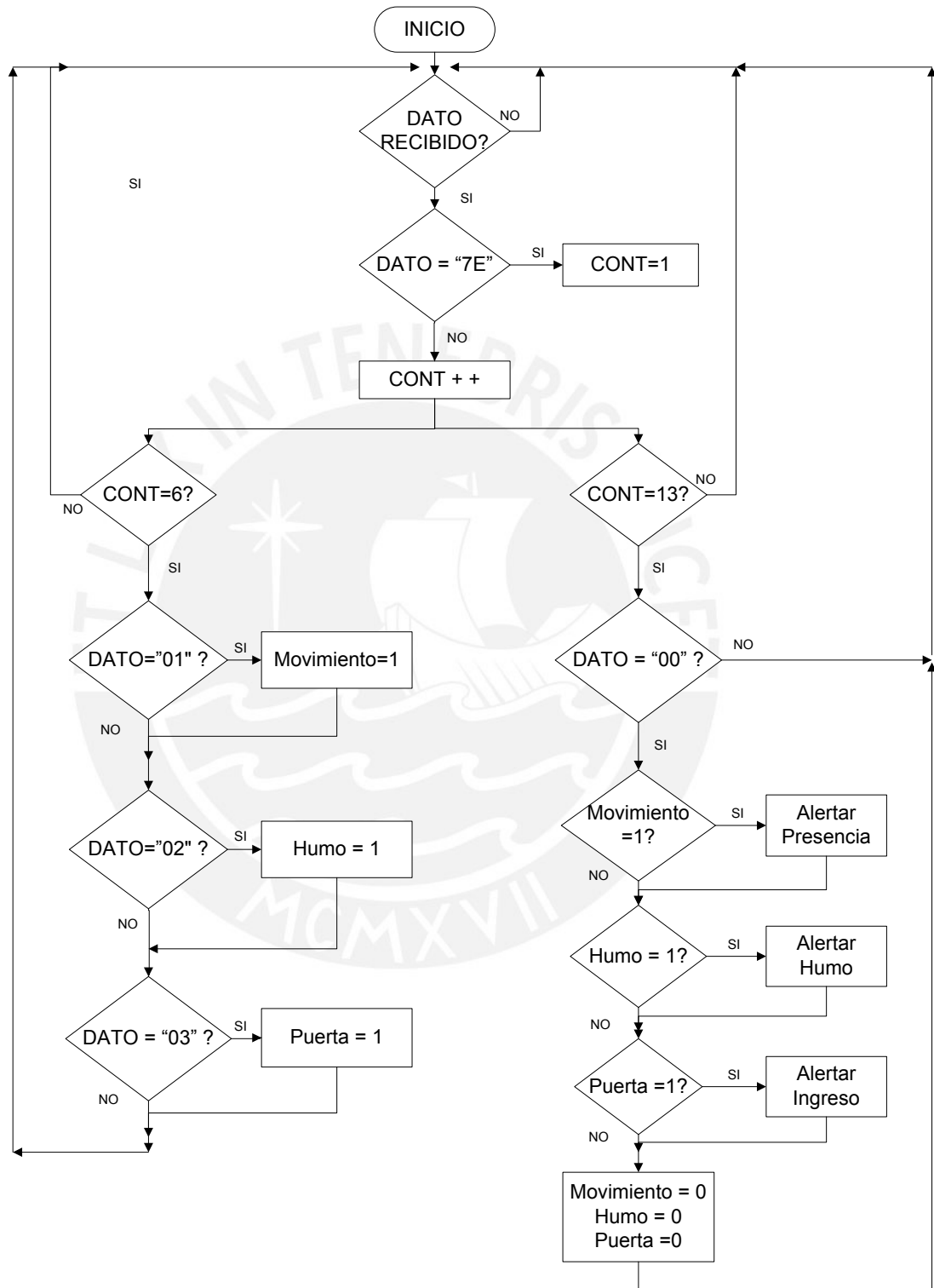


Figura 3.40: Diagrama de flujo de la detección

CAPÍTULO 4:

PRUEBAS DE LA RED DE COMUNICACIÓN USANDO XBEE, VISUALIZACIÓN DEL ESTADO DE LOS SENSORES EN LA PC.

4.1 INSTALACIÓN Y USO DEL PROGRAMA XCTU:

El programa XCTU es un software de uso libre cuya función es la de programar cada uno de los módulos Xbee. A través del mismo se define si el modulo será coordinador o nodo remoto, así como otros parámetros como (comunicación serial, visualización de tramas, etc.)

A continuación se muestran los pasos para instalar y usar el programa:

1.- Para descargar el software en línea Ingresar a la página web de Maxstream: <http://www.digi.com/support/productdefl.jsp?pid=3352&osvid=57&tp=4&s=316>.

2.- Acceder al icono de escritorio una vez instalado:



X-ctu.lnk

3.- Hacer click en la opción “Download new versions” con el fin de actualizar las bases del programa.

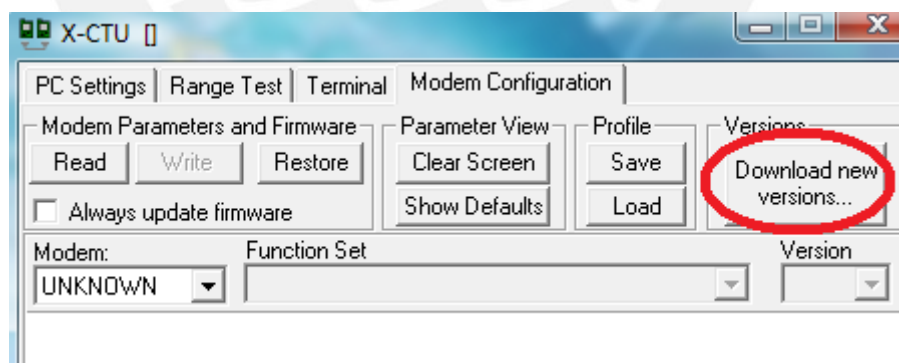


Figura 4.1: Modem Configuration – New versions

4.- Insertar el equipo xbee en el módulo de programación. Colocar el cable DB9 que permitirá la comunicación entre el MODEM y la PC. Figura 4.2

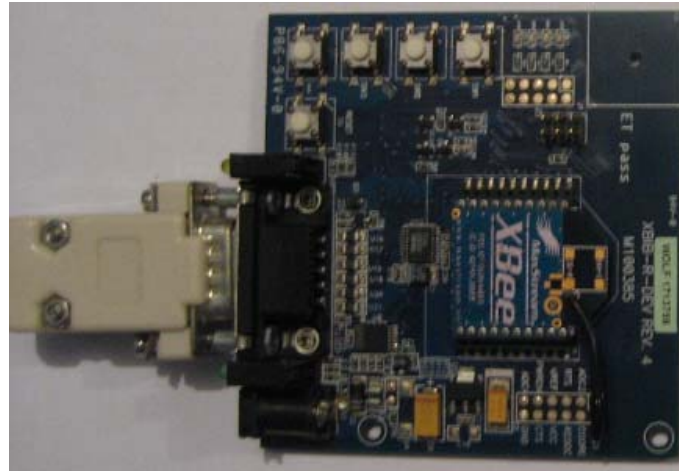


Figura 4.2: Módulo de programación XBee

5.- Hacer click en “READ”, para obtener la información del chip XBee. Ver Figura 4.3

6.- Actualizar la versión del Firmware a la fecha “10A5”. Ver Figura 4.3

7.- Hacer click en “WRITE” para grabar el firmware seleccionado en la memoria del chip. Ver Figura 4.3

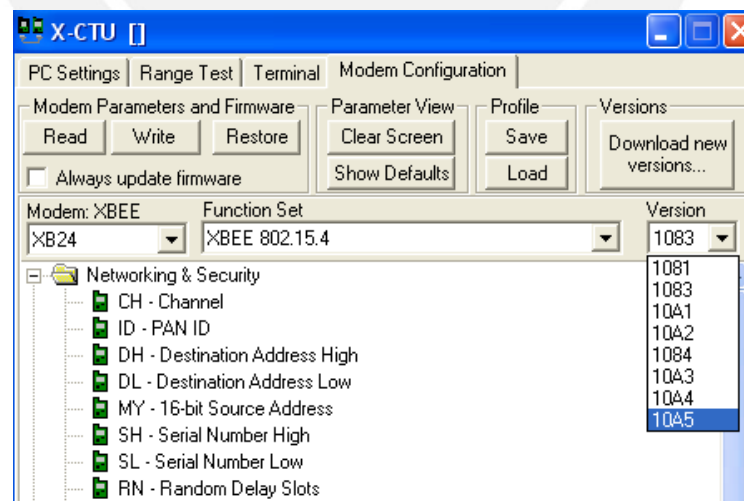


Figura 4.3: Firmware version

Programa XCTU - Funciones base:

1.- PC Settings:

Se usa para configurar los parámetros de comunicación con el puerto serial (# de puerto, velocidad, control de flujo, cantidad de bits, paridad, bits de parada)

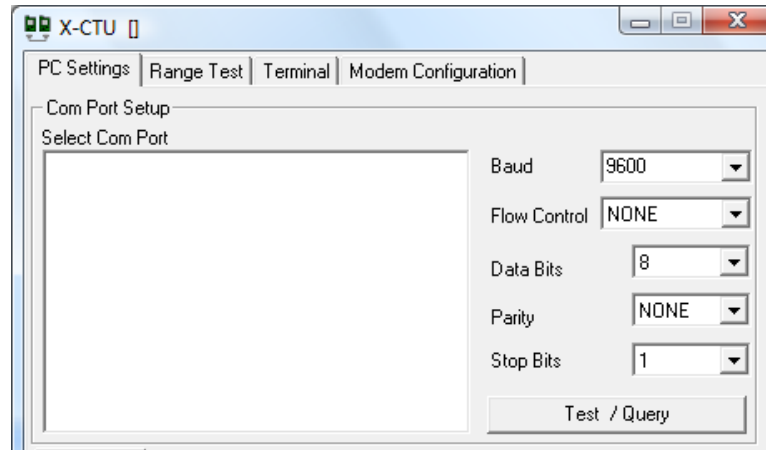


Figura 4.4: PC Settings

2. - Range Test:

Se utiliza para probar la intensidad de la señal de recepción. Esto permite conocer experimentalmente el rango de cobertura con el cual contamos y la calidad y fuerza de señal que recibimos.

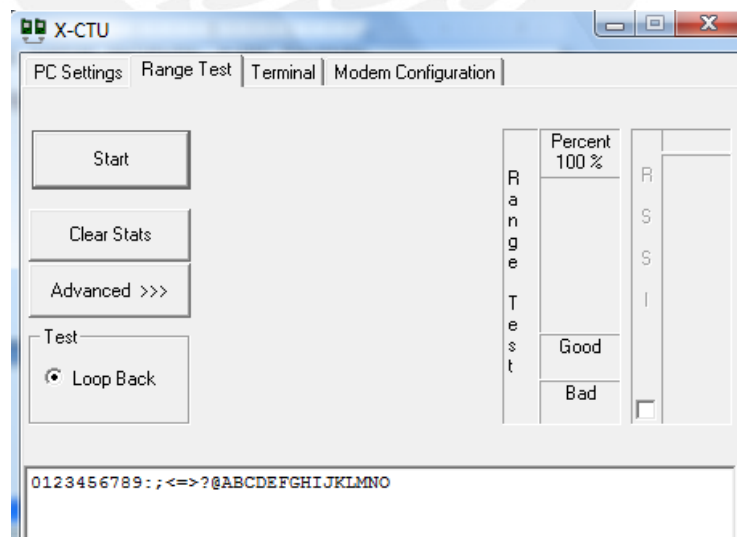


Figura 4.5: Range Test

3.-Terminal

A través de esta pestaña podemos visualizar los datos recibidos. Estos pueden ser mostrados en ASCII o Hexadecimal.

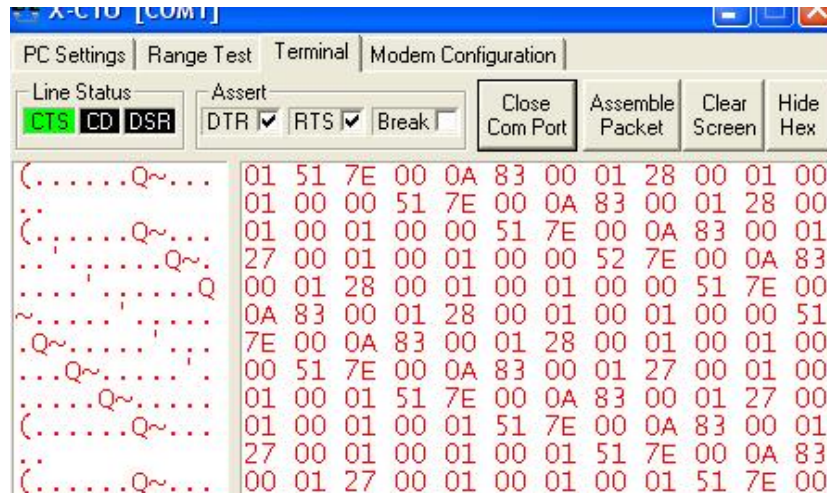


Figura 4.6: Terminal

4.- Modem Configuration

En esta pestaña se visualiza los parámetros del chip (en memoria) así como también permite la configuración y escritura sobre la misma.

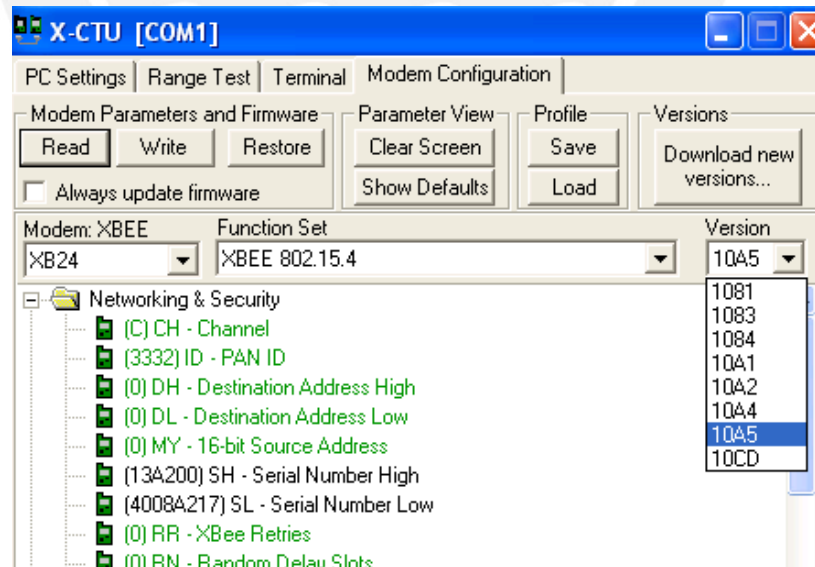


Figura 4.7: Modem Configuration

4.2 PRUEBA DE RED – MONITOREO DE LOS SENSORES.

El objetivo es visualizar a través del puerto serial (UART) las entradas de todos los módulos transmisores. Para esto se requiere configurar algunos parámetros dependiendo si se trata de un coordinador o un nodo remoto, cómo se muestra a continuación a través de los siguientes pasos:

1.- Insertar el equipo xbee en el modulo de programación. Colocar el cable DB9 que permitirá la comunicación entre el MODEM y la PC.

2.-Presionar “Read” para ver la configuración actual de los parámetros del modulo.

3.- En caso de ser un equipo coordinador configurar:

- DH y MY = 0

- DL = \$FFFF

- CE =1 (1 indica Maestro, 0 esclavo)

- IU = 1 (Activa la comunicación UART)

4.- En caso que el equipo sea un terminal se configura:

- DH y DL = 0

- MY = 1, 2, 3 ó 4 (etiqueta numerada para diferenciar cada terminal)

- CE = 0 (1 indica Maestro, 0 esclavo)

- D0 = Entrada Digital (3er valor de la lista)

- IR = 0x400 Este parámetro permite configurar la frecuencia de muestreo.

$IR * 1ms = T_{muestreo}$. En este caso se configuro un $T_{muestreo} = 1seg$.

5.- Presionar “Write” para grabar los parámetros en la memoria del XBee.

La prueba puede realizarse de dos formas: conectando la salida de los sensores acondicionadas de tal manera que arrojen valores digitales de 0v y 3.3V o mediante los pulsadores que simulen lo mismo (3.3V sin pulsar y 0V pulsando), para este último caso la figura es la siguiente:

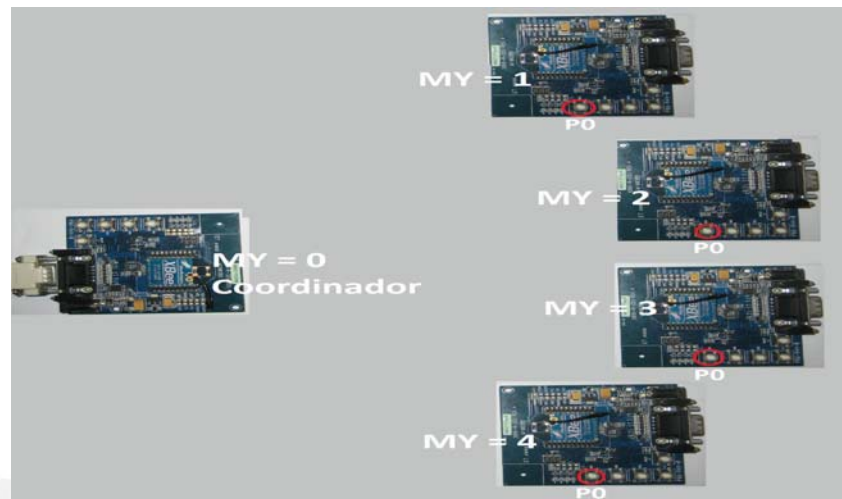


Figura 4.8: Prueba de red – Monitoreo de IO

4.3 TRAMAS DE RECEPCIÓN – DETECCIÓN Y MUESTRA DE LA INFORMACIÓN

Trama de recepción

Sin recepción de dato:

7E	00 0A	83	00 01	23	00	01	00 01	00 01	4B
----	-------	----	-------	----	----	----	-------	-------	----

- 7E Flag.(Bandera de inicio)
- 00 0A Tamaño del paquete recibido.
- 83 Código API que hace referencia a dato recibido por RF.
- 00 01 Dirección del modulo transmisor
- 23 Nivel RSSI. (Indicador de potencia de señal recibida)
- 00 Opciones.
- 01 Cantidad de muestras.
- 00 01 Configuración de las entradas. (1 digital)
- 00 01 Valor del pin digital
- 4B Checksum

Recepción de dato:

7E	00 0A	83	00 01	23	00	01	00 01	00 00	4B
----	-------	----	-------	----	----	----	-------	-------	----

- 7E Flag.(Bandera de inicio)
- 00 0A Tamaño del paquete recibido.
- 83 Código API que hace referencia a dato recibido por RF.
- 00 01 Dirección del modulo transmisor
- 23 Nivel RSSI. (Indicador de potencia de señal recibida)
- 00 Opciones.
- 01 Cantidad de muestras.
- 00 01 Configuración de las entradas. (1 digital)
- 00 00 Valor del pin digital
- 4B Checksum

Como se observa en las tramas de recepción se consideran importantes (a la hora de programar) las sombreadas en celeste. Las cuales indican la dirección del remitente (el sensor se envía) y si se detecto algún cambio o no.

A partir de esta trama y su contenido, se usa el diagrama de flujo diseñado en el capítulo 3, en el cual, en función al cambio detectado en el byte 13 se genera una pantalla de alerta para avisar al usuario.

Para simular los cambios en la pantalla se agrega una cuadrícula de Excel al programa para visualizar la trama y su respectiva pantalla de alerta al detectar un cambio en el byte 13 tal y como se ve en la figura 4.9.

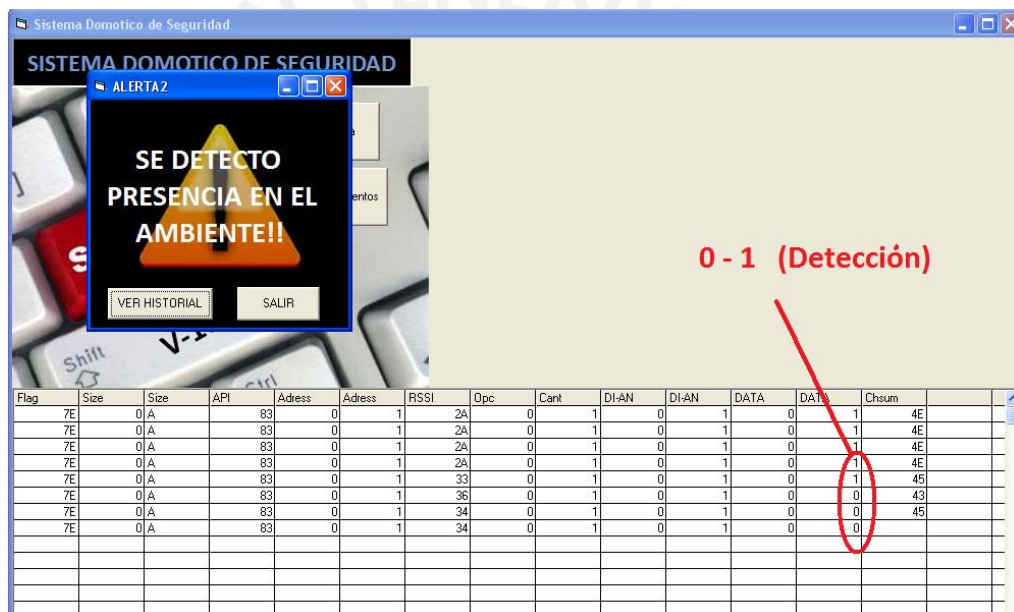


Figura 4.9: Programa Prueba de detección

4.4 CÁMARA DE SEGURIDAD – PRUEBAS DE RESOLUCIÓN Y ALMACENAJE.

Para la implementación de la cámara se hará uso del software SuperDVR, el cual viene junto con el adaptador de conector RCA- USB mencionado en el capítulo 3.

La instalación y configuración se muestra en los siguientes pasos:

- 1) Inserte el cd de instalación proporcionado del programa SuperDVR y siga los pasos de instalación. Tipo de video PAL.

2) Una vez instalado se tendrá el siguiente entorno de visualización:



Figura 4.10: Entorno de visualización –Cámara

A.- Registro, sirve de protección a la configuración del video mediante usuario y contraseña.

B.- Búsqueda y rebobinado de video, herramienta que sirve para visualizar grabaciones pasadas ya sea por fecha u hora.

C.-Configuración del sistema, herramienta para modificar los parámetros de la grabación.

D.- Apagado del programa.

E.- Visualización entre 1 y 4 cámaras.

F.- Espacio disponible en memoria.

G.- Estado de la cámara, tipo de grabación:



3) Configuración:

Los parámetros de la grabación se asignarán en el menú que se muestra a continuación. (Letra C de la figura 4.10) Los parámetros más importantes se encuentran resaltados en un círculo rojo:



Figura 4.11: Configuración Básica

Resolución: Se le asigna la menor posible (320X240) con el fin de ahorrar espacio en memoria.

Storage Disk: Se escoge la partición del disco duro donde se almacenarán los videos (por defecto se crea una carpeta en la misma con el nombre de DVR_DATA).

Manual Record: Se activará esta opción solo en el caso de que se desee hacer una grabación manual (una vez clickeado y salido del menú comienza la grabación).

Motion Detection: Se escoge esta opción como parámetro con el fin de que solo grabe cuando se detecte algún movimiento en el ambiente. Cabe mencionar que grabará hasta 10 segundos después del último movimiento detectado.

Para ambos modos de grabación se le asignará una tasa de 10 cuadros por segundo con el fin de ahorrar en un tercio la memoria de grabación (lo normal es de 30 fps).

4) Búsqueda y Rebobinado:

Para acceder a grabaciones de días anteriores, se accede a esta ventana donde las opciones importantes se encuentran encerradas en rojo:

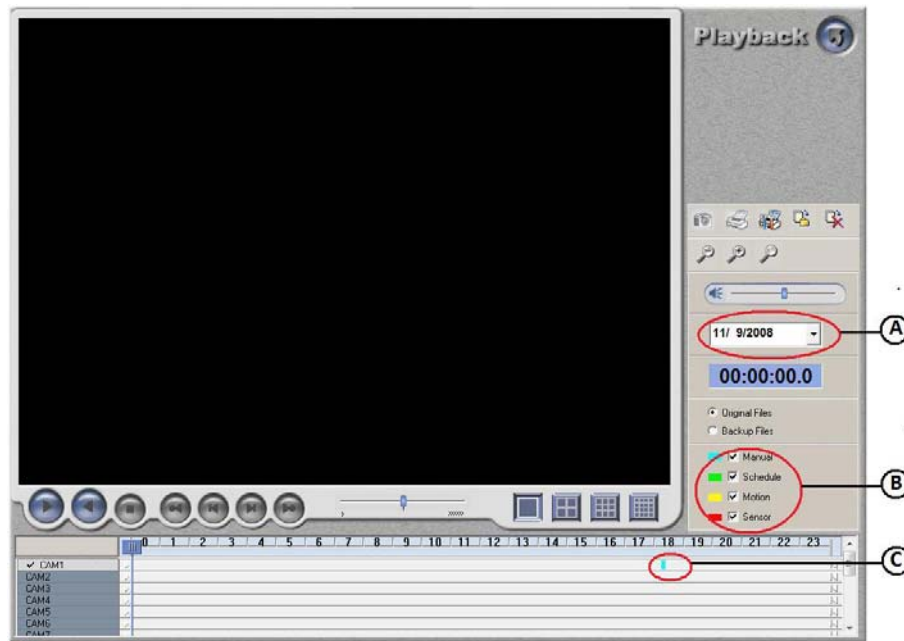


Figura 4.12: Búsqueda y Rebobinado

- A) Fecha del evento.
- B) Tipo de grabación.
- C) Hora del suceso.

5) Almacenamiento:

Debido a que el espacio en el disco es una limitante es recomendable una limpieza de la carpeta de almacenado al menos una vez por semana.

El tamaño de la grabación es de alrededor de 5MB por minuto.

4.5 IMPLEMENTACIÓN DE LOS SENSORES Y PUESTA EN MARCHA.

Basándonos en el capítulo 3 y el diseño del sensado y comunicación se procede a la implementación del sistema con la misma estructuración:

4.5.1 Sensor de Movimiento – Transmisión

Se procede a acoplar los siguientes módulos:

- Sensor de Movimiento (1).
- Acondicionamiento de la señal (2).
- Módulo de transmisión RF – Xbee (3).
- Batería.

La unión general se puede apreciar en la siguiente figura:

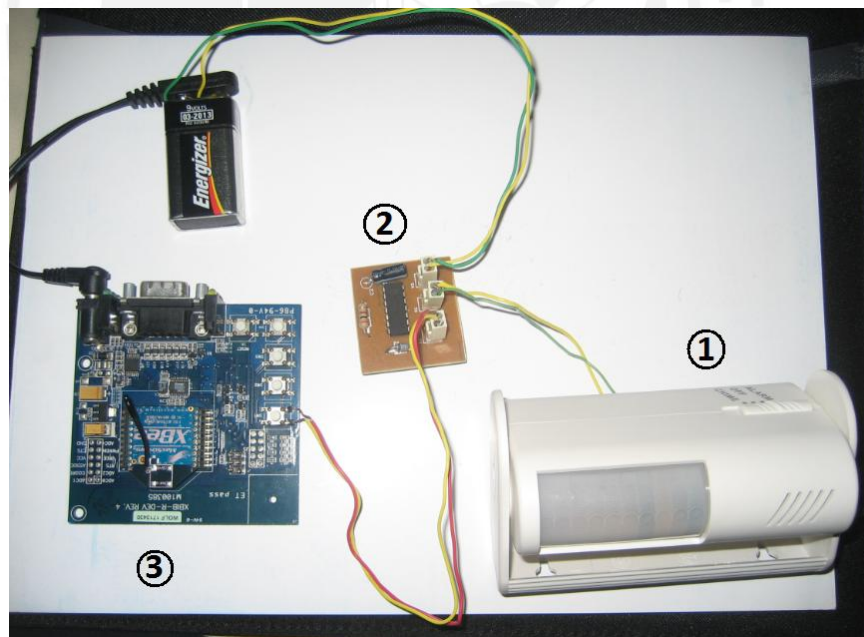


Figura 4.13: Sensor de Movimiento – Transmisión

4.5.2 Sensor de Humo - Trasmisión

Se procede a acoplar los siguientes módulos:

- Sensor de Humo (1).
- Acondicionamiento de la señal (2).
- Módulo de trasmisión RF – Xbee (3).
- Batería.

La unión general se puede apreciar en la siguiente figura:

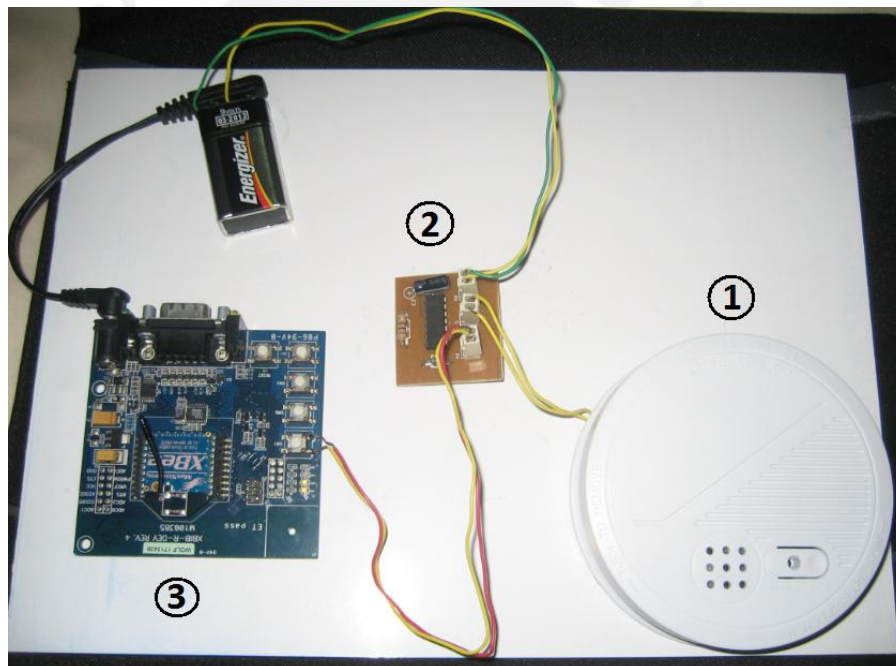


Figura 4.14: Sensor de Humo – Trasmisión

4.5.3 Detector de apertura de puertas - Trasmisión

Se procede a acoplar los siguientes módulos:

- Detector de apertura (1).
- Acondicionamiento de la señal (2).
- Fuente de voltaje 3.3V (3).
- Módulo de trasmisión RF – Xbee (4).
- Batería.

La unión general se puede apreciar en la siguiente figura:

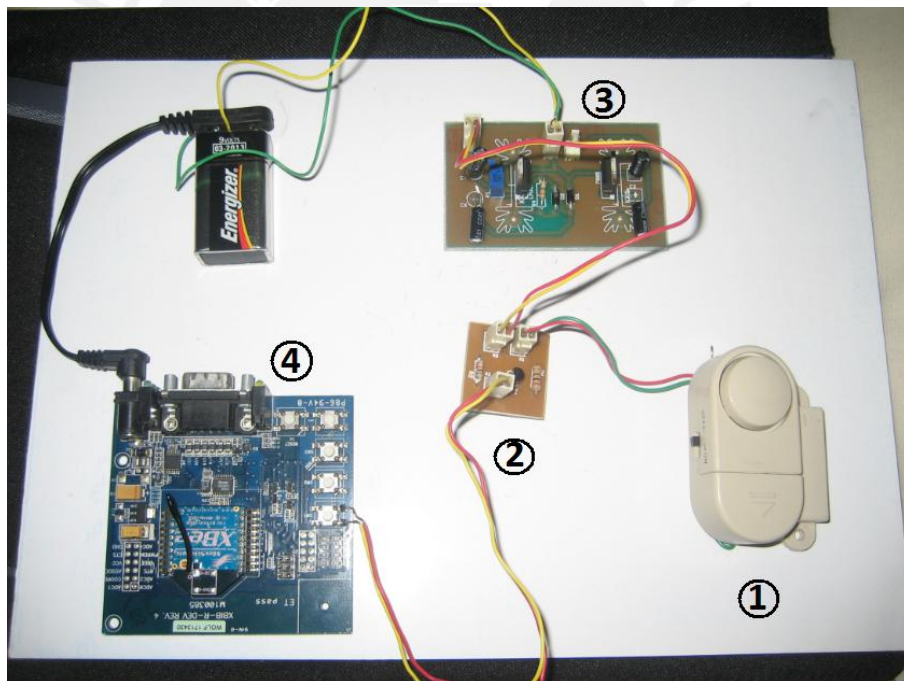


Figura 4.15: Sensor de Humo – Trasmisión

4.5.4 Cámara de seguridad

Se conecta la cámara de seguridad en el lugar diseñado en conjunto con su alimentación, del mismo modo el equipo receptor con su respectiva alimentación y conexión hacia el servidor mediante los cables RCA y adaptador a USB. Ver Figura 4.16

Donde:

- A) Alimentación de la Cámara de Seguridad.
- B) Cámara de Seguridad.
- C) Alimentación del equipo receptor.
- D) Equipo Receptor.
- E) Salida RCA.
- F) Adaptador de conector RCA – USB.
- G) Puerto USB del servidor con software de captura.

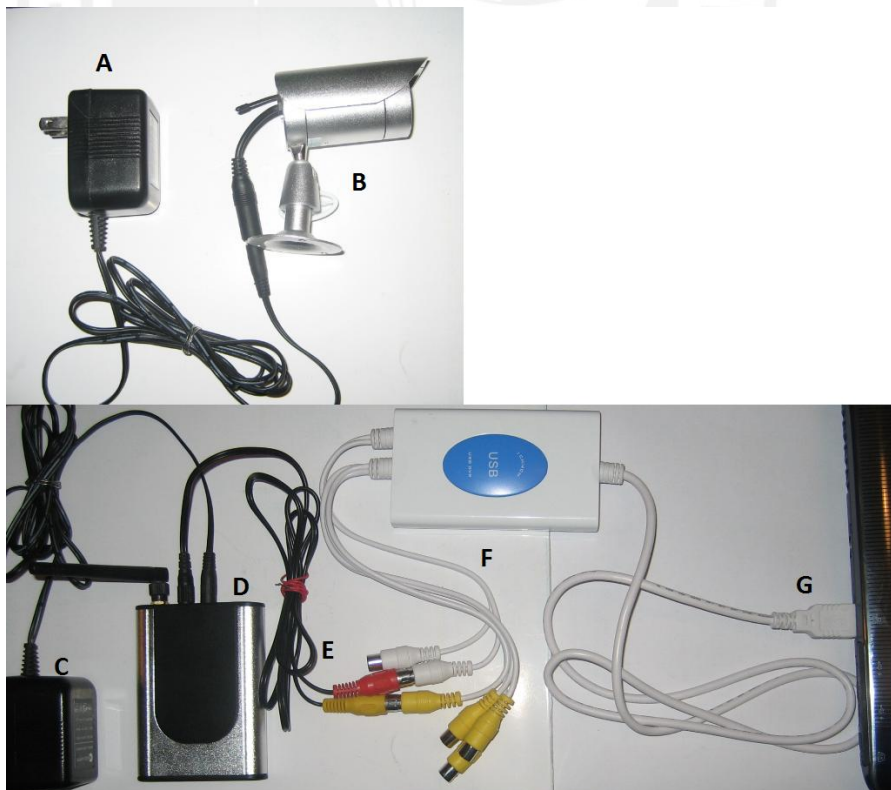


Figura 4.16: Implementación Cámara de Seguridad

4.5.5 Módulo Receptor

Se procede a conectar serialmente el módulo coordinador RF- XBee al puerto serial del servidor. La alimentación sería por transformador a 9V.

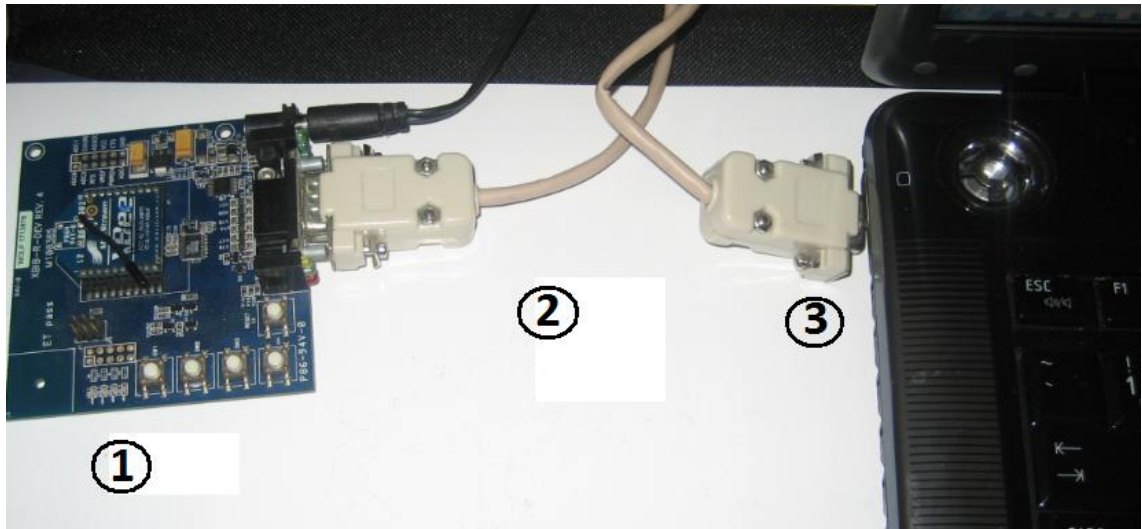
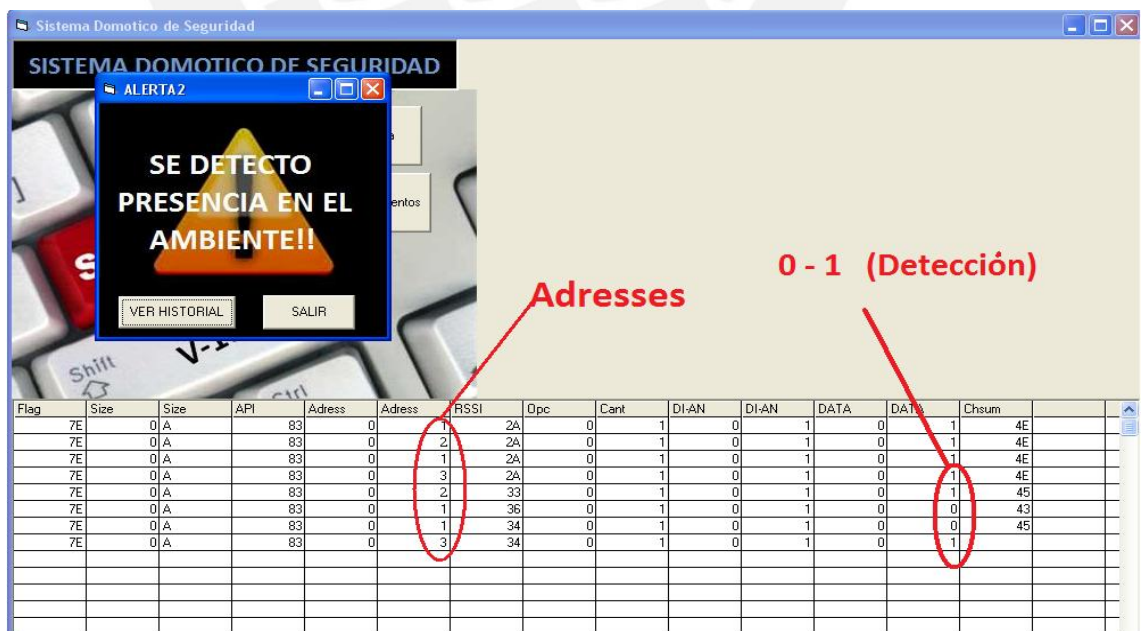


Figura 4.17: Módulo Receptor

El orden de las tramas receptadas de cada uno de los nodos (1, 2,3 ó 4) es aleatorio debido a que se encuentran configuradas con el mismo periodo de muestro (1 segundo), tal como se ve en la figura a continuación resaltado como Adresses:



SISTEMA DOMOTICO DE SEGURIDAD

ALERTA 2

SE DETECTO PRESENCIA EN EL AMBIENTE!!

VER HISTORIAL SALIR

Adresses **0 - 1 (Detección)**

Flag	Size	Size	API	Address	Address	RSSI	Opc	Cant	DI-AN	DI-AN	DATA	DATA	Chsum
7E	0	A	83	0	1	2A	0	1	0	1	0	1	4E
7E	0	A	83	0	2	2A	0	1	0	1	0	1	4E
7E	0	A	83	0	1	2A	0	1	0	1	0	1	4E
7E	0	A	83	0	3	2A	0	1	0	1	0	1	4E
7E	0	A	83	0	2	33	0	1	0	1	0	1	45
7E	0	A	83	0	1	36	0	1	0	1	0	0	43
7E	0	A	83	0	1	34	0	1	0	1	0	0	45
7E	0	A	83	0	3	34	0	1	0	1	0	1	

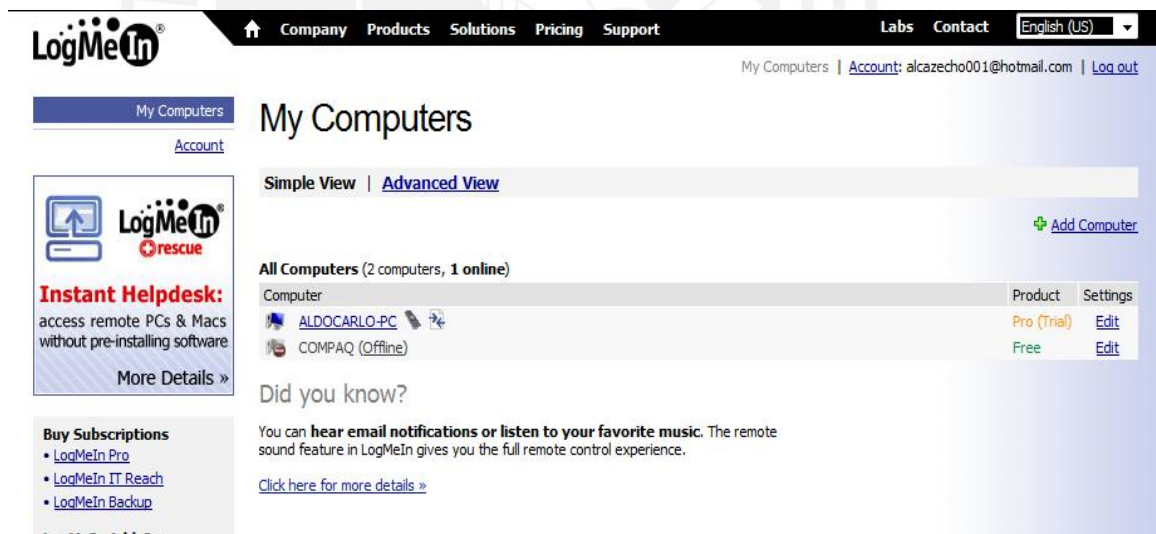
Figura 4.18: Programa de prueba con todas las tramas

4.6 ACCESO REMOTO DEL SISTEMA

Con el fin de elevar el nivel de seguridad del sistema, se usará un programa preestablecido con acceso internet con el fin de que el programa principal pueda ser accedido en cualquier parte del mundo vía página web.

El programa es llamado LogMeIn y los pasos para utilizarlo son los siguientes:

- 1.- Descargar el archivo instalador de la web principal: <https://secure.logmein.com/>, (normalmente pide una dirección de correo electrónico para la activación del mismo).
- 2.- Una vez descargado, instalarlo en la computadora que actuará como servidor.
- 3.- Al ingresar a la página de internet de LogMeIn desde una computadora externa con acceso a internet y registrarse a la misma con el usuario y contraseña brindada se tendrá acceso a las distintas computadoras donde se haya instalado el programa. Ver figura 4.19



The screenshot shows the LogMeIn web interface. At the top, there is a navigation bar with links for Company, Products, Solutions, Pricing, Support, Labs, and Contact. The user is logged in as 'alcazecho001@hotmail.com'. The main content area is titled 'My Computers' and shows a list of computers. One computer, 'ALDOCARLO-PC', is online, while 'COMPAQ' is offline. There are also promotional banners for 'Instant Helpdesk' and 'Buy Subscriptions'.

Computer	Product	Settings
ALDOCARLO-PC	Pro (Trial)	Edit
COMPAQ (Offline)	Free	Edit

Figura 4.19: Pagina Web LogMeIn

4.- Hacer click en el nombre de la computadora deseada (en caso de requerir ActiveX permitir la instalación del mismo). A continuación se abrirá una pantalla (Ver figura 4.20), donde se ingresará los datos de acceso al computador en cuestión (usuario y contraseña de ingreso a Windows).



Figura 4.20: Acceso al computador (registro)

5.- Una vez ingresado al menú de acceso al computador, se tendrá la libertad de escoger distintas opciones para el mismo. Ver Figura 4.21



Figura 4.21: Menú de opciones de acceso

6.-Seleccionar la opción “Remoto Control”, el cual permitirá un acceso inmediato a la pantalla del computador – Servidor, así como la manipulación del mismo. Ver Figura 4.22

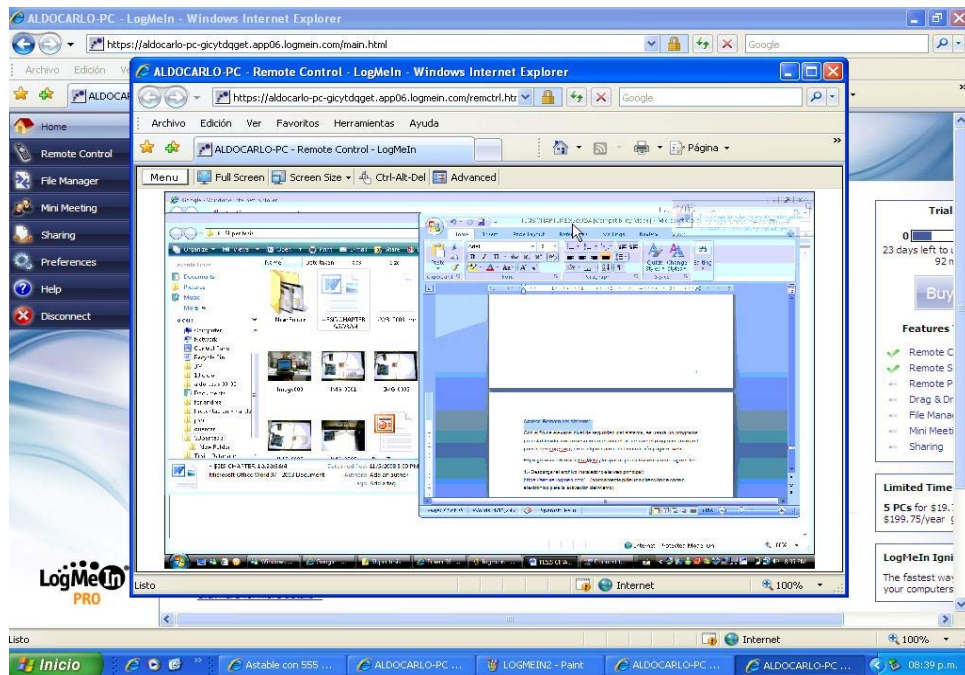


Figura 4.22: Pantalla del servidor- control

PRESUPUESTO Y COSTOS DE INSTALACION

Unid.	Descripción	P.U (S/.)	P.T(S/.)
1	Sensor de humo marca Boston Technology	30.00	30.00
1	Sensor de movimiento marca Boston Technology	35.00	35.00
2	Detector de Apertura de puertas marca EconoLux	9.00	18.00
1	Cámara de seguridad Inalámbrica	299.00	299.00
1	Adaptador de cable RCA -USB BostonTeck	439.00	239.00
1	Circuito de Acondicionamiento del sensor de humo	7.00	7.00
1	Circuito de Acondicionamiento del sensor de movimiento	7.00	7.00
2	Circuito de Acondicionamiento del detector de apertura de puertas	15.00	30.00
4	Chips de transmisión/ recepción RF XBee	60.00	240.00
4	Módulos de transmisión RF Xbee	5.00	20.00
1	Módulos de recepción RF Xbee	10.00	10.00
1	Cable de comunicación serial	8.00	8.00
1	Capacitación	-	-
4	Baterías Enercell Radioshack	8.20	32.80
1	Costos de diseño e instalación	1500.00	1500.00
	Total S/.		2475.80

CONCLUSIONES

- 1.- Es posible utilizar la alarma de cada uno de los sensores como sistema binario ON/OFF a través de un acondicionamiento de la misma y ser enviado a través de RF. Garantizando así el uso de cualquier tipo de sensor disponible en el mercado.
- 2.- Se puede sincronizar los módulos XBee con Visual Basic y programar en función de cada byte de la trama recibida, con el fin de detectar el bit donde se representa el cambio de estado (sensor activado/desactivado) y generar acciones de acuerdo al mismo.
- 3.-El protocolo Zigbee es el más adecuado para gobernar una red inalámbrica de sensores. Esto se debe en primer lugar a que los dispositivos que trabajan bajo este protocolo son económicos y consumen poca energía a comparación con otros protocolos inalámbricos como Wi-Fi, Bluetooth y Wimax, lo cual los hace perfectos para sistemas de seguridad. Y en segundo lugar poseen una transferencia de datos mucho menor, la cual no es necesaria debido a que se trabaja con un sistema ON/OFF.
- 4.- Toda red de sensores contará con un equipo coordinador y equipos terminales. El equipo coordinador será el encargado de recolectar la información sensada por los equipos terminales. Es importante mencionar que el dispositivo transmisor es el mismo en ambos casos, lo único en que se diferencian es en el modo de configuración.
- 5.- Es posible observar la pantalla de cualquier computador desde otro computador usando una página web a través de internet, lo que permite una rápida respuesta ante un atentado.
- 6.- Se logró el objetivo de bajo costo, empleando dispositivos económicos y fáciles de encontrar en el mercado, así como diseñando y programando un sistema propio y específico que no se encuentra en el mercado.

RECOMENDACIONES

- 1.- Evitar en lo posible hacer pruebas directas con el sensor de humo, puesto que ocasiona desgaste y una eventual avería.
- 2.- Colocar la cámara de seguridad en un lugar elevado y no al alcance de la mano (por encima de los 2m de altura), para evitar que gire y disminuya el rango de visión.
- 3.- Configurar usando el software de la cámara un tipo de grabado de resolución mínima y solo por sensado de movimiento, con el fin de ahorrar hasta el 90% el espacio de memoria disponible.
- 4.- Es recomendable configurar el tiempo de muestreo de los módulos de transmisión entre 1 y 5 seg. Debido a que es menor al tiempo que dura la alarma y se evita tanto tomar más de 2 veces el mismo dato como el no registrar alguno.
- 5.- Es importante el revisar periódicamente el estado de las baterías, se recomienda dos veces por mes. Asimismo la revisión del correcto funcionamiento del sistema cada dos meses.
- 6.- Se puede ampliar la tesis haciendo que la detección genere un envío de un mensaje de Texto al usuario, o una llamada a la estación local de policía.
- 7.- Se puede mejorar el presupuesto total de la implementación consiguiendo o diseñando una conexión entre los conectores tipo RCA y USB para la visualización en el servidor.
- 8.- Puede mejorarse la seguridad del sistema implementando códigos de seguridad en las computadoras asociadas al programa, mediante encriptaciones de disco duro y cuentas de administrador bajo clave.

BIBLIOGRAFIA

[1] RADIOSHACK CORPORATION

2008 Radioshack® [En línea] United States. [Consultado 03/05/2008]

<<http://www.radioshack.com/>>

[2] INTERAMSA

2003 Seguridad Electrónica- Interamsa [En línea] Perú [Consultado 15/06/2008]

<<http://www.interamsa.com/ielectronica.htm>>

[3] ORUS

2006 Orus [En línea] Perú [Consultado 15/06/2008]

<<http://www.orus.com.pe/>>

[4] SEGURYSISTEM

2006 Segurysistem [En línea] Perú [Consultado 15/06/2008]

<<http://www.segurysistem.com/>>

[5] Ministerio de Transporte y Comunicaciones

2006 Ministerio de Transporte y Comunicaciones [En línea] Perú

[Consultado 15/06/2008]

<<http://www.mtc.gob.pe/>>

[6] INEI

1998 Violencia Cotidiana en el Perú [En línea] Perú [Consultado 14/05/2008]

<<http://www.inei.gob.pe/biblioineipub/bancopub/Est/Lib0061/07-1.htm>>

[7] ZEBALLOS, Aldo

2008 Entrevista a Angelo Velarde, jefe de laboratorio V-104 PUCP

Lima: Pontificia Universidad Católica del Perú, San Miguel

[8] GLOBAL INVENTURES, INC

2008 ZigBee Alliance [En línea] United States. [Consultado 04/2008]

<http://www.zigbee.org/>

[9] WIKIMEDIA FOUNDATION INC.

Wikipedia ® [En línea] United States. [Consultado 15/04/2008]

<http://en.wikipedia.org/wiki/Main_Page>

[10] BLUETOOTH SIG, INC

2008 Bluetooth ® [En línea] United States [Consultado 28/03/2008]

<<http://www.bluetooth.com/Bluetooth/Technology/Works/>>

[11] WI-FI ALLIANCE

2007 Wi-Fi Alliance [En línea] United Status [Consultado 28/03/2008]

<<http://www.wi-fi.org>>

[12] USB TECHNOLOGY

2008 WIRELESS USB [En línea] United States [Consultado 28/03/2008]

<<http://www.usb.org/developers/wusb/>>

[13] X10 POWERHOUSE

2005-2008 X10 Powerhouse [En línea- FTP] United States [Consultado 28/03/2008]

<<ftp://ftp.x10.com/pub/manuals/technicalnote.pdf>>

[14] PROYECTOS FIN DE CARRERA

2005 Tipos de alarma antirrobo [En línea] España [Consultado 5/04/2008]

<<http://www.proyectosfindecarrera.com/alarmas-chalet.htm>>

[15] FERNÁNDEZ VALDIVIELSO, Carlos

1999 La domótica: esencia de un edificio inteligente. En: Mundo Electrónico Ed. 298, p. 56-60

[16] TING-PAT SO, Albert

1999 Intelligent building systems. Boston: Kluwer Academic, p.

[17] CONTINENTAL AUTOMATED BUILDING ASSOCIATION

2008 CABA [En línea] United States [Consultado 29/03/2008]

<<https://www.caba.org/>>

[18] DAINTREE NETWORKS

2004-2008 DaintreeNetworks [En línea] United States [Consultado 02/04/2008]

<<http://www.daintree.net/resources/index.php/>>

[19] IEEE 802.15 WORKING GROUP FOR WPAN

2008 IEEE 802.15 [En línea] United States [Consultado 04/2008]

<<http://www.ieee802.org/15/>>

[20] ZIGBEEMANIA

2008 ZigBeemania [En línea] United States [Consultado 05/2008]

<<http://www.zigbeemania.com/>>

[21] BRICOLAJE Y HOGAR

2008 Bricolaje y hogar [En línea] España [Consultado 20/04/2008]

<http://www.bricolajeyhogar.com/domotica/domotica_seguridad>

[22] MAXSTREAM

2007 Digi Internacional Maxstream [En línea] United States [Consultado 05/2008]

<<http://www.maxstream.net/>>

[23] NATIONAL INSTRUMENTS

2008 National Instruments [En línea] United States [Consultado 11/05/2008]

<<http://www.ni.com/>>