



PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

Esta obra ha sido publicada bajo la licencia Creative Commons
Reconocimiento-No comercial-Compartir bajo la misma licencia 2.5 Perú.

Para ver una copia de dicha licencia, visite
<http://creativecommons.org/licenses/by-nc-sa/2.5/pe/>



PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA



**PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ**

**DISEÑO DE UN SISTEMA AUTOMATIZADO DE SEGURIDAD CONTRA
INTRUSION EN UN EDIFICIO DE DEPARTAMENTOS UTILIZANDO EL ESTANDAR
DE TECNOLOGÍA INALAMBRICA ZIGBEE**

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

ALEJANDRO PAVEL DIAZ POLO

Asesor: Luis Angelo Velarde Criado

Lima, Abril de 2010

RESUMEN

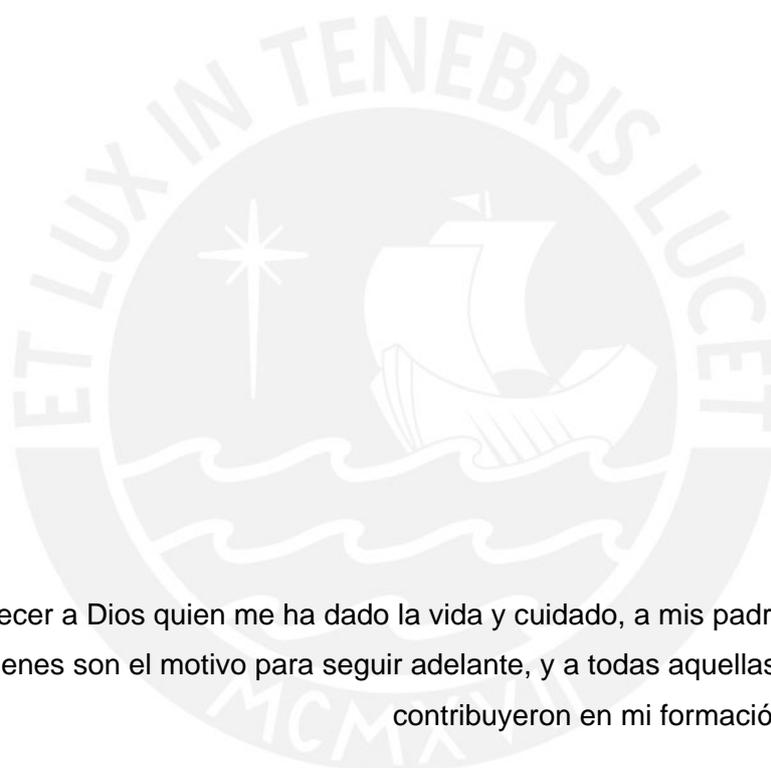
El objetivo de la presente tesis es diseñar un sistema de seguridad contra intrusión para edificios de departamentos mediante la tecnología inalámbrica ZigBee, una tecnología moderna que en la actualidad lidera la manufactura de productos para la automatización inalámbrica de la vivienda, haciendo de este un lugar seguro, confortable y con un eficiente consumo de energía.

La actual situación delincriminal en el Perú y la demanda por protección y seguridad demuestran el marco problemático de esta tesis, para lo cual se propone reemplazar el actual proceso manual de seguridad de los residentes (revisando las cerraduras y puertas del departamento, variando sus horas de salida e ingreso, etc) por un sistema automatizado que permita al usuario resguardar su vivienda de intrusiones.

Se comparan diversas tecnologías que automatizan departamentos (domótica) teniendo en consideración: la economía del producto, la capacidad energética, la escalabilidad, confiabilidad, estética, portabilidad, sencillez de uso y el bajo mantenimiento. Se elige a la tecnología inalámbrica ZigBee y para diseñar los módulos que compondrán el sistema de seguridad se elige el módulo transceptor de radiofrecuencia XBee Series 2. Para lograr una correcta cobertura de monitoreo en toda el área del departamento se diseñan los módulos de monitoreo (contacto magnético y sensor de rotura de vidrio), el módulo de aviso para el sonido de la alarma, el módulo de control remoto para activar a distancia el sistema y el módulo coordinador, el encargado del funcionamiento de todo el sistema de seguridad.

Los resultados y pruebas indican que el sistema reúne las características del sistema de seguridad que la presente tesis plantea (sección 2.3). La cobertura del sistema inalámbrico cumple para la aplicación e implementación del sistema en el departamento elegido y la duración de baterías del módulo de monitoreo estaría por encima de los 8 meses.

Podemos concluir que la propuesta es aceptable para la realidad de las familias en nuestro país puesto que el precio de venta del producto es bastante competitivo en el mercado tal como lo muestra el análisis de costo del producto en la sección 4.4.



Agradecer a Dios quien me ha dado la vida y cuidado, a mis padres y hermanas quienes son el motivo para seguir adelante, y a todas aquellas personas que contribuyeron en mi formación universitaria.

ÍNDICE

ÍNDICE DE FIGURAS	4
ÍNDICE DE TABLAS	6
INTRODUCCIÓN	7
1 LA SEGURIDAD Y LA DOMÓTICA EN LOS DEPARTAMENTOS	8
1.1 Problemática de la seguridad	8
1.1.1. <i>Situación delincriminal en el Perú.</i>	8
1.1.2. <i>Demanda ciudadana por protección y seguridad</i>	10
1.1.3. <i>Modalidades y aspectos del robo en las viviendas</i>	10
1.1.4. <i>Plan de seguridad en las viviendas</i>	11
1.1.5. <i>Declaración del marco problemático</i>	13
1.2. Sistemas domóticos en los edificios de departamentos	13
1.2.1. <i>La domótica</i>	14
1.2.2. <i>Tipología de la vivienda</i>	15
1.2.3. <i>Oferta nacional</i>	15
1.2.4. <i>Demanda nacional</i>	15
2 COMPARACIÓN DE TECNOLOGÍAS DE AUTOMATIZACIÓN	16
2.1. Sistemas cableados	16
2.1.1. <i>Konnex</i>	16
2.1.2. <i>Lonworks</i>	16
2.1.3. <i>Tecnología X-10</i>	17
2.2. Sistemas inalámbricos	17
2.2.1. <i>IEEE 802.15.4</i>	17
2.2.2. <i>ZigBee</i>	18
2.2.3. <i>Hometronic</i>	19
2.3. Características del sistema de seguridad	19
2.4. Comparación de tecnologías	20
2.4.1. <i>Elección de los Sistemas Abiertos</i>	21
2.4.2. <i>Comparación con la Tecnología X10</i>	21
2.4.3. <i>Comparación con las tecnologías Konnex, Lonworks y Hometronic</i>	22
2.4.4. <i>Comparación con la tecnología ZigBee</i>	23
2.5. Conclusión de la comparación	24
2.5.1. <i>Eliminación de las tecnologías Konnex, Lonworks y Hometronic</i>	24
2.5.2. <i>Eliminación de la tecnología X10</i>	25
2.5.3. <i>Elección de la tecnología ZigBee</i>	25
3 ESPECIFICACIÓN ZIGBEE Y ELECCIÓN DEL MÓDULO	27
3.1. Tipos de dispositivos	27

3.2.	Arquitectura.....	27
3.2.1.	Capa física	28
3.2.2.	Capa de enlace	29
3.2.3.	Capa de red.....	29
3.2.4.	Capa de aplicación	30
3.3.	Empaquetamiento	31
3.4.	Direccionamiento	31
3.5.	Seguridad	32
3.6.	Comparación de Circuitos Integrados ZigBee: Transceptores, Socs y Sips	32
3.6.1.	Texas Instruments (TI)	32
3.6.2.	Freescale	33
3.6.3.	Ember	34
3.6.4.	Microchip.....	34
3.6.5.	Atmel	34
3.6.6.	Módulos	35
3.6.7.	Radiocrafts.....	35
3.6.8.	Meshnetics	35
3.6.9.	RFM (Cirronet).....	35
3.6.10.	Jennic	36
3.6.11.	Digi (ex Maxstream).....	36
3.7.	Ventajas de los módulos.....	36
3.7.1.	Implementación de los perfiles	36
3.7.2.	Conclusión y elección	37
3.8.	Módulo Xbee Series 2 [24]	37
3.8.2.	Formación de una red ZigBee	43
3.8.3.	El Firmware AT	44
4	DISEÑO DEL SISTEMA DE SEGURIDAD CONTRA INTRUSIÓN.....	45
4.1.	Definición del edificio y departamento.....	45
4.1.1.	Características del edificio	45
4.1.2.	Características del departamento.....	46
4.2.	Funcionamiento del sistema	50
4.3.	Diseño físico de los módulos	52
4.3.1.	MÓDULO COORDINADOR.....	53
4.3.2.	MÓDULO DE MONITOREO	60
4.3.3.	MÓDULO DE AVISO.....	72
4.3.4.	MÓDULO DE CONTROL REMOTO.....	73
4.4.	Diseño lógico de los módulos	77

4.4.1. Versiones del Firmware.....	77
4.4.2. Software XCTU.....	78
4.4.3. Grabación del Firmware.....	78
4.4.4. Parámetros del XBee en cada módulo.....	79
4.4.5. Configuración del Microcontrolador.....	81
4.5. Costos del diseño.....	84
4.6. Comparativa de precios de venta.....	86
4.7. Costo de investigación del diseño del sistema de seguridad.....	87
5 PRUEBAS Y MEDICIONES.....	89
5.1. Medición de corrientes: Módulo de monitoreo.....	89
5.2. Medición de corrientes: Módulo coordinador.....	90
5.3. Prueba de rango.....	90
5.3.1. Configuración previa.....	92
5.3.2. Prueba de comunicación entre dispositivos.....	93
5.3.3. Ubicaciones de los dispositivos de prueba.....	94
5.4. Conclusiones de las pruebas.....	97
5.4.1. Ubicación de dispositivos en el departamento.....	98
CONCLUSIONES.....	99
RECOMENDACIONES.....	100
BIBLIOGRAFÍA.....	101

ÍNDICE DE FIGURAS

Figura 1.1 Émbolo de cierre muerto y Cerradura extra de seguridad	13
Figura 3.1 Las capas de la pila de protocolos para ZigBee	28
Figura 3.2 Tipo de nodos y las topologías de las redes ZigBee [9].....	30
Figura 3.3 XBee Series 2	38
Figura 3.4 Diagrama del flujo del sistema de datos en un entorno de interfaz UART (señales que se activan en baja son distinguidas con una línea horizontal sobre el nombre.)	38
Figura 3.5 Paquete de datos UART = 0x1f (31 en decimal) transmitido a través del módulo XBee. Formato de datos: 8-n-1 (bits- paridad-#de bits de parada).....	38
Figura 3.6 Diagrama del flujo interno de datos	39
Figura 3.7 Sintaxis de los comandos AT	40
Figura 3.8 Secuencia del modo de transmisión.....	41
Figura 3.9 Opciones de antena en los módulos Xbee.....	42
Figura 3.10 Dibujos mecánicos de los módulos OEM Xbee series 2.....	43
Figura 4.1 Medidas del edificio.....	46
Figura 4.2 Frente del edificio	46
Figura 4.3 Plano arquitectónico del departamento 201	47
Figura 4.4 Ubicación del módulo de monitoreo en el dormitorio 3.	48
Figura 4.5 Instalación de un sensor de rotura de vidrio.	49
Figura 4.6 Ubicación del módulo de monitoreo en la sala.	49
Figura 4.7 Ubicación del módulo de monitoreo en la mampara del balcón	50
Figura 4.8 Interacción entre el módulo control remoto y el módulo coordinador para el encendido y apagado del sistema de seguridad.....	51
Figura 4.9 Interacción entre el módulo de monitoreo y el módulo coordinador para el envío de la señal de alerta	51
Figura 4.10 Interacción entre el módulo coordinador y el módulo de aviso para el envío de la señal de alerta.....	52
Figura 4.11 Diagrama de conexionado: Fuente de alimentación con cargador de batería Elk-624 encargada de energizar al módulo coordinador.....	54
Figura 4.12 Batería de respaldo para el módulo coordinador [28].	55
Figura 4.13 Diagrama esquemático de los circuitos de alimentación del microcontrolador (izquierda) y XBee (derecha).....	55
Figura 4.14 Circuito esquemático de una fuente regulada de 6 voltios con cargador de batería e indicador de carga.	57
Figura 4.15 Buzzer DC de estado sólido	58
Figura 4.16 Diagrama esquemático de la interfaz entre el microcontrolador y el buzzer.	58
Figura 4.17 Diagrama esquemático del módulo coordinador	59
Figura 4.18 Contacto magnético para montaje en superficie	62
Figura 4.19 USP window bug glass.....	62
Figura 4.20 Circuito de pulso para despertar al microcontrolador y XBee.	63
Figura 4.21 Diagrama del estado del módulo de monitoreo por ciclos.....	68
Figura 4.22 Curva de descarga del voltaje de la pila Duracell [32].	69
Figura 4.23 Pila Duracell MN 1500-AA, una de las posibilidades de fuente de energía para los módulos de monitoreo [32].	70
Figura 4.24 Curva de descarga del voltaje de la pila LS 14500.....	70
Figura 4.25 Pila SAFT LS 14500-AA, una de las posibilidades de fuente de energía para los módulos de monitoreo [33].	71
Figura 4.26 Diagrama esquemático del módulo de monitoreo.....	71
Figura 4.27 Módulo control remoto	73
Figura 4.28 Diagrama esquemático del módulo de control remoto	75

Figura 4.29 Pila duracell tipo AAA para energizar al módulo de control remoto 76

Figura 4.30 Concluye el proceso de grabación (ver la parte inferior) 79

Figura 4.31 Cuadro de dialogo para asignar el nombre *MONITOR2* a uno de los módulos XBee..... 80

Figura 5.1 Diagrama esquemático del circuito entre el sensor (terminal) y el microcontrolador..... 90

Figura 5.2 Izquierda: XBee de monitoreo conectado serialmente a la PC mediante la Tarjeta RS-232 Development Board Part # XBIB-R. Derecha: XBee coordinador con sus baterías, es el dispositivo móvil en las ubicaciones 1, 2, 3, 4, 5, 6 y 7 de la Tabla 5.3 y la Figura 5.5. 91

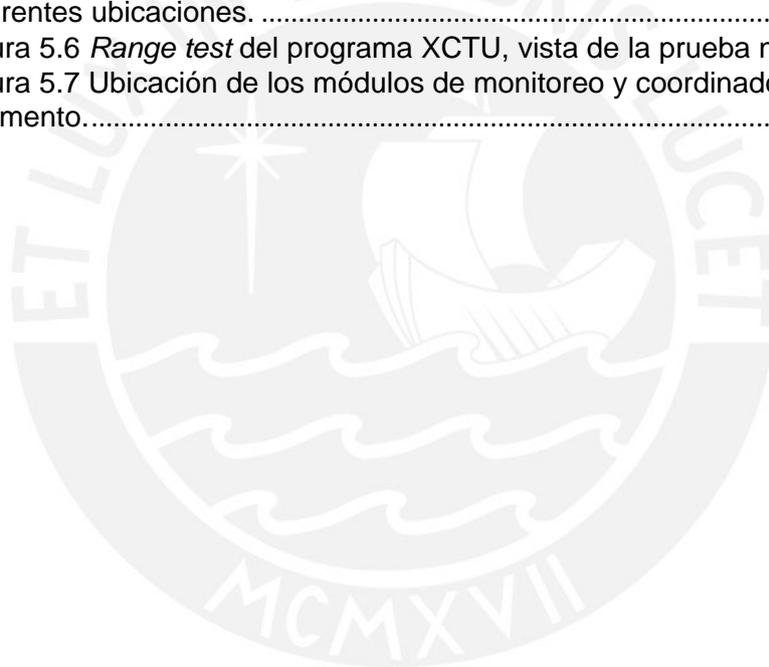
Figura 5.3 Dispositivos que intervienen en la prueba de rango. Izquierda Tarjeta RS-232 Development Board Part # XBIB-R con el XBee de Monitoreo con loopback. Derecha: Protoboard que contiene al XBee Coordinador. 93

Figura 5.4 Verificación del loopback, en azul los caracteres emitidos desde el XBee de monitoreo y en rojo los mismos caracteres pero enviados desde el XBee coordinador mediante el loopback. *Se tipeó rápidamente para observar la rapidez de la transmisión*..... 94

Figura 5.5 Distancias entre el módulo de monitoreo y el módulo coordinador en sus diferentes ubicaciones. 95

Figura 5.6 *Range test* del programa XCTU, vista de la prueba número 7. 97

Figura 5.7 Ubicación de los módulos de monitoreo y coordinador en el departamento..... 99



ÍNDICE DE TABLAS

Tabla 4.1 Consumo máximo de corrientes y cálculo de la potencia total que el módulo coordinador consume.....	54
Tabla 4.2 Funciones de los dos tipos de módulos de monitoreo.....	60
Tabla 4.3 Tipo de módulo de monitoreo según el lugar de ubicación.....	63
Tabla 4.4 Parámetros del transistor 2N3904 [30].....	64
Tabla 4.5 Estado del XBee según el estado del módulo de monitoreo al que pertenece.....	64
Tabla 4.6 Cálculo de corrientes según el estado del contacto magnético.	65
Tabla 4.7 Tiempo que el Microcontrolador y XBee permanecen dormidos y sus respectivos consumos de energía.....	67
Tabla 4.8 Versiones de firmware para cada XBee.....	78
Tabla 4.9 Valores de los parámetros principales en cada módulo del sistema de seguridad.....	81
Tabla 5.1 Resultados de la configuración previa a la prueba de rango.....	92
Tabla 5.2 Resultado de la ejecución del comando ATND en el módulo coordinador.....	93
Tabla 5.3 Resultado de las pruebas para cada una de las ubicaciones del XBee coordinador (1, 2, 3, 4, 5, 6 y 7) con respecto al XBee de monitoreo (M).....	96
Tabla 5.4 Resultado de la medición de distancias entre el coordinador y el resto de módulos de monitoreo.....	98



INTRODUCCIÓN

El actual crecimiento del sector construcción referente a los edificios de departamentos y la gran demanda por seguridad ciudadana en Lima desprenden en la presente tesis una búsqueda por mejorar el nivel de seguridad y confort en aquellas personas que viven en un edificio de departamentos. Los dueños de departamentos, enfrentan una alta probabilidad de intrusión en sus viviendas, teniendo una gran cantidad de personas desconocidas viviendo a su alrededor, ingresando a sus edificios y a las zonas comunes.

Por tal razón la presente tesis tiene por objetivo diseñar un sistema de seguridad contra intrusión para edificios de departamentos, para lo cual se ha seguido un proceso que incluye la definición del edificio y el departamento, el funcionamiento del sistema y el diseño físico-lógico de los módulos que monitorean las áreas más inseguras del departamento.

El capítulo I contiene la seguridad y la domótica en los departamentos, incluyendo la problemática de la seguridad y los sistemas domóticos en los edificios de departamentos. En el capítulo II, se hace una comparación de tecnologías de automatización, abordando los sistemas cableados, los sistemas inalámbricos, las características del sistema de seguridad, la comparación de tecnologías y la elección de la tecnología ZigBee.

El capítulo III trata de la especificación ZigBee y elección del módulo para el diseño del sistema de seguridad, incluye una comparación de los circuitos integrados ZigBee: Transceptores, Chips, Socs y Sips y el módulo elegido el: XBee Series 2.

En el capítulo IV se detalla el diseño y la elección de componentes físicos (dispositivos electrónicos) y lógicos (firmware y software) de cada uno de los módulos que conforma el sistema de seguridad en un departamento.

El capítulo V contiene las Pruebas y Mediciones, en el se incluyen la medición de corrientes: Módulo de monitoreo y Módulo coordinador, Prueba de Rango que mide la calidad de la señal recibida entre el XBee coordinador y el XBee de monitoreo; finalmente se presentan las conclusiones de las pruebas y se incluyen los anexos y la bibliografía.

1 LA SEGURIDAD Y LA DOMÓTICA EN LOS DEPARTAMENTOS

1.1 Problemática de la seguridad

La seguridad ciudadana es definida como la protección que brinda el Estado y en cuya consolidación colabora la sociedad. Actualmente, la percepción de inseguridad en el Perú, medida mediante la tasa de homicidios es muy alta, aún cuando las cifras de los distintos delitos en el país son porcentual y absolutamente más bajas que en muchos de los países latinoamericanos; así El Caribe y África del Sur presentan las mayores tasas de homicidios por cada 100,000 habitantes, Perú tiene 4.3 homicidios por cada 100,000 habitantes; por ello, el tema prioritario es desarrollar políticas y estrategias para la reducción significativa de los riesgos y amenazas que generan hechos de violencia. La seguridad ciudadana, es un factor cada vez mas importante en la vida actual, por tener un enemigo real y potencial, como es el crimen organizado y la delincuencia común en todas sus modalidades, pandillaje pernicioso, tráfico ilícito de drogas; entre otros, que cada día van en aumento por causas de la extrema pobreza, el desempleo, la desocupación, la falta de una política educativa, la influencia negativa de algunos medios de comunicación, la falta de un plan de desarrollo con visión de largo plazo, la baja asignación de recursos del tesoro público para las instituciones, la desintegración de hogares, la falta de políticas de apoyo al desarrollo local y la inadecuada legislación vigente.

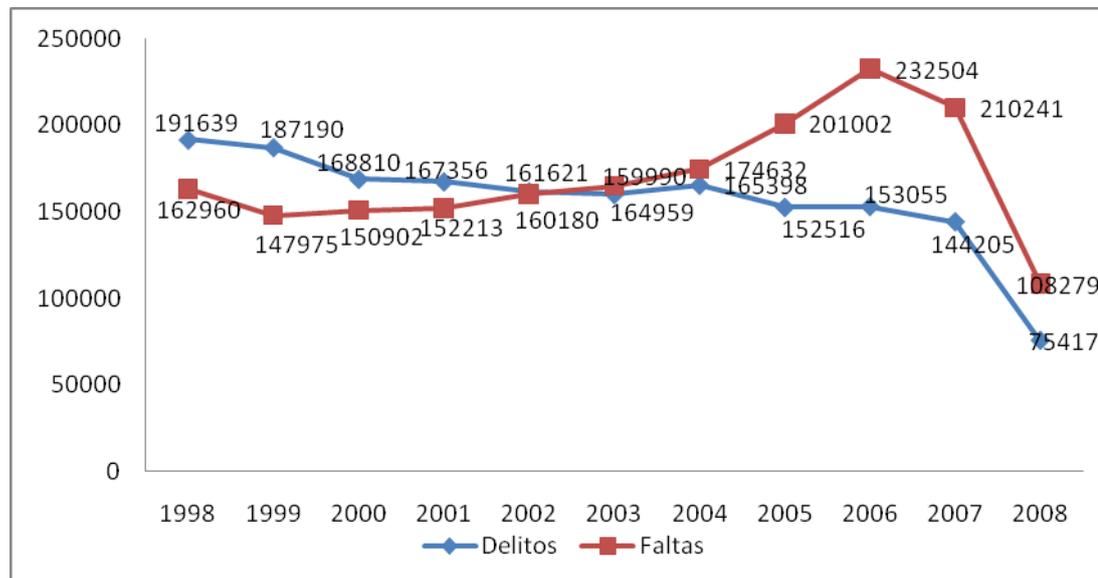
Por ello, la ciudadanía reclama una política de seguridad que resuelva y prevenga especialmente hechos que atentan contra los patrimonios privados.

1.1.1. Situación delincencial en el Perú.

La formación de una ciudadanía competente comienza en el hogar, continúa y se fortalece mediante una educación de calidad en las instituciones educativas, se consolida en la comunidad mediante la práctica cotidiana; pero la crisis de valores que en nuestro país tiene una consistencia social muy compleja, viene dando lugar a manifestaciones preocupantes en el comportamiento social y que se manifiestan sobre todo en la intolerancia, la corrupción, la agresividad, el atropello del orden social establecido, la falta de respeto a los derechos humanos; y sobre todo, el incremento de la delincuencia común y organizada. [1]

La comisión de seguridad ciudadana emitió un informe en el cual señalaba la carencia de una política integral del Estado en materia de seguridad ciudadana, este hecho motivó la promulgación de la Ley N° 27933 “Ley del Sistema Nacional de Seguridad Ciudadana”; y la elaboración del Reglamento de la Ley N° 27933 aprobado por Decreto Supremo N° 012–2003–IN del 07 de Octubre del 2003.

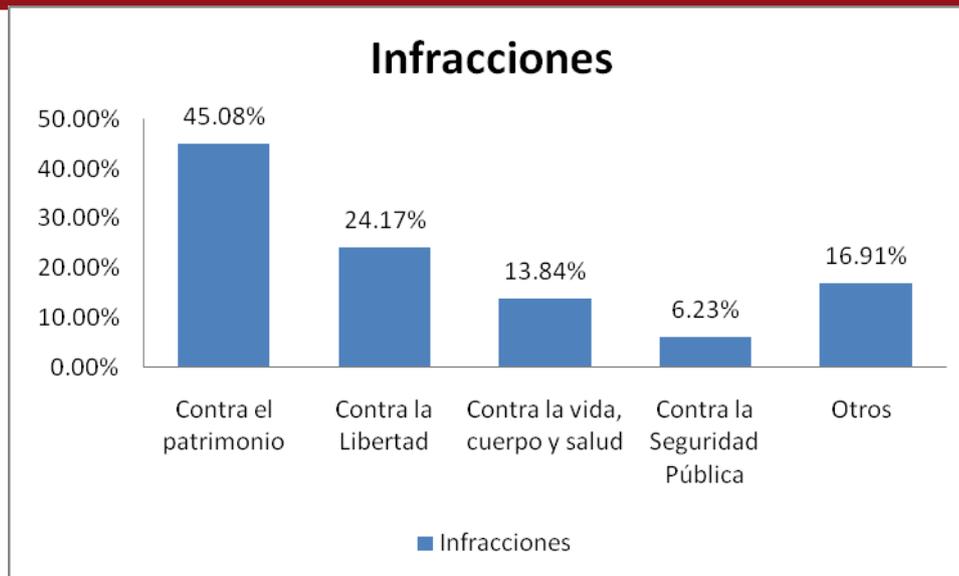
Otra información referida a la victimización es la que recopila la Policía Nacional del Perú-PNP. Así, en la siguiente ilustración se observa la evolución en un periodo de 10 años del registro de denuncias que la PNP, a través de sus Comisarías, recibe a nivel nacional.



Gráfica 1.1 Denuncias Registradas por la PNP por comisión de delitos y faltas, a nivel nacional (Fuente: Observatorio de la Criminalidad del M.P)

Según el observatorio de la criminalidad del Ministerio Público, entre enero del 2006 al 31 de diciembre del 2008 se han registrado 176,907 denuncias por presunta comisión del delito contra el patrimonio en 27 distritos judiciales; así, en el 2006 se registraron 49,088 delitos, en el 2007 62,032, en el 2008, 65,787 delitos y a marzo del 2009 se han registrado 19,768 delitos. Los distritos Judiciales con mayor número de delitos son: Lima con 30.02%, Arequipa con 9.91%, Lambayeque con 6.80%. La Libertad con 6.4%. Callao con 4.47% y otros con 42.76%. Las modalidades delictivas de mayor incidencia son: - Delito de Hurto: 28.7 %,Delito de Robo: 20.6%, - Delito de Estafa: 14.4%,-Usurpación:11.30%,-Otros 25.00%.

Las infracciones de mayor incidencia en los 27 distritos judiciales del Perú son: Contra el patrimonio 45.08%, contra la libertad 24.17%, contra la vida, cuerpo y salud 13.84%, contra la Seguridad Pública 6.23%, Otros 16.91%.



Gráfica 1.2 Infracciones de mayor incidencia en los 27 distritos judiciales

1.1.2. Demanda ciudadana por protección y seguridad

La evolución de los recursos humanos en la Policía Nacional revela un progresivo decrecimiento, al pasar de 120,000 efectivos que existían en 1985 durante la unificación de las Fuerzas Policiales, a 92,000 policías que tiene en la actualidad; es decir, en 23 años la institución policial ha sufrido una disminución del 24%, mientras que la población se ha incrementado en 60.7% (28'220,764.); lo que permite inferir que la demanda de la población por protección y seguridad es cada vez mayor en comparación a la oferta de servicios policiales. El esfuerzo de los municipios y de la sociedad civil en apoyo a las comisarías de sus jurisdicciones se viene realizando en forma aislada en varias provincias y distritos del país, pero sin criterios orientadores que posibiliten un trabajo más eficiente, que posibilite una acción integral en diferentes frentes [2].

1.1.3. Modalidades y aspectos del robo en las viviendas

Los delincuentes ingresan directamente por las vías de acceso normal, aprovechando el descuido, ausencia o falta de control del sistema de conserjería y mediante escalamientos, para lo cual aprovechan las condiciones arquitectónicas del propio edificio. En un 99% estos delitos son con información previa sobre las especies de valor que puedan mantenerse en el hogar, como joyas, dinero en efectivo, armas, obras de arte, todo de fácil transporte y en algunos casos con utilización de llaves, a cuyas copias han accedido con cooperación de alguien que haya visitado o trabajado en el mismo departamento.

Modalidad 1: Robos con muerto como 'cómplice'. Los ladrones van a velorios y se fijan en las personas que firman el registro de visitantes. Cuando observan a varias

personas que comparten el mismo apellido asumen que su casa está sola. Entonces, con directorio telefónico en mano, buscan la dirección y se dirigen a desocuparles la casa aprovechando el tiempo que se demoran en el velatorio y luego en el entierro.

Modalidad 2: Funcionarios falsos. Se presentan con uniformes de la Policía, armados, con expedientes con logos, carné y órdenes de allanamiento, simulando una operación oficial. Las estadísticas indican que siempre hay un iniciador, ya sea un conductor, una empleada del servicio o un familiar. Se da en estratos altos, una variante es con supuestos empleados de servicios públicos.

Modalidad 3: Inteligencia a los vecinos. Es una nueva modalidad frecuente en conjuntos de casas y apartamentos. Los delincuentes arriendan una vivienda por dos o tres meses con documentos falsos. Luego, le hacen inteligencia a los vecinos, estableciendo los horarios de llegada y de salida de cada uno de los miembros del grupo familiar. Cuando saben que todos están por fuera entran con llaves maestras.

1.1.4. Plan de seguridad en las viviendas

La Seguridad Ciudadana en sentido amplio es una situación social en la que no existe riesgos o peligros para los ciudadanos; es decir, que éstos pueden ejercitar libremente sus derechos y libertades sin que exista obstáculo para ello. La Seguridad Ciudadana, es el conjunto de medidas y previsiones que adopta el Estado, a través de sus instituciones y de la comunidad organizada, dentro del marco de la Ley y los derechos humanos, con la finalidad que las personas puedan desarrollar sus actividades libres de riesgos y amenazas que genera la criminalidad y delincuencia.

1.1.4.1. Criterios preventivos del dueño de casa

Disuasión. Variar los itinerarios de salida y regreso del trabajo a la casa ayuda a despistar a ladrones que estén haciendo un seguimiento.

Detección. Poner alarmas en puertas y ventanas es la forma más segura de detectar un ladrón¹, pero unos vecinos atentos y alerta frente a actividades inusuales que les notifiquen a las autoridades también son un medio efectivo de detección.

Demora. Causar una demora de cuatro minutos a un ladrón se considera generalmente como suficiente para prevenir el ingreso a un lugar de residencia. Un ladrón quiere evitar ser atrapado, de manera que mientras más tiempo requiera para forzar una puerta o ventana, mayor será su riesgo. Teniendo en mente los principios de la disuasión, la detección y la demora, usted tendrá mayores probabilidades de impedir que el ladrón tenga acceso a su objetivo.

¹ Para el diseño del sistema de seguridad se tuvo muy en cuenta esta recomendación.

1.1.4.2. Criterios preventivos en la infraestructura

Entrada Principal. Todas las puertas de entrada principal deben ser revestidas en metal o construidas en madera sólida. Una cerradura de seguridad, además de la cerradura de llave en la manija o perilla, es esencial. Usar un visor o mirilla de ángulo amplio en lugar de una cadena de puerta para observar a quienes llaman a la puerta. Una puerta enrejada ofrece protección adicional si se mantiene cerrada con seguro, el inconveniente es el daño de la estética.

Luces Interiores. Mantener algunas luces internas prendidas mientras se encuentra fuera de casa. Para crear la impresión de que hay alguien en casa, se usa un temporizador para prender y apagar luces a horas normales. Una radio sonando contribuye a crear la ilusión de que la casa está ocupada.

Integración Vecinal. Compartir con los vecinos las preocupaciones e inquietudes sobre el robo casero. Contar a los vecinos lo que se está haciendo para proteger el hogar y pedir que reporten cualquier persona o actividad sospechosa alrededor de su casa a las autoridades.

Alarmas. Conseguir alarmas residenciales contra robo en tiendas de artículos eléctricos y de ferretería, así como sistemas completos que pueden ser arrendados o comprados a compañías de alarmas. La mayoría de las alarmas residenciales emiten un fuerte ruido mediante una campana, sirena, o generador de tonos. Una alarma audible en puertas y ventanas puede ser un factor de disuasión efectivo para el ladrón aficionado. Asegurarse que familia y vecinos estén informados sobre su función y que sean capacitados para llamar a sus autoridades cuando oigan la alarma.

Puertas con bisagras. Es importante que todas las puertas exteriores con bisagras sean de construcción medular sólida (1 pulgada de grosor si son de madera) o revestidas de metal. Las puertas de núcleo hueco o de tablero aglomerado pueden ser fácilmente apaleadas. Cuando revise la seguridad de sus puertas, tener en cuenta la puerta misma, así como las bisagras, los cerrojos y cerraduras, y cualquier otro accesorio de ferretería.

Cerraduras para puertas con bisagras. La cerradura más frecuentemente usada para las puertas con bisagra es la cerradura de pestillo con la llave en la manija o perilla. Se recomienda un émbolo de cierre muerto para todas las cerraduras de llave en la manija o perilla. (Figura 1.1). Dado que las cerraduras de llave en la manija pueden ser forzadas rompiendo la manija o perilla, o abiertas introduciendo un pedazo de plástico entre la batiente y el perno o pestillo, todas las cerraduras de puertas exteriores de este tipo deben ser complementadas mediante la adición de una cerradura de seguridad.



Figura 1.1 Émbolo de cierre muerto y Cerradura extra de seguridad

Puertas corredizas de vidrio. La mejor cerradura para una puerta corrediza de vidrio es una cerradura de seguridad, que utiliza un pasador de perno cilíndrico y es operable mediante llave desde el exterior [3].

1.1.5. Declaración del marco problemático

El plan seguridad de los edificios de departamentos en nuestro país se diseña en función a las costumbres, a nuestra cultura, con limitados recursos económicos, con desconocimiento de sistemas de automatización electrónicos, que de ser tomados en cuenta, lograrían una prevención efectiva de la seguridad en el hogar, sin perjudicar la estética y con funcionamiento automático.

La gran mayoría de peruanos, dueños o inquilinos de una vivienda, realizan el proceso de seguridad de su hogar personalmente y en forma manual, revisando las cerraduras y puertas del departamento, así como también variando sus horas de salida e ingreso, o disponiendo de algún circuito de alarma precario sin automatismos que permitan un buen desempeño y confiabilidad.

Teniendo en cuenta que de las denuncias por comisión de delitos corresponden en mayor grado a delitos contra el patrimonio; que la demanda de la población por protección y seguridad es cada vez mayor en comparación a la oferta de servicios policiales y que las modalidades de robo y hurto que atentan contra el patrimonio son cada vez más variados, es por ello que el presente trabajo de tesis propone el diseño de un sistema automatizado de seguridad contra intrusión para departamentos que disminuya la brecha de todas estas carencias para la seguridad del dueño de una vivienda.

1.2. Sistemas domóticos en los edificios de departamentos

Para entender a los sistemas automatizados de seguridad del hogar se debe explicar en primer lugar el significado de la palabra domótica, así como las diferentes formas de implementación de esta ciencia.

1.2.1. La domótica

Las redes de datos en el hogar conforman la ciencia llamada domótica; de origen francés, se usa para referirse a la automatización de la vivienda. Además de este vocablo, se emplean otras expresiones para referirnos a este campo, como son homesystems, sistemas domóticos o home automation. La domótica es también la parte de la tecnología (electrónica, telecomunicaciones e informática), que integra el control y supervisión de los elementos existentes en una vivienda.

1.2.1.1. Sistemas centralizados

En un sistema de domótica de arquitectura centralizada, un controlador centralizado, envía la información a los actuadores e interfaces según el programa, la configuración y la información que recibe de los sensores, sistemas interconectados y usuarios.

1.2.1.2. Sistemas descentralizados o distribuidos

Son sistemas que se basan en un medio de comunicación. Todos los componentes que lo forman comparten la misma línea de comunicación y cada uno tiene independencia en las funciones de control y mando. Aparentemente son equipos más costosos pero ofrecen muchas ventajas como un menor coste de instalación ya que la instalación sería lineal mediante un cable BUS que realizaría la comunicación entre los diferentes nodos.

1.2.1.3. Sistema abierto

Es aquel sistema domótico que no está sujeto a pagos de licencias para su utilización, sus componentes están de acuerdo con normas que garantizan su compatibilidad, aunque procedan de diferentes fuentes de aprovisionamiento. Por lo tanto, es aquel que permitiría sustituir, cualquiera de los componentes o dispositivos preseleccionados, por uno similar de otro fabricante, que siga cumpliendo la funcionalidad y requisitos impuestos en el sistema domótico instalado.

1.2.1.4. Sistema propietario o cerrado

Es un producto o sistema desarrollado por una empresa para sólo poder interactuar con sus propios dispositivos. De esta manera, estos productos sólo pueden ser instalados e integrados con productos del propio fabricante, no es posible intercambiar dispositivos con diferentes tecnologías o de otros fabricantes.

1.2.2. Tipología de la vivienda

Los grupos demográficos que cubren las demandas de implantación de estos sistemas son matrimonios jóvenes, que pasan poco tiempo en casa, discapacitados, personas mayores y familias con varios hijos. Las viviendas que incorporan sistemas domóticos tienen el siguiente orden:

- Departamentos modernos.
- Segunda residencia (sistemas de telecontrol, de calefacción, alarmas, etc.)
- Rehabilitaciones de viviendas habitadas.

1.2.3. Oferta nacional

En nuestro país se realizó un análisis del mercado peruano de los sistemas domóticos, el cual lo realizó la empresa UNMSM Domotics Corp, encontrándose que no existen empresas, dedicadas exclusivamente al servicio de automatización de viviendas. Aunque existen empresas dedicadas a un sector más general que engloba de cierta forma la automatización de viviendas, estas empresas son [4]:

1. Elecontrol Ingenieros
2. Controlmatic
3. Siemens
4. Automatic solutions
5. Edificios inteligentes
6. Segó
7. Sensormatic
8. Servicios técnicos industriales *Bejarano*
9. La casa del intercomunicador

1.2.4. Demanda nacional

En el capítulo I se muestra una verdadera necesidad de seguridad en las viviendas peruanas, se expone como principal problema el robo en las viviendas y es así entonces como se puede deducir, tras el análisis de los sistemas domóticos, que estos sistemas pueden traer como consecuencia un impacto positivo en la solución de este problema.

Con el uso de la domótica en las viviendas se pueden brindar las siguientes soluciones: Detección de un posible intruso, Detección de rotura de vidrios en las ventanas y puertas de vidrio, Transmisión de alarmas.

2 COMPARACIÓN DE TECNOLOGÍAS DE AUTOMATIZACIÓN

2.1. Sistemas cableados

En esta sección se detallarán las características de las tecnologías que brindan una solución domótica de manera cableada.

2.1.1. Konnex

Este estándar surge de la integración de las tecnologías domóticas EIB, EHS y Batibus, para crear un único estándar europeo que sea capaz de competir ventajosamente en calidad, prestaciones y precios con otros sistemas norteamericanos como el LonWorks o CeBus. Se puede afirmar que este nuevo estándar tiene lo mejor del EIB, EHS y Batibus; aumenta considerablemente la oferta de productos para el mercado residencial el cual ha sido, hasta la fecha, el trabajo pendiente de este tipo de tecnologías. El estándar KNX incluye diversos medios de comunicación. Cada medio de comunicación puede ser utilizado en combinación con uno o más modos de configuración, permitiendo a cada fabricante escoger la combinación correcta para cada segmento de mercado y aplicación [5]. En la actualidad, se están usando o se están desarrollando los siguientes medios físicos: PL-2400: Corrientes Portadoras a 2400 bps, TP0: Par Trenzado a 4800 bps (Idéntico a nivel físico del BatiBUS), TP1: Par Trenzado / Coaxial a 9600 bps, TP2: Par Trenzado a 64 Kbps.

2.1.2. Lonworks

Es un protocolo propietario desarrollado por la empresa Echelon el cual ha sido usado por una diversidad de empresas para desarrollar sistemas propietarios de automatización [6]. Por medio de un Bus (cable) de comunicaciones que une todas las plantas de la vivienda, los módulos conectados a él comparten información unos con otros. La gran ventaja de este sistema es que queda abierto a la incorporación de nuevos elementos que se integren en la red, como pueden ser luces exteriores de jardín, riego automático, alarmas técnicas en calderas, etc, así como el hecho de disponer de un cableado virtual mediante el cual, en cualquier momento se puede reconfigurar la instalación para conseguir actuaciones y funcionalidades diferentes.

Este estándar americano de sistemas de control fue presentado por *Echelon* en el año 1992; desde entonces multitud de empresas viene usando esta tecnología para implementar redes de control distribuidas y automatización. Aunque está diseñada

para cubrir los requisitos de la mayoría de las aplicaciones de control, sólo ha tenido éxito de implantación en edificios de oficinas, hoteles o industrias, ya que, debido a su coste, no ha tenido una implantación masiva en los hogares, sobretodo porque existen otras tecnologías de prestaciones similares mucho más baratas. Esta tecnología contempla varios medios de transmisión como: cable, ondas portadoras y fibra óptica.

2.1.3. Tecnología X-10

Es una tecnología que permite la transmisión unidireccional (o bidireccional) de datos a muy baja velocidad (50 Bps) por la red eléctrica (ondas portadoras). El esquema de direccionamiento de dispositivos es muy sencillo y siempre se debe delegar a un sistema superior para tomar la iniciativa en el envío y gestión de los comandos. Los actuadores X-10 se limitan a decodificar las órdenes recibidas y ejecutarlas sin realizar ningún proceso complejo o de análisis. En general, cualquier sistema de automatización basado en X-10 hace uso de este protocolo para gobernar los actuadores instalados en la vivienda, los módulos X-10 de diferentes fabricantes son intercambiables entre sí. Las funciones complejas (escenarios, programaciones, funciones lógicas, etc) deben ser procesadas en el sistema propietario desarrollado por una empresa [7].

2.2. Sistemas inalámbricos

Las tecnologías inalámbricas han adquirido una importancia creciente debido a su bajo coste y su facilidad de instalación; en el ámbito de la domótica la comunicación inalámbrica se utiliza para la propagación física de información a través de la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión. Los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, como por ejemplo: Antenas, Laptops, PDAs, Teléfonos Celulares, etc [8].

2.2.1. IEEE 802.15.4

Es un estándar del organismo IEEE para la transmisión de datos a baja velocidad, con bajas latencias y con muy bajo consumos. Cubre el nivel físico y de acceso al medio (MAC), dando cabida que en las capas superiores se puedan elaborar sistemas propietarios.

El estándar IEEE 802.15.4 soporta múltiples topologías para su conexión en red, entre ellas la topología tipo Estrella y la topología Punto a Punto. La topología a

escoger es una elección de diseño y va a estar dado por la aplicación a la que se desee orientar; algunas aplicaciones como periféricos e interfaces de PC, requieren de conexiones de baja potencia de tipo estrella, mientras que otros como los perímetros de seguridad requieren de una mayor área de cobertura por lo que es necesario implementar una red Punto a Punto. Las características del MAC IEEE 802.15.4 son: asociación/disociación, reconocimientos de entrega de trama (ACK), mecanismos de acceso al canal, validación de trama, control de garantía de ranuras de tiempo (Slot Time), control de guías (Beacon) y barrido de canal [9].

2.2.2. ZigBee

El término ZigBee describe un protocolo inalámbrico normalizado para la conexión de una Red de Área Personal (WPAN: Wireless personal area network). El protocolo es el trabajo de más de 70 compañías que se han asociado para crear y promocionar el nuevo estándar ZigBee, propiedad de un consorcio que ha llamado “Alianza ZigBee”. Esta es diferente de los otros estándares inalámbricos, ha sido diseñado para soportar un diverso mercado de aplicaciones que requieren un bajo costo y un bajo consumo, con una conectividad más sofisticada que los anteriores sistemas inalámbricos. El estándar ZigBee enfoca a un segmento del mercado no atendido por los estándares existentes, con baja transmisión de datos, bajo ciclo de servicio de conectividad. La razón de promover un nuevo protocolo como un estándar, es para permitir la interoperabilidad entre dispositivos fabricados por compañías diferentes.

Algunas de las características de ZigBee son:

- ZigBee opera en las bandas libres ISM (Industrial, Scientific & Medical) de 2.4 GHz, 868 MHz (Europa) y 915 MHz (Estados Unidos).
- Tiene una velocidad de transmisión de 250 Kbps y un rango de cobertura de 10 a 75 metros.
- A pesar de coexistir en la misma frecuencia con otro tipo de redes como WiFi o Bluetooth su desempeño no se ve afectado, esto debido a su baja tasa de transmisión y, a características propias del estándar IEEE 802.15.4.
- Capacidad de operar en redes de gran densidad, esta característica ayuda a aumentar la confiabilidad de la comunicación, ya que entre más nodos existan dentro de una red, entonces, mayor número de rutas alternas existirán para garantizar que un paquete llegue a su destino.
- Cada red ZigBee tiene un identificador de red único, lo que permita que coexistan varias redes en un mismo canal de comunicación sin ningún problema. Teóricamente pueden existir hasta 16 000 redes diferentes en un mismo canal y

cada red puede estar constituida por hasta 65 000 nodos, obviamente estos límites se ven truncados por algunas restricciones físicas (memoria disponible, ancho de banda, etc.).

- Es un protocolo de comunicación multi-salto, es decir, que se puede establecer comunicación entre dos nodos aún cuando estos se encuentren fuera del rango de transmisión, siempre y cuando existan otros nodos intermedios que los interconecten, de esta manera, se incrementa el área de cobertura de la red [10].

2.2.3. Hometronic

El sistema Hometronic es la solución de la marca Honeywell para el control de los elementos eléctricos de una vivienda, tanto de nueva construcción como construida. Su arquitectura es modular y su medio de transmisión es vía radiofrecuencia. Esta característica reduce su instalación en una nueva obra al eliminar las canalizaciones necesarias para otros sistemas y permite implementarse fácil y rápidamente en viviendas habitadas. Su modularidad le permite adaptarse en todo momento a nuevos planteamientos de obra y ofrece a sus usuarios una mayor accesibilidad a ampliaciones futuras pues no es necesario hacer una gran inversión sino que se puede ir repartiendo en el tiempo.

Con Hometronic el control domótico sobre los equipos y circuitos eléctricos se puede hacer individualmente o agrupados en escenas, por orden directa o por programación horaria. Localmente desde los pulsadores, desde su central de pared y desde un pequeño mando a distancia en cualquier lugar de la casa y desde el exterior, tanto por teléfono fijo y/o móvil como por Internet. Su sencilla estética y su reducido tamaño permiten su instalación vista u oculta, adaptándose a todos los estilos de decoración de una vivienda. También permite controlar hasta 16 escenas que consisten en la actuación conjunta de determinados elementos en situaciones preestablecidas como por ejemplo “salir de casa”: Las luces se apagan, las persianas se bajan, el agua se corta y la calefacción se apaga [11].

2.3. Características del sistema de seguridad

Se presentan las características más importantes que se han considerado para el diseño del sistema de seguridad,

- **Económico.** El sistema de seguridad diseñado en la presente tesis debe de ser competitivo en precio e incluso abaratarlos más con el uso de nuevas tecnologías.

- **Capacidad energética.** Deberá funcionar con un mínimo energía, que contribuya a la economía del cliente y al medio ambiente con la baja en emisiones de CO₂ por consumo eléctrico.
- **Escalabilidad.** Será la capacidad del sistema de seguridad en permitir instalar o incluir un nodo de supervisión adicional.
- **Seguridad.** En este caso, podemos referirnos a la seguridad del sistema ante fallas, es necesario que el sistema indique en todo momento que errores está presentando, con la finalidad de que el usuario pueda corregirlas a tiempo. También la seguridad se refiere a las diferentes características que debe tener el sistema de seguridad para establecer una comunicación confiable entre dispositivos que asegure la transmisión correcta de datos sin colisiones u otros errores.
- **Sincronización en tiempo real.** La habilidad de transmitir datos entre todos los dispositivos en tiempo real sin errores es muy importante al momento de detectar una intrusión.
- **Estética.** La instalación del sistema de seguridad deberá también adaptarse estéticamente a viviendas terminadas en caso que hayan sido construidas sin considerar la instalación de un sistema de seguridad.
- **Portátil.** Existe un gran porcentaje de personas que viven en departamentos alquilados, por ello el sistema de seguridad deberá de ser portátil, en caso de que los habitantes del departamento quieran mudarse, el sistema se podrá mudar con ellos.
- **Sencillez.** Deberá ser fácil de usar y configurar.
- **Mantenimiento.** Como el sistema está orientado a ser utilizado por familias en departamentos, este sistema de seguridad deberá ser fácil de mantener en el tiempo. Las familias pueden adquirir el sistema al tener un bajo precio, pero sería contradictorio si es que este requiere de un mantenimiento muy frecuente.

Es en base a este conjunto de consideraciones se define el criterio de comparación entre tecnologías.

2.4. Comparación de tecnologías

De acuerdo a las características que deberá reunir el sistema de seguridad, se aplican los requerimientos (explicados en la sección anterior) a cada una de las tecnologías.

2.4.1. Elección de los Sistemas Abiertos

- **Economía para el cliente.** Como ya se expuso anteriormente, los sistemas abiertos no están sujetos a pagos de royalties o licencias para su utilización por lo que este tipo de sistemas son de gran utilidad para lograr el diseño de un sistema de seguridad accesible económicamente para los dueños de departamentos. Su mantenimiento tiene costes más bajos a comparación de los sistemas propietarios, existe una amplia gama de productos, y se tiene mucha flexibilidad y capacidad de ampliación. En el caso que se requiera el reemplazo de uno de los dispositivos, no se tendrá que buscar únicamente a un fabricante sino que existe en el mercado una amplia gama de productos que pueden reemplazarlo.
- **Economía para el fabricante.** El uso de tecnologías abiertas permite disponer de información del software y el diseño de dispositivos. La fabricación de dispositivos para el sistema de seguridad podría provenir de ingenieros peruanos obteniendo ventajas como: un ahorro en el costo de investigación versus la investigación extranjera, eliminación de costos de importación de un sistema ya diseñado, la promoción de la investigación y el desarrollo de productos electrónicos en nuestro país.

2.4.2. Comparación con la Tecnología X10

Capacidad energética. La tecnología X10 enfrenta un grave problema al estar este siempre dependiendo de la red eléctrica proveniente de las líneas eléctricas de la calle. El grave problema es que el sistema ya no funciona cuando hay un corte de energía en la red eléctrica del hogar.

Escalabilidad. La tecnología X-10 es bastante limitada en cuanto solo es posible instalar un máximo de 256 dispositivos que pueden responder a 6 funciones, lo cual también es un número reducido.

Seguridad y Confiabilidad. En este caso el hecho de que la comunicación se realice exclusivamente a través de la línea de poder no la hace confiable, pues uno de los medios menos seguros para transmitir información es precisamente la línea de poder por su alto nivel de ruido.

Costo. Tomando como referencia algunos de los dispositivos de un sistema de seguridad se mencionan los siguientes precios [12]:

Detector de movimiento interno X10:	\$ 88.81
Sensor de puertas y ventanas X10:	\$ 49.37
Mini mando llavero seguridad X10:	\$ 43.13

Estética. No necesita un tendido de cables adicional y eso asegura que no afecte la estética de las paredes y techos. Por el contrario los tomacorrientes aparecen ocupados todo el día por dispositivos de tamaños regulares, ese también es un factor que debe tomarse en cuenta al elegirse esta tecnología.

Transportable. Cada dispositivo está conectado a un tomacorriente y en caso de mudanza sencillamente se desconecta y se desinstala.

Sencillez. El sistema X10 se caracteriza por su sencillez y fácil instalación.

2.4.3. Comparación con las tecnologías Konnex, Lonworks y Hometronic

La ventaja de estas tres tecnologías es que son desarrolladas por prestigiosas empresas y alianzas tecnológicas, con el fin de obtener un producto competitivo y eficiente frente a varias alternativas en la Domótica e Inmótica. Se debe resaltar que la instalación de un sistema de seguridad con cualquiera de las 3 tecnologías se debe realizar por personal certificado.

Capacidad energética y seguridad. Al ser tecnologías aplicadas a la automatización de grandes edificios de oficinas usan la red eléctrica como suministro principal de energía teniendo como respaldo las baterías de plomo ácido. La seguridad en la comunicación entre sus dispositivos es respaldada por la calidad de las marcas mundialmente conocidas que las han desarrollado.

Escalabilidad. La escalabilidad es limitada y costosa, hay que verificar antes si el producto que se ha instalado puede albergar el número de dispositivos deseados. Con frecuencia cuando existen nuevos dispositivos que requieren ser agregados al sistema, se debe revisar que los controladores centrales permitan agregar nuevos dispositivos pues quizás ya han llegado a un límite. Si es que se pueden agregar nuevos dispositivos estos deberán de ser configurados en el controlador central, esta configuración tendrá que ser realizada por personal certificado en el equipo.

Costo. Las empresas vendedoras de productos con tecnologías Konnex, Lonworks o Hometronic (Honeywell) cobran por la instalación, la programación y el equipo o dispositivo (esto incluye costo de importación y envío) a todo eso se debe agregar el margen de ganancia de la empresa que está entre un 15 a 30% del precio de costo. Empresas como ControlMatic, especialistas en automatizar edificios, logran este tipo de instalaciones cobrando como mínimo 200 dólares por dispositivo instalado y programado, sin contar con el costo del equipo; un precio bastante elevado para el

dueño de un departamento teniendo en consideración la situación económica de las personas que viven en departamentos alquilados o departamentos pequeños.

Transportable. Lonworks brinda una automatización cableada [22]. Konnex y Hometronics brindan soluciones inalámbricas [5] en donde si se podría transportar el sistema de seguridad.

2.4.4. Comparación con la tecnología ZigBee

En esta sección se describirán las consideraciones que deberá tener un sistema de seguridad basado en la tecnología ZigBee.

Capacidad energética. La principal razón del ahorro energético en esta tecnología tiene como clave el modo “dormir”, los dispositivos ZigBee solo se despiertan para enviar mensajes y para revisar si les ha llegado alguno. Por eso las baterías, las cuales son su principal fuente de energía, podrían durar hasta un par de años sin tener que reemplazarlas o recargarlas [14].

Escalabilidad. El sistema de seguridad basado en el estándar ZigBee puede contener hasta 65536 dispositivos en una sola Red, pero un coordinador solo puede manejar hasta 255 nodos, el resto de dispositivos serian agregados a través de routers [9].

Seguridad y confiabilidad. El estándar IEEE 802.15.4, que es la base de la tecnología ZigBee, tiene mecanismos que aseguran la correcta transmisión de datos en la red. Estos mecanismos son: CSMA-CA, las tramas con acuse, y la verificación de datos. Así mismo la capa de enlace del estándar IEEE 802.15.4 especifica cuatro servicios de seguridad: control de acceso, encriptación de datos, integridad de la trama, y actualización secuencial [9].

Costo. El costo de un circuito integrado que cuente con la capacidad para desarrollar un perfil para una aplicación ZigBee es de aproximadamente 10\$ (incluye costo de envío e importación). Si no se cuenta con la capacitación para desarrollar un perfil ZigBee en una aplicación existen circuitos integrados del valor de 25\$ (incluye costo de envío e importación) que contienen un Perfil General que se puede adaptar a diversas aplicaciones específicas (Ver sección 3.6)

Estética. ZigBee, al ser una tecnología inalámbrica especialmente diseñada para automatizar redes de baja transferencia de datos (perfecta para la domótica), cuenta con circuitos electrónicos bastante pequeños. La instalación de esta tecnología no requiere de cables por lo tanto no afecta la estética de las paredes [23].

Portátil. Los nodos pueden desinstalarse fácilmente por su pequeño tamaño y porque no contiene cableado.

Sencillez. Dependerá del sistema a diseñar.

2.5. Conclusión de la comparación

Teniendo como referencia las características de los sistemas de seguridad aplicados para cada una de las tecnologías de automatización de la seguridad, en esta sección se explicarán los detalles de la exclusión de ciertas tecnologías para el diseño e implementación del sistema de seguridad a desarrollarse en la presente tesis.

2.5.1. Eliminación de las tecnologías Konnex, Lonworks y Hometronic.

La presente tesis tiene como objetivo diseñar un sistema de seguridad que principalmente sea confiable, no tenga un elevado costo y que no perjudique la estética de su vivienda. Es incuestionable la calidad de estas tres tecnologías, pero el inconveniente principal es el dinero que se tiene que invertir para obtener un sistema de seguridad. También hay que resaltar que son muy pocas las compañías en el Perú que pueden brindar una solución de automatización con estas tecnologías y al no haber competencia en el mercado de la domótica el costo se mantendrá elevado.

Además de las comparaciones detalladas en este capítulo, el uso de la tecnología Konnex resulta muy adecuado para edificios de oficinas de tamaño medio, en donde el control eléctrico prima sobre el control de grandes máquinas climatizadoras, pero no para el control y la supervisión de la seguridad anti- intrusión de un departamento. El uso de tecnología Lonworks, resulta muy adecuado cuando se trata de edificios donde el control de máquinas de climatización y las estrategias de ahorro energético priman sobre otras consideraciones. Para este tipo de proyectos con LonWorks es necesaria la utilización de herramientas de programación similares a las que se utilizan en procesos industriales. Esta tecnología es muy eficaz en su desempeño a la hora de automatizar un edificio, sin embargo el costo por sistema es más elevado que cualquier otra tecnología [13]. Además el funcionamiento de esta tecnología depende de un circuito integrado, el Neuron Chip, que es elaborado por una única empresa.

Hometronic de Honeywell, es utilizado en proyectos para viviendas y ofrece las mismas características que los sistemas más sofisticados [11] como Konnex y LonWorks, pero con un menor nivel de complejidad y por lo tanto con menos problemas de programación, ingeniería, puesta en marcha y mantenimiento. Su principal inconveniente es el costo de importación, instalación y programación.

2.5.2. Eliminación de la tecnología X10

La mayoría de nuestros hogares no están automatizados, lo más cercano que podemos disfrutar es utilizando la tecnología X10, la cual ha sido utilizada mundialmente por alrededor de 25 años pero lamentablemente esta tecnología no ha “estallado” en el círculo de la domótica.

X10 puede realizar varios automatismos interesantes como asegurar y desasegurar las puertas en ciertos tiempos, monitorear el clima, ajustar el alumbrado, **pero existen tres problemas con X-10 que no la han permitido extenderse como tecnología integral en la automatización de viviendas.** El primer problema es que esta tecnología no ofrece una comunicación de 2 vías (Rx y Tx), por lo que los dispositivos X10 pueden solamente recibir información de un computador central, pero no reportar hacia él. El segundo problema es que X10 no es una tecnología “sin cables” (wireless) ya que utiliza el tendido eléctrico en el hogar para enviar pulsos a través de esta y así activar a los dispositivos que siempre han de estar conectados a un tomacorriente, y el tercero es que siempre dependen del sistema eléctrico del departamento, si es que fallase el sistema eléctrico fallan también todos los dispositivos X10 incluido el sistema de seguridad. Se sabe, por las modalidades de robo, que en muchas de las intrusiones se corta el fluido eléctrico de la vivienda.

2.5.3. Elección de la tecnología ZigBee

Además de los beneficios que se encontraron en la evaluación tecnología de un sistema de seguridad, en la sección anterior, ahora se exponen algunas características que enriquecen la elección de una tecnología moderna, barata, que nos hace imaginar un mundo en donde los sensores se despliegan dentro y alrededor de las casas, centros de trabajo, hospitales, etc. Las redes de sensores y controladores inalámbricos nos permitirán conservar nuestros recursos, mejorar el nivel de vida e incrementar nuestra seguridad.

Necesidad de cambio

Cuando Wi-Fi y Bluetooth aparecieron, muchos usuarios de la tecnología X10 miraron a estas tecnologías emergentes como reemplazantes de la desactualizada X10, **pero ninguna de estas 2 tecnologías es idónea para la automatización de la vivienda.** Verdaderamente no necesitamos de un gran ancho de banda en las comunicaciones para automatizar una vivienda ni tampoco un gran consumo de energía, como lo hacen Wi-Fi o bluetooth, lo que nos lleva a elegir una vez más a la tecnología ZigBee.

Diseñada para el hogar

ZigBee es diferente de las otras tecnologías inalámbricas (Wi-Fi y Bluetooth), ha sido diseñada exclusivamente para soportar un diverso mercado de aplicaciones en el hogar que requieren de bajo costo y bajo consumo de energía.

Bajo Costo

Al utilizar una tecnología inalámbrica se reduce el costo de instalación y mantenimiento, no requiere de reajustes del conexionado de cables, tampoco instalaciones previas como entubado ni en la compra de fuentes de energía. Las redes inalámbricas implican un gran intercambio de información con un mínimo esfuerzo de instalación. Adicionalmente el costo de transmisores ZigBee, es bastante bajo (ver sección 3.6), con esto se puede diseñar e implementar un sistema de seguridad que seguramente sea competitivo frente a los productos de tecnologías como Konnex, Lonworks o propietarias.

Amplio rango de aplicaciones

ZigBee es una tecnología inalámbrica diseñada para automatizar el hogar, la construcción, y la industria. Los circuitos integrados ZigBee pueden automatizar el hogar incluyendo: sistemas de seguridad, sistemas de calefacción por cada habitación, controles de acceso, interruptores para luces, detectores de humo y fuego, termostatos y controles remotos para audio y video [14]. ZigBee opera a los 2.4 GHz, por lo que pertenece a la banda de frecuencias que pueden operar libremente sin ningún permiso (ver sección 3.2.1).

Posicionamiento en el mercado

Esta tecnología está imponiendo su presencia en los sectores de la industria, el hogar, la seguridad y el cuidado de la salud, lo cual es un indicador de que esta tecnología está madurando y penetrando el mercado de las redes sin cables. Además del amplio rango de aplicaciones muchos productos se incorporan desde chips y módulos la gama de productos ahora cubren alarmas, sensores, consolas y sistemas completos para diversos usos: Gestión de estacionamiento, gestión de la luz de las calles, automatización de edificios y fábricas, y cuidado de personas en hospitales [14]. En la actualidad muchos de los productos disponibles son utilizados por el sector público y para aplicaciones industriales. Los fabricantes en Korea del Sur ofrecen una gran cantidad de soluciones para la automatización de edificios y fabricas, aunque se espera que el mayor crecimiento de esta tecnología se aplique en la automatización del hogar y las redes [15].

3 ESPECIFICACIÓN ZIGBEE Y ELECCIÓN DEL MÓDULO

En el año 2002 dos grupos especialistas en estándares (ZigBee y el grupo trabajo IEEE 802) se unieron para dar a conocer la necesidad de un nuevo estándar para redes inalámbricas de bajo consumo de energía y de bajo costo para aplicaciones domóticas e industriales. Dando como resultado un nuevo estándar para áreas personales (LR-WPAN, redes inalámbricas de área personal de baja velocidad de bits) que ahora se conoce como el estándar IEEE 802.15.4. No es una tecnología, sino un conjunto estandarizado de soluciones que pueden ser implementadas por cualquier fabricante.

3.1. Tipos de dispositivos

Se definen tres tipos diferentes de dispositivos ZigBee según su papel en la red:

- **Coordinador ZigBee (ZigBee coordinator, ZC).** El tipo de dispositivo más completo. Puede actuar como director de una red en árbol así como servir de enlace a otras redes. Existe exactamente un coordinador por cada red, que es el nodo que la comienza en principio. Puede almacenar información sobre la red y actuar como su *centro de confianza* en la distribución de claves de cifrado.
- **Router ZigBee (ZR).** Además de ofrecer un nivel de aplicación para la ejecución de código de usuario, puede actuar como router interconectando dispositivos separados en la topología de la red.
- **Dispositivo final (ZigBee end device, ZED).** Posee la funcionalidad necesaria para comunicarse con su nodo padre (el coordinador o un router), 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. Un ZED tiene requerimientos [10]

En base a su funcionalidad puede plantearse una segunda clasificación:

- **FFD.** Este puede funcionar como un coordinador de red. La memoria adicional y la capacidad de computar, lo hacen ideal para hacer las funciones de Router o para ser usado en dispositivos de red que actúen de interface con los usuarios.
- **RFD.** El dispositivo de función reducida tiene funcionalidad limitadas para el bajo coste y simplicidad. Son los sensores/actuadores de la red.

3.2. Arquitectura

ZigBee es una pila de protocolos, que de manera similar al modelo OSI está constituido por diferentes capas, las cuales son independientes una de la otra. En la

Figura 3.1 se muestran las diferentes capas que conforman la pila de protocolos para ZigBee.

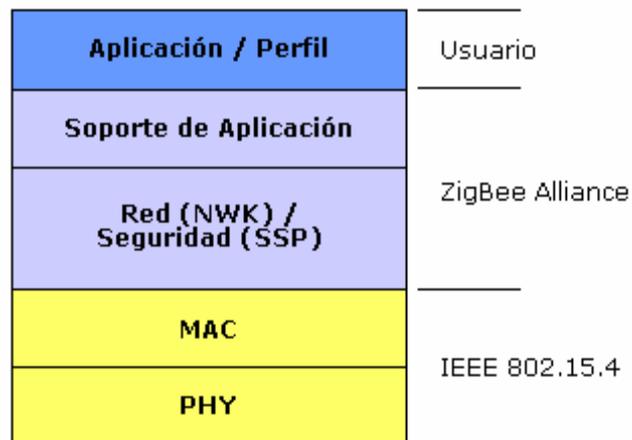


Figura 3.1 Las capas de la pila de protocolos para ZigBee

3.2.1. Capa física

Frecuencia y tasa de transmisión. El estándar IEEE 802.15.4 ofrece dos opciones de capa física: a 2.4 GHz especifica la operación en la banda Industrial, Médica y Científica (ISM), que prácticamente está disponible en todo el mundo, mientras que la capa física a 868/915 MHz, especifica la operación en la banda de 865 MHz en Europa y 915 MHz en la banda ISM en Estados Unidos. La segunda distinción es el rango de transmisión. La capa física a 2.4 GHz permite una transmisión de 250 kbps, mientras que la capa física a 868/915 MHz a 20 kbps y 40 kbps respectivamente. Este rango superior de transmisión en la capa física a 2.4 GHz se atribuye principalmente a un orden mayor en la modulación.

Canales. Se define 27 canales de frecuencia entre las tres bandas. La capa física a 868/915MHz soporta un solo canal entre los 868 y los 868.6 MHz, y diez canales entre los 902.0 y 928.0MHz. La capa física a 2.4 GHz soporta 16 canales entre los 2.4 y los 2.4835GHz con un ancho de banda de 5 MHz por canal, con el objetivo de facilitar los requerimientos de filtrado en la transmisión y en la recepción.

Sensibilidad. Las especificaciones de sensibilidad del estándar IEEE 802.15.4 detallan -85 dBm^2 para la capa física a 2.4 GHz. Naturalmente, el rango de alcance

² El dBm se define como el nivel de potencia en decibelios en relación a un nivel de referencia de 1 mW. Al utilizarse un nivel de referencia determinado (1 mW) la medida en dBm constituye una verdadera medición de la potencia y no una simple relación de potencias como en el caso de la medida en decibelios. Así, una lectura de -85 dBm significa que la potencia medida es 1.5 veces mayor que 1mW y por tanto igual a 1.5 mW.

deseado estará en función de la sensibilidad del receptor, así como de la potencia del transmisor. Los dispositivos de potencia igual a 1mW cubren un rango de entre **10-20 m**.

Interferencias. Los dispositivos que operan en la banda de 2.4 GHz pueden recibir interferencias causadas por otros servicios que operan en dicha banda. Esta situación es aceptable en las aplicaciones que utilizan el estándar IEEE 802.15.4, las cuales requieren una baja calidad de servicio (QoS), no requieren comunicación asíncrona. Distintas Pruebas han mostrado que más del 20 % de todos los paquetes ZigBee serán retransmitidos a causa de las colisiones si es que ZigBee usa un canal que traslapa un canal Wi-Fi frecuentemente usado [9].

3.2.2. Capa de enlace

La capa de enlace usa el mecanismo CSMA/CA para acceder al canal de radio frecuencia. También es responsable de la asociación/disociación, confirmación de entrega de trama (ACK), mecanismos de acceso al canal, validación de trama, control de garantía de ranuras de tiempo (Slot Time), control de guías (Beacon) y barrido de canal.

CSMA/CA. El mecanismo “Acceso Múltiple Sensible a la Portadora – Evasión de Colisión - CSMA/CA” es comúnmente utilizado para acceder a un medio físico sin cables. Antes de toda transmisión, el dispositivo tendrá que escuchar por un periodo definido para transmitir en un medio seleccionado. Si no hay transmisión alguna en progreso, empieza su propia transmisión. De otro modo este escuchará hasta que la existente transferencia termine. El propósito de este método es proveer transferencias más rápidas y confiables, inclusive si el medio esta densamente ocupado [9].

3.2.3. Capa de red

La capa de red tiene como objetivo principal permitir el correcto uso del subnivel MAC y ofrecer una interfaz adecuada para su uso por parte de la capa de aplicación. En esta capa se brindan los métodos necesarios para: iniciar la red, unirse a la red, enrutar paquetes dirigidos a otros nodos en la red, proporcionar los medios para garantizar la entrega del paquete al destinatario final, filtrar paquetes recibidos, cifrarlos y autentificarlos. Se debe tener en cuenta que el algoritmo de enrutamiento que se usa es el de *enrutamiento de malla*, el cual se basa en el protocolo *Ad Hoc On-Demand Vector Routing – AODV*. Cuando esta capa se encuentra cumpliendo la función de unir o separar dispositivos a través del controlador de red, implementa

seguridad, y encamina tramas a sus respectivos destinos; además, la capa de red del controlador de red es responsable de crear una nueva red y asignar direcciones a los dispositivos de la misma. Es en esta capa en donde se implementan las distintas topologías de red que ZigBee soporta (árbol, estrella y mesh network).

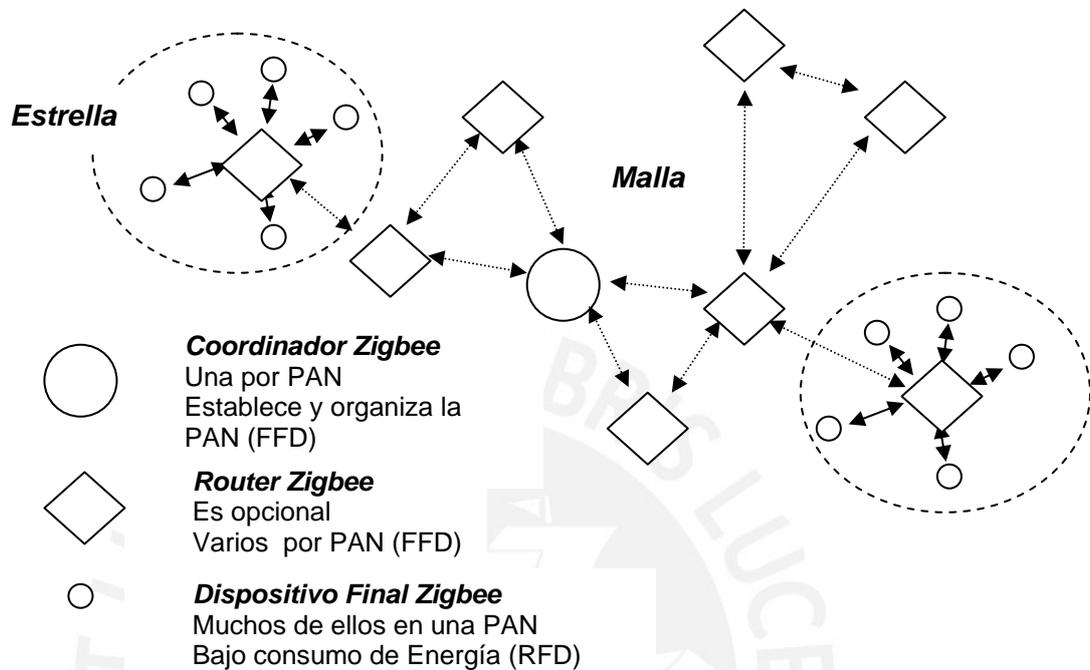


Figura 3.2 Tipo de nodos y las topologías de las redes ZigBee [9].

3.2.3.1. Topologías

En la configuración en estrella, uno de los dispositivos tipo FFD asume el rol de coordinador de red y es responsable de inicializar y mantener los dispositivos en la red. Todos los demás dispositivos ZigBee, conocidos con el nombre de dispositivos finales, ‘hablan’ directamente con el coordinador. En la configuración tipo malla, el coordinador ZigBee es responsable de inicializar la red y de elegir los parámetros de la red, pero la red puede ser ampliada a través del uso de routers ZigBee. El algoritmo de encaminamiento utiliza un protocolo de pregunta-respuesta (request-response) para eliminar las rutas que no sean óptimas, la red final puede tener hasta 254 nodos (probablemente nunca necesitamos tantos). Utilizando el direccionamiento local, tú puedes configurar una red de más de 65000 nodos [9].

3.2.4. Capa de aplicación

En el nivel conceptual más alto se encuentra la capa de aplicación que no es otra cosa que la aplicación misma y de la que se encargan los fabricantes. Es en esta capa donde se encuentran los ZDO (ZigBee Device Objects) que se encargan de

definir el papel del dispositivo en la red, si el actuará como coordinador, ruteador o dispositivo final; la subcapa APS y los objetos de aplicación definidos por cada uno de los fabricantes. Cada capa se comunica con sus capas subyacentes a través de una interfase de datos y otra de control, las capas superiores solicitan servicios a las capas inferiores, y éstas reportan sus resultados a las superiores. Además de las capas mencionadas, a la arquitectura se integran otro par de módulos: **módulo de seguridad**, que es quien provee los servicios para cifrar y autenticar los paquetes, y el **módulo de administración del dispositivo ZigBee**, que es quien se encarga de administrar los recursos de red del dispositivo local, además de proporcionar a la aplicación funciones de administración remota de red [10].

3.3. Empaquetamiento

En ZigBee, el empaquetamiento se realiza en cuatro tipos diferentes de paquetes básicos, los cuales son: datos, ACK, MAC y baliza. El paquete de datos tiene una carga de datos de hasta 104 bytes. La trama esta numerada para asegurar que todos los paquetes lleguen a su destino. Un campo nos asegura que el paquete se ha recibido sin errores. Esta estructura aumenta la fiabilidad en condiciones complicadas de transmisión [10]. La estructura de los paquetes ACK, llamada también *paquete de reconocimiento*, es dónde se realiza una realimentación desde el receptor al emisor, de esta manera se confirma que el paquete se ha recibido sin errores. Se puede incluir un *tiempo de silencio* entre tramas, para enviar un pequeño paquete después de la transmisión de cada paquete. El paquete MAC, se utiliza para el control remoto y la configuración de dispositivos/nodos. Una red centralizada utiliza este tipo de paquetes para configurar la red a distancia. El paquete baliza se encarga de “despertar” los dispositivos que “escuchan” y luego vuelven a “dormirse” si no reciben nada más. Estos paquetes son importantes para mantener todos los dispositivos y los nodos sincronizados, sin tener que gastar una gran cantidad de batería estando todo el tiempo encendidos [9].

3.4. Direccionamiento

Los dispositivos se direccionan empleando 64-bits y un direccionamiento corto opcional de 16 bits. El campo de dirección incluido en MAC puede contener información de direccionamiento de ambos orígenes y destinos (necesarios para operar punto a punto). Este doble direccionamiento es usado para prevenir un fallo dentro de la red.

3.5. Seguridad

Otro aspecto muy importante es la seguridad de las transmisiones y de los datos, los cuales son puntos clave en la tecnología ZigBee que utiliza el modelo de seguridad de la subcapa MAC IEEE 802.15.4, la cual especifica 4 servicios de seguridad:

- Control de accesos, el dispositivo mantiene una lista de dispositivos “comprobados” en la red.
- Datos encriptados, los cuales utilizan una encriptación con un código de 128 bits.
- Integración de tramas, para proteger los datos de ser modificados por otros.
- Secuencias de refresco, para comprobar que las tramas no han sido reemplazadas por otras. El controlador de red comprueba estas tramas de refresco y su valor, para ver si son las esperadas [10].

3.6. Comparación de Circuitos Integrados ZigBee: Transceptores, SOCs y SIPs³

Se debe de realizar una comparación previa de los diferentes productos que empresas de reconocido prestigio han desarrollado para la implementación de sistemas domóticos basados en tecnología ZigBee. En esta sección se compararán todas las tecnologías relacionadas a la producción de chips integrados.

3.6.1. Texas Instruments (TI)

Es uno de los productores más grandes en soluciones compatibles con ZigBee y a la fecha se conoce que TI ha desarrollado su 2da generación de soluciones ZigBee SOC lanzando al mercado 2 nuevos chips CC2520 Y CC2480A1. CC2520 es la segunda generación de los SoC ZigBee de TI, fueron lanzados en diciembre del 2007. Comparados con la generación anterior a este ofrece un mayor rango de voltajes de consumo (1.8v-3.8v), un empaque más pequeño, menor consumo de energía y un mayor rango de temperatura en operación (-40 -125° C), memoria flash

³ **SOC, System on Chip:** Se refiere a la integración de todos los componentes de un ordenador u otro sistema electrónico en un solo circuito integrado (chip). P.e. Microcontrolador, microprocesador(x86) o DSP.

SIP, System in Package: Es un número cerrado de los circuitos integrados en un solo paquete o módulo. El SIP realiza todas o la mayoría de las funciones de un sistema electrónico, y se utilizan normalmente dentro de un teléfono móvil, reproductor de música digital, etc

Transceptor: un dispositivo que realiza, dentro de un mismo empaquetado o chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones.

de hasta 728KB y un mayor alcance en la transmisión de datos. La radio sigue siendo el CC2420, pero con esta es compatible con la plataforma IEEE 802.15.1-2006. También la unidad de procesamiento es un bloque especial en lugar del núcleo 8051. No presenta una memoria programable. Toda la computación personalizada tiene que ser hecha en un procesador externo en comunicación con el CC2520 vía la interfaz SPI. Hasta el momento el CC2520 supera a otras radios en términos de sensibilidad y desempeño RF. El precio de este chip es de \$3.10 en cantidades de 100 unidades. Los kits de desarrollo están disponibles por \$649. No existen módulos que usen el CC2520 [16].

3.6.2. Freescle

Freescle tiene tranceptores (MC1319-MC1320) y SIPs (MC1321) en su portafolio de soluciones ZigBee. La primera familia de Freescle provee tranceptores compatibles totalmente con la IEEE 802.15.1, están diseñados para trabajar con la familia de microcontroladores HCS08, pero cualquier procesador con 4 líneas SPI puede ser conectado sin problema. El MC13191 fue creado para aplicaciones propietarias en la banda de 2.4GHZ. El MC13192 es un tranceptor compatible con el estándar IEEE802.15.4, el cual también puede ser usado para aplicaciones ZigBee con un microcontrolador externo y una pila ZigBee. El MC 13193 es un tranceptor para aplicaciones ZigBee que contienen la pila ZigBee Figure 8 Z-stack. La segunda generación fue lanzada en el 2006. Tiene mejores características que la primera generación que se reflejan en el tamaño del producto final (transmisión integrada, switch de recepción). Los kits de desarrollo están disponibles por \$399. Todos ellos vienen en empaquetados QFN. Los costos por compras mayores a 1000 unidades son:

MC13191: \$1.95 , MC13192: \$2.32, MC13193: \$2.80 (más el costo de licencia de la pila *ZigBee Figure 8*). Maxstream utilizaba estos chips de freescle para su producto: XBee Series 1 [17].

Familia de SIPs. Estos integrados llegan al mercado a principios del 2006 y sus capacidades son comparables al CC2430. Ellos presentan un microcontrolador de la familia HCS08 integrados con hasta 60KB de memoria flash y 4KB de memoria RAM. Debido a su memoria Flash los chips MC13212 y MC13211 si son capaces de funcionar con la pila ZigBee, por lo tanto son adecuadas para aplicaciones ZigBee sin un microcontrolador externo. La diferencia entre el MC13213 y el MC13214 está en el software que usan. El MC13213 fue creado para usar el BeeStack de Freescle mientras que el MC13214 incluye la pila de Figure 8 Z-Stack. Sin embargo ninguno de

esas dos pilas (stacks) está disponible gratis. Los kits de desarrollo están disponibles por \$349.

3.6.3. Ember

El portafolio de Ember es más pequeño que el de Freescale o el TI. Solo tienen 2 productos referidos a ZigBee y son EM250SoC y el EM260 Co-Processor.

Em250 SOC. Contiene un procesador XAP2b (recomendado por consultores de Cambridge) con una memoria flash de 120KB y 5KB de RAM, ofrece hasta un consumo de 1uA durante el modo dormir. Sin embargo las corrientes de transmisión y recepción son ligeramente superiores que las de Freescale y TI. Su especial característica es la mejora en el poder de transmisión pero con un mayor consumo de energía. Por defecto, está cargado con la pila ZigBee EmberZnet. Un solo Chip con empaquetado QFN cuesta alrededor de \$7.41 por cantidades de 2000 unidades como mínimo. Un impresionante kit de desarrollo que contiene entrenamiento y software profesional está disponible por \$10000. Un simple kit con 3 tarjetas con accesorios está disponible por \$2500. Un kit de desarrollo más pequeño de 2 tarjetas está disponible por \$500. Digi (ex Maxstream) está usando estos chips en su producto XBee Series 2 [18].

Em 260 Co Processor. Es un dispositivo que permite la separación del hardware de la aplicación del fabricante final y la pila EmberZNet ZigBee. El EM260 maneja el procesamiento de la pila y otro microcontrolador puede ser usado completamente para la aplicación. Un chip empaquetado QFN cuesta \$ 5.82 en cantidades mayores de 3500.

3.6.4. Microchip

Microchip produce solamente un solo transceptor en el 2003, el MRF24J40, este tiene un menor consumo en el modo dormir igual a 0.2uA (menor a Freescale y TI). Adicionalmente el consumo de corrientes de transmisión y recepción son menores. Esto es debido a que el microcontrolador es utilizado a 20 MHz.

El costo de un chip empaquetado QFN es de \$2.52 en cantidades de 1000. Los Kits de desarrollo están disponibles por \$300 [19].

3.6.5. Atmel

Atmel ofrece dos generaciones de transceptores RF para aplicaciones ZigBee y IEEE 802.15.4. Ambas son solo transceptores, por lo que requieren un microcontrolador

externo con la pila ZigBee conectado vía 4 hilos de comunicación SPI. Su segunda generación AT86RF231 consume tan solo 0.02uA en su modo dormir y 0.4mA cuando la radio está apagada. Tiene mejor sensibilidad que la mayoría de los chips industriales. Atmel también ofrece una “mezcla” que contiene un microcontrolador y una de sus radios. Su primera generación AT86RF230 viene en paquetes QFN y cuesta \$4.53 por un único chip en cantidades de 100 unidades. Dependiendo de un tipo de “mezcla” el rango de costo está entre los \$12 y \$24. Los Kits de demostración están disponibles por \$500 [20].

3.6.6. Módulos

Los Módulos son dispositivos basados en los SoC, SiP, o transceptores y microcontroladores. Son pequeños circuitos integrados con una interna GPIO (entradas y salidas de propósito general) e interfaces de comunicación accesibles por sus pines externos. Son usados para comunicaciones USART, pero alguno de ellos se usa para comunicaciones I2C o SPI. Estos vienen con un firmware en la memoria flash y los componentes internos no pueden ser reprogramados con un firmware personalizado ni se puede tener acceso a ellos.

3.6.7. Radiocrafts

Ofrecen dos series de módulos ZigBee. Los RC220x basados en el CC2420 de TI y con un microcontrolador de Atmel. Los RC230x, basados en el CC2430/CC2431 con un microcontrolador 8051. Su principal ventaja es el número de GPIO (Entradas y Salidas de propósito general). El consumo de corriente, tamaño, sensibilidad y rango, tienen un valor promedio en comparación.

3.6.8. Meshnetics

Un producto especial de Meshnetics es el ZigBit Amp Module. Usando su potencia de salida más alta es posible de alcanzar un rango excepcional de 4Km. Sus módulos estándar tienen una mejor sensibilidad, rango y dimensiones físicas que el resto de módulos mencionados en esta tesis pero por el contrario tienen un mayor consumo de energía mientras están despiertos [21].

3.6.9. RFM (Cirronet)

Los módulos de Cirronet ahora están fabricados bajo la marca RFM. Existen 2 familias de estos módulos, cada familia ofrece 3 versiones diferentes en poder de transmisión. Las versiones más potentes vienen con una antena integrada a la tarjeta. Estos módulos son diferentes a los demás pues requieren ser alimentados con 5

voltios y no con 3. Las demás características y parámetros están dentro del promedio. Una desventaja en las versiones de baja potencia puede ser la ausencia de la antena en la tarjeta de los módulos.

3.6.10. Jennic

Jennic también presenta 2 familias de módulos en su portafolio. El más antiguo JN5121 es superado ampliamente por su sucesor el JN5139. El JN5139 ofrece 3 tipos de antenas, cerámica, SMA y uFI. Comparado con otros módulos estos ofrecen más periféricos y mejor sensibilidad. Una desventaja es el consumo de corriente y el tamaño del módulo [22].

3.6.11. Digi (ex Maxstream)

Provee 2 familias de sus XBee módulos, ambos vienen en versiones estándar y mejorados (PRO). La primera generación, con un chip integrado de freescale es solamente compatible con el 802.15.4, mientras que el segundo (XBee Series 2) presenta la pila ZigBee, está certificada por la alianza ZigBee y está basada en la solución de Ember EM250. Este es el único módulo que viene en un empaquetado con pins. Sus parámetros o características no son excepcionales sin embargo es el más barato de todos los módulos mencionados en esta tesis [23].

3.7. Ventajas de los módulos

Existen muchos fabricantes de módulos, quienes incorporan chipsets compatibles con ZigBee, y con cualquier solución la transmisión por RF ya esta lista frecuentemente con optimizaciones por un tipo en particular de aplicación y típicamente incluyen las certificaciones FCC⁴ y ETSI como módulos RF. Quizás no se encuentre un módulo que soporte la aplicación del sistema de seguridad en particular, sin embargo si se puede encontrar un módulo que se **adapte al diseño del sistema** de modo que se ahorraría en el costo de desarrollo e implementación.

3.7.1. Implementación de los perfiles

El chipset y la pila de protocolo ZigBee están incompletas sin un “Perfil”, el cual define la aplicación que se le dará al circuito integrado y al firmware que incorpora. Existen perfiles públicos y privados: en los perfiles públicos, el logo de Certificación ZigBee

⁴ FCC: La **Comisión Federal de las Comunicaciones** (*Federal Communications Commission*) se encarga de la elaboración de normativas de Compatibilidad electromagnética, en lo que se refiere a productos electrónicos para el consumidor; es muy habitual ver en etiquetas, placas o manuales de muchos aparatos eléctricos de todo el mundo el símbolo de la FCC y la Declaración de Conformidad del fabricante hacia sus especificaciones.

está disponible, en el caso de los perfiles privados estos no pretenden ser interoperables y por esa razón no pueden ser certificados. A la fecha, solamente existe un solo perfil público ZigBee de “Iluminación”. Si se pretende desarrollar alguna solución ZigBee para alguna otra aplicación, necesariamente se tiene que utilizar algún perfil privado.

3.7.2. Conclusión y elección

Como se ha explicado en la sección anterior es bastante complicado desarrollar e implementar un perfil ZigBee privado para nuestra aplicación específica, no contamos con una licencia para el desarrollo de herramientas por parte de proveedores de la pila del protocolo ZigBee ni tampoco con el conocimiento específico para el desarrollo del Firmware ZigBee. Sin embargo, como es propuesto, podemos elegir un módulo que ya cuenta con un perfil privado de propósito general y que se adapte a nuestra aplicación específica.

Los módulos XBee Series 2 (Znet 2.5) fueron elegidos como la plataforma inalámbrica para el sistema inalámbrico de seguridad de esta tesis. Inicialmente los SoC de TI o la solución de Atmel eran consideradas posibles, pero al final el tiempo requerido para desarrollar e implementar una solución con un SoC es muy larga para el tiempo de elaboración de esta tesis, por lo que se decidió preferir a los módulos listos para usar. De acuerdo a los parámetros quizás los módulos XBee no logren el mayor desempeño, pero por su bajo precio a comparación de los otros módulos, su pequeño empaquetado, su perfil multipropósito UART y su rápida compra vía Internet hacen que esta sea la plataforma final para esta tesis.

3.8. Módulo Xbee Series 2 [24]

A continuación se detallaran aspectos y características esenciales de estos módulos que nos permitirán desarrollar una red de sensores inalámbricos que monitoreen los nodos de un sistema de seguridad para departamentos, que cumplan con los requisitos de bajo consumo de energía, amplio rango de operación, fácil implementación y sobretodo bajo costo.



Figura 3.3 XBee Series 2

Comunicación serial. Estos módulos se presentan como una interesante y atractiva alternativa, acortando el tiempo de desarrollo en la implementación de un perfil ZigBee. Este módulo posee un perfil privado que realiza una interfaz hacia un host a través de un puerto serial. Por medio de este puerto serial el módulo puede comunicarse con cualquier dispositivo que contenga el protocolo UART que sea compatible en lógica y voltaje.

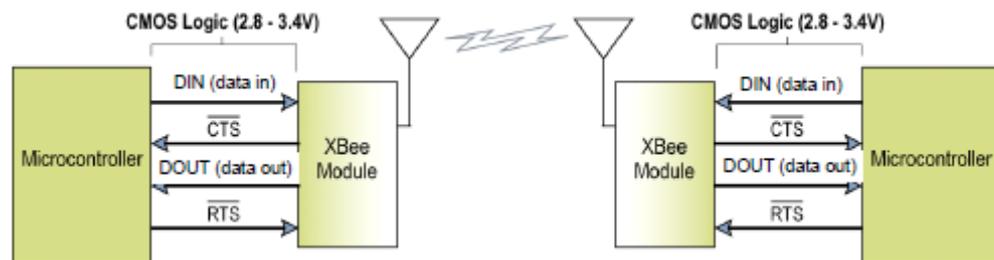


Figura 3.4 Diagrama del flujo del sistema de datos en un entorno de interfaz UART (señales que se activan en baja son distinguidas con una línea horizontal sobre el nombre.) [24].

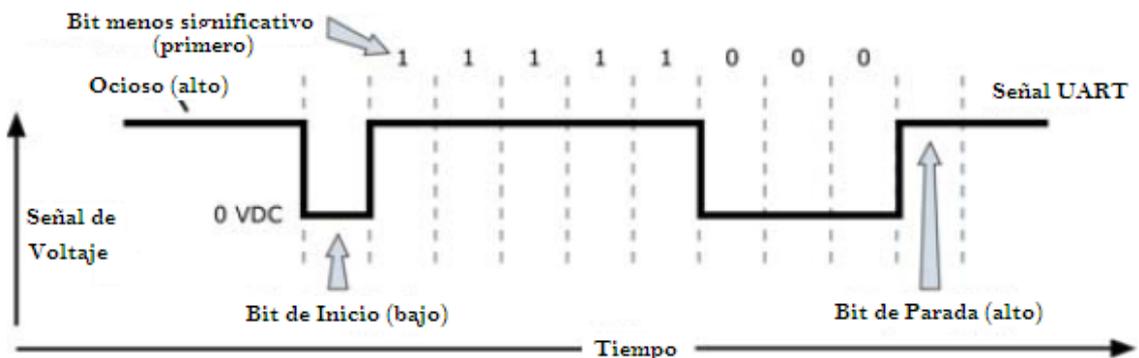


Figura 3.5 Paquete de datos UART = 0x1f (31 en decimal) transmitido a través del módulo XBee. Formato de datos: 8-n-1 (bits- paridad-#de bits de parada) [24].

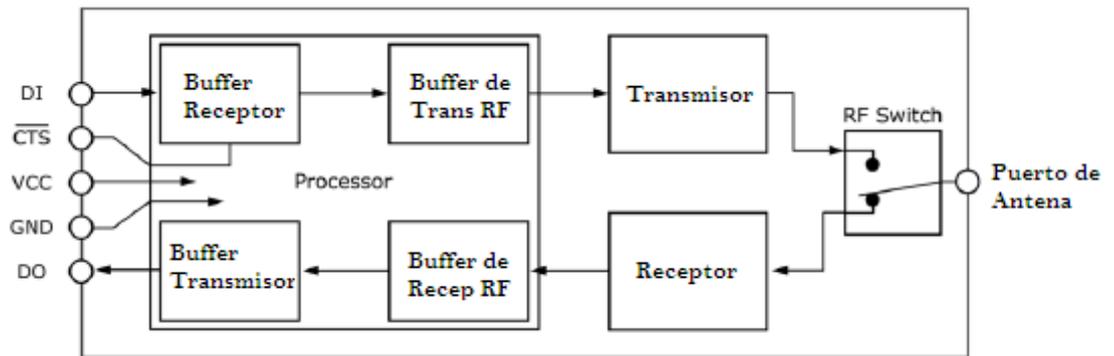


Figura 3.6 Diagrama del flujo interno de datos [24].

Protocolos de interface serial. Los módulos Xbee soportan las interfaces seriales *transparente* y *API* (Interfaz de programación de aplicaciones).

Operación transparente. Los módulos RF que contengan las siguientes versiones de firmware soportarán el modo transparente: 1.0xx (coordinador) y 1.2xx (router/dispositivo final). Al operar en modo transparente, *los módulos están configurados utilizando comandos AT* mientras que la operación API no es compatible en modo transparente. Los módulos actúan como una línea en serie de sustitución de cable, todos los datos UART recibidos a través del pin3 DIN se mantiene en cola de transmisión RF. Los datos se envían a un módulo, tal como se define por configuraciones previas de los parámetros: DH (Dirección Alta de destino) y DL (Dirección baja de destino). Cuando los datos de RF son recibidos por un módulo, los datos se envían por el pin DOUT.

Operación API. La Operación API (Application Programming Interface) es una alternativa a la operación transparente por defecto. La trama basada en operación API se extiende hacia un nivel en la cual una aplicación de host puede interactuar con las capacidades de red del módulo XBee. API provee medios alternativos para configurar al modulo y rutear datos hacia la capa de aplicación del host. La aplicación del host puede enviar trama de datos al modulo que contengan direcciones y otra información, en vez de usar el modo comando para modificar las direcciones. El modulo enviara la trama de datos hacia la aplicación del módulo conteniendo los paquetes de estado y diversa información de paquetes de datos recibidos.

La operación API facilita muchas operaciones, por ejemplo:

- Transmite datos hacia múltiples destinos sin tener que ingresar al modo comando.
- Recibe estados falla/éxito de los paquetes RF recibidos.
- Identifica la dirección de cada paquete recibido.

Modos de Operación. En esta sección se explicarán los diversos modos de operación del XBee que permiten la configuración de parámetros, el ahorro de energía y la comunicación entre dispositivos XBee.

Modo Comando. Para configurar, modificar o leer los parámetros del módulo XBee, primero se deberá ingresar al “modo de comando”, este es un estado en donde los caracteres seriales recibidos son interpretados como comandos. Una forma de configurar estos módulos son mediante el modo de comandos AT. A este modo se ingresa enviando al puerto serial del módulo los caracteres “+++”, este módulo responderá con los caracteres ASCII la palabra “OK”, lo cual quiere decir que ha ingresado exitosamente a este modo AT y está listo para ser configurado. Si la ejecución de algún comando AT resulta en error el módulo responderá con la palabra “ERROR”. Para salir del modo comando hay que escribir “CN” (enviar una cadena de caracteres al XBee).

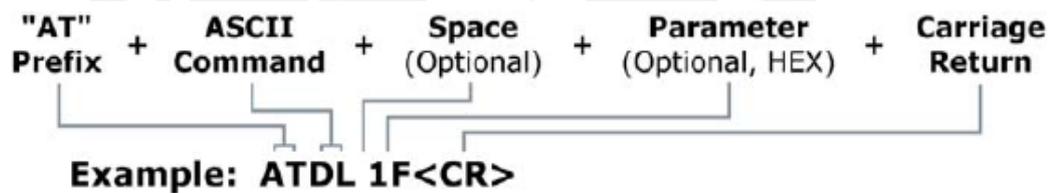


Figura 3.7 Sintaxis de los comandos AT

En la figura anterior se muestra la sintaxis de un comando AT, luego de ingresar a este modo se debe ingresar el comando deseado para ajustar los parámetros del módulo XBee, para mayores detalles de la configuración del XBee en modo comando ver el manual descargable desde: www.digi.com.

Modo Ocioso. Cuando no está transmitiendo ni recibiendo información, el módulo XBee está en este modo. El módulo se mantiene verificando si existen datos RF válidos que recibe. El módulo cambia de modo bajo las siguientes condiciones:

Modo transmisión. Los datos seriales, en el buffer de recepción serial, están listos para ser “paquetizados”.

Modo recepción. Cualquier data RF válida es recibida a través de la antena.

Modo dormir. Un comando los activa. Solo para dispositivos finales.

Modo comando. Cuando una secuencia de comandos es transmitida.

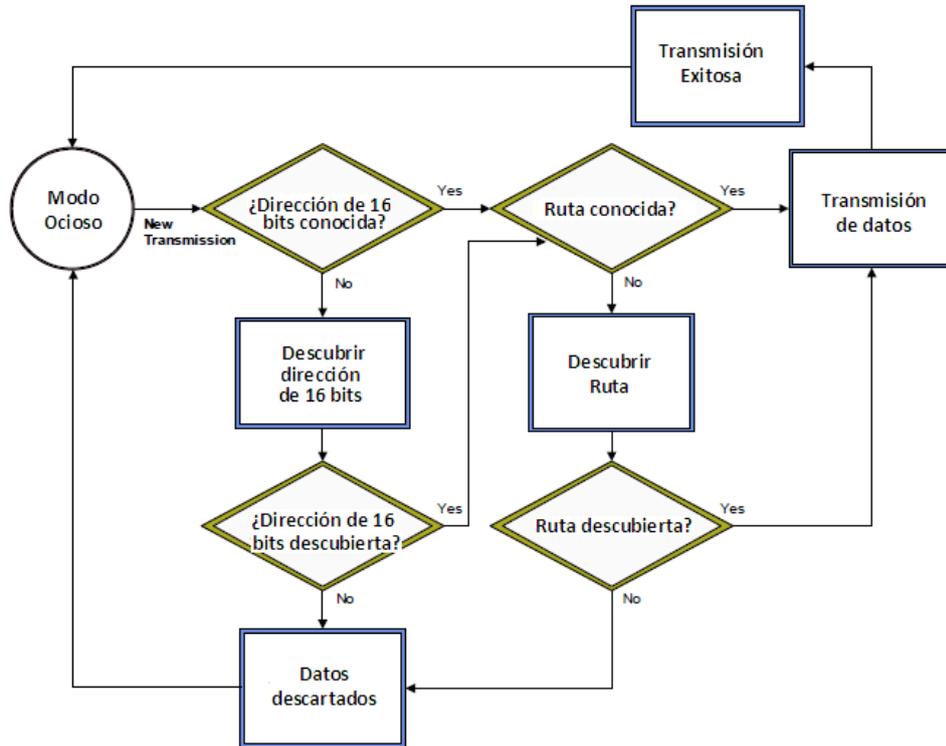


Figura 3.8 Secuencia del modo de transmisión

Versiones de hardware: Estándar y Pro.

ESPECIFICACIÓN	XBEE SERIES 2	XBEE PRO SERIES 2
Desempeño		
Rango en el interior	Hasta 40m	Hasta 100m
Rango en el exterior(con línea de vista)	Hasta 120m	Hasta 1.6Km
Potencia de transmisión	2mW (+3dBm) 1.25mW (+1dBm)	63mW (+18 dBm) 10mW (+10 dBm)
Tasa de transmisión	250Kbps	250Kbps
Sensibilidad de Recepción	-96dBm	-102dBm
Requerimientos de energía		
Voltaje de alimentación	2.1-3.6 V	3.0-3.4 V
Corriente de operación en la transmisión	40mA 35mA	295mA
Corriente de operación en la recepción	40mA 35mA	45mA
Corriente de operación en estado ocioso	15mA	15mA
Corriente en modo dormido	1uA	1uA
General		

Banda de frecuencia	ISM 2.4GHZ	ISM 2.4GHZ
Dimensiones	0.960" x 1.087" (2.438cm x 2.761cm)	0.960 x 1.297 (2.438cm x 3.294cm)
Topologías	Punto a Punto, Punto-Multipunto y Malla.	Punto a Punto, Punto-Multipunto y Malla.
Número de canales	16 Direct Sequence Channels	13 Direct Sequence Channels

Rango de alcance. El módulo representa una potencia de transmisión de unos 2mW (+3dB) y la sensibilidad del receptor es de -95dBm (con un porcentaje de error del 1%) esto le permite alcanzar distancias en un rango de 30 metros dentro de un inmueble y hasta 120 metros en espacios abiertos. La corriente de operación de estos dispositivos es de los 40mA a 3.3v, tanto para transmisión como para recepción, mientras que en el modo de bajo consumo (modo dormido) se reduce a tan sólo 1uA. El voltaje de operación es de 2.8v a 3,3v.

Antenas. Las opciones de antena son: antena chip integrada en el módulo (chip) y antena de cuarto de onda en el módulo (whip). Una antena externa también puede ser instalada. Existen dos modelos de antenas con conector U.FL (usado por ejemplo Wi-Fi Mini PCI cards) y RP(reversed-polarity) SMA (comúnmente usadas en Wi-Fi). Las siguientes antenas han sido testeadas y aprobadas para el uso con el módulo XBee ZNet 2.5 RF:

- Monopolo Whip Antenna (1.5 dBi)
- Antena chip integrada en el módulo (-1.5 dBi)
- Dipolo (2.1 dBi, Omni-directional, Articulated RS-MA, Digi part number A24-HABSM)

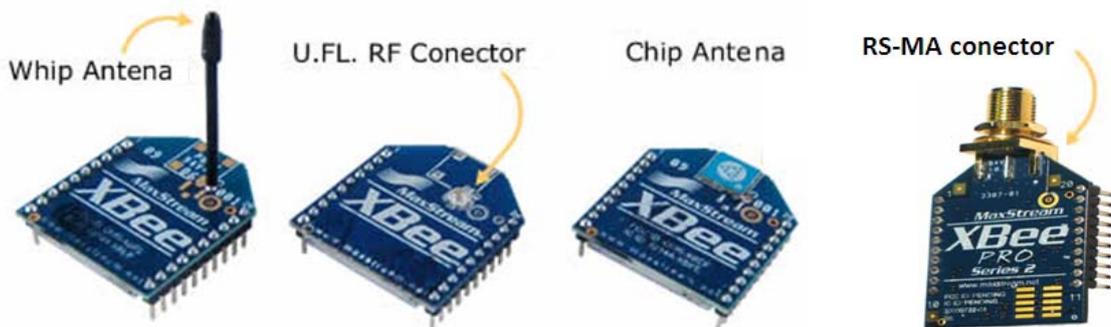


Figura 3.9 Opciones de antena en los módulos Xbee

3.8.1.1. Dimensiones

El diseño exterior está basado en un formato de 2.4cm x 2.7 cm, la conexión a al circuito impreso se realiza mediante dos conectores de 10 pines separados 2mm entre sí.

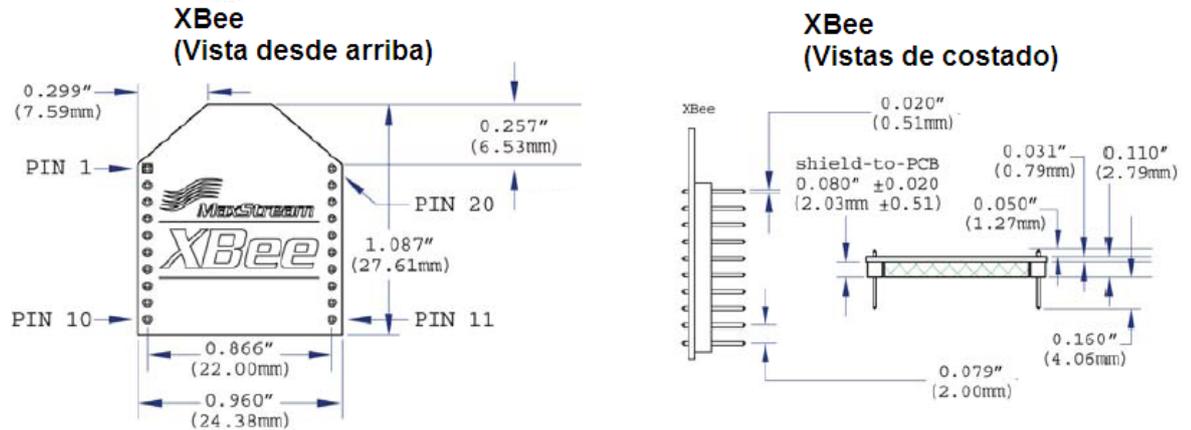


Figura 3.10 Dibujos mecánicos de los módulos OEM⁵ Xbee series 2 (Opciones de antena no especificados) [24].

3.8.2. Formación de una red ZigBee

Para crear una red ZigBee, el coordinador debe empezar en un **canal** y una dirección de su red (**PAN ID**). Una vez que los coordinadores han empezado, routers y dispositivos finales pueden asociarse a la red. Los routers y coordinadores pueden soportar hasta 8 “hijos” cada uno. La formación de esta red está gobernada por el modo de comandos AT: SC (escaneo de canales), ID (asignación de dirección de PAN), SD (duración de escaneo) y NJ (tiempo de asociación).

Coordinador. Para crear la red ZigBee (PAN), el coordinador debe de establecer un canal y obtener una dirección conocida como “Pan ID”. Una vez que el coordinador ha empezado la red, los dispositivos finales y routers pueden asociarse a la red. La formación de una red está gobernada por los comandos que controlan el proceso de seleccionar el canal y la dirección de PAN, estos son: SC (Escaneo de canales), ID (asignación de Pan ID), SD (duración del escaneo) y NJ (tiempo de asociación) que se han programado y establecido mediante el programa X-CTU. Los ajustes de SC y ID deben ser escritos usando el comando WR para preservar la formación de la red y la información de las asociaciones. Si el Xbee coordinador aun no ha seleccionado

⁵ OEM (abreviatura del inglés *Original Equipment Manufacturer*, en español sería Fabricante de Equipos Originales [F.E.O.]). Empresas o personas que adquieren dispositivos al por mayor para ensamblar computadoras o equipos de forma personalizada que presentan con su propio nombre. También se le llama al hardware que es nuevo pero ha sido sacado de su envase original para ser expuesto en stands de venta

una PAN ID o un Canal, este utilizará los comandos ID, SC u SD para realizar un escaneo de energía y un escaneo de PAN. Luego de haber completado estos escaneos, el coordinador selecciona un canal de operación y un PAN ID válidos e inicializa la PAN. Una vez que el coordinador ha seleccionado un canal y PAN ID, este mantendrá la información del canal y del PAN ID aunque haya reinicios ciclos de bajo consumo de energía.

Router/Dispositivo Final. Primero localiza al coordinador e intenta asociarse al él. Si un dispositivo final o router no se ha asociado a un red ZigBee de seguridad, este realiza un escaneo de PANs en cada canal SC en búsqueda del coordinador que opera un con una válida PAN ID. SI el ID = 0xFFFF cualquier PAN ID es considerada válida. Para otros valores de ID, el dispositivo final solo se asociará a la red que contenga la misma PAN ID preseleccionada. Los routers y dispositivos finales continúan escaneando los canales SC hasta descubrir al coordinador para asociarse.

3.8.3. El Firmware AT

El firmware AT opera de manera similar como en los módems. Ofrece algunas desventajas con respecto al firmware API, pero a cambio de sencillez al comunicarse. Básicamente los datos enviados por UART son paquetizados y enviados vía radio y viceversa. El XBee actúa como un reemplazo de cable serial.

La comunicación entre módulos XBee siempre será dirigida hacia un solo dispositivo o hacia todos (broadcast). Si se desea comunicar con más de uno, pero no de manera broadcast, se debe ingresar al modo comando, en donde funcionan los comandos AT, y es esperar 2 segundos de inactividad, cambiar de dirección de destino y empezar recién la comunicación [25].

4 DISEÑO DEL SISTEMA DE SEGURIDAD CONTRA INTRUSIÓN

El primer paso para lograr el diseño del sistema de seguridad será definir la residencia en donde se instalará, conocer las medidas de las habitaciones del departamento y localizar las áreas de mayor acceso exterior (áreas inseguras). En el presente capítulo se presentará en forma detallada el diseño y la elección de los componentes físicos (dispositivos electrónicos) y lógicos (firmware y software) de cada uno de los módulos que conforma el sistema de seguridad en un departamento.

4.1. Definición del edificio y departamento

A continuación se detallan características del edificio y el departamento que se han elegido para el diseño del sistema de seguridad. Se tomarán mediciones del área del departamento, área de cobertura de la señal, se identificarán las áreas o zonas inseguras del departamento así como las medidas del grosor de las paredes. De acuerdo a ellos y mediante las pruebas se logrará concluir si el sistema de seguridad puede implementarse en el departamento elegido.

4.1.1. Características del edificio

Se define el tamaño de la residencia en donde se instalará el sistema de seguridad, para ello se cuenta con planos de departamentos ubicados en Lima, estos están disponibles gratuitamente en Internet.

Desde el sitio en Internet www.habitat.com.pe se descarga el plano de un edificio de departamentos ubicado en la calle Elías Aguirre – Miraflores, sus características son las siguientes:

- *Área total= 560m²*
- *Altura por piso= 2.4 m*
- *Altura Total = 18 m*
- *Estacionamientos: Sótano y Primer Piso*
- *Lobby, cuarto de mantenimiento y cuarto de seguridad: Primer Piso*
- *Departamentos: Desde el segundo piso al séptimo, con cuatro departamentos por piso.*

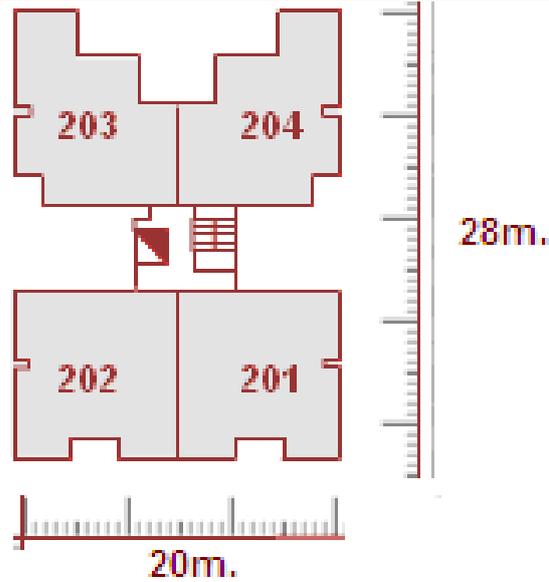


Figura 4.1 Medidas del edificio



Figura 4.2 Vista de frente del edificio

4.1.2. Características del departamento

Para realizar el diseño del sistema de seguridad primero se deberá elegir el departamento en donde será instalado, por eso elegimos aleatoriamente el departamento número 201 ubicado en la parte frontal del edificio.

MEDIDAS:

❖ Área ocupada = 99.35m²

- Sala Comedor = 28m²
- Cocina = 8 m²
- Lavanderia = 6.5 m²
- Cuarto de Servicio y baño = 8 m²
- Dormitorio Principal = 14 m²
- Dormitorio 2 = 12 m²
- Dormitorio 3 = 12 m²
- Baño 1 = 4 m²
- Baño 2 = 4 m²
- Balcón = 5 m²

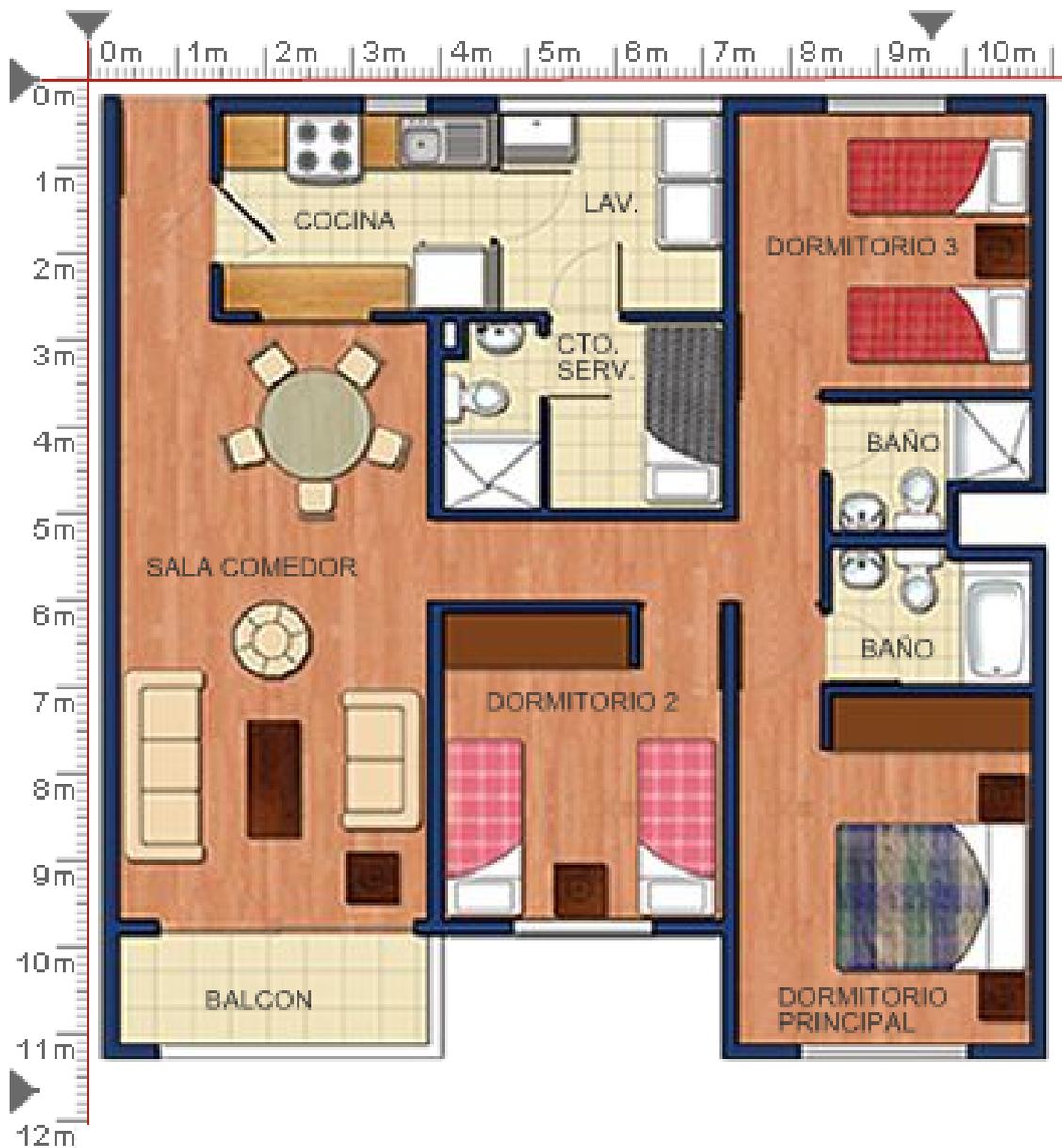


Figura 4.3 Plano arquitectónico del departamento 201

4.1.2.1. Áreas Inseguras

Para ubicar a los módulos de monitoreo primero se deben de reconocer las áreas inseguras y además definir a los dispositivos que realizarán el monitoreo o supervisión. En esta sección se reconocen las áreas potencialmente inseguras para el departamento 201.

Dormitorio principal y dormitorio 2. Estas áreas del departamento son potencialmente inseguras ya que tienen ventanas con vista a la calle.

La ventana tiene un pestillo asegurador, por lo que se considera que el dispositivo electrónico que monitoreará la intrusión por dicha ventana será un sensor de rotura del vidrio verificando la frecuencia de vibración del vidrio.

Dormitorio 3. Esta área del departamento también es potencialmente insegura debido a la ventana que posee con vista al tragaluz. Quizás esta área no es tan insegura para el 3er piso o superiores, pero es una ventana de fácil alcance en el departamento del 2do piso. De la misma manera se considera que el dispositivo electrónico que monitoreará la intrusión por dicha ventana será un sensor de rotura del vidrio.

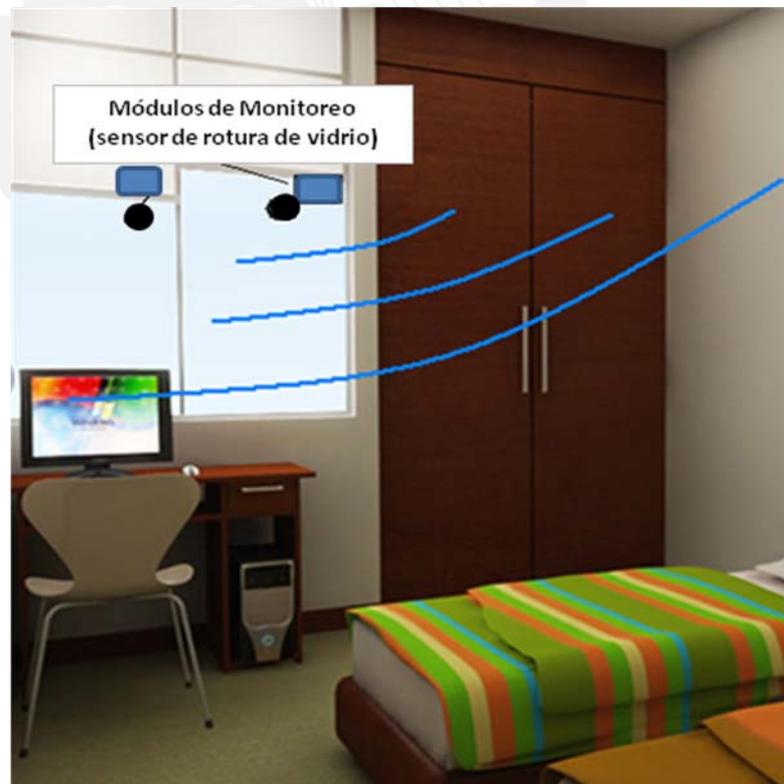


Figura 4.4 Ubicación del módulo de monitoreo en el dormitorio 3.



Figura 4.5 Instalación de un sensor de rotura de vidrio.

Sala comedor. Aquí se encuentra la puerta de ingreso y es necesaria la supervisión por medio de un contacto magnético.



Figura 4.6 Ubicación del módulo de monitoreo en la sala.

Balcón. El ingreso o salida al balcón se realiza a través de una mampara de vidrio, de la misma forma que las ventanas, se deberá de monitorear la mampara con un sensor de rotura del vidrio.



Figura 4.7 Ubicación del módulo de monitoreo en la mampara del balcón

4.2. Funcionamiento del sistema

Encendido del sistema de seguridad

1. Se pulsa el botón rojo en el módulo control remoto y este emite la señal *encender* hacia el módulo coordinador.
2. El módulo coordinador por medio del XBee receptiona la señal y la envía al microcontrolador conectado a él.
3. El microcontrolador reconoce la señal y ante cualquier intrusión, detectada por los módulos de monitoreo, activará la alarma que lleva conectado.

Apagado del sistema de seguridad

1. Se pulsa el botón verde en el módulo control remoto y este emite la señal *apagar* hacia el módulo coordinador.
2. El módulo coordinador por medio del XBee receptiona la señal y la envía al microcontrolador.
3. El microcontrolador reconoce la señal y no activará la alarma cuando los módulos de monitoreo envíen por ejemplo señales de apertura de puerta.



Figura 4.8 Interacción entre el módulo control remoto y el módulo coordinador para el encendido y apagado del sistema de seguridad

Activación de la alarma del sistema de seguridad

1. El sensor del módulo de monitoreo se activa cuando detecta alguna intrusión, esta puede ser causada, por ejemplo, por la apertura de una puerta, rotura de vidrio, sensor de presencia, etc.
2. El microcontrolador se despierta del modo de ahorro de energía, después despierta al XBee y envía la señal de alerta hacia el módulo coordinador.
3. El XBee del módulo coordinador receptiona la señal y la envía hacia el microcontrolador conectado a él.
4. El microcontrolador se encarga de activar la alarma en caso de que previamente haya sido presionado el pulsador *encender* en el control remoto.



Figura 4.9 Interacción entre el módulo de monitoreo y el módulo coordinador para el envío de la señal de alerta

5. Si el módulo coordinador recibe la señal de alerta y además se ha presionado previamente el pulsador encender, el módulo coordinador enviará una señal de alerta al módulo de aviso (ubicado en el cuarto de seguridad del edificio) 5 segundos más tarde. El retardo de 5 segundos sirve para que el usuario desactive la alarma en caso de una falsa alarma, de esa manera se evita que el coordinador envíe la alerta hacia el personal de seguridad de seguridad.
6. El XBee del módulo de aviso recepcionará la señal alerta y la enviará hacia el microcontrolador quien a su vez activará la alarma, esta vez para alertar al personal de seguridad del edificio.



Figura 4.10 Interacción entre el módulo coordinador y el módulo de aviso para el envío de la señal de alerta

4.3. Diseño físico de los módulos

Módulo XBee series 2

El módulo de radiofrecuencia XBee Series 2 funciona dentro de las especificaciones del protocolo ZigBee y sus principales características son: bajo consumo de energía para redes de sensores inalámbricos, confiabilidad y bajo costo. Está compuesto por el circuito integrado EM250 de la marca *Ember*, la pila del protocolo ZigBee es la EmberZNet 2.5.x y las transmisiones operan en la banda de los 2.4Ghz [24].

Microcontrolador

El microcontrolador se encarga de procesar todos los mensajes que recibe del XBee, de acuerdo a este procesamiento el microcontrolador gobierna la activación de la alarma o la transmisión de datos hacia el módulo de aviso. Para realizar dichas funciones se elige un microcontrolador de propósito general de muy bajo consumo de energía. En el Capítulo 5 de pruebas se utiliza el AT-mega8 de la marca Atmel pero para la implementación real de este producto se deberá de utilizar un microcontrolador específico de bajo consumo: AT-mega88P. Este microcontrolador es

de 8 bits y tiene una memoria Flash de 8Kbytes suficientes para escribir el código fuente del programa del sistema de seguridad, además posee 23 puertos de entrada/salida y el protocolo de comunicación serial UART para comunicarse con el XBee [26].

4.3.1. MÓDULO COORDINADOR

El módulo coordinador contiene los siguientes dispositivos electrónicos:

Un microcontrolador ATmega88P

Un módulo XBee PRO⁶ Series 2

Una fuente regulada de voltaje con cargador de batería

Una alarma

4.3.1.1. Ubicación

El módulo coordinador deberá ser ubicado en el lugar más céntrico de la vivienda⁷.

4.3.1.2. Funcionamiento

Este módulo contiene al módulo XBee que construye toda la red de seguridad del departamento. Sus funciones son: recibir el mensaje de *encendido* y *apagado* desde el módulo control remoto (ver Figura 4.8) recibir todos los mensajes de *alerta* de los módulos de monitoreo (ver Figura 4.9) y activar la alarma en el dormitorio principal, de esa forma alerta a los dueños de casa. Cinco segundos más tarde de haber recibido la señal de *alerta*, este módulo coordinador envía el mensaje de *alerta* al módulo de aviso que está ubicado en la zona común del edificio.

El módulo coordinador recibe la señal de alerta de los módulos de monitoreo todo el tiempo, esté o no activado el sistema de seguridad por el usuario. El módulo coordinador activa la alarma siempre que el sistema este activado (con el botón encendido del control remoto).

4.3.1.3. Fuente de Alimentación

Por considerarse el elemento más importante en la red de seguridad, el coordinador necesitará de energía eléctrica continua y regulada con respaldo de baterías y autonomía de al menos 1 hora en caso de cortes de energía comercial.

⁶ La elección del XBee Series 2 tipo PRO es opcional, para un radio de cobertura de 9 metros el sistema de seguridad puede funcionar con normalidad con un XBee Series 2 convencional. Esto según las pruebas realizadas descritas en el capítulo 5.

⁷ Para información de los rangos de alcance del sistema ver la sección 5.

En la siguiente tabla se muestra la máxima potencia consumida por el módulo coordinador, esta es calculada como resultado del consumo máximo de corriente por dispositivo.

ELEMENTO	VOLTAJE (V)	CORRIENTES (mA)	POTENCIA (mW)
XBEE PRO S2: En modo transmisión	3	295	885
MICROCONTROLADOR: Máxima corriente de salida por pin.	3	40	120
ALARMA: consumo típico cuando activo.	6	70	420
TOTAL		405	1425

Tabla 4.1 Consumo máximo de corrientes y cálculo de la potencia total que el módulo coordinador consume.

Primera opción: Fuente ELK

Se elige una fuente de alimentación regulada con una corriente de salida de hasta 1.2A y un voltaje de salida de 6VDC de marca americana ELKproducts (de 6.5Watts). Esta fuente incluye adicionalmente un cargador para baterías de capacidades 1.2Ah-10Ah, que se ajusta al requerimiento del dispositivo coordinador de la red [27].

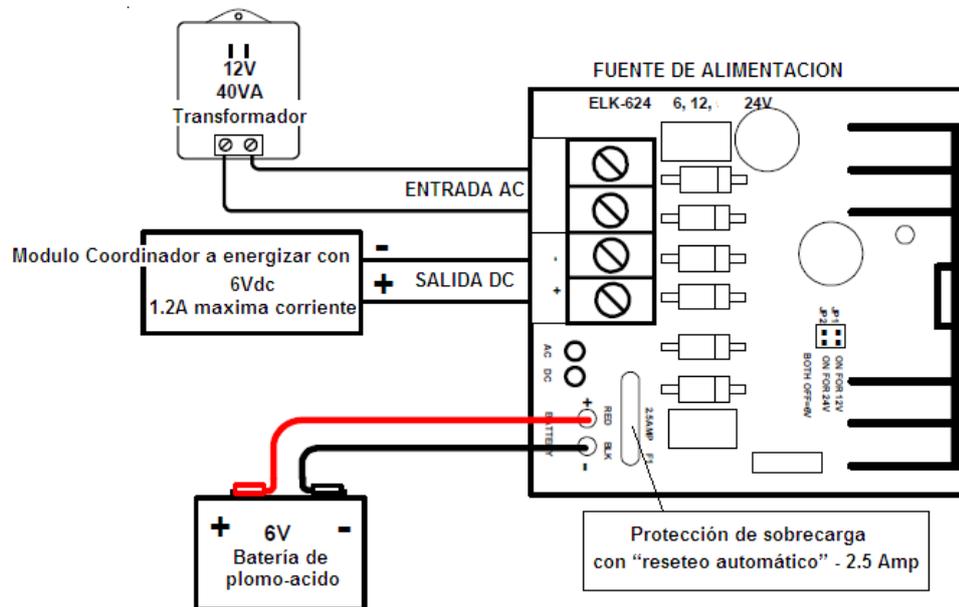


Figura 4.11 Diagrama de conexionado: Fuente de alimentación con cargador de batería Elk-624 encargada de energizar al módulo coordinador

<p>Especificaciones: Batería, 6V, 1.2AH - A506/1.2S Marca: Sonnenschein Tensión, Salida:6V Capacidad, de almacenamiento de energía:1.2Ah Tecnología, Batería:Plomo-ácido Longitud/Altura, exterior:51mm Anchura, exterior:97.3mm Profundidad, exterior:25.5mm Tipo de terminal:4.8mm x 0.8mm Corriente, de descarga máx.:40A Altura, máx.:54.9mm Temperatura, de op. máx.:50°C Temperatura, de op. mín.: -20°C Peso:0.3kg Corriente, de carga máx.:0,5A Tensión, de carga cíclica máx.:7.35V Tensión, carga cíclica mín.:7,2 V Tensión, cizallamiento de reserva máx.:7.05V Tensión, carga de reserva mín.:6,9 V</p>	
---	--

Figura 4.12 Batería de respaldo para el módulo coordinador [28].

Alimentación para el microcontrolador y el módulo de radiofrecuencia XBee S2

Como se muestra en la figura, ambos dispositivos son energizados con la fuente ELK pero con un regulador de voltaje LM317 de 3 Vdc.

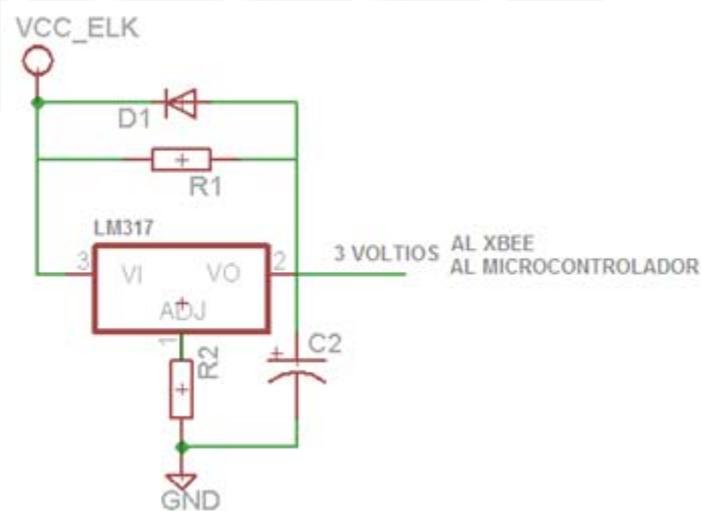


Figura 4.13 Diagrama esquemático de los circuitos de alimentación del microcontrolador (izquierda) y XBee (derecha).

Segunda Opción: Fuente regulada de fabricación local

Este circuito brinda 6V de alimentación ya sea desde la entrada (de 12Vdc) o desde su propia batería de 6v (1200ma/h), la cual además se puede cargar mientras tenga tensión entrante. La tensión de 12Vdc entra a un diodo protector de polaridad el cual deja pasar la corriente solo cuando la polaridad sea la correcta. Siguen dos capacitores de desacople y un LED con su respectiva resistencia limitadora de corriente.

Este LED, de color amarillo indica la presencia de tensión externa. Luego, un regulador positivo estabiliza la tensión a su salida en 6V y pasa por un cerámico de 100nF que filtra cualquier parásito que el regulador pueda influir. Los 6V resultantes entran al terminal Normal Abierto del relé, el cual conmuta entre tensión entrante y tensión de batería. El punto común de la llave del relé va directo a un electrolítico de 4700 μ F que mantiene la corriente estable mientras el relé cambia entre tensión de entrada y batería.

Ante la presencia de tensión en la entrada el regulador entrega a su salida 6V. El relé se encuentra con las terminales C y NA en corto por lo que los 6V del regulador son los que pasan hacia la salida de la fuente. Mientras tanto, parte de los 11V y pico que restan antes del regulador son inyectados a la batería para mantenerla en carga flotante. Esta carga la efectúa la resistencia limitadora de 33 ohms cuya potencia es 5 watts.

El diodo antes de esta resistencia hace que cuando falte la tensión entrante la batería no se descargue a través del sistema regulador impidiendo la circulación de la corriente en sentido inverso. De cortarse la tensión entrante el relé se apagará y ahora los contactos C y NC estarán en corto. Esto hace que la tensión de salida provenga de la batería, y gracias al capacitor electrolítico de 4700 μ F el cambio entre fuente entrante y batería no se nota dado que este mantiene la tensión constante mientras se efectúa el pase.

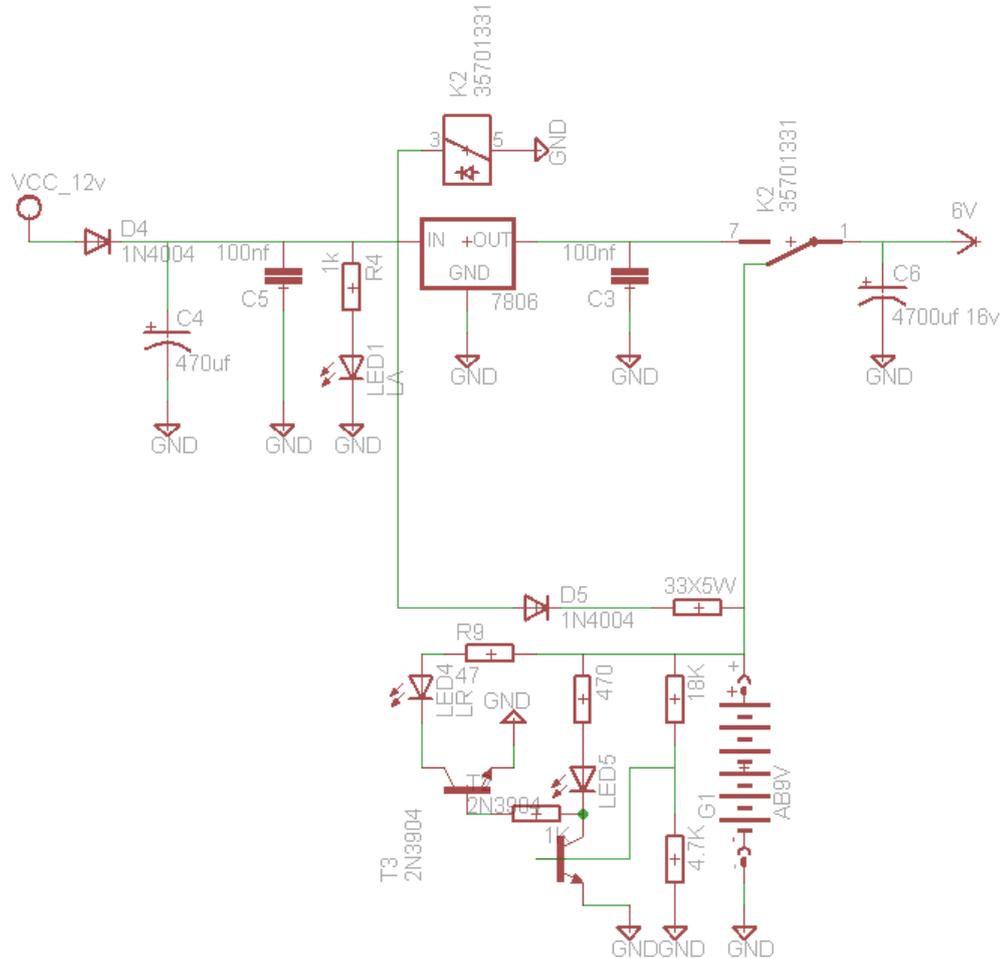


Figura 4.14 Circuito esquemático de una fuente regulada de 6 voltios con cargador de batería e indicador de carga.

4.3.1.4. La Alarma

La alarma está compuesta por un buzzer que es un dispositivo que se energiza con voltaje DC y emite un fuerte sonido de hasta 95 decibelios (dB) (más fuerte que el tráfico de la ciudad). Se utilizará un buzzer con un sonido extremadamente fuerte y está diseñado para operar en un amplio rango de voltajes de alimentación. No necesita ningún circuito (driver) para su activación, solo requiere voltaje DC. En nuestro diseño este buzzer será alimentado con 6 voltios y consumirá 4.5 mA, el buzzer es apropiado para funcionar como una alarma anti robo [29].



Figura 4.15 Buzzer DC de estado sólido

4.3.1.5. La Interfaz: Microcontrolador –Alarma

Para encender el buzzer el pin de salida del microcontrolador debe de estar en el estado alto (5 voltios), cuando eso suceda el Transistor npn 2N3904 se saturará y empezará a conducir alimentando a la bobina del relé, el contacto normalmente abierto (N.A) de este relé se cerrará dejando pasar corriente DC al buzzer. El puerto de salida del microcontrolador que saturará al transistor es el Pin D2.

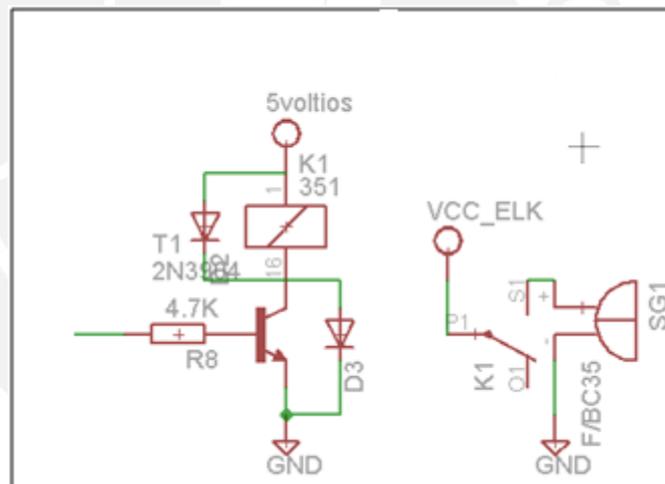


Figura 4.16 Diagrama esquemático de la interfaz entre el microcontrolador y el buzzer.

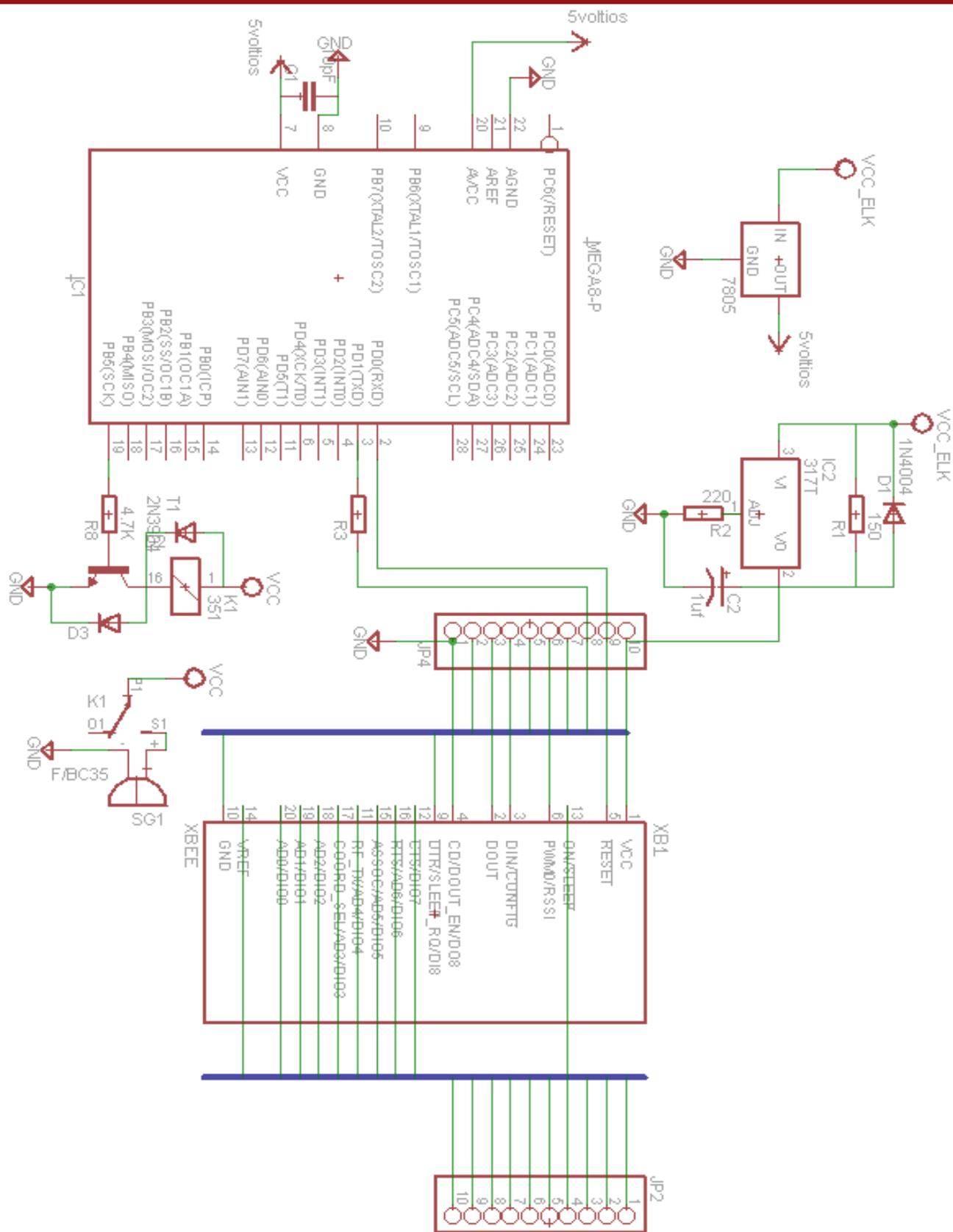


Figura 4.17 Diagrama esquemático del módulo coordinador

4.3.2. MÓDULO DE MONITOREO

Los componentes del módulo de monitoreo son esencialmente:

Un módulo XBee series 2.

Un microcontrolador ATmega88P

Dos pilas AA

Un contacto magnético o un sensor de rotura de vidrio.

Este módulo tiene la función de monitorear a los sensores que estén conectados a él. Los sensores de monitoreo (un contacto magnético, un sensor de rotura de vidrio o un detector de presencia) se comunican con el microcontrolador mediante su salida normalmente cerrada o abierta (N.C ó N.A) tal como se muestra el diagrama esquemático de la Figura 4.26

	Tipos de módulos de monitoreo	Función en cada área insegura
1	Con sensor de rotura de vidrio	Verifica rotura del vidrio de la ventana.
2	Con contacto magnetico	Verifica si la puerta está abierta o cerrada.

Tabla 4.2 Funciones de los dos tipos de módulos de monitoreo

4.3.2.1. Funcionamiento

El módulo de monitoreo tiene la principal característica de ahorrar energía y se pretende mantener a estos funcionando por **mucho tiempo** sin un cambio de baterías. El usuario debe percibir un muy bajo consumo de energía de sus sensores, tal como si se tratase de un mando de control remoto para televisor.

Por esta razón se utilizarán los modos STAND BY o DORMIDO en ambos dispositivos inteligentes (XBee y microcontrolador). La idea es que ambos dispositivos permanezcan dormidos la mayor parte del tiempo dando como resultado un mínimo consumo de energía.

Para ello en la presente tesis se propone un mecanismo de funcionamiento en donde el sensor conectado al XBee y microcontrolador (ver Figura 4.26 **Diagrama esquemático del módulo de monitoreo**) despierte a los dispositivos inteligentes mediante un *circuito de activación* también propuesto.

El microcontrolador estará conectado mediante los pines DIN y DOUT del XBee y transmitirá mensajes de alerta en caso uno de los sensores se active. Tanto el

microcontrolador como el XBee **permanecerán dormidos siempre** y la razón por la cual despiertan es la activación del contacto del sensor conectado, ya sea el sensor de rotura de vidrio o el sensor de contacto magnético.

El tiempo que permanezcan activados estos sensores determinará el tiempo que estén encendidos nuestros dispositivos, es decir el tiempo que el XBee y el microcontrolador se encuentren en estado normal y no en el estado dormido por defecto.

El caso más crítico es el módulo de monitoreo con sensor de contacto magnético, este se ha diseñado para ser instalado en la puerta principal, la cual se deduce que será abierta con mayor frecuencia en la vivienda y por consiguiente será este sensor el que más veces se active durante todo el día. En consecuencia se obtiene que el microcontrolador y el XBee presenten un mayor ciclo de activación y con ello un consumo de energía que aumentará por el lapso del tiempo⁸ que la puerta permanezca abierta.

ESTADO DE LA PUERTA	MODO DE XBEE Y MICROCONTROLADOR
Cerrada	Dormidos: ahorro de energía
Abierta	Activos: consumiendo de corriente

Para el caso del sensor de rotura de vidrio, el XBee y microcontrolador permanecerán dormidos todo el tiempo hasta que ocurra una intrusión rompiendo el vidrio de la ventana, algo muy poco frecuente; cada vez que se rompa la ventana el XBee se despertará y transmitirá.

❖ Contacto magnético

Para el diseño de la red de seguridad se utiliza un contacto magnético de montaje de superficie para aplicaciones residenciales. Su función es detectar la apertura de la puerta de ingreso. Este tipo de sensor no utiliza energía y tiene un contacto Normalmente Abierto (NA) que por medio de un circuito despertará al microcontrolador cuando el sensor se active. (Ver circuito en la sección 4.3.2.5)

⁸ Ver la sección 4.3.2.7 **Cálculo de duración de baterías: contacto magnético.** para este tipo de módulo de monitoreo.

<p>Especificaciones:</p> <p>Normalmente cerrado (puerta cerrada) Potencia nominal: 25,4 mm La cubierta oculta la resistencia final de línea (RFL) Conexión con 2 hilos Longitud del cable: 40 cm Temperatura de trabajo: -40 / +80 °C Tensión máxima: 200 Vdc. Corriente máxima de pico: 500 mA c.c. Resistencia del contacto abierto: Mayor a 100 ohm.</p>	
--	---

Figura 4.18 Contacto magnético para montaje en superficie

❖ Sensor de rotura de vidrio

Para el monitoreo de la ruptura de vidrios en las ventanas se utilizarán los sensores tipo BUG puesto que solo ellos usan un diapasón que detecta la rotura del vidrio. Se eliminan las falsas alarmas ya que el dispositivo no es activado por alguna vibración o choque.

Este tipo de sensor no utiliza energía y tiene salidas NC y NA que despertarán al microcontrolador cuando el sensor se active. Los sensores de rotura de vidrio tipo BUG son muy efectivos y además son recomendados por aseguradoras de Protección Primaria [31].

<p>Especificaciones:</p> <p>No requiere de energía para su funcionamiento. Ajustable para circuitos NC y NA. Se instala pegándolo. Protege hasta 12 metros cuadrados. Reset automático.</p>	
---	--

Figura 4.19 USP window bug glass

4.3.2.2. Ubicación

Los módulos de monitoreo estarán ubicados en las áreas inseguras según el estudio que se realizó en la sección 4.1.2.1 cada área necesitará de un módulo de monitoreo que se adapte a sus necesidades.

Lugar de ubicación	Módulo de monitoreo
Balcón	Con sensor de rotura de vidrio
Sala comedor	Con sensor magnético de apertura en la puerta de ingreso
Dormitorio principal	Con sensor de rotura de vidrio
Dormitorio 2 y 3	Sensor de rotura de vidrio

Tabla 4.3 Tipo de módulo de monitoreo según el lugar de ubicación

4.3.2.3. Circuito de pulso

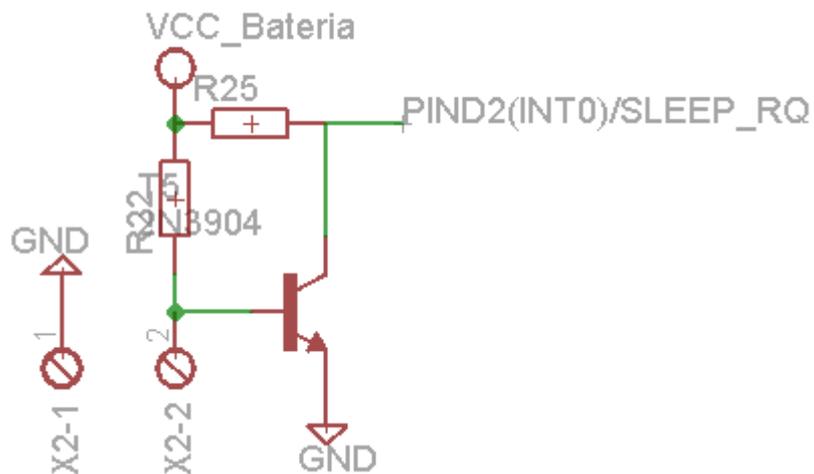


Figura 4.20 Circuito de pulso para despertar al microcontrolador y XBee.

Este es el circuito que despierta al microcontrolador y al XBee y depende del contacto del sensor (X2-1 y X2-2). Por ejemplo, para el caso del contactor magnético, este tiene a la salida un contacto normalmente cerrado por lo que necesitará de un transistor en corte y saturación para convertir el estado del contacto de salida en un voltaje que indique despertar al microcontrolador o XBee. El microcontrolador y el XBee despertarán cuando se aplique un voltaje de 3 voltios en el pin PIND2 y SLEEP_RQ respectivamente.

NOTA: Para el circuito de pulso no se consideró el diseño con un chip 74LS04 **inversor** debido a que en las pruebas realizadas tenía un consumo de 10mA tanto para el estado abierto y cerrado del contacto del sensor; esta corriente es demasiado alta para nuestra aplicación y es por ello que se elige transistores de

corte y saturación con resistencias de alto valor en la base y el colector para limitar la corriente. Este circuito de pulso deberá también consumir lo menos posible de energía, por eso se plantea los siguientes valores de resistencias:

R_c =Resistencia de colector: $R_{25}=100\text{Kohm}$,

R_b =Resistencia de la base: $R_{32}=100\text{Kohm}$

$V_{CC}= 3V$: Voltaje de alimentación del módulo de monitoreo

$V_{BASE}= 0V$ ó $3V$, voltaje brindado por el estado del sensor

De todo esto se encuentra que el transistor 2N3904 cumple con los parámetros de trabajo mencionados, sus características son:

TBJ NPN 2N3904		
PD maxima	625	mW
VBE on	0,7	V
VCE maxima	40	
VCE saturac.	0.3	
IC maxima	200	A
IB minima	0.05	
b mínimo	100	

Tabla 4.4 Parámetros del transistor 2N3904 [30].

4.3.2.4. Ahorro de Energía

Modo dormir del XBee

Desde la sección 2.3 **Características del sistema de seguridad** se ha considerado que una de las principales ventajas de este sistema de seguridad es el bajo consumo de energía y esto se logra utilizando la tecnología ZigBee con los módulos de radiofrecuencia XBee. Para ello se configura el XBee con el modo **Pin Sleep** el cual consiste en que cada vez que el pin 9 (Sleep_RQ) este en el nivel alto (3 voltios) el XBee entra en un estado de ahorro de energía llegando a consumir tan solo $1 \mu A$.

Estado del monitoreo			XBee		
Presencia	Vidrio	Puerta	Estado	Pin Sleep_RQ	Pin On/Sleep
No detecta	No rotura	Cerrada	Dormido	3V	0V
Detecta	Rotura	Abierta	Despierto	0V	3V

Tabla 4.5 Estado del XBee según el estado del módulo de monitoreo al que pertenece.

Modo dormir del microcontrolador

Es muy importante hacer dormir al microcontrolador también pues de esa manera solo consumirá $0.75\mu A$ (considerando el uso de un microcontrolador de bajo consumo de energía ATmega88). El microcontrolador estará configurado en el modo **power down** teniendo disponible las interrupciones externas INT0 e INT1 para despertarlo cuando sea requerido, de otra forma permanecerá dormido. Para nuestro caso será despertado cada vez que haya una activación en el sensor.

4.3.2.5. Cálculo de corrientes

CONTACTO MAGNÉTICO	CÁLCULO DE CORRIENTES EN EL MÓDULO DE MONITOREO
<p>CONTACTO CERRADO:</p> <p>TRANSISTOR EN CORTE</p>	<p>El transistor del circuito de pulso se encontrará en estado de corte, por lo tanto se obtienen los siguientes voltajes:</p> <p>$V_{PIND2} = V_{sleepRQ} = 3V$ (Pin Sleep del microcontrolador y XBee = "1")</p> <p>Microcontrolador: Modo Power Down XBee: Modo Pin Sleep</p> <p>$I_{XBEE} = 1\mu A$</p> <p>$I_{UC} = 0.75\mu A$</p> <p>[Malla del colector: $I1 = (V_{cc} - V_{ce}) / R25 = (3V - 3V) / 100K = 0$</p> <p>Malla de la base: $I2 = (V_{cc} - V_{be}) / R32 = (3V - 0.7V) / 100K = 23\mu A$</p> <p>$I_{CKTO} = I1 + I2 = 23\mu A$ (corriente consumida por el circuito de pulso)</p> <p>$I_{TOTAL} = 24.75\mu A$</p> <p>$P_{TOTAL} = 74.25\mu W$</p>
<p>CONTACTO ABIERTO:</p> <p>TRANSISTOR SATURACION</p>	<p>El transistor del circuito de pulso se encontrará en estado de saturación, por lo tanto se obtienen los siguientes voltajes:</p> <p>$V_{PIND2} = V_{sleepRQ} = 0V$ (Pin Sleep del microcontrolador y XBee = "0")</p> <p>Microcontrolador: Modo activo XBee= Modo Ocioso/transmisión</p> <p>$I_{XBEE} = 45mA$</p> <p>$I_{UC} = 0.3mA$</p> <p>$I_{CKTO} = 50\mu A$</p> <p>[Malla del colector: $I1 = (V_{cc} - V_{ce}) / R25 = (3V - 0.3V) / 100K = 27\mu A$</p> <p>Malla de la base: $I2 = (V_{cc} - V_{be}) / R25 = (3V - 0.7V) / 100K = 23\mu A$</p> <p>$I_{TOTAL} = 45.353mA$</p> <p>$P_{TOTAL} = 136.05mW$</p>

Tabla 4.6 Cálculo de corrientes según el estado del contacto magnético.

4.3.2.6. Elección de la fuente de energía

Los módulos de monitoreo no incluyen un regulador de voltaje para alimentar al XBee y al microcontrolador, en vez de ello se trabajará con pilas o baterías en un rango de 2.1 voltios (mínimo voltaje para energizar el XBee S2) y 3.6 voltios (máximo voltaje de una pila de litio del tamaño AA) que energizarán directamente al XBee y al microcontrolador.

Para la elección de la fuente de energía se tratará de elegir una que combine las siguientes características:

1. Bajo costo
2. Alta capacidad de almacenamiento de energía: mA/hr
3. Tamaño pequeño
4. Fácil adquisición

4.3.2.7. Cálculo de duración de baterías: contacto magnético.

*NOTA: Solo se ha considerado el cálculo de duración de las baterías en los módulos de monitoreo de contacto magnético, **no** se ha considerado el cálculo de baterías para el módulo de monitoreo con sensor de rotura de vidrio debido a que este solo se activará en caso de hurto y tanto el XBee como el microcontrolador permanecerán dormidos todo el tiempo hasta que eso suceda, logrando así un consumo mínimo de energía y una muy larga duración de sus baterías.*

Se calcula el número de veces que se activará y desactivará el pin SLEEP_RQ del XBee del módulo de monitoreo. Como se explicó en la sección anterior, no importa si el usuario enciende o apaga el sistema, los dispositivos de monitoreo siempre transmitirán cada vez que el pin SLEEP_RQ se desactive.

A continuación se calculará la duración de las baterías para el módulo de monitoreo con contacto magnético (para el monitoreo de puertas), **específicamente** para del **módulo que supervisa la puerta de ingreso y salida** al departamento, pues es el módulo que más veces se activará al día.

Variables:

N= # personas en la vivienda

ABRT= Veces que abre la puerta una persona

T= Periodo de apertura de una puerta = $86400/N \cdot ABRT$ segundos

- T_abierto= Tiempo que se mantiene la puerta abierta.
- T_cerrado= Tiempo que se mantiene la puerta abierta.
- T_batería= Tiempo de duración de la batería.

Ejemplo de cálculo:

- N= Número personas en la vivienda: 5
- ABRT= Cantidad de veces que abre la puerta o ventana una persona en 1 día = 16 (8 veces para salir y 8 veces para entrar)
- N*ABRT= Cantidad total de veces que abre la puerta las 5 personas en 1 día = 80 veces
- 1 Día = 24 horas = 1440 min = 86400 seg
- $T=86400/N*ABRT = \text{Periodo de apertura de una puerta} = 86400\text{seg}/80\text{veces} = 1080 \text{ seg.} = 18 \text{ min.}$
- T_abierto= Se define que el usuario dejará la puerta abierta por 5 segundos.

“Cada 1080 segundos de funcionamiento el módulo de monitoreo estará 5 segundos despierto, mejor dicho consumiendo 45mA”

Resultados y explicación del cálculo de baterías:

Se logra obtener como resultado que aproximadamente el periodo de abrir una puerta es de 1080 segundos para un departamento en donde viven 5 personas, saliendo en promedio 8 veces y entrando 8 veces. Consideramos que una persona cuando abre la puerta la deja abierta por 5 para luego cerrarla. Esto da como consecuencia una puerta cerrada por 1075 segundos hasta una nueva apertura, de esa manera se completa el periodo de 1080 segundos. Como se ha configurado al XBee y al microcontrolador para que se despierte cada vez que alguien abre la puerta este permanecerá despierto 5 segundos y dormido 1075 segundos.

Dando como resultado la siguiente relación:

CONTACTO CERRADO	CONTACTO ABIERTO
TIEMPO= 1075SEG	TIEMPO= 5SEG
Microcontrolador: Dormido	Microcontrolador: Despierto
XBee: Dormido	XBee= Despierto, modo Ocioso /transmisión
$I_{TOTAL}=24.75\mu A$	$I_{TOTAL}=45.353mA$
Ptotal= 74.25uW	Ptotal= 136.05mW

Tabla 4.7 Tiempo que el Microcontrolador y XBee permanecen dormidos y sus respectivos consumos de energía

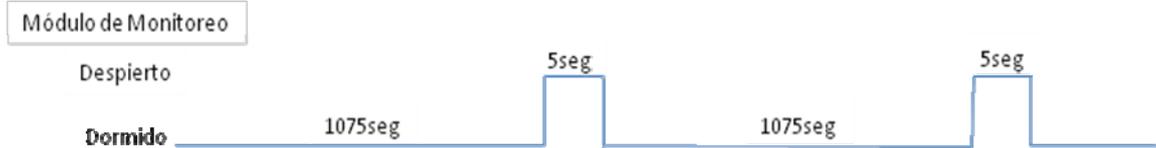


Figura 4.21 Diagrama del estado del módulo de monitoreo por ciclos

$$I_{PROMEDIO} = [(24.75\mu A \times 1075\text{seg}) + (45.353\text{mA} \times 5\text{seg})] / 1080\text{seg}$$

$$I_{PROMEDIO} = 0.2346\text{mA}$$

❖ **Pilas Duracell MN 1500-AA** [32].

Si el módulo fuera alimentado con un par de baterías alcalinas Duracell AA de 1.5v cada una con **2.850A-H**

Tiempo de duración Teórico:

$$\text{Tiempo de vida de las baterías} = (2850\text{mA-H}) / 0.2346\text{mA} = 11127.88 \text{ horas}$$

Tiempo teórico de vida de las baterías= 16.9 meses

Tiempo de duración Real:

De la Figura 4.21 se deduce:

Periodo -> T despierto

1080seg -> 5seg

2160 seg-> 10seg

3040 seg -> 15seg

....

Por la regla de 3 simple se obtiene la siguiente fórmula:

$$\mathbf{T_{despierto} = Periodo * 5 / 1080}$$

Se tiene la relación de que cada 1080 segundos (18min) el módulo de monitoreo se despierta 5 segundos, esto quiere decir que en 16.9 meses de funcionamiento el módulo de monitoreo habrá permanecido 56.33 horas despierto⁹. Por lo tanto, durante 56.33 horas el módulo de monitoreo consume 45.353mA, llevando esta información a las curvas de las pilas Duracell, **NOTA:** Se elige la segunda curva

⁹ El tiempo despierto se calcula con una regla de tres simple, siendo la fórmula:

$$T_{despierto} = Periodo * 5 / 1080$$

(24ohms: 50mA) pues es la curva de corriente que se aproxima más al consumo del XBee igual a 45mA.

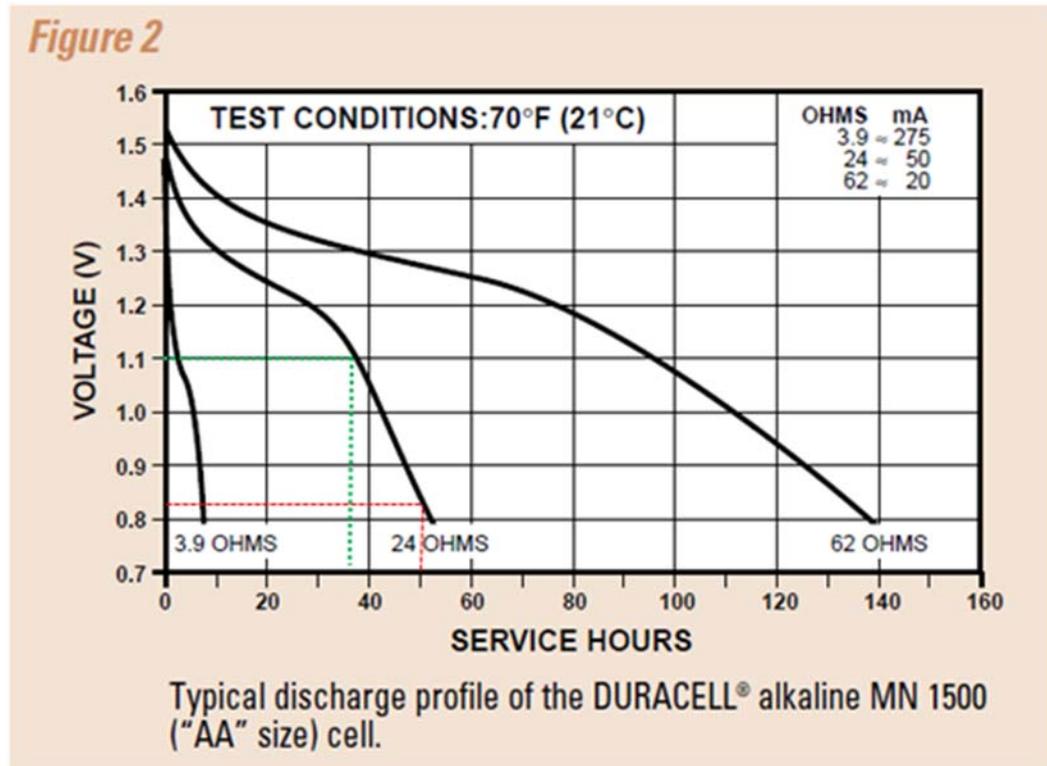


Figura 4.22 Curva de descarga del voltaje de la pila Duracell [32].

De la figura anterior se obtiene que para un tiempo de servicio de 50 horas se obtiene un voltaje en cada pila de 0.82 voltios (línea roja), lo que resultaría en **1.64 voltios con 2 pilas en serie**, voltaje que **no es válido** para energizar al módulo de monitoreo. Por lo tanto el cálculo del tiempo de vida de la batería estaría sobredimensionado si es que no se verifica con la curva del fabricante de la pila a usar.

Se necesita de un mínimo voltaje de 2.1 voltios (mínimo voltaje DC para el Xbee series 2, **ver la página 8 del manual de XBee Series 2**) para que el módulo de monitoreo pueda funcionar, tabulando esto en la segunda curva se obtiene que deberemos utilizar la pila hasta un máximo de 35 horas de servicio (**línea verde**) aproximadamente.

Las 35 horas de servicio en las pilas significan **10.5 meses** (Periodo= $T_{despierto} \cdot 1080 / 5$) que habrá funcionado el módulo de monitoreo con pilas nuevas. Por lo tanto, si es que los módulos trabajasen con estas pilas, se

recomienda cambiar las pilas Duracell MN 1500-AA cada 10 meses y así asegurar un voltaje de al menos 1.10v por pila (2.20v con 2 pilas en serie).

<p>Fabricante: Duracell Modelo: MN1500 Sistema: No recargable Tipo: Alcalina Voltaje: 1.5v Capacidad: 2850mA/H Peso: 18 gr Tamaño: AA</p>	
--	---

Figura 4.23 Pila Duracell MN 1500-AA, una de las posibilidades de fuente de energía para los módulos de monitoreo [32].

❖ **Pilas de Litio LS 14500: 3.6voltios**

Si se observa la curva de descarga de las pilas LS14500 para la curva aproximada de 47mA, se obtiene también que para cuando el voltaje llegue a 2.2v la pila tendrá un tiempo de servicio de aproximadamente 40 horas que se traduce en **12 meses de funcionamiento continuo del módulo de monitoreo.**

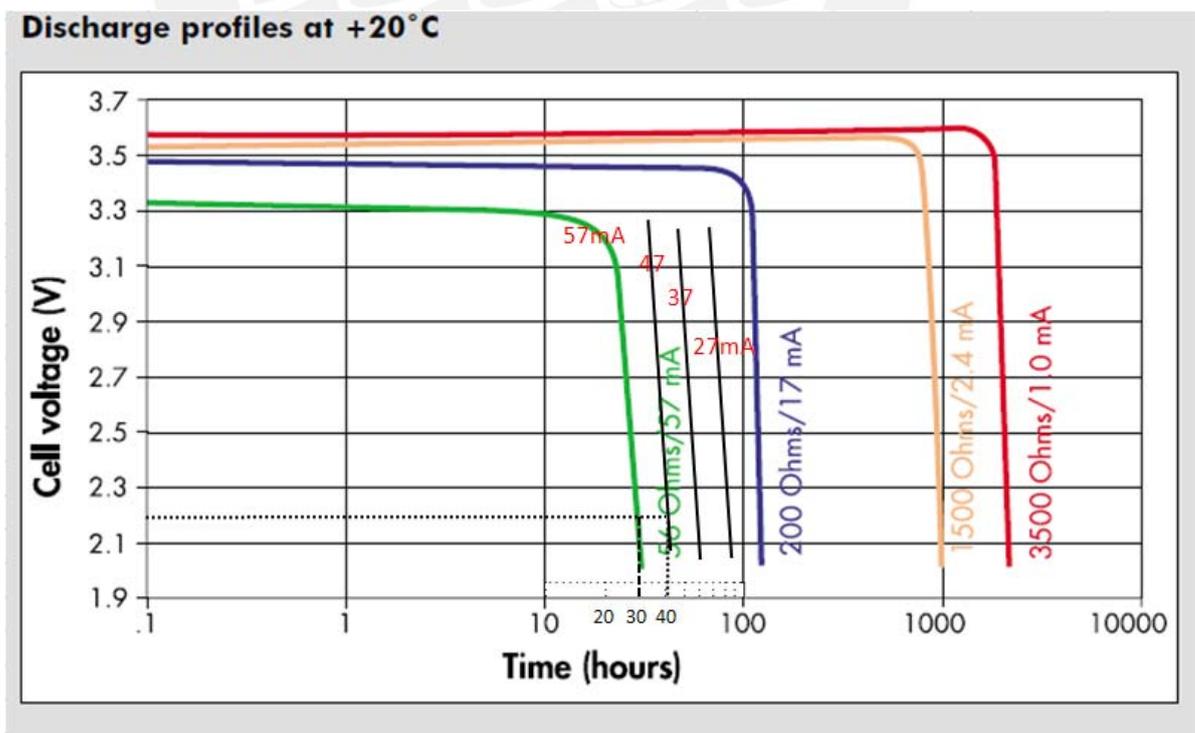


Figura 4.24 Curva de descarga del voltaje de la pila LS 14500

Fabricante: SAFT
 Modelo: LS 14500
 Sistema: No recargable
 Tipo: Litio
 Voltaje: 3.6v
 Capacidad: 2250 mA/H
 Peso: 16 gr
 Tamaño: AA



Figura 4.25 Pila SAFT LS 14500-AA, una de las posibilidades de fuente de energía para los módulos de monitoreo [33].

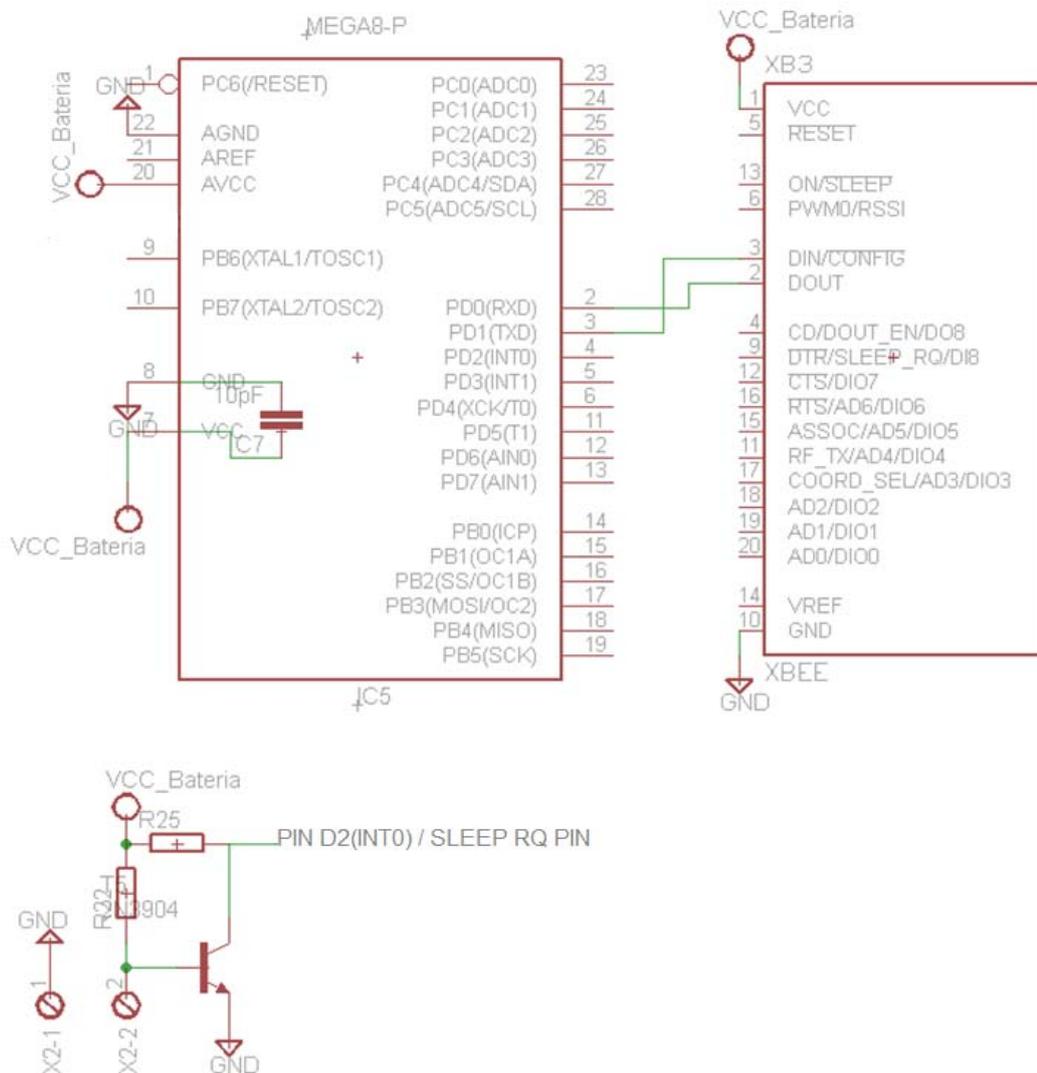


Figura 4.26 Diagrama esquemático del módulo de monitoreo

4.3.3. MÓDULO DE AVISO

4.3.3.1. Ubicación

Este módulo se encontraría en la zona común del piso del departamento y tiene como función alertar al personal de seguridad y/o conserjería. En resumen sería una extensión de la alarma que tiene el módulo coordinador.

4.3.3.2. Funcionamiento

Este módulo contiene un XBee que recibe el mensaje *alerta* del XBee coordinador y lo transmite hacia el microcontrolador conectado a él, este microcontrolador activará la alarma.

La alarma se activará 5 segundos después de detectada una intrusión, estos 5 segundos son un tiempo de guarda en caso se trate de una falsa alarma ofreciendo al usuario el tiempo suficiente para desactivar el sistema. La desactivación del buzzer se dará cuando el usuario presione el pulsador *apagar* en el control remoto. En este caso la señal *apagar* va dirigida hacia el coordinador de la red, quien recepcionará el mensaje y lo reenviará hacia el módulo de aviso, luego de esto el microcontrolador en el módulo de aviso procesará el mensaje y desactivará la alarma.

4.3.3.3. Dispositivos Electrónicos

Un microcontrolador ATmega88P (ATmega8L opcional)

Un módulo XBee PRO Series 2

Fuente regulada de voltaje con cargador de batería

Una alarma

Interfaz microcontrolador - buzzer: Transistor con relé

Se espera que al tener un XBee Series 2 PRO (en lugar de un XBee S2 estándar) la señal del coordinador pueda salir de la casa y llegar hasta la zona común, en caso no sea así se necesitará de un módulo (con un XBee de ruteador) entre ambos.

El diseño de este módulo de aviso es físicamente similar al módulo coordinador, por lo que el funcionamiento, interconexión y diseño de todos estos dispositivos son descritos en la sección 4.3.1

4.3.4. MÓDULO DE CONTROL REMOTO

El módulo coordinador contiene los siguientes dispositivos electrónicos:

Un microcontrolador ATmega88

Un módulo XBee Series 2

02 pulsadores NC

Resistencias

Dos baterías tipo AAA Duracell.

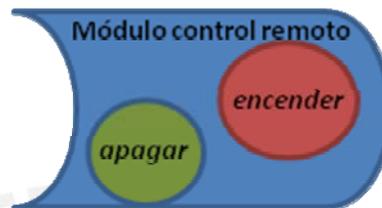


Figura 4.27 Módulo control remoto

4.3.4.1. Funcionamiento

Funciona tal como un módulo de monitoreo, con la diferencia que tiene que revisar constantemente la pulsación de 2 pulsadores, por lo que cada uno se conectará en los 02 pines de interrupción INT0 e INT1, haciendo que el microcontrolador se despierte y pueda enviar los mensajes *encender* o *apagar* (por medio del XBee) según sea el caso.

4.3.4.2. Cálculo de corrientes

A continuación se realiza en cálculo de las corrientes totales para este módulo de control remoto, siendo:

CONTACTO CERRADO:

TRANSISTOR EN CORTE

$$V_{PIND2}=3V$$

Microcontrolador: Modo Power Down

XBee: Modo Pin Sleep

$$I_{XBEE}=1\mu A$$

$$I_{UC}=0.5\mu A$$

$$\text{Malla del colector: } I1 = (V_{cc}-V_{ce})/R25 = (3V-3V)/100K = 0$$

$$\text{Malla de la base: } I2 = (V_{cc}-V_{be})/R32 = (3V-0.7V)/100K = 23\mu A$$

$$I_{TOTAL} = I1 + I2 = 1\mu A + 0.5\mu A + (23\mu A \times 2) = 47.5\mu A$$

CONTACTO ABIERTO:

TRANSISTOR EN SATURACION

$$V_{PIND2}=0V$$

Microcontrolador: Modo activo

XBee= Modo Ocioso/transmisión

$$I_{XBEE}=45mA$$

$$I_{UC}=5mA$$

$$\text{Malla del colector: } I_1=(V_{cc}-V_{ce})/R_{25}=(3V-0.3V)/100K=30\mu A$$

$$\text{Malla de la base: } I_2=(V_{cc}-V_{be})/R_{25}=(3V-0.7V)/100K=23\mu A$$

$$I_{TOTAL}=I_1+I_2= 45mA+5mA+ (53\mu A \times 2)= \mathbf{50.106mA}$$



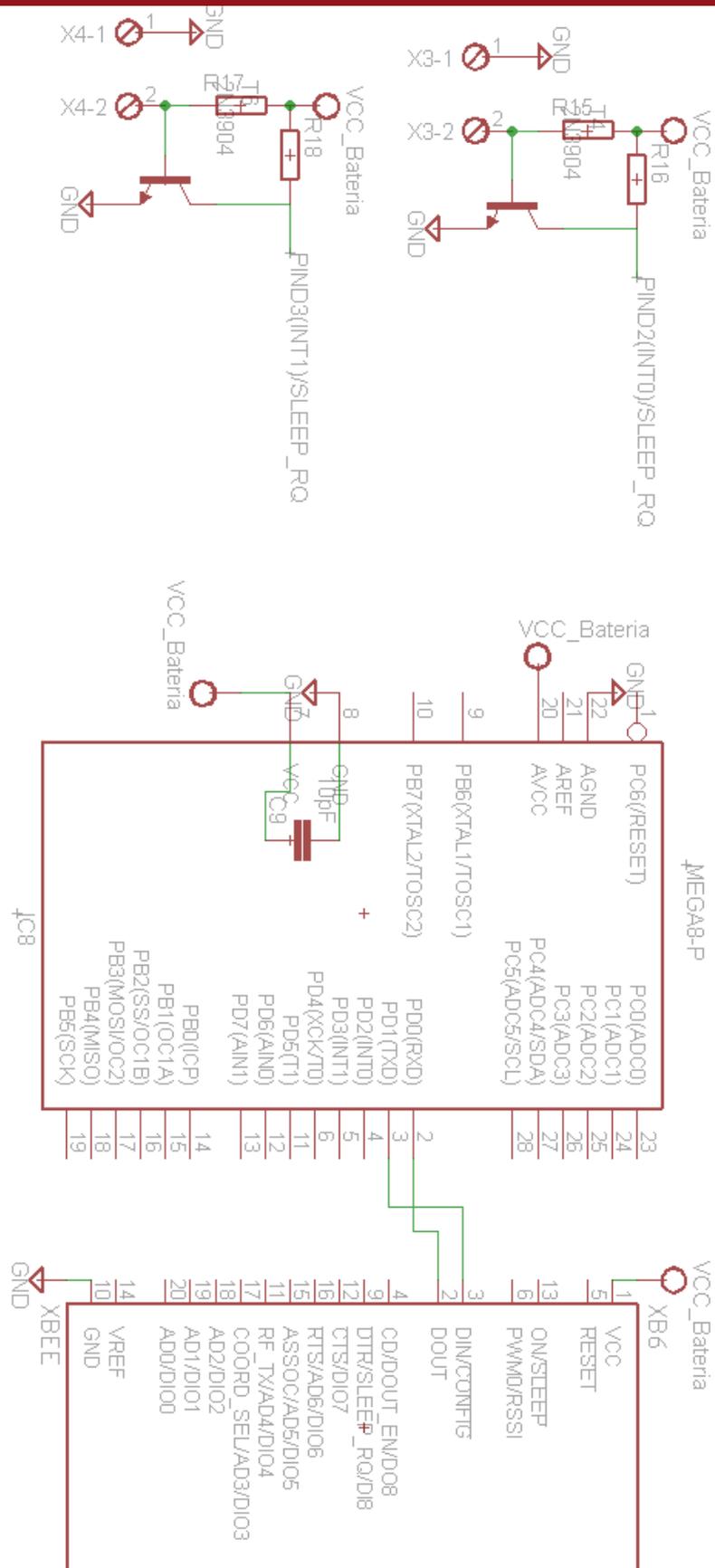


Figura 4.28 Diagrama esquemático del módulo de control remoto

4.3.4.3. Cálculo de duración de baterías

Asumiendo que cada pulsador es presionado al menos unas 3 veces al día, se muestra el ejemplo del siguiente cálculo:

- $PULSO = \text{Cantidad de veces que se presiona los pulsadores} = 6 \text{ veces}$ (3 veces pulsador “encender” y 3 veces el pulsador “apagar”)
- $1 \text{ Día} = 24 \text{ horas} = 1440 \text{ min} = 86400 \text{ seg}$
- $T = 86400 / PULSO = \text{Periodo de pulsación del control remoto} = 86400 \text{ seg} / 6 \text{ veces} = 14400 \text{ seg.} = 240 \text{ min} = 4 \text{ horas.}$
- Asumimos que el tiempo que el usuario mantiene presionado cada boton es de 2 segundos.
- Cada 4 horas el usuario despertará por 2 segundos al microcontrolador y al XBee del módulo control remoto.

El consumo de corriente promedio en 4 horas es:

$$I_{PROM} = (47.5 \mu A \times 14398 + 50.106 \text{ mA} \times 2) / 14400 = 0.054 \text{ mA}$$

Por la poca corriente promedio que utiliza el control remoto, se concluye que para este dispositivo será necesario usar dos pilas **tipo AAA** con una capacidad de 1150mA-H modelo MN2400. El tiempo de vida de las baterías para este módulo de control remoto, presionando los botones en promedio 6 veces al día, es de:

$$\text{Tiempo de vida} = 1150 \text{ mA-H} / 0.054 \text{ mA} = 3333.34 \text{ horas} = \mathbf{29 \text{ meses.}}$$

Esto quiere decir que en 29 meses de funcionamiento el módulo control remoto habrá estado **despierto 96.66 horas**.

NOTA: Este dispositivo también deberá tener el algoritmo del indicador de voltaje de batería explicado en la sección **¡Error! No se encuentra el origen de la referencia..**

Fabricante: Duracell Tamaño: AAA Modelo: MN2400 Sistema: No recargable Tipo: Alcalina Voltaje: 1.5v Capacidad: 110mA/H Peso: 11 gr	
---	---

Figura 4.29 Pila duracell tipo AAA para energizar al módulo de control remoto
4.3.4.4. Activación del Sistema de Seguridad

El control remoto está compuesto de un módulo XBee, quien se encarga de enviar el mensaje *encender* al módulo coordinador, lo cual significa que el sistema de seguridad está preparado para alarmarse en caso se detecte alguna intrusión.

La activación del sistema se producirá luego de 10 segundos de haber presionado el pulsador rojo *encender* en el control remoto, este es el tiempo de guarda que permite a todos los miembros de la familia salir de su residencia por completo. Este tiempo estará programado en el microcontrolador del módulo coordinador. A partir de ese momento cualquier intrusión detectada por lo módulos de monitoreo tendrá como consecuencia la activación de la alarma.

4.3.4.5. Desactivación del Sistema de Seguridad

Antes de abrir la puerta de ingreso/salida se tiene que desactivar el sistema mediante el pulsador verde *apagar*. En el caso que el usuario se olvide de desactivar el sistema, se activará el buzzer en el dormitorio principal, luego el módulo coordinador esperará 5 segundos para enviar el mensaje *alerta* al módulo de aviso que está ubicado en el cuarto de seguridad del edificio.

4.4. Diseño lógico de los módulos

En esta sección se explicarán los componentes del diseño lógico del sistema de seguridad, mientras por un lado se necesita configurar al XBee por medio del firmware de fábrica, también se deberá de configurar al microcontrolador como el dispositivo inteligente que manejará el comportamiento del sistema de seguridad.

4.4.1. Versiones del Firmware

Las versiones del firmware XBee Znet 2.5 tiene cuatro dígitos ABCD, esta versión puede ser mostrada en el tab TERMINAL del XCTU tipeando la sentencia *ATVR*. Este responderá con 4 números en hexadecimal (0-F). La versión es reportada así: "ABCD" en donde D es el número de la revisión desde el primer lanzamiento [25].

"B" es una variante que designa los siguientes dispositivos:

- * "0" - Coordinator, AT Command Mode (AP=0)
- * "1" - Coordinator, API Mode (AP=1,2)
- * "2" – Router / End Device AT Command Mode (AP=0)

* "3" - Router / End Device API Mode (AP=1,2)

Todas las publicaciones tendrán un número par en la letra C, y un número impar cuando se trate de desarrollos de firmware internos. La última versión fue la 1x47, lanzada el 7 de agosto del 2008 basado en el software EmberZNet 2.5.4.

La versión para la configuración de nuestros dispositivos se muestra en la siguiente tabla.

XBEEs	Version
XBee coordinador	1047
XBee en el módulo de monitoreo	1247
XBee en el módulo de aviso	1247
XBee en el módulo control remoto	1247

Tabla 4.8 Versiones de firmware para cada XBee

4.4.2. Software XCTU

El módulo XBee necesita de un firmware que especifique su funcionamiento como COORDINADOR o como ROUTER/DISPOSITIVO FINAL. Para cargarlo se necesita del programa **XCTU** el cuál es proporcionado por la empresa Digi, fabricante del módulo XBee. Este programa es una interfaz entre el XBee y la computadora, en la computadora se podrán descargar los firmwares adecuados para el uso específico de los XBee en los módulos de monitoreo, aviso, control remoto y coordinador. La descarga actualizada del programa XCTU contiene los últimos firmwares para el XBee, por lo tanto bastará con revisar el historial de actualizaciones de firmwares para elegir el firmware más moderno y que se adapte a nuestras necesidades.

4.4.3. Grabación del Firmware

Los pasos a realizar en el proceso de grabación del firmware en el módulo XBee son los siguientes:

- Descargar la versión más reciente del XCTU
- Conectar el XBee hacia un Módulo de Interfaz RS 232¹⁰
- Conectar el módulo de interfaz RS 232 hacia el puerto COM1 de la PC

¹⁰ RS-232 Development Board **Part #** XBIB-R: Mayor información a partir de la página 37 del manual: XBee™/XBee-PRO™ OEM RF Modules, Product Manual v8.x1x Beta - ZigBee Protocol

- Abrir el programa XCTU y en el tab “PCsettings” seleccionar el puerto correcto (COM1) seleccione el tipo de velocidad de bits de 9600 baudios y deje tal como están los parámetros por defecto como : (None, 8, None, 1)
- Seleccionar el tab “Modem Configuration” y presione “Read” para leer los parámetros con los que el XBee vino de fabrica.
- Seleccionar el Firmware deseado desde el menú desplegable “Version”
- Presionar “Write”
- El firmware ya estará actualizado y grabado en un solo módulo XBee S2.

Se debe de seguir los mismos pasos para grabar el firmware a todos los módulos XBee que conformarán: el módulo coordinador, el módulo de monitoreo, el módulo de aviso y el módulo de control remoto.

4.4.4. Parámetros del XBee en cada módulo

Una vez configurado el firmware del XBee se procede a configurar, en el mismo XCTU. Para el caso del coordinador se configuran los parámetros esenciales para la formación de la red y la asociación de los demás dispositivos.

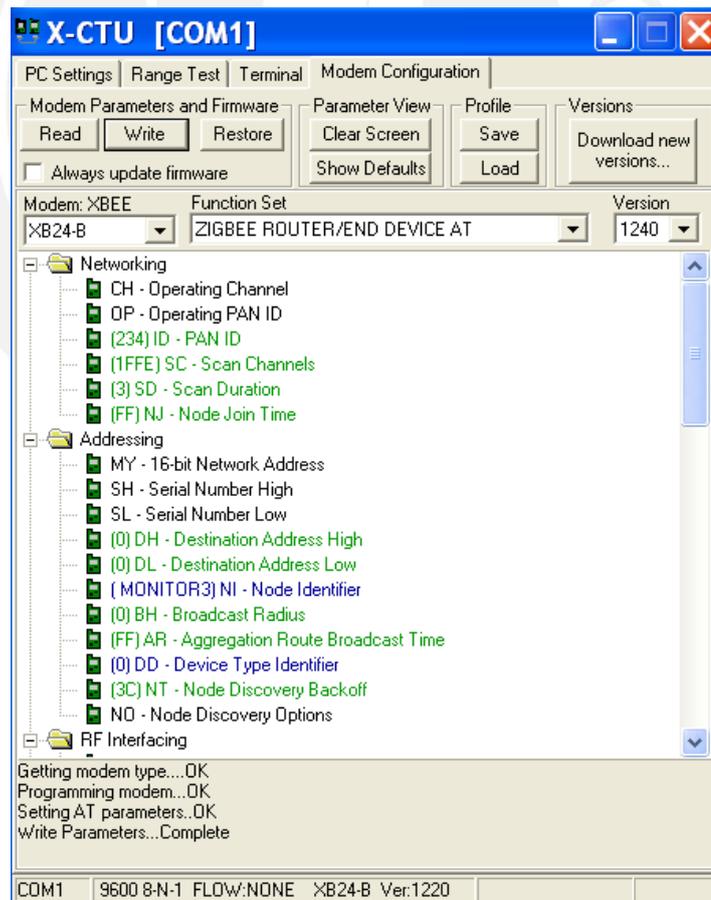


Figura 4.30 Concluye el proceso de grabación (ver la parte inferior)

La formación de esta red está gobernada por el modo de comandos AT: SC (escaneo de canales), ID (asignación de dirección de PAN), SD (duración de escaneo) y NJ (tiempo de asociación). Los parámetros como el canal de operación, la dirección o PAN ID, el tiempo de escaneo, etc. son establecidos automáticamente, el XBee realiza permanentemente un escaneo de canales libres y de esa manera elige su propio canal de operación y su dirección PAN ID. Debido a que la configuración es automática, no es necesario configurar manualmente esos parámetros en el programa XCTU, sin embargo es recomendable que al tener múltiples redes inalámbricas los XBee se configuren manualmente con su dirección de PAN.

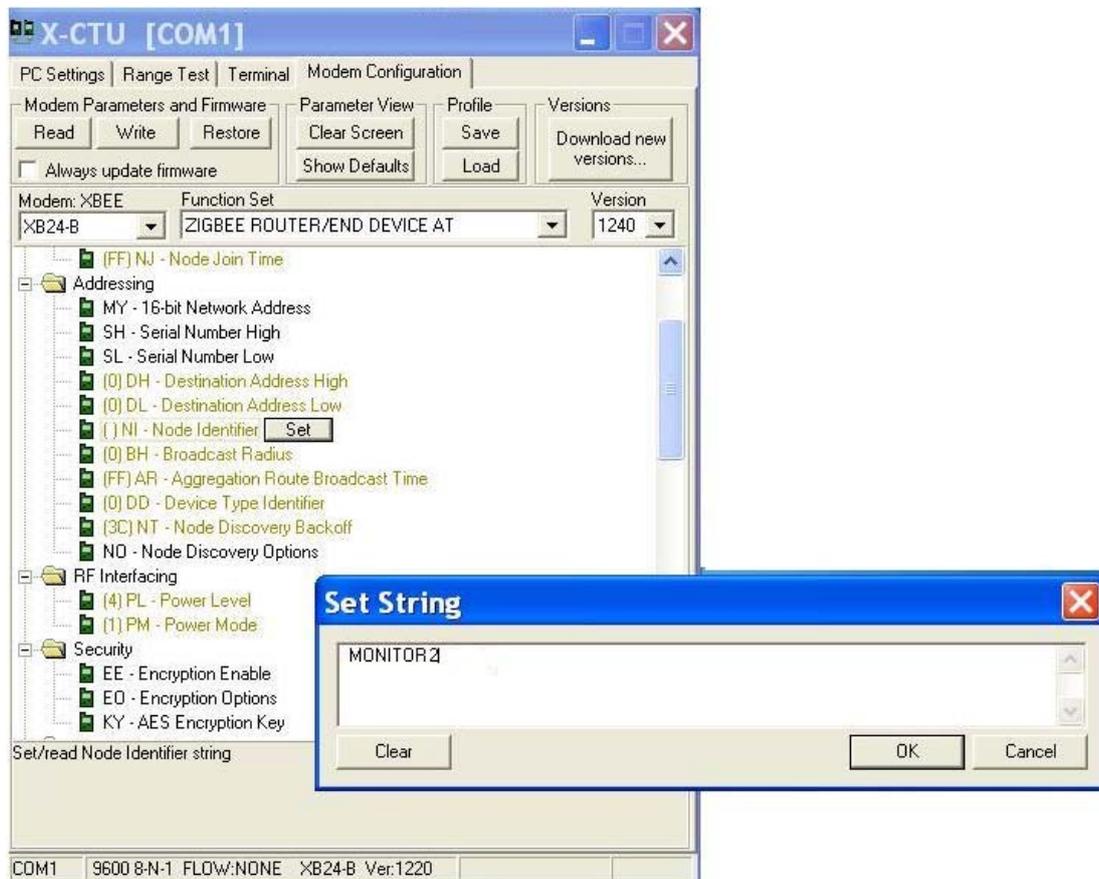


Figura 4.31 Cuadro de diálogo para asignar el nombre *MONITOR2* a uno de los módulos XBee

Para establecer la comunicación de la red de todos los módulos, es necesario establecer en cada uno un nombre o identificación. Se empieza con el XBee que es el **COORDINADOR** y se escribe este nombre en el XCTU. Luego de ello se procede a grabar con el botón “write”. El siguiente paso es identificar y establecer un nombre para los demás módulos XBee. En la aplicación del sistema de seguridad los XBee restantes (los dispositivos finales) se llamarán

respectivamente **MONITOR#**, **AVISO** y **REMOTO**. En la Figura 4.31 se muestra el cuadro de dialogo en donde se realiza la escritura de los nombres.

Una vez que ya se han establecido los nombres en cada uno de los módulos XBee estos han quedado listos para formar una red, comunicarse entre ellos y para interactuar con el microcontrolador en cada uno de sus módulos.

La siguiente es una tabla en donde se muestran los valores con los que han quedado configurados los módulos del sistema de seguridad.

PARAMETROS	LEYENDA	COORDINADOR	MONITOREO	AVISO	REMOTO
RED					
CH	Canal de operación	12	12	12	12
PAN ID	Dirección de red	234	234	234	234
SC	Canales a escanear	1FFE	1FFE	1FFE	1FFE
NJ	Tiempo de asociación	FF	FF	FF	FF
DIRECCIONAMIENTO					
MY	Dirección propia	0	1	2	3
DH	Dirección de destino	0	0	0	0
DL	Dirección de destino	FFFF	0	0	0
NI	Nombre del nodo	<i>COORDINADOR</i>	<i>MONITOREO#</i>	<i>AVISO</i>	<i>REMOTO</i>
SEÑAL RF					
PL	Nivel de Potencia	4	4	4	4
PM	Modo de Potencia	1	1	1	1
INTERFAZ SERIAL					
BD	Velocidad en baudios	9600	9600	9600	9600
NB	Paridad	ninguna	ninguna	ninguna	ninguna
MODOS DE DORMIR					
SM	Modo	0	1	0	1

Tabla 4.9 Valores de los parámetros principales en cada módulo del sistema de seguridad.

4.4.5. Configuración del Microcontrolador

Uno de los objetivos principales del diseño de los módulos de monitoreo es que consuman la menor energía posible y esta característica es posible con el microcontrolador cuando trabaja con el oscilador interno de 4Mhz, es de esa manera que puede ser energizado con 3 voltios y consumir hasta 0.5uA cuando

está dormido¹¹ (configuración solo para los módulos de monitoreo y módulo de control remoto).

La manera de configurar el microcontrolador para que trabaje con a una frecuencia de 4Mhz es programando los bits de los fusibles CKSEL, el clock seleccionado es la entrada para el oscilador AVR.

Opciones para el clock del microcontrolador	CKSEL3..0
Resonador Cristal/ceramic externo	1111 - 1010
Cristal externo de baja frecuencia	1001
Oscilador RC externo	1000 - 0101
Oscilador RC interno calibrado	0100 - 0001
Clock externo	0000

Para obtener la frecuencia de 4MHZ se deberá configurar el CKSEL con el valor de **0011**. Adicionalmente, se debe configurar al microcontrolador dependiendo de la función en cada módulo.

Configuración de la comunicación serial asíncrona USART: MÓDULOS COORDINADOR, MONITOREO, AVISO Y CONTROL REMOTO.

PARÁMETROS DE CONFIGURACIÓN	DE	SUBROUTINA UsartConf
Velocidad de comunicación: 9600 bps Datos: 8 bit de datos Número de Bits de parada= 1 bit Paridad: Ninguna Interrupciones UART: Ninguna		<pre> UsartConf: push r16 ldi r16, \$02 ;u2x =1 out ucscr, r16 ldi r16, \$18 out ucscr, r16 ldi r16, \$86 out ucscr, r16 ldi r16, high(\$0c) out ubrrh, r16 ldi r16, low(\$0c) out ubrrl, r16 pop r16 ret </pre>

¹¹ Ver la sección *electrical characteristics* del manual del ATmega8

Configuración de Puertos de Entrada y Salida. MÓDULO COORDINADOR Y AVISO.

PARÁMETROS DE CONFIGURACIÓN	DE	SUBROUTINA: PortsConf
<p>PINES DE SALIDA</p> <p>PD2: Para la activación del buzzer.</p> <p>PB1: Led indicador de recepción.</p> <p>PB2: Led indicador de Transmisión.</p> <p>PINES DE ENTRADA: Ninguno</p>		<p><i>PortsConf:</i></p> <pre>push r16 ldi r16, 0b11111111 out ddrb, r16 ldi r16, 0b11111111 out ddrd, r16 pop r16 ret</pre>

Configuración de Puertos de Entrada y Salida. MÓDULO MONITOREO Y MÓDULO CONTROL REMOTO.

PARÁMETROS DE CONFIGURACIÓN	DE	SUBROUTINA: PortsConf
<p>PINES DE ENTRADA</p> <p>PD2: Interrupción externa INT0 (pin_sleep para el módulo de monitoreo, pin_sleep_encender para el módulo control remoto)</p> <p>PD3: Interrupción externa INT1 (pin_sleep_apagar solo para el módulo control remoto).</p> <p>PINES DE SALIDA: Ninguno</p>		<p><i>PortsConf:</i></p> <pre>push r16 ldi r16, 0b11110011 out ddrd, r16 pop r16 ret</pre>

Configuración de Temporizadores. MÓDULO COORDINADOR.

PARÁMETROS DE CONFIGURACIÓN	DE	SUBROUTINA: ConfTimer
<p>Temporizador de 250ms</p> <p>Modo: CTC, TIMER COMP2.</p> <p>Preescalamiento 1:1224</p> <p>Valor del registroOCR2: 244</p> <p>(1us)x1024x244=249.8ms</p>		<p><i>ConfTimer:</i></p> <pre>push r16 ldi r16, \$0f out tccr2, r16 ldi r16, \$f4 out ocr2, r16 in r16, tmsk ori r16, \$80 out tmsk, r16 pop r16 ret</pre>

Configuración de Interrupciones Externas. MODULO DE MONITOREO Y CONTROL REMOTO

PARÁMETROS DE CONFIGURACIÓN	DE	SUBROUTINA: ConfExtr
Interrupción: INT0, PIND2 Con flanco de subida		ConfExtr: push r16 in r16, MCUCR ori r16, \$03 out MCUCR, r16 in r16, GICR ori r16, \$40 out GICR, r16 pop r16 ret

4.5. Costos del diseño

En las siguientes tablas se muestran los precios de costo de cada uno de los componentes de los módulos del sistema de seguridad. Los Precios expresados en dólares americanos

MÓDULO COORDINADOR: con fuente importada

CANTIDAD	DESCRIPCIÓN	PRECIO(USD\$)
1	Xbee Series 2 PRO*	36.00
1	Microcontrolador Atmega 8	5.00
2	Resistencias	0.30
1	Regulador de voltaje LM317	0.50
1	Conector para alimentación	0.30
1	Transistor 2N3904	0.20
1	Rele	0.50
1	Diodo 1N4001	0.30
1	Buzzer marca: MCM	5.00
1	Conector para Buzzer	0.30
1	Fuente de 6 volt. marca:ELK, modelo: 624	35.00
1	Batería Sonnenschein 6Vdc	30.00
1	Fabricación de circuito impreso	4.00
	TOTAL	117.40

MÓDULO COORDINADOR: con fuente nacional

CANTIDAD	DESCRIPCIÓN	PRECIO
1	Xbee Series 2 PRO*	36.00
1	Microcontrolador Atmega 8	5.00
2	Resistencias	0.30
1	Regulador de voltaje LM317	0.50
1	Conector para alimentación	0.30
1	Transistor 2N3904	0.20
1	Rele	0.50
1	Diodo 1N4001	0.30
1	Buzzer marca: MCM	5.00
1	Conector para Buzzer	0.30
1	Fuente de 6 volt. Fabricación local	13.10
1	Batería Sonnenschein 6Vdc	30.00
1	Fabricación de circuito impreso	4.00
	TOTAL	95.50

MÓDULO DE AVISO

CANTIDAD	DESCRIPCIÓN	PRECIO
1	Xbee Series 2	25.00
1	Transistor 2N3904	0.20
1	Microcontrolador Atmega 8	5.00
2	Resistencias	0.10
1	Conector para alimentación	0.30
3	Pilas de 1.5 VAC marca: duracell	2.20
1	Fabricación de circuito impreso	4.00
1	Buzzer marca: MCM	5.00
1	Conector para Buzzer	0.30
1	Transistor 2N3904	0.20
1	Rele	0.50
1	Diodo 1N4001	0.30
	TOTAL	43.10

MÓDULO DE MONITOREO CON CONTACTO MAGNÉTICO

CANTIDAD	DESCRIPCIÓN	PRECIO
1	Xbee Series 2	25.00
1	Contacto magnetico	3.00
1	Transistor 2N3904	0.20
1	Microcontrolador Atmega 8	5.00
2	Resistencias	0.10
1	Conector para alimentación	0.30
2	Pilas de 1.5 VAC marca: duracell	1.50
1	Fabricación de circuito impreso	4.00
	TOTAL	39.10

MÓDULO DE MONITOREO CON SENSOR DE ROTURA DE VIDRIO

CANTIDAD	DESCRIPCIÓN	PRECIO
1	Xbee Series 2	25.00
1	Sensor de rotura de vidrio	13.00
1	Transistor 2N3904	0.20
1	Microcontrolador Atmega 8	5.00
2	Resistencias	0.10
1	Conector para alimentación	0.30
2	Pilas de 1.5 VAC marca: duracell	1.50
1	Fabricación de circuito impreso	4.00
	TOTAL	49.10

MÓDULO DE CONTROL REMOTO

CANTIDAD	DESCRIPCIÓN	PRECIO
1	Xbee Series 2	25.00
2	Pulsadores	0.50
2	Transistor 2N3904	0.40
1	Microcontrolador Atmega 8	5.00
2	Resistencias	0.10
1	Conector para alimentación	0.30
2	Pilas de 1.5 VAC marca: duracell	1.50
1	Fabricación de circuito impreso	4.00
	TOTAL	36.80

4.6. Comparativa de precios de venta

La siguiente tabla muestra el cálculo del precio de venta de los productos finales de la presente tesis. Estos precios son calculados agregando un margen comercial del 20%.

PRECIO DE VENTA

DESCRIPCIÓN	PRECIO DE COSTO	PRECIO DE VENTA
MÓDULO COORDINADOR	117.40	146.8
MÓDULO DE AVISO	43.10	53.9
MÓDULO DE MONITOREO CON CONTACTO MAGNÉTICO	39.10	48.9
MÓDULO DE MONITOREO CON SENSOR DE ROTURA DE VIDRIO	49.10	61.4
MÓDULO DE CONTROL REMOTO	36.80	46.0
TOTAL	285.50	356.9
GANANCIA NETA	71.38	

El cálculo del precio de venta es con un margen comercial del 20% .

En la siguiente tabla se muestra la comparación de precios de venta del producto de la tesis y uno de los productos más comercializados en internet: el sistema de seguridad inalámbrico Powermaxplus de la reconocida marca Visonic.

COMPARATIVA DE PRECIOS DE VENTA

PRODUCTOS DESARROLLADOS EN LA TESIS	PRECIO DE VENTA	PRODUCTOS POWERMAX PLUS	PRECIO DE VENTA
MÓDULO COORDINADOR	146.75	Modulo central	173.2
MÓDULO DE AVISO	43.10	Alarma externa	134.4
MÓDULO DE MONITOREO CON CONTACTO MAGNÉTICO	48.88	Sensor de puertas y ventanas	39.1
MÓDULO DE MONITOREO CON SENSOR DE ROTURA DE VIDRIO	61.38	Detector de rotura de vidrios	119.0
MÓDULO DE CONTROL REMOTO	46.00	Mando a distancia	29.8
TOTAL	346.10	TOTAL	495.6
DIFERENCIA A FAVOR	149.51		

Nota: Todos los precios son expresados en dólares americanos.

4.7. Costo de investigación del diseño del sistema de seguridad

ITEM	TIEMPO INVERTIDO
Investigación de la necesidad del sistema de seguridad (Capítulo 1)	10 horas
Elección de la mejor tecnología (Capítulo 2)	20 horas
Investigación del modo de funcionamiento de los módulos XBee (Capítulo 3)	30 horas
Diseño y pruebas del funcionamiento del sistema (Capítulo 4)	340 horas
Pruebas del sistema y mediciones del rango de cobertura (Capítulo 5)	28 horas
Total de horas empleadas	428 horas

Costo por hora-hombre:	20.00 nuevos soles
Costo total:	S/. 8,560.00 nuevos soles
Costo total:	\$ 3,003.5 dólares americanos

Ganancia por cada sistema de seguridad vendido: \$ 71.85

En resumen, la inversión de esta investigación asciende a 3003.5 dólares, mientras que la ganancia por la venta del producto es de aproximadamente 71.85 dólares, el dinero invertido en investigación se recuperaría a partir del sistema de seguridad vendido número 43.



5 PRUEBAS Y MEDICIONES

5.1. Medición de corrientes: Módulo de monitoreo

Es muy importante corroborar los cálculos de la sección 4.3.2.5 debido a que el tiempo de duración de baterías está directamente relacionado con el consumo real de corriente del conjunto de todos los componentes del módulo de monitoreo y del módulo control remoto. Se puede encontrar fácilmente el consumo del microcontrolador y XBee en las características eléctricas especificadas en sus respectivos manuales, pero existe un circuito adicional en el módulo que suma un consumo de corriente muy importante que medir.

El sensor conectado al módulo de monitoreo mantiene abierto o cerrado un contacto, este contacto **tiene un circuito que transmita el estado abierto o cerrado** en voltaje (circuito de pulso de la sección 4.3.2.3), por lo tanto se realiza la medición de corriente para el circuito que entrega los pulsos en alta y baja (3v y 0v) al microcontrolador y al XBee, de esa manera se logra dormir al **microcontrolador y al XBee** y lograr un consumo de 1.5uA entre ambos, pero a ello, se debe añadir el consumo de corriente del circuito.

Para: $R_{25} = 180 \text{ Kohm}$ y $R_{32} = 180 \text{ Kohm}$.

MEDICIONES:

Sensor Desactivado: Contacto cerrado

$I_{SC} = 15\mu\text{A}$, corriente del circuito de pulso cuando el terminal del sensor está cerrado.

$I_{Xbee} = 1\mu\text{A}$, corriente del XBee en modo dormido (valor teórico).

$I_{UC} = 0.5\mu\text{A}$, corriente del Microcontrolador en modo dormido (valor teórico).

$I_{TOTAL} = 16.5\mu\text{A}$.

Sensor Activado: Contacto abierto

$I_{SA} = 27\mu\text{A}$, corriente del circuito de pulso cuando el terminal del sensor está abierto.

$I_{Xbee} = 45\text{mA}$, corriente del Xbee en modo ocioso/recepción (valor teórico).

$I_{UC} = 5\text{mA}$, corriente del Microcontrolador (valor teórico).

$I_{TOTAL} = 50.027\text{mA}$.

Dispositivos fijos:

Una computadora IBM Pentium IV (256MB RAM) con Windows XP con un puerto serial.

Una interfaz RS 232 entre el XBee y el puerto COM1.

Una fuente de alimentación de 9 Vdc.

Cable de comunicación serial.

Un XBee Series 2: módulo de monitoreo.

Dispositivo Móvil:

Un XBee Series 2 Coordinador con circuito loopback (cortocircuito entre DIN y DOUT).

Un protoboard.

04 pilas alcalinas de 1.5v duracell.

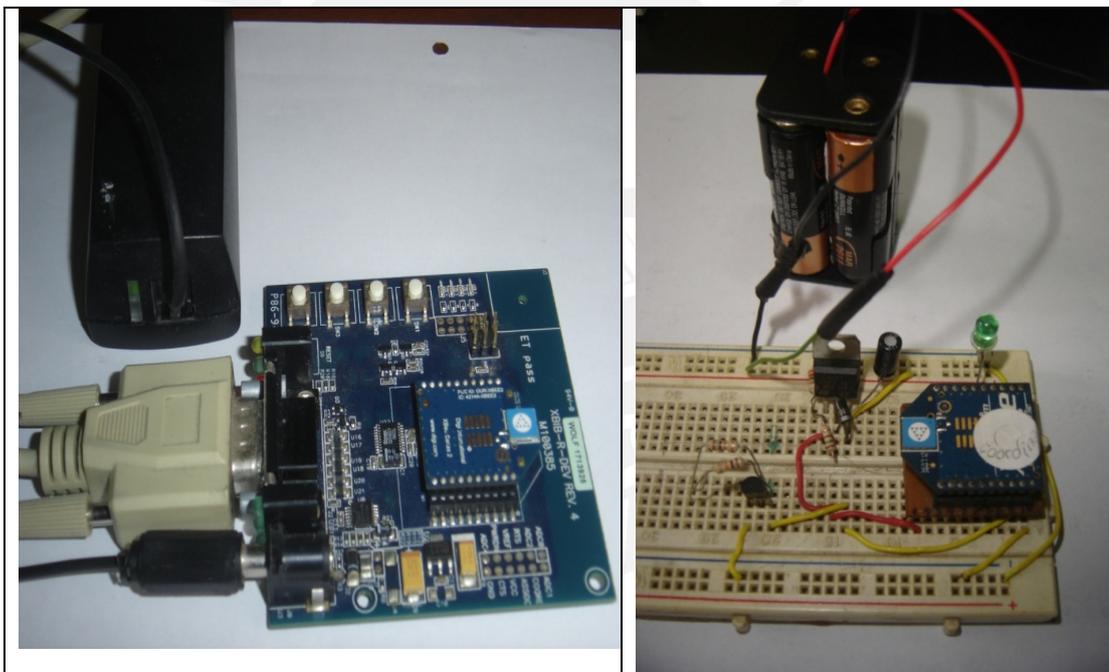


Figura 5.2 Izquierda: XBee de monitoreo conectado serialmente a la PC mediante la Tarjeta RS-232 Development Board Part # XBIB-R. Derecha: XBee coordinador con sus baterías, es el dispositivo móvil en las ubicaciones 1, 2, 3, 4, 5, 6 y 7 de la **Tabla 5.3** y la **Figura 5.5**.

A continuación se detallaran cada uno de los pasos para realizar esta prueba de rango y obtener como resultado la calidad de señal recibida versus la distancia entre módulos XBee.

5.3.1. Configuración previa

Previamente a las pruebas entre el coordinador y un módulo de monitoreo se escriben los siguientes parámetros (en el XCTU) para que primero puedan comunicarse.

<u>COORDINADOR</u>	<u>MONITOREO1</u>
ATNI COORDINADOR	ATNI MONITOREO1
ATDL 0xFFFF	ATDN COORDINADOR
ATND	ATND
2B62	0000
0013A200404A62A9	0013A200400A336E
MONITOREO1	COORDINADOR
FFFE	FFFE
01	00
00	00
C105	C105
101E	101E
ATWR	ATWR
ATCN	ATCN

Tabla 5.1 Resultados de la configuración previa a la prueba de rango.

Leyenda:

Comando ATNI: indica el nombre que se le pondrá al dispositivo, para el ejemplo se utilizaron los nombres coordinador y monitoreo.

Comando ATDL: determina el nodo de destino, en el caso del coordinador el valor 0xFFFF indica el nodo de destino como *broadcast* es decir *para todos* los dispositivos de la red.

Comando ATND: tiene como significado *node discovery*, muestra y reporta todos los Xbee encontrados. La siguiente información se mostrará por módulo Xbee encontrado.

RESULTADO	DESCRIPCION
2B62	MY: Dirección propia
0013A200404A62A9	SH: Número de serie(bits más significativos)
--	SL: Número de serie(bits menos significativos)
MONITOREO1	NI: Nombre del dispositivo (Variable length)
FFFE	PARENT_NETWORK ADDRESS (2 Bytes)
01	DEVICE_TYPE (1 Byte: 0=Coord, 1=Router, 2=End Device)
00	
C105	STATUS (1 Byte: Reserved)
101E	PROFILE_ID (2 Bytes)
	MANUFACTURER_ID (2 Bytes)

Tabla 5.2 Resultado de la ejecución del comando ATND en el módulo coordinador

Comando ATWR: con este comando se graban todas las configuraciones y cambios de parámetros en el XBee.

Comando ATCR: se sale del modo de configuración: *comando*.

5.3.2. Prueba de comunicación entre dispositivos

Se necesita realizar una prueba de comunicación antes de hacer la prueba de rango, para ello se utiliza el *loopback* (como está indicado en el manual de pruebas de rango) esta prueba se consigue cortocircuitando los pines DIN y DOUT en el XBee Coordinador que se podía mover por distintos ambientes de la casa, es decir el XBee que no está conectado en la computadora.

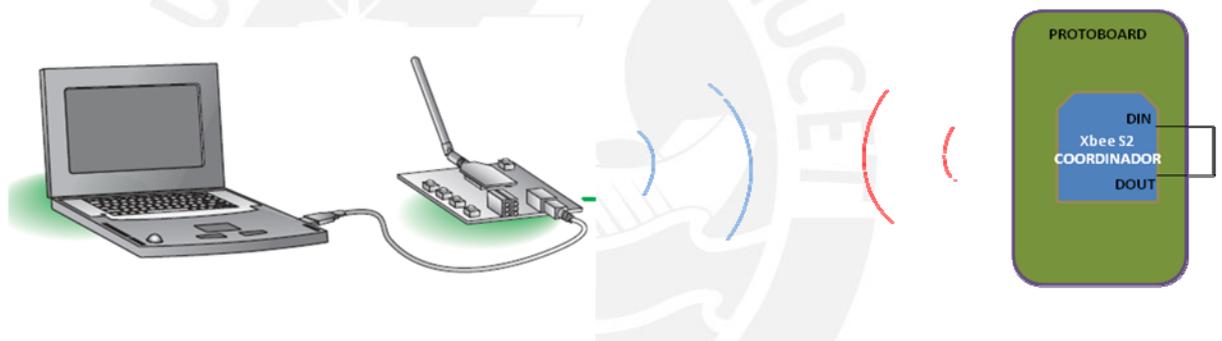


Figura 5.3 Dispositivos que intervienen en la prueba de rango. Izquierda Tarjeta RS-232 Development Board Part # XBIB-R con el XBee de Monitoreo con loopback. Derecha: Protoboard que contiene al XBee Coordinador.

La siguiente figura muestra la ventana *terminal* del programa XCTU, en este ventana se observa que todos los caracteres emitidos por el módulo de monitoreo (escritos por el usuario de color azul) son enviados inalámbricamente hasta el módulo coordinador y este (por medio del loopback) procede a devolverlos hacia el módulo de monitoreo, estos caracteres recibidos se muestran de color rojo.

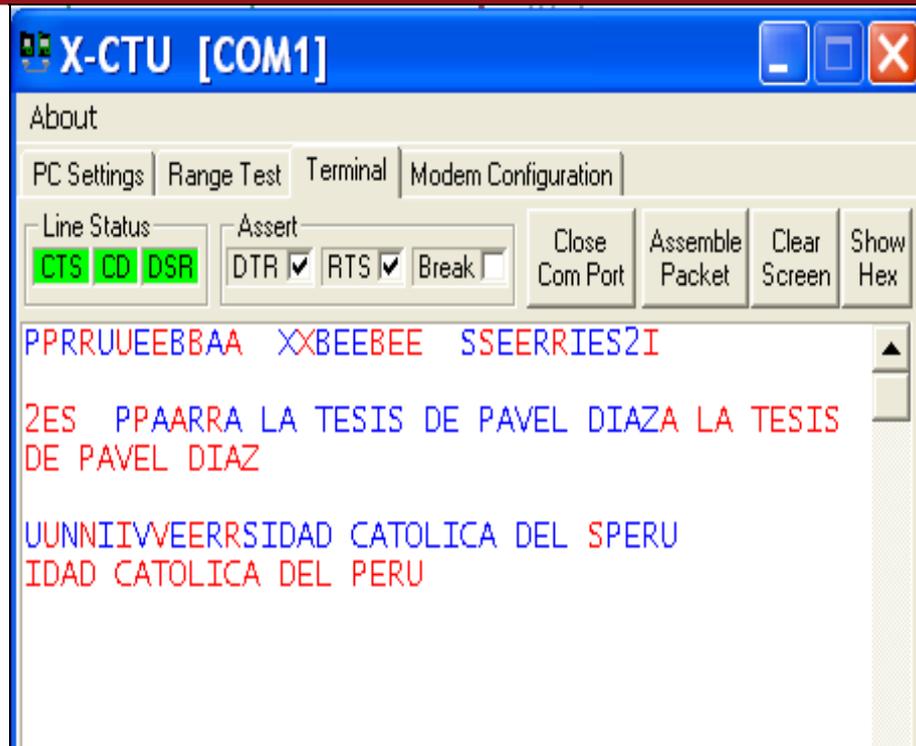


Figura 5.4 Verificación del loopback, en azul los caracteres emitidos desde el XBee de monitoreo y en rojo los mismos caracteres pero enviados desde el XBee coordinador mediante el loopback. ***Se tipeó rápidamente para observar la rapidez de la transmisión.***

5.3.3. Ubicaciones de los dispositivos de prueba

En la siguiente figura se detallan todas las ubicaciones de prueba de los 02 Xbee. El Coordinador que es el dispositivo móvil simbolizado por números del 1 al 7 correspondiente al número de la prueba. El XBee de monitoreo se ha quedado en la misma posición debido a que está conectado a una computadora de escritorio, esta simbolizado con M. Nota: todas las distancias están en metros. El plano de la vivienda que se muestra en la figura es una casa tradicional de 120m² en donde el **grosor de las paredes es de hasta 0.29metros.**

Asimismo se especifican las distancias desde el Xbee de monitoreo hacia cada una de las ubicaciones del coordinador. En esta figura se puede apreciar de mejor manera en número de paredes por cada enlace entre dispositivos.

Se considera la coordenada (0,0) a la ubicación fija del XBee de monitoreo (M).

La siguiente tabla muestra las distancias que se han logrado alcanzar en las 7 pruebas, de esto se obtiene que se puede tener un rango de alcance de hasta de 9 metros con 2 paredes de hasta 0.29 metros de grosor en el medio.

Ubicación del Xbee Coordinador móvil	Distancia entre dispositivos (Línea de vista en metros)	Número de paredes	RSSI ¹² (dBm)	%Recepción ¹³
1	1.00	0	-47	100
2	5.00	0	-58	100
3	4.33	2	-60	100
4	8.49	3	-82	93.8
5	12.46	3	-104	0
6	9.20	2	-82	95
7	8.03	3	-82	93.5

Tabla 5.3 Resultado de las pruebas para cada una de las ubicaciones del XBee coordinador (1, 2, 3, 4, 5, 6 y 7) con respecto al XBee de monitoreo (M)

La siguiente figura muestra una de las pruebas de rango vista desde el programa XCTU, para esta prueba especifica el porcentaje de paquetes comunicados exitosamente es del 93.5% entre el módulo coordinador y el módulo de monitoreo usando *loopback* (descrito en la sección 5.3.2) distanciados 8.03 metros (prueba número 7).

¹² **RSSI**: Indicador de la potencia de la señal recibida por el XBee monitor (M).

¹³ **%Recepción**: Muestra la relación entre la totalidad de mensajes enviados y los recibidos por el mismo XBee de monitoreo (M).

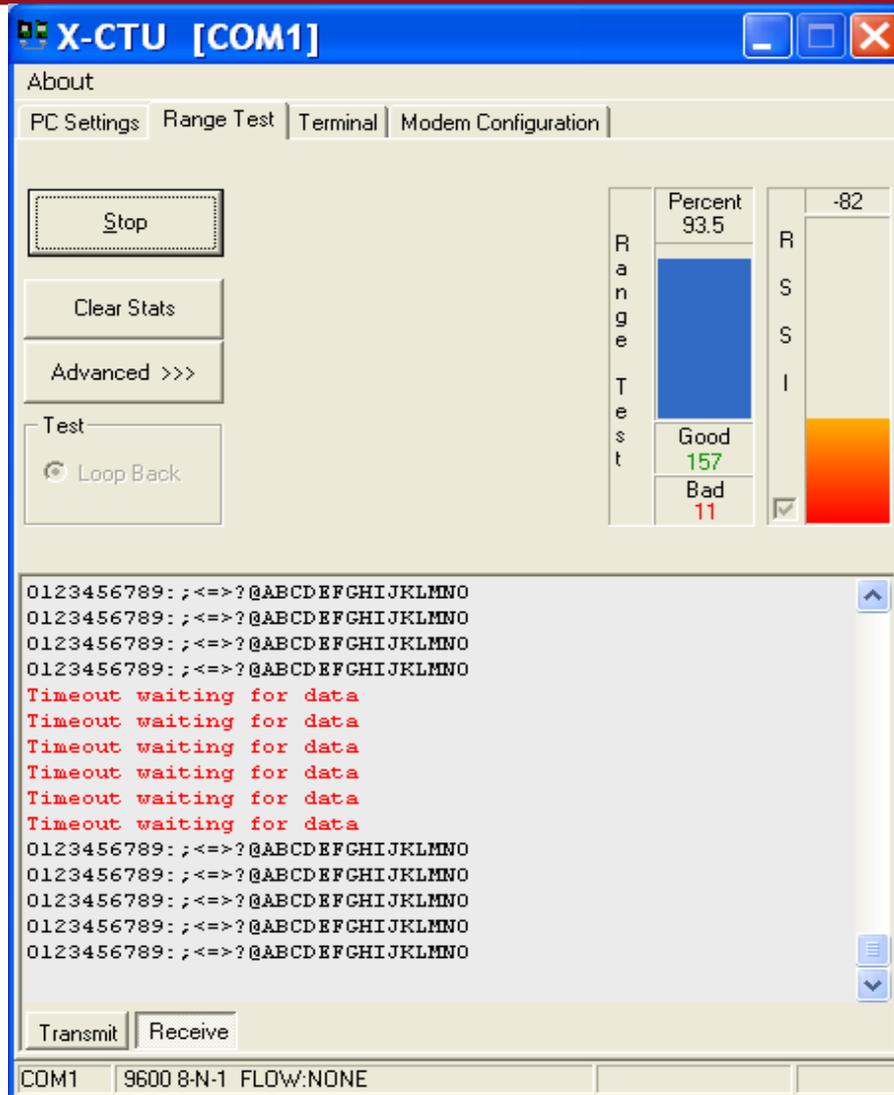


Figura 5.6 Test de Rango del programa XCTU, vista de la prueba número 7.

5.4. Conclusiones de las pruebas

A pesar de que las pruebas se realizaron con las siguientes restricciones:

5. Paredes de hasta 0.3 m de ancho.
6. Uso de un Xbee Series 2 convencional y no Xbee Series 2 PRO como módulo coordinador, el cual se propone en la tesis y en la lista de dispositivos electrónicos que forman parte del módulo coordinador.

Se obtiene un rango de alcance de comunicación de **hasta 9.2 metros con 2 paredes (prueba 6) o de 8.5 metros con 3 paredes (prueba 4)**.

Tal como se define en la sección 4, el sistema de seguridad diseñado en la presente tesis deberá usar un Xbee Series 2 PRO en el módulo del coordinador,

de esa forma podremos ver incrementado significativamente el rango de cobertura y el sistema puede ser aplicado incluso en viviendas más grandes.

5.4.1. Ubicación de dispositivos en el departamento

Para poder implementar el sistema de seguridad en el departamento elegido en la sección 4.1.2. se debe referir a la Tabla 5.3, de donde se desprende información muy relevante cuando se trata de ubicar dispositivos en el departamento. Según las conclusiones de las pruebas se puede transferir información con un 93% de seguridad con dispositivos distanciados hasta 9.2 metros con 2 paredes o de 8.5 metros con 3 paredes, conforme a ello se ubican los dispositivos del sistema de seguridad en las áreas inseguras detectadas en el departamento elegido (sección 4.1.2.).

Ubicación del módulo de monitoreo	Distancia de línea de vista(m) con respecto al coordinador	Número de paredes
Balcón: módulo de monitoreo contacto-módulo coordinador.	6.2	2
Puerta de ingreso: módulo de monitoreo contacto-módulo coordinador.	7.3	3
Dormitorio 3: módulo de monitoreo rotura de vidrio - módulo coordinador.	6.4	2
Dormitorio2: módulo de monitoreo rotura de vidrio - módulo coordinador.	4.1	1
Dormitorio principal: módulo de monitoreo rotura de vidrio - módulo coordinador.	6.2	2

Tabla 5.4 Resultado de la medición de distancias entre el coordinador y el resto de módulos de monitoreo

De la Tabla 5.4 se observa que la mayor distancia de comunicación entre dispositivos es de 7.3 metros (con 3 paredes en medio de la transmisión), y de las pruebas anteriores (Tabla 5.3) se concluye que este rango está dentro del mayor rango apropiado igual a 8.5 metros (con 3 paredes). Se asegura entonces una comunicación garantizada mayor al 93% de efectividad registrado.



Figura 5.7 Ubicación de los módulos de monitoreo y coordinador en el departamento.

CONCLUSIONES

1. El sistema de seguridad diseñado en la presente tesis asegura el cumplimiento de las condiciones descritas en la sección 2.3, las cuales describen características esenciales de: bajo costo (ver sección 4.5), bajo consumo de

energía (ver secciones 4.3.2.7 y 4.3.4.3), estética: es libre de cables y su tamaño es reducido (ver figuras: 4.5, 4.6 y 4.7), transportabilidad: es un sistema inalámbrico que se desinstala con sencillez y puede llevarse en caso de mudanza, bajo mantenimiento: al no tener cableado no se requieren reajustes y se elimina el riesgo de corte de cables por delincuentes, sencillez de uso para el cliente: el sistema tiene un control remoto de solo 2 botones, seguridad: cuenta con el respaldo de la tecnología IEEE 802.15.4 y ZigBee para las transmisiones y retransmisiones con CSMA-CA.

2. El sistema de seguridad contiene elementos esenciales como: el módulo coordinador, diferentes módulos de monitoreo: sensor de rotura de vidrio, contactos magnéticos y el módulo control remoto. Opcionalmente el sistema de seguridad también acepta la integración de un módulo de aviso para alertar en la zona común piso del departamento.
3. Se pueden agregar **hasta 8 módulos de monitoreo** por cada módulo Coordinador o Router. Eso quiere decir que no hay un número limitado de controles remotos, módulos de monitoreo o de aviso.
4. El módulo de monitoreo mayormente usado será el de la puerta de ingreso, y para este caso se ha calculado que la duración de sus baterías será 10 meses siendo energizado con dos pilas AA Duracell. Para el módulo de rotura de vidrio la duración de la pila sería bastante larga.
5. Las transmisiones en línea de vista entre los módulos de seguridad están aseguradas mediante las pruebas realizadas en el capítulo 5, estas aseguran un rango de hasta 8.3 metros cruzando 3 paredes de hasta 29cm de espesor cada una.
6. Los módulos de monitoreo diseñados se pueden adaptar fácilmente a cualquier sensor de seguridad que tenga contactos NA/NC (ver la sección 4.3.2.3). Se puede ampliar la gama de sensores de seguridad y diseñar módulos de monitoreo con sensores de presencia, sensores de humo, etc.

RECOMENDACIONES

1. Realizar el diseño y las pruebas de implementación del módulo de ruteo, este serviría para extender la señal de alarma hacia un módulo de aviso ubicado

por ejemplo en el cuarto de seguridad del edificio o en la caseta de guardianía más cercana. Para ello se recomienda utilizar un módulo de radiofrecuencia XBee series 2 del tipo PRO y realizar pruebas de rango o cobertura de la señal.

2. Se recomienda implementar y realizar las pruebas del caso con fuente descrita en la sección 4.3.1.3, de esa manera se reduciría el costo del módulo coordinador **en USD\$ 21.9.**
3. Realizar el diseño e implementación de un módulo que convierta las señales de alerta en tramas Ethernet para enviarlas a través de Internet hacia la comisaría más cercana por medio. Se recomienda utilizar la mejor aplicación con el dispositivo ConnectPort X, totalmente compatible con el módulo XBee series 2. Adicionalmente se deberá de diseñar e implementar un sistema de monitoreo remoto en la comisaría.
4. Mediante los contactos secos NA/NC de los módulos de monitoreo se pueden conectar otros tipos de sensores domóticos como de control de luminarias, o de persianas. Se recomienda diseñar física y lógicamente el trabajo de un sistema más completo que incorpore ahorro energético y confort adicionalmente al sistema de seguridad.
5. Se necesita hacer un flujo de caja en función a las horas hombre invertidas en la investigación, al precio de costo y al margen comercial, para calcular el retorno de inversión de la presente tesis; así como el análisis de la demanda del mercado, un plan de manufactura y un plan de marketing para impulsar la venta del producto.

BIBLIOGRAFÍA

[1]

- CONASEC
2003 *Plan Nacional del Sistema de Seguridad Ciudadana.*
Consulta: 19 de Octubre de 2006.
<http://www.seguridadidl.org.pe/sistema.htm>
- [2]
PANIAGUA, Alberto
2006 *¿Donde estamos? 10 temas clave de cara a las elecciones 2006.* Lima: Nova Print SAC. Consulta: 15 Mayo 2009.
www.transparencia.org.pe/documentos/01_competitividad.pdf
- [3]
ASOCIACION NACIONAL DE ALGUACILES
2001 *Prevención de Robos Caseros-Cómo Proteger su Hogar.* Alexandria, Virginia. Consulta: 26 de Octubre de 2006.
www.usaonwatch.org/assets/.../ProtectYourHome_Espanol.pdf
- [4]
RODRIGUEZ, Eduardo.
2004 *Domótica*, Lima. Consulta: 5 de Noviembre de 2006.
<http://sipan.inictel.gob.pe/internet/tx/domotic.htm>
- [5]
DOMOTICA.NET
2006 *La Asociación Konnex: Principales Ventajas*, Consulta: 5 de Noviembre del 2006. <http://www.domotica.es/knx>
- [6]
INTERACT
2000 *Lonwork*. Consulta: 5 de Noviembre de 2006.
<http://odisea.ii.uam.es/esp/recursos/Lonwork.htm>
- [7]
SIMELEC
2005 *Sistemas De Control : Tecnologías, Sistemas y Normativas.* Comisión HogarDigital. Madrid : CHD, 2005, Vol. GT2 v1. Consulta: 5 de Noviembre del 2006
<http://www.coit.es/pub/ficheros>
- [8]
DOMOTICA 365
2009 *Sistemas Inalámbricos*. Consulta: 3 de OCTubre del 2009.

<http://www.domotica365.com/domotica-sistemas-inalambricos-vsubservicios-1318.html>

[9]

MAYNE, Jordi

2005

IEEE 802.15.4 y ZigBee. Consulta: 12 de Noviembre 2006

www.bairesrobotics.com.ar/data/ieee_zigbee_silica.pdf

[10]

Valverde, Jorge

2005

El Estándar Inalámbrico ZigBee. Consulta: 15 de Marzo

2010. <http://www.seccperu.org/files/ZigBee.pdf>

[11]

MILLENIUM TECHNOLOGIES

2005

Hometronic: Hogares que piensan en ti. Consulta: 20

Febrero 2008

http://www.gonzaloarechavala.com/millennium/catalogo_hometronic.pdf

[12]

SUPER INVENTOS

2008

Sistemas de Alarmas X10. Consulta: 20 Febrero del

2008. <http://www.superinventos.com/seguridadx10.htm>

[13]

CASAINTELIGENTE EUROPA S.L.

2008

¿Qué tecnología domótica necesito?. Consulta: 29 Febrero

del 2008. <http://www.bovestreet.com/info/tecnologia.php>

[14]

GEER, David

2005

Users make a Beeline for ZigBee sensor technology. IEEE

Computer Society. Vol. 38, no. 12, pp. 16-19 Consulta: 17

de Marzo del 2009. <http://www2.computer.org>

[15]

TELECOM PRODUCTS

2008

ZigBee product and application ranges expand as adoption picks up. Consulta: 17 de Marzo del 2009.

http://www.telecom.globalsources.com/gsol/I/Mobile_wireless/a/9000000100588.htm

[16]

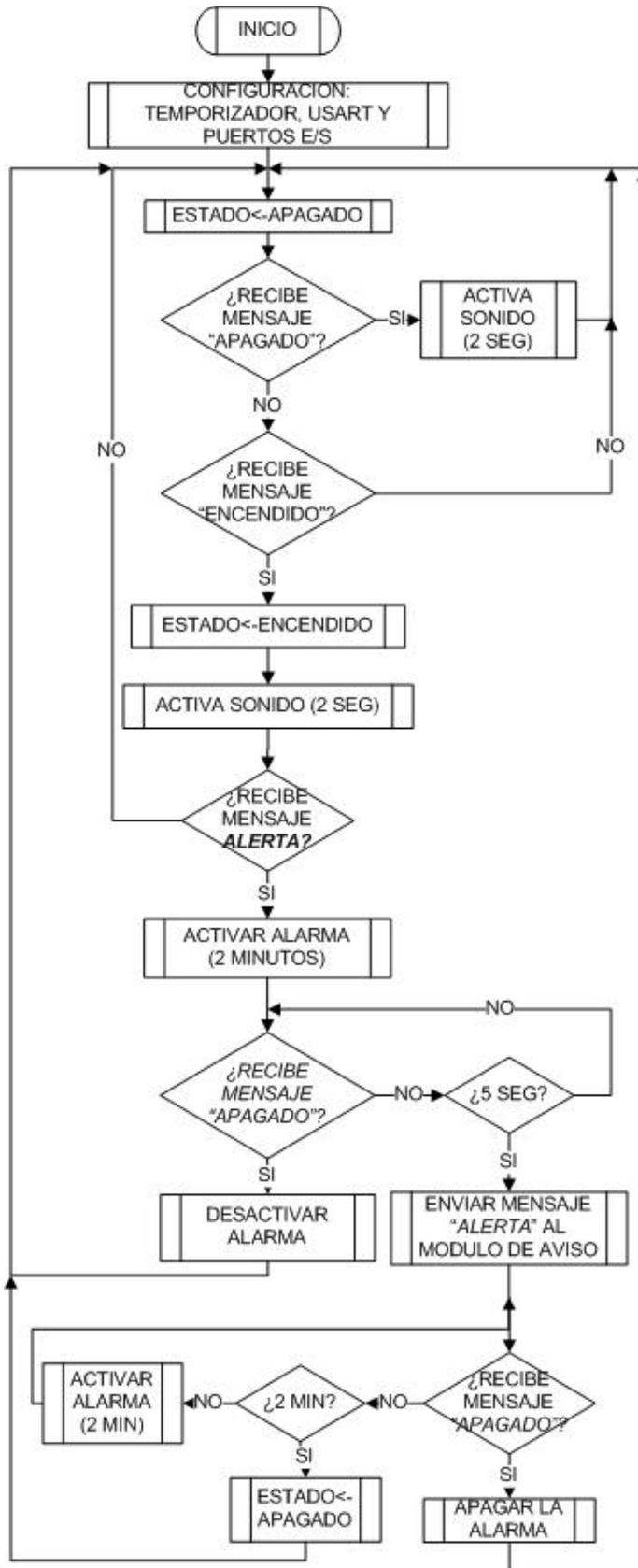
- TI
2009 *Texas Instrument CC2520*. Consulta: 27 de Setiembre del 2009. <http://focus.ti.com/docs/prod/folders/print/cc2520.html>
- [17]
Freescale
2009 *Freescale, MC13192*. Consulta: 27 de Setiembre del 2009. http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=MC13192
- [18]
Ember
2009 *Ember EM250*. Consulta: 29 de Setiembre del 2009. [http://www.ember.com/pdf/120-4024-000_EM250UserGuide.pdf#search="em250"](http://www.ember.com/pdf/120-4024-000_EM250UserGuide.pdf#search=)
- [19]
Microchip
2009 *Microchip: MRF24J40*. Consulta: 29 de Setiembre del 2009. <http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en027752>
- [20]
Atmel
2009 *Atmel: AT86RF230*. Consulta: 01 de Octubre del 2009. http://www.atmel.com/dyn/products/product_card.asp?part_id=3941
- [21]
Meshnetics
2009 *Meshnetics: Measuring range performance of ZigBit Amp*. Consulta: 03 de Octubre del 2009. <http://www.meshnetics.com>
- [22]
Jennic
2009 *Jennic Web*. Consulta: 03 de Octubre del 2009. <http://www.jennic.com>
- [23]
NOVAK, Petr

- 2008 *El uso de comunicaciones inalámbricas en las pequeñas redes médicas.* Praga : EIKA, 2008. Consulta: 10 de Diciembre del 2008.
- [24]
Digi International
2008 *Xbee ZigBee Networks. XBee™ ZNet 2.5/XBee-PRO™ ZNet 2.5 OEM RF Modules Manual.* Minnetonka : s.n., 2008. v1.x.4x. pag22. Consulta: 17 de Mayo del 2009.
<http://www.digi.com/products/wireless/zigbee-mesh/>
- [25]
Digi International
2009 *XBee Series 2 firmware revision history.* Minnetonka : s.n., Consulta: 17 de Mayo del 2009
www.digi.com/support/kbase
- [26]
Atmel
2007 *Manual del ATmega8 y ATmega88.* Consulta: 25 de Octubre del 2008. www.atmel.com/literature
- [27]
ELK Products
2006 *Power Supply and Battery Charger ELK-P624.* Consulta: 17 de Mayo del 2009. <http://www.elkproducts.com/pdf/P624-instructions.pdf>
- [28]
Sonnenschein
2006 *Battery 6v, 1.2mAH.* Consulta: 20 de Junio del 2009
<http://es.farnell.com>
- [29]
MCMElectronics
2006 *Solid State Electronic Buzzer - 12VDC* Consulta: 08 de Junio del 2009.
<http://www.mcmelectronics.com/product/DISTRIBUTED-BY-MCM-28-1650-/28-1650>
- [30]
KEC

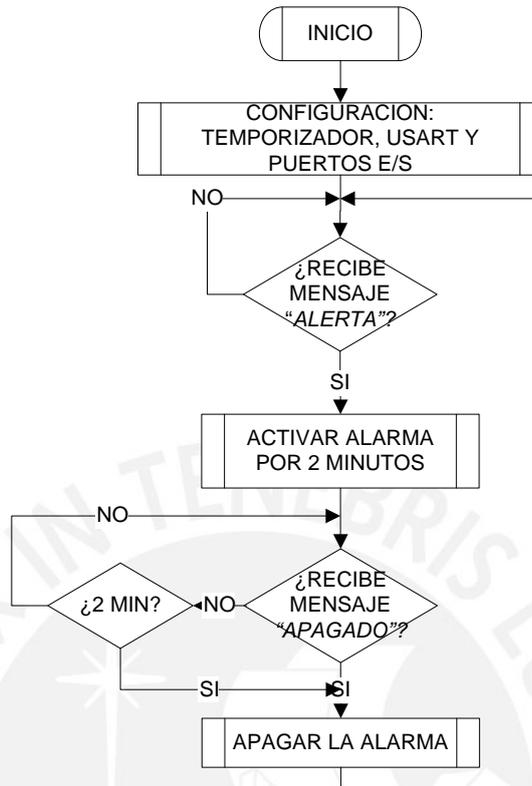
- 2002 *2N3904 Semiconductor technical data*. Consulta: 17 de Marzo del 2009.
<http://www.datasheetarchive.com/datasheet-pdf/018/DSA00306639.html>
- [31]
Window Bugs
- 2002 *USP Window Bug Glass Break Detector (White)*. Consulta: 17 de Marzo del 2009.
<http://www.homesecuritystore.com/p-166-724-usp-window-bug-glass-break-detector-white.aspx>
- [32]
Duracell
- 2002 *Duracell. Alkaline-Manganese Dioxide*. Consulta: 17 de Marzo del 2009. <http://www1.duracell.com/oem/Pdf/ATB-full.pdf>
- [33]
SAFT
- 2009 *LS-14500 AA 3.6V lithium battery*. Consulta: 17 de Marzo del 2009. <http://www.batteryjunction.com/plc-ls14500-ba.html>
- [34]
Atmel
- 2007 *Manual ATmega88: ADC Voltage Reference*. Pag. 253. Consulta: 25 de Abril del 2009. www.atmel.com/literature
- [35]
DIGI
- 2009 *How to perform a range test*. Consulta: 20 de Febrero del 2009.
http://ftp1.digi.com/support/documentation/90001067_a.pdf

ANEXO 1: DIAGRAMAS DE FLUJO DEL SISTEMA DE SEGURIDAD

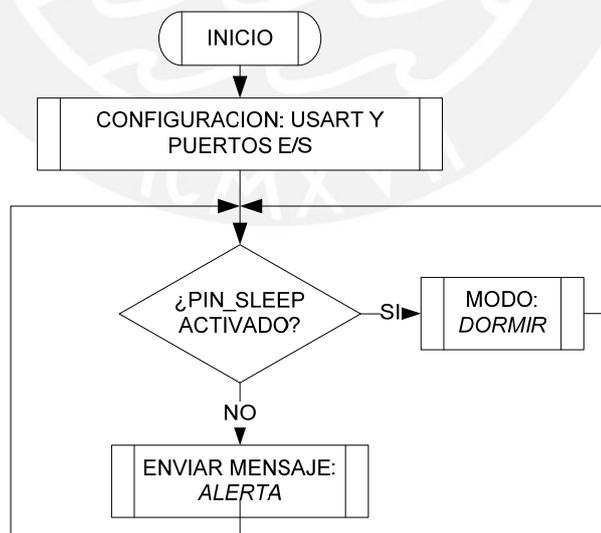
MÓDULO COORDINADOR



MÓDULO DE AVISO



MÓDULO DE MONITOREO



MÓDULO DE CONTROL REMOTO

