Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica.

TRABAJO DE DIPLOMA

Propuesta de diseño de MODEM de RF.

Autor: Luis Enrique Velázquez Velázquez.

Tutor: Msc. Alain Sebastián Martínes Laguardia

.

Santa Clara

2008

"Año 50 de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Propuesta de diseño de MODEM de RF.

Autor: Luis Enrique Velázquez Velázquez.

levelazquez@uclv.edu.cu

Tutor: Msc. Alain Sebastián Martínes Laguardia

alaguardia@uclv.edu.cu

Santa Clara

2008

"Año 50 de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Eletrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Autor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

En la ciencia no hay calzadas reales, y sólo tendrán esperanzas de acceder a sus cumbres luminosas aquellos que no teman fatigarse al escalar por senderos escarpados.

Karl Marx; Londres, Marzo 18 de 1872.

DEDICATORIA

Con mucho cariño, para mis abuelos, como un importante paso en pro de la “casa de placa” que siempre prometí; a mi papá por confiar siempre en su “ingeniero”; a mi mamá y a mi hermana por ser siempre su niño lindo, a mi tía y mis primos por quererme tanto, a todos aquellos que se vieron comprometidos algún día en mi formación como buen ser humano y muy especial a mi novia por su eterna paciencia, a todos ellos, les dedico éste, mi modesto esfuerzo.

AGRADECIMIENTOS

A mi tutor, por ser más que eso, un amigo; a mi buen amigo Yoandy porque sin su ayuda no hubiera sido posible; a Mercedes y mis queridos suegros por su valioso aporte; a mi eterno profesor de marxismo, José A. Chang, porque ¿qué es sino la vida una eterna política? y a mis insuperables, nuevos y viejos amigos porque con sus risas hicieron esta etapa de mi vida inolvidable; a todos ellos ¡muchas gracias!

TAREA TÉCNICA

1. Estudiar los sistemas de detección de anomalías.
2. Describir las principales técnicas de detección de anomalías en red.
3. Estudiar los principales criterios existentes para lograr un análisis de red eficiente.
4. Estudiar las principales características del lenguaje PHP. Profundizar en las relacionadas con el trabajo a nivel de red.
5. Diseñar el software usando las funciones de PHP anteriormente seleccionadas y un soporte Web para este, capaz de lograr la interacción en la red necesitada.
6. Adicionar prestaciones a la herramienta como ejecución de tareas programadas como respuesta.
7. Poner a prueba la herramienta implementada, utilizando las pruebas creadas, con el objetivo de verificar sus potencialidades y validar su aplicación.
8. Confrontar los resultados, del período de prueba, con criterios de expertos y si es posible con otras aplicaciones (o los resultados de dichas aplicaciones), que empleen técnicas similares.
9. Documentar el sistema con el objetivo de su comprensión por parte de los posibles operadores de la herramienta y de los desarrolladores de aplicaciones similares, extendiendo así su valor teórico-práctico.

Firma del Autor

Firma del Tutor

RESUMEN

El uso actual de computadoras interconectadas a través de una red se hace imprescindible. Mantener una adecuada gestión de dicha red para su correcto funcionamiento es objetivo fundamental de todo administrador, para este propósito puede ser muy útil una herramienta que sea capaz de analizar el comportamiento en tiempo real, así como llevar un historial de todos los cambios ocurridos, gestión de ancho de banda, conectividad de equipos entre otras prestaciones acerca de la red en cuestión. Existen en la actualidad diversidad de herramientas y técnicas dedicadas al monitoreo de la red y a la detección de anomalías. Una adecuada clasificación y comprensión de las mismas puede apoyar la gestión de redes, al documentar que técnica emplear en cada escenario. En este marco se desarrolla el presente trabajo, en el cual se estudian diversos métodos empleados para la detección de anomalías y el monitoreo de la red proponiendo una herramienta capaz de monitorear determinados dispositivos de la red (lista negra), con la cual podamos especificar bien las deficiencias y anomalías a resolver o determinar fraudes en la red como cambios de IP o incremento de flujo que entorpecen el correcto funcionamiento de la red.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Hoy en día, Internet junto con las redes corporativas juega un mayor papel en la creación y avance de vías de aprendizaje y negocios. En este sentido se necesita tener compañías y gobiernos motivados a través de todo el mundo para desarrollar sofisticadas y complejas redes de información. Tales redes contemplan diversas series de tecnologías, incluyendo almacenamiento de datos distribuidos, técnicas de encriptación y autentificación, voz y video sobre IP, accesos remotos e inalámbricos y servicios Web, permitiendo una mayor accesibilidad para logar la interacción directa con todos los servicios que se ofrecen.

Todos estos aspectos hacen a las redes de hoy muy vulnerables a los ataques así como a los intrusos. Ejemplo; en la encuesta anual de seguridad y cibercrimen del 2005, realizada por el Computer Security Institute y el FBI en los Estados Unidos, se señaló que las pérdidas financieras debido a ataques e intrusiones en sus redes corporativas fueron de alrededor de los $130 millones de dólares [1].

Según los estudios recientes de veinte a cuarenta nuevas vulnerabilidades en redes y productos de computadoras comúnmente usados son descubiertos como promedio cada mes. Tales vulnerabilidades provocan una inseguridad en el ambiente de la informática y sistemas de redes. Todo este ambiente de inseguridad ha dado origen al desarrollo en todo el mundo, del campo de la prevención y detección de intrusos, o sea a la elaboración de sistemas de detección de intrusos para complementar el trabajo de los firewall (cortafuego).

Estos sistemas de detección de intrusos de red (NIDS) pueden clasificarse ya sea como la detección de firmas (huellas) o de anomalías en red. El enfoque basado en las firmas, que es generalmente sobre la base de firmas ya conocidas de ataques o vulnerabilidades, es ampliamente desplegado en diversos productos de la industria de seguridad. Mientras la detección de anomalías, que trata de identificar los ataques basados en los perfiles de

actividades normales de la red, se encuentra todavía, en muchos aspectos, en fase de investigación.

Anomalía de red típicamente se refiere a las circunstancias cuando las operaciones de red se apartan de la conducta normal de esta. Las anomalías pueden surgir debido a diversas causas, tales como mal funcionamiento de los dispositivos de red, la mala configuración en los servicios de red y sistemas operativos, la sobrecarga de la red, ataques maliciosos de denegación de servicio, aplicaciones no recomendadas instaladas por los usuarios, un elevado nivel de esfuerzo de los usuarios para descubrir la red y recabar información sobre la misma y sus dispositivos y las intrusiones que perturban la prestación normal de servicios de red. Estos eventos anómalos perturban el comportamiento normal de algunos datos mensurables de la red.

La definición de la conducta normal para medir los datos de la red depende de varios factores específicos tales como la dinámica de la red estudiada en términos de volumen de tráfico, tipo de datos de red disponibles, y los tipos de aplicaciones que se ejecutan en la red. Diversas son las técnicas empleadas por los sistemas de detección de anomalías y muchas de ellas se encuentran documentadas en nuestros días, una revisión de las principales abordando sus ventajas e inconvenientes puede ser realizable y constituirá de relevante interés en dicho campo de investigación.

Como resultado final de todas estas técnicas, seria presumiblemente, un “lista negra” que incluye un conjunto de computadoras o usuarios los cuales serian presuntos agentes de comportamiento anómalo, lograr un constante chequeo de estos seria de vital importancia para conocer su actividad y avisar a los autoridades pertinentes para una completa gestión de seguridad de red. Técnicas existentes de monitoreo de red son muchas, lograr la utilización de una de estas en pro de dicho asunto seria de notable ayuda para los encargados de mantener el correcto funcionamiento de su correspondiente red de computadoras.

Precisamente, en ese sentido se dirige el trabajo que aquí se presenta, en cual se aborda en el capítulo 1 el estudio y descripción de las técnicas existentes para la detección de anomalías y de intrusos como un aspecto general. Se revisa el estado del arte de estos, se describe y se toma decisiones en cuanto a sus ventajas e inconvenientes. En el capítulo 2 se

describe y analiza detalladamente las principales técnicas usadas en desarrollo de sistemas de detección de anomalías. Observando sus particularidades y su aplicabilidad en nuestro entorno de trabajo. Ya en el capítulo 3 de propone el diseño de la aplicación de monitorización específica de dispositivos de red abordando las posibles implicaciones, se implementa el sistema de análisis de red realizando pruebas que sustenten su aplicabilidad y la validación de los resultados, terminando así con la documentación de dicho Sistema.

Capitulo 1: CONCEPTOS GENERALES.

1.1 Introducción.

El presente capítulo está dedicado a realizar un análisis de los conceptos más generales de los MODEMs. Dicho análisis incorpora los antecedentes históricos, una caracterización de la MODEM; así como una descripción del estado del arte a nivel mundial.
Se hará una referencia de los principales productores y una muestra de los productos que se venden el mercado.

1.2 LINEAS A 2 ó 4 HILOS.

Una línea a 4 hilos (4W) es un par de líneas de 2 hilos (2W), una par para transmitir y un para recibir, de esta forma es posible mantener separadas las señales que van en direcciones diferentes. En algunos casos se combinan líneas 4W con 2W, el elemento que permite unir los dos tipos de líneas se llama transformador híbrido.

1.3 LINEAS DEDICADAS Y CONMUTADAS.

Las líneas privadas, dedicadas, arrendadas o punto a punto (usualmente 4W) están disponibles todo el tiempo para el uso exclusivo entre dos modems. Si el medio de transmisión es una línea telefónica, las características de esta línea serán garantizadas y usualmente estables. Si el medio de transmisión incluye radio-enlaces, la calidad será variable como en caso de líneas no dedicadas.

Los modems con capacidad de discado (dial-up modems) pueden establecer conexiones punto a punto dentro de la red pública telefónica conmutada (RPTC) discando el número del abonado deseado. La calidad del circuito no está garantizada y las líneas serán una combinación de 2W y 4W.

1.4 SIMPLEX, HALF-DUPLEX, FULL_DUPLEX.

Estos términos describen tanto a modems como canales de transmisión. Un modem full-duplex no puede funcionar sobre un canal half-duplex y modems half-duplex pueden en algunos casos funcionar en modo full-duplex.

Simplex: significa que las señales solo pueden transmitirse en una dirección solamente. Un modem remoto empleado en un sistema de telemetría puede funcionar en modo simplex.

Half-Duplex: estos modems pueden transmitir señales en ambos sentidos, pero no en ambos simultáneamente. Un canal telefónico vía satélite con muy gran retardo, incluye a veces dispositivos supresores de eco (ver Problemática de Redes) que permiten transmitir en una sola dirección por vez, esto convierte al canal en half-duplex. Los supresores de eco están lentamente siendo reemplazados por circuitos canceladores de eco que son teóricamente dispositivos full-duplex.

Cuando un modem no comparte circuitería entre transmisor y receptor puede transmitir y recibir simultáneamente si se usa una línea a 4 hilos.

Cuando un módem es conectado a una línea de 2 hilos, su impedancia de salida difícilmente sea idéntica a la impedancia de entrada de la línea, y una parte de la señal transmitida es reflejada hacia atrás. Por esta razón los receptores full-duplex son deshabilitados cuando su transmisor local esta operando.

Full-Duplex: cuando estos modems operan en una línea de 2 hilos deben ser capaces de separar la señal recibida de la señal transmitida reflejada, como veremos más adelante esto puede conseguirse de dos formas: por FDM en la cual cada señal en una diferente dirección ocupa una banda de frecuencia diferente y es separada por filtrado, la segunda forma es por cancelación de eco (EC) en la cual una réplica de la señal transmitida reflejada sintetizada localmente es substraída de la señal recibida.

Un modem 4800/4800 bps es full-duplex ya que puede transmitir y recibir simultáneamente a la máxima velocidad. Uno de 4800/0 es half-duplex y uno 4800/300 de 4800 bit/s con un canal de retorno de 300 bit/s se suele llamar full-duplex asimétrico.

1.5 MODEMS SINCRONICOS Y ASINCRONICOS.

Sincrónico significa que los datos son acompañados por una señal de reloj. Los datos sincrónicos son siempre agrupados en bloques y es responsabilidad de la fuente de los datos ensamblar esos bloques dentro de tramas y agregar bits extras para detectar y/o corregir errores de acuerdo a alguno de los muchos protocolos existentes (BISYNC, SDLC, HDLC, etc). La fuente de datos y el destino esperan que el modem sea transparente a este tipo de datos. Al mismo tiempo el modem ignora la estructura que se use para empaquetar los datos.

Los datos asincrónicos no estarán acompañados por ningún tipo de reloj, y los modems transmisor y receptor conocen solo la tasa nominal de datos. Para prevenir el deslizamiento (slipping) de datos debido a la diferencia entre los relojes de los modems, los datos se agrupan en bloques muy pequeños (caracteres) con bits de entramado (bits de arranque y parada); el más común de los códigos usados es 7 bits definido por ANSI con paridad par; este es un subset del alfabeto internacional nro. 5 definido por el CCITT en la recomendación V.3.

Más allá del formato sincrónico o asincrónico en que los modems reciban los datos, internamente, todos los modems actuales codifican y modulan esos datos en forma sincrónica. De esta forma si un modem acepta caracteres en formato asincrónico, el transmisor debe contar con algún modo de sincronizar estos datos. La forma más común de hacer esto es modificar la duración de los bits de arranque y parada como modo de absorber las diferencias de velocidades entre el reloj con el cual los bits fueron generados en la fuente y el reloj interno del modem.

1.6 MODULACION.

Los MODEMs utilizan modulación de amplitud, de fase, de frecuencia o una combinación de ellas. La forma más simple y económica de modulación es FSK.

1.6.1 MODEMS FSK.

Estos MODEMs utilizan en su versión más sencilla cuatro frecuencias dentro del ancho de banda utilizable del canal telefónico. Un modem típico full-duplex de 2 hilos transmite a 1070Hz para representar un ‘0’ y a 1270 Hz para el ‘1’ y recibe a 2025Hz y 2225Hz ‘0’ y ‘1’ respectivamente. Esta técnica ha sido ampliamente utilizada para modems de baja velocidad (hasta 1200 b/s). Modems FSK más sofisticados utilizan múltiples portadoras en lugar de solo dos.

1.6.2 MODEMS PSK.

Estos MODEMs alteran la fase de la portadora para representar al ‘0’y al ‘1’. Una mejora de este esquema es codificar la señal digital no en la fase de la portadora sino en los cambio de fase de la misma (DPSK) esto reduce la complejidad en los circuitos de recuperación de portadora. La modulación PSK hace un uso más eficiente del espectro que FSK aunque su implementación implica mayor complejidad circuital.

Es normal emplear modulación multinivel 4-PSK y 8-PSK en modems de alta velocidad.

1.6.3 MODEMS QAM.

QAM es una extensión de la modulación PSK multifase en la cual se manipula no solo la fase de la portadora sino también su amplitud.

Muchos modems actuales de alta velocidad usan esta técnica.

1.7 DEMODULACION.

Demodulación es el proceso de traslación en frecuencia de la señal recibida pasabanda a bandabase. Hay tres tipos de demodulación:

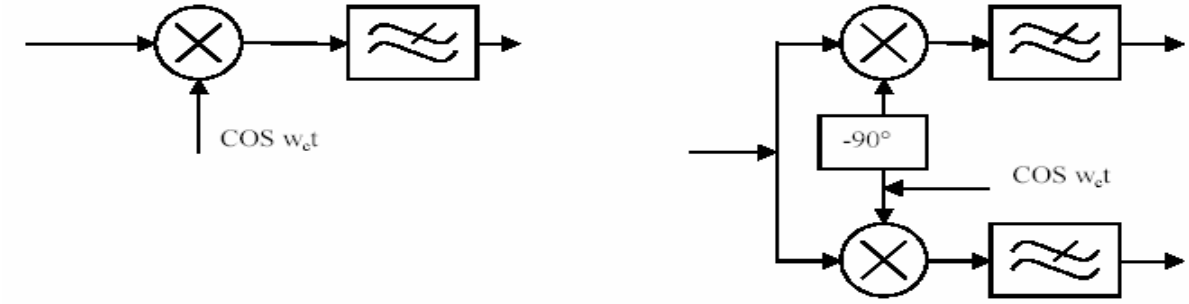
Demodulación coherente o demodulación sincrónica:

La fase de la señal es deducida de su relación con una portadora generada localmente, puede usar demodulación homodina o sincrodina.

La demodulación homodina significa el uso de la misma portadora transmitida como un piloto junto con la misma señal, en cambio sincrodina implica el uso de una portadora generada localmente que está de alguna manera sincronizada con la portadora implícita en la señal. Un ejemplo de homodina es la demodulación SSB (BLU) y de sincrodina es QAM.

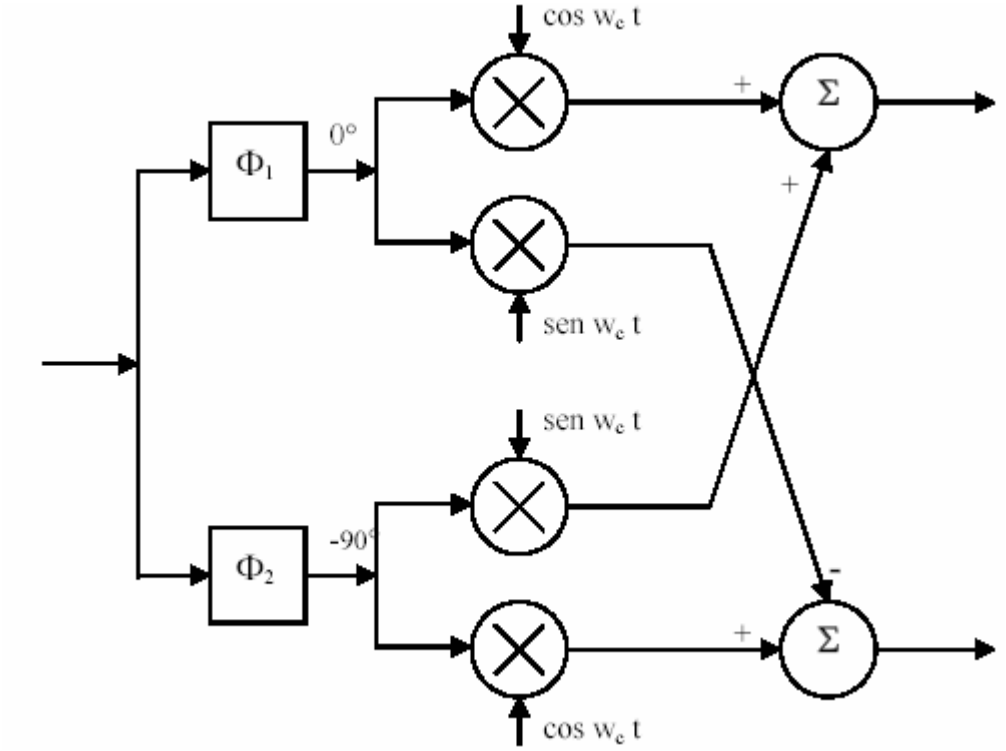
Las figuras siguientes muestran dos demoduladores coherentes, uno unidimensional y el otro bidimensional (QM: modulación en cuadratura).

El filtro pasabajo debe rechazar la banda lateral superior generada en el proceso de demodulación que comienza en fc-(1+α) fs/2, aún para sistemas de banda ancha (fs/fc > ½) como en V.33, la atenuación de 46dB necesaria para prevenir que la S/N a la entrada de 30dB sea reducida por el "ruido" de la banda lateral superior por más de 0.1dB es fácil de conseguir.



Los multiplicadores son más fáciles de implementar si la portadora es una onda cuadrada. Esto no impone una exigencia mayor sobre los filtros pasabajos debido a que los productos de intermodulación indeseados que se agregan, la banda lateral inferior de la tercera armónica de la portadora, se superpone (9.5dB más abajo) con la banda lateral superior de la fundamental.

La banda lateral superior puede ser eliminada también por el método de Hartley mostrado en la figura siguiente.

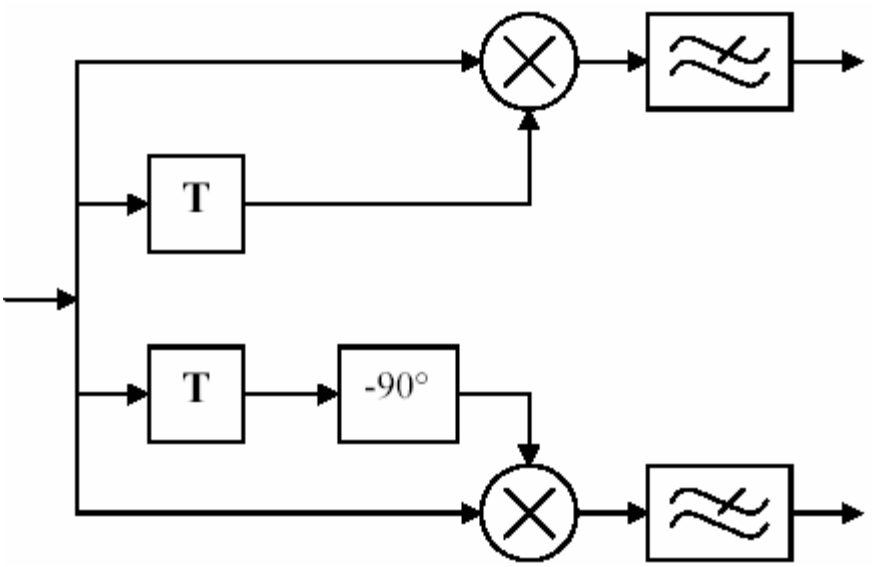


Demodulación no coherente o demodulación libre:

Este demodulador puede implementarse con cualquiera de los dos esquemas anteriores, excepto que en este caso el oscilador es libre a la frecuencia de la portadora, por lo tanto es un caso particular de demodulación heterodina. Este proceso normalmente es seguido de un ecualizador adaptativo y rotación como describimos más adelante.

Demodulación diferencial:

Ya sea con demodulación coherente o no coherente es necesario una etapa previa de detección coherente. La figura siguiente muestra un demodulador diferencial bi-dimensional convencional:



Una condición importante en el demodulador diferencial es que la frecuencia de la portadora fc debe ser un múltiplo entero de la tasa de símbolo fs. El desplazamiento de fase provocado por la red retardo de la parte superior del diagrama es:

$$\Phi p(\omega) = (\omega c - \omega)\, T + \Phi c$$

Entonces:

$$\frac{\partial \Phi_p}{\partial \omega} = T \qquad \text{y} \qquad \Phi_p(\omega_p) = \Phi_c$$

Puede parecer que solo es necesario un retardo T, solo se ha dibujado de esa forma para enfatizar las dos operaciones separadas. Si el defasador a -90° es combinado con el retardo, el circuito puede expresarse como:

$$\Phi q\,(\omega) = (\omega c - \omega)\, T + \Phi c - \pi/2$$

Para entender el funcionamiento del circuito, supongamos que la señal recibida se deriva de uno de los cuatro patrones posibles: $\Delta\Phi$= 0, 90°, 180°, o 270°.

La señal recibida será:

$$s(t) = A_m \cos 2\pi\left(\frac{f_c + mf_s}{4}\right)t + (1 - A_m)\cos 2\pi\left(\frac{f_c - f_s + mf_s}{4}\right)t$$

Donde m = 0, 1, 2, o 3

Las salidas de los dos filtros pasa bajos para t = kT son:

$$x_p(kT) = \cos(\Phi_c - \frac{k\pi}{2})$$
$$x_q(kT) = \cos(\Phi_c + \frac{(1-k)\pi}{2})$$

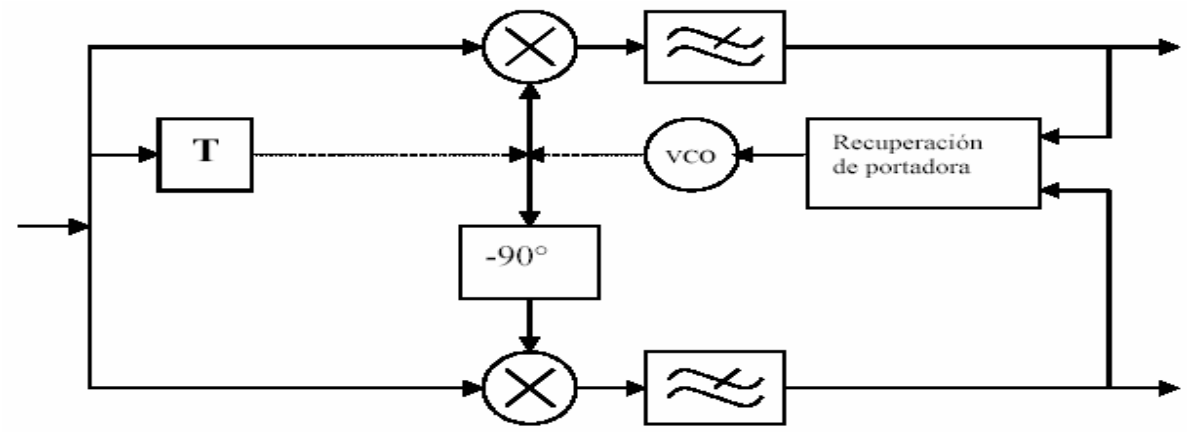
Si las redes de retardo se diseñan de forma tal que Φc = 0, entonces:

$$x_p(kT) = \cos(\frac{k\pi}{2})$$
$$x_q(kT) = \text{sen}(\frac{k\pi}{2})$$

Sin embargo los valores muestreados de xp y xq solo pueden valer +1, -1, o 0. En la práctica es más conveniente utilizar valores de Φc igual a cualquier múltiplo impar de $\pi/4$. Entonces en los instantes de muestreo xp y xq solo puede adoptar los valores $+1/\sqrt{2}$ y $-1/\sqrt{2}$, y puede utilizarse un detector de cruce por cero para el detector.

La figura siguiente muestra un demodulador diferencial genérico con dos alternativas para generar los multiplicandos en fase y cuadratura. Puede verse que la única diferencia con respecto a un demodulador sincrónico es la fuente de la que se extrae la portadora.

En la práctica, cada multiplicando debe limitarse para hacer más sencilla la tarea del multiplicador (es decir se envían muestras en lugar de señales continuas).



Demodulador QAM genérico con dos fuentes de recuperación de portadora

1.7.1 Comparación entre detección sincrónica y detección no-coherente:

1.7.1.1 a. Ventajas de la demodulación no coherente:

Para receptores simples que no requieren ecualización adaptativa, es menos costoso de implementar.

Para modems que requieren una inicialización muy rápida, el hecho de que no se requiera tiempo para que el oscilador de la portadora local se enganche en fase es una ventaja significativa.

1.7.1.2 b. Desventajas de la demodulación no coherente:

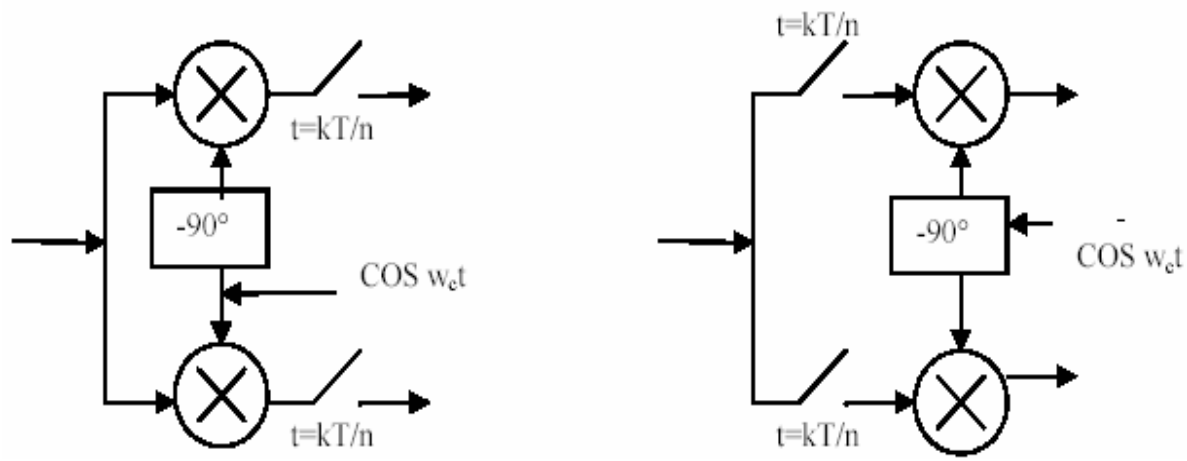
Es inferior en rendimiento, ya que dos señales “con ruido” son empleadas en la detección en lugar de una señal con ruido y una señal estable, se reduce por lo tanto la S/N. Para un demodulador 4 PSK la diferencia de S/N entre ambos métodos es 2.3dB cuando el número de fase crece este valor tiende asintóticamente a 3dB.

Es mucho más complicado de combinar con ecualizadores adaptativos.

1.7.2 Demodulación muestreada.

Si se utilizan portadoras senoidales, no es necesario emplear filtros pasabajos. Se puede usar un demodulador de Hartley seguido por un muestreador.

Los muestreadores se colocan a la salida de los dos multiplicadores, aunque como los multiplicadores son dispositivos sin memoria, también pueden moverse a la entrada de los multiplicadores como muestra la figura siguiente:



La frecuencia de muestreo puede ser igual a la tasa símbolo o algún múltiplo entero pequeño de esa tasa. En la mayoría de los modems para línea telefónica, la frecuencia de la portadora del transmisor es un múltiplo racional de tasa de símbolos:

$fc=Mfs/N$

donde M y N son enteros pequeños.

En un receptor elemental la señal analógica es procesada (filtrada, etc), demodulada a banda base y luego ingresa a un detector de umbral. La salida continua del detector es muestreada digitalmente, y el resultado es pasado al decodificador.

1.8 NORMALIZACION y PROTOCOLOS.

Desde un punto de vista técnico existen innumerables soluciones a la hora de diseñar un modem. Sin embargo, a fin de facilitar enlaces internacionales y evitar la proliferación innecesaria y antieconómica de soluciones particulares, existen organismos nacionales (EIA en USA) e internacionales (UIT-T) que han normalizado una serie de modems que cubren prácticamente todo el espectro de necesidades presentes.

Esta normalización permite que puedan conectarse entre sí modems de diferentes fabricantes.

Los 3 parámetros que definen un tipo de modem son:

- Velocidad de transmisión.
- Tipo de línea de transmisión.
- Tipo de modulación.

Los protocolos son las reglas necesarias para la interacción de los equipos de comunicaciones y son generalmente implementadas por programas que se ejecutan en el equipo terminal de datos (DTE) aunque algunas pueden estar implementadas en el hardware.

Los protocolos establecen las reglas para:

Agrupación de bits y caracteres - framing –

Detección y corrección de errores - control de error –

Numeración de mensajes - secuenciamiento -

Separación de caracteres de control y de datos - transparencia –

<<sorting-out receiving and sending equipment >>- control de línea –

Acciones requeridas para establecimiento - control de establecimiento -

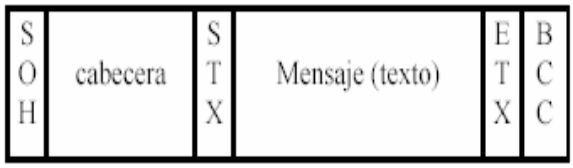
Acciones requeridas para la terminación de la comunicación - control de timeout –

Los protocolos pueden ser:

Orientados a caracteres como el BiSync (Binary Synchronous Data Transmssion - IBM).

CL: clase (tipo de mensaje)
CT: contador (cant.caracteres de mensaje)
F: bandera
R:número de respuesta
S: número de mensaje
A: dirección destino
CRC: chequeo por redundancia cíclica

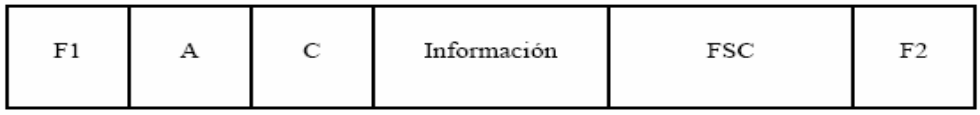
- Orientados al bit como el SDLC (Synchonous Digital Link Control - IBM).



SOH: Comienzo de la cabecera
STX: Comienzo del mensaje (texto)
ETX: Fin del mensaje
BCC: Caracter de chequeo de bloque

caracteres 1 variable 1 variable 1 1

- Orientados al byte como el DDCMP (Digital Data Communication Message Protocol - DIGITAL).



F1: Indicador comienzo trama (01111110)
A: Dirección destino
C:Control
FSC: Secuencia de control de trama (CRC)
F2: Indicador fin trama (01111110)

1.8.1 MODEM V.16.

MODEM para transmisión de señales analógicas en medicina.

1.8.2 MODEM V.19.

MODEM para la transmisión paralela de datos utilizando las frecuencias de señalización telefónicas.

1.8.3 MODEM V.20.

MODEM para la transmisión paralela asincrónica, de datos de aplicación universal sobre la red

RTPC. Para explotación half dúplex.

Se utiliza modulación multifrecuente con portadora en 920+8n Hz.

Interfaz con el ETD: V.30/V.31

1.8.4 MODEM V.21.

Estos MODEMs pueden trabajar en modo full-dúplex sobre líneas a 2 hilos, son de baja velocidad (300 bit/s) y para transmisión asincrónica. El canal telefónico se divide en dos mitades una para transmitir y la otra para recibir.

Esta recomendación está orientada a la transmisión por red telefónica conmutada, obviamente, pueden operar en líneas dedicadas a dos hilos.

1.8.5 MODEM V.22.

Está orientada a la transmisión a través de la red telefónica general conmutada (RTGC) o por circuitos arrendados punto a punto, permitiendo comunicaciones full-dúplex sobre 2 hilos en ambos casos. La tasa en la línea es 600 baudios (600 símbolos/seg).

Utiliza modulación DPSK, con frecuencias portadoras de 1200Hz ± 0.5Hz y 2400Hz ± 1Hz para el canal inferior y superior respectivamente. La velocidad binaria transmitida será de 1200 bit/s ± 0.01% con una velocidad de símbolos de 600 bit/s ± 0.01%

1.8.6 MODEM V.22 bis.

La recomendación V.22 bis permite velocidades de 1200 y 2400 bit/s. A velocidad reducida es compatible con la recomendación V.22. Utiliza modulación QAM. La tasa en la línea es 600 baudios.

1.8.7 MODEM V.23.

Este tipo de modems es de amplia aplicación en el servicio de videotexto (VIDEOTEX). El método de modulación es FSK como en el V.21, pero está pensado para transmitir a mayor velocidad. Dado el gran ancho de banda que implica utilizar FSK, cada canal de transmisión ocupa todo el canal telefónico. Para transmitir en modo dúplex se requieren líneas a 4 hilos.

No obstante, el canal de transmisión no llega a ocupar toda la banda disponible, esta recomendación permite el uso de un canal secundario de baja velocidad (75 bit/s). El uso del canal secundario es opcional y su aplicación en general es para señales de control.

1.8.8 MODEM V.26.

Esta recomendación está orientada a las comunicaciones punto a punto por línea dedicada de 4 hilos. Utiliza modulación 4-DPSK. Como puede observarse en la tabla siguiente se han normalizado posibilidades de normalización que se identifican como “A” y “B”. Opcionalmente puede incluirse un canal secundario con modulación FSK idéntico al de la recomendación V.23.

DIBIT	Cambio de fase SOLUCION “A”	Cambio de fase SOLUCION “B”
00	0°	+ 45°
01	+ 90°	+ 135°
11	+ 180°	+ 225°
10	+ 270°	+ 315°

1.8.9 MODEM V.26 bis.

Es una modificación de la norma anterior para utilizar estos modems sobre red conmutada o dedicada a 2 hilos. El modo de trabajo es half-dúplex y se modula de acuerdo a la solución “B”.

Las siguientes son las principales características:

VELOCIDAD : 2400 bps
TRANSMISION : SINCRONICA
LINEA : DEDICADA o COMUN 2 HILOS
MODO : HALF DUPLEX
MODULACION : 4-DPSK
INTERFAZ LOGICO : V.24 y V.28
CANAL SECUNDARIO : IDENTICO A V.23

También tiene un modo de replegado de velocidad a 1200 bps, diseñado para cuando las líneas no soportan 2400 bps. En este caso se modula en 2-PSK con 90° para el 0 y 270° para el 1, de manera de conservar la compatibilidad.

1.8.10 MODEM V.26 ter.

Está dedicado a las comunicaciones full dúplex sobre circuitos de 2 hilos a 2400 bps en modo síncrono, con modulación 4-DPSK. Esto es posible gracias a la incorporación de un circuito de cancelación de eco. Portadora a 1800 Hz.

1.8.11 MODEM V.27.

Esta recomendación define las características de los modems utilizados en transmisión a 4800 bit/s por líneas dedicadas a 4 hilos. Utiliza modulación 8-DPSK con la correspondencia de fase indicada en la tabla siguiente:

TRIBIT	001	000	010	011	111	110	100	101
CAMBIO FASE	0°	+45°	+90°	+135°	+180°	+225°	+270°	+315°

Características:
VELOCIDAD : 4800 bps
TRANSMISION : SINCRONICA
LINEA : DEDICADA A 4 HILOS CALIDAD ESPECIAL

MODO : FULL DUPLEX O HALF DUPLEX
MODULACION : 8-DPSK
PORTADORA : 1800 Hz
INTERFAZ LOGICO : V.24 y V.28
CANAL SECUNDARIO : OPCIONAL COMO EN V.23

1.8.12 MODEM V.27 bis.

Se modificó la recomendación anterior para poder trabajar sobre líneas de calidad normal con modo de replegado a 2400 bps.

VELOCIDAD : 4800 / 2400 bps
LINEA : 2 ó 4 HILOS CALIDAD NORMAL ó ESPECIAL (2 hilos: half-dúplex, 4 hilos: full-dúplex)
MODULACION : 8-DPSK / 4-DPSK
CANAL SECUNDARIO : 75 bps (opcional)

1.8.13 MODEM V.27 ter.

Se fijan las condiciones para transmisión por red RTPC a 4800 bit/s con posibilidad de replegado a 2400 bit/s.

VELOCIDAD : 4800 / 2400 bps
LINEA : RED TELEFONICA CONMUTADA
Incluye un seudoaleatorizador con polinomio generador: 1 + x-6 + x-7

1.8.14 MODEM V.29.

Se define un modem para trabajar a 9600 bps sobre líneas privadas de calidad especial a 4 hilos en full duplex o 2 hilos en half duplex. Capacidad de replegado a 7200 y 4800 bps.

Se utiliza un método especial de modulación 16 QAM. Al igual que en el 16 QAM convencional se trata de señales octafase con modulación de amplitud en dos niveles por fase.

1.8.15 MODEM V.32

VELOCIDAD	: 9600, 4800 bps
TRANSMISION	: ASINCRONICA ó SINCRONICA
LINEA	: CONMUTADA ó DEDICADA
MODO	: FULL DUPLEX con cancelación de eco
MODULACION	: 16 QAM
PORTADORA	: 1800 Hz

V.32 dispone de dos canales en sentido opuesto. Estos canales comparten aproximadamente del mismo ancho de banda. Esto es posible ya que estos modem emplean cancelación de eco. Esto permite al modem distinguir la señal recibida de su propia señal transmitida.

1.8.16 MODEM V.32 bis (1991).

Este MODEM está designado a las conexiones con la RTPC y en circuito dedicados (o arrendados) de tipo telefónico a 2 hilos punto a punto, en modo full dúplex. Se utiliza la técnica de separación de canales por cancelación de eco. Es compatible con los modems V.32 a 9600 y 4800 bit/s. La modulación es QAM con transmisión síncrona en línea de 2400 símbolos por segundo, con portadora a 1800 Hz. V32bis soporta 2 tasas de operación por encima de la tasa máxima de V32 (12kbps y 14.4kbps con 64 y128 puntos de señal respectivamente).

1.8.17 MODEM V.33.

Define un modem de 14400 bit/s para usar sobre línea dedicada a 4 hilos. Puede pensarse como una versión simplificada de la recomendación V32 ya que si bien es full duplex no incluye cancelador de eco porque no está pensado para funcionar en circuitos de 2 hilos.

1.8.18 MODEM V.Fast y V32terbo.

Son MODEMs de transición entre V.32 y V.34.

V32terbo es la solución adoptada por ATT, es en realidad una mejora a los modems V32bis y por lo tanto mucho menos complejos que la generación siguiente V34. Permiten

transmitir a 16.8kbps y 19.2kbps, todas las demás características son iguales a la recomendación V32bis.

VFC (V.Fast Class) (1993) es una solución propietaria de Rockwell para transmitir a 28.8kbps. Se basa en las propuestas del UIT-T para la recomendación V34 sin embargo no es compatible con esta última. A esta norma también se la llamó V.Fast.

1.8.19 MODEM V.34 (1994).

La recomendación V34 no solo significa un aumento importante en la tasa de operación respecto de V32bis sino también en cuanto a complejidad de funcionamiento. Entre las nuevas funciones que incorpora V34 están: capacidad de transmisión asimétrica, canal de transmisión auxiliar, codificación no lineal, precodificación y un aumento significativo en la cantidad de estados del codificador Trellis. Las tasas de operación disponibles son 21.6kbps, 24kbps, 26.4kbps y 28.8kbps.

1.8.20 MODEM V.34bis (1995).

Es una extensión del estándar V34. Soporta dos nuevas tasas de operación: 31.2kbps y 33.6kbps.

1.8.21 MODEM V.36.

Esta recomendación define las normas para la transmisión de señales digitales sobre una línea constituida por un grupo primario de un sistema múltiplex MDF, con ancho de banda de 60- 180KHz.

La señal transmitida corresponde a una modulación de amplitud de banda lateral única de una portadora de 100 KHz. Esta portadora se modula por una señal en banda base sin componente de continua.

Estos modems se instalaban en las centrales telefónicas pero están desapareciendo en la medida que la red de transporte es digitalizada bajo los sistemas PDH o SDH.

VELOCIDAD : 48000/56000/64000 y 72000 bps
TRANSMISION : SINCRONICA
LINEA : GRUPO PRIMARIO
MODO : FULL DUPLEX
MODULACION : AM-BLU
PORTADORA : 100 KHz
INTERFAZ LOGICO : V.24, V.10 y V.11

1.8.22 Protocolos MNP.

Creados por la empresa Microcomm, los protocolos MNP (Microcomm Networking Protocol) se han incorporado como parte del firmware de los modems de éste y otros fabricantes.

MNP1: Protocolo de corrección de errores a nivel de byte para terminales asíncronos.

MNP2: Idem MNP1 en modo full dúplex.

MNP3: Protocolo de corrección a nivel de bit, en modo síncrono SDLC (Synchronous Data Link Control, protocolo de control de enlace (similar al HDLC) para transmisiones síncronas desarrollado por IBM) full dúplex. El ETD transmite en modo asíncrono hasta el modem y entre modems trabajan en modo síncrono. Emplea paquetes de longitud fija.

MNP4: Protocolo de corrección de errores a nivel de paquete de longitud variable y adaptable en función de la calidad de la línea, para ser empleado en modems asincrónicos.

MNP5: Protocolo de corrección y compresión, para modems asincrónicos. Combina la utilización de codificación Huffman con la técnica run leng, consiguiendo una eficacia de 2:1. Unos niveles de compresión más avanzada se definen en MNP7 y MNP8.

MNP6,9,10: Servicios extendidos; por ejemplo, para simular líneas full dúplex sobre enlaces half dúplex.

1.9 Estado del arte a nivel mundial.

Dentro de los principales fabricantes de MODEM a nivel mundial se encuentran compañías como:

Cellution INC, Data-Linc Goup, MaxStream, Xstream, etc.

Entre los principales parámetros de los MODEMs se encuentran la potencia de salida, la tasa de transferencia de datos, la frecuencia de operación, sensibilidad del receptor, distancia que alcanza, voltaje de alimentación, etc.

Los productos que se venden actualmente tienen características muy diversas que se adecuan a las más diversas aplicaciones y especificaciones adecuándose a los más diversos requisitos. Dentro del mercado se encuentran productos que pueden batir distancias que se encuentran entre algunos metros y hasta 70 u 80 Km. Dentro de las potencias se encuentran MODEM que trabajan con 10Mw (LinkWiser-400) y otros que alcanzan los 5W (UAR500). Las razones de transferencia de datos han evolucionado mucho y llegan a los Mbps. Dentro de las bandas de frecuencia existe una gran diversidad ya que muchas de estas se encuentran restringidas a distintas zonas geográficas. Existen bandas como: 313/915 MHz; 2,4 GHz; 999MHz; 315/433 MHz etc. Con el apoyo de estas y otras características se hará una valoración para el desarrollo de nuestro diseño.

1.10 Conclusiones.

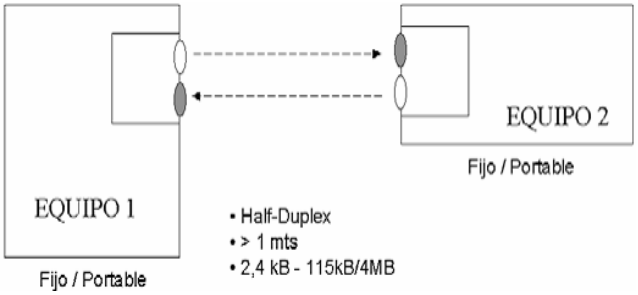
En este capítulo hemos pretendido abordar los aspectos concernientes a los MODEM, muy en particular a los conceptos más generales. Luego de este análisis determinamos desarrollar el diseño del hardware del MODEM. Esto implica el desarrollo de una serie de diseños y de especificaciones que explicaremos en el capitulo siguiente.

Capitulo 2: Harware.

2.1 Comunicaciones Inalámbricas

Una comunicación inalámbrica es cuando la vía de unión entre sistemas no son cables u otro elemento físico, solo se emplea un determinado segmento del espectro radioeléctrico. Sus principales ventajas son que permiten una facilidad de emplazamiento y reubicación, evitando la necesidad de establecer un cableado y mejorando la rapidez en la instalación. Las técnicas utilizadas son: por Infrarrojos (IR), y por radiofrecuencia (RF).

Infrarrojos: Sólo permiten comunicaciones para pequeñas distancias, los puntos de conexión deben ser siempre visibles, el campo de aplicación es limitado, su uso aún es muy extendido.



Radio Frecuencia: Permite comunicaciones de corto y medio alcance, puede atravesar obstáculos y paredes, el campo de aplicación es muy grande.

En este trabajo sólo se van a tratar los sistemas de Radio Frecuencia o “wireless RF”.

2.2 Análisis de las principales características de los MODEM.

Las transmisiones de datos entre equipos electrónicos sin cables se están aplicando cada vez más debido a los medios tecnológicos actuales, donde los sistemas empotrados que se colocan en distintos dispositivos típicamente añaden esta prestación gracias a los circuitos

integrados que permiten hacer un diseño sin disponer de cara instrumentación para RF, ya que estos dispositivos requieren pocos componentes externos.

Para lograr el desarrollo de un producto con la mayor calidad posible, es necesario investigar los mercados y las industrias para evaluar las necesidades cambiantes y las nuevas tendencias, y desarrollar tecnologías que se enfrenten a esos retos.

• Seguridad, integridad de los datos y fiabilidad en ambientes con mucho ruido.

• Comunicaciones de alta calidad a gran distancia.

• Solidez industrial y compatibilidad con el medio ambiente.

• Facilidad de instalación y un funcionamiento que no necesita servicio de mantenimiento.

La investigación se ha enfocado en el desarrollo de tecnologías inalámbricas para sistemas industriales, de rendimiento probado sobre el terreno, que pueden funcionar en las condiciones más difíciles.

2.2.1 Tecnologías

Dentro de las comunicaciones inalámbricas primero se usaron módulos de RF con componentes discretos unidireccionales y precisamente para no tener que depender del diseño de una circuitería en RF. Posteriormente con la aparición de circuitos transmisores completamente integrados con las funciones de emisor y receptor, en diferentes bandas de frecuencia que se fueron estandarizando en las diferentes zonas (Europa y USA), han permitido poderlos utilizar en los diferentes campos de aplicación industrial, comercial, y medico, como: control remoto, transmisión de datos en sensores o sistemas de adquisición de datos, en monitorización médica o de la salud, etc.

Existen un grupo de tecnologías para comunicación inalámbrica como por ejemplo: Wi-Fi, Bluetooth, WiMax, ZigBee, etc. Para el desarrollo de nuestro producto se ha decidido utilizar la tecnología ZigBee. A continuación se hará un análisis del por que de nuestra elección.

2.2.2 ZigBee

La necesidad de empresas de informática y de telecomunicaciones de desarrollar una interfaz abierta y de bajo coste para facilitar la comunicación entre dispositivos dio como resultado la tecnología ZigBee. La idea de ZigBee empezó a finales de los 90 cuando muchos ingenieros se planteaban que Wi-Fi y Bluetooth dejaban un hueco vacío para cierto tipo de aplicaciones.

Bluetooth ofrece poca potencia de transmisión por lo que no logra tener amplia cobertura (máximo, cientos de metros).

Wi-Fi por su parte, presenta una pérdida de velocidad, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear. La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Uno de los puntos débiles (sino el gran punto débil) es el hecho de no poder controlar el área que la señal de la red cubre, por esto es posible que la señal exceda el perímetro del edificio y alguien desde afuera pueda visualizar la red y esto es sin lugar a dudas una mano para el posible atacante. Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

En la siguiente tabla se muestran las principales características de cada una de las tecnologías mencionadas: el estándar de comunicaciones, la máxima velocidad de transmisión, el consumo de corriente típico en transmisión y el consumo de corriente en “standby”.

ZigBee (WPAN)	Bluetooh (WLAN/WPAN)	Wi-Fi (WLAN)
IEEE 802.15.4	IEEE 802.15.1	IEEE 802.11x
250 kbps	1 Mbps	Hasta 54 Mbps
TX: 35 mA	TX: 40 mA	TX: > 400 mA
Standby: 3 µA	Standby: 200 µA	Standby: 20 mA

Tabla 2.1 Comparativa de ZigBee, Bluetooth y Wi-Fi

Por lo tanto si el objetivo es diseñar un sistema de bajo consumo el cual no necesite de altas velocidades, nos quedan los sistemas ZigBee, pensados específicamente para este tipo de conexiones.

En el año 2000 se da a conocer el nuevo estándar para redes inalámbricas de bajo consumo y de bajo coste para aplicaciones domóticas e industriales, se conoce como el 802.15.4, o más conocido como ZigBee (se completó en 2003 y fue ratificado a finales de 2004.). ZigBee es diferente de los otros estándares inalámbricos, ha sido diseñado para soportar un diverso mercado de aplicaciones con una conectividad más sofisticada.

La razón de promover un nuevo protocolo como un estándar es para permitir la interoperabilidad entre dispositivos fabricados por compañías diferentes. Este importante estándar define el hardware y el software, el cual ha sido descrito en los términos de conexión de redes, como las capas físicas (PHY), y la capa de control de acceso al medio (Mac). La alianza ZigBee ha añadido las especificaciones de las capas red (NWK) y aplicación (APL) para completar lo que se llama la pila o stack ZigBee.

Se pueden ver los reducidos requisitos de memoria de programa de ZigBee . Las aplicaciones ZigBee son típicamente muy simples. La potencia está en la conexión de redes y el hecho de que los dispositivos “end point” de ZigBee puedan "dormir", es decir, caer en modo modo de bajo consumo.

Los módulos ZigBee serán los transmisores inalámbricos más baratos jamás producidos de forma masiva. Con un coste estimado alrededor de los 2 euros dispondrán de una antena integrada, control de frecuencia y una pequeña batería.

En los últimos años ZigBee ha logrado evolucionar un grupo de características integrales dentro de las que destacan:

- Escalabilidad de red -- Un mejor soporte para las redes más grandes, ofreciendo más opciones de gestión, flexibilidad y desempeño.
- Fragmentación -- Nueva capacidad para dividir mensajes más largos y permitir la interacción con otros protocolos y sistemas.
- Agilidad de frecuencia -- Redes cambian los canales en forma dinámica en caso que ocurran interferencias.

- Gestión automatizada de direcciones de dispositivos - El conjunto fue optimizado para grandes redes con gestión de red agregada y herramientas de configuración.
- Localización grupal -- Ofrece una optimización adicional de tráfico necesaria para las grandes redes.
- Puesta de servicio inalámbrico -- El conjunto fue mejorado con capacidades seguras para poner en marcha el servicio inalámbrico.
- Recolección centralizada de datos -- El conjunto fue sintonizado específicamente para optimizar el flujo de información en las grandes redes.

Dentro de los principales rivales de ZigBee se encuentra WiMax. Esta tecnología soporta varios cientos de usuarios por canal, con un gran ancho de banda y es adecuada tanto para tráfico continuo como a ráfagas, siendo independiente de protocolo; así, transporta IP, Ethernet, ATM, etc. y soporta múltiples servicios simultáneamente ofreciendo Calidad de Servicio (QoS), por lo cual resulta adecuado para voz sobre IP (VoIP), datos y vídeo. Por ejemplo, la voz y el vídeo requieren baja latencia pero soportan bien la pérdida de algún bit, mientras que las aplicaciones de datos deben estar libres de errores, pero toleran bien el retardo.

Pero pierde con ZigBee en cuanto a la tolerancia a las interferencias. Esta tecnología es muy sensible a los cambios climáticos por lo que sus transmisiones sufren de mucho ruido cuando las condiciones del clima no son favorables. ZigBee, además de ser más robusta a estas interferencias del clima y estar más a nivel mundial implementada (que esto siempre es una ventaja), su principal objetivo es el bajo consumo y el bajo coste. También es bueno decir que no todo relacionado a WiMax está claro. De acuerdo con la consultoría Prince & Cook, los impulsores de la tecnología WiMax (Intel, Nokia, NEC y Alcatel) se han demorado en llegar a un acuerdo sobre las especificaciones de un patrón que permita certificar los equipamientos. Esto, sumado otras cuestiones, atrasan la aceptación de la tecnología.

Uno de los aspectos más característicos de ZigBee son los servicios que ofrece para el soporte de comunicaciones seguras. Se protege el establecimiento y transporte de claves, el cifrado de trama y el control de dispositivos. Se apoya en el marco definido

por IEEE 802.15.4; la seguridad depende de la correcta gestión de las claves simétricas y la adecuada implementación de los métodos y políticas de seguridad.

Basándose en estos argumentos expuestos anteriormente es que se decidió utilizar ZigBee. En la tabla 2.2 mostramos el campo de aplicaciones de algunas tecnologías inalámbricas:

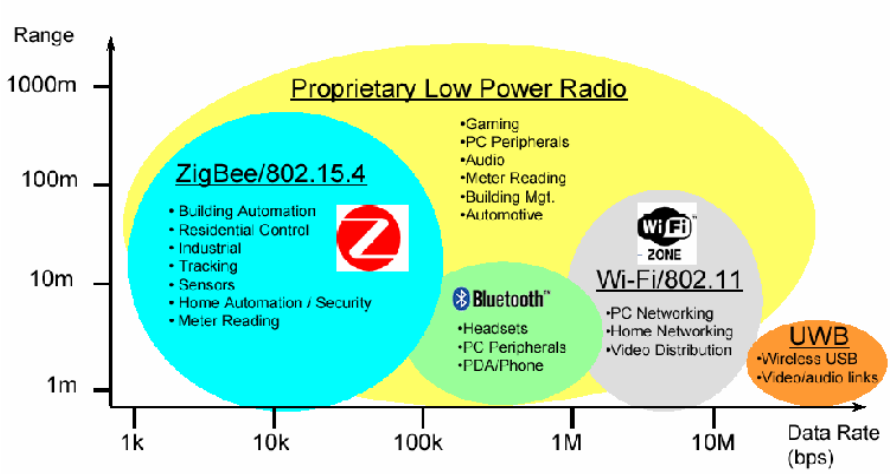


Tabla 2.2 Aplicaciones de algunas tecnologías.

2.2.3 Comparación de las características de los MODEM.

Basados en estas tecnologías y empleando distintas bandas de frecuencia se han construido distintos tipos de MODEM inalámbricos. A continuación mostramos un grupo de los mismos que nos permitirán hacer una comparación de sus principales características, lo que nos dará una mejor visión a la hora de diseñar nuestro producto.

MODEM	LinkWiser -400	LRDM-4000	SRM6000	UAR500	XBee-PRO PKG
Compañía	Cellution INC	Ring Line Corporation	Data-Linc Goup	RF DataTech	MaxStream

Frecuencia de transmisión	424-447MHz	902-928MHz - opcional: 866-868MHz y 460.2 -463.2MHz	902-928 MHz	820 – 950MHz	2.4GHz
Sensibilidad del receptor	-120dBm	-106dBm	-108dBm	(-116dBm) - (-120dBm)	-100dBm
Interfase	RS-232C, RS-485	RS485/422	RS232 -opcional: RS422 y AE485	RS232	RS232
I/O data rate	1200 – 2400 bps	2.4 – 19.2 Kbps	144 - 188 Kbps	9600bps	250Kbps
Espaciamiento entre canales	12. 5khz	200KHz	230KHz	12.5, 20 ó 25KHz	–
Distancia que alcanza	1.6km (1 milla)	5 – 20km	40-56km (25-35millas)	35 Km	1.6km (1 milla)
Potencia de salida	10mW	1W	1W	5Watts	100mW
Voltaje de alimentación	(-0.5) - (5vol)	100-240VAC 12VDC	10.5 – 18.0 VDC; 12 VDC	(10V – 15.5DC); 12VDC	(5) – (14 VDC)
Consumo de corriente	35mA	TX: 500mA RX: 50mA	TX: 650 mA RX: 100 mA	TX:300mA- 2A RX: 70mA	TX: 300 mA RX: 80 mA
Temperatura de	(-20) – (65℃)	(-30) – (80℃)	(-40) - (75℃)	(-30)-(60℃)	(-40)–(85℃)

operación					

Tabla 2.3: Característica de los MODEM.

En la tabla 2.3 se relacionan un importante número de características a tener en cuenta a la hora de analizar un MODEM. Algunas de estas características son:

- Banda de frecuencia empleada. Es la frecuencia central de transmisión veamos cómo se distribuye el uso de las mismas a nivel mundial (figura 2.1

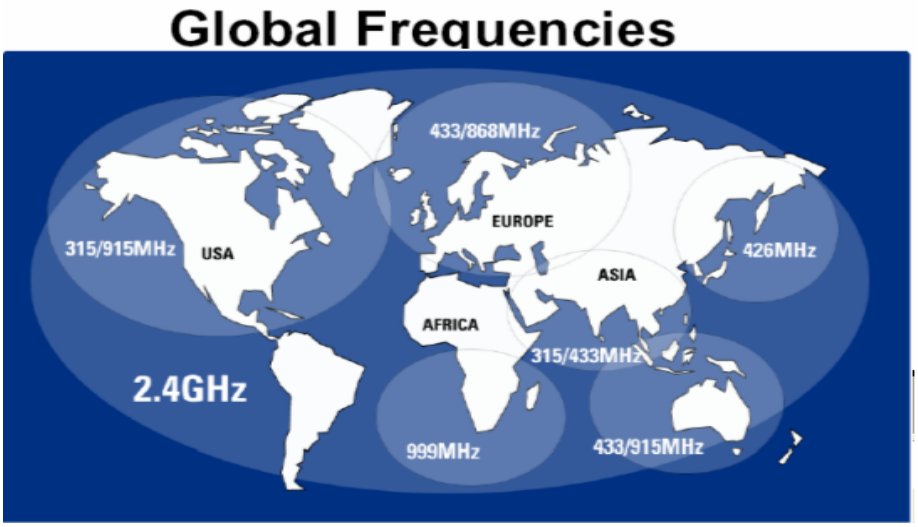


Figura 2.1: Distribución de las frecuencia a nivel mundial.

Como podrán observar la frecuencia de mayor aceptación mundial es la de la banda de 2.4GHz. Aunque con otras bandas de frecuencias se pueden cubrir mayores distancias (como 900MHz) estas se encuentran limitadas en uso por regulaciones gubernamentales de uso del espacio radioeléctrico en distintas zonas geográficas (Cuba es uno de esos casos).

-Distancia que alcanza: Es el radio de acción clasificado que puede cubrir en condiciones óptimas.

-Espaciamiento entre canales: Es el espacio en frecuencia que ocupa cada canal.

- I/O data rate: Velocidad de operación. Es la velocidad con que el MODEM es capaz de transmitir el tren de datos de información.

-Sensibilidad del receptor:

- Potencia de salida:

2.4 Requerimiento que debe cumplir el MODEM.

Después de realizar un análisis detenido de las principales características de este grupo de MODEM, se enfoco la atención en los requerimientos que pide el usuario, y que debe cumplir el producto. El MODEM debe trasmitir con 1 watt de potencia, en la banda de 2.4GHz, con una velocidad de transmisión de 19200 bps y con comunicación RS232.

2.4.1 Comparación con otros MODEM.

Dentro de los MODEM que se relacionan el la tabla 2.3 el XBee-PRO PKG cumple con algunas de las características que debe tener el producto en el que se esta trabajando. Cumple con la banda de frecuencia (2.4GHz), con la velocidad de transmisión (250Kbps) y con interfase RS232 aunque solo bate una 1 milla (1.6Km) de distancia. Este MODEM se puede encontrar en el mercado con un precio de $110.00. A modo de comparación, se puede decir que nuestro producto debe batir una distancia superior a los 20 Km y su precio debe estar alrededor de los $100. Como se observa, uno de los principales objetivos de este trabajo es el ahorro de presupuestos, a demás de la creación de un producto propio, por lo que si se comprase un MODEM que bata esta distancia (superior los 20 Km) nos costaría mucho más que nuestro diseño.

Otro MODEM que podemos analizar es el LRDM-4000. Este no utiliza interfase RS232 y trabaja en las bandas de 902-928MHz y de forma opcional en las de 866-868MHz y 460.2 - 463.2MHz, por lo que no cumple con estas especificaciones de nuestro producto, pero si cumple con la velocidad de transmisión (2.4 – 19.2 Kbps) y con 1watt de potencia de salida, además de alcanzar una distancia máxima de 20 Km que es aceptable para nuestras necesidades.

2.5 Chips con los que se puede implementar el proyecto

Para el diseño de un MODEM se utilizan una serie de chips. Dentro del análisis que se realizó a los distintos MODEM que se mostraron anteriormente, se hizo una selección de los chips más utilizados y de mayor rendimiento con el objetivo de seleccionar el más adecuado para realizar nuestro diseño. A continuación se observará en la tabla 2.4 una muestra de los que cumplen con las características que se requieren para que nuestro producto cumpla con los requerimientos del usuario:

chips	Compañía	Temperatura de operación	Modulación	I/O data rate	Alimentación
MC13192 (2.4GHz)	Motorola	(-40)-(85 °C)	O-QPSK	250kbps	2.0V - 3.4 V
CC2400 (2.4GHz)	Texas Intruments	(-40)-(85°C)	FSK/GFSK	10kbps/250kbps /1Mbps	(1.8 V)
CC2520 (2.4GHz)	Texas Intruments	(-40) -(125°C)	O-QPSK	250kbps	1.8 V – 3.8 V
FLC800C (2.4GHz)	DATA-LINC GROUP	0 - 50°C	CCK, DQPSK o DBPSK	11Mbps	5 VDC

Tabla 2.4: Característica de los chips.

Como podemos observar, todo este grupo de chips cumplen con los requerimientos que debe tener el dispositivo. La elección para el diseño fue el CC2520 de la firma Texas Instruments. Para esta selección se tuvo en cuenta la facilidad de implementación y la no necesidad de gran número de componentes externos, esto hace menos complejo nuestro

diseño y existe una amplia bibliografía con información sobre este chip. Este chip esta diseñado para ser acoplado mediante comunicación SPI a un Microcontrolador lo que lo hace ideal para interfasearlo con el DsPIC que sirve de centro de la aplicación de UAV de nuestro usuario.

2.5 Hardware.

Como podemos observar, se requiere de muy pocos componentes externos para la operación del CC2520. Este es un circuito típico de uso (figura 2.2).

Al usar una antena desequilibrada tal como un monopolo, se debe optimizar su funcionamiento. El balun se puede poner en ejecución usando los inductores y los condensadores discretos baratos solamente o conjuntamente con las líneas de la transmisión que substituyen los inductores discretos.

.2.5.1 Resistor de polarización.

El resistor de polarización R231 se utiliza para fijar una corriente de polarización exacta. ¿Una alta precisión (±1%) 56k? el resistor debe ser utilizado.

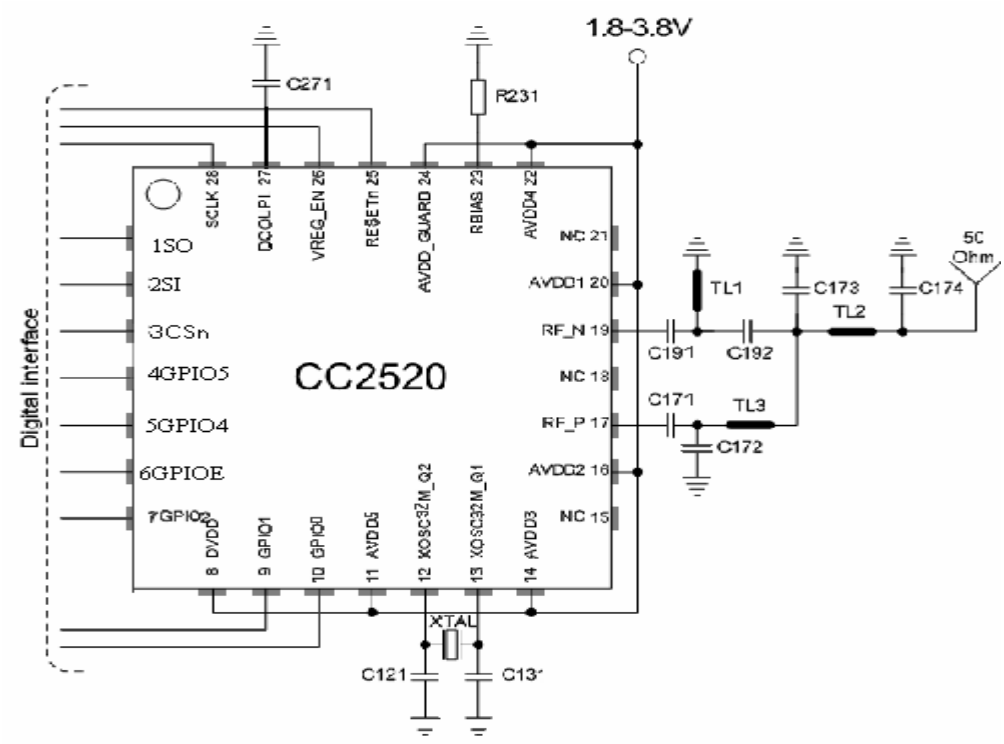


Figura 2.2 Diseño

2.5.2 Cristal

Un cristal externo 32MHz con dos condensadores de cargan (C121 y C131), se utiliza para el oscilador.

Es posible alimentar una señal single-ended al ping XOSC32M_Q1 y no utilizar así un cristal.

2.5.3 Regulador digital de voltaje.

Encendido el regulador de voltaje provee 1.8 V a la parte digital del CC2520. C271 es un condensador de desemparejamiento para el regulador de voltaje. Observar que esto no se debe utilizar para proporcionar energía al otro IC's.

El desacoplamiento apropiado de la fuente de alimentación se debe utilizar para el funcionamiento óptimo. La colocación y el tamaño de los condensadores de desacople y del

filtro de la fuente de alimentación son muy importantes para alcanzar el mejor funcionamiento da la aplicación.

2.5. # Elegir la interconexión más conveniente con un microcontrolador.

Conectar las 4 señales de SPI; CSn, SCLK, SI y SO al microcontrolador.

Se requieren estas señales para configurar CC2520 e intercambiar datos por él.

Conectar RESETn con el microcontrolador. Usar la señal de RESETn es la manera recomendada de reajustar CC2520 por ejemplo después de accionar para arriba. Si ahorrar un pin es crítico, el pin de RESETn se puede conectar con VDD.

Conectar VREG_EN al microcontrolador permitirá poner CC2520 en LPM2 para ahorrar energía. VREG_EN puede ser conectado con VDD y dejar así siempre el regulador encendido. Si el ahorro de energía no es importante, ésta puede ser una manera aceptable de ahorrar un pin.

Conectar uno o más GPIOs al microcontrolador es opcional.

El número de GPIOs a conectar depende del uso. Conectar más GPIOs con el microcontrolador da generalmente más flexibilidad y menos tráfico de SPI porque reduce la necesidad de reconfigurar las GPIOs para diversas aplicaciones.

Si CC2520 proporciona el reloj al microcontrolador, GPIO0 se debe conectar con la entrada de reloj del microcontrolador. Después de reajuste, GPIO0 hará salir una señal del reloj del 1MHz con 50% de ciclo útil.

Capitulo 3:

3.1 Estados de CC2520

CC2520 tiene tres estados de funcionamiento (figura3.1). En todos estos estados se aplica un voltaje de fuente al circuito.

LPM2 (bajo consumo): el regulador digital de voltaje es apagado (VREG_EN=0) y el reloj no esta trabajando. No se conserva ningunos datos. Todos los módulos análogos están en modo de bajo consumo.

LPM1 (bajo consumo): el regulador de voltaje digital está encendido (VREG_EN=1), pero ningún reloj están funcionando. Se conservan los datos. Los módulos analógicos son controlados por la parte digital y están en modo de bajo consumo.

Modo Activo: el regulador de voltaje digital es encendido (VREG_EN=1) y el reloj del oscilador de cristal está funcionando. La señal de bajo consumo es controlada por la parte digital.

Existen dos modos de poner el chip en modo activo, pero se explicará el que es recomendado por el fabricante que es el que utilizaremos:

Primeramente el pin RESETn debe ser punto bajo hasta que el regulador interno se halla estabilizado. Esto toma típicamente 0.1 ms, después el pin de RESETn es puesto 1 y CSn a 0, entonces se esperara a que el oscilador de cristal de comienzo a su funcionamiento, esto por lo general demora 0.2 ms (ver parámetros del cristal en la referencia). Por ultimo se pone CSn a 1 y entonces el chip se encuentra en modo activo.

Para nuestro trabajo no se esta interesado en los modos de bajo consumo, por lo que se configurará para que siempre esté en modo activo.

3.2 Señales SPI (Serial Peripheral Interfase).

La interfaz SPI se utiliza para dar instrucciones al CC2520 y transferir datos entre CC2520 y un microcontrolador. Esta interfaz auxiliar del CC2520 consiste en tres señales de entrada (CSn, SCLK y SI) y una señal de salida (SO).

3.2.1. CSn

Es la señal de encendido del SPI y es controlado por el microcontrolador. Se utiliza como un reset activo asincrónicamente al módulo SPI. Debe ser puesto en bajo durante todas las operaciones del SPI.

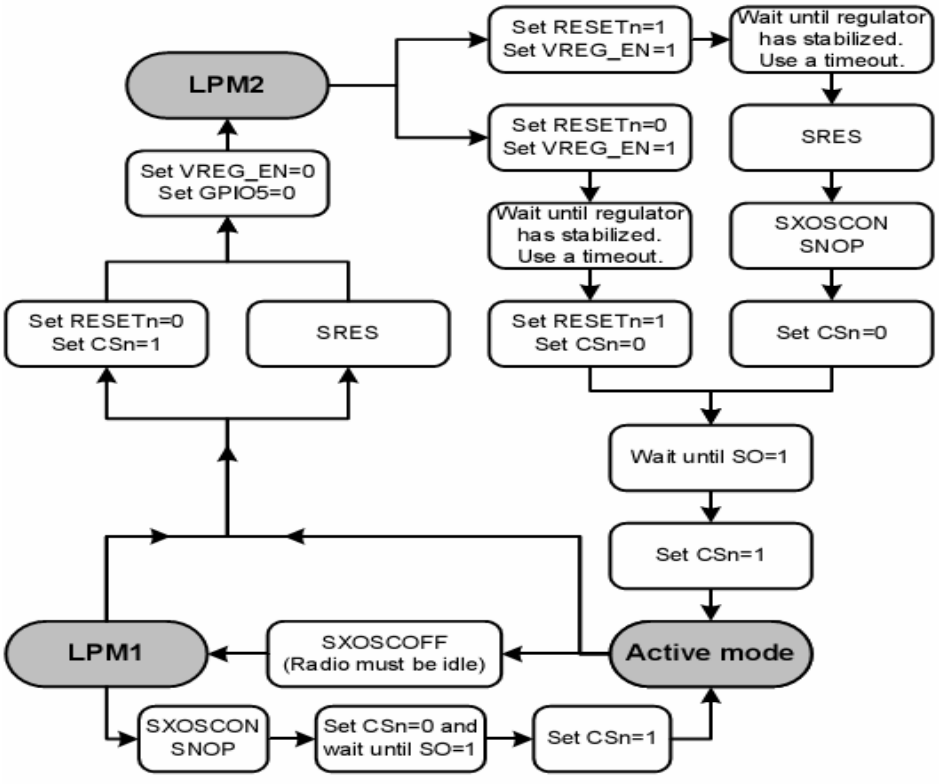


Figura 3.1 Estados.

3.2.2 SCLK

Es controlado por el microcontrolador y es un reloj de entrada de información al CC2520. Es asincrónico al reloj interno del XOSC en el ship. La frecuencia máxima del SCLOK es de 8 megaciclos. No hay requisitos mínimos para la frecuencia.

3.2.3 SI

Es la entrada de datos en serie del microcontrolador al CC2520.Los datos serán enviados con MSB (primero el bit 7 en cada octeto de comando de la instrucción).

Los datos se deben insertar en el borde negativo del SCLOK y serán registrados el CC2520 por el borde positivo siguiente del SCLOK.

3.2.4 SO

Es la salida de datos en seria del CC2520 al microcontrolador. Los datos se registran hacia afuera en el borde negativo del SCLOK, así que la señal SO debe muestrearse en el borde positivo siguiente del SCLOK. Los datos serán enviados con MSB. Se configurará SO como entrada cuando CSn es alto o RESETn es bajo.

3.3 Transmisión.

Existen tres modos de transmisión:

1. No CSMA-CA.
2. Unslotted CSMA-CA.
3. Slotted CSMA-CA.

La forma de transmisión se iniciará por las siguientes acciones:

- El comando STXON: [permite TX después de la calibración (si no se ha realizado ya) Si una trama se está recibiendo actualmente se levanta una excepción de RX_FRM_ABORTED].

-La señal de SAMPLED_CCA no es actualiza.

- El comando STXONCCA: (Si CCA indica un canal despejado. Permitir la calibración, entonces TX si no, no hacer nada También muestrear el valor de la señal de estado CCA, y la almacena en registro de estado).

- Aborta en curso de transmisión / recepción y obliga a hacer una calibración de TX seguida por la transmisión.

-La señal de SAMPLED_CCA es actualizada.

3.3.1 Modos de transmisión.

3.3.1.1 No CSMA-CA (figura 3.2):

En este modo de transmisión se utiliza la instrucción STXON. Cuando se ejecuta la instrucción no se actualiza la señal SAMPLED_CCA, es decir, no se comprueba si existe un canal despejado. La excepción de SFD será levantada cuando el campo de SFD de la trama se haya transmitido. En el extremo de la trama, la excepción de TX_FRM_DONE será levantada cuando la trama completa se haya transmitido con éxito. Si esto ocurre, se tiene la opción de la retransmisión. Para apoyar la retransmisión simple de paquete, el CC2520 no suprime contenido de TX FIFO mientras que se transmite. Después de que una trama se haya transmitido con éxito, el contenido del FIFO se deja sin cambios. Para retransmitir el mismo paquete otra vez, recomenzar simplemente usando el comando STXON (en el modo de transmisión No CSMA-CA).

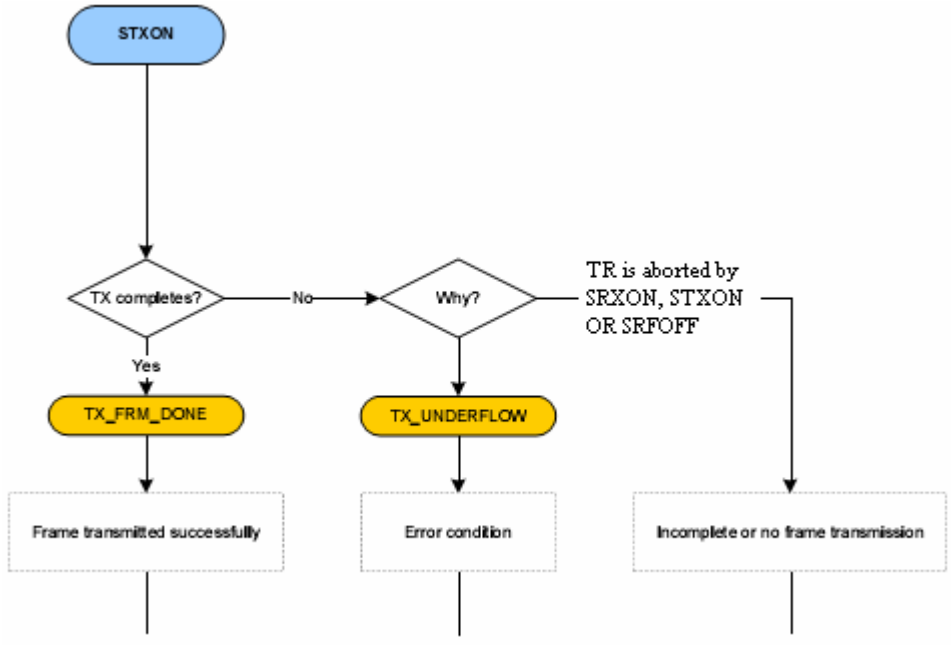


Figura 3.2

La transmisión puede que no se complete por dos razones. Primeramente, están las condiciones de error por desbordamiento. El desbordamiento puede ocurrir cuando el TX FIFO se llena y se procura escribir otro octeto, o cuando el TX FIFO esta vacío y CC2520 trata de traer otro octeto para la transmisión. Cuando estas condiciones se producen se levantan las señales TX_OVERFLOW y TX_UNDERFLOW. En el caso de que no se levanten ninguna de estas señales, es posible que se haya sido interrumpida la transmisión por los comandos SRXON (activa la resección), STXON (activar nuevamente la transmisión) o SRFOFF (se desactiva la transmisión o la recepción).

Para limpiar el TX FIFO se utiliza el comando SFLUSHTX. Si se quiere retransmitir la trama volver a copiarla en el TX FIFO o escribir la siguiente trama para continuar la transmisión.

3.3.1.2Unslotted CSMA-CA (figura 3.3):

Este modo de transmisión se comienza con el comando STXONCCA. Si se indica que hay un canal despejado (SAMPLED_CCA = 1), comienza la transmisión, si no (SAMPLED_CCA = 0), entonces no ocurre ninguna acción. En el caso de que la transmisión comience y sea interrumpida por alguno de los factores analizados anteriormente, se pueden ejecutar las mismas acciones que en el modo de transmisión No

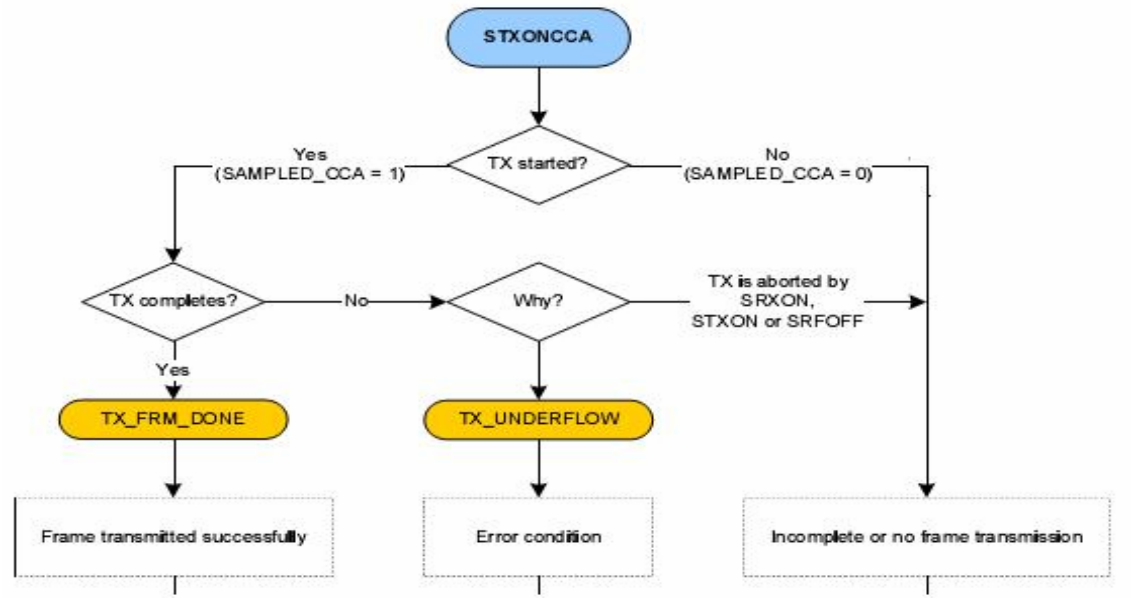


Figura 3.3

CSMA-CA, con la diferencia de que si se va a efectuar la retransmisión se comienza con el comando STXONCCA.

3.3.1.3 Slotted CSMA-CA (figura 3.4):

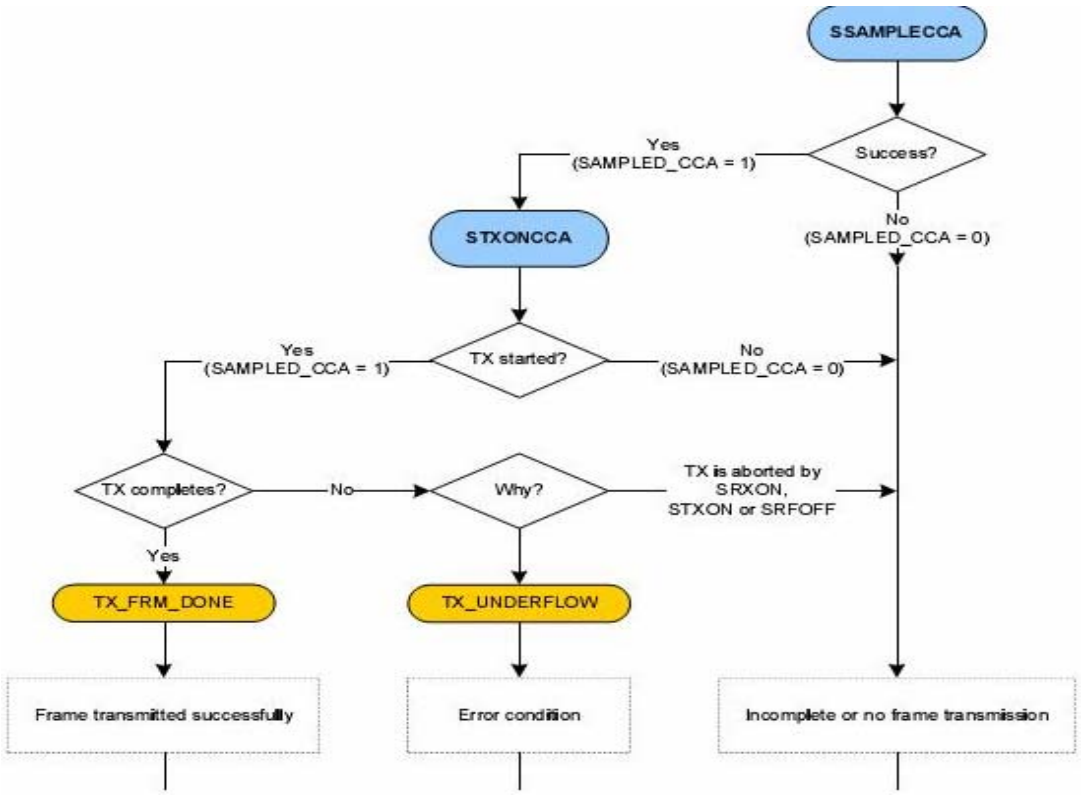


Figura 3.4

En este modo se inicia la transmisión con le señal de SSAMPLECCA. Esta señal muestrea el valor de CCA y lo almacena el registro de estado. Si no se encuentra un canal despejado, no se ejecuta ninguna acción, pero si CCA=1, se llama al comando STXONCCA el que vuelve a muestrear el canal, y si se confirma el canal despejado, se calibra el canal y se comienza la transmisión.

.

.

PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
Crystal frequency			32		MHz
Crystal frequency accuracy requirement	Including initial tolerance, aging and temperature dependency, as specified by [2]. Can be relaxed using on-chip crystal tuning (see below).	- 40		40	ppm
ESR				60	Ohm
C_0				7	pF
C_L				16	pF

PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
Crystal tuning range (C_{tune})	Only adding capacitance is possible		7		pF
Crystal tuning step size			0.4		pF
Crystal tuning drift	In % of applied tuning		+/-10		%
CRYSTAL TUNING USING CC2520 EM 2.1 REFERENCE DESIGN (NX3225DA, C_L = 16 pF) :					
Start-up time	NDK crystal NX3225DA, C_L=16 pF		0.2		ms
Crystal tuning step size			3		ppm
Crystal tuning range			-45		ppm
CRYSTAL TUNING USING OTHER CRYSTALS, ALL NUMBERS ARE ESTIMATES :					
Start-up time	NDK crystal NX4025DA, C_L=13 pF		0.2		ms
Crystal tuning step size			8		ppm
Crystal tuning range			-120		ppm
Start-up time	NDK crystal NX5032SA, C_L=10 pF		0.1		ms
Crystal tuning step size			10		ppm
Crystal tuning range			-160		ppm

Table 13: Status byte contents

Status byte (MSB clocked out first)		
Bit no	**Signal**	**Description**
7	XOSC stable and running	0: XOSC off or not yet stable 1: XOSC stable and running (Digital part has clock)
6	RSSI valid	0: RSSI value is not valid 1: RSSI value is valid
5	EXCEPTION channel A	0: No exceptions selected in EXCMASKAn has corresponding flag in EXCFLAGn set 1: At least one exception selected in EXCMASKAn has corresponding flag EXCFLAGn set
4	EXCEPTION channel B	0: No exceptions selected in EXCMASKBn has corresponding flag in EXCFLAGn set 1: At least one exception selected in EXCMASKBn has corresponding flag EXCFLAGn set
3	DPU H active	0: No high priority DPU instruction is currently active. 1: A high priority DPU instruction is currently active.
2	DPU L active	0: No low priority DPU instruction is currently active. 1: A low priority DPU instruction is currently active.
1	TX active	0: Device is not in TX mode 1: Device is in TX mode
0	RX active	0: Device is not in RX mode 1: Device is in RX mode

Conclusiones y Recomendaciones

Conclusiones

Las conclusiones deben estar en correspondencia con los objetivos planteados. Deben ser breves, precisas y convincentes. Es importante destacar que las conclusiones no son un recuento de lo que se realizó en el trabajo.

Para una mejor comprensión pueden ser numeradas y si algún caso lo requiere, pueden ser comentadas.

1 Conclusión 1

2 Conclusión 2

3 Conclusión 3

Recomendaciones

La posibilidad de incluir las recomendaciones permite al diplomante sugerir qué hacer con sus resultados y aportes.

1 Recomendación 1

2 Recomendación 2

3 Recomendación 3

La extensión de estos aspectos no debe exceder de cinco páginas.

Referencia Bibliografica

[1] C. S. Institute, "F.B.o. Investigation," in *10th Annual Computer Crime and Security Survey*, 2005, pp. 1–23.

[2] J. P. Anderson, "Computer security threat monitoring and surveillance.," James P Anderson Co., Washington, Reporte Técnico 98-17, Abril 1980 1980.

[3] S. Kumar and E. H. Spafford, "An application of pattern matching in intrusion detection.," The COAST Project, Purdue University. , West Lafayette., Reporte Técnico CSD-TR-94-013 Junio 17, 1994 1994.

[4] S. E. Smaha., "Haystack: An intrusion detection system.," in *The IEEE Fourth Aerospace Computer Security Applications Conference.*, Orlando, FL., 1998, pp. 37- 44.

[5] D. E. Denning and P. G. Neumann, "Requirements and Model for IDES - A Real-time Intrusion Detection System.," Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493., Reporte Técnico 83F83-01-00, 1985.

[6] T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathm, C. Jalali, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey, "A Real-time Intrusion Detection Expert System (IDES)." Computer Science Laboratory, SRI International, Menlo Park, CA, USA., Reporte Técnico Final, Febrero 1992 1992.

[7] D. Anderson, T. Frivold, A. Tamaru, and A. Valdes, "Next generation intrusion detection expert system (NIDES)." Science Laboratory, SRI International., Menlo Park, CA, USA., Reporte Técnico SRI-CSL-95-0, Mayo,1994 1994.

[8] D. Anderson, T. F. Lunt, H. Javitz, A. Tamaru, and A. Valdes, "Detecting Unusual Program Behavior Using the Statistical Component of the Next-generation Intrusion Detection Expert System NIDES)," Computer Science Laboratory,SRI International., Menlo Park, CA, USA, Reporte Técnico USA SRI-CSL-95-06, Mayo, 1995 1995.

[9] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans.," *Journal of Computer Security.*, vol. 10, pp. 105–136., 2002.

[10] N. Ye, S. M. Emran, Q. Chen, and S. Vilbert, "Multivariate statistical analysis of audit trails for host-based intrusion detection," *IEEE Transactions on Computers*, vol. 51, pp. 810 - 820, 2002.

[11] C. Kruëgel, T. Toth, and E. Kirda, "Service specific anomaly detection for network intrusion detection," in *2002 ACM symposium on Applied computing*, Madrid, Spain, 2002, pp. 201–208.

[12] R. A. Maxion and F. E. Feather, "A case study of Ethernet anomalies in a distributed computing environment," *IEEE Transactions on Reliability*, vol. 39, pp. 433 - 443, 1990.

[13] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, "A sense of self for unix processes," in *IEEE Symposium on Research in Security and Privacy*, Oakland, CA, USA, 1996, pp. 120–128.

[14] S. A. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion Detection using sequences of system calls," *Journal of Computer Security.*, vol. 6, pp. 151–180, 1998.

[15] W. W. Cohen, "Fast effective rule induction," in *12th International Conference on Machine Learning*, Tahoe City, CA,, 1995, pp. 115–123.

[16] E. Eskin, S. J. Stolfo, and W. Lee, "Modeling system calls for intrusion detection with dynamic window sizes," in *DARPA Information Survivability Conference & Exposition II*, Anaheim, CA, 2001, pp. 165–175.

[17] C. Warrender, S. Forrest, and B. Pearlmutter, "Detecting intrusions using system calls: alternative data models," in *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1999, pp. 133–145.

[18] D. Heckerman, "A Tutorial on Learning With Bayesian Networks," Microsoft Research, Reporte Técnico MSRTR-95-06, Marzo, 1995 1995.

[19] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, "Bayesian event classification for intrusion detection," in *19th Annual Computer Security Applications Conference*, Las Vegas, NV, 2003.

[20] A. Valdes and K. Skinner, "Adaptive model-based monitoring for cyber attack detection," in *Recent Advances in Intrusion Detection Toulouse* France, 2000, pp. 80-92.

[21] N. Ye, M. Xu, and S. M. Emran, "Probabilistic networks with undirected links for anomaly detection," in *IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, West Point, NY,, 2000.

[22] P. A. Porras and P. G. Neumann, "EMERALD: event monitoring enabling responses to anomalous live disturbances," in *20th NIST-NCSC National Information Systems Security Conference*, Baltimore, MD, USA, 1997, pp. 353–365.

[23] R. A. Calvo, M. Partridge, and M. A. Jabri, "A comparative study of principal component analysis techniques," in *Ninth Australian Conference on Neural Networks*, Brisbane, Qld, Australia, 1998.

[24] H. Hotelling, "Analysis of a complex of statistical variables into principal components," *Journal of Educational Psychology*, vol. 24, pp. 417 – 441, 498 – 520., 1993.

[25] W. Wang and R. Battiti, "Identifying intrusions in computer networks with principal component analysis," in *The First International Conference on Availability, Reliability and Security*, Vienna, Austria, 2006, pp. 270 – 279.

[26] M. L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L. Chang, "A novel anomaly detection scheme based on principal component classifier," in *IEEE Foundations and New Directions of Data Mining Workshop*, Melbourne, FL, USA, 2003, pp. 172–179.

[27] N. Ye and Y. Z. C. M. Borror, "Robustness of the Markov-chain model for cyber-attack detection," *IEEE Transactions on Reliability*, vol. 53, pp. 116-123., 2004.

[28] D. Y. Yeung and Y. Ding, "Host-based intrusion detection using dynamic and static behavioral models," in *Pattern Recognition*. vol. 36, 2003, pp. 229 – 243.

[29] M. V. Mahoney and P. K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic Department of Computer Sciences," Florida Institute of Technology, Melbourne, FL, USA, Reporte Técnico CS-2001-4, Abril, 2001 2001.

[30] M. V. Mahoney and P. K. Chan, "Learning Models of Network Traffic for Detecting Novel Attacks Computer Science Department," Florida Institute of Technology, Melbourne, FL, USA, Reporte Técnico CS-2002-8,, Agosto, 2002 2002.

[31] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 34, pp. 579–595., 2000.

[32] M. V. Mahoney and P. K. Chan, "Learning nonstationary models of normal network traffic for detecting novel attacks," in *Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Edmonton, Canada, 2002, pp. 376–385.

[33] W. Lee, R. A. Nimbalkar, K. K. Yee, S. B. Patil, P. H. Desai, T. T. Tran, and S. J. Stolfo, "A data mining and CIDF based approach for detecting novel and distributed intrusions," in *3rd International Workshop on Recent Advances in Intrusion Detection (RAID 2000)*, Toulouse, France, 2000, pp. 49 – 65.

[34] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," in *7th USENIX Security Symposium (SECURITY-98)*, Berkeley, CA, USA, 1998, pp. 79 – 94.

[35] W. Lee, S. J. Stolfo, and K. W. Mok, "Adaptive intrusion detection: a data mining approach," *Artificial Intelligence Review* vol. 14, pp. 533–567., 2000.

[36] R. Grossman, "Data Mining: Challenges and Opportunities for Data Mining During the Next Decade," Reporte Técnico 1997.

[37] J. R. Quinlan, "C4.5: Programs for Machine Learning," in *Morgan Kaufman Publishers* Los Altos, CA: Morgan Kaufman Publishers, 1993.

[38] W. Lee, S. J. Stolfo, and K. W. Mok, "A data mining framework for building intrusion detection models," in *IEEE Symposium on Security and Privacy*, Oakland, CA 1999, pp. 120–132.

[39] S. M. Bridges and R. B. Vaughn, "Fuzzy data mining and genetic algorithms applied to intrusion detection," in *National Information Systems Security Conference*, Baltimore, MD, 2000.

[40] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," in *19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS)*, Atlanta, GA, 2000, pp. 301–306.

[41] W. Li, "Using Genetic Algorithm for Network Intrusion Detection," C.S.G., Reporte Técnico 2004.

[42] M. M. Pillai, J. H. P. Eloff, and H. S. Venter, "An approach to implement a network intrusion detection system using genetic algorithms," in *2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, Stellenbosch, Western Cape, South Africa, 2004, pp. 221–228.

[43] J. Gomez and D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," in *IEEE Workshop on Information Assurance*, United States Military Academy, NY, 2001.

[44] M. Crosbie and G. Spafford, "Applying genetic programming to intrusion detection," in *AAAI Symposium on Genetic Programming*, Cambridge, MA, 1995, pp. 1–8.

[45] A. K. Ghosh, C. Michael, and M. Schatz, "A real-time intrusion detection system based on learning program behavior," in *Third International Workshop on Recent Advances in Intrusion Detection* Toulouse, France, 2000, pp. 93–109.

[46] A. K. Ghosh and A. Schwartzbard, "A study in using neural networks for anomaly and misuse detection," in *Eighth USENIX Security Symposium*, Washington, DC, 1999, pp. 141–151.

[47] A. K. Ghosh, A. Schwartzbart, and M. Schatz, "Learning program behavior profiles for intrusion detection," in *1st USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, CA, USA, 1999.

[48] J. L. Elman, "Finding structure in time," in *Cognitive Science*. vol. 14, 1990, pp. 179–211.

[49] M. Ramadas and S. O. B. Tjaden, "Detecting anomalous network traffic with self-organizing maps," in *6th International Symposium on Recent Advances in Intrusion Detection*, Pittsburgh, PA, USA, 2003, pp. 36–54.

[50] W. Lee, S. J. Stolfo, P. K. Chan, E. Eskin, W. Fan, M.Miller, S. Hershkop, and J. Zhang, "Real time data mining-based intrusion detection," in *Second DARPA Information Survivability Conference and Exposition*, Anaheim, CA, 2001, pp. 85–100.

[51] K. M. C. Tan and R. A. Maxion, "Determining the operational limits of an anomaly-based intrusion detector," *IEEE Journal on Selected Areas in Communication*, vol. 2, pp. 96–110, 2003.

[52] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen net for anomaly detection in network security," *IEEE Transactions on Systems, Man and Cybernetics —PART B: Cybernetics*, vol. 35, pp. 302–312, 2005.

[53] V. Barnett and T. Lewis, "Outliers in Statistical Data," *Wiley*, 1994.

[54] C. C. Aggarwal and P. S. Yu, "Outlier detection for high dimensional data," in *ACM SIGMOD International Conference on Management of Data*, 2001, pp. 37–46.

[55] M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," in *ACM SIGMOD International Conference on Management of Data*, Dallas, TX, USA, 2000, pp. 93–104.

[56] S. Ramaswamy, R. Rastogi, and K. Shim, "Efficient algorithms for mining outliers from large data sets," in *ACM SIGMOD International Conference on Management of Data*, Dallas, TX, USA, 2000, pp. 427–438.

[57] V. Hautamaki, I. Karkkainen, and P. Franti, "Outlier detection using k-nearest neighbour graph," in *17th International Conference on Pattern Recognition*, Los Alamitos, CA, USA, 2004, pp. 430–433.

[58] Y. Liao and V. R. Vemuri, "Use of K-nearest neighbor classifier for intrusion detection," *Computers & Security*, vol. 21, pp. 439–448, 2002.

[59] L. Ertöz, E. Eilertson, A. Lazarevic, P. N. Tan, V. Kumar, J. Srivastava, and P. Dokas, "The MINDS - Minnesota intrusion detection system," in *Next Generation Data Mining*, MIT Press, Boston, 2004.

[60] R. Agrawal, T. Imielinski, and A. Swami, "Mining association rules between sets of items in large databases," in *ACM SIGMOD Conference on Management of Data*, Washington, DC, 1993, pp. 207–216.

[61] J. Hipp, U. Güntzer, and G. Nakhaeizadeh, "Algorithms for association rule mining - a general survey and comparison," in *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Boston, MA, USA, 2000, pp. 58–64.

[62] D. Barbará, J. Couto, S. Jajodia, and N. Wu, "ADAM: a testbed for exploring the use of data mining in intrusion detection," *ACM SIGMOD Record:SPECIAL ISSUE: Special section on data mining for intrusion detection and threat analysis*, 2001.

[63] E. Tombini, H. Debar, L. Mé, and M. Ducassé, "A serial combination of anomaly and misuse IDSes applied to HTTP traffic," in *20th Annual Computer Security Applications Conference*, Tucson, AZ, USA, 2004.

[64] D. Newman, J. Snyder, and R. Thayer, "Crying wolf:False alarms hide attacks," in Network World, 2002.

[65] S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection " *ACM Transactions on Information and System Security*, vol. 3, pp. 186–205, 2001.

[66] J. Gaffney and J. Ulvila, "Evaluation of intrusion detectors: a decision theory approach," in *2001 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2001, pp. 50 -61.

[67] S. J. Stolfo, W. Fan, and W. Lee, "Cost-based modeling for fraud and intrusion detection: results from the JAM Project," in *DARPA Information Survivability Conference & Exposition*, 2000, pp. 130 - 144.

[68] J. McHugh, "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection," *ACM Transactions on Information and System Security,* vol. 3, pp. 262–294, 2000.

[69] K. M. C. Tan, K. S. Killourhy, and R. A. Maxion, "Undermining an anomaly-based intrusion detection system using common exploits," in *Fifth International Symposium on Recent Advances in Intrusion Detection*, Zurich, Switzerland, 2002, pp. 54–73.

[70] S. Axelsson, "Research in intrusion-detection systems: a survey," Chalmers University of Technology, Goteborg, Sweden, Reporte Técnico 98-17, 1998.

[71] J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo, "Anomaly detection methods in wired networks: a survey and taxonomy," *Computer Communications,* vol. 27, pp. 1569–1584, 2004.

[72] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers, "Insider threat study: computer system sabotage in critical infrastructure sectors," U.S.S. Service and C.M.U. Software Engineering Institute, Reporte Técnico 2005.