REDES INALÁMBRICAS DE CONTROL

KAREN NATALIA GUTIÉRREZ ORTIZ
GUSTAVO ADOLFO PINTO HERRERA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
MINOR EN AUTOMATIZACIÓN INDUSTRIAL
CARTAGENA
2006

REDES INALÁMBRICAS DE CONTROL

KAREN NATALIA GUTIERREZ ORTIZ
GUSTAVO ADOLFO PINTO HERRERA

Monografía para optar por el título de
Ingeniero Electrónico con énfasis en Automatización Industrial

Director
FRANCISCO TRESPALACIOS
Ingeniero Electrónico

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
MINOR EN AUTOMATIZACIÓN INDUSTRIAL
CARTAGENA
2006

Cartagena de Indias D.T. y C, Octubre 17 de 2006

Señores
Comité evaluador
Programa de Ingeniería Eléctrica y Electrónica
Universidad Tecnológica de Bolívar

Cordial Saludo

Nos dirigimos a ustedes con el fin de presentar la monografía titulada "**REDES INALÁMBRICAS DE CONTROL**", desarrollada para su estudio y evaluación como requisito fundamental del Minor en Automatización Industrial, para optar al titulo de Ingeniero Electrónico.

En espera que esta cumpla con las normas pertinentes establecidas por la institución quedamos a su disposición para cualquier aclaración.

Karen Natalia Gutiérrez Ortiz
c.c # 45'542.942 de Cartagena

Gustavo Adolfo Pinto Herrera
c.c # de 8.854.703 de Cartagena

Francisco Trespalacios Vergara
Director de la Monografía

Nota de aceptación

Firma del jurado

Firma del jurado

Cartagena de Indias D.T. y C, Octubre de 2006

A mis padres, Manuel y Odalis,
y a mi novio Alberto
principales motores en mi vida.

Karen Gutiérrez Ortiz.

En memoria de mis abuelas
Micaela y Asteria, y a mis padres
Emiro y Evelia, con su guía y apoyo
conseguí culminar exitosamente
este camino.

Gustavo A. Pinto Herrera

AGRADECIMIENTOS

A Manuel Gutierrez y Odalis Ortiz por su confianza y motivación.

A Alberto Gutierrez, ingeniero mecánico, por sus aportes y constante motivación.

A Francisco Trespalacios, ingeniero electrónico y director de esta monografía, por su orientación y colaboración.

Al personal de Mantenimiento Industrial del Cerrejón por sus aportes.

A José Luís Villa, ingeniero electrónico, por su colaboración.

A todos los profesores del Minor en Automatización Industrial 2005 – 2006 por compartir sus valiosos conocimientos.

Octubre 17 de 2006, Cartagena – Bolívar

Señores
Universidad Tecnológica de Bolívar

Yo Karen Natalia Gutierrez Ortiz, identificada con el numero de cedula 45.542.942 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catalogo online de la Biblioteca de la Universidad.

Karen Natalia Gutierrez Ortiz
cc #45.542.942 de Cartagena

Octubre 17 de 2006, Cartagena – Bolívar

Señores
Universidad Tecnológica de Bolivar

Yo Gustavo Adolfo Pinto Herrera, identificado con el numero de cedula 8.854.703 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para hacer uso de mi trabajo de grado y publicarlo en el catalogo online de la Biblioteca de la Universidad.

Gustavo Pinto Herrera
c.c # de 8.854.703 de Cartagena

CONTENIDO

Pag.

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ADLS (*ASIMETRIC DIGITAL SUBSCRIBER LINE O LÍNEA DIGITAL DE CONEXIÓN ASIMÉTRICA*): Se trata de una técnica para transmitir datos por la línea telefónica de un modo asimétrico, ya que la velocidad de recepción de datos es diferente a la de envío. Permite enviarlos desde 128 Kbps hasta 612 Kbps, y recibirlos desde (evoluciona) 1,544 Mbps hasta 6 Mbps. Requiere un MODEM especial.

ANTENAS DIRECCIONALES: La señal que emitida por este tipo de antenas como su nombre lo indica es direccional y proporciona una ganancia que oscila entre los 15 y los 21 dBi. Hay que enfocarla directamente al lugar con el que se quiere enlazar.

ANTENAS OMNIDIRECCIONALES: Se les llama también antenas de fuste vertical. Se utilizan principalmente para emitir la señal en todas las direcciones. En realidad la señal que emite en es forma de óvalo, y sólo emite en plano (no hacia arriba ni hacia abajo).

BRIDGE: dispositivo que soporta comunicaciones entre redes de área local. Los bridges pueden ser equipados para soportar el servicio Frame Relay a las LAN que sirven. Un bridge con capacidad Frame Relay encapsula las tramas de la LAN en tramas de Frame Relay para poder transmitirlas a través de la red hacia la LAN

de destino. Los bridges son generalmente utilizados para interconectar segmentos de LAN por medio de una WAN.

BSSID, BASIC SERVICE SET IDENTIFICATION: Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo Ad-Hoc.

DHCP (*DYNAMIC HOST CONFIGURATION PROTOCOL*): EL protocolo de configuración dinámica de host es un estándar IP diseñado para simplificar la administración de la configuración IP del host. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica a los clientes DHCP de la red, de direcciones IP y otros detalles de configuración relacionados.

DSSS: Esquema de modulación de amplio espectro en el que cada símbolo (grupo de bits) se multiplica por un código de spreading llamado secuencia de chip para aumentar la banda de frecuencias de la señal. El aumento de ancho de banda está controlado por la norma IEEE 802.11.

ESSID, EXTENDED SERVICE SET IDENTIFICATION: Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

ETSI (*EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE*): Instituto Europeo de Normas de Telecomunicaciones) es un organismo sin ánimo de lucro creado al objeto de disponer del foro adecuado para la elaboración de las

normas de telecomunicación que faciliten la estandarización del sector, y por lo tanto el avance hacia el Mercado Único Europeo

HIPERLAN: HIgh Performance Radio Local área Network.

HOPS (SALTO): Término utilizado para denominar cada uno de los pasos que es preciso dar para llegar de un punto de origen a otro de destino a lo largo de una red con la ayuda de direccionadores (routers).

HUB: Dispositivo de red multipuerto para la interconexión de equipos vía Ethernet o wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

MULTIPATH: Es la variación de la señal causada cuando las señales de radio toman varios caminos desde el transmisor al receptor.

NIC: Network Interface Card o tarjeta de interfaz de red, es un dispositivo electrónico que permite a una DTE (Data Terminal Equipment) computador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom, etc)

SSID (SERVICE SET IDENTIFICATION): Es nombre que se le da a la red inalámbrica para que todos los dispositivos la reconozcan y consta de 32

caracteres alfanuméricos. En principio, todos los equipos que estén bajo el mismo SSID, son "visibles" por todos y de esta manera se pueden comunicar.

WPAN: Área de red personal inalámbrica.

INTRODUCCION

Desde el principio una de las grandes necesidades del hombre ha sido la comunicación en todos los campos de la vida. Desde siempre la curiosidad lo ha llevado a diseñar, desarrollar y perfeccionar técnicas para modernizar cada vez mas algo tan básico como enviar y recibir un mensaje. Si a este necesidad de comunicación del hombre se le suma la constate lucha por optimizar por medio de la automatización y el control todos los procesos aparecen las ***redes industriales de control.***

Pero con el crecimiento de la industria también aparecen nuevos retos si se tiene en cuenta, por ejemplo, que el cuarto de control en una planta de tratamiento de agua puede encontrarse a varios cientos de metros del lugar en donde se encuentra el deposito principal en donde se almacena el agua que se desea tratar cuyo nivel debe ser monitoreado constantemente. Como este son muchos los casos y por ende, muchas las variables que pueden existir en un proceso industrial en el que se requiere constante monitoreo y control a distancia o en lugares de difícil acceso en donde pueden ser de mucha ayuda (o la única solución) las **redes inalámbricas de control.**

A continuación se presenta un documento que contiene Información básica sobre el paso y el presente de las redes inalámbricas de control, así como las técnicas para la modulación de las señales utilizadas para la transmisión como los métodos existentes para brindar seguridad a este tipo de redes. Se enumeran cada uno de los elementos básicos que cada red inalámbrica debe tener.

Por ultimo se resume toda la teoría presentando tres aplicaciones reales de redes inalámbricas de control, como también los pasos necesarios para implementar una red inalámbrica de control monitorear y control el proceso de extracción, transporte y almacenamiento de agua proveniente de los pozos subterráneos que abastecen la Planta de Agua de la Mina de Carbón del Cerrejón Zona Norte.

1. MARCO TEÓRICO

1.1 UN POCO DE HISTORIA

En Mayo de 1985 la FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en Spread Spectrum (SS), con las opciones DS (Direct Sequence) y FH (Frequency Hopping, tras varios años de investigación y experimentos con infrarrojos y microondas. Pero esto no sucedió antes de que se hablara por primera vez de redes inalámbricas de manera oficial en 1979 cuando se hicieron públicos los resultados de un experimento consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica, realizado por ingenieros de IBM en Suiza.

Entre 1985 hasta 1990 se consiguieron los resultados que demostraban un desarrollo en la investigación del campo de las LAN inalámbricas (*WLAN: Wirless Local área Network*) con aplicación empresarial. Estos resultados fueron presentados en 1991 en donde s mostraban redes que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802. Hasta entonces, estas redes habían tenido una aceptación marginal en el mercado. Las razones eran varias:

✓ No existía una norma y menos un estándar, lo que ocasionaba que los diferentes fabricantes desarrollaran sus propias soluciones, utilizando frecuencias y tecnologías muy distintas y normalmente incompatibles.

✓ Altos precios que reflejan los costos de investigación para desarrollar soluciones tecnológicas propietarias.

✓ Reducidas prestaciones si las comparamos con sus homologas cableadas: las redes inalámbricas únicamente permitían el soporte de datos, mientras que por una red de cableado era posible llevar multitud de aplicaciones tanto de voz, como de datos, vídeo, etcétera, y además, velocidades de transmisión significativamente menores.

Innumerables investigaciones y el establecimiento de estándares, han llevado a las WLAN a ser parte esencial en todos los campos donde los que se desee implementar, por medio del establecimiento de los elementos básicos, las velocidades de transmisión y las técnicas de modulación, Información utilizada por los fabricantes de productos de comunicación y automatización industrial para diseñar equipos que, en la actualidad son perfectamente compatibles con las redes inalámbricas que cumplan con su mismo estándar de fabricación.

1.2 REDES DE ÁREA LOCAL (LAN)

LAN es la abreviatura de **Local área Network** (Red de Área Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación

más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

1.2.1 LAN's inalámbricas (WLAN): estas redes más que venir a reemplazar a las cableadas aparecen como una alternativa cuando la transmisión es a grandes distancias o en lugares de difícil acceso. Además, por medio un la topología Infraestructura, también se convierte en una extensión de la LAN tradicional.

Las WLAN han adquirido importancia en muchos campos como en la industria, gobierno, incluido el de la medicina. Las redes inalámbricas se implementan a partir de enlaces basados en el uso de la tecnología de microondas y en menor medida de infrarrojos.

Las redes inalámbricas pueden dividirse en ***Redes inalámbricas de área local*** y ***Redes inalámbricas para comunicación móvil***.

La diferencia fundamental entre ambas radica en los modos de transmisión. Las LAN inalámbricas emplean transmisores y receptores que se encuentran en los edificios en que se usan mientras que las comunicaciones móviles inalámbricas usan las compañías de telecomunicaciones telefónicas u otros servicios públicos en la transmisión y recepción de las señales.

¿Como funciona una red inalámbrica?: Cada puerto de acceso tiene una lista de los clientes inalámbricos con los que puede asociarse. Cuando un cliente

inalámbrico, por ejemplo un computador, está listo para comunicarse con la red, su tarjeta de red inalámbrica difunde una señal de radio. Cuando el punto de acceso detecta una señal de un cliente inalámbrico asociado, la señal es contestada y se establece una conexión con la red. Un cliente inalámbrico puede estar asociado con varios puntos de acceso diferentes, bien sea por una mayor cobertura mediante puntos de acceso situados en un área de servicio específica o porque el cliente inalámbrico se está desplazando de un punto de acceso a otro punto de acceso que está dentro del área de cobertura extendida.

1.2.2 Redes Inalámbricas en la industria: El hombre actual, en su afán de simplificar y optimizar los procesos, cada día busca la forma de aprovechar los avances de la tecnología; es así como la principal aplicación de las redes inalámbricas se encuentra en la industria en donde se conjugan todos los elementos básicos, que serán detallados mas adelante, con cada uno de los dispositivos propios del proceso para dar paso a grandes y sofisticadas redes inalámbricas de control que frente a las redes tradicionales ofrecen las siguientes ventajas, sea cual sea el proceso en el que se desee implantar :

- ✓ **Movilidad:** Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.

- ✓ **Facilidad de instalación:** Evita obras para tirar cable por muros y techos.

- ✓ **Flexibilidad:** Permite llegar donde el cable no puede.

✓ **Reducción de costos:** Cuando se dan cambios frecuentes o el entorno es muy dinámico el coste inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.

✓ **Escalabilidad:** El cambio de topología de red es sencillo y trata igual pequeñas y grandes redes. Un buen Hub inalámbrico deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red. Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a su red inalámbrica con un adaptador USB inalámbrico o un Ethernet Client Bridge.

Las aplicaciones industriales que pueden llegar a tener las redes inalámbricas de control son múltiples, basta con estudiar muy bien el proceso y diseñar la red ideal tendiendo en cuenta factores como la distancia, es espacio, el terreno, la misma naturaleza del proceso y hasta el presupuesto, entre otros. Este documento presenta aplicaciones reales de las redes ***inalámbricas de control*** pero es bueno tener claro los conceptos básicos que tienen que ver con la conformación, la modulación, la seguridad y los estándares bajo los cuales se rigen las red LAN y WLAN.

2 ELEMENTOS DE UNA RED INALÁMBRICA

2.1 ELEMENTOS BÁSICOS DE UNA RED INALÁMBRICA

Para llevar a cabo el diseño y posterior instalación de una red inalámbrica es necesario conocer los elementos básicos que deben estar presentes en la configuración. Dependiendo de la aplicación de la red se irán añadiendo los dispositivos correspondientes.

2.1.1 Cliente: Cada computador o terminal que acceda a la red como cliente debe estar equipado con una tarjeta de red. Las más comunes son de tipo PC Card (para portátiles) aunque pueden conectarse a una ranura PCI estándar mediante una tarjeta adaptadora.

Figura 2.1 Equipos típicos que representan los clientes inalámbricos

2.1.2 Puntos de Acceso (PA): Este dispositivo, que funciona como un HUB tradicional, permite agregar fácilmente y de una manera rápida otros dispositivos

inalámbricos que amplían su cobertura y su operabilidad, así como la ampliación a zonas inaccesibles de una red LAN convencional.

A pesar de que varias líneas de productos inalámbricos ofrecen el PA como un modulo compacto, es posible utilizar un computador como PA, si este posee una tarjeta de red configurada para tal fin.

Figura 2.2 Puntos Acceso

2.1.3 Tarjetas de red (TR): Es el dispositivo que se instala del lado del usuario inalámbrico de la red (WLAN), llamada también *Network Interface Card (NIC)* o **tarjeta adaptadora**. Así como las tradicionales placas de red que se instalan en un PC para acceder a una red LAN cableada, las Tarjetas de Red Inalámbricas dialogan con el Punto de Acceso (PA) quien hace de punto de acceso a la red cableada.

La *figura 2.3* muestra tres tipos diferentes de tarjetas de Red Inalámbrica que se clasifican según el tipo de conexión necesaria a la computadora:

USB ***PCMCIA*** ***PCI***

Figura 2.3: Tipos de tarjetas de red

✓ ***Tarjeta de Red Inalámbrica USB:*** Esta se utiliza cuando la conexión a la computadora se realiza a través del puerto USB de la misma. Suele utilizarse estos adaptadores cuando se desea una conexión externa fácilmente desconectadle o portable.

✓ ***Tarjeta de Red Inalámbrica PCI:*** Es utilizada cuando la conexión a la computadora se realiza a través de su slot interno PCI. Suele utilizarse estos adaptadores cuando se desea que la instalación dentro del PC.

✓ ***Tarjeta de Red Inalámbrica PCMCIA:*** Ideales cuando la conexión a la computadora se realiza a través de su slot PCMCIA, casi siempre en computadores portátiles.

2.1.4 Antenas: Se utilizan solamente para amplificar la señal, así que no siempre son necesarias. Las antenas direccionales emiten en una sola dirección y es preciso orientarlas "a mano". Dentro de este grupo están las de Rejilla, las Yagi,

las parabólicas, las "Pringles" y las de Panel. Las antenas omnidireccinales emiten y reciben señal en 360º.

2.1.5 Pigtail: Es simplemente el cable que conecta la antena con la tarjeta de red. Es el único cable necesario en una WLAN y hay que vigilar posibles pérdidas de señal.

2.2 ELEMENTOS DE UNA RED INALÁMBRICA DE CONTROL

Para el caso de una red inalámbrica de control, es necesario contar con elementos que permitan, además de enviar y recibir Información, manipular las variables que intervienen en el proceso que se desee controlar. Los siguientes son algunos de los elementos que están presentes en este tipo de redes:

2.2.1 PLC (programable logia controller) o API (Automata programable industrial): este es un equipo electrónico, programable en lenguaje no informático, que sustituye los circuitos auxiliares o de mando de los sistemas automáticos. A él se conectan los captadores (finales de carrera, pulsadores, etc...) por una parte, y los actuadores (bobinas de contactores, lámparas, peque os receptores, etc...) por otra y diseñado para controlar en tiempo real y en ambiente de tipo industrial, procesos secuénciales, electrónico, etc...

Composición básica de un PLC:

- ✓ Fuente de alimentación
- ✓ CPU
- ✓ Módulo de entrada
- ✓ Módulo de salida
- ✓ Terminal de programación
- ✓ Periféricos.

2.2.2 Unidad remota de control o terminales remotos (RTU, remot terminal units): RTU se le llama a cualquier dispositivo (sea este inteligente o no, autónomo o asistido, interrogado o alarmístico), ubicado a una distancia considerable, que se encuentra en constante comunicación con un sistema central de control, servidor o Host. En realidad, los PLC's hacen parte de este grupo de dispositivos si se examina con detalle las características.

Composición básica de una RTU:

- ✓ Adquisidor de datos.
- ✓ CPU.
- ✓ Equipo de comunicaciones (radio y antena).
- ✓ Modem
- ✓ Fuente de alimentación (baterías o paneles solares).
- ✓ Batería de emergencia.
- ✓ Bornero interfase de I/O.

2.2.3 Radio Modem: Cualquier tipo de módem (MOdulador/DEModulador) se encarga de convertir un flujo de datos digitales banda base en una señal analógica apropiada para ser transmitida sobre el medio, y viceversa. Los radio módems están destinados a aplicaciones en las cuales es necesario transmitir la señal vía radio, como por ejemplo interconexión de ordenadores a través de LAN o MAN inalámbricas, sistemas MMDS o LMDS, envío y recepción de mensajes o faxes a través de GSM, telemetría, localización automática de vehículos, vending, etc.

Así pues, los radio módems deben estar preparados para transmitir sobre un entorno más hostil que el cable, a menudo sujeto a desvanecimientos, propagación multicamino (multipath) o interferencias. Esto obliga a emplear mecanismos de modulación distintos a los empleados en los módems de cable. Al mismo tiempo, dado que en algunos casos es necesario dotar de movilidad al dispositivo, aparecen nuevos problemas como el tamaño o la autonomía del dispositivo. Para la transmisión, los radio módems disponibles comercialmente suelen utilizar las bandas ISM de 900 MHz (902-928 MHz), 2,4 GHz (2400-2483,5 MHz) y 5,8 GHz (5725-5850 MHz).

2.2.4 Sistemas de Posicionamiento Global (GPS): Para proporcionar geoposicionamientos en tiempo real y capacidades de control de la posición, los GPS incorporan una capacidad extra para ingeniería móvil, que aumenta considerablemente su eficacia. Con los GPS, los servidores de geoingeniería pueden hacer “localizaciones intuitivas”. Esta intuición en la localización del usuario en el campo permite al servidor anticipar la información que necesitará el usuario y transmitirla automáticamente. También permiten sistemas de aviso que determinan a quien enviar al lugar de emergencia o incidente de mantenimiento no

programado basándose en la proximidad del personal así como en las capacidades y equipo disponible apropiado para el suceso.

3 TOPOLOGÍAS PARA REDES INALÁMBRICAS

El grado de complejidad de una red de área local inalámbrica es variable, esto depende de las necesidades a cubrir y los requerimientos del sistema que se deseen implementar, por lo tanto se pueden utilizar diversas configuraciones de red. A continuación se describen las topologías utilizadas para redes inalámbricas para las redes inalámbricas las dos principales configuraciones son ***Ad – Hoc*** e ***Infraestructura***.

3.1 AD HOC O MANET'S (IBSS: SERVICIO BÁSICO INDEPENDIENTE)

En la *figura 3.1* se muestra la configuración básica de una red Ad - Hoc, llamada también **punto a punto** o **peer to peer** en donde existe comunicación directa entre terminales móviles equipados con la correspondiente tarjeta adaptadora o **tarjeta de red** para comunicaciones inalámbricas; aquí, los dispositivos simplemente envían los paquetes de información "al aire", con la esperanza de lleguen a su destino. Este tipo de red no requiere infraestructura fija ni administración centralizada, donde las estaciones, además de ofrecer funcionalidades de estación final deben proporcionar también servicio de encaminamiento, retransmitiendo paquetes entre aquellas estaciones que no

tienen conexión inalámbrica directa. Es así como las tareas de señalización y la sincronización son controladas por una estación.

Para esta topología la distancia a la que se encuentran ubicada los nodos juegan un papel muy importante ya que a mayor dispersión geográfica de cada nodo, mas dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si.

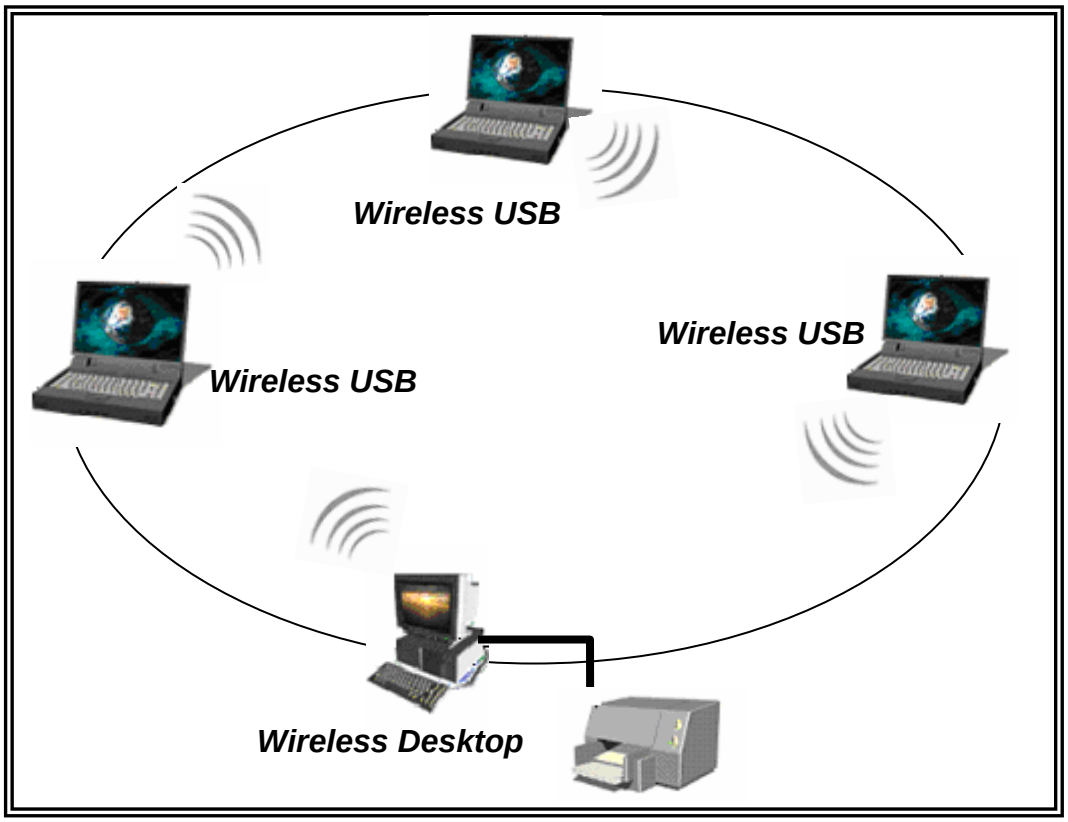


Figura 3.1 Configuración de una red Ad Hoc

3.1.1 Características de la red ad hoc: la red Ad hoc tiene varios inconvenientes comparada con las redes infraestructura, uno de ellos es que este tipo de red no permite la posibilidad de trasmitir tramas entre dos estaciones que no se "oyen" mutuamente. De esta manera frente a la topología Infraestructura, la Ad – hoc ofrece menor cobertura, pero en compensación permite un menor retraso en la transmisión y mayor capacidad.

3.2 INFRAESTRUCTURA

En esta topología una red inalámbrica se conecta a una red cableada por medio un dispositivo llamado **Punto de Acceso (PA)**, que es el nodo central y funciona como un *Hub* tradicional, enviando directamente los paquetes de información a cada computador de la red. Para poder establecer la comunicación, todos los nodos deben estar dentro de la zona de cobertura del PA.

Con este nuevo elemento es posible doblar el alcance de la red inalámbrica ya que la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso. Además, los puntos de acceso se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos.

3.2.1 Modo de funcionamiento de la red Infraestructura:

- ✓ **Identificación de PA's y redes disponibles:** El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas,

primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

- ✓ **Elección de red, verificación y asociación de PA's:** La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación mediante el cual el punto de acceso y la estación intercambian información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

- ✓ **Inicio de la transmisión:** En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas, pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica. El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones.

✓ **Acciones para evitar colisiones:** Entre las estaciones se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "*petición para emitir*" y "*listo para emitir*", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el PA y puede evitar transmitir durante ese intervalo.

✓ **La sincronización:** Entre las estaciones de la red, la señalización se controla mediante *las tramas de señalización periódicas* enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora.

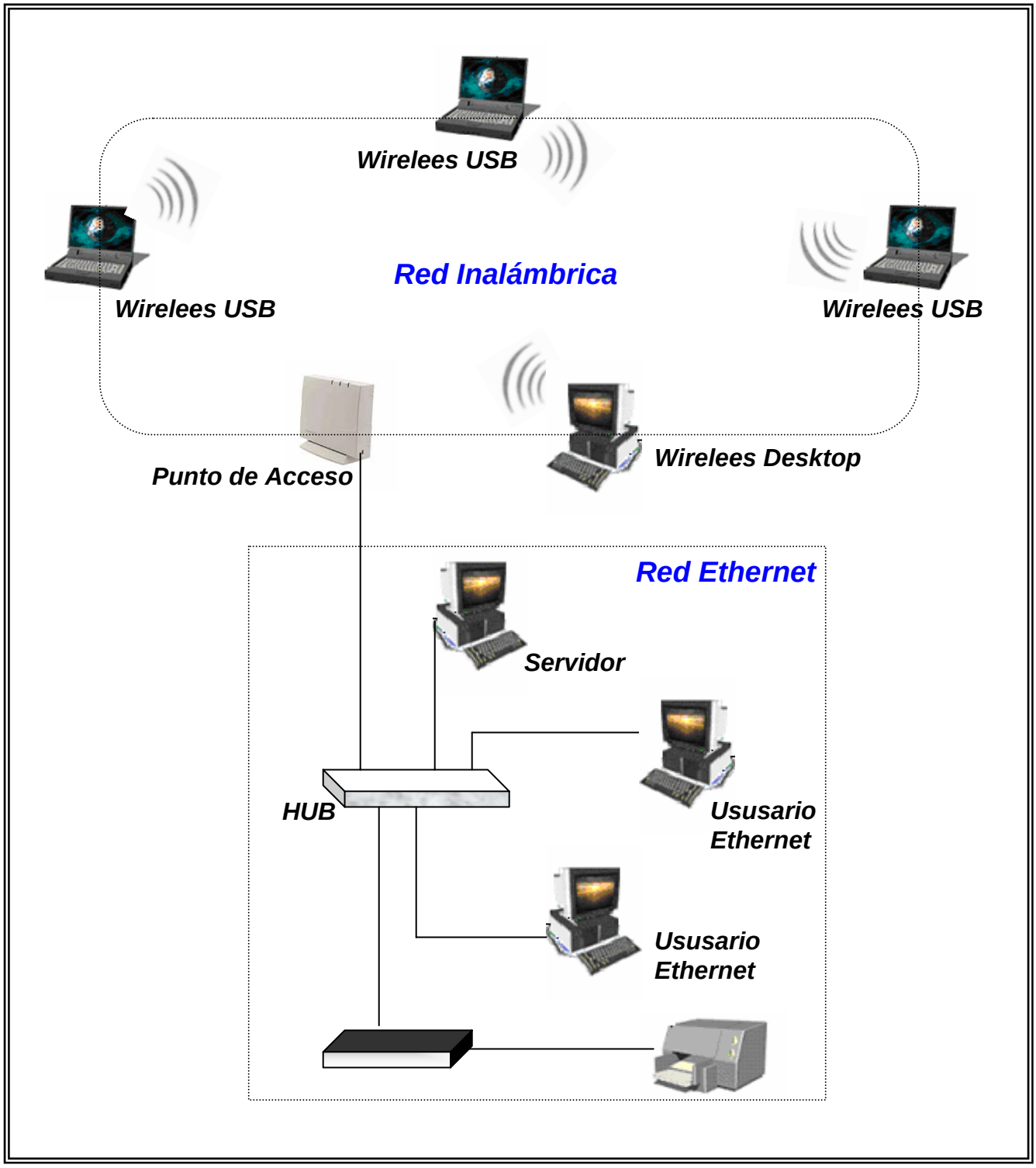


Figura 3.2 Configuración de una red Infraestructura

3.3 ELECCIÓN DE LA TOPOLOGÍA A IMPLEMENTAR.

La elección de la topología se realiza teniendo en cuenta las necesidades que se desean cubrir con la red, el espacio a cubrir, el número de clientes estimado, etc. Como se ha mencionado anteriormente, la topología Ad Hoc es la base para las diferentes configuraciones de los elementos que componen una red inalámbrica, incluso, la red Infraestructura esta compuesta por una red Ad – Hoc en donde los dispositivos inalámbricos se comunican a través de un Punto de Acceso con una red LAN tradicional. A partir de esto se presentan otros tipos de configuración dependiendo de los elementos que componen la red.

3.3.1 Puente constituido por PC dedicado o un servidor: Requiere la instalación de tarjetas ISA 16 bits o PC-CARD inalámbricos, según se trate de un PC (o TPV) o de un portátil respectivamente, en los correspondientes slot de expansión de los distintos equipos que constituyan la red. Aquí el punto de acceso debe poseer además una tarjeta normal como las que se utilizan para red cableada. Las características de las tarjetas inalámbricas son idénticas, salvo la configuración del NIC que actuara como *puente o bridge*, esta será especificada mediante software.

Resulta de especial importancia en la topología de infraestructura un adecuado estudio de la ubicación de los puntos de acceso respecto de las estaciones clientes y respecto de la red cableada para optimizar la instalación, o sea el acceso de los clientes inalámbricos y la no redundancia de dichos puntos de acceso.

3.3.2 Puente constituido por un Punto de Acceso: Requiere la instalación de un Punto de Acceso y de las tarjetas ISA o PC - CARD inalámbricos necesarias según el número de equipos que constituyan la red. Mediante la instalación de múltiples Puntos de Acceso como *bridges*, se hace posible unir varias células o redes basadas en PCs que a su vez estarían unidos por un *backbone*. Además de la ampliación de la zona de acción la subred inalámbrica proporciona la posibilidad de desplazarse dentro de ella por parte de los portátiles, que al perder contacto con su punto de acceso pasan a buscar otro, sin perder la comunicación.

Utilizando la combinación de cualquiera de las los configuraciones anteriormente descritas y antenas omnidireccionales o unidireccionales, surgen configuraciones aplicables para redes ubicadas en edificio. Las siguientes figuras ilustran la conexión entre tres edificios utilizando antenas unidireccionales (*figura 3.3*) y antenas omnidireccionales (*figura 3.4*)

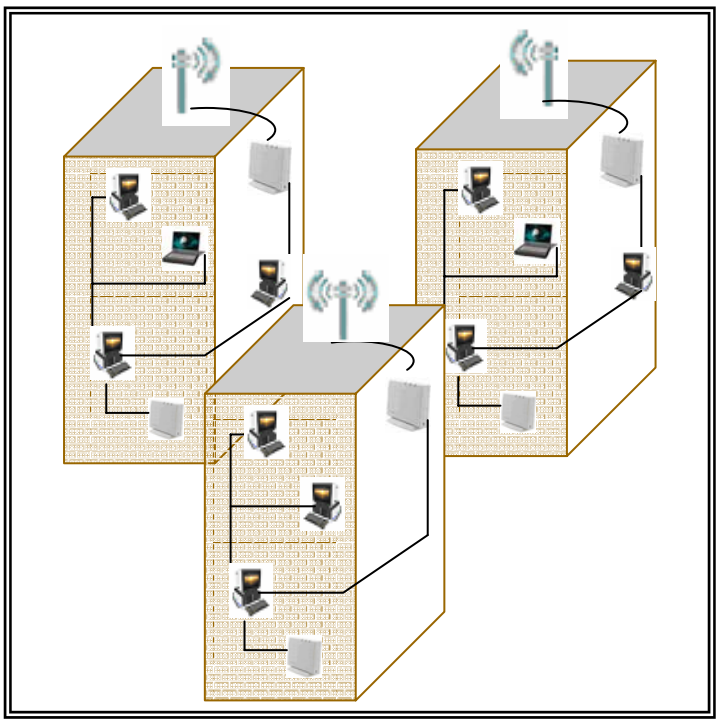


Figura 3.3 Edificios en conexión inalámbrica por medio de antenas unidireccionales.

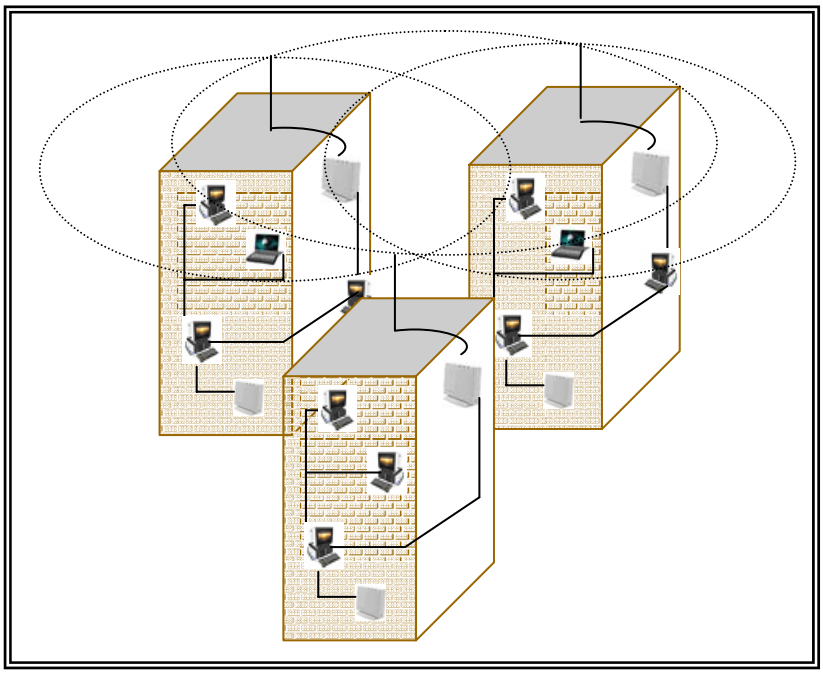


Figura 3.4 Edificios en conexión inalámbrica por medio de antenas omnidireccionales.

3.3.3 Mesh Networks: llamadas también redes acopladas, las redes **Mesh**, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los PA están dentro del rango de cobertura de alguna ***tarjeta de red*** **(TR)** que directamente o indirectamente está dentro del rango de cobertura del PA.

También permiten que las TRs se comuniquen independientemente del PA entre sí. Esto quiere decir que los dispositivos que actúan como TR pueden no mandar directamente sus paquetes al PA sino que pueden pasárselos a otros TRs para que lleguen a su destino.

Para que esto sea posible es necesario contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos o **Hops,** o con un número que aún no siendo el mínimo sea suficientemente bueno. Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

4. TÉCNICAS DE MODULACIÓN PARA DISTRIBUIR LA SEÑAL CONVENCIONAL EN EL ESPECTRO.

La Tecnología de Espectro Extendido es un tipo de modulación RF que utiliza señales de transporte cuya anchura de banda es intencionalmente mucho mayor que la información transportada tal que su nivel de energía o amplitud es muy cercano al nivel de ruido. Las principales características de esta tecnología son:

- ✓ Difícil de detectar o remodular.
- ✓ Puede ser distribuida en un amplio rango de frecuencias.
- ✓ Difícil de Interceptar
- ✓ Se desempeña en 2 tipos principales de modulación:
    - Secuencia Directa
    - Salto de Frecuencia (Frecuency Hopping)

La gran mayoría de los sistemas inalámbricos emplean la tecnología de Espectro Extendido (Spread Spectrum). La tecnología de Espectro Extendido está diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad. Es decir, más ancho de banda es consumida con respecto al caso de la transmisión en banda angosta, pero el 'trueque' (ancho de banda/potencia) produce una señal que es en efecto más fuerte y así más fácil de detectar por el receptor que conoce los parámetros de la señal de espectro extendido que está siendo difundida. Si el receptor no está sintonizado a la frecuencia correcta, una señal de espectro extendido se miraría como ruido en el fondo. Otra característica del espectro disperso es la *reducción de interferencia* entre la señal procesada y otras señales no esenciales o ajenas al sistema de comunicación.

4.1 FHSS, FRECUENCY HOPING SPREAD - SPECTRUM (*ESPECTRO – EXTENDIDO DE SALTO DE FRECUENCIAS*)

Esta técnica esta basada en la transmisión en diferentes bandas de frecuencias, produciéndose saltos de una a otra de una forma aleatoria que es imposible

predecir, para lo cual utiliza un portador de banda angosta y cambia frecuencia con un patrón que es conocido por el transmisor y el receptor. Sincronizados de una manera adecuada, el efecto neto es mantener un solo canal lógico, distribuyendo la banda de frecuencias en canales muy anchos. Para un receptor no intencionado, FHSS parece ser un impulso de ruido de corta duración y una señal interferente situada en la banda del canal, afecta por completo a la transmisión y puede producir la pérdida de toda la información.

Las principales características del funcionamiento del FHSS son:

- ✓ Debido a que los datos erróneos son descartados y pueden ser retransmitidos, el método es altamente confiable.

- ✓ El receptor reensambla sus paquetes a su forma original.

- ✓ No importa que tan fuerte sea la interferencia, el sistema FHSS mantendrá su comunicación.
- ✓ El paquete que no es enviado exitosamente en una frecuencia dada, es re-enviado en otra frecuencia.

- ✓ Los datos entrantes se dividen en paquetes individuales más pequeños y se transmiten en frecuencias separadas.

Cuando se transmite utilizando esta técnica es posible pasar un mensaje de un canal a otro, varias veces por segundo hasta conseguir 40 frecuencias de transmisión diferentes, de esta manera se elimina el riesgo de bloqueo del sistema por interferencias de otros sistemas.

La principal aplicación de esta técnica es el almacenamiento ya que la fiabilidad de la comunicación supera cualquier otro aspecto, pero no se puede desconocer que en las redes de radio multiterminal es donde se saca el mayor provecho de FHSS ya que se pueden enviar datos simultáneamente por canales separados.

4.2 DSSS, DIRECT- SEQUENCE SPREAD SPECTRUM TECHNOLOGY (*ESTEPECTRO – EXTENDIDO DE SECUENCIA DIRECTA*)

Mediante esta técnica se genera un patrón redundante de bits por cada bit de información real transmitido. Este patrón de bits se le llama ***chip*** o ***código chipping***, en donde, mientras más largo sea el *chip*, mayor es la probabilidad de que la información original pueda ser recuperada para lo cual se requiere mayor ancho de banda. Aunque uno o más bits en el *chip* resulten dañados durante la transmisión, técnicas estadísticas incluidas en el radio pueden recuperar la información original sin la necesidad de que ésta sea retransmitida. Para un receptor no intencionado DSSS parece un ruido de baja potencia de banda ancha y es repelido por la mayoría de los receptores de banda angosta.
En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida, para lo cual requiere un procesador de señal digital para correlacionar la señal de entrada.

Estos sistemas, llamados también multicanal, utilizan hasta tres canales intercambiables en el caso de interferencias. La transmisión se realiza enviando varias veces la información codificada, para compensar las eventuales

perturbaciones, con el inconveniente de alargar la transmisión del mensaje, a expensas de la velocidad. Además, por la dispersión de la potencia, el riesgo de interferencia con señales de nivel bajo persiste.

4.3 ELECCIÓN DE LA TECNOLOGÍA DE MODULACIÓN, FHSS O DSSS.

Al igual que para la elección de la topología que se debe implementar, en cuanto a la tecnología de modulación es necesario tener en cuenta la necesidad que se desea suplir con la red diseñada. Los aspectos descritos mas adelante muestran una comparación entre FHSS y DSSS que permite tener un mejor criterio en el momento de realizar la elección.

4.3.1 Rendimiento: El aprovechamiento o rendimiento[1] del canal es mejor con DSSS que con FHSS. Esto se debe a que FHSS utiliza un protocolo más complejo que DSSS, esto implica un mayor número de bits informativos. Este protocolo permite mayores capacidades en cuanto a movilidad y robustez que el que usa DSSS que es mas sencillo y proporciona velocidades de transferencia de datos más elevadas en conexiones punto a punto (entre salto y salto FHSS necesita un tiempo para chequear la banda, identificar la secuencia de salto y asentarse en la misma).

4.3.2 Capacidad total de la red: La capacidad de proceso o *throughput* efectivo total de la red puede definirse como la capacidad de proceso agregada máxima. En este aspecto la superioridad de FHSS aparece debida a que puede ofrecer un mayor número de canales sin solapamiento en base otra vez a la propia filosofía

de FHSS, concretamente DSSS puede llegar hasta un máximo de 3 canales de 2 Mbps en la banda de 2,4 GHz, con lo que puede alcanzar hasta un máximo de 10 Mbps de capacidad frente a los 24 Mbps que se obtienen con FHSS a base de 15 canales de 1,6 Mbps.

4.3.3 Los solapamientos: las razones por las que se presenta solapamiento en la zona de acción de los puntos de acceso son:

✓ En grandes redes WLANs donde las distancias son muy grandes para los radios de acción existentes, se solapan varios puntos de acceso para asegurar una cobertura continua

✓ Cercanía entre distintas WLANs que comparten un área.

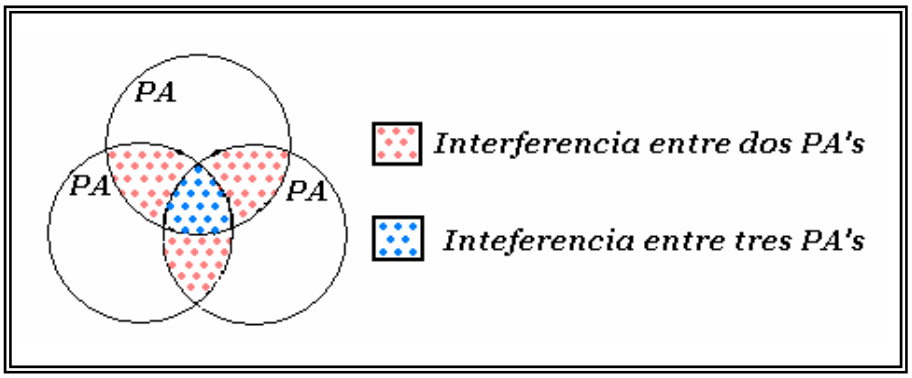


Figura 4.1 Esquema de interferencias

En ambos casos el solapamiento implica que las estaciones afectadas recibirán señales de distintos puntos de acceso, DSSS soporta un máximo de tres canales solapados sin interferencias, en el mejor de los casos, a partir de los cuales las

[1] Relación entre bits informativos y nº total de bits enviados

interferencias producirán rendimiento significativamente menor. Sin embargo, FHSS debido a su modelo de sincronización puede proporcionar mas canales sin solapamiento, o mejor, con solapamiento pero usando distintos canales en distintas frecuencias y con distintas frecuencias de sincronización. De hecho se podría incluso doblar el ancho de banda en un área añadiendo un segundo punto de acceso y configurándolo para un nuevo canal.

4.3.4 Fiabilidad. La norma IEEE 802.11 describe el FHSS LAN siguiendo un esquema de modulación en frecuencia *(FSK, Frecuency Shift Keying*) y a una velocidad estándar de 1 Mbps, pudiendo llegar a 2 Mbps en condiciones óptimas. DSSS queda descrito en un esquema de modulación en fase (DPSK, Bynary Phase-Shift Keying) a velocidades de 1 Mbps en condiciones de ruido y QPSK (Quadrature Phase-Shift Keying) a velocidades de 2 Mbps en condiciones de calidad.

4.3.5. Interferencia multipath: La interferencia multipath[2], consiste en una distorsión de la señal originada por la reflexión múltiple de las ondas de radio en estructuras como paredes, puertas y otros. Esto hace que la señal que se disperse en el tiempo, con lo cual llega a la antena receptora como una serie de múltiples señales en instantes ligeramente diferentes, lo que genera una atenuación de la señal conocida como *fading*. En este contexto, FHSS es inmune ya que al estar basado en el salto a diferentes frecuencias el multipath queda automáticamente contrarrestado. Sin embargo, DSSS puede solucionar este problema aumentando la capacidad de la antena, lo que genera costes y complejidad añadidos.

[2] Esta interferencia es asociada estrechamente a las comunicaciones por radio.

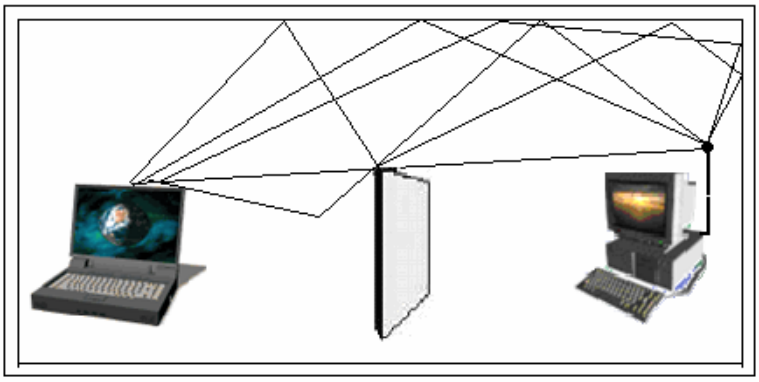


Figura 4.2 El fenómeno de la interferencia multipath

4.3.6. Seguridad y encriptación. Diversos artículos señalan que DSSS utiliza un código de *spreading*[3] extremadamente simple y que, consecuentemente, es fácil relativamente interceptar la información mediante un algoritmo bien definido que permita convertir la señal a su estado inicial, una vez captada a lo largo del camino de transmisión. Sin embargo, FHSS utiliza un número muy elevado de combinaciones de *dwell times* y *secuencias de hopping* para encriptar la señal, lo cual dificulta considerablemente la intercepción de la información. En este sentido, DSSS tiene que utilizar técnicas adicionales de criptografía que añaden costos y complejidad.

5. SEGURIDAD

Cuando de redes inalámbricas se trata, el tema de la seguridad es supremamente importante debido a que el mismo hecho de que la transmisión en este tipo de redes se realiza a través de una parte del espectro electromagnético que es compartido por todas las redes inalámbrica, es posible que un dispositivo pueda

[3] En este caso se refiere la secuencia Chip

acceder a una red diferente a la que pertenece. Esto puede ocurrir con puntos de accesos, PC's o incluso, teléfonos móviles.

Es por esto que existen procedimientos para detectar redes inalámbricas y determinar si existe o no un mecanismo de seguridad y por supuesto que también se cuenta con técnicas para lograr que la red diseñada cumpla con todos los requisitos para ser una red segura en la cual solo puedan acceder aquellos dispositivos autorizados.

5.1 MÉTODOS PARA BRINDAR SEGURIDAD A LAS REDES INALÁMBRICAS

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- ✓ Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

- ✓ Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

- ✓ Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva. Existen varios métodos para lograr la configuración segura de una red

Teniendo en cuenta la Información anterior, el paso siguiente consiste en tomar las medidas necesarias para lograr que la red inalámbrica sea segura, para lo cual resugiere:

- ✓ Cambiar las claves por defecto cuando se instale el software del Punto De Acceso.
- ✓ Control de acceso seguro con autentificación bidireccional.
- ✓ Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- ✓ Configuración WEP, la seguridad del cifrado de paquetes que se transmiten es fundamental en las redes inalámbricas, la codificación puede ser más o menos segura dependiendo del tamaño de la clave creada y su nivel, la más recomendable es de 128 Bits.
- ✓ Crear varias claves WEP, para el punto de acceso y los clientes y que varíen cada día.

5.1.1 Sistema de cifrado WEP: Se trata del primer mecanismo implementado y fue diseñado para ofrecer un cierto grado de privacidad, pero no puede equiparse (como a veces se hace) con protocolos de redes tales como IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio. WEP utiliza una clave secreta, que consiste en un código cifrado de emisión/recepción utilizada para la encriptación de los paquetes antes de su retransmisión aplicando a los datos originales una operación lógica XOR (O exclusiva). El algoritmo utilizado para la encriptación es RC4.

5.1.2 Sistema de cifrado WEP2: Es una modificación del protocolo WEP realizada el año 2001, como consecuencia de una serie de vulnerabilidades que se descubrieron. No obstante, todavía hoy no existe ninguna implementación completa de WEP2.

5.1.3 Open System Authentication: Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de encriptación, incluso cuando se ha activado WEP.

5.1.4 Access Control List (ACL): Si bien no forma parte del estándar, la mayor parte de los productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la, dirección MAC de cada STA, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista de control de acceso (ACL).

5.1.5 Closed Network Access Control: Sólo se permite el acceso a la red a aquellos que conozcan el nombre de la red, o SSID. Éste nombre viene a actuar como contraseña. Es imprescindible que el SSID, sea distinto al que el aparato trae por defecto, es decir, se debe personalizar una haya sido instalada la red.

5.2 MÉTODOS PARA LA PROTECCIÓN DE REDES INALÁMBRICAS

5.2.1 Filtrado de direcciones MAC: este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (*Media Access Control*) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

✓ No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

✓ Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un *sniffer*, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como **AirJack6** o **WellenReiter**, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.

✓ En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

5.2.2 Wired Equivalent Privacy (WEP): El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

Estas son desventajas de la clave WEP:

✓ La mayoría de instalaciones emplean WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

✓ WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo. Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP.

5.2.3 Las VPN: Una red privada virtual (*Virtual Private Network, VPN*) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las **VPN** resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN[4] si se emplea *switching*. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

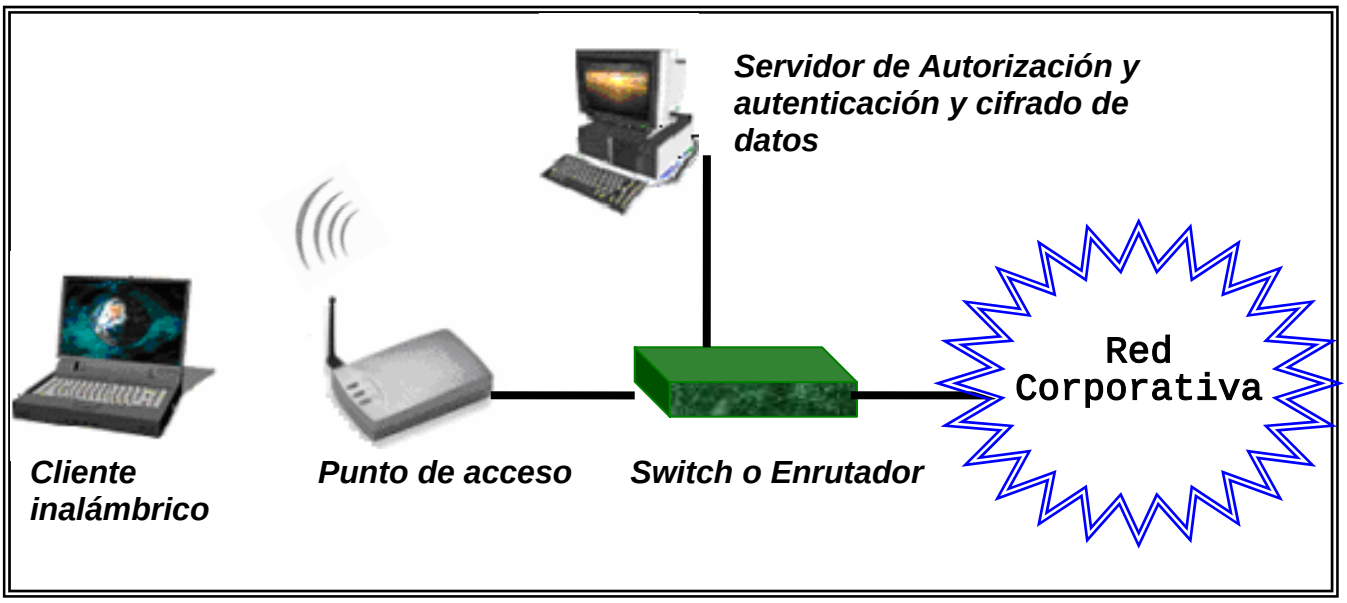


Figura 5.1Estructura de una VPN para acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los

[4] Red de area local virtual

datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

5.2.4 802.1x: es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. El protocolo 802.1x involucra tres participantes (Figura 5.2).

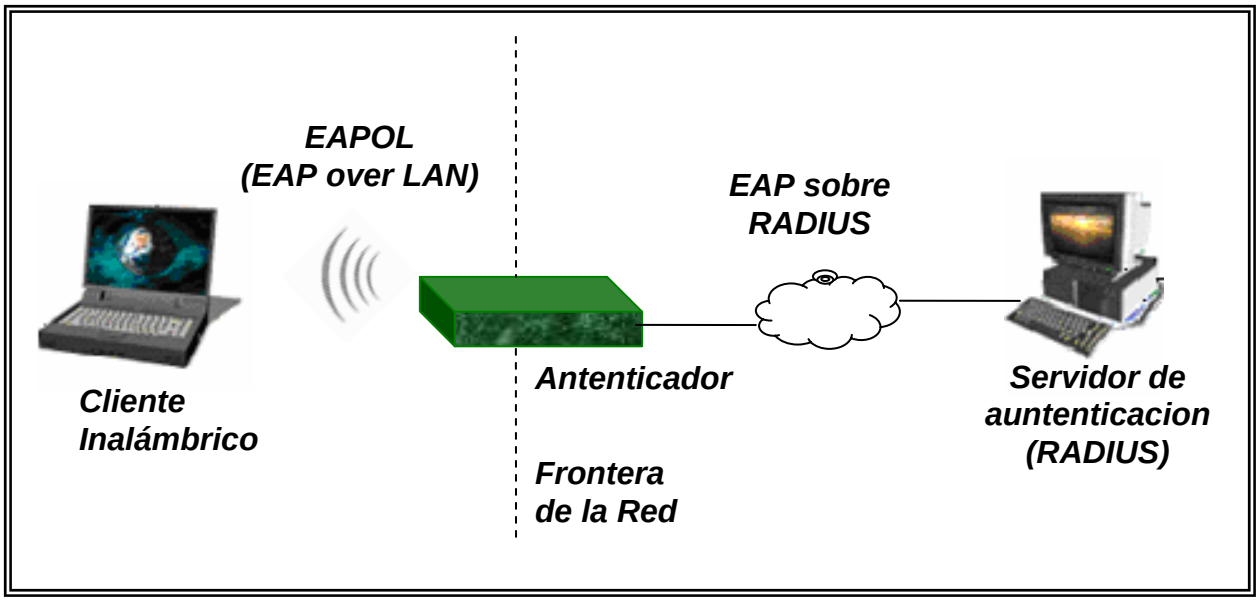


Figura 5.2 Arquitectura de un sistema de autenticación 802.1x.

✓ *El suplicante*, o equipo del cliente, que desea conectarse con la red.

✓ *El servidor de autorización/autenticación* es el que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS ***(Remote Authentication Dial-In User Service).*** Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.

✓ *El autenticador*, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del *suplicante*. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza. EAPOL (EAP over LAN)
La autenticación del cliente se lleva a cabo mediante el protocolo EAP (*Extensible Authentication Protocol*) y el servicio ***RADIUS***, de la siguiente manera:

a. El proceso inicia cuando la estación de trabajo se enciende y logra enlazarse o asociarse con un punto de acceso. En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.

b. La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.

c. El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/ Identity.

d. La estación se identifica mediante un mensaje EAP-Response/ Identity.

e. Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS *Access Request* al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.

f. El servidor de autenticación responde con un mensaje RADIUS Access-Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.

g. El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.

h. Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.

i. El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

5.2.5 WPA (WI-FI Protected Access): este un estándar propuesto por los miembros de la *Wi-Fi Alliance* (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. Para solucionar el problema de cifrado de los datos, WPA

propone un nuevo protocolo para cifrado, conocido como ***TKIP*** (*Temporary Key Integrity Protocol*). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama.. El mecanismo de autenticación usado en WPA emplea 802.1x y EAP. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- ✓ ***Modalidad de red empresarial***: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- ✓ ***Modalidad de red casera o PSK (Pre-Shared Key):*** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso.

6. ESTÁNDARES

Cuando se habla de redes inalámbricas es común encontrar los términos 802.11, ZigBee, HiperLAN, Bluetooth, Wi - Fi... Estos nombres corresponden a los estándares que convierten en la base de los fabricantes para desarrollar sus productos permitiendo definir especificaciones técnicas y aplicaciones.desarrollan organismos reconocidos internacionalmente5, que una vez desarrollados se

6.1 IEEE 802.11

Las redes IEEE 802.11 suponen la apuesta del IEEE por las redes inalámbricas. Toda ellas se basan en una red tipo Ethernet y, aunque su filosofía es la misma, difieren en la banda de frecuencia utilizada, el ancho de banda que ofrecen, etc. Este protocolo define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. La siguiente modificación fue designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente

se incorporo un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores.

6.1.1 802.11b o Wi-Fi (Wireless Fidelity): Como ya se mencionó en la sección 6.1, **el 802.11b o WI – FI** es el estándar que trabaja en el rango de velocidades de 5 hasta 11 Mbps a una frecuencia de 2,4 GHz (de uso libre y sin licencia). Este estándar robusto y maduro apareció en julio de 1999 y presenta la característica de que sus equipos son compatibles con los del **802.11g**, que trabajan en la misma frecuencia.

La desventaja de trabajar bajo este estándar radica en el hecho de trabajar en una frecuencia sin regulación, ya que esto podría causar interferencias con hornos microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Sin embargo, si las instalaciones **802.11b** están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el coste de sus productos, aunque esto suponga utilizar una frecuencia sin regulación.

[5] Ejemplo de esto son la IEEE y la ETSI.

6.2 ZIGBEE

En muchas ocasiones, cuando se menciona **ZigBee**, se relaciona inmediatamente con 802.15.4 Antes de definir las características de **ZigBee**, es importante resaltar que 802.15.4 es un estándar de radio bajo la familia WPAN y ZigBee es la especificación definiendo las aplicaciones de red capaces de soportar esos dispositivos.

La principal característica de **ZigBee** es que esta diseñado para operaciones de baja potencia, permitiendo que un dispositivo ZigBee pueda dejarse sin utilizar por un periodo largo de tiempo sin necesidad de volver a cargar la batería, lo que es de gran utilidad ya que elimina la necesidad del operador de recargar la batería frecuentemente.

Este estándar esta diseñado para dar servicio a dispositivos con baja transmisión de datos a comparación de dispositivos que requieren banda ancha para transmitir video y gráficos. Las aplicaciones posibles son la automatización de la casa, sensores inalámbricos, juguetes interactivos y controles remotos.

6.2.1 ZigBee Alliance: es un grupo de compañías que trabajan conjuntamente para desarrollar software de aplicación estandarizado por encima de la norma 802.15.4 del IEEE. La meta de ZigBee Alliance es suministrar a los clientes sistemas para el trabajo en cualquier campo, con la mayor flexibilidad posible, presentando la tecnología inalámbrica del ZigBee en innumerables dispositivos. Phillips Electronic North America actualmente es una de las más de 100 compañías miembros de ZigBee Alliance.

Los cuatro principales objetivos de este grupo son: Definir las capas de red, seguridad y software de aplicación del protocolo; suministrar interoperabilidad y pruebas de ajuste para los dispositivos ZigBee; promocionar la marca mundialmente y manejar la evolución de la tecnología.

6.3 HIPERLAN

En Europa el **ETSI** ha desarrollado el estándar de redes inalámbricas **HiperLAN** y **HiperLAN2** (*High Performance Radio LAN type 2*) que compiten como alternativas a los estándares IEEE 802.11a y IEEE 802.11b.

6.3.1 HiperLan 1: Variante inicial de la ETSI, se definió a principios de los años 90, concretamente en el periodo que va de 1991-1996. Fue desarrollado para mejorar las prestaciones de 1/2 Mbps del 802.11 y permitir la conexión de terminales portátiles en configuración Ad-hoc. Está basado en un soporte asíncrono de transferencia de datos, sin calidad de servicio alguno y con un método de acceso basado en CSMA/CD (carrier-sense multiple access multiple access with collision avoidance). Incluía cuatro estándares diferentes, de los cuales el denominado **Tipo 1** es el que verdaderamente se ajusta a las necesidades futuras de las WLAN, estimándose una velocidad de 23.5 Mbps.

6.3.2 HiperLan 2: HiperLAN2 se desarrollo en el proyecto *Broadband Radio Access Networks (BRAN)* de ETSI, iniciado en 1997, y tiene mejores perspectivas por la coordinación entre organismos de normalización (ETSI en Europa y ARIB en Japón) y el interés de fabricantes europeos y japoneses. Los estándares **802.11a** e **HiperLAN2** son muy parecidos en el nivel físico, pero HiperLAN2 añade

funcionalidades y ventajas en cuanto a control de potencia y cambio automático de frecuencia en caso de interferencia.

HIPERLAN/2 fue diseñado teniendo en cuenta los requerimientos de una red multimedia inalámbrica, la cual debería cumplir con los requisitos de calidad de servicio (QoS) tal como lo hace una red ATM alambrada. Entre los servicios que pueden ser soportados por la red HIPERLAN/2 se encuentran:

- ✓ Conferencias multimedia.
- ✓ Telefonía/Audio.
- ✓ Aplicaciones generales de redes de computadoras.
- ✓ Bases de datos multimedia.
- ✓ Seguridad y monitoreo.
- ✓ Navegación por Internet.

El proyecto ETSI BRAN ha trabajado también en otros dos sistemas complementarios de HiperLAN2, llamados ***Hiperaccess*** e ***Hiperlink***. El primero es básicamente una versión de HiperLAN2 para enlaces fijos punto a punto con la misma velocidad y mayor alcance, que puede servir como bucle de acceso radio para usuarios residenciales y pequeñas empresas o para conectar WLAN's en HotSpots a la Internet. El segundo es un enlace inalámbrico en la banda de 17 GHz de alta velocidad y cortó alcance, que se puede usar para sustituir el cableado a los puntos de acceso, por ejemplo para interconectar HiperLAN2 e Hiperaccess.

6.4 SP100 DE ISA.

La asociación de instrumentación, sistemas y automatización, ISA, fundada en 1945 tiene como objetivo desarrollar estándares, proporcionar educación, entrenamiento y certificación a profesionales de la industria así como publicar libros y artículos técnicos referentes a su campo de operación.

Recientemente esta asociación, patrocinadora de la fundación de la federación de la automatización, formó el comité de ISA-SP100 el cual esta encargado de crear estándares, las prácticas recomendadas y los informes necesarios para el diseño y la implementación de redes inalámbricas de control en la industria. La ***Figura 6.1*** muestra la clasificación que presenta ISA para el desarrollo del estándar.

Category	Class	Application	Description
Safety	0	Emergency action	*(always critical)*
Control	1	Closed loop regulatory control	*(often critical)*
	2	Closed loop supervisory control	*(usually non-critical)*
	3	Open loop control	*(human in the loop)*
Monitoring	4	Alerting	*Short-term operational consequence (e.g., event-based maintenance)*
	5	Logging and downloading/uploading	*No immediate operational consequence (e.g., history collection, sequence-of-events, preventive maintenance)*

Importance of message timeliness increases ↑

Figura 6.1 Clasificación para desarrollo de ISA-SP100[6]

[6] Tomado de la pagina WEB oficial de ISA

Como ya se ha mencionado, este estándar esta en desarrollo por lo cual ISA a presentado una convocatoria para que las organizaciones, grupos de investigación o personas interesadas, aporten sus conocimientos e ideas. Teniendo en cuenta la anterior clasificación el SP-100 presenta las siguientes subdivisiones:

6.4.1 ISA-SP100.11, *Wireless for Industrial Process Measurement and Control:* Esta es la parte del estándar SP100 encargada de definir las especificaciones para lazos de control industrial así como el monitoreo. En el se hace referencia a la ***Interconexión de sistemas abiertos*** incluyendo la configuración de la red y del dispositivo.

6.4.2 ISA-SP100.14*, Wireless Network Optimized for Industrial Monitoring:* este es la parte del estándar dirigido a los sectores específicos de la clase 4 y 5[7], específicamente aplicaciones de monitoreo de proceso y equipos inventario. Estas aplicaciones pueden incluir tareas que están clasificadas como control poco crítico.

El estándar también debe estar dirigido a las necesidades específicas de sensores y la automatización en el ambiente del industrial como la coexistencia, la robustez a la interferencia, la interoperabilidad con redes de infraestructura de la planta, etc.

[7] Según la clasificación hecha por ISA, presentada en la figura 6.1.

7. APLICACIONES

Las redes inalámbricas de control son aplicables en todos los campos de la industria, en cualquier proceso. Es así como, teniendo como base los elementos presentados en el ***capitulo 2***, solo es necesario configurar el PA de tal forma que pueda recibir y enviar Información a los nuevos y modernos equipos diseñados para controlar, automatizar y monitorear los procesos industriales actuales, ya sea en el campo de la minería, los alimentos, la producción de plástico, la industria energética, etc.

A continuación dos aplicaciones en redes inalámbricas de control para la industria moderna.

7.1 EN LA MINERÍA.

La minería presenta labores que son muy críticas y que requieren ser monitoreadas constantemente, en lugares demasiado distantes y poco accesibles. Concretamente en la mina a cielo abierto mas grande del mundo, Cerrejón, existen muchísimos procesos en los que las redes inalámbricas de control son la solución para monitoreo y control.

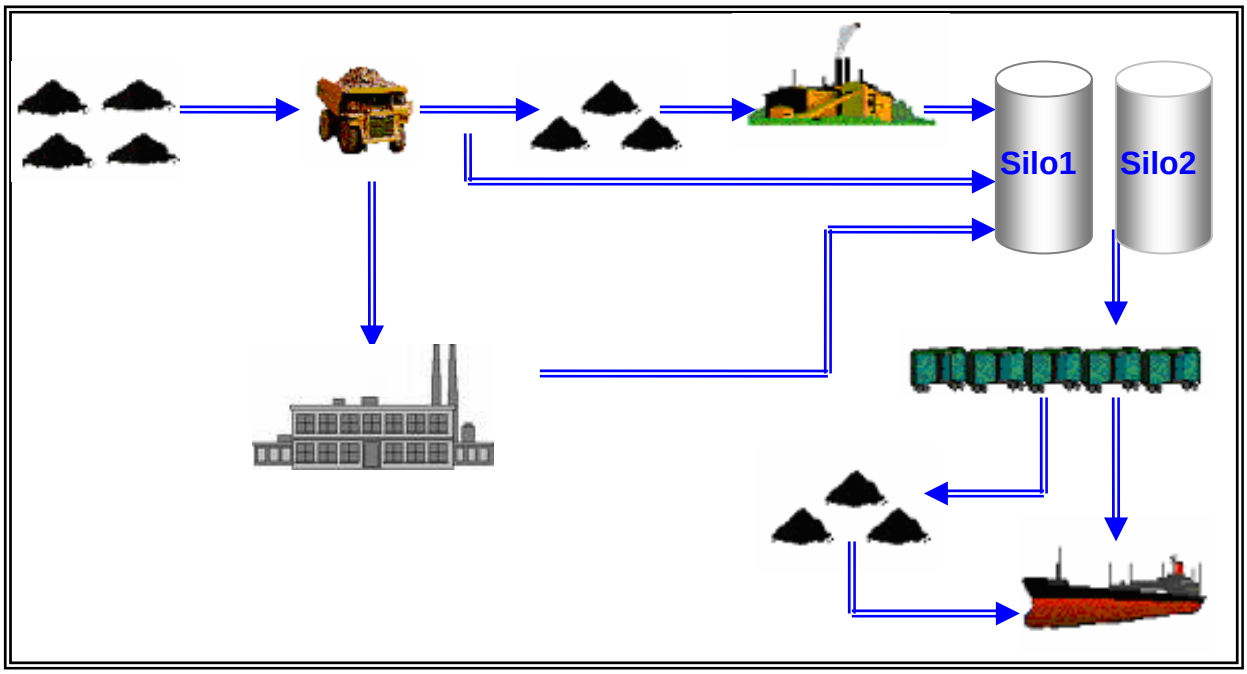


Figura 7.1 Esquema general del proceso de trituración y lavado del carbón

Un proceso en el cual se puede observar esto es el que se lleva a cabo en las plantas de trituración y lavado del carbón representado en la figura 7.1. Todo empieza con la llegada de los camiones cargados de carbón (Ver figura 7.2) procedente de las zonas de minería. Este carbón es almacenado en tolvas que lo conducen a las plantas de trituración[8]. Cuando se ha conseguido el tamaño ideal, el carbón es dirigido a la planta de lavado por medio de bandas transportadoras (ver figura 7.3) y de allí, hacia los silos en donde se almacena para luego cargar el tren (ver figura 7.4).

[8] El carbón es triturado hasta conseguir una granulometría de 2".

Figura7.2 Camión descargando en las tolvas

Figura 7.3 Bandas transportadoras

Figura 7.4 Silos para almacenamiento del carbón

Todo este proceso es monitoreado y controlado desde un sistema central (figura7.5) y la red es híbrida (una parte cableada y la otra inalámbrica). A medida que el carbón avanza a través de todos los subproceso, el analista del cuarto control puede verificar la cantidad y el tamaño y puede variar parámetros como la velocidad de las bandas y el tiempo de cargue del tren.

A largo de toda la red se encuentran sensores de todo tipo y diversos PLC's, entre otros elementos propios de una red de control. La parte de la red que constituye el segmento inalámbrico es la que tiene que ver con la recolección del agua que alimenta la planta de lavado. Esta es tomada de una laguna que se encuentra a 1Km aprox., de la planta. En la laguna se encuentra una bomba que es accionada por medio de un sistema electrónico que recibe la señal de mando desde el cuarto

de control vía inalámbrica. Las dos antenas involucradas en este proceso se encuentran en el tope de los silos y en el poste que contiene la caja de control de la bomba. Aunque esta es la principal función de la red (encender / apagar la bomba), el sistema electrónico también es capaz de enviar información sobre flujo del liquido extraído, de esta manera genera una alarma, en caso de ser necesario, si la bomba deja de succionar agua.

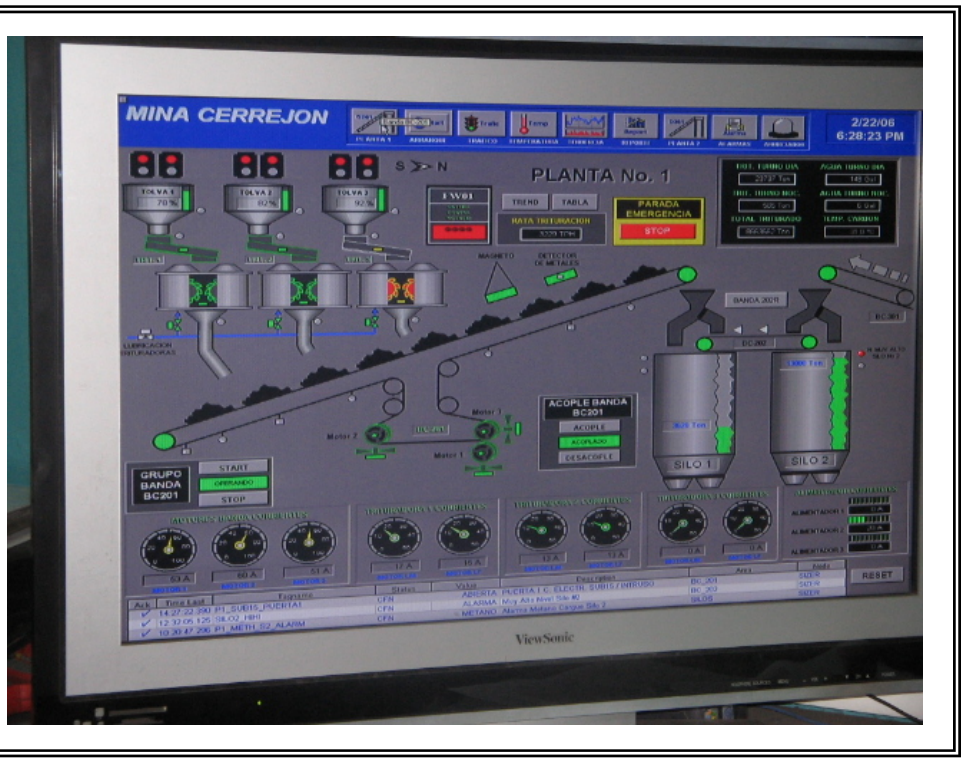


Figura7.5 Imagen de uno de los monitores del control de las plantas de carbón - mina

7.2 EN TELEMETRÍA.

Las redes inalámbricas actualmente representan una herramienta ideal para la telemetría siendo utilizados ampliamente en las industrias modernas para mejorar el manejo de producción y el mantenimiento, minimizando los costos de producción y mantenimiento, logrando aumentar la rentabilidad, sobre todo en los procesos en los cuales lo que se desea monitorear, registrar y controlar se encuentra a gran distancia del centro de control.

La telemetría se utiliza en grandes sistemas, tales como las naves espaciales o las plantas químicas, debido a que facilita la monitorización automática y el registro de las mediciones, así como el envío de alertas, con el fin de que el funcionamiento sea seguro y eficiente, así como también es utilizado por las empresas prestadoras de servicios públicos o cualquier otra proceso en el que se necesite reciben las instrucciones y los datos necesarios para operar, mediante comandos a distancia.

Entre las variables que se pueden manipular se tiene voltaje, velocidad, flujos, estados de válvula, corriente de un motor, presión en una tubería. Y como ejemplo de lo que se puede manipular hacer partir un motor o una bomba, abrir o cerrar una válvula, regular la velocidad de una correa transportadora. Por lo anterior se puede deducir que la telemetría es útil y prácticamente necesaria en cualquier proceso industrial y si se implementa de forma inalámbrica es todavía mucho más eficiente.

En el ***capitulo 8*** se toma como ejemplo para diseñar una red inalámbrica de control un caso en el que se desea monitorear y controlar el proceso de succión y

recolección de agua de unos pozos subterráneos. Aquí se vera en detalle un ejemplo claro y real de telemetría.

7.3 EN PLANTAS EMBOTELLADORAS

El proceso de embotellado en la industria ha sido uno de los que ha evolucionado junto con la automatización industrial. En las plantas donde se hace necesario embotellar un producto, cada uno de los avances que tenga la automatización representa ahorro de costos, gracias a la reducción de tiempos improductivos, incremento del rendimiento, posibilidad de programación inalámbrica con fines de mantenimiento.

Las redes de control inalámbricas brindan información para el control en tiempo real, lo que permite tomar decisiones oportunas tales como cerrar y abrir válvulas con gran rapidez.

Tomada de www.siemens.com/scalance

8 EJEMPLO PRACTICO: POZOS ABASTECEDORES – PLANTA DE AGUA MINA.

Para el diseño y posterior implementación de cualquier sistema de control es necesario seguir una serie de pasos para cumplir con los requisitos mínimos en el momento de elegir los equipos ideales para el proceso. El caso especifico de los sistemas inalámbricos un buen análisis del proceso y su entorno son la clave del éxito en el buen funcionamiento de la red diseñada.

En este documento presentamos como ejemplo real la necesidad de diseñar una red inalámbrica para monitoreo y control de los pozos subterráneos abastecedores de la planta de agua de la mina de carbón del Cerrejón en La Guajira colombiana.

8.1 CARACTERÍSTICAS DEL PROCESO

8.1.1 Descripción del problema: Para el abastecimiento de la Planta de Agua – Mina se cuenta con 17 pozos subterráneos, ubicados a lo largo de un tramo del río Ranchería El bombeo de agua hacia la planta esta programado de tal forma que los pozos no trabajan simultáneamente. Se desea tener la posibilidad de poner en marcha o detener el funcionamiento de cada una de las bombas que contienen estos pozos, con el fin de tener el control desde la planta.

La *figura 8.1* muestra la caja de control de cada uno de los pozos se encuentran los elementos básicos para el suministro de energía para cada bomba, así como un temporizador que representa el único mecanismo de control, utilizado para la programación antes mencionada.

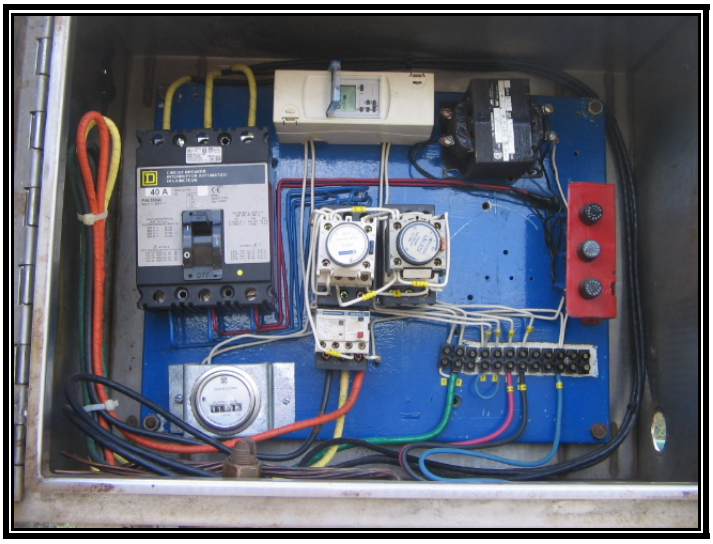


Figura 8.1 Caja de control de los pozos[9]

8.1.2 Propósito de control: Como fue anteriormente mencionado, el propósito de control es el encendido/apagado remoto del mecanismo de bombeo de los pozos hacia la planta, dependiendo de las necesidades que se tengan en el momento, según las exigencias del proceso.

8.1.3 Variables controladas: El sistema de encendido/apagado de cada una de las bombas de los 17 pozos.

8.1.4 Variables manipuladas: El flujo del agua dentro del pozo.

[9] Todas las fotografías de los procesos del Cerrejón referenciadas en este documento fueron tomadas por Karen Gutierrez y son utilizadas con la autorización correspondiente.

8.2 ANÁLISIS DEL PROCESO Y SU ENTORNO.

8.2.1 Distancia entre cada pozo y la planta de agua: Es importante tener en cuenta la distancia que existe entre cada uno de los pozos y el sitio de ubicación del cuarto de control debido a que los equipos utilizados en telemetría tienen un rango de alcance determinado. La ***Tabla 1*** muestra la longitud en metros que hay desde cada uno de los pozos y el reservorio ubicado en la planta de agua – Mina.

Para el diseño es necesario tener en cuenta que no existe línea de vista entre la Planta de Agua y los pozos por lo que se hace necesario ubicar otro punto dentro de la mina que pueda servir para colocar una antena que realice el enlace entre pozos y planta.

POZO	DISTANCIA [m]
1A	3308.7
3	7892.18
4A	5087.01
5	7656.21
7	7101.09
8	6923.03
9	5683.68
9A	4637.13
11A	4657.9
12	6203.69
13	6226.76
14	5460.57
15A	8208.42
16A	8482.991
17	1803.84
18	3061.49
19	3536.69

Tabla 1: Distancia entre pozo y planta de agua

8.2.2 Características del terreno: Los pozos abastecedores de agua de la planta de agua – Mina están ubicados a lo largo de un tramo del rió Ranchería (Ver **Anexo C**), muy cerca del área de minería.

Por la carretera que conduce de los pozos a la planta transita diariamente equipo pesado que transporta carbón. Este hecho junto con el análisis realizado a la información presentada en la ***tabla 1***, en donde el pozo mas cercano a la planta se encuentra a 2km aprox. y el mas distante a 8km aprox., hace necesario que el sistema telemétrico que se va a diseñar sea inalámbrico, primero por las características del terreno y segundo por la distancia tan evidentemente larga que podría causar perdida de información en el camino, lo que se traduce en perdida de dinero y tiempo, y error en la toma de decisiones debido a una señal errada sobre el funcionamiento del proceso.

8.3 SOLUCIÓN

La solución al problema descrito es diseñar una red inalámbrica que permita el telecomando del encendido/apagado de las bombas sumergibles de los pozos subterráneos.

Luego de poner en consideración la información recopilada del proceso de encendido/apagado de las bombas de cada uno de los pozos, el terreno, la distancia, entre otros, se propone la línea de productos **CANOPY** de **Motorola** para realizar el enlace inalámbrico entre el cuarto de control y la Planta de Agua, y los **PLC's LOGO!** de **Siemens** para realizar la labor de control y adquisición de datos local en los pozos.

La línea CANOPY cuenta con los módulos básicos para implementar una red inalámbrica (PA, SM, BH) con tecnología que ofrece grandes velocidades y zonas de cobertura grandes. El papel de estos equipos en el sistema de telegestión es extender la red Ethernet para permitir el flujo de Información entre el cuarto de control y los pozos, la labor de monitoreo y control será realizada por el PLC el cual sustituirá algunos de los elementos ubicados en la caja de control, lo que se traduce en ahorro de dinero y espacio. Con la programación adecuada el PLC podrá:

- ✓ Encender y apagar el motor de la bomba de succión.

- ✓ Realizar la tarea de rotación de pozos[10].

- ✓ Presentar alarma que indiquen cuando el pozo este seco para no poner a trabajar la bomba en seco.

- ✓ Mostrar medición de flujo a la salida de los pozos.

8.3.1 Línea CANOPY: Los equipos CANOPY ofrecen tres líneas para trabajar en tres rangos de frecuencias diferentes, todas ellas sin licencia. La elegida para este diseño es la de 5.2GHz que ofrece mayor ancho de banda y robustez para aplicaciones empresariales.

[10] Este es el procedimiento mediante el cual se asignan los días o las horas en las que se realizara la extracción en cada uno de los pozos.

Los módulos necesarios para realizar el montaje de la red inalámbrica son:

Módulos de Punto de Acceso (PA): El Punto de Acceso distribuye y recibe Información desde y hacia los SM que estarían ubicados en cada uno de los pozos. Cada punto de acceso funciona con una antena direccional de 60 grados para proporcionar cobertura a máximo 200 SM. Un arreglo de 6 PA o ***clúster*** como el de la *figura 8.2* puede prestar servicios a un máximo de 1,200 Módulos Suscriptores con cobertura en todas las direcciones (360º).

Módulo Suscriptor (SM)**:** Los Módulos Suscriptores que se observan en la *figura 8.3,* son transceptores que se ubican en cada uno de los puntos a donde se desea llegar para recibir y enviar Información.

Módulo de Administración de Clústeres (CMM)**:** El CMM suministra alimentación para hasta seis unidades AP. Contiene un receptor para el Sistema de Posicionamiento Global (GPS) y un Conmutador Ethernet reforzado.

Supresores de Sobrecargas**:** El Supresor de Sobrecargas 300SS de uso externo protege el equipo contra las descargas de rayos. También se necesita una unidad 300SS para proteger la conexión entre la red y el Módulo de Administración de Clústeres (CMM).

Antena GPS**:** Esta antena alimenta el Receptor GPS en el Módulo de Administración de Clústeres (CMM), lo cual genera pulsos de sincronización precisos en el sistema.

***Modulo Backhaul*:** este es el modulo necesario para las conexiones punto a punto. Para mayor alcance se le adiciona un receptor pasivo como se puede ver en la *figura 8.4*[11].

Las especificaciones técnicas completas de cada unos de los equipos CANOPY se pueden consultar en el **Anexo A.**

Figura 8.2 Cluster de PA

Figura 8.3 Modulo Suscriptor

Figura 8.4 Backhaul con receptor pasivo

[11] Todas las fotografías de los equipos Canopy presentadas en este documento fueron tomadas de http://www.motorola.com/canopy

La *figura 8.5* muestra el esquema de conexión de los equipos Canopy cuya forma de funcionamiento es la siguiente. En cada uno de los puntos finales de control de instala un SM y en una sitio central que cumpla con los requerimientos de distancia y línea de vista se instala el cluster con la cantidad de PA necesarios para cubrir todos los SM. En el mismo sitio de ubicación del cluster se instala un BH que concentra la señal proveniente del cluster y la envía por medio de un enlace Punto a Punto a otro BH que finalmente envía la señal al destino final.

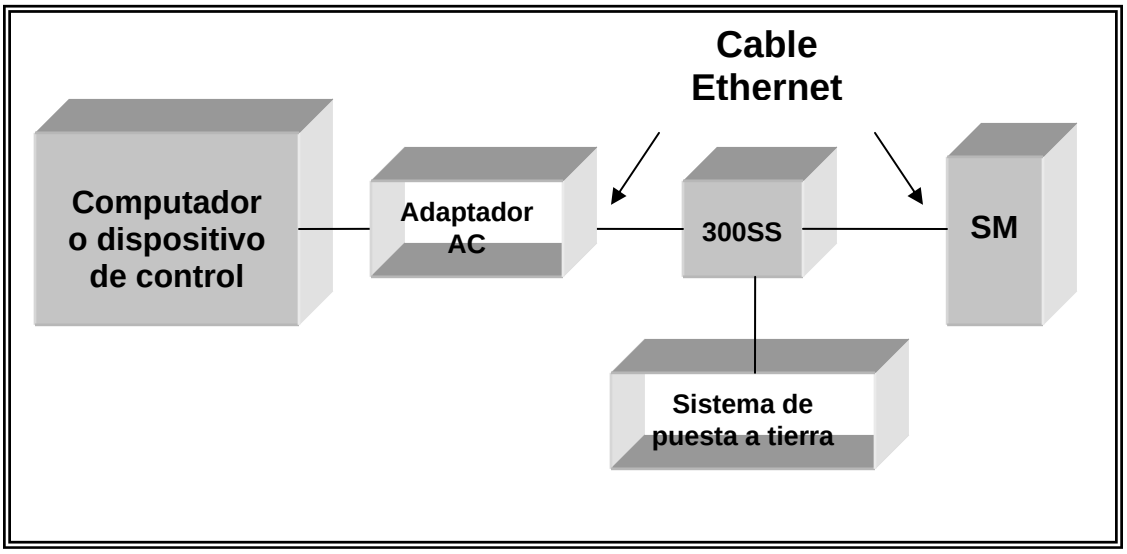


Figura 8.5 Esquema de conexión de los equipos Canopy entre punto de control y SM.

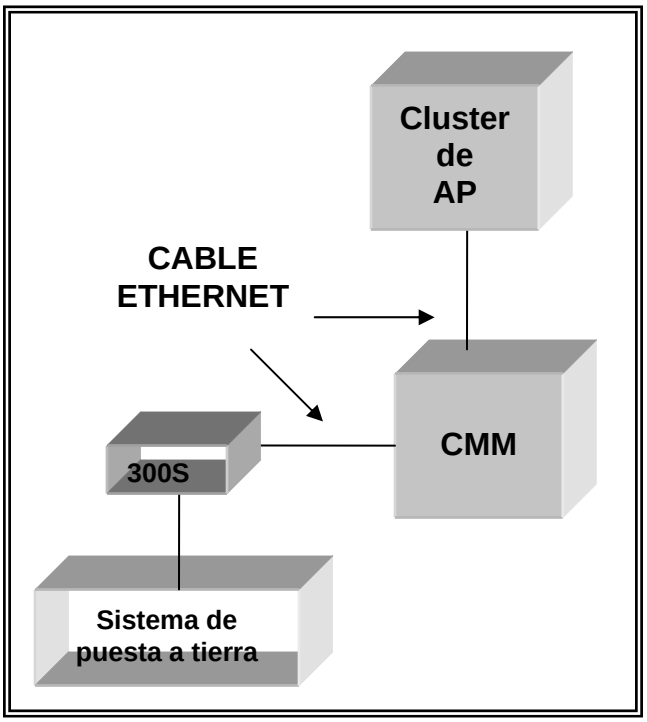
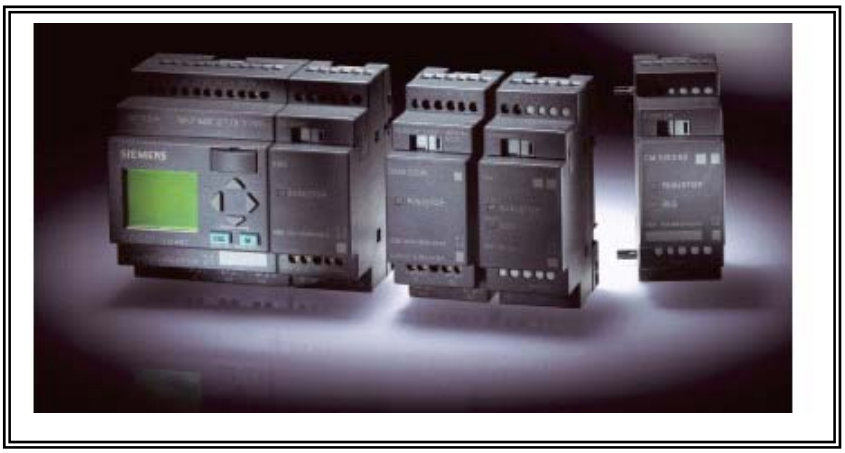


Figura 8.6 Esquema de conexión de los equipos Canopy entre CMM y cluster de PA.

8.3.2 PLC LOGO! DE SIEMENS: Como ya se ha mencionado, la labor de adquisición de datos y control es del PLC LOGO! de la marca Siemens. Esta incluido en la propuesta debido a su pequeño tamaño y sus funciones básicas que facilitan la programación necesaria para cumplir con los objetivos principales de controlar las bombas y monitorear flujo.



Tomada de www.siemens.com/logo

Las principales características de este equipo son:

- ✓ Control.
- ✓ Unidad de mando y visualización con retroiluminación.
- ✓ Fuente de alimentación.
- ✓ Interfaz para módulos de ampliación.
- ✓ Interfaz para módulo de programación (Card) y cable para PC.
- ✓ Funciones básicas habituales preprogramadas, por ejemplo para conexión retardada, desconexión retardada, relés de corriente, e interruptor de software.
- ✓ Temporizador.
- ✓ Marcas digitales y analógicas.

De las variaciones que ofrece LOGO!, se propone el **LOGO! 12/24RC** porque brinda la entradas analógicas y digitales, con la posibilidad de ampliación según las necesidades con los módulos diseñados para este fin. Las especificaciones técnicas de este equipo se pueden consultar en el **Anexo B** así como también los diferentes módulos de ampliación.

Los números **12** y **24** representan la versión y el tipo de alimentación que requiere el PLC, la **R** quiere decir que la salida es de relee y la **C** que posee temporizador semanal integrado.

8.3.3 UBICACIÓN DE LOS EQUIPOS: En cada uno de los 17 pozos es necesario colocar un PLC, cuya función ya ha sido descrita en páginas anteriores. Por su tamaño es posibles instalarlo en la actual caja de control. Elementos como el horómetro y temporizador seria removidos ya que el PLC en su programación es capaz de realizar sus funciones. Es necesario entonces un transformador para lograr la alimentación ideal de este dispositivo.

En el mismo poste de la caja de control se deben colocar los SM, conectados al PLC para recibir y enviar la Información como se muestra en la *figura 8.6.*

Con el fin de cubrir los 360ºC se hace indispensable la conexión Punto a Multipunto que enlazaría cada uno de los SM con el Cluster de PA cuya ubicación estratégica seria un punto entre los pozos 12 y 9A debido a que desde allí tendría conexión directa con todos los SM. En este mismo punto deberá estar instalado un BH para recolectar todas las señales provenientes del Cluster por medio de Administrador de Cluster. El enlace entonces seria punto a punto con el BH

instalado tope de los Silos[12] (ver figura silos), desde allí se realizaría otro enlace punto a punto con el BH ubicado en la planta de agua. La *figura 8.7* presenta un esquema general de ubicación de los equipos seleccionados.

Todo este proceso es posible monitorearlo desde la página Web de Canopy ingresando la dirección IP[13] de cada uno de estos equipos.

[12] Este es el punto más alto de toda la mina, elegido para realizar el enlace ya que tiene línea de vista con los pozos y el cuarto de control.
[13] La dirección IP asignada por el fabricante puede ser modificada por el usuario a su gusto para mayor seguridad.

Figura 8.7 Ubicación de Equipos seleccionados sobre área de la Mina (Ver anexo C)

CONCLUSIÓN

Así como el resto de los avances de la tecnología, la automatización industrial representa un gran ahorro de tiempo y dinero en los procesos industriales. Mas aun, las redes de control industrial conformadas por equipos que permitan la movilidad y el acceso a sitios donde las redes tradicionales no puedan llegar, así como también seguridad en envió y recepción de información, lo cual se traduce en confiabilidad, constituyen una de las herramientas mas útiles con las que pueda contar la industria en la actualidad.

En esta monografía se han mostrado los fundamentos de la redes de área locales inalámbricas y su potencial utilización a nivel industrial en redes de control. En el campo industrial es muy reciente su uso y todavía no se cuenta con estándares robustos para ampliar su empleo en múltiples aplicaciones, sin embargo, con las experiencias que se han tenido a nivel de instrumentación de campo y sistemas de control es muy promisorio el futuro próximo. Muestra de ello es la solución que se planteó en el capitulo 8 de esta monografía para una necesidad especifica en la planta de aguas de las minas del Cerrejón en la Guajira Colombiana.

En el mercado existe una gran variedad de equipos que se pueden adaptar a la cualquier red inalámbrica de control dependiendo del proceso en que se va a aplicar. Pero también se puede encontrar equipos diseñados para aplicaciones específicas en procesos que se llevan a cabo en fábricas embotelladoras, empresas ensambladoras de automóviles, entre otras. Entre estas líneas de equipos no se puede dejar de mencionar la instrumentación inalámbrica que cada

vez toma mas fuerza en la industria sobretodo en aplicaciones donde la medición de variables en el proceso represente peligro para el operario o sea una zona de difícil acceso.

Con un buen diseño, teniendo en cuenta las características del proceso y el tipo de variable que se va a medir, se elige la topología y lo equipos adecuados para satisfacer las necesidades del proceso que dependiendo de su entorno necesitara una red inalámbrica que brinde robustez, movilidad y/o llegar a sitios de difícil acceso.

REFERENCIAS BIBLIOGRÁFICAS

- ✓ MADRID Molina, Juan Manuel. Seguridad en redes inalámbricas 802.11, Universidad Icesi.
- ✓ STROTHMAN, Jim. Wireless control?: OK, if 'slow' and not critical...
- ✓ BELLIDO Bañares, Gonzalo. Seminario Sistematización y Automatización como herramienta para la gestión del agua.
- ✓ www.isa.org
- ✓ http://www.ieee.org/
- ✓ http://www.wi-fiplanet.com/
- ✓ http://alumno.ucol.mx/mariela/public_html/sss.htm
- ✓ http://www.vnunet.es/Especiales/Infraestructuras/20030411006
- ✓ www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/in.asp
- ✓ http://www.camyna.com/documentacion.php
- ✓ www.pucelawireless.net
- ✓ www.wlana.org/learn/educate.htm
- ✓ www.34t.com/box-docs.asp?doc=634 –
- ✓ http://www.warchalking.org
- ✓ http://www.microsoft.com/spain/seguridad/guidance/topics/cryptographyetc.mspx
- ✓ http://www.netmotionwireless.com/resource/whitepapers/security.asp
- ✓ http://www.cites.uiuc.edu/vpn/vpn4wireless.html
- ✓ http://www.diariopyme.cl/newtenberg/1639/article-62206.html
- ✓ http://standards.ieee.org/wireless/
- ✓ www.data-linc.com
- ✓ www.vmonitor.com
- ✓ http://www.lynsa.com

- ✓ www.motorola.com
- ✓ www.siemens.com

ANEXOS

ANEXO A

ESPECIFICACIONES TECNICAS DE LOS PRODUCTOS CANOPY

1. MODULO SUSCRIPTOR

Rango de Frecuencia de Operación U – NII de Banda Media	5.25 a 5.35 GHz
Método de acceso	TDD/TDMA
Velocidad de señalización	10Mbps
Tipo de modulación	BFSK de índice alto (optimizado para rechazo de interferencia)
Portadora para interferencia, conocida también como fluctuación	3dB $1*10^{-4}$ BER a -65 dBm
Sensibilidad de receptor	-83 dBm $1* 10^{-4}$ BER
Rango de operación (en todos los climas)	Hasta 3.2 Kilómetros con antena integrada
Energía del transmisor	Cumple con el limite FCC UNII ERP
Potencia o corriente eléctrica DC	24 VDC a 0.3 Amp (estado activo
Interfaz	10/100 Base T, duplas medio/total Velocidad auto negociada (cumple con 802.3
Protocolos soportados por Canopy	Transporte de capa de 2 de interrupción, con soporte para todos los protocolos comunes de Ethernet incluyendo IPV6, NetBIOS, DHCP, IPX, etc.
Trayectoria de actualización del software	Descargado remotamente en Flash mediante vinculo RF
Administración de redes	HTTP, TELNET/FTP, SNMP
Ambiental:	

Viento **Temperatura**	190 Km/hr -30 a 55 ºC
Dimensiones	11.75¨H * 3.4¨W * 3.4¨D
Peso	1 Lb (0.45Kg)

2. PUNTO DE ACCESO

Rango de Frecuencia de Operación U – NII de Banda Media	5.25 a 5.35 GHz
Método de acceso	TDD/TDMA
Velocidad de señalización	10Mbps
Tipo de modulación	BFSK de índice alto (optimizado para rechazo de interferencia)
Portadora para interferencia, conocida también como fluctuación	3dB $1*10^{-4}$ BER a -65 dBm
Sensibilidad de receptor	-84 dBm $1* 10^{-4}$ BER
Rango de operación (en todos los climas)	Hasta 3.7 Kilómetros con antena integrada
Corriente DC	24 VDC a 0.3 Amp (estado activo)
Energía del transmisor	Cumple con el limite UNII ERP de FCC
Potencia o corriente eléctrica DC	24 VDC a 0.3 Amp (estado activo
Interfaz	10/100 Base T, duplas medio/total Velocidad auto negociada (cumple con 802.3
Protocolos soportados por Canopy	Transporte de capa de 2 de interrupción, con soporte para todos los protocolos comunes de Ethernet incluyendo IPV6, NetBIOS, DHCP, IPX, etc.
Trayectoria de actualización del software	Intermitente
Administración de redes	HTTP, TELNET/FTP, SNMP
Ambiental: **Viento** **Temperatura**	 190 Km/hr -30 a 55 ºC
Dimensiones	11.75¨altura * 3.4¨ancho * 3.4¨Profundidad
Peso	1 Lb (0.45Kg)

Dimensiones	5.2¨ altura * 5¨ancho * 1.7¨profundidad
Espacio entre los orificios de montaje	4.25¨
Tamaño de tapas removibles	0.75¨
Peso	0.4 Lbs
Temperatura de operación	-30ºC a 55ºC
Conectores internos	RJ - 45

3. MODULO SUPRESOR DE PICOS

4. MODULO BACKHAUL

Rango de Frecuencia de Operación U – NII de Banda Media	5.725 a 5.825 GHz
Método de acceso	TDD/TDMA
Velocidad de señalización	10Mbps
Tipo de modulación	BFSK de índice alto (optimizado para rechazo de interferencia)
Portadora para interferencia, conocida también como fluctuación	3dB $1*10^{-4}$ BER a -65 dBm
Sensibilidad de receptor	-84 dBm $1* 10^{-4}$ BER
Rango de operación (en todos los climas)	Hasta 3.2 Kilómetros con antena integrada
Corriente DC	24 VDC a 0.3 Amp (estado activo)
Energía del transmisor	Cumple con el limite UNII ERP de FCC
Potencia o corriente eléctrica DC	24 VDC a 0.3 Amp (estado activo
Interfaz	10/100 Base T, duplas medio/total Velocidad auto negociada (cumple con 802.3
Protocolos soportados por Canopy	Transporte de capa de 2 de interrupción, con soporte para todos los protocolos comunes de Ethernet incluyendo IPV6, NetBIOS, DHCP, IPX, etc.
Administración de redes	HTTP, TELNET/FTP, SNMP
Ambiental: **Viento** **Temperatura**	 190 Km/hr -30 a 55 ºC
Dimensiones	11.75¨altura * 3.4¨ancho *
Peso	1 Lb (0.5Kg)

ANEXO B

ESPECIFICACIONES TÉCNICAS DEL PLC LOGO! DE SIEMENS

1. VARIANTES DISPONIBLES

Designación	Alimentación	Entradas	Salidas	Características
LOGO! 12/24RC	12/24 VDC	8 digitales[14]	4 relés de 10A	
LOGO! 24	24 VDC	8 digitales	4 transistores de 24V A 03 AMP	Sin reloj
LOGO! 24RC	24VAC/24DC	8 digitales	4 relés de 10A	
LOGO! 230RC	115...240 V AC/DC	8 digitales	4 relés de 10A	
LOGO! 12/24RCo	12/24VDC	8 digitales	4 relés de 10A	Sin display Sin Teclado
LOGO! 24o	24VDC	8 digitales	4 transistores 24V a 0.3 Amp	Sin display Sin Teclado
LOGO! 24RCo	24VDC/24VDC	8 digitales	4 relés 10 Amp	Sin display Sin Teclado
LOGO! 230RCo	150...240 VDC/DC	8 digitales	4 relés 10 Amp	Sin display Sin Teclado

Nota: EL PLC propuesto para el proyecto es el señalado con el ovalo rojo.

[14] De ellos pueden utilizarse alternativamente: 2 entradas analógicas (0 ... 10V) y 2 entradas rápidas (computacionales rápidos (contador de avance/retroceso, interruptor de valor umbral)).

2. DATOS TECNICOS LOGO! 12/24RC

Fuente de alimentación	
Tensión de entrada	12/24V DC
Rango admisible	18.8...28,8 VAC
Frecuencia de red admisible	47...63 Hz
Consumo de corriente **12 VAC** **24 VAC**	 30…140 mA 20...75 mA
Compensación de fallos de Tensión **12 VAC** **24 VAC**	 típ. 2 ms típ. 5 ms
Potencia disipada **12 VAC** **24 VAC**	 0.3 ... 1.7 W 0.4 ... 1.8 W
Tamponaje del reloj a 25ºC	típ. 80 h
Exactitud del reloj de tiempo real	Max 2 s / dia
Entradas digitales	
Cantidad	8
Tensión de entrada para **Señal 0** **Señal 1**	 <5 VDC >8VDC
Intensidad de entrada para **Señal 0** **Señal 1**	 <1 mA <0.05 mA >1.5 mA >0.1 mA
Tiempo de retardo para **Cambio de 0 a 1** **Cambio de 1 a 0**	 tip 1.5 ms tip 1.5 ms
Entradas digitales	
Cantidad	2

Margen	0...10VDC, impedancia de entrada de 76Ω
Tensión de entrada máxima	28.8VDC
Longitud del conductor (sin blindaje)	100m
Salidas digitales	
Cantidad	4
Tipo de salidas	Salidas a relee
Separación galvanica	Si
Activación de una entrada digital	Si
Resistencia a corto circuito 1	Contactor potencia B16, 600A

ANEXO C
POZOS DE ABASTECIMINENTO LOCALIZACION GENERAL