UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DEL ALGORITMO DE ENCRIPTAMIENTO AES EN UNA RED WiMAX PARA INSTITUCIONES GUBERNAMENTALES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

WILMER OSWALDO CUADROS COTOS

PROMOCIÓN

2001 – II

LIMA – PERÚ
2011

ESTUDIO DEL ALGORITMO DE ENCRIPTAMIENTO AES EN UNA RED WiMAX PARA INSTITUCIONES GUBERNAMENTALES

DEDICATORIA

A mis queridos padres, que siempre creyeron en mí y me dieron las herramientas para seguir hacia adelante, dándome ejemplos dignos de superación y entrega.

SUMARIO

WiMAX es un estándar de comunicación de última generación, iniciado por el IEEE y especialmente diseñado para proveer accesos vía radio de alta capacidad a distancias inferiores a 50 kilómetros y con tasas de transmisión de hasta 70 Mbps.

Las soluciones WiMAX se pueden aplicar en multitud de escenarios (enlaces punto a punto, redes metropolitanas, cobertura de hot-spots WiFi, redes empresariales, backbones, etc.) con altas garantías de disponibilidad y estabilidad. El propósito de este estudio es hacer un resumen sobre las tecnologías que hacen posible el funcionamiento de WiMAX.

Así, se presentan en primer lugar las técnicas más comunes de acceso al medio y las definidas en el estándar WiMAX, para continuar con una breve explicación sobre el tipo de antenas.

A continuación, se hace una recopilación de las novedades en procesado de señal que se incluyen dentro del estándar, con la principal novedad de las modulaciones OFDM. Seguidamente, se hace un análisis de las bandas de frecuencia en que se realizan los despliegues WiMAX, comentando las particularidades y beneficios de cada una de ellas, así como las peculiaridades de los despliegues de uso libre y con licencia. Para finalizar se revisara los resultados obtenidos en el demostrador, se valida que la solución WiMAX es totalmente viable para dar servicio Internet a zonas rurales. Se demostrara que servicios que requieren elevados anchos de banda como son los de videoconferencia, se pueden llevar a cabo con una alta calidad. Además, se ha probado que estas prestaciones se pueden conseguir a unas distancias de unos 1.5 - 2 Km entre la estación base y el terminal de usuario.

Para garantizar que estos enlaces sean seguros, utilizaremos la encriptación AES para dar un buen soporte de confiablidad de toda la información a transmitir [1].

INDICE

PROLOGO

De manera histórica, la comunicación ha demostrado ser el mecanismo más efectivo para la resolución de problemas y la evolución humana, al grado de que en la actualidad, los sistemas de telecomunicaciones son elementos indispensables en cualquier sociedad debido a que proveen el medio más eficaz para el desarrollo de los procesos de comunicación a nivel mundial. Por lo importante que son las comunicaciones en la actualidad, existen localidades totalmente incomunicadas, debido a temas de infraestructura, que no facilita la implementación de una red de telefonía básica, ya sea por lo agreste de la zona como el costo de realizar dicha implementación .

La solución a realizarse es la implementación de una red interna apoyándonos en la tecnología inalámbrica, siendo la más óptima el uso del sistema WiMAX.

El despliegue de una red WIMAX es corto a comparación del despliegue de otros medios de comunicación (cableado). El costo de los equipos es relativamente alto, pero el tiempo de recuperar la inversión sería corto a comparación de depender de una red de capital privado. Esta solución es óptima para comunidades de población pequeñas, donde la posibilidad de implementar una red privada de comunicación es muy baja.

Entre los alcances y usuarios potenciales son:

Educación y cultura (Ministerio de Educación, institutos y universidades).

Mejoras en los programas educativos, tanto en contenidos como en la disponibilidad de los mismos.

Mayor interacción en el proceso enseñanza-aprendizaje.

Entre las aplicaciones tenemos tele-secundarias, tele-preparatorias, educación superior a distancia o semi presencial, videoconferencias, etc.

Salud (Ministerio de Salud, Hospitales Estatales).

Atención y detección de enfermedades, detección y control de epidemias, Servicios médicos especializados a distancia y en tiempo real.

Entre las aplicaciones tenemos la tele-medicina en sitios fijos, interconexión de centros de salud, acceso a bases de datos con información sobre enfermedades.

Telefonía rural (Habitantes de localidades rurales que carecen de este servicio).

La red permitirá cursar llamadas telefónicas, por lo que podrá ser concesionado a particulares que deseen proveer el servicio.

Organismos Públicos (JNE, ONPE, Defensa Civil).

La población ejercerá su derecho de los comicios electorales, apoyo en la prevención en desastre y la atención de emergencias.
Entre las aplicaciones tenemos la implementación del sistema del voto electrónico en los comicios electorales.

En el capítulo I describe la necesidad que tiene las localidades y comunidades que se encuentran aisladas.

En el capítulo II nos enfocaremos del sistema WiMAX para realizar la comunicación entre las localidades aisladas.

En el capítulo III describe la seguridad para aplicar en el enlace WiMAX, para este conexión aplicaremos como encriptación de seguridad al algoritmo AES.

En el capítulo IV describe aplicación para realizar el enlace basado en el sistema WiMAX aplicando como algoritmo de encriptación al AES. Esta implementación se desarrollara bajo el escenario de 2 comunidades, una cuenta con todos los servicios (San Jerónimo de Surco) y la otra comunidad solo cuenta con el servicio electrificado (Huaquicha).

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

Este capítulo se orienta en el planteamiento de ingeniería del problema. Inicialmente se describe el problema y el objetivo del trabajo, complementariamente se evalúa el problema de ingeniería y se evalúa el problema planteado.

1.1 Descripción del Problema

En la actualidad existen muchas regiones donde la mayoría de las comunidades no cuenta con los servicios básicos y se encuentran incomunicadas. Por lo cual el gobierno busca soluciones para integrar a dichas comunidades y puedan ser apoyados por órganos estatales, que genere desarrollo y mejore su calidad de vida.

Uno de los motivos principales de la incomunicación de dichas zonas es lo agreste y de difícil acceso, lo cual dificulta la implementación de un medio de comunicación. Otro de los motivos es el distanciamiento que existe entre las comunidades, lo cual la solución exige que dichas comunidades se mantenga interconectada; que sus escuelas cuenten con el servicio básico de datos (internet), que dejo de ser un lujo y pasó a ser una necesidad.

La red que se implemente deberá contar con un sistema de seguridad que sea flexible, confiable y escalable para futuros servicios.

Los requerimientos solicitados para esta implementación son:

- **Conexión**
- **Movilidad**
- **Flexibilidad**
- **Sencillez**
- **Seguridad**

Así también se debe tomar en cuenta la vigencia en el tiempo de la solución brindada, debido a que la tecnología avanza y con estos la capacidad de procesamiento, por lo tanto aumentara la capacidad para encontrar la clave de cifrado utilizando el método de la fuerza bruta, por tal motivo el presente documento tiene una vigencia en el tiempo de 3 a 5 años que es el tiempo en que cambia la tecnología. En este panorama se detallan los requerimientos solicitados por la empresa, para la implementación del acceso a la red con seguridad basada con encriptamiento.

1.1.1 Conexión

Este requerimiento indica la conexión punto a multipunto, la cual debe contar con seguridad.

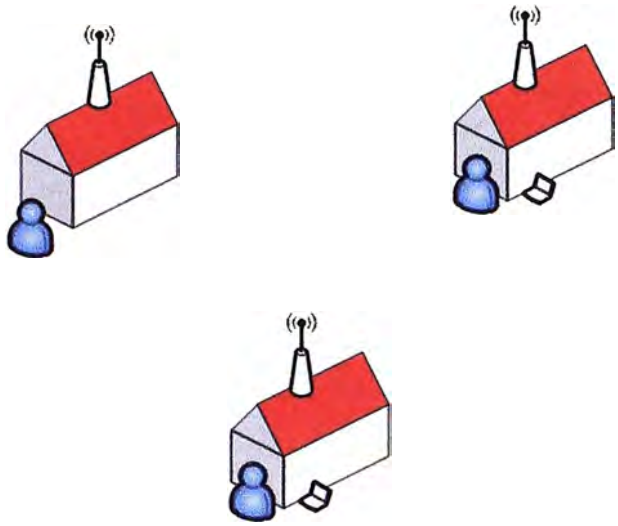

Fig.1.1 Requerimiento de conexión

1.1.2 Movilidad

Este requerimiento indica que el usuario final pueda movilizarse por toda esta localidad, contando con equipos portátiles (laptops), y los estudiantes podrán dar provecho al programa OLPC (One Laptop Per Child), apoyándonos en la tecnología wireless.

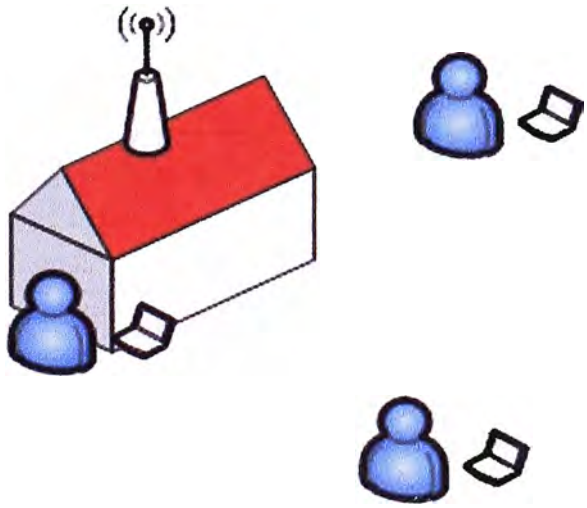

Fig.1.2 Requerimiento de movilidad

1.1.3 Flexibilidad

Este requerimiento indica que el usuario final pueda trabajar en cualquier punto de la comunidad con la misma configuración de la interface inalámbrica, sin algún problema de conexión y sin la necesidad que un soporte tenga que configurar el acceso por cada local, ya que este proceso para el usuario final es burocrático y tedioso, lo cual genera fastidio y frustración.

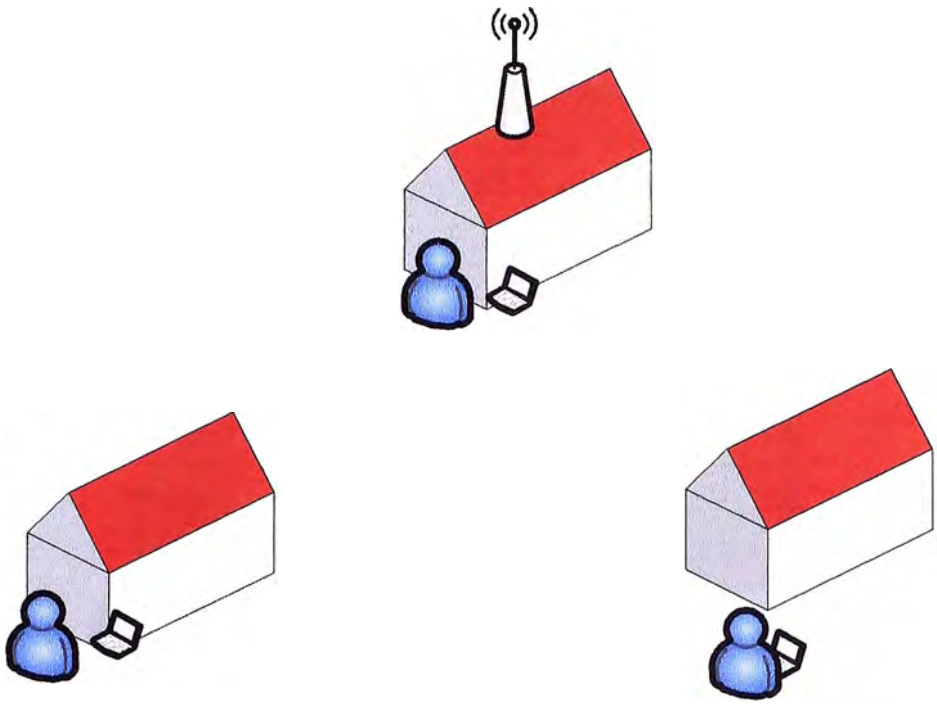

Fig.1.3 Requerimiento de flexibilidad

1.1.4 Sencillez

Este requerimiento hace referencia en la forma de conexión, esta debe ser lo más fácil posible para el usuario final, con la finalidad de pasar desapercibido y no afecte sus labores diarias.

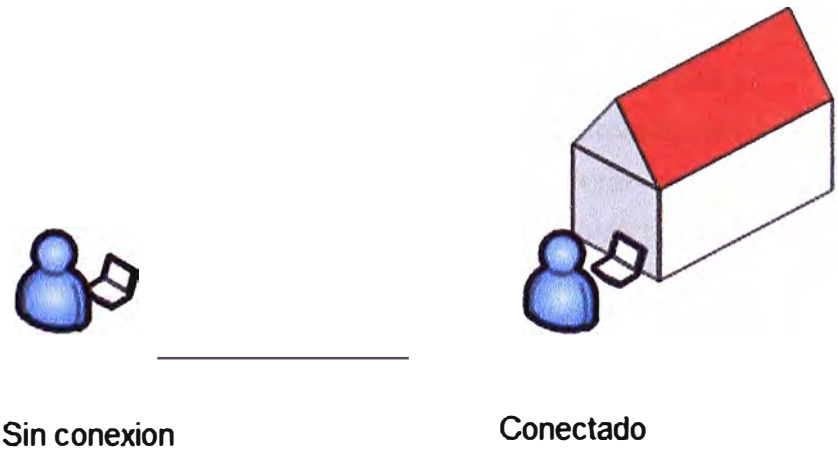

Fig.1.4 Requerimiento de sencillez

1.1.5 Seguridad

En los inicios de este tipo de redes se utilizaba un acceso abierto, debido a este motivo cualquier persona dentro del radio de alcance del equipo de acceso podía acceder a sus servicios libremente y de esta manera podría realizar actos ilícitos como robo de información. Al observar este problema las empresas comenzaron a utilizar el primer algoritmo de cifrado publicado por la IEEE, conocido como WEP (Wired Equivalent Privacy), para su tiempo este fue una solución viable, pero en la actualidad se ha desarrollado software que puede determinar la clave y por lo tanto este método no es

seguro para una empresa. Por consiguientes se aplicara una encriptación más robusta WPA2-AES.

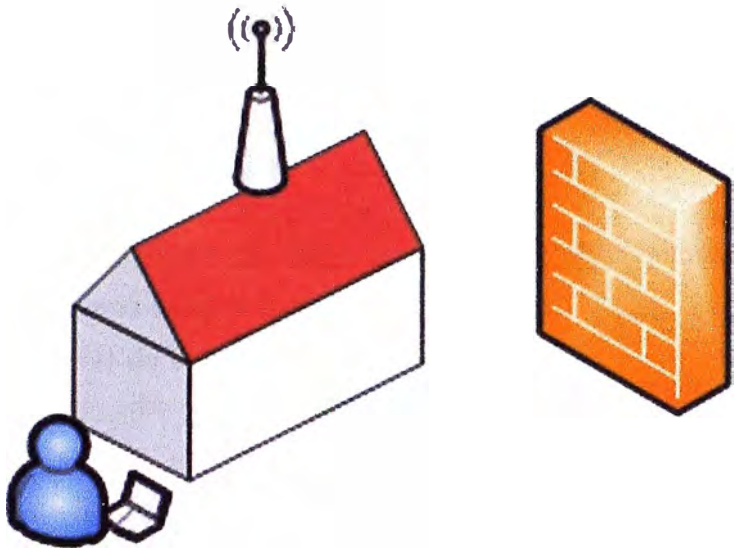

Fig.1.5 Requerimiento de seguridad

1.2 Objetivo del trabajo

Desarrollar, mantener y operar una red de telecomunicaciones de alto beneficio social, a través del despliegue de infraestructura tecnológica sustentable.

Diseñar una red de telecomunicaciones de alta disponibilidad, que permita transmitir voz, datos y video a tiempo real, a las pequeñas comunidades rurales.

Establecer convenios con diversas instituciones y empresas para integrar una serie de aplicaciones contenidos a la red, que permitan explotar de manera adecuada la infraestructura tecnológica la implementación de este proyecto hacia el resto del territorio peruano.

1.3 Evaluación del problema.

En función a los requerimientos establecidos en la sección anterior, se constituye el problema de brindar comunicación a las comunidades alejadas, aprovechando un enlace punto a multipunto con una comunidad que cuenta con todos los servicios básicos de comunicación (telefonía, internet). La tecnología más recomendada para enlaces punto a multipunto es el WIMAX cuya seguridad estará basada utilizando como encriptación el algoritmo AES.

Una vez recepcionada la señal, esta se tendrá que distribuir a la comunidad, por tratarse de comunidades pequeñas, se tendrá que implementar una red con tecnología wireless.

Capítulo II
MARCO TEORICO CONTEXTUAL

En este capítulo se exponen las bases teóricas conceptuales más importantes para la comprensión del sistema descrito en el presente informe.

2.1 Descripción general de WiMAX o IEEE 802.16

Debido a la revolución de las telecomunicaciones ha permitido la aparición de tecnologías digitales de banda ancha para dar acceso a Internet a grandes velocidades vía cable (DSL, Cable-Modem) y vía radio (3G o UMTS). La aparición es debida al hecho de que cada vez existen más organizaciones, escuelas, empresas y zonas residenciales donde el acceso a Internet es primordial, ya sea por temas de negocio, académicos o de distracción, hecho que hace que aumente la cantidad de usuarios que se quieren conectar. Es por este motivo que se tuvo que aumentar el ancho de banda de los sistemas para poder soportar la conectividad de más usuarios a altas velocidades. No obstante, el acceso a Internet con estas tecnologías cubre principalmente a zonas con una alta densidad de población y probabilidad elevada de frutos económicos como por ejemplo las ciudades, un objetivo principal de los proveedores de servicios. Esto significa que aquellos sitios con escasa densidad de población, apartados de la ciudad y también de las centralitas de los mismos proveedores, no podrán aprovechar los beneficios de las tecnologías anteriores debido al elevado costo del cableado.

Quizás se podría pensar que posibles alternativas para evitar el cable en la última milla sería el acceso por UMTS (Universal Mobile Telecommunications System); la respuesta es que no y esto es debido por la principal razón de que el costo de una BS de UMTS es mayor que la de una BS de WiMAX, además del elevado precio que supone mantener licencias de bandas frecuenciales para UMTS.

Para hacer frente a esta contrariedad y poder dar solución para conectividad a Internet, principalmente en las zonas rurales a alta velocidad, se creó en el año 1998 el grupo de IEEE 802.16 para poder desarrollar un estándar en el que permitía desarrollar un sistema wireless de banda ancha basado en la topología punto-multipunto con visión directa (LOS) en la banda de operación de 10 GHz-66GHz. Este estándar aceptado en Diciembre del 2001, se basaba en una sola portadora en la capa física y con multiplexación por división de frecuencia (TDM) en la capa de control de acceso al medio (MAC). El inconveniente de este estándar es la utilización de una sola portadora

para la transmisión y frecuencias de portadoras extremadamente altas, hecho que limitaba aplicaciones de conectividad fija.

Con el tiempo el grupo de IEEE 802.16 produjo subsecuentemente 802.16a como un arreglo al estándar 802.16 para permitir aplicaciones sin visión directa en la banda de 2GHz-11GHz, uso de múltiples subportadoras OFDM, topologías punto-multipunto y en malla y una amplia variedad de canales con diferentes anchos de banda. Estas mejoras se reflejan en dos nuevos estándares o revisiones del estándar original IEEE 802.16a: el estándar IEEE 802.16-2004 conocido como WiMAX fijo (en el resto del documento se referirá a WiMAX) y el estándar IEEE 802.16e-2005 conocido como WiMAX móvil. Tanto una como la otra no requieren LOS dado que operan en bandas de frecuencias más bajas que la primera variante de WiMAX 802.16.

IEEE 802.16-2004 es una de las futuras revisiones de IEEE 802.16a que opera a la misma banda frecuencial y también utiliza OFDM para transmitir múltiples símbolos a usando 256 subportadoras. Esta variante es una especificación de IEEE 802.16d o WiMAX fijo ya que se creó con el objetivo de dar cobertura a emplazamientos fijos. Cuando se dice especificación se refiere a que IEEE 802.16d fue adoptado por WiMAX Forum, una organización que se creó con la finalidad de permitir la interoperabilidad entre equipos de diferentes fabricantes.

WiMAX Forum es una organización industrial sin ánimo de lucro conformada a partir de los operadores de telecomunicaciones y compañías de componentes y equipamientos para certificar y promover la compatibilidad e interoperabilidad de los productos de banda ancha basados en el estándar IEEE 802.16. Uno de los principales objetivos de este organismo es acelerar la introducción de estos sistemas en el mercado.

En la **Fig. 2.1** muestra una de las aplicaciones de WiMAX en el que una estación base puede dar servicio en un zona empresarial, en una área residencial y a vehículos en movimiento en su celda. IEEE 802.16e-2005 o WiMAX móvil se puede considerar como una versión mejora de su predecesor, el IEEE 802.16-2004 ya que permite dar cobertura no tan solo fija sino también móvil en el sentido que los usuarios móviles pueden mantener la comunicación sin que se perciba el cambio de asociación entre estaciones base por medio del procedimiento de handover.

La diferencia a nivel físico entre WiMAX fijo y WiMAX móvil es el número de subportadoras utilizadas para modular los símbolos de información. Como ya se ha dicho, IEEE 802.16-2004 solamente soporta 256 subportadoras OFDM por usuario mientras que IEEE 802.16e-2005 ofrece un número de subportadoras hasta un máximo de 2048 que se pueden asignar a diferentes usuarios mediante el esquema de acceso múltiple ODFMA, es decir, el acceso al canal es por medio de unas ciertas subportadoras asignadas por la BS.

Observamos en la **TABLA 2.1** las diferencias entre los diferentes estándares adoptados por IEEE y por WiMAX Forum que permite la interoperabilidad entre los diferentes fabricantes indicando la banda de frecuencias de operación, la capa PHY (capa física) a utilizar y otros parámetros **[2]**.

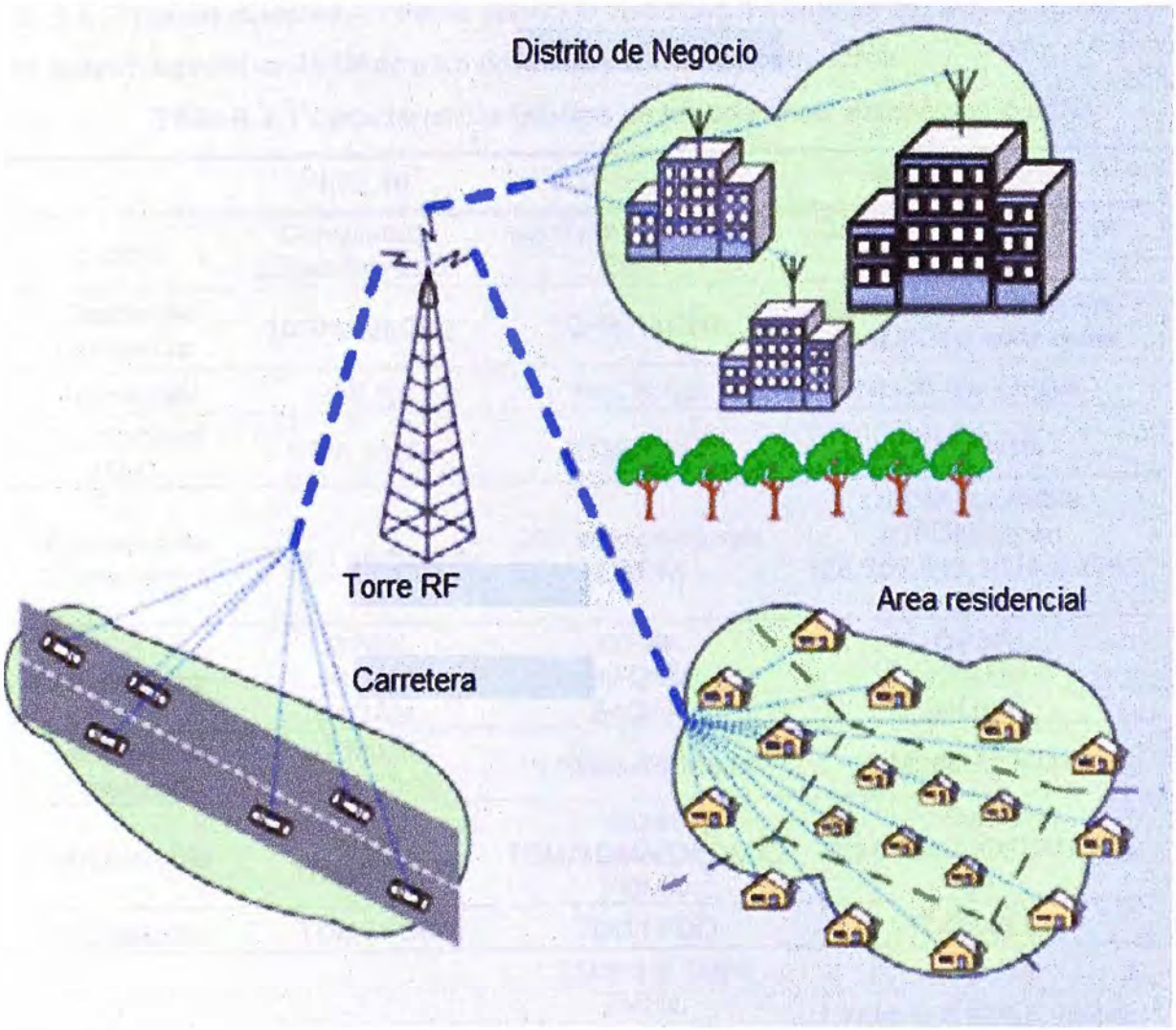

Fig. 2.1. Aplicación de WiMAX

2.2 Características principales

En este capítulo se menciona las características que hacen de WiMAX una tecnología, fiable, robusta y adaptable a cualquier ambiente debido a su gran número de opciones que ofrece y que se comentan a continuación.

2.2.1 En la capa física

-**Capa física basada en OFDM**: La capa física de WiMAX está basada en OFDM, un esquema que permite una buena resistencia al efecto multi camino (multipath) incluso en condiciones NLOS.

-**OFDMA:** Es una técnica utilizada por WiMAX móvil para el acceso múltiple aprovechando la diversidad multiusuario donde cada usuario es asignado a una serie de subportadoras o subcanales.

-Elevados máximos de velocidad: Debido al conjunto de las técnicas de modulación y codificación adaptativa, así como de la diversidad de antenas y de la multiplexación espacial, WiMAX permite conseguir una elevadas velocidades máximas. Por ejemplo, trabajando un ancho de banda de 10MHz y el esquema de duplexado TDD con una tasa de 3:1 (3 tramas downlink - 1 trama uplink) la velocidad máxima en capa física (grossrate) es aproximadamente 25 Mbps para downlink y 6.7 Mbps para uplink.

TABLA 2.1 Características básicas de los diferentes estándares WiMAX

	802.16	802.16-2004	802.16e-2005
Estado	Completado Diciembre 2001	Completado Junio 2004	Completado Diciembre 2005
Banda de frecuencia	10GHz-66GHz	2GHz-11GHz	2GHz-11GHz para fijo; 2GHz-6GHz para móvil
Aplicación	LOS fija	NLOS fija	NLOS fija y móvil
Arquitectura MAC	PTM, malla	PTM, malla	PTM, malla
Esquema de Transmisión	Solo 1 portadora	256 subportadoras OFDM	OFDM escalable (OFDMA) con 128,256,512,1024 o 2048 subportadoras
Modulación	QPSK 16QAM 64QAM	QPSK 16QAM 64QAM	QPSK 16QAM 64QAM
Velocidad de transmisión	32 Mbps-134.4 Mbps	1 Mbps-75 Mbps	1 Mbps-75 Mbps
Multiplexado	Burst TDM/TDMA	Burst TDM/TDMA/OFDM/OFDMA	Burst TDM/TDMA/OFDM/OFDMA
Duplexado	TDD i FDD	TDD i FDD	TDD i FDD
Anchos de banda de canal	20MHz, 25MHz, 28MHz	1.75MHz,3.5Mhz, 7MHz, 10MHz, 15MHz, 8.75MHz 14MHz, 1.25MHz, 5MHz,	1.75MHz,3.5Mhz, 7MHz, 10MHz, 15MHz, 8.75MHz 14MHz, 1.25MHz, 5MHz,
Designación interfaz aérea	Wireless MAN-SC	Wireless MAN-OFDM	Wireless MAN-OFDM
Implementación Wimax	Ninguna	256-OFDM	OFDMA escalable

-Velocidad y ancho de banda escalables: Esta característica es solo para IEEE 802.16e-2005 con el modo escalable OFDMA. Permite adaptar la velocidad con el ancho de banda del canal disponible. Cuanto más grande es el ancho de banda del canal, más grandes será el tamaño de la FFT y eso implica más sub portadoras habrá en el canal facilitando un aumento de la tasa de datos o velocidades de transmisión.

-**Modulación y codificación adaptativa (AMC):** Esta técnica es una de las principales características que hacen que WiMAX sea una tecnología que se adapte al usuario en función de un canal variante en el tiempo.

Esta técnica cambia la modulación y/o la codificación FEC teniendo en cuenta la SNR instantánea que el receptor WiMAX recibe en un instante de tiempo. Por esto se llama adaptativa, ya que utiliza la mejor modulación y/o codificación para cada MAC PDU o sub trama de usuario que mejora notablemente su velocidad de información.

-**Soporte para técnicas de múltiples antenas:** Además de OFDM y AMC para aumentar la tasa de transmisión, WiMAX permite incorporar antenas adicionales al transmisor/receptor. Concretamente, la velocidad se aumenta gracias a las técnicas de antenas avanzadas tales como: beamforming, codificación en espacio-tiempo (STC) y multiplexación espacial.

2.2.2 En la capa MAC

-**Retransmisiones de capa de enlace:** WiMAX utiliza una de las técnicas utilizada en muchas redes de computadoras que se conoce como ARQ. Esta técnica permite retransmitir aquellos paquetes enviados al destino del cual el transmisor no ha recibido ninguna justificación de recepción a través del ARQ. Cada paquete trasmitido es reconocido por el receptor y este último envía una justificación de la recepción.

-**Soporte por FDD y TDD:** Tanto IEEE 802.16-2004 como IEEE802.16e-2005 soportan duplexado FDD y TDD. TDD será el duplexado definitivo para el destino de WiMAX ya que dispone de más ventajas: Más eficiencia espectral ya que no son necesarias dos bandas de frecuencias.

Utilizando TDD se pueden tener enlaces asimétricos y por lo tanto más flexibilidad a la hora de escoger las velocidades de downlink y de uplink, reciprocidad del canal para los dos enlaces y al operar en una sola banda frecuencial, menos complejidad en los equipos.

-**Designación de recursos dinámicos y flexibles para usuario:** La designación de recursos a los usuarios como ancho de banda en los canales de bajada y subida, es controlado por un programa de la estación base. Aun así, cuando existe diversidad multi-usuario, la designación puede estar realizada en tiempo (TDM), en frecuencia (OFDM) o en espacio (AAS). El estándar permite la designación de los anchos de banda en estos tres dominios.

-**Calidad del servicio (QoS):** La capa MAC de WiMAX tiene una arquitectura orientada a conexión que está diseñada para soportar una diversidad de aplicaciones, incluyendo servicios de voz y multimedia con una diversidad de usuarios con múltiples conexiones/usuario. QoS de Wimax ofrece tasa de bits constante, tasa de bits variables,

flujo de tráfico en tiempo no real y tráfico de datos best-effort de manera que permite adaptarse a los requerimientos QoS de cada conexión de usuario.

-Soporte para la movilidad: La variante de WiMAX móvil incluye una serie de mecanismos que permiten al usuario obtener una conectividad móvil, eficiente y muy robusta para aplicaciones tolerantes a los retardos, como VoIP especialmente en casos de cambio de estación base (handover).

Técnicas como estimación de canales frecuentes, ahorro de potencia, sub canalización de uplink y control de potencia también son especificadas en el soporte para aplicaciones móviles.

2.3 Seguridad en redes WiMAX

La seguridad WiMAX es compatible dos estándares de encriptación de calidad, DES3 y AES, que es considerado tecnología de vanguardia. Básicamente, todo el tráfico en redes WiMAX debe ser encriptado empleando el Counter Mode con Cipher Block Chaining Message Authentication Code Protocol (CCMP) que utilizan AES para transmisiones seguras y autenticación de la integración de datos **[3]**.

2.4 Definición de Instituciones Gubernamental

Las instituciones gubernamentales es la agrupación de organismos administrativos del Estado que cumple, o hace cumplir la política o voluntad expresada en las leyes que existe en el País. Esta clasificación está incluido dentro del sector público: al Poder Legislativo, Poder Ejecutivo, Poder Judicial y organismos públicos autónomos, instituciones, empresas y personas que realizan alguna actividad económica en nombre del Estado y que se encuentran representadas por el mismo, es decir, que abarca todas las actividades que el Estado posee o administra.En las instituciones gubernamentales en donde se podría utilizar este servicio de WiMAX son los siguientes:

2.4.1 Educación y cultura (Ministerio de Educación, institutos y universidades).

Mejoras en los programas educativos, tanto en contenidos como en la disponibilidad de los mismos. Mayor interacción en el proceso enseñanza-aprendizaje.

Entre las aplicaciones tenemos tele-secundarias, tele-preparatorias, educación superior a distancia o semi presencial, videoconferencias, etc.

2.4.2 Salud (Ministerio de Salud, Hospitales Estatales).

Atención y detección de enfermedades, detección y control de epidemias, servicios médicos especializados a distancia y en tiempo real.

Entre las aplicaciones tenemos la tele-medicina en sitios fijos, interconexión de centros de salud, acceso a bases de datos con información sobre enfermedades.

2.4.3 Telefonía rural (Habitantes de localidades rurales que carecen de este servicio).

La red permitirá realizar llamadas telefónicas, por lo que podrá ser concesionado a particulares que deseen proveer este servicio. Entre la comunicación y la interacción de las redes humanas, para el bienestar de las familias y las comunidades.

2.4.4 Organismos Públicos (JNE, ONPE, Defensa Civil).

La población ejercerá su derecho de los comicios electorales, apoyo en la prevención de desastres y en la atención de emergencias.

Entre las aplicaciones tenemos la implementación del sistema del voto electrónico en los comicios electorales.

CAPITULOIII
INTRODUCCIÓN ALGORITMO ENCRIPTADO AES

3.1 Reseña e introducción AES (Advanced Encryption Standar)

AES es el nuevo estándar de cifrado simétrico elegido por el NIST, después de un periodo de competencia entre 15 algoritmos sometidos. El 2 de Octubre del 2000 fue escogido el algoritmo Rijndael como AES, el estándar reemplazó de TDES, para ser usado en los próximos 20 años. Esta información describe de forma detallada el algoritmo y algunas de sus características.

El algoritmo Rijndael fue elegido por el NIST (National Institute of Standards and Technology), para ser el estándar en los próximos 20 años y es denominado AES (Advanced Encryption Standar). Rijndael fue escogido después de pasar un periodo de análisis durante aproximadamente 3 años, Rijndael fue elegido como la mejor opción dentro de 15 candidatos, sus principales características fueron su fácil diseño, su versatilidad en ser implementado en diferentes dispositivos, así como ser inmune a los ataques conocidos hasta la fecha, soportar bloques de datos de 128 bits y claves de 128, 192, y 256 bits. La idea básica general es tener un estándar que mejore el "performance" de TDES y sea resistente a los ataques conocidos.

La descripción de AES que llevaremos toma el siguiente forma;

AES (Advanced Encryption Standar) es el nuevo estándar de criptografía simétrica asumido en el FIPS (Federal Information Processing Standards). En este reporte estamos comprometidos a poder dar de la manera más simple la descripción total del algoritmo, y dar algunas características de gran importancia.

Desde 1977 que apareció la primera versión del estándar FIPS, asume como estándar el algoritmo DES (Data Encryption Standar), y sus posteriores reafirmaciones en 1983, 1988, 1993, y 1999. Casi siempre había visto opiniones controversiales de DES, sin embargo nunca fue dado un ataque que derivara por completo la clave secreta partiendo de la información pública, pero su corta longitud de clave lo comprometía poco a poco. La última reafirmación de DES en octubre de 1999 realmente fue suplantado por TDES, que es una versión múltiple de DES, designado como TDEA (Triple Data Encryption Algorithm). De hecho, ya se tenían planes de buscar un substitución definitivo a DES. A pesar de un número grande de algoritmos que en la época estaban presente como: IDEA, RC5, 3-way, FEAL, LOKI, SAFER, SHARK, NIST decidió convocar a un

concurso que tuvo como principales objetivos obtener un algoritmo simétrico que certifique su seguridad para los próximos 20 años a partir del año 2000. La invitación apareció el 2 de enero de 1997, se admitieron 15 algoritmos, en agosto de 1998 en la primera conferencia AES se debatieron los algoritmos sometidos y posteriormente en la segunda conferencia AES en marzo de 1999, se realizaron los últimos comentarios. Para que en agosto de 1999 se comunicaran los 5 finalistas: MARS, RC6, Rijndael, Serpent y Twofish. En abril del 2000 se llevó a cabo la tercera conferencia AES, recibiendo los últimos análisis, para que finalmente el 2 de octubre del año 2000 se diera a conocer el ganador y se dispuso al Algoritmo RIJNDAEL como AES.

Esto llego a ser asumido oficial en noviembre 26 el 2001 en el FIPS. A partir de esa fecha hay conferencias especiales para analizar la situación actual de AES, la última se llevada a cabo en mayo del 2004.

El algoritmo Rijndael fue designado especialmente para garantizar seguridad, que significa estar protegida de los ataques conocidos, tener un diseño simple, y poder ser realizado en la mayoría de los escenarios posibles, desde dispositivos con recursos limitados, como smart cards, hasta procesadores paralelos. El tiempo permitido que AES sea adaptado poco a poco, desde los protocolos más usados como SSL, hasta las aplicaciones más especializadas, como VoIP.

La descripción de AES es simple si se cuentan con todos los elementos. Esta consiste en dos partes, la primera en el proceso de cifrado y la segunda en el proceso de generación de las subclaves, una primera aproximación se muestra la siguiente **Fig.3.1.**

Entonces la descripción de AES consiste de dos partes, en describir el proceso de "Cifrado" y el proceso de "Generación de las subclaves" o "Extensión de la clave K". El bloque de cifrado tiene una longitud de 128 bits, la longitud de la clave K varia de 128, 192 y 256 bits, en cada caso AES tiene 10,12, y 14 rondas respectivamente.

El proceso de cifrado consiste esencialmente en la descripción de las 4 transformaciones básicas de AES:

-ByteSub

-ShiftRow

-MixColumns

-AddRoundKey

Es significativo mencionar que el caso de Rijndael las funciones o transformaciones básicas son ligeramente diferentes en el proceso de descifrado, sin embargo es poco el esfuerzo necesario para poder comprender todo.

Los autores del algoritmo escribieron un libro que se ha tomado como referencia oficial donde se describe con mayor profundidad varios aspectos aquí expuestos **[4]**.

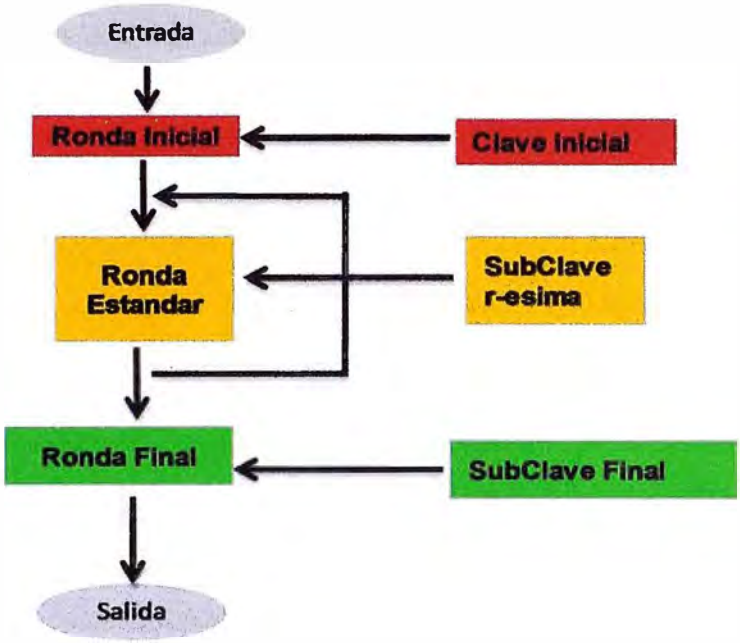

Fig. 3.1 Proceso de cifrado

De manera un poco más detallada el algoritmo AES llega a ser:

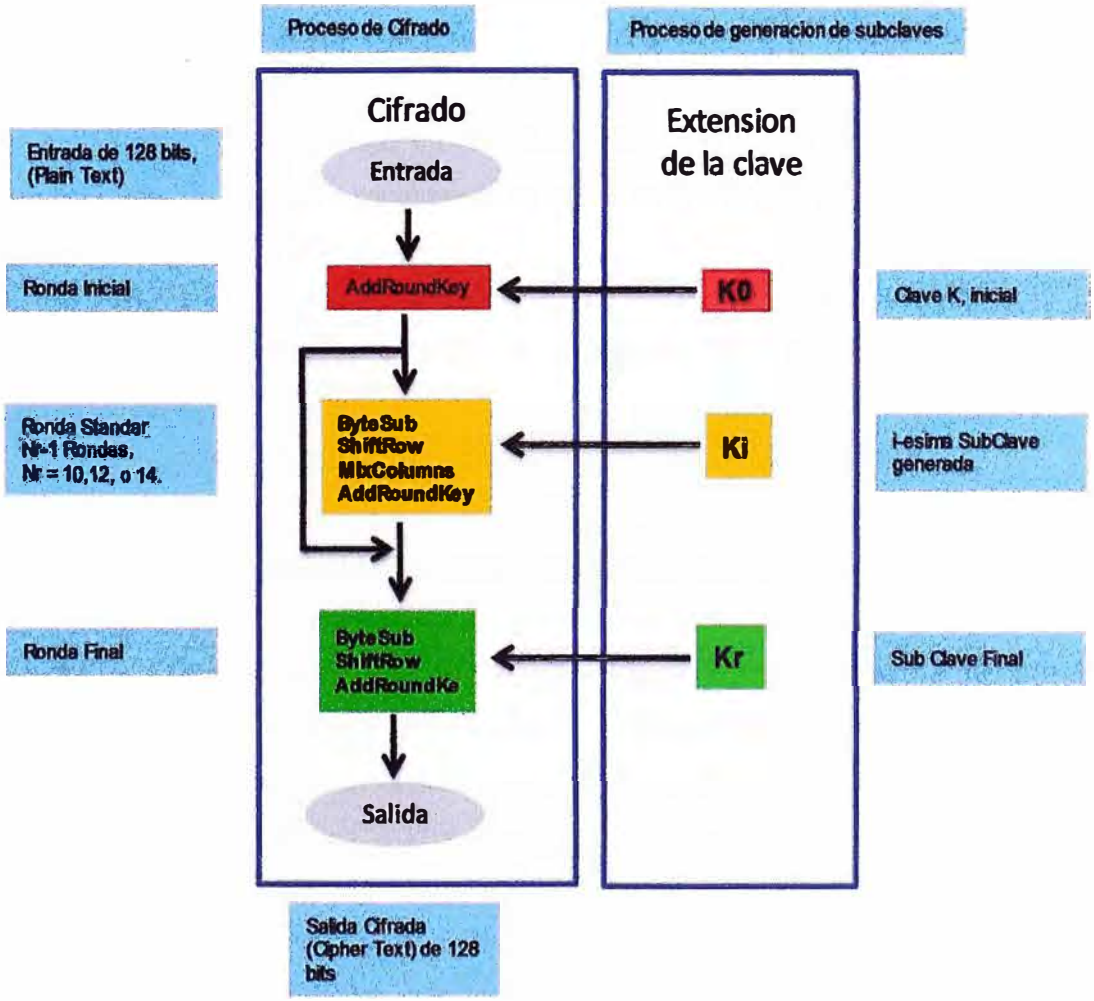

Fig. 3.2 Proceso de generación de las subclaves

3.2 Preliminares matemáticos

La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado. La seguridad del cifrado Rijndael se basa en el desorden provocado en el contenido del texto en claro al aplicarle una serie de permutaciones y otras operaciones matemáticas.

Algunas de estas operaciones se realizan a nivel de byte, representado mediante el campo llamado GF (2^8) y otras a nivel de palabras de cuatro bytes.

Para la comprensión del algoritmo es necesario conocer cada una de estas operaciones, para lo cual se deberá introducir una serie de conceptos matemáticos antes de iniciar el estudio del algoritmo propiamente dicho.

3.2.1 Representación de un byte en el campo GF (2^8)

El campo GF (2^8) se trata de un campo finito en el que los elementos (en nuestro caso bytes) serán caracterizados como polinomios de grado 7 y con coeficientes binarios, esto es, en {0,1}.

Un byte b se compone de 8 bits que caracterizamos como b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0 donde b_7 representa el bit de mayor peso y b_0 al de menor. Así podemos representar el byte como un polinomio cuyos coeficientes son los bj con j=0..7 y donde estos bj pueden tomar los valores 0 ó 1.

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 \quad \textbf{(3.1)}$$

Por ejemplo, un byte que represente el valor hexadecimal '57' (en binario 01010111) se corresponde con el polinomio:

$$0x^7 + 1x^6 + 0x^5 + 1x^4 + 0x^3 + 1x^2 + 1x^1 + 1 = x^6 + x^4 + x^2 + x + 1 \quad \textbf{(3.2)}$$

Un byte que represente el valor hexadecimal '83' (en binario 10000011) se corresponde con el polinomio:

$$1x^7 + 0x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1 = x^7 + x + 1 \quad \textbf{(3.3)}$$

a) Suma

La suma de dos elementos del campo GF (2^8) es la suma de dos polinomios, por lo que el resultado será otro polinomio. La suma de los coeficientes se corresponde con una suma módulo 2 términos a término. Se puede comprobar que esta suma se corresponde con una operación EXOR (denotada por $\oplus$) entre los coeficientes de los polinomios.

Por ejemplo, se puede efectuar la suma de los elementos del apartado anterior:

$$(57 + 83) = (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2 \quad \textbf{(3.4)}$$

Podemos comprobar que el conjunto de los polinomios de grado menor o igual que 7 y con coeficientes pertenecientes a Z2 forman un grupo conmutativo con la suma, es decir, es una operación interna, que cumple la propiedad asociativa, conmutativa, tiene elemento neutro y tiene simétrico. Debido a la existencia de simétrico podemos referirnos

a la operación resta, ya que se puede definir la resta de a y b, donde a y b son polinomios, como la suma de a con el simétrico de b.

b) Multiplicación

Al referirnos a la multiplicación empleada en el algoritmo Rijndael nos estaremos refiriendo realmente a la multiplicación de dos elementos del conjunto GF(2^8), es decir polinomios de grado menor o igual que 7 y con coeficientes en Z2 pero cuyo resultado se expresa modulo m(x) donde $m(x) = x^8 + x^4 + x^3 + x + 1$. Nótese que m(x) se puede representar en hexadecimal con el valor '11B' y se puede comprobar que es un polinomio irreducible. El propósito de realizar la multiplicación módulo m(x) es con el fin de que el resultado obtenido en la operación siga siendo un polinomio de grado menor que 8, por lo que la operación seguiría siendo a nivel de byte.

Por ejemplo, la operación multiplicación de los valores hexadecimales '57' y '83'sería:

$$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = \quad \textbf{(3.5)}$$

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x^5 + x^3 + x^2 + x) + (x^{13} + x^{11} + x^9 + x^8 + x^7) \quad \textbf{(3.6)}$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \quad \textbf{(3.7)}$$

Como se puede apreciar este polinomio es de grado mayor que 8 por lo que no pertenece a GF (2^8) y así la operación no se realiza a nivel de byte. Para remediar esto y conseguir que la multiplicación siga siendo una operación interna en GF (2^8) expresamos el resultado obtenido modulo m(x)

$$(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \bmod m(x) \quad \textbf{(3.8)}$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \bmod (x^8 + x^4 + x^3 + x + 1) \quad \textbf{(3.9)}$$

$$= x^7 + x^6 + 1 \quad \textbf{(3.10)}$$

Un caso destacado en cuanto a la multiplicación de polinomios en GF (2^8) es cuando nos surge la multiplicación de un polinomio b(x) de grado 7 por el polinomio c(x)= x

$$a(x) \bullet b(x) = x \bullet (b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0) \quad \textbf{(3.11)}$$

$$= b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \quad \textbf{(3.12)}$$

Como se puede apreciar, este polinomio no pertenece a GF (2^8) ya que su grado es 8.

Para que la operación sea interna en GF (2^8) dividimos entre $m(x) = x^8 + x^4 + x^3 + x + 1$ como hemos visto anteriormente.

Si el coeficiente b_7 de b(x) tiene valor 0, la operación será simplemente una función identidad de a(x)•b(x) ya que, como el grado de este polinomio es menor que el grado de m(x) el resto de la división entre m(x) será el propio polinomio a(x)•b(x).

$$(b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod (x^8 + x^4 + x^3 + x + 1) \quad \textbf{(3.13)}$$

$$= b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \quad \textbf{(3.14)}$$

Si el coeficiente b_7 de b(x) tiene valor 1, la división de a(x) •b(x) entre m(x) será en realidad una resta, ya que ambos polinomios tienen el mismo grado.

$$(b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod (x^8 + x^4 + x^3 + x + 1) \quad \textbf{(3.15)}$$

$$= (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) - (x^8 + x^4 + x^3 + x + 1) \quad \textbf{(3.16)}$$

$$= b_6x^7 + b_5x^6 + b_4x^5 + (b_3 - 1)x^4 + (b_2 - 1)x^3 + b_1x^2 + (b_0 - 1)x - 1 \quad \textbf{(3.17)}$$

$$= b_6x^7 + b_5x^6 + b_4x^5 + (b_3 + 1)x^4 + (b_2 + 1)x^3 + b_1x^2 + (b_0 + 1)x + 1 \quad \textbf{(3.18)}$$

Se puede observar que estas dos operaciones se pueden implementar con 4 funciones EXOR: 3 sobre los bits b_3, b_2, b_1 para la resta con los respectivos coeficientes de m(x), y una cuarta función EXOR que compruebe el valor del bit b_7 de b(x) para saber la operación a realizar, es decir, la función resta o la función identidad.

A esta operación se le denota b = xtime(a). Si se aplica esta operación reiterativamente encontraremos una manera sencilla y fácil de implementar el producto de un polinomio por una potencia de x.

$$b(x) \bullet x = \text{xtime}(b(x)) \quad \textbf{(3.19)}$$

$$b(x) \bullet x^2 = (b(x) \bullet x) \bullet x = \text{xtime}(b(x)) \bullet x = \text{xtime}(\text{xtime}(b(x))) \quad \textbf{(3.20)}$$

$$b(x) \bullet x^3 = (b(x) \bullet x) \bullet x = (\text{xtime}(\text{xtime}(b(x)))) \bullet x \;\; \text{xtime}(\text{xtime}(\text{xtime}(b(x)))) \quad \textbf{(3.21)}$$

3.2.2 Representación de palabras en el campo GF (2^8)

Tener en cuenta que indicamos como "palabra" a una agrupación de bytes. En este sentido una palabra constituida por cuatro bytes se puede representar como un polinomio de grado menor o igual que tres.

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \quad \textbf{(3.22)}$$

$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \quad \textbf{(3.23)}$$

La operación suma de polinomios se ejecuta a través de unas operaciones EXOR byte a byte, al igual que se hacía anteriormente al representar un byte mediante un polinomio de grado menor que 7. Esta operación es interna en GF (2^8) ya que la adición de dos polinomios de grado menor que 4 nos dará como resultado otro polinomio de grado menor que 4.

En cuanto a la operación multiplicación, nos encontramos de nuevo con la dificultad del apartado anterior. La multiplicación puede no ser una operación interna en GF (2^8), por lo que el producto de dos palabras de 4 bytes puede no ser representable por una palabra de 4 bytes, es decir, mediante un polinomio de grado menor que 4.

$$a(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \quad \textbf{(3.24)}$$

$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \quad \textbf{(3.25)}$$

$$a(x) \bullet b(x) = c(x) = c_6x^6 + c_5x^5 + c_4 + c_3x^3 + c_2x^2 + c_1x + c_0 \quad \textbf{(3.26)}$$

donde

$$c_0 = a_0 \bullet b_0 \quad \textbf{(3.27)}$$

$$c_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1 \quad \textbf{(3.28)}$$

$$c_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \quad \textbf{(3.29)}$$

$$c_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3 \quad \textbf{(3.30)}$$

$$c_4 = a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3 \quad \textbf{(3.31)}$$

$$c_5 = a_3 \bullet b_2 \oplus a_2 \bullet b_3 \quad \textbf{(3.32)}$$

$$c_6 = a_3 \bullet b_3 \quad \textbf{(3.33)}$$

Para resolver esta discusión se ha propuesto una solución semejante a la del apartado anterior: el resultado de la operación multiplicación se expresa módulo un polinomio de grado 4. Los autores del algoritmo Rijndael han elegido el polinomio $M(x)= x^4 + 1$ para tal fin. En este caso M(x) no es un polinomio irreducible como se le había exigido al anterior m(x). Esto va a impulsar que algunas de las multiplicaciones que realicemos puedan dar como consecuencia que no tenga inverso. En el caso del algoritmo Rijndael este caso no se va a presentar nunca ya que siempre se multiplica por polinomios que poseen inverso.

$$(a(x) \bullet b(x)) \bmod (x^4 + 1) = d(x) \quad \textbf{(3.34)}$$

donde

$$d(x) = d_3x^3 + d_2x^2 + d_1x + d_0 \quad \textbf{(3.35)}$$

Para hallar d_3, d_2, d_1, d_0 empleamos una sencilla regla:

$$x^j \bmod (x^4+1) = x^{j \bmod 4} \quad \textbf{(3.36)}$$

Así dispondremos los siguientes valores:

$$d_0 = a_0 \bullet b_0 \oplus a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3 \quad \textbf{(3.37)}$$

$$d_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1 \oplus a_3 \bullet b_2 \oplus a_2 \bullet b_3 \quad \textbf{(3.38)}$$

$$d_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \oplus a_3 \bullet b_3 \quad \textbf{(3.39)}$$

$$d_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3 \quad \textbf{(3.40)}$$

Otra forma de expresar esta operación es mediante el uso de matrices

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \bullet \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad \textbf{(3.41)}$$

Un caso especial de la multiplicación de polinomios es la multiplicación de un polinomio b(x) por el polinomio x.

$$b(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \quad \textbf{(3.42)}$$

$$d(x) = x \bullet b(x) = b_3x^4 + b_2x^3 + b_1x^2 + b_0x \quad \textbf{(3.43)}$$

Dividimos d(x) entre $M(x)= x^4 + 1$ para obtener un polinomio de grado menor que cuatro

$$c(x) = d(x) \bmod (x^4 + 1) = b_2x^3 + b_1x^2 + b_0x + b_3 \quad \textbf{(3.44)}$$

Esta multiplicación también se puede expresar como el producto de dos matrices, de la misma forma que la matriz anterior pero cuyos elementos son sustituidos todos '00', a excepto los a1, que se sustituyen por el valor '01'.

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 00 & 00 & 00 & 01 \\ 01 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 \\ 00 & 00 & 01 & 00 \end{bmatrix} \bullet \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \qquad \textbf{(3.45)}$$

De igual forma que en el caso de los polinomios de grado menor que siete, que representaban a los bits de un byte, si aplicamos repetidamente esta multiplicación conseguiremos una manera rápida y sencilla de multiplicar un polinomio por cualquier potencia de x **[5]**.

3.3 Micro AES.

Como una primera vista al algoritmo AES veamos esta versión reducida que designamos Micro-AES, tiene la similar estructura que AES, y nos servirá para poder entender enseguida con mayor facilidad la descripción completa de AES.

El algoritmo Micro-AES trabaja sobre un texto de 16 bits y crea un texto cifrado de 16 bits, con una clave de 16 bits. Micro-AES consiste en dos procedimientos, el de cifrado dónde se aplican 4 funciones básicas tantas veces como se desee y el proceso de la derivación de las subclaves denominado programa de claves, la idea de hacer una versión simplificada ha sido usada como un primer vistazo al algoritmo AES, pero también un estilo de cripto análizarlo, es decir, una intentar un ataque en la versión simplificada para después extenderlo a la versión completa. De manera gráfica Micro-AES puede mostrarse en la **Fig. 3.3.**

Se observa que el algoritmo Micro-AES consiste de 8 aplicaciones de funciones, de las cuales son efectivamente 4, SubByte, ShiftRow, MixCol, y AddKey, dónde se aplican casi dos veces, excluyendo en la segunda ronda a MixCol, y adicionando una aplicación más de AddKey antes de la primera ronda, con la subclave K_0. Esto se comprueba en el proceso de descifrado.

Entonces la descripción de Micro-AES consiste en la descripción de las 4 funciones básicas, con el programa de claves que nos generara K_0, K_1, K_2 a partir de la clave inicial K.

Todas las funciones se aplican como ya se dijo a un plain texto de 16 bits que puede ser visto como un arreglo de 4 medios-bytes, donde cada medio-byte consiste de 4 bits cada uno. La variable a la que se aplican las anteriores funciones es la entrada de 16 bits ($b_0b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}b_{13}b_{14}b_{15}$), que estará dividida en 4 partes $P_0P_1P_2P_3$ de 4 bits cada una, conocida como estado P y toma la siguiente forma matricial:

Donde cada conjunto de 4 bits (½ byte) se le asigna el polinomio $b_0 + b_1x + b_2x^2 + b_3x^3$ elemento de GF(16) = GF(2)[x]/($x^4 + x + 1$) **[5]**.

De la misma forma la clave inicial K consiste de 16 bits y se representa por la matriz siguiente:

P_0	P_2
P_1	P_3

=

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_4b_5b_6b_7$	$b_{12}b_{13}b_{14}b_{15}$

(3.46)

K_0	K_2
K_1	K_3

(3.47)

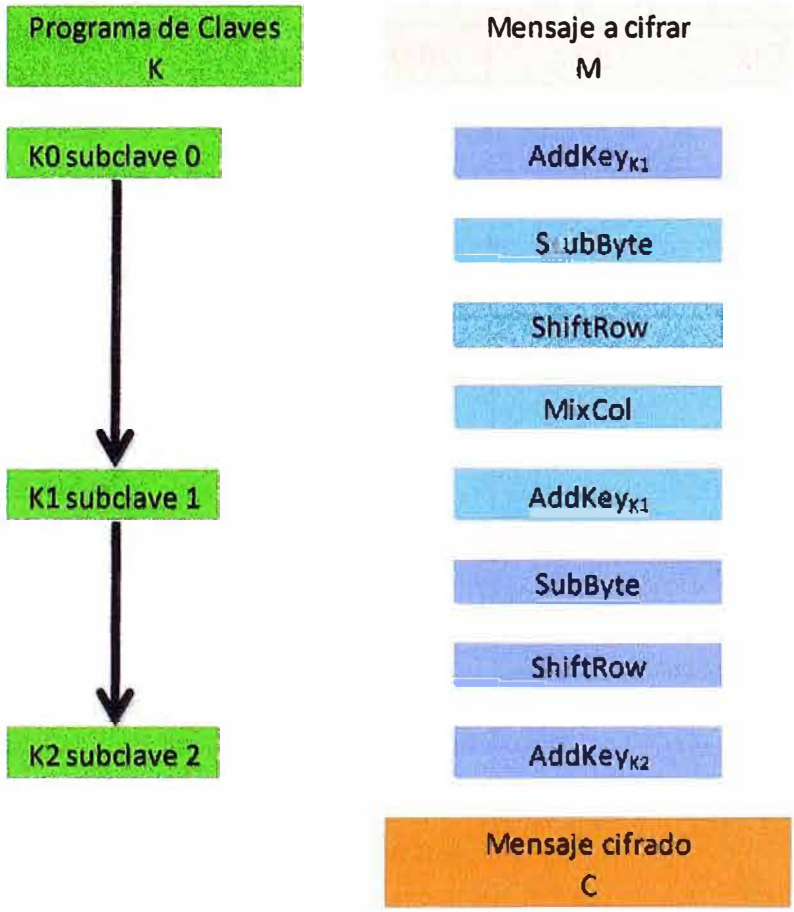

Fig. 3.3 Algoritmo Micro AES

3.3.1 SubByte

Esta función substituye cada ½-byte de 4 bits, por otro ½-byte según la Sbox de la siguiente manera:

La S-Box se obtiene por dos etapas, la primera es considerando cada ½-byte como elemento del campo finito GF(16) = GF(2)[x]/($x^4 + x + 1$) , es decir un campo de 16 elementos. Entonces se le asigna a cada elemento su inverso multiplicativo (al 0000 se le asigna el mismo 0000).

El segundo paso es aplicar un mapeo lineal que tiene la siguiente forma:

Si tenemos como salida de la inversión al ½-byte $b_0b_1b_2b_3$ se le asigna el polinomio $N(x) = b_3 x^3 + b_2 x^2 + b_1 x + b_0$, y considere los polinomios constantes $a(x) = x^3 + x^2 + 1$, y $b(x) = x^3 + 1$ en $GF(2)[x] / (x^4 + 1)$.

Entonces el segundo paso es:

$$N(x) \rightarrow a(x)\, N(x) + b(x) \text{ módulo } x^4 + 1 \qquad \textbf{(3.48)}$$

Los resultados de estos dos pasos los tenemos en la siguiente **TABLA 3.1**:

TABLA 3.1 Resultado de SubByte

x^i	$x^i \bmod (x^4 + x + 1)$	Bits	$(x^i)^{-1}$	$((x^3 + x^2 + 1)(x^i)^{-1} + (x^3+1)) \bmod (x^4+1)$
x	x	0010	1001	1010
x^2	x^2	0100	1101	1101
x^3	x^3	1000	1111	0110
x^4	x+1	0011	1110	1011
x^5	$x^2 + x$	0110	0111	1000
x^6	$x^3 + x^2$	1100	1010	1100
x^7	$x^3 + x + 1$	1011	0101	0011
x^8	$x^2 + 1$	0101	1011	0001
x^9	$x^3 + x$	1010	1000	0111
x^{10}	$x^2 + x + 1$	0111	0110	0101
x^{11}	$x^3 + x^2 + x$	1110	0011	1111
x^{12}	$x^3 + x^2 + x + 1$	1111	1000	0111
x^{13}	$x^3 + x^2 + 1$	1101	0100	1110
x^{14}	$x^3 + 1$	1001	0010	0010
x^{15}	1	0001	0001	0100

Obviamente el elemento 0000 tiene como correspondencia el elemento 1001.

Si queremos ver a la aplicación N(x)a(x)N(x) b(x) módulo x^4+1 de manera matricial, veamos primero la representación del producto de dos polinomios.

$$\begin{aligned} a(x)\, n(x) &= (a_0 + a_1 x + a_2 x^2 + a_3 x^3)(n_0 + n_1 x + n_2 x^2 + n_3 x^3) \\ &= a_0 n_0 + (a_1 n_0 + a_0 n_1) x + (a_2 n_0 + a_1 n_1 + a_0 n_2) x^2 \\ &\quad + (a_3 n_0 + a_2 n_1 + a_1 n_2 + a_0 n_3) x^3 \end{aligned} \qquad \textbf{(3.49)}$$

$$+ (a_3n_1 + a_2n_2 + a_1n_3)\, x^4$$
$$+ (a_3n_2 + a_2n_3)\, x^5 + a_3n_3x^6$$

Si ahora aplicamos el módulo $x^4 + 1$

$$\begin{aligned}(x)\, n(x) = {} & (a_0n_0 + a_3n_1 + a_2n_2) \\ & + (a_1n_0 + a_0n_1 + a_3n_2 + a_2n_3)\, x \\ & + (a_2n_0 + a_1n_1 + a_0n_2 + a_3n_3)\, x^2 \\ & + (a_3n_0 + a_2n_1 + a_1n_2 + a_0n_3)\, x^3 \\ & = d_0 + d_1x + d_2x^2 + d_3x^3\end{aligned} \qquad \textbf{(3.50)}$$

Que en forma matricial queda como:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \bullet \begin{bmatrix} n_0 \\ n_1 \\ n_2 \\ n_3 \end{bmatrix} \qquad \textbf{(3.51)}$$

Entonces la aplicación L(x) = a(x)N(x)+c(x) módulo $x^4 + 1$ la podemos representar como:

$$\begin{bmatrix} l_0 \\ l_1 \\ l_2 \\ l_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} n_0 \\ n_1 \\ n_2 \\ n_3 \end{bmatrix} + \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \qquad \textbf{(3.52)}$$

Por ejemplo 0101 → 0011

0011 $x^3 + x^2 + 1$ 0101 $x^3 + 1$

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \textbf{(3.53)}$$

Otro ejemplo 0011 → 1111

1111 $x^3 + x^2 + 1$ 0011 $x^3 + 1$

$$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \textbf{(3.54)}$$

En términos de aplicación la variable estado de componentes ½-bytes la función SubBytes se ve como:

P_0	P_2	→	$S(P_0)$	$S(P_2)$
P_1	P_3		$S(P_1)$	$S(P_3)$

(3.55)

o

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_4b_5b_6b_7$	$b_{12}b_{13}b_{14}b_{15}$

→

S - box($b_0b_1b_2b_3$)	S - box($b_8b_9b_{10}b_{11}$)
S - box($b_4b_5b_6b_7$)	S - box($b_{12}b_{13}b_{14}b_{15}$)

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_4b_5b_6b_7$	$b_{12}b_{13}b_{14}b_{15}$

→

S - box($b_0b_1b_2b_3$)	S - box($b_8b_9b_{10}b_{11}$)
S - box($b_4b_5b_6b_7$)	S - box($b_{12}b_{13}b_{14}b_{15}$)

(3.56)

Resumiendo como:

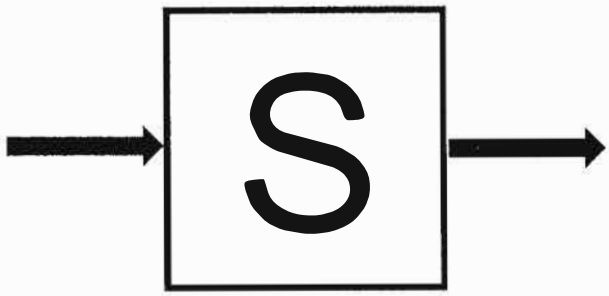

Fig. 3.4 SubByte

3.3.2 ShiftRow

Esta aplicación es muy sencilla y solo aplica un shift a la segunda fila de la matriz estado, de la siguiente manera:

P_0	P_2
P_1	P_3

→

P_0	P_2
P_1	P_3

(3.57)

O en representación de bits:

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_4b_5b_6b_7$	$b_{12}b_{13}b_{14}b_{15}$

→

$b_0b_1b_2b_3$	$b_8b_9b_{10}b_{11}$
$b_{12}b_{13}b_{14}b_{15}$	$b_4b_5b_6b_7$

(3.58)

Y que abreviamos gráficamente como:

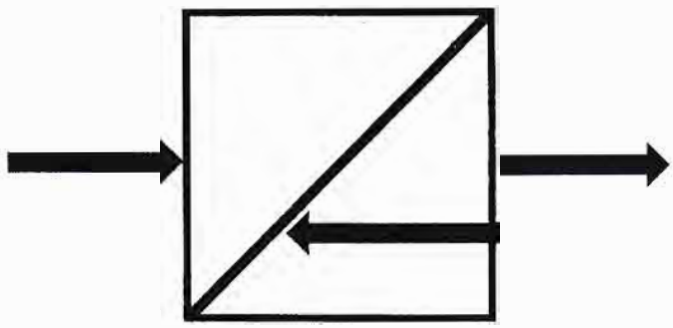

Fig. 3.5 ShiftRow

3.3.3 MixCol

La función MixCol se aplica a cada columna, las columnas aparece como un elemento de $GF(2^4)[x]/(x^2 + 1)$, es decir como polinomio de grado 1 con coeficientes en el campo $GF(2^4)[x]$ (polinomios de grado 3). Es decir son elementos de la forma $(a_0 + a_1x)GF(2^4)[x]/(x^2 + 1)$ donde a_1, a_2 $GF(2^4)$.

La función MixCol multiplica a cada columna del estado por un polinomio constante $c(x)=3+2x$ de $GF(2^4)[x]$ $/(x^2 +1)$. Para observar más explícitamente la aplicación de MixCol primero veamos qué forma tiene el producto de dos polinomios en $GF(2^4)[x]$ $/(x^2 +1)$.

Si $(a_0 + a_1x)$, $(b_0 + b_1x)$ son dos polinomios, entonces $(a_0 + a_1x).(b_0 + b_1x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_1b_1)x^2$

Como $x^2 + 1 = 0$, tenemos que:

$$(a_0 + a_1x).(b_0 + b_1x) = (a_0b_0 + a_1b_1) + (a_0b_1 + a_1b_0)x = c_0 + c_1x \quad \textbf{(3.59)}$$

En la forma matricial se ve como:

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} a_0 & a_1 \\ a_1 & a_0 \end{bmatrix} \bullet \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \quad \textbf{(3.60)}$$

Entonces la función MixCol queda como:

P_0	P_2
P_1	P_3

→

Q_0	Q_2
Q_1	Q_3

(3.61)

Que para cada columna y en forma matricial significa

$$\begin{bmatrix} Q_0 \\ Q_1 \end{bmatrix} = \begin{bmatrix} 0011 & 0010 \\ 0010 & 0011 \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \end{bmatrix} \quad \textbf{(3.62)}$$

$$\begin{bmatrix} Q_2 \\ Q_3 \end{bmatrix} = \begin{bmatrix} 0011 & 0010 \\ 0010 & 0011 \end{bmatrix} \begin{bmatrix} P_2 \\ P_3 \end{bmatrix}$$

Donde 0011=3, y 0010=2 elementos del campo GF(16).

Finalmente lo resumimos como:

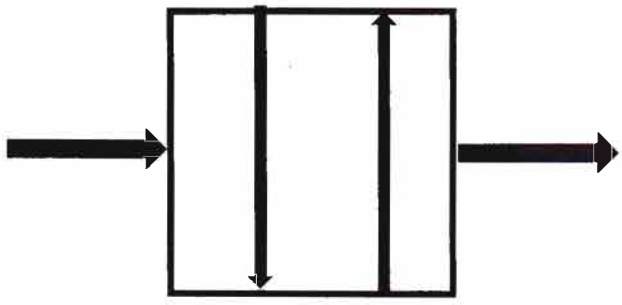

Fig. 3.6 MixCol

3.3.4 AddKey

La función AddKey simplemente efectúa un XOR entrada con entrada del estado con la clave correspondiente.

$$\begin{array}{|c|c|}\hline P_0 & P_2 \\ \hline P_1 & P_3 \\ \hline\end{array} \oplus \begin{array}{|c|c|}\hline K_0 & K_2 \\ \hline K_1 & K_3 \\ \hline\end{array} = \begin{array}{|c|c|}\hline P_0 \oplus K_0 & P_2 \oplus K_2 \\ \hline P_1 \oplus K_3 & P_3 \oplus K_3 \\ \hline\end{array} \qquad \textbf{(3.63)}$$

Lo simplificamos como:

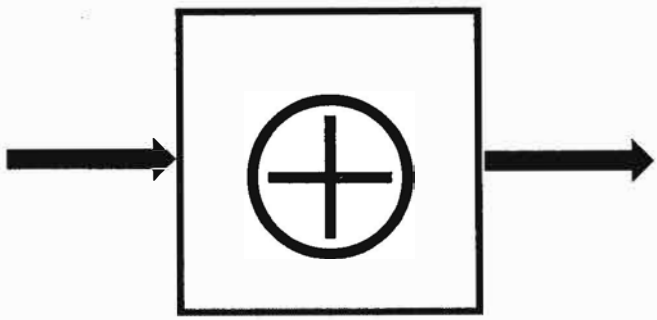

Fig. 3.7 AddKey

Programas de claves

En esta sección se justificara cómo se obtiene las claves K_0, K_1, y K_2 a partir de K. El programa de claves consiste en alcanzar el arreglo W[ ], de 6 bytes, donde W[0],W[1] son los dos bytes de la clave $K=K_0$, para obtener K_1, y K_2 se extiende el arreglo W a los bytes W[2],W[3],W[4], y W[5]. Donde K_1=W[2]W[3], y K_2=W[4]W[5].

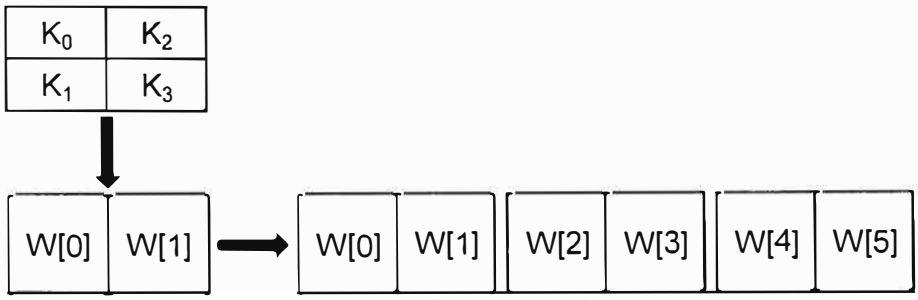

Fig. 3.8 Programa de claves

Por lo tanto es bastante saber cómo se elaboran las extensiones de W[2],W[3],W[4],W[5] a partir de W[0],W[1].

Para la extensión de W primero determinemos los siguientes elementos:

Sea RC[i] = x i+2 GF(24) , N0 N1 es la concatenación de dos ½-bytes, entonces sea RCON[i] = RC[i]0000 es un byte, y Rot(N0N1) = N1N0 , así como Sub(N0N1) = S – Box(N0)S – Box(N1).

W[0] = K (11110000)

W[1] = K (00001111)

W[2] = W[0] RCON[1] Sub(Rot(W[1]))

W[3] = W[1] W[2]

W[4] = W[2]RCON[2]Sub(Rot(W[3]))

W[5] = W[3] W[4]

Definitivamente la descripción final gráfica de Baby-AES queda de la siguiente forma:

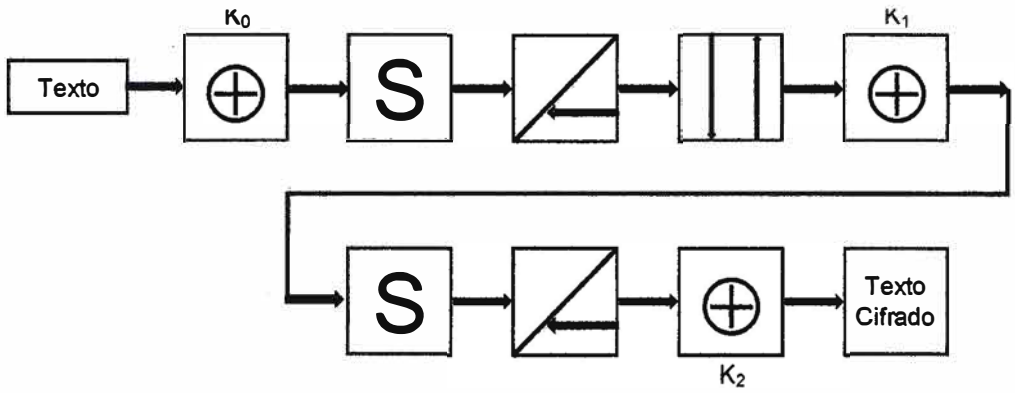

Fig. 3.9 Descripción final **[6]**

3.4 Análisis teórico de AES

Como se explicó anteriormente, dependiendo del tamaño de la clave el algoritmo de encriptamiento toma un mayor tiempo para procesar la información. En la **Fig. 3.10** se muestra una comparación de los tiempos de procesamiento versus la cantidad de datos en bytes, como se observa el algoritmo AES128 es el más rápido y aunque la clave es más corta y por lo tanto menos seguro que los algoritmos AES192 y AES256, este

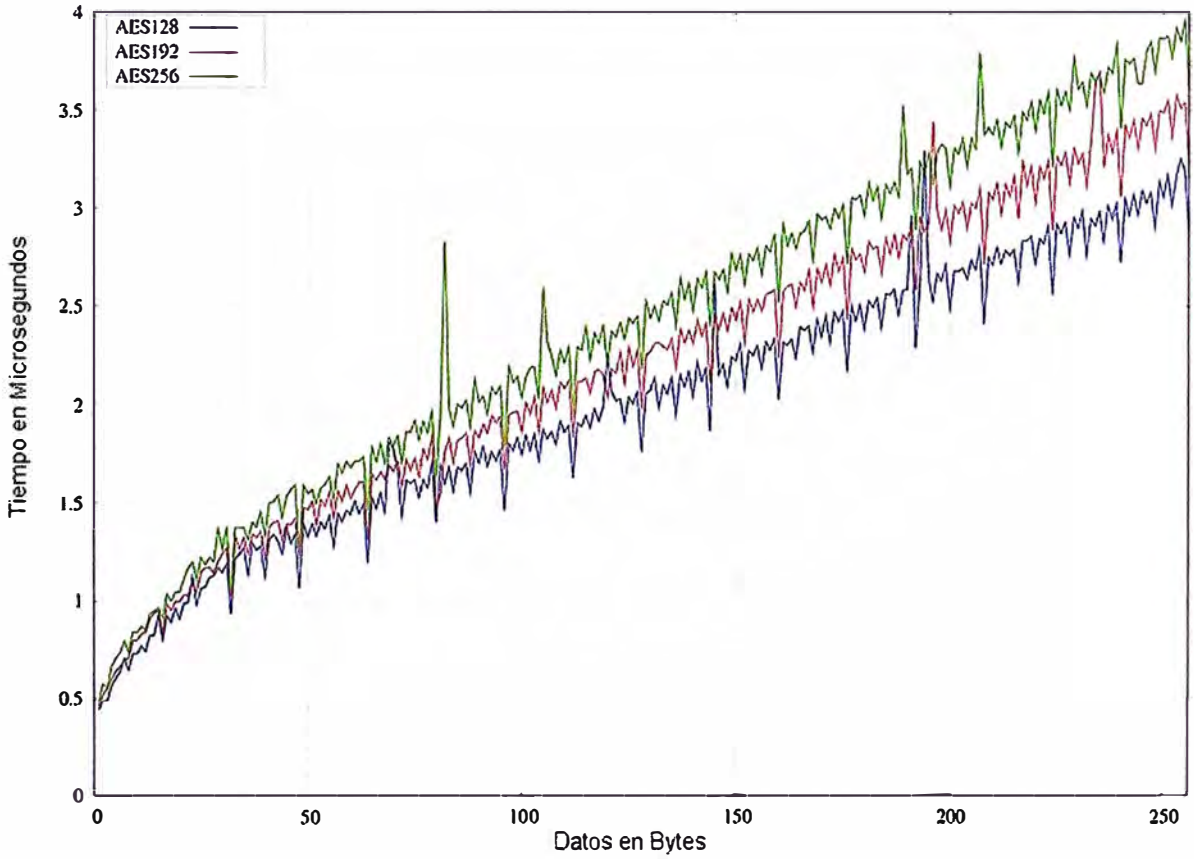

Fig. 3.10 AES128 vs AES192 vs AES256

tamaño de clave se recomienda para las implementaciones. Para el estudio de caso presentado en este trabajo, el algoritmo de encriptamiento empleado es el AES128.

3.5 Comparación de AES con otros algoritmos de Cifrado

En la **Fig. 3.10** nos muestra un gráfico de la velocidad de procesamiento en Mbytes/seg versus vs la cantidad de datos ingresados expresado en bytes, estos resultados se han obtenido aplicando los diferentes métodos de cifrado a un mismo bloque de datos, y ejecutados en un misma máquina, los métodos de cifrado mencionado en la **Fig. 3.11** son los que participaron en el concurso AES, dos de los cuales son los más utilizados por los fabricantes, estos son Rijndael y 3DES, encontrándose que el Rijndael puede procesar la misma cantidad de información en menos tiempo, por tal motivo Rijndael es el algoritmo recomendado para nuestras implementaciones.

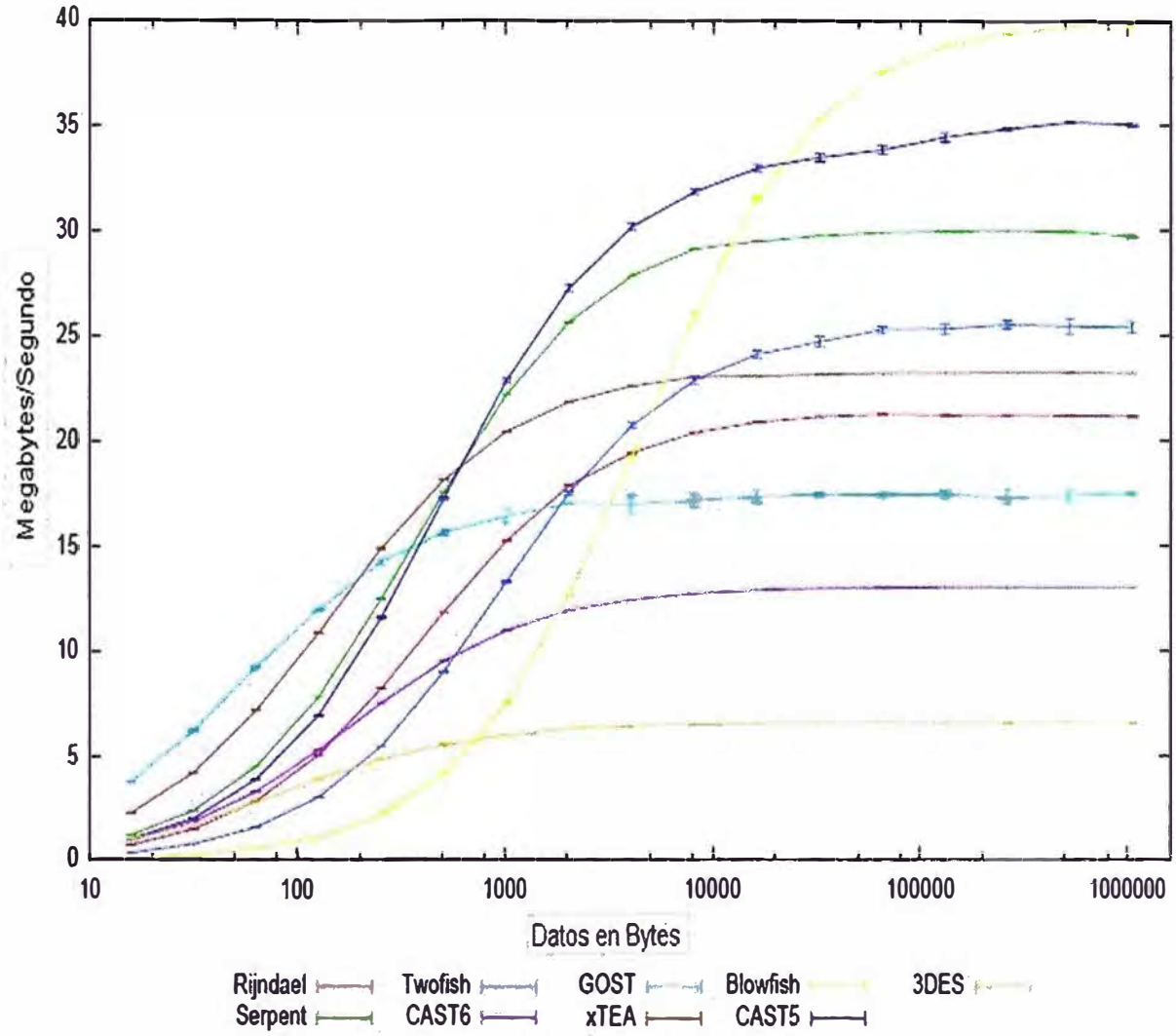

Fig.3.11 Comparación métodos de cifrado

Capítulo IV
PLANTEAMIENTO Y APLICACIÓN DE INGENIERIA DEL PROBLEMA

4.1 Descripción del Problema

San Jerónimo de Surco es una localidad a 30 Km de Chosica, la cual cuenta con todo los servicios básicos. A una distancia de 2 Km se encuentra la comunidad de Huaquicha, el cual cuenta únicamente con el servicio de electrificación.

La comunidad de Huaquicha cuenta con una escuela de Educación Primaria, que alberga a 100 estudiantes aproximadamente, proveniente de comunidades cercanas.

La comunidad de Huaquicha es la localidad más cercana a San Jerónimo de Surco, y no hay ningún tipo de medio de comunicación, cuyo único medio de conexión a San Jerónimo de Surco es un camino improvisado, construido por los habitantes de la comunidad.

La implementación de un sistema de comunicación, seria de una enorme contribución a la comunidad, lo cual contaría con los básicos sistemas de comunicación, el cual cuenta cualquier ciudad.

Fig. 4.1 Ubicación de San Jerónimo y Huaquicha

4.1.1 Posibles soluciones

Existen muchas técnicas para implementar y brindar una solución al problema planteado de comunicación, de las cuales mencionamos:

a) Enlace Satelital.

El enlace satelital es una medio de conexión utilizada en su mayoría en lugares muy inhóspitos o alejados, esta solución es mayormente empleado en zonas petroleras, minas cuya lugar geográficos es casi inaccesible.

La implementación de un enlace satelital básicamente consta de un transmisor en la estación terrena dirigida hacia el satélite que esta a su vez lo retransmite hacia algún proveedor **[7]**.

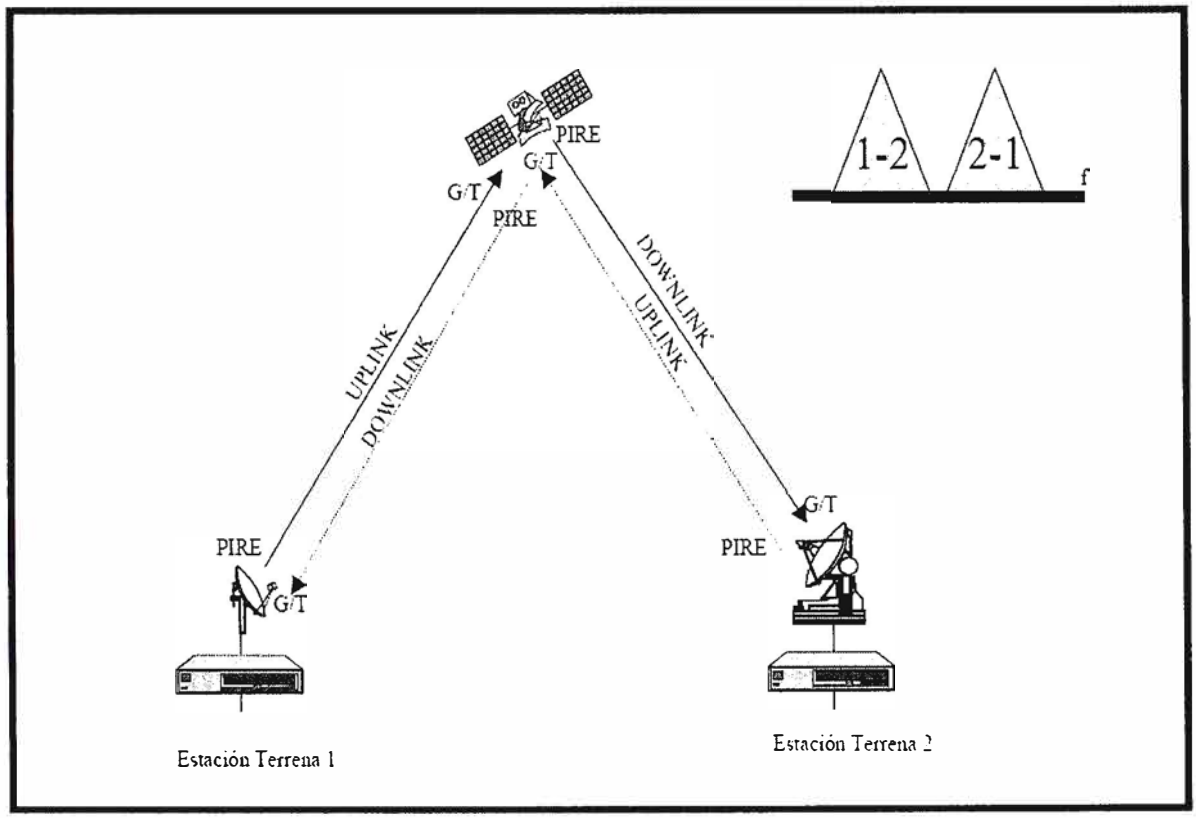

Fig. 4.2 Enlace satelital

Empresas que brinda servicio de voz:

-BIG LEO: IRIDIUM (66 satélites a 900 Km)

-GLOBALSTAR (48 satélites 1400km)

-GEO: INMARSAT (Mini-M)

Empresa que brinda servicio de datos:

-LITTLE LEO: ORBCOM (messaging) 26 satélites a 785km (24 en órbita inclinada cada plano a 45º con 8 satélites cada uno y 2 en órbita polar).

-BIG LEO: TELEDESIC (700Km) en desarrollo. Red ATM satelital.

-GEO: Sistemas en desarrollo en la banda Ka (trabajarán en anillo)

-MEO: GPS (21 satélites a 20.000km aproximadamente)

Ventajas y desventajas del enlace satelital

-Ventajas

Tiene mayor cobertura en comparación a otros medios de transmisión.

Es fácil y rápida su implementación.

Es portátil

-Desventajas

Menor ancho de banda

Su implementación y mantenimiento es relativamente costoso.

b) Red de fibra óptica

Las redes de fibra óptica se emplean cada vez más en telecomunicación, debido a que las ondas de luz tienen una frecuencia alta y la capacidad de una señal para transportar información aumenta con la frecuencia.

En las redes de comunicaciones por fibra óptica se emplean sistemas de emisión láser. Aunque en los primeros tiempos de la fibra óptica se utilizaron también emisores LED, en el 2007 están prácticamente en desuso.

Aplicaciones

LAN de fibra son ampliamente utilizadas para comunicación a larga distancia, proporcionando conexiones transcontinentales y transoceánicas, ya que una ventaja de los sistemas de fibra óptica es la gran distancia que puede recorrer una señal antes de necesitar un repetidor o regenerador para recuperar su intensidad. En la actualidad, los repetidores de los sistemas de transmisión por fibra óptica están separados entre sí unos 100 km, frente a aproximadamente 1,5 km en los sistemas eléctricos. Los amplificadores ópticos recientemente desarrollados pueden aumentar todavía más esta distancia.

En resumen las redes de fibra óptica son un modelo de red desarrollado para satisfacer las necesidades crecientes de capacidad de transmisión y seguridad, con la mayor economía posible. Los avances en la purificación de la fibra óptica y el concepto de multiplexación por división de longitud de onda (WDM) hicieron que la fibra óptica fuese ideal para hacer redes de comunicación.

Entre las redes existentes de fibra óptica existen:

Redes FDDI

Redes 10 base F

Fast Ethernet 100 base FX

Gigabit Ethernet 1000 base FX y 1000 base LX

Redes de alta velocidad SDH/Sonet

Redes HFC

-Ventajas

La fibra óptica hace posible navegar por Internet a una velocidad de dos millones de bps.
Acceso ilimitado y continuo las 24 horas del día, sin congestiones.
Video y sonido en tiempo real.
Fácil de instalar.
Es inmune al ruido y las interferencias, como ocurre cuando un alambre telefónico pierde parte de su señal a otra.
Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.
Carencia de señales eléctricas en la fibra, por lo que no pueden dar sacudidas ni otros peligros. Son convenientes para trabajar en ambientes explosivos.
Presenta dimensiones más reducidas que los medios preexistentes.
El peso del cable de fibras ópticas es muy inferior al de los cables metálicos, capaz de llevar un gran número de señales.
La materia prima para fabricarla es abundante en la naturaleza.
Compatibilidad con la tecnología digital.

-Desventajas

Sólo pueden suscribirse las personas que viven en las zonas de la ciudad por las cuales ya esté instalada la red de fibra óptica.
El costo es alto en la conexión de fibra óptica, las empresas no cobran por tiempo de utilización sino por cantidad de información transferida al computador, que se mide en megabytes.
El costo de instalación es elevado.
Fragilidad de las fibras.
Disponibilidad limitada de conectores.
Dificultad de reparar un cable de fibras roto en el campo.

c) Enlaces inalámbricos

Una red inalámbrica es como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable.

Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar porta cables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

Por el otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un hacker puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

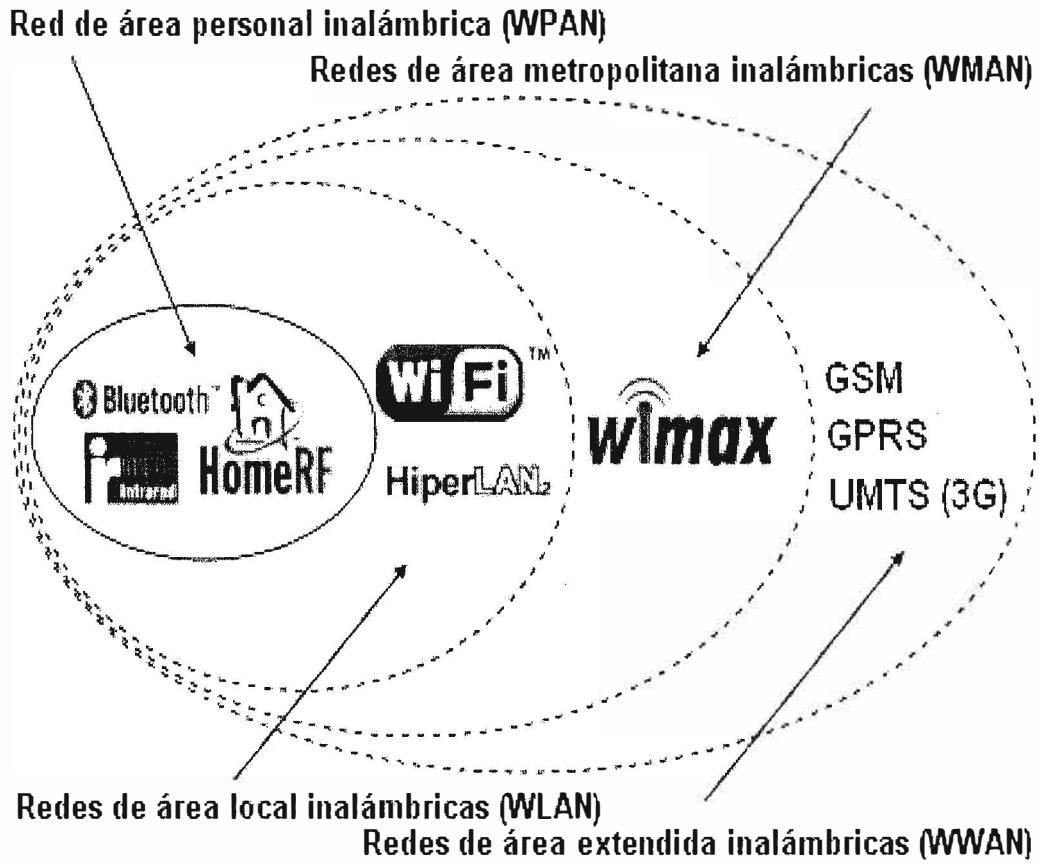

Fig. 4.3 Enlaces inalámbricos

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (denominada área de cobertura**[8]**.

4.1.2 Mejor alternativa para realizar el enlace

Por ser una zona con una densidad poblacional muy baja, el flujo de información no sería muy elevado, por consiguiente habría la necesidad de contar con una red que no sea muy costosa y que cuente con un ancho de banda aceptable. Por tales motivos y por las opciones mencionadas en el **Capítulo 1.2** se optaría por un enlace inalámbrico basándonos en la tecnología WIMAX cuyas características son:

Es una tecnología muy utilizada para enlace punto a punto por ser un enlace confiable.

El tiempo de implementación es rápido.

El costo de los equipos no es caro.

La tecnología cuenta con seguridad basada en encriptaciones actuales y robustas.

Cuenta con ancho de banda de 108Mbps a más.

Es verdad que la red de fibra óptica es la mejor opción, pero el costo y el tiempo de implementación son elevados, se podría proyectar dicha solución a largo plazo.

4.2 Estudio de la zona del Enlace

Se realizó el estudio en la zona, para corroborar si las condiciones geográficas son óptimas para realizar el enlace punto a punto desde el pueblo de San Jerónimo de Surco con la comunidad de Huaquicha. Como se aprecia en la **Fig. 4.4**, las comunidades se encuentran distanciadas por un tramo de 2 Km.

Fig. 4.4 Vista superior de San Jerónimo de Surco y Huaquicha

Se realizó el estudio del perfil de la zona, para observar si contaba con línea de vista en ambas localidades y se obtuvo el siguiente resultado:

-San Jerónimo de Surco se encuentra a 2067mts. sobre el nivel de mar.

-Huaquicha se encuentra a 2638 mts. sobre el nivel del mar.

Se observa en la **Fig. 4.5** que existiría una obstrucción geográfica a una distancia de 0.75 Km entre el pueblo de San Jerónimo de Surco hacia Huaquiche.

Fig. 4.5 Perfil del recorrido del enlace de San Jerónimo a hacia Huaquiche

4.3 Simulación del enlace

Utilizando como herramienta el software radio mobile, realizamos una simulación de enlace entre las comunidades San Jerónimo de Surco hacia Huaquiche, con las siguientes condiciones:

Equipo transmisión y receptor de 500 mwatts.

Antenas directivas de ganancia de 24 dbi

Torres con la siguiente distribución:

-San Jerónimo de Surco: torre de 15 mts.

-Huaquiche: torre de 18 mts.

Con todos estos datos calculados por con el software radio mobile nos garantizó un enlace sólido y una óptima señal para los puntos definidos.

-Se obtuvo un enlace sólido. **Fig. 4.6**

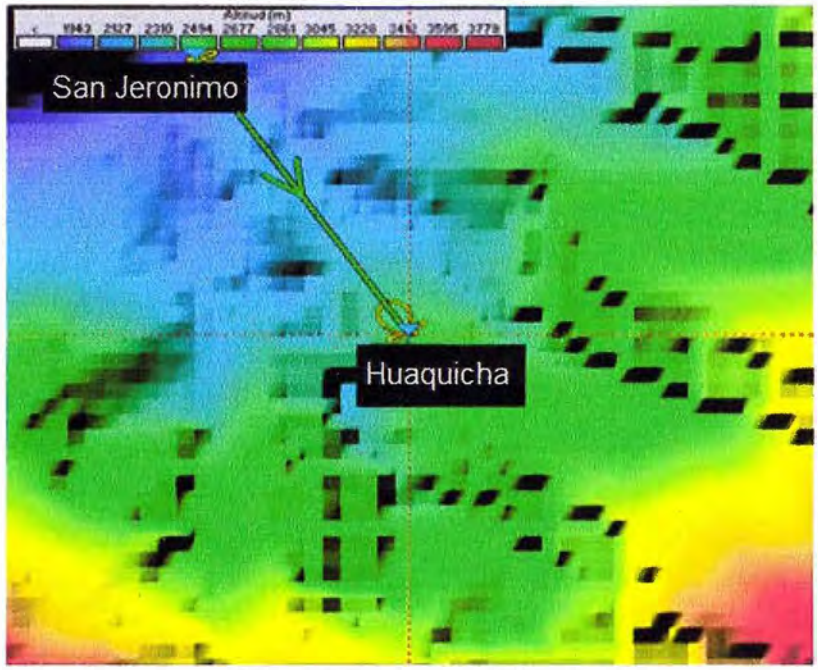

Fig. 4.6 Diagrama del Enlace

Se lograra un enlace cuya señal promedio seria de 64 db. **Fig. 4.7**

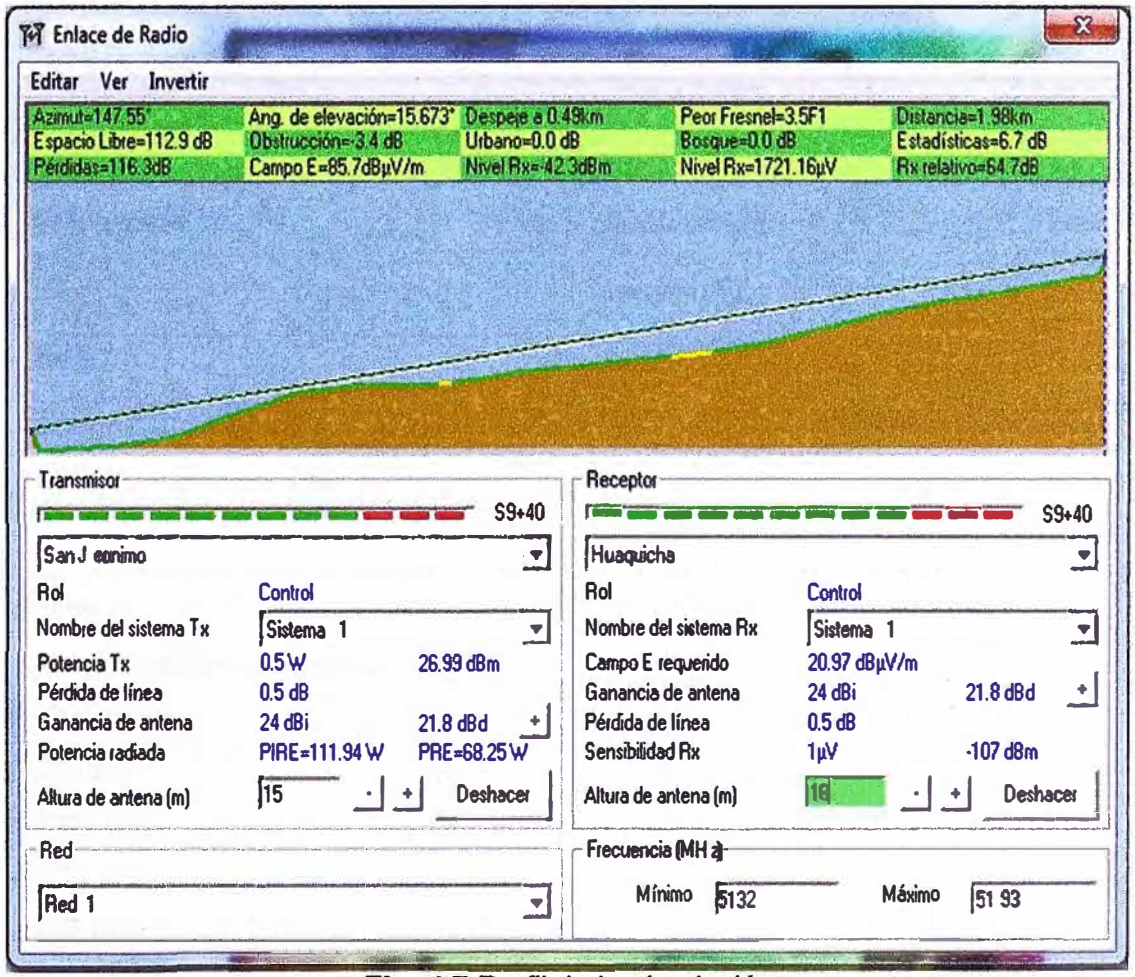

Fig. 4.7 Perfil de la simulación

Con el montaje de las torres se lograría una mejor línea de vista entre ambas comunidades. **Fig. 4.8**

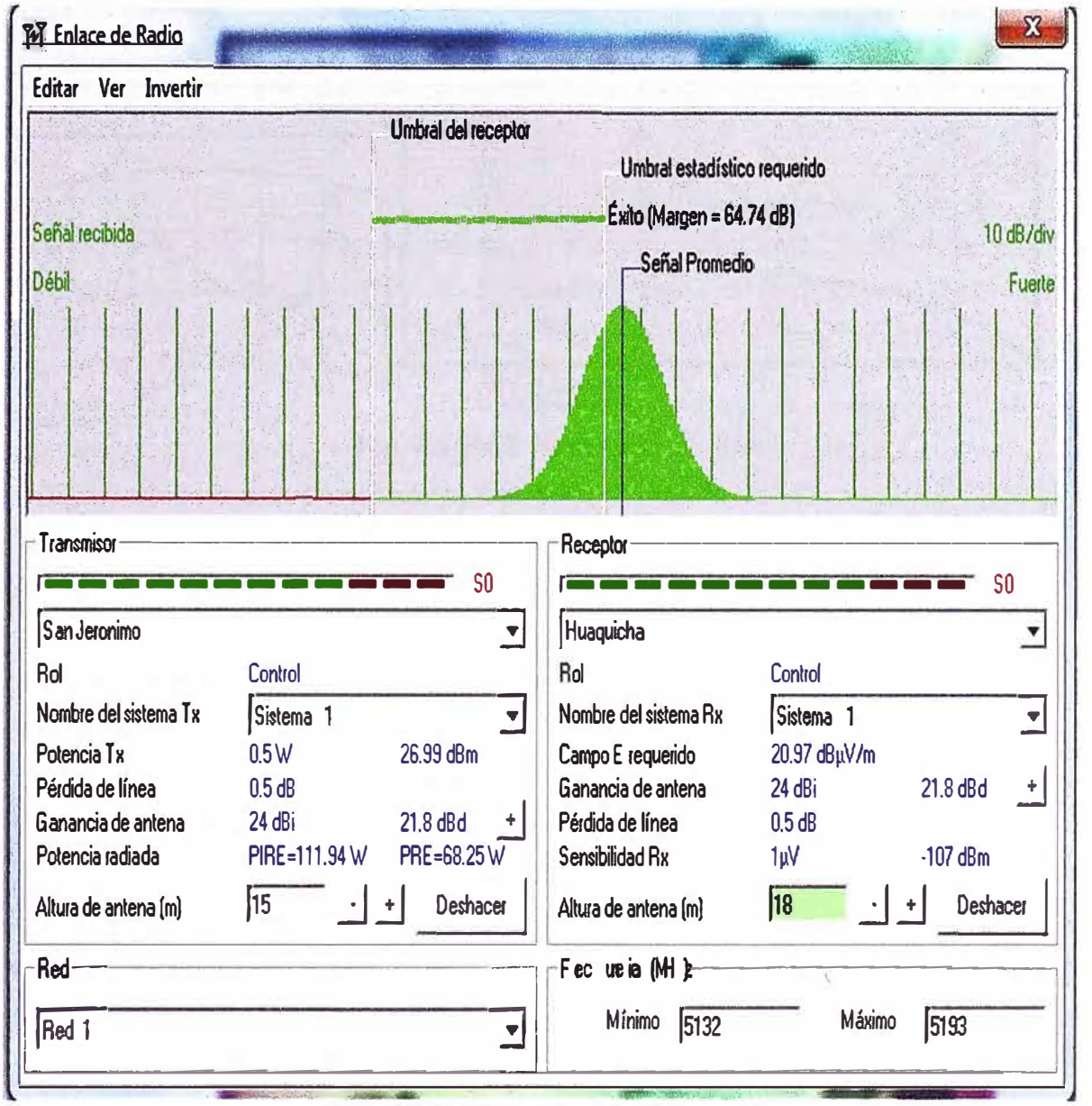

Fig. 4.8 Grafica del umbral promedio

4.4 Cálculo matemático para hallar las alturas de las antenas

Ahora realizaremos los cálculos para hallar las alturas de las antenas en las 2 localidades.

4.4.1 Condiciones del enlace:

D_1=0,75Km.

D_2=1.32Km.

Ha= 2067 mts.

Hb=2638 mts.

H= 2250 mts.

K=4/3 (coeficiente de curvatura de la tierra)

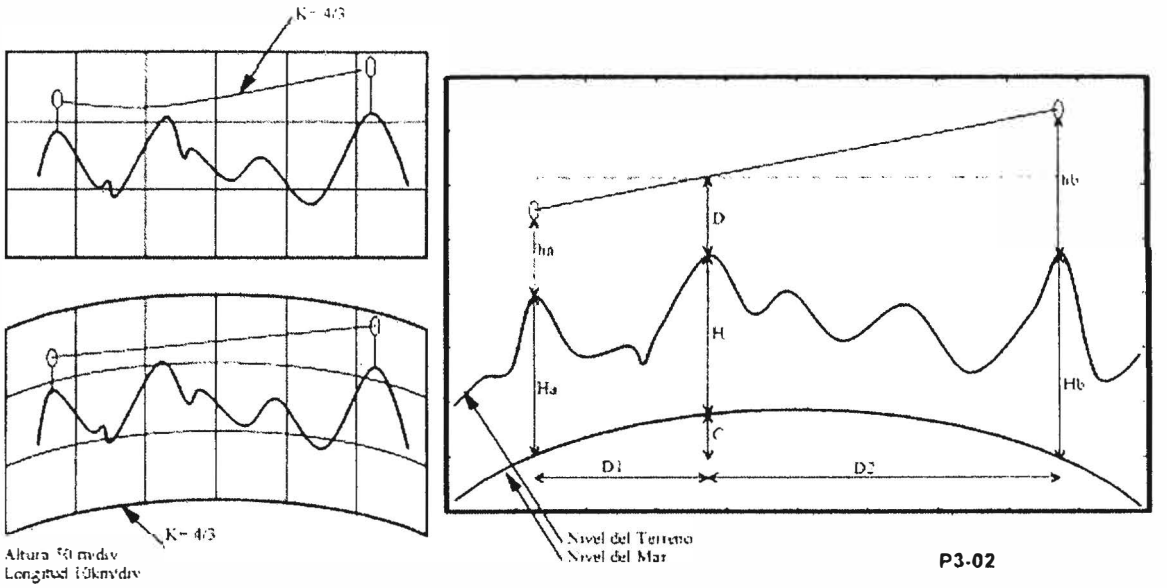

Fig. 4.9 Perfil de la zona de enlace

4.4.2 Cálculo de la curvatura C de la Tierra

$$C = 4(D1*D2)/(51*K) = 4(0,75*1,32)/(51*1,333) = 0,058 \text{ m} \quad \textbf{(4.1)}$$

Por ser una distancia corta (2,07 km) el valor de C es casi imperceptible.

4.4.3 Criterios para determinar la altura de antenas

• **H1=** Ha+ha altura del terreno sobre el nivel del mar más la altura de la antena en la estación A.

$$\textbf{H1=} \ 2067\text{mts} + ha \quad \textbf{(4.2)}$$

• **H2=** Hb+hb corresponde a la misma definición en la estación B.

$$\textbf{H2=} \ 2638 + hb \quad \textbf{(4.3)}$$

• **H3=** C+H+D altura del rayo en el obstáculo constituido por la curvatura del terreno más la altura del obstáculo sobre el nivel del mar, más un despegamiento adicional por difracción.

$$\textbf{H3=} \ 0,058 \text{ m} + 2250 \text{ m} + 39,912 \text{ m} = 2289,97 \text{ m} \quad \textbf{(4.4)}$$

• **D1, D2** son las longitudes desde las estaciones A y B hasta el obstáculo.

$$(H3-H1).d2 = (H2-H3).D1 \quad \textbf{(4.5)}$$

$$(2289,97 - 2067 - ha).1,32 = (2638 + hb - 2289,97).0,75 \quad \textbf{(4.6)}$$

$$294,3204 - 1,32ha = 261.0225 + 0,75hb \quad \textbf{(4.7)}$$

$$33.2979 - 1,32ha = 0,75hb \quad \textbf{(4.8)}$$

TABLA 4.1 Posibles valores de altura de las antenas

Hb	Ha
3	23,53
5	22,38
10	19.54

16,70	15
15	**18**
12,72	22
10.45	26
-3.18	50

4.4.4 Comparación de la simulación de enlace con el cálculo matemático.

Como se puede apreciar en la simulación **Capitulo 4.3** las alturas de las torres que se asumieron para obtener una línea de vista coincide con los cálculos matemáticos, por consiguiente los valores que se obtiene en la simulación del enlace serán aceptables para nuestra implementación **[10]**.

4.5 Implementación del enlace

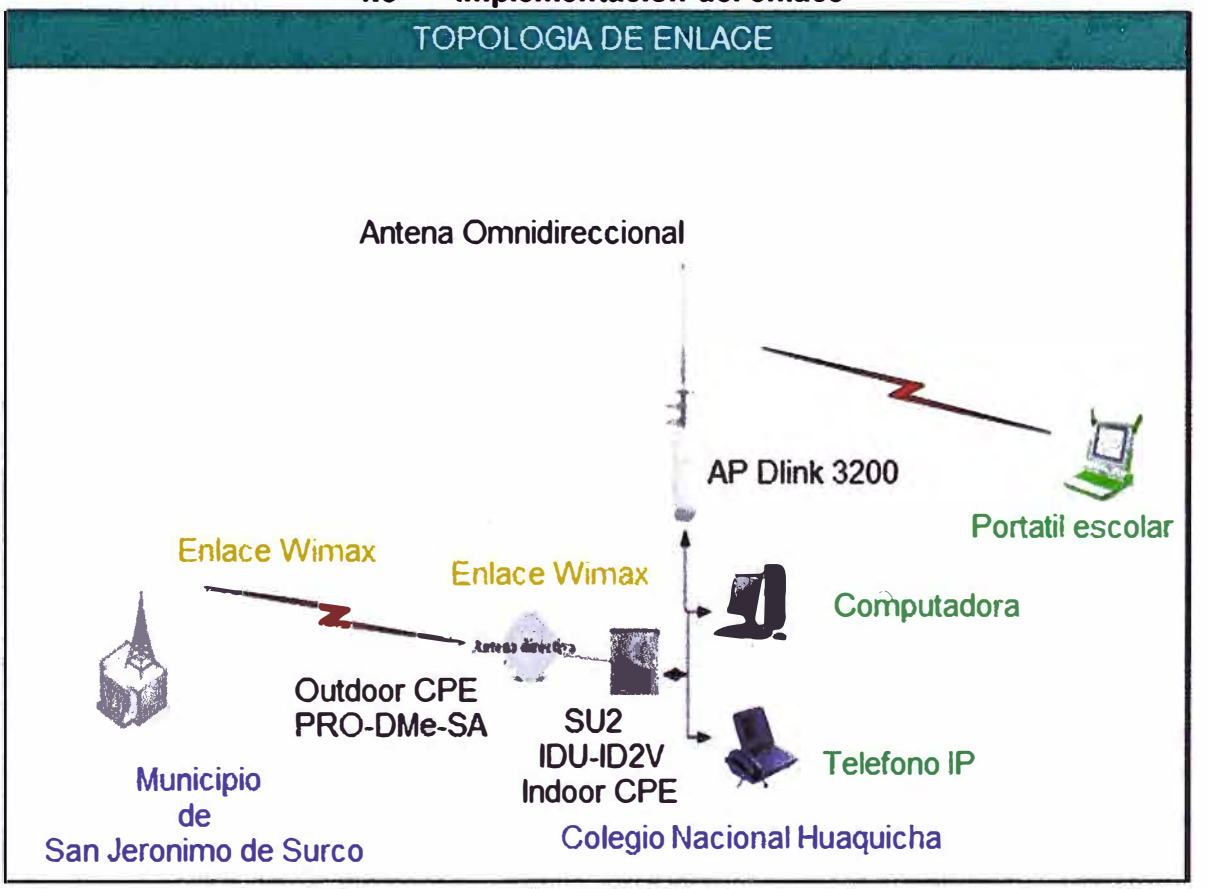

Fig.4.10 Diagrama de Enlace

4.6 Enlace y distribución a realizar

El enlace a realizar entre la estación Base (San Jerónimo) y la estación terminal (Huaquicha) es WiMAX y para la distribución nos basaremos en WiFi.

4.6.1 Enlace WiMAX

a) Terminal WiMAX de emplazamiento fijo (IDU-CPE-1D2V SIP-RJ)

El terminal WiMAX IDU-1D2V es un equipo para aplicaciones indoor imaginado para poder brindar a los usuarios una combinación de telefonía IP o VoIP y servicios de datos

de banda ancha. Este terminal dispone de una interfaz Ethernet y dos interfaces POTS para servicios de voz primarios y cuyos tipos de conectores pueden ser: RJ-11 o un terminal block.

El IDU-1D2V o IDU-DV es un gateway de voz y se rige sobre los protocolos estándares H.323 y SIP para el establecimiento de llamadas IP. Soporta codecs de habla estrechos (comprimidos) o anchos (descomprimidos), supresión del silencio, cancelación del eco de línea y parámetros de telefonía regionales. Los servicios de clase 5 tales como llamada en espera, desvío de llamada y llamada a 3 también están soportados.

El VG-1D2V soporta además de telefonía-IP, acceso a Internet o a cualquier otro servicio basado en Ethernet. La unidad puede estar instalada detrás de un router/NAT ya que tiene soporte para NAT57 permitiendo que los paquetes de voz puedan alcanzar al Gate Keeper para inicializaciones de llamadas bidireccionales. El voice gateway puede manejar hasta 16 VLANs simultáneamente permitiendo ofrecer diferentes servicios a usuarios finales que se encuentren conectados detrás del terminal.

Dos unidades IDU-DV pueden ser conectadas en cascada proporcionando de esta manera 4 líneas POTS independientes sobre una sola unidad radio outdoor. El terminal IDUDV puede ser administrado y supervisado remotamente y/o localmente utilizando SNMP o un servidor web integrado.

El terminal WiMAX CPE-IDU-DV soporta el protocolo DRAP que es un protocolo fundamentado en IP/UDP entre el IDU-DV i un servidor DRAP que es suficiente de proporcionar en forma dinámica asignación de recursos (ejemplo: ancho de banda) en realizaciones de llamadas.

Mediante el uso de este protocolo no es necesaria una configuración específica en el IDU-DV ya que el protocolo suministra un mecanismo de autodescubrimiento de forma que el IDUDV puede localizar y registrarse con el servidor DRAP.

El IDU-DV se comunica con la unidad outdoor Breeze MAX PRO-CPE y le suministra potencia (54 VDC) sobre un cable de categoría 5 con conector RJ-45. La unidad ODU contienen un módem, cabezal RF, procesamiento de datos y una antena plana de 17 dBi de ganancia o una conexión a una antena externa, tal y como se describe en la **TABLA 4.3**. El CPE-ODU suministra conexiones sirviendo como una plataforma eficiente para servicios de banda ancha. El ODU proporciona conexión a la estación base, funcionalidad como bridge, clasificación y configuración del tráfico. Esta unidad outdoor puede tener una antena directiva incorporada como es el caso del modelo SA o debe conectarse a una antena externa como es el caso del modelo SE. En el modelo SE, la antena que se ha utilizado es una omniazimutal de 2.5 dBi de ganancia y cuya forma redonda se muestra en la **Fig. 4.12** junto con la unidad outdoor del modelo SA.

Fig. 4.11 Terminal WiMAX indoor IDU-1D2V

Fig. 4.12 Unidad outdoor.PRO-S-CPE, modelos SA y SE.

El CPE-ODU suministra conexiones sirviendo como una plataforma eficiente para servicios de banda ancha. El ODU proporciona conexión a la estación base, funcionalidad como bridge, clasificación y configuración del tráfico. Esta unidad outdoor puede tener una antena directiva incorporada como es el caso del modelo SA o debe conectarse a una antena externa como es el caso del modelo SE. En el modelo SE, la antena que se ha utilizado es una omniazimutal de 2.5 dBi de ganancia y cuya forma redonda se muestra en la **Fig. 4.12** junto con la unidad outdoor del modelo SA.

La **TABLA 4.3** muestra las especificaciones de la unidad outdoor PRO-S-CPE.

TABLA 4.3 Especificaciones radio del terminal WiMAX PRO-S-CPE

Ítem	1.**Descripción**	
Frecuencia	Uplink (MHz)	3399.5 - 3500
	Downlink (MHz)	3499.5 - 3600
Modo de operación	FDD, Halfduplex.	
Ancho de banda de canal	1.75 MHz 3.5 MHz	
Resolución de la frecuencia central	0.125 MHz	
Antena integrada (modelo SA)	17 dBi de ganancia, 20oAZx20oEL, polarización vertical/horizontal	
Puerto de antena (modelo SE)	SMA, 50 Ohm	
Máxima potencia de entrada	20 dBm antes de saturación 0 dBm antes de deterioro	
Rango de potencia de transmisión (al puerto de antena)	[-26 dBm, 20dBm] con 1 dBm de resolución. Potencia de transmisión máxima: 20 dBm +/- 1 dB máximo. Rango dinámico ATPC: 46 dB	
Modulación	Modulación OFDM 256 BPSK, QPSK, QAM16, QAM64	
FEC	Codificación Convolucional 1/2, 2/3, 3/4.	
Throughput bruto downlink/uplink	Máximo: 12 Mbps, con QAM 64 3/4. Mínimo: 1.4 Mbps con BPSK 1/2	

b) Descripción de la estación base WiMAX

BreezeMAX es una tecnología diseñada por la empresa Alvarion fundamentada en el estándar de WiMAX IEEE 802.16/ETSI HIPERMAN para poder ofrecer un gran múltiple de servicios a bajo costo y alta velocidad a través de un medio radiado a un conjunto de

organizaciones clientes (clientes en zonas empresariales, en zonas residenciales, en zonas educativas, etc.) que forman una red wireless de área metropolitana (WMAN). La banda licenciada que ofrecen los equipos BreezeMAX está comprendida en 3-4 GHz. Existen en concreto 3 bandas frecuenciales: 3.3 GHz, 3.5 GHz y 3.6 GHz.

Fig. 4.13 Micro Estación Base BreezeMAX Alvarion

La micro estación base uBST provee toda la funcionalidad necesaria para comunicarse con los SUs o unidades suscritoras y conectarse al backbone del ISP. La µBST soporta full duplex, alta potencia y múltiples portadoras (debido a la modulación multiportadora de OFDM). La µBST ha sido proyectada para proporcionar una alternativa a la estación base modular BreezeMAX y una solución de bajo coste en lugares donde el número de unidades suscritoras está limitado y solo uno o dos sectores son necesarios (i.e: áreas de comunidades).

La estación base modular puede ofrecer hasta siete sectores. La µBST está constituida por la unidad micro estación base indoor y la unidad radio outdoor. La unidad indoor provee toda la funcionalidad necesaria para poder dar servicio a dos sectores. Existen dos modelos: uno que se alimenta de AC (110 o 220 V) y el otro que se alimenta en DC (-48 V). Las funcionalidades de la µBST incluyen:

- Conectividad Ethernet al backbone a través de una interfaz de red 100BASE –T.
- Clasificación del tráfico e iniciación de establecimiento de conexión.
- Conmutación de datos basados en políticas.
- Agente SNMP centralizado para gestionar la micro estación base y todos sus Sus registrados. Este agente permite una gestión en banda (In-Band) y fuera de banda (Out-Of-Band). Esta última se realiza a través de una interfaz de red 10/100 BASE-T.
- Soporte para configuración local, monitorización y debugging a través de una interfaz serie RS-232.

TABLA 4.4 Especificaciones radio de la micro estación base BreezeMAX 3000

Ítem	**Descripción**		
Frecuencia	Banda	Uplink (MHz)	Downlink (MHz)
	AU-ODU-3.5b	3450-3500	3550-3600
Modo de operación	FDD, Halfduplex.		
Ancho de banda de canal	1.75 MHz 3.5 MHz		
Resolución de la frecuencia central	0.125 MHz		
Puerto de Antena (AU-ODU)	Tipo N, 50 Ohm.		
Máxima potencia de entrada al puerto de antena (interfaz ODU)	-50 dBm antes de saturación, -17 dBm antes de deterioro		
Rango de potencia de salida al puerto de antena (interfaz ODU)	13 dBm-28 dBm.		
Modulación	Modulación OFDM 256. BPSK, QPSK, QAM16 y QAM64		
FEC	Codificación Convolucional: 1/2, 2/3 y ¾		
Throughput bruto: downlink/uplink	Máximo: 12 Mbps, con QAM 64 3/4. Mínimo: 1.25 Mbps con BPSK 1/2.		
Máximo número de Sus	250 usuarios		
Multiplexado	TDMA		

4.6.2 Distribución WiFi:

Para la distribución del servicio dentro de la comunidad de Huaquicha, se utilizar los siguientes equipos:

a) Antena omnidireccional hyperlink hg2413u-nf

La Antena HG2412U-NF es una antena omnidireccional de gran rendimiento muy compacta diseñada para la banda de ISM de 2.4GHz. Es adecuada para conexiones multipunto y aplicaciones móviles donde se desea una amplia cobertura. Compatible con 802.11b de IEEE y 802.11g, Bluetooth.

Especificaciones:

Electrical Specifications:Frequency: 2400-2500 MHz

-Gain: 12 dBi

-Polarization: Vertical

-Vertical BeamWidth: 8°

-Horizontal BeamWidth: 360°

-Impedance: 50 Ohm

-Max. Input. Power: 50 Watts

-VSWR: <1.5:1 avg.

MechanicalSpecificationsWeight: 1.7 lbs. (0.8 kg)

-Length: 48 in. (1.2m)

-Diameter: 0.740in. (18.8mm)

-Radome Material: Gray Fiberglass

-Mounting: 2.0" Diametermastmax.

-WindSurvival:> 150 MPH

-RoHSCompliant: Yes

-Operating Temperature: -40°C to 85°C (-40° F to 185° F)

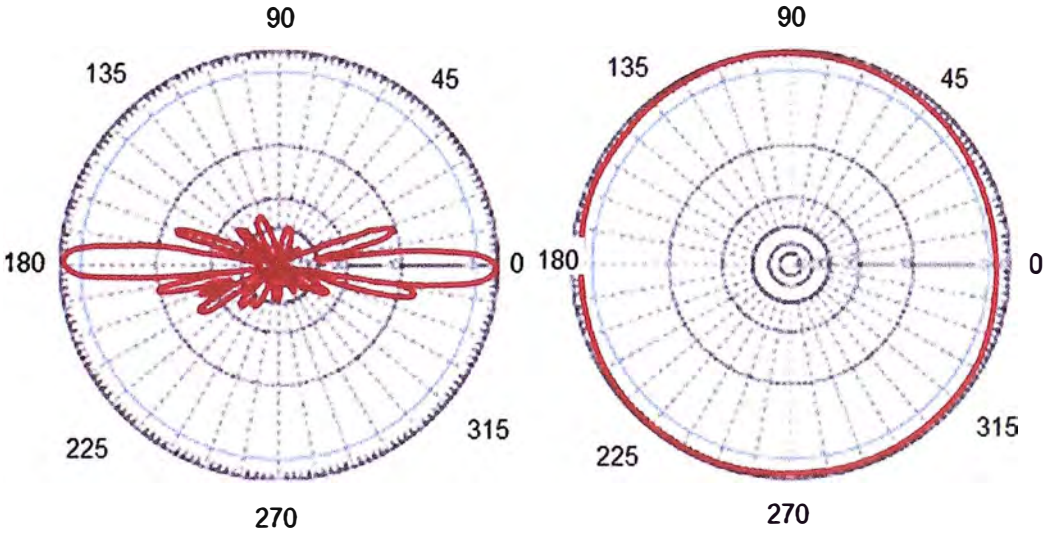

Fig. 4.14 Patrón de radiación

b) Acces Point Dlink modelo 3200ap

-Soporte de PoE (Power over Ethernet), 802.3af

-Soporte de MultiplesSSID's

-Soporte WDS para sus diferentes modos de operación

-Soporte 11g, 108Mbps Modo Turbo

-Robusto Access Point para soluciones Indoor

El D-Link DWL-3200AP es un poderoso, robusto y fiable Access Point para operar en entornos de empresas con diversos negocios.

Diseñado para instalaciones Indoor, este Access Point provee opciones avanzadas de seguridad para los administradores de red, permitiéndoles desplegar una administración muy robusta en redes wireless.

El Access Point DWL-3200AP soporta Power Over Ethernet (PoE) y provee dos antenas de alta ganancia para una óptima cobertura wireless.

Principales Características y Facilidades:

-Soporte WDS para sus diferentes modos de operación.

-Soporte de Múltiples SSID's.

-Soporte 11g, 108Mbps Modo Turbo.

-Robusto Access Point para soluciones Indoor.

-Soporte de PoE (Power over Ethernet), 802.3af.

-Soporte WEP.

-Soporte WPA, AES y 802.11i.

-Seguridad Ampliada, con soporte de ACL, 802.1x y filtrado de direcciones MAC.

-Administración versátil, vía D-Link D-View, SNMP v3, Web, Telnet y AP Manager.

4.7 Seguridad del enlace

Enseguida se revisara las diferentes variedades de seguridad existente y veremos cuál es el más adecuado para nuestra necesidad.

4.7.1 Tipos de Encriptamiento

La implementación de una red inalámbrica es corta a comparación de otras redes, pero es vulnerable a ataques, o de accesos de usuarios ajenos a la red. El cual la información que es transportada por el enlace puede ser víctima de robo o manipulación de datos, lo cual sería perjudicial para una red gubernamental. Se han creado mecanismos para evitar ataques a la red, pero ya algunos mecanismos serian inservibles por contar con las siguientes deficiencias:

a) Filtrado por MAC

En la actualidad este método tiene problemas de seguridad ya que se ha encontrado la manera de rastrear (con un Sniffer) la red inalámbrica buscando una MAC autorizada y luego esta es duplicada, haciendo que el intruso pueda ingresar a la red.

b) Encriptación WEP

El "Wired Equivalent Privacy" o "Privacidad Equivalente a Cableado" es uno de los primeros método de encriptación que se utilizó para mejorar la seguridad en el acceso inalámbrico, pero lamentablemente a este método también se le ha encontrado falencias,

y en la actualidad existe en internet software libre que pueden desencriptar este protocolo y por lo tanto también podrían ingresar a la red.

c) Encriptación WPA

El "WiFi Protected Access" o el "acceso protegido WiFi", fue la mejora que se realizó al método de encriptación WEP hasta que saliera el estándar de la IEEE, al cual se le llamo WPA2 que es el más seguro en el campo de las TI.

4.7.2 Encriptación WPA2

El WPA2 está basado en el estándar IEEE 802.11i. WPA2 es la implementación aprobada por WiFi Alliance del estándar 802.11i y es compatible con WPA. WPA2 ofrece un alto nivel de seguridad incluyendo el algoritmo AES **Capitulo 3**. WPA2 puede habilitarse en 2 versiones: WPA2 personal y WPA2 enterprise. WPA2 personal protege de acceso no autorizado a la red utilizando una contraseña establecida. WPA2 entreprise verifica a los usuarios de la red a través de un servidor.

El AES utiliza una llave temporal de 128 bits y un vector de inicialización de 48 bits en el proceso de encriptación. Los métodos de autenticación utilizados por el 802.11i utilizan el estándar IEEE 802.11x y el protocolo TKIP.

a) TKIP(Temporal Key Integrity Protocol)

Este protocolo está compuesto por:

Código de integración de mensajes (MIC), el cual encripta el ckecksumjunto con las direcciones MAC y los datos.

Reduce la posibilidad de calcular una determinada llave.

Utiliza un VI (vector de inicialización) de 48 bits, llamado TSC (TKIP Sequence Counter) descarta paquetes recibidos fuera de orden.

La utilización del TSC extiende la vida útil de la llave temporal.

Pueden intercambiarse 2^{48} paquetes utilizando la misma llave temporal.

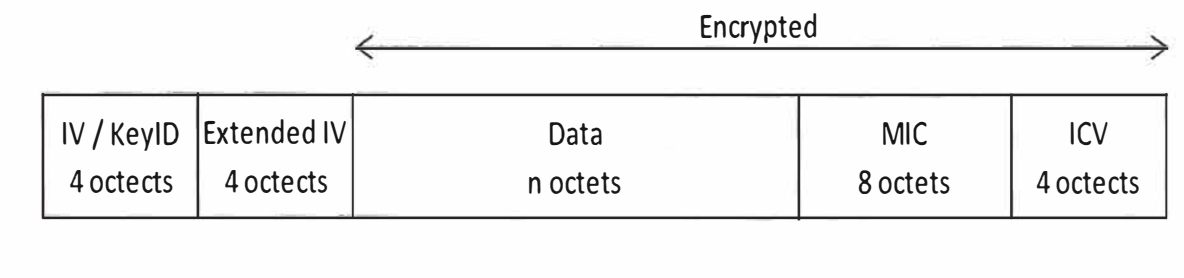

Fig. 4.15 Estructura de encriptación TKIP

Proceso de encapsulación.

Se combina la llave temporal, la dirección del emisor y el TSC para obtener una llave de 128 bits que dividida en la llave RC4 de 104 bits y la IV para una encapsulación tipo WEP para el estudio.

El MIC se calcula sobre las direcciones físicas y el MSDU.

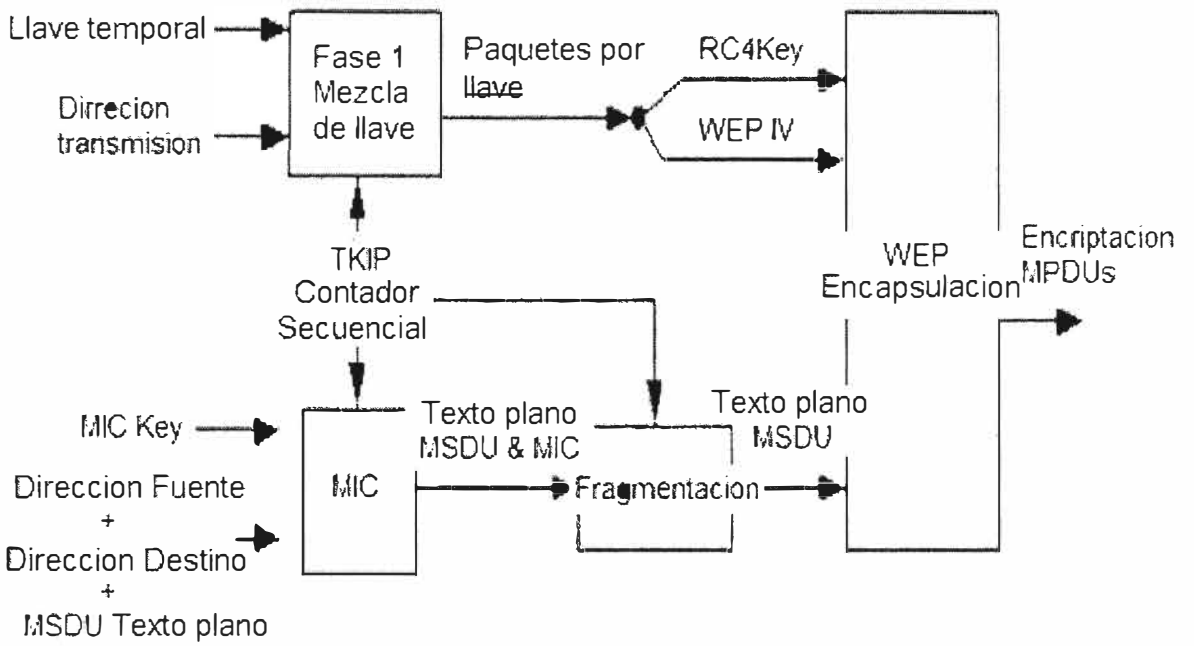

Figura 4.16 Proceso de encriptamiento de TKIP

Proceso de desencriptación

Se examina el TSC para asegurar que tiene un valor mayor del paquete recibido anteriormente (evita ataque recepción)

Se calcula el valor MIC sobre el MSDU recibido y desencriptado y se compara con el valor recibido.

b) CCMP (Counter Mode with CBC-MAC Protocol)

Es un protocolo que complementa al TKIP.

Su método de encriptación es basado en AES

Tiene un cifrado simétrico con bloques de 128 bits

Hace uso obligatorio del 802.11i

El formato de la trama tras la encriptación CCMP

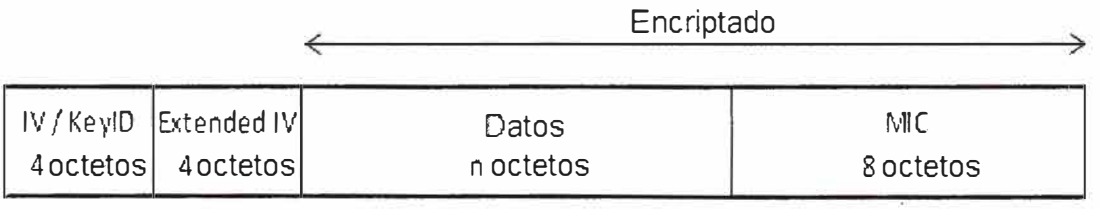

Fig. 4.17 Estructura de encriptación de CCMP

CCMP utiliza un IV de 48 bits denominado PN (Packet Number) utilizado para calcular el MIC y la encriptación de la trama.

La encriptación de los bloques utiliza la misma llave temporal derivada de la llave principal.

El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama.

El IV se convierte en un bloque AES y su salida a través de la operación XOR compone el siguiente bloque AES **[11]**.

4.7.3 Proceso de encriptación en el enlace punto a punto

Una vez explicado el método de encriptación e implementado el enlace, veremos el mecanismo y los pasos que se realiza para brindar seguridad a nuestra red.

Una de las característica principales que cuenta un sistema WiMAX, aparte de su robustez en los enlaces, es de contar con el mecanismo de seguridad (IEEE 802.11i), utilizada también por el sistema WiFi.

Los pasos que se realizan al encriptar una trama es la siguiente:

En la capa 2 la trama es encriptada (WAP2-AES), generando una llave de autenticación.

La trama una vez encriptado es enviada hacia los otros terminales por medio del RF **Fig.4.18**, la cual esta debe contar con la llave de autenticación, caso contrario podrá capturar las tramas pero no podrá acceder al contenido de ellas.

Una vez que el usuario final ingrese su llave de autenticación, podrá tener acceso a toda la información que se le envíe.

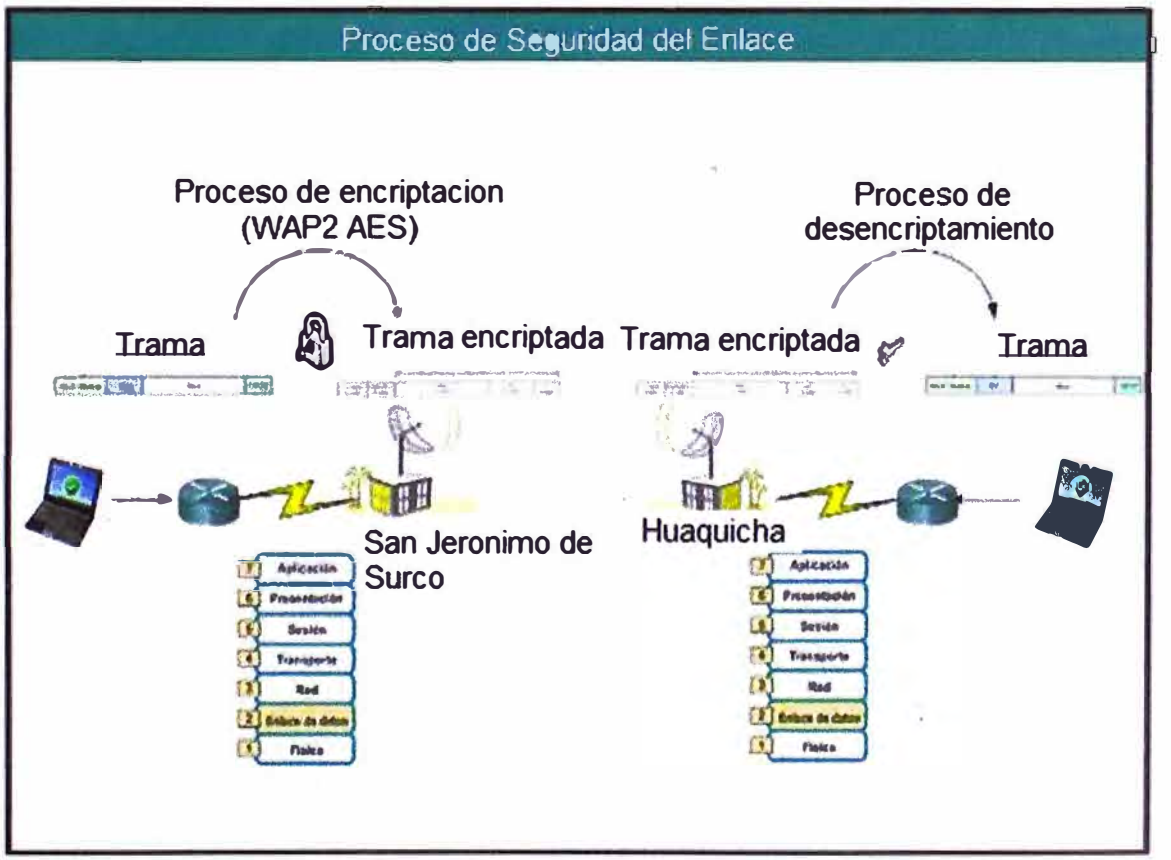

Fig. 4.18 Proceso de encriptación y autenticación

La especificación 802.11i ofrece un nivel de seguridad capaz para complacer a la mayoría de las agencias gubernamentales. Sin embargo, AES requiere un chip dedicado, por lo cual los dispositivos WiMAX cuenta con equipos que pueden soportar la encriptación AES desde 128 bits como mínimo, lo cual podría generar una latencia imperceptible en nuestro enlace, a diferencia de WiFi. Otras características de 802.11i es el keycaching (cache de llave), lo que facilita la rápida reconexión con el servidor para los usuarios que se han ido temporalmente fuera de línea, y pre-autenticación, que permite una rápida "roaming", y es ideal para su uso con aplicaciones avanzadas, tales como Voz sobre Protocolo de Internet (VoIP).

4.8 Análisis económico comparativo

Ahora mostraremos el análisis económico de enlace satelital, vía fibra óptica y enlace WiMAX, en donde se observa que el enlace Wimax es el más económico para ser implementado en este proyecto.

Tabla 4.5 Costo de enlace satelital

Implementación con enlace satelital	
Antena parabolica	600
ODU	1500
Enrutador satelital	1400
LNB	600
Fuente de Alimentación	120
Cables y ferreterías	300
Alquiler mensual de servicio de internet satelital 128K	800
Costo total en dólares	5320

Tabla 4.6 Costo de enlace con fibra óptica

Implementación con fibra óptica	
Instalación de 20 postes de cemento de 10 mts.	10000
Tendido de fibra mono modo auto soportados (2000 metros)	40000
Conectores SPF (2)	1000
Media Converter TFC marca Trendnet (2)	600
Swich Cisco 3950 (2)	1200
Alquiler mensual de servicio de internet 1Mbs	200
Costo total en dólares	53000

Tabla 4.7 Costo de enlace con WiMAX

Implementación con enlace WiMAX	
Motorola Canopy 5.4 Ptp 400 (2)	2500
Cables y ferretería	400
Instalación de Torre de 12 mts. (2)	1200
Alquiler mensual de servicio de internet 1Mbs	200
Costo total en dólares	4300

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El uso de la red inalámbrica basándonos en tecnología Wimax es una óptima solución para la integración con zonas rurales, aprovechando su arquitectura de punto-multipunto.

2. Las instituciones gubernamentales pueden dar un gran uso de estos enlaces, puesto tendría mayor cercanía hacia zonas alejadas y rurales, para brindarles programas de ayuda, educación, capacitación, etc.

3. Con el proyecto VOTO ELECTRONICO, esta podrá utilizar la infraestructura para que la población más alejada pueda ejercer su derecho de elegir a sus autoridades.

4. Se podrá implementar telefonía y servicio de internet en las escuelas de las zonas rurales, y así dar uso de los equipos donados a los estudiantes con el programa OLPC (Una Laptop por niño).

5. La red WiMAX cuenta con un mecanismo de seguridad basado en algoritmos de encriptación de las cuales la más segura es el AES.

6. El método de encriptación AES es en la actualidad el algoritmo de cifrado más seguro en el sector de las tecnologías de la información, es utilizado en diversidad de aplicaciones.

7. Siendo AES un algoritmo público, varios han sido los intentos por burlar su seguridad, pero no se reconoce ninguno que pueda lograrlo.

8. Los nuevos equipos portátiles obligan a los usuarios utilizar cada vez más los medios inalámbricos para acceder a su información, siendo cada vez de más importancia las velocidades de acceso y los métodos de seguridad.

Recomendaciones

1. Para el cifrado AES utilizar en lo posible claves de 128 bits para que no consuma recursos memoria y CPU.

2. Para que el acceso inalámbrico funcione correctamente se necesita brindar un mantenimiento anual probando el área de cobertura, para este caso podemos utilizar un equipo portátil y movilizarse por todo el local revisando, conectividad, potencia de la señal y velocidad de acceso.

3. Separar en 2 redes independientes (VLans), uno para datos y otro para telefonía.

4. Contar con un servidor de Telefonía, dentro de la comunidad de San Jerónimo de Surco, para brindar telefonía a zonas rurales.

5. Si se utiliza este acceso inalámbrico para intercambiar paquetes de voz sería recomendable aplicar calidad de servicio (QoS).

6. Para brindar mayor seguridad es recomendable la implementación de un servidor Radius, en especial si la red es utilizado por algún órgano gubernamental.

ANEXO A
CONFIGURACIÓN BÁSICA DE LA ESTACIÓN BASE WIMAX

En esta sección se describe los pasos necesarios para realizar una configuración básica de la micro estación base WiMAX de Alvarion mediante el programa de gestión BreezeLITE.

Con la configuración básica se tendrá una red WiMAX funcionando cumpliendo los requisitos de nivel físico. Para empezar la **Fig. A.1** muestra la pestaña General de la estación base. En ella se puede añadir unos identificadores formados por un nombre, una localización y un contacto.

El resto es solo información referente al equipo (versión del firmware, temperatura, tiempo de funcionamiento, etc.) y parámetros de configuración irrelevantes para la puesta en funcionamiento de la red.

Posteriormente en la pestaña Air Interface que se muestra en la **Fig. A.2** se debe configurar:

- Identificación de la BS: La identificación de la estación base consta de 6 grupos de tres dígitos cada uno. Los primeros 3 grupos definen el ID del operador de red, los siguientes dos grupos definen la identificación de la celda en concreto y el último grupo define la identificación del sector.

- ARQ Status: El parámetro ARQ habilitado/deshabilitado controla si se usa un algoritmo ARQ para detectar errores y solicitar retransmisiones de mensajes unicast (aplicable solo para servicios BestEfforty Non Real Time).

- Max. CellRadius: Este parámetro es usado para adaptar varios parámetros de timing de nivel MAC en el momento en que se recibe un mensaje para alcanzar su destinación. El retardo temporal es dependiente sobre la distancia entre transmisor receptor.

Los parámetros de timing deberían ser adaptados al retardo más grande esperado, es decir, la distancia más grande entre la estación base y el terminal SU servido por ésta. Un SU que se encuentre localizado a una distancia mayor que el configurado en este parámetro, será rechazado durante el proceso de acceso a la red.

Este parámetro debe de ser de 10 Km o equivalentemente el tiempo de símbolo que es de 68μs.

- Multi Rate Support: Aquí se configuran las constelaciones básicas que se usarán en los enlaces de uplink / downlink y además se debe tener activado el algoritmo de modulación y codificación adaptativa.

- Bandwith: Ancho de banda del sistema, 3.5 MHz, en el caso de WiMAX 802.16-2004.

- ATPC Parameters: Se especifica el nivel óptimo de potencia en recepción en la estación base en el que todas las transmisiones deberían ser recibidas por las unidades

AUODU para asegurar un rendimiento óptimo. El rango es de [-103:-60] dBm. Por otro lugar el algoritmo de control automático de potencia debe estar habilitado.

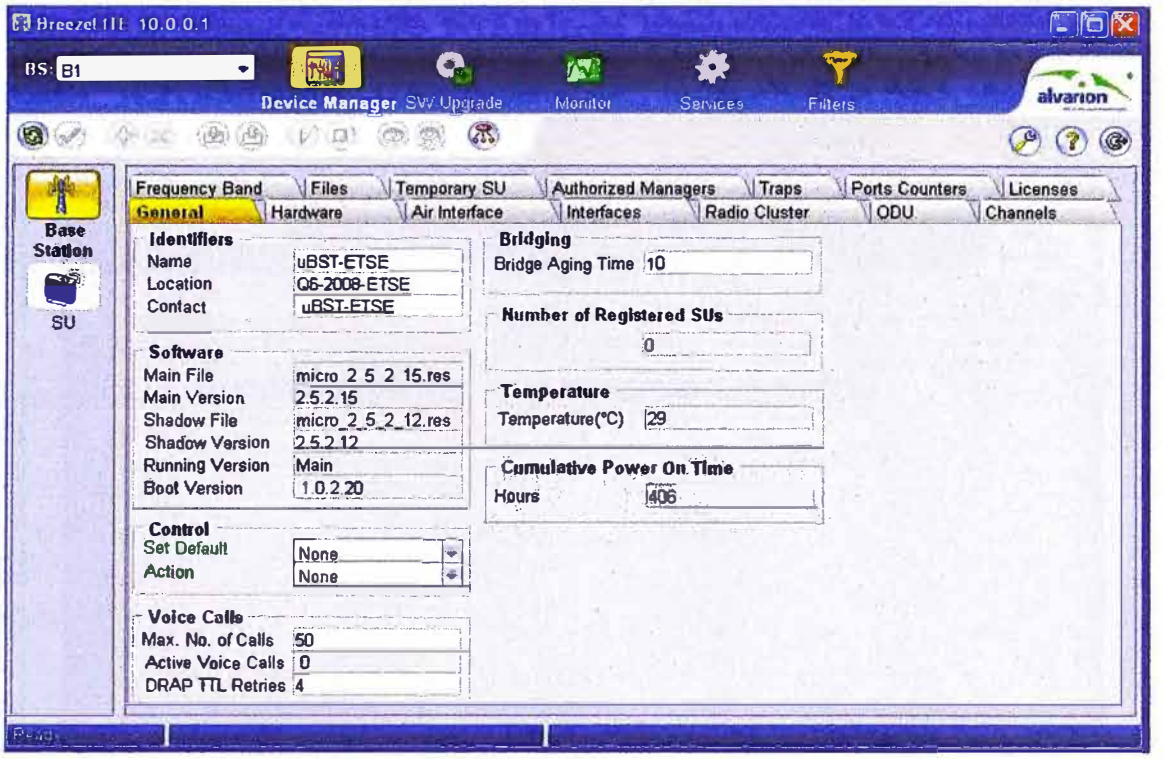

Fig. A.1 Pestaña General de la estación base BreezeLITE

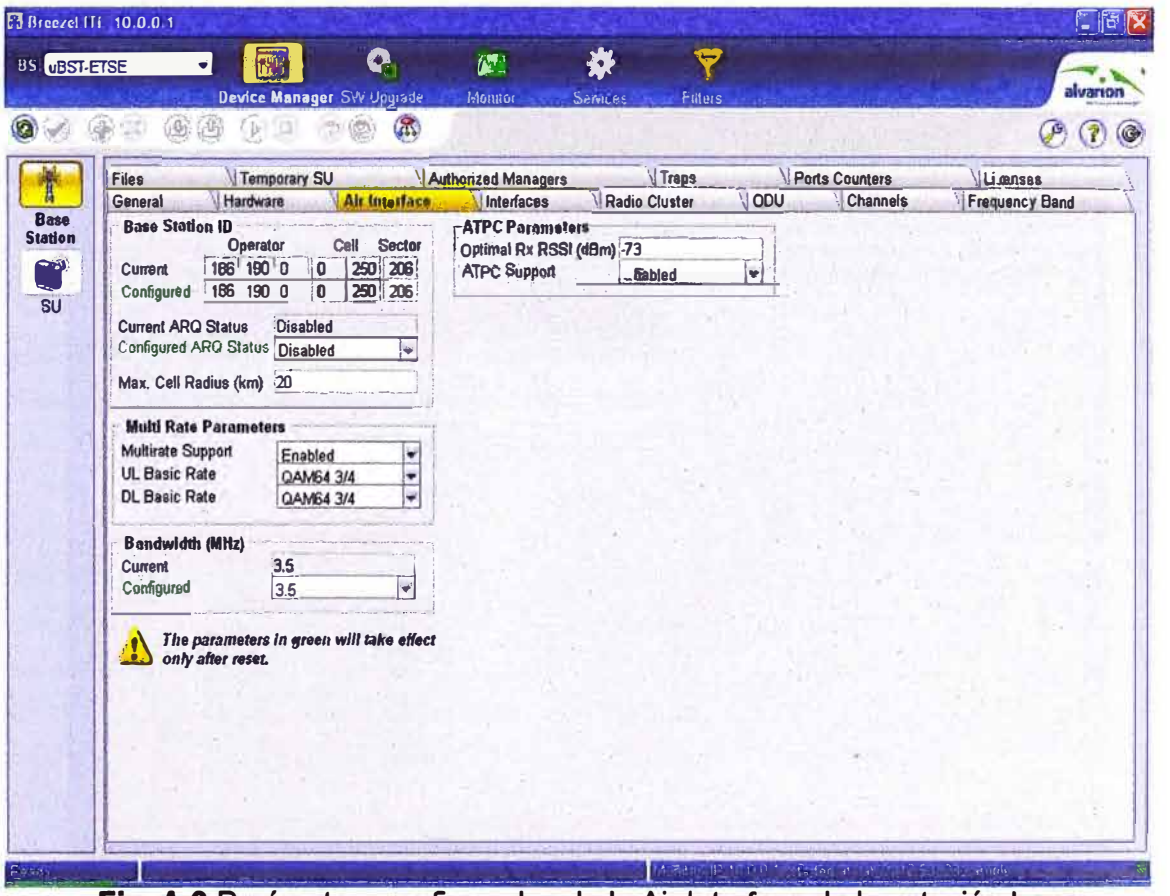

Fig. A.2 Parámetros configurados de la Air Interface de la estación base

Para especificar la potencia de transmisión (sin considerar la antena) se utiliza la pestaña de ODU que se muestra en la **Fig. A.3**. La banda de frecuencia configurada es la 3.5b equivalente a uplink: 3450-3500 MHz y downlink: 3550-3600 MHz. La frecuencia de transmisión de downlink se configura en la pestaña channels como se indica en la **Fig.A.4**.

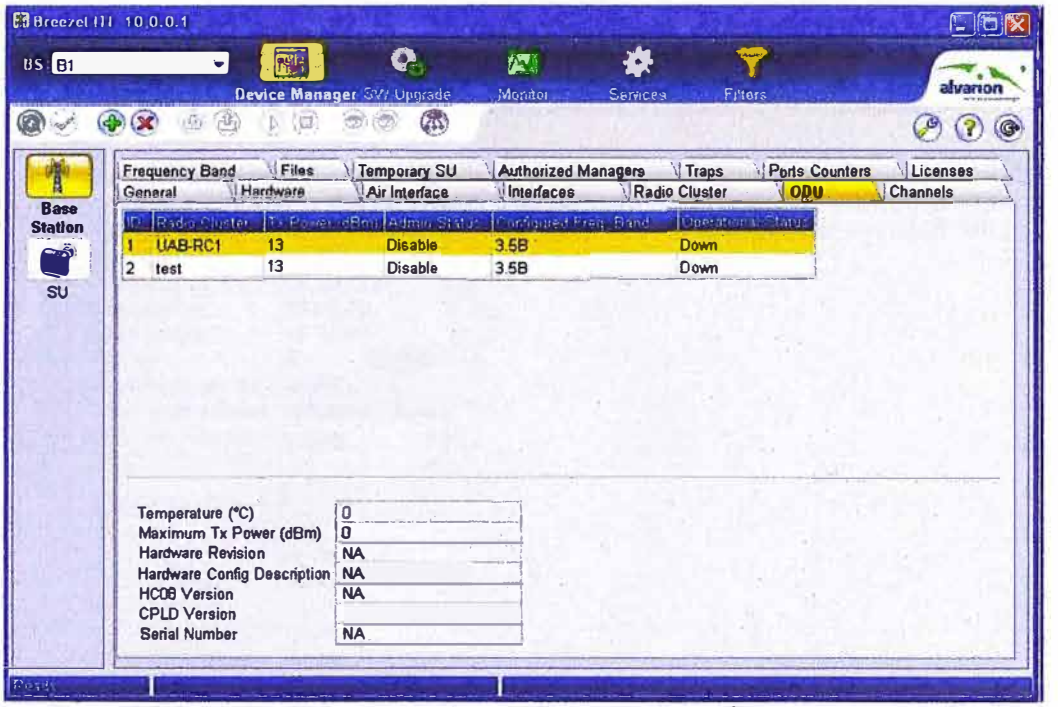

Fig. A.3 Potencia de transmisión configurada (el máximo es de 28 dBm).

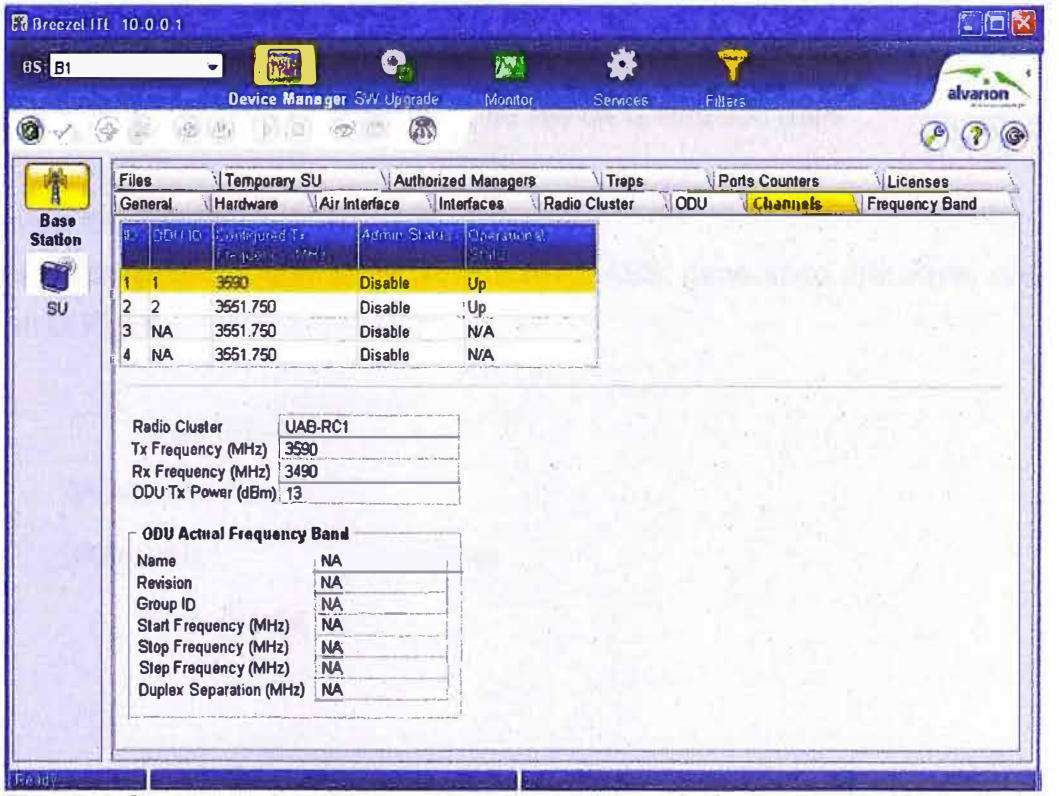

Fig. A.4 Configuración de la frecuencia de transmisión en el canal de bajada.

Con el proceso realizado hasta este punto ya se tendría una red WiMAX en funcionamiento. Para que los usuarios puedan acceder a Internet se debe conectar la estación base a un dispositivo de nivel 3, a un router por ejemplo y configurar las direcciones de sus interfaces de red y de gestión. La **Fig. A.5** muestra la configuración que se tiene en la estación base WiMAX.

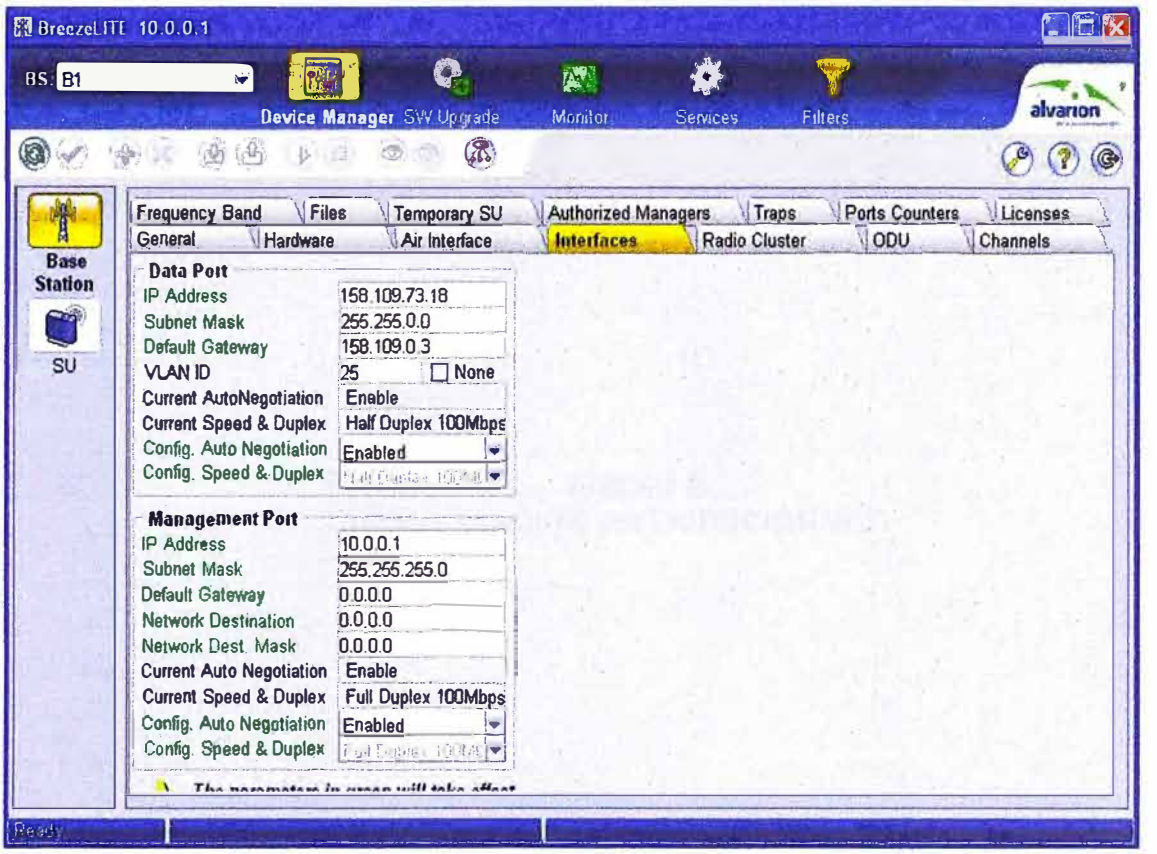

Fig. A.5 Configuración de red de la estación base

Encriptación del enlace

El enlace contara con una encriptación WPA2-AES, generando una llave, como se muestra en la **Fig. 6**.

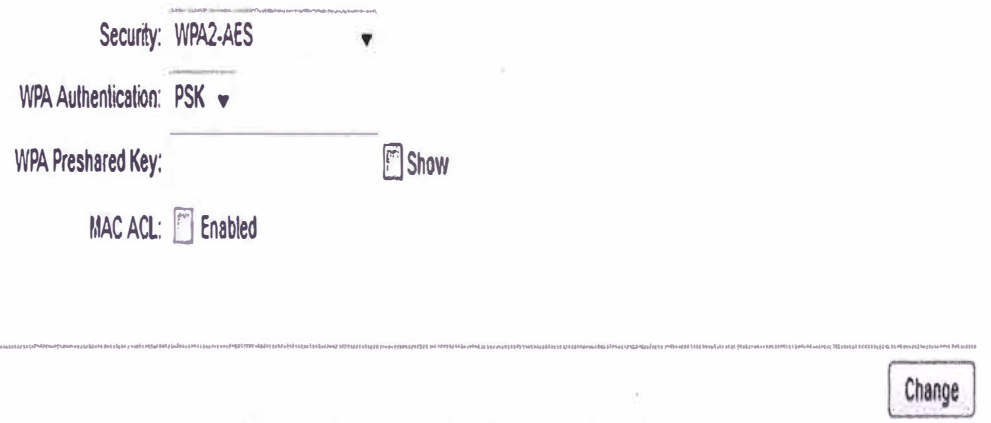

Fig. A.6 Encriptamiento WPA2-AES

ANEXO B
CONFIGURACION DISTRIBUCIÓN WiFi

Configuración de la Estación Base

-Asignamos el SSID "Comunidad Huaquicha"

-Habilitamos la opción Auto ChannelScan, para que coja la frecuencia más óptima.

-Habilitamos la Autenticación WPA2 utilizando el algoritmo AES.

-Le asignaremos una llave de seguridad de 128 bits.

Configuración de los Equipos Terminales

Para los visitantes la configuración es más sencilla, solo tienen que brindar doble click al SSID Comunidad Huaquicha y colocar la llave, como se muestra en la **Fig. 2**.

Fig. B.1 Ingresando la clave para ingresar a la red visita

BIBLIOGRAFIA

1. Michael W. Thelander, "WIMAX Oportunidades y desafíos en un mundo inalámbrico".

2. Dr. Víctor Rangel Licea, "Modelado de redes WiMAX"
Facultad de Ingeniería Universidad Nacional Autónoma de México 2009

3. Joaquín Navarro Lucas, "Redes inalámbricas Wimax".
Albert Angeles Vázquez, "Despliegue y análisis de la cobertura de una red WiMAX basada en IEEE 802.16-2004".

4. Loyola Eduardo Sánchez Daniel, "Evaluación del algoritmo de encriptación AES".

5. Jorge Alfonso Briones Garcia, "Advanced Encryption Standard Rijndael".

6. José de Jesús Angel, "AES - Advanced Encryption Standard".

7. Modelo de Enlace Satelital.
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/peredo_a_s/capitulo3.pdf.

8. Características de la fibra ópticas.
http://es.scribd.com/doc/6539516/01-Caracteristicas-de-Las-Fibras-Opticas.

9. Introducción a las redes inalámbricas.
http://es.kioskea.net/contents/wireless/wlintro.php3.

10. Ing. Julio Cesar Lozano Salas, "Diseño de radioenlace".
Universidad Nacional de Ingenieria

11. Julio Cesar Ardita, "Análisis de WPA/WPA2 Vs WEP".