ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTOR: ARELLANO CARVAJAL, JORGE FERNANDO

TEMA: INTERCEPTACIÓN, MONITORIZACIÓN Y DEMODULACIÓN NXDN™ DE SEÑALES DIGITALES EN TIEMPO REAL

DIRECTOR: DR. OLMEDO, GONZALO

CODIRECTOR: ING. BERNAL, PAÚL

SANGOLQUÍ, 16 DE MARZO DE 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICADO

Dr. Gonzalo Olmedo e Ing. Paúl Bernal MSc.

CERTIFICAN

Que el trabajo titulado **"INTERCEPTACIÓN, MONITORIZACIÓN Y DEMODULACIÓN NXDN™ DE SEÑALES DIGITALES EN TIEMPO REAL"**, realizado por el SR. TNTE. TÉC. AVC. **JORGE FERNANDO ARELLANO CARVAJAL**, con C.C. 180306104-1, ha sido guiado y revisado periódicamente y cumple las normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas - ESPE.

Debido a que se trata de un trabajo de investigación para las Fuerzas Armadas del Ecuador, NO recomiendan su publicación.

Sangolquí, 16 de marzo de 2015.

Dr. Gonzalo Olmedo
DIRECTOR

Ing. Paúl Bernal MSc.
CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, Tnte. Téc. Avc. Jorge Fernando Arellano Carvajal

DECLARO QUE:

El proyecto de grado denominado **"INTERCEPTACIÓN, MONITORIZACIÓN Y DEMODULACIÓN NXDN™ DE SEÑALES DIGITALES EN TIEMPO REAL"** ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las fuentes que se incorporan en las referencias bibliográficas.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 16 de marzo de 2015.

Jorge Fernando Arellano Carvajal
Tnte. Téc. Avc.
C.C. 180306104-1

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Tnte. Téc. Avc. Jorge Fernando Arellano Carvajal

Autorizo a la Universidad de las Fuerzas Armadas- ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo **"INTERCEPTACIÓN, MONITORIZACIÓN Y DEMODULACIÓN NXDN™ DE SEÑALES DIGITALES EN TIEMPO REAL",** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 16 de marzo de 2015

Jorge Fernando Arellano Carvajal

Tnte. Téc. Avc.

C.C. 180306104-1

DEDICATORIA

A Dios, quien ha sido mi gran fuente de valor, fuerza y sobre todo de sabiduría.

A mis queridos padres, quienes me han brindado todo su apoyo, amor y comprensión, con el único afán de verme como una persona que tiene a todo momento como pilar principal los valores inculcados en el hogar y como un hombre fiel a sus principios durante el conseguimiento de las metas planteadas.

A mi amada esposa, quien ha sido y es mi mejor amiga, mi compañera fiel que brinda amor y dedicación a nuestro hogar a cada instante.

A mi alejado primogénito José Fernando, quien siempre se encuentra presente en mi mente y corazón a pesar del poco tiempo compartido y vivido como padre e hijo.

A mis adoradas y tiernas hijas, quienes son una magnífica inspiración en la búsqueda de una vida buena y plena.

A mis apreciados abuelos, quienes siempre han estados presentes en cada éxito y fracaso.

A mis estimados hermanos, quienes a pesar de las adversidades han puesto en primer lugar a la unión familiar. Y finalmente a todas aquellas personas que me han brindado su amistad, confianza y gratitud.

AGRADECIMIENTO

En primer lugar brindo mi agradecimiento eterno a Dios por todas las bendiciones y malas experiencias vividas, en especial por estas últimas, porque gracias a ellas me pude dar cuenta que hay que ser valiente para enfrentar el duro trajín de la vida, que uno nunca se puede dar por vencido por más problemas que se tenga que enfrentar, además entendí que si alguna vez alguien te brinda maldad, tu solo puedes responder con bondad.

En segundo lugar agradezco a mis padres y en especial a mi hermana Mónica, porque siempre me han dado todo lo necesario para alcanzar mis sueños y metas propuestas, siendo un apoyo incondicional durante toda mi vida.

También debo resaltar un sincero agradecimiento a los docentes que me han ayudado a que esta tesis sea una realidad palpable en beneficio de mi querida Fuerza Aérea Ecuatoriana, a mi Director y Codirector, el Dr. Gonzalo Olmedo y el Ing. Paul Bernal. No puedo dejar a un lado mi gratitud hacia el Ing. Juan Pablo Robelly, quien me ha brindado su apoyo incondicional en el desarrollo e implementación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Hoy en día el que controle el *espectro electromagnético* tendrá un arma poderosa contra fuerzas enemigas en el campo de batalla, por tal razón, el presente trabajo de tesis trata sobre las *Medidas de Apoyo Electrónico de Guerra Electrónica* (monitorización e interceptación en *tiempo real*) aplicadas a las comunicaciones de voz sin encriptar con tecnología *NXDN*™ de fuerzas opuestas. En primer lugar, se hace una aclaración y comparación entre GE y la Inteligencia de Señales, puesto que existe gran confusión y escaso conocimiento sobre estos temas en FF.AA. del Ecuador; además, también se indica el funcionamiento y características técnicas del protocolo de radio móvil terrestre anteriormente mencionado. Posterior se diseña un sistema para la monitorización *(con el receptor portátil R&S®PR100)*, interceptación *(con el software R&S®GX430)*, demodulación y decodificación en *tiempo real* de señales digitales *NXDN*™ de comunicación de voz no encriptada *(con la herramienta matemática MatLab® y el dispositivo USB-3000™ P25)*. Luego para un mejor entendimiento del funcionamiento y desempeño del estándar *NXDN*™ se realiza una simulación de la transmisión y recepción con la ayuda de MatLab®, en diferentes escenarios de canal con desvanecimiento plano estático (con y sin línea de vista), además de que se hace un análisis del funcionamiento del equipo USB-3000™ P25 con el mismo software (codificación y decodificación de un tono de prueba y una se frase específica). Finalmente se realizan conclusiones y recomendaciones sobre la tecnología usada y el sistema diseñado.

PALABRAS CLAVES:

- **GUERRA ELECTRÓNICA**
- **INTELIGENCIA DE SEÑALES**
- **PROTOCOLO NXDN™**
- **MEDIDAS DE APOYO ELECTRÓNICO**
- **TIEMPO REAL**

ABSTRACT

Today, whoever controls the electromagnetic spectrum will have a powerful weapon against enemy forces on the battlefield, for this reason, this thesis is about the *Electronic Support Measures* of *Electronic Warfare* (monitoring and interception in *real time*) applied to *NXDN*™ technologies of voice communication unencrypted of opposing forces. First, a clarification and comparison between GE and *Signals Intelligence* is made, as there is much confusion and little knowledge on these subjects in the Armed Forces of Ecuador; further, the technical characteristics and operation of the land mobile radio protocol are also indicated. Then, a system is designed for monitoring (with R&S®PR100 portable receiver), interception (with R&S®GX430 software), demodulation and decoding in *real time* of digital signal NXDN™ of voice communication not encrypted (with MatLab® and the USB-3000™ P25 device). After, for a better understanding of the operation and performance of *NXDN*™ standard, a simulation for transmission and reception through different scenarios with static flat fading channel (with and without line of sight) is developed with MatLab®; in addition, an analysis of the operation of the USB-3000™ P25 device is performed with the same software (encoding and decoding of a test tone and a phrase). Finally conclusions and recommendations about the technology used and the designed system are made.

KEYWORDS:

- **ELECTRONIC WARFARE**
- **SIGNALS INTELLIGENCE**
- **PROTOCOL NXDN™**
- **ELECTRONIC SUPPORT MEASURES**
- **REAL TIME**

PRÓLOGO

Como Oficial Técnico de la FAE en la especialidad de Comunicaciones y como miembro activo de las Fuerzas Armadas del Ecuador, es mi deber e interés aclarar las definiciones y campos de acción de Guerra Electrónica e Inteligencia de Señales, en vista que existe una gran confusión sobre estos temas en nuestra gloriosa institución e inclusive en personal que ha realizado diferentes trabajos de tesis e investigación en la Universidad de Fuerzas Armadas - ESPE, especialmente en el ámbito de sus aplicaciones en el campo de batalla, llevando a mal interpretar que la SIGINT es parte de la GE, lo cual no es verdadero puesto que en la realidad son cosas diferentes, que en ciertas ocasiones la una se vale de la otra y viceversa. Por tal motivo en el presente trabajo de tesis expongo una breve introducción y comparación de mencionadas acciones militares, para solventar sus conceptos, definiciones y aplicaciones.

Otro gran objetivo que tiene este trabajo es ser una base de inicio para el desarrollo tecnológico de la Guerra Electrónica en el país, con la finalidad de dejar de depender de tecnologías extranjeras en la explotación de estas poderosas armas militares en contra de fuerzas enemigas.

En la actualidad las comunicaciones móviles terrestres de banda estrecha NXDN™ en latinoamérica son muy utilizadas por organizaciones lícitas e ilícitas, razón por la cual el entendimiento de las características técnicas y funcionamiento exacto de este protocolo permitirá realizar la Guerra Electrónica a grupos delincuenciales que usen dicha tecnología, específicamente con Medidas de Apoyo Electrónico (monitorización e interceptación de señales). Para cumplir con lo descrito se procederá a desarrollar y elaborar el diseño de un sistema que permitirá realizar la monitorización, interceptación y demodulación en tiempo real de señales digitales NXDN™.

La propuesta del diseño se valdrá en las etapas de monitorización e interceptación del equipo receptor portátil R&S®PR100 y el software para análisis de señales R&S®GX430, en la demodulación se apoyará de la herramienta matemática MatLab® y en la decodificación de voz del dispositivo USB-3000™ P25 en su versión estándar con su software controlador usb3kcom.exe.

Finalmente para entender de mejor manera el comportamiento y funcionamiento del estándar de banda estrecha NXDN™ se realiza una simulación de la transmisión y recepción usando el mismo sobre diferentes tipos de desvanecimientos planos estáticos, uno en donde existe línea de vista entre transmisor y receptor y otro donde no existe línea de vista, todo con la ayuda de MatLab® y ciertas funciones propias del software. Si se deseara realizar posteriormente una implementación del diseño de GE, este último paso sería de mucha importancia para el correcto y eficiente funcionamiento del sistema.

GLOSARIO

A

AES *Advanced Encryption Standard*, Estándar de Encriptación Avanzada

AM *Amplitude Modulation*, Modulación de Amplitud

AWGN *Additive white Gaussian noise*, Ruido Aditivo Gaussiano Blanco

B

BER *Bit Error Rate*, Tasa de Error de Bits

C

COMINT *Communications Inteligence*, Inteligencia de Comunicaciones

Comms ES *Communications Electronic Support*, Apoyo Electrónico de Comunicaciones

CPFSK *Continuous Phase Frequency Shift Keying*

D

DES *Data Encryption Standard*, Estándar de Encriptación de Datos

DF *Direction Finding*, Radiogoniometría

DOA *Direction of Arrival,* Dirección de Arrivo

dPMR *digital Private Mobile Radio*, Radio Móvil Privada digital

DSP *Digital Signal Processing*, Procesamiento Digital de señales

DVSI *Digital Voice Systems, Inc.*

E

EA *Electronic Attack*, Ataque Electrónico

ECCM Contra-contramedidas Electrónicas

ECM *Electronic Countermeasures*, Contramedidas Electrónicas

ELINT *Electronic Inteligence*, Inteligencia Electrónica

EOB *Electronic Order of Battle*, Orden Electrónica de Batalla

EP *Electronic Protection*, Protección Electrónica

EPM *Electronic Protection Measures*, Medidas de Protección Electrónica

ES *Electronic Support*, Apoyo Electrónico

ESM *Electronic Support Measures*, Medidas de Apoyo Electrónico

EW *Electronic Warfare*, Guerra Electrónica

F

FF.AA Fuerzas Armadas

FCC *Federal Communications Commission*, Comisión Federal de Comunicaciones

FDMA *Frecuency Division Multiple Access*, Acceso Múltiple por División de Frecuencias

FEC *Forward Error Correction*, Corrección de Errores en Recepción

FIPS *Federal Information Process Standard*, Estándar de Procesos de Información Federal

FM *Frequency Modulation*, Modulación de Frecuencia

FSK *Frequency Shift Keying*, Modulación por Desplazamiento de Frecuencia

FSW *Frame Synchronization Word*

G

GE Guerra Electrónica

GEOINT *Geospatial Intelligence*, Inteligencia Geoespacial

GPS *Global Positioning System***,** Sistema de posicionamiento global

H

HF *High Frecuency*, Alta Frecuencia

HUMINT *Human Intelligence*, Inteligencia Humana

I

IDAS *ICOM Digital Advanced System*, Sistema Avanzado Digital ICOM

IEEE *Institute of Electrical and Electronics Engineers,* Instituto de Ingenieros Eléctricos y Electrónicos

IF *Intermediate Frequency,* Frecuencia Intermedia

IMINT *Imagery Intelligence*, Inteligencia de Imágenes

IQ data *In-phase and quadrature data,* Datos en fase y cuadratura

ISI *Intersymbol Interference*, Interferencia Intersimbólica

L

LAN *Local area network,* Red de Área Local

LICH *Link Information Channel*, Canal de Control de Enlace

LMR *Land Mobile Radio*, Radio Móvil Terrestre

LOS *Line of Sight*, Línea de Vista

M

MASINT *Measurement and Signature Intelligence*, Inteligencia de Medición y firma

MIMO *Multiple Input – Multiple Output, Múltiples Entradas – Múltiples Salidas*

N

NIST *National Institute of Standards and Technology*, Instituto Nacional de Estándares y Tecnología

NLOS *Non Line of Sight*, No Línea de Vista

O

OSINT *Open Source Intelligence*, Inteligencia de Fuente Abierta

P

Pb Probabilidad de Bit Erróneo

PC *Personal Computer*, Computadora Personal

PCM *Pulse Code Modulation*, Modulación por impulsos codificados

Pe Probabilidad de Símbolo Erróneo

R

Radar ES *Radar Electronic Support*, Apoyo Electrónico de Radares

RC *Remote Control,* Control Remoto

RF *Radio Frequency,* Radio Frecuencia

R&S *Rhode&Schwarz*

S

SCCH *Signal Control Channel, Canal de Control de Señal*

SCPI *Standard Commands for Programmable Instruments, Comandos Estándar para Instrumentos Programables*

SD *Secure Digital*

SER *Symbol Error Rate,* Tasa de Símbolos Erróneos

SIGINT *Signals Inteligence*, Inteligencia de Señales

SIMO *Single Input – Multiple Output, Múltiples Entradas – Múltiples Salidas*

SNR *Signal to Noise Ratio*, Relación señal a ruido

U

UHF *Ultra High Frecuency*, Ultra Alta Frecuencia

V

VCH *Voice Channel*, Canal de Voz

VHF *Very High Frecuency*, Muy Alta Frecuencia

W

WAV Apócope de WAVE que es un formato de archivo de sonido

CAPÍTULO 1

INTRODUCCIÓN

1.1. ANTECEDENTES

La *Guerra Electrónica (GE)* tiene sus inicios en el sector militar desde el efectivo uso del radar en la *Batalla de Inglaterra* en la *Segunda Guerra Mundial*, debido a que Gran Bretaña a partir del año de 1938 tuvo a su servicio una gran cadena de antenas de radio (entre los 22 y 28 MHz) en la costa este y sur de la isla, la cual funcionó como el primer radar de vigilancia aérea de la historia, detectando la invasión de aeronaves enemigas, permitiendo así derrotar a la Alemania Nazi en su plan expansivo en este territorio. A este arreglo de antenas se lo conoció con el nombre de *"Chain Home"* **(Sanfuentes) (Braun, 1992)**.

Hoy en día el concepto de GE ha tenido grandes cambios y avances tecnológicos, llegando a englobar cualquier acción militar sobre el uso del *espectro electromagnético*, es decir, toda aquella interacción entre dos o más sistemas que transmiten y/o reciben emisiones de radiofrecuencia con el propósito de utilizar el espectro radioeléctrico en beneficio propio, negando a su vez su uso al oponente **(Gallardo, 2013) (Trobiani, 2008)**.

Con lo ya expuesto no es difícil deducir que en estos tiempos el control del *espectro electromagnético* se ha convertido en un arma poderosa y peligrosa en contra de fuerzas enemigas, razón por la cual en el *Ecuador* el organismo más interesado en explotar este campo son las *Fuerzas Amadas*, especialmente como ayuda para la toma de decisiones a corto plazo. Cabe indicar que para el desarrollo y aplicación de Guerra Electrónica en el país existe una gran dependencia de tecnologías desarrolladas por otros países, creando grandes limitantes económicas e intelectuales para su buen empleo, por lo que sería muy interesante sumar esfuerzos en este ámbito con la elaboración de esta tesis, claro que hay que saber establecer límites en su aplicación.

1.2. JUSTIFICACIÓN E IMPORTANCIA

En la actualidad el bando que conquiste el *espectro electromagnético* habrá conseguido una posición dominante y vital en el desarrollo de los conflictos bélicos o lucha contra otras organizaciones, por tal razón hay gran interés por parte de las *Fuerzas Armadas del Ecuador* por el desarrollo y dominio de la *Guerra Electrónica*. Lamentablemente por el escaso manejo y conocimiento de este concepto existen grandes vacíos teóricos en ciertas definiciones como *Guerra Electrónica* en sí y la *Inteligencia de señales (SIGINT)*, llegando a mezclar sus campos de acción, lo cual se puede comprobar en la doctrina impartida en el *Grupo de Guerra Electrónica del Comando Conjunto de las FF.AA.* y en diferentes tesis relacionadas con el tema que han sido desarrolladas en la *Universidad de Fuerzas Armadas – ESPE*.

Un gran inicio para el *Desarrollo de la GE en el país*, específicamente en las *Medidas de apoyo electrónico (ESM)*, es intervenir en tecnologías nuevas, que tengan una gran aceptación en la región, por tal motivo se ha elegido trabajar con *NXDN*™ , que es una moderna técnica de radio para comunicaciones móviles digitales terrestres que han adoptado los fabricantes *ICOM* y *Kenwood*, quienes son

líderes en el mercado de sistemas de comunicaciones en América **(NXDN Forum Website, 2014) (Mosquera, 2012)**. Algo muy importante de señalar es que gracias a la gran seguridad que brindan los equipos que incorporan esta tecnología, tanto organizaciones lícitas como ilícitas la usan, siendo las principales, compañías de seguridad pública y privada, crimen organizado, cárteles, entre otros, llegando a tener una gran acogida en el mercado latinoamericano de acuerdo al *Boletín Informativo número 22 de SYSCOM de Abril del 2013*.

La elaboración y funcionamiento exitoso de este proyecto se convertirá en la base inicial del *Desarrollo de la GE* basada en *tecnologías de DSP* dentro de la *FF.AA del Ecuador*, para las cuales el conocimiento, la aplicación y el manejo adecuado de este campo es muy necesario y esencial como un arma poderosa en contra del enemigo, puesto que después de haber obtenido la información transmitida por fuerzas opuestas durante este proceso, servirá de herramienta para realizar la SIGINT y la COMINT **(Díaz & Benjamín, 2011) (Adamy, 2011)**. Será un pequeño paso, pero a la vez muy significativo.

1.3. ALCANCE DEL PROYECTO

Con el *diseño, simulación* y *evaluación de* un sistema que permita ejecutar *la monitorización, interceptación y demodulación de una señal digital NXDN™ de voz sin encriptar en tiempo real*, en primer lugar se pretende dar una aclaración y afianzamiento a las *Fuerzas Armadas del Ecuador* sobre conceptos y definiciones de *Guerra Electrónica* e *Inteligencia de Señales*, para que luego puedan realizar su correcta aplicación en el campo de acción, además que busca ser la base para el inicio del *desarrollo de la GE* en esta institución. Como segundo punto, pero en el ámbito personal se intenta afianzar los conocimientos sobre nuevas *tecnologías de telecomunicaciones* y el *procesamiento digital de señales*.

El diseño comienza con la *monitorización* de emisiones de señales que usen el protocolo técnico para comunicaciones móviles *NXDN*™, para después realizar su *interceptación*, todo esto mediante el equipo receptor portátil *R&S®PR100*, el cual es un dispositivo creado por la empresa alemana *Rhode&Schwarz* para aplicaciones de radio monitoreo en el campo, el mismo que se apoya del software *R&S®GX430* **(Rhode&Schwarz, 2014)**, también desarrollado por la misma empresa, para analizar la señal anteriormente interceptada. Con este hardware y software se convierte la señal interceptada a *banda base* mediante *demodulación I/Q (en fase y cuadratura)*, y a través de un algoritmo integrado a estos (generado con la herramienta matemática *MatLab*®) se realizará la *demodulación y ecualización* en *tiempo real* de la misma.

Finalmente para poder entender y escuchar de una manera adecuada el mensaje receptado, se procede a la *decodificación de canal* y *decodificación de fuente* por medio del dispositivo *USB-3000*™ *P25* en su versión estándar **(Digital Voice Systems, Inc., 2014)**. Cabe mencionar que este equipo mencionado permite realizar la codificación y decodificación de fuente con el *vocoder AMBE+2*™ y la codificación y decodificación de canal con *Códigos Golay*, los cuales forman parte del protocolo.

Ya una vez hecho el diseño del sistema se realizará una *simulación en MatLab*® de la *transmisión y recepción de voz sin encriptar* con el *protocolo NXDN*™, para comprender de mejor manera el comportamiento, funcionamiento y desempeño de esta tecnología.

1.4. OBJETIVOS

1.4.1. General

Diseñar, simular y evaluar un sistema para la monitorización, interceptación y demodulación de señales digitales NXDN™ de voz sin encriptar en tiempo real.

1.4.2. Específicos

- Aclarar conceptos y definiciones de Guerra Electrónica (GE) e Inteligencia de Señales (SIGINT).
- Analizar el estándar NXDN™ y los diferentes componentes que lo comprenden de manera teórica.
- Diseñar un sistema para la monitorización, interceptación y demodulación de señales digitales NXDN™ de voz sin encriptar en tiempo real.
- Simular el diseño del sistema para la monitorización, interceptación y demodulación de señales digitales NXDN™ de voz sin encriptar en tiempo real.

CAPÍTULO 2

FUNDAMENTO TEÓRICO

2.1. GUERRA ELECTRÓNICA (GE)

En la guerra moderna todos los niveles y modalidades de combate requieren de equipos electrónicos para la obtención de mejores resultados, por esta razón a la guerra electrónica que es toda actividad tecnológica y electrónica para controlar el espectro radioeléctrico en beneficio propio con la finalidad de neutralizar el ataque enemigo, se la considera como un arma vital en la conducción de las operaciones, puesto que es una acción militar que permite determinar, explotar, reducir o impedir el uso hostil del espectro radioeléctrico por parte del adversario **(Díaz & Benjamín, 2011) (González & Hoyos, 2007)**.

A la guerra electrónica también se le abrevia como *EW*, ya que viene del inglés *Electronic Warfare* y debido al amplio contenido que abarca este tema se la estudia, desarrolla y explota en tres diferentes campos, los cuales se detallan a continuación:

2.1.1. Medidas de apoyo electrónico (ESM o ES)

ESM es la abreviatura tradicional que viene del inglés *Electronic Support Measures* y *ES* es la nomenclatura moderna que viene del inglés *Electronic Support*. Estas medidas son acciones encaminadas a monitorizar (controlar o supervisar) y/o interceptar (intervenir) señales del entorno electromagnético emitidas por el enemigo, para posteriormente poder medir sus parámetros, realizar su análisis, clasificación, registro, localización e incluso la identificación del emisor, proporcionando así una fuente de información necesaria para la toma de decisiones inmediatas relacionadas con las *Contramedidas electrónicas* y las *Medidas de protección electrónica*. Estas pueden ser orientadas tanto para las comunicaciones (*Comms ES*) o también para los radares (*Radar ES*).

Comms ES

Estas medidas se centran en las características de la señal de comunicación transmitida por el enemigo, como su tipo, el nivel de la modulación, la ubicación y movimiento de los transmisores, en sí ayudan a una respuesta táctica rápida una vez que se ha determinado las capacidades del enemigo o inclusive también sus intenciones.

Gracias a esta medida se puede elaborar la *Orden Electrónica de Batalla - Electronic Order of Battle (EOB)* y apoyar a la interferencia de comunicaciones del adversario **(Adamy, 2011)**.

Radar ES

Con estas medidas se monitorean e interceptan las señales emitidas por radares, con el fin de detectar rápidamente cuál de estos pertenecen al enemigo, permitiendo determinar sus comportamientos de uso, además de localizar sus ubicaciones **(Adamy, 2011)**.

2.1.2. Contramedidas electrónicas (ECM o EA)

ECM es la abreviatura tradicional que viene del inglés *Electronic Countermeasures* y *EA* es la nomenclatura moderna que viene del inglés *Electronic Attack*. Estas medidas son acciones que mediante la perturbación, engaño o neutralización del espectro electromagnético del enemigo, buscan reducir o impedir el uso eficaz de este en contra de nuestras fuerzas **(Sistema de observación y prospectiva tecnológica - SOPT, 2009)**.

2.1.3. Medidas de protección electrónica (EPM o EP)

EPM es la abreviatura tradicional que viene del inglés *Electronic Protection Measures* y *EP* es la nomenclatura moderna que viene del inglés *Electronic Protection*. Cabe indicar que anteriormente estas eran conocidas como *Contra-contramedidas Electrónicas* o *ECCM*. Estas medidas son acciones orientadas a asegurar el uso propio del espectro electromagnético a pesar del empleo de las ESM y las ECM por parte del enemigo **(Sistema de observación y prospectiva tecnológica - SOPT, 2009)**.

2.2. RECOPILACIÓN DE INTELIGENCIA

Es una etapa del Ciclo de la Inteligencia en donde se realizan actividades para recolectar información a partir de varias fuentes, tomando en cuenta las prioridades de requerimientos obtenidos en la *fase de planeación* **(Secretaría de Gobernación - SEGOB, 2013)**. Esta se apoya de la *SIGINT, HUMINT, MASINT, GEOINT, OSINT e IMINT*. Ver *Figura 1*.

Figura 1. El Ciclo de Inteligencia

2.2.1. Inteligencia de señales (SIGINT)

La SIGINT proviene del *Ciclo de Inteligencia*, netamente de la *Recopilación de Inteligencia*. Es una actividad mediante la cual se interceptan y analizan señales o comunicaciones transmitidas a través de radiaciones electromagnéticas por parte del enemigo, en donde la información obtenida sirve de ayuda para la toma de decisiones estratégicas a largo plazo. La SIGINT agrupa a *COMINT* y a *ELINT*

(Sistema de observación y prospectiva tecnológica - SOPT, 2009) (Alpha-ES GmbH).

Inteligencia de Comunicaciones (COMINT)

Es el desarrollo de inteligencia a través de la interceptación y análisis de las emisiones realizadas por los *sistemas de comunicaciones* del enemigo. Con COMINT se puede realizar el monitoreo (*búsqueda*) de frecuencias, la interceptación de frecuencias, el registro de señales, la detección de la dirección (*DF - Direction Finding*), entre otras actividades pasivas o silenciosas indetectables por parte del adversario **(González & Hoyos, 2007) (Adamy, 2011)**.

Inteligencia Electrónica (ELINT)

Es el desarrollo de inteligencia y la obtención de información técnica a través de la interceptación y el análisis de las señales emitidas por *sistemas de no comunicaciones* del enemigo, con el propósito de determinar sus capacidades y vulnerabilidades **(Adamy, 2011)**.

2.3. ESM VS. SIGINT

Las ESM apoyan a la toma de decisiones tácticas a corto plazo, mientras que la SIGINT como una actividad para la recolección de inteligencia apoya a la toma de decisiones estratégicas a largo plazo **(Sistema de observación y prospectiva tecnológica - SOPT, 2009)**. Ambas están diseñadas para recibir señales emitidas por el enemigo, pero su diferencia radica en las razones por las que se reciben estas. El ambiente en los que funcionan estos sistemas también marca algunas diferencias

técnicas, como el enfoque de diseño del sistema, el hardware y el software. A continuación se presenta en la *Tabla 1* sus principales diferencias **(Adamy, 2011)**:

Tabla 1.

ESM vs. SIGINT

	Sistemas ESM	Sistemas SIGINT
Misión	**Comms ES:** Identificar y localizar los emisores de comunicaciones enemigas para permitir el desarrollo de la EOB y apoyar la interferencia de comunicaciones. **Radar ES:** Identificar y localizar los radares enemigos para permitir la advertencia de amenazas y apoyar las contramedidas de radar.	**COMINT:** Interceptar las comunicaciones del enemigo y determinar sus capacidades y las intenciones de la información emitida por este. **ELINT:** Encuentra e identifica nuevos tipos de amenazas.
Tiempo	La puntualidad de los resultados es fundamental para la misión.	La puntualidad de los resultados no es demasiado crítico.
Datos recogidos	Reúne solo datos suficientes para determinar el tipo de amenaza, modo de funcionamiento y la ubicación.	Reúne todos los datos posibles sobre las señales recibidas para apoyar su análisis detallado.

Fuente: (Adamy, 2011)

2.4. PROTOCOLO NXDN™

NXDN™ es un *protocolo digital de banda estrecha* para comunicaciones de *radio terrestres móviles* (*LMR*) de *doble vía* o *two-way*, con la capacidad de proporcionar servicios de voz y/o datos por el mismo canal, que ha sido desarrollado y adoptado por los fabricantes *Icom Incorporated* (con su tecnología *IDAS*™) y *JVC KENWOOD Corporation* (con su tecnología *NEXEDGE*®), con la finalidad de cumplir dentro de los Estados Unidos con el *Mandato de la Comisión Federal de Comunicaciones* (*FCC)* sobre *banda estrecha en las bandas de VHF y UHF* que es un requisitos de *eficiencia espectral* **(NXDN Forum Website, 2014).** Cabe señalar que las empresas anteriormente mencionadas son líderes en el mercado de sistemas de comunicaciones en la región y sus equipos son usados tanto por organizaciones lícitas e ilícitas, tales como compañías de seguridad, crimen organizado, cárteles, entre otros, puesto que han tenido una gran acogida en el mercado latinoamericano.

NXDN™ en la actualidad es un protocolo abierto, soportado por el *Foro de NXDN™* o *NXDN-Forum*, el cual está constituido por varias empresas, incluyendo un fabricante de radio y un fabricante testeador **(KENWOOD, 2011)**. Cabe mencionar que los estándares que conforman este protocolo han crecido y madurado bastante, incluyendo diversas soluciones individuales, varios tipos *encriptaciones (DES* y *AES)* y de *Trunking* o *enlace troncal* (Ver *Figura 2*) **(NXDN Forum Website, 2014)**.

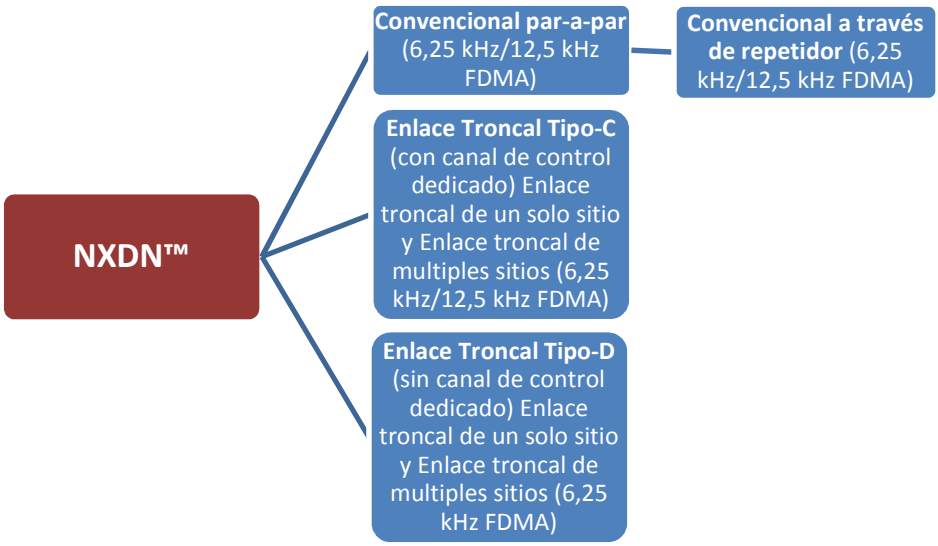


Figura 2. Serie de estructuras del estándar NXDN™
Fuente: (NXDN Forum Website, 2014)

Además NXDN™ comparado con sistemas analógicos cuenta con un mejor *Forward Error Correction (FEC)*, ofreciendo comunicaciones de voz menos susceptibles al ruido y con un alto grado de confidencialidad. Su cobertura es casi similar, pero según pruebas de campo en muchos casos proporciona una huella más ancha con una claridad superior a diferentes intensidades de señal gracias a que tiene una mejor sensibilidad. Ahora los usuarios pueden recibir llamadas en áreas que antes estaban fuera de su alcance, en sí este protocolo reduce las llamadas perdidas y la necesidad de repetición de estas **(KENWOOD, 2011)**. Para un mejor

entendimiento de la calidad de audio y cobertura nos podemos fijar en la *Figura 3* que se presenta a continuación.

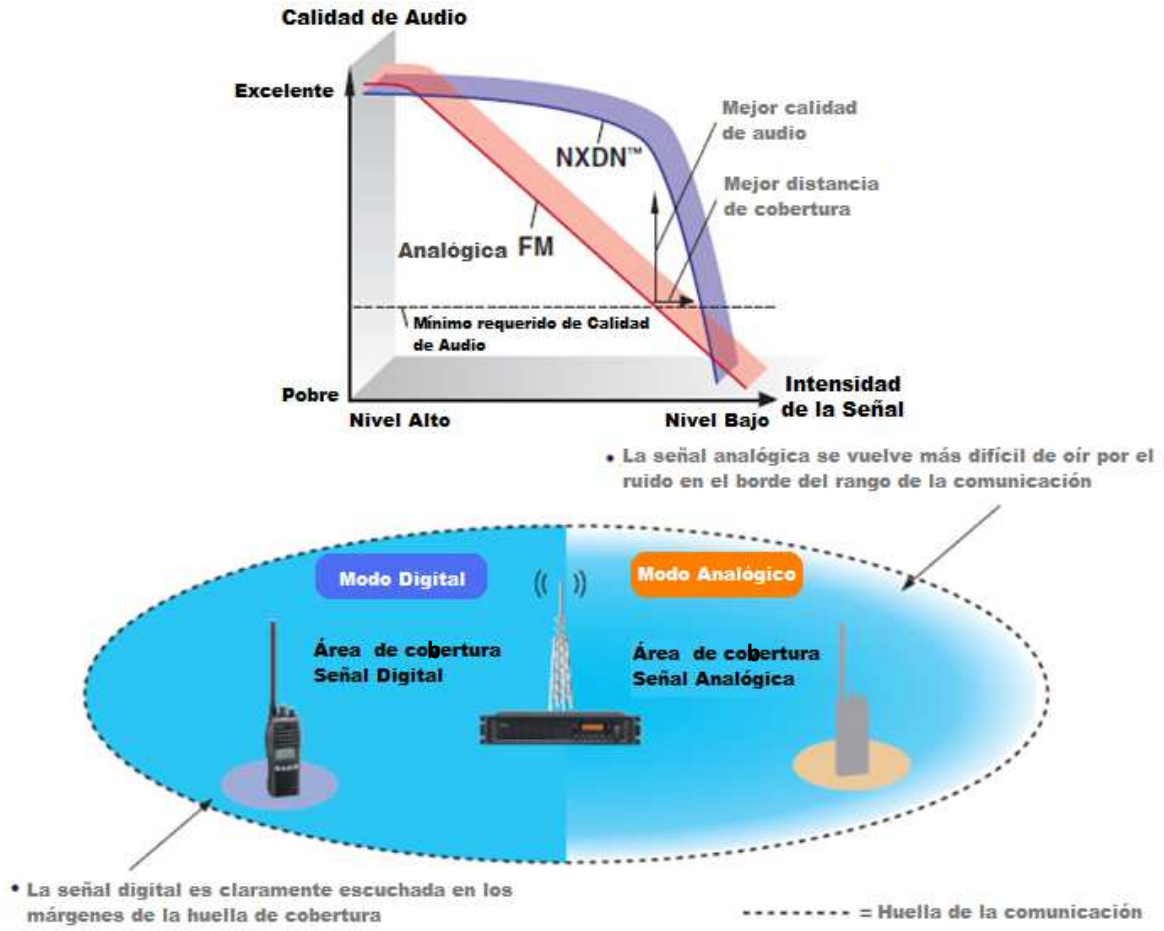


Figura 3. Sistema Analógico vs. NXDN™ - Calidad de Audio y Cobertura
Fuente: (NXDN Forum Website, 2014)

Por la migración a la tecnología digital los primeros productos que salieron fueron radios convencionales y repetidores que tenían la capacidad de "*dual-mode*" para operar en modo digital y analógico a la vez. Hoy en día se cuenta con equipos de fácil uso y reparación puesto que usan componentes más económicos, compatibles con los modelos análogos y de modo mixto.

Este protocolo contiene varias funciones, pero cada fabricante acorde a las necesidades del mercado que va a servir determina cuales va a usar, aunque hay algunas que son obligatorias. Las siguientes son las más comunes: capacidad single-site y multi-site, capacidad de llamada individual y de grupo, funciones de datos (texto corto, GPS y mensajes de estado), *roaming,* un máximo de hasta 60000 identificaciones por sistema y/o capacidad de área amplia de red a través de enlaces IP **(NXDN Forum Website, 2014)**.

2.4.1. Evolución

A continuación se indicará los hechos más relevantes dentro de la evolución del protocolo NXDN™.

- En el año de *1997* la FCC en los EE.UU anunció el mandato de *Relocalización* o *Refarming*, para LMR en las bandas VHF y UHF.
- En el *2003* las empresas de comunicaciones Icom Incorporated y Kenwood Corporation (ahora JVC KENWOOD Corporation) hicieron una alianza tecnológica para desarrollar el protocolo digital de banda estrecha NXDN™.
- En la *International Wireless Communications Expo* del *2005* fue anunciado el desarrollo del protocolo NXDN™.
- Ya para el *2006* los primeros productos NXDN™ fueron lanzados al mercado.
- En el año *2008* se conformó el *Foro de NXDN*™ con ocho empresas miembros. En el posterior año se añadieron cinco nuevas empresas y abrieron el sitio web oficial (*http://www.nxdn-forum.com/*).
- El Foro se amplió a 16 miembros en el *2010*, el mismo que anunció una colaboración informal con la *Asociación dPMR* (estándar abierto europeo que se basa en una tecnología digital similar de 6,25 kHz con FDMA).

- En el *2011* cinco nuevas empresas se unieron al Foro, completando un total de 21 miembros. En este año también se añadieron al protocolo NXDN™ los estándares de *encriptación DES y AES*, y el protocolo de enlace troncal "Tipo-D".
- El foro de NXDN™ en el *2012* alcanzó un total de 30 empresas miembros. Además se renovó su sitio web y se abrió el conjunto de estándares NXDN™ **(NXDN Forum Website, 2014)**.

2.4.2. Especificaciones Técnicas

La plataforma de NXDN™ utiliza un hardware similar a la estructura básica de los diseños de radio analógica FM, pero con una adición de componentes y circuitos de capacidad digital. En la *Tabla 2* se puede diferenciar las diferentes especificaciones técnicas del protocolo digital de banda estrecha NXDN™.

Tabla 2.

Especificaciones Técnicas del Protocolo NXDN™

Método de acceso	FDMA	
Modulación	**Nyquist 4-level FSK**	
Vocoder	**AMBE+2™**	
Ancho de banda del canal	**6,25 kHz**	12.5 kHz
Tasa de transmisión	**4800 bps (2.4ksymbols/s)**	9600 bps
Tasa del codec	**3600 bps (Voz: 2.45 kbps; Corrección de Error: 1.15 kbps)**	7200 bps
Convencional	**Sí**	
Operación de Troncalización	**Sí** **Tipo C y Tipo-D**	Sí Tipo-C
Cifrado digital	**Sí (15-bit/32000 claves)**	
Encriptación	**Sí (AES / DES)**	

Fuente: (NXDN Forum Website, 2014)

La *codificación de fuente* con el *Vocoder AMBE+2*™ es un componente clave en el protocolo de banda estrecha NXDN™, puesto que digitaliza la voz sin perder sus

matices naturales, la comprime, reduce el ruido, además que incluye *codificación FEC (Códigos de Golay)*. Luego, una vez que ya se ha digitalizado el audio, el *procesador digital de señales (DSP)* del radio empaqueta juntos los protocolos del vocoder, señalización, control y más codificación FEC, para que después de pasar por un *filtro transmisor* los paquetes se modulen en una única forma de onda digital *4-level FSK*, transformándose así en una interfaz de aire digital con *baja tasa de error de bits (BER)*, lo cual se traduce en una *comunicación robusta*, inclusive en áreas con débil intensidad de señal. Además esta interfaz de aire encaja dentro de *canales con ancho de banda estrecho de 12,5 kHz o 6,25 kHz*, satisfaciendo así los requisitos de *eficiencia espectral*. En NXDN™ el usuario accede a un canal de frecuencia en cualquier punto en el tiempo con el método *FDMA* **(KENWOOD, 2011)** . Para más información ver *Anexo "A"*.

Vocoder AMBE+2™

El término vocoder significa *codificador/decodificador de voz* y es una parte fundamental de cualquier sistema de radio digital, puesto que convierte la señal analógica de la voz en un flujo digital de bits y viceversa.

El vocoder AMBE+2™ fue desarrollado por *Digital Voice Systems, Inc. (DVSI)* y es un algoritmo de software dentro de un *procesador digital de señales (DSP)* que permite la digitalización de la voz en un flujo compacto de bits sin pérdida de sus matices naturales, transmisión espectralmente eficiente, velocidad de transmisión baja (desde 2,0 hasta 9,6 kbps), buen rendimiento de audio, buen desempeño en entornos ruidosos, además que introduce *codificación FEC* mediante *Códigos de Golay* **(KENWOOD, 2011) (NXDN Forum Website, 2014)**.

Se distinguen dos versiones, la *v 1.4* que fue lanzada en el año 2005, la cual mejora la calidad del audio; y la *v 1.6* que fue lanzada en el año 2009, la cual introdujo mejoras en el rechazo de ruido de fondo de alta frecuencia y mejoras en la capacidad del codificador de voz para transmitir tonos, tales como tonos de señalización telefónica **(Oblak) (Digital Voice Systems, Inc., 2014)**.

Modulación Nyquist 4-level FSK

NXDN™ usa modulación digital no lineal *tipo Nyquist 4-level FSK (Frequency Shift Keying of level 4 - Modulación por Desplazamiento de Frecuencia de nivel 4)* que maneja un esquema de símbolos no correlacionados, es decir, cuando una radio recibe información en un flujo de pulsos binarios los agrupa en *Dibits* (4 combinaciones diferentes), para posterior asignarle a cada combinación un *Símbolo* y una *Frecuencia de Desviación* (Desviación de Frecuencia = 700 kHz) **(NXDN Forum Website, 2014) (Tourrilhes, 2000)**. Ver *Tabla 3*.

Tabla 3.

Esquema de mapeo de símbolos y frecuencias de desviación para la modulación 4 level-FSK en NXDN™

Información (dibit)	Símbolo NXDN™	Frecuencia de Desviación
01	+3	+1050 Hz
00	+1	+350 Hz
10	-1	-350 Hz
11	-3	-1050 Hz

Fuente: (NXDN Forum Website, 2014)

Este tipo de modulación se utiliza a menudo para transmitir datos digitales de forma fiable sobre redes alámbricas y enlaces inalámbricos con tasas de datos bajas.

En la *Figura 4* podemos apreciar el diagrama del proceso de modulación y demodulación del protocolo NXDN™.

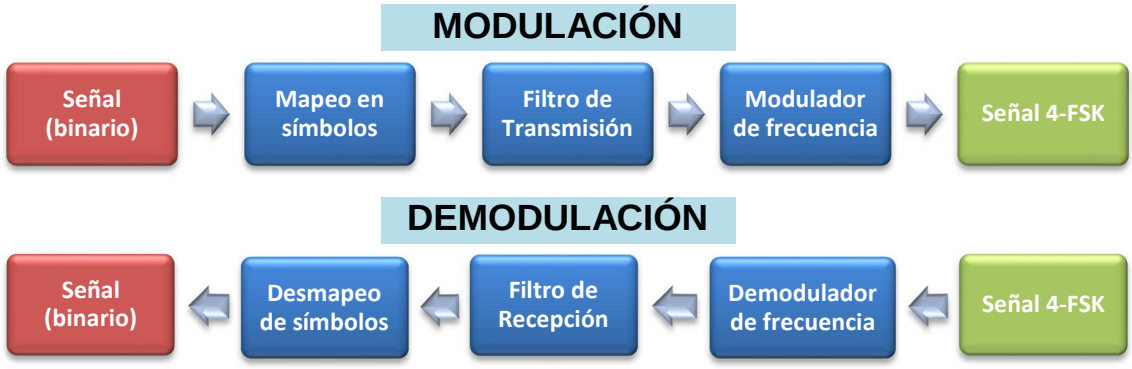


Figura 4. Modulación y demodulación de NXDN™

Método de Acceso FDMA

El *Acceso Múltiple por División de Frecuencias (Frecuency Division Multiple Access - FDMA)* es una técnica de acceso múltiple que divide el ancho de banda de un sistema de comunicación en bandas de frecuencia menores con una separación suficiente entre ellas (*llamada banda de guarda*) para evitar interferencia entre canales adyacentes, lo que permite asignar a cada usuario una banda de frecuencia propia. Cabe indicar que este método no necesita sincronizar a los usuarios para que puedan disponer de un canal **(Shami, Maier, & Assi, 2008)**. En la siguiente *Figura 5* se indica como un ancho de banda es dividido entre N usuarios.

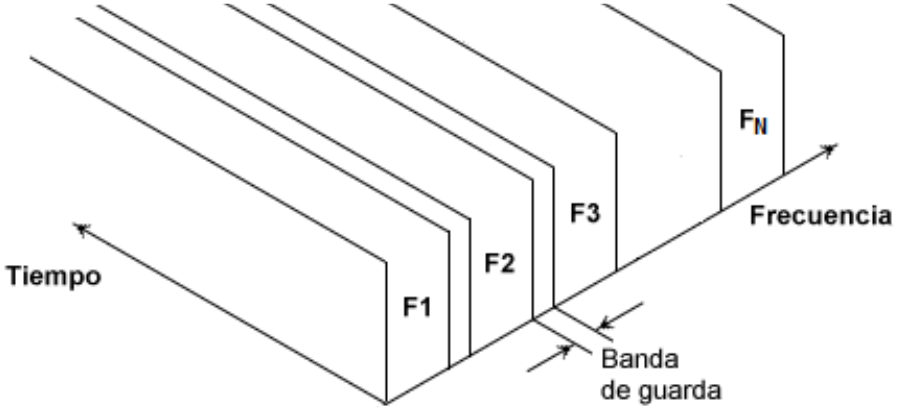


Figura 5. Acceso Múltiple por División de Frecuencias (FDMA)

Enlace Troncal Tipo-C Y Tipo-D

El *enlace troncal tipo-C* es un sistema centralizado que se basa en una arquitectura donde un canal de control dedicado realiza la lógica del enlace troncal y la asignación de canales de tráfico. En cambio el *enlace troncal tipo-D* es un sistema lógico de distribución basado en una arquitectura donde no se utiliza canal de control y todos los canales disponibles en el sistema pueden funcionar como canales de tráfico **(NXDN Forum Website, 2014)**.

Encriptación DES y AES

El *Estándar de Encriptación de Datos (Data Encryption Standard - DES)* es un sistema de cifrado simétrico por bloques de 64 bits, en donde su algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en el cifrado y descifrado de la información **(Kioskea, 2014)**.

El *Estándar de Encriptación Avanzada (Advanced Encryption Standard - AES)* es una técnica de cifrado de clave simétrica que utiliza un algoritmo de cifrado en bloques que permite a la información ser cifrada (convierte los datos en una forma ininteligible llamado texto cifrado) y descifrada (convierte el texto cifrado a su forma original), por tal razón se lo puede utilizar para proteger datos electrónicos. El algoritmo AES es capaz de utilizar llaves criptográficas de 128, 192, y 256 bits para cifrar y descifrar datos en bloques de 128 bits **(National Institute of Standards and Technology - NIST, 2001)**.

DES es remplazado por AES en vista de que en Noviembre del 2001 fue elegido por el *National Institute of Standards and Technology (NIST*) como un *Estándar de Procesos de Información Federal (FIPS-197)* que proporciona una encriptación más segura; además también el Gobierno de EEUU en Junio del 2003 anunció que es un estándar suficientemente seguro para proteger la información clasificada, cuya divulgación pública puede causar daños excepcionalmente graves a la seguridad nacional **(Bitberry Software ApS; Blomsterhaven 42; DK-4300 Holbaek, 2014)**.

2.4.3. Mandato de Banda Estrecha de la FCC

La *Comisión Federal de Comunicaciones (FCC)* de los Estados Unidos de América crea en el año de 1997 el *Mandato de Relocalización o Refarming*, que hoy es conocido como *Mandato de Banda Estrecha o Narrowbanding* para la *LMR* en las bandas de *VHF* y *UHF* (por debajo de 512 MHz), como un requisito de *eficiencia espectral* para que exista un mayor acceso al espectro por parte de los usuarios del sector público y privado, teniendo como fecha límite de su cumplimiento el 1 de enero del 2013 **(Public Safety and Homeland Security Bureau, 2014)**.

Este mandato como primera fase requería el equivalente de al menos un usuario por cada *12,5 kHz para canales de voz o datos,* con una capacidad de al menos 9,6 kbps. Pero la intención de la FCC en la segunda fase era exprimir aún más las bandas de *VHF (de 150 a 174 MHz)* y UHF *(de 421 a 512 MHz*) a al menos *un usuario por cada 6,25 kHz*, lo cual solo se puede conseguir de forma digital **(KENWOOD, 2011)**.

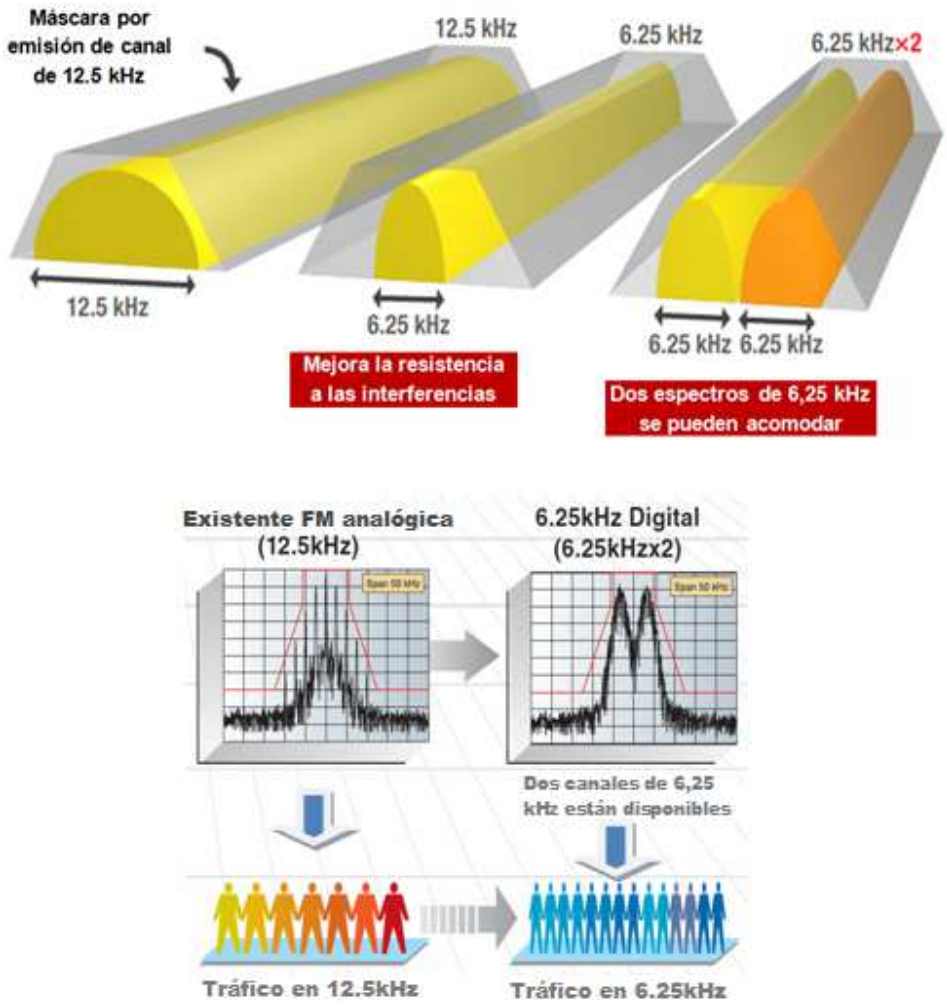


Figura 6. Eficiencia Espectral
Fuente: (KENWOOD, 2011) y (NXDN Forum Website, 2014)

CAPÍTULO 3

DISEÑO DEL SISTEMA PARA LA MONITORIZACIÓN, INTERCEPTACIÓN, DEMODULACIÓN Y DECODIFICACIÓN DE SEÑALES DIGITALES NXDN™ DE VOZ SIN ENCRIPTAR EN TIEMPO REAL

El diseño de este sistema se centra en la parte de la *demodulación del protocolo de banda estrecha NXDN™,* exactamente de las *transmisiones de voz sin encriptar* que usan un *ancho de banda de 6,25 kHz*. Cabe señalar que antes del proceso mencionado se debe emplear las *ESM de Guerra Electrónica* con la finalidad de *monitoriza*r el espectro electromagnético en búsqueda de señales emitidas por fuerzas enemigas que usan esta tecnología de LMR, para luego realizar su *interceptación*. A continuación en la *Tabla 4* se detalla las especificaciones técnicas del protocolo NXDN™ a utilizar en este diseño.

Tabla 4.

Especificaciones técnicas del protocolo NXDN™ con ancho de banda de 6,25 kHz

Método de acceso	FDMA
Modulación	**4-level FSK**
Vocoder	**AMBE+2™**
Ancho de banda del canal	**6,25 kHz**
Tasa de transmisión	**4800 bps (2.4ksymbols/s)**
Tasa del codec	**3600 bps (Voz: 2.45 kbps; Corrección de Error: 1.15 kbps)**
Operación de Troncalización	**Sí (Tipo C y Tipo-D)**
Encriptación	**Sí (AES / DES)**

Fuente: (NXDN Forum Website, 2014)

3.1. APLICACIÓN DE GUERRA ELECTRÓNICA PASIVA EN TIEMPO REAL

Como este trabajo de investigación brinda todos los datos técnicos del protocolo NXDN™, se hace fácil realizar la parte inicial del diseño del sistema, la cual consiste en la aplicación de *Guerra Electrónica pasiva* con dos de las medidas de las *ESM*, que a continuación se las detalla:

3.1.1. Monitorización de una Señal Digital NXDN™

La monitorización es una *medida de las ESM de EW*, que mediante una acción pasiva permite *controlar o supervisar* una señal en haz a través de un monitor. Hay que tener muy en cuenta que en este proyecto se la debe aplicar después de que ya se conoce el lugar en donde transmiten las fuerzas opuestas con el protocolo NXDN™, información que se obtiene con anterioridad, gracias a previas actividades de *recopilación de Inteligencia* realizadas en las ubicaciones próximas a los transmisores del oponente. Ahora, la mejor ubicación para realizar la monitorización debe ser en puntos estratégicos, los cuales se pueden obtener con la ayuda de la *medida de parámetros* de las señales receptadas, que es otra medida de las ESM y cuyo estudio no se realizará en el presente trabajo.

NXDN™ es una *tecnología de radio digital two-way* y como otras de este tipo imponen retos en el monitoreo y detección debido a su estrecho ancho de banda, baja potencia y modulación digital, por tal motivo para realizar Guerra Electrónica pasiva con las ESM en este tipo de tecnología es indispensable utilizar receptores muy sensibles. Para este diseño una excelente opción es el *receptor portátil R&S®PR100* con sus diferentes tipos de *antenas directivas para UHF y VHF*, dispositivos creados por la empresa alemana Rhode&Schwarz, para aplicaciones de radio monitoreo en el campo, que gracias a su tamaño compacto y bajo peso

permiten operar en condiciones duras. Algo muy interesante de resaltar es que opera en una amplia gama de frecuencias desde los 9 kHz a los 7,5 GHz **(Rhode&Schwarz, 2014)**. Ver *Figura 7*, *Figura 8* y *Anexo "A"*.

Figura 7. Receptor Portátil R&S®PR100 y tipos de antenas directivas para diferentes rangos de frecuencias
Fuente: (Rhode&Schwarz, 2014)

Volviendo al diseño, con este dispositivo se pretende realizar un barrido de frecuencias en rangos definidos de *VHF (de 150 a 174 MHz)* y UHF *(de 421 a 512 MHz*), para la radio monitorización del espectro electromagnético en *búsqueda y detección* de emisiones del protocolo NXDN™ realizadas por parte del enemigo, lo cual se logra cuando la señal excede el nivel predefinido del umbral. Algo muy importante de indicar es que cuando ya se conoce el rango exacto en que opera el oponente se puede efectuar un escaneo o barrido de frecuencias más selectivo, es decir, *búsqueda y clasificación automática,* lo cual se consigue con el equipo anteriormente mencionado en su modo de control remoto (*R&S®PR100-RC*), con

apoyo del *software R&S®GX430*, que también es desarrollado también por la empresa Rhode&Schwarz, **(Rhode&Schwarz, 2014)**. Ver *Figura 9*.

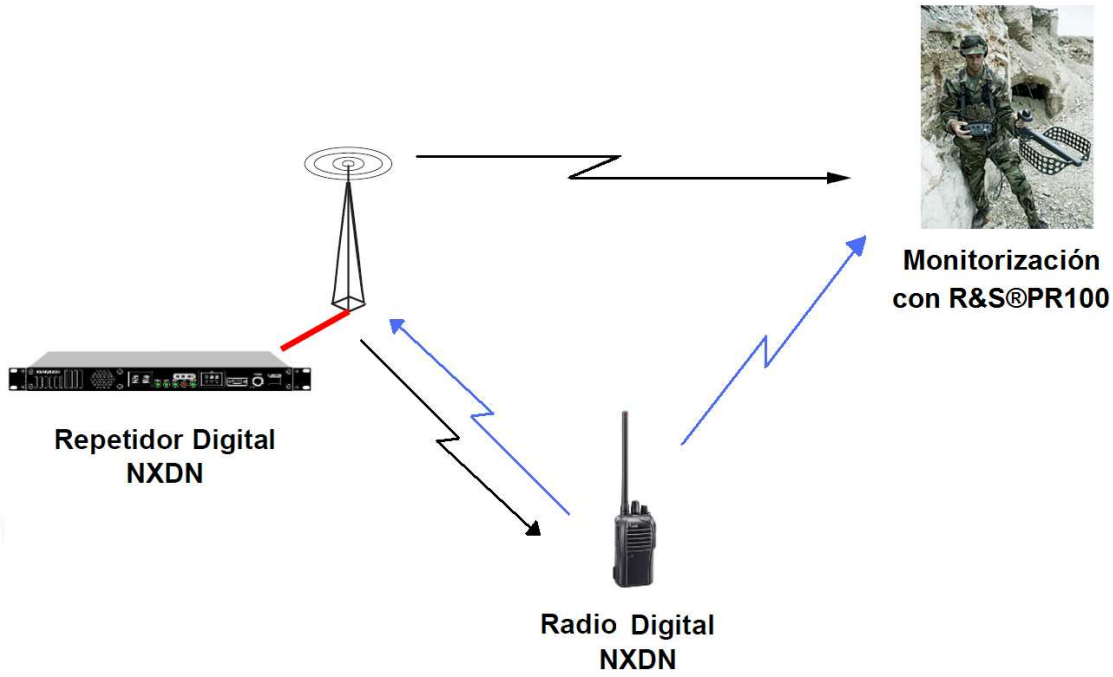


Figura 8. Monitorización con el Receptor Portátil R&S®PR100 de emisiones del protocolo NXDN™

Figura 9. Comunicación entre el R&S®PR100-RC y el software R&S®GX430
Fuente: (Rhode&Schwarz, 2014)

Monitorización en Tiempo Real de una Señal con el Protocolo NXDN™

Una vez que ya se encuentra localizado el sector en donde opera el enemigo y se conoce el rango de frecuencias que usan para la emisión de señales con el protocolo NXDN™, se procede a la *monitorización automática* con la ayuda del *receptor portátil R&S®PR100-RC* y el *software R&S®GX430* **(infodefensa.com)**. Este hardware y software permiten de una forma gráfica ver el espectro de la señal, el tipo de modulación y nivel de la misma (4-level FSK), ancho de banda (6,249073 kHz), frecuencia mínima (-3,091179 kHz) y frecuencia máxima (3,157895 kHz). Ver *Figura 10*.

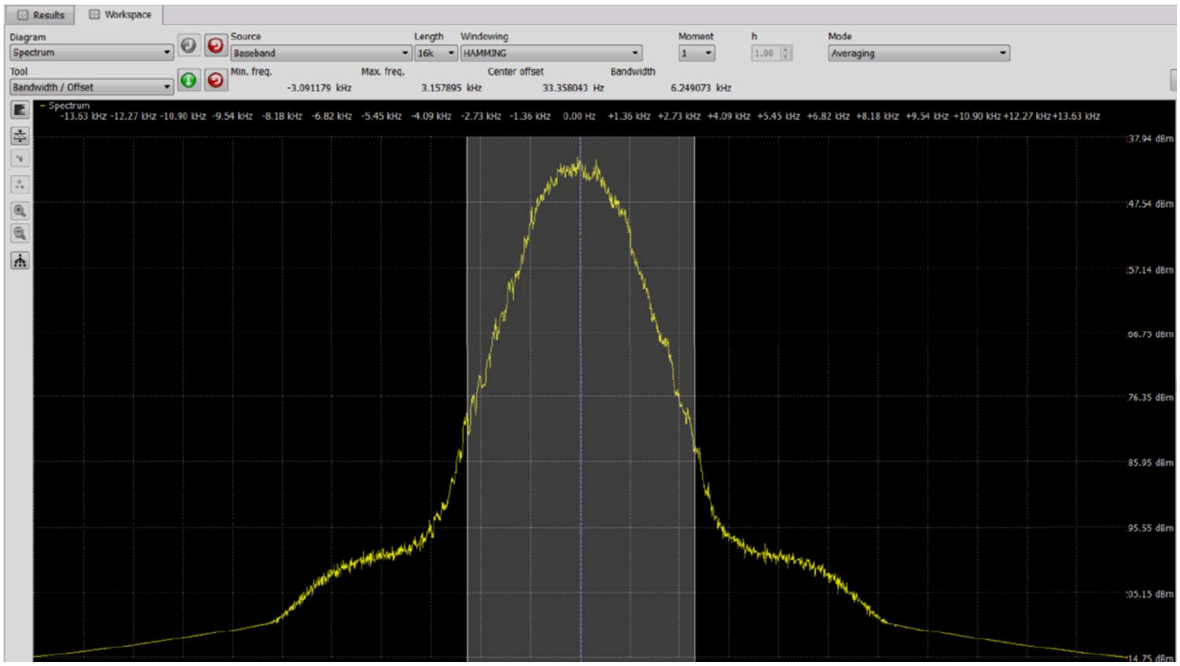


Figura 10. Diagrama del espectro de la señal NXDN™ Monitorizada, Frecuencia (eje de las abscisas) vs. Potencia de la señal (eje de las ordenadas)

En la *Figura 10* también se puede apreciar que en el espectro de la señal NXDN™ monitorizada no se pueden diferenciar las portadoras.

3.1.2. Interceptación de una Señal Digital NXDN™

Una vez realizada la monitorización se prosigue con la interceptación de las señales enemigas. Entiéndase a esta medida de las ESM de EW como una acción de *intervenir, participar o actuar de una forma entrometida y determinada dentro de un proceso de transmisión electromagnética enemiga*.

Este proceso también se lo realiza mediante el empleo del equipo *receptor portátil R&S®PR100-RC* y el *software R&S®GX430*, para descomponer en *tiempo real* la *envolvente compleja de la señal interceptada* en *datos de fase y cuadratura (demodulación IQ)* **(Rhode&Schwarz, 2014)**.

Esta parte del diseño se lo podría realizar solo con el equipo receptor, sin embargo el *software R&S®GX430* brinda una *librería* o *API de integración* para insertar algoritmos dentro del mismo, capacidad que se aprovecha en el paso siguiente del proyecto para integrar en una función de la librería el *Script de MatLab®* creado para la *demodulación, decodificación y escucha de la señal interceptada*, la misma que será llamada periódicamente siempre que los datos IQ estén disponibles. Ver *Figura 11*.

Para un mejor conocimiento, empleo y manejo del receptor portátil R&S®PR100 y del software R&S®GX430 es recomendable apoyarse del *Anexo "B"*.

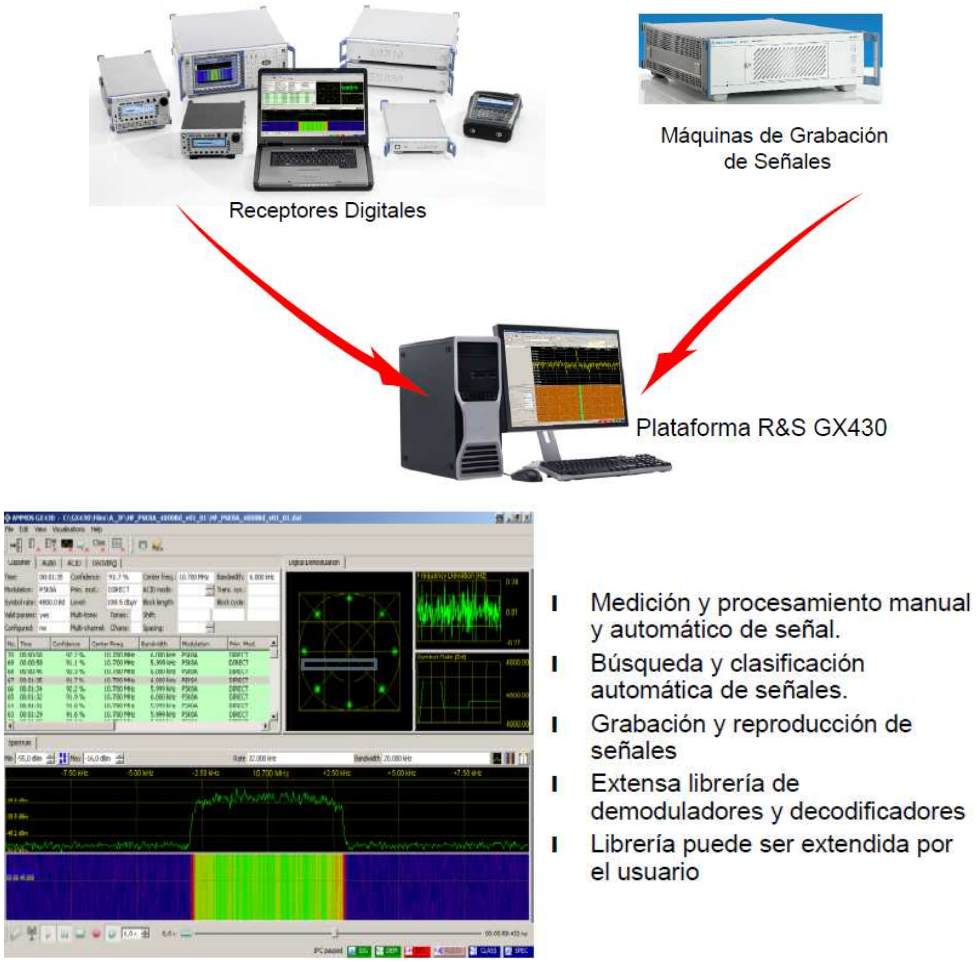


Figura 11. Características principales de la plataforma R&S®GX430
Fuente: (Rhode&Schwarz, 2014)

Interceptación en Tiempo Real de la Señal Monitorizada

Una vez que se han detectado emisiones del protocolo NXDN™ por parte del enemigo se procede a la *interceptación* de estas señales con la ayuda del *receptor portátil R&S®PR100-RC* y el *software R&S®GX430, para su posterior demodulación IQ* en *tiempo real.*

El software también permite ver el *diagrama de la frecuencia instantánea de la señal NXDN™*, donde se puede apreciar de una mejor manera a las cuatro diferentes portadoras de -1050, -350, 350 y 1050 Hz, aunque no están del todo separadas debido al ISI. Ver *parte central derecha de la Figura 12*.

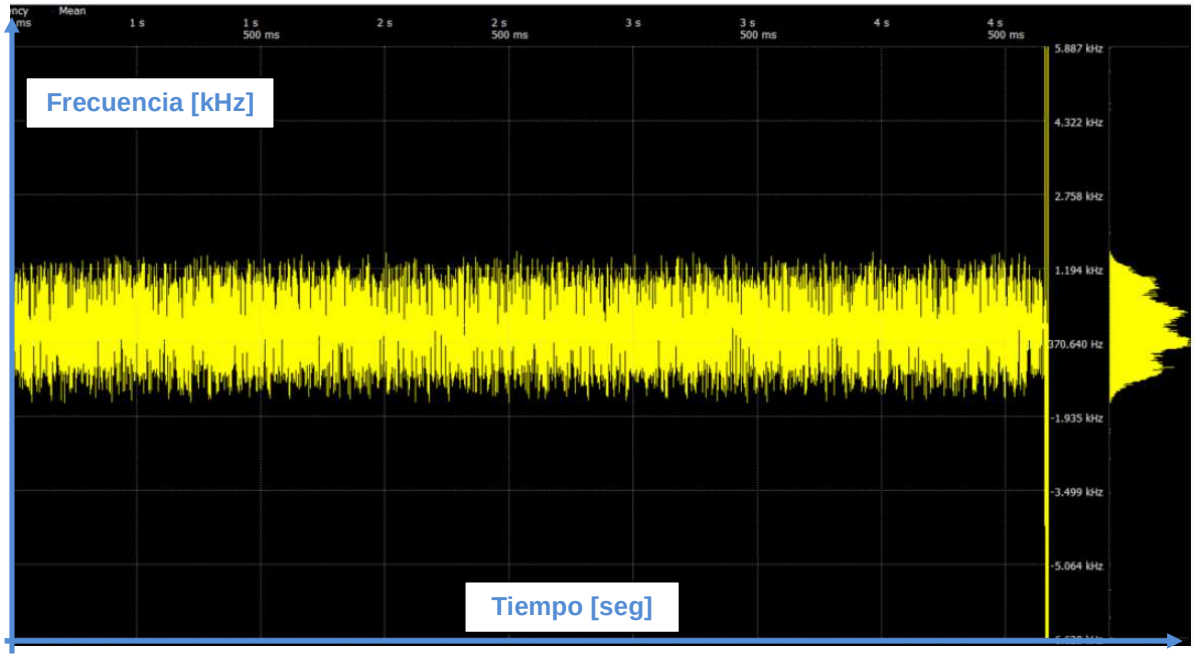


Figura 12. Diagrama de la Frecuencia Instantánea de la señal NXDN™ interceptada

3.2. DEMODULACIÓN EN TIEMPO REAL DE LA SEÑAL INTERCEPTADA

Como segunda parte en el diseño de este proyecto de tesis se tiene la *demodulación en tiempo real* de la señal enemiga interceptada, mediante la ayuda del *software matemático MatLab®*. En la *Figura 13* se puede distinguir los diferentes procesos a seguir, los mismos que serán detallados posteriormente:

Figura 13. Demodulación de NXDN™
Fuente: (NXDN Forum Website, 2014)

3.2.1. Demodulación 4 level-FSK de la Señal Interceptada

En vista que la señal interceptada *(envolvente compleja)* está en *datos IQ*, se procede a realizar su *demodulación 4 level-FSK* con el software MatLab®, mediante un detector de frecuencia, ya sea generando el código de este o usando una función propia de la herramienta matemática, para lo cual se vale de los datos que contienen la *Tabla 3* y *Tabla 4*.

A la salida de este paso se obtendrá la misma señal interceptada pero en su representación de símbolos.

3.2.2. Ecualización de la Señal Demodulada

Por diseño el sistema del protocolo NXDN™ para mejorar la *eficiencia espectral* ocasiona una considerable *interferencia entre símbolos (ISI)*, por tal motivo es necesario incorporar un *ecualizador en la recepción* para compensarla. Hay que tener en cuenta que la ISI puede ser causada por distorsión de amplitud o de fase, problemas de sincronismo o limitación del ancho de banda del canal.

El ecualizador consiste en crear un *filtro de coseno levantado en la recepción* con la *herramienta matemática MatLab®,* con la finalidad de compensar la *ISI* que tiene incorporada la señal obtenida mediante la interceptación, o también se puede usar funciones propias del software, claro que hay que adaptarle con las características técnicas del protocolo.

A continuación en la *Figura 14* se indica el diagrama de recepción con el protocolo NXDN™ y las funciones de transferencia de los filtros usados en dicha tecnología **(NXDN Forum, 2012)**.

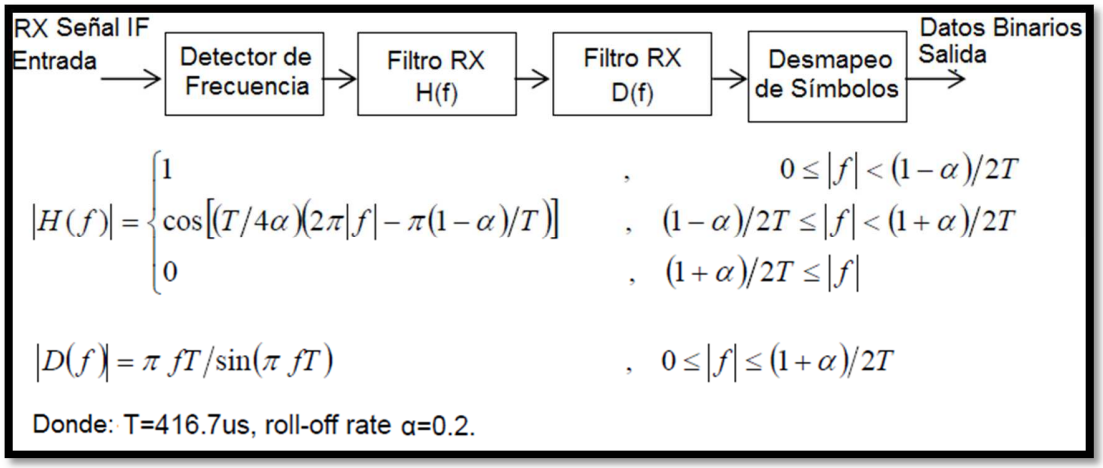


Figura 14. Diagrama del Demodulador 4-FSK de NXDN™ y Funciones de Transferencia de los Filtros en la recepción
Fuente: (NXDN Forum Website, 2014)

3.2.3. Desmapeo de Símbolos

En este paso se realiza el *desmapeo de símbolos (conversión de los símbolos* a *dibits),* como se muestra en la *Tabla 3*.

Cabe señalar que la secuencia de *datos binarios* obtenida en esta etapa aún necesita ser introducida a un proceso de *decodificación de canal* y *decodificación de fuente,* para poder escuchar el audio transmitido dentro de la señal interceptada **(NXDN Forum Website, 2014)**.

3.3. DECODIFICACIÓN DE CANAL DE LA SEÑAL

Este proceso inicia con la *sincronización* de la señal con la ayuda del *Preamble* y el *FSW (Frame Synchronization Word)*, para finalmente efectuar el *desempaquetamiento de los paquetes de voz sin encriptar.* Ver *Figura 15* y *Figura 16*. Todo este proceso se encuentra bien detallado en el documento técnico *"NXDN TS 1-E Version 1.1".*

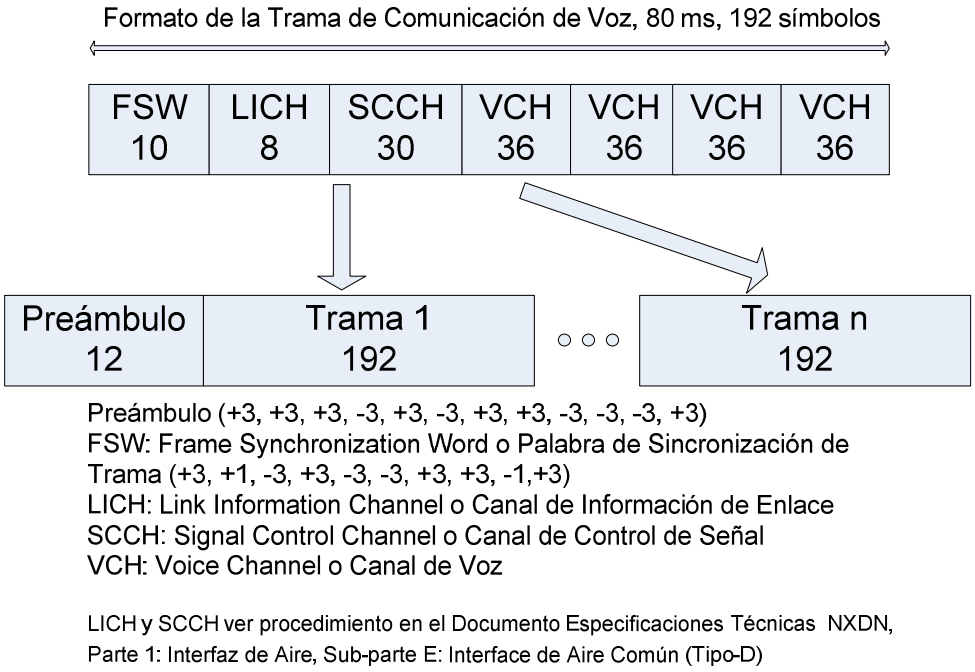
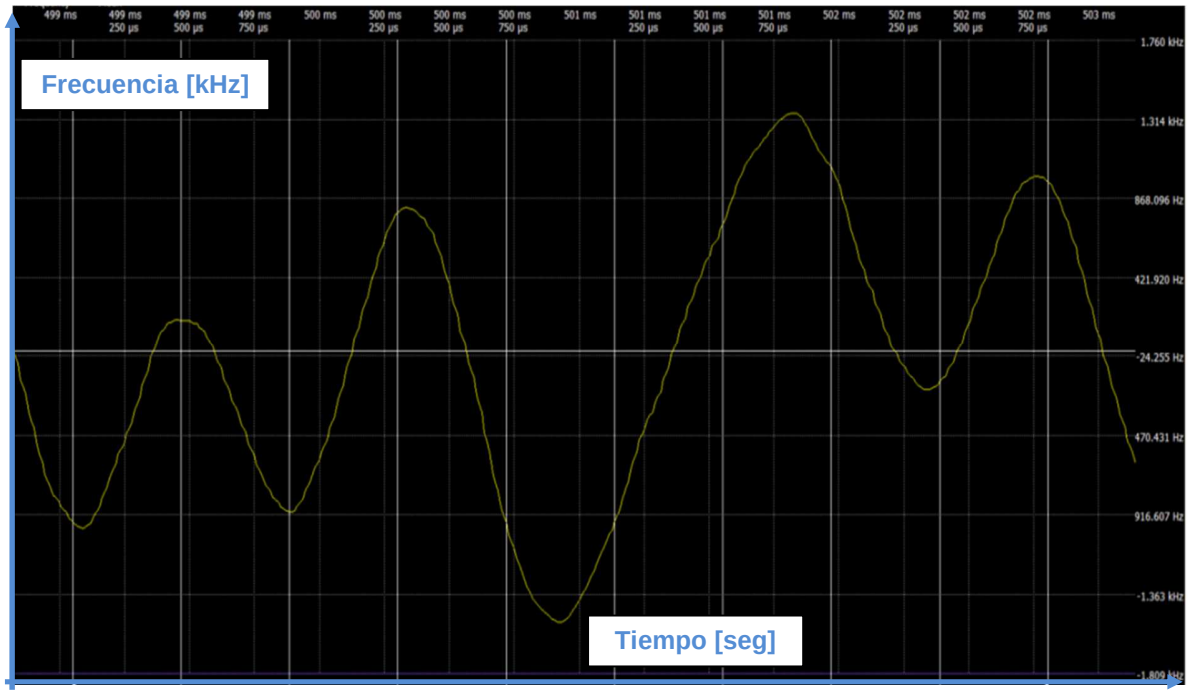


Figura 15. Estructura de la Trama de Comunicación de Voz en el protocolo NXDN™
Fuente: (NXDN Forum Website, 2014)



Symbol	-3, +1, -3, +3, -3, -3, +3, +3, -1, +3
HEX	CDF59

Figura 16. FSW en el Diagrama de la Frecuencia Instantánea de la señal NXDN™ interceptada

3.4. DECODIFICACIÓN DE FUENTE DE LA SEÑAL

Una vez que la señal se encuentra demodulada, ecualizada, sincronizada y desmapeada se procede con la *decodificación de fuente* de la misma, con la ayuda del dispositivo *USB-3000™ P25 en su versión estándar (hardware vía interfaz de USB)* y la *herramienta matemática MatLab®.* Hay que tener en cuenta que equipo anteriormente mencionado permite realizar la *codificación y decodificación de fuente* con el *vocoder AMBE+2™*, el mismo que incorpora *FEC* mediante *Códigos de Golay* **(Digital Voice Systems, Inc., 2014)**.

Antes de empezar con este proceso se debe instalar correctamente el aparato en una PC que tenga el *sistema operativo Windows® XP o Windows Vista®*, acorde como lo indica su *manual de usuario*, primero verificando en el *Administrador de Dispositivos* el puerto con que se realizará la comunicación USB-PC (*Serial Port COMXX*) y luego comprobando su correcto funcionamiento en una *ventana de Command Prompt* con las instrucciones *usb3kverify.bat* y *usb3kversion.bat* dentro del directorio *C:/usb3000/bin* **(Digital Voice Systems, Inc., 2014)**. Ver *Figura 17*, *Figura 18*, *Figura 19* y *Manual de Usuario* del *USB-3000™ P25 en su versión estándar.*

Esta tesis la instalación se realizó en *Windows Vista®*, puesto que *Windows® XP* perdió el soporte técnico que le brindaba la empresa Microsoft®.

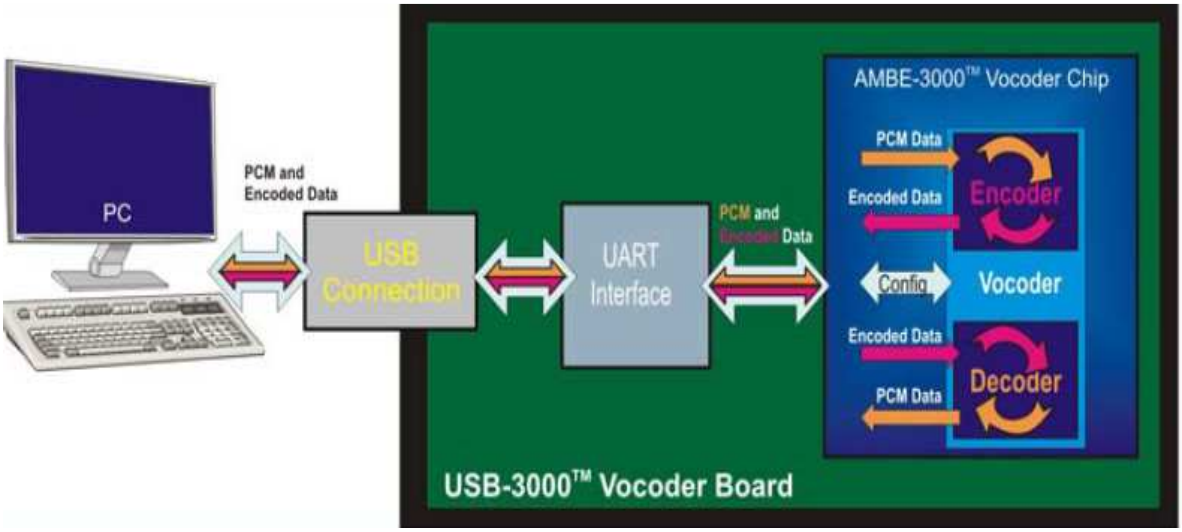


Figura 17. Diagrama de bloques del USB-3000™
Fuente: (Digital Voice Systems, Inc., 2014)

UART Baud Rates	Switch Position 1	Switch Position 2	Switch Position 3	Switch Position 4 (Not Used)
28,800	ON	ON	ON	OFF
57,600	ON	ON	OFF	OFF
115,200	ON	OFF	ON	OFF
230,400	ON	OFF	OFF	OFF
460,800	OFF	ON	ON	OFF

DVSI strongly recommends using the default COM Port Baud rate of 460,800 baud.

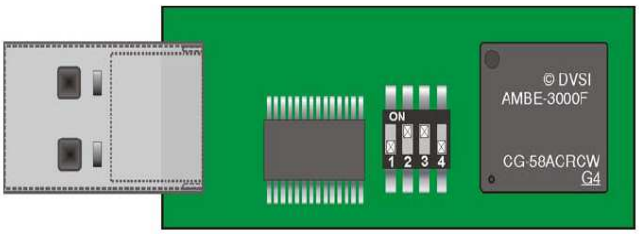


Figura 18. Default Switch settings (460,800 Baud) del USB-3000™ P25
Fuente: (Digital Voice Systems, Inc., 2014)

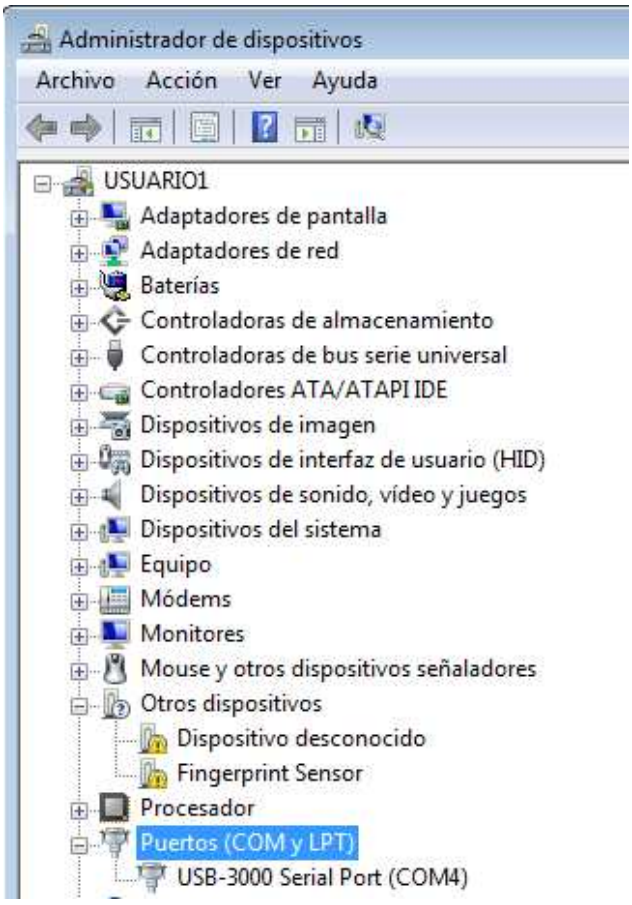


Figura 19. Verificación del Serial Port COM del USB-300

Para la *decodificación* se debe ejecutar el software *usb3kcom.exe* en una *ventana de Command Prompt* dentro del directorio *C:/usb3000/bin*, de la siguiente manera, ver *Figura 20*.

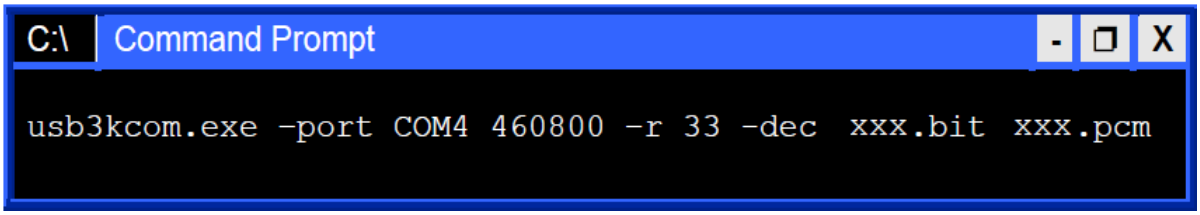


Figura 20. Instrucción para decodificar a 3600bps (Voz: 2.45 kbps y Corrección de Error: 1.15 kbps)

Donde:

COM4	Es el *COM Port* de la PC con que se comunica con el USB-3000™ P25.
460800	Es la velocidad de transmisión en baudios de la conexión con la PC.
-r 33	Es el *Rate Index* que indica la velocidad a la que el archivo ".bit" va a ser decodificado (3600bps; voz: 2.45 kbps y corrección de errores: 1.15 kbps).
-dec	Modo decodificación.
xxx.bit	Es el nombre del archivo que va a ser decodificado.
xxx.pcm	Es el nombre del archivo donde se guardará lo decodificado.

El proceso detallado se lo puede realizar mediante MatLab®, ejecutando el software *usb3kcom.exe* dentro del mismo, de la siguiente manera: *"!usb3kcom.exe -port COM4 460800 -r 33 -enc C:\usb3000\tv\xxx.pcm xxx.bit"*.

Ahora si la señal de voz transmitida por el oponente esta *encriptada*, la única manera de *desencriptarla* es siguiendo los siguientes pasos: primero remover el FEC, luego realizar la desencriptación (*sea AES o DES*) y por último descomprimir la señal. Esta parte no se realizará en el presente trabajo.

Para un mejor entendimiento del protocolo NXDN™ es recomendable revisar la información en el *Anexo "A"* y *Anexo "B"*. Además de los documentos técnicos: *NXDN™ Technical Specifications 1-E Version 1.1*, *NXDN™ Technical Specifications 1-A Version 1.3* y *NXDN™ Technical Specifications 1-B Version 1.3*.

CAPÍTULO 4

SIMULACIÓN EN MATLAB® DE LA TRANSMISIÓN Y RECEPCIÓN CON EL PROTOCOLO NXDN™

Para comprender mejor como funciona y se comporta esta tecnología, se realizó una simulación de la transmisión y recepción usando el protocolo digital de banda estrecha para comunicaciones de radio móviles terrestres de doble vía NXDN™ mediante el *software MatLab*®. La *Figura 21* muestra la estructura de la simulación.

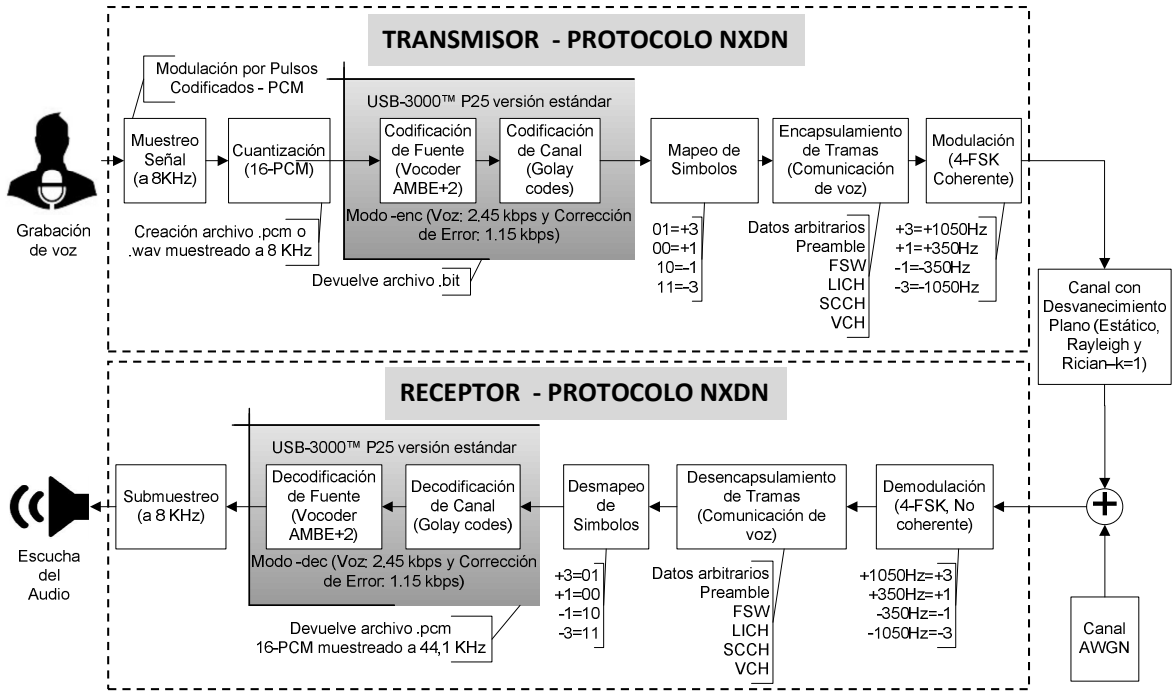


Figura 21. Simulación de la Transmisión y la Recepción con el Protocolo NXDN™

4.1. MUESTREO Y CUANTIFICACIÓN

Mediante la *tarjeta de audio (micrófono),* controlada por el software MatLab® se graba un audio en un archivo *".pcm",* con un muestreo y una cuantificación *PCM de 16 bits* respectivamente y una frecuencia de muestreo de *8 kHz*.

4.2. CODIFICACIÓN Y DECODIFICACIÓN

Posterior se realiza la etapa de *codificación de fuente (vocoder AMBE+2™)* y *codificación de canal (Golay Codes)* mediante el dispositivo USB-3000™ P25 en su versión estándar (su software es propietario), con un *Rate Index de 33 (Codec Rate=3600bps – Voz=2.45 kbps y Corrección de Errores=1.15 kbps)*, el mismo que es controlado por el software MatLab®. Para la etapa de *decodificación de fuente* y *decodificación de canal* se utiliza el mismo equipo.

4.2.1. Análisis del Equipo USB-3000™ P25 en su Versión Estándar

Después de realizar pruebas de codificación y decodificación con el equipo se puede observar que el dispositivo con el *software de fábrica (usb3kcom.exe)* en su *modo de codificación "-enc"* solo permite realizar la codificación de fuente y la codificación de canal de un archivo de audio ".pcm" o también de un archivo de voz ".wav" en un archivo ".bit", mas no la encriptación del audio; además que en su *modo de decodificación "-dec"* permite realizar la decodificación de fuente y la decodificación de canal de un archivo ".bit" en un archivo ".pcm", mas no la desencriptación del archivo ".bit". Cabe señalar que si se desea realizar el proceso de encriptación y de desencriptación se debe realizar modificaciones en el código fuente que está en el archivo "usb3kcom.c", como se muestra en la *Figura 22*.

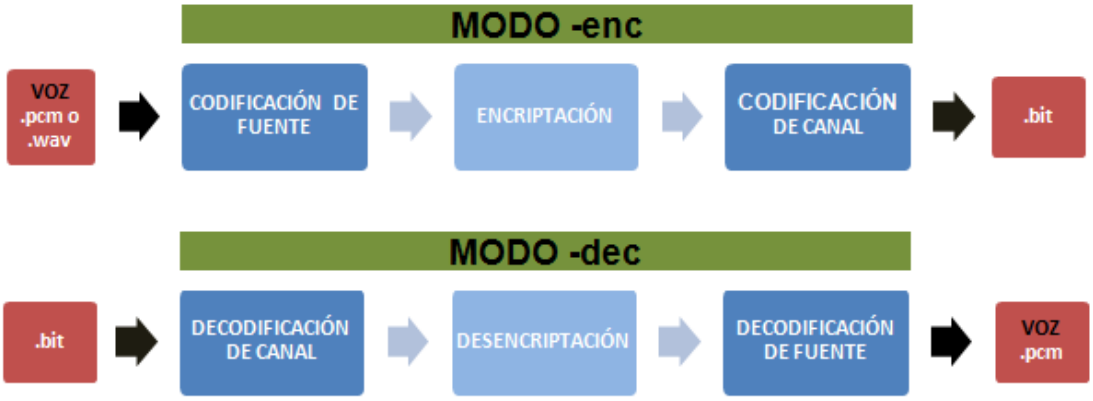


Figura 22. Modificación del software del USB-3000™ P25 para la Encriptación y Desencriptación

En este proyecto no se necesita realizar modificación alguna en el código fuente del software de control del dispositivo, puesto que solo está diseñado para comunicaciones que usan el protocolo NXDN™ y no están encriptadas.

Para un mejor entendimiento de cómo trabaja el USB-3000™ P25 se realizaron las siguientes pruebas:

1. Con la ayuda de MatLab® se crea cuatro archivos de audio ".pcm" de una señal senoidal *"sin(2π*500*t)"* (ver *Figura 23*), con una resolución de muestreo PCM de 16 bits; el primero *"mono_Ori.pcm"* con una señal mono y una frecuencia de muestreo de 8 kHz; el segundo *"mono1_Ori.pcm"* con una señal mono y una frecuencia de muestreo de 44,1 kHz; el tercero *"stereo_Ori.pcm"* con una señal estéreo sin desfase y una frecuencia de muestreo de 8 kHz; y el cuarto *"stereo1_Ori.pcm"* con una señal estéreo sin desfase y una frecuencia de muestreo de 44,1 kHz.

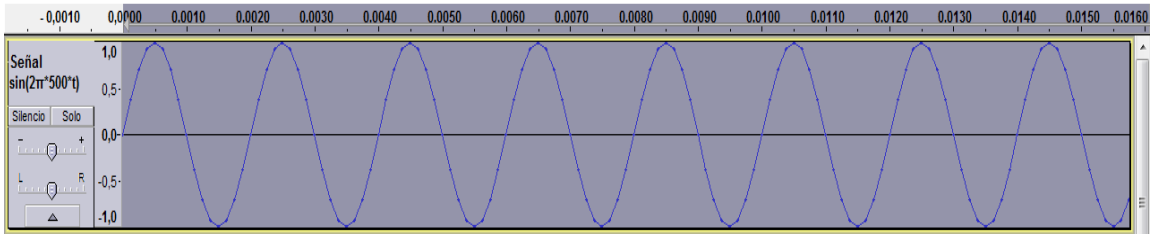


Figura 23. Señal senoidal sin(2π*500*t)

2. Posterior se realiza la codificación y decodificación de los cuatro archivos de audio ".pcm" con el equipo USB-3000™ P25 en su versión estándar con un *rate index* de 33, obteniendo cuatro archivos *(mono.pcm, mono1.pcm, stereo.pcm y stereo1.pcm)*, todos de audio estéreo, con una resolución de muestreo PCM de 16 bits y una frecuencia de muestreo de 44,1 kHz. Se puede observar mejor los resultados gráficamente gracias al *software Audacity*®, ya que este permite ver la forma de onda de las señales de los archivos de audio.

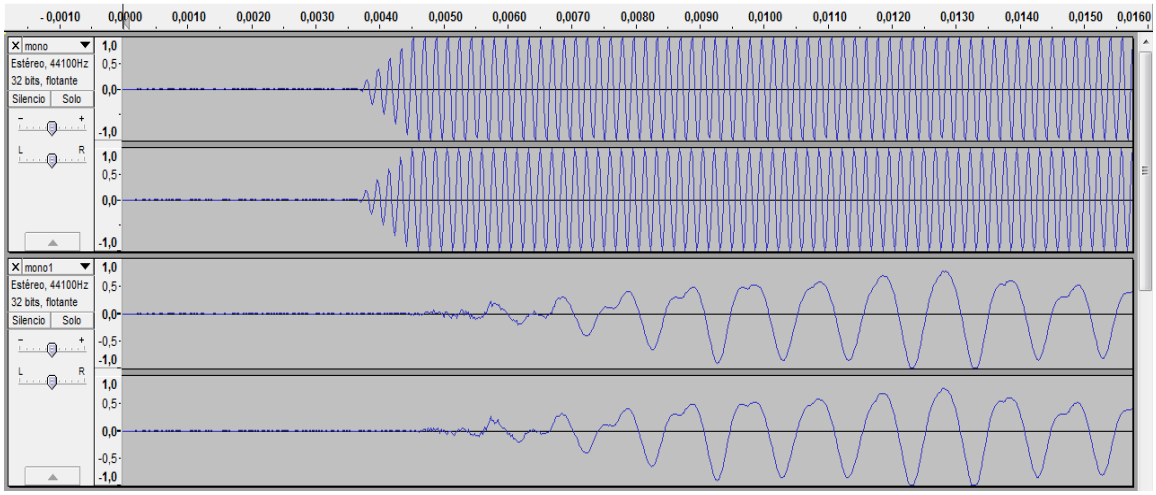


Figura 24. Vista en Audacity® de mono.pcm y mono1.pcm

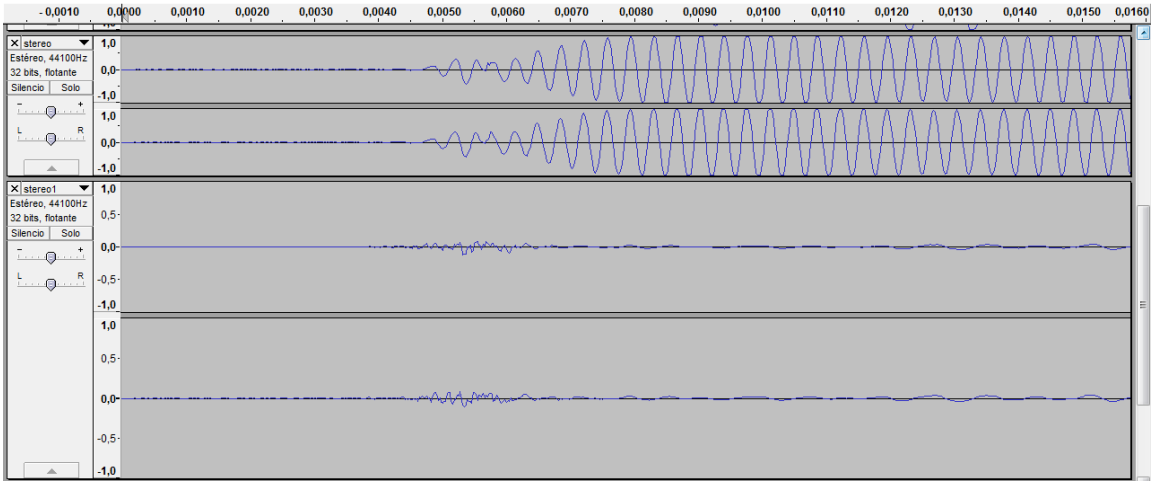


Figura 25. Vista en Audacity® de stereo.pcm y stereo1.pcm

3. Con el *software Toolsoft Audio Manager* se pueden escuchar los archivos ".pcm" y reconocer sus diferencias audibles, además que presenta todas sus propiedades, lo cual se detalla en la *Tabla 5*.

Tabla 5.

Archivos de audio originales vs. Archicos codificados y decodificados con el USB-3000™ P25

Archivos Originales						
Nombre	**Tipo Archivo**	**Resolución Muestreo**	**Número Canales**	**Frecuencia Muestreo**	**Tamaño Archivo**	**Duración**
mono_Ori	PCM	16 bits	Mono	8 kHz	31,2 kB	2'
mono1_Ori	PCM	16 bits	Mono	44,1 kHz	172 kB	2'
stereo_Ori	PCM	16 bits	Estéreo	8 kHz	62,5 kB	2'
stereo1_Ori	PCM	16 bits	Estéreo	44,1 kHz	344 kB	2'
Archivos Codificados y Decodificados con el Equipo USB-3000™ P25 - Versión Estándar						
Nombre	**Tipo Archivo**	**Resolución Muestreo**	**Número Canales**	**Frecuencia Muestreo**	**Tamaño Archivo**	**Duración**
mono	PCM	16 bits	Estéreo	44,1 kHz	31,5 kB	0,183'
mono1	PCM	16 bits	Estéreo	44,1 kHz	172 kB	1,001'
stereo	PCM	16 bits	Estéreo	44,1 kHz	62,8 kB	0,364'
stereo1	PCM	16 bits	Estéreo	44,1 kHz	344 kB	2'

Los resultados que nos brindan estos dos software en la *Figura 24*, *Figura 25* y *Tabla 6*, indican que el archivo que va a ser codificado y decodificado con el equipo USB-3000™ P25 en su versión estándar debe ser estéreo y

no mono, puesto que este equipo siempre a su salida dará un archivo de audio *estéreo* con una resolución de muestreo PCM de 16 bits. También indica que debe ser muestreado a una frecuencia de 44,1 kHz, pero hay un inconveniente, que muestreado a esta frecuencia sufre mucha distorsión la señal de audio, además que la amplitud disminuye notablemente, aunque esto último es solucionable. Ahora la que se muestrea a 8 kHz no sufre mucha distorsión de la señal (poco solo al principio), pero el gran inconveniente es que varía bastante su tiempo de duración.

4. Como aun presenta dificultades la elección de la frecuencia de muestreo, se realiza otra prueba con los software MatLab® y Audacity®, que consiste en crear otros dos archivos de audio estéreo ".pcm" de la frase *"esta es una prueba de sonido"*, con una resolución de muestreo PCM de 16 bits. El primero *"pruebavoz.pcm"* con una frecuencia de muestreo de 8 kHz, mientras que el segundo *"pruebavoz1.pcm"* con una de 44,1 kHz, obteniendo después del proceso de codificación y decodificación con el equipo los archivos *"voz.pcm"* y *"voz1.pcm"* respectivamente.

   Al escuchar los dos audios originales se puede apreciar que el que tiene una frecuencia de muestreo de 44,1 kHz presenta una mejor calidad de audio que la que tiene una de 8 kHz.

   Al instante de pasar estos dos audios por el proceso de codificación y decodificación se aprecia que "voz.pcm" esta *sobre muestreado*, mientras que "voz1.pcm" es muy similar al original, pero este último al momento de escucharlo presenta mucha distorsión de la señal, además que la voz se escucha muy sintetizada. Ver *Figura 26* y *Figura 27*.

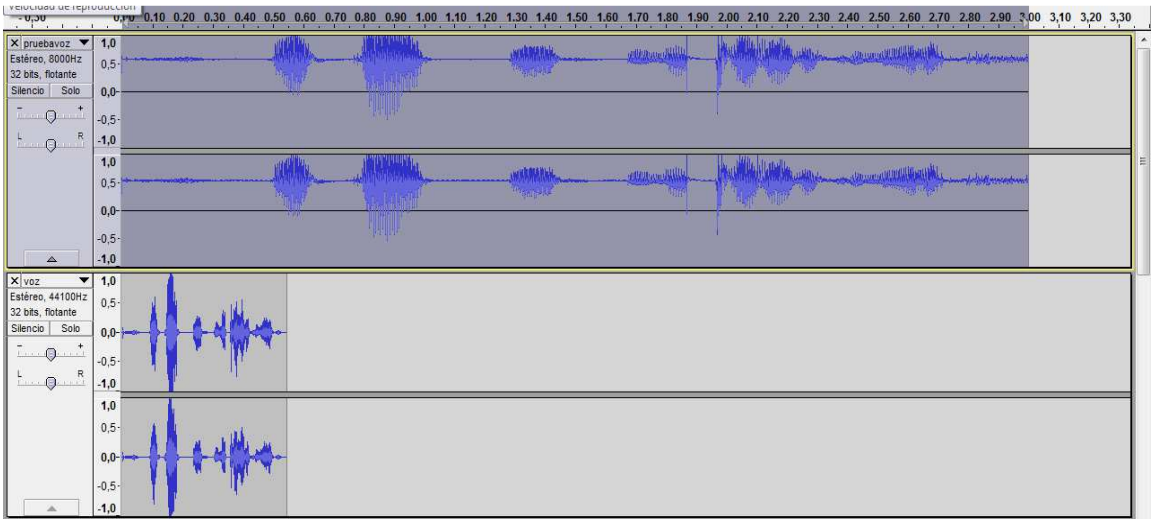


Figura 26 . Vista en Audacity® de pruebavoz.pcm y voz.pcm

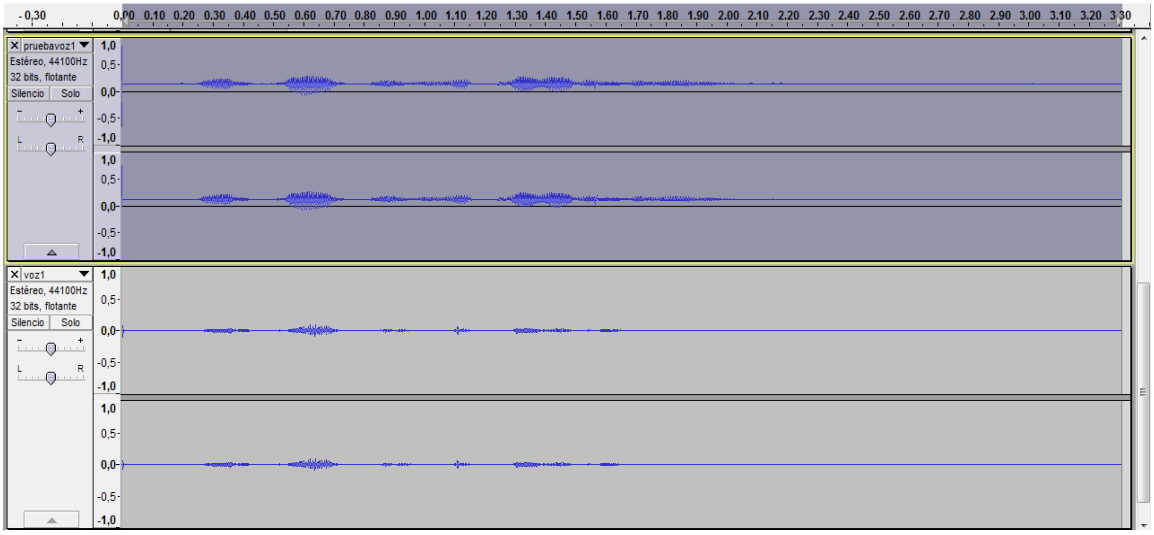


Figura 27. Vista en Audacity® de pruebavoz1.pcm y voz1.pcm

Al cambiar la frecuencia de muestreo al archivo “voz.pcm” a 8 kHz, se obtiene una señal de audio poco distorsionada por el proceso de codificación y decodificación, y al escuchar el audio es muy similar a la original. Entonces aquí se comprueba la teoría de lo que es un vocoder, el cual trabaja mejor a frecuencias cercanas al audio, por tal razón es preferible trabajar con una frecuencia de muestreo de 8 kHz, aunque al

final se tenga que modificar la frecuencia de muestreo del audio procesado de 44,1 kHz a 8 kHz, ver *Figura 28* y *Tabla 6*.

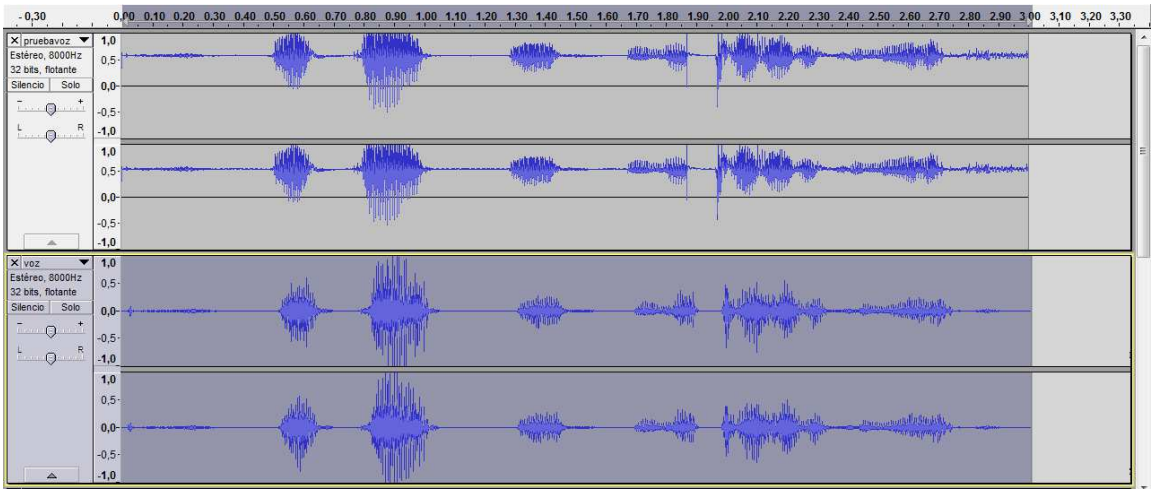


Figura 28. Vista en Audacity® de pruebavoz.pcm y voz.pcm (frecuencia de muestreo modificada a 8 kHz)

Tabla 6.

Audios originales vs. Archivos codificados y decodificados de la frase "esta es una prueba de sonido"

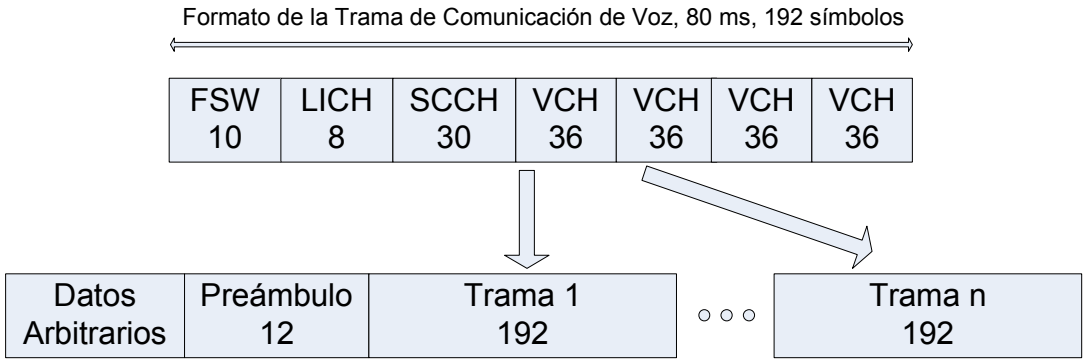
Archivos Originales						
Nombre	**Tipo Archivo**	**Resolución Muestreo**	**Número Canales**	**Frecuencia Muestreo**	**Tamaño Archivo**	**Duración**
pruebavoz	PCM	16 bits	Estéreo	8 kHz	93,7 kB	3’
pruebavoz1	PCM	16 bits	Estéreo	44,1 kHz	570 kB	3,309’
Archivos Codificados y Decodificados con el Equipo USB-3000™ P25 - Versión Estándar						
Nombre	**Tipo Archivo**	**Resolución Muestreo**	**Número Canales**	**Frecuencia Muestreo**	**Tamaño Archivo**	**Duración**
voz	PCM	16 bits	Estéreo	44,1 kHz	94 kB	0,546’
voz1	PCM	16 bits	Estéreo	44,1 kHz	570 kB	2’
Archivo modificado la frecuencia de muestreo de 44,1 kHz a 8 kHz						
Nombre	**Tipo Archivo**	**Resolución Muestreo**	**Número Canales**	**Frecuencia Muestreo**	**Tamaño Archivo**	**Duración**
voz	PCM	16 bits	Estéreo	8 kHz	94 kB	3,01’

4.3. MAPEO Y DESMAPEO DE SÍMBOLOS

En esta parte se toma al archivo ".pcm", el cual contiene toda la voz codificada (codificación de fuente y de canal) en una secuencia de bits, a estos se los agrupa de dos *(convierte en dibit)* para posterior convertirlos en 4 valores diferentes de *símbolos (01=+3; 00=+1; 10=-1 y 11=-3)*. En cambio en el desmapeo se sigue el paso inverso, en donde a los cuatro diferentes valores de símbolos se los convierte en *dibits (+3=01; +1=00; -1=10 y -3=11)*, para por ultimo guardarlos como una secuencia de bits dentro de un archivo ".pcm".

4.4. ENCAPSULADO Y DESENCAPSULADO DE TRAMAS

En esta sección se estructuran las *tramas de comunicación de voz (192 símbolos cada una)*, como se muestra en la *Figura 29*:



Preámbulo (+3, +3, +3, -3, +3, -3, +3, +3, -3, -3, -3, +3)
Datos Arbitrarios (se adhieren 10 símbolos aleatorios)
FSW: Frame Synchronization Word o Palabra de Sincronización de Trama (+3, +1, -3, +3, -3, -3, +3, +3, -1,+3)
LICH: Link Information Channel o Canal de Información de Enlace
SCCH: Signal Control Channel o Canal de Control de Señal
VCH: Voice Channel o Canal de Voz

Figura 29. Encapsulamiento Protocolo NXDN™
Fuente: (NXDN Forum Website, 2014)

Se comienza con el *FSW* que contiene a los *símbolos "+3, +1, -3, +3, -3, -3, +3, +3, -1, +3"*, después los símbolos en *LICH* y *SCCH* son *arbitrarios (en esta simulación no se toma en cuenta el protocolo)* y finalmente en *VCH* se encapsula toda la voz mapeada en el paso anterior (sin ningún proceso adicional). Finalmente ya estructuradas todas las tramas se introducen antes de estas, *datos arbitrarios (10 símbolos aleatorios)* y el *preámbulo (con los símbolos +3, +3, +3, -3, +3, -3, +3, +3, -3, -3, -3, +3)*.

Para el *desencapsulado* de tramas se realiza el proceso inverso, en donde mediante la ayuda del preámbulo y el FSW de la primera trama se *sincroniza la señal* para luego eliminar los datos arbitrarios y el preámbulo. Por último como ya se conoce la ubicación exacta de los campos que conforman las tramas, se *extraen* los VCH de todas estas sin modificar el orden de la secuencia, para posterior guardarlos dentro de un archivo ".bit".

4.5. MODULACIÓN Y DEMODULACIÓN

Para la modulación se utiliza *Tabla 7* y una función propia de MatLab® llamada *"fskmod(x,M,freq_sep,nsamp,Fs)"*, en donde: "x" es la secuencia de símbolos (se realizó la siguiente modificación: +3=3, +1=2, -1=1 y -3=0); "M" es el nivel de la modulación (M=4); "freq_sep" es la desviación de frecuencia en Hz entre las 4 diferentes frecuencias de desviación (freq_sep=700); "nsamp" es la cantidad de muestras por símbolo (nsamp=2, 4 y 8); y "Fs" es la frecuencia de muestreo (Fs=2800). Esta función por default permite realizar una *modulación coherente* y a la salida entrega la *envolvente compleja* de la señal modulada.

Tabla 7.

Mapeo de símbolo en simulación en MatLab®

Símbolo NXDN™	Símbolo fskmod	Frecuencia de Desviación
+3	3	+1050 Hz
+1	2	+350 Hz
-1	1	-350 Hz
-3	0	-1050 Hz

Para la *demodulación* que es el proceso inverso, se utiliza la función *"fskdemod(x,M,freq_sep,nsamp,Fs)"*, con las mismas variables de entrada. Al final se obtiene una secuencia de símbolos que deben modificarse (3=+3, 2=+1, 1=-1 y 0=-3). Esta función permite hacer solo la demodulación no coherente de la envolvente compleja de la señal modulada, pero si se desea hacer una *demodulación coherente* se debe usar un *demodulador CPFSK (Continuous Phase FSK)*.

Para el cálculo de la *probabilidad de símbolos errados* (P_E) y *probabilidad de bits errados* (P_B) de una *demodulación 4-FSK ortogonal con detección no coherente*, se puede valer de la siguiente expresión matemática:

$$P_E = \sum_{m=1}^{M-1} (-1)^{m+1} \binom{M-1}{m} \frac{1}{m+1} exp\left[-\frac{m}{m+1}\frac{kE_b}{N_O}\right] \tag{3.1}$$

$$P_B = \frac{M/2}{M-1} P_E \tag{3.2}$$

$$k = \log_2 M \tag{3.3}$$

En donde:

$\mathrm{M} =$ Nivel de la modulación.
$k =$ Número de bits por símbolo.

4.5.1. Envolvente Compleja

La envolvente compleja de una señal es una herramienta matemática, también llamada *señal paso bajo equivalente*, que se utiliza para el análisis de ciertas expresiones de modulaciones analógicas o también para representar una señal *paso banda* en *fase (componente real*) y *cuadratura (componente imaginaria)*. Estas dos componentes mencionadas son *ortogonales (están en cuadratura)* y no se interfieren la una con la otra, es decir, son *independientes* y por tal razón pueden ser transmitidas y receptadas con circuitos simples, simplificando el diseño de radios digitales **(Faúndez, 2001)**.

Para poder comprender matemáticamente como se obtiene la envolvente compleja de una señal, se debe conocer sobre la *Trasnformada de Hilbert* $\hat{x}(t) = H\{t(T)\}$, la cual se obtiene al pasar una señal $x(t)$ a través de un filtro $H(f)$ y cuya función de transferencia es:

$$H(f) = -j.sign(f) \qquad (Cracterización\ Frecuencial) \quad (3.4)$$

$$\emptyset(f) = -\frac{\pi}{2} sign(f) \qquad (Fase) \quad (3.5)$$

$$h(t) = \frac{1}{\pi t} \qquad (Cracterización\ Temporal) \quad (3.6)$$

Donde:

$$sign(f) = \begin{cases} 1 & f > 0 \\ 0 & f = 0 \\ -1 & f < 0 \end{cases} \tag{3.7}$$

Siendo la representación gráfica como se muestra en la *Figura 30* y la representación del sistema como se muestra en la *Figura 31*.

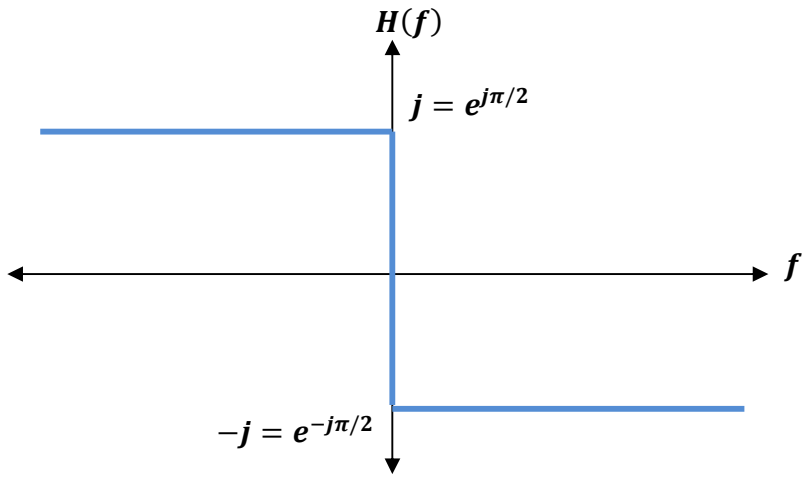


Figura 30. Representación gráfica de la Transformada de Hilbert

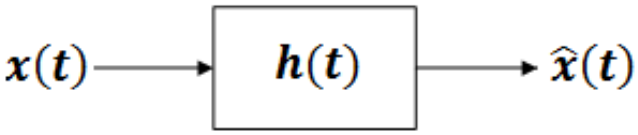


Figura 31. Sistema de la Transformada de Hilbert

$$\hat{x}(t) = \frac{1}{\pi}\int_{-\infty}^{\infty}\frac{x(\tau)}{t-\tau}d\tau = x(t) * \frac{1}{\pi t} \qquad (Transformada\ de\ Hilbert) \quad (3.8)$$

$$x(t) = -\frac{1}{\pi}\int_{-\infty}^{\infty}\frac{\hat{x}(\tau)}{t-\tau}d\tau = -\hat{x}(t) * \frac{1}{\pi t} \qquad (Transformada\ Inversa\ de\ Hilbert) \quad (3.9)$$

Esta transformada produce un desplazamiento $\pi/2$ para frecuencias negativas y de $-\pi/2$ para frecuencias positivas. Y permite obtener la pre-envolvente de la señal de la manera siguiente:

$$x_+(t) = x(t) + j\hat{x}(t) \qquad (Señal\ Analítica\ Positiva) \quad (3.10)$$

$$x_-(t) = x(t) - j\hat{x}(t) \qquad (Señal\ Analítica\ Negativa) \quad (3.11)$$

Ya para la obtención de la señal paso bajo equivalente se sigue con el siguiente procedimiento matemático:

$$\tilde{x}(t) = x_+(t)exp(-j2\pi f_c t) \quad (3.12)$$

$$\tilde{x}(t) = x_I(t) + jx_Q(t) \quad (3.13)$$

$$x(t) = Re[x_+(t)] = Re[\tilde{x}(t)exp(j2\pi f_c t)] = x_I(t)cos(j2\pi f_c t) - x_Q(t)sen(j2\pi f_c t) \quad (3.14)$$

Donde x_I es la *componente en fase* y x_Q es la *componente en cuadratura*. En la *Figura 32* se muestra el modelado para una señal paso bajo equivalente.

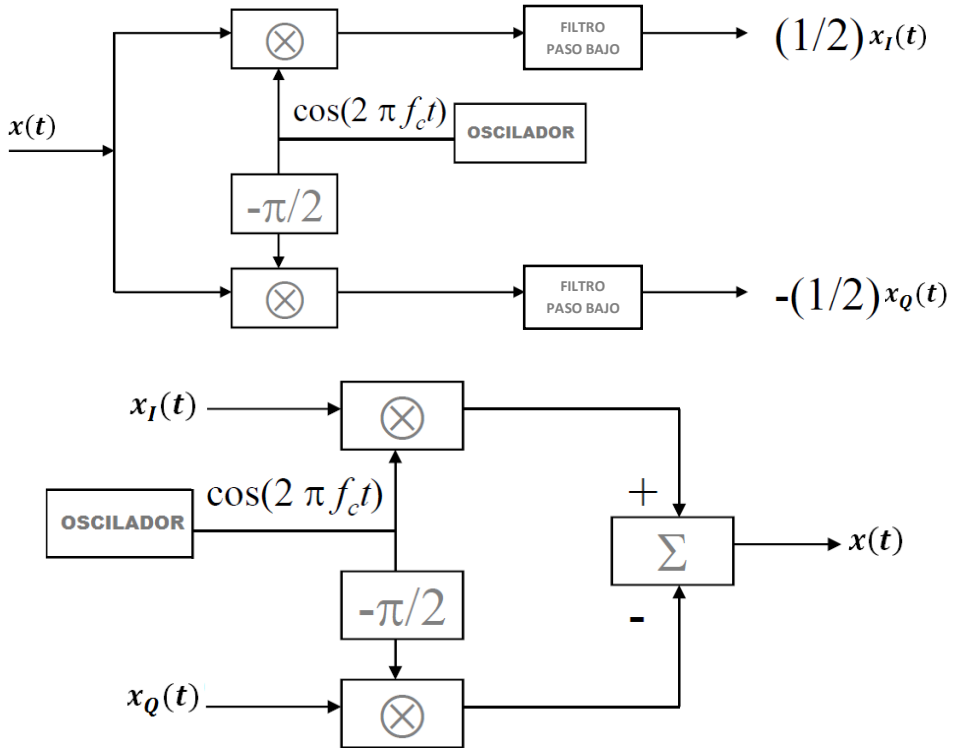


Figura 32. Modelado Paso Bajo Equivalente

4.5.2. Análisis de Ortogonalidad de las Frecuencias de Desviación

La frecuencia f_1 de la señal $S_1(t)$ es *ortogonal* con la frecuencia f_2 de la señal $S_2(t)$ si la *correlación* de ambas señales es *igual a cero*, es decir, si se cumple lo siguiente:

$$S_1(t) = A\cos(2\pi f_1 t + \varphi_1) \tag{3.15}$$

$$S_2(t) = A\cos(2\pi f_2 t + \varphi_2) \tag{3.16}$$

$$\int_{kT}^{(k+1)T} S_1(t)S_2(t)dt = 0\,, \qquad k = 01,2,\ldots.,\infty \tag{3.17}$$

En donde:

T = Periodo de la señal con menor frecuencia.

A = Amplitud de la señal.

En una modulación FSK coherente el desfase de la primera señal φ_1 y el desfase de la segunda señal φ_2 son los mismos, es decir, $\varphi_1 = \varphi_2$.

En MatLab® se puede realizar esta operación mediante la función *"trapz(t,S1.*S2)"*, en donde: "trapz" permite calcular una aproximación de la integral de una señal discreta a través del método trapezoidal; "t" es el tiempo de la señal; y "S1" y "S2" son dos señales discretas con sus respectivas frecuencias, las cuales están multiplicadas elemento a elemento mediante el operador matemático ".*".

Tabla 8.

Correlación entre las Frecuencias de Desviación

Señales	Frecuencias de Desviación
$S_1(t) = A\cos(2\pi f_1 t + \varphi_1)$	f1=+1050 Hz
$S_2(t) = A\cos(2\pi f_2 t + \varphi_2)$	f2=+350 Hz
$S_3(t) = A\cos(2\pi f_3 t + \varphi_3)$	f3=-350 Hz
$S_4(t) = A\cos(2\pi f_4 t + \varphi_4)$	f4=-1050 Hz
Resultados	
Correlación entre $\boldsymbol{S_1}$ y $\boldsymbol{S_2}$=7.3070e-20	
Correlación entre $\boldsymbol{S_1}$ y $\boldsymbol{S_3}$= -7.3070e-20	
Correlación entre $\boldsymbol{S_1}$ y $\boldsymbol{S_4}$= -0.0014	
Correlación entre $\boldsymbol{S_2}$ y $\boldsymbol{S_3}$= -0.0014	
Correlación entre $\boldsymbol{S_2}$ y $\boldsymbol{S_4}$= -7.3070e-20	
Correlación entre $\boldsymbol{S_2}$ y $\boldsymbol{S_4}$= 7.3070e-20	

Los datos de la *Tabla 8* indican que las diferentes correlaciones tienen valores cercanos a cero, esto significa que las frecuencias de las señales son no correladas, por ende son ortogonales. Otra forma de saber si dos frecuencias son ortogonales, es graficando las dos señales en el periodo de la señal con menor frecuencia, en el cual la de mayor frecuencia se repite n número de veces (n es un numero entero), o también se puede identificar si dos frecuencias son ortogonales si una es múltiplo de la otra. En la *Figura 33* se puede identificar de manera gráfica la ortogonalidad entre dos señales.

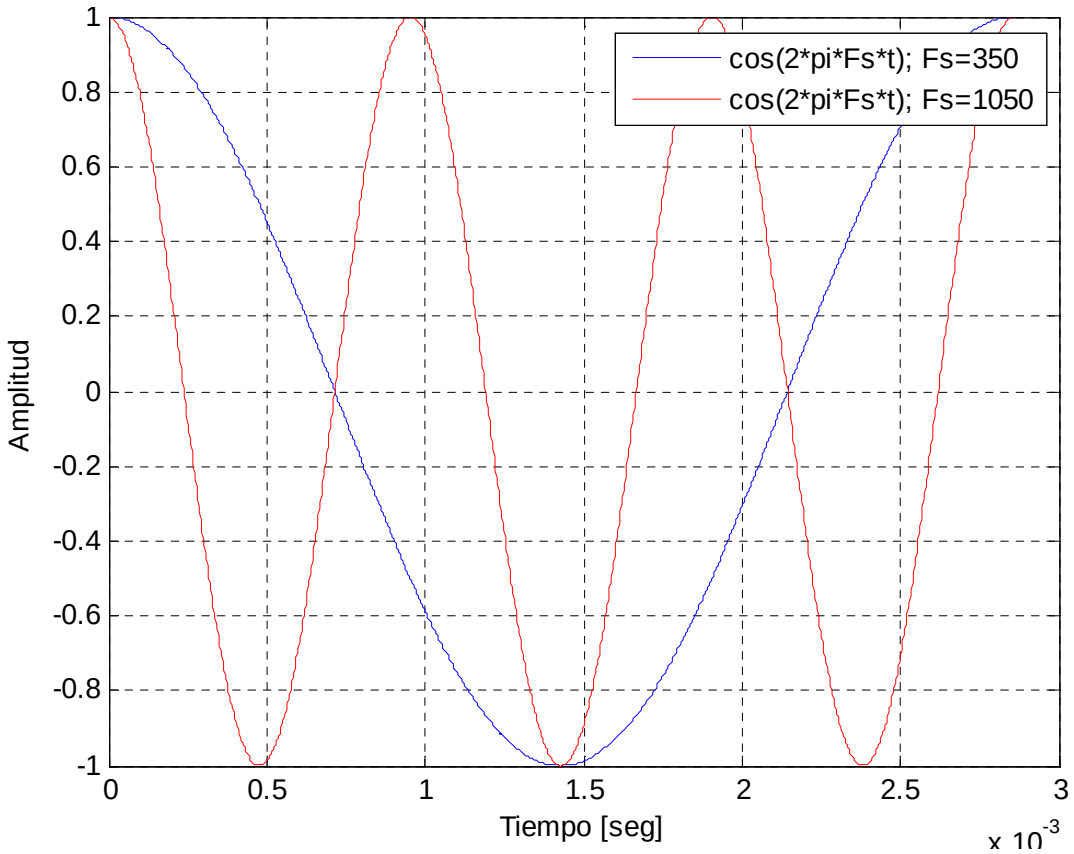


Figura 33. Comprobación gráfica de la Ortogonalidad entre dos señales

4.6. CANAL AWGN

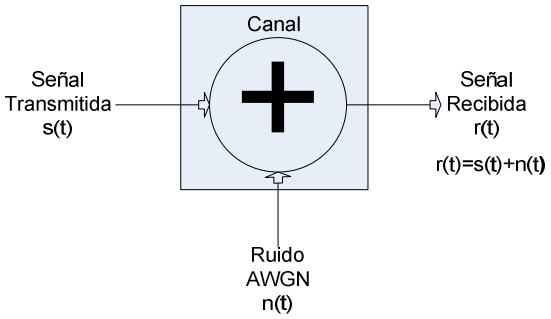


Figura 34 . Canal AWGN

En esta parte se suma a la envolvente compleja de la señal modulada un *Ruido Aditivo Gaussiano Blanco (AWGN)* mediante la función de MatLab® "awgn(xmod,SNR,'measured',[],'dB')", en donde: "xmod" es la envolvente compleja de la señal modulada; "SNR" es la relación señal a ruido; "measured" indica que la potencia de la señal va a ser medida antes de añadirle ruido; y "dB" indica que los valores de SNR van a estar en dB. La simulación consiste en ir variando la *cantidad de muestra por símbolo (2, 4 y 8)* y la E_s/N_0 , para lo cual hay que recordar que:

$$E_s/N_0\,(dB) = E_b/N_0\,(dB) + 10log_{10}(K) \tag{3.18}$$

$$SNR(dB) = E_s/N_0\,(dB) - 10log_{10}(nsamp) \tag{3.19}$$

En donde:

E_s/N_0 = Energía de símbolo por densidad espectral de potencia del ruido.

$E_b\,/N_0$ = Energía de bit por densidad espectral de potencia del ruido.

k = Número de bits por símbolo.

SNR = Relación señal a ruido.

$nsamp$ = Número de muestras por símbolo.

Para un mejor entendimiento se puede comprueba la eficiencia de los tipos de demoduladores (coherentes y no coherentes) con la ayuda función *"berawgn(Eb_No,'fsk',M,COHERENCE)"*, en donde: "Eb_No" es la energía de bit por densidad espectral de potencia del ruido en dB (esta variable va cambiando su valor); "fsk" es el tipo de modulación (FSK ortogonal); "M" es el nivel de la modulación (M=4); y "COHERENCE" si es 'coherent' permite una detección coherente y si es 'noncoherent' permite una detección no coherente. Esta función entrega la *BER (tasa de bits errados)* de una modulación 4-*FSK ortogonal* sobre un *canal AWGN*. En la *Figura 35* se aprecia que una detección coherente es mejor que una no coherente.

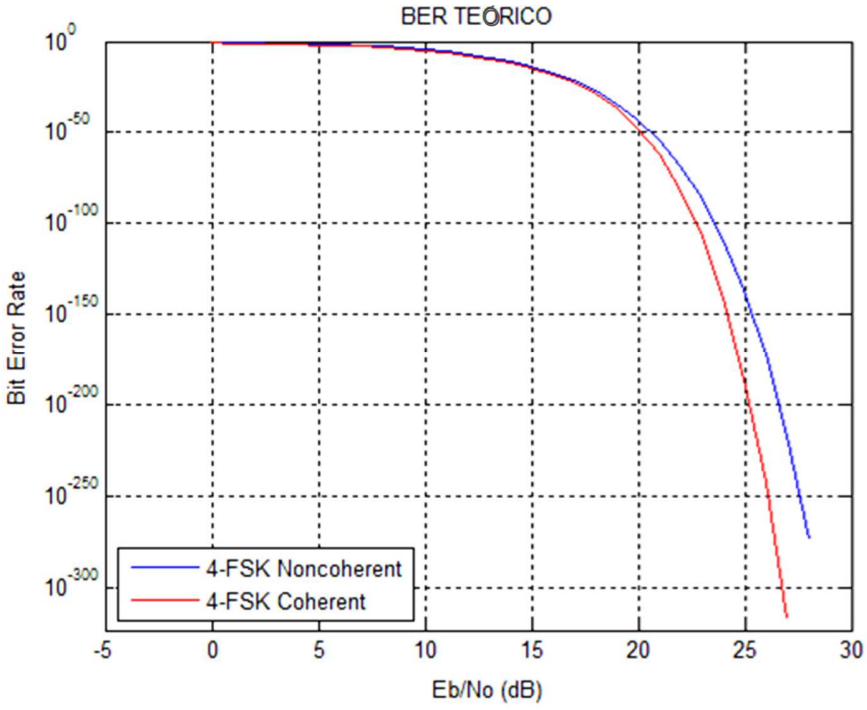


Figura 35. BER Teórico sobre un canal AWGN, 4-FSK Coherente vs. 4-FSK no Coherente

Posterior con la función *"[num,BER] = biterr(inbit,outbit)"*, se calcula la cantidad de bits errados en "num" y la tasa de bits errados en "BER" entre la señal banda base entrante en bits "inbit" y la señal banda base saliente en bits "outbit".

Para el cálculo de la *probabilidad de símbolos errados* ($\boldsymbol{P_E}$) se vale de la siguiente expresión matemática:

$$P_E = \frac{M-1}{M/2} P_B \tag{3.20}$$

En donde:

$P_B =$ Probabilidad de bits errados o BER.

$P_E =$ Probabilidad de símbolos errados o *tasa de símbolos eErrados (SER)*.

En la *Tabla 9*, en la *Figura 36* y en la *Figura 37* se puede apreciar los resultados obtenidos con la simulación en la herramienta matemática MatLab® de la transmisión y recepción de 17433 bits, usando el protocolo NXDN™ con una modulación 4-FSK ortogonal y detección no coherente sobre un canal AWGN.

Tabla 9.

Resultados de la simulación en MatLab® de la Tx-Rx con modulación 4-FSK ortogonal y detección no coherente sobre un Canal AWGN

Con 8 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	P_E	**Demodulación**
6 dB	2.9897 dB	-3.0309 dB	0.0979	13646	0.1469	A VECES
7 dB	3.9897 dB	-2.0309 dB	0.061	8502	0.0915	A VECES
8 dB	4.9897 dB	-1.0309 dB	0.0345	4803	0.0518	A VECES
9 dB	5.9897 dB	-0.0309 dB	0.0158	2203	0.0237	A VECES
10 dB	6.9897 dB	0.9691 dB	0.0057	798	0.0086	A VECES
12 dB	8.9897 dB	2.9691 dB	0.4089e-03	57	6.1335 e-04	SIEMPRE
14 dB	10.9897 dB	4.9691 dB	0.1435e-04	2	2.1525e-05	SIEMPRE
16 dB	12.9897 dB	6.9691 dB	0	0	0	SIEMPRE
Con 4 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	P_E	**Demodulación**
7 dB	3.9897 dB	0.9794 dB	0.0609	8488	0.0914	A VECES
8 dB	4.9897 dB	1.9794 dB	0.035	4884	0.0525	A VECES
9 dB	5.9897 dB	2.9794 dB	0.0158	2209	0.0237	A VECES
10 dB	6.9897 dB	3.9794 dB	0.0059	818	0.0089	A VECES
12 dB	8.9897 dB	5.9794 dB	0.2583e-03	36	3.8745 e-04	SIEMPRE
14 dB	10.9897 dB	7.9794 dB	0.1435e-04	2	2.1525e-05	SIEMPRE
16 dB	12.9897 dB	9.9794 dB	0	0	0	SIEMPRE
Con 2 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	P_E	**Demodulación**
9 dB	5.9897 dB	5.9897 dB	…	…	…	NUNCA
10 dB	6.9897 dB	6.9897 dB	0.0487	6784	0.0731	A VECES
12 dB	8.9897 dB	8.9897 dB	0.0173	2405	0.026	A VECES
14 dB	10.9897 dB	10.9897 dB	0.0038	534	0.0057	SIEMPRE
16 dB	12.9897 dB	12.9897 dB	0.4089e-03	57	6.1338 e-04	SIEMPRE
18 dB	14.9897 dB	14.9897 dB	0.1435e-04	2	2.1522e-05	SIEMPRE
20 dB	16.9897 dB	16.9897 dB	0	0	0	SIEMPRE

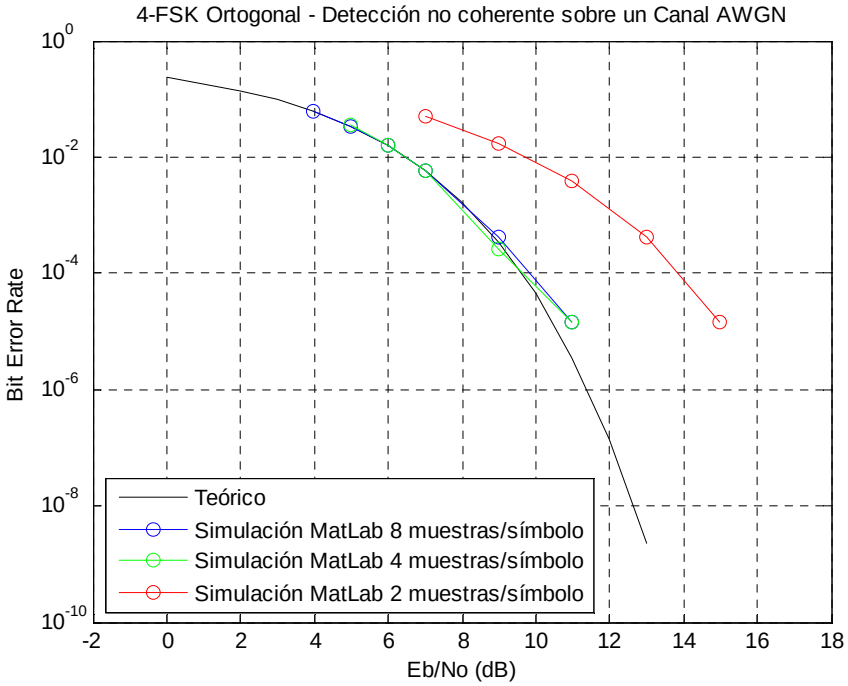


Figura 36. Simulación MatLab® Canal AWGN, Eb/No (dB) vs. BER

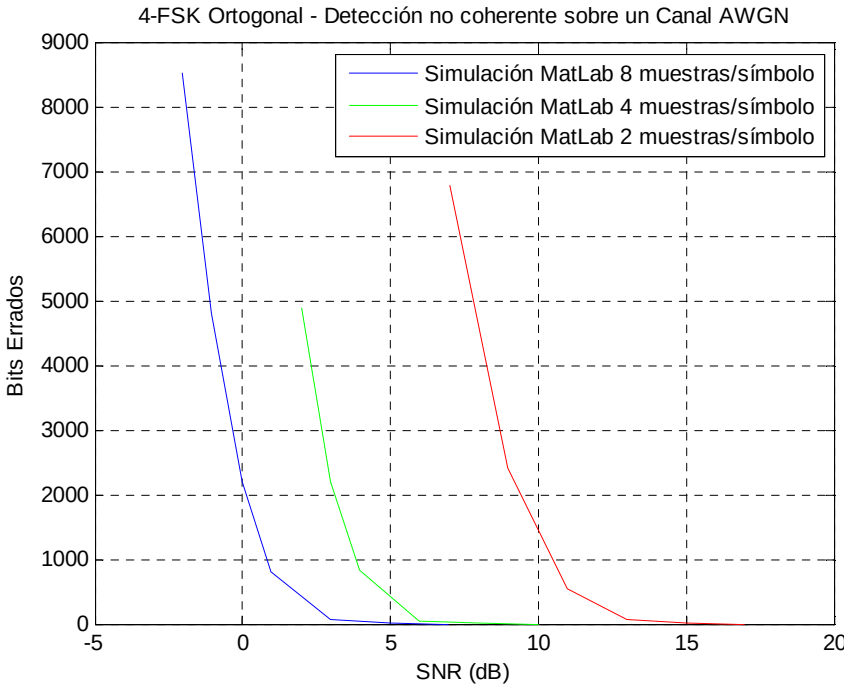


Figura 37. Simulación MatLab® Canal AWGN, SNR (dB) vs. Bits Errados

Los datos obtenidos en la simulación demuestran que los resultados con 4 y 8 muestras por símbolo están muy cercanos a los teóricos, además que son muy similares entre sí en la $\boldsymbol{E_b/N_0}$, en la BER, en la cantidad de bits errados y en la detección, mas no en la SNR, puesto que con 8 es menor en 3dB que con 4. Ahora con 2 muestras por símbolo presenta un BER mayor por cada dB de la $\boldsymbol{E_b/N_0}$, en sí presenta la peor detección de todos.

4.7. DESVANECIMIENTO PLANO CON LÍNEA DE VISTA

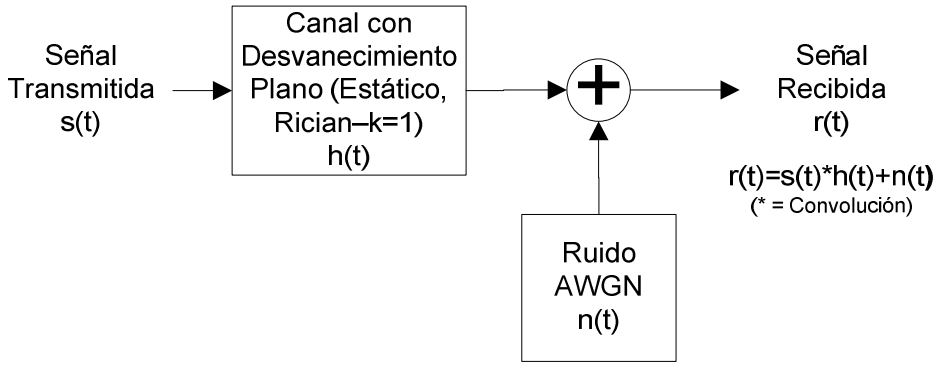


Figura 38. Canal Rician

Antes de sumarle un ruido AWGN a la señal transmitida se le introduce a un *canal con desvanecimiento plano con línea de vista (LOS) y estático*, mediante la creación de un objeto *"chan=ricianchan"* en MatLab® y la función *"filter(chan,x)"* para modelar el efecto del canal sobre la señal, donde: "chan" es el canal; y "x" es la señal trasmitida. Es decir, este es un canal con multitrayectos de banda estrecha con distribución Rician donde el desplazamiento máximo de Doppler es igual a cero (transmisor y receptor están en reposo). Este canal depende del factor de desvanecimiento "k", el cual es una razón entre las potencias de la componente directa de la señal y los componentes del multitrayecto.

$$k = \frac{Potencia\ de\ la\ componente\ directa}{Potencias\ de\ la\ componente\ multitrayecto} = \frac{v}{\sigma^2} \qquad (3.21)$$

En la simulación el valor de *k* es igual a 1. Hay que recordar que cuando *k=0* el canal se comporta como un *canal Rayleigh*, mientras que cuando *k tiende al infinito* se comporta como un *canal Gaussiano Rice*, lo cual se puede apreciar en la *Figura 39*.

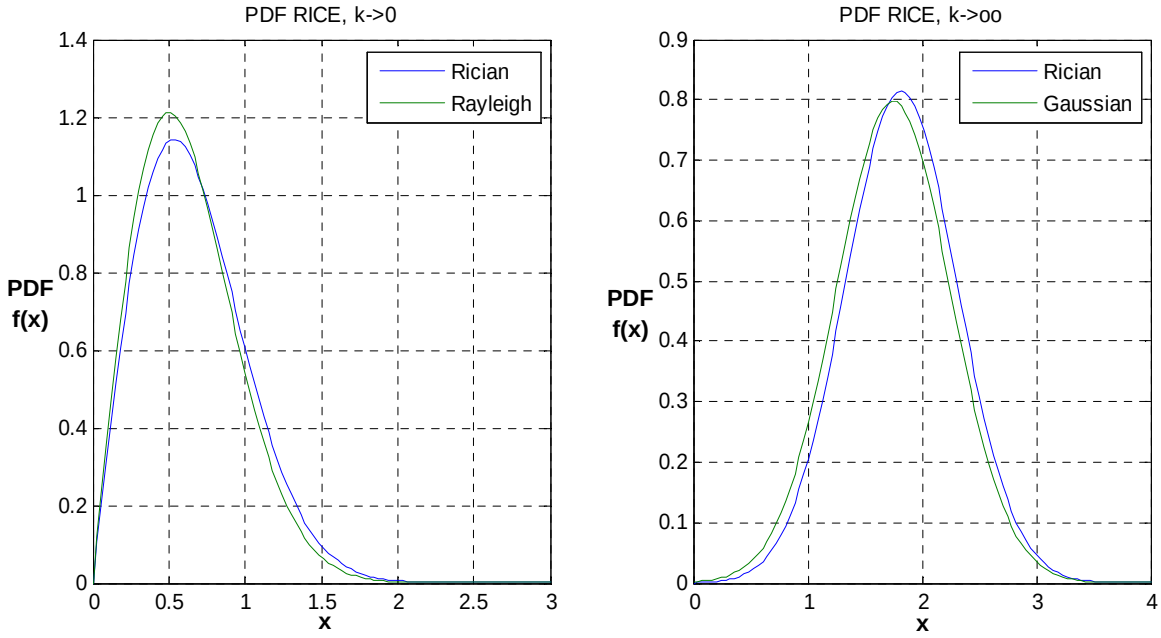


Figura 39. PDF (Función Densidad de probabilidad) Rician, cuando tiende a cero y cuando tiende al infinito

En la *Tabla 11* se encuentran los resultados obtenidos en la simulación hecha en la herramienta matemática MatLab® de la transmisión y recepción usando una modulación 4-FSK ortogonal con detección no coherente sobre un canal Rician estático con k=1. También se puede apreciar el comportamiento del sincronizador y del decodificador.

Tabla 10.

Resultados de la simulación en MatLab® de la Tx-Rx con modulación 4-FSK ortogonal y detección no coherente sobre un Canal Rician estático con k=1

Con 8 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	**Sincronización**	**Decodificación**
6 dB	2.9897 dB	-3.0309 dB	0.09796	13882	Inestable	Inestable
7 dB	3.9897 dB	-2.0309 dB	0.0616	8591	Inestable	Inestable
8 dB	4.9897 dB	-1.0309 dB	0.0324	4515	Inestable	Inestable
9 dB	5.9897 dB	-0.0309 dB	0.0156	2171	Inestable	Inestable
10 dB	6.9897 dB	0.9691 dB	0.0061	849	Inestable	Inestable
12 dB	8.9897 dB	2.9691 dB	4.0892e-04	57	Estable	Inestable
14 dB	10.9897 dB	4.9691 dB	0	0	Estable	Estable
16 dB	12.9897 dB	6.9691 dB	0	0	Estable	Estable
Con 4 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	**Sincronización**	**Decodificación**
7 dB	3.9897 dB	0.9794 dB	0.0620	8646	Inestable	Inestable
8 dB	4.9897 dB	1.9794 dB	0.0344	4799	Inestable	Inestable
9 dB	5.9897 dB	2.9794 dB	0.0161	2248	Inestable	Inestable
10 dB	6.9897 dB	3.9794 dB	0.0059	824	Inestable	Inestable
12 dB	8.9897 dB	5.9794 dB	3.8740e-04	54	Estable	Inestable
14 dB	10.9897 dB	7.9794 dB	0	0	Estable	Estable
16 dB	12.9897 dB	9.9794 dB	0	0	Estable	Estable
Con 2 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	**Sincronización**	**Decodificación**
9 dB	5.9897 dB	5.9897 dB	…	…	No procede	Inestable
10 dB	6.9897 dB	6.9897 dB	0.0492	6864	Inestable	Inestable
12 dB	8.9897 dB	8.9897 dB	0.0173	2406	Inestable	Inestable
14 dB	10.9897 dB	10.9897 dB	0.0036	505	Estable	Inestable
16 dB	12.9897 dB	12.9897 dB	3.0131e-04	42	Estable	Inestable
18 dB	14.9897 dB	14.9897 dB	0	0	Estable	Inestable
20 dB	16.9897 dB	16.9897 dB	0	0	Estable	Inestable

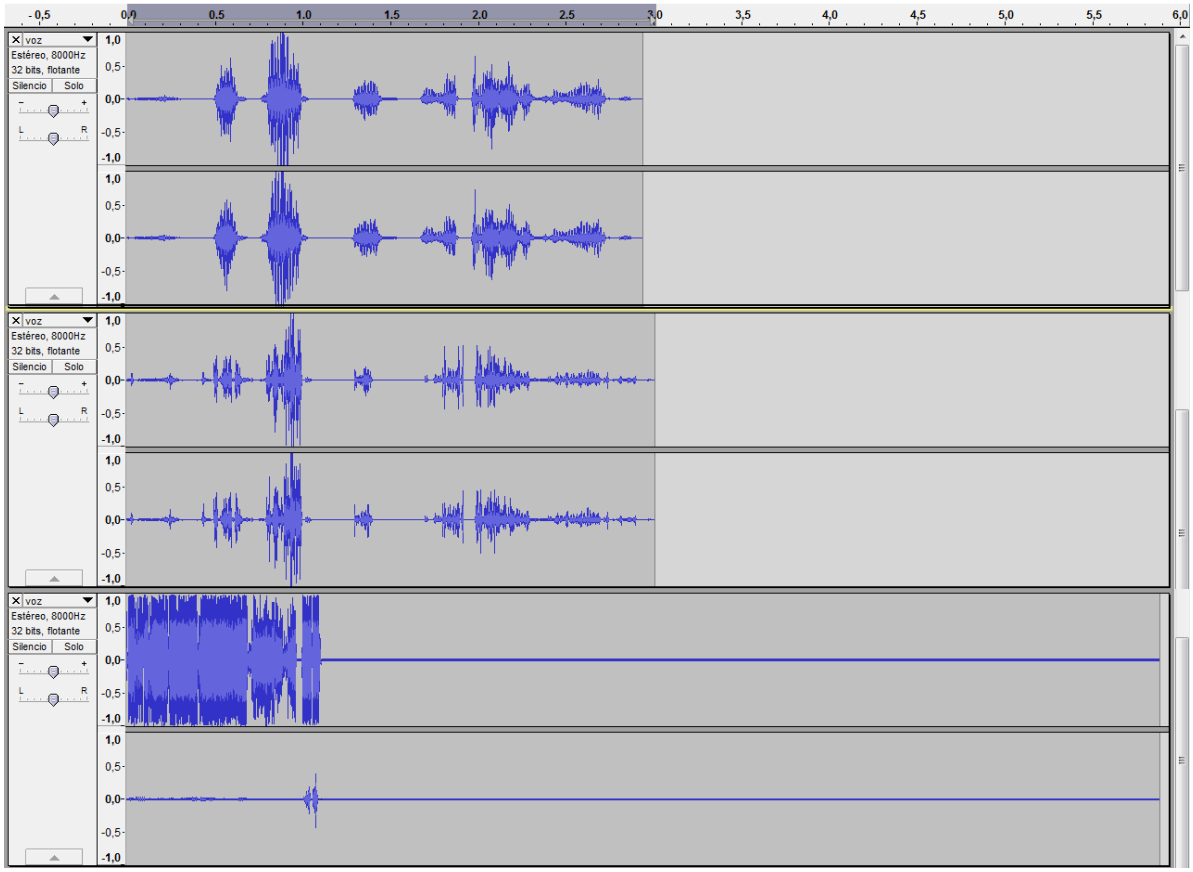


Figura 40. Degeneración de la señal de audio sobre un Canal Rician (k=1) y una modulación 4-FSK ortogonal con detección no coherente (con 8 muestras/símbolo), visto desde el software Audacity®

En la *Figura 40* se puede apreciar la degradación de la señal de audio sobre un canal Rician (k=1) y una modulación 4-FSK ortogonal con detección no coherente con 8 muestras por símbolo, cabe señalar que la degradación de la señal de audio con 4 muestras por símbolo es similar con la primera. En cambio en la *Figura 41* se puede apreciar la degradación de la señal de audio con 2 muestras por símbolo.

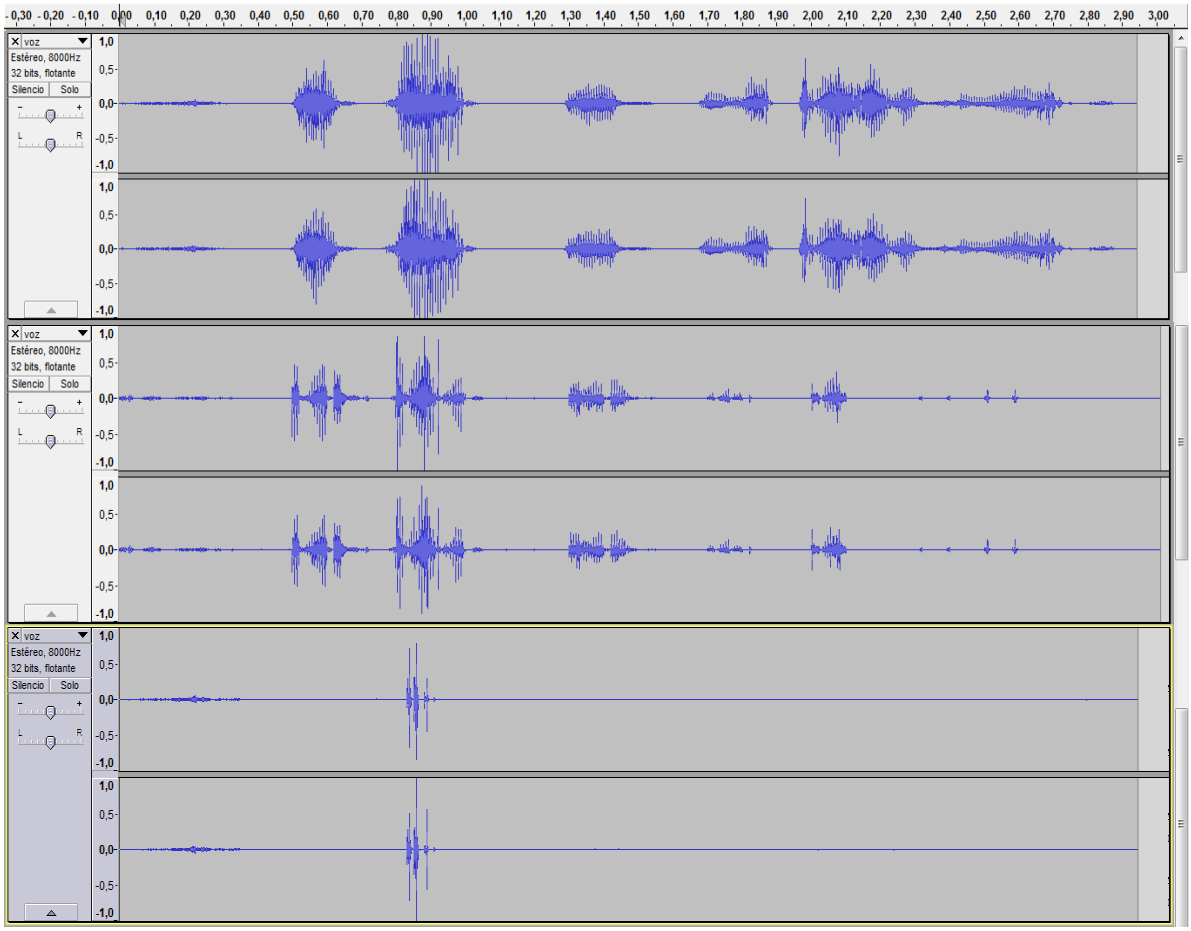


Figura 41. Degeneración de la señal de audio sobre un Canal Rician (k=1) y una modulación 4-FSK ortogonal con detección no coherente (con 2 muestras/símbolo), visto desde el software Audacity®

4.8. DESVANECIMIENTO PLANO SIN LÍNEA DE VISTA

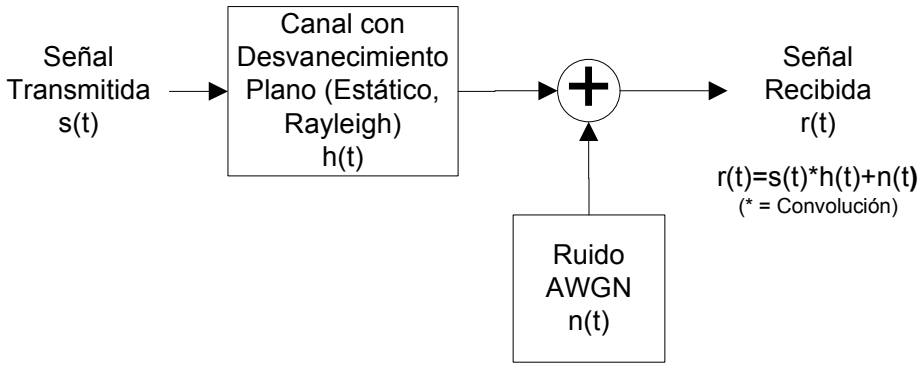


Figura 42. Canal Rayleigh

Al igual que el anterior, antes de sumarle un ruido AWGN a la señal transmitida se le introduce a un *canal con desvanecimiento plano sin línea de vista (NLOS) y estático*, mediante la creación de un objeto *"chan= rayleighchan"* en MatLab® y la función *"filter(chan,x)"* para modelar el efecto del canal sobre la señal, donde: "chan" es el canal; y "x" es la señal trasmitida. Es decir, este es un canal con multitrayectos de banda estrecha con *distribución Rayleigh* donde el desplazamiento máximo de Doppler es igual a cero (transmisor y receptor están en reposo). En este tipo de canal solo existen componentes del multitrayecto y no componente directa de la señal, por lo tanto este canal es más agresivo en desvanecimiento plano que uno de Rician.

Tabla 11.

Resultados de la simulación en MatLab® de la Tx-Rx con modulación 4-FSK ortogonal y detección no coherente sobre un Canal Rayleigh estático

Con 8 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	**Sincronización**	**Decodificación**
6 dB	2.9897 dB	-3.0309 dB	0.0975	13584	Inestable	Inestable
7 dB	3.9897 dB	-2.0309 dB	0.0625	8709	Inestable	Inestable
8 dB	4.9897 dB	-1.0309 dB	0.0340	4739	Inestable	Inestable
9 dB	5.9897 dB	-0.0309 dB	0.0163	2278	Inestable	Inestable
10 dB	6.9897 dB	0.9691 dB	0.0057	811	Inestable	Inestable
12 dB	8.9897 dB	2.9691 dB	2.9413e-04	41	Estable	Inestable
14 dB	10.9897 dB	4.9691 dB	0	0	Estable	Estable
Con 4 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	**Sincronización**	**Decodificación**
7 dB	3.9897 dB	0.9794 dB	0.0629	8766	Inestable	Inestable
8 dB	4.9897 dB	1.9794 dB	0.0345	4803	Inestable	Inestable
9 dB	5.9897 dB	2.9794 dB	0.0158	2209	Inestable	Inestable
10 dB	6.9897 dB	3.9794 dB	0.0059	818	Inestable	Inestable
12 dB	8.9897 dB	5.9794 dB	3.0131e-04	42	Estable	Inestable
14 dB	10.9897 dB	7.9794 dB	0	0	Estable	Estable
Con 2 muestras/símbolo						
EsNo	**EbNo**	**SNR**	**BER**	**bits errados**	**Sincronización**	**Decodificación**
9 dB	5.9897 dB	5.9897 dB	…	…	No procede	Inestable
10 dB	6.9897 dB	6.9897 dB	0.0496	6916	Inestable	Inestable
12 dB	8.9897 dB	8.9897 dB	0.0172	2396	Inestable	Inestable
14 dB	10.9897 dB	10.9897 dB	0.0039	544	Estable	Inestable
16 dB	12.9897 dB	12.9897 dB	3.9457e-04	55	Estable	Inestable
18 dB	14.9897 dB	14.9897 dB	7.1740e-06	1	Estable	Inestable
20 dB	16.9897 dB	16.9897 dB	0	0	Estable	Inestable

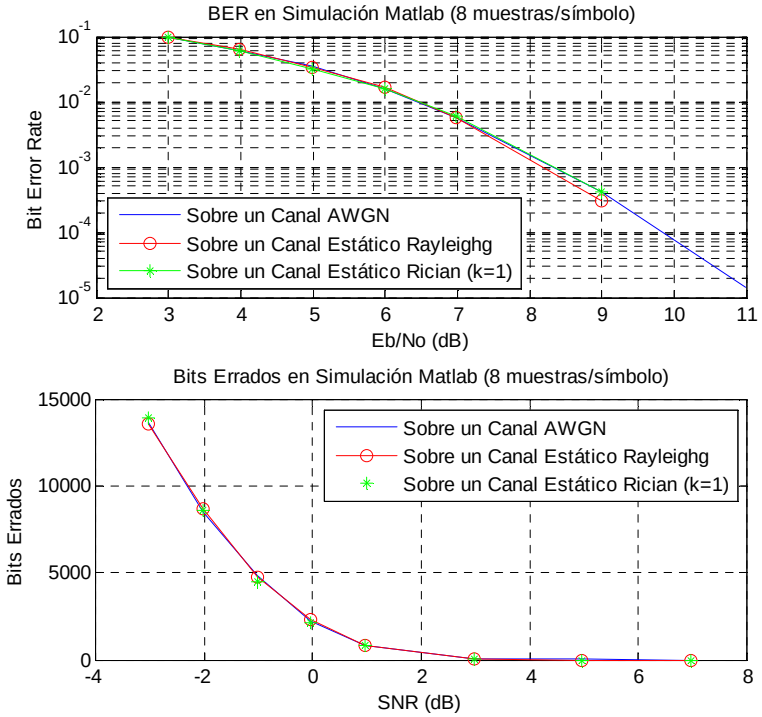


Figura 43. Comportamiento con diferentes Canales con 8 muestras por Símbolo

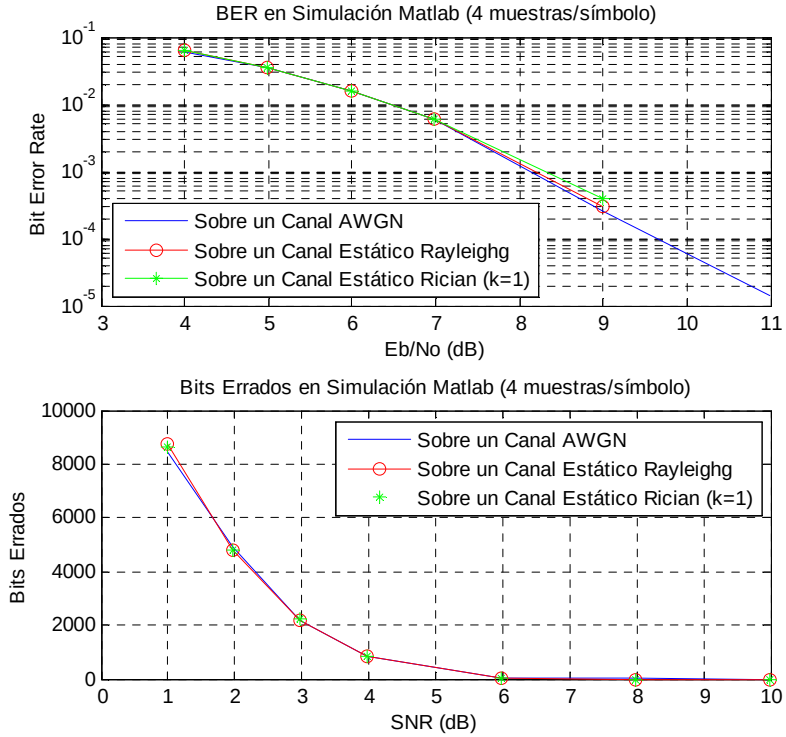


Figura 44. Comportamiento con diferentes Canales con 4 muestras por Símbolo

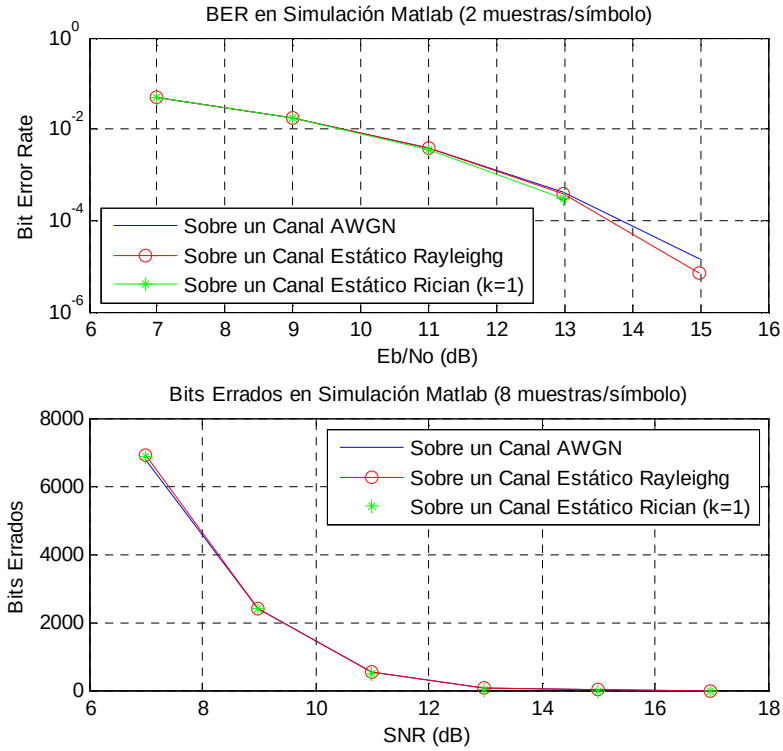


Figura 45. Comportamiento con diferentes Canales con 2 muestras por Símbolo

Los resultados obtenidos con el canal Rician *(Tabla 10)* y con el canal Rayleigh *(Tabla 11)*, demuestran gráficamente en la *Figura 43, Figura 44* y *Figura 45*, que no producen cambio alguno o relevante al sistema de transmisión y recepción con el protocolo NXDN™.

Ahora en la *Figura 46, Figura 47* y *Figura 48* se puede apreciar una comparación gráfica entre el comportamiento del sincronizador y del decodificador que se encuentran conformando el sistema de transmisión y recepción usando el protocolo NXDN™.

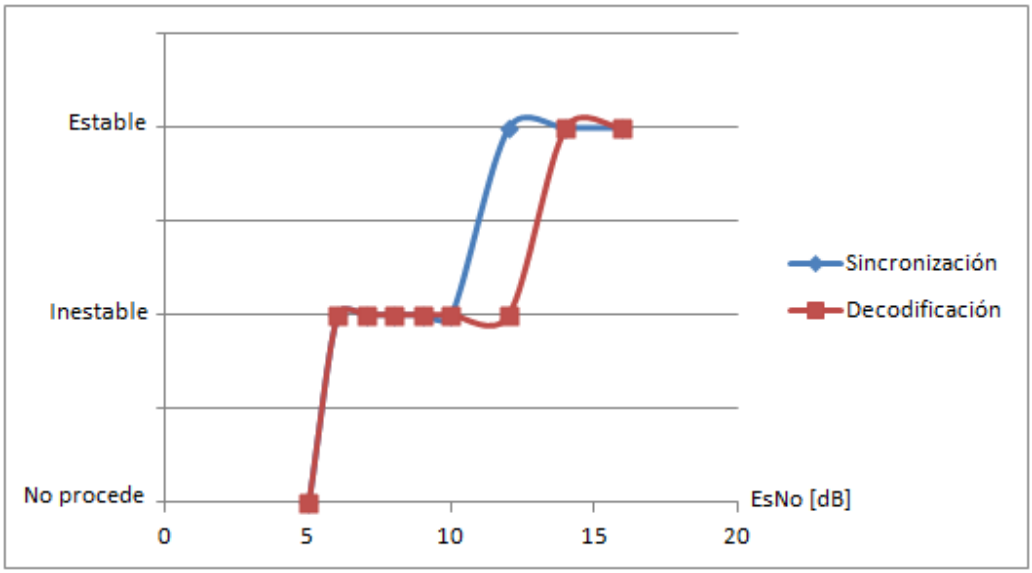


Figura 46. Comparación del comportamiento entre el Sincronizador y el Decodificador del Sistema (Con 8 muestras/símbolo)

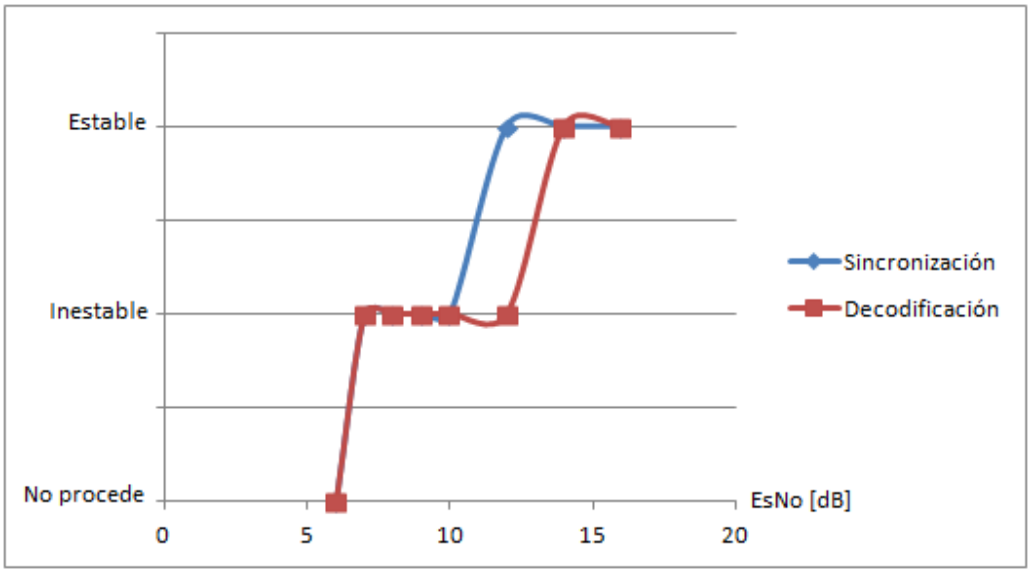


Figura 47. Comparación del comportamiento entre el Sincronizador y el Decodificador del Sistema (Con 4 muestras/símbolo)

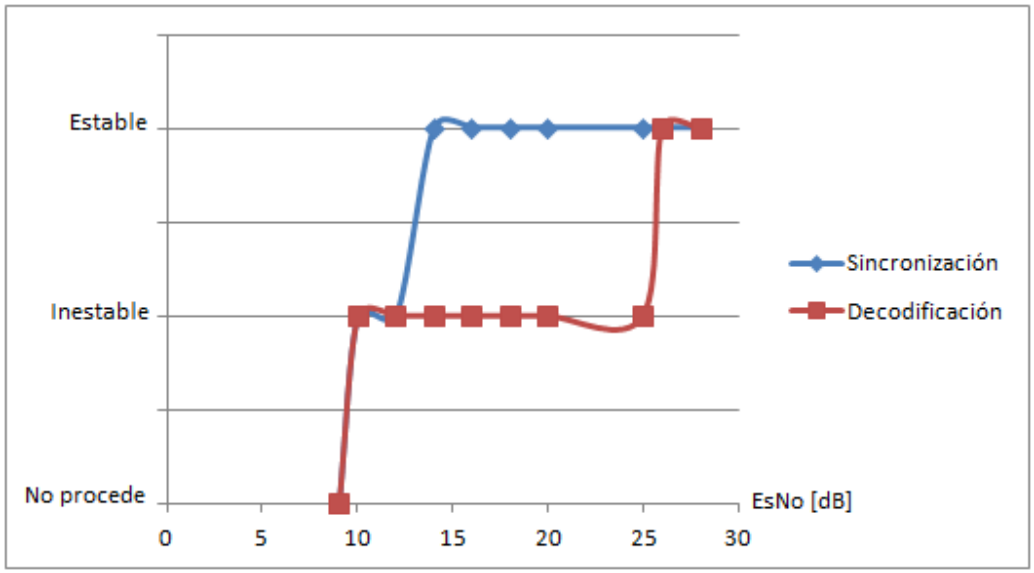


Figura 48. Comparación del comportamiento entre el Sincronizador y el Decodificador del Sistema (Con 2 muestras/símbolo)

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La Guerra Electrónica es un arma poderosa que permite el control y el uso del espectro electromagnético en contra de fuerzas enemigas para la toma inmediata decisiones en el campo de batalla y se preocupa de las características técnicas de la tecnología a intervenir, mientras que la Inteligencia de Señales es la Inteligencia producida al recolectar y analizar la información que se transmite con la tecnología a intervenir, además que no depende mucho del tiempo como la anterior.
- El Protocolo de banda estrecha para comunicaciones móviles terrestres NXDN™ es una tecnología muy utilizada en Latinoamérica, tanto por organizaciones licitas como ilícitas, gracias a las grandes prestaciones técnicas que presta, por tal razón es de gran interés por parte de Fuerzas Armadas del Ecuador el poder intervenir este protocolo. Además esta tesis es un gran inicio para el desarrollo de GE en el Ecuador, permitiendo generar tecnología propia y eliminando la gran dependencia de tecnologías extranjeras.
- Al fijarse bien en la definición de interceptación es fácil entender que todo el proceso realizado en el diseño del sistema para la demodulación en tiempo real del estándar NXDN™, pasa a ser parte de esta Medida de Apoyo Electrónico, es decir, la demodulación es parte de la interceptación.

- Este diseño es eficiente para realizar la Interceptación a transmisiones de voz que usen el protocolo NXDN™, mas no para las transmisiones de datos. Además que también permite obtener en tiempo real la información transmitida, algo muy relevante para la toma de decisiones en el frente de batalla. Cabe indicar que se lo puede adaptar para la transmisión de datos modificando en la parte de decodificación de canal o desencapsulamiento de tramas.
- El receptor portátil R&S®PR100 con el software R&S®GX430, gracias a su API de integración que permite la integración de diferentes algoritmos, pueden convertirse en un receptor universal móvil para varios tipos de tecnologías de telecomunicaciones. Lo negativo es su gran costo económico.
- El receptor portátil R&S®PR100 y el software R&S®GX430, en ocasiones para la intervención de ciertas tecnologías con software propietario, tendrán que adicionar software y hardware, como es en el caso del protocolo NXDN™, donde tuvieron que trabajar en conjunto con el dispositivo USB-3000™ P25 y su software controlador usb3kcom.exe.
- La simulación en MatLab® de la transmisión y recepción con el protocolo NXDN™ realizada con diferentes tipos de desvanecimientos planos estáticos, con y sin línea de vista, permitió conocer el funcionamiento exacto de la tecnología de radio móvil, lo cual para una fase de implementación del diseño para la monitorización, interceptación y demodulación en tiempo real de señales digitales NXDN™, será una pieza clave y fundamental en la creación de algoritmos que se implementarán al receptor portátil R&S®PR100 y al software R&S®GX430, gracias a su API de integración.
- Según el manual de usuario, el dispositivo USB-3000™ P25 en su modo de codificación -enc trabaja solo con archivos “.pcm”, pero se pudo demostrar que trabaja de igual manera con archivos “.wav”. Además también indica que el archivo que va a ser codificado debe tener una resolución de muestreo PCM de 16 bits, con una frecuencia de muestreo de 8 kHz, pero al momento que se va a comprobar el correcto funcionamiento del aparato, los archivos de prueba que da el fabricante tienen una frecuencia de muestreo de 44,1 kHz, lo

cual produce grandes confusiones; para lo con las pruebas realizadas con el equipo y los software MatLab® y Audacity® se pudo demostrar que es mejor audiblemente trabajar con archivos que tengan una frecuencia de muestreo de 8 kHz, aunque al final después del proceso de codificación y decodificación se obtenga un archivo con una frecuencia de muestreo de 44,1 kHz y se lo tenga que submuestrear a 8 kHz.

- Los resultados obtenidos en la simulación de la transmisión y recepción con el protocolo NXDN™ indican que los canales con desvanecimiento plano estático, tanto con línea de vista (Rician) como sin línea de vista (Rayleigh), no producen gran inconveniente al sistema de comunicación, puesto que solo afectan a la amplitud y a la fase de la señal. En cambio el canal AWGN tiene gran incidencia en el comportamiento del sistema, específicamente en la tasa de bits errados, que cuando es muy alta el sistema no sincroniza la señal gracias a la gran cantidad de bits errados y por ende no se logra el desencapsular las tramas.
- Se realizó una comparación relativa entre el sincronizador y el decodificador (con el dispositivo USB-3000™ P25) que se encuentran conformando el sistema simulado en MatLab® para la transmisión y recepción con el protocolo NXDN™, en donde se puede observar que ambos no proceden en la misma EsNo en los diferentes escenarios de modulación a 2, 4 y 8 muestra/símbolo (el sincronizador no detecta y el decodificador no puede reconstruir la señal de audio), de ahí el comportamiento de estos dos procesos mencionados se vuelve inestables (a menor EsNo el sincronizador necesita mayor número de repeticiones del proceso para cumplir con su función y el decodificador reconstruye con mayor deterioro la señal de audio debido a la gran cantidad de paquetes desbordados), y por último estos llegan a estabilizarse a mayor EsNo y por ende a trabajar sin problema alguno (el sincronizador se estabiliza con menor EsNo). Además el sincronizador y el decodificador tienen un similar comportamiento a 4 y 8 muestras por símbolo, siendo las únicas diferencias que a 4 muestras/símbolo necesita 1dB más de EsNo para llegar al estado de inestable y 3dB más de SNR para tener igual BER; mientras que

a 2 muestras/símbolo tiene el peor desempeño, puesto que tiene un mayor BER.

5.2. RECOMENDACIONES

- El receptor portátil R&S®PR100 además puede ser usado eficazmente para *Direction Finding (DF)*, que es la acción de localizar el lugar en donde se están realizando las emisiones enemigas, lo cual es conocido también como Radiogoniometría.
- Si se desea trabajar en tiempo real con la herramienta matemática MatLab® en diferentes tipos de simulaciones, se debe realizar la siguiente configuración en el software: escribir *rtwintgt -setup* en la ventana de comandos de MatLab® para configurar el *Real-Time Windows Target* y después de que la instalación se haya completado, configurar el *MatLab® Distributed Computing Server* acorde a las instrucciones descritas en www.mathworks.com/distconfig.
- Al momento de intervenir una tecnología de telecomunicaciones cualquiera que sea esta, se debe conocer bien sus especificaciones técnicas y si se desea realizar algoritmos para su demodulación o manipulación, se debe entender su correcto funcionamiento (son de gran ayuda las simulaciones con medios informáticos), para un buen desarrollo y desempeño de los mismos.
- Para mejorar el proceso de la sincronización de la señal receptada en el sistema simulado para la transmisión y recepción con el protocolo NXDN™, es recomendable introducir un filtro de coseno levantado para minimizar el efecto de la interferencia intersimbólica (esta tecnología ya tiene un filtro diseñado el cual se puede apreciar en la Figura 14); mientras que para disminuir el BER de la señal receptada en esta simulación, se ve indispensable la introducción de los algoritmos de la codificación de canal en el encapsulamiento de las tramas.

- Para la simulación de un sistema con mayor ISI es recomendable que los canales de Rician y Rayleigh no sean estáticos, siendo la variable a atender en estos casos el desplazamiento máximo de Doopler.
- Para mejorar la cobertura y el alcance en el campo de batalla del receptor portátil R&S®PR100, se ve recomendable trabajar con antenas inteligentes, las cuales mediante su arreglo de antenas y unidad de procesamiento digital de señales permitirían direccionar el lóbulo de radiación hacia los equipos que van a ser monitorizados e interceptados *(Beamforming o Filtrado Espacial)*, en el momento preciso que estos estén transmitiendo; además que facilitaría identificar la dirección de llegada de la señal *(Direction of Arrival - DOA)*, parte esencial para realizar *Direction Finding (DF)*. Esta tecnología mencionada, aparte de ser amigable con el medio ambiente gracias a que no radia energía a todas direcciones, sino solo a puntos específicos, ayuda al ahorro energético del equipo.
- Otra tecnología que permitiría mejorar la cobertura y el alcance en el campo de batalla del receptor portátil R&S®PR100 es el receptor MIMO (SIMO o diversidad en recepción), el cual adicionalmente elimina los efectos negativos que existen sobre un canal con multitrayectos, puesto que crea una recepción multidimensional que se vale de los múltiples trayectos que sigue la señal en el proceso de transmisión, para mejorar el *througput* y la fiabilidad y reducir la probabilidad de errores. Aquí el *Beamforming* permite aumentar la sensibilidad del dispositivo hacia la dirección donde se está realizando las transmisiones enemigas y gracias a su unidad de procesamiento digital de señales se podría conseguir la DOA para DF.

REFERENCIAS BIBLIOGRÁFICAS

Adamy, D. (2011). ES vs SIGINT. *The Journal of Electronic Defense* .

Alpha-ES GmbH. *Signal Intelligence (SIGINT).* Geretsried.

Bitberry Software ApS; Blomsterhaven 42; DK-4300 Holbaek. (2014). *BitZipper*. Obtenido de Encriptación AES - seguridad de datos: http://www.bitzipper.com/es/aes-encryption.html

Bolaños, M. C. (Octubre de 2009). *Sistema de Guerra Electrónica.* Obtenido de http://es.slideshare.net/daniel_b4e/guerra-electronica

Braun, E. (1992). El radar y la Batalla de Inglaterra. En E. Braun, *Electromagnetismo: De la ciencia a la tecnología.* México.

Díaz, L., & Benjamín, D. (2011). *Propuesta de diseño, para modernizar el Sistema de Interceptación en Telecomunicaciones (SIMTEL), aplicando el sistema COMINT de Guerra Electrónica.* Latacunga.

Digital Voice Systems, Inc. (2014). *DVSI Products*. Obtenido de http://www.dvsinc.com/products/products.htm

Faúndez, M. (2001). *Sistemas de Comunicaciones.* Barcelona: Marcombo.

Gallardo, J. L. (13 de Mayo de 2013). *Blogueros y Corresponsales de la Revolución*. Obtenido de bloguerosrevolucion.ning.com/profiles/blogs/la-guerra-electr-nica-y-su-importancia-para-planificar-las

González, J., & Hoyos, A. (2007). *Modernización y repotenciación del sistema de DF (direction finding) del vehículo de guerra electrónica pasiva de la Fuerza Terrestre Ecuatoriana COMINT y diseño del sistema de comunicación con el vehículo de guerra electrónica activa Jamming.* Sangolquí.

infodefensa.com. (s.f.). Obtenido de Una radiomonitorización más rápida y precisa gracias al receptor portátil de Rohde & Schwarz: http://www.infodefensa.com/latam/2009/03/30/comunicado-una-radiomonitorizacion-mas-rapida-y-precisa-gracias-al-receptor-portatil-de-rohde-schwarz.html

KENWOOD. (2011). *NEXEDGE*. Obtenido de http://nexedge.kenwood.com/technologies.html

Kioskea. (2014). *Introducción al cifrado mediante DES*. Obtenido de http://es.kioskea.net/contents/130-introduccion-al-cifrado-mediante-des

Mosquera, J. (2012). *Rediseño de un Sistema de Radiocomunicaciones VHF, para aprovechar las Ventajas de una Tecnología Digital.* Quito.

Multiradio S.A. (s.f.). Obtenido de Digital Migration with iDAS: www.multiradio.com

National Institute of Standards and Technology - NIST. (26 de Noviembre de 2001). Federal Information Processing Standard, Publication 197, Advanced Encryption Standard. Estados Unidos.

National Security Agency. (9 de Septiembre de 2012). *Signals Intelligence*. Obtenido de www.nsa.gov/sigint/

NXDN Forum. (2012). *Especificaciones Técnicas NXDN, Parte 1: Interfaz de Aire, Sub-parte E: Interface de Aire Común (Tipo-D).*

NXDN Forum Website. (2013). *NXDN.*

NXDN Forum Website. (2014). *NXDN Forum Website*. Recuperado el Enero de 2014, de NXDN: www.nxdn-forum.com

Oblak, J. (s.f.). The AMBE+2™ version 1.6 Vocoder.

Public Safety and Homeland Security Bureau. (2014). *VHF / UHF Narrowbanding Information* . Obtenido de http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html

Rhode&Schwarz. (2014). *Productos*. Recuperado el 01 de 2014, de www.rohde-schwarz.com/en/home_48230.html

Sanfuentes, J. P. (s.f.). *Historia del Radar.* Recuperado el Enero de 2014, de Meteovallirana: www.meteovallirana.es/mediapool/96/966160/data/historia_del_radar.parker.pdf

Secretaría de Gobernación - SEGOB. (12 de 11 de 2013). *Ciclo de Inteligencia*. Obtenido de http://www.cisen.gob.mx/intCicloInt.html

Shami, A., Maier, M., & Assi, C. (2008). *Broadband Access Networks: Technologies and Deployments.* Davis: Biswanath Mukherjee .

Sistema de observación y prospectiva tecnológica - SOPT. (2009). *La Guerra electrónica en España.* Madrid: Secretaría General Técnica del Ministerio de Defensa de España.

Tourrilhes, J. (3 de Agosto de 2000). Wireless Overview - The radio modem. Palo Alto, California, Estados Unidos.

Trobiani, I. A. (2008). *Clasificación Automática de Emisiones Radar Mediante Redes Neuronales.* Buenos Aires.

ACTA DE ENTREGA - RECEPCIÓN

En la ciudad de Sangolquí, a los 20 días del mes de Marzo de 2015, los suscritos Sr. Tnte. Téc. Avc. Jorge Fernando Arellano Carvajal, quien entrega su proyecto de tesis titulado **"INTERCEPTACIÓN, MONITORIZACIÓN Y DEMODULACIÓN NXDN™ DE SEÑALES DIGITALES EN TIEMPO REAL"**, y Sr. Ing. Carlos Paúl Bernal Oñate MSc. Director de la carrera de Ingeniería en Electrónica y Telecomunicaciones de la Universidad de Fuerzas Armadas – ESPE, quien recibe el documento para su posterior registro en el archivo del Departamento de Eléctrica y Electrónica, nos constituimos en las oficinas Departamento de Eléctrica y Electrónica de la Universidad de Fuerzas Armadas – ESPE, con el objeto de realizar la diligencia de entrega - recepción correspondiente.

Para constancia de lo actuado y en fe de conformidad y aceptación, suscriben la presente acta de entrega - recepción las personas que intervienen en esta diligencia.

Tnte. Téc. Avc. Jorge Arellano	Ing. Paul Bernal MSc.
C.C. 180306104-1	C.C. 1709775637
ENTREGUÉ CONFORME	**RECIBÍ CONFORME**