UNIVERSIDAD DEL CEMA
Buenos Aires
Argentina

Serie
DOCUMENTOS DE TRABAJO

Área: Ingeniería Informática

TRANSMISIÓN DE MENSAJES ENCRIPTADOS EN SISTEMAS DE RADIO HF

Gabriel López

Noviembre 2018
Nro. 666

www.cema.edu.ar/publicaciones/doc_trabajo.html
UCEMA: Av. Córdoba 374, C1054AAP Buenos Aires, Argentina
ISSN 1668-4575 (impreso), ISSN 1668-4583 (en línea)
Editor: Jorge M. Streb; asistente editorial: Valeria Dowding <jae@cema.edu.ar>

TRANSMISIÓN DE MENSAJES ENCRIPTADOS EN SISTEMAS DE RADIO HF

Ing. Gabriel López[*]

Noviembre 2018

Resumen: El presente trabajo pretende analizar la factibilidad para establecer una posible arquitectura de infraestructura y de aplicaciones destinado a la transmisión de voz y datos, que integre el empleo de equipos de transmisión HF de carácter propietario, el desarrollo de aplicaciones de Software de uso libre, el empleo protocolos de transmisión de carácter propietario y el empleo de algoritmos de encriptado de uso libre, con la finalidad de incrementar la seguridad en una red radioeléctrica de transmisión de datos.

A fin de poder comprender la finalidad de este trabajo se describirá la arquitectura del Sistema Integrado de Comunicaciones de Área (ITACS) presentado por la firma HARRIS (sistema de comunicaciones que entrega capacidades de interoperatividad entre todas las bandas y trabajo en redes LAN/WAN), con la finalidad de poder conocer su funcionamiento. También es necesario describir el protocolo de encriptado TRIVIUM para empleo del resguardo de datos a ser transferidos por HF. con la finalidad de poder ser integrado a nuevos desarrollos de software. Por último, se describen los protocolos de transmisión y encriptado de carácter propietario que emplean actualmente los equipos de radio.

[*] Los puntos de vista del autor no necesariamente representan la posición de la Universidad del Cema.

Tabla de Contenidos

Contenido:

I. Introducción

Pensar que no es necesario preservar la información sensible de una organización, es ponerla en riesgo, por tal motivo desde los mismos comienzos de la escritura, se tomaban todas las medidas necesarias para resguardar la misma.

En la actualidad la transmisión de datos basadas en nuevas tecnologías son empleadas en todos los niveles que componen a las organizaciones, ya sea estratégico, operativo y administrativo.

Las bases de datos, los sistemas informáticos, las telecomunicaciones y las facilidades multimedia se emplean para apoyar procesos tales como la toma de decisiones, la comunicación interna y externa y la gestión del conocimiento.

Con su uso, todos los niveles organizacionales se benefician al incorporar mejoras en los procesos de negocio, en sus procedimientos y también como parte componente de su cultura.

Aquellas organizaciones, que realizan procesos de alto riesgo, han incorporado nuevos medios de comunicaciones con la finalidad de incrementar la eficiencia a la hora de tener que tomar decisiones.

El solo hecho de la incorporación de estas nuevas herramientas, no asegura que la organización en cuestión esté en óptimas condiciones de responder en forma eficaz y eficiente ante un evento que se le presente.

Para efectuar previsiones y estar en capacidad de afrontar las mencionadas situaciones, la protección de los datos y de la información resulta esencial y esto se ha perfeccionado con el transcurso del tiempo.

Con la incorporación y el empleo de estos sistemas y de las tecnologías de la comunicación bajo un enfoque sinérgico, se logra que se generen entornos de trabajo que alcanzan resultados superiores al trabajo individual, permitiendo preservar el secreto de la información, el intercambio seguro de las mismas y la seguridad de que sean recibidas en tiempo y forma.

I.I Internet

Un cambio radical que ha sucedido en lo referente al acceso a la información es el uso de Internet. .

Cada organización desarrolla o incorpora sistemas que le permiten dar una solución a los problemas que son inherentes a las funciones que ejecutan. En tal sentido es aquí donde las comunicaciones son de una importante utilidad para las organizaciones.

El aspecto más importante que resaltar del empleo de las comunicaciones es que las mismas permiten que la información fluya con mayor rapidez, lo que posibilita su rápida difusión, uso y empleo, sobre

todo en lo que respecta a la necesidad de la misma al ser empleada como un importante requisito en el apoyo a la toma de decisiones.

A medida que el uso de Internet se expande la criptografía se hace cada vez más necesaria e intrusiva, se recibe y se envía información encriptado de manera transparente, como por ejemplo cada vez que se ingresa a un sitio de bancos y se ejecutan transacciones monetarias.

El desarrollo de estos sistemas criptográficos requiere de expertos en informática, en sistemas, en comunicaciones, en estadística y en matemáticas, por mencionar algunos.

A la hora de tener que desarrollar un sistema criptográfico es necesario la confluencia de todos los especialistas mencionados anteriormente.

I.II Comunicaciones.

El inventor e ingeniero italiano Guglielmo Marconi, ganador del Nobel de Física en 1909, patentó el primer sistema útil de telegrafía sin hilos, a través de señales por radio. En 1901 estableció comunicación inalámbrica entre Europa y América.

En 1933 Edwin Armstrong describe un sistema de radio de alta calidad, inmune a los parásitos radioeléctricos, utilizando la modulación de frecuencia (FM). A finales de la década este procedimiento se establece de forma comercial, al montar a su cargo el propio Armstrong una emisora con este sistema.

En 1963, se establece la primera comunicación radio vía satélite.

A principios de los 90, experimentadores radioaficionados comienzan a utilizar ordenadores personales para procesar señales de radio mediante distintas interfaces (Radio Packet).

Hoy en día la radio a través de Internet avanza con celeridad, por eso, muchas de las grandes emisoras de radio empieza a experimentar con emisiones por internet, la primera y más sencilla es una emisión on-line.([1])

I.III Criptografía.

La palabra criptografía proviene del griego kryptos, que significa esconder y gráphein, escribir, es decir, escritura escondida.

La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

[1] Extracto de breve historia de las comunicaciones http://www.icarito.cl/enciclopedia/articulo/segundo-ciclo-basico/educacion-tecnologica/historia-de-la-tecnologia/2009/12/71-6278-9-4-medios-de-comunicacion-electronicos.shtml

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o descencriptar)

Algunos de los ejemplos de su uso son la protección de archivos informáticos y la protección de transacciones financieras informáticas.

La criptografía tiene grandes conexiones con las ciencias informáticas, matemáticas y el análisis de algoritmos.

El progreso de la informática ha beneficiado tanto a la criptografía como a los criptógrafos.

II. Marco Teórico.

II.I Clasificación de las frecuencias de radio.

- Frecuencias Extremadamente Bajas: Llamadas ELF, (Extremely Low Frequencies)
  Son aquellas que se encuentran en el intervalo de 3 a 30 Hz.
- Frecuencias Super Bajas: Llamadas SLF, (Super Low Frequencies)
  Son aquellas que se encuentran en el intervalo de 30 a 300 Hz.
- Frecuencias Ultra Bajas: Llamadas ULF, (Ultra Low Frequencies)
  Son aquellas que se encuentran en el intervalo de 300 a 3000 Hz
- Frecuencias Muy Bajas: Llamadas VLF, (Very Low Frequencies)
  Son aquellas que se encuentran en el intervalo de 3 a 30 kHz.
  El intervalo de VLF es usado típicamente en comunicaciones gubernamentales y militares.
- Frecuencias Bajas: Llamadas LF, (Low Frequencies)
  Son aquellas que se encuentran en el intervalo de 30 a 300 kHz. Los principales servicios de comunicaciones que trabajan en este rango están la navegación aeronáutica y marina.
- Frecuencias Medias: Llamadas MF, (Medium Frequencies)
  Son aquellas que se encuentran en el intervalo de 300 a 3000 kHz. Las ondas más importantes en este rango son las de radiodifusión de AM (530 a 1605 kHz).
- Frecuencias Altas: Llamadas HF, (High Frequencies)
  Son aquellas que se encuentran en el intervalo de 3 a 30 MHz. A estas se les conoce también como "onda corta". Es en este intervalo que se tiene una amplia gama de tipos de radiocomunicaciones como radiodifusión, comunicaciones gubernamentales y militares. Las

comunicaciones en banda de radioaficionados y banda civil también ocurren en esta parte del espectro.

- Frecuencias Muy Altas: Llamadas VHF, (Very High Frequencies)

  Son aquellas que se encuentran en el intervalo de 30 a 300 MHz. Es un rango popular usado para muchos servicios, como la radio móvil, comunicaciones marinas y aeronáuticas, transmisión de radio en FM (88 a 108 MHz) y los canales de televisión del 2 al 12 [según norma CCIR (Estándar B+G Europa)]. También hay varias bandas de radioaficionados en este rango.

- Frecuencias Ultra Altas: Llamadas UHF, (Ultra High Frequencies)

  Son aquellas que se encuentran en el intervalo de 300 a 3000 MHz, incluye los canales de televisión de UHF, es decir, del 21 al 69 [según norma CCIR (Estándar B+G Europa)] y se usan también en servicios móviles de comunicación en tierra, en servicios de telefonía celular y en comunicaciones militares.

- Frecuencias Super Altas: Llamadas SHF, (Super High Frequencies)

  Son aquellas que se encuentran en el intervalo de 3 y 30 GHz y son ampliamente utilizadas para comunicaciones vía satélite y radioenlaces terrestres. Además, pretenden utilizarse en comunicaciones de alta tasa de transmisión de datos a muy corto alcance mediante UWB. También son utilizadas con fines militares, por ejemplo en radares basados en UWB.

- Frecuencias Extremadamente Altas: Llamadas EHF, (Extrematedly High Frequencies)

  Son aquellas que se encuentran en el intervalo de 30 a 300 GHz. Los equipos usados para transmitir y recibir estas señales son más complejos y costosos, por lo que no están muy difundidos aún.

Nombre	Abreviatura	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
Extra baja frecuencia	ELF	1	3-30 Hz	100.000–10.000 km
Súper baja frecuencia	SLF	2	30-300 Hz	10.000–1000 km
Ultra baja frecuencia	ULF	3	300–3000 Hz	1000–100 km
Muy baja frecuencia	VLF	4	3–30 kHz	100–10 km
Baja frecuencia	LF	5	30–300 kHz	10–1 km
Media frecuencia	MF	6	300–3000 kHz	1 km – 100 m
Alta frecuencia	HF	7	3–30 MHz	100–10 m
Muy alta frecuencia	VHF	8	30–300 MHz	10–1 m
Ultra alta frecuencia	UHF	9	300–3000 MHz	1 m – 100 mm
Súper alta frecuencia	SHF	10	3-30 GHz	100-10 mm
Extra alta frecuencia	EHF	11	30-300 GHz	10–1 mm

Gráfico Nro. 1 – Tabla clasificación de las ondas de radio.

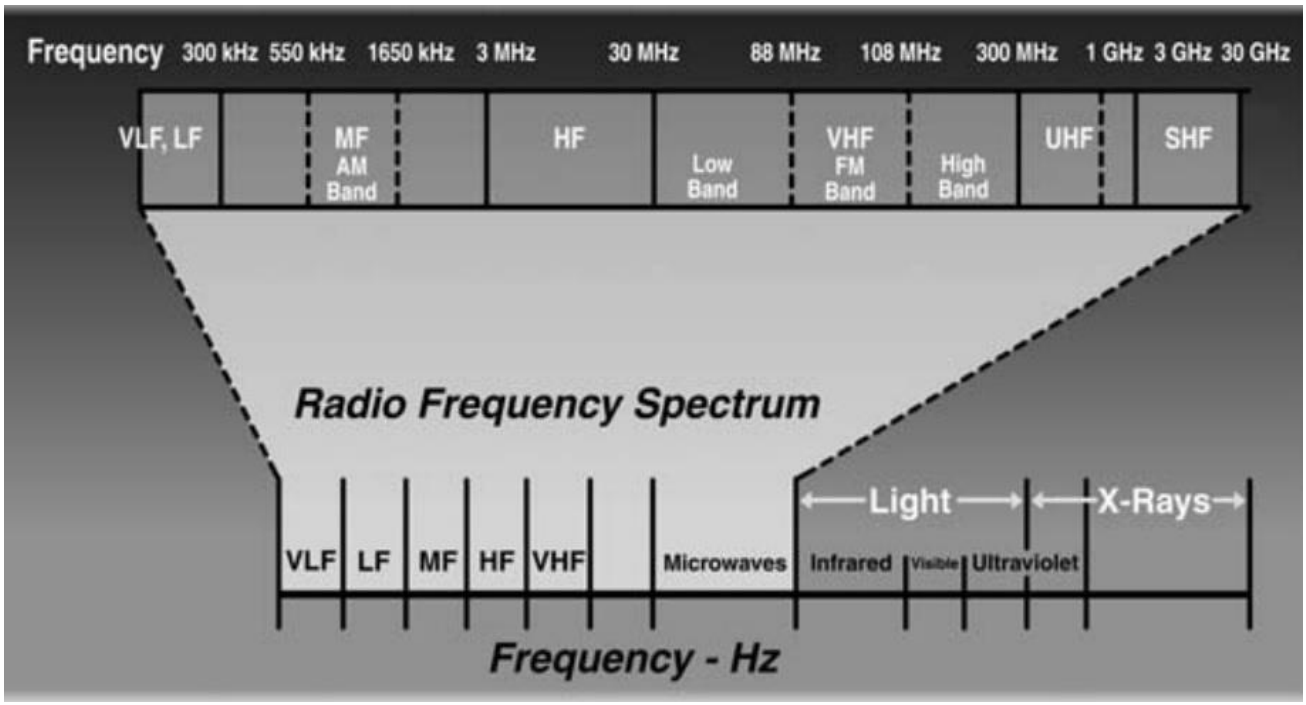

Gráfico Nro. 2 – Tabla del espectro de frecuencia de las ondas de radio.

II.II Mejoramiento del uso de la banda de HF

Es la banda de frecuencias del espectro radioeléctrico comprendidas entre los 3 MHz y los 30 MHz.

Las ondas de radio de la banda de HF se propagan fundamentalmente por reflexión en la ionosfera.

Dado que las longitudes de onda correspondientes son del orden de las decenas de metros, la banda de HF también recibe el nombre de banda decamétrica.

- Empleo de frecuencias de radio HF.

  La transmisión en HF, se puede utilizar para ser empleada en:

  - Transmisión Línea de Vista (Line Of Sight – LOS):

    Alcance: Normalmente menos de 30 km.

    Ventaja: Permite la posibilidad de alta velocidad de transmisión de datos.

    Limitaciones: Por obstáculos del terreno o curvatura de la tierra.

    Otros factores: El rango de alcance está también en función de la altura de antena, la frecuencia y el nivel de potencia.

  - Onda Superficial de Tierra (Ground Surface Wave – GSW):

    Alcance: Útil es de hasta 50 km sobre la tierra, 300 o más kilómetros sobre el mar.

    Ventaja: La tasa de transferencia de datos son generalmente altas, pero pueden haber algunas limitaciones dependiendo de la forma de onda usadas.

    Limitaciones: El alcance depende de funcionamiento frecuencia y obstrucciones del terreno. Requiere antenas verticalmente polarizadas.

    Otros factores: Históricamente utilizado para comunicaciones de voz.

  - Más Allá Línea de Vista (Beyond Line Of Sight – BLOS):

    Alcance: 400 km con cerca de incidencia Vertical de la ionosfera (NVIS). 2

    Ventaja: No está limitada por la obstrucción terreno, puede comunicarse a través de montañas etc.

    Limitaciones: El funcionamiento a menudo depende de las condiciones de la ionosfera y de los ciclos solares. Establecimiento de enlace automático (Authomatic Link estableshiment – ALE): ayuda a resolver el problema de selección de frecuencia operativo.

    Otros factores: Requiere antenas polarizadas horizontalmente.

    Frecuencias generalmente restricción a < 10 MHz. + voz o baja/media velocidad de datos, la tasa de transferencia de datos depende de la forma de onda.

  - Comunicaciones de largo alcance (Long Range Communications – LRC)

    Alcance: Hasta 4.000 kilómetros y más allá.

    Ventajas: La misma radio de HF puede proporcionar comunicaciones que van de corto alcance a largo alcance.

Limitaciones: Rango depende de la antena, nivel de potencia, las condiciones atmosféricas. La selección de frecuencia de operación es más difícil, emplear ALE es muy útil aquí. A menudo requiere antenas direccionales.

Otros factores: Después de la II Guerra Mundial, la industria de comunicaciones dio vuelta su atención a otras tecnologías, conduciendo a un período de lento crecimiento en las comunicaciones de radio de alta frecuencia (HF) durante la década de 1960 y 1970.

Como resultado de eso, muchos comunicadores actuales no tienen una comprensión de lo que son las capacidades modernas de comunicación de HF.

Con la incorporación de la tecnología digital, la comunicación por radio de HF se debe considerar como una ventaja y se deben explotar la versatilidad del medio, incluso en los niveles de baja potencia.

II.III Introducción al Establecimiento Automático de Enlace. (Automatic Link Establishment – ALE).

Es el modo de operación en HF que permite la transmisión de señales de voz y datos a otras estaciones de una red a través de uno o varios conjuntos de frecuencias acordados previamente.

Siendo Internet de acceso masivo, ha generado una gran demanda y uso en lo que respecta a las comunicaciones de banda ancha.

Se desarrollan aplicaciones que hacen uso de datos más pesaos y críticos, como ser imágenes, audio y vídeo.

Estas nuevas aplicaciones pueden transmitir datos entre ellas y con el empleo de la banda ancha permiten de esta manera la transmisión de información a gran velocidad ya sea de imágenes, video, audio y datos.

Las comunicaciones de HF, dependen tanto de la frecuencia utilizada como de las condiciones atmosféricas. Pero ciertos eventos naturales pueden afectar las transmisiones radiales como ser las tormentas eléctricas o la radiación solar, disminuyendo en forma sensible su capacidad y hasta anulando la misma.

Otros factores que pueden disminuir la eficacia de las comunicaciones pueden ser variación de las condiciones de propagación a lo largo de una comunicación, una baja relación de Señal/Ruido, ruido e interferencias que afectan la tasa de transmisión de datos, múltiples trayectorias de la señal y la estabilidad del enlace.

Disminuir la incidencia de estos factores impone un gran desafío a superar, de forma de utilizar este medio como soporte de comunicaciones de banda ancha en cuenta en el momento de transmitir datos, y sobre todo si se quiere transmitir datos a muy alta velocidad.

Recientemente se ha liberado el estándar MIL-STD-188-110C que contiene un apéndice D en el que se define una nueva familia de protocolos para la transmisión de datos a alta velocidad utilizando anchos de banda de 3 Khz a 24 Khz, en pasos de 3 Khz. Esta familia de protocolos está apoyada módems equipados con tecnología MIL-STD-188-110B.

Todas estas tecnologías han hecho desarrollar lo que se conoce ALE-4G, cuarta generación del estándar ALE.

Las radios que implementan los modos ALE disponen de una base de datos interna en la que se almacena información sobre la calidad de los enlaces, de forma que al establecerse un enlace con otra estación se utilizará la frecuencia más óptima, en base a mediciones en las que se tiene en cuenta la relación señal a ruido (SNR) disponible.

La utilización de ALE requiere la selección previa de un conjunto de frecuencias, cuyo número suele oscilar entre 4 y 7, con el objetivo de establecer los enlaces de la forma más rápida posible.

ALE fue desarrollado con varios objetivos, entre ellos facilitar el trabajo de los operadores de radio HF y establecer un estándar de interoperabilidad.

Actualmente, existen las siguientes variantes de ALE:

- ALE 2G.

  Definido en 1988 a través del estándar MIL-STD-188-141A y del estándar civil FED-STD-1045A.

  Se trata del estándar de facto mundial para ALE. Actualmente, las especificaciones para ALE 2G se recogen en el estándar MIL-STD-188-141B.

- ALE 3G.

  Definido a finales de los 90 en el estándar MIL-STD-188-141B, ampliando las capacidades de 2G pero manteniendo la interoperabilidad con el mismo.

  En ALE 3G, todas las estaciones de una malla escanean las frecuencias de forma sincronizada, al contrario de lo que sucede en 2G.

  Por otro lado, la forma de onda de los módems 3G es más robusta que la de los 2G, permitiendo el establecimiento de enlace con peores condiciones de propagación.

La esencia de los sistemas ALE es la selección automática de canal, el escaneo de canales en la recepción y un procedimiento de llamada selectiva que emplea módems digitales robustos que permiten el establecimiento rápido de enlaces entre la estación que llama y la llamada.

II.IV Introducción Ventajas del empleo de ALE

- Transmisión de datos:

  En los modernos equipos de radio se puede incorporar un receptor GPS, pidiendo de esta manera enviar información precisa, como ser posición, distancia, estado, etc., a través de redes de la comunicación en forma periódica o por solicitud.

  La información de posicionamiento también puede ser enviada usando el modo Push, para asegurar la salida de los mensajes.

  Los equipos también poseen una interfaz de Ethernet LAN, conexión USB, dispositivo de almacenamiento, conexión a impresora y cámara de video.

- Robustez:

  La incorporación de certificados interoperables (Joint Interoperability Test Command – JITC) y de los protocolo STANAG 5066 y el protocolo de transferencia de datos comprimido (Compressed File Transfer Ptotocol – CFTP), se puede garantizar la transferencia de datos libre de errores a través del enlace de radio.

  Por otra parte, la radio puede configurarse para utilizar el protocolo STANAG 4538 (3G ALE) de enlace rápido y los protocolos ARQ Set-up (FLSU) y ARQ (Automatic Repeat-reQuest) que son protocolos utilizados para el control de errores en la transmisión de datos, garantizando de esta forma la integridad de estos y lograr una transmisión de datos libre de errores.

- Seguridad

  Todas las comunicaciones por aire son de extremo a extremo y cifradas.

  El acceso a la unidad está restringido por medio de un Número de Identificación Personal (PIN).

  Todos los mensajes almacenados localmente están cifrados.

  Una función Zeroize se presta desde el teclado, que elimina todas las claves criptográficas y la información confidencial.

II.V Protocolo Propietario y el problema de la transmisión segura.

Las organizaciones requieren procesar altos volúmenes de información, para lo cual deben transmitir y recibir en todo tiempo.

Esto genera un gran volumen de tráfico y como resultado de esto se produce la saturación del espectro en la banda HF.

Por un lado, existe el problema de la gran transmisión de datos y la poca disponibilidad de ancho de banda para la frecuencia de HF. (Esto se soluciona en gran medida con la implementación del protocolo ALE.)

El segundo problema es la transmisión de datos segura, es decir sin que sea capturada por otra persona. (Esto se soluciona en gran medida con la implementación de la criptografía dentro de las radios.)

Pero la mayoría de los equipos de radio que tiene incorporados módulos de criptografía dentro de su equipamiento, son de carácter propietario, lo que no permite conocer como es el proceso de encriptado de la información.

Si a esta limitación se le incorpora la posibilidad de que alguien fuera de la organización cuente con los mismos sistemas de radios, es muy probable que esa información, aunque sea transmitida en forma encriptada, pueda ser capturada y pasada a texto claro, poniendo en riesgo a toda la organización.

Para superar los mencionados problemas es necesaria la creación de módulos de aplicaciones por fuera de estos sistemas cerrados, de tal manera que se pueda preservar la seguridad, la confidencialidad y la integridad de la información a transmitir.

Para lo cual es necesario comprender el funcionamiento de la transmisión de datos por paquetes en la frecuencia de la banda HF.

Las radios poseen la funcionalidad de conexión de datos que, sumado a la capacidad de Desarrollo de módulos de Software específicos por terceros, lo que permite incrementar sus capacidades y su funcionalidad.

Se pueden desarrollar módulos bajo los siguientes sistemas operativos:

- Windows PCs
- Mobile 6.x PDAs

Posee la siguiente capacidad de envío de mensajes.

- Mensajes de texto.
- Mensajes de Formato Variable (VMF)

- Cursor On Target (COT) en progreso.
- JC3IEDM en progreso
- Mensajes de texto: permiten múltiples ventanas para traspaso de información a nivel individual o grupos.
- Mensajes VMF.
- Mensajes de Cursor on Target (COT), permite interfaces a otros sistemas de usan COT.
- Mensajes basados en la plataforma de intercambio de datos e información en conjunto C3.

II.VI El desarrollo de aplicaciones sobre radios.

Los nuevos equipos de radio poseen conexión a puerto con interfaz de red 10Base2 o 10BaseT a las redes externas, lo que permite que estos dispositivos puedan establecer enlaces de datos con computadoras y ejecutar aplicaciones que tomen como input los datos provenientes por las radios a efectos de ser procesados y mostrados en pantalla.

El modem serial de 9600 bps que cumple con los estándares STANAG 4539 y MIL-STD-188-110B, maximiza el procesamiento de mensajes, imágenes, conocimiento situacional y otros datos.

Las radios son construidas sobre una plataforma digital común con un controlador de red integrado, permitiendo que las radios provean comunicaciones para aplicaciones basadas en red, tales como conocimiento situacional, mapeo, mensajería y manejo de la información, permitiendo de esta manera la transmisión de datos de alta velocidad

Las radios propietarias poseen un software de Aplicación de Programación de Radio (RPA) embebido, incluido en el dispositivo para facilitar la generación y descarga de los parámetros de configuración.

El RPA ayuda a eliminar errores de programación que pudieran ocurrir cuando el ingreso de datos se hace manualmente.

Otro software embebido es el "Chat", que es una aplicación basada en la plataforma Windows que proporciona mensajería instantánea y transferencia de archivos utilizando las capacidades de tercera generación de las radios.

II.VII Encriptación y Algoritmos

III.VII.I. El problema de la encripción Incorporada:

Los sistemas de radio tienen incorporado el módulo de encriptado Citadel®, que es el que provee la seguridad de voz y datos.

La encriptación incorporada y el uso extensivo de los Protocolos de Internet estándar aseguran que las comunicaciones sean sencillas, perfectas y seguras.

Como se mencionó al principio del trabajo este módulo de cifrado es de carácter propietario, es decir que no se puede acceder al código ni a sus funciones, de tal manera que no puede ser modificado.

Es decir que, en el caso de una transmisión de datos en texto claro, la radio mediante el empleo del módulo de encriptado Citadel®, realiza el cifrado del mismo y lo envía a otra estación a efectos de que sea descifrado y leído por el receptor.

De esta manera se asegura la confidencialidad, la autenticidad y la seguridad del mensaje, pero la pregunta a formularse es que pasa si alguien posee el mismo equipamiento y puede capturar el mensaje transmitido.

El atacante tendría acaso acceso al mensaje y de esta forma se violaría la confidencialidad, la autenticidad y la seguridad, pudiendo producir graves inconvenientes.

Una forma de salvar el problema es desarrollando aplicaciones, en entorno Windows para que sea interoperable con las radios, que procedan a cifrar mensajes, armando los paquetes para la transferencia de datos y enviándolos a la radio para que ahora si sean cifrados por el módulo de encriptado Citadel®.

En el caso que el mensaje sea interceptado, al poder descifrarlo solo tendría acceso al texto cifrado por la aplicación desarrollada y no al texto claro original, de esta manera se podría conservar la confidencialidad, la autenticidad y la seguridad del mensaje.

III.VII.II. El algoritmo TRIVIUM

- Generalidades de un cifrado en cadena.

Existe el Criptosistema perfecto, un algoritmo que permite que el mensaje cifrado jamás pueda ser descifrado por quien no sea el auténtico receptor del mismo. Fue creado en 1917 por Vernan y Mauborgne en los laboratorios de la empresa AT&T. Se debe tener una clave de igual longitud a la del mensaje a transmitir.

El emisor y el receptor deben tener una copia de la misma y cada uno debe destruirla al acabar de usarla, pues si se reutiliza el sistema pierde la seguridad.

Esa es la razón por la que se le conoce con el nombre de Cuaderno de Uso Único o One Time Pad. La clave debe ser aleatoria y se usa tanto para cifrar como para descifrar.

Es por ello que el emisor y el receptor deben compartir la clave y mantenerla secreta y se lo clasifica a este criptosistema como Simétrico o de Clave Secreta.

Shannon, en 1949 demostró la invulnerabilidad de este esquema al satisfacer los requerimientos de Secreto Perfecto de la naciente Teoría de la Información.

Sin embargo, podemos apreciar dos debilidades, no en el sistema propiamente dicho, sino en la implementación en el mundo real del mismo: el problema de la generación y la distribución de las claves por canales seguros.

Una propuesta de solución para el problema de la generación es que un procedimiento determinístico pueda generar la clave y así realizar el cifrado. Tal clave no sería aleatoria, sino Pseudo-aleatoria y debiera satisfacer requerimientos adicionales para hacerla criptográficamente segura.

En la moderna era binaria la clave es una enorme secuencia de bits y el cifrado/descifrado se realiza por una simple suma bit a bit xor entre el mensaje y la clave.

- LFSR y Non-LFSR.

Hoy en día es ampliamente conocido el uso de Linear Feedback Shift Register (LFSR) para generar secuencias pseudo-aleatorias con período y complejidad lineal controladas.

En la actualidad se cuenta con una importante cantidad de resultados y aplicaciones: para el diseño de algoritmos criptogaficos, para el análisis de la complejidad de una secuencia binaria (algoritmo de Berlekamp-Massey), para códigos correctores de errores y para generación de claves. Sin embargo, debido a su naturaleza lineal, los LFSRs resultan ser por sí sólo inseguros: es sabido que cuando 2n bits (consecutivos) de la secuencia de salida de un LFSR es conocida, toda la sucesión resulta ser totalmente predecible.

Asimismo, diseños de sistemas basados en LFSRs intentan agregar no linealidad combinando entre otras cosas sus salidas a través de una función no lineal, sin embargo esto tampoco ofrece la seguridad deseada.

Mientras que la teoría detrás de los LFSRs es sólida y bien entendida, muchos problemas fundamentales relacionados con los NLFSRs son problemas abiertos, uno de ellos por ejemplo, es determinar el período (o una cota del período) de la secuencia de salida de un NLFSR.

En los últimos años ha comenzado a aparecer literatura en torno a estos registros no lineales y también sistemas de cifrado en cadena (stream ciphers) que utilizan de alguna manera

NLFSRs, tal es el caso de la familia TRIVIUM [De Cannière-Preneel], BIVIUM[], CUADRIVIUM[].

El algoritmo Trivium ha resultado ser finalista en el concurso europeo e-Stream del año 2005 [4]. Al día de hoy, al aplicarle diferentes técnicas de criptoanálisis no se conocen ataques efectivos contra este generador [2, 3, 4].

En el año 2012 la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) han publicado la norma ISO/IEC 29192-3:2012. En ella se especifican dos algoritmos de cifrado de flujo para ser utilizados en criptografía liviana: el Enocoro y el Trivium.

Hoy en día es ampliamente conocido el uso de Linear Feedback Shift Register (LFSR) para generar secuencias pseudo-aleatorias con período y complejidad lineal controladas. Aunque el estudio de los LFSRs comenzó alrededor de los años `60 [5, 6] y continuó durante mucho tiempo.

Los Nonlinear Feedback Shift Register (NLFSs), son una generalización de los anteriores y resultaron estar por mucho tiempo postergados. Sin embargo, se revitalizó su estudio con el advenimiento de la llamada "Criptografía Liviana": la criptografía que puede ser montada sobre plataformas de poco poder de cálculo como una tablet o un teléfono inteligente.

Pero también en una cantidad de otros dispositivos tales como marcapasos, procesadores centrales montados en autos de alta gama, grúas, tractores y cosechadoras de alto desempeño, entre otros.

- Seudo-Còdigo del Trivium

INPUT: s0, s1,...,s287 initial state, integer n., si ε {0,1}.

OUTPUT: binary sequence {kt}

1.Initialization.

t1 = s65 ⊕ s92

t2 = s161 ⊕ s176

[2] McDonald, C. and Pieprzyk, C. "Attacking Bivium with MiniSat", Cryptology ePrint Archive, Report 2007/040, 2007

[3] Raddum, H."Cryptanalytic Results on Trivium", eSTREAM, ECRYPT Stream Cipher Project, Report 2006/039, 2006

[4] Maximov, A. and Biryukov, A. "Two Trivial Attacks on Trivium", Selected Areas in Cryptography, Lecture Notes in Computer Science, Vol.4876, Springer, 2007.

[5] Golomb. "Shift Register Sequences". Aegean Park Press, 1982.

[6] Massey, J.L. "Shift-register synthesis and BCH decoding". IEEE Transactions on Information Theory 15, 1969

t3 = s242 ⊕ s287

2.While (t<n) do the following:

2.1 kt = t1⊕ t2 ⊕ t3

2.2 t1 = t1 ⊕ s90 ⊗s91 ⊕ s170
t2 = t2 ⊕ s174⊗s175 ⊕ s263
t3 =t3 ⊕ s285⊗s286 ⊕ s68

2.3 (s0;s1;..;s92) =(t3;s0;..;s91)
(s93;s94;..;s176) =(t1;s93;..;s175)
(s177,s178;..;s287)=(t2;s177;..;s285)

3.Return {kt}

El algoritmo que se propondrá entonces para ser implementado es el algoritmo TRIVIUM, que tiene la cualidad de realizar operaciones lógicas, por lo que su implementación resulta favorable tanto en hardware como en software, en términos de ciclos informáticos; obteniendo así un sistema de cifrado potente y capaz de ser utilizado en equipos de recursos limitados.

Este sistema proporcionará las siguientes funcionalidades:

- El módulo cifrará (bajo el algortimo Trivium) toda captura de datos.
- El Software verificará si la secuencia generada por el módulo de cifrado corresponde a una secuencia lógica.
- El módulo descifrador (con la secuencia descifradora) embebido en la PC descifrará la información recibida.

Diagrama de flujo de la implementación del módulo cifrador

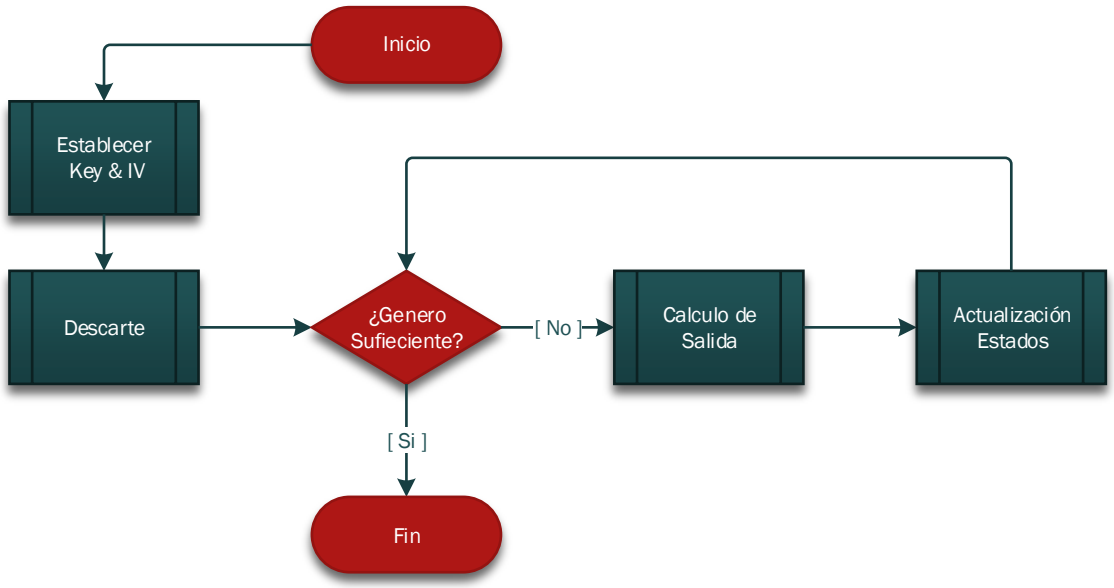

Gráfico Nro. 3 – Diagrama de flujo del módulo cifrador [7]

Diagrama de flujo de la implementación del módulo descifrador

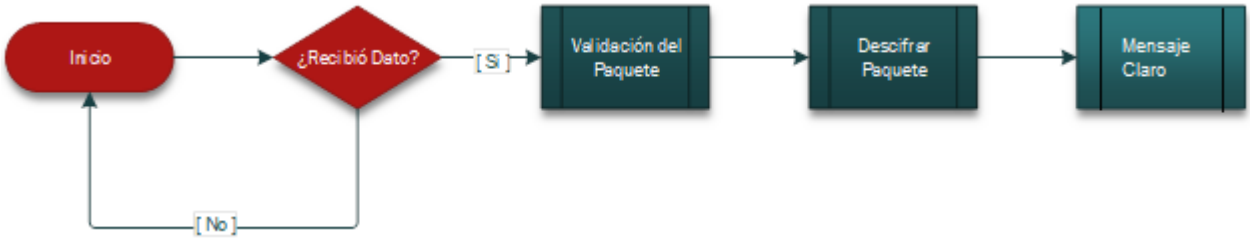

Gráfico Nro. 4 – Diagrama de flujo del módulo descifrador [8]

Para la implementación de la comunicación entre el microcontrolador y la antena RF se optó por la utilización del protocolo de comunicación SPI, por sobre I2C.

[7] Proyecto de Promoción y Síntesis - Sistema de Cifrado de Imágenes bajo Trivium (SCIT) Año 21014 Alumnos
[8] Proyecto de Promoción y Síntesis - Sistema de Cifrado de Imágenes bajo Trivium (SCIT) Año 21014 Alumnos

Al estar priorizando la tasa de transferencia por sobre otras ponderaciones, el SPI es el protocolo a utilizar sobre el I2C.

Por un lado SPI es un protocolo full-duplex, mientras que I2C no lo es.

Asimismo, SPI no define ningún límite de velocidad específico y su implementación normalmente llega a velocidades superiores a los 10 Mbps.

Por el otro lado, el protocolo I²C está limitado a 1Mbps en "Fast Mode" y a 3.4 Mbps en "High Speed Mode", mientras que este último requiere buffers de entrada y salida específicos, no siendo estos de fácil adquisición.

SPI	I2C
Requiere conexión mediante 3 o 4 cables	Requiere solamente conexión mediante 2 cables
Soporta alta velocidad de comunicación full-duplex	Su concepto de "alta velocidad" resulta ser de menor tasa que la del SPI
Consume menos energía	Consume más energía
Requiere señales adicionales para administración múltiples dispositivos en el mismo bus	Soporta múltiples dispositivos en el mismo bus de transmisión sin la necesidad de añadir señales
No verifica que la información haya sido recibida correctamente	Verifica la transmisión de la información mediante el dispositivo esclavo
No es capaz de transmitir PCB	Puede transmitir PCB a bajas velocidades
Es más caro de implementar	Es más barato de implementar
Solamente soporta un único dispositivo maestro en el bus de comunicación	Soporta múltiples dispositivos maestros
Es más susceptible al ruido que I2C	Es menos susceptible al ruido
Sólo puede enviar información en distancias cortas	Puede enviar información en distancias largas, con una tasa de transferencia menor

Grafico Nro. 5 – Tabla comparativa del protocolo SPI e I2C. [9]

[9] Proyecto de Promoción y Síntesis - Sistema de Cifrado de Imágenes bajo Trivium (SCIT) Año 21014 Alumnos

III. Conclusiones.

El presente trabajo está enfocado en el marco de integrar desarrollos ya implementados o tomar como base explicaciones teóricas ya abordadas, con la finalidad de interrelacionar componentes que no fueron desarrollados específicamente para resolver el problema planteado, pero que por medio de la vinculación de conocimiento se pueda elaborar una posible solución al tema presentado.

No se pretende desarrollar aplicaciones de ningún tipo, ni realizar mejoras en el equipamiento. Sin embargo, la explotación de las capacidades de los desarrollos sobre la posibilidades de escalamiento que presentan los equipos de tecnologías modernas, permiten maximizar los logros, superando barreras que presentan dificultades que no son franqueables simplemente con la aplicación de soluciones de mercado.

Por lo que queda propuesta una posible solución la cual no sería alcanzable sin la intervención de un equipo multidisciplinario y con la participación de los diferentes actores involucrados.

IV. Glosario

Abreviatura	Significado	Traducción
ADP	Aplicación de desarrollo propio	Aplicación de desarrollo propio
AM	Amplitude Modulation	Amplitud modulada
ALE	Automatic Link Establishment	Establecimiento automático de enlace
BLOS	Beyond Line Of Sight	Más Allá Línea de Vista
CCIR	International Radio Consultative Committe	Comité Consultivo Internacional de Radio Comunicaciones
COT	Cursor on Target	Cursor on target
EHF	Extrematedly High Frequencies	Extra alta frecuencia
ELF	Extremely Low Frequencies	Extra baja frecuencia
FM	Frecuency Modulation	Frecuencia Modulada
GSW	Ground Surface Wave	Onda Superficial de Tierra
HF	High Frequencies	Alta frecuencia
JC3IEDM	Joint C3 Information Exchange Data Model	Modelo de intercambio de datos conjunto C3
LF	Low Frequencies	Baja frecuencia
LOS	Line Of Sight	Transmisión Línea de Vista
LRC	Long Range Communications	Comunicaciones de largo alcance
MHz	Mega Hertz	Mega Hertz
MF	Medium Frequencies	Media frecuencia
RPA	Radio Programming Aplication	Aplicación de Programación de Radio
SHF	Super High Frequencies	Súper alta frecuencia
SLF	Super Low Frequencies	Súper baja frecuencia
STANAG	Standardization Agreement	Acuerdo de Normalización
UHF	Ultra High Frequencies	Ultra alta frecuencia
UIT	International Communication Union	Unión Internacional de Comunicaciones
ULF	Ultra Low Frequencies	Ultra baja frecuencia
UWB	Ultrta Wide Band	Ultra banda Ancha
VHF	Very High Frequencies	Muy alta frecuencia
VLF	Very Low Frequencies	Muy baja frecuencia
XML	eXtensible Markup Language	lenguaje de Marcas Extensible

V. Tabla de cuadros y gráficos

VI. Bibliografía

- RadioCom-DigitalAge1 – Segunda edición octubre de 2005, Harris Corporation 2005 Library of Congress Catalog Card Number: 96-94476 Harris Corporation, RF Communications Division, Radio Communications in the Digital Age Volume One: HF Technology, Edition 2.
- RadioCom-DigitalAge2 – Segunda edición octubre de 2005, Harris Corporation 2005 Library of Congress Catalog Card Number: 96-94476 Harris Corporation, RF Communications Division, Radio Communications in the Digital Age Volume One: HF Technology, Edition 2.
- http://ondas4cm9ymad15.blogspot.com.ar/2015/04/espectro-electromagnetico.html
- http://www.ipellejero.es/hf/glosario/
- MIL-STD-188-141B. "Interoperability and Performance Standards for Medium and High Frequency Radio Systems", Notice 1, 31 August 2001; Appendix C "Third-Generation HF Link Automation".
- "Frequency-adaptive communication systems and networks in the MF/HF bands". International Telecommunication Union. Radiocommunication Bureau. Edition 2002.
- STANAG 4538, "Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links", Edition 1, North Atlantic Treaty Organization, 2000.
- Criptografía básica – Especialización Cripto –Criptografía – CRIPTO II – Escuela Suprior Técnica. Año 2014.
- Proyecto de Promoción y Síntesis - Sistema de Cifrado de Imágenes bajo Trivium (SCIT) Año 21014 Alumnos de la Escuela Superior Técnica.
- ALE_standard_188_141B.pdf – Department of Defense Interface Standard Interoperability and Performance Standards for Medium and High Frequency Radio Systems distribution statement: Approved for public release; distribution unlimited.
- Breve historia de las comunicaciones http://www.icarito.cl/enciclopedia/articulo/segundo-ciclo-basico/educacion-tecnologica/historia-de-la-tecnologia/2009/12/71-6278-9-4-medios-de-comunicacion-electronicos.shtml
- McDonald, C. and Pieprzyk, C. "Attacking Bivium with MiniSat", Cryptology ePrint Archive, Report 2007/040, 2007.
- Raddum, H."Cryptanalytic Results on Trivium", eSTREAM, ECRYPT Stream Cipher Project, Report 2006/039, 2006.

- Maximov, A. and Biryukov, A. “Two Trivial Attacks on Trivium”, Selected Areas in Cryptography, Lecture Notes in Computer Science, Vol.4876, Springer, 2007.
- Golomb. “Shift Register Sequences”. Aegean Park Press, 1982.
- Massey, J.L. “Shift-register synthesis and BCH decoding”. IEEE Transactions on Information Theory 15, 1969.