# Sistema de seguridad en capa física (SCF) empleando descomposición algebraica del canal para sistemas de comunicaciones inalámbricas OFDM

**Francisco Javier Guerra Manchego, Alex Cartagena Gordillo**

francisco.guerra@ucsp.edu.pe, acartagena@ucsp.edu.pe

Universidad Católica San Pablo, Perú
Campus Campiña Paisajista s/n Quinta Vivanco, Barrio de San Lázaro
Arequipa – Perú

**Resumen**: *La seguridad en las Comunicaciones Inalámbricas OFDM es un gran desafío que se han planteado los investigadores en los últimos años debido a la naturaleza de libre acceso del medio de transmisión. La mayor parte de las soluciones vienen tradicionalmente dadas por mecanismos criptográficos que se implementan en las capas superiores del modelo OSI. En este artículo, se presenta un sistema de Seguridad en Capa Física (SCF) considerando como escenario un sistema de comunicaciones que emplea el estándar IEEE 802.11a en presencia de un espía. El sistema propone el uso de la Descomposición Algebraica de Canal, el cual es único entre el transmisor y el receptor legítimo, éste provee la clave de seguridad a través del uso de las matrices $U_k$, $\Delta_k$ y $V_k$ obtenidas al realizar tal proceso. La matriz $V_k$ es la que multiplica a los símbolos OFDM siendo ésta la matriz encriptadora de datos, en tanto, en el receptor se tiene a las matrices $U_k$, $\Delta_k$ que representan las matrices desencriptadoras. Por otro lado, el espía, quien posee un canal de propagación distinto, no podrá desencriptar los datos que se transmiten. El nivel de seguridad se mide a través de los altos niveles obtenidos de BER (Bit Error Rate) del atacante en comparación del receptor legítimo.*

**Palabras clave**: Seguridad en capa física, descomposición algebraica del canal, OFDM, comunicaciones inalámbricas.

**Abstract**: *OFDM Wireless Communications security is a great challenge that researchers have been addressing due to the open-access nature of the transmission medium. Most of the solutions are traditional cryptographic mechanisms that are frequently implemented at the upper OSI-model layers. This paper presents a Security system at the Physical Layer (SPL) considering a wireless communication system as the scenario with the presence of an eavesdropper. This scenario uses the IEEE 802.11a standard. The following system proposes to employ Algebraic Channel Decomposition, which is unique among the original transmitter and receiver, it also provides a security key by using Uk, Δk y Vk matrices, obtained through the decomposition process. The $V_k$ matrix is the one that multiplies the OFDM symbols resulting on the encryption data function matrix, while at the receiver, we consider the $U_k$, $\Delta_k$ matrices, which represent the decrypting matrices. On the other hand, the eavesdropper, who owns a different propagation channel, will not be able to decrypt the transmitted information. The security level is quantified by comparing the BER (Bit error rate) values measured at the eavesdropper and the original receiver.*

**Keywords**: Security at the Physical Layer, algebraic channel decomposition, OFDM, wireless communication.

## 1 Introducción

En los últimos años, las comunicaciones inalámbricas han tenido un gran impacto en la sociedad, ya que a través de ellas las personas pueden estar conectadas en cualquier momento y en cualquier lugar, lo que ha provocado una gran demanda en el uso de esta tecnología. Al mismo tiempo, los avances tecnológicos desarrollados por los diversos fabricantes de dispositivos y redes inalámbricas han sido revolucionarios, entre los que se encuentran el uso de antenas inteligentes, codificadores, MIMO (Multiple Input Multiple Output) y la mejora en la eficiencia del espectro gracias a OFDM (Orthogonal Frecuency Division Multiplexing).

OFDM es una técnica de modulación que utiliza múltiples portadoras ortogonales sobrepuestas, convirtiéndose en un sistema de modulación muy popular para transmisión de señales de banda ancha sobre canales inalámbricos [Aguayo01]. Actualmente, OFDM es la interface aérea inalámbrica para diversos estándares, como el de televisión digital DVB-T (Digital Video Broadcasting Terrestrial) y ISDB-T (Integrated Service of Digital Broadcasting Terrestrial), además de las normas Wi-Fi, Wi-MAX (Worldwide Interoperability for Microwave Access) y LTE (Long Term Evolution).

Sin embargo, las tecnologías inalámbricas traen consigo importantes riesgos de seguridad, debido a que la información se envía por medio de ondas de radio y las señales viajan de manera libre, de manera que cualquier individuo equipado con una antena con las características adecuadas podría recibir la señal y analizarla.

A esto hay que añadir que toda información que es transmitida entre redes es un bien valioso y protegerla ha sido una tarea que se ha desarrollado continuamente [Cifuentes+04]. Las soluciones desarrolladas utilizan algoritmos criptográficos como WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), y WPA2. A pesar de ello, estos algoritmos tienen vulnerabilidades que los espías han logrado atacar. Es por ello que el incremento de los niveles de seguridad ha apuntado al desarrollo de mecanismos de seguridad en capa física, en la que se aplican técnicas directamente sobre la modulación, codificación y otros componentes de la capa física, permitiendo una comunicación más segura y fiable [Chang+11].

Entre los diversos mecanismos de seguridad en capa física se encuentran los desarrollados en [Vakili+08] en la que se propone una técnica que combina la Codificación Turbo y un Sistema de Cifrado AES (Advanced Encryption Standard). La Codificación Turbo es usada para establecer una comunicación segura, y se basa en la generación de números pseudo-aleatorios para seleccionar N bits de M bits codificados con Turbo Código. Por otro lado, en [Sanchez00], [Poveda00] se desarrolla la técnica de codificación por Espectro Ensachado, consiste en que una señal es ampliada por una secuencia de Pseudo-Ruido (PN). La mayor ventaja del espectro ensanchado es la alta inmunidad obtenida frente a interferencias. La recepción se realiza mediante el proceso de desensanche, el cual consiste en la suma binaria de la señal recibida con una señal local que es la réplica de la señal empleada en la transmisión.

En [Gollakota+11], se presenta una técnica que consiste en enviar muestras de la señal original y la réplica de manera aleatoria, el receptor bloquea al azar la muestra en la transmisión original, o la correspondiente muestra en la repetición. Ahora bien, debido a que el espía no conoce la muestra de señal que ha sido bloqueada, no podrá decodificar correctamente los datos. En tanto, en [Jarot+10] se desarrolla un esquema de seguridad que consiste en combinar dos técnicas, el cifrado y la precompensación del canal. La técnica del cifrado consiste en transformar la constelación de la señal original en una constelación rotada, ésta rotación se realiza basada en una clave generada por AES que la conoce tanto el transmisor como el receptor legítimo. Así mismo, se asume un canal simétrico, con lo que se realiza una precompensación del canal para enviar los símbolos rotados. El receptor legítimo es capaz de decodificar los símbolos enviados a través de la rotación de los símbolos que se han generado por la clave.

En este artículo, se presenta el desarrollo de un sistema de de Seguridad en Capa Física para sistemas de Comunicación Inalámbrica OFDM que utiliza la descomposición algebraica del canal de comunicación como clave de seguridad entre un transmisor y receptor legítimo, lo que permite que un atacante, al no tener conocimiento sobre el canal de comunicación, no sea capaz de desencriptar la información que se transmite.

El resto del artículo está organizado de la siguiente manera. En la sección 2, se describen las Características de las Comunicaciones Inalámbricas, la Capa Física basada en el estándar IEEE 802.11, OFDM, la Descomposición Singular de Valores y la Estimación de Canal. El diseño del sistema de seguridad es desarrollado en la sección 3, y las simulaciones y resultados se presentan en la sección 4. El artículo finaliza con la sección 5, en la cual se presenta las conclusiones y el trabajo futuro.

# 2 Revisión de conceptos

## 2.1 Características de las Comunicaciones Inalámbricas

En [Deza07] se menciona que las comunicaciones inalámbricas consisten en la transmisión y recepción de información a través de ondas electromagnéticas que viajan por el espacio libre. La ausencia de cableado ofrece movilidad a los usuarios, flexibilidad en la topología de la red y escalabilidad. Sin embargo, también presentan algunos inconvenientes como son el menor ancho de banda, la dificultad de añadir seguridad y garantizar ciertos niveles de QoS (Quality of Service).

## 2.2 Capa física

El objetivo de la capa física en una comunicación inalámbrica es crear señales electromagnéticas siendo éstas las que representen a los bits de las tramas de la capa de enlace de datos. A continuación, se detalla el funcionamiento de la capa física basado en el estándar IEEE 802.11.

En [Espinosa+11], [Batalla+09], se menciona que la capa Física está dividida en dos subcapas: PLCP (Physical Layer Convergence Protocol) y PMD (Physical Medium Dependent). La subcapa PMD se encarga de la transmisión de las tramas. En tanto, la subcapa PLCP proporciona el mecanismo de detección de portadora y el CCA (Clear Channel Assessment). El CCA es una señal que la capa MAC tiene que identificar para determinar si el canal está libre u ocupado. El encapsulado que se realiza a nivel de capa Física se muestra en la Figura 1.

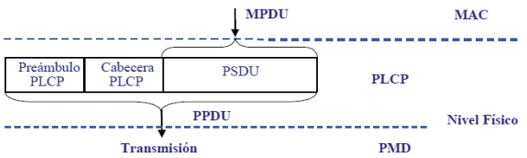


Figura 1: Encapsulado en la Capa Física

## 2.3 OFDM

Según [Vergara08], [Valverde10], [Artés07] OFDM consiste en una multiplexación en frecuencia de diferentes portadoras, donde cada una transporta información modulada en M-QAM o M-PSK. El principio básico de OFDM es dividir la secuencia de datos en *N* subcanales de datos paralelos modulados por *N* subportadoras. En la Figura 2 se muestra el espectro de frecuencia de OFDM, donde las subportadoras están sobrepuestas sin introducir ICI (Intercarrier Interference). Para esto, las subportadoras deben ser ortogonales entre sí, esto es caracterizado en la siguiente expresión:

$$\int_0^T \cos(w_i t)\cos(w_j t)\,dt = 0 \quad i \neq j \qquad \text{(Ec. 1)}$$

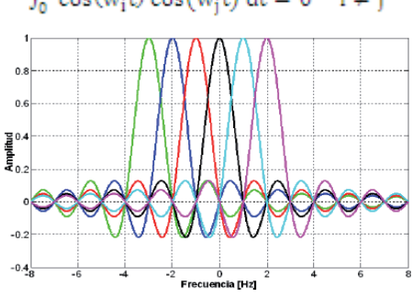


Figura 2: Espectro de frecuencia de OFDM con 6 sub-portadoras

La señal OFDM se obtiene a través del uso de la IFFT (Inverse Fast Fourier Transform) de los símbolos complejos generados de la modulación M-QAM o M-PSK. Por otro lado, los símbolos que llegan al receptor está compuesto de dos partes, una parte perteneciente a un símbolo OFDM previamente transmitido y otras pertenecientes a versiones atrasadas del propio símbolo que es denominado como ISI (Inter Symbol Interference) Para combatir este efecto, en OFDM se adiciona un CP (Cyclic Prefix) antes o después del símbolo resultante de la IFFT, con ello se garantiza la periodicidad del nuevo símbolo.

En la Figura 3, se muestra el diagrama de bloques de un transmisor y receptor OFDM, donde se aprecia el uso de la IFFT y la inserción del CP para la transmisión de una señal OFDM.

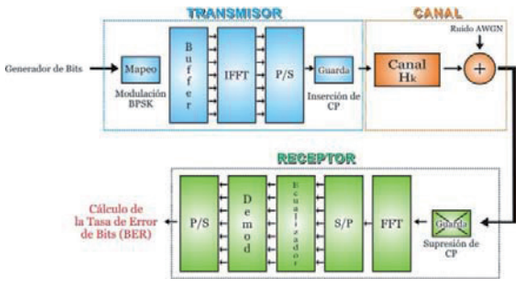


Figura 3: Diagrama de Bloques de un Transmisor y Receptor OFDM

## 2.4 Estimación de canal

En [Cordero09] se menciona que conocer el canal de transmisión cuando trabajamos en comunicaciones inalámbricas OFDM permite mejorar el procesado que se realiza a la señal recibida. Para ello, una herramienta muy útil son los algoritmos de estimación de canal.

Típicamente en los sistemas OFDM la técnica de estimación de canal se conoce como PSAM (Pilot Symbol Assisted Modulation). La principal ventaja de estos métodos es su simplicidad, pero presentan la desventaja de reducir la eficiencia espectral y de energía del sistema. En la Figura 4 se presenta el diagrama de bloques de un transmisor/receptor OFDM que usa esta técnica.

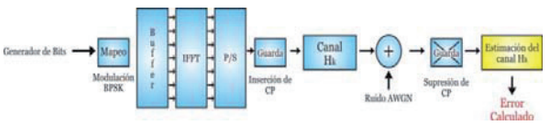


Figura 4: Transmisor/Receptor OFDM en banda base con bloque de Estimación de Canal

Entre los diversos algoritmos de estimación de canal asistido por datos se tiene: Estimador ML (Maximun Likelihood), estimador LSE (Least Square Error) y MMSE (Minimun Mean Square Error).

El autor [Miao06] desarrolla el estimador ML en el que se considera un modelo de canal $h$ con respuesta al impulso finito de orden $l$, el cual es expresado en (Ec. 2).

$$h = \{h[1], h[2], \ldots, h[l]\}^T \quad \text{(Ec. 2)}$$

En el receptor se tiene $n$ muestras recibidas en $y$, así

$$y = \{y[0], y[1], \ldots, y[n-1]\}^T. \quad \text{(Ec. 3)}$$

Por lo que, tenemos el siguiente modelo lineal.

$$y = \mathbf{S}h + v. \quad \text{(Ec. 4)}$$

Donde $\mathbf{S}$ es una matriz Toeplitz de orden $n \times l$, la cual consiste de las muestras de la secuencia de entrada $s[n]$, $n = 0, 1, \ldots, n-1$, dada por:

$$\mathbf{S} = \begin{bmatrix} s[0] & s[n-1] & \cdots & s[n-l+1] \\ s[1] & s[0] & & s[n-l+2] \\ \vdots & \vdots & \ddots & \vdots \\ s[n-1] & s[n-2] & \cdots & s[0] \end{bmatrix} \quad \text{(Ec. 5)}$$

Y $v$ es un vector de ruido descrito en (Ec. 6).

$$v = \{v[0], v[1], \ldots, v[n-1]\}^T \quad \text{(Ec. 6)}$$

Sea $\theta$ el vector de parámetros desconocidos, el cual puede contener el canal $h$. Asumimos que el espacio de probabilidades, el cual describe conjuntamente tanto el vector de ruido $v$ como el vector de entrada $s$, es conocido. Entonces, es posible obtener la función de densidad de probabilidad conjunta del vector de observación $y$, el cual se escribe como $f_y(y;\theta)$, a esta función se denomina como la función de máxima verosimilitud. El Estimador de Máxima Verosimilitud se obtiene al encontrar la solución de:

$$\frac{\partial f_y(y;\theta)}{\partial \theta} = 0 \quad \text{(Ec. 7)}$$

Por otro lado, en el estimador MMSE el principal resultado es derivar las ecuaciones de Wiener-Hopf que proveen los coeficientes del filtro óptimo FIR (Finite Impulse Response) para la estimación del canal. Como se aprecia en la Figura 5, $d[n]$ es la respuesta estimada de $y[n]$. Para lograr la estimación se necesita tener dos procesos estacionarios en sentido amplio, $s[n]$ y $y[n]$, los cuales son estadísticamente relacionados uno con otro. Así mismo, tenemos que asumir que las funciones de autocorrelación $r_s[k]$ y $r_y[k]$, y la función de correlación cruzada $r_{ys}[k]$, son conocidas.

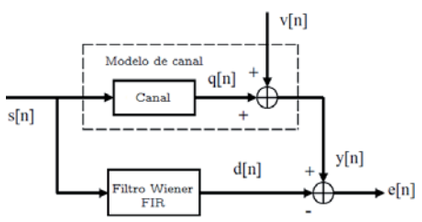


Figura 5: Estimador MMSE basado en la solución Wiener-Hopf

Los coeficientes del filtro Wiener FIR, $w[n]$, se obtienen minimizando el mínimo error cuadrático de la salida del filtro $d[n]$ comparado con la salida del modelo de canal $y[n]$. Esto es obtenido a través de la siguiente expresión:

$$w[n] = R_s^{-1}[n] r_{ys}[n] \quad \text{(Ec. 8)}$$

## 2.5 Descomposición singular de valores

En [Villegas09] se menciona que la Descomposición Singular de Valores (SVD) se basa en la determinación de que cualquier matriz $\mathbf{A}$ de dimensiones $m \times n$ puede ser

escrita como el producto de: Una matriz **U** de columnas ortogonales de dimensiones $m \times n$; una matriz diagonal **W** de $n \times n$ con elementos positivos o ceros, los cuales son los valores singulares de **A**; y por la transpuesta de una matriz **V** de $n \times n$.

*Definición:*

Sean *m, n* enteros positivos y $\mathbf{A} \in C^{mxn}$. Una descomposición en valores singulares de **A** es una factorización de la forma:

$$\mathbf{A} = \mathbf{UWV^T} \quad \text{(Ec. 9)}$$

Donde: $\mathbf{U} \in C^{mxn}$ y $\mathbf{V} \in C^{mxn}$. Además,

$$W = \begin{cases} \begin{bmatrix} \text{Diag}(\sigma_1, \dots \sigma_n) \\ 0_{m-n\,x\,n} \end{bmatrix} \text{ si } m \geq n \\ [\text{Diag}(\sigma_1, \dots \sigma_n)\ 0_{m\,x\,n-m}] \text{ si } n \geq m \end{cases} \quad \text{(Ec. 10)}$$

En cualquier caso, $\sigma_1 \geq \cdots \geq \sigma_s \geq 0$, *s=mín{m,n}*, son números reales no negativos ordenados de mayor a menor y se llaman valores singulares de **A**. Además, a los vectores $\mu_1, \dots, \mu_m$ y $v_1, \dots, v_n$, los cuales conforman las columnas de **U** y **V,** se le llama vectores singulares de A por la izquierda y por la derecha, respectivamente.

**Algoritmo 1** Proceso para hallar las matrices U, W y V

**Formular**: $\mathbf{S} = \mathbf{AA^T}$

**Encontrar:**

Valores propios de **S**: $\sigma_1^2 \geq \cdots \geq \sigma_m^2 \geq 0$

Conjunto ortonormal $u_1, u_2 \dots u_m$ de vectores propios de **S** y construir la matriz $\mathbf{U} = [u_1 u_2 \dots u_m]$ y la matriz diagonal **W.**

**Hacer:**

$\mathbf{V_1} = \mathbf{A^T U_1 W_r^{-1}}$, siendo $\mathbf{U_1} = [u_1 u_2 \dots u_r]$ las primeras *r* columnas de **U**. Encuentre una matriz $\mathbf{V_2}$, tal que $\mathbf{V_1^T V_2} = \mathbf{0}$, $\mathbf{V} = [\mathbf{V_1}\ \mathbf{V_2}]$

# 3 Diseño del sistema de seguridad

## 3.1 Escenario de la solución propuesta

El escenario donde se desarrolla la propuesta es mostrado en la Figura 6. Se consideran los siguientes puntos:

- Existen dos nodos de comunicación, transmisor y receptor legítimo.
- Los nodos utilizan antenas omnidireccionales.
- Se tiene la presencia de un atacante
- La potencia de transmisión del Nodo A y del Nodo B son iguales.

La presente propuesta analiza el peor caso que se puede presentar en una comunicación inalámbrica, esto es, cuando el espía está incluido dentro del rango de cobertura del transmisor y del receptor, ya que éste puede escuchar tanto la transmisión del nodo A como la del nodo B.

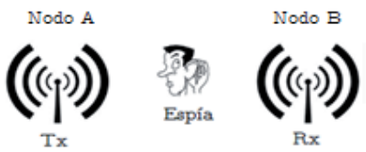


Figura 6: Escenario del problema estudiado

## 3.2 Descripción de la solución propuesta

Para establecer una comunicación entre los nodos A y B, es necesario realizar un intercambio inicial de símbolos, denominado proceso de saludo. El objetivo de este proceso es establecer un acuerdo previo entre los nodos de comunicaciones para poder enviar información. Además, se puede estimar el canal en el receptor legítimo y realizar la descomposición matricial del canal de modo que una de las matrices sea enviada hacia el transmisor, quien se encargará de transmitir los símbolos codificados. Este proceso se muestra en la Figura 7.

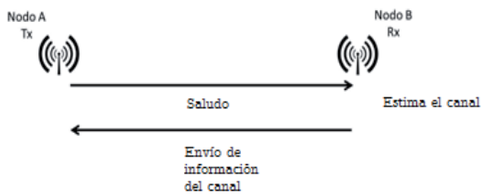


Figura 7: Proceso de Saludo

El detalle de cada trama se describe a continuación.

Primera trama: Considerada como una trama de saludo enviada por el Nodo A hacia el Nodo B, contiene un patrón de bits (secuencia fija).

Segunda trama: El Nodo B recibe el patrón de bits y con ellos estima el canal, una vez realizado ello, procede a la descomposición matricial de donde se obtienen tres matrices $\mathbf{U}_k$, $\mathbf{\Delta}_k$ y $\mathbf{V}_k$. La matriz $\mathbf{V}_k$ es enviada al transmisor, quien se encargará de codificar los datos.

A continuación, se consideran algunos supuestos que se han tomado en cuenta para el desarrollo de la propuesta:

a. Se supone que se ha desarrollado previamente el proceso de autenticación entre el transmisor y el receptor. Este proceso implica en la identificación de usuarios legítimos, llevándose a cabo antes del proceso de encriptación de datos. Se debe tener en consideración que los problemas referidos a autenticación y husmeo son independientes y la presente propuesta es aplicable para los ataques de husmeo.
b. Se supone que el proceso de saludo es realizado con éxito entre los nodos de comunicación.
c. Se supone que existe el hardware adecuado para poder desarrollar el mecanismo propuesto.

d. Se considera que el atacante cuenta con un canal de propagación $\mathbf{H}_{ka}$ distinto al del receptor legítimo $\mathbf{H}_k$. Esto debido a que se considera que el atacante se encuentra a una distancia mayor a media longitud de onda (mayor a 6cm. en sistemas OFDM convencionales), tal como se presenta en [Tahir00], con lo que el canal de propagación es variante en tiempo y espacio.
e. El tipo de canal de propagación es un canal con desvanecimiento con Función de Densidad de Probabilidad Rayleigh.
f. El tipo de ruido considerado en el canal es del tipo AWGN (Additive White Gaussian Noise).

La solución propuesta se desarrolla en la capa física, específicamente en el bloque del canal de propagación. Se propone realizar un cambio en los símbolos de transmisión OFDM, los que serán multiplicados con la matriz $\mathbf{V}_k$., obtenida al realizar la SVD a la matriz de propagación $\mathbf{H}_k$. El diagrama de bloques del sistema de seguridad propuesto se muestra en la Figura 8.

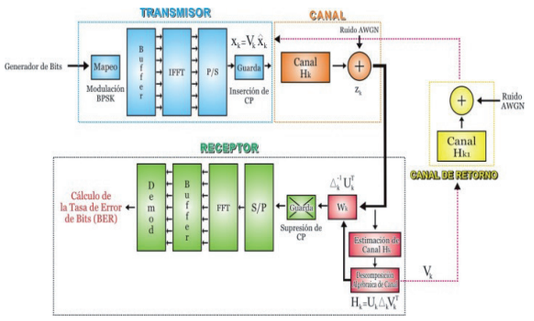


Figura 8: Diagrama de bloques del Sistema de Seguridad.

## 3.3 Descomposición algebraica del canal de propagación

Durante el proceso de saludo se asume que el transmisor envía una cierta cantidad de símbolos al receptor legítimo. Estos símbolos servirán para que el receptor pueda estimar el canal, y luego realizar la descomposición algebraica del canal estimado, donde se obtiene tres matrices, una de las matrices, la matriz $\mathbf{V}_k$, es transmitida hacia el transmisor, para que con ella comience el proceso de encriptación de la información. Así mismo el receptor debe tener una matriz desencriptadora $\mathbf{W}_k$, esta matriz consta de la matriz unitaria $\mathbf{U}_k$ y la matriz diagonal $\mathbf{\Delta}_k$. Donde $\mathbf{W}_k$ es descrita a través de la siguiente expresión:

$$\mathbf{W}_k = \Delta_k{}^{-1}.\mathbf{U}_k{}^{\mathbf{T}} \qquad \text{(Ec. 11)}$$

A continuación se detalla el proceso de encriptación y desencriptación de datos.

Sea $h$ el canal de propagación modelado entre el transmisor y receptor legítimo, el cual puede ser descrito como un filtro FIR de $l$ coeficientes complejos de la forma:

$$h = [h(0)\ h(1)\ \dots h(l-1)] \qquad \text{(Ec. 12)}$$

Se define la matriz de convolución de canal $\mathbf{H}_k$, como una matriz cuadrada Toeplitz de tamaño $k \times k$ donde la primera columna de la matriz está dada por $(h^T, \theta_{1n}{}^T)$ y la primera fila viene dada como $(h(0), \theta_{k-1})$, donde $n=k-l-1$ y $\theta_{1n}$ es un vector fila de *m-ceros*, por lo que la matriz $\mathbf{H}_k$ puede ser definida como:

$$\mathbf{H}_k = \begin{bmatrix} h(0) & 0 & 0 & \dots & 0 & 0 \\ h(1) & h(0) & 0 & \dots & 0 & 0 \\ \vdots & & \vdots & \dots & 0 & 0 \\ h(l-1) & h(l-2) & h(l-3) & \dots & h(0) & 0 \\ 0 & h(l-1) & h(l-2) & \dots & h(1) & h(0). \end{bmatrix} \qquad \text{(Ec. 13)}$$

Mediante el uso de la SVD, descomponemos la matriz $\mathbf{H}_k$ en tres matrices representadas de la siguiente forma:

$$\mathbf{H}_k = \mathbf{U}_k \Delta_k \mathbf{V}_k^T \qquad \text{(Ec. 14)}$$

Donde $\mathbf{U}_k$ y $\mathbf{V}_k$ son matrices cuadradas de dimensiones $k$ x $k$ que contienen los vectores singulares: izquierdo y derecho del canal $\mathbf{H}_k$, respectivamente. La matriz diagonal cuadrada $\Delta_k$ de dimensiones $k \times k$ contiene los valores singulares.

Cada símbolo generado por medio de OFDM es representado como un vector de $k$-elementos de la siguiente forma:

$$\widehat{\mathbf{x}_k} = \left[\widehat{x^1}\widehat{x^2} \dots \widehat{x^k}\right]^T \qquad \text{(Ec. 15)}$$

A continuación, se utiliza la matriz $\mathbf{V}_k$, como matriz encriptadora, la cual multiplica a cada símbolo transmitido, con lo que cada símbolo transmitido es:

$$\mathbf{x}_k = \mathbf{V}_k \widehat{\mathbf{x}_k} \qquad \text{(Ec. 16)}$$

Por lo tanto, los símbolos recibidos al pasar por el canal matricial $H_k$ y al ser sumados por una componente de ruido AWGN, $z_k$, serán representados de la siguiente forma:

$$\mathbf{y}_k = \mathbf{H}_k \mathbf{V}_k \widehat{\mathbf{x}_k} + \mathbf{z}_k \qquad \text{(Ec. 17)}$$

Una vez recibido cada símbolo, se procede a realizar el proceso de desencriptación, ello se logra multiplicando el símbolo recibido por la matriz $W_k$. Finalmente, cada símbolo desencriptado en el receptor tiene la forma de:

$$\widehat{\mathbf{x}_k^r} = \widehat{\mathbf{x}_k} + \mathbf{z}_k^r \qquad \text{(Ec. 18)}$$

Donde la componente de ruido AWGN $\mathbf{z}_k^r$ viene dado por:

$$\mathbf{z}_k^r = \Delta_k{}^{-1} \mathbf{U}_k \mathbf{z}_k \qquad \text{(Ec. 19)}$$

## 3.4 Simulaciones y resultados

### 3.4.1 Simulación de los estimadores de canal

En esta sección se realiza la simulación de los estimadores de canal presentados en la sección 2.4, lo que

nos permite elegir el algoritmo de canal a utilizar en la simulación del Sistema de Seguridad.

El detalle de la simulación se realiza a continuación.

a. Se genera una cantidad de 64 bits aleatorios de 0's y 1's, con igual probabilidad de aparición.
b. La transmisión de los bits se ha realizado con modulación BPSK.
c. IFFT sobre estos bits mapeados.
d. Conversión paralela a serie y se le agrega el prefijo cíclico.
e. Transmisión del símbolo sobre un canal de tipo Rayleigh, al cual se le ha añadido ruido AWGN con diferentes valores de $E_b/N_0$ para el cálculo del error.
f. En el receptor se elimina el prefijo cíclico.
g. Estimación de canal con los algoritmos de canal LSE y MMSE.

En la Figura 9, se muestra las curvas del MSE (Minimun Square Error) calculados para los algoritmos LSE y MMSE. Se puede apreciar la curva del Estimador MMSE presenta una caída más pronunciada que el estimador LSE para diferentes valores de SNR (Signal Noise Ratio), por lo que el estimador MMSE tiene un menor error en comparación del LSE, aunque la complejidad del MMSE es mayor que la del LSE, esto se produce porque en la derivación de MMSE se ha supuesto el conocimiento de la correlación del canal y la varianza de ruido.

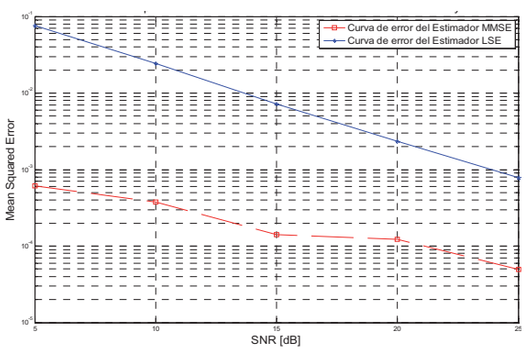


Figura 9: Curva de MSE para LSE y MMSE

### 3.4.2 Simulación del sistema de seguridad en capa física

La simulación de la Capa Física se basa en el Estándar 802.11a, al cual se le han añadido los bloques de seguridad descritos en la Figura 8.

El primer escenario de simulación se muestra en la Figura 10, el atacante realiza la Descomposición Algebraica de su canal estimado $\mathbf{H}_{ka}$, de modo que intenta desencriptar los datos que han sido multiplicados con la matriz $\mathbf{V}_k$.

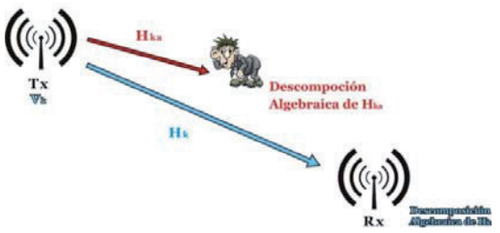


Figura 10: Escenario de simulación donde el atacante realiza la Descomposición algebraica de su canal

En la Tabla 1 se muestran los parámetros de simulación de la Capa Física basada en el Estándar 802.11a.

Tabla 2: Parámetros de la simulación

| Parámetro | Valor |
|---|---|
| Número de subportadoras de datos | 52 |
| Número de IFFT/FFT | 64 |
| Separación entre subportadoras | 0.3125 Mhz |
| Duración de Prefijo Cíclico | 0.8 µs |
| Período de símbolo | 4 µs |
| Retardo esparcido del canal | 0.5 µs |
| Ancho de banda | 20 Mhz |
| Duración de la muestra | 4 ms |

En la Figura 11, se muestran las curvas de BER para el receptor legítimo con conocimiento perfecto de canal y con estimación de canal, así como la curva de BER del atacante. Es clara la diferencia que existe entre las curvas del receptor legítimo y del atacante. Para el atacante, la cantidad de errores cometidos es considerable, llegando a ser constante para los diferentes valores de $E_b/N_o$( Energy per bit to Noise power spectral density Ratio). En tanto, la curva de BER del receptor legítimo cae conforme los valores de $E_b/N_o$ se incrementan, lo que demuestra que cualquier atacante que se encuentre en el medio de la comunicación no será capaz de desencriptar la información que se transmite.

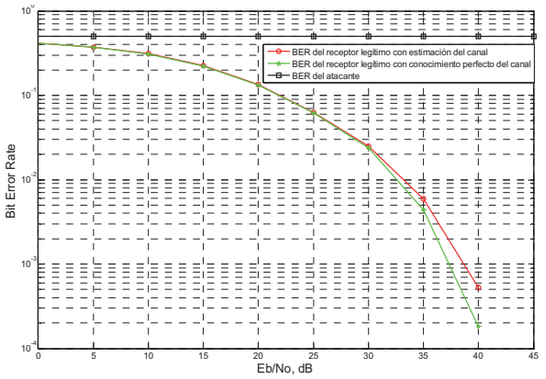


Figura 11: Curvas de BER vs $E_b/N_o$ para el receptor legítimo y atacante

En la Figura 12, se muestra la curva de BER obtenida del atacante cuando conoce que se realizado la encriptación de datos e intenta realizar su propia descomposición algebraica de Canal.

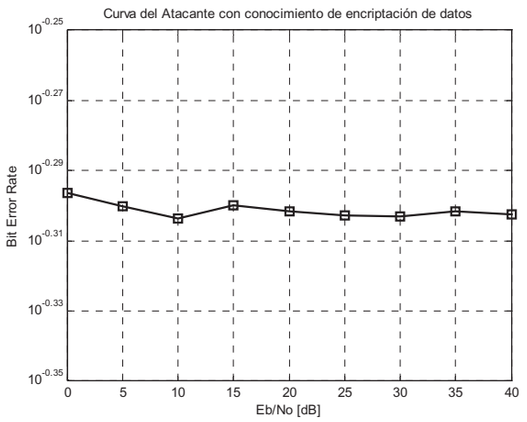


Figura 13: Curva de BER del atacante con conocimiento de encriptación de datos

A continuación, se presenta un segundo escenario de simulación, tal como se aprecia en la Figura 13, donde ahora el atacante no realiza la descomposición algebraica de su canal estimado $\mathbf{H}_{ka}$, ya que él asume que la información no está siendo encriptada.

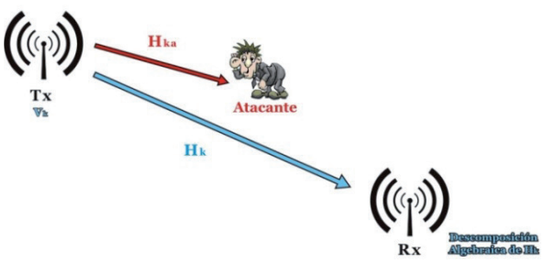


Figura 13. Escenario de simulación donde el atacante no realiza la Descomposición algebraica del canal

En la Figura 14 se aprecia la curva de BER obtenida cuando el atacante desconoce que los símbolos transmitidos presentan algún tipo de encriptación.

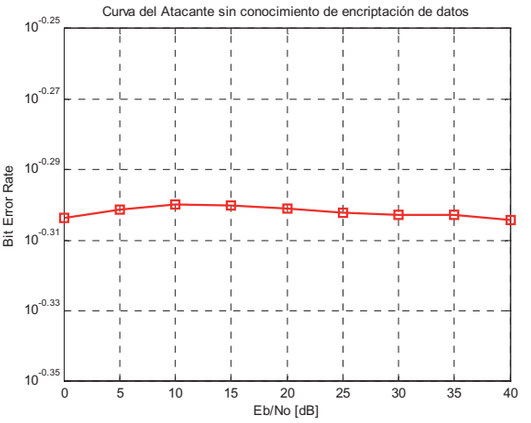


Figura 14: Curva de BER del atacante sin conocimiento de encriptación de datos

En ambos escenarios presentados, las curvas de BER presentan valores altos error, con lo que se demuestra que en ambas situaciones la tasa de error de bits transmitidos para el atacante es considerable en comparación con el receptor legítimo.

## 4 Conclusiones y trabajos futuros

A partir del diseño de la plataforma presentada, se desprenden las siguientes conclusiones:

a. El estimador de canal MMSE presenta buenas prestaciones en cuanto al error de estimación bajo cierta SNR en comparación con el estimador LSE, lo cual es beneficioso dado que es necesario tener un conocimiento casi perfecto del canal de propagación en el transmisor ya que el canal es la clave que permite proveer seguridad en la comunicación.

b. Es factible implementar seguridad a nivel de capa física en OFDM usando la SVD del canal de propagación. La seguridad brindada por el mecanismo propuesto es evaluada a través de los valores de BER del receptor legítimo y del atacante.

c. En los resultados que se han obtenido se muestra que los valores de BER del atacante altos en comparación con los valores de BER del receptor legítimo, esto debido a que el atacante al no tener conocimiento del canal del receptor legítimo, trata de desencriptar la información a través de las matrices obtenidas por la SVD de su propio canal $\mathbf{H}_{ka}$.

Como posibles trabajos futuros se considera los siguientes puntos:

a. En las simulaciones realizadas, se ha usado dos nodos en presencia de un espía, como trabajo futuro se propone extender a múltiples nodos en presencia de múltiples espías de tal forma que se pueda evaluar la influencia de estos sobre los resultados obtenidos.

b. Realizar simulaciones de capa física para diferentes estándares de comunicación inalámbrica OFDM como LTE, Wi-MAX, IEEE 802.11n entre otros y

analizar los resultados obtenidos y compararlos con trabajos previos.

c. Analizar los tiempos referidos a los procesos de estimación de canal y la aplicación de la SVD en el nodo transmisor.

## Referencias bibliográficas


[Aguayo01] Aguayo, M. Modulación Multiportadora Adaptativa para Canales Selectivos en Frecuencia con Desvanecimientos. Universidad de Málaga, Málaga, 2001.

[Artés07] Artés, A. Comunicaciones digitales. Madrid, España: Pearson Educación S.A., 2007.

[Batalla+09] Batalla, O. Seguridad en 802.11: Estudio y desarrollo de un sistema de gestión para EAP-TLS. Universida Politécnica de Cataluña, Barcelona, 2009

[Chang+11] Chang, S. et. al, Physical Layer Security in Wireless Networks: A Tutorial, Wireless Communications, 2011.

[Cifuentes+04] Cifuentes, J. & Narvaez, C. Detección de Vulnerabilidades de Sistemas Operativos Linux y Unix en Redes TCP/IP, 2004.
http://www.univalle.edu.co/~telecomunicaciones/trabajos_de_grado/informes/tg_JesusCifuentes_CesarNarvaez.pdf

[Cordero09] Cordero, M. Técnicas de estimación de canal en la capa física Wireless MAN-OFDM de la norma IEEE 802.16e, Universidad de Sevilla, Sevilla, 2009.

[Deza07] Deza, E. Estudio de Aplicaciones de Redes de Comunicaciones Inalámbricas Ad-Hoc para Sistemas a bordo de Automóviles. Universidad Politécnica de Catalunya, Catalunya, 2007.

[Espinosa+11]Espinosa, R. Uso de un FPGA (Field Programmable Gate Array) para la Implementación de la Sección de Banda Base de la Capa Física de un Transmisor basado en el Estándar IEEE 802.11n en modo Greenfield, 2011.
http://bibdigital.epn.edu.ec/bitstream/15000/3969/1/CD-3732.pdf

[Gollakota+11] Gollakota, D. & Katabi, S. Physical Layer Wireless Security Made Fast and Channel Independent, in International Conference on Computer Communications, Shanghai, 2011.

[Jarot+10] Jarot, S. et. al Siddiqi, M. Wireless Physical Layer Security using Chanel State Information, in International Conference on Computer and communication Engineering, Kuala Lumpur, 2010.

[Miao06] Miao, G. Signal Processing for Digital Communications. Norwood, Massachusetts, 2006.

[Poveda00] Poveda, J. Espectro Ensanchado, Ingeniería, vol. 5, 2000.

[Sanchez00] Sanchez, J. CDMA: Comunicaciones de Espectro Ensanchado, 2000.
http://www.raco.cat/index.php/Buran/article/download/178725/240325.

[Tahir00] Tahir, M et al. Wireless Physical Layer Security Using Encryption and Channel Pre-Compensation. International Conference on Computer Applications and Industrial Electronics, Kuala Lumpur, 2010.

[Vakili+08]Vakili,V. et. al. Combination of Turbo Coding and Cryptography in Non-Geo Satellite Communication Systems, in International Symposium Telecommunications, Tehran, 2008.

[Valverde10] Valverde, C. Implementación de un Sistema OFDM en un dispositivo SFF SDR. Universidad Carlos III, Madrid, 2010

[Vergara08]Vergara, J. Simulación de un esquema de modulación/demodulación OFDM utilizando un Modelo de Canal Multitrayectoria. Escuela Superior Politécnica del Litoral, Guayaquil, 2008.

[Villegas09] Villegas, M. Marmolejo. Tópicos en Álgebra Lineal, 2009.
http://matematicas.univalle.edu.co/~mimarmol/topicosenalgebralineal.pdf