UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:

INGENIERÍA ELECTRÓNICA

Trabajo de titulación previo a la obtención del título de:
INGENIERO E INGENIERA EN ELECTRÓNICA

TEMA:

ANÁLISIS DE ALGORITMOS DE SEGURIDAD PARA EL PROTOCOLO IEEE 802.16D (WIMAX-FIJO)

AUTOR Y AUTORA:

ALAN DAVID AREQUIPA TAYUPANTA
MIREYA ELIZABETH PATIÑO CAMPOVERDE

TUTOR:

MANUEL RAFAEL JAYA DUCHE

Quito, junio del 2016

Cesión de derechos de autor

Nosotros Alan David Arequipa Tayupanta y Mireya Elizabeth Patiño Campoverde con documento de identificación N° 1716597065 y con documento de identificación N° 1723503148 respectivamente, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: ANÁLISIS DE ALGORITMOS DE SEGURIDAD PARA EL PROTOCOLO IEEE 802.16D (WIMAX-FIJO), mismo que ha sido desarrollado para optar por el título de: Ingeniero e Ingeniera Electrónica, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autores reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....
Arequipa Tayupanta Alan David
1716597065

.....
Patiño Campoverde Mireya Elizabeth
1723503148
Junio del 2016

Declaratoria de coautoría del docente tutor

Yo, declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación ANÁLISIS DE ALGORITMOS DE SEGURIDAD PARA EL PROTOCOLO IEEE 802.16D (WIMAX-FIJO) realizado por AREQUIPA TAYUPANTA ALAN DAVID y PATIÑO CAMPOVERDE MIREYA ELIZABETH, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerados como trabajo final de titulación.

Quito, junio 2016

Manuel Rafael Jaya Duche
1710631035

ANÁLISIS DE ALGORITMOS DE SEGURIDAD PARA EL PROTOCOLO IEEE 802.16 D (WIMAX- FIJO)

Alan Arequipa[1], Mireya Patiño[2], Rafael Jaya[3]

Resumen

El presente trabajo tiene como objetivo analizar los algoritmos de seguridad para el protocolo IEEE 802.16d, transmitiendo distintas cadenas de caracteres (desde 6 bits hasta 32 bits), para esto, se preparó un escenario de investigación WIMAX (Una estación base, dos clientes receptores, un agente extraño a la red) en el software OMNET++ a través del cual, se realizó la implementación de algoritmos AES(Estándar de Encriptación Avanzada) y DES (Standard de Encriptación de datos) para observar la protección que brindan a la información que se transmite y se recibe. De los resultados obtenidos y analizados, se observó que el índice de coincidencia del protocolo DES es mayor con un 5,67% frente a AES, lo que muestra que tan vulnerable es encontrar el tamaño de la TEK de una cadena String; por otro lado, el tiempo de cifrado y descifrado del algoritmo DES es notablemente superior con el (88.34% / 89.42%) en relación a AES, además se verificó que el índice de seguridad del algoritmo AES proporciona un 23,29% con respecto a DES.

Palabras Clave: AES, criptografía, DES, seguridad, Wimax.

Abstract

This paper aims to analyze the security algorithms for the IEEE 802.16d protocol, transmitting different strings (from 6 bits to 32 bits), for this, a research scenario WIMAX (A base station, two receiver was simulated clients, a stranger to the network) agent in the OMNET software ++ through which, the implementation of algorithms AES (Advanced Encryption Standard) and DES (Standard data Encryption) to observe the protection afforded to information was made that transmitted and received. From the results obtained and analyzed, it was found that the matching ratio of DES protocol is higher with 5.67% against AES, which shows that it is vulnerable to find the size of the TEK of a String; on the other hand, the time of encryption and decryption algorithm is DES with significantly higher (88.34% / 89.42%) relative to AES, also it was verified that the security index of AES algorithm provides a 23.29 % compared to DES.

Keywords: AES, Cryptography, DES, Security, Wimax

[1] Estudiante de Ingeniería Electrónica - Universidad Politécnica Salesiana, Egresado.
[2] Estudiante de Ingeniería Electrónica - Universidad Politécnica Salesiana, Egresado.
[3] Profesor de Ingeniería Electrónica – Universidad Politécnica Salesiana

1. Introducción

En la actualidad la seguridad informática realiza procesos de gestión de riesgo para evaluar la información a proteger, y en función de los datos recolectados, establecer medidas preventivas y/o correctivas que eliminen riesgos o que los reduzcan hasta niveles manejables. [**1**]

Los efectos de los ataques comprometen la integridad y confidencialidad de la información al punto de degradarla [**2**]. Las organizaciones deben adoptar medidas de seguridad que resulten adecuadas y eficientes en pos de conocer las herramientas que sean útiles para contrarrestar amenazas. [**3**]

Wimax genera algunas interrogantes respecto al nivel de seguridad que maneja provocando que no sea una tecnología en auge como es el caso de Wi-Fi y por ende un freno considerable cuando se trata de inversiones de alto nivel [**4**]. La unión del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y el "WiMax Fórum" han pensado en fomentar un ambiente sólido y confiable para las redes Wimax. Para lo cual, la información es protegida por algoritmos de seguridad.

Estos algoritmos brindan características de seguridad para el paso de la información de un extremo a otro, pero con la incertidumbre de que en el camino se enfrenten con ataques intrusivos. Cada algoritmo posee características propias como: tiempo de cifrado, tiempo de descifrado, índice de coincidencia e índice de seguridad.

La investigación en este manuscrito, analiza las características antes mencionadas de AES y DES en un entorno de simulación en el software OMNET++, mediante estos indicadores se podrá dar una visión clara de que protocolo brinda mejores prestaciones; con el tiempo de cifrado/ descifrado se podrá saber que algoritmo trabaja en un menor período al procesar una cadena String de hasta 32 caracteres.

El índice de coincidencia muestra que tan vulnerable es encontrar el tamaño de la TEK de una cadena String; y finalmente el índice de seguridad verifica el porcentaje de seguridad que viaja la información de extremo a extremo.

El resultado del presente trabajo muestra que el algoritmo AES permite obtener mejoras en tiempo de un 88.34% al momento de cifrar y en un 89.42% al descifrar una cadena String, además encontrar el tamaño de la TEK en una serie de caracteres con AES es un 5.67% improbable con respecto a DES; y con el algoritmo AES el índice de seguridad presenta un 23.29% de robustez al recorrido de la información en una red Wimax-fija.

2. Fundamentación

Las redes WiMax emplean mecanismos de cifrado para cuidar por la integridad y confidencialidad de los datos. Para ello, entre la BS (Base Station) y la SS (Service Station) crean claves de cifrado llamadas TEKs (Traffic Encryption Keys). Las TEKs son utilizadas en el proceso de cifrado de los algoritmos simétricos estos son: DES y AES [**5**].

2.1 Cifrado simétrico y asimétrico.

En la criptografía existen dos categorías de funcionamiento que se basa en el tipo de claves de seguridad, empleadas para cifrar y descifrar los datos.

1) *Cifrado Asimétrico:* Conocida como la criptografía de clave PÚBLICA. Se utiliza dos claves: la que es conocida (público), que se utiliza para el cifrado y la clave privada para el descifrado que solamente es conocida por un usuario.

2) *Cifrado Simétrico:* Conocida como la criptografía de clave SECRETA, utiliza una clave para cifrar y descifrar el mensaje, previamente el emisor y el receptor conocen de la misma, si un agente extraño descubre la clave el sistema se vuelve vulnerable a cualquier ataque. [**6**]

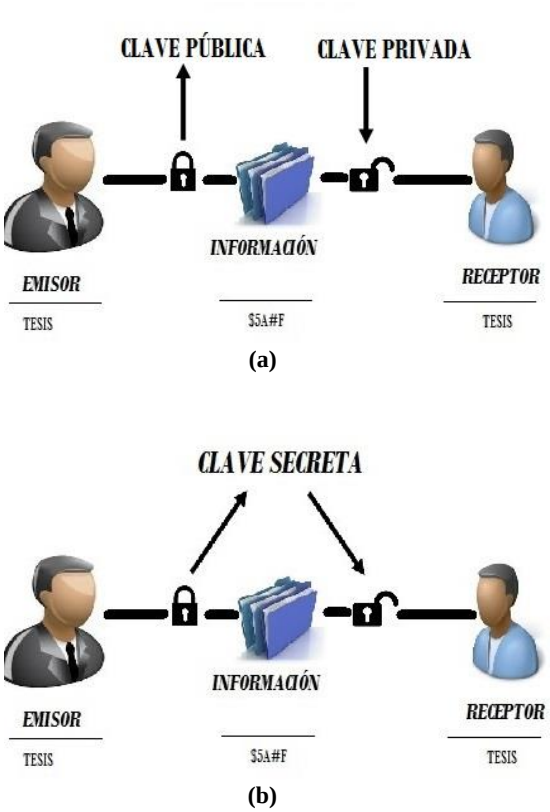

Figura 1. Proceso de clave para criptografía:(a) Simétrico, (b) Asimétrico.

2.2 DES

El propósito de la creación de este algoritmo fue encontrar un nivel de seguridad para el mensaje de transmisión, pero que sea eficaz y adaptable a varios usos; con la utilización de una clave tanto para el cifrado y el descifrado [**7**]. La peculiaridad de este algoritmo es que cifra por bloques completos de bits de acuerdo al tamaño de la TEK, por el motivo de la investigación la llave tiene una longitud de 8 bits logrando obtener hasta 4 llaves cuando se cifra de 24 a 32 bits; cuando ya no existen más caracteres por cifrar en el último bloque, los espacios sobrantes (en blanco) se rellenan con ceros al momento del cifrado, para poder completar este bloque.

2.3 AES

Es uno de los algoritmos de cifrado por bloque más seguros, veloz, flexible y más utilizados en la actualidad de código abierto desde el año 2001 que fue nombrado Standard [**8**].
Este trabaja haciendo varias sustituciones, transformaciones no lineales e intercambios, que se ejecutan en bloques de datos. Estas operaciones se hacen en rondas hasta poder cifrar completamente la trama, cabe recalcar que el mensaje mantiene la misma longitud durante todo el proceso, en la investigación el tamaño siempre va hacer 32 bits.

2.4 Índice de coincidencia

Es un índice que permite encontrar aproximadamente el tamaño de la TEK con la cual se cifra un texto plano, su funcionamiento se basa en el análisis de la variación de frecuencias relativas de cada carácter, respecto a un bloque String. Cuando crece el número de caracteres por ende crece la TEK y la distribución que existe en el bloque tiende a ser más uniforme. [**9**]

Este índice se calculó con la ayuda del método de ataque intrusivo de Kasiski que analiza el tamaño de la cadena y la probabilidad de encontrar dos caracteres iguales dentro de la cadena String. Ver ecuación (1).

$$IC = \sum_{i=1}^{32} \frac{n_i(n_i-1)}{n(n-1)} \quad (1)$$

2.5 Índice de seguridad

Este índice de seguridad mide la eficiencia de asegurar los datos cifrados contra los ataques intrusivos que se pueden presentar desde que el paquete sale desde el emisor hasta el momento que llega al receptor. Este se calculó con la ayuda del método de ataque intrusivo Suma Parcial que analiza los valores que contiene la TEK y el tiempo que se demora en conseguir esos datos.

2.6 Tiempo de cifrado y descifrado

El tiempo de cifrado es aquel período que ocupa cambiar la información de texto comprensible a una forma incomprensible a simple vista humana, por otro lado el tiempo de descifrado es el periodo que se utiliza para realizar el proceso inverso al mencionado anteriormente

3. Metodología

3.1 Diseño del escenario Wimax-fijo

Para la configuración y simulación de una red Wimax punto a multipunto para la implementación de los algoritmos de seguridad, para lo cual, se ubicó una estación base (wimaxbase) que es la encargada de la retransmisión de la información; dos nodos de acceso, uno de ellos fue configurado con emisor y el otro como receptor (ann y bob); y finalmente un agente extraño a la red (carlos) que es el encargado de enviar los ataques intrusivos para encontrar las diferencias entre los dos algoritmos de seguridad. Como se observa en la figura 2.

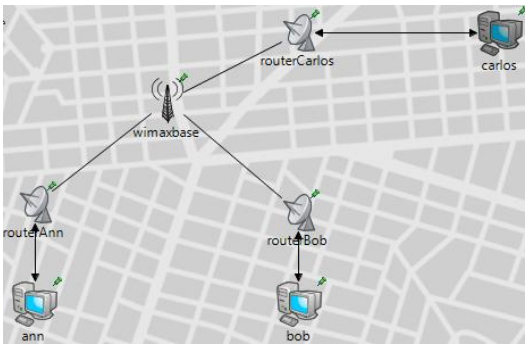

Figura 2. Escenario de investigación

En la figura 3, se observa el proceso de obtención de los datos de comparación, comienza con la elección del algoritmo de seguridad (figura 4), luego se ingresa la cadena de caracteres (6 a 32 bits) como se nota en la figura 5; estos caracteres se van a cifrar en el emisor para el posterior envío, en la recepción se descifra el mensaje; de esa manera se encuentra los dos primeros parámetros de comparación.

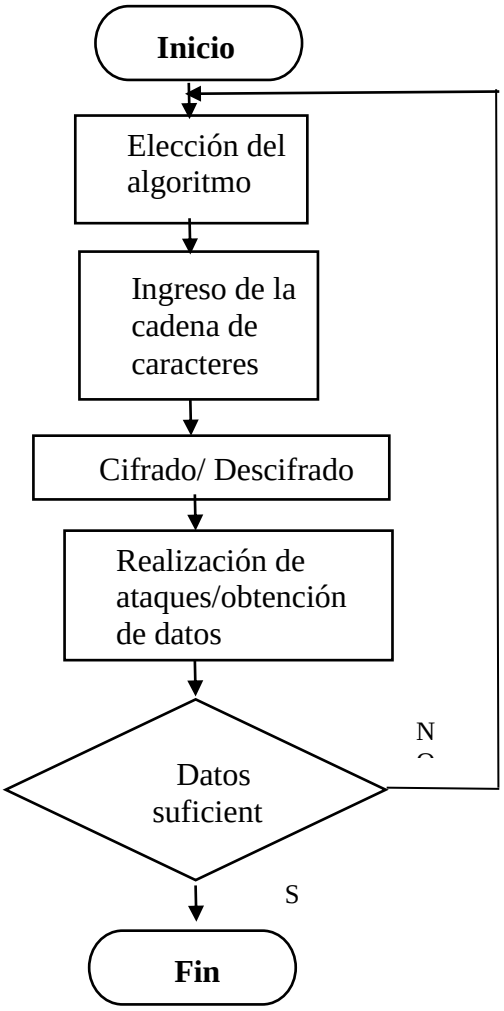

Figura 3. Proceso de obtención de datos

Cuando el mensaje va camino hacia el receptor, el agente extraño se encarga de aplicar ataques intrusivos al mensaje codificado para trabajarlo y así encontrar los otros 2 factores de comparación: es decir, el índice de coincidencia y de seguridad, como se aprecia en la figura 6.

Este proceso se repite hasta encontrar valores que sean útiles para el proceso de comparación. (Figura 7)

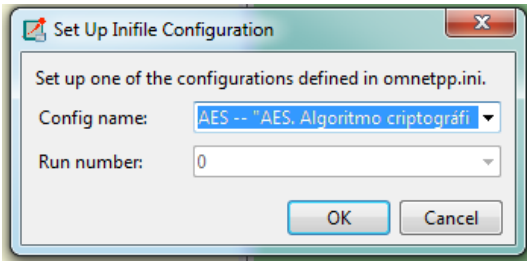

Figura 4. Elección del algoritmo AES

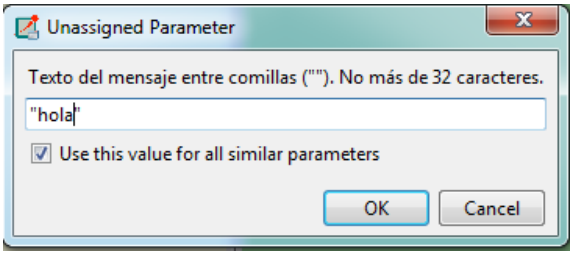

Figura 5. Ingreso cadena de caracteres

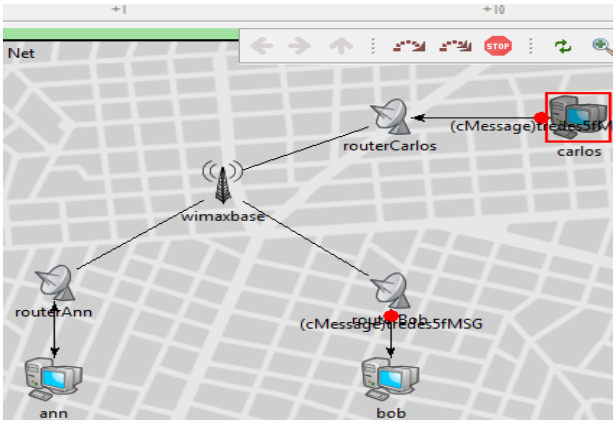

Figura 6. Recepción de información del agente extraño

```
Plugin path: ./plugins
ann Mensaje cifrado:  .
Inicializado PC: ann .
Mensaje original: hola .
aes : Mensaje cifrado: EC05E6BF74EFA192BF5EF38EE08024FA8F2CC99EFCCD8899BE33D766573
Tiempo de cifrado:  87.905815 milisegundos .
ann enviará el primer mensaje .
bob recibe un mensaje de ann .
Mensaje original: hola .
Tiempo de descifrado:  35.251568 milisegundos .
bob evía un mensaje a ann .
aes : Mensaje cifrado: EC05E6BF74EFA192BF5EF38EE08024FA8F2CC99EFCCD8899BE33D766573
Tiempo de cifrado:  38.375126 milisegundos .
carlos recibe un mensaje de ann para bob .
Mensaje: EC05E6BF74EFA192BF5EF38EE08024FA8F2CC99EFCCD8899 .
Indice de coincidencia:  254 .
Indice de seguridad:  32 .
ann recibe un mensaje de bob .
Mensaje original: hola .
Tiempo de descifrado:  33.912903 milisegundos .
ann evía un mensaje a bob .
aes : Mensaje cifrado: EC05E6BF74EFA192BF5EF38EE08024FA8F2CC99EFCCD8899BE33D766573
Tiempo de cifrado:  36.590237 milisegundos .
carlos recibe un mensaje de bob para ann .
Mensaje: EC05E6BF74EFA192BF5EF38EE08024FA8F2CC99EFCCD8899 .
Indice de coincidencia:  254 .
Indice de seguridad:  32 .
bob recibe un mensaje de ann .
Mensaje original: hola .
Tiempo de descifrado:  29.450678 milisegundos .
bob evía un mensaje a ann .
```

Figura 7. Obtención de valores para la comparación

3.2 Tiempo de cifrado y descifrado

El paquete que se envía sale desde el usuario "ann", el mismo que ya está codificado y ya calculado el tiempo de cifrado; en la recepción "bob" se encarga del descifrado y el cálculo del tiempo que le tomo en realizar esa acción. A través de la siguiente ecuación:

$$Tiempocif = t_{fin} - t_{ini} \quad (2)$$

3.3 Ataque intrusivo por el método de Kasiski

El usuario "Carlos", escucha el paquete de datos que fue enviado, para aplicar el método de criptoanálisis **Kasiski** y así obtener un parámetro más de comparación "Índice de coincidencia", este ataque es el que permite encontrar el valor aproximado del tamaño de la TEK de una cadena String cifrada.

Con ello se obtiene un número adimensional en el rango de 1 al 300, entre más alto es el indicador, las posibilidades de descifrar la cadena String son más altas.

3.4 Ataque intrusivo por el método Suma Parcial

Finalmente para encontrar un "índice de seguridad" entre los dos algoritmos en comparación se aplicó el método de criptoanálisis Suma Parcial, el cual realiza sumas parciales de las posiciones de cada elemento dentro del rango asignado por la cadena de caracteres para que pueda identificar por deducción los valores de la TEK y el tiempo que le conlleve en conseguirlo se muestra como el valor porcentual del índice.

4. Resultados

Tabla 1: Tiempo Promedio en el Proceso de Cifrado para el Algoritmo AES y DES

Tiempo de Cifrado para El Algoritmo AES [ms]	Tiempo de Cifrado para el Algoritmo DES [ms]
37,3	153,5
34,1	154,2
39,3	241,0
37,7	555,5
13,4	328,0
25,2	296,7

Mediante los resultados obtenidos en la Tabla 1, se pudo observar la diferencia que existe en el tiempo de cifrado del algoritmo AES como en el DES, en cada uno de los mensajes transmitidos en el algoritmo AES se tiene un tiempo de cifrado el cual oscila entre 13,4 ms y 39,3 ms; el cual permitió obtener un tiempo promedio de 33 ms; y utilizando el algoritmo DES, se obtuvo un tiempo de cifrado entre 153,5 ms y 555,5 ms;

Tabla 2: Tiempo Promedio en el Proceso de Descifrado para el Algoritmo AES y DES

Tiempo de Descifrado para El Algoritmo AES [ms]	Tiempo de Descifrado para el Algoritmo DES [ms]
34,8	154,4
35,5	129,4
28,1	149,7
17,8	339,1
35,7	398,7
22,8	329,3

En la tabla 2, se observa el tiempo de descifrado entre el algoritmo AES y DES, obteniendo como resultados para AES valores entre 17,8 ms y 35,7 ms, y para el algoritmo DES tiempos entre 128.3 ms y 444,7 ms.

Tabla 3: Promedio Índice de Coincidencia para el Algoritmo AES y DES

Promedio Índice de Coincidencia AES	Promedio Índice de Coincidencia DES
204,7	278
272	263
92	123
90	123
254	254
254	254

En la tabla 3, se observan valores del índice de coincidencia de AES y DES, los valores encontrados son: el mínimo es de 90 y el máximo es de 278.

Tabla 4: Promedio Índice de Seguridad para el Algoritmo AES y DES

Promedio Índice De Seguridad AES	Promedio Índice De Seguridad DES
50	20,7
53	46
55	47
75	74,3
80	37,3
85	77.7

En la Tabla 4, se presenta el funcionamiento que tiene el índice de seguridad de AES y DES para lo cual el algoritmo AES presenta altos niveles de seguridad obteniendo como un valor mínimo de 53 y un valor máximo de 85, a comparación del algoritmo DES que presenta como un valor mínimo de 20.7 y un valor máximo de 77.7.

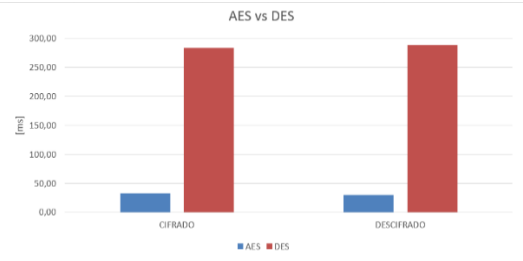

Figura 8. AES vs DES, tiempo de cifrado/descifrado

La figura 8, refleja el valor promedio de los tiempos analizados de los dos algoritmos. En AES el valor de cifrado es de 33 ms y el descifrado de 30.4 ms. DES presenta valores de 283 ms y 287.5 ms de cifrado y descifrado respectivamente, lo que infiere que DES se demora un 88.34% y un 89.42% para los procesos de cifrado y descifrado en comparación del algoritmo AES.

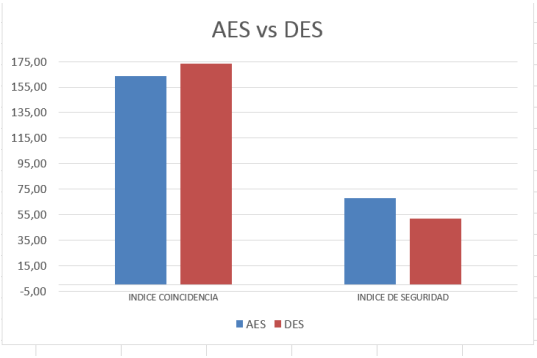

Figura 9. AES vs DES, índice de coincidencia e índice de seguridad

La figura 9, muestra la comparación de los valores promedios de los índices: Coincidencia y Seguridad (AES y DES). Analizando el índice de Coincidencia, el algoritmo DES presenta un índice de 5,67% mayor comparado con AES.

El índice de Seguridad refleja una superioridad de AES del 23,29% frente a DES.

5. Discusión

Existen algunos trabajos relacionados que confirman que el protocolo de seguridad AES brinda mejores prestaciones que el protocolo DES. Así se tiene por ejemplo el realizado por los profesores Penchalaiah y Seshadri donde se analizaron las ventajas, similitudes y limitaciones de AES con respecto a DES [**10**]. Ellos trabajaron con procesadores de 8 bits obteniendo como resultados: tiempo de cifrado de 28.8 ms y para el descifrado de 28.0 ms hablando del algoritmo AES. En el presente trabajo para AES el valor de tiempo de cifrado es de 33 ms y el descifrado de 30.4 ms. Comparando los resultados que se obtuvo hay similitud debido a que se maneja similar número de bits pero la variación recae a que en este trabajo se trabajó en una simulación de hasta 32 bits mientras que el otro grupo de investigación lo realizó con equipos físicos.

De igual forma, Yuri Medina y Haider Miranda aportaron con una comparación de tres algoritmos: DES, 3DES y AES [**11**]. Analizaron teóricamente 12 parámetros basándose en publicaciones de trabajos experimentales de los cuales resalta la seguridad, concluyendo que AES es considerado seguro con respecto a los otros 2 algoritmos; comparando con el presente trabajo los resultados experimentales confirman que el algoritmo AES proporciona altos niveles de seguridad.

Existen otros trabajos que analizan características de los algoritmos pero en diferentes ambientes, en la primera publicación utilizan equipos de 2.99 GHz CPU y 2 GB RAM, en el segundo caso se utiliza el lenguaje C [**12**] [**13**]. En contraste con los antes mencionados trabajos, el presente nota la importancia del funcionamiento de estos algoritmos en una red Wimax-fija, con el plus que se analiza el índice de coincidencia el cual trata de encontrar el valor aproximado del tamaño de la TEK de una cadena String.

5. Propuesta de mejoras

Tras realizar el análisis de los resultados obtenidos, se sugiere las siguientes recomendaciones.

Utilizar el algoritmo de seguridad AES en una red Wimax- fija ya que el mismo ha demostrado ser seguro al momento de cifrar y descifrar los caracteres, con lo que se obtiene menor vulnerabilidad en comparación con DES.

De las pruebas realizadas en un entorno Wimax se pudo observar que enviando cadenas de caracteres de 32 bits y al menos un carácter especial se obtiene cifrados más robustos, pero hay la posibilidad de aumentar la complejidad del algoritmo de cifrado enviando cadenas de caracteres de 128 o 256 bits.

Otra posibilidad para reducir el tiempo cifrado/descifrado y obtener mejores resultados trabajando con palabras de 32 bits o más, sería trabajar con un microprocesador y utilizarlo a su máxima capacidad.

Tras la experiencia adquirida en la realización de la investigación, existe la posibilidad de estudiar y analizar los algoritmos de seguridad en ambientes móviles es decir para una red 802.16 e (Wimax-móvil)

6. Conclusiones

El algoritmo de seguridad AES presenta diferencias notables en rendimiento frente al algoritmo DES, resultando que AES tiene un funcionamiento superior que DES debido a las siguientes razones que lo ratifican: El algoritmo AES permite obtener mejoras en tiempo de un 88.34% al momento de cifrar y en un 89.42% al descifrar una cadena String de hasta 32 caracteres; además encontrar una coincidencia en una serie de caracteres con AES es un 5.67% improbable con respecto a DES, ya que este utiliza una TEK fija para cifrar en todos los casos expuestos; lo que con lleva a que el índice de seguridad presente un 23.29% de robustez al recorrido de la información en una red Wimax-fija.

7. Agradecimientos

Se agradece al MSc. Rafael Jaya Duche por su colaboración y conocimientos para el desarrollo del presente trabajo.

8. Referencias

[1] Alvarez Luis. (2005) Universidad Iberoamericana. [Online]. http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

[2] P Galdámez, "Seguridad Informática," *Actualidad Tic* , vol. 5-6, no. 1, 2003.

[3] Bernardo Mejía. (2012) Universidad Nacional Autónoma de México. [Online]. http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2561/Tesis.pdf?sequence=1

[4]E Ugalde. (2015) Mundo Contact. [Online]. http://mundocontact.com/cobra-auge-la-tecnologia-wifi-802-11ac/

[5]Albentia Systems. (2011, Enero) [Online]. http://www.albentia.com/Docs/WP/ALB-W-000006spA4_Seguridad%20en%20redes%20WiMAX.pdf

[6]J Mendoza, "Demostración de cifrado simétrico y asimétrico," *Ingenius*, vol. 3, pp. 47-49, 2008.

[7]C Sanchéz. (2014) Teoría de la información y teoría de códigos. [Online]. http://www.cesans.net/cripto/DES_Diferencial-Carlos_Sanchez.pdf

[8]Laura Vargas. (2010, Enero) Escuela de Ingeniería Eléctrica de Costa Rica. [Online]. http://eie.ucr.ac.cr/uploads/file/proybach/pb2009/pb2009_036.pdf

[9]J Muñoz, S Díaz, and J Carillo, "Criptoanálisis basado en el índice de coincidencia," *Contactos*, vol. 4, pp. 14-21, 199.

[10]N Penchalaiah and R Seshadri, "Effective Com - parison and Evaluation of DES and Rijndael Algori-thm (AES)," *International Journal of Computer Scien - ce and Engineering*, vol. 2, pp. 1641-1645, 2010.

[11]Y Medina and H Miranda, "Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES," *Mundo FESC*, vol. 9, pp. 14-21, 2015.

[12]N Singhal and J Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization," *International Journal of Computer Trends and Technology*, pp. 177-181, 2011.

[13]A Al Tamimi. (2008) Washington University in St.Louis. [Online]. http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf.pdf