OLIMPIA. Revista de la Facultad de Cultura Física de la Universidad de Granma.
Vol.14 No.43, abril-junio 2017. ISSN: 1817-9088. RNPS: 2067. olimpia@udg.co.cu

Original

EDUCACIÓN EN SEGURIDAD CRIPTOGRÁFICA PARA REDES INALÁMBRICAS CON TECNOLOGÍAS WIFI, BLUETOOTH Y WIMAX

Cryptographic security in wireless networks with WiFi, Bluetooth and WiMAX technologies

MSc. Yasser Cesar Alvarado-Salinas, Instituto Superior Tecnológico José Ochoa León, yalvarado@uees.edu.ec, Ecuador.

MSc. Pedro Osbel Nuñez-Izaguirre. Universidad estatal de Guayaquil, yalvarado@uees.edu.ec, Ecuador.

Recibido: 30/04/2017- Aceptado: 31/05/2017

RESUMEN

Este artículo analiza la importancia de la seguridad criptográfica empleada en las redes inalámbricas con tecnología WiFi, Bluetooth y WiMAX, tomando en cuenta las enmiendas efectuada por el Instituto de Ingenieros Eléctricos y Electrónicos, para cada una de estas redes, así como la importancia educativa de su conocimiento. Para aquello, se estudia los mecanismos de cifrado y de autenticación que emplean estas tecnologías inalámbricas para garantizar la seguridad de la información. Además se indican los ataques comunes que sufren las redes, las vulnerabilidades del algoritmo de cifrado, las ventajas y desventajas así como los medios efectivos de aplicación. Con base en la investigación, se puede concluir que las tecnologías inalámbricas estudiadas han implementado el sistema criptográfico AES, empleando los diferentes modos de cifrados que posee para proteger la información. Además, se destaca que WiMAX es más seguro y robusto en comparación con WiFi puesto que existen muchas técnicas para vulnerar su seguridad.

Palabras clave: IEEE, WiFi, Bluetooth, WiMAX, AES, CCM

ABSTRACT

This article analyzes the cryptographic security used in wireless networks with WiFi, Bluetooth and WiMAX technology, taking into account the amendments made by the Institute of Electrical and Electronic Engineers, for each of these networks. For that, we study the mechanisms of encryption and authentication used by these wireless technologies to ensure the security of information. In addition, common attacks on networks, vulnerabilities of the encryption algorithm, the advantages and disadvantages as well as the effective means of application are

indicated. Based on the research, it can be concluded that the wireless technologies studied have implemented the AES cryptographic system, using the different modes of encryption that it has to protect the information. In addition, it is highlighted that WiMAX is more secure and robust compared to WiFi since there are many techniques to violate your security.
Key words: IEEE, WiFi, Bluetooth, WiMAX, AES, CCM

INTRODUCCIÓN

El Instituto de Ingenieros Eléctricos y Electrónicos, más conocido por sus siglas en ingles IEEE (*Institute of Electrical and ElectronicsEngineers*), es un asociación mundial enfocada en compartir y aplicar los avances de las tecnologías de la información y ciencias en general, mediante la creación de estándares reconocidos internacionalmente(IEEE, 2015).

El IEEE ha definido estándares para las redes inalámbricas de área local (WLAN, *Wireless Local Area Network*), de área personal (WPAN, *Wireless Personal Area Network*) y de área metropolitana (WMAN, *WirelessMetropolitanArea Network*), lo que ha permitido el surgimiento de tecnologías inalámbricas que son utilizadas mundialmente, como lo son: WiFi, Bluetooth, ZigBee y WiMax(Lackner, 2011, pág. 14).Cada una de estas tecnologías emplea algún método criptográfico para garantizar la privacidad de los datos, evitando que sean interceptados por terceros y que se violen los principios de la seguridad de la información, como son: la confidencialidad, la disponibilidad y la integridad de los datos(Zhang & Pierre, 2008).

Sin embargo, el problema de seguridad en las tecnologías inalámbricas siempre estará presente, ya sea, por causa de personas malintencionadas o por la debilidad del método criptográfico utilizado. Además, existen herramientas de software y técnicas de ataques informáticos que pueden vulnerar todo un sistema de seguridad. Por tal razón, es necesario analizar la evolución de los métodos criptográficos empleados en cada una de las tecnologías inalámbricas, puesto que, cada una de las enmiendas que ha realizado la IEEE a los estándares, mencionados anteriormente, ha sido con el objetivo primordial de mejorar la seguridad del método criptográfico para garantizar la seguridad y evitar vulnerabilidades.

Por lo tanto, el objetivo de este artículose concentra en analizar la seguridad de los métodos criptográficos empleados en las redes inalámbricas con tecnología Wi-Fi, Bluetooth y WiMAX, mediante la revisión bibliográfica para identificar la robustez del algoritmo de cifrado, el tamaño de la clave, los medios efectivos de aplicación, así como las ventajas y desventajas de cada una de las tecnologías mencionadas.

WI-FI y el estándar IEEE 802.11

El estándar 802.11 fue definido en el año 1997, y a lo largo de su trayectoria ha sufrido varias enmiendas lo que ha provocado que surjan varias versiones del mismo estándar, cada vez mejoradas, como por ejemplo: 802.11a, 802.11b, 802.11g, 802.11i y 802.11n. Esta última versión que fue ratificada en el año 2009, es la que la utilizan hoy en día, muchos dispositivos con tecnología WiFi. En enero del año 2014, el IEEE estableció una nueva versión conocida como 802.11ac, la misma que duplica las capacidades de velocidad de datos de la versión 802.11n, puesto que proporcionar un rendimiento en gigabit (Perahia & Stacey, 2013).

Por consiguiente, una red WiFi utiliza dos componentes de seguridad: el de autenticación y el cifrado de datos. Para el mecanismo de autenticación existen varios métodos como por ejemplo: el método OSA (*Open SystemAuthentication*, Autenticación de Sistema Abierto) que consiste en autenticar todas la peticiones de los usuarios; el método SKA (*Shared Key Authentication*, Autenticación de Clave Compartida), que se basa en que cada estación debe tener una clave compartida para lograr autenticarse(Chui, 2008), (Lee, 2014) y(Castro, 2005, pág. 28). Además, entre los mecanismos de seguridad para el cifrado de datos están: WEP, WPA y WPA2. Cada uno de estos mecanismos emplea un algoritmo criptográfico con el fin de proveer seguridad en la conexión y privacidad en los datos (Martínez & Gómez, 2009, pág. 85), (Poddar & Choudhary, 2014, pág. 1).

Sistema criptográfico en el mecanismo WEP

WEP (*WiredEquivalentPrivacy*, Privacidad Equivalente al Cable), utiliza el algoritmo criptográfico denominado RC4, con claves de 64 o 128 bits, los mismos que están divididos en dos grupos: 24 bits para el Vector de Inicialización (IV) y 40 o 104 bits para la clave compartida, la misma que tiene que ser distribuido manualmente. En cambio, el vector de inicialización se genera de forma dinámica y debe ser diferente para cada trama. Ambas partes, emisor y receptor, debenconocer la clave secreta y el IV. Por tal razón, la clave se almacena en la configuración de cada dispositivo de red, mientras que la IV se produce en un extremo y se envía dentro de la propia trama al otro extremo (Lackner, 2011, pág. 21), (Lashkari, Mansoor, & Danesh, 2009).

La debilidad del mecanismo WEP se presenta en la construcción de la clave del algoritmo RC4, especialmente porque posee una misma clave que se utiliza para cifrar y descifrar los datos. Por lo tanto, basta con realizar el análisis de trafico de alrededor de 5000 paquetes para tener

el 50% de posibilidades de obtener la clave, puesto que no hay protección contra la repetición de mensajes (Lehembre, 2006, pág. 14), (Mantin, 2005) y(Barajas, 2004, pág. 2).

Sistema criptográfico en el mecanismo WPA

WPA o también llamado Acceso protegido Wi-Fi, es un estándar de *Wi-Fi Alliance* que usa WEP, pero protege los datos con un algoritmo de cifrado TKIP (por sus sigla en inglés *Temporal Key IntegrityProtocol*, Protocolo de Integridad de Clave Temporal), que es mucho más robusto y seguro que RC4. TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar. WPA utiliza un Código de Integridad de Mensaje (*MessageIntegrityCode* - MIC), también conocido como el algoritmo *Michael*(Huang, Susilo , & Seberry, 2014). El MIC incluye un mecanismo que mitiga los intentos de ataque para vulnerar el cifrado TKIP(Jiang, 2014), (Mathews & Hunt, 2007), (Poddar & Choudhary, 2014, pág. 5).

Además, para evitar ataques, donde un tercero intenta adivinar una suma de comprobación o atacar el algoritmo Michael con la ayuda de una estación inalámbrica, TKIP sólo permite un pequeño número de mensajes, donde la suma de comprobación CRC32 es correcto, pero el MIC es incorrecto. Debido CRC32 sigue siendo buena en la búsqueda de errores de transmisión al azar, ese tipo de mensajes indicarían un ataque. Si hay más de dos de estos mensajes son recibidos por una estación dentro de un minuto, TKIP se desactiva por un minuto y se sugiere una renegociación de las llaves (Tews, 2007, pág. 111), (LASHKARI & MANSOORI, 2009).

Sistema criptográfico en el mecanismo WPA2

WPA2 incluye el nuevo algoritmo de cifrado AES (*AdvancedEncryption Standard*, Cifrado Avanzado Estándar), se trata de un algoritmo de cifrado de bloque, a diferencia del RC4 que es de flujo, este utiliza 128 bits como tamaño de bloque y para las claves utiliza 128, 192 o 256 bits(Mathews & Hunt, 2007), (Khan, Mast, Loo, & Salahuddin, 2008, pág. 8).

Además, el cifrado de bloques, se compone de un tipo de sistema de cifrado de clave simétrica que utiliza grupos de bits de una longitud fija. Un sistema de cifrado de clave simétrica es un conjunto de instrucciones o algoritmo que utiliza la misma clave para el cifrado y el descifrado. En la implementación WPA2, los bits están codificadas (utilizando una longitud de clave de 128 bits o más) en bloques de texto claro, que se calculan de forma independiente, en lugar de un flujo de clave que actúa a través de un flujo de entrada de datos del texto claro (Mathews & Hunt, 2007). La diferencia entre WPA y WPA2, es que esta última substituye el cifrado RC4 por

CCMP (*CounterModewithCipher Block ChainingMessageAuthenticationCodeProtocol,* Protocolo Modo Contador con Encadenamiento de Bloques de Cifrado de Mensajes de Código de Autenticación) que utiliza AES(Arana, 2006), (Prodanovic & Simic, 2007, pág. 247). CCMP consta de un algoritmo de privacidad llamado:*CounterMode* (CTR, modo contador); así como, el algoritmo de integridad y autenticidad conocido como CBC-MAC (Arana, 2006), (Tews, 2007).

Aunque el mecanismo WPA2 ofrece un nivel superior de seguridad en comparación con los otros dos mecanismos analizados anteriores, sin embargo, también es vulnerable a ataques que afectan la disponibilidad de la red inalámbrica (Arana, 2006), (Hassinen, 2006, pág. 5).

Comparativade los mecanismos WEP, WPA y WPA2.

	WEP (802.11)	**WPA**	**WPA2 (802.11i)**
Cifrado	RC4	TKIP	AES
Integridad	CRC-32	MIC (Michael)	CCM - CCMP
Tamaño de la clave	64 o 128 bits (24 bits IV y 40 o 104 bits de Clave)	128 bits para el cifrado 64 bits para la autenticación	128 a 256 bits
Seguridad	Débil	Fuerte	Más Seguro
Ventajas	Se implementa sobre la capa MAC (Control de Acceso al Medio) y dota de seguridad a las comunicaciones en redes 802.11 con un coste de recursos muy bajo.	• Soluciona Problemas del mecanismo WEP • Nuevo protocolo para cambiar la clave de forma dinámica cada cierto tiempo.	• Utiliza cifrado de bloques de 128, 192 o 256 bits. • Necesita menos ancho de banda
Desventajas	• Fácil de romper. • Vulnerabilidad • Debilidad del vector de inicialización (IV) • Las claves de usuario son estáticas. • Carece del servicio de autenticación.	• No todas las tarjetas inalámbricas son compatibles. • No cumple con la norma 802.11i. • Clave compartida entre estaciones	• Requiere un hardware específico que cumpla con el estándar IEEE 802.11i
Medios efectivos de aplicación	Sólo para usuarios domésticos y aplicaciones no críticas	Sólo para usuarios domésticos y aplicaciones no críticas	Usuarios domésticos y empresariales.
Ataques	• Análisis de paquetes para intentar descifrar el Tráfico. • Ataques activos basados en la introducción de paquetes • Fuerza bruta	• DoS o ataques de denegación de servicio. • Ataque por diccionario	• DoS o ataques de denegación de servicio • Inundaciones de datos • Secuestro de sesión • Fuerza Bruta

Tabla 1:Comparación entre los mecanismos WEP, WPA y WPA2

Fuente: Khan et al.(2008), Poddar y Choudhary(2014), Mathews y Hunt(2007).

El estándar IEEE 802.15 para redes WPAN

El estándar IEEE802.15, es el estándar especializado para las redes inalámbricas de área personal (WPAN), con un rango de señal de 1 a 10 m. Exige pocos requisitos y fue diseñado para la conexión de periféricos de forma inalámbrica como a un dispositivo móvil o la adición de componentes a un sistema de cine en casa(Freeman, 2005). En esta sección se analizaran el mecanismo cifrado empleado en la comunicación Bluetooth (802.15.1) y en la red de sensores ZigBee (802.15.4)(Gutiérrez, Callaway, & Barre, 2003).

Método criptográfico en la comunicación Bluetooth

La tecnología Bluetooth es un estándar global de comunicación inalámbrica conocido también como el estándar IEEE 802.15.1 (IEEE802, 2015), que permite la transmisión de voz y datos entre diferentes equipos mediante un enlace de radiofrecuencia. Bluetooth está diseñado para funcionar en una red inalámbrica de corto alcance denominada*peer-to-peer* (punto a punto). El modelo de seguridad de Bluetooth se basa en dos medidas: Autenticación y Cifrado de Enlace(Microsoft, 2008).

Bluetooth permite comunicar múltiples dispositivos simultáneamente, a través de una *picored*, dónde un dispositivo actúa de gestor (o maestro) y es posible disponer de hasta 7 dispositivos adicionales (o esclavos). Un dispositivo Bluetooth puede incluso pertenecer a varias *picoredes* (*scatternet*) (Pérez, Picó, & Siles, 2013)

Desde el punto de vista de seguridad, Bluetooth implementa tres mecanismos de protección: a) Autentificación, para verificar la identidad entre dispositivos a través del proceso de emparejamiento en su primera conexión o a través de las claves de enlace en conexiones posteriores; b) Autorización, para establecer el nivel de acceso y las restricciones sobre la utilización de los perfiles y servicios disponibles; y c) Cifrado, para proteger los datos intercambiado con una clave derivada de la clave de enlace. Bluetooth utiliza la función de autenticación de E1, que se basa en el algoritmo SAFER +. SAFER significa seguro y rápido cifrado de rutina(Pérez, Picó, & Siles, 2013), (Umesh & Nagabhooshanam, 2012), (Pérez, Picó, & Siles, 2013).

Además, existen 4 clase de Bluetooth como son: BR, EDR, HS y LE. El cifrado para Bluetooth EDR y HS, es un cifrado de flujo, llamado E0,que afecta a todo el tráfico de datos. El cifrado E0, no es un algoritmo aprobado por los Estándares Federales de Procesamiento de

Información (FIPS).El cifrado para Bluetooth LE es diferente las otras versiones. Una diferencia es que el Resultados del emparejamiento se obtiene en la generación de una clave a largo plazo (LTK) en lugar de la clave de enlace. Es decir, un dispositivo determina la LTK de forma segura y lo envía al otro dispositivo durante el emparejamiento, en lugar de que los dos dispositivos generen la misma clave individualmente (Phan & Mingard, 2010).

Bluetooth LE introduce el uso de AES (128 bits), con cifrado CBC-MAC (AES-CCM). Además de proporcionar el cifrado fuerte, basada en estándares, la inclusión de AES-CCM aplana el camino para la validación FIPS-140 nativa.Además, LE también presenta características tales como direcciones privadas dispositivo y firma de datos. Nuevas claves criptográficas llamado Clave de Resolución de Identidad (IRK) y firma de conexión Resolución de claves (CSRK). El uso de una dirección privada periódicamente cambiante mitiga amenazas por lo que se puede afirmar que esta nueva implementación de cifrado, eleva en gran medida el nivel de seguridad(NIST, 2012), (Pérez, Picó, & Siles, 2013).

Comparativa entre las tecnologías Bluetooth

	Bluetooth	
	BR/EDR/HS	**LE**
Cifrado	E0 - SAFER+ (BR no cifra)	AES-CCM
Distancia de Radio	10 m	50 m
Numero de Esclavos	7 activos	Sin limite
Tamaño de la clave	128 bits	128 bits
Seguridad	Débil	Fuerte
Ventajas	• Inalámbrico • Barato • Automático • Compatibilidad • Baja interferencia • Intercambio de voz y datos	
Desventajas	• Cantidad limitada de esclavos • Limitado radio de acción entre los periféricos: 10 metros • Consumo de batería, cuando está en el modo visible. • Trasferencia de datos lenta cuando son archivos grandes.	
Medios efectivos de aplicación	• Transmisión de audio • Control remoto para aparatos de audio y vídeo • Llamadas telefónicas inalámbricas • Sincronización de información	
Ataques	• Bluetracking • Bluesnarfing • Bluebugging • Bluejacking	

Tabla 2: Comparativa entre Bluetooth

Fuente: Téllez et al.(2010), Bertolín(2011), Parra González et al.(2009)yCosta et al.(2007)

El estándar IEEE 802.16 y la red WMAN

El estándar IEEE 802.16 fue diseñado para las redes de área metropolitana (WMAN), siendo ratificado en el año 2002 y desde entonces ha sufrido algunas enmiendas apareciendo algunas versiones de este estándar como por ejemplo: 802.16a, 802.16c, 802.16d y 802.16e(Ruiz Padilla, 2006). Este último fue ratificado en el año 2005 y se caracteriza por que estandariza dos aspectos importantes como son: La capa física (PHY) y la capa de control de acceso (MAC)Por último, en el año 2009 se hace público la enmienda 802.16j que se extiende principalmente soporte móvil y no introduce ninguna nueva funcionalidad de seguridad(Eklund, Marks, Stanwood, & Wang, 2002).

La familia de estándares 802.16 recibe el nombre de *WirelessMAN*, sin embargo el nombre comercial para el este estándar es WiMAX. En esta sección se analizaran el mecanismo de cifrado empleado en una red la WiMAX para la protección de datos (Kuppuswamy & Shah, 2014).

Método criptográfico en WiMax

Debido a que WiMAX está enfocado a redes metropolitanas mucho más grandes que las de área local, por lo que la seguridad es verdaderamente muy relevante. Por consiguiente WiMAX define en su pila de protocolos, varios mecanismos de seguridad dedicados a garantizar los cuatro principios de la seguridad de la información mencionado en la introducción de este documento (Lackner, 2011, pág. 431).

Por lo tanto, WiMAX, al igual que WiFi, con el objetivo de carecer de vulnerabilidades utiliza dos componentes de seguridad: el de autenticación y el cifrado de datos.El estándar IEEE 802.16j 2009, al igual que WiFi, define dos filosofías de autenticación: OSA y SKA. En el primer mecanismo se obtiene una respuesta, sea de aceptación o negación, de la Estación Base (BS). El segundo mecanismo utiliza el proceso de clave compartida, con una Estación de Usuario (SS) para obtener una autorización del BS. El proceso anterior se lo hace en el protocolo PKM (*Privacy Key Management*, Administración de Clave Privada)(Albentia, 2011, pág. 3).

Además, PKM también se encarga del refresco de claves y de la re-autorización periódica. Permite tres tipos de autenticación:1) La autenticación RSA, basada en certificados X.509 y encriptación RSA; 2) Protocolo de autenticación extensible (EAP); y 3) Autenticación basada en RSA seguido de autenticación EAP. Toda la información de seguridad entre partes que se comunican, son parte de las llamadas asociaciones de seguridad (SA). SA son un conjunto de

parámetros que se utilizan para la autenticación, autorización y cifrado. La información compartida depende de la suite de cifrado elegido y por lo general incluye las claves de cifrado y vectores de inicialización (IV) necesarios para el proceso de cifrado(Lackner, 2011, pág. 432). A diferencia de otras tecnologías, WiMAXtiene ciertas ventajas que garantizan la confidencialidad en las redes, como por ejemplo: a) Robustez en los algoritmos utilizados; b) Tiempo de vida variable a sus claves generadas dinámicamente; y c) Cifrado independiente para cada flujo de datos. Sin embargo no se puede garantizar que está exento de un ataque. Un escenario se puede dar mediante el robo de identidad lo que provocaría en el usuario una pérdida de servicio durante largos períodos de tiempo y en el sistema puede conducir a la pérdida financiera limitada o robo de los recursos. Otro escenario es en el caso de no utilizar AES lo que provocaría consecuencias a corto plazo para el usuario y el sistema. Con esta vulnerabilidad existe la posibilidad de denegación de servicio (Jha & Dalal, 2010), (Taeshik & Wook, 2007).

Características de WiMAX

	WiMAX(802.16e)
Cifrado	CBC(DES), CBC(AES), CTR(AES), CCM(AES)
Autenticación	AES-CCM 128 bits
Generación de clave	Dot16KDF
Clave de cifrado	RSA- cifrado con 1048 bits
Seguridad	Fuerte, Robusto
Ventajas	•Gran ancho de banda •Independencia del protocolo •Alto nivel de seguridad.
Desventajas	•Limitación de potencia para prever interferencias con otros sistemas. •Alto consumo de batería en los dispositivos. •Interferencias
Medios efectivos de aplicación	•Acceder a una red empresarial. •Acceder a Internet sin necesidad de cables. •Conectarse sin cables con un pc, un PDA, un teléfono móvil con conexión WiMAX. •Servicio de HotSpot •Acceder a servicios de VoIP sin cables.
Ataques	•Denegación de servicio (DoS). •Robo de identidad

Tabla 3: Características de WiMAX

Fuente: Ahson & Ilya(2008), (Evren & Kai-Oliver, 2008)

CONCLUSIONES

La mayoría de las tecnologías inalámbricas analizadas en el presente documento han adoptado el cifrado AES con una longitud de clave mínima de 128 bit, lo cual es un mecanismo criptográfico verdaderamente difícil de romper. Aun así, se debe estar preparado ante la aparición de algún ataque efectivo que puede vulnerar los mecanismos de seguridad como son: el de autenticación y el cifrado de datos.

Además, ya sea un usuario doméstico o una organización, se debe efectuar las configuraciones necesarias para implementar seguridades criptográficas en los entornos de red más utilizados, como lo es el WiFi, debido a que existe una gran comunidad de Hackers especializados en violar la seguridad de este tipo de redes. Así mismo, existe una gran cantidad de aplicaciones informáticas utilizadas para tal fin. Sin embargo, el entorno de WiMAX, aun no sufre esto problemas, debido, quizás al certificado X.509 y sus firmas digitales para la autenticación, a más de su cifrado RSA con 1048 bits de clave, que lo convierte en cifrado irrompible, al menos en este milenio.

Como futuros trabajos de investigación, se puede ampliar la investigación a otras redes inalámbricas, como por ejemplo: la red Ultra Wide Band (UWB). De igual forma, un trabajo futuro anexada a la presente investigación, es el estudio de la criptografía cuántica, la criptografía de curva elíptica y su implementación en las redes inalámbricas. Por último, se plantea la propuesta de analizar y evaluar al algoritmo RC5 y RC6, que reemplaza al ya roto RC4, destacando sus diferencias, sus mejoras y los usos efectivos.

REFERENCIAS BIBLIOGRÁFICAS

1. Ahson, S. A., & Ilya, M. (2008). *WiMAX: Standards and Security.* EEUU: Taylor & Francis
2. Albentia. (30 de Octubre de 2011). *Seguridad en redes WiMAX 802.16-2009.* Obtenido de http://www.albentia.com/Docs/WP/ALB-W-000006spA4_Seguridad%20en%20redes%20WiMAX.pdf
3. Arana, P. (2006). Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) . *Irstu*.
4. Barajas, S. (7 de Junio de 2004). *Saulo.Net.* Obtenido de http://www.saulo.net/des/SegWiFi-art.pdf
5. Bertolín, J. A. (2011). Identificación, análisis y evaluación de la seguridad en las comunicaciones con tecnología ZigBee . *REE*, 141-121.
6. Castro, R. (2005). Avanzando en la seguridad de las redes WIFI. *Boletín de RedIRIS*, 23-32.

7. Chui, S. H. (2008). Seguridad en redes inalámbricas 802.11. *Universidad Central de Venezuela*, 10-13.
8. Costa, A., Antônio, R., & Mattos Mendes, L. A. (2007). Evolução das Redes Sem Fio: Um Estudo Comparativo Entre Bluetooth e ZigBee. *unipac*.
9. Eklund, C., Marks, R., Stanwood, K., & Wang, S. (2002). IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access. *IEEE Communications Magazine* , 98-107.
10. Evren, E., & Kai-Oliver, D. (2008). WiMAX-Security – Assessment of the Security Mechanisms in IEEE 802.16d/e. *Detken*.
11. Freeman, R. L. (2005). *Fundamentals of Telecommunications.* New Jersey: Wiley Interscience.
12. Gutiérrez, J., Callaway, E. H., & Barre, R. (2003). *Low-rate Wireless Personal Area Networks: Enabling Wireless.* EEUU: IEEE.
13. Hassinen, T. (2006). Overview of WLAN security. *Seminar on Network Security*.
14. Huang, J., Susilo , W., & Seberry, J. (2014). Observations on the Message Integrity Code in IEEE802.11 Wireless LANs. *Citeseerx 5M*.
15. IEEE. (2015). *IEEE Advancing Technology for Humanity*. Obtenido de https://www.ieee.org/about/index.html