Vestigium

ISSN 1794-8940 © 2009
Corporación Universitaria Unitec
Bogotá, D. C.

Diseño y desarrollo de software analizador de usuarios en entornos wireless

Jaime Andrés Chaparro Sánchez [a]

Palabras clave:
Wireless, Mac, Wi-Fi, OFDM, MySQL, Ad- Hoc.

[a]Corporación Universitaria Unitec

Recibido: 25.06.2009
Revisado: 22.09.2009
Aceptado: 08.12.2009

Correspondencia al autor:
jchaparro@unitec.edu.co

Resumen

Una red construida con tecnología inalámbrica se comporta de un modo totalmente diferente a una construida en cable, ya que las primeras van por el aire y, por lo tanto, exigen rendimiento, seguridad y administración que deben tenerse en cuenta para lograr una buena calidad en la comunicación. Por lo tanto, este artículo propone explicar el desarrollo de un software que permita hacer un análisis detallado de los equipos que se encuentren en un entorno inalámbrico determinado y, de esta manera, tomar decisiones acerca del acceso a la red. El desarrollo de esta investigación concierne a todas las personas y empresas que, de una u otra manera, deseen proteger la información de sus redes inalámbricas

Citación: Chaparro, J. A. (2009). Diseño y desarrollo de software analizador de usuarios en entornos wireless. *Vestigium. Rev. Acad. Univ.*, [número especial], 53-53

ARTÍCULO DE INVESTIGACIÓN

Design and development of a users analyzer software in wireless environments

Abstract: A wireless network is built to run differently from one built using cable. It demands extra performance reliability, security and administration to achieve good quality communication. Therefore, this article explains the development of software that provides a detailed analysis of the equipment on a given wireless environment and, thus, makes decisions about how to access the network. The development of this research relates to all the persons and companies who, in one way or another, wish to protect information on their wireless networks.

Keywords: Wireless, Mac, Wi-Fi, OFDM, MySQL, Ad - Hoc.

Design e desenvolvimento de software analisador de usuários em entornos wireless

Resumo: Uma rede construída com tecnologia inalámbrica se comporta de um modo totalmente diferente a uma construída com cabo, já que as primeiras vão pelo ar e, portanto, exigem rendimento, segurança e administração que devem ser considerados para conseguir uma boa qualidade na comunicação. Portanto, este artigo propõe explicar o desenvolvimento de um software que permita fazer uma análise detalhada dos equipamentos que se encontrem em um entorno inalámbrico determinado e, desta maneira, tomar decisões acerca do acesso à rede. O desenvolvimento desta pesquisa concerne a todas as pessoas e empresas que, de uma ou de outra maneira, desejem proteger a informação de suas redes inalámbricas.

Palavras-chave: Wireless, Mac, Wi-Fi, OFDM, MySQL, Ad- Hoc.

Introducción

Actualmente, el crecimiento de las redes inalámbricas se da en forma exponencial debido a la facilidad en el montaje y prestaciones que este tipo de redes ofrece. Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio y éstas, en principio, pueden viajar más allá de las paredes y filtrarse en habitaciones, casas, oficinas contiguas o llegar hasta la calle.

No obstante, su problema radica en que una persona con el equipo adecuado y conocimientos básicos podría, no sólo utilizar la conexión a Internet, sino también acceder a la red interna o a equipos específicos, los cuales pueden poseer carpetas compartidas, y de tal forma analizar toda la información que viaja por la red, mediante *sniffers* (programas enfocados a capturar la información que transita por las redes de datos), obteniendo así contraseñas y contenido privado personal o corporativo.

Es por esto que se han realizado diferentes estudios en el tema, con el fin de mantener un control en este tipo de redes tan utilizadas, pero que por su naturaleza requieren cierto tipo de seguridad. La empresa que más estudios e investigaciones ha realizado hasta la fecha en redes inalámbricas es Ericsson, la cual por medio de los ingenieros Peisa, Wager y Sågfors generaron grandes avances en transportes direccionados (Peisa, et al. 2007), pero enfocándose básicamente a los medios, protocolos y mejoras en la transmisión, dejando en un segundo plano la seguridad inalámbrica que este tipo de tecnologías requiere. Otros estudios de redes inalámbricas han sido realizados en la Universidad Politécnica Salesiana del Ecuador, en el año 2006 enfocándose básicamente en recepción y propagación de señales Wi-Fi para radio localización, donde se tienen en cuenta las potencias de las señales pero dejan a un lado la parte de la seguridad.

A nivel empresarial, varias instituciones creadoras de software han desarrollado diferentes programas para determinar qué redes inalámbricas se encuentran en un entorno, pero enfocándose más al ingreso sin permiso (*sniffers*) de los usuarios, más que a cuidar la red propia.

Por todo lo anterior, se hace necesario un estudio enfocado en crear una solución inteligente para que los usuarios de redes inalámbricas cuiden mejor su información.

El proyecto de investigación desarrollado en la Corporación Universitaria Unitec y denominado *Software analizador de entornos wireless* pretende crear una herramienta capaz de mantener un control mucho más detallado de los usuarios permitidos para accesar redes inalámbricas, enfocando el control en el reconocimiento de las *direcciones de control de acceso al medio* (o MAC, *Media Access Control Address*) las cuales son inmodificables en forma permanente.

Es de gran importancia el desarrollo e investigación en este tipo de tecnologías, ya que así como crecen los usuarios de este tipo de redes, asimismo crece el número de personas interesadas en ingresar de forma no permitida a informaciones de tipo privado. Hoy en día en el entorno empresarial mucha de la información que circula por sus redes maneja los activos de la empresa, sin tener en cuenta los problemas que la pérdida o falta de esta información acarrea sobre la compañía, haciendo de ésta una materia de estudio enfocada en el control de las personas permitidas para circular por dicha red. Según estudios de PCMAG, sólo en Estados Unidos cuatro de cada diez redes inalámbricas son vulneradas por *hackers* (personas que buscan acceso a redes privadas para demostrar sus capacidades) debido a la falta de seguridad y control sobre este tipo de redes (Albaneisius, 2007).

En países menos desarrollados, como el nuestro, no se tiene un estudio exacto de la cantidad de vulnerabilidades que presentan este tipo de redes, pero sí se sabe que la seguridad que ofrecen estas redes en países del tercer mundo es mucho menor, de ahí la relevancia que enmarca este tema de investigación.

El desarrollo de esta investigación propone una herramienta a nivel de software, como una solución integral al problema de acceso de redes inalámbricas, haciendo uso de bases de datos exclusivas para mantener un control de usuarios permanente en el entorno de dicha red. Por lo tanto, el resultado que pretende alcanzar es crear un programa, enfocado al sector empresarial, que permita al administrador de redes llevar un control mucho más estricto en los usuarios que acceden a su red, permitiendo por bases de datos exclusivas autenticar usuario por usuario mediante las MAC de cada equipo.

Descripción del problema de investigación

El desarrollo agigantado de esta tecnología genera un tema de estudio enfocado en el análisis a soluciones de temas de seguridad de este tipo de redes.

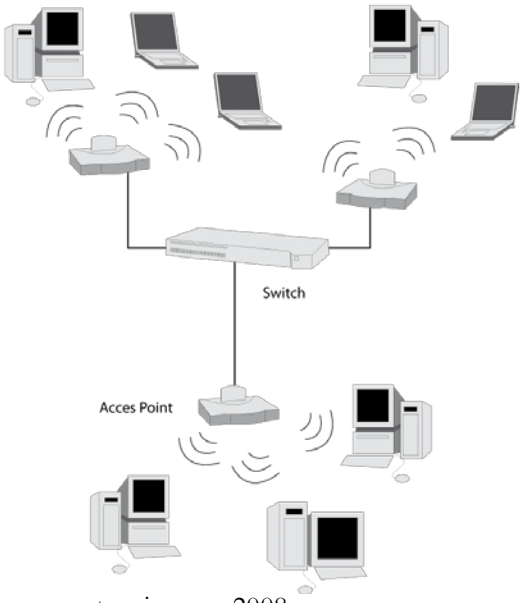
El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de infraestructura en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen sede en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o más redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya.

Aún peor, como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa (Madrid, J. M.,2003). Por todo lo anterior, se hace necesario realización del diseño y desarrollo de un software analizador de entornos inalámbricos que permita el acceso controlado en este tipo de infraestructuras, enfocado al sector empresarial, cuyo activo muchas veces es la información.

Bases Teóricas

"Cuando hablamos de Wi-Fi nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas de radio, también llamada WLAN (wireless lan, red inalámbrica) o estándar IEEE 802.11. Wi-Fi no es una abreviatura de Wireless Fidelity, simplemente es un nombre comercial" (Gutierrez& Beltrán, 2005). El diseño de una red inalámbrica se puede observar de una manera mucho más clara en la figura 1, donde se observa que una red inalámbrica no es el remplazo de las redes cableadas, sino una extensión de dicha tecnología.

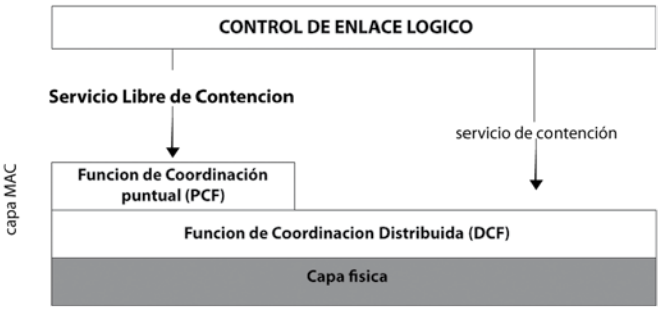
Figura 1. *Estructura básica de una red inalámbrica Wi-Fi*



Fuente: competencia.com, 2008.

Este estándar pertenece a la familia 802, y se enfoca en la descripción y características del nivel físico del enlace de datos del modelo OSI, como se observa en la figura 2.

Figura 2. *Arquitectura del 802.11*

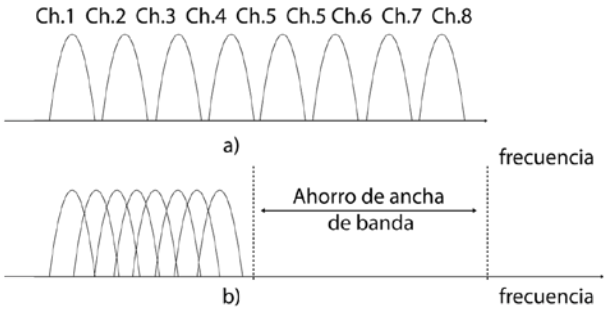


En el nivel físico se describe la técnica y los tipos de modulación que se emplean para realizar la transmisión de datos de una red inalámbrica. El estándar IEEE 802.11 utiliza la técnica de espectro ensanchado o SS; esta técnica consiste en utilizar una banda de frecuencia ancha para trasmitir tramas de baja potencia, alcanzando una velocidad entre 1 y 2 Mbps.

El SS se divide en FHSS (espectro ensanchado por salto de frecuencia) y en DSSS (espectro ensanchado por secuencia directa). El FHSS consiste en dividir el espectro electromagnético en saltos de frecuencia de 1Mhz formando más o menos 75 canales distintos. La transmisión se lleva a cabo de un canal a otro y sólo se usa este canal durante muy poco tiempo (Hernando, 2006). Por su parte, la técnica del DSSS consiste en trasmitir para cada bit enviado una secuencia de bits definidos por un algoritmo ya desarrollado y estandarizado. En este proceso cada bit establecido en 1, es reemplazado por una secuencia de bit y cada bit establecida en 0 es reemplazada por su complemento (Peterson, & Davie, 2003).

Otra técnica utilizada recientemente, la cual mejora la velocidad de transmisión y disminuye el ruido del medio inalámbrico, es la multiplexación por división de frecuencia ortogonal (OFDM). Ésta consiste en dividir el espectro en canales paralelos angostos cada uno con diferente frecuencia y siendo esta ortogonal; esto disminuye la interferencia y gana espacio de una manera bastante considerable (Huidobro, & Roldán, 2005), como se puede ver en la figura 3:

Figura 3. *a.) Técnica multiportadora convencional, b.) Modulación con portadoras ortogonales*



Fuente: uvirtual.ufpso.edu.co

Así como es se observó anteriormente la reutilización del espectro en la transmisión de información inalámbrica, es importante ver las políticas de transmisión, mediante el nivel de control de enlace lógico (LLC), el cual se encarga de iniciar y finalizar la transmisión y realizar la confirmación de recepción de las tramas. El subnivel MAC gestiona el acceso al medio de los dispositivos que hacen parte de la red (Instituto Tecnológico Virtual, 2007).

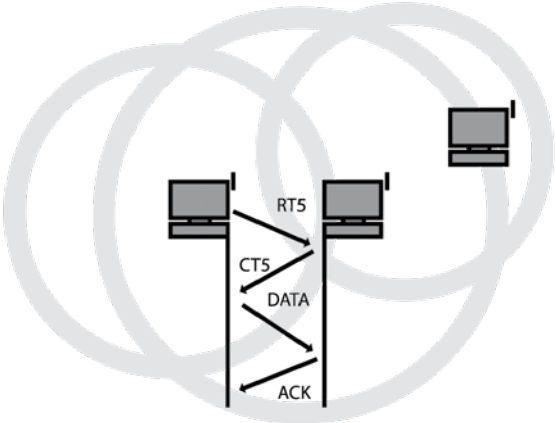
Control del medio

Esta es la principal función de la capa MAC, ya que en cada capa se administran los permisos de acceso a los dispositivos que pertenecen a la red para evitar colisiones y pérdida de información; de esta manera y por tratarse de una red no cableada se presta para una mayor probabilidad de pérdidas. Para esto la capa MAC tiene dos técnicas (Rábanos, 1993): DCF (función de coordinación distribuida), la cual controla la transmisión por medio de unos conjuntos de servicios que se comunican con toda la infraestructura de

la red. Esta técnica utiliza el protocolo CSMA/CA, encargado de detectar la portadora y prevenir colisiones. Este protocolo permite el acceso de los dispositivos y autoriza la transmisión cuando el canal está libre y si un dispositivo de la red desea trasmitir debe escuchar primero el entorno. Si la red está ocupada éste deberá esperar para transmitir. Si por el contrario el canal está libre durante un periodo de tiempo (DIFS), la estación puede trasmitir la señal (Flynn & McIver-McHoes, 1997).

Para esto el dispositivo trasmite un paquete que es llamado RTS donde está el mensaje: "listo para enviar". Este paquete, además de este aviso, tiene la cantidad de información que desea enviar y su velocidad de transmisión. El receptor que por lo general es un punto de acceso (AP), responderá con un mensaje "permitido transmitir" o CTS dando paso al dispositivo para comenzar a enviar la información. Después de esto y cuando el Receptor (AP) recibe el paquete, éste envía un aviso de acuse de recibo o ACK. Entre tanto, los otros dispositivos reciben el mensaje de canal ocupado y debe esperar a que reciban el mensaje de canal libre para competir por medio de transmisión. En la figura 4 se aprecia lo anterior (Madrid, 2003).

Figura 4. *Método de acceso de protocolo CSMA/CA*



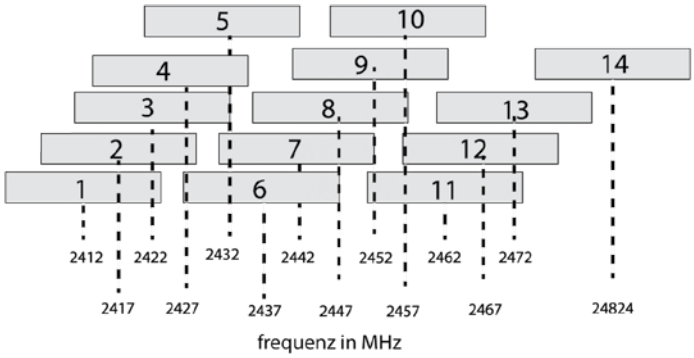
Fuente: http://es.kioskea.net, 2007

Canal de transmisión

El estándar IEEE 802.11 ha definido 14 canales, pero para Colombia son 11 los regulados por el Ministerio de Comunicaciones (2009). Estos canales tienen más o menos 22 Mhz de ancho y una separación entre canal y canal de 5 MHz; esta pequeña separación permite que estos se solapen o se interpongan por lo que no es recomendable diseñar una red entre canales seguidos.

Los canales más óptimos y recomendados son: el 1, 6 y 11. A continuación se detalla por medio de la siguiente figura la distribución de los canales (Tanenbaum, 2003).

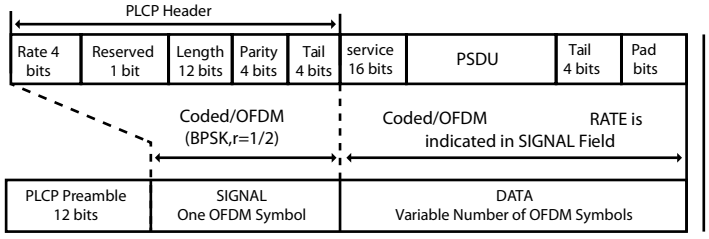
Figura 5. *Distribución del espectro electromagnético*



Fuente: jhosephd, 2006

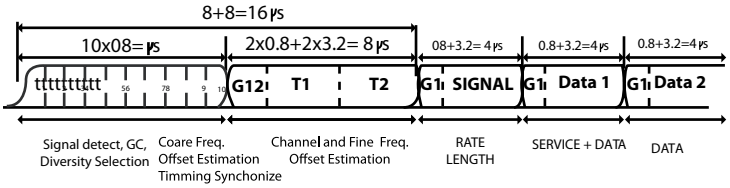
En la figura 6 se estudia el protocolo PPDU (unidad de protocolo de datos) (Tomasi, 2003), mientras que la figura 7 muestra la estructura del protocolo OFDM, presente en la capa física en la que se encuentra la dirección MAC de los equipos dentro de una red inalámbrica.

Figura 6. *Estructura MAC 802.11 formato PPDU*



Fuente: Interwifi, 2008

Figura 7. *Formato Trama OFDM 802.11*



Fuente: Interwifi, 2008

Como se puede apreciar en la figura 7, la estructura de la trama OFDM, en sus 8 microsegundos están señalados con G12:T1:T2 (Arvind, & Prasad, 2007), allí se lleva la información de la frecuencia y canal estimado para la transmisión. El resultado de PSDU incluye los siguientes campos impuestos por la capa MAC.

El corazón o centro de este proyecto se encuentra en las tramas de administración (campos impuestos por la capa MAC), ya que son las encargadas de llevar la información más importante, de la cual podemos identificar plenamente a todos y cada uno de los equipos que se encuentren en una red determinada.

La figura 8 muestra cada una de las partes de la trama del subnivel MAC, el formato general de una trama 802.11, el cual se utiliza para todas las tramas de datos y de control, aunque no todos los campos se utilizan en todos los casos; los campos son los siguientes:

Control de trama: se compone de dos octetos y se utilizan para colaborar en la entrega de tramas de datos entre estaciones.

Tipo: este campo describe si la trama pertenece a datos, control o gestión.

To DS/From DS: identifica si la trama envía o se recibe al/del sistema de distribución. En redes ad hoc tanto to DS como From DS están en cero, estos se activan si trabajan un tipo de red de infraestructura.

Mas fragmentos: se activa si se usa fragmentación.

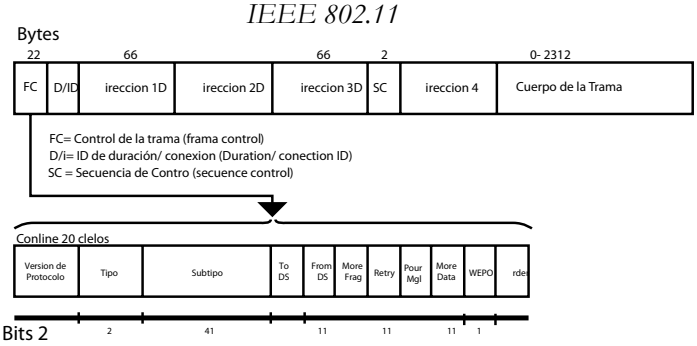
Retry: se activa si la trama es una retransmisión. Power Management: se activa si la estación utiliza el modo de economía de potencia.

More Data: se activa si la estación tiene tramas pendientes en un punto de acceso.

WEP: se activa si se utiliza el mecanismo de autenticación y encriptado.

Order: se utiliza con el servicio de ordenamiento estricto.

Figura 8. *Formato general de la trama del subnivel MAC del IEEE 802.11*



Fuente: Universidad de Catarina, 2007.

ID de duración/conexión: este campo tiene diversos usos y adopta una de las tres formas posibles:

1) Modo duración NAV, el cual representa el número de milisegundos que se espera que permanezca el medio ocupado; 2) tramas transmitidas durante los periodos sin contención, para uso con redes de infraestructura; 3) tramas PS-POLL, sondeo de ahorro de potencia. Los PC pueden elegir ahorrar capacidad de batería desactivando las antenas. Éstas se despiertan periódicamente.

Direcciones: estos cuatro campos contienen las direcciones de la estación que transmite (dirección 1), la que recibe o destino (dirección 2), el punto de acceso origen (dirección 3) y el punto de acceso destino (dirección 4).

Control de secuencia: contiene un subcampo de 4 bits (número de fragmento) utilizado para la fragmentación y el reensamblado, y un número de secuencia de 12 bits utilizado para numerar las tramas enviadas entre el un transmisor dado y un receptor.

Cuerpo de la trama: contiene una MSDU completa o un fragmento de la misma o información de control MAC. Una MSDU es un bloque de datos que el usuario MAC le pasa a la capa MAC, generalmente en la forma de un PDU LLC. Si una MDDU es demasiado grande para ser transmitida en una sola trama MAC, puede ser fragmentada y transmitida en una serie de tramas.

FCS: secuencia de comprobación de trama, trata de una comprobación cíclica de 32 bits. (Universidad de Catarina, 2007).

En general, antes de la transmisión de cualquier trama siempre debe existir un algoritmo de acceso al medio para poder realizar la comunicación entre las diferentes máquinas. Este algoritmo se define según el siguiente diagrama de flujo (Figura 9, *véase* anexo 1) en donde se explica, paso a paso, la forma de enlace de las máquinas para la posterior comunicación (Luk, 1993).

Basado en la figura anterior se puede observar la forma como transmite información una tarjeta de red inalámbrica y, partiendo de este concepto (diagrama de flujo), es posible trabajar en la captura de paquetes que contengan esta información, para ser procesada y, de esta manera, mantener un control claro, óptimo y seguro de los usuarios permitidos en un red.

Teorías genéricas basadas en ingeniería

Teniendo en cuenta la magnitud del proyecto se determinó la utilización de las siguientes herramientas que permitirán el desarrollo para el aplicativo, como la principal función del software es brindar seguridad a la red, se debe trabajar sobre una plataforma estable y confiable y tener en cuenta el uso de un lenguaje de programación robusto, práctico y que permita reutilización de código para futuras mejoras.

Plataforma: debido al lenguaje de programación que se utilizará y a que las aplicaciones basadas en sistemas estables pueden proporcionar consistencia de la interfaz de usuario a lo largo de múltiples plataformas de hardware, sistemas operativos y en el caso de nuestro proyecto de red, la aplicación trabajara bajo plataformas de Windows.

Lenguaje de programación: el lenguaje de programación a utilizar será JAVA, para lo cual se dará a conocer sus principales ventajas y características: Java es un lenguaje de programación orientado a objetos. A diferencia de los lenguajes de programación convencionales, que generalmente están diseñados para ser compilados a código nativo, Java es compilado en un *bytecode* que es ejecutado (usando normalmente un compilador JIT), por una máquina virtual Java (Ciberaula Java, 2010).

El lenguaje en sí mismo toma mucha de su sintaxis de C y C++, pero tiene un modelo de objetos mucho más simple. El lenguaje Java se creó con cinco objetivos principales (Ciberaula Java, 2010):

- Usar la metodología de la programación orientada a objetos.
- Permitir la ejecución de un mismo programa en múltiples sistemas operativos.
- Incluir por defecto soporte para trabajo en red.
- Diseñarse para ejecutar código en sistemas remotos de forma segura.
- Ser fácil de usar y tomar lo mejor de otros lenguajes orientados a objetos.

Según el estándar IEEE 830 de 1998 (Institute

of Electrical and Electronics Engineers, 1998) estos serían los requisitos que tendrá el software del proyecto:

Perspectiva del software: el software que se construirá, será una aplicación que recoja información de los equipos que están en el entorno electromagnético de la red, y mediante esta información administrar el acceso.

Funciones de software: este software tendrá las siguientes funciones:

1. Hará una búsqueda de equipos en el entorno por medio de su MAC.
2. Mostrará características de estos equipos como el nombre de identificación de red y su dirección IP.
3. Por orden del administrador de la red, la aplicación podrá almacenar información estadística.
4. Administrará el acceso a los equipos detectados en el entorno, mediante la búsqueda.

Requisitos tecnológicos: este software será utilizado en equipos locales que tengan una tarjeta inalámbrica, ya que la finalidad de éste será la de arrogar datos de interés de las redes que están en un rango determinado. Para esto se requiere los siguientes requisitos de software y hardware.

Hardware:
- Computador de escritorio o portátil.
- Una tarjeta inalámbrica, externa o interna de 54mbps mínimo.

Software:
- Sistema operativo Windows XP Service Pack 2.
- Software de la tarjeta inalámbrica (opcional).
- Servicios de configuración rápida de la red inalámbrica de iniciado automático, si se desea que sea Windows quien administre esta conexión.

Servicio: esta aplicación servirá como herramienta para el control de acceso mediante la captura de las MAC de equipos que estén en el entorno de la red inalámbrica. También proporcionará información básica de estos equipos para su estudio.

Observaciones: el objetivo primordial en la evolución de esta nueva tecnología es brindar un aporte al desarrollo de la misma y que siga su avance. Por esta razón se quiere que este proyecto quede a disposición de futuras mejoras para el avancé y el mejoramiento del mismo. De esta manera, las mejoras que se realicen serán de interés público y así se genera soporte de los avances que se hagan en dicho proceso.

Conclusiones

En general, los sistemas de seguridad de información en una red deben estar enmarcados dentro de una política adecuada. El riguroso proceso de una política previamente definida evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información y garantizan la calidad y confidencialidad de la información presente en los sistemas de cualquier red; es por esto que este proyecto pretende desarrollar un aplicativo como solución integral y transparente a la problemática de la seguridad inalámbrica, ofreciendo a los usuarios una solución imperceptible en cuanto a sus labores diarias, pero una herramienta muy efectiva a cualquier administrador de red, para tomar acciones efectivas en favor de la seguridad de su dominio.

Con el desarrollo de este proyecto se espera comprender las acciones que realiza la tarjeta de red para el reconocimiento del medio y de los equipos que se encuentren en una red. Además los pasos que debe realizar para solicitar el acceso al medio.

Por medio de la investigación que se realiza con la elaboración del proyecto se pretende identificar los procesos que genera la capa de enlace para interpretar y negociar el acceso al entorno. En la investigación de la captura y la identificación del medio se da un pequeño aporte al

desarrollo de las redes inalámbricas, para el mejoramiento del control del medio como procedimiento de seguridad.

Finalmente, se puede concluir de forma general, que existe un notable interés en implantar cada día más sistemas inalámbricos, esto puede atribuirse a varias razones: el auge tecnológico, la necesidad de una mayor movilidad, la disminución en los costos de implementación además de ser capaces de ofrecer servicios en sitios donde los sistemas cableados no pueden llegar.

Nuevos estándares surgen para poder así mejorar la tecnología ofrecida por el sistema inalámbrico, logrando incrementar la calidad de los servicios ofrecidos. En fin, la búsqueda seguirá siendo por integrar todos los servicios en una red única híbrida, que permitan conexiones física e inalámbrica, pero con sistemas de seguridad los suficientemente confiables, en redes, donde hoy en día muchas empresas basan sus activos en la información que este tipo de infraestructura maneja y que por la misma razón, muchas otras personas están permanentemente tratando de accesar sin autorización.

Referencias

Albaneisius, C. (2007, 4 de abril). Comcast cuts off bandwidth hogs. *PCMAG*. Recuperado desde http://www.pcmag.com/article2/0,2817,2111373,00.asp

Arvind, V., & Prasad, S. (2007). *FSTTCS 2007: Foundation of Software Technology and Theoretical Computer Science*. Berlin: Springer.

Ciberaula Java (2009). *La tecnología Java*. Recuperado desde http://java.ciberaula.com/articulo/tecnologia_java/

Flynn, I., & McIver-McHoes, A. (1997). *Understanding operating systems* (2a ed.). Boston: PWS Publishing.

Gutierrez, G., & Beltrán, A. (2005). Sistema de información para servicios prestados en redes ad-hoc (Tesis de grado). Universidad Manuela Beltrán, Bogotá, Colombia.

Huidobro, J. M., & Roldán, D. (2005). *Comunicaciones en redes WLAN: WiFi, VoIP, multimedia y seguridad*. México: Limusa.

Institute of Electrical and Electronics Engineers. (1998). *IEEE approved draft standard dictionary of measures to produce reliable software*. Recuperado desde http://ieeexplore.ieee.org/Xplore/guesthome.jsp

Instituto Tecnológico Virtual. (2007). *Control de enlace lógico LLC*. Recuperado el 4 de abril de 2009 desde http://www.mitecnologico.com/Main/ControlDeEnlaceLogicoLlc

Interwifi. (2008). *Estándar 802a*. Recuperado desde http://www.laserwifi.com/estander802a.11.htm

jhosephd. (2009, 8 de noviembre). *Industrial Wireless* [Blog post]. Recuperado desde http://ecoinstrumentacion.wordpress.com/2009/11/08/industrial-wireless/

Luk, F. (1993). *Advanced signal processing algorithms, architectures, and implementations IV*. San Diego, Estados Unidos: Society of Photo-optical Instrumentation Engineers.

Madrid, J. M. (2003, enero-junio). Seguridad en redes inalámbricas 802.11. *Sistemas & Telemática*, (3), 13-28.

Ministerio de Comunicaciones [Colombia] (2009). *Repartición del espectro*. Recuperado desde http://www.mincomunicaciones.gov.co

Misra, I. S., & Pani, C. (2007). Performance studies of MPLS based integrated architecture for 3G-WLAN scenarios with QoS provisioning. En R. Bestak, B. Simak, & E. Koszlowska (Eds.), *Personal wireless communications: The 12th IFIP International Conference on Personal Wireless Communications* (pp. 157-168). New York: Springer-IFIP.

Peisa, J., Wager, S., Sågfors, M., Torsner, J., Göransson, B., Fulghum, T., Cozza, C., & Grant, S. (2007). *High speed packet access evolution: concept and technologies*. Ericsson Research. Recuperado desde http://www.ericsson.com/article/wireless_access_networks_20100209132003

Peterson, L. L., & Davie, B. (2003). *Computer networks: A system approach* (3a ed.). San Francisco, Estados Unidos: Morgan Kaufmann.

Rábanos, J. M. (1993). *Transmisión por radio*. Madrid: Ramón Areces.

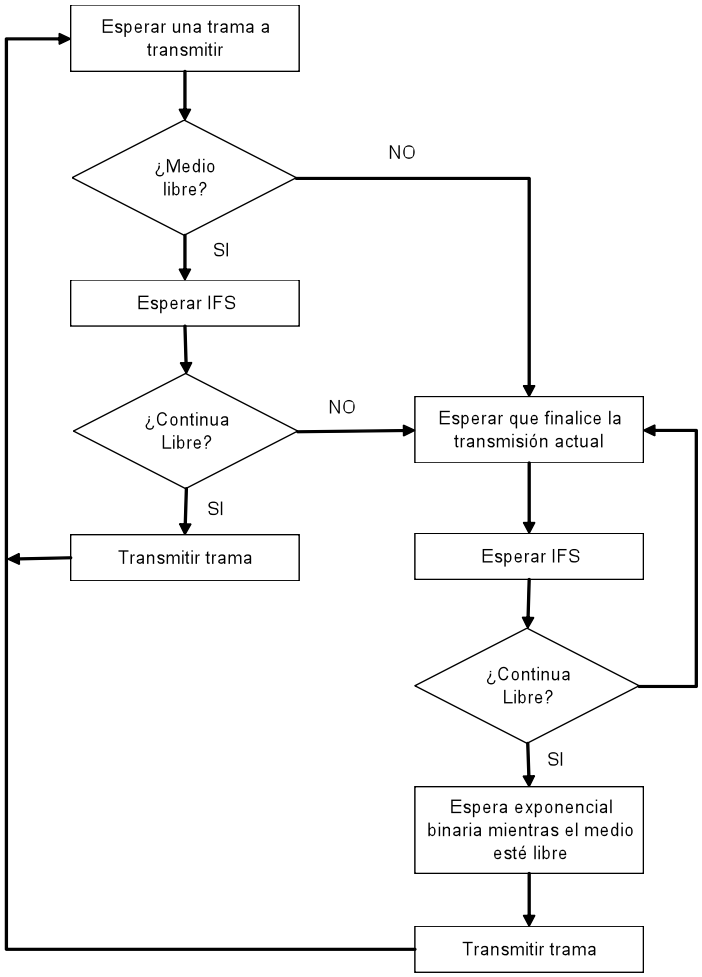
Tanenbaum, A. (2003). *Redes de computadoras* (4ª ed.). México, D. F.: Pearson Educación.

Tomasi, W. (2003). *Sistemas de comunicaciones electrónicas* (4ª ed.). México, D. F.: Prentice Hall.

Universidad de Catarina. (2007). *WLAN Red de área local*. Recuperado desde: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/de_l_j/capitulo3.pdf

Anexo 1

Figura 9. *Lógica de control de acceso al medio en IEEE 802.11*



Jaime Chaparro es Ingeniero electrónico de la Universidad Pontificia Bolivariana (Bucaramanga) y Especialista en Telecomunicaciones de la misma universidad. Postulado a Magíster en ingeniería de la Universidad pontificia Bolivariana de Medellín. Docente investigador, Universidad Manuela Beltrán. Investigador-docente, Corporación Universitaria Unitec.

Protección de los cinco (detalle)
Acrílico sobre lienzo
1 mt 80 cm x 1 mt 50 cm
2004