ESTADO DEL ARTE EN LA DETECCIÓN DE INTRUSIONES EN REDES 802.1

Luis Andrés Balseca Guzmán
Ing. Carlos Romero, Ing. Fabián Sáenz
Departamento de Eléctrica y Electrónica Escuela Politécnica del Ejército
Av. El Progreso S/N, Sangolquí, Ecuador

E-mail: luisandres2424@hotmail.com,
cgromero@espe.edu.ec, fgsaenz@espe.edu.ec

Resumen—El presente documento presenta un análisis de las características, estándares, arquitectura y dispositivos de las redes 802.11. Para posteriormente identificar los diferentes riesgos y tipos de ataques informáticos a los cuales se encuentran expuestos estas redes. Se identifican también los diferentes mecanismos de seguridad existentes que introducen niveles básicos y avanzados de seguridad en las redes inalámbricas. Así también se señala una herramienta muy empleada para la detección de intrusiones, los llamados sistemas de detección de intrusos inalámbricos (WIDS), se presentará su definición configuraciones y taxonomía.
Finalmente se recopila información significativa y actualizada de diferentes artículos académicos con el objetivo de identificar las diferentes técnicas e investigaciones desarrolladas para la detección de intrusiones en redes 802.11

I. INTRODUCCIÓN

Las redes inalámbricas han ganado mucha popularidad en los últimos tiempos, esta popularidad ha crecido hasta tal punto en que las podemos encontrar en casi cualquier ámbito de nuestra vida cotidiana, teléfonos inalámbricos, ordenadores y teléfonos móviles son algunos de los ejemplos más evidentes. La implementación más popular de red inalámbrica para entornos de redes de área local es el estándar IEEE 802.11 también popularmente conocidas como redes Wi-Fi.

La naturaleza del medio inalámbrico ofrece múltiples retos, un administrador necesita conocer qué está ocurriendo en su red, tanto desde el punto de vista de la seguridad como desde el punto de vista de la depuración de errores y optimización del rendimiento, tareas en las que la encriptación sólo cubre algunos aspectos y dificulta otros. En respuesta a esta demanda, ya han surgido soluciones, los sistemas de detección de intrusiones, estos sistemas permiten al administrador conocer si se están realizando ataques sobre su red, también pueden proporcionar servicios de localización del atacante e incluso implementan medidas activas para evitar intrusiones, como por ejemplo ataques DoS que eviten que los usuarios de nuestra red sean víctimas de ataques de hombre en el medio. A pesar de la necesidad de este tipo de herramienta, el estándar 802.11 es relativamente nuevo y complejo.

II. REDES 802.11

IEEE 802.11 es un conjunto de estándares para la comunicación de computadoras en redes inalámbricas de área local, desarrollados por el Comité IEEE 802 de la IEEE en las bandas públicas de frecuencia de radio de 5 GHz y 2.4 GHz.

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí.

2.1 CLASIFICACIÓN

A continuación se incluye un cuadro con la clasificación de los estándares 802.11 y sus características:

Tabla.1. Extensiones de la norma 801.11

Extensión	**Velocidad transmisión máxima (Mbps)**	**Banda de frecuencia**	**Radio de cobertura**
IEEE 802.11 a/h	54 Mbps	5 GHz	85 m
IEEE 80211b	11 Mbps	2.4 GHz	50 m
IEEE 802.11g	54 Mbps	2 4 GHz	65 m
IEEE 802.11n	300 Mbps	5 GHz	120 m

2.2 ARQUITECTURA DE LAS REDES 802.11

El modelo desarrollado por el grupo de trabajo del IEEE 802.11 se basa en sistemas divididos en células y permiten dos tipos de arquitectura:

-**Ad-hoc:** los dispositivos se conectan directamente entre ellos, sin necesidad de un punto de acceso o AP (Access Point)

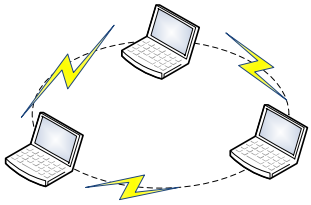

Fig. 2. Red Ad-hoc

-**Infraestructura:** todos los dispositivos realizan la comunicación inalámbrica a través de un punto de acceso o AP.

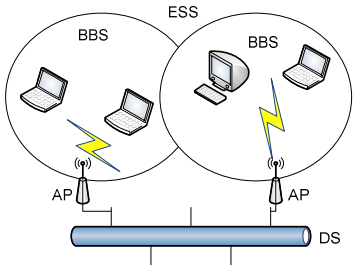

Fig. 3. Red Infraestructura

2.3 ESTRUCTURA

Las redes 802.11 tienen en común todas las capas del modelo OSI, a excepción de la capa MAC y la capa física (PHY), que están optimizadas para la transmisión inalámbrica.

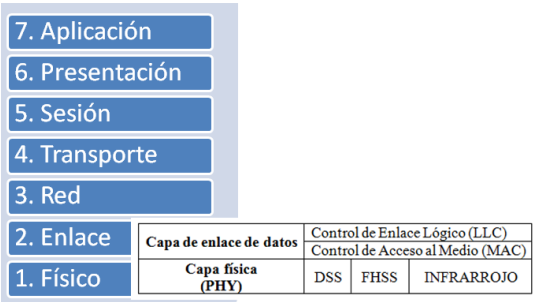

Fig. 4. Modelo OSI

2.3.1. Capa Física

La capa física define las especificaciones eléctricas y el tipo de señal para la transmisión de datos.

El estándar 802.11 ofrece tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa (DSSS)
- Espectro expandido por salto de frecuencias (FHSS)
- Luz infrarroja en banda base.

2.3.2. Capa de Enlace

La capa de enlace de datos se encarga de describir cómo se empaquetan y verifican los bits de manera que no tengan errores.

Está compuesta por dos subcapas:

- Control de enlace lógico (LLC).
- Control de acceso al medio (MAC).

2.3.3 Tipos de tramas

El protocolo MAC del estándar IEEE 802.11 distingue tres tipos de tramas con diferentes funciones: tramas de control, de datos y de gestión. Estos tipos están definidos por el campo FC (Frame Control) de la cabecera MAC del 802.11.

Frame Control Format (2 bytes = 16 bits)

Protocol	Type	Subtype	To Ds	From DS	More Frag	Retry	PW Mgt	More Data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
b0 b1	b2 b3	b4 b5 b6 b7	b8	b9	b10	b11	b12	b13	b14	b15

Fig. 5. Formato del Frame Control

- Tramas de Gestión: Establecen y mantienen la comunicación.
- Tramas de Control: Estas tramas tienen funciones de coordinación, ayudan en la entrega de datos.
- Tramas de Datos: Estas tramas llevan mucha información administrativa y, además, los datos que se quieren transmitir a través de la red 802.11

III. SEGURIDAD EN REDES 802.11

Para poder planear e implementar mecanismos de seguridad se debe primero conocer los diferentes tipos de amenazas a los que se encuentran expuestas las redes 802.11.

3.1. AMENAZAS A UNA RED 802.11

Una amenaza es cualquier tipo de evento o acción que puede producir un daño sobre los componentes que contienen, mantienen o guardan información.

3.1.1. Tipos de Amenazas

- Escuchas Ilegales

En una red 802.11 la principal amenaza es el potencial de que un tercero no autorizado escuche ilegalmente las señales de radio intercambiadas entre una estación inalámbrica y un Access Point, comprometiendo la confidencialidad de la información.

- Acceso no Autorizado

Es una amenaza donde un intruso puede introducirse en el sistema de una red WLAN, disfrazado como un usuario autorizado.

- Interferencias Aleatorias e Intencionadas

Las interferencias de señales de radio constituyen otro tipo de amenaza, que muchas de las veces son accidentales y provocadas por aplicaciones que trabajan en las bandas que no requieren licencias.

- Amenazas Físicas

Estas amenazas comprenden cualquier tipo de daño o destrucción de una parte de la infraestructura física, sea fortuita o planeada.

3.2 ATAQUES SOBRE REDES WI-FI

3.2.1. Clasificación de los ataques

- Ataques Pasivos

Es cuando alguien no autorizado accede a la

información, pero no realiza ninguna modificación de la misma.
Dentro de esta categoría se encuentran dos tipos:
- Vigilar/Espiar. Es aquel en el que el atacante monitorea el contenido de las transmisiones para descubrir el contenido de la información, se utiliza un dispositivo inalámbrico y un software apropiado denominado Sniffer.
- Analizar el Tráfico. Permite al atacante capturar la información transmitida y descubrir datos sobre los parámetros de la comunicación, como el ESSID, contraseñas, Direcciones MAC o IP, etc.

- Ataques Activos

Es con el cual se consigue tener acceso a la red, estos generan acciones evidentes en la red, por lo que facilitan su detección pero son difíciles de prevenir.

Dentro de las actividades más comunes se tiene:
- La Suplantación. Es un robo de identidad que consiste en hacerse pasar por un usuario autorizado para acceder a la información.
- Retransmisión. El atacante se coloca entre el emisor y el receptor, recibe la información y la retransmite, para evitar ser descubierto.
- Modificación. Se basa en modificar mensajes legítimos añadiendo o eliminando parte del contenido.
- Denegación de Servicio. El atacante impide la utilización normal de las transmisiones Wi-Fi. Estos ataques son muy difíciles de evitar y muy fáciles de realizar.

3.3 MECANISMOS DE SEGURIDAD

El estándar 802.11 define varios métodos para lograr la configuración segura de una red inalámbrica, cada método logra un nivel diferente de seguridad.

3.3.1 Protocolos de cifrado

- WEP (Wired Equivalent Privacy)

Este mecanismo necesita dos elementos importantes, en primer lugar se encuentran los vectores de inicializacion (IV's) el cual es un valor de 3 bytes que cambia en cada uno de los paquetes enviados y por otro lado está la clave WEP. Además de esto WEP utiliza el algoritmo de encriptación simétrico RC4 que toma los IV y la clave WEP para crear una clave "cifrada" (por llamarlo de alguna manera) esta clave viene incluida en el interior de cada paquete que se envía en texto claro.

- WPA (Wifi Protected Access)

WPA se distingue por tener una distribución dinámica de claves y nuevas técnicas de integridad y autentificación.
WPA se basa en el uso de un protocolo llamado TKIP (Temporal Key Integrity Protocol), una envoltura del WEP, que cambia las claves dinámicamente a medida que el sistema es utilizado, aparece una función MIC (Message Integrity Check) para controlar la integridad de los mensajes, detectando la manipulación de los paquetes.

- WPA2 (IEEE 802.11i)

WPA y WPA2 difieren poco conceptualmente, distinguiéndose principalmente en el algoritmo de cifrado que emplean. Mientras WPA se basa en el uso del algoritmo TKIP, que está basado en RC4 al igual que WEP, WPA2 utiliza CCMP (Counter-mode/CBC-MAC Protocol) basado en AES (Advanced Encrytion System), más potente que TKIP, recomendado por el NIST (Instituto Nacional de Estándares y Tecnología), de los más fuertes y difíciles de "crackear" hoy en día, que utiliza un cifrado simétrico de 128 bits.

3.3.2 ACL – Filtro de Direcciones MAC

Para incrementar la seguridad inalámbrica es posible configurar el AP para que acepte solo ciertas direcciones MAC y bloquee todas las demás, es decir, se crea una lista de direcciones MAC que serán permitidas por el AP para conectarse.

3.3.3 Cortafuegos (Firewall)

Es un dispositivo formado por uno o varios equipos que se sitúa entre una red interna y una red externa; de forma que todo el tráfico con la red exterior, tanto de entrada como de salida, debe pasar a través de él para que éste lo analice y decida si lo bloquea o no.

3.3.4. CNAC (Closed Network Access Control)

Este método está basado en desactivar el broadcast del ESSID en las tramas beacon utilizadas para que las estaciones detecten los Puntos de Acceso, por lo que impide que los dispositivos que no conocen el ESSID puedan asociarse a la red.

3.3.5 SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS)

- Definición

Un IDS (Intrusión Detection System) es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.
Algunas de las características deseables para un IDS son:
- Deben estar continuamente en ejecución con un mínimo de supervisión.
- Se deben recuperar de las posibles caídas o problemas con la red.
- Debe poderse analizar él mismo y detectar si ha sido modificado por un atacante.

- Debe utilizar los mínimos recursos posibles.

➢ COMPONENTES FUNCIONALES

Los IDS constan de los siguientes componentes:

- Dispositivo de recolección de Datos (sensor): se encarga de la recolección de datos desde el sistema monitorizado.
- Detector (motor de análisis de detección de intrusiones): procesa los datos obtenidos de sensores para identificar actividades intrusivas.
- Base de Datos: contiene la información recogida por los sensores, pero en formato pre-procesado (por ejemplo, la base de conocimientos de los ataques y sus firmas, los datos filtrados, perfiles de datos, etc.) Esta información es generalmente proporciona por la red y los expertos de seguridad.
- Dispositivo de Configuración: proporciona información sobre el estado actual del sistema de detección de intrusiones (IDS).
- Componente de Respuesta: inicia acciones cuando se detecta una intrusión. Estas respuestas pueden ser tanto automático (activo) o ser referidas a la interacción humana (inactivo).

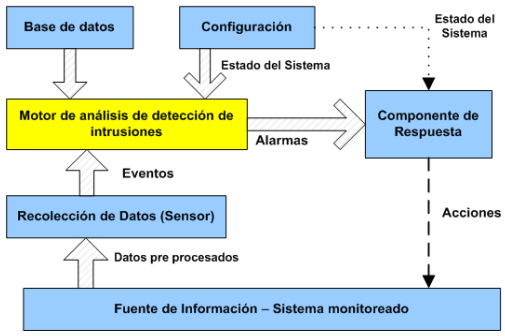

Fig. 5. Arquitectura de un IDS

➢ CLASIFICACIÓN

La taxonomía de los sistemas de detección de intrusos ha sido tratada en numerosos trabajos, de los que destacan los de Hervé Debar [1] y Stefan Axelsson [2] de Chalmers University of Technology en Suecia. En la figura 6 se muestra una clasificación de los IDS en función de todos estos criterios. Cada uno tiene distintos usos, ventajas y desventajas.

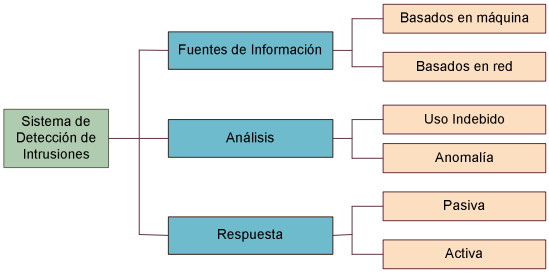

Fig. 6. Esquema de clasificaciones de ID

1. Fuentes de información

Esta clasificación se basa en el lugar donde el IDS analizará el tráfico, es decir, el tipo de protección que se dará al sistema.

➢ IDS basados en red (NIDS)

Estos IDS detectan ataques capturando y analizando paquetes de la red. Escuchando en un segmento, un NIDS (Network IntrusionDetectionSystem) puede monitorear el tráfico que afecta a múltiples hosts que están conectados a ese segmento de red, protegiendo así a estos hosts.

➢ IDSs basados en host (HIDS)

Están diseñados para monitorear, analizar y dar respuesta a la actividad de un determinado terminal (host). Su principal característica es que sólo protegen el terminal en el que se ejecutan.

2. Tipo de análisis

Los IDS pueden ser clasificados en dos grandes grupos, atendiendo al tipo de analizador o procesador de eventos:

➢ Los sistemas basados en uso indebido

Analizan el tráfico de la red y lo comparan con unas firmas (o reglas) previamente definidas.

➢ Los sistemas basados en detección de anomalías

Se centran en buscar actividades sospechosas en el sistema. Para ello, durante una fase inicial se debe entrenar el IDS para que se creen perfiles de actividad normal y legítima. A partir de ahí, el sistema informa de cualquier actividad que encuentre sospechosa

3. Respuestas de los IDS

Una vez se ha producido un análisis de los eventos y se han detectado ataques, el IDS reacciona. Las respuestas se pueden agrupar en dos tipos:

➢ Respuestas pasivas

En este tipo de respuestas se notifica al responsable de seguridad de la organización, al usuario del sistema atacado. También es posible avisar al administrador del sitio desde el cual se produjo el ataque avisándole de lo ocurrido, pero es posible que el atacante monitoree el correo electrónico de esa organización o que haya usado una IP falsa para su ataque.

➢ Respuestas activas

Las respuestas activas son acciones automáticas que se toman cuando ciertos tipos de intrusiones son detectados. Se puede establecer dos categorías:

- Recopilación de información adicional: consiste en incrementar el nivel de sensibilidad de los sensores para obtener más pistas del posible ataque (por ejemplo, capturando todos los paquetes que vienen de la fuente que originó el ataque durante un

cierto tiempo o para un máximo número de paquetes).

- Cambio del entorno: otra respuesta activa puede ser la de parar el ataque; por ejemplo, en el caso de una conexión TCP se puede cerrar la sesión establecida al atacante y a la víctima o filtrar en el router de acceso o en el firewall la dirección IP del intruso o el puerto atacado para evitar futuros ataques.

➢ SISTEMAS DE DETECCIÓN DE INTRUSIONES 802.11

"Un sistema inalámbrico 802.11 de detección de intrusiones (WIDS) consiste en un grupo de sensores y una unidad central que trabajan juntos para proporcionar supervisión del espectro inalámbrico." [1]

1. Arquitectura

Un WIDS puede ser:

➢ Centralizado

Es la combinación de sensores individuales los cuales recopilan y remiten todos los datos 802.11 a un analizador central, donde los datos son almacenados y procesados.

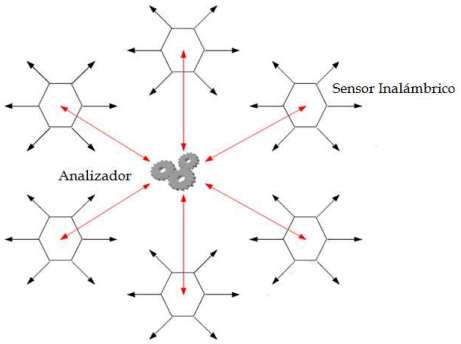

Fig. 7. Esquema de un WIDS centralizado

Ventajas

- Permite una fácil administración de protección a áreas grandes de redes 802.11. Expansiones a la red afectan solamente a él analizador.
- Permite una gran visión de lo que ocurre en todas las partes de la redes 802.11.

Desventajas

- Si el analizador falla, los sensores se vuelven inútiles y toda la red queda sin la protección.

➢ Distribuido

Suele incluir uno o más dispositivos que se encargan tanto de la recolección y procesamiento de la información de los IDS.

Ventajas

- No hay un solo punto de fallo.

Desventajas

- El costo de sensores con alta capacidad de procesamiento puede llegar a ser exagerado cuando muchos sensores son requeridos.
- La administración de múltiples sensores de procesamiento de información puede ser más difícil que la de un modelo centralizado.
- Expansiones en la red provocará una reprogramación en todos los sensores.

IV. TÉCNICAS EN LA DETECCIÓN DE INTRUSIONES EN REDES 802.11

Las propuestas para la detección de intrusos en un ambiente inalámbrico son variadas [3]. A continuación se describen las principales técnicas que han sido implementadas o que se encuentran en investigación. Este estudio se centra en la clasificación por el método de análisis para la detección de intrusiones, donde se tiene a las detecciones de uso indebido y de anomalías.

4.1. DETECCIÓN DE USO INDEBIDO

La detección de usos indebidos se puede implementar de las siguientes formas:

4.1.1 Firmas Simples

La detección de firmas compara los eventos que ocurren, con las cadenas o firmas almacenadas en una base de datos de escenarios de ataque en busca de coincidencias.
Su principal inconveniente es la necesidad de desarrollar e incorporar a la base de datos una firma nueva para cada nuevo tipo de ataque o vulnerabilidad descubierta.

4.1.2 Análisis de Transición de Estados

Se crean a partir de la construcción de una máquina de estados finitos. Los escenarios de ataques se representan como una secuencia de transiciones que caracterizan la evolución del estado de seguridad de un sistema. Cuando el autómata alcanza un estado considerado como una intrusión, se lanza la alarma. Algunas ventajas son las siguientes:

- Las transiciones ofrecen una forma de identificar una serie de patrones que conforman un ataque.

- El diagrama de estados define la forma más sencilla posible de definir un ataque. Así, el motor de análisis puede utilizar variantes del mismo para identificar ataques similares.

- El sistema puede detectar ataques coordinados y lentos.

Sin embargo, presentan algunas desventajas:

[1] "Sistemas de detección de intrusiones en redes 802.11 Wireless LAN," NaujRevilo Blog Security.

- El lenguaje utilizado para describir los ataques es demasiado limitado, y en ocasiones puede resultar insuficiente para recrear ataque más complejos.

- El análisis de algunos estados puede requerir más datos del objetivo, por parte del motor. Esto reduce el rendimiento del sistema.

4.1.3 Sistemas Expertos

Los sistemas expertos tienen el conocimiento codificado mediante reglas de implicación (condición-acción) de tipo "if-then-else"para examinar los datos. Realizan análisis mediante funciones internas al sistema, de forma completamente transparente al usuario.

Una de las ventajas más importantes de utilizar reglas "if-then" es que mantiene separados el control de razonamiento y la formulación de la solución del problema.
La principal desventaja que se plantea es que los patrones no definen un orden secuencial de acciones.

4.2 DETECCIÓN DE ANOMALÍAS

La detección de anomalías puede implementarse de las siguientes formas:

4.2.1 Modelos Estadísticos

Las variables y características se miden en escalas de tiempo determinados y estadísticamente perfiladas para desarrollar una línea de base de un comportamiento normal o esperado del equipo o de la red monitoreada. La divergencia de esta línea de base que excede un umbral dará lugar a una alerta. Seleccionando las variables y características correctas de perfil suele ser una tarea de enormes proporciones y la elección de los atributos equivocadas pueden conducir a una alta tasa de falsos positivos.

Ventajas
- Aprenden adaptativamente el comportamiento de los usuarios.

-No requieren el mantenimiento que necesitan los sistemas de detección de usos indebidos.

- No utilizan bases de firmas o patrones. Esto implica, contar con un modelo que utilice las métricas precisas, y que se adapte adecuadamente a los cambios de comportamiento de los usuarios.

Desventajas
- Puede ser paulatinamente entrenada, cosa que no ocurre con la detección de usos indebidos. Un usuario malicioso que supiera que está siendo monitorizado, podría cambiar intencionadamente su actitud para que, en un momento dado, el sistema identificara como normal un comportamiento hostil.

- Gran consumo de recursos que utilizan frente a otros modelos propuestos. Los análisis estadísticos normalmente requieren más tiempo de proceso que los sistemas de detección de usos indebidos.

- No pueden reconocer directamente ataques realizados mediante sucesiones de eventos en un determinado orden. Esto representa una seria limitación, dado el elevado número de intrusiones basadas en estas características.

4.2.2 Modelos basados en la especificación

La detección de anomalías que usa modelos basado en la especificación no se basa en la recolección estadística que representa el comportamiento correcto del sistema o de la red monitoreada. En cambio, el comportamiento correcto esperado es explícitamente dado en un modo declarativo. Esto se conoce como una especificación. Las desviaciones de esta especificación son tratadas como eventos maliciosos. Una especificación puede estar basada en las transiciones de estado que se producirían durante el comportamiento normal.
La mayor fortaleza de las técnicas basadas en anomalías es que son capaces de detectar ataques tanto existentes como nuevos, sin tener que volver a configurar o actualizar en cualquier forma [4].

4.3 TÉCNICAS COMPLEMENTARIAS

Existen varias técnicas que a pesar de no pertenecer específicamente al dominio de los sistemas de detección de intrusiones mejoran el rendimiento de estos.

4.3.1 Correlación de alertas

Las técnicas basadas en correlación de alertas compararan con todas las alertas y amenazas que tengan atributos o características parecidas (ej: dirección IP origen, IP destino, puertos objetivo). Las alertas cuyos atributos posean un alto nivel de similitud se agrupan en alertas generales ya existentes o se crea nuevas si ninguna de las existentes encaja dentro del intervalo de confianza definido.

4.3.2 Minería de datos

La minería de datos es un conjunto de técnicas que no necesitan intervención humana para extraer los modelos que representan bien ataques, o bien el uso legítimo del sistema.
La detección de intrusiones basada en minería de datos proporciona la oportunidad de aprender un modelo generalizado. Este modelo puede detectar

ataques hasta ese momento nunca vistos mediante el análisis de datos en bruto procedentes de BSM (Basic Security Module) de sistemas UNIX o de herramientas ampliamente difundidas como Network Fligth Recorder.

4.3.3 Detección de MAC Spoofing

MAC Spoofing (Suplantación de MAC) permite a un atacante asumir la dirección de un nodo de la red 802.11 y lanzar a ataques a dicha red utilizando la identidad del nodo legítimo.
Un número de diferentes técnicas se han sugerido para detectar la actividad de suplantación de MAC en una red 802.11. Estas son tratadas a continuación:

- Monitoreo del número de secuencia

Se basa en el uso del campo de control de secuencia de las tramas MAC 802.11. Este campo de 2 bytes de longitud contiene un número de secuencia de 12 bits, que se utiliza para numerar las tramas transmitidas entre un transmisor y un receptor dado y un número de fragmento de 4 bits, que se utiliza para la fragmentación y reensamblaje (véase la Figura 8).

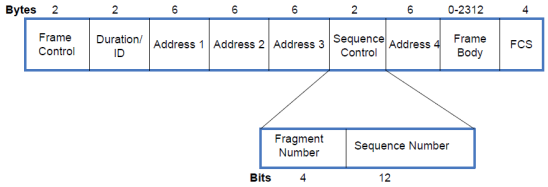

Figura 8. Campo de control de secuencia de la trama MAC 802.11

El protocolo 802.11 requiere que todos los nodos de la red 802.11 incrementen de forma monótona el campo de número de secuencia de 12 bits en la cabecera MAC para cada transmisión de tramas de gestión y datos. Los cambios abruptos en números de secuencia para una dirección MAC particular, se utilizan como un indicador de la suplantación de MAC.

- Fingerprinting

Se basa en función de las características únicas. La combinación de controlador de dispositivo, chipset de radio y firmware proporciona a cada nodo WLAN una huella digital única de su implementación 802.11.

El fingerprinting de nodos en redes 802.11 también se puede realizar en la capa física. Hall et al. [26] sugieren el uso de huellas digitales de radio frecuencia (RFF) para la detección de suplantación de MAC donde el RFF (Radio Frequency Fingerprinting) identifica de forma exclusiva las huellas digitales de la señal que genera un receptor transmisor. Mediante el uso de la las huellas del receptor transmisor de una dirección MAC, cualquier intento de falsificar la dirección MAC se puede detectar.

- Determinación de la Ubicación

La localización de un nodo en particular se determina generalmente mediante sus valores de intensidad de señal, se basa en el principio de que un atacante no podrá copiar la fuerza de la señal que recibe el sensor desde una estación, sucede porque la fuerza de la señal recibida depende del receptor como del emisor, con lo que si un atacante se encuentra en una ubicación física diferente, la probabilidad de que al sensor le llegue una trama con una fuerza de señal parecida a las que emite la estación legítima es muy baja.

Una vez que se conoce la ubicación de una dirección MAC, cualquier cambio en su ubicación pueden ser utilizados como una indicación de la actividad MAC spoofing.

4.3.4 Agentes Autónomos para la Detección de Intrusiones

La principal carencia de los primeros IDS es que los datos son recogidos por un solo sensor, además, algunos de los que intentan solucionar esta desventaja utilizan una colección de datos distribuida, pero analizada por una consola central. Por lo que se ha introducido el término de Agente Autónomo definido como una entidad software capaz de analizar actividades de una manera flexible e inteligente, capaz de funcionar continuamente y de aprender por su experiencia y la de otros agentes, además de comunicarse y cooperar con ellos. Los agentes son autónomos porque son entidades que se ejecutan independientemente y no necesitan información de otros agentes para realizar su trabajo.

4.3.5 Redes neuronales

Las redes neuronales son sistemas artificiales que tratan de copiar la estructura de las redes neuronales biológicas con el fin de alcanzar una funcionalidad similar.

Las redes neuronales artificiales [5] tratan de emular tres conceptos claves:
- Procesamiento paralelo, derivado de que los miles de millones de neuronas que intervienen, por ejemplo en el proceso de ver, están operando en paralelo sobre la totalidad de la imagen

- Memoria distribuida, mientras que en un computador la información está en posiciones de memoria bien definidas, en las redes neuronales

biológicas dicha información está distribuida por la sinapsis de la red, existiendo una redundancia en el almacenamiento, para evitar la pérdida de información en caso de que una sinapsis resulte dañada.

- Adaptabilidad al entorno, por medio de la información de las sinapsis. Por medio de esta adaptabilidad se puede aprender de la experiencia y es posible generalizar conceptos a partir de casos particulares.

4.4 ANÁLISIS DE LAS TÉCNICAS EMPLEADAS EN LA DETECCIÓN DE INTRUSIONES

La estrategia más utilizada para la detección de intrusiones consiste en la detección de uso indebido (patrones) para reconocer ataques previamente conocidos. La mayoría de los sistemas disponibles en el mercado son de este tipo. Sin embargo, la detección de uso indebido puede acarrear varios problemas como la incapacidad de detectar los ataques nuevos y sus variantes. Mientras que las técnicas basadas en anomalías detectan desviaciones en el comportamiento esperado o normal de los sistemas y las redes, las cuales pudieran constituir intentos de ataques. Por tal motivo, las técnicas basadas en el descubrimiento de anomalías son potencialmente capaces de detectar los ataques existentes y los nuevos, sin la necesidad de ser pre-configurados o actualizados de ninguna manera [6].

La selección de campos de utilidad para la detección de intrusiones en redes 802.11 depende de las características y de los atributos a los cuales están caracterizados y constituye la etapa más crítica en la implementación del clasificador de intrusiones. El problema mayor ha sido, para muchos, la manera de seleccionar campos óptimos que puedan ser evaluados por el algoritmo de aprendizaje escogido para el detector. En [7], los autores proponen un algoritmo conciso de selección de los mejores campos de utilidad de la trama MAC del estándar 802.11 que caracterizan de manera eficiente el tráfico normal y distinguen el tráfico anormal con especificaciones de intrusiones. En [7] se llegó a la selección los siguientes atributos:

Tabla.2. Lista del conjunto óptimo de características.

Caraterística	**Descripción**
IsWepValid	Indica si la verificación WEB ICV[2] es exitosa.
DurationRange	Indica si el valor de duración es bajo (<5ms), medio (entre 5-20ms), o alto (>20 ms).
MoreFragment	Indica si una trama es o no fragmentada.
ToDS	Indica si la trama está destinada al sistema de distribución.
WEP	Indica si la trama es procesada por el protocolo WEB.
CastingType	Indica si la dirección de destino es unicast, multicast o broadcast.
Type	Indica el tipo de la trama (Gestión, Control o Datos)
SubType	Indica el subtipo de la trama

Si se desarrolla un modelo que describa el comportamiento normal de una red 802.11, utilizando solo los parámetros de paquetes de control y gestión de la capa de enlace, se podría obtener un detector de intrusiones basado en anomalías que detecte las intrusiones nuevas y las conocidas para este tipo de tráfico.

V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se realizó un análisis de las ventajas y desventajas de la utilización de redes 802.11. Y se mostró la importancia de la seguridad y de la detección de intrusiones en las redes 802.11.

- Además de las vulnerabilidades existentes en los protocolos implementados para la seguridad en redes 802.11, tales como las de los protocolos WEP, la posibilidad del cambio de las direcciones MAC entre otros, existen vulnerabilidades inherentes al formato y uso de las tramas MAC dependiendo del tipo de trama que se está analizando. Estas vulnerabilidades constituyen unas de las bases de las amenazas a las cuales están sometidas las redes 802.11. Por lo que si los WIDS son capaces de detectar tramas falsificadas serán capaces de detectar la mayoría de los ataques.

- Los sistemas de detección de intrusiones presentan un mayor grado de integridad al resto de la infraestructura de seguridad. Cumplen además cuatro funciones principales: monitorizar, detectar y responder a la actividad que se considere sospechosa.

- Los detectores de uso indebido pueden reconocer ataques conocidos, siendo posible la actualización de sus bases de ataques periódicamente de forma similar a como ya se hace con los antivirus. Los detectores de anomalía son una de las herramientas de seguridad más prometedoras, pudiendo detectar ataques no conocidos, valiéndose de gran variedad de métodos de análisis.

- La obtención de un WIDS que detecta intrusiones en la capa de enlace constituye un gran avance en la solución de los problemas de inseguridad de las redes inalambricas, ya que la capa de enlace es la que caracteriza el acceso al medio inalámbrico.

[2] Valor de comprobación de integridad (Integrity Check Value).

- La arquitectura WIDS puede ser centralizada o descentralizada. En los sistemas centralizados, los datos se correlaciona en una ubicación central y las decisiones y las acciones se realizan sobre la base de esos datos. En los sistemas descentralizados, las decisiones se toman en el sensor.

5.2 RECOMENDACIONES

- Con los nuevos protocolos que aparecen en el mercado, algunos inclusive usan canales múltiples, un WIDS tendrá que ser compatible con todos los protocolos de velocidad más alta y baja.

- Generalmente las redes inalámbricas son fáciles de detectar, por lo que es necesario establecer políticas de seguridad y tomar las medidas de seguridad adecuadas a la hora de implementar estas redes.

- Los WIDS pueden sufrir de la generación de falsas alarmas. Esto conduce a la reacción inapropiada frente a un ataque. Se necesita tener un mejor y más preciso identificador de intrusiones para reducir significativamente sus falsos positivos.

- Con el aumento del tráfico de red también crecen las necesidades de recursos de sistema por parte de los detectores. Una de las soluciones que se están empezando a aplicar consiste en la fabricación de soluciones específicas basadas en hardware, que alivien en cierto modo la carga de proceso a la que están sometidos los sistemas de detección. Probablemente esta opción será bastante común en muchos de los productos que están por venir.

- Los sensores tienen una capacidad limitada para recibir las señales fiables en una célula y la efectividad los WIDS reducirá significativamente si los sensores no se colocan en una ubicación apropiada.

REFERENCIAS

[1] Hervé Debar, Marc Dacier, and Andreas Wespi, “Towards a Taxonomy of Intrusion Detection Systems”, Computer Networks, vol. 31, pp. 805-22, 1999.

[2] Axelsson, S. Intrusion Detection Systems: A Taxonomy and Survey. Technical Report 99-15, Dept. of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden.

[3] Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 – 196. Wireless/Mobile Network Security, chapter 7 “A Survey on Intrusion Detection in Mobile Ad Hoc Networks”, 2006.

[4] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 125–134, 2003.

[5] Haykin S. Neural Networks, McMaster University , Ontario, Canada 1994.

[6] H. Debar and J.Viinikka, "Intrusion detection: Introduction", en FOSAD 2004/2005, 2005.

[7] MOSER, M., Ataques a Clientes Inalámbricos EN EL PUNTO DE MIRA. 2009.

BIBLIOGRAFÍA

- 802.11, A. S. (1999). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

- Aironjack. (2010). CONCEPTOS BÁSICOS DE REDES WIFI Y SU SEGURIDAD. Obtenido de http://www.elhacker.net/manual_hacking_wireless.html

- Alfaro, E. J. Implantación de un IDS en la U. de Valencia. Obtenido de http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

- Alliance, W. F. (2013). Obtenido de http://www.wi-fi.org

- Bace, R., & Mell, P. (Noviembre 2001). Intrusion Detection System. Elseiver Ltd.

- Balsubramaniyan, J., Garcia-Fernandez, J., Isacoff, D., & Spafford, E. (1998). An Intrusion Detection Using autonomous Agent.

- Boob, P., & Jadhav, S. (Agosto 2010). Wireless Intrusion Detection System. International Journal of Computer Applications.

- Borghello, C. (2009). Detección de Intrusos en Tiempo Real. Obtenido de http://www.segu-info.com.ar/proteccion/deteccion.html

- Borisov, N., Goldberg, I., & Wagner, D. (Julio 2001). Intercepting mobile communications: The

insecurity of 802.11.

- Cañás, J. (marzo de 2013). Obtenido de Introducción a las Redes Inalambricas 802.11: http://www.microalcarria.com/descargas/documentos/Wireless/wireless.pdf

- Chiu, S. H. Seguridad en Redes Inalámbricas 802.11. Obtenido de http://www.ciens.ucv.ve:8080/genasig/sites/redesmov/archivos/Seguridad%20en%20Redes%20Inalambricas%20802.pdf

- Componentes y Topologías de una Red Inalámbrica. (2007). Obtenido de http://ieeestandards.galeon.com/aficiones1573328.html

- EISIC, U. F. (2009). DEFENSAS Y ATAQUES A LA SEGURIDAD EN REDES WLAN.

- Estándar IEEE 802.11. (2011). Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/de_l_j/capitulo2.pdf

- Institute of Electrical and Electronics Engineers. (2013). Obtenido de http://www.ieee.org

- Intelligraphics. (noviembre de 2011). Introduction to IEEE 802.11. Obtenido de http://www.intelligraphics.com/introduction-ieee-80211

- Mar, U. I. (2005). MONITORIZACIÓN DE REDES 802.11. Obtenido de http://ants.inf.um.es/staff/lolo/files/monitorizacion.pdf

- Pablete, O. (2005). An Overview of the Wireless Intrusion Detection System. SANS Institute.

BIOGRAFÍAS

Luis Andrés Balseca Guzmán
Nació en Quito - Ecuador, en 1988.
Realizo sus estudios secundarios en el Colegio San Gabriel obteniendo el título de Físico Matemático en el 2005. Realizó sus estudios en la Escuela Politécnica del Ejército en la carrera de Ingeniería Electrónica, Redes y Comunicación de Datos.

Carlos Gabriel Romero Gallardo.
Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército (2002) y Especialista en Proyectos de Investigación Científica y Tecnológica en la Universidad Complutense de Madrid (2006).
Candidato a PhD Universidad Nacional de la Plata.
Es profesor de la Escuela Politécnica del Ejército.
Sus áreas de interés e investigación son Seguridad de la Información, Networking con TCP/IP e Implementación de servicios y aplicaciones con software libre

Fabián Gustavo Sáen Enderica
Ingeniero en Electrónica, graduado en la Escuela Politécnica del Ejército, con Maestría en Ciencias en Ingeniería Electrónica y especialidades en Redes de telecomunicaciones, así como administración y economía de las telecomunicaciones y actualmente es candidato a Doctor en Ciencias
Ha trabajado en varias empresas de comunicaciones, así como es docente Universitario, de pregrado y postgrado en el Ecuador.
Ha sido representante de la CEPAL en el tema de TICs y discapacidades, así como como coordinador del grupo de investigación en ayudas tecnológicas para discapacitados en la ESPE.