REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 13. No. 1, enero-abril, 2014, p. 82-98 ISSN 1729-3804

DETECCIÓN DE NODOS EN EL ENTORNO INALÁMBRICO (Wi-Fi)

WIRELESS WI-FI NODES DETECTION

Ing. Lucy Coya Rey1, Ing. Talia O. Ledesma Quiñones2, Dr. C. Walter Baluja García3, Ing. Luis A. Marichal Alcántara4
1 Complejo de Investigaciones Tecnológicas Integradas (CITI), lucy.cr@udio.cujae.edu.cu
2 Complejo de Investigaciones Tecnológicas Integradas (CITI), talia.lq@udio.cujae.edu.cu
3 Instituto Superior Politécnico "José A. Echeverría", walter@tesla.cujae.edu.cu
4 Instituto Superior Politécnico "José A. Echeverría", luismarichal@electrica.cujae.edu.cu

RESUMEN: Los monitores de red (sniffers) son herramientas muy importantes para la gestión de redes, ya que su función principal es monitorizar y analizar el tráfico circulante. Existen en el mercado sniffers de paquetes muy completos y con gran cantidad de prestaciones, tanto para redes alambradas como para entornos inalámbricos, aunque algunas son poco difundidas o existen únicamente en software propietarios. Este es el caso de las facilidades necesarias no solo para monitorizar el tráfico, sino también para detectar los dispositivos inalámbricos existentes en un entorno dado. El objetivo principal de este artículo es proponer algoritmos de trabajo, basados en las tramas 802.11 y la información que brindan sus campos, que posibiliten la identificación de los nodos en el entorno inalámbrico. Los algoritmos fueron implementados en una herramienta de código abierto que carecía de dicha prestación y se realizaron pruebas de campo que comprueban la efectividad de los mismos.

Palabras Clave: monitores de red, monitorizar, tramas 802.11, algoritmos de trabajo

ABSTRACT: Sniffers are very important tools for network management because their main function is to monitor and analyze traffic sent through the network. There are very complete packet sniffers with a lot of benefits in the market, both for wired networks and for wireless environments, although some of these are less known or exist only in proprietary software. This is the case of the necessary facilities not only to monitor traffic, but also to detect existing wireless devices in a given environment. The main objective of this paper is to propose work algorithms, based on 802.11 frames and the information provided by their fields, enabling the identification of the nodes in the wireless environment. The algorithms were implemented in an open source tool that lacked this feature and field tests were conducted to verify their effectiveness.

Keywords: sniffers, monitor, 802.11 frames, work algorithms

INTRODUCCIÓN

Las redes inalámbricas WLAN (del inglés Wireless Local Area Network) han pasado de ser un complemento de las alambradas a ser una alternativa que se ha disparado en popularidad en la última década. El estándar 802.11 de la IEEE (del inglés Institute of Electrical and Electronics Engineers) también denominado Wi-Fi (del inglés Wireless Fidelity), ha ido ganando seguidores en el universo de las redes de comunicación, siendo cada vez más utilizado y difundido.

Los dispositivos que lo soportan ofrecen una gran cantidad de facilidades que resultan muy atractivas para los usuarios. Sin embargo, el medio físico empleado (ondas electromagnéticas) es por naturaleza inseguro y susceptible de ser interceptado, lo que se vuelve un aspecto desfavorable al abrir un espacio para ataques a través de él y poner en riesgo la integridad de toda la red.

La monitorización y el análisis de la red inalámbrica se ha vuelto cada vez más importante a medida que las telecomunicaciones modernas se han ido complejizando y expandiendo. El análisis del tráfico y la detección de nodos constituyen prestaciones vitales para conocer la composición de la red, en aras de garantizar que no existan usuarios, dispositivos o servicios no autorizados, formando parte del entorno inalámbrico.

IDENTIFICACIÓN DE NODOS EN EL ENTORNO INALÁMBRICO (802.11)

Una herramienta destinada a la monitorización de las WLAN debe contar con determinadas prestaciones de relevancia para su trabajo, tales como:

- Capturar paquetes en el entorno inalámbrico 802.11.
- Aplicar filtros de captura y de visualización de paquetes.
- Trabajar con capturas realizadas por herramientas similares.
- Mostrar el contenido de los paquetes capturados e identificar protocolos por capas.
- Identificar los nodos en la red (autorizados o no) del entorno inalámbrico (de forma pasiva y activa), proporcionando detalles de ellos.
- Identificar las sesiones de comunicación establecidas.
- Recuperar los contenidos transferidos en las sesiones.
- Identificar y escuchar llamadas de Voz sobre IP (VoIP).
- Mostrar estadísticas sobre el estado y los principales parámetros de calidad de la comunicación.
- Permitir la gestión de la información de captura y análisis a través de una base de datos.

El presente artículo aborda en profundidad cómo implementar la prestación de la identificación de los nodos inalámbricos, utilizada para determinar quiénes son solamente hosts, quiénes se desenvuelven como puntos de acceso (AP, del inglés Access Point), así como el modo de comunicación o trabajo (Infraestructura/Ad hoc). Esto resulta de enorme significación para que los administradores puedan percatarse de intrusiones y brechas de seguridad, identificarlas y contrarrestarlas.

Para desarrollar los algoritmos que permitirán implementar esta prestación se realizó primeramente un estudio de las tramas utilizadas en el entorno inalámbrico Wi-Fi.

El estándar 802.11 define varios tipos de tramas las cuales cumplen con un objetivo específico. Estas pueden ser clasificadas según la función que realizan en la WLAN, por lo que van a existir tramas de datos, que transportan la información de capas superiores, tramas de gestión que permiten mantener las comunicaciones y tramas de control para, como su nombre indica, controlar el acceso y empleo del medio.

A continuación se realizará un análisis de aquellas tramas y de los campos que resultan de utilidad para la detección de los nodos inalámbricos y sus modos de trabajo.

Formato general de una trama 802.11

El formato de trama MAC (Figura. 1) incluye un conjunto de campos de orden fijo en todas las tramas. Los campos de Address 2, Address 3, Sequence Control, Address 4 y el Frame Body, sólo están presentes en ciertos tipos de tramas [1].

Figura 1. Formato general de la trama MAC [1].

Campos de Dirección (Address 1, Address 2, Address 3, Address 4)

Hay cuatro campos de direcciones en el formato MAC. Estos campos se utilizan para indicar el BSSID (Basic Service Set Identifier), la dirección de origen (SA, del inglés Source Address), la dirección de destino (DA, del inglés Destination Address), la dirección de la estación transmisora (TA, del inglés Transmitter Address) y la dirección de la estación receptora (RA, del inglés Receiver Address). El uso de determinado campo de dirección se especifica por la posición relativa de este (1-4) en la cabecera MAC, independiente del tipo de dirección presente en ese campo [1].

Campo de control de trama (Frame Control)

El campo Frame Control (Figura. 2) se compone de los siguientes subcampos: Versión del Protocolo (Protocol Version), Tipo (Type), Subtipo (Subtype), To DS, From DS, Más Fragmentos (More Fragments), Reintentar (Retry), Administración de Potencia (Power Management), Más Datos (More Data), Trama Protegida (Protected Frame) y Orden (Order) [1].

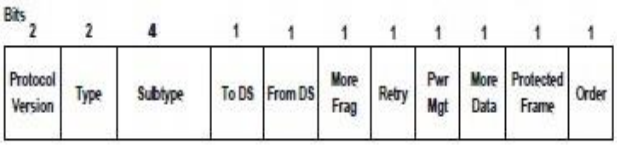

Figura 2. Formato del campo de control de trama (Frame Control) [1].

Campos Tipo y Subtipo (Type, Subtype)

Estos campos son de 2 bits y 4 bits de longitud respectivamente y juntos identifican la función de la trama. Cada tipo de trama está representado por varios subtipos. En [1] se definen las combinaciones válidas de tipo y subtipo.

Campo To DS

Este campo tiene 1 bit de longitud y se coloca en 1 en los tipos de tramas de datos destinados al DS (del inglés Distribution System), lo que incluye todos los tipos de tramas de datos enviados por estaciones asociadas a un AP. El campo To DS se establece en 0 en el resto de las tramas [1].

Campo From DS

Este campo tiene 1 bit de longitud y se coloca en 1 en los tipos de tramas de datos que salen del DS, mientras se establece en 0 en el resto de las tramas [1]. Las combinaciones de bits To/From DS y sus significados se muestran en la Tabla I.

Tabla I: Posibles combinaciones de los bits From DS y To DS [1].

Combinaciones To/From DS	Significado
To DS = 0 From DS = 0	La trama de datos es enviada de una estación a otra en el mismo IBSS. Estos *bits* se establecen en cero en las tramas de gestión y de control igualmente.
To DS = 1 From DS=0	Trama de datos destinada al Sistema de Distribución.
To DS = 0 From DS =1	Trama de datos saliendo del Sistema de Distribución.
To DS =1 From DS = 1	La trama es enviada de un AP a otro AP en el DS Inalámbrico.

Tramas de Control

En este tipo de trama en el campo Frame Control, la mayoría de los subcampos tienen valor 0.Debido a que los bits From/To DS se establecen en 0, no se puede determinar por esta vía el modo de trabajo de los nodos, a no ser que se trate de las tramas Contention Free End (CF-End),CF-End + CF-Ack o PS-Poll que son intercambiadas entre los APs y las estaciones, o sea, en modo infraestructura [2].

Tramas de datos

El contenido de los campos de dirección en este tipo de trama depende de la combinación de los bits From/To DS (Tabla II). Si el campo se muestra como no aplicable (N/A), este es omitido. Address 1 siempre guarda la dirección del futuro receptor o receptores en caso de que sea una trama multicast, mientras Address 2 guarda la dirección de la estación que está transmitiendo la trama [1].

Tabla II: Contenido de los campos de dirección según los bits From DS y To DS [1].

To DS	*From DS*	*Addr 1*	*Addr 2*	*Addr 3*	*Addr 4*
0	*0*	DA	SA	BSSID	N/A
0	*1*	DA	BSSID	SA	N/A
1	*0*	BSSID	SA	DA	N/A
1	*1*	RA	TA	DA	SA

• DA: dirección MAC del destino de la trama de datos o de un fragmento de esta.

• SA: dirección MAC del origen de la trama de datos o de un fragmento de esta.

• RA: dirección MAC del AP en el DS que es el próximo receptor inmediato de la trama.

• TA: dirección MAC del AP en el DS que está transmitiendo la trama [1].

El BSSID de una trama de datos se determina como sigue [1]:

• Si la estación es un AP o está asociada a uno, el BSSID es la dirección del AP.

• Si la estación es un miembro de un IBSS, el BSSID es el IBSS.

Tramas de gestión

Existen varias tramas de gestión definidas según el estándar 802.11, pero se abordarán con mayor detalle las tramas utilizadas en el algoritmo de identificación de los nodos inalámbricos.

Trama Beacon

Las tramas Beacon anuncian la existencia de una red y son transmitidas en intervalos regulares para posibilitar que los dispositivos inalámbricos sean capaces no solo de identificar la red, sino también de seleccionar parámetros que les permitan asociarse a ella. En una red de infraestructura son los APs los encargados de transmitir estas tramas e identifican un BSS, mientras que dentro de un IBSS la responsabilidad de transmisión de las tramas Beacon es distribuida [1, 2].

Esta trama incluye algunos campos fijos dentro de su cuerpo [1, 2], de los cuales el Capability Information (Figura. 3) es el que interesa para los posteriores algoritmos de trabajo, debido a que sus dos primeros bits ESS e IBSS son mutuamente excluyentes y en dependencia de cómo se encuentren configurados, proporcionarán información relevante sobre los modos de trabajo.

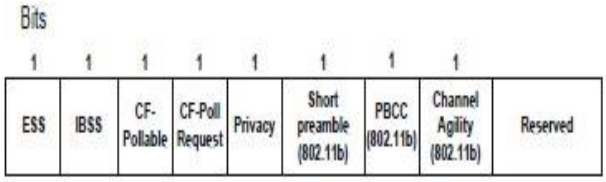

Figura. 3: Formato del campo fijo Capability Information dentro de la trama Beacon [2].

Probe Request

Las estaciones móviles hacen uso de las tramas Probe Request cuando deciden realizar un escaneo activo de un área en busca de redes 802.11. Contiene al SSID y en la cabecera las direcciones fuente y destino (SA, DA) y el BSSID [1, 2].

Existen tarjetas inalámbricas con drivers que les permiten asociarse a cualquier red, por lo que envían el SSID por difusión en las tramas Probe Request [2].

Probe Response

Es la trama que se envía como respuesta a la trama Probe Request si esta ha encontrado una red con parámetros compatibles. En redes de infraestructura es el AP el encargado de transmitir esta trama, pero en redes ad hoc esta tarea le corresponde a la estación que envió la última Beacon, que deberá ser quien responda las solicitudes durante el siguiente intervalo Beacon. Algunos de los campos son mutuamente excluyentes y se aplican las mismas reglas que en las tramas Beacon por su similitud [1, 2].

Authentication

La autenticación es el proceso de intercambio de identidades, ya sea entre dos estaciones (modo ad hoc), o con un AP (modo infraestructura) [2].

Existen diferentes algoritmos de autenticación representados por determinado número en el campo correspondiente. El proceso de autenticación puede conllevar varios pasos (en dependencia del algoritmo), por lo que existe un número de secuencia para cada trama enviada durante el intercambio [1, 2].

Association Request y Association Response

El proceso de asociación ocurre únicamente en las redes infraestructura, ya que son los APs los que requieren de este paso para que los clientes queden debidamente vinculados a él [2].

La estación móvil solicita una asociación con un AP y la notificación del éxito o el fracaso de esa petición se devuelve a la estación móvil mediante la respuesta.

Reassociation Request y Reassociation Response

La trama Reassociation Request es enviada por la estación si esta se mueve temporalmente del área de cobertura de un AP y desea reasociarse nuevamente a él, a lo que este responderá mediante la trama Reassociation Response [2].

La reasociación incluye un campo fijo dentro del cuerpo de la trama, que indica la dirección MAC del AP al cual la estación se encuentra actualmente asociada. La inclusión de esta información le posibilita al nuevo AP contactar al antiguo y transferir datos de asociación.

Proceso de establecimiento de la conexión.

Para poder desarrollar un algoritmo correspondiente a la identificación de nodos inalámbricos, es necesario conocer el proceso de establecimiento de la conexión en una red Wi-Fi.

El proceso de establecimiento de la conexión entre un par de nodos o más, o de un nodo y un AP en una red inalámbrica transcurre por tres estados consecutivos: scanning y sincronización, autenticación y asociación. Ni la etapa de scanning ni la de asociación son obligatorias para una satisfactoria comunicación.

En el primer estado el nodo encuentra un canal en el cual un AP está operando, define los parámetros de configuración y se sincroniza. El scanning puede hacerse pasivo o activo. En el primer caso el nodo escucha el canal de radio y espera por la transmisión de una trama Beacon. Si el scanning es activo, en cada canal de radio el nodo transmite una trama Probe Request que provoca la transmisión de una trama Probe Response. Durante el proceso de sincronización, el nodo establece los valores de Timestamp y el identificador BSSID recibidos del AP y las tramas previas.

Terminado el proceso anterior, el nodo comienza el estado de autenticación. En el estándar 802.11 se describen dos tipos de autenticación: sistema abierto y autenticación a través de llaves precompartidas, aunque un tipo más de autenticación se define en la especificación IEEE 802.11i [3]. Cuando se emplea autenticación abierta, entre el nodo y un AP existe un intercambio de dos tramas, la primera es una encuesta y la segunda una respuesta. La autenticación por medio de llaves pre-compartidas asume que el nodo y el AP soportan protocolos de encriptación compatibles y realizan un intercambio de cuatro tramas entre ambos.

En el estado final de asociación el nodo envía una trama de encuesta de asociación al AP y este transmite una respuesta, finalmente se le asigna al nodo un identificador de asociación [4].

Algoritmo genérico propuesto para la identificación pasiva de nodos

La identificación de los nodos inalámbricos que se propone hace uso de todos los tipos de trama, empleando un análisis que se enfoca en los campos de utilidad.

En la Figura. 4 se muestra el algoritmo genérico para la identificación de nodos inalámbricos, donde cada uno de los bloques que lo componen incluye otros algoritmos que serán abordados más adelante. El algoritmo supone que los paquetes ya han sido validados (cumplen con la norma) antes de comenzar a procesarlos.

Los pasos son los siguientes:

1. Captura de una trama 802.11.

2. Se determina si la trama capturada es de datos verificando que el campo Tipo=10 y en caso positivo se ejecuta el algoritmo Trama de Datos (Tipo=10) y se procede al paso 1. En caso negativo se ejecuta el paso 3.

3. Si no es una trama de datos, entonces se comprueba si es una trama de gestión verificando que el campo Tipo=00 y en caso positivo se ejecuta el algoritmo Trama de Gestión (Tipo=00) y se procede al paso 1. En caso negativo se ejecuta el paso 4.

4. Si no es una trama de gestión, entonces se pregunta si es una trama de control de Tipo=01 y en caso positivo se ejecuta el algoritmo Trama de Control (Tipo=01) y se procede al paso 1. Si la trama no fuera válida, esta se descarta y se procede al paso 1.

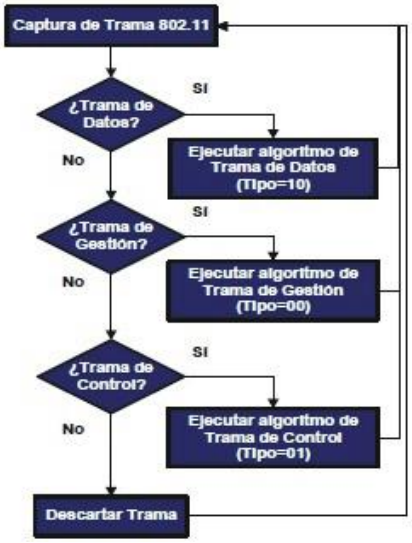

Figura 4. Algoritmo genérico para la identificación pasiva de nodos inalámbricos.

A continuación se describen los procesos que se llevan a cabo en los bloques que representan algoritmos particulares: Ejecutar el algoritmo Trama de Datos, Ejecutar el algoritmo Trama de Gestión y Ejecutar el algoritmo Trama de Control.

Algoritmo Trama de Datos (Tipo=10)

El algoritmo en cuestión (Figura. 5) se ejecuta una vez se haya determinado que se trata de una trama de datos. Hace uso de los bits From/To DS para determinar si la red es de infraestructura o ad hoc, y de acuerdo a la combinación detectada permite definir cuál dirección MAC dentro de la trama es un cliente o un AP. Cada uno de sus pasos se describe a continuación:

1. Se verifica si los bits From DS=0 y To DS=0, en caso positivo se notifica que la red opera en modo ad hoc. La dirección MAC del cliente destino estará en el campo Address 1, la dirección MAC del cliente fuente en el campo Address 2 y el BSSID en el campo Address 3. En caso negativo se pasa al paso 2.

2. Si los bits From DS y To DS presentan cualquier combinación diferente de 00, automáticamente se define que la red se encuentra operando en modo infraestructura y se procede con el algoritmo.

3. Se comprueba el valor de los bits From DS=1 y To DS=0, en caso positivo la dirección MAC del cliente destino se encontrará en el campo Address 1, la dirección MAC del AP en el campo Address 2 y la dirección MAC del cliente fuente en el campo Address 3. En caso negativo se ejecuta el paso 4.

4. Se comprueba el valor de los bits From DS=0 y To DS=1, y en caso positivo la dirección MAC del AP se encontrará en el campo Address 1, la dirección MAC del cliente fuente en el campo Address 2 y la dirección MAC del cliente destino en el campo Address 3. En caso negativo se procede paso 5.

5. La única variante posible es entonces From DS=1 y To DS=1 la cual no se señaliza. La dirección MAC del AP receptor se encontrará en el campo Address 1, la dirección MAC del AP transmisor se encontrará en el campo Address 2, la dirección MAC del cliente destino en el campo Address 3 y la dirección MAC del cliente fuente en el campo Address 4.

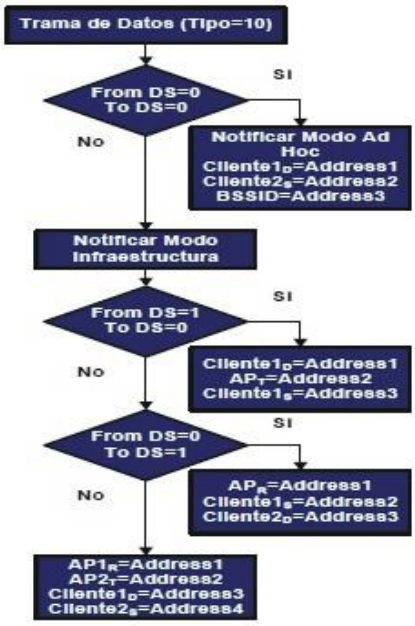

Figura 5. Algoritmo Trama de Datos (Tipo=10).

Algoritmo Trama de Gestión (Tipo=00)

El algoritmo propuesto (Figura. 6) se ejecuta una vez detectado que la trama capturada es de gestión. Primero se analizan cada uno de los subtipos de tramas de gestión con el objetivo de determinar de antemano los modos de trabajo, ya que si son tramas que se originan durante el proceso de asociación, por ejemplo, se puede decir que se está trabajando en modo infraestructura debido a que en modo ad hoc este no se realiza.

De cada trama se extraerán las direcciones MAC de los clientes y APs, dependiendo del modo de trabajo detectado. Las secuencias de pasos son:

1. Se verifica si el Subtipo=1000 (Beacon) o si el Subtipo=0101 (Probe Response) y en caso

positivo se procede a verificar el campo fijo Capability Information en los pasos 1.1 y 1.2. En caso negativo se ejecuta el paso 2.

1.1 Si el bit ESS=0 y el bit IBSS=1, entonces se notifica que la red opera en modo ad hoc. La dirección MAC del cliente destino estará en Address 1 y la dirección MAC del cliente fuente en Address 2. En caso negativo se ejecuta el paso

1.2. Se notifica que la red se encuentra trabajando en modo infraestructura. La dirección MAC del cliente destino se encontrará en Address 1 y la dirección MAC del AP fuente en Address 2.

2. Se verifica si el Subtipo=0100 (Probe Request) y en caso positivo se determina que la dirección MAC del cliente fuente se encontrará en Address 2 y se procede a los pasos 2.1 y 2.2. En caso negativo se ejecuta el paso 3.

2.1 Si los campos Address 1 y Address 3 contienen la misma dirección MAC, entonces se procede con los pasos 2.1.1 y 2.1.2. En caso negativo se ejecuta el paso 2.2.

2.1.1 Si el campo Address 1 contiene la dirección de difusión (broadcast = FF:FF:FF:FF:FF:FF), entonces se notifica que es un mensaje de difusión. En caso negativo se ejecuta el paso 2.1.2.

2.1.2 Si el campo Address 1 no contiene la dirección de difusión, entonces se notifica que la red opera en modo infraestructura y Address 1 tendría la dirección MAC del AP destino.

2.2 Si los campos Address 1 y Address 3 no contienen la misma dirección MAC, en Address 1 se encontraría la dirección MAC de un nodo destino del cual no podría obtenerse información de si es un cliente o un AP.

3. Se verifica si el Subtipo=1011 (Authentication) o si el Subtipo=1100 (Deauthentication) y en caso positivo se procede a los pasos 3.1, 3.2 y 3.3. En caso negativo se ejecuta el paso 4.

3.1 Si los campos Address 1 y Address 3 contienen la misma dirección MAC, entonces se notifica que la red está operando en modo infraestructura y Address 1 contendría la dirección MAC del AP destino y Address 2 la dirección MAC del cliente fuente. De lo contrario se ejecuta el paso 3.2.

3.2 Si los campos Address 1 y Address 3 no tienen la misma dirección MAC, entonces se verifica si los campos Address 2 y Address 3 son iguales. En caso positivo se notifica que la red está operando en modo infraestructura y Address 1 contendría la dirección MAC del cliente destino y Address 2 la dirección MAC del AP fuente. En caso negativo se ejecuta el paso 3.3.

3.3 Si los campos Address 2 y Address 3 no contienen la misma dirección MAC, entonces se notifica que la red está en modo ad hoc y Address 1 contendría la dirección MAC del cliente destino y Address 2 la dirección MAC del cliente fuente.

4. Se verifica si el Subtipo=0000 (Association Request) y en caso positivo se notifica que la red opera en modo infraestructura. La dirección MAC del AP destino estará en Address 1 y la dirección MAC del cliente fuente en Address 2. En caso negativo se ejecuta el paso 5.

5. Se verifica si el Subtipo=0001 (Association Response) o si el Subtipo=0011 (Reassociation Response) y en caso positivo se notifica que la red opera en modo infraestructura. La dirección MAC del cliente

destino se encontrará en Address 1 y la dirección MAC del AP fuente en Address 2. De lo contrario se ejecuta el paso 6.

6. Se verifica si el Subtipo=0010 (Reassociation Request) y en caso positivo se notifica que la red está en modo infraestructura. La dirección MAC del AP destino se encontrará en Address 1, la dirección MAC del cliente fuente en Address 2 y en el campo Current AP Address dentro del cuerpo de la trama estará la dirección MAC del AP previo al cual estaba asociado el nodo. En caso negativo se ejecuta el paso 7.

7. Se verifica si el Subtipo=1001 (ATIM, del inglés Announcement Traffic Indication Message) y en caso positivo se notifica que la red está operando en modo ad hoc. La dirección MAC del cliente destino se encontrará en Address 1 y la dirección MAC del cliente fuente en Address 2. En caso negativo se ejecuta el paso 8.

8. Se verifica si el Subtipo=1010 (Disassociation) y en caso positivo se notifica que la red está operando en modo infraestructura y se procede a los pasos 8.1 y 8.2.

8.1 Si los campos Address 1 y Address 3 contienen la misma dirección MAC, Address 1 tendría la dirección MAC del AP destino y Address 2 la del cliente fuente. En caso negativo se ejecuta el paso 8.2.

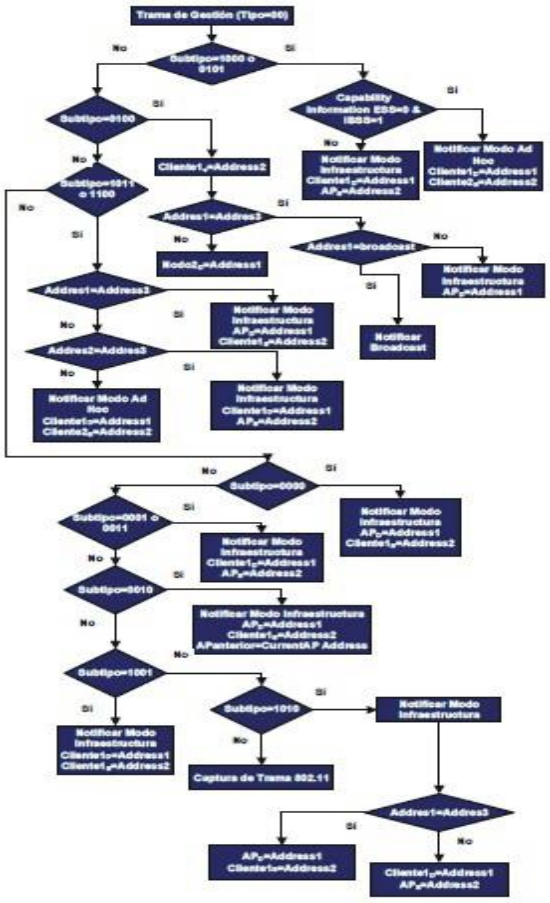

Figura 6. Algoritmo Trama de Gestión (Tipo=00).

8.2 Si los campos Address 1 y Address 3 no contienen la misma dirección MAC, Address 1 contendría la dirección MAC del cliente destino y Address 2 la del AP fuente.

9. En caso de no ser ninguna de las tramas de gestión anteriores se continúa con la captura de la siguiente trama 802.11.

Algoritmo Trama de Control (Tipo=01).

El algoritmo (Figura. 7) se ejecutará una vez se haya determinado que la trama detectada es de Tipo=01. Este basa su funcionamiento en identificar los diferentes subtipos de tramas de control para así determinar las direcciones MAC de los nodos que se están comunicando. La secuencia de pasos se enumera a continuación:

1. Se verifica si el Subtipo=1010 (PS-Poll) y en caso positivo se notifica que la red opera en modo infraestructura. La dirección MAC del AP receptor se encontrará en Address 1 y la dirección MAC del cliente transmisor en Address 2. En caso negativo se pasa al paso 2.

2. Se verifica si el Subtipo=1110 (CF-End) o si el Subtipo=1111 (CF-End + CF-ACK) y en caso positivo se notifica que la red opera en modo infraestructura. La dirección MAC del AP se encontrará en Address 2. En caso negativo se ejecuta el paso 3.

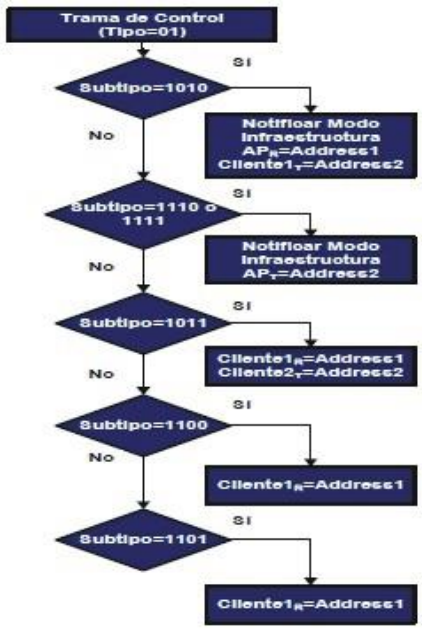

Figura 7. Algoritmo Trama de Control (Tipo=01).

3. Se verifica si el Subtipo=1011 (RTS) y en caso positivo la dirección MAC del cliente receptor se encontrará en Address 1 y la dirección MAC del cliente transmisor en Address 2. En caso negativo se ejecuta el paso 4.

4. Se verifica si el Subtipo=1100 (CTS) y en caso positivo la dirección MAC del cliente receptor estará en Address 1. En caso negativo se ejecuta el paso 5.

5. Se verifica si el Subtipo=1101 (ACK) y en caso positivo la dirección MAC del cliente receptor estará en Address 1.

Pruebas de campo

La aplicación que finalmente se conformó, llamada WifiGossip, tiene como base la herramienta NetworkMiner [5] (software de código abierto) al que se le adaptaron e implementaron los algoritmos descritos anteriormente. Para comprobar la veracidad de los mismos se realizaron varias pruebas de campo divididas en dos grupos, en el primero se capturó tráfico de una red ad hoc y en el segundo se trabajó en una red infraestructura. Los resultados fueron analizados con WifiGossip.

Dispositivos utilizados

Durante las pruebas de campo se emplearon varios dispositivos y tarjetas inalámbricas capaces de soportar los estándares 802.11 a, b y g. A continuación se mencionan cada uno de ellos:

- Dos tarjetas inalámbricas D-Link DWA-160 Xtreme N™ Dual Band.
- Una computadora equipada con una tarjeta inalámbrica NETGEAR 108 Mbps Wireless PCI Adapter WG311T.
- Una laptop equipada con una tarjeta inalámbrica ASUS (WL-107g) USB Wireless Network Adapter Versión 6.4.6.8.
- Un AP NETGEAR's ProSafe 802.11g Wg302.

Descripción de los escenarios de prueba

A continuación se describen cada uno de los escenarios de prueba y se analizan los resultados obtenidos.

Escenario #1 Red Ad Hoc

Este escenario (Figura. 8) se realiza en interiores, está conformado por un ordenador de escritorio y una laptop (MAC: 000EA6F7CCB5) que se comunican en modo ad hoc y otro ordenador de escritorio que es el encargado de supervisar el tráfico. A una máquina se le conectó la tarjeta inalámbrica D-Link (MAC: 1CBDB98935CA) y se configuró con la dirección IP 100.9.3.250, mientras la otra posee la tarjeta integrada NETGEAR (MAC: 001B2FCB895D); la laptop se configuró con la dirección IP 100.9.3.100. Se observan y analizan los resultados de la captura con el prototipo WifiGossip.

Figura 8. Escenario #1 Red Ad Hoc.

En este primer escenario, las PCs se encuentran estáticas. Desde cada uno de los hosts se realiza la descarga de documentos por vía HTTP (del inglés Hyper Text Transfer Protocol) y a través de recursos compartidos.

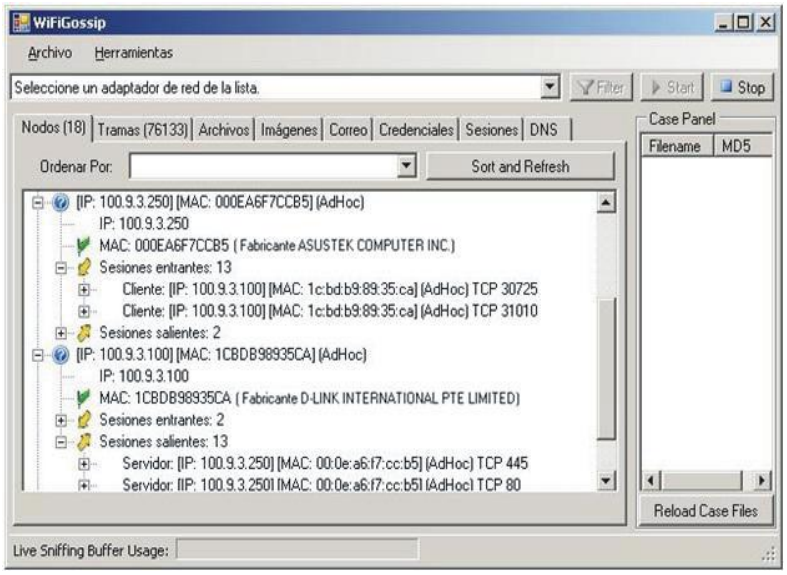

Figura 9. Escenario 1: Nodos inalámbricos mostrados en WifiGossip.

Esta prueba tiene como objetivo comprobar que la herramienta prototipo identifica los nodos participantes en la comunicación y su modo de trabajo.

En la Figura. 9 se muestra la captura realizada con WifiGossip. Se aprecia cómo han sido detectados los nodos y se ha identificado que se encuentran operando en modo ad hoc.

Escenario #2 Red de Infraestructura

Se realiza igualmente en interiores y está conformado por un host (estático durante el transcurso de la prueba) equipado con una tarjeta D-Link (MAC: 1CBDB98935CA) que se asocia al AP (BSSID/MAC: 001B2F353148) para conformar una red de infraestructura, y otro host que posee la tarjeta integrada NETGEAR (MAC: 001B2FCB895D) donde se monitoriza el tráfico y se visualiza con WifiGossip. Se analizan entonces los resultados obtenidos.

Figura 10. Escenario #2 Red de Infraestructura.

La prueba consiste en visualizar el proceso de establecimiento de la conexión entre el AP y la estación inalámbrica.

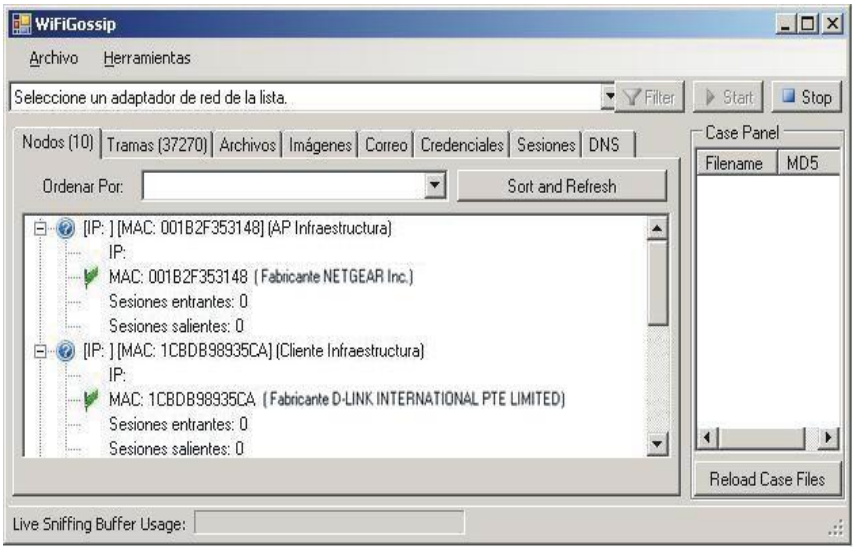

Figura 11. Escenario 2: Nodos inalámbricos mostrados con WifiGossip.

Se observa al igual que ocurre con el primer escenario, los nodos inalámbricos detectados e identificados por sus direcciones MAC y su modo de trabajo, que en este caso es infraestructura.

CONCLUSIONES

Con el objetivo de facilitar el trabajo de los administradores de la seguridad de las redes WLAN, las herramientas de monitorización y análisis de tráfico deben contar con un grupo de prestaciones que les posibiliten una mayor eficacia en sus tareas.

En el presente artículo se han propuesto un grupo de algoritmos de trabajo que posibilitan la identificación pasiva de los nodos inalámbricos y sus modos de trabajo. Estos basan su funcionamiento en el empleo de determinados campos dentro de las tramas 802.11, que permiten obtener información específica de cada nodo dentro de la red.

Estos algoritmos constituyen un importante aporte a la comprensión y el desarrollo de soluciones de supervisión de tráfico y dispositivos de las WLAN.

Se realizaron pruebas de campo empleando una herramienta a la cual se le implementaron dichos algoritmos, comprobándose que estos funcionaban correctamente.

Los próximos esfuerzos de trabajo se centran en la optimización del algoritmo general y la inclusión de métodos activos de detección en la herramienta prototipo.

REFERENCIAS

1. Society, I.C., 802.11 IEEE Standard for Information technologyTelecommunications and information exchange between systems Local and metropolitan area networksSpecific requirements.Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1999.

2. Gast, M.S., 802.11® Wireless Networks: The Definitive Guide. 2002: O´Reilly. 464.

3. Gast, M.S., 802.11® Wireless Networks: The Definitive Guide. 2002: O´Reilly. 464.

4. Chaiko, Y., Analytical Model of Connection Establishment Duration Calculation in Wireless Networks. 2008.

5. Hjelmvik, E., NetworkMiner. 2011 [cited 2012 17 de febrero]; Available from: http://www.netresec.com/?page=NetworkMiner.