REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 10. No. 3, septiembre-diciembre, 2011, p. 51-60 ISSN 1729-3804

Vulnerabilidades en el formato y uso de la trama 802.11

Keita Sory Fanta[1], Walter Baluja García[2]

[1] CUJAE, Estudiante de Maestría en Telemática, 9na. Edición, ksory2004@hotmail.com

[2] CUJAE, Doctor en Ciencias, walter@tesla.cujae.edu.cu

RESUMEN

La detección de intrusiones se basa en la monitorización de eventos en los sistemas de computadoras en busca de patrones conocidos de ataques o situaciones anómalas. Esta detección se lleva a cabo en redes cableadas e inalámbricas.

No obstante, los mecanismos de detección tanto en un tipo de redes como en las otras, no utilizan generalmente información de la capa de enlace.

En la línea de cubrir esta importante insuficiencia el presente artículo analiza las vulnerabilidades de la trama de la familia 802.11, a fin de considerar la necesidad y sentar las bases para disponer de algoritmos que detecten ataques realizados empleando dichos protocolos.

Palabras claves: 802.11, capa de enlace, detección de intrusiones, redes inalámbricas, seguridad.

Introducción

A pesar de las preocupaciones como la crisis económica mundial, la industria de las tecnologías inalámbricas disfruta de nuevos avances científico-técnicos, gracias a la satisfacción de sus usuarios en el tema de la movilidad e integración de los servicios en el ámbito de las telecomunicaciones. Eso se debe, entre otros, a los avances de la nano electrónica y la miniaturización de los circuitos integrados [1,2].
En el marco del desarrollo de esas tecnologías está la implementación de las redes inalámbricas, aparecidas en las últimas décadas como complemento de las cableadas en los lugares donde el cable es una limitante.
Conocida comúnmente como WLANs (Wireless Local Area Networks), las redes inalámbricas tienen múltiples aplicaciones. Suelen utilizarse conjuntamente con las redes cableadas como red de interconexión entre ellas, o en casos de emergencia debido a la congestión. También suelen usarse como alternativa en salones de reuniones eventuales donde no es imprescindible el cableado [2-5], o como servicio complementario en zonas urbanas (hoteles, cafés, tiendas, y otros).
La seguridad es un aspecto de vital relevancia al hablar de redes inalámbricas por el amplio despliegue que han alcanzado. Las WLANs, al igual que cualquier sistema de comunicaciones, representan importantes ventajas para los usuarios y los servicios pero sufren de problemas de seguridad debido a vulnerabilidades propias que las exponen [4, 6, 7].
Por ejemplo, para tener acceso a una red cableada es imprescindible una conexión física al cable, mientras que a una red inalámbrica se puede acceder sin ni siquiera estar ubicado en las dependencias de la organización donde está implementada dicha red [6].
El canal de las redes inalámbricas, al contrario que en las redes cableadas, debe considerarse inseguro. La escucha de la información transmitida (ataque pasivo) y la inyección de nuevos paquetes o la modificación de los ya existentes (ataques activos) obligan tener las mismas precauciones que se tienen para el envío de datos a través de Internet [4, 6].

Seguridad en 802.11

Conscientes de estos problemas de seguridad, varias publicaciones y normas sobre soluciones, métodos o mecanismos de protección han sido publicados por investigadores y expertos [6]:
• En 1999 surge el WEP (Wired Equivalet Privacy), basado en el mecanismo de encriptación RC4 para proteger la confidencialidad de la información. Este ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.
• En 2004 *5+ se aprobó la 802.11i como una nueva norma por parte de la IEEE (Institute of Electrical and Electronics Engineers), para dotar de suficiente protección a las redes WLANs, empleando varios mecanismos de seguridad.
• No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi decidió lanzar una solución de seguridad intermedia, hasta que estuviese disponible la 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados del desarrollo de la norma. El resultado, en 2003, fue el WPA (WiFi Protected Access), mucho más fuerte que WEP y que actualmente se emplea en su versión 2 [7].

Sin embargo, el desarrollo exponencial de herramientas de descubrimiento y diagnóstico de redes WiFi (Wireless Fidelity) (como Kishmet, NetStumber, Nessus, y demás) así como los mecanismos de capturas e inyección de tráfico en la red, hacen posible a intrusos capacitados romper muchos de estas soluciones si disponen del tiempo y del nivel de acceso necesario.

Adicionalmente, estudios realizados por investigadores y expertos en el campo de la seguridad recomiendan la implementación de mecanismos adicionales como la implementación de ACL (Access Control List), ocultamiento del SSID (Service Set Identification) de los APs (Access Point), entre otros, para esquivar la actividad de los intrusos [6].

Uno de los mecanismos que habitualmente es empleado con más éxito en las redes de datos son los detectores de intrusiones (IDS). Estas herramientas se basan en la monitorización de eventos en los sistemas de computadoras en busca de patrones conocidos de ataques o situaciones anómalas. Esta detección se lleva a cabo en redes cableadas e inalámbricas. Sin embargo, los IDS rara vez analizan la información que viaja en las tramas del nivel de enlace en las redes que protegen. En el presente artículo se abordará este tema para el caso de las redes inalámbricas pues a este nivel se presentan importantes vulnerabilidades y ataques.

Vulnerabilidades Asociadas a las tramas de control del 802.11

Además de las vulnerabilidades existentes en los protocolos implementados para la seguridad en redes WiFi, tales como las de los protocolos WEP, existen vulnerabilidades inherentes al formato y uso de las tramas MAC dependiendo del tipo de trama que se está analizando. Por ejemplo, existe la posibilidad de cambio o falsificación de las direcciones en las tramas de datos. Estas vulnerabilidades constituyen unas de las bases de las amenazas a las cuales están sometidas las WLANs.

En este artículo se hace énfasis en las vulnerabilidades asociadas a las tramas de gestión y de control de 802.11, a partir de las cuales se realizan importantes ataques de denegación de servicios (DoS).

Las figuras 1, 2 y 3 muestran el formato de los paquetes de control: RTS (Ready To Send), CTS (Clear To Send) y ACK (Acknowledgement) respectivamente. Se puede notar que en las tramas CTS y ACK no se incluye la dirección de la fuente, con el objetivo de minimizar el tamaño de esos paquetes y garantizar mayor velocidad, característica fundamental de las tramas de control [9].

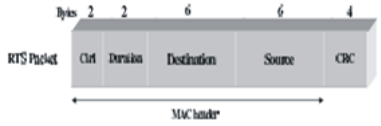

Figura 1. Trama RTS [9].

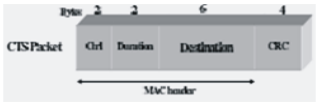

Figura 2. Trama CTS [9]

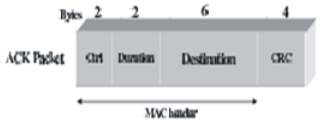

Figura 3. Trama ACK [9]

Cuando ocurre el mecanismo RTS/CTS entre un transmisor y un receptor (parte del protocolo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)), los nodos ubicados en el rango del transmisor se privan de todo tipo de transmisión al escuchar un paquete RTS en el medio y de la misma manera se comportan los nodos ubicados en el rango del receptor al escuchar el paquete CTS en el medio [9-11].

Al recibir el paquete CTS, el transmisor deduce que proviene del destinatario correspondiente y no verifica la dirección de origen del mismo.

De igual forma, como no se concibe en el protocolo 802.11 que dos nodos transmitan al mismo tiempo y por el mismo canal, un receptor transmite la trama ACK sin necesidad de una autenticación de la misma.

Un nodo malicioso puede aprovechar estas debilidades para producir ataques que no son identificados por los sistemas de seguridad implementados habitualmente [9].

Otro problema inherente a la ausencia de la dirección de fuente en los paquetes CTS es que el atacante puede generar paquetes CTS falsos tras la transmisión de un RTS (Ready To Send) con la intensión de bloquear la transmisión de los nodos (virtual jamming en inglés) existentes en su entorno.

También el intruso puede generar paquetes ACK falsos tras una transmisión sin éxito. La idea detrás de ese mecanismo es que cuando un nodo transmite un paquete cualquiera, espera la confirmación de recepción exitosa de dicho paquete (ACK), en el caso contrario (producto de una colisión o de paquetes recibidos con errores) no recibirá esa confirmación. En esta situación, y vencido un temporizador, se debe proceder a la retransmisión del paquete. El intruso es capaz de aprovechar esa situación generando paquetes ACK falsos para dar la impresión de recepciones exitosas y, por lo tanto, de que no hay problemas en la red, que los destinos están todos disponibles, entre otros [9].
Adicionalmente, también existen ataques que utilizan el Vector de Localización de Red (NAV), utilizado por el protocolo CSMA/CA. Este vector se inicializa con el campo Duración de la Cabecera MAC (tiempo estimado que debe estar el canal disponible para transmitir la trama). Existen 2 bytes después del campo FC (Frame Control) que representan esa duración. Es un valor de 16 bits, de tal forma que si el bit más significativo está en cero, el valor del resto de bits será el valor con el que se inicializa NAV. Es decir, NAV como mucho puede valer. Dicho de otra forma, el tiempo máximo que se puede reservar para la retransmisión de una trama es de 32.768 microsegundos [9, 12, 13].
Todas las estaciones de la red monitorizan las tramas y las cabeceras, de tal forma que durante la transmisión de una trama, los nodos leen la duración de la misma y añaden ese tiempo extra como tiempo de contención antes de enviar sus datos, el envío de cientos (o miles) de paquetes con duración de 32.768 μs se convierte en un ataque de denegación de servicios para toda la red.

Otras vulnerabilidades en las tramas del 802.11

Las tramas de administración en el estándar 802.11 no tienen protección criptográfica implementada. Los paquetes de manejo de la comunicación viajan en texto claro, posibilitando la obtención de la dirección MAC del AP o del nodo cliente por simple análisis del tráfico capturado por parte del intruso [14]. Luego se puede suplantar el AP legítimo con el uso de la falsificación de direcciones (MACSpoofing) y lanzar ataques de des-autenticación, de des-asociación u otros como los de agujero negro (blackhole).
Los ataques más importantes en las WLANs son los de denegación de servicio basado en congestionar el tráfico de usuario entre la estación móvil y el AP. El tráfico de usuario, los datos de señalización y los datos de control son obstruidos impidiendo con ello su transmisión en el canal de radio [7]. Otra manera de impedir que la información o los datos sean transmitidos es introducir paquetes de protocolos con problemas específicos [15, 16].

Ataques de CTS falsos: Mecanismo de creación de CTS falsos.
Los ataques DoS causados por paquetes CTS falsos consisten en transmitir paquetes CTS sin que se haya transmitido el paquete RTS correspondiente. En ese caso, los nodos que existen en el rango de transmisión del intruso retienen sus deseos de transmitir denegando así el acceso de los mismos a la red [9].
Para llegar a ello, el atacante usa un algoritmo muy sencillo que se explica a continuación [9].
< Chequear primero si el NAV es igual a cero y entonces ver el estado del canal:
• Si el canal está ocupado, espera un tiempo T=DIFS+Backoff
• En el caso contrario, crea el CTS falso a una dirección destino falsa, iniciando así el ataque.

En la figura siguiente se muestra el diagrama de flujo del ataque.

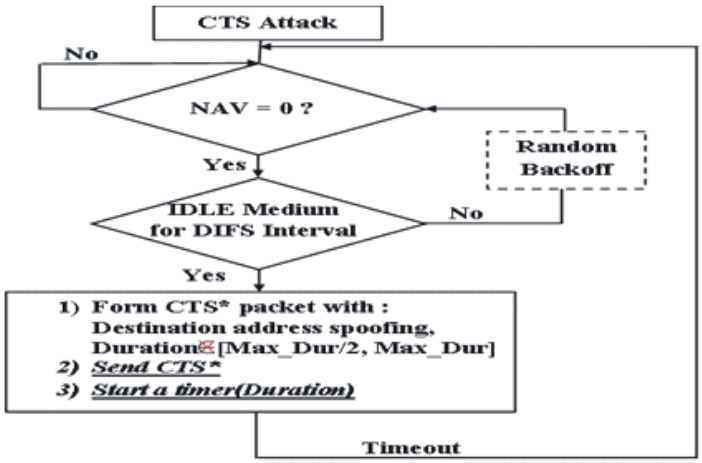

Figura 5. Diagrama de flujo del ataque CTS [9]

Ataque de ACK falsos: Mecanismo de creación de ACK falsos.

La idea consiste en confirmar la recepción de los paquetes enviados por un nodo transmisor a un nodo receptor cuando realmente esos paquetes no fueron recibidos. El transmisor no retransmitirá esos paquetes ya que recibió una confirmación de recepción (ACK falsos) denegando así el servicio [9].

Suponiendo que A y B son los nodos transmisor y receptor respectivamente, y que M es un nodo malicioso, el mecanismo de ACK falsos consiste en lo siguiente:

El nodo M primero necesita saber el NAV_{RTS} o el NAV_{CTS} y también las direcciones de los nodos A y B.

De acuerdo a los valores de NAV_{RTS} o NAV_{CTS} el nodo M puede determinar un tiempo T_{coll} (Tiempo de colisión) al cual inicia el ataque. Este último consiste en dos partes esenciales:

Primero, el atacante envía un paquete al nodo B al tiempo T_{coll} con la intención de colisionar al nodo B. Ese tiempo está definido por un valor aleatorio en el intervalo [$B_{\min}$, $B_{\max}$] donde [9]:

$$\begin{cases} B_{\min} = \dfrac{NAV_{CTS} - T_{ACK} + SIFS}{2} \\ B_{\max} = NAV_{CTS} - (T_{ACK} + SIFS + T_{JAM}) \end{cases} \quad \text{Ec 1}$$

Donde :

T_{JAM} Es el tiempo de propagación del paquete que causará la colisión en el nodo B.

es Short InterFrame Spacing. Tiempo intertrama.

Segundo, el atacante manda el ACK falso hacia el nodo A al tiempo $T_{validate}$ tal que:

$$T_{validate} = NAV_{CTS} - T_{ACK} - SIFS \quad \text{Ec 2}$$

Cuando el nodo A recibe el paquete ACK después de un tiempo T_{out}, no se da cuenta de la anomalía causada por ese paquete (ACK falso). T_{out} Es el tiempo máximo entre el tiempo donde el nodo A inició su transmisión de datos y la recepción del paquete ACK:

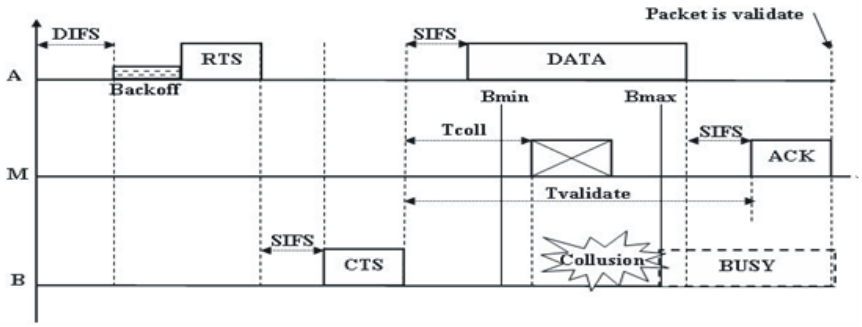

Figura 6. Mecanismo de creación del ACK falso [9].

$$T_{out} = T_{DATA} + MPD + SIFS + T_{ACK} + MPD \quad \text{Ec 3}$$

Donde:
MPD es el máximo retardo causado por la propagación.

El atacante debe velar por los tiempos $T_{validate}$ y T_{out} de tal modo que $T_{validate} < T_{out}$ sino el nodo transmisor puede detectar el problema y retransmitirá el paquete.

Cuando el atacante escucha el paquete RTS, determina entonces las direcciones de los nodos transmisor y receptor, y espera por el paquete CTS durante un tiempo T_1

T_1 Está definido por el tiempo SIFS, el tiempo de propagación del paquete CTS () y por el retardo máximo de propagación MPD:

$$T_1 = SIFS + T_{CTS} + MPD \quad \text{Ec 4}$$

Después de haber escuchado el paquete CTS al tiempo T_1 , el atacante selecciona el tiempo T_{coll} y $T_{validate}$, y arranca los temporizadores correspondientes. En el caso contrario, repite el algoritmo del ataque.

Cuando escucha CTS a T_1, vela por el temporizador T_{coll} . Al agotar ese temporizador, el atacante envía el paquete al nodo B con la intensión de crear la colisión. Entonces vela por el temporizador $T_{validate}$ y cuando se agota ese último, envía el paquete ACK falso al nodo A para validar el paquete de datos transmitido. A continuación se presenta en la figura 7 el diagrama de flujo de ese algoritmo.

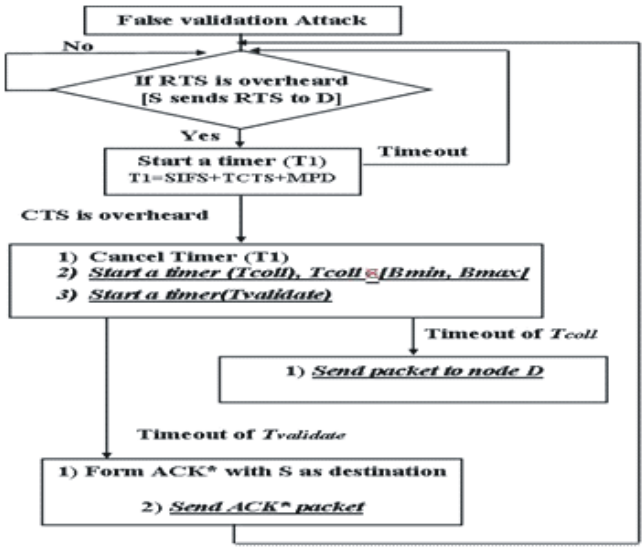

Figura 7. Diagrama de flujo del algoritmo de creación del ACK falso [9].

Ataque de duración.

En el ataque de duración, el atacante envía una trama con el campo NAV fijado a su valor máximo (32 ms). Esto evita que cualquier estación utilice el medio compartido antes que el tiempo NAV llegue a cero. Antes de la expiración del contador, el atacante envía otra trama con iguales características. Repitiendo este proceso, el atacante puede denegar acceso a la red inalámbrica [17, 18].

Ataques de des-autenticación y de des-asociación.

En estos ataques, el atacante falsifica una trama de des-autenticación o de des-asociación, como si ésta fuera originada desde el punto de acceso. Al recibirla, la estación se desconecta y trata de reconectarse nuevamente a la estación base. Este proceso es repetido indefinidamente para mantener a la estación desconectada de la estación base. El atacante puede también asignar a la dirección de recepción la dirección de difusión, de esta forma puede atacar a todas las estaciones asociadas con la estación base víctima. Este ataque es posible gracias a la suplantación de identidad del AP por falsificación de la dirección MAC del mismo (MACSpoofing). No obstante, se ha comprobado que algunas tarjetas de red inalámbricas ignoran este tipo de tramas de des-autenticación [18, 19].

Ataques Hombre en el Medio

También conocido como "Mono en medio", se utiliza la variante M-I-M para suplantar el AP. El intruso tiene que convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.
De esta forma toda la información que determinados clientes envían y reciben siempre pasa por el nodo del intruso. Este es un ataque muy común en lugares públicos donde la conexión inalámbrica es un servicio agregado (cafés, tiendas, entre otros).

Trabajos relacionados

Varios artículos y trabajos han sido publicados sobre los problemas de vulnerabilidades en la trama 802.11 y la no existencia de técnicas IDS a ese nivel. Adicionalmente, los esfuerzos de muchas investigaciones han quedado mayoritariamente comprendidos en cuatro categorías: enrutamiento seguro, credibilidad y gestión de llaves, protección de la disponibilidad del servicio, y detección de intrusiones. La detección de intrusiones es sugerida como un mecanismo complementario cuando los otros mecanismos de seguridad han fracasado y el atacante ha conseguido el acceso a la red [20].
En [9], se reportan ataques que resultan de las vulnerabilidades a las cuales están expuestas los paquetes de control de las tramas 802.11. En [18], se propone un algoritmo para la selección de campos de utilidad a fin de contrarrestar posibles debilidades de los mismos. En [21], se explica el uso de la programación genética en la implementación de WIDS para la solución de ataques de tipos DoS en redes 802.11. En [22], se materializa el uso y las importancias de las redes neuronales en la implementación de los sistemas de detección de intrusiones.

Trabajo futuro

Se trabaja en el diseño e implementación de algoritmos que permitan la detección de varios de los ataques aquí descritos. Resulta prácticamente inexistente la defensa ante los ataques que utilizan las tramas de control y gestión de las conexiones entre los nodos inalámbricos como los ataques CTS, RTS, ACK, des-autenticación y otros.

CONCLUSIONES

Existen varios ataques importantes que explotan las debilidades existentes en el formato y uso de las tramas 802.11. Como consecuencia de estos ataques puede afectarse seriamente la disponibilidad de los servicios inalámbricos de una red, pues los mecanismos de seguridad tradicionales, como los IDS, normalmente no detectan o impiden el éxito de esta actividad intrusiva.

Resulta necesaria la adopción rápida de soluciones de seguridad. En ese ámbito y de acuerdo a lo analizado anteriormente, la obtención de soluciones alternativas de detección de intrusiones para los protocolos de la capa de enlace sería sin duda una de los avances más convenientes.

Actualmente se trabaja en la obtención de algoritmos de detección para la capa de enlace de WiFi, como parte de la solución de los problemas de inseguridad de las redes inalámbricas.

REFERENCIAS

1. Timothy R. Schmoyer, Y.X.L.a.H.L.O. (2004) Wireless Intrusion Detection and Response.

2. Anabel F, Castillo Mora, R.F.C.C., Consultorías para la determinación de brechas de seguridad de una red inalámbrica. 2006, Escuela Superior Politécnico del Litoral: Guayaquil, Ecuador. p. 247.

3. Carlos Varela, L.D. (2002) Redes Inalámbricas. 18.

4. Juan P. Asturias Sueira, J.R.E.A., Sistema de ubicación geográfica de una terminal de una red WiFi. 2004, Francisco Marroquin: Guatemala. p. 62.

5. Lorente, O.S., Implementación de un modelo de canal inalámbrico para redes 802.11 bajo el simulador ns-2 2005, Politécnica de Catalunya: Catalunya. p. 70.

6. Cruz, F.L.C.d.l., "Fuerzas armadas de la region andina en el contexto de la seguridad cibernetica, en concordancia con la resolución de la O.E.A. AG/RES. 2004 (XXXIV-O/04)". 2004, Del Salvador Buenos Aires,Argentina.

7. Perez, J.W., Análisis de la Seguridad en las Redes WiFi, en Telecomunicaciones y Telematica. 2009, ISPJAE-CUJAE: Habana. p. 114.

8. Alcatel-Lucent, W.A.D., Transformación de la seguridad IP de extremo a extremo en los entornos corporativos. Octubre 2007.

9. Abderrezak Rachedi , A.B. (2008) Smart Attacks based on Control PacketsVulnerabilities with IEEE 802.11 MAC. 6.