"Ataques de denegación de servicio en redes Wireless"

por Gabriel Verdejo Alvarez, revisado el 29 de Mayo de 2004.

1. Introducción

Después del gran auge de Internet en los años noventa y tras la expansión de los teléfonos móviles en el nuevo milenio, las redes sin hilos o *wireless* se han convertido en la perita en dulce de las comunicaciones.

El abaratamiento de costes de conexión, la mejora de la tecnología y la expansión de Internet mediante cables (xDSL, PLC…) ha llevado a una conexión generalizada de los hogares y empresas a Internet [WWW1]. Sin embargo el problema de extender esta conectividad dentro del hogar o en las distintas plantas de una fábrica mediante complicados cableados persistía de forma inamovible.

La consolidación de la telefonía móvil ha obligado al rápido avance de las tecnologías sin hilos que se han visto aún más potenciadas por el gran aumento de ventas de ordenadores portátiles y sistemas personales o PDA. Si dispongo de una batería que me permite moverme por mi casa/empresa/universidad, ¿Por qué debo permanecer conectado a un cable para acceder a Internet?

2. La tecnología Wireless

Actualmente podemos encontrar varias especificaciones de conexiones a redes sin hilos que se agrupan en el estándar 802.11 de IEEE [WWW2], también referenciado en la bibliografía como 802.11x [KM03]. Esta especificación se subdivide en varias categorías según la velocidad de transferencia que proporcionan y la frecuencia de radio que utilizan para sus transmisiones.

802.11a [Bow02][Gei02]: Esta tecnología usada principalmente en Estados Unidos y Japón proporciona conectividad desde 11 a 54Mbps en la frecuencia de los 5Ghz. El alcance es de unos 100 metros.

802.11b [WWW6]: Denominada también Wi-Fi se utiliza principalmente en Europa y proporciona conectividad de hasta 11Mbps utilizando una frecuencia de 2.4Ghz. El alcance es de 100 metros.

802.11g [KM03]: Denominada también Wi-Fi 2.0 se usa en Europa y proporciona conectividad de hasta 54Mbps utilizando una frecuencia de 2.4Ghz. El alcance es de unos 100 metros.

El esquema básico de este tipo de redes (ver figura 1-1) se basa en la existencia de un punto de acceso (*access point*) conectado a la red de cable. Este dispositivo proporciona acceso sin hilos a los posibles clientes mediante unas antenas de radio (obviamente cualquiera que reciba esta señal puede interaccionar con ella).

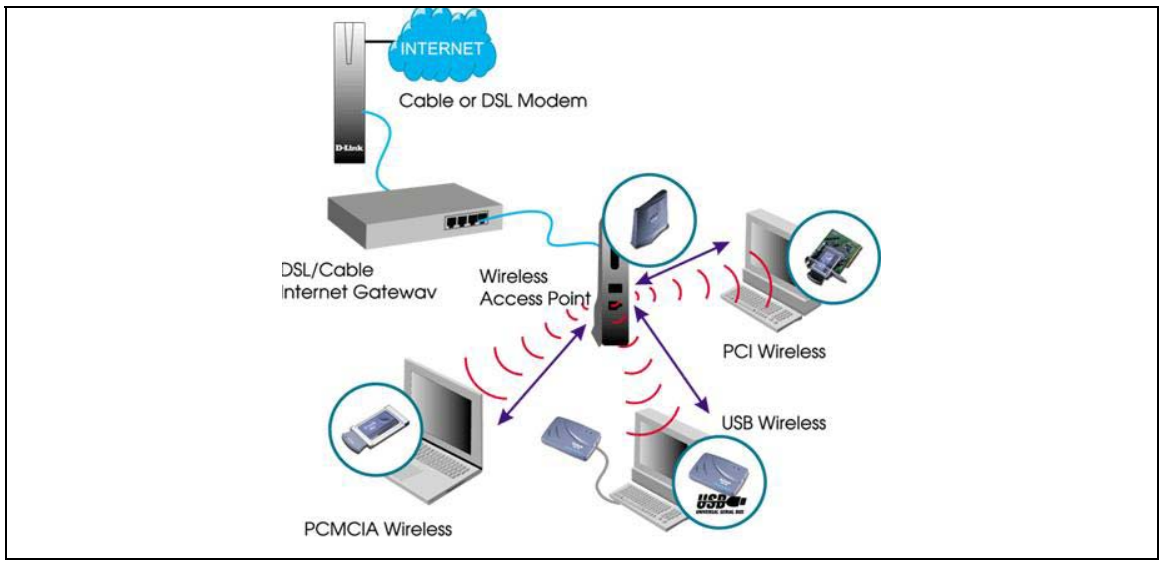

Fig. 1-1: Esquema de una red sin hilos.

Al igual que pasa con los conectores de los enchufes entre los distintos países, la diferencia entre las bandas radioeléctricas utilizadas en USA y Europa es debida a que cada país asigna su espacio de frecuencias para los distintos usos según su propio criterio. En Europa la banda de 5Ghz está destinada a las comunicaciones militares y hasta hace pocos meses en España era ilegal su uso.

Destacar que Mbps (Mega bits per second) [WWW7] hace referencia al número de bits que circulan por segundo, de esta forma como un byte son ocho bits debemos dividir entre 8 para obtener el rendimiento máximo real. Obviamente esto hace referencia al máximo teórico y dista mucho del rendimiento real obtenido, por otro lado cada edificio/espacio es distinto. Para ver comparativas puedes consultar [Gei04][Fli01].

3. Ataques DOS en redes Wireless

Las redes sin hilos, al igual que cualquier transmisión de tipo radio-eléctrico como la televisión, se pueden ver afectadas por interferencias o ruido que puede empeorar la calidad de la señal.

En el caso de la televisión esto puede visualizarse como una imagen borrosa o problemas con el sonido. Sin embargo nosotros continuamos recibiendo algún tipo de imagen y sonido, dependiendo del grado de interferencia, que puede permitirnos con mayor o menor comodidad seguir viendo la televisión hasta que arreglemos la antena o cesen las interferencias.

En el caso de las redes wireless lo que se realiza son transferencias de paquetes de información. Cada paquete contiene entre otros datos las direcciones de origen y destino, número de paquete dentro de la secuencia de transmisión, la información a transferir y un valor de comprobación de la integridad del paquete (CRC) para asegurar que no han existido errores en la transmisión.

De esta forma a diferencia de la televisión o la radio no podemos "perder" o recibir un paquete de información erróneo y continuar tranquilamente. Este paquete debe ser retransmitido hasta que llegue de forma correcta y en la secuencia o posición adecuada (ver figura 1-2).

El ataque más obvio a las redes sin hilos consiste en la emisión de ruido de forma que consigamos degradar los paquetes de datos transmitidos de forma que se vuelva prácticamente imposible la comunicación. De hecho, si el atacante logra un simple cambio en un bit del paquete de datos, el CRC lo detectará y se deberá retransmitir.

- Utilizaremos como ejemplo la transmisión de un fichero .pdf que contiene el texto "**Ataques DOS en redes Wireless. Por Gabriel Verdejo Alvarez**".

- Como hemos indicado las transmisiones en las redes sin hilos se efectúan en bloques o paquetes de información. En nuestro caso obtenemos 4 paquetes a transmitir ordenados según la secuencia 1,2, 3 y 4.

"Ataques DOS"	*" en redes Wirel"*	*"ess. Por Gabriel"*	*"Verdejo Alvarez."*
Bloque1	Bloque2	Bloque3	Bloque4

```
While (1)
      {
         Sub_bloque = Obtener_bloque_de_Datos();

         While (  calcular_crc(Sub_bloque) != OK)          ⇐ ATAQUE DOS
                  Sub_bloque = Obtener_bloque_de_Datos();

         Reconstruir_secuencia_sub_bloques(datos_originales, Sub_bloque);
      }
```

Fig. 1-2: Ejemplo de transmisión de datos en redes sin hilos.

Las redes wireless implementan mecanismos de modulado de la señal como el **FHSS** (*Frecuency Hop Spread Spectrum*) [Gar03] para minimizar el impacto de esta técnicas de ataque limitando su efectividad al rango adyacente al atacante.

Esta técnica se basa en variar las frecuencias de transmisión continuamente de forma que el atacante deba ir modificando también su frecuencia de emisión. Como esta ya no es siempre la misma los ataques indiscriminados basados en la "inyección" de ruido al canal dejan de ser tan efectivos y permiten mantener el servicio.

El uso de técnicas correctoras de errores en lugar de simples comprobaciones (CRC) de la integridad de los datos minimizaría aún más el impacto de este tipo de ataques de denegación de servicio basados en la "fuerza bruta".

3.1 La nueva vulnerabilidad publicada en AusCert (AA-2004.02)

La nueva vulnerabilidad encontrada este mes de mayo en el protocolo 802.11 [Gra04][Ros04][WWW10] permite la denegación de servicio en la mayoría de redes wireless actuales con una simple PDA o un ordenador portátil.

La vulnerabilidad se encuentra en la capa **MAC** (*Medium Access Control*) de la especificación 802.11. Al igual que pasa en las redes Ethernet las redes sin hilos utilizan un mecanismo denominado CSMA/CA (*Carrier Sense Multiple Access/with Collision Avoidance*) para el control de acceso al medio.

La idea subyacente es que dado que todos los dispositivos wireless de una misma red comparten el mismo canal, sólo uno de ellos puede estar transmitiendo a la vez. Una analogía seria un turno de preguntas y respuestas en una conferencia. Si disponemos de un solo micrófono solamente una persona puede acceder simultáneamente a preguntar.

Sin embargo al igual que sucede en la conferencia anterior, la respuesta es oída por todos los presentes. En el caso de las redes sin hilos cada dispositivo escucha el canal hasta que lo encuentra libre. Una vez que está disponible el dispositivo transmite la información deseada, de ahí el nombre de CSMA.

Podría llegar a pasar que dos o más dispositivos escucharan a la vez y creyeran que el canal está libre. De esta forma ambos transmitirían a la vez creando una interferencia o colisión múltiple que eliminaría ambos mensajes, de ahí la parte CA. En este caso los dispositivos implicados paran de transmitir y esperan un tiempo aleatorio antes de repetir todo el proceso de nuevo.

Para minimizar la posibilidad de colisiones en estas redes se utiliza un mecanismo denominado CCA (*Clear Channel Assessment*) [WWW13][WWW14] que se implementa físicamente en los dispositivos y que consiste en ir comprobando la señal recibida para determinar el momento en que el canal está libre y puede ser utilizarlo.

El ataque "simplemente" consiste falsear este mecanismo de forma que todos los dispositivos que utilicen el CCA crean que siempre está ocupado. Como no se produce transmisión hasta que el canal esté libre, tenemos que mientras el atacante permanezca transmitiendo en su ámbito de cobertura la red sin hilos queda inutilizada totalmente (ver figura 1-3).

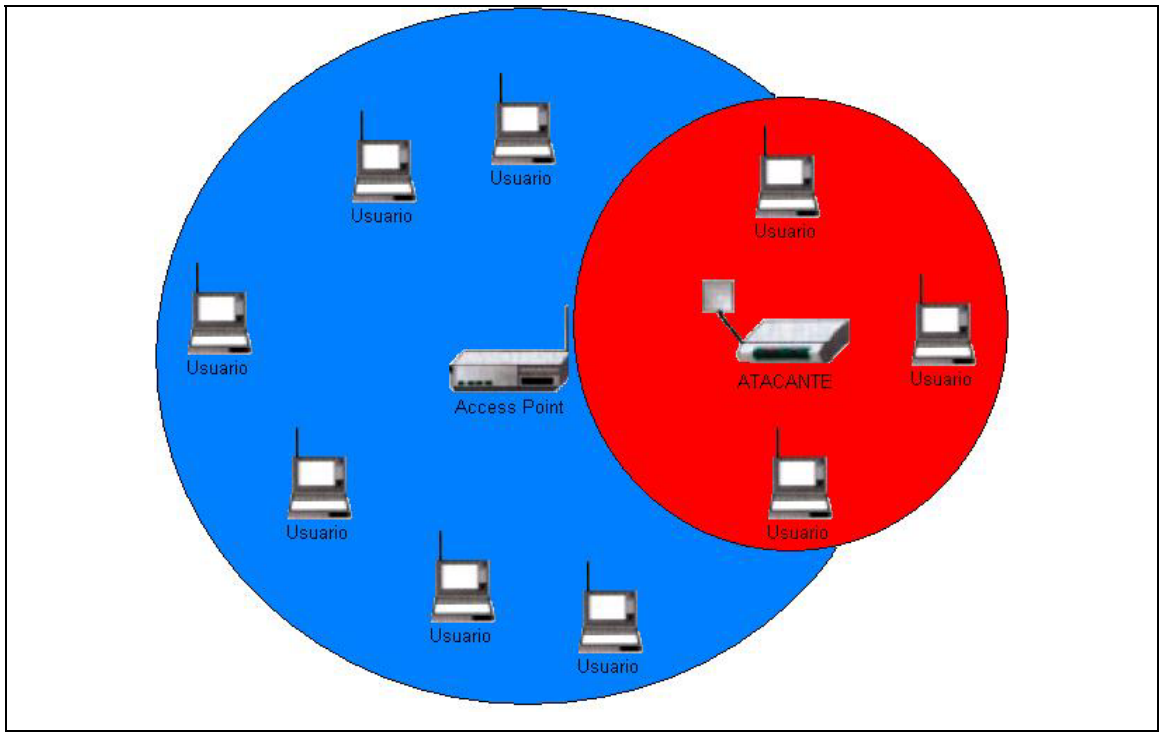

Fig. 1-3: Esquema de una red sin hilos.

El peligro de este ataque se basa principalmente en dos aspectos fundamentales:

1. Cualquier dispositivo wireless puede realizar este ataque sin necesidad de complejas modificaciones o programas específicos.

2. Debido a que esta vulnerabilidad ataca la base del propio protocolo 802.11 implementado en el hardware de los dispositivos, no hay posibilidad de mitigarlo o parchearlo en los sistemas vulnerables. Por otro lado el uso de técnicas de cifrado o seguridad complementarias no sirven para minimizar o eliminar este tipo de ataques.

Cabe destacar finalmente que este ataque tan sólo persiste en tanto que el atacante continúa transmitiendo. Los dispositivos afectados son todos aquellos que implementan 802.11b y 802.11g en modo de transmisión inferior a 22Mbps. Los que implementan 802.11a y 802.11g en modo 54Mbps no están afectados por esta vulnerabilidad.

BIBLIOGRAFÍA

[WWW1] http://www.noticias3d.com/articulos/200306/plc/1.asp
[WWW2] http://www.ieee.org/
[WWW3] http://standards.ieee.org/announcements/80211gfinal.html
[WWW4] http://www.nwfusion.com/reviews/2002/0617bg1.html
[WWW5] http://www.microsoft.com/windowsxp/expertzone/columns/bowman/02july29.asp
[WWW6] http://www.homenethelp.com/802.11b/index.asp
[WWW7] http://www.homenethelp.com/web/explain/about-network-speeds.asp
[WWW8] http://www.oreillynet.com/pub/a/wireless/2001/05/03/longshot.html
[WWW9] http://www.wi-fiplanet.com/tutorials/article.php/3337861
[WWW10] http://www.auscert.org.au/render.html?it=4091
[WWW11] http://www.securityfocus.com/news/8575
[WWW12] http://www.infoworld.com/article/04/05/13/HNwifi_1.html
[WWW13] http://www.wlana.org/learn/80211a.htm
[WWW14]http://www.mpirical.com/companion/mpirical_companion.html#http://www.mpirical.com/companion/IP/CCA_-_Clear_Channel_Assessment.htm
[WWW15] http://kaslab.sinroot.net/jornadas/actividades.html

[Fli01] Rob Flickenger, "***A wireless long shot***", [WWW8], 2001.
[Bow02] Barb Bowman, "***802.11a wireless Networking***", [WWW5], Microsoft 2002.
[Gei02] Jim Geier, "***802.11a becomes a contender***", [WWW4], 2002.
[Gar03] Pablo Garazlar Sagarminaga, "***Ataques de denegación de servicio en redes inalámbricas (Wi-Fi)***", [WWW15], 2003.
[KM03] Stuart J. Kerry, Karen McCabe "***Popular wireless local area networks gain large boost in speed***", [WWW3], IEEE 2003.
[Gei04] Jim Geier, "***802.11a vs 80211g in homes***", [WWW9], 2004.
[Gra04] Patrick Gray, "***New flaw takes WiFi off the air***", [WWW11], 2004.
[Ros04] Sandra Rossi, "***Critical 802.11 wireless flaw identified***", [WWW12], 2004.