Capítulo 3

Protocolo WEP (*Wired Equivalent Privacy*)

El algoritmo WEP es el estándar opcional de seguridad utilizado en redes inalámbricas 802.11b y 802.11a. El WEP está implementado en la capa de control de acceso al medio (MAC, *Media Access Control*). En general, esta capa administra y mantiene la comunicación entre los nodos de una red coordinando el acceso a una canal y utilizando protocolos que mejoren las comunicaciones sobre el medio inalámbrico.

El algoritmo WEP protege las comunicaciones inalámbricas contra ataques de intrusos y previene de acceso no autorizado a una red inalámbrica. El WEP fue diseñado para proveer autenticación de usuarios, privacidad de datos e integridad de datos en una forma equivalente a una red cableada LAN [JAG04]. En las siguientes secciones se explica cada uno de estos componentes y cómo se aplican al protocolo WEP para encriptar y decriptar la información en redes IEEE 802.11.

3.1 Componentes del WEP

El WEP consta de cuatro componentes esenciales para su funcionamiento: una llave secreta, un vector de inicialización, el algoritmo RC4 y el CRC-32 o Código de Redundancia Cíclica de 32 bits.

3.1.1 Llave secreta

La mayoría de los puntos de acceso utilizados en redes IEEE 802.11 utilizan llaves secretas estáticas que comparten con los usuarios de la red para iniciar una transmisión

de datos. Estas llaves se utilizan para encriptar información con el algoritmo RC4. Generalmente una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado [HSI04].

Esta llave normalmente es de 40 bits aunque existen implementaciones que usan llaves de 104 bits con el fin de ofrecer un nivel mayor de seguridad [BOR05], aunque como se verá más adelante en este capítulo, el hecho de incrementar el tamaño de la llave compartida no es suficiente para garantizar privacidad de la información.

3.1.2 Vector de inicialización

El WEP utiliza la llave compartida para generar una secuencia de llaves a través del RC4, que servirá para encriptar la información. Para evitar encriptar todos los paquetes con la misma secuencia de llaves, se utiliza un vector de inicialización (IV) de 24 bits que minimiza la probabilidad de alimentar el RC4 con las mismas entradas.

Así, la entrada que alimenta al RC4 se compone de 64 o 128 bits en total, conformados por 40 o 104 bits respectivamente de la llave compartida y 24 bits del IV. Algunos sistemas asignan al vector de inicialización el valor de 0 al inicio de la transmisión, y aumentan este valor unitariamente por cada paquete transmitido. Después de que se alcanzan los 16 millones de paquetes enviados, el valor del IV regresa a 0. Otros sistemas eligen el valor del IV aleatoriamente, pero existe la posibilidad de reutilizar el valor después de haber transmitido alrededor de 5000 paquetes [BOR05].

3.1.3 Algoritmo RC4

RC4 es el algoritmo de cifrado de flujo más usado en la actualidad. Fue creado por Ron Rivest en 1987 y se mantuvo en secreto hasta que se hizo público en 1994. Los cifrados de flujo funcionan expandiendo una llave o cadena de bits, en una clave arbitrariamente larga de bits pseudo aleatorios [FLU01]. En el caso del WEP, la llave se forma por el vector de inicialización y la llave secreta compartida. Estas llaves alimentan al algoritmo RC4 para generar la secuencia de llaves utilizada para encriptar y decriptar información.

3.1.4 Código de Redundancia Cíclica

Una manera de asegurar que la información enviada en forma electrónica por una red no ha sido modificada, es utilizando las sumas de verificación (*checksums)*. Un procedimiento simple de suma de verificación puede utilizarse para calcular el valor de un archivo y después compararlo con su valor previo. Si las sumas de verificación son iguales, el archivo no ha sufrido cambios. Si las sumas no son iguales, el archivo habrá sido alterado [SIY95]. En el caso de redes inalámbricas, en lugar de calcular el valor de un archivo, se calcula el valor de una cadena de bits correspondiente a un mensaje transmitido.

Para calcular las sumas de verificación se utilizan códigos de redundancia cíclica (CRC) también llamados códigos polinómicos. Los CRC son muy utilizados en la práctica para la detección de errores en largas secuencias de datos.

Estos códigos se basan en el uso de un polinomio generador *G(X)* de grado *r*, y en el principio de que *n* bits de datos binarios se pueden considerar como los

coeficientes de un polinomio de orden *n-1*. Por ejemplo, los datos 10111 pueden tratarse como el polinomio $x^4 + x^2 + x^1 + x^0$.

A estos bits de datos se le añaden *r* bits de redundancia de forma que el polinomio resultante sea divisible por el polinomio generador, sin generar un residuo. El receptor verificará si el polinomio recibido es divisible por *G(X)*. Si no lo es, habrá un error en la transmisión [COD06].

El WEP utiliza el CRC32, que se refiere al polinomio generador utilizado para verificar la integridad de la información [CRC06]:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \qquad (3.1)$$

En el WEP, la suma de verificación resultante después de aplicar el CRC32 sobre el texto plano, se conoce como ICV (*Integrity Check Value*). Este valor se utiliza en los procesos de encriptación y decriptación del WEP como se verá más adelante.

3.2 Funcionamiento del WEP.

Para llevar a cabo los procesos de encriptación y decriptación de información, el WEP utiliza los cuatro componentes mencionados en la sección anterior. Estos procesos se describen en las sub-secciones siguientes.

3.2.1 Proceso de encriptación del WEP.

El proceso de encriptación del WEP se realiza para cada paquete transmitido y se describe en los pasos siguientes (ver Figura 3.1) [BOR05]:

1) El transmisor calcula el ICV (valor de 4 bits) usando el CRC 32 sobre el mensaje a transmitir y lo concatena al mismo.
2) El transmisor elige el IV y lo concatena a la llave compartida.
3) El IV y la llave secreta compartida alimentan al RC4 que funciona como Generador de Números Pseudo Aleatorios (PRNG), para generar una secuencia de llaves.
4) El transmisor encripta el mensaje original haciendo la operación XOR entre éste y la secuencia generada en el paso anterior.
5) El transmisor envía el vector de inicialización seguido por el mensaje encriptado.

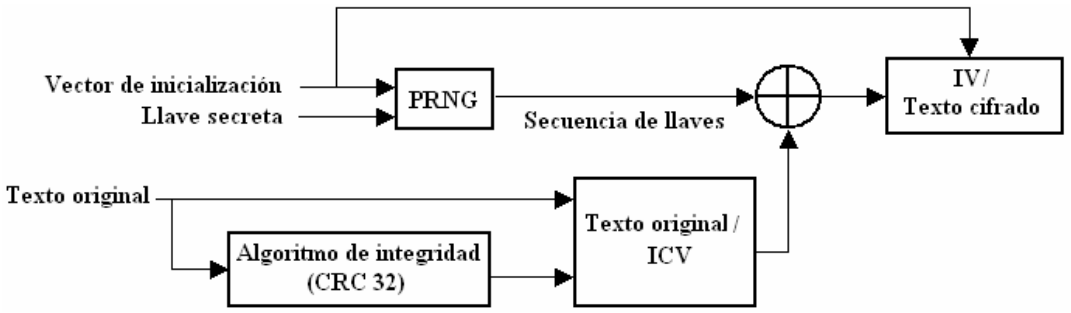

Figura 3.1 Diagrama bloques del proceso de encriptación del WEP [BOR05]

El texto cifrado y el IV viajan por el enlace inalámbrico hacia el receptor, el cual deberá decriptar la información. Es importante notar que el vector de inicialización se envía sin ningún tipo de encriptación, lo cual es una de las principales causas de las debilidades del WEP presentadas más adelante en este capítulo.

En la Figura 3.2 se muestra la trama completa enviada de transmisor a receptor distinguiendo la parte encriptada que consiste de los datos y el ICV calculado por el

CRC32, del encabezado MAC de la trama y el vector de inicialización que no están encriptados.

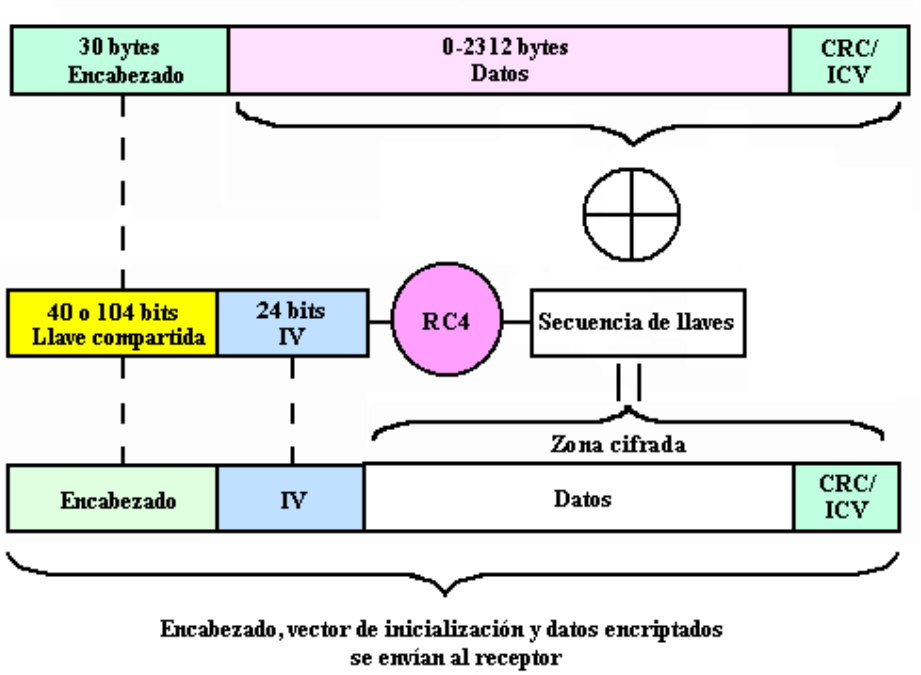

Figura 3.2. Parte encriptada de la trama 802.11.

3.2.2 Proceso de decriptación del WEP.

Al igual que en la encriptación, la decriptación en el receptor se realiza para cada trama 802.11, este proceso se describe en los pasos siguientes (ver Figura 3.3) [BOR05]:

1) El receptor utiliza el IV enviado por el transmisor y la llave secreta compartida para generar una secuencia de llaves con el algoritmo RC4.
2) El receptor realiza la operación XOR entre la secuencia de llaves y el texto cifrado recibido para calcular el texto original y el ICV.
3) Con el CRC-32 se calcula el valor ICV del texto original ya obtenido.
4) Si los valores ICV son iguales, acepta el mensaje; de otra forma lo rechaza.

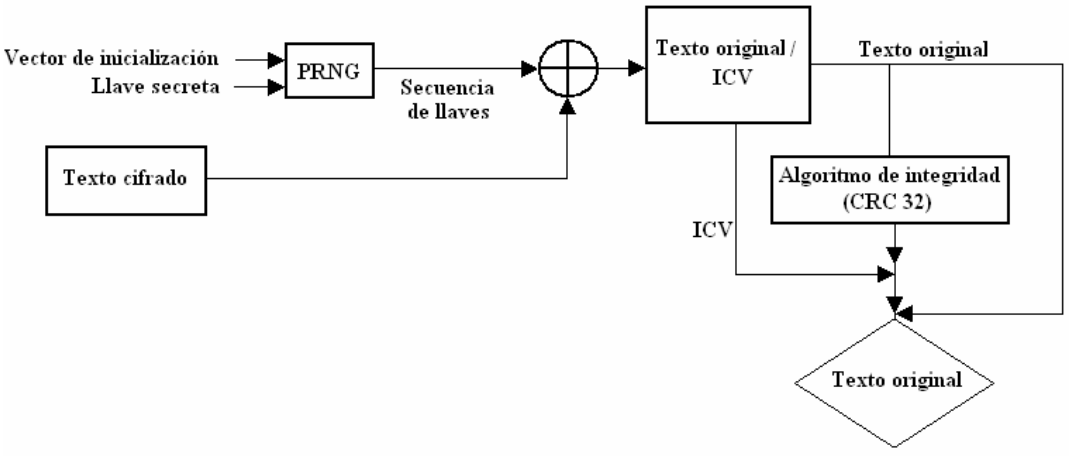

Figura 3.3 Diagrama bloques del proceso de decriptación del WEP [BOR05]

Como se ve en la Figura 3.2, el encabezado MAC de la trama y el vector de inicialización no están encriptados porque lo que el proceso de decriptación del WEP mostrado en la Figura 3.3 se aplica únicamente al campo de datos y CRC (datos cifrados) de la trama 802.11.

3.3 Debilidades del WEP.

Se consideran debilidades aquellas características del WEP que lo hacen un protocolo vulnerable contra ataques a sus mecanismos de seguridad. Estos ataques pueden violar las características de privacidad, autenticidad e integridad de la información. A continuación se mencionan las debilidades más importantes.

- El algoritmo RC4 es susceptible a ataques de fuerza bruta (ver sección 3.4).
- Manejo de las llaves y tamaño de la llave.

  El manejo de las llaves no está especificado en el WEP. Sin un manejo de llaves, estas permanecen útiles durante mucho tiempo. La mayoría de los usuarios del WEP tienen una sola llave compartida con cada nodo de la red. El punto de

acceso y los clientes deben estar programados con la misma llave. Sincronizar el cambio de llaves es difícil y tedioso. El tamaño de la llave es de 40 bits. El estándar 802.11 no especifica otro tamaño de llave más que de 40 bits. Algunos fabricantes han extendido el tamaño de la llave a 104 bits, que es más resistente a ataques de fuerza bruta [BOR05].

- El vector de inicialización es muy pequeño.

  El IV del WEP es de 24 bits. Así, puede generar 16,777,216 secuencias de llaves diferentes a través del RC4 para una llave compartida dada de cualquier tamaño.

  Si una secuencia de llaves generada con un IV dado, es obtenida por un atacante, éste puede decriptar paquetes que hayan sido encriptados con el mismo vector de inicialización. De esta forma el atacante no necesita saber la llave compartida secreta, puesto que ya conoce la secuencia de llaves [BOR05].

- El CRC32 no es apropiado.

  Desafortunadamente, el CRC-32 no provee integridad absoluta contra posibles ataques, aún cuando los datos y el CRC estén protegidos por la encriptación del WEP. El CRC-32 es una función lineal de los datos. El WEP encripta al hacer la operación XOR entre la secuencia de llaves y los datos, y el XOR es también un operador lineal. Así, un atacante que obtenga un mensaje encriptado por el WEP, puede fácilmente cambiar las posiciones de los bits a su elección, y puede ajustar el código CRC-32 del mensaje para hacerlo concordar con el mensaje modificado. Esto se puede hacer a través de la encriptación RC4, al hacer el XOR con las cadenas de bits calculadas [WOO03].

3.4 Tipos de ataques al WEP.

A continuación se mencionan las diferentes formas de atacar al protocolo WEP [BOR05]:

a) Ataque pasivo: Un intruso puede reunir dos textos cifrados que estén encriptados con la misma secuencia de llaves, a partir de esto puede recuperar el texto original. Al realizar la operación XOR entre el cifrado y un texto original, puede recuperar las llaves y así decriptar los demás datos.

b) Ataque activo para insertar tráfico: Si un intruso conoce un paquete con su respectivo texto cifrado, puede generar una secuencia de llaves y puede encriptar paquetes construyendo un mensaje al calcular su CRC y haciendo el XOR con la secuencia de llaves. Este texto cifrado puede mandarse a una estación móvil de la red como un paquete válido.

c) Ataque activo de ambas estaciones: Si un atacante predice tanto la información como la dirección IP destino de un paquete, puede modificar los bits apropiados para transformar la dirección IP destino para mandar paquetes a un nodo diferente. El paquete puede ser decriptado por el punto de acceso y mandarlo como texto original a la computadora del atacante.

d) Ataque basado en tabla: Un atacante puede elaborar una tabla de decriptación usando vectores de inicialización, y a partir de cierta información sin encriptar, puede calcular la secuencia de llaves. Con esta tabla, el intruso puede decriptar

todos los paquetes enviados sobre el enlace inalámbrico, independientemente de sus vectores de inicialización.

e) Ataque por fuerza bruta: Un ataque de este tipo, es un procedimiento en el que a partir del conocimiento del algoritmo de cifrado empleado, y el par de texto plano con su respectivo texto cifrado, se prueban posibles combinaciones de secuencias de llaves con algún miembro del par hasta obtener el otro miembro.

Existen programas capaces de ejecutar los tipos de ataques mencionados anteriormente. Estas aplicaciones están disponibles de forma gratuita en Internet por lo que cualquier persona con conocimientos básicos de computación podría utilizaras.

Por lo visto en este capítulo, el WEP no garantiza la privacidad ni la integridad de la información que circula en una red inalámbrica, por lo que es necesario implementar nuevos mecanismos de seguridad.

3.5 Descifrando el WEP.

De acuerdo a la Figura 3.1, se puede descifrar el WEP siguiendo los pasos realizados en el siguiente ejemplo [JAM05]:

- Un usuario “A” hace que un usuario “B” encripte una serie de textos originales.
- “A” puede observar los textos cifrados que “B” generó al realizar la operación XOR entre los textos originales y las secuencias de llaves obtenidas con cada vector de inicialización.

- “A” conoce el texto cifrado y los textos originales, por lo que haciendo la operación XOR entre ambos textos, puede calcular las secuencias de llaves.
- Ahora “A” conoce las secuencias de llaves con las que se encriptó cada paquete de texto original.
- La siguiente vez que se utilice el mismo vector de inicialización para encriptar un texto original, “A” podrá decriptarlo.