Capítulo 7

Conclusiones y trabajo futuro

En esta tesis se presentó el funcionamiento del protocolo WEP y se analizaron las características que generan sus debilidades en materia de seguridad. Como una alternativa que elimina las debilidades del WEP, se presentó el algoritmo conocido como Técnica de Inserción de Caracteres Falsos y Compresión (FCICT). Además de analizar las características de cada algoritmo, se crearon interfaces visuales en las cuales se pudo observar y comparar el funcionamiento de ambos algoritmos, mostrando las ventajas que tiene el algoritmo FCICT sobre el WEP.

7.1 Conclusiones.

Las redes inalámbricas más usadas actualmente siguen usando el protocolo WEP como mecanismo de seguridad. Las características de este protocolo ofrecen muchas posibilidades para que los atacantes de redes, accedan fácilmente a una red y puedan interceptar y modificar la información que circula por la misma para sus propios propósitos.

El hecho de que sea el método más utilizado en el mundo para proteger redes inalámbricas, significa también que el mayor número de usuarios de estas redes se encuentra desprotegido contra posibles ataques. Por esto se han desarrollado nuevas técnicas que eliminan las deficiencias del WEP. Algunas de estas alternativas requieren simplemente una actualización en los dispositivos electrónicos que forman parte de una red inalámbrica. Tal es el caso de WPA y el estándar 802.11i que utiliza WPA2 y TKIP,

que ya se utiliza en la actualidad, principalmente en empresas que requieren de un alto nivel de seguridad.

En esta tesis se presenta una alternativa conocida como Técnica de Inserción de Caracteres Falsos y Compresión (FCICT). Esta técnica propone un algoritmo que actúa directamente sobre el WEP modificando los datos encriptados por el algoritmo RC4. Esta modificación de los textos cifrados consiste en la inserción de caracteres falsos utilizando una técnica de reemplazo o el algoritmo de compresión de Huffman.

Con el fin de comparar al WEP con la técnica FCICT, se realizaron ambas simulaciones en Matlab creando interfases gráficas para cada algoritmo, que permiten ingresar una cadena de texto y realizar el proceso de encriptación y decriptación del mismo (ver Apéndice A).

En el capítulo 6 se muestran las simulaciones realizadas en Matlab y los resultados de las mismas. Claramente se pudo observar el efecto que tiene la técnica FCICT aplicada sobre el algoritmo del WEP. La inclusión de caracteres falsos en el texto cifrado del RC4 dificulta en gran medida muchos de los ataques realizados normalmente para romper la seguridad del WEP.

Esto se debe a que la mayoría de los ataques a redes se basan en la recuperación de datos encriptados con las mismas secuencias de llaves, y a través de operaciones XOR entre los datos encriptados puede obtener las secuencias de llaves de encriptación y decriptar los datos. Si un intruso intenta realizar el mismo procedimiento con datos encriptados por la técnica FCICT, obtendría la información alterada respecto a la que

esperaría obtener. Esto se puede observar en las simulaciones visuales en la parte correspondiente al intruso.

Así mismo se analizó el efecto de la variable *m* comprobando que su valor es directamente proporcional a la probabilidad de un intruso de encontrar los caracteres falsos y descifrar la información. De esto se deduce que el valor ideal para *m* es 1, ya que se inserta la mayor cantidad posible de caracteres falsos lo cual disminuye la probabilidad que tiene un intruso de decriptar la información correcta. De acuerdo a los resultados obtenidos se puede decir que la técnica FCICT elimina muchas debilidades del WEP y su aplicación en redes inalámbricas es una opción eficiente que lograría una mejora importante en el área de seguridad.

Como en todas las ramas de la ciencia y la tecnología, la evolución de los procesos actuales es necesaria para satisfacer las necesidades cambiantes de la sociedad. En el área de redes inalámbricas, la técnica FCICT es un paso más en esta evolución para brindar mayor seguridad a los usuarios.

7.2 Trabajo futuro.

Este algoritmo podría ser implementado en algún dispositivo electrónico tal como un FPGA, con el objetivo de probar su funcionamiento más allá de la simulación en un lenguaje de programación. Esta implementación podría incluir el Código de Redundancia Cíclica (CRC32) y la inclusión de un vector de inicialización para ejecutar la técnica FCICT, tal y como trabajaría en una red inalámbrica.

Para realizar mejoras a este algoritmo se puede analizar su funcionamiento desde la perspectiva de ataques específicos a una red. Suponer un ataque específico a la red por parte de un intruso, es un paso primordial para empezar un análisis del algoritmo que lleve a mejorar el mismo.