Capítulo 1

Introducción

En este capítulo se presentan los antecedentes del tema central de la tesis que proporcionan al lector los elementos que le permitan entender el contexto de la misma, para plantear posteriormente el problema a resolver en este trabajo. Una vez planteado el problema, se presenta el objetivo de la tesis así como una breve descripción de las tareas a realizar y los resultados esperados que cumplan con dicho objetivo. En la sección final de este capítulo, se incluye la organización de la tesis, donde se describe brevemente el contenido de cada capítulo de la misma.

1.1 Antecedentes

Desde sus inicios, el hombre ha buscado formas de comunicarse con sus semejantes para poder compartir sus pensamientos y sentimientos. Esta necesidad lo llevó a la creación de un lenguaje hablado de comunicación, así como otras técnicas que van desde la pintura y escritura, hasta otras más rudimentarias. Cualquier método que utilizara, el objetivo era el mismo: transmitir ideas a otros individuos.

Con el paso del tiempo, los avances tecnológicos han permitido desarrollar formas de comunicación más avanzadas como pueden ser la telefonía e Internet, mismas que hoy en día son usadas en todo el mundo.

Sin duda Internet es el medio de comunicación más importante en la actualidad. Comunicando a millones de computadoras alrededor del mundo, Internet ha

transformado a la sociedad mundial en todos los aspectos. Su uso va en aumento tanto en organizaciones como en los hogares, haciendo que cada día crezca el número de personas que tienen acceso a la red mundial.

Conforme fue creciendo el número de personas y compañías que usaban Internet, hubo la necesidad de conectar varias computadoras entre sí, con el fin de que los usuarios pudieran compartir información entre ellas de forma rápida y segura. Por esto surgieron estándares con características específicas que permitían conectar varios nodos, formando así una red de computadoras.

El estándar IEEE 802.3, llamado así por el nombre de un comité de estandarización del *Institute of Electrical and Electronics Engineers* (IEEE) que lo produjo, ha sido el más usado en empresas y hogares hasta nuestros días. También conocidas como redes *Ethernet* o *LAN* (*Local Area Network*), estas utilizan conexiones cableadas entre los nodos de la red que pueden ser de fibra óptica o cables de cobre.

Posteriormente, los avances tecnológicos provocaron una tendencia a agregar a los sistemas de comunicación ya establecidos, la característica de movilidad del usuario. La movilidad consiste en la capacidad de un usuario para poder intercambiar datos con otros elementos de la red a través una conexión inalámbrica establecida dentro de un área de cobertura determinada, eliminando la necesidad de permanecer en un punto fijo para establecer y mantener dicha conexión.

Para proveer con movilidad a los usuarios de redes de computadoras, se creó el estándar IEEE 802.11 para redes inalámbricas, también conocidas como redes *WLAN*

(*Wireless Local Area Network*). Este estándar permite que los usuarios establezcan una conexión inalámbrica a una red con características similares a las de una red *LAN*, como velocidades de transmisión, seguridad, entre otras.

Una de las ventajas que ofrece una red inalámbrica es que cualquier usuario que se encuentre dentro del área de cobertura de la red puede tener acceso a la misma pero para un intruso esto es una oportunidad para entrar en la red con la posibilidad de leer, usar y modificar los datos que circulan por la misma.

Por esta razón, el estándar IEEE 802.11 incluye el protocolo de seguridad WEP (*Wired Equivalent Privacy*), que está diseñado para ofrecer un nivel de seguridad equivalente al de una red de área local (LAN). El WEP busca establecer una protección similar a la ofrecida por las medidas de seguridad de redes cableadas encriptando los datos que circulan por la WLAN. La encriptación de datos protege el vulnerable enlace inalámbrico entre clientes y puntos de acceso; una vez implementada esta medida de seguridad, se pueden agregar otros mecanismos de seguridad típicos de las LAN para asegurar privacidad, como acceso protegido por contraseña, redes virtuales privadas (VPN), y autenticación [JAG04].

1.2 Planteamiento del problema

Se ha demostrado que el WEP tiene debilidades que permiten a los intrusos obtener información, modificarla o eliminarla de una red inalámbrica 802.11, lo cual perjudica directamente a los usuarios ya que la privacidad de la información que envían o reciben no está garantizada.

El WEP basa su funcionamiento en un algoritmo que genera llaves de encriptación aleatorias, a partir de dos entradas. Una de estas entradas es fija y la otra es un vector que cambia constantemente con la finalidad de alimentar al algoritmo con entradas diferentes y generar llaves de encriptación distintas.

En una red inalámbrica, el transmisor envía este vector sin encriptar junto con la información encriptada por las llaves, al receptor, para que con dicho vector calcule las llaves para decriptar la información que recibió.

El problema de este mecanismo de seguridad es que si un intruso en la red intercepta la información enviada por el transmisor, podría calcular las llaves para decriptar la información a partir del vector que obtuvo. Esta característica del WEP es la causante de ataques diferentes que pueden realizarse contra una red protegida con este protocolo, y violar sus mecanismos de seguridad para obtener o alterar información que circule por la red.

Es importante señalar que la mayoría de las redes inalámbricas en el mundo usan el protocolo WEP para brindar seguridad a los usuarios [HOL05]. Debido a esto, es necesario desarrollar técnicas que protejan de una forma más efectiva la seguridad en las redes.

1.3 Objetivo de la tesis.

En esta tesis se simulará una mejora en el protocolo WEP utilizando Matlab como lenguaje de programación. Dicha mejora permite eliminar algunas de las deficiencias

más notables del protocolo WEP. Así mismo, se elaborará una interfase gráfica que permita simular el algoritmo mientras se muestra gráficamente la ejecución del mismo.

Estas deficiencias se pretenden resolver implementando una mejora del algoritmo RC4 (Ron Rivest code # 4), que consiste en la utilización de la técnica conocida como Técnica de Inserción de Caracteres Falsos y Compresión (FCICT), dentro del algoritmo RC4. Esta técnica permite que el protocolo WEP sea invulnerable a ataques por fuerza bruta, haciendo de la decriptación de mensajes un proceso complicado para intrusos, contrarrestando varias debilidades del WEP.

De esta forma se lograría una mejora importante en el protocolo WEP, que brindaría seguridad a los usuarios de redes inalámbricas 802.11, proporcionándoles privacidad, autenticidad e integridad de la información.

1.4 Organización de la tesis.

El trabajo reportado en esta tesis consiste en 7 capítulos y 4 apéndices, los cuales se describen a continuación.

En el capítulo 2 se presenta la teoría referente a las redes inalámbricas IEEE 802.11 mencionando las topologías y características generales de este estándar, así como los requerimientos necesarios para implementar una red inalámbrica.

En el capítulo 3 se describe el funcionamiento del WEP, explicando detalladamente cada una de las partes que componen este protocolo. De igual forma se

mencionan las características causantes de las debilidades que en materia de seguridad tiene el WEP y se analiza porqué es necesario implementar mejoras en este protocolo.

En el capítulo 4 se describen técnicas y protocolos de seguridad existentes que han surgido por la necesidad de eliminar las debilidades del WEP para ofrecer un nivel mayor de seguridad a los usuarios de redes inalámbricas.

En el capítulo 5 se profundiza en la técnica FCICT, que es la alternativa simulada en esta tesis, describiendo su funcionamiento y explicando cómo este algoritmo ayuda a eliminar las debilidades más comunes del WEP.

En el capítulo 6 se presentan las simulaciones realizadas en la interfase gráfica creada en Matlab. Estas simulaciones corresponden a ejecuciones del algoritmo WEP y la técnica FCICT, misma que se simuló con dos algoritmos posibles: la técnica de reemplazo y compresión de Huffman. Se presentan también simulaciones de la técnica FCICT donde se analiza el efecto de una variable de la cual depende la probabilidad que tiene un atacante de romper el mecanismo de seguridad. Los resultados de estas simulaciones se exponen y analizan en la parte final del capítulo, incluyendo tablas comparativas que ayudan a comprender las ventajas y desventajas de la técnica FCICT.

En el capítulo 7 se muestran las conclusiones obtenidas de la realización de esta tesis. Así mismo se aportan algunas ideas, que toman como base lo elaborado en esta tesis y pueden usarse para realizar un posible trabajo futuro que contribuya con nuevas aportaciones.

En la última parte de esta tesis se muestran las referencias bibliográficas consultadas para su realización y se incluyen los apéndices que incluyen imágenes de las simulaciones realizadas en Matlab para cada caso, así como el código elaborado para programar cada algoritmo con su respectiva interfase gráfica.