

Índice.

Capítulo 1

- 1.1 Antecedentes
- 1.2 Planteamiento del problema
- 1.3 Objetivo de la tesis.
- 1.4 Organización de la tesis.

Capítulo 2

- 2.1 Introducción a redes inalámbricas IEEE 802.11
- 2.2 Características generales de una red IEEE 802.11
 - 2.2.1 Componentes de una WLAN
 - 2.2.2 Topologías WLAN
 - 2.2.3 Trama del estándar 802.11
- 2.3 Evolución del estándar IEEE 802.11
 - 2.3.1 IEEE 802.11b
 - 2.3.2 IEEE 802.11a
 - 2.3.3 IEEE 802.11g

Capítulo 3

- 3.1 Componentes del WEP
 - 3.1.1 Llave secreta
 - 3.1.2 Vector de inicialización
 - 3.1.3 Algoritmo RC4
 - 3.1.4 Código de Redundancia Cíclica
- 3.2 Funcionamiento del WEP.
 - 3.2.1 Proceso de encriptación del WEP.
 - 3.2.2 Proceso de decriptación del WEP.
- 3.3 Debilidades del WEP.
- 3.4 Tipos de ataques al WEP.
- 3.5 Descifrando el WEP.

Capítulo 4

- 4.1 Estándar IEEE 802.1X.
- 4.2 Red privada virtual (VPN).
- 4.3 Capa de sockets seguros (SSL).
- 4.4 Temporal Key Integrity Protocol (TKIP).
- 4.5 Acceso protegido de fidelidad inalámbrica (WPA).
- 4.6 Estándar 802.11i y WPA2 (Acceso protegido de fidelidad inalámbrica 2)
- 4.7 Técnica de Inserción de Caracteres Falsos y Compresión (FCICT, Fake Character Insertions and Compression Technique)

Capítulo 5

5.1 Funcionamiento de la FCICT.

5.1.1 Generación de la secuencia de llaves

5.1.2 Encriptación FCICT utilizando la técnica de reemplazo.

5.1.3 Decriptación FCICT utilizando la técnica de reemplazo.

5.1.4 Encriptación FCICT utilizando el algoritmo de compresión de Huffman.

5.1.5 Decriptación FCICT utilizando el algoritmo de compresión de Huffman.

5.2 Ventajas de la técnica FCICT sobre el WEP.

Capítulo 6

6.1 Introducción

6.2 Encriptación y decriptación de información del WEP.

6.3 Encriptación y decriptación de información usando la técnica FCICT con técnica de reemplazo y valor m igual a 1.

6.4 Encriptación y decriptación de información usando la técnica FCICT con técnica de reemplazo y valor m igual a 4.

6.5 Encriptación y decriptación de información usando la técnica FCICT con técnica de reemplazo y valor m igual a 8.

6.6 Encriptación y decriptación de información usando la técnica FCICT con algoritmo de compresión de Huffman.

Capítulo 7

7.1 Conclusiones.

7.2 Trabajo futuro.

Bibliografía

Apéndice A: Imágenes de las simulaciones en la interfase gráfica de Matlab.

Apéndice B: Código en Matlab de la simulación del WEP.

Apéndice C: Código en Matlab de la simulación de la FCICT con técnica de reemplazo.

Apéndice D: Código en Matlab de la simulación de la FCICT con algoritmo de compresión de Huffman.