Resumen

Actualmente, las redes inalámbricas de computadoras son utilizadas en organizaciones y hogares de todo el mundo debido a las ventajas que ofrecen comparadas con redes cableadas. Aunque existen varios estándares de comunicación capaces de implementar redes inalámbricas, esta tesis se enfoca en el estándar IEEE 802.11 por ser el mayormente utilizado en la actualidad. Las redes que funcionan bajo las especificaciones de este estándar se conocen también como WLAN *(Wireless Local Area Network).*

Al utilizar el aire como medio de transmisión de datos, cualquier usuario con un dispositivo inalámbrico compatible con dicho estándar puede ingresar a la red. Por esto, el estándar 802.11 incluye un protocolo de seguridad llamado WEP (*Wired Equivalent Privacy*) encargado de encriptar la información que se envía por la red con el objetivo de que únicamente el receptor indicado pueda decriptarla.

A través del tiempo, se han encontrado debilidades en el WEP que permiten a usuarios no autorizados por la red (intrusos) violar la seguridad de la red fácilmente. Esto ha motivado el desarrolló de nuevos mecanismos de seguridad que eliminen las deficiencias del WEP.

En esta tesis se analiza y simula el funcionamiento de un WEP mejorado conocido como Técnica de Inserción de Caracteres Falsos y Compresión (FCICT, *Fake Character Insertions and Compression Technique*). Esta técnica modifica los datos encriptados por el WEP de tal manera que sólo puedan ser decriptados por el receptor

indicado. Esto elimina algunas de las debilidades del WEP haciendo más difícil el proceso de decriptación de información para un intruso.

Para simular tanto la técnica FCICT como el WEP, se crearon interfases visuales en el lenguaje de programación Matlab, las cuales nos permiten interactuar con el algoritmo y observar los resultados de forma clara.

En dichas interfases se realizaron simulaciones de ambos mecanismos de seguridad. Los resultados de tales simulaciones nos permiten diferenciar entre los datos encriptados por la técnica FCICT y los encriptados por el WEP. Así mismo podemos notar que los procedimientos más comunes que utilizan los intrusos para romper la seguridad del WEP, no serían efectivos al aplicarse en la técnica FCICT. Por lo tanto, esta técnica elimina las debilidades más importantes del WEP y podría ofrecer mayor seguridad a usuarios de redes inalámbricas.

Sin embargo, así como la tecnología avanza, los atacantes pueden desarrollar técnicas que les permitan romper la seguridad de alternativas más seguras que puedan surgir en el futuro, incluyendo la técnica FCICT.

A pesar de esto, la técnica FCICT presenta ventajas notables en comparación con el WEP y por ahora se muestra como una alternativa viable y eficiente que elimina las deficiencias principales del WEP, y que pudiera ofrecer mayor seguridad a los usuarios de redes inalámbricas.