## RESUMEN

Esta tesis documenta el desarrollo de un sistema de detección de intrusos en redes de computadoras basado en el protocolo HTTP (*Hypertext Transfer Protocol*). Se describe el modelado y simulación de dicho sistema utilizando redes neuronales recurrentes y señalando sus ventajas en comparación a otros sistemas de seguridad comúnmente utilizados.

El sistema de detección de intrusos está basado en la identificación y clasificación de anomalías en el flujo de datos en una red. Se presenta un panorama actual del estado de la seguridad en línea como contexto y justificación al desarrollo del presente proyecto y se hace una descripción detallada de los tipos de ataques esperados junto con la clasificación del sistema de detección de intrusos desarrollado en comparación a las demás alternativas en este campo.

El sistema fue diseñado mediante programación en MATLAB® utilizando la arquitectura de redes neuronales conocida como Redes Neuronales Recurrentes completamente conectadas, capaces de trabajar en tiempo real mientras están conectadas a Internet. Se desarrollaron rutinas para implementar el algoritmo de entrenamiento en tiempo real para la red creada y se hizo una comparación entre el resultado del entrenamiento con este algoritmo y el de propagación hacia atrás en el tiempo para determinar cuál sería mejor en términos de resultados y desempeño.

El objetivo de este proyecto de tesis fue demostrar que las redes neuronales recurrentes son más rápidas, exactas y adaptables para su aplicación en un sistema de detección de intrusos que los tipos de redes utilizados en una tesis anterior la cual se basó únicamente en redes tipo *feedforward* y redes Elman (redes parcialmente conectadas). Se

analizarán las ventajas y desventajas conceptuales de los tipos de red para finalmente ofrecer una conclusión definitiva sobre la mejor opción para implementar un sistema de detección de intrusos capaz de trabajar en tiempo real, y se corroborará dicho resultado con los porcentajes numéricos de las medidas de desempeño de cada red.

Los resultados finales al terminar el proyecto fueron los esperados, manifestando que las redes neuronales recurrentes son superiores a las demás en velocidad de convergencia y efectividad, alcanzando 94% en porcentaje de clasificación correcta de ataques a la red perpetrados por intrusos en un tiempo de 60 *epochs*, a comparación de 106 *epochs* y menos del 90% en clasificación para una red Elman. Sin embargo, las redes neuronales recurrentes poseen una complejidad importante como desventaja, la cual aumenta exponencialmente con el número de neuronas en la red.