Capítulo 7. Conclusiones y trabajo a futuro

En este capítulo se analizan los resultados obtenidos entre los distintos modelos contemplados en el estudio. Resaltando las características de las redes neuronales que utilizan funciones de transferencia wavelet como una alternativa a modelos tradicionales, mejorando de manera significativa la velocidad de convergencia e indicadores como tasas de falsos positivos y falsos negativos.

7.1. Conclusiones

A lo largo del tiempo diversas técnicas han sido propuestas para mejorar la detección de conductas dañinas en las redes de comunicación, en este contexto el uso de redes neuronales aplicadas en los sistemas de detección de intrusos demuestra ser una alternativa eficiente y una área de investigación promisoria.

En términos de velocidad de convergencia el modelo basado en la red neuronal auto recurrente SRWNN – MRW necesitó 60 épocas de entrenamiento contra 81 del modelo recurrente totalmente conectado, dejando en último lugar al modelo Elman con 160. Sin embargo el costo computacional requerido por el modelo recurrente totalmente conectado es del orden de $O(n^4)$ catalogándolo como el más costoso en términos de recursos computacionales. Es decir que tomando en cuenta los índices de clasificación e identificación, el modelo auto recurrente con wavelets SRWNN – MRW con una complejidad computacional de $O(n^2)$ ofrece una aproximación cercana al recurrente totalmente conectado a un costo computacional menor.

Las medidas en las tasas de falsos positivos y falsos negativos indican que aunque el modelo Elman obtuvo una menor tasa de falsos positivos emitidos, éste también posee la tasa de falsos negativos más alta de todos los modelos. Este comportamiento se puede analizar a través de los indicadores estadísticos de especificación y sensibilidad. La especificación se define como la probabilidad de que un patrón inofensivo de entrada sea catalogado por el IDS como tráfico de red normal. La sensibilidad es la probabilidad de que el IDS catalogue a un patrón dañino de entrada como un ataque al sistema. Una vez señaladas estas dos probabilidades tenemos que el modelo Elman posee una alta probabilidad de especificación, alrededor de 96%, lo que explica el bajo índice de falsos positivos. Por otra parte, el modelo Elman posee una sensibilidad muy baja, 78%, lo que explica el alto porcentaje en su tasa de falsos negativos. En un IDS ideal los indicadores de especificación y sensibilidad deben ser altos, aunque en aplicaciones prácticas nunca se obtiene un 100%, resultando en la emisión de falsos positivos y falsos negativos [FAW04].

Tomando en cuenta lo anterior, el modelo recurrente totalmente conectado y el auto recurrente con wavelets (SRWNN) resultan con tasas más equilibradas de falsos positivos y falsos negativos siendo estas 7.24%, 6.53% para el primero y 7.24%, 8.52 para el segundo. Es de recalcar que las tasas obtenidas por el modelo propuesto (SRWNN - MRW) fueron de 5.43% y 9.65%, estableciendo un mejor resultado en la tasa de falsos positivos que las dos arquitecturas mencionadas anteriormente.

El gráfico ROC demuestra que la aplicación de redes neuronales a los modelos de detección de intrusos funciona de manera significativa debido a que los 4 modelos contemplados se ubican en la región triangular superior, lo que permite establecer que su desempeño se aleja del comportamiento aleatorio definido por la línea y = x. En el gráfico se puede apreciar que respecto al costo, mientras el modelo Elman se ubica más al oeste de la gráfica, los modelos restantes están orientados más al este señalando una emisión mayor de falsos positivos. Si se considera el eje de los verdaderos positivos tenemos claramente que los modelos recurrente totalmente conectado y auto recurrente con wavelets (SRWNN y SRWNN - MRW) superan a Elman considerablemente, estableciendo sus ventajas al momento de la detección de patrones dañinos. El modelo Elman se dice que es más conservador que los restantes debido a que lleva a cabo una clasificación positiva de los patrones solo con evidencia firme y como consecuencia posee un índice bajo de falsos positivos, pero al mismo tiempo con la desventaja de tener una tasa baja de verdaderos positivos. Por el contrario los modelos recurrente totalmente conectado y auto recurrentes con wavelets (SRWNN y SRWNN - MRW) pueden ser llamados liberales debido a que llevan cabo una clasificación positiva con evidencia más ligera resultando en una mejor clasificación de ataques con el costo de tener una tasa de falsos positivos más alta [FAW04].

Como se puede observar en los resultados del capítulo anterior, la red neuronal recurrente totalmente conectada y la auto recurrente con wavelets (SRWNN - MRW) obtuvieron los mejores resultados en los indicadores de clasificación e identificación, siendo estos 93.15%,84.23 y 92.19%, 84.23% respectivamente. Estas medidas ubican a los modelos anteriores como los candidatos más factibles en la implementación del sistema de detección de intrusos que pueda cumplir con niveles de seguridad requeridos en una red de comunicaciones.

Las redes neuronales wavelet son un nuevo tipo de redes neuronales desarrolladas en los últimos años que combinan la teoría de las redes neuronales y el procesamiento wavelet. La principal característica de estas arquitecturas es que las funciones de transferencia de las unidades de procesamiento son cambiadas por funciones derivadas de una wavelet madre, para dar lugar a lo que se conoce como neurones wavelet o *wavelons*. De igual manera que en las redes neuronales convencionales, dentro del campo de redes neuronales wavelet existen distintas estructuras como la red con alimentación hacia adelante o la recurrente, el presente trabajo ha centrado su atención en las topologías

recurrentes debido a que en trabajos anteriores éstas han obtenido las mejores medidas de desempeño [SAN05]. Durante el desarrollo de este proyecto se ha presentado el modelo auto recurrente con wavelets (SRWNN - MRW) para conocer su desempeño aplicado en los sistemas de detección de intrusos, obteniendo excelentes resultados que comprueban la eficiencia del procesamiento wavelet en las redes neuronales.

Esta tesis ha desarrollado un nuevo modelo de detección de intrusos basado en una arquitectura recurrente con funciones de transferencia wavelet. El proceso de construcción de dicho modelo abarcó el diseño de la topología, deducción del algoritmo de aprendizaje de la red neuronal, pre procesamiento de los datos, implementación y finalmente la evaluación de resultados. Después de una evaluación de los parámetros de desempeño, los resultados obtenidos permiten establecer la factibilidad de su implementación debido a que los valores obtenidos en esta arquitectura se ubican en las mejores posiciones respecto a otros modelos estudiados. Los resultados comparativos obtenidos serán considerados dentro de un artículo de divulgación científica que sirva a los investigadores en el área de seguridad informática como referencia en la aplicación de redes neuronales recurrentes wavelet en los IDS.

Una de las características más positivas del modelo auto recurrente con wavelets (SRWNN - MRW) es su velocidad de convergencia ya que puede alcanzar ciertas medidas de eficiencia con un número menor de épocas de entrenamiento y de esta manera facilitar el proceso de aprendizaje cuando se tiene un conjunto de muestras grande, todo esto haciendo un uso menor de recursos computacionales que otros modelos como el recurrente totalmente conectado.

7.2. Trabajo a futuro

En esta investigación se presentó la estructura de una red neuronal recurrente con wavelets wavelets (SRWNN - MRW) junto con su algoritmo de aprendizaje, aplicada a un sistema de detección de intrusos. Debido a que la investigación en el área de seguridad informática está en continuo desarrollo es necesario conocer el potencial de otros modelos que implementen las unidades *wavelon* con otros esquemas de interconexión y algoritmos de aprendizaje.

Cuando el esquema recurrente considera conexiones de retroalimentación desde la capa de salida a la capa de entrada tenemos modelos como: dinámico con wavelets [OUS98], espacio estado wavelet [BOR07]. Estos modelos representan oportunidades para obtener mejores resultados en los distintos indicadores estadísticos que hemos definido en este trabajo y conocer más sobre el potencial de las redes neuronales wavelet en el área de detección de intrusos. Además de los modelos citados brevemente, existen distintos

algoritmos de aprendizaje para las redes neuronales que pueden ser utilizados como opciones a los presentados. Estos algoritmos permitirán analizar el rendimiento durante la etapa de aprendizaje respecto a los algoritmos ya conocidos. Algunos ejemplos de dichos algoritmos son: Metropoli Monte Carlo, Algoritmos genéticos o algoritmos de optimización combinacional.