7. CONCLUSIONES Y TRABAJO A FUTURO

En este capítulo se discuten los resultados finales de manera comparativa, haciendo énfasis en la justificación de haber elegido un IDS basado en RNN como opción más eficiente para los requerimientos del problema planteado. También se proponen posibles caminos de investigación para ahondar en el tema de los IDS y redes neuronales en trabajo a futuro que deberá mejorar los resultados obtenidos.

7.1 CONCLUSIONES

Las ilimitadas opciones en términos de conectividad y comunicación que existen hoy en día debido a la tecnología que hace posible la existencia de redes de computadoras ha traído consigo la inevitable necesidad de proteger cada uno de los elementos que pertenecen a dichas redes de usuarios no deseados. Esto es debido a que el hecho mismo de que muchos equipos estén interconectados entre sí hace posible que cualquiera que tenga acceso a la red afecte a cada uno de los elementos que la conforman, con consecuencias potencialmente catastróficas de usarse dicha conexión de una forma errónea.

El protocolo de transferencia de hipertexto (HTTP), el más usado entre su tipo y asociado fuertemente con Internet, es de particular interés, ya que es posible que la transmisión y recepción de datos dentro de una red siguiendo este protocolo sea corrompida por un intruso en la red, o simplemente interceptada. Por lo general, al haber un ataque al flujo de información en una red se producen anomalías características que lo identifican como algo que está fuera de lugar y que por consiguiente debe interrumpirse y ser prevenido en ocasiones posteriores [1,2].

Los diferentes tipos de arquitectura de las redes neuronales se adecuan mejor a cierto tipo de aplicaciones de acuerdo a sus ventajas y desventajas. En este caso, el

interés fue que la red desarrollada pudiera trabajar *on-line*, actualizando los valores de sus pesos en tiempo real y de esta manera funcionar adecuadamente en un IDS. Tras el modelado, simulación y pruebas de tres tipos de redes neuronales diferentes, se ha demostrado que la premisa inicial de considerar a las redes recurrentes completamente conectadas es la mejor opción.

Esta tesis ha logrado su objetivo al lograr modelar y simular una RNN, creado asimismo rutinas de inicialización, entrenamiento, prueba y evaluación para esta red utilizando MATLAB®. Hemos comparado el desempeño de la red creada con aquellas redes ya disponibles en el paquete matemático por medio de funciones especializadas, y hemos cumplido con las expectativas del problema, mejorando los resultados anteriores en términos de porcentajes de error y de funcionamiento correcto.

El único inconveniente de una RNN es su complejidad de cálculo al utilizar el RTRL, demandando órdenes de $O(n^4)$, lo que se traduce en una elevada demanda de tiempo de procesamiento que no obstante se ha compensado por medio de parámetros de diseño cuidadosamente seleccionados para capitalizar sus características positivas y así adecuar la red a la aplicación específica que contemplemos, la creación de un IDS operacional.

Finalmente, es importante resaltar el hecho de que una vez creada, esta red neuronal puede ser entrenada y probada con datos procedentes de cualquier aplicación siempre y cuando se le dé un formato correcto a los datos. De la misma manera que el código creado puede identificar ataques basados en HTTP, puede servir para calcular trayectorias, identificar firmas falsas a partir de muestras verdaderas o reconocer personas por medio de su voz si los datos en cuestión son pre-procesados en maneras similares a como se hizo en este caso. Las redes neuronales son el futuro de la

investigación en muchos campos debido a su gran adaptabilidad y promesa de desarrollo.

7.2 TRABAJO A FUTURO

Durante la investigación, se encontraron muchos artículos de científicos que han trabajado sobre la mejora de los algoritmos de entrenamiento de las redes neuronales. En particular, Williams y Zipser [14], Mak, Ku y Lu [15] y Mak [16] sugieren, entre otros, el uso de algoritmos como el *Truncated Backpropagation* y el FRTRL (*Fast RTRL)* como alternativas para mejorar el desempeño de las redes neuronales.

También se han propuesto enfoques híbridos [16] que combinan ciertas características de diferentes métodos para ofrecer mejores resultados en menor tiempo y evidentemente con un costo menor en términos de procesamiento. Todas estas vertientes de investigación son opciones atractivas para proyectos posteriores que deseen mejorar los resultados de esta tesis con el fin de tener menores porcentajes de error y mayores porcentajes de identificación de ataques en un IDS.

A pesar de haber sido abandonadas por algún tiempo después de su descubrimiento, las redes neuronales han demostrado tener potencial para la resolución de problemas que formas tradicionales de programación no tienen. El encontrar otras aplicaciones que sean un reto para las redes neuronales desarrolladas es una opción más para aquellos que deseen trabajar sobre este tema en el futuro. El límite, en este caso, es únicamente la creatividad.