CAPITULO 8 CONCLUSIONES Y TRABAJO A FUTURO.

En este capítulo se analizan los resultados obtenidos en el apartado anterior realizando conclusiones finales y se presentan las opciones de trabajo a futuro que permiten darle continuidad a este proyecto.

8.1 CONCLUSIONES

El uso de las redes neuronales como tecnología adaptiva para la detección de intrusos es viable y ofrece una solución a este problema como ningún Sistema basado en comparación de firmas. Un sistema de este tipo no es capaz de reconocer ataques completamente nuevos, o variaciones de las formas conocidas. Sin embargo, debido a que las redes neuronales son capaces de hallar patrones en los datos, tienen la posibilidad de hallar ataques nuevos.

La red Elman mostró el mejor desempeño obteniendo un 90 % de efectividad con datos completamente desconocidos para la red, de manera que el uso de este tipo de red, se presenta como la mejor opción de implementación. Si comparamos este resultado con la eficiencia que tienen los sistemas basados en reconocimiento de firmas, se verá que se ha logrado un muy alto porcentaje de efectividad, ya que un sistema basado en firmas no es capaz de reconocer ataques nuevos.

El proyecto de tesis alcanzo su objetivo general, al determinar el modelo de red neuronal más adecuado para enfrentar un problema de esta naturaleza, demostrando la capacidad de las redes neuronales para trabajar con datos reales hallando los patrones suficientes para poder generalizar en nuevos datos.

A lo largo de este proyecto de tesis se profundizó en los conceptos que enmarcan el diseño de sistemas de detección de intrusos para redes de comunicación al igual que los conceptos que definen las tecnologías adaptivas utilizadas, sirviendo de modelo de

investigación base, para el desarrollo e implementación posterior de un sistema de esta índole.

Las redes neuronales tienen todavía muchas aplicaciones por ser implementadas, y lograron hallar orden donde parecía haber caos, ya que a simple vista, no hubiéramos podido acertar a detectar ataques en los datos que la red sí pudo detectar. Su estabilidad se basa en su flexibilidad y su capacidad de ver donde difícilmente se puede ver, se basa en su complejidad de funcionamiento y paradójicamente en su simplicidad estructural.

8.2 TRABAJO A FUTURO.

Este proyecto puede continuar si se realiza la implementación en un *FPGA* de la red neuronal que lleva a cabo la detección de Intrusos. De esta manera, tendríamos un sistema de detección de Intrusos sin la necesidad de gastar en equipo de cómputo especial para este problema, haciendo más eficiente y económica la Detección de Intrusos.

Otra sugerencia de trabajo a futuro es la puesta a prueba de otras redes neuronales más complejas con paradigmas de aprendizaje distintos, como podría ser el caso del aprendizaje no supervisado.

Finalmente la etapa de implementación de este diseño, se puede llevar a cabo desde distintos enfoques, como podría ser la, ya mencionada, implementación en dispositivos programables, haciendo un hardware de detección de intrusos, o colocar la red neuronal en software destinando una computadora para correr este software de protección en redes.

Un estudio a profundidad del protocolo *HTTP*, permitiría hallar nuevos patrones de entrenamiento, y si permitimos que la red adapte sus parámetros libres constantemente, estaremos en vías de tener un Sistema de Detección de Intrusos actualizado y ajustado a los distintos tipos de ataques. Por otro lado restaría estudiar otros protocolos de comunicación

en redes de comunicación, y siguiendo el mismo método de diseño de este proyecto, podríamos hallar modelos de detección de intrusos que se ajusten a cada protocolo.