Resumen

A medida que las redes de comunicación crecen y se interconectan con otras redes públicas, estas quedan expuestas a sufrir distintos tipos de ataques que explotan vulnerabilidades en su infraestructura, resultado de la evolución continua de los ataques y la incorporación de nuevos métodos y técnicas. Aún cuando los ataques con frecuencia son iniciados desde el exterior, el aislamiento físico del segmento de red no garantiza la protección contra incidentes originados en el interior, es entonces cuando se hace necesario incorporar distintos niveles de protección para preservar la confidencialidad e integridad de la información de los usuarios.

Los sistemas para detección de intrusos representan un componente importante dentro de las herramientas de defensa disponibles, su objetivo principal es detectar actividades no autorizadas e identificar de manera positiva ataques al sistema. A lo largo del desarrollo de estos sistemas se ha experimentado con distintos enfoques en su implementación, para mejorar su efectividad en la detección de ataques y adaptabilidad en la evolución de los mismos, motivando la investigación en distintas áreas como la inteligencia artificial y la estadística.

Un enfoque considerado en los sistemas para detección de intrusos es el uso de redes neuronales. Este modelo está inspirado en el proceso biológico del cerebro humano, considera distintas unidades interconectadas llamadas neurones, organizadas en capas. Cada unidad posee conexiones de entrada mediante las cuales recibe estímulos del medio externo o de otras unidades y conexiones de salida que transmiten el procesamiento de la entrada al aplicar una función de transferencia. Dentro de la implementación de sistemas para detección de intrusos que utilicen redes neuronales, existe una gran variedad de arquitecturas aplicadas, encontrando en cada una distintos resultados en la detección de ataques o conductas intrusivas.

En los últimos años distintos modelos de redes neuronales artificiales han sido propuestos, entre estos destaca las redes neuronales artificiales wavelets. Las redes neuronales wavelet implementan el procesamiento wavelet como parte de su funcionamiento a través del cambio de las funciones de transferencia tradicionales como la sigmoide por funciones wavelet. La combinación de ambas teorías busca aprovechar las características de análisis y descomposición del procesamiento wavelet junto con las propiedades de aprendizaje, adaptación y generalización de las redes neuronales. En esta investigación, el objetivo es mejorar los índices de detección y clasificación de ataques a los sistemas de redes de comunicación a través de un sistema para detección de intrusos que implemente en su funcionamiento una red neuronal recurrente wavelet.

La aportación principal de esta investigación consiste en la definición de una nueva arquitectura recurrente con wavelets, dicha arquitectura describe un nuevo esquema de interconexiones entre las unidades de procesamiento, características dinámicas de estas y su distribución entre las distintas capas. Las propiedades recurrentes del modelo se presentan a través de auto conexiones en las unidades de procesamiento, representando de esta manera estados de memoria. A partir de la definición de la arquitectura se propone el algoritmo de aprendizaje para la etapa de entrenamiento, este algoritmo establece la forma en la que se actualizarán los parámetros ajustables en cada ciclo.

Los resultados reportados por el modelo propuesto permiten establecer una mayor velocidad de convergencia en la etapa de entrenamiento frente a arquitecturas recurrentes tradicionales y recurrentes con wavelets. También se reconoce su capacidad en la detección de intrusos dando un porcentaje de efectividad de 92.19% y su baja emisión de falsas alarmas con una tasa de 5.43%.