CAPITULO 1. INTRODUCCIÓN

En este capítulo se plantea el problema de la detección de intrusos y se proponen los objetivos que esta tesis cumple y la solución que se diseñara para el problema en cuestión.

1.1 PLANTEAMIENTO DEL PROBLEMA

La aparición en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la Seguridad Informática cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestro ordenador se conecta a Internet, se abren ante nosotros toda una nueva serie de posibilidades, sin embargo estas traen consigo toda una serie de nuevos y, en ocasiones complejos tipos de ataque. Dichos ataques pueden ser caracterizados como anomalías en el comportamiento usual del flujo de datos en dicha red de comunicaciones.

El proyecto de tesis a realizar consiste en el diseño de un sistema de detección de intrusos (*IDS*) basado en la utilización de una red neuronal. Dicha red neuronal deberá ser primeramente definida y posteriormente entrenada para observar los patrones de comportamiento del flujo de datos en una red de comunicaciones de tal manera que esta red neuronal sea capaz de detectar una anomalía en el flujo de datos que pudiera corresponder a un ataque en la red de comunicaciones.

Se puede definir un sistema de detección de intrusos (*IDS*) como un sistema que recolecta y analiza información procedente de distintas áreas de una red de computadoras con el objetivo de identificar posibles fallos de seguridad. Este análisis en busca de intrusiones incluye tanto los posibles ataques externos como los internos [VER03].

La Figura 1.1 muestra la forma en que un dispositivo de detección de intrusos puede funcionar en el esquema general de redes de computadoras.

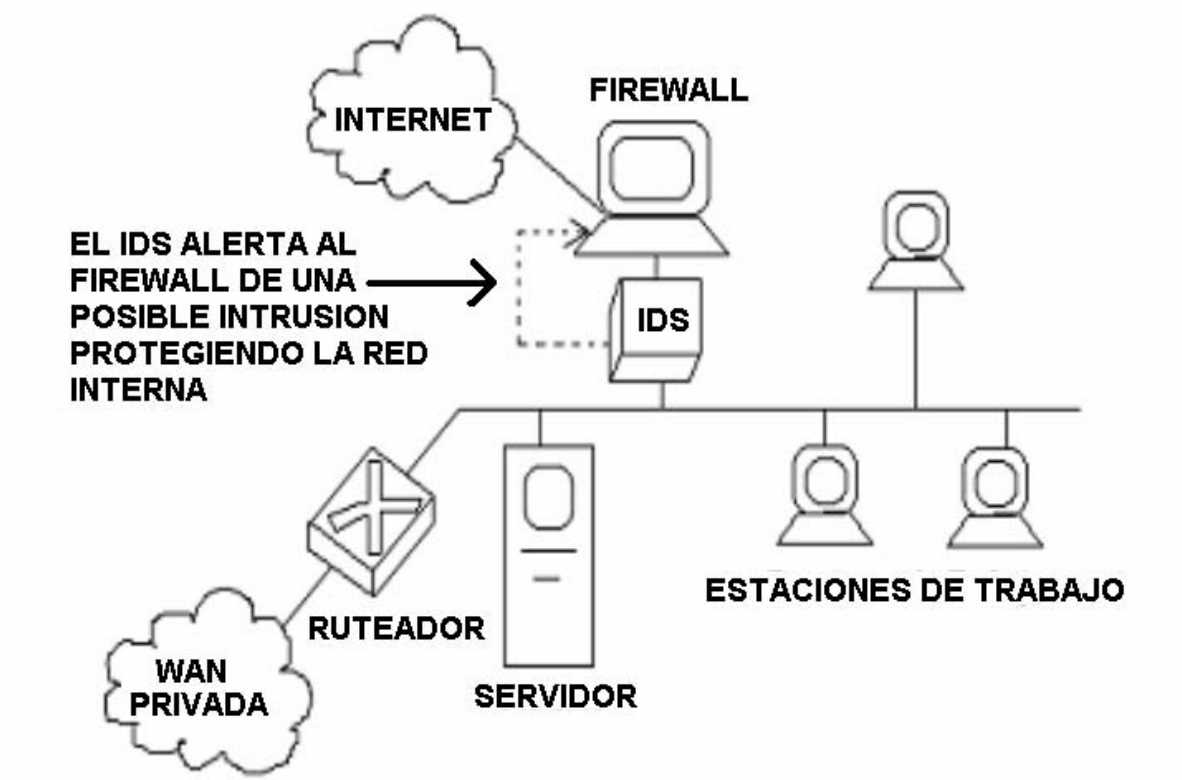

Figura 1.1. Sistema de Detección de Intrusos.

Existen dos tipos de enfoques que se han desarrollado para la detección de intrusos, la detección de anomalías (*anomaly detection*) y de uso erróneo (*misuse detection*). El enfoque de uso erróneo tiene la limitante de que únicamente puede ser capaz de detectar ataques conocidos [PLA01]. Las firmas utilizadas en estos *IDS* usualmente son simples patrones que permiten detectar ataques ya conocidos. Su funcionamiento es el mismo que el de los antivirus, se basan en encontrar coincidencias de ataques ya conocidos en el tráfico actual de la red. Debido a esto los *IDS* basados en uso erróneo no serán capaces de detectar ataques nuevos o variaciones de las firmas conocidas.

Debido a las limitantes de un sistema basado en la detección de uso erróneo, el proyecto de tesis a desarrollar, tomará en cuenta el enfoque de detección de anomalías, ya que este enfoque permite detectar ataques nuevos y completamente desconocidos. De manera que el sistema sea capaz de discernir si un requerimiento en Internet tiene un comportamiento normal, o intrusivo.

El diseño de sistemas de detección de intrusos ha llevado a las investigaciones a desarrollar variadas técnicas para realizar una detección de intrusos eficiente. En este campo de investigación se han desarrollado distintos diseños que permiten trabajar de manera eficiente como en [MAN02] y en [BIV02]. Sin embargo, aún no se ha alcanzado un estado definitivo en el cual la detección de intrusos se lleve a cabo de forma absolutamente confiable. Es por esto que el resultado que se pretende obtener en esta tesis es el de servir como base a un sistema de detección de intrusos con posibilidades de desarrollo a futuro.

En esta tesis se plantea la utilización de redes neuronales para detectar intrusos, tomando en cuenta las ventajas que una red neuronal puede proporcionarnos. Y enfocando el problema desde la perspectiva de las redes neuronales, basados en el proyecto desarrollado por la Universidad Javeriana de Bogotá, Colombia [TOR03].

1.2 OBJETIVO DE LA TESIS

El objetivo general de este proyecto de tesis es obtener un modelo de red neuronal suficientemente acercado a detectar la intrusión indeseada en una red de comunicaciones, aproximándonos al modelo más eficiente que la naturaleza de la red neuronal nos permita alcanzar, obteniendo suficientes resultados para tomar una decisión en cuanto a la eficiencia del modelo utilizado, sus limitaciones y sus alcances.

1.3 ORGANIZACIÓN DE LA TESIS

La tesis se ha desarrollado de tal forma que el lector pueda adentrarse en los conceptos teóricos que envuelven a un problema de esta índole y posteriormente pueda seguir paso a paso el diseño del sistema que hemos obtenido en este proyecto evaluando sus capacidades y eficiencia. Para esto la tesis se ha dividido en 8 capítulos que se desarrollan como se muestra a continuación.

CAPITULO 2. En el segundo capítulo se presentan los conceptos principales de sistemas de detección de intrusos, redes de computación y ataques en Internet, vislumbrando las tecnologías aplicables a solucionar este problema.

CAPITULO 3. En el tercer capítulo se introducen los conceptos que describen a las redes neuronales como tecnología adaptiva de reconocimiento de patrones, pasando por su estructura, algoritmo de entrenamiento y enfocándonos paulatinamente al uso de redes neuronales para clasificación de patrones.

CAPITULO 4. En el cuarto capítulo se presenta la descripción de los distintos algoritmos que permiten a la red, funcionar con mayor eficiencia como clasificadora de patrones, y se presentarán las distintas técnicas de diseño que nos permitirán hallar el mejor modelo de red para la detección de intrusos.

CAPITULO 5. En el quinto capítulo se presenta un problema simple de clasificación de patrones, en el cual se pondrán a prueba los conocimientos obtenidos en la primera parte de adaptación teórica, obteniendo resultados prácticos que nos ayuden a determinar el diseño del problema que estamos tratando agregándole cada vez mayor complejidad, para hacer claros los conceptos del diseño de un sistema de tal magnitud.

CAPITULO 6. En el sexto capítulo se realiza la preparación adecuada de toda la información para el desarrollo final del sistema de detección de intrusos para redes de comunicación, llevando al lector de la mano en cada uno de los pasos que se presentan en esta etapa de diseño de este sistema.

CAPITULO 7. En el séptimo capítulo se describen las pruebas realizadas para comprobar la eficiencia del sistema, haciendo dos tipos de pruebas de distinta naturaleza con cada diseño de *IDS* obtenido en el apartado anterior. De esta manera se obtienen resultados cuantitativos que permiten apreciar la eficiencia del sistema.

CAPITULO 8. El octavo capítulo esta destinado a las conclusiones finales de este proyecto presentando las opciones de trabajo a futuro y analizando los resultados obtenidos en el apartado anterior. La idea general de este proyecto, es que pueda servir como referencia, para que trabajos posteriores puedan reproducir los resultados obtenidos en esta tesis, y partir de esta base para la implementación final del sistema de detección de intrusos.