1. Pendahuluan

1.1 Latar Belakang

Intrusi dalam dunia jaringan komputer merupakan suatu tindakan memasuki suatu sistem komputer tanpa melalui proses otorisasi atau tindakan melebihi batas hak akses [2]. Intrusi di sini dapat diartikan sebagai suatu ancaman atau serangan. Misalnya adanya usaha dari entitas luar untuk masuk dan mengakses sumber daya dalam sebuah jaringan komputer dengan cara yang ilegal, atau usaha untuk merusak jalannya sebuah sistem dalam jaringan komputer yang dapat menyebabkan terganggunya proses bisnis sebuah organisasi.

Intrusion Detection System (IDS) merupakan sebuah *tool* untuk mendeteksi jika terjadi intrusi dalam suatu jaringan komputer, sedangkan *Intrusion Prevention System* (IPS) merupakan pengembangan dari IDS. IPS dapat secara aktif melawan suatu ancaman atau serangan yang ditujukan untuk suatu jaringan komputer dengan cara menghentikan proses penyerangan, sehingga kerusakan aset dalam jaringan komputer dapat dicegah, sedangkan IDS hanya sekedar mendeteksi jika sedang terjadi suatu serangan.

Jaringan Syaraf Tiruan (JST) merupakan salah satu metode dalam ilmu *Artificial Intelligence* yang berupa model matematis untuk meniru cara kerja otak manusia. JST merupakan algoritma non-linier yang telah banyak digunakan untuk memecahkan masalah pengenalan pola. Dalam mengenali suatu pola, JST dapat melakukan generalisasi sehingga dapat mengenali pola baik yang pernah dilatihkan maupun yang belum pernah dilatihkan kepada JST tersebut sebelumnya.

Penggunaan teknik JST dalam deteksi intrusi merupakan sebuah riset yang menjanjikan karena merupakan cara yang efisien untuk meningkatkan performa dari IDS baik yang berbasis *misuse detection* maupun *anomaly detection* [9]. Untuk IDS yang berbasis *misuse detection*, JST dapat digunakan untuk melakukan generalisasi beberapa *signature*, sedangkan untuk IDS yang berbasis *anomaly detection*, JST dapat dimanfaatkan untuk meningkatkan tingkat pengenalan pola terhadap suatu serangan sehingga dapat mengurangi *false-alarm*.

Oleh karena itu, tugas akhir ini membahas tentang desain IPS yang kemampuan deteksi intrusinya ditentukan dari hasil pengolahan dalam JST yang telah melalui proses pelatihan (*training*). JST berperan sebagai komponen penentu atau pendeteksi terjadinya intrusi atau serangan dalam suatu jaringan komputer.

1.2 Perumusan Masalah

Topik permasalahan yang dibahas dalam tugas akhir ini adalah:

1. Bagaimana cara mengimplementasikan JST dalam suatu IPS.
2. Bagaimana bentuk rancangan arsitektur JST dan bagaimana bentuk pola/*signature* yang dipakai untuk input dalam *training* dengan algoritma belajar propagasi balik untuk digunakan dalam IPS
3. Seberapa handal arsitektur JST yang dirancang dalam tugas akhir ini dalam mengklasifikasi mana serangan dan mana yang bukan serangan.

Sedangkan yang menjadi batasan masalah dalam tugas akhir ini adalah :

1. IPS yang dirancang merupakan IPS yang berbasis jaringan kabel (*Network IPS*) .
2. Desain arsitektur JST yang dibangun hanya digunakan untuk membedakan mana serangan dan mana yang bukan serangan. Tidak termasuk menentukan jenis serangan.
3. Paket data yang menjadi input dalam IPS adalah paket data yang menggunakan IP versi 4.
4. Pengujian dilakukan secara *offline* menggunakan dataset berupa hasil *dump* dari *realtime traffic*.
5. Algoritma propagasi balik yang digunakan adalah algoritma propagasi balik yang standar.

1.3 Tujuan

Tujuan dari pembuatan tugas akhir ini adalah :

1. Mengimplementasikan JST dalam suatu IPS.
2. Menentukan bentuk *signature* yang digunakan sebagai input dalam JST.
3. Menentukan dan menguji berbagai macam arsitektur JST dengan algoritma belajar propagasi balik untuk dicoba diimplementasikan dalam IPS.
4. Mengukur dan menganalisis hasil *training* dari beragam arsitektur JST yang telah ditentukan serta implemantasinya dalam IPS dalam mengklasifikasi mana yang merupakan serangan dan mana yang bukan serangan.

1.4 Metodologi Penyelesaian Masalah

Adapun tahap-tahap dalam menyelesaikan masalah ini antara lain :

1. Studi Literatur
   Pada tahap ini dilakukan pencarian beberapa informasi untuk mendukung pengerjaan tugas akhir ini, yaitu :
   - Artikel, tutorial, atau dokumentasi dari IPS terkait yang membahas cara-cara untuk mengimplementasikan JST ke dalam suatu IPS.
   - Artikel atau makalah yang membahas tentang pemanfaatan metode JST dalam pendeteksian intrusi.
   - Buku atau artikel yang membahas tentang JST dan IPS untuk memperdalam pemahaman sehingga desain sistem yang dihasilkan dalam tugas akhir ini bisa optimal.
2. Pengumpulan dan Pengolahan Data
   Data untuk pengujian didapat dari DARPA *Intrusion Detection Dataset*. Dari data tersebut diambil beberapa data yang diperlukan untuk pengujian. Yaitu data berupa rekaman *traffic* jaringan dalam format *tcpdump*.
3. Perancangan Sistem
   Berapa hal yang dirancang dalam tugas akhir ini adalah :
   - Macam-macam Arsitektur JST untuk pengujian.
   - Bentuk *signature* sebagai input JST.
   - Bentuk implementasi JST dalam IPS.
4. Pelatihan
   Pelatihan (*training*) dilakukan pada JST yang telah didesain dengan

menggunakan data *training* hasil dari tahap 2 di atas. Hasil *training* adalah berupa parameter JST yang kemudian diimplementasikan ke dalam IPS.

5. Pengujian
   Pengujian (*testing*) dilakukan terhadap JST hasil *training* dengan menggunakan data *testing* yang didapat dari tahap 2.
6. Analisis
   Analisis dilakukan dari hasil pengujian. Yang menjadi parameter dalam analisis adalah akurasi tingkat pengenalan terhadap serangan dan kemunculan *false alarm* (*false positive* dan *false negative*).
7. Kesimpulan
   Terakhir merupakan kesimpulan apakah arsitektur JST yang telah ditentukan dan bentuk *signature* yang digunakan dalam tugas akhir ini baik digunakan untuk membantu mendeteksi serangan dalam IPS atau tidak.
8. Penulisan Laporan
   Hasil tahapan-tahapan diatas didokumentasikan secara lengkap dalam sebuah laporan yang merupakan *output* utama dalam tugas akhir ini.