IMPLEMENTASI JARINGAN SYARAF TIRUAN DENGAN ALGORITMA BELAJAR PROPAGASI BALIK SEBAGAI PENDETEKSI SERANGAN PADA INTRUSION PREVENTION SYSTEM

IMPLEMENTATION OF ARTFICIAL NEURAL NETWORK WITH BACKPROPAGATION LEARNING ALGORITHM FOR ATTACK DETECTION ON INT

Fuat Yosanto[1], Niken Dwi Cahyani[2], Retno Novi Dayawati[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Intrusi dalam dunia jaringan komputer merupakan suatu tindakan menembus otoritas atau tindakan melebihi hak akses terhadap suatu sistem komputer. Intrusi ini dapat mengancam kelancaran proses bisnis suatu organisasi atau perusahaan. Salah satu solusi untuk mengatasi intrusi ini adalah dengan menggunakan Intrusion Prevention System (IPS). IPS merupakan perkembangan dari Intrusion Detection System. IPS akan merespon suatu kejadian intrusi dengan tindakan yang dapat menghentikan terjadinya intrusi. Dalam tugas akhir ini dibuat suatu implementasi IPS dengan jaringan syaraf tiruan (JST) sebagai komponen penentu terjadinya intrusi atau serangan. JST dalam IPS diimplementasikan dalam bentuk Snort Dynamic Rules. JST memerlukan pelatihan sebelum dapat diimplementasikan kedalam suatu IPS. Proses training dicoba untuk dilaksanakan dengan algoritma belajar propagasi balik standar. Pengujian dilakukan terhadap bermacam-macam arsitektur JST dengan input berupa informasi packet header. Data untuk pelatihan JST diambil dari DARPA Intrusion Detection Dataset. Terakhir beberapa arsitektur JST dengan algoritma belajar propagasi balik ini dianalisis apakah cocok untuk digunakan dalam bidang IPS. Dalam tugas akhir ini ditemukan bahwa arsitektur JST yang diuji belum dapat diimplementasikan secara baik dalam IPS.

Kata Kunci : intrusion prevention system, jaringan syaraf tiruan, propagasi balik.

Abstract

In term of computer network, intrusion is an action to break the authority or to exceed the privilege in computer system. Intrusion can threat the business process work flow in the organization or company. Intrusion Prevention System (IPS) is a solution to overcome this issue. IPS is the successor of Intrusion Detection System. IPS will respond the intrusion event by stopping the intrusion. In this thesis there are IPS developed by implementing artificial neural network (ANN) as the component to determine intrusion/attack. However, the ANN need to be trained before it can be implemented in IPS. Training is conducted by using standard backpropagation learning algorithm. The experiment involves several ANN architecture with packet header information as the input. The training data is taken from DARPA Intrusion Detection Dataset. Finally, the ANN architectures in the experiment are evaluated for the feasibility to be implemented in IPS. This thesis discovered that some ANN architectures in the experiment are not good enough to be implemented in IPS.

Keywords : intrusion prevention system, artificial neural network,backpropagation.

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.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari pengujian dan analisis yang diperoleh, maka kesimpulan yang dapat ditarik adalah sebagai berikut

1. JST dapat diimplementasikan dalam IPS Snort dengan menjadikannya sebagai *Dynamic Rules*.
2. Bentuk *signature* berupa nilai-nilai dalam *packet header* dapat digunakan sebagai input untuk JST untuk deteksi intrusi.
3. Beberapa macam arsitektur JST dalam tugas akhir ini telah ditentukan dan diuji, tetapi belum ditemukan bentuk arsitektur JST yang cukup baik untuk diimplementasikan dalam IPS, karena hasil pengujian dari arsitektur JST yang dibuat dalam tugas akhir ini tidak dapat menunjukkan hasil yang memuaskan.

5.2 Saran

Berikut merupakan saran untuk pengembangan selanjutnya:

1. Perlu dicoba macam-macam arsitektur JST, yang tidak terbatas pada MLP saja untuk menemukan bentuk arsitektur JST yang cocok untuk diimplementasikan dalam IPS.
2. Diperlukan adanya optimasi pada algoritma propagasi balik yang digunakan untuk menghasilkan JST dengan kemampuan generalisasi yang baik dalam deteksi intrusi.
3. Perlu dilakukan kajian lebih lanjut mengenai ruang lingkup klasifikasi bagi JST dalam deteksi intrusi dengan menggunakan informasi paket header sebagai inputnya sehingga dapat memperjelas bagaimana kebutuhan dan tugas yang harus dilakukan JST.

Daftar Pustaka

[1] Anbalagan, E, C. Puttamadappa, E. Mohan, B. Jayaraman, dan Srinivasaro Madane, 2008, "Datamining and Intrusion Detection Using Back-Propagation Algorithm for Intrusion Detection". Medwell Journals International Journal of Soft Computing 3 (4) : 264-270 (tersedia : http://medwelljournals.com/fulltext/ijsc/2008/264-270.pdf).

[2] Baker, Andrew R. dan Joel Esler, 2007, "Snort IDS and IPS Toolkit", Syngress Publishing Inc.

[3] Dao, Vu N.P dan Rao Vemuri, 2002, "A Performance Comparison of Different Back Propagation Neural Networks Methods in Computer Network Intrusion Detection". University of California.

[4] Da Silva, Jacson, 2007, "Redes Neurais Artificiais Para Sistemas de Deteccao de Intrusos"

[5] Desai, Neil, 2003, "Intrusion Prevention System : The Next Step in The Evolution of IDS". (tersedia : http://www.securityfocus.com/infocus/1670 di akses 24 Oktober 2009).

[6] Haykin, Simon, 1994, "Neural Networks: A Comprehensive Foundation", Macmillan Publishing Company: New York

[7] Hermawan, Arif, 2006, "Jaringan Syaraf Tiruan: Teori dan Aplikasi", Penerbit ANDI: Yogyakarta.

[8] Mahoney, Matthew V. dan Philip K. Chan, 2001, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic", Florida Institute of Technology Technical Reports CS-2001-04.

[9] Philipe, Jean, 2001, "Application of Neural Networks to Intrusion Detection", SANS Institute.

[10] Rehman, Rafeeq Ur, 2003, "Intrusion Detection Systems with Snort", Prentice Hall: New Jersey.

[11] Sourcefire, 2009, "Snort Users Manual version 2.8.5". The Snort Project

[12] Suyanto, 2007, "Artificial Intelligence", Penerbit Informatika: Bandung.

[13] Tanenbaum, Andrew S, 2003, "Computer Networks, Fourth Edition", Prentice Hall: New Jersey.

[14] Yoo, InSeon dan Ulrich Ultes-Nitsche, 2002, "An Intelligent Firewall to Detect Novel Attacks", University of Southhampton.