Deteksi Serangan *Denial of Service (DoS)* menggunakan Algoritma *Probabilistic Neural Network* (PNN)

Astri Cahyaningtyas[1], Parman Sukarno[2], Muhammad Arief Nugroho[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]astricahyaningtyas@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]arif.nugroho@telkomuniversity.ac.id

Abstrak

Salah satu masalah keamanan dalam jaringan komputer adalah serangan *Denial of Service* (DoS). Serangan DoS mengakibatkan pengguna dari akses layanan normal tidak dapat mengakses jaringan komputer dikarenakan penyerang mengonsumsi sumber daya yang berlebihan. Hal tersebut terjadi karena deteksi serangan DoS yang masih belum optimal. Untuk menyelesaikan masalah diatas, diusulkan membangun *Intrusion Detection System* (IDS) dengan metode *anomaly-detection* yang menggunakan algoritma *machine learning* yaitu *Probabilistic Neural Network* (PNN) untuk mendeteksi serangan DoS secara optimal. Pada penelitian ini, implementasi PNN dalam mendeteksi serangan DoS menggunakan NSL-KDD dataset dengan 13 fitur pilihan dan menghasilkan nilai akurasi tertinggi daripada algorima lain yaitu sebesar 98,06%.

Kata kunci : Keamanan Jaringan Komputer, *Probabilistic Neural Network* (PNN), *Denial of Service* (DoS).

Abstract

One of the security issue in computer network is Denial of Service (DoS) attack. DoS attack cause users who from normal service can not access network because attacker consumes excessive resources. It happens because the detection of DoS attacks is still not optimal. To solve the problem above, it is recommended to build Intrusion Detection System (IDS) with anomaly-detection that use machine learning algorithms, namely Probabilistic Neural Network (PNN) to improve DoS attacks optimally. In this study, the implementation of PNN for detecting DoS attacks using the NSL-KDD dataset with 13 selected features and produced the highest accuracy value than the other algorithms which is 98,06%.

Keywords: Computer Network Security, Probabilistic Neural Network (PNN), Denial of Service (DoS),

1. Pendahuluan

Latar Belakang

Meskipun ada banyak ancaman aktif di Internet, *Denial of Serangan Service* (DoS) adalah salah satu serangan paling umum di jaringan komputer. Serangan DoS mencegah pengguna dari akses layanan normal, dikarenakan penyerang mengonsumsi sumber daya jaringan komputer, memori, prosesor, dan lain-lain yang berlebihan [1]. Serangan DoS yang paling umum adalah ketika penyerang membanjiri(*flood*) jaringan komputer dengan banyak *request* pada saat bersamaan, membuat server tidak dapat merespon banyak *request* tersebut sehingga mengakibatkan pengguna yang sah tidak dapat berkomunikasi dengan server [1]. *Intrusion Detection System* (IDS) dan teknik pencegahan tradisional, seperti *firewall*, mekanisme kontrol akses, dan enkripsi, memiliki beberapa keterbatasan dalam melindungi jaringan dan sistem komputer dikarenakan serangan-serangan dalam jaringan komputer semakin canggih [12]. Selain itu, sebagian besar sistem yang dibangun berdasarkan teknik-teknik seperti itu memiliki tingkat deteksi positif palsu dan negatif palsu yang tinggi serta kurangnya adaptasi yang terus-menerus terhadap perubahan *malicious behavior* [12].

IDS adalah perangakat keamanan yang digunakan untuk memonitor lalu lintas jaringan komputer atau aktivitas sistem secara *real-time* dan akan mengirimkan peringatan kepada administrator atau mengambil beberapa tindakan aktif setelah serangan diidentifikasi [13]. Ada dua metode dalam melakukan *intrusion detection* yaitu *signatured-based detection* dan *traditional anomaly-based detection*. Kedua metode tersebut masih memiliki kelemahan diantaranya adalah *low intelligence* dan kemampuan adaptasi yang lemah pada skenario aplikasi yang berbeda-beda, serta kesulitan dalam memproses *dataset* yang berukuran sangat besar [13]. Dalam dekade terakhir, beberapa teknik *machine learning* telah diterapkan pada masalah *intrusion detection* dengan harapan dapat meningkatkan tingkat deteksi dan kemampuan beradaptasi [12]. Banyak teknik *machine learning* yang diperkenalkan dalam menangani masalah ini, yang paling banyak digunakan adalah *Artificial Neural Network* (ANN) [13]. Namun,

hasil penelitian menggunakan metode ANN-*based* masih tidak memuaskan dan tingkat ketelitian masih rendah [13].

Pada tugas akhir ini, penulis melakukan penelitian dalam mendeteksi serangan DoS menggunakan algoritma *Probabilistic Neural Network* (PNN). PNN merupakan suatu metode jaringan saraf tiruan (*neural network*) yang menggunakan pelatingan (*training*) *supervised*. Dalam penelitian ini, PNN digunakan untuk klasifikasi dengan dua kategori yaitu kategori normal dan kategori serangan DoS. Penulis memanfaatkan NSL-KDD sebagai *dataset* karena NSL-KDD *dataset* adalah *dataset* terbaik untuk menyimulasikan dan menguji performansi dalam pendeteksian serangan [4].

Topik dan Batasannya

Rumusan masalah dalam penelitian ini adalah karena metode IDS (*signatured-based detection* dan *traditional anomaly-based detection*) masih memiliki keterbatasan yaitu *low intelligence* dan tingkat adaptasi yang lemah, sehingga dibutuhkan metode IDS yang dapat mengalami masalah tersebut. Penelitian ini dilakukan untuk meningkatkan keamanan jaringan komputer dengan cara mendeteksi serangan DoS menggunakan algoritma *Probabilistic Neural Network* (PNN). Untuk menyimulasikan dan menguji performansi algoritma PNN, penulis menggunakan NSL-KDD *dataset* dengan 13 fitur terpilih.

Tujuan

Tujuan penelitian ini untuk meningkatkan keamanan jaringan komputer dengan cara mendeteksi serangan DoS menggunakan algoritma *Probabilistic Neural Network* (PNN). Keterkaitan antara tujuan, pengujian, dan kesimpulan dapat dilihat pada Tabel 1.

Tabel 1. **Keterkaitan antara tujuan, pengujian dan kesimpulan**

No	Tujuan	Pengujian	Kesimpulan
1	Meningkatkan keamanan jaringan komputer dengan cara mengimplementasikan algoritma PNN untuk deteksi serangan DoS dan menghasilkan akurasi.	Algoritma PNN berhasil mendeteksi serangan dengan menggunakan NSL-KDD dataset yang memiliki 113.270 *data train* dan 15.451 *data test*.	Hasil deteksi algoritma PNN memiliki akurasi sebesar 98,06%.

Organisasi Tulisan

Organisasi tulisan pada jurnal tugas akhir ini adalah sebagai berikut. Bab 1 mendeskripsikan pendahuluan yang berisi latar belakang, topik dan batasannya, tujuan, dan organisasi tulisan. Bab 2 membahas tentang studi terkait yang mendukung penulisan atau pengerjaan tugas akhir. Bab 3 memberikan penjelasan sistem yang dibangun. Hasil evaluasi yang menjadi tujuan dari penelitian ini ada di dalam Bab 4. Di akhir jurnal terdapat Bab 5 yang menarik kesimpulan dari penelitian ini.

2. Studi Terkait

Untuk memecahkan masalah *network security* diperlukan *intrussion detection*. *Intrusion detection* adalah suatu proses monitoring kejadian yang terjadi pada sistem atau jaringan komputer serta menganalisisnya untuk mengetahui aktivitas tersebut termasuk normal atau intrusi [5]. Metode *intrusion detection* diklasifikasikan menjadi tiga kategori: *Signature-based Detection* (SD), *Anomaly-based Detection* (AD) dan *Stateful Protocol Analysis* (SPA). *Signature-based* (SD) adalah *pattern* yang sesuai dengan serangan atau ancaman yang diketahui dengan cara membandingkan *pattern* terhadap peristiwa yang ditangkap untuk mengenali kemungkinan intrusi, *signature-based* juga dikenal dengan *Knowledgebased Detection* atau *Misuse Detection* karena menggunakan *knowledge* yang diakumulasikan oleh serangan dan *vulnerability* yang spesifik [5]. *Anomaly-based detection* (AD) atau yang disebut dengan *Behavior-based detection* adalah penyimpangan perilaku yang diketahui, dan profil mewakili normal atau ekspektasi perilaku yang berasal dari monitoring aktivitas reguler, koneksi jaringan komputer, host atau pengguna selama periode waktu tertentu [5]. Profil dapat berupa statis atau dinamis, dan dikembangkan untuk banyak atribut seperti upaya login yang gagal, penggunaan processor, jumlah email yang dikirim, dan lain-lain [5]. Kemudian, AD membandingkan profil normal dengan peristiwa yang diamati untuk mengenali serangan signifikan[5]. *Anomaly-detection* mengalami peningkatan popularitas karena menjadi efektif terhadap serangan baru yaitu dengan memanfaatkan algortima *machine learning* [2]. Ada banyak algoritma klasifikasi dalam *machine learning* yang dilatih dan digunakan untuk deteksi serangan dalam jaringan komputer, untuk lebih meningkatkan kinerja