ISSN: 2087-1716
Jurnal Ilmiah ILKOM Volume 8 Nomor 3 (Desember 2016)

ANALISIS STATISTIK LOG JARINGAN UNTUK DETEKSI SERANGAN DDOS BERBASIS NEURAL NETWORK

Arif Wirawan Muhammad[1], Imam Riadi[2], Sunardi[3]
[1]arif1508048009@webmail.uad.ac.id, [2]imam.riadi@mti.uad.ac.id, [3]sunardi@mti.uad.ac.id
[1]Universitas Ahmad Dahlan Yogyakarta

Abstrak

Distributed denial-of-service (DDoS) merupakan jenis serangan dengan volume, intensitas, dan biaya mitigasi yang terus meningkat seiring berkembangnya skala organisasi. Penelitian ini memiliki tujuan untuk mengembangkan sebuah pendekatan baru untuk mendeteksi serangan DDoS, berdasarkan log jaringan yang dianalisis secara statistik dengan fungsi *neural network* sebagai metode deteksi. Data pelatihan dan pengujian diambil dari CAIDA DDoS Attack 2007 dan simulasi mandiri. Pengujian terhadap metode analisis statistik terhadap log jaringan dengan fungsi neural network sebagai metode deteksi menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, dan DDoS) sebesar 90,52%. Adanya pendekatan baru dalam mendeteksi serangan DDoS, diharapkan bisa menjadi sebuah komplemen terhadap sistem *Intrusion Detection System* (IDS) dalam meramalkan terjadinya serangan DDoS.

Kata kunci: DDoS, *Neural Network*, Log Jaringan.

1. Pendahuluan

Distributed denial-of-service (DDoS) merupakan jenis serangan yang telah ada sejak tahun 1990, dimana volume dan intensitas DDoS terus meningkat. Pada akhir tahun 2014, dilaporkan bahwa serangan DDoS merupakan teknik serangan yang paling populer [1]. Dengan demikian, DDoS merupakan salah satu ancaman utama dunia maya dan menjadi masalah utama keamanan *cyber*. DDoS disebut sebagai senjata pilihan *hacker* karena telah terbukti menjadi ancaman permanen bagi pengguna, organisasi dan infrastruktur di Internet. Di sisi lain, serangan jaringan merupakan risiko untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi [2].

Deteksi dini serangan DDoS adalah proses fundamental yang dilakukan secara otomatis oleh *Intrusion Detection System* (IDS). IDS yang ada sekarang ini pada umumnya menggunakan teknik deteksi yang jauh dari sempurna jika dibandingkan dengan teknik serangan *cyber* yang semakin modern [3]. Sistem IDS pada umumnya hanya memantau dan memberikan penanda terhadap aktivitas jaringan yang mencurigakan dan langsung dilaporkan sebagai alert, sehingga memberikan dampak adanya volume alert yang terlalu besar dengan tingkat rata-rata false-positive yang tinggi. Hal itu disebabkan karena lalu lintas data jaringan merupakan sesuatu yang bersifat non-stasioner [4]

Pengenalan pola serangan DDoS pada IDS memiliki dua kelemahan. Pertama, karena defisit TCP/IP. Bagi hacker, serangan DDoS sangat mudah untuk dimulai, sementara korban sulit untuk menyadari. Selain itu, serangan DDoS mengalami perkembangan teknik yang mutakhir sebagai contoh adalah serangan SYN-*Flood*. Secara umum sebuah paket tunggal SYN, merupakan paket yang bersifat legal pada aktivitas jaringan sehingga sulit dideteksi sebagai artefak abnormal oleh IDS, sehingga IDS cukup sulit untuk membangkitkan *alert* apakah jaringan sedang diserang oleh SYN-*Flood*. Kedua, adanya masalah *alert* bersifat *false-positive* yang sering terjadi pada IDS yang berbasis *signature,* dimana pola jaringan normal dideteksi sebagai serangan DDoS, sehingga ketika benar-benar terjadi serangan DDoS waktu untuk menentukan dan melakukan tindakan mitigasi secara cepat untuk mengamankan jaringan tidak bisa dilaksanakan seefisien mungkin [5].

Penelitian ini memiliki tujuan untuk mengembangkan sebuah pendekatan baru yang dapat mendeteksi serangan DDoS secara efisien, berdasarkan pada analisis statistik terhadap log aktivitas jaringan menggunakan metode *neural network* sebagai fungsi deteksi. Data pelatihan dan pengujian diambil dari CAIDA DDoS Attack 2007 dan simulasi mandiri. Penelitian yang akan dilaksanakan diharapkan mampu menjawab :

1. Bagaimana cara memanfaatkan analisis statistik yang ditunjang dengan metode *neural network* sebagai metode deteksi serangan DDoS berdasarkan pada log aktivitas jaringan.
2. Bagaimana performa deteksi serangan DDoS yang didasarkan pada analisis statistik terhadap log aktivitas jaringan menggunakan metode *neural network* sebagai fungsi deteksi berdasarkan data pelatihan dan pengujian.

2. Landasan Teori

Penelitian mengenai deteksi serangan DDoS dengan menganalisis nilai entropi artefak jaringan dalam kondisi jaringan normal dan abnormal yang dipengaruhi oleh DoS, *port scanning* dan *worm* menghasilkan kesimpulan bahwa nilai entropi dari artefak jaringan saling berkorelasi [6]. Penelitian [7] memanfaatkan fungsi entropi maksimal untuk membangun angka distribusi jaringan yang normal dan kemudian menggunakan entropi relatif untuk mendeteksi anomali/serangan DDoS.

Penelitian [8] menggunakan model distribusi jaringan yang didasarkan pada atribut TCP/IP sehingga menghasilkan kombinasi atribut yang cukup besar. Paket data artefak jaringan harus diberi label dan diurutkan sehingga langkah preprocessing menjadi kompleks dan menurunkan kemampuan untuk mendeteksi serangan DDoS secara cepat. Metode *K-Means Clustering* juga digunakan untuk mengklasifikasikan serangan DDoS, dengan menggunakan fitur deteksi yaitu protokol TCP, UDP, Flag, nomor port, dan menghasilkan tingkat pengenalan yang baik [9].

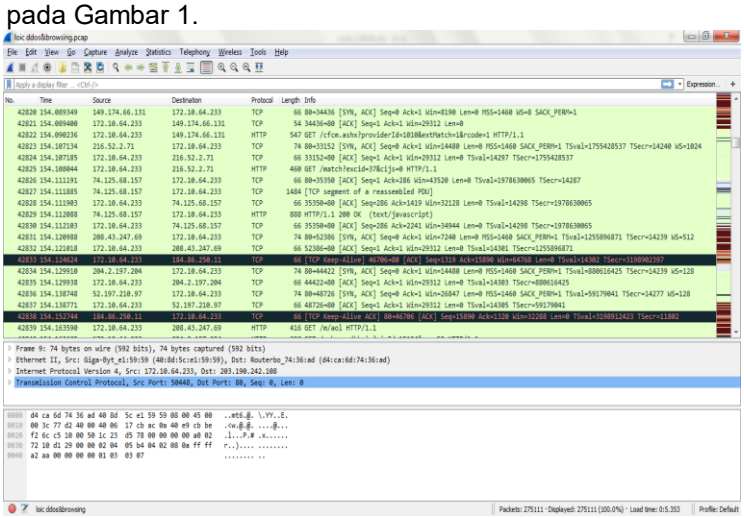
Metode *neural network* secara *unsupervised learning* dan algoritma EM telah digunakan untuk mendeteksi adanya serangan DDoS pada penelitian [10] berdasarkan dataset DARPA untuk membentuk suatu *alert cluster* dan menghasilkan kesimpulan bahwa terjadi penurunan jumlah *cluster* serangan dimana pada awalnya berdasarkan dataset DARPA terdapat 21 cluster serangan, ternyata hanya bisa dikelompokkan menjadi 13 cluster serangan, sehingga terdapat kesalahan pemisahan di mana alert dari jenis serangan yang sama dikelompokkan menjadi *cluster* yang berbeda. Sementara penelitian [11] mendeteksi adanya serangan DDoS dengan teknik SVM-RIPPER untuk menghasilkan *alert cluster*. Dan memberikan kesimpulan bahwa teknik SVM-RIPPER mampu untuk menghasilkan *alert cluster* dalam deteksi serangan DDoS dengan baik. Penelitian [12] membuktikan bahwa metode *neural network* mampu digunakan untuk mendeteksi serangan DDoS yang bersifat serangan jenis baru, dan dapat digunakan dalam lingkungan Hadoop dan Hbase.

Berdasarkan penelitian terdahulu yang telah dipaparkan, maka diusulkan sebuah pendekatan baru dalam mendeteksi serangan DDoS dengan memanfaatkan analisis statistik terhadap log aktivitas jaringan dengan metode neural network sebagai fungsi deteksi. Adanya pendekatan baru dalam mendeteksi serangan DDoS diharapkan bisa menjadi komplemen IDS dalam mengamankan jaringan dari serangan DDoS.

3. Metode

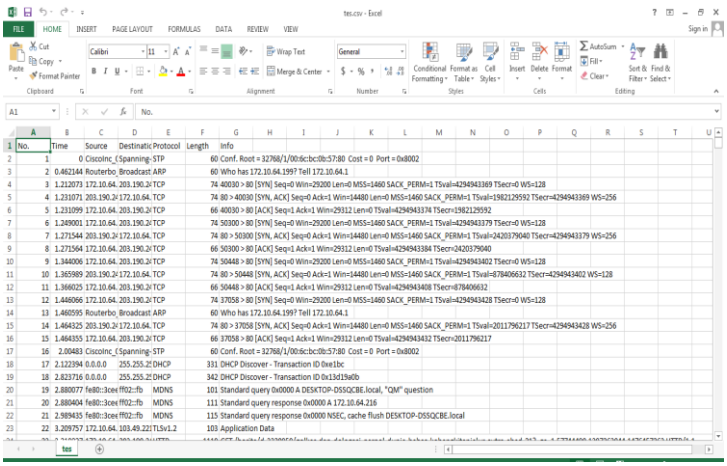
Metode penelitian yang akan dilaksanakan dibagi menjadi beberapa tahapan sebagai berikut :

1. Pengambilan log dari simulasi serangan jaringan menggunakan LOIC dan dataset DDoS yang diterbitkan oleh CAIDA DDoS Attack 2007 (UCSD, 2007) dalam bentuk format .pcap. Seperti yang tersaji pada Gambar 1.



Gambar 1. Pengambilan Log.

2. Ekstraksi log. Yaitu mengubah bentuk file .pcap menjadi bentuk .csv sehingga data log dapat diolah lebih lanjut. Seperti yang tersaji pada Gambar 2.



Gambar 2. Ekstraksi Log

3. Kuantifikasi dari ekstraksi log secara statistik secara *fixed moving average window* selama lima detik, sebagai input *neural network*. Karakteristik aktivitas jaringan yang dihasilkan dari kuantifikasi secara statistik terhadap log aktivitas jaringan adalah sebagai berikut :

    a. Rata-Rata Ukuran/Panjang Paket. Merupakan nilai yang menyatakan rata-rata ukuran/panjang dalam satu *window/frame* waktu tertentu.
    b. Jumlah Paket. Merupakan total paket dalam satu *window/frame* waktu tertentu.
    c. Variansi Waktu Kedatangan Paket. Merupakan nilai akar dari deviasi waktu kedatangan paket, yang dinyatakan dengan rumus pada persamaan 1

$$Variansi\ waktu = \sqrt{\frac{\sum(tn-\bar{t})^2}{n}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

tn = waktu paket diterima
$\bar{t}$ = rata-rata waktu paket diterima

    d. Variansi Ukuran/Panjang Paket. Merupakan nilai akar dari deviasi ukuran/panjang paket, yang dinyatakan dengan rumus pada persamaan 2.

$$Variansi\ ukuran = \sqrt{\frac{\sum(pn-\bar{p})^2}{n}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

pn = panjang paket diterima
$\bar{p}$ = rata-rata panjang paket diterima

    e. Kecepatan Paket/Detik. Merupakan banyaknya aliran paket data dalam satu window/frame waktu tertentu, yang dihitung dengan rumus pada persamaan 3.

$$Kecepatan\ paket = np * \frac{1}{T.akhir - T.awal} \quad \ldots\ldots\ldots\ldots\ldots (3)$$

Dengan np = jumlah paket
T.akhir = waktu akhir paket diterima
T.awal = waktu awal paket diterima

    f. Jumlah Bit. Merupakan jumlah total bit data yang terdapat dalam satu *window/frame* waktu tertentu.

4. Membentuk jaringan *neural network*.
5. Melakukan pelatihan terhadap *neural network* menggunakan 30% data dari hasil analisis statistik log aktivitas jaringan.
6. Melakukan pengujian terhadap *neural network* menggunakan 70% data dari hasil analisis statistik log aktivitas jaringan.
7. Menganalisis untuk kerja deteksi serangan DDoS dari metode yang diterapkan.

4. Hasil

Keenam karakteristik aktivitas jaringan yang dihasilkan dari analisis statistik log aktivitas jaringan digunakan sebagai *input* dari *neural network* yang memiliki pola tiga *hidden layer* dan satu *output layer*. Output dari *neural network* adalah tiga kondisi yang mewakili kondisi jaringan yaitu kondisi normal yang diwakili angka 1 (satu), *slow* DDoS yang diwakili angka 2 (dua), dan DDoS yang diwakili angka 3 (tiga).

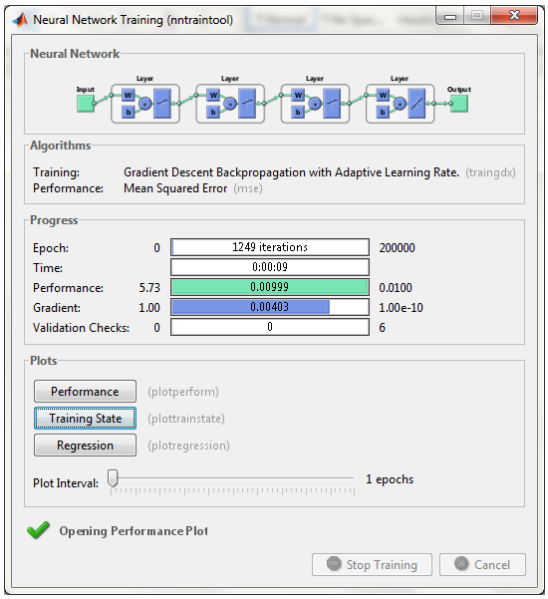
Dalam *hidden layer* pada layer pertama dan kedua memiliki tiga belas neuron dan layer ketiga memiliki enam neuron. Sedangkan *output* layer memiliki satu neuron. Secara ringkas, layer dan fungsi aktivasinya tersaji pada Tabel 1.

Tabel 1. Layer dan Fungsi Aktivasi

No	Layer	Jumlah Neuron	Fungsi Aktivasi
1.	Input	6	-
2.	Hidden-1	13	Logsig
3.	Hidden-2	13	Logsig
4.	Hidden-3	6	Logsig
5.	Output	1	Purelin

Neural network yang digunakan menggunakan pelatihan *backpropagation* dengan fungsi *traingdx* dan memiliki konfigurasi sebagai berikut :

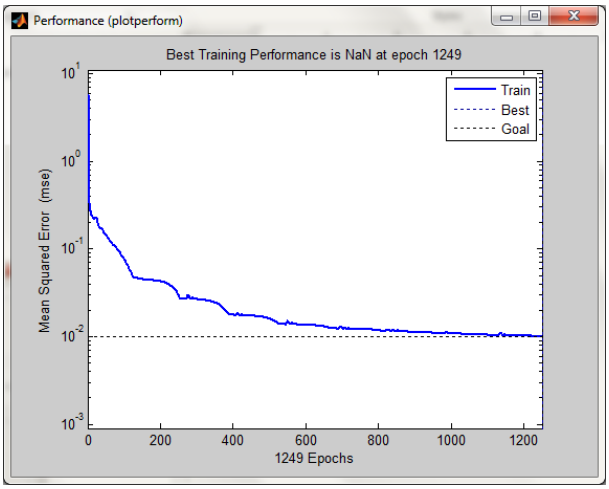
1. Epoch = 200000.
2. Learning rate = 0,5.
3. Momentum = 0,95.
4. Goal Mean Square Error (MSE) = 0,01.



Gambar 3. Hasil Pelatihan *Neural Network*

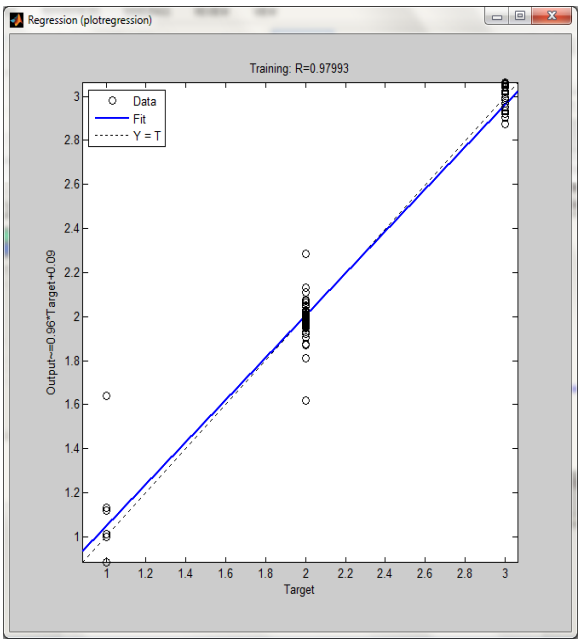
Hasil pelatihan *neural network* tersaji pada Gambar 3, terlihat dimana nilai minimal dari *mean square error (*MSE) yang telah ditetapkan sebesar 0,01, tercapai pada *epoch* 1249 dengan gradien sebesar 0,00403.

Sehingga dapat disimpulkan bahwa neural network telah mencapai kondisi maksimal dalam pelatihannya, sebagaimana yang tersaji pada grafik performa neural network pada Gambar 4.



Gambar 4. Grafik Performa *Neural Network*

Dari hasil pelatihan jaringan didapatkan plot regresi dengan nilai R sebesar 0,97993 seperti yang tersaji pada Gambar 5. Yang berarti bahwa bobot-bobot pada *neural network* berhasil memberikan hasil optimal dalam pengenalan pola data *input.*



Gambar 5. Grafik Regresi *Neural Network*

Setelah dilaksanakan pelatihan terhadap *neural network*, maka selanjutnya menguji *neural network* dengan data uji, dan didapatkan prosentase rata-rata pengenalan terhadap tiga kondisi serangan DDoS sebesar 90,52%, seperti yang tersaji pada Tabel 2.

Tabel 2. Hasil Pengujian *Neural Network*

No	Kondisi	Data Uji	Error	Prosentase Pengenalan
1.	Normal	14	2	85,71%
2.	Slow DDoS	152	7	95,39%
3.	DDoS	42	4	90,47%
Rata-Rata Pengenalan				90.52%

Prosentase pengenalan yang dihasilkan berada diatas 90%. Hal ini menunjukkan bahwa pendekatan baru dalam mendeteksi serangan DDoS dengan memanfaatkan analisis statistik terhadap log aktivitas jaringan dengan metode neural network sebagai fungsi deteksi mampu mengenali serangan DDoS dengan baik. Untuk menghasilkan tingkat pengenalan yang lebih baik lagi, maka ada beberapa parameter yang dapat dioptimasi, antara lain :

1. Memperbanyak jumlah data pelatihan.
2. Optimasi jumlah *neuron* dan *hidden layer* pada *neural network.*
3. Konfigurasi pelatihan *neural network* (*momentum, learning rate, epoch, dan goal MSE*).
4. Penyesuaian fungsi pelatihan, dan fungsi aktivasi *layer neural network*.

.

5. Kesimpulan dan saran

Pendekatan baru yang diusulkan dalam mendeteksi serangan DDoS dengan metode neural network dengan fungsi fixed moving average window (FMAW) menghasilkan prosentase rata-rata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, Dan DDoS) sebesar 90,52%. Prosentase pengenalan yang dihasilkan berada diatas 90%. Hal ini menunjukkan bahwa pendekatan baru dalam mendeteksi serangan DDoS dengan memanfaatkan analisis statistik terhadap log aktivitas jaringan dengan metode neural network sebagai fungsi deteksi mampu mengenali serangan DDoS dengan baik. Untuk menghasilkan tingkat pengenalan yang lebih baik lagi, maka ada beberapa parameter yang dapat dioptimasi yaitu, memperbanyak jumlah data pelatihan, optimasi jumlah neuron dan hidden layer pada neural network, konfigurasi pelatihan neural network (momentum, learning rate, epoch, dan goal mean square error), penyesuaian fungsi pelatihan, dan fungsi aktivasi layer neural network. Diharapkan dengan adanya pendekatan baru dalam mengenali serangan DDoS bisa menjadi sebuah komplemen terhadap sistem IDS yang telah untuk meminimalisir serangan DDoS pada sebuah jaringan.

.

Daftar Pustaka

[1] Arbor Networks, “Worldwide Infrastructure Security Report,” vol. IX, pp. 1–83, 2014.

[2] W. Hurst, N. Shone, and Q. Monnet, “Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures,” 2015.

[3] T. Ishitaki, D. Elmazi, Y. Liu, T. Oda, L. Barolli, and K. Uchida, “Application of Neural Networks for Intrusion Detection in Tor Networks,” *Proc. - IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2015*, pp. 67–72, 2015.

[4] J. Wu, X. Wang, X. Lee, and B. Yan, “Detecting DDoS attack towards DNS server using a neural network classifier,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6354 LNCS, no. PART 3, pp. 118–123, 2010.

[5] E. Balkanli, J. Alves, and A. N. Zincir-Heywood, “Supervised Learning to Detect DDoS Attacks,” *IEEE Int. Conf. Adv. Comput. Commun. Informatics*, 2014.

[6] A. M. Chandrasekhar and K. Raghuveer, “Intrusion Detection Technique by Using K-Means, Fuzzy Neural Network and SVM Classifiers,” *2013 Int. Conf. Comput. Commun. Informatics*, pp. 1–7, 2013.

[7] A. Olabelurin, S. Veluru, A. Healing, and M. Rajarajan, “Entropy Clustering Approach for Improving Forecasting in DDoS Attacks,” 2015.

[8] W. Gautama, Y. Purwanto, and T. W. Purboyo, “Anomali Trafik, DDoS, Flash Crowd, Isodata, Clustering, Manhattan Distance, Dunn Index,” *Int. J. Appl. Inf. Technol.*, pp. 1–8, 2016.

[9] A. Iswardani and I. Riadi, “Denial of Service Log Analysis Using Density K- Means Method,” *J. Theor. Appl. Inf. Technol.*, no. April, 2016.

[10] R. Smith, N. Japkowicz, M. Dondo, and P. Mason, “Using Unsupervised Learning for Network Alert Correlation,” *Univ. Ottawa Canada*, 2008.

[11] A. Saied, R. E. Overill, and T. Radzik, “Detection of Known and Unknown DDoS Attacks Using Artificial Neural Networks,” *J.M. Corchado al. PAAMS 2014 Work.*, vol. 172, pp. 385–393, 2015.

[12] T. Zhao, D. C. T. Lo, and K. Qian, “A Neural Network Based DDoS Detection System Using Hadoop and HBase,” *Proc. - 2015 IEEE 17th Int. Conf. High Perform. Comput. Commun. 2015 IEEE 7th Int. Symp. Cybersp. Saf. Secur. 2015 IEEE 12th Int. Conf. Embed. Softw. Syst. H*, pp. 1326–1331, 2015.