INTEGRASI METODE NORMALIZED RELATIVE NETWORK ENTROPY DAN NEURAL NETWORK BACKPROPAGATION (BP) UNTUK DETEKSI DAN PERAMALAN SERANGAN DDoS

Imam Riadi, Sunardi, Arif Wirawan Muhammad
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
Email: imam.riadi@mti.ac.id

Abstrak – ***Distributed denial-of-service (DDoS) merupakan jenis serangan dengan volume dan intensitas DDoS terus meningkat dengan biaya mitigasi yang terus meningkat seiring berkembangnya skala organisasi. Penelitian ini memiliki tujuan untuk mengembangkan sebuah pendekatan baru untuk mendeteksi dan membentuk cluster jenis serangan DDoS, berdasarkan pada karakteristik aktivitas jaringan dengan mengintegrasikan metode Normalized Relative Network Entropy (NRNE) sebagai estimator awal terhadap anomali aktivitas jaringan, dan metode Neural Network Backpropagation (BP) sebagai fungsi supervised learning terhadap pola anomali berdasarkan output dari NRNE. Data training yang digunakan dalam adalah log file dari KDD Cup 1999 yang diterbitkan oleh DARPA. Untuk pengujian real-world attack, digunakan data yang diterbitkan oleh CAIDA 2007. Pengujian simulation attack digunakan software DDoS Generator. Pengujian normal traffic digunakan data CAIDA 2011. Adanya pendekatan baru dalam mendeteksi serangan DDoS, diharapkan bisa menjadi sebuah komplemen terhadap sistem IDS dalam meramalkan terjadinya serangan DDoS.***

Kata Kunci – ***DDoS, Entropy, Neural Network, IDS, Supervised Learning***

I. PENDAHULUAN

Distributed denial-of-service (DDoS) merupakan jenis serangan yang telah ada sejak tahun 1990-an, dimana volume dan intensitas DDoS terus meningkat. Pada akhir tahun 2013, dilaporkan [1] bahwa serangan DDoS merupakan teknik serangan yang paling populer untuk tahun tersebut. Dengan demikian, berdasarkan informasi tersebut memantapkan DDoS sebagai ancaman utama dunia maya dan merupakan masalah utama keamanan cyber. DDoS sekarang disebut sebagai "senjata pilihan" hacker [2] 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 [3].

Skala dan biaya untuk menanggulangi serangan dalam bisnis dunia maya naik hampir dua kali lipat dibandingkan dengan tahun sebelumnya, studi dari Arbor Network dan Akamai [4] menguatkan dugaan bahwa menghentikan DDoS adalah mustahil. Pada studi tersebut terungkap bahwa mitigasi dari serangan DDoS yang ada sekarang ini justru membuat perusahaan/organisasi sasaran DDoS tetap berada dalam plan yang telah direncanakan hacker, karena antara serangan dan plan mitigasi sangat berkaitan erat.

Deteksi dini serangan DDoS adalah proses fundamental yang dilakukan secara otomatis oleh System Intrusion Detection (IDS). Intrusion Detection System (IDS) yang ada sekarang ini pada umumnya menggunakan teknik deteksi yang jauh dari sempurna jika dibandingkan dengan teknik serangan cyber yang semakin modern [5][6][7][8]. Sistem IDS 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 tinggi. Hal itu disebabkan karena lalu lintas data data jaringan merupakan sesuatu yang bersifat non-stasioner [9].

II. JARINGAN SYARAF TIRUAN

Jaringan syaraf tiruan merupakan suatu sistem pemrosesan informasi yang memiliki karakteristik sama dengan sistem jaringan saraf biologi. Pada dasarnya JST mencoba meniru cara kerja otak manusia, khususnya neuron. JST mempunyai karakteristik yang dimiliki oleh otak manusia, diantaranya adalah kemampuan untuk belajar dari pengalaman.

Semua keluaran atau kesimpulan yang ditarik oleh jaringan didasarkan pada pengalamannya selama mengikuti proses pembelajaran/pelatihan. Hal yang ingin dicapai dengan melatih jaringan saraf tiruan adalah untuk mencapai keseimbangan antara kemampuan memorisasi dan generalisasi. Kemampuan memorisasi adalah kemampuan jaringan saraf tiruan untuk mengambil kembali secara sempurna sebuah pola yang telah dipelajari, dan kemampuan generalisasi adalah untuk menghasilkan respons yang bisa diterima terhadap pola-pola input yang serupa (namun tidak identik) dengan pola-pola yang sebelumnya telah dipelajari.

ISBN: 978-602-19568-1-6

Jaringan saraf tiruan memiliki beberapa arsitektur jaringan yang digunakan dalam berbagai aplikasi, arsitektur jaringan saraf tiruan tersebut, antara lain single layer network, multilayer network, multilayer network dengan umpan balik dan recurrent network. Arsitektur jaringan multilayer network, yang memiliki 3 jenis layer, yaitu layer input, layer output dan hidden layer. Setiap unit di dalam layer input pada jaringan backpropagation selalu terhubung dengan setiap unit yang berada pada layer tersembunyi. Demikian juga setiap unit pada layer tersembunyi selalu terhubung dengan unit pada layer output.

Aturan pelatihan jaringan backpropagation terdiri dari 2 tahapan, feedforward dan backward propagation. Algoritma pelatihan jaringan backpropagation terdiri dari 3 tahapan, yaitu:

1. Tahap umpan maju (feedforward)
2. Tahap umpan mundur (backpropagation)
3. Tahap peng-update-an bobot dan bias

A. *Entropy*

Entropy adalah konsep keacakan, di mana terdapat suatu keadaan yang tidak dapat dipastikan kemungkinannya.

Entropy timbul jika prediktabilitas/kemungkinan rendah (low predictable) dan informasi yang ada tinggi (high information). Informasi adalah sebuah ukuran ketidakpastian, atau entropy, dalam sebuah situasi. Semakin besar ketidakpastian, semakin besar informasi yang tersedia dalam proses komunikasi. Ketika sebuah situasi atau keadaan secara lengkap dapat dipastikan kemungkinannya atau dapat diprediksikan (highly predictable), maka entropy informasi tidak ada sama sekali. Kondisi inilah yang disebut dengan negentropy. Entropi dirumuskan seperti pada persamaaan 1.

$$\mathrm{H(P)} = \sum_{i=1}^{n} P(x_i) \log P(x_i) \qquad (1)$$

B. *Relative Network Entropy*

Penelitian [10] memperkenalkan metode *bernama relative entropy* atau yang biasa disebut Kullback-Leibler(KL), yang mana mempu memberikan perhitungan terhadap perbedaan diantara dua distribusi probabilitas. Yang dirumuskan pada persamaan 2.

$$D(P \| Q) = \sum_{i=1}^{n} P(x_i) \log \frac{P(x_i)}{Q(x_i)} \qquad (2)$$

C. *Normalized Relative Network Entropy*

Penelitian [11] menyempurnakan metode Relative Network Entropy menjadi Normalized Relative Network Entropy (NRNE), dengan alasan bahwa metode relative Network Entropy kurang mampu untuk mendeteksi anomali dalam traffic jaringan yang memiliki dimensi protokol data yang besar. Dengan metode NRNE penelitian [11] memberikan hasil optimal dalam mendeteksi DDoS. NRNE dianalogikan dengan konsep varians. Sebagaimana terlihat pada Tabel 1.

Tabel 1. Konsep NRNE

The Variance	Normalized Relative Network Entropy(NRNE)
$\bar{x}$:the average value	Q_j :The distribution of attribute j
$(x_i - \bar{x})^2$:the square deviation	$D(P_j \| Q_j) = \sum_{i=1}^{n} P(x_i) \log \frac{P(x_i)}{Q_j(x_i)}$: The relative entropy of attribute j
$\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2$:the variance	$\frac{1}{n}\sum_{j=1}^{n}\sum_{i=1}^{n} P(x_i) \log \frac{P(x_i)}{Q_j(x_i)}$:The NRNE on all attributes

III. METODE PENELITIAN

Penelitian ini memiliki tujuan untuk mengembangkan sebuah pendekatan baru yang dapat mendeteksi serangan DDoS secara efisien, berdasarkan pada karakteristik aktivitas jaringan menggunakan metode Normalized Relative Network Entropy (NRNE) sebagai estimator awal terhadap anomali aktivitas jaringan, dan metode Neural Network BP sebagai fungsi supervised learning terhadap pola anomali berdasarkan output dari NRNE serta menganalisis performa integrasi dua metode tersebut dengan cara menguji dengan real-world attack, ,simulation attack dan normal traffic, sehingga didapatkan nilai false-positive rate. Data training yang digunakan dalam penelitian adalah log file dari KDD Cup 1999 yang diterbitkan oleh DARPA [12]. Untuk pengujian real-world attack, digunakan data yang diterbitkan oleh CAIDA 2007 [13]. Pengujian simulation attack digunakan software DDoS Generator [14] yang dilaksanakan di Laboratorium Fakultas Teknik Elektro UAD (LFTE-UAD). Pengujian normal traffic difunakan data CAIDA 2011 [15].

Penelitian yang akan dilaksanakan diharapkan mampu menjawab :

1. Bagaimana cara menerapkan metode Normalized Relative Network Entropy (NRNE) untuk mendeteksi anomali jaringan dalam serangan DDoS,
2. Bagaimana cara menerapkan metode Neural Network BP sebagai proses lanjutan dari hasil output NNRE,
3. Bagaimana nilai *false-positive rate* dari proses deteksi yang menggunakan kombinasi metode Normalized Relative Network Entropy dan Neural Network BP, jika dibandingkan dengan metode lain yang telah ada.

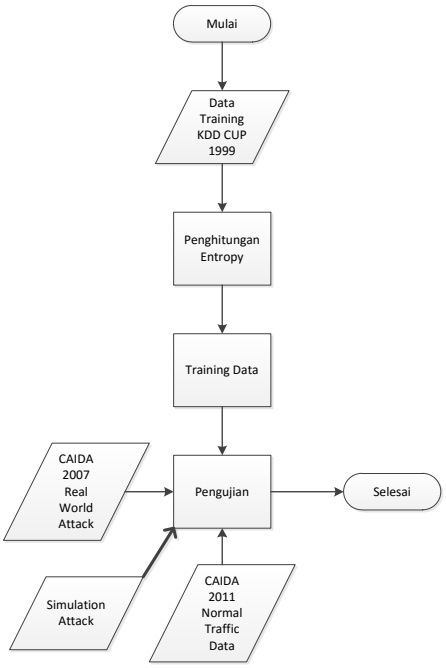
Dengan adanya pengujian performa dari pendekatan baru yang telah dipaparkan, maka diharapkan bisa menjadi solusi dalam proses deteksi dan peramalan adanya serangan DDoS.

ISBN: 978-602-19568-1-6

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

1. Pengambilan data, dari KDD Cup 1999 yang diterbitkan oleh DARPA.
2. Analisis awal data yang dilaksanakan dengan cara mencari nilai entropi yang terdapat pada log lalu lintas jaringan sebagai estimator awal anomali
3. Mengolah nilai entropi menggunakan Neural Network BP.
4. Pengujian hasil training Neural Network BP menggunakan data real-world attack yang diterbitkan oleh CAIDA 2007.
5. Pengujian hasil training Neural Network BP menggunakan data simulation-attack menggunakan software DDoS Generator.
6. Pengujian hasil training Neural Network BP dengan data CAIDA 2011.
7. Analisis akhir untuk menjelaskan kinerja metode yang digunakan yang ditandai dengan nilai false-positive rate dalam mendeteksi DDoS.

Diagram prosedur penelitian tersaji pada Gambar 2.



Gambar 2. Prosedur Penelitian

IV. HASIL DAN PEMBAHASAN

Pengenalan pola serangan DDoS pada IDS memiliki dua kelemahan. Pertama, karena defisit TCP/IP [12]. 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 misalnya, merupakan paket yang bersifat legal pada aktivitas jaringan yang sulit dideteksi sebagai pola abnormal oleh metode pengenalan pola IDS pada umumnya, sehingga IDS cukup sulit untuk membangkitkan alert apakah jaringan sedang diserang oleh Syn-Flood. Kedua, adanya masalah false-positif yang sering terjadi pada IDS yang berbasis signature. Sehingga memakan waktu untuk menentukan dan melakukan tindakan mitigasi secara cepat untuk mengamankan jaringan.

Penelitian [16] [17] [18] menganalisis entropi paket yang memiliki atribut berbeda dalam kondisi normal dan kondisi abnormal. Kondisi abnormal dipengaruhi oleh jenis serangan yang berbeda, seperti DoS, port scanning dan worm. Penelitian [16] telah menghasilkan kesimpulan lebih lanjut bahwa entropi nilai-nilai atribut yang berbeda sangat berkorelasi. Penelitian [16] memanfaatkan nilai entropi maksimal untuk membangun dasar nilai distribusi jaringan yang normal dan kemudian menggunakan entropi relatif untuk mendeteksi anomali. Namun, dalam penelitian [10] model distribusi awal yang digunakan didasarkan pada atribut TCP/IP saja yang berarti kombinasi atribut yang berbeda yang besar. Selain itu, paket data yang dihasilkan dari sniffing harus diberi label dan diurutkan sesuai dengan fitur mereka. Kompleksnya preprocessing yang dlaksanakan menurunkan kemampuan untuk mendeteksi anomali secara cepat.

Penelitian [19] menyebutkan bahwa output dari IDS dianggap kurang bagus jika satu jenis serangan saja dapat menimbulkan beberapa jenis *alert*. Sedangkan pada umumnya IDS menghasilkan volume *alert* yang cukup tinggi [20]. Sehingga para peneliti mengusulkan perlunya agregasi informasi dan korelasi dari *alert* tersebut. Menurut penelitian [20] teknik agregasi informasi tersebut disebut sebagai post-IDS analisis, dengan kondisi:

1. Adanya alert dalam jumlah besar.
2. Heterogenitas alert.
3. Alert palsu dan insiden yang belum dikenal sebelumnya.
4. Sulitnya menghubungkan/mencari relasi alert aktual dengan alert sebelumnya.
5. Tidak adanya tingkat keandalan dan prioritas peringatan.

Tantangan di atas membuat investigasi, analisis forensik digital, dan mitigasi memakan waktu dan rawan kesalahan.

Penelitian yang dilaksanakan Smith et al [21] menggunakan jaringan syaraf tiruan dan algoritma EM

ISBN: 978-602-19568-1-6

yang digunakan untuk membentuk suatu grup *alert*, untuk mengatasi masalah nomor 4 yang telah dipaparkan sebelumnya. Dari hasil penelitian [21] berdasarkan dataset DARPA yang pada mulanya terdapat 21 cluster serangan, ternyata hanya bisa dikelompokkan menjadi 13 cluster serangan, karena menggunakan unsupervised learning. Sehingga terdapat kesalahan pemisahan di mana alert dari jenis serangan yang sama dikelompokkan menjadi cluster yang berbeda. Sementara Panacea [22] menyajikan sistem serupa yang teknik SVM atau RIPPER untuk mengkategorikan peringatan. Dan hanya dapat mengklasifikasikan serangan yang tidak melibatkan payload seperti port scan dan DDoS.

Berdasarkan penelitian terdahulu yang telah dipaparkan, maka pendekatan baru yang diusulkan dalam mendeteksi serangan DDoS pada penelitian ini, diharapkan bisa menjadi sebuah komplemen terhadap sistem IDS yang telah ada dengan tujuan untuk meminimalisir serangan DDoS pada sebuah jaringan.

V. KESIMPULAN

Distributed Denial of Service (DDoS) merupakan jenis serangan yang telah ada sejak tahun 1990-an, dimana volume dan intensitas DDoS terus meningkat. Skala dan biaya untuk menanggulangi serangan dalam bisnis dunia maya naik hampir dua kali lipat dibandingkan dengan tahun sebelumnya.

Pengenalan pola serangan DDoS pada IDS memiliki kelemahan yaitu adanya defisit TCP/IP, dan adanya masalah false-positif yang sering terjadi pada IDS yang berbasis signature. Sehingga memakan waktu untuk menentukan dan melakukan tindakan mitigasi secara cepat untuk mengamankan jaringan.

Penelitian yang menggunakan jaringan syaraf tiruan dan algoritma EM mampu membentuk suatu grup *alert*, namun kurang mampu untuk membentuk cluster jenis serangan. Sedangkan penelitian yang memanfaatkan nilai entropi maksimal untuk membangun dasar nilai distribusi jaringan yang normal dan kemudian menggunakan entropi relatif untuk mendeteksi anomali berdasarkan pada atribut TCP/IP justru membuat preprocessing terlalu kompleks yang menurunkan kemampuan untuk mendeteksi anomali secara cepat. Deteksi anomali dengan metode NRNE penelitian memberikan hasil optimal dalam mendeteksi DDoS.

Pendekatan baru yang diusulkan dalam mendeteksi serangan DDoS dengan mnggabungkan metode NRNE dan jaringan syaraf tiruan, diharapkan bisa menjadi sebuah komplemen terhadap sistem IDS yang telah ada dengan tujuan untuk meminimalisir serangan DDoS pada sebuah jaringan dan mampu membentuk cluster jenis serangan DDoS secara tepat dan meminimalisir false-positive rate.

DAFTAR PUSTAKA

[1] Hackmageddon. Intranets: I know with what weapons World War III will be fought. [Online]. Available: http://hackmageddon.com/page/4

[2] Bloomberg BussinessWeek. Intranets: You Don't have to be an Evil Hacker Genius to bring Down PlayStation. [Online]. Available: http://www.businessweek.com/articles/2014-08-26/ddos-attacks-aresoaring

[3] R. Heady, G. Luger, A. Maccabe, M. Servilla, The architecture of a Network Level Intrusion Detection System, Technical Report CS90-20, University of New Mexico, August, 1990.

[4] eSecurity Planet. Intranet: DDoS attack growing but how much. [Online]. Available: http://www.esecurityplanet.com/networksecurity/ddosattacks-growing-but-how-much.html

[5] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey", ACM Computing Surveys (CSUR), vol. 41, no. 3, pp. 15, 2009

[6] A. Tajbakhsh, M. Rahmati, and A. Mirzaei , "Intrusion Detection Using Fuzzy Association Rules", Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[7] J. Yu, H. Lee, M.S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM", Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[8] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic", IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512-525, April, 2011.

[9] S. Lee, G. Kim and S. Kim, "Self-adaptive and dynamic clustering for online anomaly detection", Expert Systems with Applications, vol. 38, no. 12, pp. 14891-14898, 2011.

[10] Yu Gu, A.McCallum and D.Towsley. "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation" Tech. rep., Department of Computer Science, UMASS, Amherst, 2005. In https://www.usenix.org/events/imc05/tech/full_papers/gu/gu.pdf

[11] Qian Quan, Che Hong-Yi, Zhang Rui, "Entropy Based Method for Network Anomaly Detection". 15th IEEE Pacific Rim International Symposium on Dependable Computing, vol. 978-0-7695-3849-5, no. 09, pp.189-191. 2009.

[12] MIT: Mit lincoln laboratory-darpa intrusion detection evaluation. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html (1999)

[13]The CAIDA UCSD "DDoS Attack 2007" Dataset http://www.caida.org/data/passive/ddos-20070804 dataset.xml

[14] The CAIDA UCSD Anonymized Internet Traces 2011 -

ISBN: 978-602-19568-1-6

http://www.caida.org/data/passive/passive_2011_dataset.xml
[15]https://www.usenix.org/legacy/event/deter07/tech/full_papers/mirkovic/mirkovic_html/DeterPerfs.html
[16] G. Nychis V. Sekar, D. G. Anderson, etc. "An Empirical Evaluation of Entropy-based Anomaly Detection" Proceedings of the 8th ACM SIGCOMM conference on Internet measurement,, ACM Press, 2008,pp151-156.
[17] D.Brauckhoff, B. Tellenbach, A. Wagner, etc. "Impact of traffic sampling on anomaly detection metrics." Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. ACM Press, 2006, pp159-164.
[18] A.Lakhina, M. Crovella, and C. Diot. "Mining anomalies using traffic feature distributions". Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications.ACM Press, 2005, pp217-218
[19] S.A. Mirheidari, S. Arshad, and R. Jalili, "Alert Correlation Algorithms: A Survey and Taxonomy", In Cyberspace Safety and Security, pp. 183197, Springer International Publishing, 2013.
[20] J. Viinikka, H. Debar, L. Mé, and R. Séguier, "Time series modeling for IDS alert management", In Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 102-113, March, 2006
[21] R. Smith, N. Japkowicz, M. Dondo, and P. Mason, "Using unsupervised learning for network alert correlation", In Advances in Artificial Intelligence, pp. 308-319, Springer Berlin Heidelberg, 2008.
[22] D. Bolzoni, S. Etalle, and P.H. Hartel, "Panacea: Automating attack classification for anomaly-based network intrusion detection systems", In Recent Advances in Intrusion Detection, pp. 1-20, Springer Berlin Heidelberg, January, 2009.

ISBN: 978-602-19568-1-6