**JISKa,** Vol. 1, No. 3, Januari, 2017, Pp. 115 – 122
**ISSN 2527 -5836**

# Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window

**Arif Wirawan Muhammad [(1)], Imam Riadi [(2)], Sunardi [(3)]**
Program S2 Teknologi Informasi, Universitas Ahmad Dahlan
Jalan Prof. Dr. Soepomo, S.H., Umbulharjo, Daerah Istimewa Yogyakarta 55164
e-mail : arif1508048009@webmail.uad.ac.id

**Abstract**

*Distributed denial-of-service (DDoS) is an attack type which volume, intensity, and mitigation costs continue to rise with a growing scale of the organization. This study has the objective to develop a new approach to detect DDoS attacks, based on the characteristics of network activity using a neural network with functionality of fixed moving average window (FMAW) as a detection method. Data taken from the training and testing of DDoS Attack Caida 2007 and standalone simulation. Testing of methods produces the average percentage detection of three network conditions (normal, slow DDoS, Dan DDoS) amounted to 90.52%. A new approach in detecting DDoS attacks, is expected to be a complement to the IDS system in predicting the occurrence of DDoS attacks.*

***Keywords : DDoS, Fixed Moving Average Window, Neural Network, IDS***

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 pada karakteristik aktivitas jaringan menggunakan neural network dengan fungsi fixed moving average window (FMAW) sebagai metode deteksi. Data pelatihan dan pengujian diambil dari CAIDA DDoS Attack 2007 dan simulasi mandiri. Pengujian terhadap 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%. Adanya pendekatan baru dalam mendeteksi serangan DDoS, diharapkan bisa menjadi sebuah komplemen terhadap sistem IDS dalam meramalkan terjadinya serangan DDoS.

**Kata Kunci : DDoS, Fixed Moving Average Window, Neural Network, IDS**

## 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 (ArborNetworks, 2014). 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 (BussinessWeek, 2014). Di sisi lain, serangan jaringan merupakan risiko untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi (Zhao et.al, 2015).

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 menguatkan dugaan bahwa menghentikan DDoS adalah mustahil (ArborNetworks, 2014). 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 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 (Thatte et.al.,2011). Sistem IDS pada umumnya hanya memantau dan

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 (Lee et al.,2011).

Pengenalan pola serangan DDoS pada IDS memiliki dua kelemahan. Pertama, karena defisit TCP/IP (B.Cid, 2015). 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 (Eray et al.,2014).

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 telah dilaksanakan oleh Nychis et al. (2008) dan menghasilkan kesimpulan bahwa nilai entropi dari artefak jaringan saling berkorelasi. Nychis, Sekar, & Anderson (2008) memanfaatkan fungsi entropi maksimal untuk membangun angka distribusi jaringan yang normal dan kemudian menggunakan entropi relatif untuk mendeteksi anomali/serangan DDoS. Penelitian yang dilaksanakan oleh Gautama et al. (2016) 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. (Riadi et al.,2012).

Metode neural network secara unsupervised learning dan algoritma EM telah digunakan untuk mendeteksi adanya serangan DDoS oleh Smith et al. (2008) 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 (Smith et al.,2008). Sementara penelitian yang dilaksanakan oleh Bolzoni et al. (2009) 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. Saied et al. (2015) membuktikan bahwa metode neural network mampu digunakan untuk mendeteksi serangan DDoS yang bersifat serangan jenis baru, dan dapat digunakan dalam lingkungan Hadoop dan Hbase (Zhao et al.,2015).

Berdasarkan penelitian terdahulu yang telah dipaparkan, maka diusulkan sebuah pendekatan baru dalam mendeteksi serangan DDoS dengan menggunakan metode neural network dengan fungsi fixed moving average window berdasarkan karakteristik aktivitas jaringan yang diambil dari log.

Penelitian ini memiliki tujuan untuk mengembangkan sebuah pendekatan baru yang dapat mendeteksi serangan DDoS secara efisien, berdasarkan pada karakteristik aktivitas jaringan menggunakan metode neural network dengan fungsi fixed moving average window (FMAW) sebagai metode deteksi. Data pelatihan dan pengujian diambil dari CAIDA DDoS Attack 2007 dan simulasi mandiri. Penelitian yang akan dilaksanakan diharapkan mampu menjawab :

1. Bagaimana cara menerapkan metode neural network dengan fungsi fixed moving average window (FMAW) sebagai metode deteksi serangan DdoS

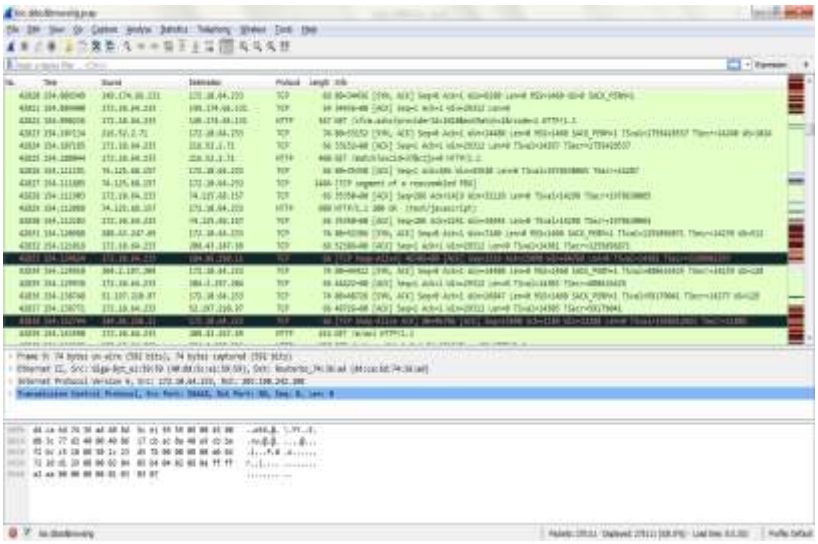
2. Bagaimana performa deteksi DDoS dengan neural network dengan fungsi fixed moving average window (FMAW) berdasarkan data pelatihan dan pengujian.

Pendekatan baru dalam mendeteksi serangan DDoS diharapkan bisa menjadi komplemen IDS dalam mengamankan jaringan dari serangan DDoS.

## 2. METODE PENELITIAN

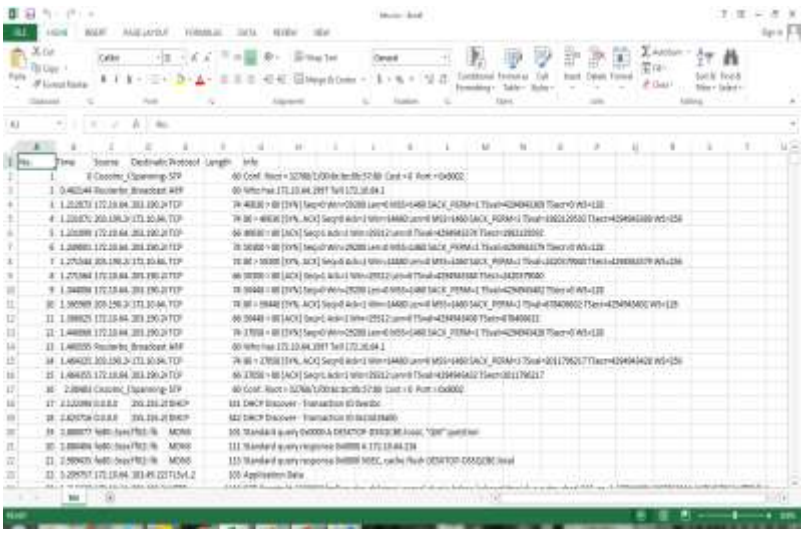
Prosedur penelitian yang akan dilaksanakan dibagi menjadi beberapa tahapan sebagai berikut :

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 dengan fungsi *fixed moving average window* selama lima detik, sebagai *input neural network*. Karakteristik aktivitas jaringan yang dihasilkan dari

kuantifikasi dari ekstraksi log dengan fungsi *fixed moving average window* selama lima detik 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

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

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.

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

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.

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

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 kuantifikasi ekstraksi log.
6. Melakukan pengujian terhadap *neural network* menggunakan 70% data dari hasil kuantifikasi ekstraksi log.
7. Menganalisis untuk kinerja metode *neural network* dengan fungsi *fixed moving average window* (FMAW) dalam mendeteksi serangan DDoS.

## 3. HASIL DAN PEMBAHASAN

Keenam karakteristik aktivitas jaringan tersebut 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 |

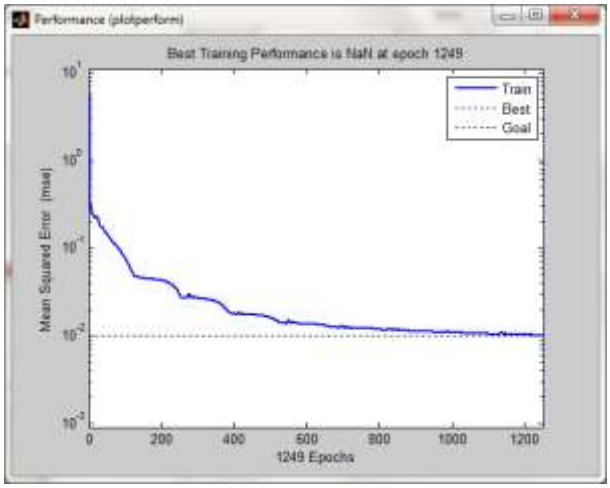
*Neural network* yang digunakan menggunakan pelatihan *backpropagation* dengan fungsi *traingdx* dan memiliki konfigurasi sebagai berikut :

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

Hasil pelatihan *neural network* tersaji pada Gambar 1, terlihat dimana nilai minimal dari *mean square error (*MSE) yang telah ditetapkan sebesar 0,01, tercapai pada *epoch* 1249 dengan gradien sebesar 0,00403.

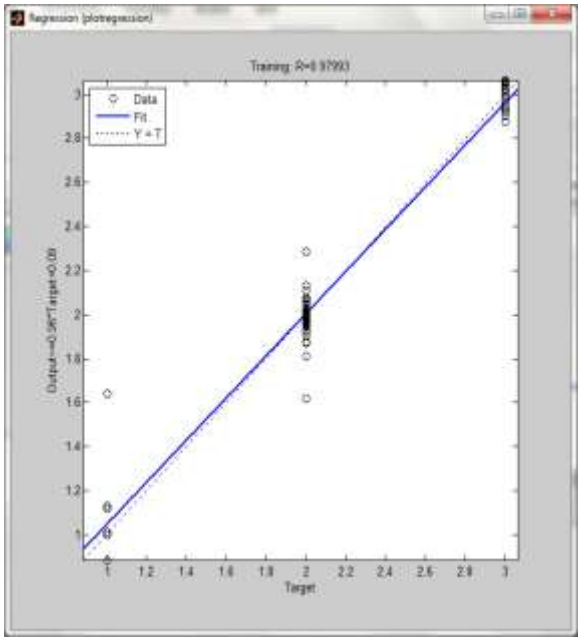

**Gambar 3. Hasil Pelatihan *Neural Network***

Sehingga dapat disimpulkan bahwa neural network telah mencapai kondisi maksimal dalam pelatihannya, sebagaimana yang tersaji pada grafik performa neural network pada Gambar 2.




**Gambar 4. Grafik Performa *Neural Network***

Dari hasil pelatihan jaringan didapatkan plot regresi dengan nilai R sebesar 0,97993 seperti yang tersaji pada Gambar 3. 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 metode metode *neural network* dengan fungsi *fixed moving average window* (FMAW), 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*.

## 4. KESIMPULAN

Distributed denial-of-service (DDoS) merupakan jenis serangan yang telah ada sejak tahun 1990, 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 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.

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 metode metode neural network dengan fungsi fixed moving average window (FMAW), 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

ArborNetworks. (2014). Worldwide Infrastructure Security Report. Burlington: Arbor Networks Security Division.

B.Cid, D. (2015, 9 3). Analyzing Popular Layer 7 Application DDoS Attacks. Retrieved from SUCURI Blog: https://blog.sucuri.net/2015/09/analyzing-popular-layer-7-application-ddos-attacks.html

Bolzoni, D., Etalle, S., & Hartel, P. (2009). Panacea: Automating attack classification for anomaly-based network intrusion detection systems. In Recent Advances in Intrusion Detection (pp. 1-20). Berlin: Springer Berlin Heidelberg.

BussinessWeek, B. (2014, 8 26). Intranets: You Don't have to be an Evil Hacker Genius to bring Down PlayStation. Retrieved from Bloomberg: http://www.businessweek.com/articles/2014-08-26/ddos-attacks-aresoaring

Eray, B., Jander, A., & A.Nur. (2014). Supervised Learning to Detect DDoS Attacks. IEEE Journal, 14.

Lee, S., Kim, G., & Kim, S. (2011). Self-adaptive and dynamic clustering for online anomaly detection. Expert Systems with Applications, 14891-14898.

Nychis, G., Sekar, V., & Anderson, D. G. (2008). An Empirical Evaluation of Entropy-based Anomaly Detection. Proceedings of the 8th ACM SIGCOMM conference on Internet measurement, 151-156.

R. Heady, G. L. (2009). The architecture of a Network Level Intrusion Detection System. Mexico: University of New Mexico.

Riadi, I., Istiyanto, J. E., Ashari, A., & Subanar. (2012). Log Analysis Technique using Clustering in Network Forensics. International Journal of Computer Science and Information Security.

Saied, A., Overill, R. E., & Radizk, T. (2015). Artificial Neural Networks in the detection of known and unknown DDoS attacks: Proof-of-Concept. London: Department of Informatics, King´s College London, Strand, WC2R 2LS, UK.

Smith, R., Japkowicz, N., Dondo, M., & Mason, P. (2008). Using unsupervised learning for network alert correlation. Advances in Artificial Intelligence, 308-319.

Thatte, G., Mitra, U., & Heidemann, J. (2011). Parametric Methods for Anomaly Detection in Aggregate Traffic. IEEE/ACM Trans. Networking, 512-525.

UCSD, T. C. (2007). DDoS Attack 2007. Retrieved from The CAIDA UCSD: http://www.caida.org/data/passive/ddos-20070804_dataset.xml

Zhao, T., Lo, D. C.-T., & Qian, K. (2015). A Neural Network Based DDoS Detection System Using Hadoop and HBase. IEEE 17th International Conference on High Performance Computing and Communication, 1326-1331.