Kombinasi Metode Partial Rank Correlation dan Flow Correlation Coefficient untuk Membedakan DDoS dengan Flash Crowds

Calvin Kamtoso, Agustinus Noertjahyana, Rolly Intan
Program Studi Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jln. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
calvinkmts@gmail.com, agust@petra.ac.id, rintan@petra.ac.id

ABSTRAK

Bertumbuhnya jumlah pengguna internet menyebabkan serangan *DDoS* pun menjadi berkembang, hal ini tentu menyebabkan mendeteksi sebuah *DDoS* menjadi tantangan sendiri. Di sisi lain terdapat flash crowds yang merupakan trafik yang berasal dari user valid dalam jumlah yang sangat besar. Berkembangnya serangan *DDoS* menyebabkan membedakan *flash crowds* dan *DDoS* menjadi semakin susah.

Penelitian ini akan dilakukan dengan menggabungkan dua metode *partial rank correlation* dan *flow correlation coefficient*. Metode *partial rank correlation* dapat digunakan untuk mendeteksi *low-rate* dan *high-rate* serangan *DDoS*. Metode *flow correlation coefficient* dapat digunakan untuk membedakan *DDoS* dengan *flash crowds*, tetapi metode ini tidak dapat mendeteksi *low-rate* serangan *DDoS*.

Dengan pengujian yang dilakukan dapat diketuhui apakah dengan menggabungkan kedua metode dapat menghasilkan program yang dapat membedakan trafik *DDoS*, *flash crowds*, atau bukan. Lalu apakah dengan menggabungkan kedua metode dapat meningkatkan akurasi *detection rate* dan *false positive alarm rate* dibandingkan ketika masing-masing metode berjalan masing-masing.

Kata Kunci: *DDoS, Flash Crowds, Partial Rank Correlation, Flow Correlation Coefficient, DDoS Detection*

ABSTRACT

With the growing of internet user, causing DDoS attacks to also become more sophisticated. This of course causing DDoS detection became a challenge itself. On the other hand, there is flash crowds which is a traffic generated from a huge amount of valid user. While DDoS attack is becoming more sophisticated, it causes discrimination a DDoS attacks from flash crowds become more challenging.

This research will be conducted by combining two methods of partial rank correlation and flow correlation. Partial rank correlation itself can be used to detect low-rate and high-rate DDoS attacks. Meanwhile flow correlation coefficient can be used to discriminate DDoS from flash crowds, albeit it is lacking the capability to detect low-rate DDoS attacks.

With the test carried, it can be acknowledged whether combining two methods could produce a program that could detect DDoS, flash crowds, or not. Then whether by combining the two methods could increase the accuracy of detection rate and false positive alarm rate of said program than when each method is run independently.

Keywords: *DDoS, Flash Crowds, Partial Rank Correlation, Flow Correlation Coefficient, DDoS Detection*

1. PENDAHULUAN

Distributed *Denial of Service (DDoS)* merupakan serangan berskala besar terhadap suatu jaringan, salah satunya internet. Dengan bertumbuhnya jumlah penggunaan internet, serangan *DDoS* pun semakin berkembang, mendeteksi serangan *DDoS* menjadi tantangan tersendiri dalam dunia keamanan. Beberapa teknik yang digunakan untuk mendeteksi *DDoS* adalah dengan analisis *traffic* suatu jaringan [11], mengitung *entropy* dan *frequencey-sorted distributions of selected packet attributes* [6]. Teknik – teknik yang telah ada ini sebagian besar hanya terbatas terhadap pendeteksian *DDoS*. *DDoS* dapat diklasifikasikan menjadi dua yakni, *low-rate DDoS* dan *high-rate DDoS*. *Low-rate DDoS* merupakan merupakan serangan *DDoS* dengan jumlah paket yang lebih rendah dibandingkan *High-rate DDoS* yang cukup untuk membuat *DDoS* terjadi dengan tujuan untuk menghindari deteksi. *Low-rate DDoS* menghasilkan trafik yang terlihat normal sehingga deteksi menjadi susah [1][3][4].

Di sisi lain *flash crowds* meruapakan jaringan yang *valid*, berasal dari *user*. *Flash crowds* ini bisa terjadi kapan saja, dimana *user* dengan jumlah yang sangat besar meng-akses sebuah jaringan mengakibatkan *traffic* yang sangat mirip dengan serangan *DDoS [2]*. Hal ini menjadi tantangan untuk dapat membedakan apakah *flash crowds* yang sedang terjadi ataukah sebuah serangan *DDoS* [17]. Beberapa Teknik yang digunakan untuk melakukan pembedaan *DDoS* dari *flash crowds* adalah menggunakan *probability metrics* [10], *packet arrival pattern* [14], dan *information distance* [15]. Teknik – teknik yang digunakan ini hanya sebatas akan melakukan pembedaan akan *DDoS* dan *flash crowds*. Salah satu teknik untuk mengatasi yang digunakan terhadap *flash crowds* adalah *graphical puzzles* yang digunakan untuk membedakan apakah sebuah *request* dilakukan oleh *bot* ataukah manusia [13]. *Flow Correlation Coefficient* digunakan untuk membedakan *DDoS* dengan *flash crowds*, dimana *datasets* untuk *flash crowds* diambil dari *log* trafik 1998 *FIFA World Cup*, dan *datasets* untuk *DDoS* dibuat dengan menggunakan *tool Mstream* [16].

Masalah yang timbul adalah metode *flow correlation coefficient* berasumsi *DDoS* yang terjadi hanya berasal dari satu jenis *bot*, hal ini tidak demikian di lapangan dan metode ini belum pernah

dijalankan pada *datasets* yang berasal dari trafik yang sesungguhnya. Metode *partial rank correlation* di sisi lain tidak dapat mendeteksi adanya *flash crowds* atau tidak.

Penelitian ini bertujuan menggabungkan metode *partial rank correlation* dan *flow correlation coefficient* untuk mendeteksi sebuah serangan *DDoS* dan menentukan apakah terdapat *flash crowds* jika tidak ada *DDoS* yang. Diharapkan dengan menggabungkan 2 metode ini dapat dihasilkan pendeteksian yang lebih akurat dan program pendeteksi dapat menentukan apakah pada trafik yang dimonitor terdapat *DDoS*, *flash crowds*, atau bukan.

2. LANDASAN TEORI

2.1 Distributed Denial of Service

Distributed denial of service (DDoS) merupakan serangan yang terjadi ketika sistem telah terinfeksi dengan jumlah yang besar melakukan *request* ke sebuah atau lebih jaringan yang menyebabkan jaringan tersebut menjadi tidak dapat menerima *request* dari pengguna yang sesungguhnya [8][12] ditunjukkan pada Gambar 2.1. DDoS pada umumnya memiliki *botnets* yang menjadi salah satu alat untuk melakukan serangan. *Botnets* ini dapat diatur agar dapat bertindak seperti *flash crowds* [17] dengan menirukan pola trafik yang menirukan flash crowds. Serangan *DDoS* dapat diklasifikasikan menjadi 2 yakni *low-rate* dan *high-rate*. Umumnya serangan *low-rate* diasosiasikan dengan beberapa *protocol* yang spesifik, tetapi secara umum *low-rate* merupakan serangan yang lebih kompleks dibadingkan dengan *high-rate* dimana penyerang mengirimkan paket dalam jumlah yang rendah untuk menghindari deteksi *DDoS* tetapi cukup untuk membuat efek *DDoS* muncul pada sistem korban [4].

2.2 Flash Crowds

Flash crowds merupakan trafik dalam jumlah besar yang dihasilkan dari pengguna yang sesungguhnya. Trafik dari *flash crowds* ini menyerupai trafik yang ada pada *DDoS*, *flash crowds* terjadi secara lebih natural seperti jika sedang terjadi berita yang menggemparkan, di sisi lain distribusi dari sumber IP yang melakukan request pada flash crowds berjumlah banyak dan menyebar sedangkan pada *DDoS IP* yang ada hanya terbatas pada mesin-mesin yang terinfeksi [8].

2.3 Partial Rank Correlation

Partial Rank Correlation merupakan metode perhitungan ranking partial korelasi koefisien antara dua *variable* ketika efek dari variable ketiga di munculkan. Hubungan linear yang sempurna memiliki rank correlation bernilai +1, negative relationship dengan nilai -1, dan tidak ada *linear relationship* ditunjukkan dengan nilai rank correlation 0.

$$r = 1 - 6 \sum_{i=1}^{N} \frac{D_i}{N(N^2-1)} \quad (1)$$

Untuk menghitung *rank correlation* dalam sebuah populasi yang kontinu (non-numerik) digunkan dengan yang disebut *grade correlation*. *Spearman coefficient* r merupakan salah satu perhitungan untuk *grade correlation*. Setelah mendapat tiga rank, didapat tiga nilai r, lalu diaplikasikan pada *product moment partial* formula maka akan didapatkan sebuah *partial coefficient* ditunjukkan pada (2.2) [8].

$$r_{XY.Z} = \frac{r_{XY} - r_{XZ} * r_{YZ}}{\sqrt{1-r_{XZ}^2} * \sqrt{1-r_{YZ}^2}} \quad (2)$$

2.4 Flow Correlation Coefficient

Flow correaltion coefficient merupakan teknik yang digunakan untuk mengindikasikan *similiarity* antara 2 *flows*.

Let Xi and Xj (i != j) be two network flows with the same length N. We define the correlation coefficient of the two flows as

$$\rho X_i, X_j = \frac{r X_i, X_j [k]}{\frac{1}{N}[\sum_{n=1}^{N-1} x_i^2 \sum_{n=1}^{N-1} x_j^2]^{1/2}} \quad (3)$$

2.5 Detection Rate

Detection rate merupakan seberapa sering deteksi yang sering terjadi. Yang digunakan sebagai salah satu tolak ukur akan akurasi dari suatu *detection sistem*. *Detection rate* mengambarkan rasio dari *true positive* dengan total sampel yang dideteksi oleh program pendeteksi [9].

$$DR = \frac{TP}{TP+FN} \quad (4)$$

2.6 False Positive Rate

False positive rate merupakan alarm yang dihasilkan ketika kondisi yang terdeteksi yang tidak seharusanya memberikan alarm. Menggambarkan rasio dari *false positive* dengan total sampel yang dideteksi oleh program pendeteksi [9].

$$FPR = \frac{FP}{FP+TN} \quad (5)$$

2.7 NS-3

Network Simulator 3 (ns-3) merupakan alat yang digunakan untuk melakukan simulasi terhadap suatu jaringan yang dikembangkan dari ns-2.

3. DESAIN SISTEM

3.1 Analisis Permasalahan

Penelitian tentang menggabungkan mendeteksi *Low-rate* dan *High-rate DDoS* dan membedakkanya dari *Flash Crowds* dilakukan dengan bertumbuhnya jumlah penggunaan internet serangan *DDoS* pun semakin berkembang [5]. Di sisi lain dengan bertumbuhnya jumlah pengguna internet, *Flash Crowds* yang merupakan sebuah trafik jaringan yang dihasilkan dari banyak *user* yang sesungguhnya pun juga semakin banyak. *DDoS* dan *Flash Crowds* merupakan hal yang mirip dimana keduanya dapat menyebabkan hilangnya suatu akses terhadap sebuah servis [7].

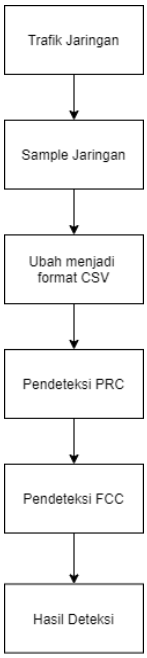
3.2 Desain Sistem

Desain sistem yang akan dikembangkan adalah dengan menggabungkan dua metode yang berbeda yakni *partial rank correlation* untuk membedakan apakah sebuah serangan *DDoS* yang terdeteksi dikategorikan menjadi *Low-rate* atau *High-rate*, *Low-rate DDoS* merupakan serangan yang lebih kompleks dibandingkan *High-rate DDoS*, dimana *Low-rate* memiliki banyak kemungkinan untuk lebih sering tidak terdeteksi oleh *DDoS detection system* pada umumnya. Lalu ada juga metode *flow correlation coefficient* yang dapat digunakan untuk

membedakan *DDoS* dengan *Flash Crowds*. Desain sistem yang diajukan adalah ketika *network* berjalan akan dilakukan deteksi apakah terdapat *DDoS* atau tidak, jika tidak terdeteksi ada *DDoS* maka akan dilakukan pengecekan apakah ada *flash crowds* yang terdeteksi atau tidak.

Pertama untuk sebuah trafik pada sebuah jaringan, dilakukan pengambilan sampel selama 5 menit, yang kemudian dibagi menjadi *interval* yang lebih kecil sebesar 10 detik. Sampel tersebut kemudian disimpan ke dalam bentuk *file* PCAP atau *network capture file*. Dilakukan konversi *format file* untuk dilakukan pemrosesan lebih lanjut ke dalam bentuk CSV.

Setelah selesai melakukan pemrosesan pada *file network* yang telah dikonversi menjadi CSV file, program dijalankan pada file tersebut. Setelah program selesai berjalan maka akan dihasilkan nilai PRC dan FCC, yang digunakan untuk mengambil keputusan apakah sebuah trafik mengandung *DDoS*, *flash crowds*, atau trafik normal.



Gambar 1. Desain Program Pendeteksi.

3.2.1 Partial Rank Correlation

Berikut akan diberikan *pseudo-code* untuk program pendeteksi yang menggunakan *partial rank correlation*.

1. Membuat sampel trafik network berdasarkan periode, T = 0, dimana *Sample the network traffic X* yang diterima berdasarkan sampel periode T
2. Hitung *Correlation Coefficient* untuk r_{XY}, r_{XZ}, r_{YZ} menggunkan

$$r_{XY} = \frac{\mathrm{cov}(X,Y)}{\sigma_X * \sigma_y} \quad (6)$$

3. Hitung *partial rank correlation* $r_{XY.Z}(x)$ dengan menggunkan rumus

$$r_{XY.Z} = \frac{r_{XY} - r_{XZ} * r_{YZ}}{\sqrt{1-r_{XZ}^2} * \sqrt{1-r_{YZ}^2}} \quad (7)$$

4. Lakukan komparasi *rank value* untuk trafik yang mencurigakan menggunakan ekuasi

$$r_{XY.Z}(x) = \begin{cases} 1, r_{XY.Z} < \delta_1 \; or \; r_{XY.Z} \geq \delta_2 \\ 0, \delta_1 \leq r_{XY.Z} \geq \delta_2 \end{cases} \quad (8)$$

5. Bandingkan dengan *threshold* untuk mengecek apakah $r_{XY.Z}(x) < \delta_1$ atau $r_{XY.Z}(x) \geq \delta_2$. Jika iya, maka keluarkan sebuah alarm yang menyatakan sedang terjadi serangan *DDoS*.
6. Kembali ke step 2

3.2.2 Flow Correlation Coefficient

Berikut merupakan *pseudo-code* untuk program pendeteksi yang menggunakan *flow correlation coefficient*.

1. Untuk M *network flows* yang telah dilakukan sampling $\{X_1, X_2, X_3, \ldots, X_M\}$ dengan sebuah interval x
2. Kita dapat temukan *flow correlation coefficient* dari 2 network flows, $X_i \; (1 \leq i \leq M)$ dan $X_j \; (1 \leq j \leq M, \; i \neq j)$.
3. Hitung I_{X_i,X_j} yang digunakan sebagai indikator untuk *similarity flow* X_i dan X_j, I_{X_i,X_j} hanya memiliki 2 nilai yakni 1 untuk *DDoS* dan 0 untuk yang lainnya.
4. Lalu kita temukan δ = 0.6. yang digunakan sebagai *threshold* untuk membedakan.
5. Lalu kita hitung *attack positive probability* dengan ekuasi sebagai berikut untuk menambahkan penguatan pengambilan keputusan:

$$\Pr(I_A = 1) = \frac{\sum_{1 \leq i,j \leq M, i \neq j} I_{X_i,X_j}}{\binom{M}{2}} \quad (9)$$

6. Lalu kita dapat tentukan dengan I_A yang merupakan indikator serangan *DDoS* dimana I_A= 1 merupakan serangan *DDoS*. Lalu kita gunakan *threshold*, untuk mengambil keputusan apakah *network flow* tersebut terdapat *DDoS* atau merupakan *flash crowds*.

3.3 Desain Pengujian Sistem

Desain pengujian sistem adalah dengan menggunakan *dataset* untuk digunakan pada sistem yang telah dibuat. Dengan adanya 2 metode, pengujian akan dilakukan dengan menjalankan masing-masing metode secara individu dan menjalankan sesuai dengan desain sistem yang diajukan. Lalu hasil dari masing-masing pengujian akan dibandingkan dengan penelitian akan *dataset* dimana akan didapatkan *false positive alarm* dan *detection rate* dari masing-masing pengujian. Sehingga dari pengujian ini didapatkan apakah dengan menggabungkan kedua metode dapat meningkatkan performa dilihat dari parameter yang disebutkan.

Berikut merupakan rincian dari Langkah-langkah pengujian yang dilakukan:

1. Mempersiapkan 4 datasets, 1998 FIFA *World Cup*, ISCXIDS2012, CICDDoS2019, *datasets* yang dihasilkan dari NS-3.

2. Menjalankan program pendeteksi partial rank correlation pada masing-masing datasets, kemudian akan didapatkan akurasi dari metode ini.
3. Menjalankan program pendeteksi *flow correlation coefficient* pada masing-masing *datasets*, yang kemudian dapat ditentukan untuk nilai threshold yang dibutuhkan, sehingga dapat menghitung akurasi dari metode *flow correlation coefficient*.
4. Menjalankan program pendeteksi dengan metode gabungan, kemudian didaptkan akurasi dari metode gabungan. Setelah itu ditentukan apakah dengan menggabungkan kedua metode, dapat meningkatkan akurasi pendeteksian DDoS, flash crowds, atau tidak.

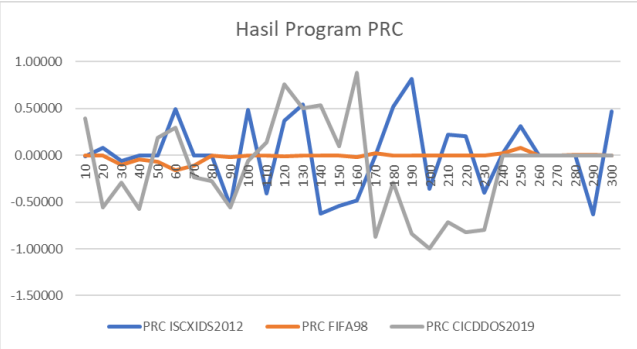
4. PENGUJIAN SISTEM

4.1 Proses Pengujian

Pengujian akan dibagi menjadi beberapa bagian. Bagian pertama dan kedua akan menjelaskan pengujian dengan menjalankan masing masing metode, yakni *partial rank correlation* dan *flow correlation coefficient* secara independen. Masing-masing metode akan dijalankan pada 3 datasets yang telah diketahui jenis *network*-nya. Pada bagian berikutnya akan dijelaskan hasil penggabungan kedua metode, yang dijalankan pada 3 *datasets* yang sama dengan sebelumnya. Lalu pada bagian terakhir akan dijelaskan bagaimana masing-masing metode dan metode gabungan bekerja pada *datasets* yang dihasilkan melalui simulasi program NS-3.

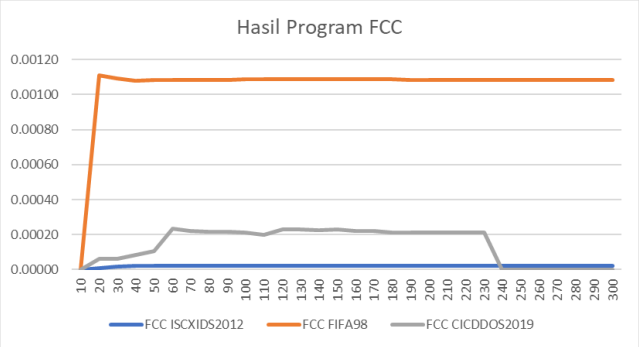
4.2 Hasil Pengujian

Berdasarkan hasil program PRC yang dijalankan pada ketiga datasets 1998 FIFA *World Cup*, ISCXIDS2012, dan CICDDoS2019. Trafik normal dan DDoS memiliki rentang yang berdekatan. Dengan *threshold* yang didapatkan dari studi literatur PRC memiliki akurasi sebesar 65% dengan *false positive alarm rate* 53%.



Gambar 2. Hasil Program Pendeteksi PRC

Pada Gambar 3. dapat dilihat jika trafik untuk masing-masing datasets berada pada rentang nilai yang berbeda. Melalui grafik ini diambil kesimuplan untuk *threshold* DDoS diambil nilai 0.00015 dan untuk *threshold* diambil nilai 0.001. Pada studi literatur yang dilakukan tidak didapatkan nilai *threshold* yang digunakan sehingga dengan pengujian yang dilakukan ini diharapkan untuk dapat menghasilkan nilai threshold yang dapat digunakan dalam program pendeteksi. Dasar pengambilan nilai threshold untuk ini adalah pada *datasets* yang mengandung DDoS dengan nilai 0.00015 didapatkan akurasi pendeteksian untuk DDoS sebesar 78%, dimana jika kita menggunakan nilai 0.0002 maka akan dihasilkan akurasi sebesar 73%. Begitu pula dengan *threshdold* untuk *flash crowds* yang merupakan nilai paling dekat dengan rata-rata rentang nilai pada *datasets flash crowds*.



Gambar 3. Hasil Program Pendeteksi FCC

Program gabungan dari PRC dengan *flow correlation coefficient* dijalankan pada 3 datasets yakni, 1998 *FIFA World Cup*, ISCXIDS2012, CICDDoS2019. Program akan dijalankan selama 5 menit, yang dibagi menjadi interval 10 detik.

Pada *datasets* 1998 FIFA *World Cup*, penggabungan program diatas, program dapat mengindentifikasi trafik *flash crowds* dengan akurasi 97%. Tidak ada peningkatan akurasi yang didapat dari menggabungkan 2 metode.

Pada datasets ISCXIDS2012, dengan menggabungkan 2 metode kita melihat jika false positive alarm tetap sebesar 53%. Sama dengan ketika program PRC dijalankan pada *datasets* ISCXIDS2012. Karena dalam mendeteksi DDoS *flow correlation coefficient* berdasarkan studi literasi tidak dapat mendeteksi *low-rate* DDoS sehingga nilai DDoS yang dihasilkan oleh PRC lebih diprioritaskan dibandingkan nilai *ignore* milik *flow correlation coefficient*.

Pada datasets CICDDoS2019, Setelah menggabungkan 2 metode, akurasi dari deteksi DDoS dapat naik menjadi 91%.

Program juga dijalankan pada dataset yang dihasilkan dari simulasi NS-3. *Datasets* yang dikembangkan pada NS-3 merupakan DDoS. Trafik yang dihasilkan ini berdurasi selama 10 detik.

Tabel 1. Hasil Program PRC pada *Datasets* dari NS-3

Interval	No. of Packets	PRC	Results
10	730749	-0.0000047193	Ignore

Berdasarkan Tabel 1. pengujian program PRC tidak dapat mendeteksi *DDoS* yang dibuat simulasi NS-3.

Tabel 2. Hasil Program FCC pada *Datasets* dari NS-3

Interval	No. of Packets	FCC	Results
10	730749	0.0000000000	Ignore

Berdasarkan Tabel 2. pengujian program FCC tidak dapat mendeteksi *DDoS* yang dibuat simulasi NS-3.

Tabel 3. Hasil Uji Program Gabungan pada *Datasets* dari NS-3

Interval	No. of Packets	PRC	FCC	Results
10	730749	Ignore	Ignore	Ignore

Berdasarkan Tabel 3. Program gabungan dari PRC dengan *flow correlation coefficient* dijalankan pada *datasets* yang dihasilkan dari simulasi NS-3. Program yang digabung tidak dapat mendeteksi *DDoS* yang seharusnya ada pada trafik yang dihasilkan dari simulasi NS-3.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil pengujian yang dilakukan pada sistem, maka dapat disimpulkan bahwa:

- Menggabungkan kedua metode *partial rank correlation* dan *flow correlation coefficient* dapat digunakan untuk membedakan trafik yang merupakan *DDoS*, *flash crowds*, atau bukan. Dimana pada metode *partial rank correlation* hanya dapat menentukan *DDoS* atau bukan, pada metode *flow correlation coefficient* dapat menentukan *DDoS*, *flash crowds*, atau bukan.
- Menggabungkan kedua metode *partial rank correlation* dan *flow correlation coefficient* membuat akurasi/*detection rate* menjadi lebih baik. Dimana pada datasets CICDDoS2019, metode *partial rank correlation* menghasilkan akurasi/*detection rate* sebesar 65%, pada metode *flow correlation coefficient* menghasilkan akuras/*detection rate* 78%. Penggabungan metode menghasilkan akurasi/*detection rate* sebesar 91%.
- Menggabungkan kedua metode *partial rank correlation* dan *flow correlation coefficient* tidak dapat membuat *false positive alarm rate* menjadi lebih baik. Pada *datasets* ISCXIDS2012 metode *partial rank correlation* memiliki *false positive alarm rate* sebesar 53%, dimana pada metode gabungan nilai tersebut tidak menurun.

5.2 Saran

Berdasarkan hasil pengujian yang dilakukan pada sistem maka disarankan untuk melakukan penyempurnaan dan pengembangan program lebih lanjut yakni:

- Diperlukan penelitian lebih lanjut untuk menghitung hubungan antara nilai yang dihasilkan dari metode *partial rank correlation* dan *flow correlation coefficient*. Agar dapat mempengaruhi nilai akurasi/*false positive alarm rate* pada program pendeteksi metode gabungan.
- Diperlukannya penelitian lebih lanjut dalam mengembangkan datasets menggunakan NS-3 untuk menyerupai kondisi trafik yang sesungguhnya.

6. DAFTAR PUSTAKA

[1] Ain, A., Bhuyan, M., Bhattacharyya, D., & Kalita, J. (n.d.). Rank Correlation for Low-Rate DDoS Attack Detection: An Empirical Evaluation (Rep.).

[2] Behal, S., Kumar, K., & Sachdeva, M. (2017). Discriminating flash events from DDoS attacks: A comprehensive review. International Journal of Network Security, 19(5), 734-741. doi:10.6633/IJNS.201709.19(5).11

[3] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Information metrics for low-rate DDoS attack detection: A comparative evaluation. 2014 Seventh International Conference on Contemporary Computing (IC3). doi:10.1109/ic3.2014.6897151

[4] Bhuyan, M., Kalwar, A., Goswami, A., Bhattacharyya, D., & Kalita, J. (2015). Low-Rate and High-Rate Distributed DoS Attack Detection Using Partial Rank Correlation. 2015 Fifth International Conference on Communication Systems and Network Technologies. doi:10.1109/csnt.2015.24

[5] Dhingra, A., & Sachdeva, M. (2018). DDoS detection and discrimination from flash events: A compendious review. 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC). doi:10.1109/icsccc.2018.8703335

[6] Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (n.d.). Statistical approaches to DDoS attack detection and response. Proceedings DARPA Information Survivability Conference and Exposition. doi:10.1109/discex.2003.1194894

[7] Gera, J., & Battula, B. P. (2018). Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds. EURASIP Journal on Information Security, 2018(1). doi:10.1186/s13635-018-0079-6

[8] Kendall, M. G. (1942). Partial Rank Correlation. Biometrika, 32(3/4), 277. doi:10.2307/2332130

[9] Lasisi, A., Ghazali, R., & Herawan, T. (2016). Application of Real-Valued Negative Selection Algorithm to Improve Medical Diagnosis. Applied Computing in Medicine and Health, 231-243. doi:10.1016/b978-0-12-803468-2.00011-4

[10] Li, K., Zhou, W., Li, P., Hai, J., & Liu, J. (2009). Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics. 2009 Third International Conference on Network and System Security. doi:10.1109/nss.2009.35

[11] Privalov, A., Lukicheva, V., Kotenko, I., & Saenko, I. (2019). Method of Early Detection of Cyber-Attacks on Telecommunication Networks Based on Traffic Analysis by Extreme Filtering. Energies, 12(24), 4768. doi:10.3390/en12244768

[12] Singh, K. J., & De, T. (2017). Mathematical modelling of DDoS attack and detection using correlation. Journal of Cyber Security Technology, 1(3-4), 175-186. doi:10.1080/23742917.2017.1384213

[13] Srikanth Kandula, Dina Katabi, Matthias Jacob, and Arthur Berger. 2005. Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds. In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2 (NSDI'05). USENIX Association, USA, 287–300

[14] Thapngam, T., Li, S., Zhou, W., & Beliakov, G. (2011). Discriminating DDoS attack traffic from flash crowd through packet arrival patterns. 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). doi:10.1109/infcomw.2011.5928950

[15] Yu, S., Thapngam, T., Liu, J., Wei, S., & Zhou, W. (2009). Discriminating DDoS Flows from Flash Crowds Using

Information Distance. 2009 Third International Conference on Network and System Security. doi:10.1109/nss.2009.29

[16] Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., & Tang, F. (2012). Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient. IEEE Transactions on Parallel and Distributed Systems, 23(6), 1073-1080. doi:10.1109/tpds.2011.262