Analisis *Long Range Dependence* Untuk Sistem Deteksi Anomali Trafik Dengan Hurst Estimator Menggunakan Metode Periodogram

Analysis Long Range Dependence For Traffic Anomaly Detection System With Hurst Estimator Using Periodogram Method

Henri Topan[1], Yudha Purwanto[2], Hafidudin[3]
[1,2]Prodi S1 Teknik Komputer, Fakultas Teknik Elektro, Universitas Telkom
[3]Prodi D3 Teknik Telekomunikasi, Fakultas Ilmu Terapan, Universitas Telkom
nrieovan@gmail.com[1], om_yudha@yahoo.co.id[2], hafidudin@gmail.com[3]

Abstrak

Anomali trafik merupakan sebuah fenomena pada internet yang menjadi topik hangat penelitian saat ini. Beberapa contoh anomali trafik tersebut adalah Serangan DDoS dan *flashcrowd*. Saat ini intensitas serangan DDoS semakin meningkat. Oleh karena itu, penelitian dalam sistem deteksi trafik anomali banyak dilakukan saat ini. Banyak metode yang digunakan untuk mendeteksi trafik anomali tersebut, salah satunya adalah dengan metode statistik jaringan yaitu dengan *Long Range Dependence*.Pada penelitian-penelitian yang telah dilakukan sebelumnya, sebagian besar peneliti hanya menggunakan satu metode analisis saja. Sehingga hanya dapat mendeteksi serangan DDoS tanpa ada analisis penunjang untuk memperkuat akurasi pendeteksian serangan. Pada penelitian ini, dilakukan penggabungan metode analisis yaitu analisis *autocorrelation*, *hyperbollivcaly decay*, dan *autocovarians*. Sehingga metoda ini diharapkan memiliki tingkat akurasi yang lebih baik. Hasil akhir dari penelitian ini adalah berupa metode pendeteksian anomali trafik dengan parameter output berupa *false positive rate* yang rendah dan *detection rate* yang tinggi.

Kata Kunci: Trafik anomali, DDoS, *Long Range Dependence*

Abstract

Traffic anomaly is a phenomenon on the internet that is becoming a hot topic research for now. Some of traffic anomaly is DDoS attack and flashcrowd. The attack of DDoS was more increased today. Because of that, there was many research on traffic anomaly detection system. It has many method to detect the traffic anomaly, one of that is by using network statistic method which is using the long range dependence.On the research that have been done before, most researchers only use one analysis method. So that can only detect DDoS attacks without any supporting analysis that can make the better accuracy. On this research the method has three analysis it is autocorrelation analysis, hyperbollicaly decay analysis, and autocovarians analysis. So this method can have better acuracy. The end result of this research is in the form of traffic anomaly detection method with output parameters in the form of a low false positive rate and a high detection rate.

Keywords: Traffic anomalies, DDoS, Long Range Dependence

1. Pendahuluan

Pada saat ini kebutuhan akan internet sangat tinggi, dikarenakan kemampuan internet yang sangat membantu dalam kehidupan manusia. Oleh karena hal itu, dalam jaringan internet dikenal suatu parameter yang bernama *Quality of Service* (*QoS*), *QoS* merupakan sebuah parameter penting dalam jaringan internet, karena *QoS* ini merupakan sebagai penilai dalam layanan jaringan internet, semakin besar nilai *QoS* maka kualitas suatu jaringan menjadi semakin baik, kualitas yang baik ini sangat dibutuhkan khusunya untuk menunjang kualitas suatu layanan seperti multimedia, VoIP, dan masih banyak lagi. Arsitektur dari *QoS* itu sendiri, didesain untuk menunjang layanan-layanan yang dapat menaikkan nilai *QoS* tersebut. Teknik yang digunakan oleh provider untuk meningkatkan *QoS* adalah dengan mengkombinasikan teknik klasifikasi, manajemen antrian, penjadwalan, dan *congestion management*. Akan tetapi kekurangan dari *QoS* adalah tidak mampunya untuk men-*drop* paket apa yang harus di-*drop* saat trafik sedang tinggi, tingginya trafik ini tentu akan menurunkan nilai dari *QoS* itu sendiri. Beberapa hal yang dapat memebuat trafik menjadi tinggi adalah *FlashCrowd* dan juga serangan *flooding* trafik (Purwanto, et al., 2014).

Metode yang digunakan dalam penelitian ini adalah *traffic anomaly based* atau pendeteksian berdasarkan anomaly yang terjadi didalam trafik. Metode ini memiliki beragam metode dan yang digunakan dalam penelitian ini adalah sifat *long range dependence* (*LRD*). Pada penelitian yang telah dilakukan oleh Ming Li (Li, 2004), sifat

Long Range Dependence dapat mendeteksi serangan DDoS dengan melihat bagaimana bentuk dari suatu trafik. Selain itu penelitian yang telah dilakukan oleh Delio Brignoli (Brignoli, 2008), sifat LRD juga dapat mendeteksi suatu serangan DDoS, dengan menggunakan parameter-parameter sifat LRD. Kelebihan dari metode ini adalah kemampuannya yang dinamis, yaitu dapat beradaptasi dengan berbagai jenis trafik. Sehingga walaupun tidak memiliki basis data, metode ini tetap dapat mendeteksi serangan DDoS pada suatu trafik.

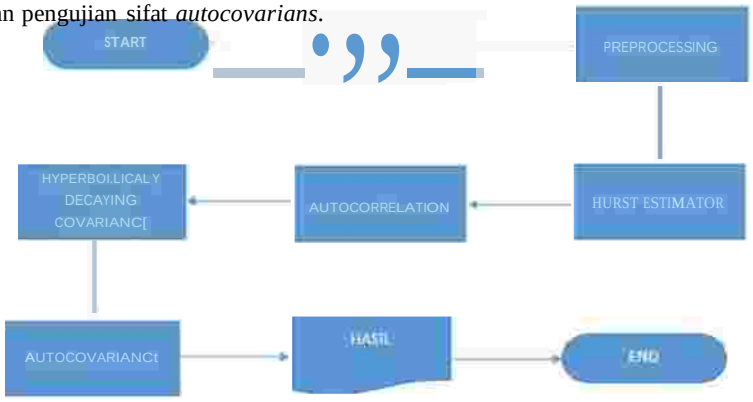
Tujuan dari penelitian ini adalah menganalisa hasil dari sifat *Long Range Dependence* dengan menggunakan tiga analisis dalam mendeteksi anomali trafik. Analisis tersebut dimulai dari proses *pre-processing*, perhitungan, analisis data trafik, pendeteksian, pengambilan keputusan, dan pengukuran keberhasilan sistem.

Metodologi penelitian yang digunakan adalah pertama dengan melakukan studi literatur yaitu mempelajari dan memahami mengenai *anomaly traffic*, sistem pendeteksian *anomaly traffic*, dasar-dasar LRD, serta metode yang dapat digunakan dalam penelitian ini dari berbagai referensi buku, artikel, jurnal, atau referensi dari internet. Selanjutnya merancangan sistem deteksi anomali dengan *pre-processing* dan kemudian pegujian sifat LRD. Setelah itu menganalisis hasil pengujian dengan parameter-parameter yang telah ditentukan untuk mengetahui kemampuan algoritma dan faktor-faktor yang mempengaruhi hasil yang didapat.

2. Perancangan

2.1. Gambaran Umum Sistem

Secara umum gambaran sistem dapat digambarkan dalam gambar 1 proses perancangan sistem yang dilakukan diantaranya adalah dengan melakukan persiapan data, melakukan *preprocessing* untuk mendapatkan fitur yang digunakan dalam proses selanjutnya. Dilanjutkan dengan Kemudian dilakukan pengujian pada tiga sifat dari LRD yaitu pengujian sifat *autocorrelation*, pengujian sifat *hyperbollicaly decay* dan pengujian sifat *autocovarians*.



Gambar 1 Gambaran Umum Sistem LRD

2.2. *Preproccessing*

Preprocessing merupakan tahap selanjutnya setelah memperoleh dataset trafik yang digunakan, yaitu dataset normal *CAIDA 2014*, dataset *DDoS CAIDA 2007* dan dataset flashcrowd *World Cup 1998*. Ketiga dataset tersebut dlakukan pengolahan agar dapat dijadikan masukan proses analisis. Pada dataset *DDoS CAIDA 2007*, data trafik berupa *raw* data trafik pada level *network* dan belum dilakukan *labelling* tipe serangan. Untuk dataset normal *CAIDA 2014* berupa hasil capture *raw* paket pada level network yang direkam berdasarkan tanggal, bulan, tahun.

Pada setiap dataset tersebut diproses untuk mendapatkan masukan untuk langkah-langkah selanjutnya. Masukan yang diperlukan adalah jumlah paket yang datang pada suatu *IP destination* setiap detik, jumlah *size* dari paket yang datang pada suatu *IP Destination* setiap detik, dan jarak antara waktu kedatangan paket. Jarak antara waktu kedatangan paket digunakan pada proses estimasi hurst eksponen. Sedangakn jumlah paket pada setiap detik dan jumlah size pada setiap detik digunakan dalam pengecekan sifat-sifat LRD.

Sedangkan pada dataset World Cup 1998, data trafik yang berupa *binary log files* di ekstrak ulang menjadi *Common Log Format* dengan program *WorldCup_tools* yang telah tersedia. Lalu dari data trafik *Common Log Format* dilakukan pengolahan seperti kedua dataset sebelumnya yaitu dengan mencari paket yang datang pada suatu *IP destination* setiap detik, jumlah *size* dari paket yang datang pada suatu *IP Destination* setiap detik, dan jarak antara waktu kedatangan paket. Keadaan *flashcrowd* dapat diketahui dari hasil hitung *flow* dan paket per detik saat *preprocessing*.

2.3. Hurst Estimator Periodogram

Periodogram biasanya digunakan untuk mengidentifikasi domain sebuah perioda atau frekuensi dari sebuah *time series.* Hal ini dapat menjadi sebuah alat yang sangat membantu untuk mengidentifikasi suatu pola dominan dari sebuah seri. Informasi tentang *confidence interval,* efesiensi dan *robustness* diperlukan dalam metoda periodogram, parameter yang digunakan harus tepat, sehingga mendapatkan sampel yang optimal dan tepat dari periodogram tesebut, sehingga dapat meminimalisir proses dalam fungsi untuk mencari nilai yang tepat. I merupakan nilai dari periodogram suatu seri waktu,I memiliki rumus :

$$I(\lambda) = \frac{}{2n} \left| \sum_{j=1}^{N} X_j e^{i} \right|^2 \quad (1)$$

.

2.4. Pengujian sifat LRD

Dalam pengecekan sifat LRD yang dilakukan antara lain adalah dengan menggunakan tiga tahapan, yaitu pengecekan dengan hasil *autocorrelation*, hasil *hyperbolically decaying covarians*, dan hasil *autocovarians.* Pada langkah pertama akan dilihat hasil dari fungsi *autocorrelations* tersebut, apabila trafik tersebut SRD maka nilai *autocovarians* tersebut akan bernilai nol atau negatif sehingga *autocorrelations* dari data tersebut dianggap tidak menuju tak hingga, sedangkan apabila trafik tersebut LRD, maka nilai yang terbentuk tidak aka nada yang bernilai negatif, sehingga dapat dikatakan bahwa *autocorrelation* dari data tersebut menuju tak hingga.

Setelah pengecekan hasil *autocorrelation,* akan dilanjutkan pada tahap yang kedua, yaitu *hyperbolically decaying covarians*, pada tahap kedua ini akan awalnya akan ditentukan nilai *hurst* (H) dari data yang digunakan, setelah nilai H ditentukan maka nilai tersebut akan dijadian sebagai basis dari penentuan *hyperbollicaly decaying.* Apabila data tersebut merupakan LRD, maka *hyperbollicaly decating* akan terbentuk.

Tahap ketiga merupakan pengecekkan nilai *autocovarians,* pada tahap ini data akan dihitung nilai *autocovarians*nya, apabila data tersebut LRD, hubungan data dalam waktu yang berbeda akan kuat, sehingga nilai *autocovarians* data tersebut tidak aka nada yang bernilai nol maupun negatif, sedangkan apabila data tersebut SRD, maka hubungan data dalam waktu yang berbeda akan menurun dengan cepat, sehingga nilai *autocovarians* yang terbentuk akan bernilai nol atau negatif dalam waktu tertentu. Apabila data yang diteliti tersebut memiliki sifat LRD, maka data tersebut akan memiliki nilai *autocorellation* yang menuju tak hingga, memiliki *hyperbollicaly decay*, dan nilai *autocovarians* yang tidak bernilai nol maupun negatif.

2.4.1. Autocorrelation

Autocorrelation merupakan suatu deret yang menghitung perbedaan waktu kedatangan antar suatu paket, dimana paket tersebut merupakan sebuah *random process* dari suatu jaringan. Yaitu setiap paket yang ada tidak memiliki keterkaitan dengan paket sebelumnya. *Autocorrelation* memiliki rumus:

$$= — \quad (2)$$

R_k = *Autocorrelation*
C_k = Waktu kedatangan antar paket
C_0 = Varians

2.4.2. Hyperbollicaly Decay

Hyperbollicaly decaying merupakan penurunan (*decay*) dari *autocorrelation* yang menandakan bahwa penurunan tersebut lebih lambat dibandingkan penurunan eksponensial (Sheluhin, et al., 2007), *hyperbollicaly decay* memiliki rumus:

$$R(k) \cong (k)^{2H-2} L(t) \quad (3)$$

R_k = *Autocorrelation*
H = nilai *Hurst*
$L_{(t)} = 1/\log_{(t)}$

2.4.3. Autocovariance

Covarians merupakan sebuah perhitungan seberapa banyak dua buah variabel acak berubah secara bersamaan. Apabila nilai suatu variabel yang lebih besar berhubungan dengan nilai yang lebih besar pula, maka aan terjadi hal yang sama pula dengan nilai yang lebih kecil. Apabila nilai covarians tersebut berniali positif, maka menandakan bahwa adanya kesamaan sifat pada variabel tersebut, sedangkan apabila bernilai negative, menandakan bahwa adanya kecenderungan linear dalam variabel tersebut. *Autocovarians* merupakan suatu fungsi yang menghitung covarians proses tersebut dengan dirinya sendiri dalam waktu tertentu. Apabila *autocovarians* dinormalisasi dengan cara membagi *autocovarians* tersebut dengan varians (σ^2), maka akan menghasilkan *autocorrelation* dari fungsi tersebut, maka rumus dari *autocovarians* adalah:

$$= — \qquad (4)$$

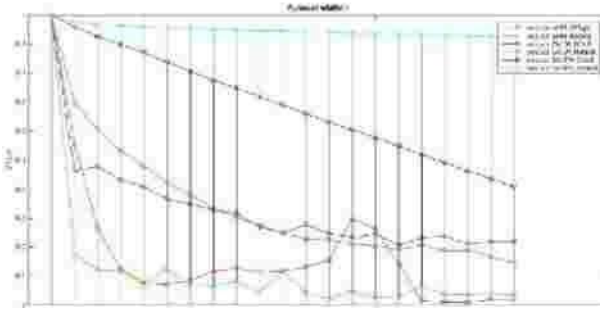
r_k = *Autocovarians*
R_k = *Autocorrelation*
σ^2 = Varians

3. Pembahasan

Penggunaanan deteksi trafik anomali dengan analisis tingkah laku LRD dalam internet trafik merupakan sesuatu hal yang baru. Seperti yang sudah dijelaskan sebelumnya, LRD memiliki tiga ciri khas utama. Ketiga ciri khas utama tersebut adalah *autocorrelation*, *hyperbollicaly decay*, dan *autocovarians*. Ketiga ciri khas ini memiliki peranan penting dalam menentukan trafik normal dan trafik anomaly. Input dari simulasi ini adalah dataset CAIDA normal dan DARPA normal untuk pengecekan trafik normal dan trafik CAIDA DdoS dan DARPA DDoS untuk trafik DDoS, seluruh dataset tersebut telah diakui validitasnya dalam penelitian-penelitan sebelumnya. Sementara untuk dataset flashcrowd digunakan dataset *World Cup 1998*. Analisis terbagi ke dalam empat bagian yaitu estimasi eksponen Hurst, peningkatan stasioner, perubahan skala spasial, dan proses agregat.

3.1. Pengujian sifat *autocorrelation*.

Dalam proses pengecekan nilai *autocorrelation* (R_k) ini dilakukan dengan menggunakan lima buah dataset dengan tiga jenis trafik yang berbeda, yaitu dataset WC'98, dataset CAIDA DDoS, dataset CAIDA normal, dataset DARPA DDoS, dataset DARPA Normal, data yang diambil dari setiap dataset adalah *count/s* sebanyak 1500 data dari detik ke 0-1500. Pada proses ini dicari nilai *autocorrelation* dari kelima dataset tersebut, setelah itu dilakukan pengecekan dari nilai *autocorrelation* kelima dataset tersebut. Pengecekan yang dilakukan adalah dengan melihat apakah ada nilai *autocorrelation* yang minus atau tidak, apabila ada maka nilai *autocorrelation* dataset tersebut tidak menuju tak hingga ($R_k \neq \infty$). Apabila tidak terdapat niai minus maka *autocorrelation* tersebut dikatakan menuju tak hingga ($R_k = \infty$). Selain itu pengecekkan ini juga bertujuan untuk menentukan apakah dataset yang digunakan memiliki salah satu sifat LRD yaitu nilai *autocorrelation* yang menuju tak hingga ($R_k = \infty$).



Gambar 2 Pengujian autocorrelaton seluruh dataset

Dari hasil yang didapat pada pengecekkan nilai autocorrelation yang ditunjukkan pada gambar 2, menunjukan bahwa pada dataset trafik normal yaitu CAIDA normal (garis magenta) dan DARPA normal (garis hijau) memiliki nilai *autocorrelation* yang menuju tak hingga, hal yang sama juga terjadi pada trafik *worldcup* pagi hari (garis biru) dan *worldcup* sore hari (garis biru muda) yang juga memiliki nilai *autocorrelation* yang menuju tak hingga. Sedangkan dalam trafik DDoS memiliki hasil *autocorrelation* yang sama pula, yaitu pada dataset DDoS DARPA (garis hitam) memiliki hasil autocorrelation menuju tak hingga dan pada dataset CAIDA DDoS (garis merah) memiliki *autocorrelation* yang menuju tak hingga pula. Meskipun seluruh dataset tersebut telah memenuhi salah

satu sifat LRD akan tetapi hasil dari nilai autocorrelation ini masih belum tentu menunjukkan bahwa trafik tersebut merupakan *Long Range* atau *Short Range*.

3.2. Hasil *Hurst Estimator Periodogram*

Dalam pencarian nilai *hurst* digunakan rumus (4) pada hal.9, dalam mencari nilai hurst, yang dilakukan pertama adalah dengan melakukan *Fast Fourier Transform* (FFT) pada data yang diteliti, FFT dilakukan untuk mengubah domain data tersebut kedalam domain frekuensi. Setelah itu hasil FFT tersebut akan dikalikan dengan $\frac{1}{2n}$. Pada pencarian nilai *hurst* ini dataset yang digunakan sama dengan

dataset yang digunakan pengujian sebelumnya yaitu dengan menggunakan lima buah dataset dengan tiga jenis trafik yang berbeda, yaitu dataset *WC'98*, dataset CAIDA DDoS, dataset CAIDA normal, dataset DARPA DDoS, dataset DARPA Normal, data yang diambil dari setiap dataset adalah *count/s* sebanyak 3790 data dari detik ke 0-3790. Berikut ini adalah hasil pencarian nilai *hurst* :

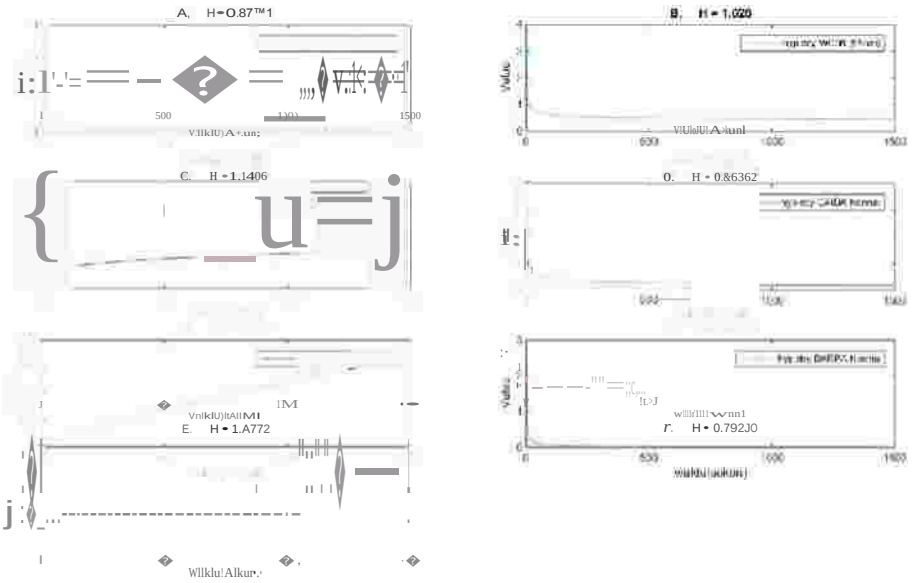
Dataset	Nilai *Hurst*
World Cup'98 pagi hari	0.8777
World Cup'98 sore hari	1.0260
CAIDA DDoS	1.1406
CAIDA Normal	0.9636
DARPA DDoS	1.4772
DARPA Normal	0.7924

Table 1 Hasil Hurst

Berdasarkan tabel 4-1, nilai hurst yang didapat untuk dataset normal yaitu CAIDA normal dan DARPA Normal mendapatkan nilai *hurst* 0.9636 (CAIDA) dan 0.7924 (DARPA), hal ini sesuai dengan penelitian yang telah ada yaitu dataset normal berada pada nilai $0.5 \leq H \leq 1$ dan memenuhi sifat LRD. Untuk dataset DDoS, yaitu CAIDA DDoS dan DARPA DDoS memiliki nilai *hurst* 1.1406 (CAIDA) dan 1.4772 (DARPA), hasil ini juga sesuai dengan penelitian yang telah ada yaitu untuk dataset DDoS terdapat diluar jangkauan dari nilai dataset normal dan tidak memenuhi. Sedangkan untuk hasil dari dataset *WC'98* mendapatkan nilai *hurst* 0.8777 untuk *WC'98* pagi dan 1.0260 untuk *WC'98* sore hari. Hal ini menandakan bahwa dataset *WC'98* masih tergolong kedalam trafik normal, tetapi untuk semakin memperjelas apakah dataset tersebut memenuhi sifat LRD maka dilakukan pengujian untuk LRD tahap kedua yaitu pengujian sifat *Hyperbollicaly Decaying Covariance*.

3.3. Pengujian sifat *hyperbollicaly decay*

Dalam pengecekkan ini, parameter nilai H (*hurst*) merupakan parameter terpenting, karena nilai H tersrbut yang menunjukkan apakah trafik tersebut *hyperbolic decaying* atau tidak. Pengecekkan ini bertujuan untuk menentukkan apakah dataset yang digunakan memenuhi salah satu sifat dari LRD. Dalam proses ini data yang digunakan masih sama dengan data sebelumnya yaitu dengan menggunakan lima buah dataset yang sama. Pada proses ini yang dilakukan pertama adalah mencari nilai *hurst*, setelah itu nilai *hurst* yang didapat akan dijadikan parameter sesuai dengan rumus (3). Berikut ini adalah hasil *hyperbollicaly decay* berdasarkan nilai *hurst* yang didapat pada tabel 1.

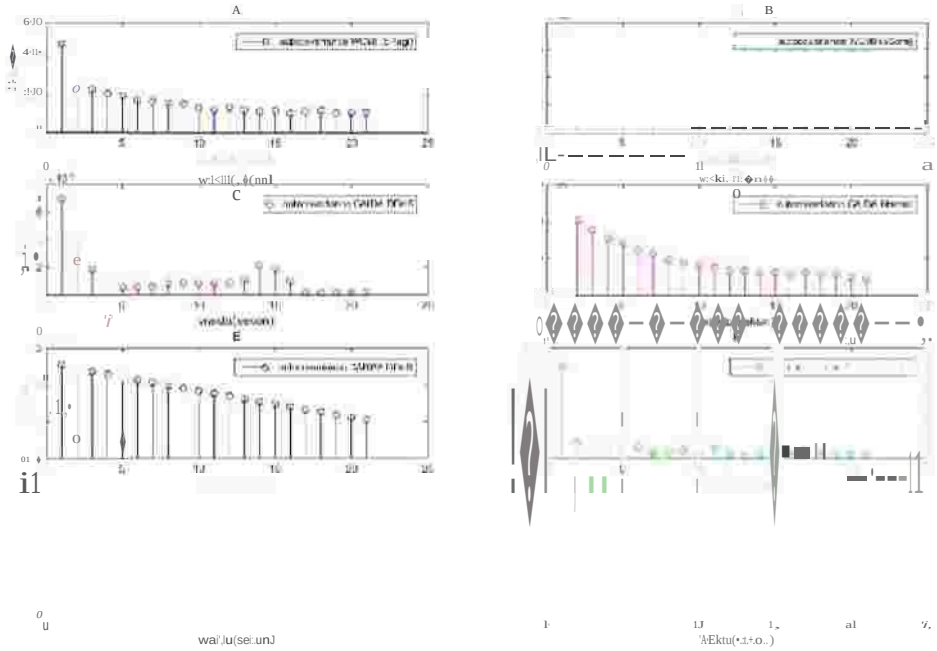


Gambar 3 Hasil Hyperbollicaly Decay WC'98 *5Pagi (A),* WC'98 *5Sore (B), CAIDA DDoS (C), CAIDA Normal (D), DARPA DDoS (E), DARPA Normal (F)*

Dari hasil pengecekkan yang didapat sesuai dengan gambar 3, dataset *world cup'98* pagi hari (A) dan *world cup'98* sore hari (B) yang merupakan dataset *flashcrowd* dengan nilai *hurst* 0.8777 (pagi) dan 1.0260 (sore) memiliki *hyperbollicaly decay*, begitu pula dengan dataset normal yang terdiri dari dataset CAIDA normal (D) dan DARPA normal (F) dengan *hurst* 0.9636 (CAIDA normal) dan 0.7924 (DARPA normal) juga memiliki *hyperbollicaly decay*. Sedangkan pada dataset DDoS, terdapat perbedaan hasil, pada dataset CAIDA DDoS (C) dengan *hurst* 1.1406 tidak memiliiki *hyperbollicaly decay*, tetapi terbentuk *hyperbollicaly growth*, begitu pula pada dataset DARPA DDoS (E) dengan *hurst* 1.4772 tidak memiliki *hyperbollicaly decay*. Maka dari hasil yang didapat dapat diambil kesimpulan bahwa *hyperbollicaly decay* terjadi apabila nilai *hurst* trafik tersebut berada pada range 0.5<H<1.03, hal ini sama dengan penelitian yang telah ada sebelumnya.

3.4. Pengujian sifat *autocovarians*

Proses dalam tahap ini yaitu, akan dicari nilai *autocovarians* dari dataset yang digunakan dan akan dilakukan pengecekan nilai *autocovarians* tersebut, apabila dataset yang diteliti memiliki nilai *autocovarians* negative, maka dataset tersebut akan dianggap nilai *autocovarians* nya tidak menuju tak hingga, apabila tidak terdapat nilai negatif maka nilai *autocovarians* dataset tersebut dianggap menuju tak hingga, pengecekkan ini dilakukan sebagai pendukung keputusan apakah dataset tersebut memiliki sifat LRD atau tidak, karena apabila dataset tersebut memiliki sifat LRD, maka nilai *autocovariansnya* akan menuju tak hingga. Dalam pengujiannya dataset yang digunakan sama seperti pengujian sebelumnya yaitu lima buah dataset yang tersdiri dari dataset WC'98, CAIDA DDoS, CAIDA normal, DARPA DDoS ,dan DARPA normal. Fitur yang digunakan juga sama seperti sebelumnya, yaitu count/s sebanyak 1500 data dimulai dari detik ke- 0-1500. Gambar 4 adalah hasil dari proses ini.



Gambar 4 Hasil Autocovarians WC'98 *5Pagi (A),* WC'98 *5Sore (B), CAIDA DDoS (C), CAIDA Normal (D), DARPA DDoS (E), DARPA Normal (F)*

Hasil yang didapat pada pengecekan hasil *autocovarians* sesuai dengan gambar 4-16, bentuk *autocovarians* yang hampir menyerupai dengan hasil yang didapat dengan hasil *autocorrelation*, pada dataset normal, baik CAIDA normal (D) dan DARPA normal (F) tidak memiliki nilai negative sehingga dapat dikatakan bahwa nilai *autocovarians* dari dataset tersebut menuju tak hingga dan memenuhi parameter sebagai LRD, begitu pula dengan dataset *WC'98* pagi hari (A), *WC'98* sore hari (B), CAIDA DDoS (C), dan DARPA DDoS (F) yang juga memiliki nilai *autocovarians* yang menuju tak hingga dan memenuhi sifat sebagai LRD. Nilai *autocovarians* yang menuju tak hingga menandakan bahwa hubungan kesamaan antar data dalam waktu yang berbeda sangat kuat, sehingga penurunan yang terjadi tidak sampai membuat nilai *autocovarians* menjadi nol atau minus. Sedangkan nilai *autocovarians* yang negative menandakan hubungan kesamaan antar data pada waktu yang berbeda tidak kuat dan berkurang dengan cepat, sehingga nilai *autocovarians* menjadi nol atau minus pada waktu tertentu.

Dari hasil yang didapat dari tiga tahapan pengujian sifat LRD, didapatkan hasil bahwa pada dataset normal DARPA dan CAIDA, menunjukkan bahwa dataset tersebut memiliki sifat LRD, hal ini dibuktikan dengan nilai autocorrelation yang menuju tak hingga, memiliki hyperbollicaly decay, dan juga memiliki hubungan kesamaan antar data yang kuat pada waktu yang berbeda berdasarkan hasil autocovarians. Pada dataset WC'98 yang merupakan dataset untuk flashcrowd juga menunjukan bahwa data tersebut memiliki sifat LRD, begitu pula ditunjukan oleh hasil dati dataset DARPA DDoS. Sedangkan pada dataset CAIDA DDoS menunjukan bahwa datast tersebut tidak memenuhi kriteria sifat LRD, hal ini dibuktikan dengan nilai autocorrelation tidak menuju tak hingga, tidak terbentuknya hyperbollicaly decay, dan hubungan antar data yang menurun drastis sehingga nilai autocovarians menjadi nol atau minus pada waktu tertentu, maka dengan hasil tersebut dataset CAIDA DDoS memiliki sifat SRD.

Selain itu hubungan nilai H dengan sifat LRD juga sangat erat karena nilai H tersebut sebagai penentu apakah terjadi hyperbollycali decay atau tidak, nilai H yang optimal dalam pembentukan hyperbollicaly decay adalah pada nilai 0.5< H <1.03 karena pada jangkauan nilai tersebut, hyperbollycaly akan terbentuk, sedangkan apabila nilai H kurang atau lebih dari jangkauan tersebut, hyperbollycaly decay tidak akan terbentuk, karena terjadi hyperbollicaly growth pada data tersebut.

4. Kesimpulan

Dari hasil analisis yang dilakukan pada penelitian ini dapat diambil beberapa kesimpulan bahwa *Long Range Dependence* dapat digunakan untuk mendeteksi anomaly trafik, hal ini dibuktikan dengan hasil yang didapat, hasil pengujian dataset normal dan flashcrowd menunjukkan bahwa kedua jenis trafik tersebut memiliki sifat LRD, sedangkan hasil pengujian trafik DDoS tidak memiliki sifat LRD.

Nilai *hurst* yang menjadi salah satu parameter dalam pengujian memiliki nilai yang tidak pasti, dikarenakan setiap data yang berbeda akan menghasilkan nilai *hurst* yang berbeda pula, rentang nilai *hurst* yang memenuhi untuk memiliki sifat LRD adalah $0.5 \leq H \leq 1.03$ karena pada rentang tersebut *hyperbollicaly decay* dapat terbentuk.

Saran pengembangan selanjutnya dari metode ini adalah dengan menggabungkannya dengan metode pendeteksian yang lain, sehingga dapat menghasilkan suatu metode yang memiliki tingkat akurasi lebih baik.

Daftar Pustaka

Brignoli, D., 2008. *DDoS Detection Based On Traffic Self-Similarity,* New Zealand: University of Canterbury.

Li, M., 2004. An Approach to Reliably Identifying Signs of DDOS Flood Attacks on LRD Traffic Pattern Recognition. *Computers & Security,* April, 23(7), pp. 549-558.

Purwanto, Y., K., H. & Rahardjo, B., 2014. Survey : Metode dan Kemampuan Sistem Deteksi Anomali Trafik. *Security and Protection.*

Sheluhin, O. I., Smolskiy, S. M. & Osin, A. V., 2007. *Self-Similar Processes in Telecommunications.* Chicester: John Wiley & Sons Ltd..