ANALISA SERANGAN DISTRIBUTED DENIAL OF SERVICE DAN FLASH CROWDS

MAKALAH TUGAS KULIAH
Operasi Keamanan dan Incident Response
EL6115

Oleh
MADE INDRA WIRA PRAMANA
NIM : 23215323

Dosen
DR. IR. BUDI RAHARDJO

SEKOLAH TEKNIK ELEKTRO DAN INFOMATIKA
PROGRAM MAGISTER TEKNIK ELEKTRO
INSTITUT TEKNOLOGI BANDUNG
2016

ABSTRAK

Abstrak – *Distributed Denial of Service* (DDoS) merupakan serangan yang dilakukan dengan membanjiri jaringan, server, ataupun situs web secara masif. Tujuan serangan DDoS adalah menghabiskan kapasitas akses yang tersedia, sehingga pelayanan jaringan akan terhenti. Selain DDoS, pelayanan jaringan juga dapat terhenti jika terjadi *flash crowds,* event ini terjadi saat terdapat berita besar sehingga jaringan diakses secara masif dalam saat yang bersamaan. Hal utama yang membedakan antara serangan DDoS dan *flash crowds* adalah kemunculannya, jika DDoS terjadi secara instan, peningkatan *traffic* jaringan saat *flash crowds* terjadi secara gradual. *Traffic* DDoS hanya memiliki tujuan untuk menghabiskan kapasistas akses, sedangkan *traffic flash crowds* adalah *request* yang legal, karena itu untuk mengatasi DDoS tanpa menghentikan layanan, diperlukan pertimbangan tertentu. Hal ini dibutuhkan, misalnya dalam membangun sebuah *intrusion detection system* (IDS), maka IDS tersebut harus dapat membedakan antara serangan DDoS dan *flash crowds.* Penelitian yang terkait dengan DDoS dan *flash crowds* biasanya menggunakan analisa terhadap dataset *traffic* yang sudah tersedia, yaitu dataset DARPA 1998 dan World Cup 1998.

Kata kunci: *distributed denial of service, flash crowds, traffic*.

DAFTAR ISI

Bab I Pendahuluan

I.1 Latar Belakang

Pengguna internet hingga tahun 2016 telah mencapai angka 3,5 miliar [1], angka tersebut didominasi oleh pengguna dari Benua Asia sekitar 48,4% dari total pengguna. Dengan sekian banyak pengguna internet, sektor bisnis mengalami keuntungan besar dengan angka penjualan tahunan mencapai US$2,2 triliun [2], nilai tersebut tidak akan dicapai dengan mudah tanpa adanya internet. Keberadaan internet memang telah membawa banyak manfaat, banyak pihak mengunakan peluang yang didapat dari internet untuk melakukan berbagai hal, contohnya berita yang awalnya hanya berupa media cetak mulai diterbitkan secara elektronik, pembelajaran dapat dilakukan secara jarak jauh melalui video, perbankan dapat memberi layanan melalui internet, dan masih banyak contoh lainnya yang dapat dilihat secara nyata di kehidupan sehari-hari. Di sisi lain, banyak resiko yang timbul dari penggunaan internet, misalnya pencurian informasi sensitif, persaingan tidak sehat, hingga pencucian uang.

Distributed denial-of-service (DDoS) adalah salah satu serangan siber yang ditargetkan pada pelayanan, dengan DDoS, *availability* dari pelayanan menjadi ancaman utamanya. Secara umum, DDoS diluncurkan dengan cara mengirim paket yang berjumlah banyak dalam rentang waktu yang lama atau dengan mengirim paket berukuran besar dalam waktu yang instan, sehingga *server* akan mengalami *crash* akibat kelebihan beban *traffic*. Pada tahun 2016 telah terjadi setidaknya 9.630 insiden serangan DDoS dengan target utamanya menyasar industri permaninan online, informasi teknologi, layanan IT, dan sektor keuangan [3]. Pelayanan *server* tidak hanya bisa berhenti akibat adanya serangan DDoS, *server* juga dapat mengalami kelebihan beban *traffic* jika akses menuju *server* dilakukan oleh *client* yang jumlahnya melebihi *resource* yang dialokasikan oleh *server* tersebut. Fenomena ini disebut *flash crowds*, meskipun memiliki kesamaan efek, *flash crowd* bukan merupakan serangan siber layaknya DDoS, karena itu penyedia layanan harus dapat membedakan antara fenomena *flash crowds* dan serangan DDoS untuk dapat mengadakan pelayanan tanpa menghentikan *request* yang legal.

I.2 Rumusan Masalah

Kemunculan *flash crowds* dan serangan DDoS dapat terjadi secara bersamaan, bahkan penyerang mulai mengaburkan serangan DDoS hingga menyerupai *flash crowds* sehingga sulit untuk dibedakan. Kegagalan *server* melayani *client* adalah salah satu tujuan dari serangan DDoS. Untuk dapat membedakan antara kedua *traffic,* diperlukan metode-metode khusus, metode tersebut tentunya dibangun berdasarkan landasan yang kuat, misalnya dengan memerhatikan jumlah paket per waktu dalam jaringan atau jumlah *request* per *client*.

I.3 Tujuan Penelitian

Penelitian ini dilakukan untuk membuktikan adanya perbedaan antara serangan DDoS dan *flash crowd.* Selain mencari perbedaan, penelitian ini juga dilakukan untuk mencari metode yang tepat untuk mengatasi masalah tersebut. Dari penelitian ini, penyedia layanan dapat mengambil langkah yang tepat untuk mengatasi kedua masalah tersebut dengan pendekatan yang berbeda untuk masing-masing insiden.

I.4 Batasan Masalah

Penelitian berfokus pada karakteristik yang dapat membedakan antara serangan DDoS dan *flash crowds*. Metode-metode yang dapat digunakan untuk membedakannya memanfaatkan karakteristik kedua jenis *traffic* tersebut dijabarkan dalam pembahasan.

Bab II Tinjauan Pustaka

II.1 Distributed Denial of Service (DDoS)

Dalam keamanan informasi, terdapat sebutan "CIA Triad" yang mengacu pada tiga aspek utama, yaitu *confidentiality, integrity,* dan *availability.* Serangan DDoS secara khusus menyasar aspek *availability* dengan cara menghabiskan *resource* yang dimiliki *server.* Serangan DDoS terkadang sulit untuk dideteksi, selain karna *spoofing,* serangan DDoS juga dilakukan dengan memanfaatkan *bot, bot* tersebut adalah komputer-komputer yang telah terinfeksi *malware* sehingga dapat dikendalikan oleh penyerang, perangkat tersebut bisa juga disebut *zombie.* Jika komputer telah terjangkit *malware* dan menjadi *zombie,* penyerang akan mengirimkan perintah ke seluruh *bot* untuk melakukan serangan ke alamat tertentu. Tidak semua orang bisa melakukan serangan DDoS, tapi jasa DDoS ini tersedia dengan harga sewa US$10-US$1.000 per hari [4] di pasar gelap. Pada tahun 2016 telah tercatat *traffic* DDoS dengan rata-rata 5.51Gbps [3].

Penelitian terkait pencegahan DDoS sering kali menggunakan *dataset* KDD Cup [5] dan DARPA [6] sebagai *test case,* sayangnya analisa *dataset* KDD Cup menunjukan *dataset* memiliki kekurangan yang memengaruhi performanya, sehingga tidak derekomendasikan untuk penelitian [7]. Teknik dalam serangan DDoS sangat beragam, dalam *dataset* DARPA [6], beberapa jenis dengan rincian sebagai berikut :

a. Apache2 : Targetk serangan adalah *web server* apache, karakteristik serangan ini adalah serangan dilakukan dengan mengirim *http request* dengan *header* yang berjumlah lebih dari seharusnya. Saat serangan ini dilakukan, beban server dapat meningkat hingga 5 kali atau lebih dari beban normal.
b. Arppoison : Tujuan serangan ini untuk menipu *hosts* pada *ethernet* yang sama untuk salah mengenal *Mac address* alamat-alamat yang ada di dalam jaringan, karena itu penyerang harus berada dalam jaringan lokal tersebut.

Karakteristik serangan ini adalah serangan memanfaatkan *protocol* ARP untuk mengacaukan *request*.

c. Back : Target serangan adalah *web server* apache, berbeda dengan Apache2, serangan ini memiliki karakteristik dimodifikasi pada URL yang dikirimkan sehingga memuat banyak *frontslash* "/". Jika menerima *request* ini, *server* akan disibukkan dengan proses membaca URL yang panjang, sehingga antrian dalam *server* meningkat.

d. Chrashiis : Target serangan adalah *web server* NT IIS, karakteristik serangan ini adalah GET *request* yang *malformed* lewat telnet menuju *port* 80.

e. Dosnuke : Serangan dilakukan dalam sambungan NetBios, karakterisitknya serangan dilakukan dengan mengirim data Out of Band ke *port* 139.

f. Land : Memanfaatkan kelemahan pada TCP/IP versi lama, serangan ini tidak dapat dilakukan pada TCP/IP versi baru karena celah keaman ini hanya ada di versi lama, karakteristik serangan ini adalah paket yang dikirim berbentuk SYN dengan alamat *source* dan *destination* yang sama.

g. Mailbomb : Serangan DDoS tidak hanya dalam bentuk *request*, email juga dapat digunakan sebagai media serangan, jumlah mail yang berlebihan akan memenuhi antrian server dan dapat menyebabkan *crash*, karakteristiknya adalah jumlah mail yang banyak, jumlah mail yang dianggap mailbomb berbeda-beda pada tiap server.

h. SYN Flood : Setiap aplikasi TCP/IP rentan terhadap serangan ini, karakteristiknya adalah jumah paket SYN dikirimkan dari alamat dalam host yang *unreachable.*

i. Ping of Death : Salah satu bentuk serangan yang sederhana adalah paket ICMP (ping) yang memiliki karakteristik ukuran lebih dari 64.000 bytesm serangan ini hanya efektif pada OS versi lama.

j. Self ping : Dengan satu paket ping, sebuah perangkat dapat mengalami *crash*, karakteristiknya adalah *multicast interfcae* yang digunakan dalam paket *echo_request* adalah *localhost*.

k. Smurf : Serangan dengan paket ping dapat dilakukan dari pihak bukan penyerang, caranya adalah dengan *IP spoofing* menggunakan *IP address* korban, saat penyerang mengirimkan *echo request* dengan alamat korban, maka korban akan menerima *echo replies* dalam jumlah banyak, karakteristik serangan ini adalah perangkat korban menerima *echo replies* saat perangkat tersebut tidak mengirimkan *echo request*.

l. Syslogd : Syslogd *service* pada Solaris *server* memiliki celah keamanan yang dapat dieksploitasi untuk *denial-of-service*, karakteristik serangan ini adalah *request* untuk melakukan *DNS lookup* pada suatu *IP address* yang tidak sesuai dengan *DNS record*.

m. TCP Reset : Sambungan pada *TCP connection* dapat diserang dengan mengirimkan paket *TCP reset* yang telah di-*spoof* sehingga sambungan terputus. Karakteristik serangan ini adalah paket yang dikirim tidak dikirim dari alamat yang asli, dapat dilihat dari sesi TCP.

n. Teardrop : Serangan pada TCP/IP versi lama ini dilakukan dengan mengirimkan paket yang urutannya tidak tepat, karena versi lama TCP/IP memiliki kesalahan dalam proses pengurutan paket. Karakteristik serangan ini adalah *fragmented IP datagrams* yang memiliki size yang salah.

o. UDP Strom : Efek dari UDP Storm adalah sistem melambat dan antrian yang panjang diakibatkan data stream yang tidak memiliki akhir di antara dua *UDP port*. Karakteristik serangan ini adalah sumber paket *spoofed* berasal dari luar jaringan.

II.2 Flash crowds

Istilah *flash event* pertama kali digunakan dalam [8] untuk mendeskripsikan kejadian yang menyebabkan terjadinya *flash crowds*, istilah ini digunakan agar studi yang dilakukan dapat menjelaskan karakteristik yang membedakan antara DDoS dan *flash crowds. Flash event* sering kali dipicu oleh kontroversi atau berita besar pada sebuah situs web, maka dari itu, karakteristik yang membedakannya dengan DDoS cukup sederhana, misalnya situs pendaftaran ulang akademik tidak akan dibanjiri *traffic* di saat selain masa pendaftaran ulang. Terjadinya *flash crowds* juga tidak hanya pada situs web yang sudah dikenal, misalnya *slashdot effect* [9] yang terjadi karena sebuah situs kecil disebutkan dalam situs yang ramai diakses, maka pengunjung dari situs besar ini akan mengakses situs kecil tersebut dan terjadi *flash crowds.* Data yang banyak digunakan dalam penelitian *flash crowds* adalah dataset World Cup 1998 [5], telah diugnakan dalam The Third International Knowledge Discovery and Data Mining Tools Competition, dataset ini memuat *request* yang diterima oleh situs web World Cup dari 30 April 1998 hingga 26 Juli 1998 dengan total sebanyak 1.352.804.107 *request* dalam bentuk *access log*.

Flash event terkadang dapat diprediksikan sebelum terjadi, misalnya saat rilis produk baru yang telah ditunggu-tunggu oleh publik, maka pada tanggal rilis tersebut kemungkinan akan *predictable flash event*. *Flash* event juga dapat terjadi saat bencana alam atau sebuah insiden besar, keejadian itu disebut *unpredictable flash event*. Dalam praktek, server web biasanya menggunakan *Content Distribution Network* (CDN) untuk menghindari beban *traffic* yang berlebihan. Dengan menggunakan CDN, konten dari situs web didistribusikan ke beberapa jaringan lain yang dapat meneruskannya ke pengguna, pengguna yang mengakses situs web akan disuguhkan konten dari jaringan CDN terdekat darinya, dengan begitu akses dapat dilakukan lebih cepat dan tidak harus mengakses server web dari situs tersebut secara langsung. Pada kenyatannya, CDN tidak selalu menjadi jawaban dalam mencegah terjadinya *flash crowds*, hal ini dapat disebabkan oleh beberapa alasan. Masalah lain adalah serangan DDoS dapat disamarkan menjadi mirip dengan *flash crowds*, sehingga semakin sulit untuk membedakan antara keduanya.

Bab III Pembahasan

III.1 Karakteristik Pembeda

Jika dilihat dengan mata telanjang, DDoS dan *flash crowds* sulit dibedakan karena sama-sama menghilangkan aspek *availability*. Pentingnya membedakan antara kedua *traffic* tersebut dikarenakan DDoS bukan merupakan *request* yang perlu dilayani, berbeda dengan *flash crowds* yang merupakan *request* dari pengunjung yang asli. Hasil penelitian Jung dkk [8] menemukan bahwa terdapat beberapa karakteristik yang dapat membedakan antara keduanya, karakteristik tersebut dapat dilihat pada Tabel III.1.

Tabel III.1 Karakteristik yang membedakan antara *flash crowds* dan *denial of service* didapat dari hasil penelitian Jung dkk [8].

Karakteristik	***Flash crowds***	***Denial of Service***
Volume *traffic*	Kenaikan jumlah *request* terjadi bersamaan, puncaknya dapat bervariasi.	
Jumlah dan distribusi *client*	Terjadi kenaikan jumlah *client,* distribusi diperkirakan mengikuti distribusi populasi dalam ISP dan jaringan.	Kenaikan jumlah *client* atau beberapa *client* mengirim *request* dalam jumlah besar, distribusinya tidak mengikuti distribusi populasi.
Penumpukan *cluster*	Penumpukan terjadi secara signifikan saat sebelum dan saat *flash crowds* terjadi.	Penumpukan sangat kecil.
Rerata *request* per *client*	Rerata *request* menurun seiring melambatnya *server*.	Rerata *request* stabil saat serangan terjadi, berbeda dari keadaan normal.
Berkas dalam *request*	Popularitas akses mengikuti distribusi menyerupai Zipf.	Tidak mengikuti distribusi akibat *request* yang sama atau pada berkas berukuran besar.

Dengan karakteristik tersebut, *server* dapat memantau jaringan sehingga saat terjadi penurunan performa dan *server* akan mengabaikan beberapa *request*, *server* dapat mengabaikan *malicious request* yang dihasilkan dari bot. Secara normal, *client* tidak akan mengakses berkas yang sama secara berulang-ulang kali, mengirimkan *request* dalam jumlah besar, atau meminta akses pada berkas berukuran besar. *Server* dapat mengawasi *client* dan mengabaikan *request* dengan ciri yang menyimpang dari keadaan normal. Tindakan lain yang dapat dilakukan dalam *server* adalah melakukan *clustering* pada saat jaringan dalam keadaan normal, *cluster* tersebut akan menjadi bahan pertimbangan untuk mengabaikan *request* yang tidak datang dari *cluster* tersebut atau memiliki perbedaan yang jauh.

Pembagian *traffic* dalam *cluster* tersebut didukung oleh riset yang dilakukan oleh Munz dkk [10]. Tahap yang dilakukan dalam perancangan model *network data mining* meliputi pemilihan data sebagai sampel, *preprocessing* untuk mempersiapkan data, *transformation* untuk merubah data agar dapat direkayasa dengan *data mining*, proses penggalian informasi dengan *data mining*, dan evaluasi sebagai akhir tahap. Pengumpulan ini mirip seperti metode pengumpulan *cluster* dari *traffic* yang pernah dilayani yang diajukan oleh Jung dkk [8]. Munz dkk menggunakan algoritma K-means untuk melakukan *clustering* pada dataset dan *traffic* yang telah dibuat, hasilnya menunjukan bahwa jarak antar *ping flood* ke *cluster* dari *traffic normal* menjauh, berarti, kemiripan antara keduanya semakin menurun, selain itu jarak terhadap *cluster* dari *traffic anomaly* mendekat, sehingga dapat disimpulkan bahwa *traffic* dari *ping flood* bukan merupakan *traffic normal*, hal ini juga dapat disebabkan oleh kemiripan antara karakteristik yang dimiliki *traffic anomaly* menyerupai karakteristik *ping flood*. Penelitian ini tidak memba

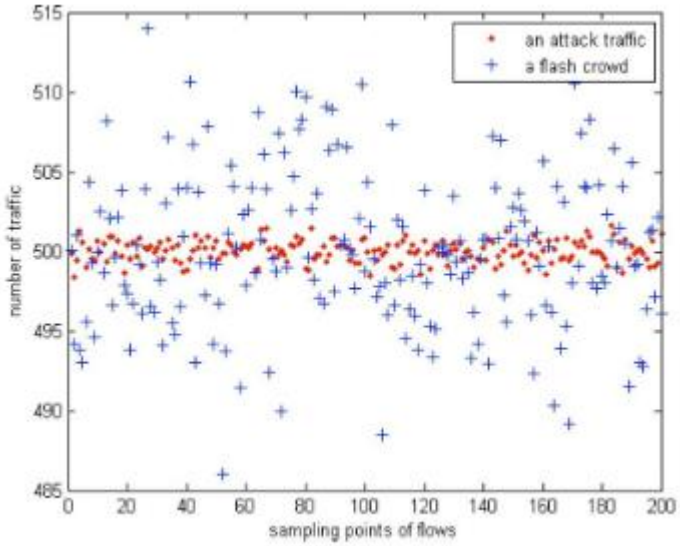
Lebih jauh, perbedaan *flash crowds* dan DDoS dapat diukur dengan perbedaan parametrik. Dalam penelitian Bhatia dkk [11] menjelaskan, dalam serangan DDoS, penyerang akan mengirim perintah secara serentak pada botnet untuk memaksimalkan serangan, sehingga *traffic* yang datang akan meningkat drastis dalam waktu singkat, sedangkan di kondisi *flash crowds* sangat kecil kemungkinan informasi menyebar secara bersamaan, sehingga peningkatan *traffic* terjadi secara

gradual. Dengan melihat perbedaan rerata kedatangan *traffic*, dapat dibedakan antara *traffic* DDoS dan *traffic flash crowds*. Jumlah kemunculan *request* dari alamat baru juga dapat digunakan sebagai pembanding, dalam *flash crowds* informasi menyebar secara luas seiring waktu, sehingga kemunculan alamat IP baru akan terjadi secara terus menerus namun, sedangkan dalam DDoS botnet menyerang secara bersamaan, sehingga *server* menerima *request* dari alamat IP baru dalam jumlah banyak dan terjadi secara bersamaan, setelah itu kemunculan alamat IP baru tidak akan terjadi secara signifikan seperti sebelumnya. Dari alamat-alamat tersebut akan dikirimkan *request* dalam jumlah besar untuk menghabiskan *resource* yang dimiliki oleh *server*, sehingga jumlah *request* per alamat IP akan sangat jelas terlihat, berbeda dengan pengunjung yang hanya mengirim *request* terkait informasi tertentu yang diinginkannya. Dari parameter tersebut, pengembangan pencegahan DDoS dapat dilakukan tanpa harus mengorbankan *request* dari pengunjung.

III.2 Flow Correlation

Penyerang dapat mengatur serangan DDoS yang dilakukan sedemikian rupa hingga menyerupai *traffic flash crowds,* metode ini dikenal dengan *flash crowds attack.* Penyedia layanan biasanya menggunakan *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA) untuk membedakan antara bot dan manusia. Ditinjau dari sisi pengguna, penerapan CAPTCHA justru membuat pengguna tidak nyaman. Menurut Yu dkk [12] alternatif yang dapat digunakan adalah dengan memerhatikan ciri-ciri yang dimiliki oleh bot, kinerja bot dimulai dari perintah yang dikirim oleh penyerang menuju botnet, dalam hal ini biasanya digunakan tools yang sama. Ciri lain adalah alir *traffic* serangan jika dilihat pada sisi korban serangan, merupakan *traffic* yang bersumber dari beberapa sumber berbeda, namun memiliki nilai standard deviasi yang tidak jauh berbeda, jika dibandingkan dengan nilai standard deviasi dari *traffic flash crowds* yang sebenarnya, nilai tersebut biasanya lebih kecil dari *traffic flash crowds*. Alasan perbedaan korelasi alir *traffic* adalah karena penyerang perlu menghasilkan *traffic* yang tinggi untuk dapat membuat korban mengalami *crash*, karena itu *traffic* yang

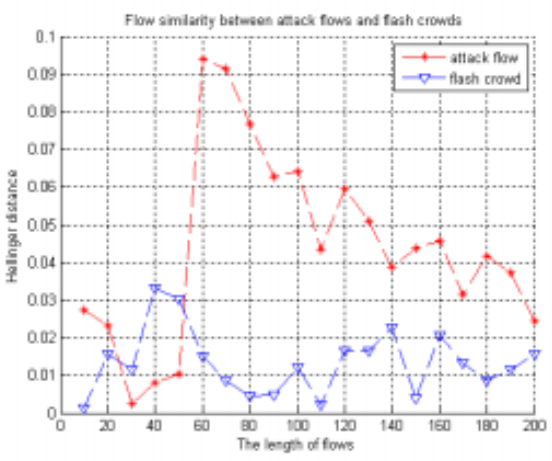
dibuat akan melebihi jumlah *traffic* pengguna yang asli. Perbedaan ini dapat dilihat pada Gambar III.1.



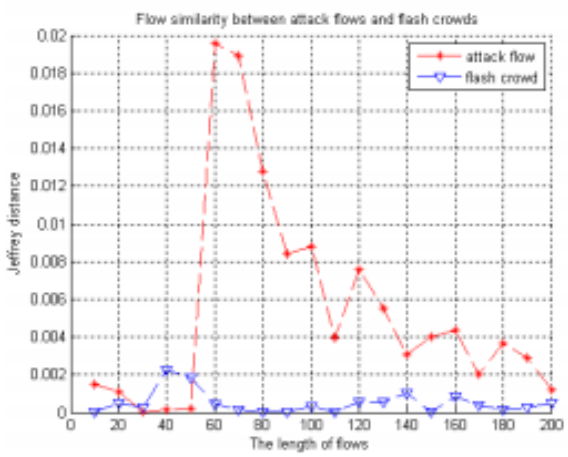
Gambar III.1 Alir *traffic* serangan memiliki perbedaan yang sedikit terhadap *traffic* serangan lain, sedangkan *traffic flash crowds* sangat bervariasi dalam alirannya [12].

III.3 Information Distance

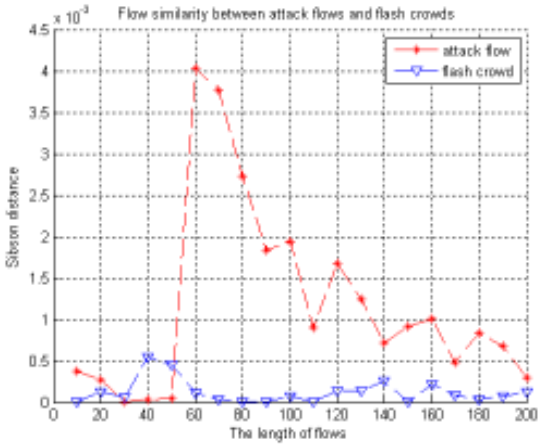
Paket yang dikirim dalam jaringan selalu melewati *router* dalam proses mencapai tujuannya, hal ini dimanfaatkan untuk bertukar informasi antar *router* yang berada di tempat berbeda oleh Yu dkk [13] untuk mengukur similaritas antar paket dalam router. Metode yang digunakan adalah mengambil sampel dari alir *traffic* dalam router, kemudian mengukur distribusi probabilitasnya, router lain melakukan hal yang sama, kemudian kedua router akan bertukar nilai distribusi probabilitas untuk dibandingkan. Pengukuran yang dilakukan menggunakan pengukuran jarak Helinger, Jeffreys, dan Sibson. Paket yang memiliki nilai jarak melebihi *threshold* yang ditentukan tidak akan dilayani, karena dianggap sebagai paket serangan. Eksperimen yang dilakukan Yu dkk [13] berhasil membedakan antara DDoS dan *flash crowds* dengan menggunakan metode ini, hasil terbaik didapat dari pengukuran Sibson dengan tingkat akurasi terbaik mencapai 65%. Hasil penelitian dapat dilihat pada Gambar III.2, Gambar III.3, dan Gambar III.4. Metode ini tidak hanya dapat dilakukan pada *router* yang berada dalam ISP yang sama, namun semua *router* dalam jaringan internet dapat dimanfaatkan untuk pertukaran informasi.



Gambar III.2 Nilai similaritas *traffic* diukur menggunakan pengukuran Helinger [13].



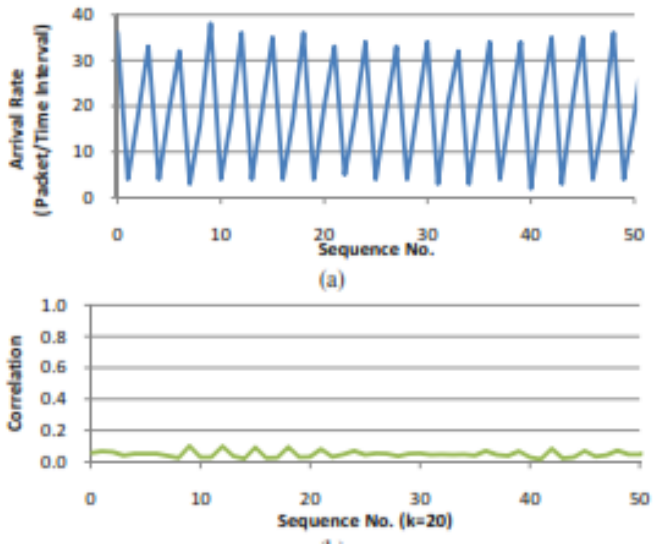
Gambar III.3 Nilai similaritas *traffic* diukur menggunakan pengukuran Jeffrey [13].



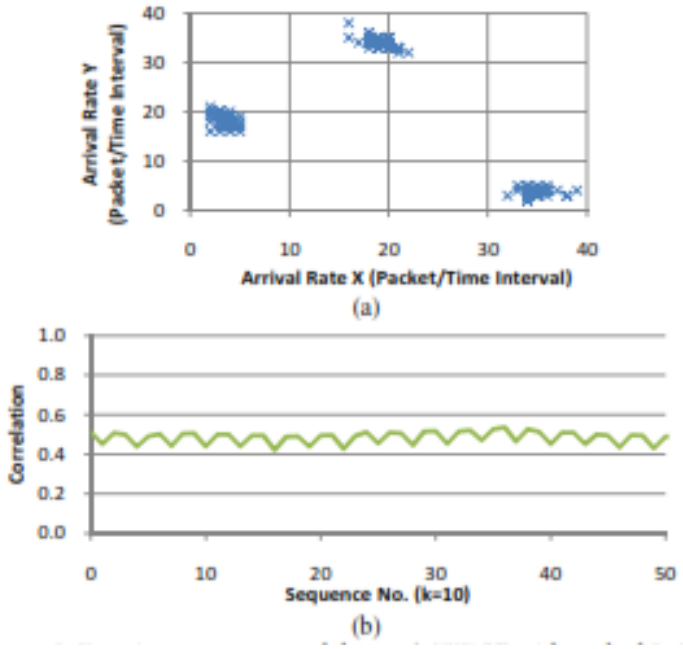
Gambar III.4 Nilai similaritas *traffic* diukur menggunakan pengukuran Sibson [13].

III.4 Packet Arrival

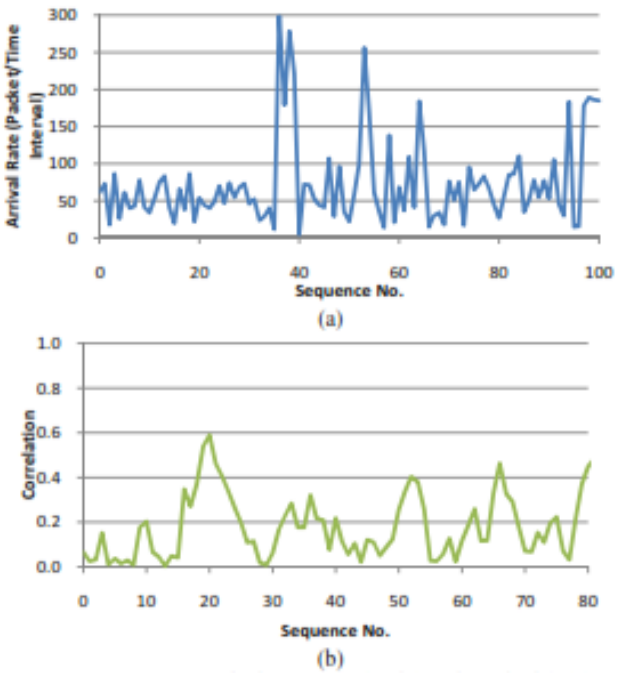
Misalkan pada suatu waktu terjadi *flash crowds,* jika penyerang melakukan serangan pada saat yang bersamaan, maka akan sulit untuk mendeteksi *traffic* serangan DDoS tersebut dan efek serangan DDoS akan muncul lebih cepat dikarenakan adanya *flash crowds.* Namun, dari penelitian yang dilakukan, kemunculan paket dari serangan DDoS memiliki pola yang dapat dikenali, berbeda dengan kemunculan paket *flash crowds* yang distribusinya acak karena dihasilkan oleh manusia, bukan melalui program seperti bot. Thapngam dkk [12] melakukan eksperimen pada tiga dataset sampel dengan dua metode yang berbeda, hasilnya pola kemunculan paket dapat dilihat dengan jelas, hasil tersebut dapat dilihat pada Gambar III.5, Gambar III.6, Gambar III.7, Gambar III.8, Gambar III.9, dan Gambar III.10. Menggunakan metode koefisien korelasi Pearson, pola dalam kemunculan paket dapat ditelusuri, metode korelasi pertama diambil dari rerata kemunculan dan waktu kemunculan, sedangkan metode korelasi kedua diambil dari rerata kemunculan saja. Korelasi berfungsi untuk mengukur ketergantungan dua variabel terhadap nilai yang diharapkan, hasil nilai korelasi memiliki rentangan dari -1 sampai 1. Untuk mengurani kesalahan deteksi, Thapngam dkk menggunakan *threshhold* sebagai pembatasan dalam analisanya, *threshold* tersebut dibagi menjadi batas atas dan batas bawah. Dataset pertama dan ketiga dalam eksperimen didapat dataset World Cup 98 [5], dataset pertama memiliki rerata kemunculan yang mirip dengan serangan, sedangkan dataset ketiga memiliki rerata kemunculan seperti *flash crowds*. Dataset kedua dari serangan Mstream memiliki rerata kemunculan yang acak. Eksperimen pertama mendeteksi dataset 1 sebagai serangan jika menggunakan metode 1 dengan tingkat *confidence* 94%, sedangkan metode 2 tidak mendeteksi serangan. Eksperimen kedua berhasil mendeteksi serangan menggunakan kedua metode yang ada dengan tingkat *confidence* 85%. Eksperimen ketiga tidak mendeteksi *flash crowds* sebagai serangan dengan tingkat *confidence* 85% sehingga *traffic* dapat dilayani oleh *server*.



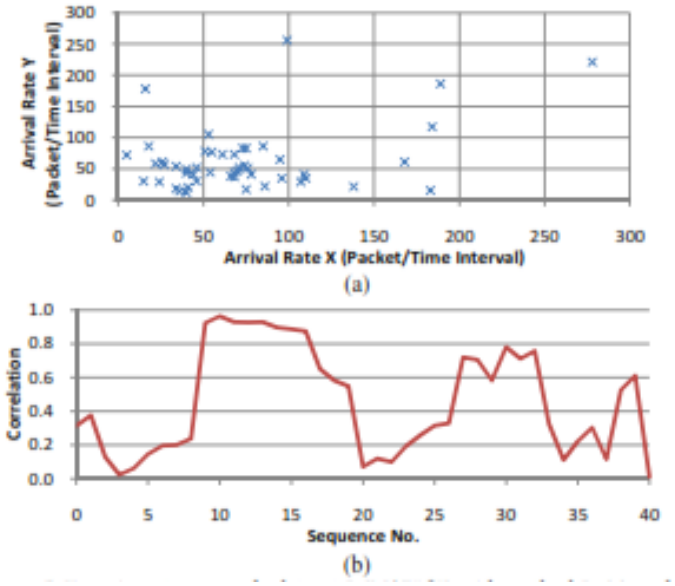
Gambar III.5 Percobaan pada dataset 1 menggunakan metode 1 dengan ukuran sampel k=20 [13].



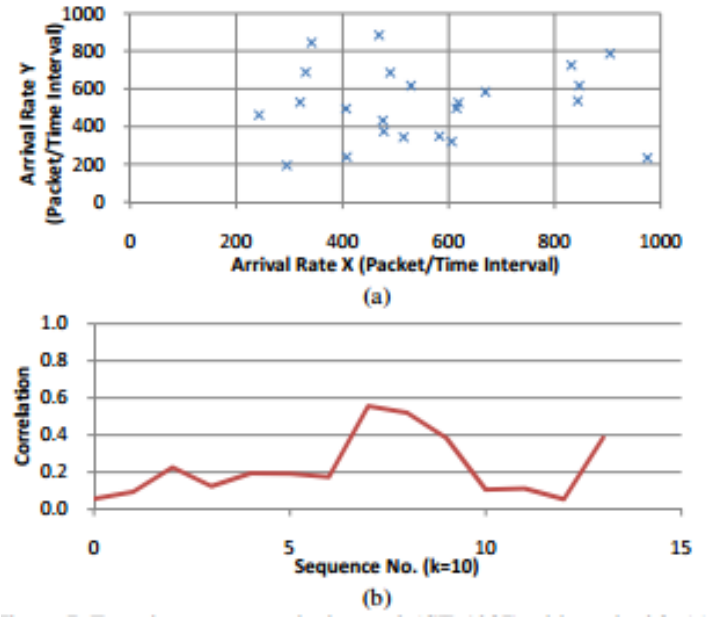
Gambar III.6 Percobaan pada dataset 1 menggunakan metode 2 dengan ukuran sampel k=10 [13].



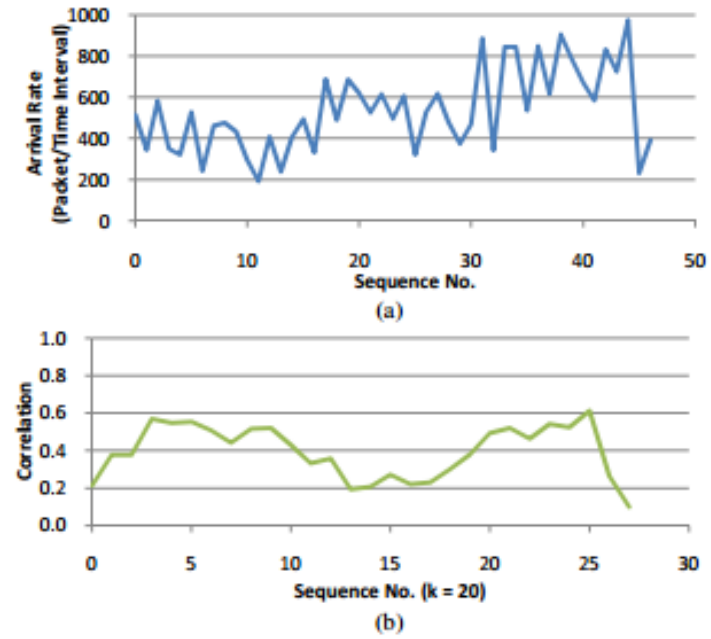
Gambar III.7 Percobaan pada dataset 2 menggunakan metode 1 dengan ukuran sampel k=20 [13].



Gambar III.8 Percobaan pada dataset 2 menggunakan metode 2 dengan ukuran sampel k=10 [13].



Gambar III.9 Percobaan pada dataset 3 menggunakan metode 1 dengan ukuran sampel k=10 [13].

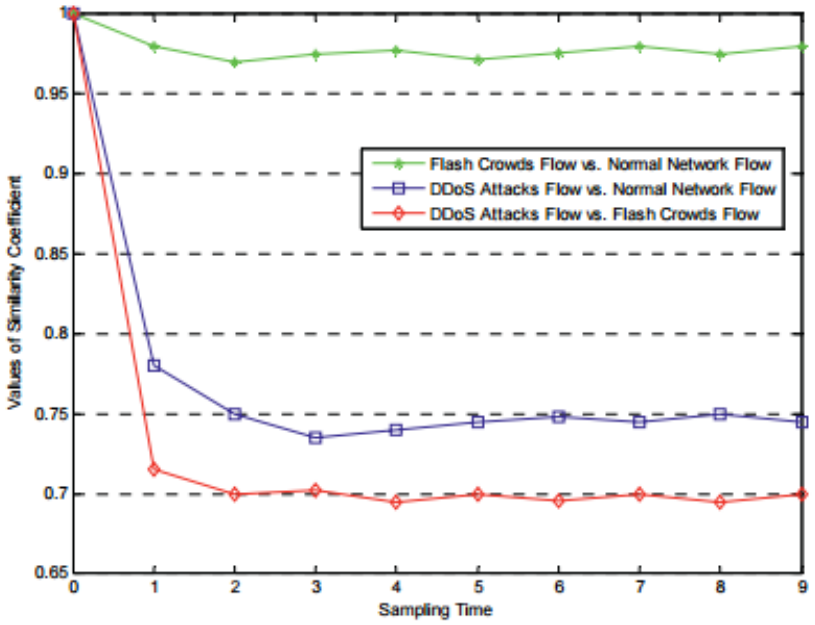


Gambar III.10 Percobaan pada dataset 3 menggunakan metode 2 dengan ukuran sampel k=20 [13].

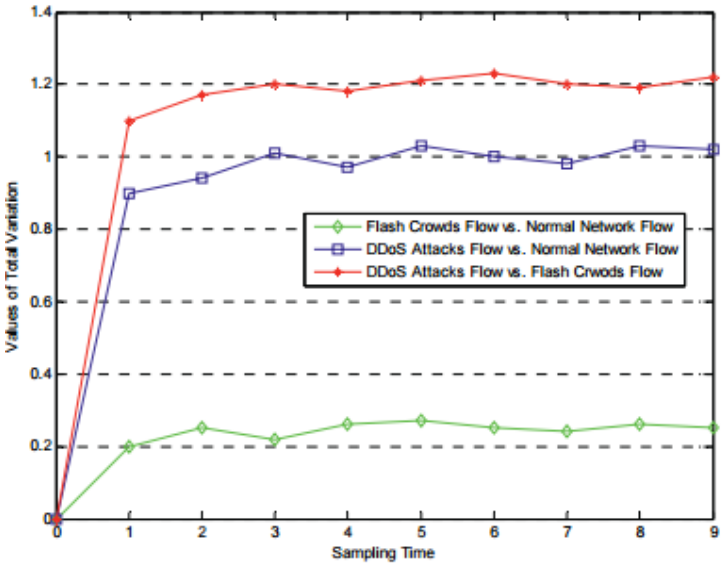
III.5 Probability Metrics

Pendekatan probabilitas dapat diginakan dalam membedakan serangan DDoS dan *flash crowds* seperti yang dilakukan oleh Li dkk [15] dengan menggabungkan pengukuran Bhattacharyya (*similarity coeficient*) dan *total variation*. Pengkuran

yang dilakukan hampir sama dengan *information distance* yaitu melibatkan pengukuran similaritas antara dua distribusi probabilitas memanfaatkan karakteristik yang membedakan serangan DDoS, *flash crowds* dan *traffic* normal yaitu tujuan akses; distribusi alamat IP *client;* dan peningkatan atau pengurangan kecepatan *traffic.* Tahapan yang dilakukan dimulai dari melakukan *sampling*, kemudian jumlah paket yang memiliki karakteristik tertentu seperti alamat IP dan ukuran paket akan dihitung dalam interval yang ditentukan, kemudian distribusi probabilitas akan dihitung secara paralel, selain itu *total variation* dan *similarity coefficient* juga dihitung secara paralel. Hasil akhir akan mengklasifikasi paket sebagai serangan DDoS jika nilai *total variation* dan *similarity coefficient* berada dalam *threshold* yang ditetapkan, sedangkan jika nilai *total variation* kurang dari batas atas *threshold* namun *similarity coefficeint* berada di atas batas bawah *threshold*, maka paket dianggap sebagai *flash crowds*. Kedua jenis *traffic* akan menghasilkan peringatan, namun hanya pakat dari *traffic* DDoS yang akan diabaikan. Nilai *total variation* dan *similarity coefficient* pada eksperimen dapat dilihat pada gambar.



Gambar III.11 *Total variation* pada ketiga jenis *traffic* [15].



Gambar III.12 *Similarity coefficient* pada ketiga jenis *traffic* [15]

III.6 Entropy Variation

Metode mengenali *traffic* DDoS dan *flash crowds* biasanya melibatkan pengumpulan sampel paket atau membutuhkan alokasi *resource* yang besar pada *router*, namun metode *entropy variation* yand diajukan oleh Katiyar dkk [16] tidak memerlukan kedua hal tersebut karena tidak melibatkan label paket. *Entropy variation* adalah konsep pengukuran perubahan dalam distribusi alir *traffic* pada *router* dalam waktu tertentu, dalam penelitian ini, fitur yang digunakan dalam penghitungan *entropy* adalah alamat IP sumber, alamat IP tujuan, port sumber, dan port tujuan. Metode *entropy variation* bertujuan untuk mendeteksi sumber penyerang dalam DDoS, misalkan dalam sebuah jaringan terdapat tiga alir *traffic* yang berbeda, satu alir *traffic* berupa *traffic* normal dan lainnya merupakan kombinasi *traffic* normal dan serangan DDoS. *Router* yang dilewati oleh *traffic* serangan DDoS akan mendeteksi peningkatan *traffic*, *router* yang tidak dilewati *traffic* serangan DDoS tidak akan mendeteksi hal tersebut, dengan *entropy* pada target serangan dan *router*, sumber serangan dapat diketahui, sehingga dapat dihentikan.

Bab IV Kesimpulan

IV.1 Kesimpulan

Dari penelitian ini dapat diambil kesimpulan sebagai berikut :

1. *Request* dari *client* saat *flash crowds* dikategorikan sebagai *traffic anomaly* namun pelayanan tidak dihentikan, berbeda dengan serangan DDoS yang harus diabaikan.
2. Meskipun memiliki kemiripan, karakteristik tertentu dapat digunakan sebagai pembanding antara kedua jenis *traffic*.
3. Metode dan karakteristik yang telah diteliti memungkinkan untuk membedakan antara serangan DDoS, *flash crowds*, dan *traffic* normal.
4. Server pelu terus memperbarui metode yang diterapkan karena beragamnya jenis serangan DDoS, sehingga dapat mengenali jika terdapat serangan jenis baru.

IV.2 Saran

Dari penelitian ini saran untuk penelitian selanjutnya sebagai berikut :

1. Pengembangan metode baru dengan algoritma lain dapat memanfaatkan karakteristik yang ada, sehingga diharapkan ke depannya muncul metode adaptif yang dapat mengenali *traffic anomaly* tanpa menghabiskan *resource.*
2. *Server* harus mengabaikan *traffic* serangan DDoS, namun tetap melayani *traffic* lain saat terjadi *flash crowds*, sehingga *server* harus menggunakan layanan seperti CDN untuk mencegah gangguan layanan *flash crowds*.

DAFTAR PUSTAKA

[1] InternetLiveStats.com, "Internet Users," [Online]. Available: http://www.internetlivestats.com/internet-users/. [Accessed 18 February 2017].

[2] J. Stevens, "Internet Stats & Facts for 2016," [Online]. Available: https://hostingfacts.com/internet-facts-stats-2016/. [Accessed 18 Feburary 2017].

[3] Verizon Enterprise, "Data Breach Investigations Reports," 2016.

[4] Symantech Corporation, "Internet Security Threat Report," 2016.

[5] M. A. a. T. Jin, "1998 World Cup Web Site Access Logs," August 1998. [Online]. Available: http://www.acm.org/sigcomm/ITA/. [Accessed 13 2 2017].

[6] LINCOLN LABORATORY, "DARPA INTRUSION DETECTION EVALUATION," MASSACHUSETTS INSTITUTE OF TECHNOLOGY , 1998.

[7] E. B. W. L. a. A. A. G. Mahbod Tavallaee, "A Detailed Analysis of the KDD Cup 99 Dataset," *IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2009)* , 2009.

[8] B. K. M. R. Jaeyeon Jung, "Flash Crowds and Denial of Service Attacks," in *International conference on World Wide Web*, Honolulu, 2002.

[9] P. M. M. B. T. Stading, "Crowds, Peer-to-Peer Caching Schemes to Address Flash," in *First International Workshop on Peer-to-Peer Systems*, 2002.

[10] S. L. G. C. Gerhard Munz, "Traffic Anomaly Detection Using K-Means Clustering," in *In GI/ITG Workshop MMBnet*, 2007.

[11] G. M. A. T. E. A. Sajal Bhatia, "Parametric Differences Between a Real-world Distributed Denial-of-Service Attack and a Flash Event," in *Sixth International Conference onAvailability, Reliability and Security*, 2011.

[12] W. Z. W. J. S. G. Y. X. F. T. Shui Yu, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," in *IEEE Transactions on Parallel and Distributed Systems*, 2011.

[13] S. Y. W. Z. G. B. Theerasak Thapngam, "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns," in *IEEE Conference on Computer Communications Workshops*, 2011.

[14] W. Z. P. L. J. H. J. L. Ke Li, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics," in *Third International Conference on Network and System Security*, 2009.

[15] U. K. S. B. Pragya Katiyar, "Detection and Discrimination of DDoS Attacks from Flash Crowd Using Entropy Variation," in *International Journal of Engineering and Technology*, 2013.

[16] T. T. J. L. S. W. W. Z. Shui Yu, "Discriminating DDoS Flows from Flash Crowds Using Information Distance," in *Third International Conference on Network and System Security*, 2009.