Analisis restorasi layanan jaringan menggunakan *StopIt* dan RTBH dalam perbandingan. Studi kasus: kontra serangan DDoS

Theo Yohanes Paskah[1], Dodi Wisaksono Sudiharto[2], Muhammad Arief Nugroho[3]

[1, 2, 3]Fakultas Informatika, Universitas Telkom, Bandung
[1]theoyp@student.telkomuniversity.ac.id, [2]dodiws@telkomuniversity.ac.id, [3]arif.nugroho@telkomuniversity.ac.id

Abstrak

***Distributed Denial of service* (DDoS) merupakan salah satu jenis serangan yang paling populer dalam kegiatan kriminal di dunia maya. Tujuan utamanya adalah membatasi atau memberhentikan akses pada suatu layanan. DDoS menggunakan *botnet* dengan jumlah banyak dalam waktu yang bersamaan, inilah yang membedakan DDoS dengan serangan DoS yang hanya berasal dari 1 perangkat saja. Hingga saat ini serangan DDoS masih menjadi serangan yang paling populer digunakan. Dalam penelitian ini dilakukan perbandingan antara dua algoritma pertahanan DDoS yang cukup mirip jenis dan cara kerjanya, kedua algoritma tesebut adalah *StopIt* dan RTBH. *StopIt* dan RTBH memiliki kesamaan yaitu memberhentikan aliran data dari sumber serangan menuju target melalui filtering pada *router,* perbedaan keduanya terletak pada posisi filter data terletak. Pada *StopIt* filter data berada di *router* terdekat dengan sumber serangan berasal. Sedangkan RTBH meletakan filter data pada *router* yang berada dalam satu jaringan dengan targer serangan. Penelitian ini membandingkan kinerja kedua algoritma tersebut dalam memulihkan ketersediaan jaringan ketika terjadi serangan DDoS. Pengujian kedua algoritma ini dilakukan dengan menggunakan NS-3 sebagai program simulasi. Kemudian dilakukan analisis terhadap hasil simulasi yang telah dijalankan untuk melihat algoritma mana yang memiliki kinerja lebih baik. Hasilnya adalah *StopIt* memiliki kinerja yang lebih baik walaupun kerjanya lebih lambat dibanding dengan RTBH, namun StopIt tidak membuang semua aliran data yang menuju target serangan.**

Kata kunci : *DDoS, StopIt, Remote Triggered Black Hole*

Abstract

Distributed Denial of Service is a popular type of cyber attack used to conduct criminal activity. Main goal of the attack is to hinder or blocking router to some or all service provided a service provider. DDoS is using a lot of botnet at a same time to deploy attack, and that is the main difference between DDoS and DoS that only using one device to do the attack. Even nowadays DDoS is still one of the most popular attack used by criminals. This study is going to compare two DDoS defense algorithms that have similarities in type and how they work, those algorithms are StopIt and RTBH. Main similarities between the two are both algorithms work by stopping data traffic from attack source to the target by filtering placed on router, while the main difference is where the filter is positioned. StopIt placed their filter on routers that are nearest with the attack source. Meanwhile RTBH install its filter on routers that are within the same AS as the attack target. Both algorithm capabilities are tested to restore network service when DDoS attack is happening. The test is done by simulating both algorithm using NS-3 as simulator. Then analysis is done to compare which one is the better algorithm. The result is StopIt performs better compared to RTBH even though it works slower than RTBH but StopIt also didn't stop all data traffic to the target.

Key word : DDos, *StopIt,* Remote Triggered Black Hole.

Pendahuluan

Latar Belakang

Lebih dari lima dekade telah berlalu sejak dibuatnya sistem jaringan komputer. Pada awalnya jaringan komputer digunakan hanya untuk kepentingan militer. Setelah berakhirnya perang dingin, banyak institusi pendidikan yang mulai mengembangkan sistem jaringan komputer untuk kepentingan penelitian. Hingga pada akhirnya, jaringan yang kita kenal dengan nama internet dapat digunakan oleh publik.

Teknologi internet sudah menjadi bagian yang tidak dapat dipisahkan dari kehidupan sehari-hari. Hampir semua barang elektronik yang ada, kini saling terhubung melalui jaringan internet. Namun, adanya teknologi ini turut menciptakan kejahatan yang semula hanya berada di dunia nyata, kini juga merambah ke dunia maya. Salah satu jenis kejahatan yang populer, seperti serangan terhadap suatu layanan, sudah menjadi hal yang umum untuk dihadapi setiap harinya, terutama oleh para administrator jaringan. Jenis serangan semacam ini dapat menyebabkan layanan yang seharusnya dapat digunakan, menjadi sulit untuk digunakan, bahkan lebih jauh, layanan tersebut sama sekali tidak dapat digunakan. Dengan banyaknya aliran data yang terjadi setiap detik, dapat dibayangkan

kerugian yang ditimbulkan ketika transaksi data yang memerlukan suatu layanan, terhambat atau terhenti sama sekali.

DDoS merupakan salah satu jenis serangan yang dapat menghambat user untuk menggunakan suatu layanan, bahkan mematikan sama sekali layanan tersebut [1]. Pada DDoS, sebuah serangan umumnya digunakan untuk menghambat atau menghentikan transaksi data dengan cara menghabiskan sumber daya pada jaringan maupun *server* [2], [3]. Pada umumnya yang menjadi target utama dari serangan DDoS adalah *server-server* penting, seperti: bank, pelelangan, toko online, dan media sosial [4], [5]. Pada tahun 2010 terjadi serangan DDoS pada *server* Twitter secara besar yang berakibat pada matinya layanan selama beberapa jam [6]. Salah satu serangan DDoS terbesar yang mencapai 1 Tbps dan tidak hanya menggunakan komputer saja, namun juga menggunakan *smart devices* seperti CCTV dan kamera pribadi [4]. Berdasarkan data dari *Cisco Annual Cyber Security Report* tahun 2017, DDoS menempati urutan kedua sebagai masalah yang menghabiskan banyak sumber daya manusia dan waktu [5]. Sehingga DDoS menjadi ancaman serius bagi seluruh pengguna jasa internet.

Secara umum, terdapat algoritma yang dapat digunakan untuk menahan serangan DDoS. Algoritma tersebut dapat dibagi menjadi dua jenis, yaitu: *capabilities-based* dan *filter-based* [7], [8]. Algoritma *filter-based* bekerja dengan cara memvalidasi dan melakukan penanganan paket data menggunakan *filter* yang dipasang di berbagai level pada sebuah jaringan. *Filter* tersebut dibagi lagi menjadi dua, yaitu: *ingress filtering* dan *egress filtering*, yang dibedakan melalui arah paket ketika melewati filter yang ada [7], [8]. Sedangkan untuk *capabilities-based, algoritma ini* bekerja dengan pendekatan bahwa setiap sumber paket dapat menentukan asal paket yang diterima dan memberikan hak khusus dalam bentuk *capability*. *Capability* ini kemudian ditempelkan pada setiap paket dari pengirim dan akan diperiksa oleh setiap *router* yang dilewati sebelum diteruskan ke tujuan [7].

Pada penelitian ini, akan dibandingkan dua algoritma yang dapat digunakan untuk menahan serangan DDoS tersebut, yaitu: *StopIt* dan *Remote Triggered Black Hole* [9], [10]. Pada dasarnya, kedua algoritma tersebut termasuk ke dalam kategori *filter-based* yang bekerja pada level AS. Alasan mengapa algoritma *filter-based* yang dipilih pada penelitian ini, karena secara umum memiliki kinerja yang lebih baik dibandingkan dengan *capabilites-based* [7]. Perbedaan utama dari kedua algoritma ini adalah letak filter yang digunakan pada jaringan. Pada Algoritma *StopIt*, filter diletakkan pada *server* khusus yang berhubungan dengan semua akses *router* yang berada dalam AS. Sedangkan pada *Remote Triggered Black Hole*, filter diletakan pada *router*, dan memiliki *trigger* yang terhubung kesemua *router* yang terletak di NOC.

Studi kasus dilakukan dengan cara mensimulasikan serangan dan juga menganalisis efektivitas dari Alogritma *StopIt* dan *Remote Triggered Black Hole* menggunakan NS-3 [11]. Parameter utama yang dipakai sebagai acuan adalah waktu yang dibutuhkan oleh kedua algoritma tersebut sejak serangan DDoS dimulai sampai dengan pulihnya layanan, sehingga bisa digunakan tanpa gangguan yang berarti, kemampuan algoritma dalam skala jaringan yang lebih besar, dan kompleksitas ketika algoritma tersebut diimplementasikan di dunia nyata.

Topik dan Batasannya

Berdasarkan latar belakang yang dituliskan di atas, maka dapat dirumuskan permasalahan yang akan diteliti dalam pengerjaan tugas akhir ini adalah perbandingan kedua algoritma pertahanan terhadap serangan DDoS.

Adapun batasan masalah dalam pengerjaan tugas akhir ini adalah jenis serangan yang disimulasikan adalah DDoS aktif yaitu *flooding based botnet-attack*, parameter yang dipakai sebagai pengukuran adalah *Mean Time to Restore Service* yaitu waktu lamanya serangan terjadi dan algoritma pertahanan mulai aktif dan selesai mengatasi serangan, dan juga melihat kemampuan kedua algoritma dalam skala jaringan yang lebih besar dan kesulitan dalam impelentasi keduanya.

Tujuan

Berdasar dari permasalahan yang ditulis di atas, maka tujuan dari tugas akhir ini adalah membandingkan kemampuan restorasi layanan jaringan dari algoritma *StopIt* dan *Remote Triggered Black Hole* terhadap serangan DDoS menggunakan simulator ns3.

Organisasi Tulisan

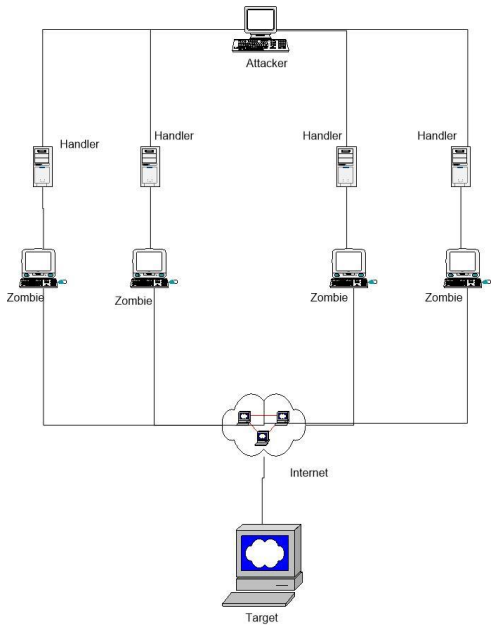
Selanjutnya akan dijelaskan studi yang mendukung tugas akhir ini pada bagian Studi Terkait, rancangan sistem yang dibangun pada bagian Sistem yang Dibangun, hasil pengujian beserta analisanya di bagian Evaluasi, dan yang terakhir kesimpulan dari tujuan tugas akhir ini berdasarkan hasil dan analisa hasil pengujian pada bagian kesimpulan.

1. Studi Terkait

Distributed Denial of Service (DDoS)

DDoS merupakan serangan terpopuler pada jaringan dan sumber dayanya [12]. DDoS merupakan turunan dari *Denial of Service* (DoS) dan yang membedakannya adalah jumlah sumber serangan tersebut. Pada DDoS sumber serangan berasal dari banyak perangkat sedangkan DoS hanya berasal dari satu perangkat saja[3]. DDoS dapat dibedakan menjadi dua jenis yaitu aktif dan pasif, DDoS aktif merupakan serangan yang dilakukan secara sengaja sedangkan pasif dapat dilihat sebagai 'serangan' yang tidak dimaksudkan untuk menghabiskan sumber daya jaringan yang tersedia.

Permasalahan dengan DDoS pada umumnya adalah sulitnya membedakan antara *packet* yang *legitimate* dengan *packet* yang bermaksud melumpuhkan jaringan dan juga respon yang terkadang lambat ketika serangan terjadi[12]. Pada umumnya serangan DDoS baru diketahui ketika *server* atau jaringan sudah hampir mati atau dirasakan adanya lag (respon yang sangat lambat) yang cukup mengganggu[12].

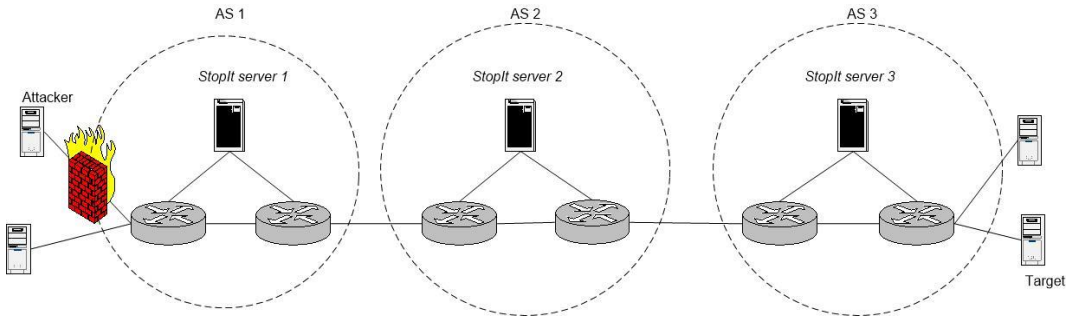


Gambar 2.1 Ilustrasi DDoS

StopIt

StopIt merupakan sebuah algoritma pertahanan DoS yang bersifat *filter-based*. Arsitektur utama dari *StopIt* adalah *closed-control*, dan *open-service* [9]. Algoritma ini memungkinkan penerima data untuk menghentikan aliran data yang tidak diinginkan sehingga dapat bertahan dari banyak serangan DoS yang menggunakan bot. Algoritma ini juga dapat bertahan dengan baik terhadap serangan *filter exhaustion* dan *bandwidth flooding* yang ingin mengacaukan instalasi filter dalam jaringan [9]. Algoritma ini juga memungkinkan pemblokiran pengiriman paket data dari suatu sumber selama waktu yang ditentukan. Dalam sistem yang menggunakan *StopIt*, setiap *server* pada masing-masing AS mengatur permintaan filtering dan saling mengetahui *IP address* masing-masing menggunakan mekanisme BGP [9].

StopIt bekerja dengan cara memblokir pengiriman data pada *router* terdekat dengan sumber serangan terjadi. Pada saat dideteksi adanya serangan, maka *server* akan melakukan permintaan pemblokiran data secara upstream atau mendekati sumber serangan.



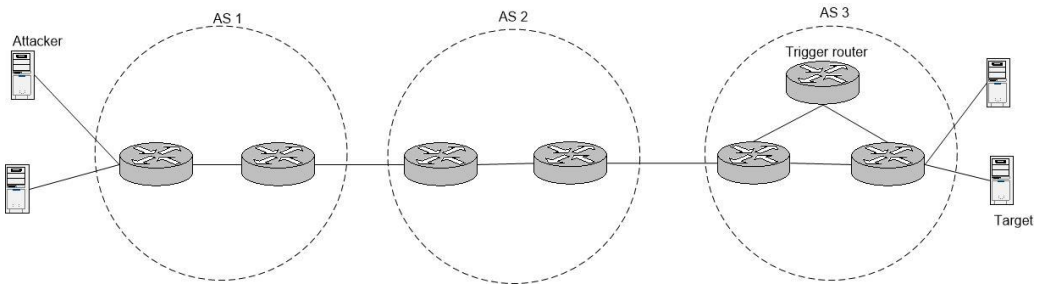
Gambar 2.2. Ilustrasi jaringan logika *StopIt* [9]

Remote Triggered Black Hole

Black hole dalam persepsi jaringan, digunakan dengan cara meneruskan lalu lintas data, dengan maksud menghilangkan data yang diteruskan tersebut [10]. Pada saat serangan DDoS telah terdeteksi, maka seluruh trafik serangan dapat dilumpuhkan dengan cara mengarahkan trafik serangan tersebut ke black hole yang posisinya didesain untuk berada di *router*. Secara umum cara kerja algoritma RTBH dapat dibagi menjadi dua yaitu, *source-based* dan *destination-based* [10]. RTBH filter diletakkan pada *router* agar serangan DDoS dapat dilumpuhkan sebelum masuk ke dalam jaringan.

Yang menjadi pembeda antara keduanya adalah lokasi *black hole routing*. Pada *destination based*, lokasi *black hole routing* adalah *router* yang terdapat dalam satu AS dengan target serangan, sedangkan pada *source based* instalasi *black hole routing* berada di *router* AS sumber serangan. Pada penelitian ini algoritma yang akan digunakan adalah *destination based* RTBH atau yang biasa ditulis d/RTBH.

RTBH bekerja dengan cara meneruskan trafik serangan menuju null0 *interface*. Null0 merupakan sebuah *pseudointerface* yang selalu aktif namun tidak dapat menerima atau meneruskan aliran data. Penerusan trafik serangan ke null0 merupakan cara umum dalam filterisasi aliran data, sehingga trafik serangan akan terbuang. Pada umumnya, RTBH bekerja menggunakan protokol BGP (*Border Gateway Protocol*). *Trigge*r *router* akan mengirimkan pembaruan pada *router* untuk meneruskan aliran data yang tidak diinginkan menuju null0 *interface*. *Trigger* pada RTBH dapat diaktifkan secara otomatis oleh sistem maupun manual oleh pemilik layanan.



Gambar 2.3 Ilustrasi jaringan logika RTBH [10]

	StopIt	d/RTBH
Tipe	*Filter based*	*Filter based*
Posisi filter	*Router* sumber serangan	*Router* target serangan
Avalability target	Ya, setelah serangan diblokir	Tidak, semua aliran data dibuang
Trigger	*StopIt* server	*Router*
Posisi trigger	Setiap AS dalam jaringan	AS target saja

Tabel 1 Perbedaan *StopIt* dan d/RTBH

ns-3

ns-3 merupakan sebuah simulator jaringan komputer yang bersifat diskrit. ns-3 merupakan perangkat lunak gratis yang berlisensi GNU GPLv2 yang ditujukan untuk penggunaan penelitian [11]. Perangkat lunak ini mampu digunakan untuk mensimulasikan jalannya paket melalui suatu jaringan komputer yang telah didesain. Dalam penelitian ini yang dimodelkan dalam ns-3 meliputi DNS *server*, *router* dengan kemampuan filtering, *StopIt server*, dan DNS *client*.

Quality of Service (QoS)

Service level agreement atau yang biasa disingkat SLA merupakan persetujuan formal antara penyedia jasa layanan dan pengguna layanan atas kualitas layanan yang akan dipenuhi oleh penyedia jasa tersebut [13]. Sebagai contoh adalah besarnya kapasitas akses data yang dapat digunakan oleh pengguna *web server*, ketika kapasitasnya sudah terlewati maka penyedia jasa layanan tetap dapat memberikan layanan namun tidak harus memenuhi SLA yang telah disetujui sebelumnya, karena jasa yang ditetapkan dalam SLA sudah dipenuhi.

Salah satu metode yang digunakan untuk mengetahui apakah SLA sudah dipenuhi atau belum pada jaringan komputer adalah dengan menilik *Quality of Service* (QoS). Di dalam SLA terdapat beberapa parameter QoS yang menjadi acuan apakah layanan yang disediakan sudah memenuhi standar atau belum.

QoS merupakan salah satu parameter yang dapat digunakan untuk menentukan tingkat kelayakan layanan suatu sistem jaringan komputer. Secara umum QoS untuk sebuah jaringan dapat dibagi menjadi enam kategori, yaitu: *availability, delivery, latency, bandwidth, MTBF (Mean Time Between Failure),* dan *MTRS (Mean Time to Restore Service)* [14]. Parameter kuantitatif yang digunakan adalah MTRS yang menyatakan waktu rata-rata sebuah masalah/gangguan dapat ditangani.[14]. Alasan digunakannya MTRS dan bukan MTBF karena MTBF lebih sering digunakan dalam perhitungan masa hidup suatu perangkat keras. MTBF juga dapat dihitung dari gagalnya salah satu komponen saja maupun kegagalan secara sistematis.[15], karena yang dianggap sebagai penyebab gagal hanya serangan DDoS maka parameter yang lebih cocok adalah MTRS.

2. Pemodelan sistem

Pada bagian ini akan dilakukan pembahasan mengenai pembuatan model simulasi yang akan digunakan serta parameter-parameter yang digunakan. Pembahasan meliputi arsitektur jaringan, aliran data serangan dan juga parameter yang akan digunakan.

Desain Jaringan

Pada bagian ini, akan dijelaskan desain jaringan yang akan disimulasikan pada penelitian ini. Arsitektur jaringan komputer yang dimodelkan dapat dibagi menjadi tiga bagian utama yakni, sumber serangan, jaringan antara/penghubung serta target serangan. Jaringan pada sumber serangan terdiri dari 2 AS (Autonomus System), masing-masing berisi 10 host dan 50%-nya corrupt. Untuk jaringan penghubung terdiri dari 2 AS dan untuk jaringan yang menjadi target serangan terdiri dari 1 AS, namun target serangan tertuju pada salah satu host saja. Serangan DDoS akan berasal dari 20 DNS *client* yang 50%nya akan menjadi *botnet*. Target serangan ddos merupakan DNS *server* Arsitektur jaringan ini memiliki bandwidth sebesar 10Mbps dan delay 1ms.

Salah satu yang menjadi alasan utama mengapa DNS server yang menjadi target adalah karena fungsi DNS server yang vital dalam jaringan internet. Sebagai komponen yang berfungsi menerjemahkan url menjadi IP address dan juga menjadi penghubung antara berbagai jaringan. Karena fungsinya yang cukup penting inilah mengapa DNS server sering menjadi target serangan DDoS. Sedangkan penggunaan trafik DNS juga berdasarkan data yang diberikan pada Q4 2017 oleh Kaspersky yang menyatakan bahwa trafik DNS merupakan trafik yang paling sering disalahgunakan oleh pelaku kriminal dunia maya dalam serangan DDoS [16].

Berikut ditampilkan beberapa parameter trafik jaringan dan *server* yang akan disimulasikan
Trafik DDoS:

- Jumlah : 100pkt/s
- Besar : 200bytes

Trafik *legitimate*:

- Jumlah : 3pkt/s
- Besar : 450bytes

DNS *server*

- Resource : 8
- Buffer size : 200
- Mean service time : 5ms

Parameterl

Parameter yang digunakan sebagai alat pengukuran dalam simulasi ini adalah MTRS (Mean Time to Restore Service) dikarenakan akibat utama dari serangan DDoS adalah lumpuhnya sistem dan berhentinya layanan. Lama waktu yang diperlukan sejak dimulainya serangan, deteksi, dan penanganan serangan menjadi salah satu objek utama dalam penelitian. Parameter lain yang dipakai adalah skalabilitas dan kompleksitas implementasi kedua algoritma tersebut.

Untuk parameter kuantitatif akan diisi oleh data yang didapatkan dari simulasi yang dijalankan. Sedangkan untuk parameter kualitatif akan dibandingkan dari beberapa paper yang tersedia.

Skenario Pengujian

Pada bagian ini akan dijelaskan skenario pengujian yang akan dilaksanakan. Setelah arsitektur jaringan dan dua algoritma yang disebutkan di atas dimodelkan dalam ns3 akan dilakukan simulasi sebanyak tiga kali pada masing-masing algoritma yang kemudian datanya akan dirata-rata untuk memenuhi parameter kuantitatif. Total waktu simulasi berjalan adalah 30 detik dan serangan DDoS dimulai pada detik ke-10. Dalam pengujian kali ini

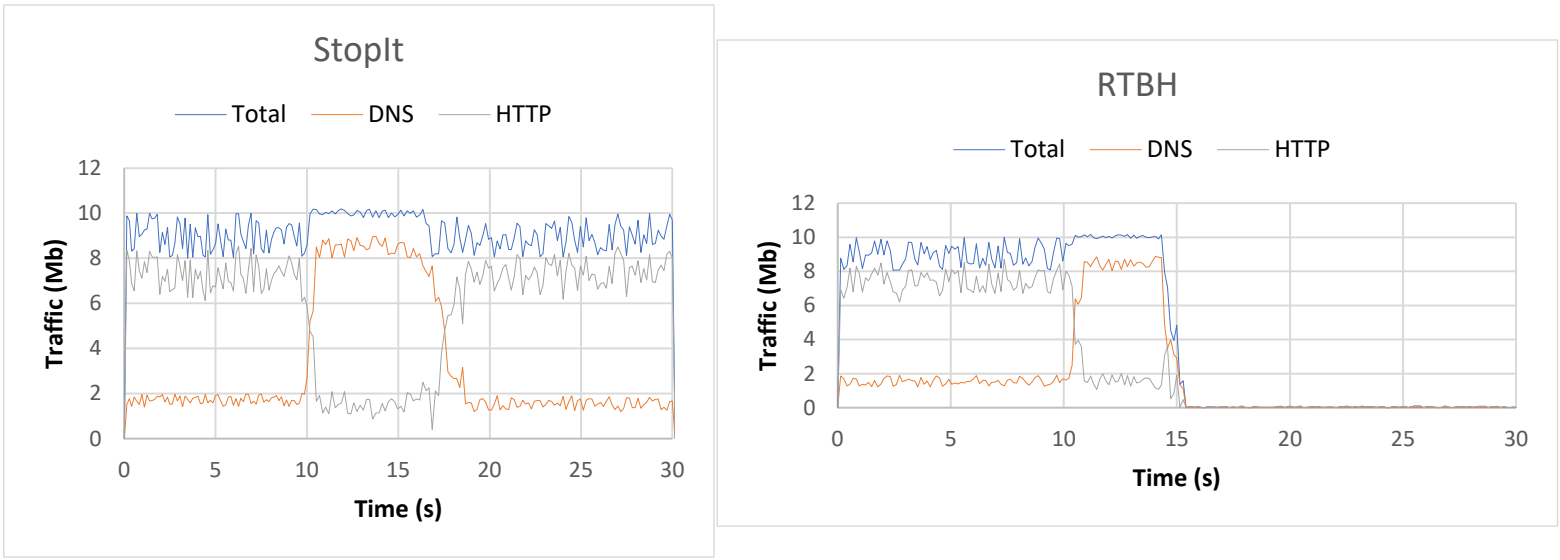
yang akan menjadi perbedaan utama adalah waktu yang dibutuhkan untuk melakukan filterisasi aliran data setelah DDoS di deteksi. Tidak ada perbedaan yang cukup berarti pada waktu deteksi diakibatkan penelitian ini menggunakan *StopIt server* sebagai pengganti *trigger router* pada algoritma RTBH. *StopIt server* memiliki tugas yang sama dengan *trigger router* yaitu merubah routing pada suatu *router* pada *access router* terdekat dengan penyerang atau *edge router* yang berada dalam satu AS dengan target serangan.

3. Evaluasi

Metode evaluasi yang dilakukan pada tugas akhir ini adalah simulasi. Model jaringan dan algoritma pertahanan yang sudah diimplementasikan menggunakan ns3. Setelahnya simulasi dijalankan sebanyak tiga kali untuk masing-masing algoritma, kemudian data yang berupa waktu dirata-ratakan. Akan dilakukan juga analisis dari kedua algoritma tersebut secara teoritis berdasarkan dari beberapa publikasi yang telah melakukan pengujian lebih lanjut pada kedua algoritma tersebut.

3.1 Hasil Pengujian

Hasil dari simulasi algoritma pertahanan menggunakan ns3 dapat dilihat di chart ini. Dalam simulasi ini jaringan dijalankan secara normal hingga dimulainya serangan DDoS pada t=10s. Setelah serangan dimulai *StopIt server* berhasil mendeteksi serangan pada t≈3s. Setelah kedua algoritma tersebut berhasil mendeteksi adanya serangan maka *StopIt* mulai bekerja dengan cara melakukan filtering data yang diterima dimulai dari *router* terdekat dengan target serangan dan meneruskan perintah filtering secara upstream kepada *StopIt server* yang berada dalam satu AS dengan penyerang, kemudian *StopIt server* akan melakukan pemblokiran aliran data dari sumber serangan melalui *access router* terdekat dengan penyerang.. Sedangkan RTBH bekerja dengan cara memblokir semua aliran data yang menuju target serangan melalui *edge router* baik paket data yang *legitimate* maupun paket data serangan. Dalam penelitian ini *StopIt server* dimodifikasi sehingga ketika terdeteksi adanya serangan DDoS maka pengubahan *routing* dilakukan pada *edge router* yang terdapat dalam satu AS dengan target.



Grafik 1 Traffic data simulasi

3.2 Analisis Hasil Pengujian

Dari hasil pengujian dapat dilihat bahwa RTBH memiliki waktu deteksi dan kerja yang lebih cepat dibandingkan dengan *StopIt*. Hal ini disebabkan karena *StopIt* harus mengirimkan perintah filtering dimulai dari *router* dalam AS terdekat dengan target serangan hingga *router* dalam AS terdekat dengan sumber serangan. RTBH berhasil menangani serangan dari 10 *botnet* dalam waktu t ≈ 5s dari sejak serangan dimulai sedangkan *StopIt* membutuhkan waktu hingga t ≈ 6s untuk menahan serangan DDoS secara penuh. Jika kita hanya melihat waktu deteksi dan kerja saja maka dapat dilihat bahwa RTBH jauh lebih baik dibandingkan degan *StopIt*.

Namun perlu diingat juga bahwa RTBH akan memblokir sermua aliran data yang menuju targer serangan baik data yang *legitimate* maupun aliran serangan. Dapat dikatakan bahwa RTBH ikut ‘membantu’ tujuan dari pelaku serangan yaitu menghalangi atau memberhentikan jasa layanan. Grafik di atas menunjukan aliran data yang terjadi dari dimulainya simulasi, kemudian DDoS dimulai pada t = 10s kemudian algoritma mulai bekerja setelah DDoS

berhasil dideteksi pada t ≈ 13s, *StopIt* berhasil menangani serangan dengan rata-rata t = 6,1s sedangkan RTBH memiliki rata-rata waktu t = 5,1s. Dari grafik di atas dapat dilihat terdapat dua trafik data utama yang dianggap menggambarkan keadaan trafik normal yaitu trafik HTTP dan DNS, namun ketika serangan DDoS menggunakan trafik DNS dimulai dapat dlihat bahwa trafik HTTP langsung menurun secara drastis.

Dilihat dari segi parameter kualitatif yang disebutkan di atas yakni skalabilitas dan kompleksitas implementasi keduanya. Skalabilitas berhubungan dengan kemampuan algoritma tersebut apabila skala jaringan dan serangan yang diperbersar. Sedangkan kompleksitas merupakan tingkat kesulitan yang akan dihadapi ketika algoritma tersebut akan diimplementasikan dalam dunia nyata. Secara skalabilitas, kedua algoritma dapat bekerja dengan baik, *StopIt* dapat menahan serangan *botnet* dengan jumlah hingga 7000 penyerang per detiknya [9] dan sanggup menangani serangan *botnet* hingga 10 juta dalam waktu 30 menit. Sedangkan destination based RTBH juga sudah diimplementasikan di dunia nyata dan mampu menangani serangan sebesar 110Gbps dalam waktu 30 menit [17].

Parameter kualitatif selanjutnya yang akan kita tinjau adalah kompleksitas implementasi. Destination RTBH memiliki komplesitas implementasi yang cukup rendah, karena pengguna cukup memiliki trigger *router* dan melakukan konfigurasi table routing menuju null0 interface ataupun alamat IP lain yang dikehendaki. Beberapa penyedia jasa layanan mengarahkan paket data yang diblokir menuju sinkhole untuk dianalisis ataupun menuju server khusus yang kemudian dapat melakukan proses scrubbing pada paket data yang diterima dan kemudian meneruskan data tersebut ke tujuannya. Sedangkan untuk *StopIt* memiliki komplesitas yang lebih tinggi dan juga biaya yang lebih mahal dibandingkan dengan RTBH. Untuk bekerja dengan lancar, *StopIt* memerlukan server khusus di tiap AS yang berada dalam jaringan untuk meneruskan perintah filtering dari satu server ke server lainnya. Selain itu kode program *StopIt* yang jauh lebih rumit dibandingkan dengan RTBH juga membuat implementasi semakin sulit.

4. Kesimpulan

Berdasarkan sejumlah pengujian yang telah dilakukan dan juga beberapa publikasi yang telah dibaca, dapat disimpulkan bahwa kedua algoritma memiliki kelebihan dan kelemahan masing-masing. Jika dilihat dari parameter yang disebutkan di atas maka dapat dilihat bahwa RTBH memiliki performansi yang lebih baik dibandingkan dengan *StopIt*. Namun perlu diingat bahwa kelemahan paling besar dari RTBH adalah pemblokiran semua aliran data menuju IP tujuan sehingga secara tidak langsung membantu proses DDoS. *StopIt* memiliki kelebihan yaitu kemampuan filterisasi paket data sehingga tidak masih ada aliran paket data yang tetap mencapai IP tujuan. Dalam penulisan ini juga masih belum digunakan beberapa varian kedua algoritma yang tersedia seperti *StopIt* + DiffServ ataupun s/RTBH menggunakan uRPF ataupun kombinasi dengan algoritma lain.

Kesimpulan yang dapat diambil dari penelitian ini adalah, secara total StopIt memiliki kemampuan yang lebih baik dibandingkan dengan RTBH sesuai fungsi restorasi. RTBH memang dapat mengatasi serangan DDoS dalam waktu yang lebih singkat namun dengan kelemahan utamanya yaitu membuang semua aliran data baik serangan maupun aliran *legitimate* yang menuju target. Jika kelemahan ini dapat diatasi maka RTBH dapat menjadi pilihan yang lebih baik.

Daftar Pustaka

[1] K. Zeb, O. Baig, and M. K. Asif, "DDoS attacks and countermeasures in cyberspace," *2015 2nd World Symp. Web Appl. Networking, WSWAN 2015*, 2015.

[2] M. Geva, "Ensuring QoS During Bandwidth DDoS Attacks," Bar-Ilan University, 2013.

[3] C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks," *Internet Protoc. J.*, vol. 7, no. 4, pp. 13–36, 2004.

[4] M. Alvarez *et al.*, "IBM X-Force Threat Intelligence Index 2017 The Year of the Mega Breach," no. March, pp. 1–30, 2017.

[5] Cisco, "Cisco 2017 Annual Cyber Security Report," *WD info*, p. 2004, 2003.

[6] J. D. Sutter, "Twitter hit by denial-of-service attack," 2009. [Online]. Available: http://edition.cnn.com/2009/TECH/08/06/twitter.attack/index.html.

[7] S. Mishra and R. K. Pateriya, "A Comparative Study on Capability v/s. Filtering based Defense Mechanisms," *Int. J. Comput. Appl.*, vol. 93, no. 11, pp. 29–35, 2014.

[8] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, p. 39, 2004.

[9] X. Liu, X. Yang, and Y. Lu, "StopIt: Mitigating DoS Flooding Attacks from Multi-Million Botnets," Irvine, 2008.

[10] W. Kumari and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding," *IETF*, pp. 1–15, 2009.

[11] G. Carneiro, H. Fontes, and M. Ricardo, "Fast prototyping of network protocols through ns-3 simulation

model reuse," *Simul. Model. Pract. Theory*, vol. 19, no. 9, pp. 2063–2075, Oct. 2011.
[12] A. Sanmorino and S. Yazid, "DDoS Attack detection method and mitigation using pattern of the flow," *2013 Int. Conf. Inf. Commun. Technol.*, pp. 12–16, 2013.
[13] "Performance Reporting Concepts and Definitions," in *TMF701*, 2001.
[14] H. Lee, M. Kim, J. W. Hong, and G. Lee, "QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring," Pohang, 2002.
[15] J. T. Daly, L. A. Pritchett-Sheats, and S. E. Michalak, "Applicatin MTTFE vs. platform MTBF: A fresh perspective on system reliability and application throughput for computations at scale," *Proc. CCGRID 2008 - 8th IEEE Int. Symp. Clust. Comput. Grid*, pp. 795–800, 2008.
[16] Kaspersky, "Kaspersky Lab DDoS Intelligence Quarterly Report Q4 2017," 2017. [Online]. Available: https://securelist.com/ddos-attacks-in-q4-2017/83729/.
[17] PaloAltoNetworks, "DDoS Mitigation," 2014.