ANALISIS SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA JARINGAN *SOFTWARE DEFINED NETWORK* (SDN) MENGGUNAKAN *PLATFORM CONTROLLER OPENDAYLIGHT* DAN *MININET*

TUGAS AKHIR

Irham Ramdoni
41516110152

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2020

ANALISIS SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA JARINGAN *SOFTWARE DEFINED NETWORK* (SDN) MENGGUNAKAN *PLATFORM CONTROLLER OPENDAYLIGHT* DAN *MININET*

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Irham Ramdoni
41516110152

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2020

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	:	41516110152
Nama	:	Irham Ramdoni
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial of Service (DDoS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 1 September 2020

Irham Ramdoni

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Irham Ramdoni
NIM	:	41516110152
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial of Service (DDoS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 1 September 2020

Irham Ramdoni

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Irham Ramdoni
NIM	:	41516110152
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial of Service (DDoS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Menyatakan bahwa Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis		Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi		Diajukan	✓
		Jurnal Nasional Terakreditasi	S2		
		Jurnal International Tidak Bereputasi		Diterima	
		Jurnal International Bereputasi			
	Disubmit/dipublikasikan di :	Nama Jurnal	: JUITA (Jurnal Informatika)		
		ISSN	: e-ISSN: 2579-8901 / p-ISSN: 2086-9398		
2	Kertas Kerja, Merupakan material haasil penelitian sebagai kelengkapan Artikel Jurnal. Terdiri dari (minimal 4)	Literatur Review			[✓]
		Hasil analisa & perancangan aplikasi			[✓]
		Source code			[✓]
		Data set			[✓]
		Tahapan eksperimen			[✓]
		Hasil eksperimen seluruhnya			[✓]
		....			
3	HAKI Disubmit / Terdaftar	HKI		Diajukan	
		Paten		Tercatat	
		No & Tanggal Permohonan	:		
		No & Tanggal Pencatatan	:		

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 1 September 2020

Irham Ramdoni

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110152
Nama	:	Irham Ramdoni
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial Of Service (DDOS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 25 Agustus 2020

Menyetujui,

(Desi Ramayanti, S.Kom., MT)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110152
Nama	:	Irham Ramdoni
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial Of Service (DDOS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 25 Agustus 2020

Menyetujui,

(Sabar Rudiarto, S.Kom.,M.Kom)

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110152
Nama	:	Irham Ramdoni
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial Of Service (DDOS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 25 Agustus 2020

Menyetujui,

(Harni Kusuiyati, ST.,MKom)

MERCU BUANA

LEMBAR PENGESAHAN

NIM	:	41516110152
Nama	:	Irham Ramdoni
Judul Tugas Akhir	:	Analisis Serangan Distributed Denial Of Service (DDOS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 25 Agustus 2020

Menyetujui,

(Dr. Ida Nurhaida, MT)
Dosen Pembimbing

Mengetahui,

(Diky Firdaus, S.Kom, MM)	(Desi Ramayanti, S.Kom, MT)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Irham Ramdoni
NIM	:	41516110152
Pembimbing TA	:	Dr. Ida Nurhaida, MT
Judul	:	Analisis Serangan Distributed Denial Of Service (DDOS) Pada Jaringan Software Defined Network (SDN) Menggunakan Platform Controller Opendaylight Dan Mininet

Abstrak - *Software Defined Network* (*SDN*) memberikan kontrol penuh terhadap aktivitas yang ada dalam jaringan tersebut, sehingga dalam kinerja jaringan *SDN* semua dibebankan dan dikontrol oleh aplikasi kontroler. Dengan proses seperti itu, kecenderungan untuk mendapatkan serangan akan menjadi lebih besar, seperti serangan *Distributed Denial of Service* (*DDoS*). Atas dasar itu penelitian ini bertujuan untuk menganalisis dampak dari serangan *Distributed Denial of Service* (*DDoS*) pada jaringan *SDN* dengan mengukur parameter *Quality of Service (QoS) seperti delay, jitter, packet loss,* dan *throughput*. Nilai-nilai yang didapatkan dari paramater tersebut kemudian dibandingkan dengan standar dari *Telecommunications and Internet Protocol Harmonization Over Networks* (*TIPHON*). Setelah melakukan perancangan, pengujian dan analisis dihasilkan nilai rata rata tertinggi dengan serangan sebesar 0,502024 ms untuk *delay*, 0,95% untuk *packet loss*, 7,587685 ms untuk *jitter*, dan 187570 kbps untuk *throughput.*

Kata kunci: Software Defined Network, DDoS, QoS, Mininet, OpenDayLight.

ABSTRACT

Name	:	Irham Ramdoni
Student Number	:	41516110152
Counsellor	:	Dr. Ida Nurhaida, MT
Title	:	Analysis Of Distributed Denial Of Service (Ddos) Attacks On Defined Network (Sdn) Software Network Using Opendaylight And Mininet Controller Platform

Abstract - Software Defined Network (SDN) gives full control over the activities that exist in the network, so that in SDN network performance all are charged and controlled by the controller application. With such a process, the tendency to get attacks will be greater, for example Distributed Denial of Service (DDoS). Based on that, this study aims to analyze the impact of Distributed Denial of Service (DDoS) attacks on SDN networks by measuring Quality of Service (QoS) parameters such as delay, jitter, packet loss, and throughput. The values obtained from these parameters are then compared with the standards of the Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON), after carrying out the design, testing and analysis of the highest average value with an attack of 0.502024 ms for delay, 0.95% for packet loss, 7,587685 ms for jitter, and 187570 kbps for throughput.

Keywords: Software Defined Network, DDoS, QOS, Mininet, OpenDayLight.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT, yang telah melimpahkan taufiq, hidayah, tuntunan dan bimbingan serta hidayah-Nya sehingga Tugas Akhir yang merupakan salah satu syarat untuk menyelesaikan pendidikan pada Program Sarjana Teknik Informatika Universitas Mercubuana dapat terselesaikan.
Penulis menyadari bahwa tanpa bantuan dan bimbingan semua pihak yang terlibat dalam penyusunan Tugas Akhir ini mungkin dalam proses penulisannya tidak akan sempurna. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Ngadino Surip, selaku Rektor dari Universitas Mercubuana.
2. Ibu Desi Ramayanti S.kom, MT, selaku ketua Fakultas Ilmu Komputer.
3. Bapak Anies Cherid, SE, MTI, selaku Dosen PA saya.
4. Ibu Dr. Ida Nurhaida, MT selaku dosen pembimbing yang meluangkan waktu kepada penulis dalam rangka penyelesaian laporan Tugas Akhir ini.
5. Bapak Ricky Tahalele selaku Kepala General Affair di Yayasan Budi Pekerti Luhur yang telah memberi izin kepada penulis untuk mengadakan penelitian. .
6. Para staf karyawan di Yayasan Budi Pekerti Luhur terima kasih telah membantu penulisan laporan Tugas Akhir ini.
7. Orang Tua dan teman-teman yang senantiasa mendukung penulis baik secara moril maupun materil.

Akhir kata, Penulis menyadari bahwa Tugas Akhir ini masih jauh dari kesempurnaan. Maka dibutuhkan masukan dan kritikan yang bersifat membangun dari semua pihak sehingga dapat memberikan kontribusi kepada mereka yang membutuhkan referensi dari karya tulis ini untuk kepentingan yang lebih luas.

Jakarta, 14 Agustus 2020
Penulis

DAFTAR ISI

NASKAH JURNAL

ANALISIS SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (DDOS) PADA JARINGAN *SOFTWARE DEFINED NETWORK* (SDN) MENGGUNAKAN *PLATFORM CONTROLLER OPENDAYLIGHT* DAN *MININET*

(Distributed Denial Of Service (DDOS) Attacks Analysis on Software Defined Network (SDN) using Opendaylight and Mininet Controller Platform)

Irham Ramdoni[1], Ida Nurhaida[2]

[1,2]*Juruasan Teknik Informatika , Universitas Mercu Buana*
[1,2]*Jl. Meruya Selatan No.1, RT.4/RW.1, Meruya Selatan, Kec. Kembangan, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11650*
[1]41516110152@student.mercubuana.ac.id
[2]ida.nurhaida@mercubuana.ac.id

Abstrak - ***Software Defined Network* (*SDN*) memberikan kontrol penuh terhadap aktivitas yang ada dalam jaringan tersebut, sehingga dalam kinerja jaringan *SDN* semua dibebankan dan dikontrol oleh aplikasi kontroler. Dengan proses seperti itu, kecenderungan untuk mendapatkan serangan akan menjadi lebih besar, seperti serangan *Distributed Denial of Service* (*DDoS*). Atas dasar itu penelitian ini bertujuan untuk menganalisis dampak dari serangan *Distributed Denial of Service* (*DDoS*) pada jaringan *SDN* dengan mengukur parameter *Quality of Service (QoS) seperti delay, jitter, packet loss,* dan *throughput.* Nilai-nilai yang didapatkan dari paramater tersebut kemudian dibandingkan dengan standar dari *Telecommunications and Internet Protocol Harmonization Over Networks* (*TIPHON*). Setelah melakukan perancangan, pengujian dan analisis dihasilkan nilai rata rata tertinggi dengan serangan sebesar 0,502024 ms untuk *delay*, 0,95% untuk *packet loss*, 7,587685 ms untuk *jitter*, dan 187570 kbps untuk *throughput.***

Kata kunci: Software Defined Network, DDoS, QoS, Mininet, OpenDayLight.

Abstract - Software Defined Network (SDN) gives full control over the activities that exist in the network, so that in SDN network performance all are charged and controlled by the controller application. With such a process, the tendency to get attacks will be greater, for example Distributed Denial of Service (DDoS). Based on that, this study aims to analyze the impact of

Distributed Denial of Service (DDoS) attacks on SDN networks by measuring Quality of Service (QoS) parameters such as delay, jitter, packet loss, and throughput. The values obtained from these parameters are then compared with the standards of the Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON), after carrying out the design, testing and analysis of the highest average value with an attack of 0.502024 ms for delay, 0.95% for packet loss, 7,587685 ms for jitter, and 187570 kbps for throughput.

Keywords: Software Defined Network, DDoS, QOS, Mininet, OpenDayLight.

I. PENDAHULUAN

Software Defined Network (SDN) merupakan salah satu evolusi yang terjadi dalam perkembangan jaringan komputer [1] di mana jaringan *SDN* berbeda dengan konsep jaringan konpensional biasa. Teknologi *SDN* memiliki dua karakteristik, [2] terletak dari pemisah antara *control plane* dengan *data plane*, dengan Arsitektur *SDN* yang memisahkan antara *control plane* dan *data plane* bertujuan agar manajemen jaringan lebih mudah dan fleksibel [3]. Selain itu juga dari pemisahan *data plane* dan *control plane* pada perangkat jaringan komputer seperti *router* dan *switch* memungkinkan untuk memprogram perangkat tersebut sesuai dengan yang diinginkan secara terpusat. [4] Program yang dimaksud berupa aplikasi *controller software define network (SDN)*. *Controller SDN* adalah aplikasi *SDN* yang mengelola *flow control* untuk mengaktifkan *inteligence networking*. *Controller SDN* bekerja berdasarkan protokol seperti *OpenFlow*.

OpenFlow adalah protokol yang digunakan di jaringan *SDN* yang letaknya antara *control plane* dan *data plane*, dengan protokol *openflow* memungkinkan pengaturan *routing* dan pengiriman paket ketika melalui sebuah *switch* [3] sehingga *server* dan *client*-nya dapat berkomunikasi dalam sebuah jaringan yang ada. Secara garis besar protokol, *openflow* berfungsi sebagai bagian utama proses komunikasi antar kedua perangkat tersebut. Sebagai perangkat pusat, *openflow controller* memiliki fungsi utama dalam komunikasi, [5] karena kontroler lah yang mengatur dan melakukan perintah terhadap *switch* yang terlibat dalam infrastruktur. [6]

Opendaylight adalah sebuah proyek *open source software* dalam naungan *Linux Foundation* [7] yang termasuk ke dalam aplikasi *controller* jaringan *software defined network (SDN)*. *Opendaylight* merupakan sebuah infrastruktur *controller* yang memiliki ketersediaan tinggi, *modular*, *extensible*, *scalable* dan *multi-protocol*, dibangun untuk penyebaran *SDN* di jaringan *heterogen*, *multi-vendor*, serta modern. [8]

Mininet merupakan *emulator* jaringan yang mensimulasikan koleksi dari *host-end*, *switch*, *router*, dan *link* pada *single kernel Linux*. Masing-masing elemen ini disebut sebagai "*host*" dan menggunakan virtualisasi ringan untuk membuat sistem tampilan tunggal sehingga terlihat seperti jaringan yang lengkap, menjalankan kernel, sistem, dan *user code* yang sama. [8] *Mininet* dapat menciptakan jaringan virtual yang realistis, menjalankan *real kernel*, *switch* dan kode aplikasi, pada *single machine* (baik berupa *physical machine, virtual machine*, atau *cloud*). *Mininet* sangat berguna untuk pengembangan riset, pengajaran, serta penelitian. Selain itu juga *Mininet* bisa digunakan untuk pengembangan dan eksperimen dengan *openflow* dan *SDN*. [9]

Quality of Service (QOS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis [10]. Teknologi pengiriman paket data dalam jaringan komputer digunakan untuk kebutuhan yang semakin luas dan juga kompleks secara global. [11] Saat ini jaringan komputer dituntut untuk dapat melayani banyak *host* dalam satu waktu dengan jarak pengiriman yang semakin beragam *QOS* diperlukan sebagai sebuah metode untuk memenuhi kriteria pelayanan sistem bagi pengguna, yaitu *confidentiality, integrity*, dan *availability*, [12] sehingga suatu jaringan dan memiliki kelemahan dan kelebihan masing-masing. [13] Klasifikasi *QOS* berdasarkan *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)* dapat mengkategorikan *Quality of Service*

(QOS) berdasarkan kriteria nilai yang didapat saat pengujian yang selanjutnya akan dianalisis dan disimpulkan kinerja dari sebuah jaringan yang sudah dibangun, khususnya dari aspek *delay, packet loss, jitter* dan *througput* nya apakah termasuk ke kategori sangat bagus, bagus, sedang atau jelek. Dengan menganalisa performansi jaringan seperti *delay, packet loss, jitter* dan *throughput* dapat diketahui kualitas jaringan yang digunakan. [14]

Pada penelitian ini, penulis akan menguji dan menganalisa jaringan *Software Defined Network (SDN)* yang akan dibangun diatas sistem virtual topologi menggunakan *Mininet* dan sistem *controller* menggunakan *OpendayLight*. Selanjutnya akan dilakukan uji coba serangan *Distributed Denial of Service (DDoS)*, Pengguna jahat membanjiri sumber daya jaringan dengan sejumlah besar *traffic* dengan paket yang tidak berguna untuk menghabiskan sumber daya. [15]

Dengan jenis serangan *SYN flooding attack*, serangan ini bisa melumpuhkan koneksi ke sebuah server karena banyaknya paket yang masuk. [16] Terdapat beberapa variabel yang akan diuji dalam penelitian ini seperti *delay, packet loss, jitter* dan *throughput*. Data yang didapatkan akan diolah dan dianalisis sehingga dapat diketahui sejauh mana arsitektur *SDN* terdampak. Karena dari beberapa peneliti, salah satu kelemahan dari Arsitektur jaringan *SDN* dengan protokol *openflow* apabila *controler* tidak dapat diakses oleh perangkat jaringan melalui protokol *openflow* maka jaringan gagal bekerja. [16]

II. METODE

Metode yang dilakuakan dalam penelitian ini adalah studi literatur, konsep mengumpulkan bahan atau materi dari jurnal yang relevan yang dijadikan referensi dan dengan menerapkan metode pengembangan sistem menggunakan *Network Development Life Cycle (NDLC)*. *NDLC* dijadikan metode yang digunakan sebagai acuan (secara keseluruhan atau secara garis besar) pada proses pengembangan dan perancangan sistem jaringan komputer.[17]

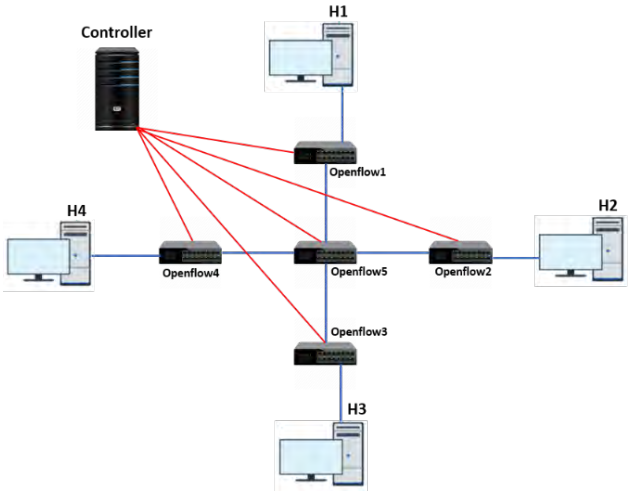
Dalam melakukan studi konfigurasi terhadap *Mininet, OpenDayLight*, dan semua *software* yang dibutuhkan dalam melakukan penelitian serta melakukan studi konsep serangan *Distributed Denial of Service (DDoS).*

A. Analisys

Merupakan tahap awal peniliti, melakukan analisa permasalahan yang muncul ketika instalasi dan konfigurasi *hardware* atau *software* untuk membangun topologi jaringan *Software Defined Network (SDN)* yang nantinya dijadikan sebagai bahan pengambilan data dalam penelitian.

B. Design

Pada tahap ini akan menggambarkan design topologi jaringan yang dibuat untuk jaringan *Software Defined Network (SDN).* Berikut adalah topologi yang digunakan untuk melakukan simulasi :



Gambar 1. ***Topologi Software Defined Network (SDN)***

Hardware & Software yang dibutuhkan dalam penelitian :

Hardware	Software	Versi	Keterangan
Core i5 4 Core, Ram 8Gb, Hdd 320Gb	OS Windows Server 2019 STD	Terupdate	OS Utama
	OS Ubuntu Desktop	20.01	OS untuk kontroler Opendaylight
	OpenDayLight	Karaf 0.8.4	Aplikasi kontroler
Core i5 4 Core, Ram 8Gb, Hdd 320Gb	OS Windows 10	Terupdate	OS Utama
	OS Ubuntu Desktop	18.04	Os untuk virtual Topologi SDN
	Mininet	2.2.2	Aplikasi virtual Topologi Mininet
	Wireshark	Terupdate	Aplikasi untuk trace lalulintas data
	Distributed Internet Traffic Generator (D-ITG)	2.8.1	software pengujian pengambilan data QOS

Gambar 2. ***Informasi Spesifikasi***

C. Simulation Prototype

Pada tahap ini adalah melakukan simulasi *prototype* dari jaringan yang sudah dibuat, lalu selanjutnya dilakukan pengujian dan analisis lanjutan. Tahap ini juga menggunakan semua komponen atau *tools* yang dibutuhkan seperti topologi virtual yang dibuat di *Mininet*, *Kontroler Opendaylight*, dan *(Distributed Internet Traffic Generator) D-ITG* [18] sebagai software pengujian pengambilan data *QOS*, aplikasi D-ITG mengirimkan data sesuai dengan jenisnya. [19] Pengukuran merujuk kepada *QOS* berdasarkan *Tabel Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)* bisa dilihat pada Tabel 1.

TABEL 1. TELECOMMUNICATIONS AND INTERNET PROTOCOL HARMONIZATION OVER NETWORKS (TIPHON)

Menghitung Delay

Kategori Delay	Besar Delay
Sangat Bagus	<150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	>450 ms

Menghitung Packet Loss

Kategori Degredasi	Packet Loss
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Jelek	25%

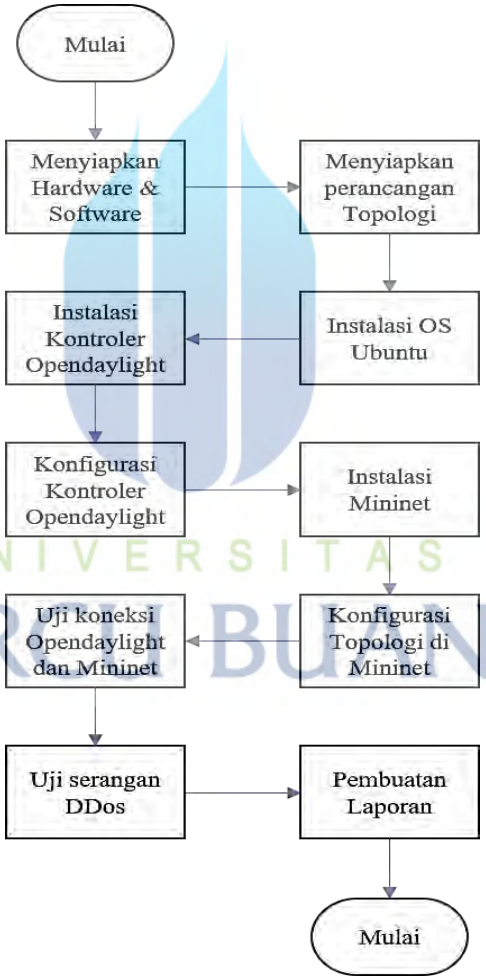
Menghitung Jitter

Kategori Degredasi	Jitter
Sangat Bagus	0 ms
Bagus	0 s/d 75 ms
Sedang	76 s/d 125 ms
Jelek	125 s/d 225 ms

Menghitung Throughput

Kategori Degredasi	Throughput
Sangat Bagus	100 %
Bagus	75 %
Sedang	50 %
Jelek	< 25 %

Penerapan detail rancangan dan desain untuk dilakukan pengujian dan analisis sebagai berikut tahapan-tahapan proses dari penelitian.



Gambar 3. *Tahapan Penelitian*

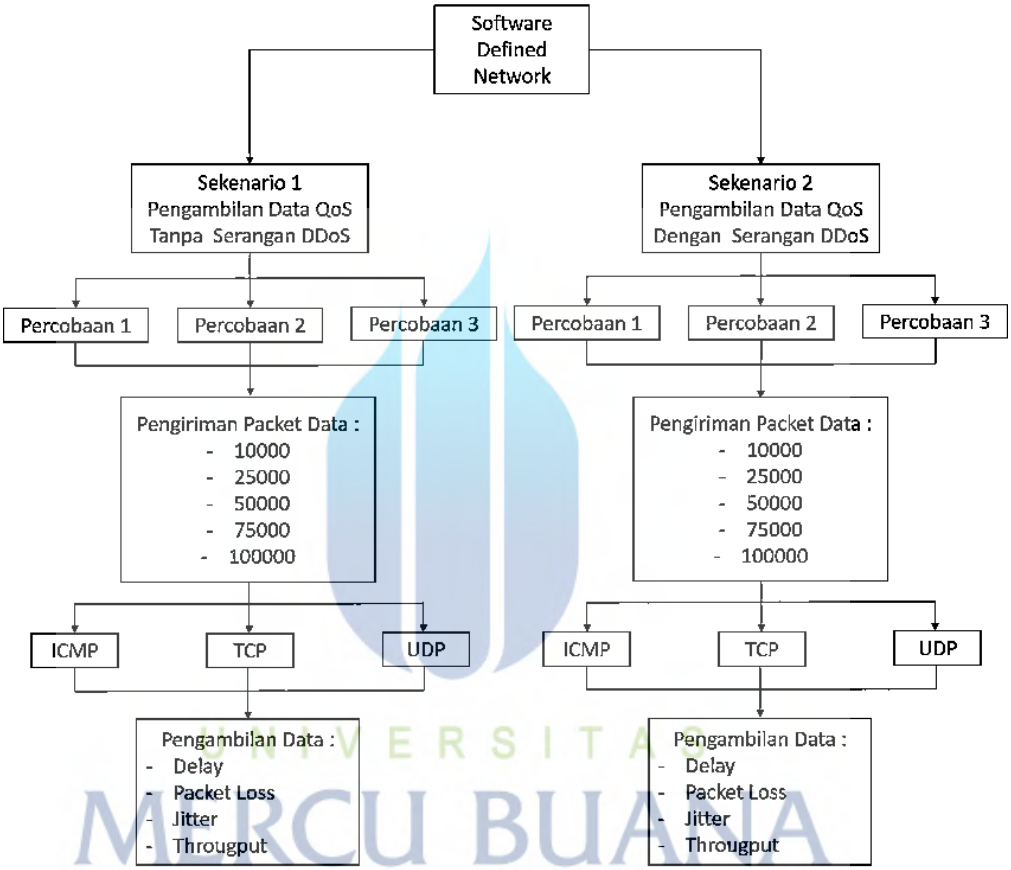
Tahap penelitian ini dimulai dari menyiapkan perangkat yang berkaitan dengan penelitian ini, yaitu 3 buah *pc* dan kabel *UTP* untuk menyambungkan jaringan. Penelitian ini juga menggunakan *software* kontroler *OpenDaylight* versi *Oxygen 0.8.4*, virtual topologi *Mininet versi 2.2.2* dan *software* pengujuan *Quality of Service (QOS)* menggunakan *D-ITG*. Pengukuran *QoS* dilakukan untuk mengukur tingkat performa jaringan apabila jaringan yang telah dibangun dan dibentuk dengan skenario tertentu dialiri

dengan trafik dari beragam jenis, [20] seperti trafik data protokol *ICMP*, *TCP* dan *UDP*. Untuk keterangan lebih detailnya dapat dilihat di gambar 2.

III. HASIL PEMBAHASAN

Sekenario Uji Serangan dan Pengambilan Data

Sekenario dalam uji serangan *Distributed Denial of Service (DDoS)* menggunakan jenis serangan *Sys Flood Attack* dengan pengambilan data saat tanpa serangan dan di saat serangan, lebih jelasnya seperti dibawah ini.



Gambar 4. ***Diagram sekenario pengambilan data QoS***

Sekenario Pertama (Tanpa Serangan)

Mengukur serangan *QOS* paket *ICMP*, *TCP*, dan *UDP* tanpa serangan *DDoS* dengan masing masing sepuluh kali percobaan. Di setiap percobaan akan ada lima kali pengambilan nilai *QOS* dengan pengiriman paket data sebesar 10000, 25000, 50000, 75000, dan 100000 *byte* perdetik dengan lama waktu pengiriman data selama 60 detik di setiap percobaanya.

Sekenario Kedua (Dengan Serangan)

Mengukur serangan *QOS* paket *ICMP*, *TCP*, dan *UDP* menggunakan serangan *DDoS* dengan masing masing sepuluh kali percobaan. Di setiap percobaan akan ada lima kali pengambilan nilai *QOS* dengan pengiriman paket data sebesar 10000, 25000, 50000, 75000, dan 100000 *byte* perdetik dengan lama waktu pengiriman data selama 60 detik di setiap percobaanya.

```
root@TA-SDN:~/mininet/custom/D-ITG-2.8.1-r1023/bin# ./ITGSend -T ICMP -a 192.16
8.0.102 -C 100000 -t 60000
ITGSend version 2.8.1 (r1023)
Compile-time options: bursty multiport
Started sending packets of flow ID: 1
Finished sending packets of flow ID: 1
```

Gambar 5. ***Tampilan Pengiriman Paket menggunakan D-ITG***

```
------------------------------------------------------------
**********  TOTAL RESULTS  **********
------------------------------------------------------------
Number of flows          =            1
Total time               =    59.999788 s
Total packets            =       381998
Minimum delay            =     0.000010 s
Maximum delay            =     0.119288 s
Average delay            =     0.000190 s
Average jitter           =     0.000012 s
Delay standard deviation =     0.003393 s
Bytes received           =    195582976
Average bitrate          =  26077.822275 Kbit/s
Average packet rate      =   6366.655829 pkt/s
Packets dropped          =         1502 (0.39 %)
Average loss-burst size  =   500.666667 pkt
Error lines              =            0
------------------------------------------------------------
```

Gamabr 6. ***Tampilan histori Penerimaan Paket menggunakan D-ITG***

Gambar di atas menunjukan contoh proses pengambilan data dengan *D-ITG* di sisi pengirim dan penerima, jika proses pengiriman data sudah selesai maka dari sisi penerima akan bisa melihat parameter nilai *Quality of Service (QOS)* yang terekam di sisi penerima.

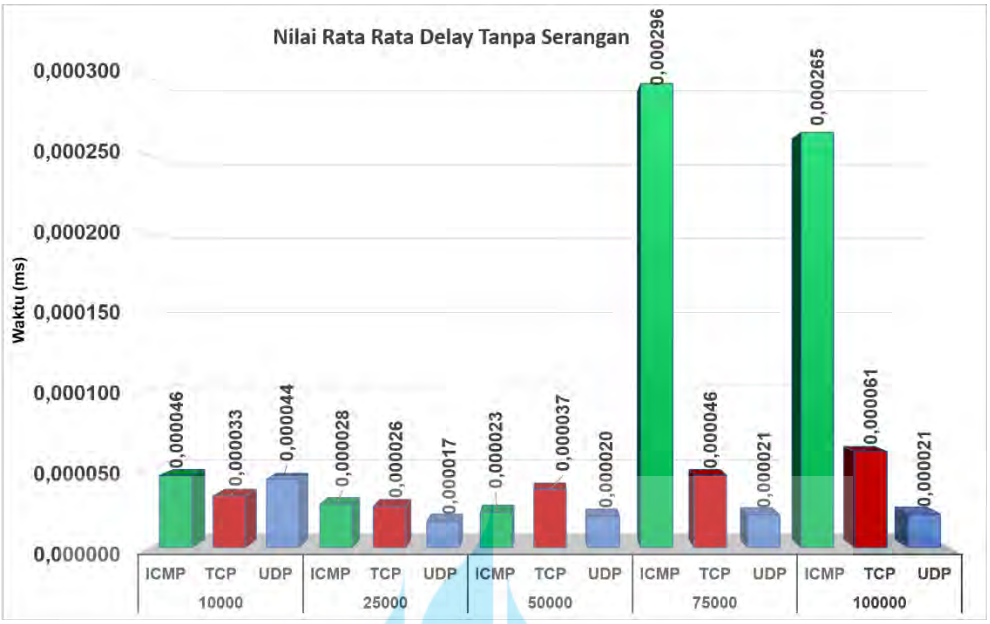
Penyerangan menggunakan jenis serangan *Sys Flood Attack* dengan terus menerus selama proses pengiriman data menggunakan *D-ITG* dan pengambilan data.

```
root@TA-SDN:~/mininet/custom# ping 192.168.0.101 -f
PING 192.168.0.101 (192.168.0.101) 56(84) bytes of data.
```

Gambar 7. ***Tampilan Penyerangan Sys Flood Attack***

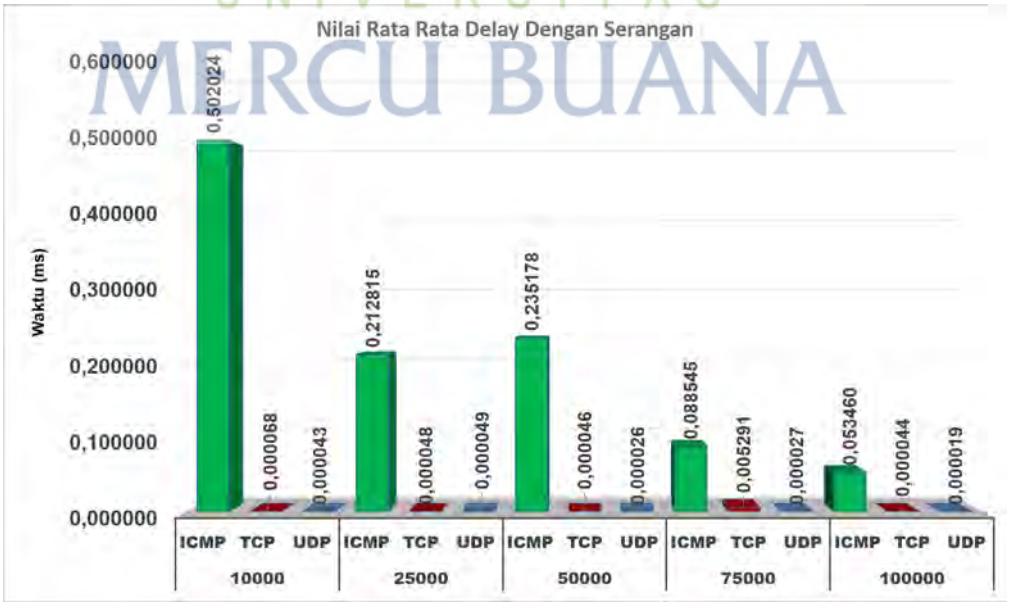
Hasil pengambilan data *Quality of Service (QoS)* menggunakan *software D-ITG* baik tanpa serangan atau dengan serangan *Sys Flood Attack* sebagai berikut.

Pengambilan Data *Quality of Service* (*QOS*) Nilai *Delay*



Gambar 8. ***Nilai delay tanpa serangan***

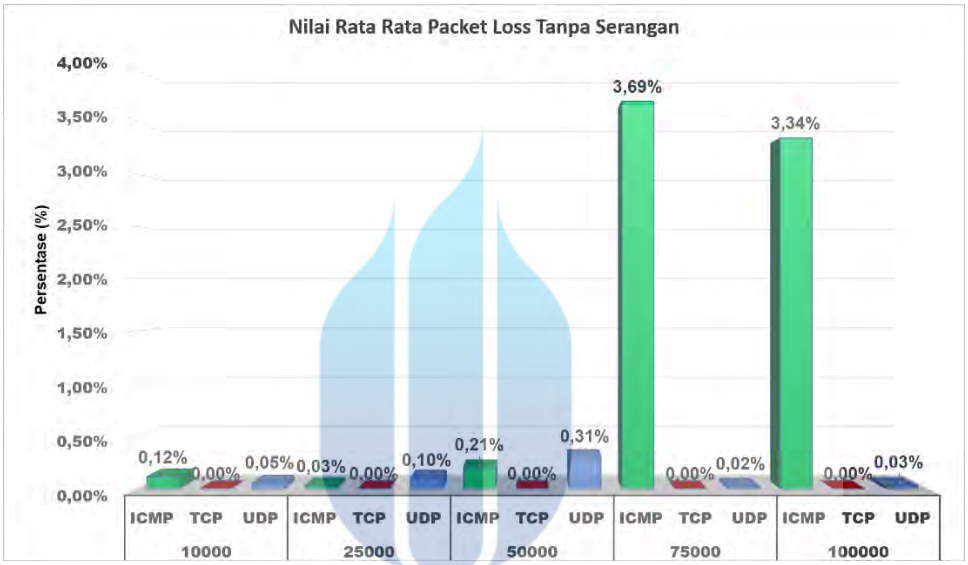
Pengujian *delay* protokol *ICMP*, *TCP* dan *UDP* tanpa serangan dengan lama waktu pengujian 60 detik dengan 10 kali percobaan menghasilkan nilai rata rata *ICMP* tertinggi di saat pengiriman paket data 75000 dengan nilai rata-rata *delay* sebesar 0,000296ms; nilai rata-rata *TCP* tertinggi di pengiriman paket data 100000 dengan nilai rata rata *delay* 0,000061ms; dan rata-rata *UDP* tertinggi bernilai rata-rata *delay* 0,00044ms di pengiriman paket data 10000. Sedangkan nilai terendah yang dihasilkan untuk protokol *ICMP* nilai rata-rata *delay* sebesar 0,000023ms di paket data 50000, protokol *TCP* di pengiriman paket data 25000 dengan rata-rata *delay* 0,000026s, dan protokol *UDP* menghasilkan nilai rata-rata 0,000017ms.



Gambar 9. ***Nilai delay dengan serangan***

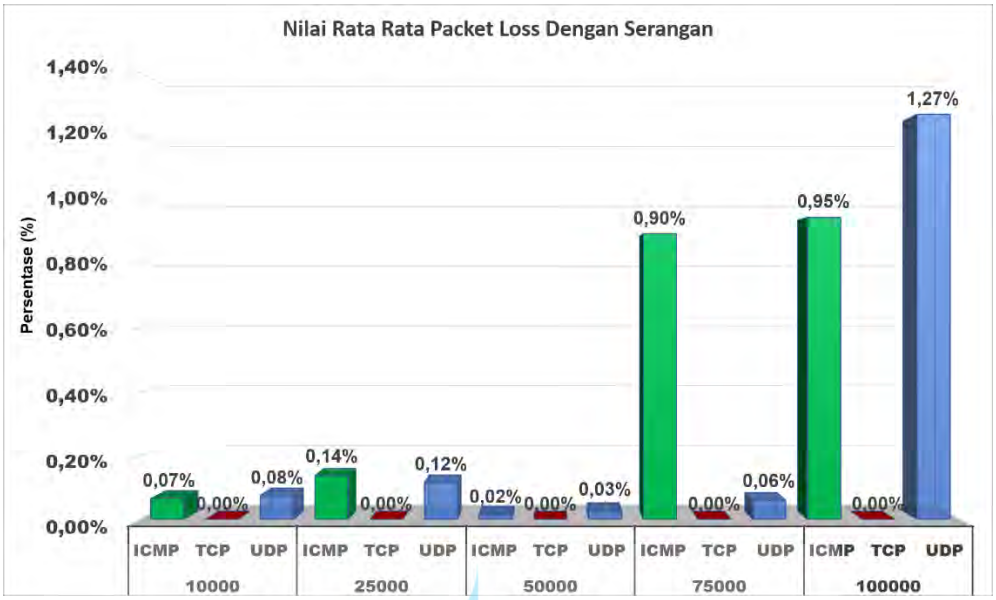
Dari hasil pengujian seperti yang digambarkan di Gambar 9, dapat dilihat hasil rata-rata pengukuran *delay* dengan besaran paket data 10000 sampai 100000 dengan serangan. Pada saat pengujian protokol *ICMP*, *TCP* dan *UDP* dilakukan dengan lama waktu 60 detik dengan 10 kali percobaan dihasilkan nilai tertinggi *delay* di pengiriman paket data 10000 di protokol *ICMP* dengan nilai rata-rata *delay* sebesar 0,502024s, untuk protokol *TCP* nilai rata-rata saat pengiriman paket data 75000 dengan nilai 0,005291s, dan di protokol *UDP* pengiriman paket data 25000 dengan nilai rata-rata *delay* 0,000049s. Sedangkan nilai terendah dihasilkan di saat pengiriman paket data 100000 di protokol *ICMP* sebesar 0,053460s dan *TCP* sebesar 0,000044s, dan nilai rata rata terendah untuk protokol UDP pada saat pengiriman paket data 100000 dengan nilai *delay* 0,000019s.

Pengambilan Data *Quality of Service* (*QOS*) Nilai Packet Loss



Gambar 10. ***Nilai packet loss tanpa serangan***

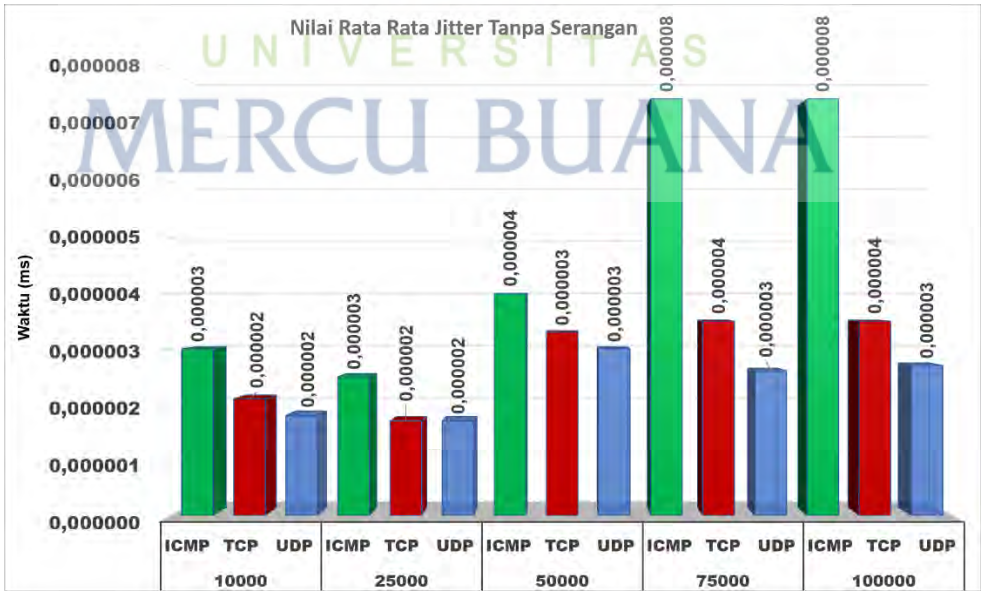
Dari hasil pengujian tanpa serangan yang ditunjukan pada Gambar 10 untuk mencari nilai packet loss dengan protokol *ICMP*, *TCP*, *UDP* dan pengiriman paket data dari 10000 sampai 100000 menghasilkan nilai rata-rata *packet loss* dengan nilai tertinggi di pengiriman paket data 75000 di protokol *ICMP* dengan nilai rata-rata 3,69%, protokol UDP di pengiriman paket data 50000 dengan nilai rata-rata 0,31%. Sedangkan nilai terendah didapat di protokol nilai rata-rata sama 0,01%.



Gambar 11. ***Nilai packet loss dengan serangan***

Dari hasil pengujian dengan serangan untuk mencari nilai *packet loss* seperti yang tergambarkan di Gambar 11, nilai rata rata yang didapat dari pegujian protokol *ICMP*, *TCP*, *UDP* dan pengiriman paket data dari 10000 sampai 100000 menghasilkan nilai rata-rata *packet loss* dengan nilai tertinggi di pengiriman paket data 100000 dengan nilia rata-rata 0,95% di protokol *ICMP* dan untuk protokol *UDP* nilai tertinggi dengan nilai rata-rata 1,27% di pengiriman paket data yang sama. Sedangkan nilai terendah di protokol *ICMP* dan *UDP* di pengiriman paket data 50000 dengan nilai rata-rata *packet loss* 0,02% untuk *ICMP* dan 0,03% *UDP*.

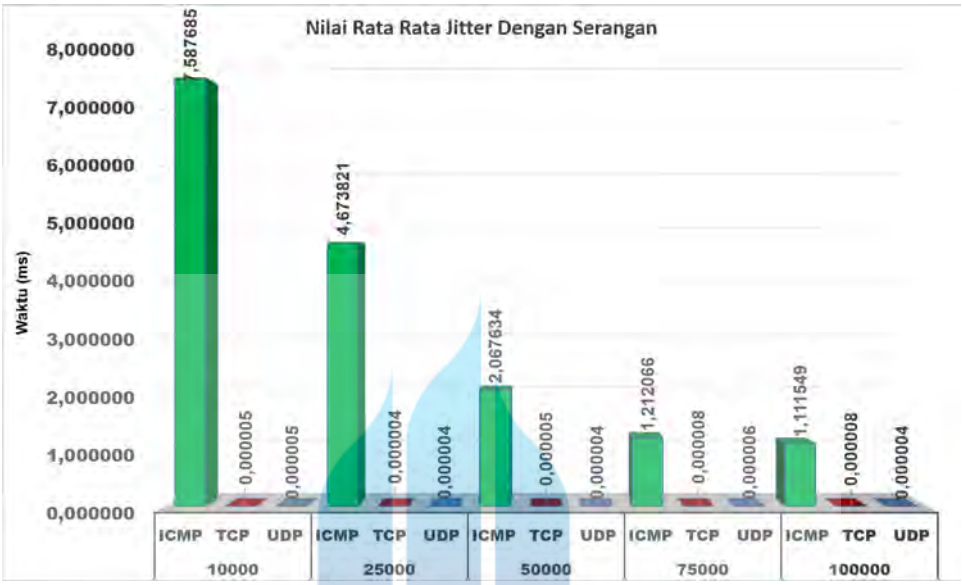
Pengambilan Data *Quality of Service* (QOS) Nilai *Jitter*



Gambar 12. ***Nilai jitter tanpa serangan***

Dari hasil pengujian *jitter* yang ditunjukan Gambar 12 pengujian protokol *ICMP, TCP* dan *UDP* tanpa serangan dengan lama waktu pengujian 60 detik dihasilkan nilai tertinggi

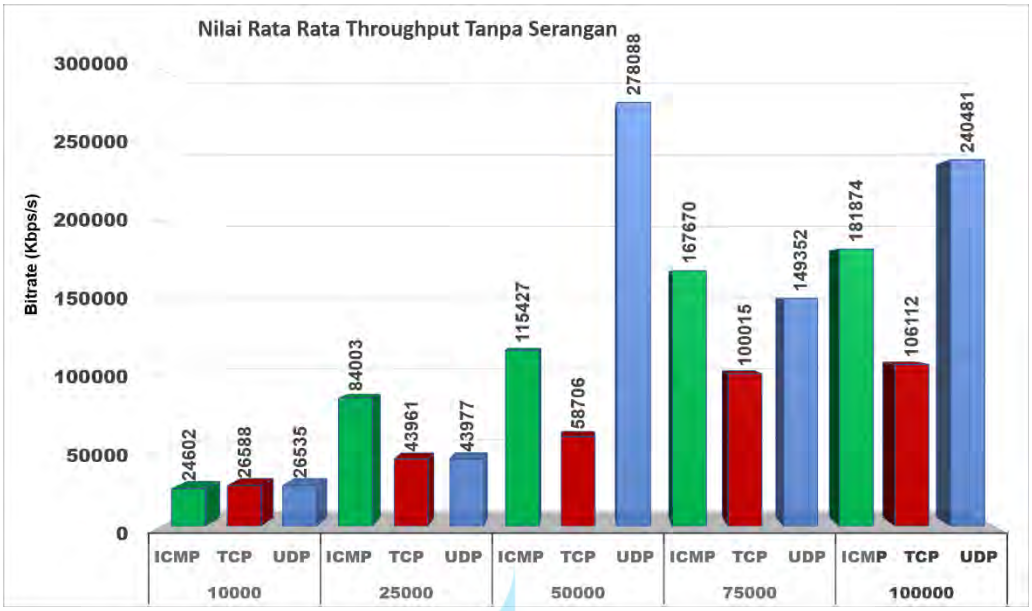
di saat pengiriman paket data 75000 dan 100000 dengan nilai rata-rata *jitter* sebesar 0,000008ms untuk protokol *ICMP*, 0,000004ms di protokol *TCP* dengan pengiriman paket data yang sama, untuk protokol *UDP* dengan pepengiriman paket data 50000, 75000, dan 100000 dengan nilai *jitter* 0,000003ms. Sedangkan nilai terendah yang dihasilkan untuk protokol *ICMP* di pengiriman paket data 10000 dan 25000 dengan nilai rata-rata *jitter* sebesar 0,000003ms, masih pengiriman paket data yang sama protokol *TCP* dan *UDP* sebesar 0,000002ms.



Gambar 13. ***Nilai jitter dengan serangan***

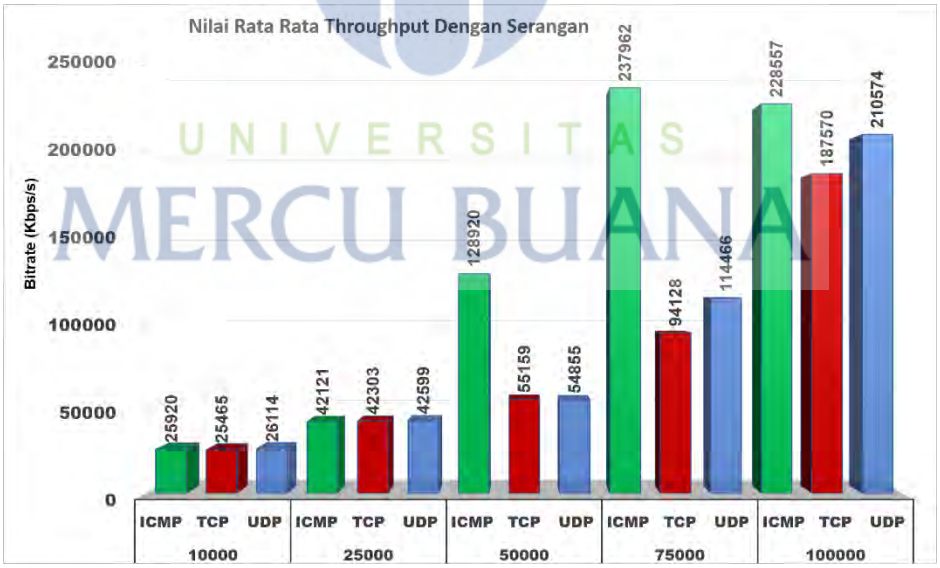
Dari hasil pengujian *jitter* yang ditunjukan Gambar 13 pada saat pengujian protokol *ICMP*, *TCP* dan *UDP* dengan serangan lama waktu pengujian 60 detik dihasilkan nilai tertinggi di saat pengiriman paket data 10000 dengan nilai rata-rata *jitter* sebesar 7,587685ms di protokol *ICMP*, 0,000008ms di protokol *TCP* dengan pengiriman paket data 75000 dan 100000, dan untuk protokol *UDP* sebesar 0,000006ms dengan pengiriman paket data 75000. Sedangkan nilai terendah yang dihasilkan untuk protokol *ICMP* di pengiriman paket data 100000 dengan nilai rata-rata *jitter* sebesar 1,111549ms, protokol *TCP* dangan pengiriman paket data 25000 sebesar 0,000004ms, sedangkan untuk protokol *UDP* di pengiriman paket data 50000 dan 100000 menghasilkan nilai rata-rata 0,000004ms.

Pengambilan Data *Quality of Service* (*QOS*) Nilai *Throughput*



Gambar 14. ***Nilai throughput tanpa serangan***

Nilai rata-rata *throughput* saat uji coba tanpa serangan seperti yang ditunjukan pada Gambar 14 menunjukan nilai tertinggi rata-rata *throughput* untuk protokol *ICMP* sebesar 181874 kbps dipengiriman paket data 100000, protokol *TCP* sebesar 106112 kbps di pengiriman paket data yang sama, dan untuk protokol *UDP* sebesar 240481 kbps di pengiriman paket data 50000. Sedangkan untuk nilai rata-rata terkecil *throughput* di protokol *ICMP*, *TCP* dan *UDP* semuanya di pengiriman paket data 10000 sebesar 24602 kbps untuk *ICMP*, 26588 kbps untuk *TCP*, dan untuk *UDP* sebesar 26535 kbps.



Gambar 15. ***Nilai throughput dengan serangan***

Uji coba dengan serangan untuk mencari nilai *throughput* seperti yang ditunjukan pada Gambar 15 menunjukan nilai tertinggi rata-rata *throughput* untuk protokol *ICMP* sebesar 237961 kbps di pengiriman paket data 75000, protokol *TCP* sebesar 187570 kbps di pengiriman data 100000, dan untuk protokol *UDP* sebesar 210574 kbps di pengiriman paket data 100000. Sedangkan untuk nilai rata-rata terkecil *throughput* yang didapat di protokol *ICMP*, *TCP* dan *UDP* semuanya terdapat di uji coba pengiriman paket data 10000

dengan nilai rata rata sebesar 25920 kbps untuk *ICMP*, 25645 kbps untuk *TCP*, dan untuk *UDP* sebesar 26114 kbps.

IV.PENUTUP

A. Simpulan

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa nilai yang didapat dari hasil uji coba baik tanpa serangan maupun dangan serangan didapatkan nilai rata rata sebagai berikut :

1. Nilai rata rata *delay* tertinggi selama pengujian baik itu tanpa serangan maupun dengan serangan dengan nilai rata-rata untuk protokol ICMP 0,502024s, TCP 0,005291s, dan juga UDP 0,000049s.
2. Nilai rata rata *packet loss* tertinggi selama pengujian baik itu tanpa serangan maupun dengan serangan dengan nilai rata-rata untuk protokol ICMP 3,69%, dan UDP 1,27%.
3. Nilai rata rata *jitter* tertinggi selama pengujian baik itu tanpa serangan maupun dengan serangan dengan nilai rata-rata untuk protokol ICMP 7,587685ms, TCP 0,000008ms, dan juga UDP 0,000006ms.
4. Nilai rata rata *throughput* tertinggi selama pengujian baik itu tanpa serangan maupun dengan serangan dengan nilai rata-rata untuk protokol ICMP 0,10237961 kbps, TCP 187570 kbps, dan juga UDP 240481 kbps.
5. Dari hasil yang didapat dengan nilai rata rata tertinggi *delay, packet loss, jitter* dan *throughput* masih masuk ke dalam kategori sangat baik menurut standar dari Tabel 2. Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

B. Saran

Untuk lebih sepesifik, dalam penelitian selanjutnya bisa menggunakan perangkat langsung yang diaplikasikan langsung ke dalam topologi *Software Defind Netwrok (SDN*) untuk didapatkan nilai yang bisa dibandingkan. dengan jaringan yang ada di virtual Mininet atau sejenisnya.

UCAPAN TERIMA KASIH

Terima kasih untuk Yayasan Budi Pekerti Luhur telah mengijinkan melakukan penelitian untuk memenuhi tugas akhir.

DAFTAR PUSTAKA

[1] A. Yasin and I. Mohidin, “Dampak Serangan DDoS pada Software Based Openfow Switch di Perangkat HG553,” *J. Technopreneur*, vol. 6, no. 2, p. 72, 2018.

[2] Y. S. H. Roni Fernando Simarmata, Rohmat Tulloh, “Simulasi Jaringan Software Defined Network Menggunakan Protokol Routing Ospf Dan Ryu Controller,” *e-Proceeding Appl. Sci.*, vol. 4, no. 3, pp. 2887–2896, 2018.

[3] I. Ummah, “Perancangan Simulasi Jaringan Virtual Berbasis Software-Define Networking,” *Indones. J. Comput.*, vol. 1, no. 1, pp. 95–106, 2016.

[4] A. Irmawati, I. D. Irawati, and Y. S. Hariyani, “Implementasi Protokol Routing Ospf Pada Software Defined Network Berbasis Routeflow,” *E-Proceeding Apllied Sci.*, vol. 2, no. 3, pp. 1053–1061, 2016.

[5] D. Halomoan, M. Z.-J. T. I. Kaputama, and undefined 2017, “Karakteristik Openflow Controller dengan ONOS,” *Jurnal.Kaputama.Ac.Id*, vol. 1, no. 1, pp. 10–14, 2017.

[6] R. Kartadie, E. Utami, and E. Pramono, “Prototipe Infrastruktur Software-Defined Network Dengan Protokol OpenFlow Menggunakan UBUNTU Sebagai Kontroler,” *Dasi*, vol. 15, no. 1, 2014.

[7] R. Kartadie and B. Satya, “Uji Performa Kontroler Floodlight Dan Opendaylight Sebagai

Komponen Utama Arsitektur Software-Defined Network," *Semnasteknomedia Online*, no. February 2015, 2015.

[8] M. H. Hidayat and N. R. Rosyid, "Analisis Kinerja dan Karakteristik Arsitektur Software-Defined Network Berbasis OpenDaylight Controller," *Citee*, no. 2085–6350, pp. 194–200, 2017.

[9] E. Safrianti, L. O. Sari, R. A. Mahan, J. Elektro, and F. Teknikniversitas, "Data Unri Menggunakan," pp. 5–9, 2019.

[10] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 162–172, 2016.

[11] I. Nurhaida and I. Ichsan, "Congestion Control Pada Jaringan Komputer Berbasis Multi Protocol Label Switching (Mpls)," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 11, no. 1, pp. 77–88, 2020.

[12] D. H. JANIUS, "Analisis Qos Video Streaming Pada Jaringan Wireless Menggunakan Metode HTB (Hierarcichal Token Bucket)," *Skripsi Jur. Tek. Inform. Fak. Sains dan Teknol. Univ. Islam Negeri Sultan Syarif Kasim Riau Pekanbaru*, 2013.

[13] R. T. Jurnal, "Analisis Kinerja Routing Protokol RIPng Dengan OSPFv3 Pada Jaringan IPV6 Tunneling," *Petir*, vol. 10, no. 2, pp. 56–36, 2018.

[14] T. Anggita and H. Fitriawan, "ANALYTICAL STUDY OF QoS (Quality of Service) IN THE IMPLEMENTATION OF VOICE COMMUNICATION APPLICATION VoIP (Voice over Internet Protocol) ON THE INTRANET NETWORK AT," no. 2, pp. 141–155, 2012.

[15] M. F. Muntaha, P. H. Trisnawan, and R. Primananda, "Implementasi Intrusion Prevention System (Ips) Berbasis Athena Untuk Mencegah Serangan Ddos Pada Arsitektur Software-Defined Network (Sdn)," vol. 3, no. 7, pp. 6847–6855, 2019.

[16] A. Yasin, E. Utami, and E. Pramono, "Pengujian Serangan Distributed Denial of Service (DDoS) Di Jaringan Software-Defined Pada GNS3," *J. Teknol. Inf.*, vol. XI, no. 32, pp. 1–8, 2016.

[17] R. Kurniawan, "Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode NDLC (Network Development Life Cycle) Pada BPU Bagas Raya Lubuk Linggau," *J. Ilm. Betrik*, vol. 7, no. 01, pp. 50–59, 2016.

[18] K. NUGROHO and D. P. SETYANUGROHO, "Analisis Kinerja RouteFlow pada Jaringan SDN (Software Defined Network) menggunakan Topologi Full-Mesh," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 7, no. 3, p. 585, 2019.

[19] D. F. Mubarok, "Analisis Penerapan Dan Uji Performa Intrusion Detection System (Ids) Pada Jaringan Berbasis Software Defined Network (Sdn) Analisis Penerapan Dan Uji Performa Intrusion Detection System," no. November 2017, 2018.

[20] K. Anam and R. Adrian, "Analisis Performa Jaringan Software Defined Network Berdasarkan Penggunaan Cost Pada Protokol Ruting Open Shortest Path First," *Citee*, pp. 1–8, 2017.

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul di atas. Kertas kerja berisi semua material hasil penelitan Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan:

A. literature review
B. Hasil analisa & perancangan aplikasi
C. Source Code
D. Tahapan eksperimen

Hasil eksperimen secara keseluruhan