



UNIVERSITAS INDONESIA

**ANALISIS PERFORMANSI JARINGAN *BIDIRECTIONAL*
TUNNELING MOBILE IPV6 DENGAN SERANGAN
DISTRIBUTED DENIAL OF SERVICE PADA APLIKASI FTP**

SKRIPSI

ALDIANSAH PRAYOGI

0906557511

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

DEPARTEMEN TEKNIK ELEKTRO

TEKNIK KOMPUTER

DEPOK

JUNI 2013



UNIVERSITAS INDONESIA

**ANALISIS PERFORMANSI JARINGAN *BIDIRECTIONAL*
TUNNELING MOBILE IPV6 DENGAN SERANGAN
DISTRIBUTED DENIAL OF SERVICE PADA APLIKASI FTP**

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

ALDIANSAH PRAYOGI

0906557511

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

DEPARTEMEN TEKNIK ELEKTRO

TEKNIK KOMPUTER

DEPOK

JUNI 2013

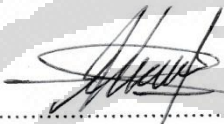
HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Aldiansah Prayogi

NPM : 0906557511

Tanda Tangan

: 

Tanggal

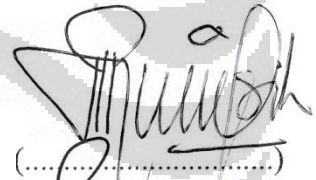
: 14 Juni 2013

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : Aldiansah Prayogi
NPM : 0906557511
Program Studi : Teknik Komputer
Judul Skripsi : **ANALISIS PERFORMANSI JARINGAN
*BIDIRECTIONAL TUNNELING MOBILE
IPV6 DENGAN SERANGAN *DISTRIBUTED
DENIAL OF SERVICE* PADA APLIKASI FTP***

Telah dipresentasikan dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia.

Pembimbing : Ir. A. Endang Sriningsih M.T. Si



(.....)

Penguji : Dr. Ir. Anak Agung Putri Ratna M. Eng



(.....)

Penguji : Muhammad Salman S. T., M. IT



(.....)

Ditetapkan di : Depok

Tanggal : 14 Juni 2013

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT karena berkat rahmat-Nya saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini bertujuan untuk memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Komputer pada Fakultas Teknik Universitas Indonesia. Dalam penyelesaian penulisan skripsi ini, saya mengucapkan terima kasih kepada:

1. Ir. Endang Sriningsih MT, Si selaku dosen pembimbing yang telah bersedia menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam menyusun skripsi ini.
2. Orang tua dan keluarga yang selalu mendukung dan mendoakan saya demi kesuksesan skripsi ini.
3. Muhammad Iqbal, Jihan Prama, Ihsan Nugraha, Mahesa Adhitya Putra, dan Ivan Farhan Fauzi selaku teman sebimbingan skripsi.
4. Teman-teman Laboratorium Digital Universitas Indonesia yang selalu menjadi inspirasi saya.

Saya mohon maaf jika terdapat kekurangan dan kesalahan dalam segala hal terkait penulisan skripsi ini. Kritik dan saran saya harapkan untuk membangun skripsi ini. Saya berharap agar skripsi ini dapat memberikan hal yang positif dan berguna bagi pengembangan ilmu pengetahuan dan teknologi di Indonesia.

Depok, 14 Juni 2013



Aldiansah Prayogi

**HALAMAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Aldiansah Prayogi
NPM : 0906557511
Program Studi : Teknik Komputer
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis Karya : Skripsi

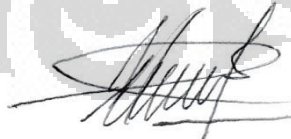
demikian perkembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul:

**ANALISIS PERFORMANSI JARINGAN *BIDIRECTIONAL*
TUNNELING MOBILE IPV6 DENGAN SERANGAN
DISTRIBUTED DENIAL OF SERVICE PADA APLIKASI FTP**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Depok
Pada tanggal: 14 Juni 2013
Yang menyatakan,



(Aldiansah Prayogi)

ABSTRAK

Nama : Aldiansah Prayogi
Program Studi : Teknik Komputer
Judul : ANALISIS PERFORMANSI JARINGAN
BIDIRECTIONAL TUNNELING MOBILE IPV6
DENGAN SERANGAN *DISTRIBUTED DENIAL OF SERVICE* PADA APLIKASI FTP

Mobile IPv6 merupakan komunikasi perangkat mobile yang memungkinkan koneksi tetap terhubung meskipun berpindah dari *Home Network* ke *Foreign Network*. Dalam mempertahankan koneksi, terdapat beberapa metode, salah satunya adalah *Bidirectional Tunelling*. Jaringan *Bidirectional mobile IPV6* dengan aplikasi FTP yang di rancang akan diuji performanya dengan serangan *Distributed Denial of Service* yang dibedakan besar paket data serangannya. Parameter pengukuran yang digunakan adalah transfer time, delay, throughput, dan packet loss. Transfer time, delay, dan packet loss di *Home Network* saat diserang DDoS 2600KB mencapai kenaikan 392.78%, 372.46%, dan 11446.48. Sedangkan throughput di *Home Network* saat diserang dengan DDoS 2600KB mencapai penurunan 77.83%. Performansi jaringan dengan aplikasi FTP di *Home Network* memiliki kinerja yang lebih baik dibandingkan di *Foreign Network*. Dari hasil pengukuran dapat disimpulkan semakin besar paket data serangannya maka semakin berpengaruh terhadap buruknya parameter tersebut. Namun dengan semakin besarnya paket data serangan maka semakin lama pengiriman flooding paket data tersebut akibat pemrosesan yang semakin berat juga. Hal tersebut yang mengakibatkan perbedaan persentase terlalu signifikan pada paket data serangan yang terlalu besar.

Kata kunci:

Mobile IPv6, FTP, Distributed Denial of Service, transfer time, delay, throughput, packet loss.

ABSTRACT

Name : Aldiansah Prayogi
Study Program : Computer Engineering
Title : PERFORMANCE ANALYSIS OF BIDIRECTIONAL
MOBILE IPV6 WITH DISTRIBUTED DENIAL OF
SERVICE ATTACK ON FTP APPLICATION

Mobile IPv6 is a communication between mobile devices which allow the connection stays alive even move from the Home Network to the Foreign Network. In maintaining the connection, there are some of methods, one of them is Bidirectional Tunneling. Bidirectional mobile IPv6 network with FTP application which is designed will be tested its performance with the Distributed Denial of Service attack which is distinguished its large attack data packets. Measurement parameters used are the transfer time, delay, throughput, and packet loss. Transfer time, delay, and packet loss in the Home Network when its attacked with DDoS 2600KB increase 392.78%, 372.46%, and 11446.48%. While the throughput in the Home Network when its attacked with DDoS 2600KB decrease 77.83%. This network performances with the FTP application in the Home Network has a better performance than in the Foreign Network. The measurement result, bigger attack data packet which is used will be more powerful against bad that parameters. But bigger attack data packet make sending flood data packet slower because the process is harder too. This thing that causing the percentage difference is not too significant on attack data packet which is too big.

Keywords:

Mobile IPv6, FTP, Distributed Denial of Service, transfer time, delay, throughput, packet loss.

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	ii
HALAMAN PENGESAHAN.....	iii
KATA PENGANTAR	iv
HALAMAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	v
ABSTRAK.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiii
BAB 1	1
PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Tujuan.....	2
1.3 Metodologi penelitian.....	2
1.4 Pembatasan masalah.....	3
1.5 Sistematika penulisan	3
BAB 2	5
<i>MOBILE</i> INTERNET PROTOCOL VERSI 6.....	5
2.1 IPv6.....	5
2.1.1 Pengalamatan IPv6	6
2.2 <i>Mobile</i> IPv6	11
2.2.1 <i>Bidirectional Mobile</i> IPv6	15
2.2.2 <i>Route Optimization Mobile</i> IPv6.....	17
2.2.3 <i>Handover Mobile</i> IPv6	18
2.4 Keamanan Jaringan pada <i>Mobile</i> IP	26
2.4.1 <i>Distributed Denial of Service</i>	27
BAB 3	29
KONFIGURASI DAN IMPLEMENTASI APLIKASI FTP PADA JARINGAN <i>BIDIRECTIONAL MOBILE</i> IPv6 SERTA SERANGANNYA.....	29

3.1	Topologi Jaringan	29
3.2	Spesifikasi Sistem.....	30
3.2.1	Spesifikasi Hardware.....	30
3.2.2	Spesifikasi <i>Software</i>	32
3.3	Skenario Penyerangan	34
3.3.1	Skenario Pertama.....	34
3.3.2	Skenario Kedua.....	36
3.3.3	Skenario Ketiga	38
3.3.4	Skenario Keempat.....	40
3.4	Pembuatan Sistem.....	42
3.4.1	Instalasi Kernel.....	43
3.4.2	Instalasi UMIP dan RADVD.....	43
3.4.3	Instalasi Wing FTP Server.....	43
3.4.4	Rekayasa Trafik.....	44
3.4.5	Konfigurasi Node	45
BAB 4	47
ANALISIS PERFORMANSI JARINGAN <i>BIDIRECTIONAL MOBILE IPv6</i>		
DENGAN APLIKASI FTP.....		47
4.1	Pengujian Parameter Performansi	47
4.2	Mekanisme Serangan.....	51
4.3	Analisis Parameter Performansi	51
4.3.1	Analisis Transfer Time	51
4.3.2	Analisis Delay.....	60
4.3.3	Analisis Throughput	69
4.3.4	Analisis Packet Loss.....	79
BAB 5	89
KESIMPULAN.....		89
DAFTAR REFERENSI		90
LAMPIRAN 1		91
KONFIGURASI KERNEL DAN UMIP		91
1.1	Pengunduhan kernel	91
1.2	Penginstalan UMIP.....	92

1.3 Program <i>init.d mip6d</i>	92
LAMPIRAN 2.....	96
KONFIGURASI <i>HOME AGENT & HOME ROUTER</i>	96
2.1 Konfigurasi Interface <i>Home Agent</i>	96
2.2 Konfigurasi <i>static routing</i>	96
2.3 Konfigurasi beberapa fungsi pada <i>home router</i>	96
2.4 Konfigurasi <i>mip6d.conf</i> pada <i>Home Agent</i>	96
2.5 Konfigurasi <i>setkey.conf</i>	97
2.6 Konfigurasi <i>radvd.conf</i>	98
LAMPIRAN 3.....	99
KONFIGURASI <i>FOREIGN ROUTER</i>	99
3.1 Konfigurasi Interface <i>Foreign Agent</i>	99
3.2 Konfigurasi <i>static routing</i>	99
3.4 Konfigurasi beberapa fungsi pada <i>foreign router</i>	99
3.5 Konfigurasi <i>radvd.conf</i>	99
LAMPIRAN 4.....	100
<i>CORRESPONDENT NODE</i>	100
4.1 Konfigurasi Interface <i>Correspondent Agent</i>	100
4.2 Konfigurasi <i>static routing</i>	100
4.3 Konfigurasi <i>mip6d.conf</i>	100
LAMPIRAN 5.....	101
<i>MOBILE NODE</i>	101
5.1 Konfigurasi <i>mip6d.conf</i>	101
5.2 Konfigurasi beberapa fungsi <i>mobile node</i>	102

DAFTAR GAMBAR

Gambar 2.1 Format header IPv6	7
Gambar 2.2 <i>Mobile IP</i>	11
Gambar 2.3 <i>Bidirectional tunneling</i>	16
Gambar 2.4 <i>Route optimization tunneling</i>	17
Gambar 2.5 <i>Horizontal Handover</i>	18
Gambar 2.6 <i>Vertical handover</i> dengan ISP yang sama.....	19
Gambar 2.7 <i>Vertical handover</i> dengan ISP yang berbeda	19
Gambar 2.8 Model dari FTP	23
Gambar 2.9 Distributed Denial of Service	28
Gambar 3.1 Gambar rencana topologi jaringan	29
Gambar 3.2 <i>Mobile Node</i> pada saat di <i>Home Network</i>	35
Gambar 3.3 <i>Mobile Node</i> saat berpindah ke <i>Foreign Network</i>	36
Gambar 3.4 <i>Mobile Node</i> pada saat di <i>Home Network</i> dan diserang dengan DDoS 200KB	37
Gambar 3.5 <i>Mobile Node</i> saat pindah ke <i>Foreign Network</i> dan diserang dengan DDoS 200KB	38
Gambar 3.6 <i>Mobile Node</i> pada saat di <i>Home Network</i> dan diserang dengan DDoS 1400KB	39
Gambar 3.7 <i>Mobile Node</i> saat pindah ke <i>Foreign Network</i> dan diserang dengan DDoS 1400KB	40
Gambar 3.8 <i>Mobile Node</i> pada saat di <i>Home Network</i> dan diserang dengan DDoS 2600KB	41
Gambar 3.9 <i>Mobile Node</i> saat pindah ke <i>Foreign Network</i> dan diserang dengan DDoS 2600KB	42
Gambar 4.1 Hasil Wireshark sebelum di- <i>filter</i>	48
Gambar 4.2 Hasil Wireshark setelah di- <i>filter</i>	48

Gambar 4.3 <i>Summary</i> dari Wireshark	50
Gambar 4.4 Grafik perbandingan transfer time di <i>Home Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	55
Gambar 4.5 Grafik perbandingan transfer time di <i>Foreign Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	58
Gambar 4.6 Grafik perbandingan transfer time seluruh keadaan sebelum dan sesudah diserang.....	59
Gambar 4.7 Grafik perbandingan delay di <i>Home Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	65
Gambar 4.8 Grafik perbandingan delay di <i>Foreign Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	67
Gambar 4.9 Grafik perbandingan delay seluruh keadaan sebelum dan sesudah diserang	68
Gambar 4.10 Grafik perbandingan throughput di <i>Home Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	74
Gambar 4.11 Grafik perbandingan throughput di <i>Foreign Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	76
Gambar 4.12 Grafik perbandingan throughput seluruh keadaan sebelum dan sesudah diserang.....	78
Gambar 4. 13 Grafik perbandingan packet loss di <i>Home Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	84
Gambar 4. 14 Grafik perbandingan packet loss di <i>Foreign Network</i> sebelum dan sesudah diserang dengan <i>Distributed Denial of Service</i>	86
Gambar 4. 15 Grafik perbandingan packet loss seluruh keadaan sebelum dan sesudah diserang.....	87

DAFTAR TABEL

Tabel 4. 1 Transfer time pada <i>Home</i> dan <i>Foreign Network</i> sebelum diserang.....	52
Tabel 4. 2 Transfer time pada <i>Home Network</i> dengan serangan <i>Distributed Denial of Service</i>	54
Tabel 4. 3 Transfer time pada <i>Foreign Network</i> dengan serangan <i>Distributed Denial of Service</i>	56
Tabel 4. 4 Delay pada <i>Home</i> dan <i>Foreign Network</i> sebelum diserang.....	62
Tabel 4. 5 Delay pada <i>Home Network</i> dengan serangan <i>Distributed Denial of Service</i>	63
Tabel 4. 6 Delay pada <i>Foreign Network</i> dengan serangan <i>Distributed Denial of Service</i>	66
Tabel 4. 7 Throughput pada <i>Home</i> dan <i>Foreign Network</i> sebelum diserang.....	71
Tabel 4. 8 Throughput pada <i>Home Network</i> dengan serangan <i>Distributed Denial of Service</i>	72
Tabel 4. 9 Throughput pada <i>Foreign Network</i> dengan serangan <i>Distributed Denial of Service</i>	75
Tabel 4. 11 Packet loss pada <i>Home</i> dan <i>Foreign Network</i> sebelum diserang.....	81
Tabel 4. 12 Packet loss pada <i>Home Network</i> dengan serangan <i>Distributed Denial of Service</i>	82
Tabel 4. 13 Packet loss pada <i>Foreign Network</i> dengan serangan <i>Distributed Denial of Service</i>	85

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Teknologi jaringan yang semakin berkembang membuat teknologi jaringan ini menjadi suatu kebutuhan. Untuk memenuhi kebutuhan komunikasi data, komunikasi melalui jaringan internet menjadi hal utama saat ini. Dengan menjadikan internet sebagai media komunikasi yang umum maka jumlah pengguna jaringan internet juga akan semakin bertambah. Dengan bertambahnya kebutuhan akan jaringan internet ini maka banyak aspek yang harus diperhatikan, salah satunya adalah ketersediaan alamat IP yang merupakan hal mendasar dalam teknologi jaringan. Setiap pengguna internet harus memiliki satu alamat IP untuk dapat menggunakan layanan komunikasi melalui internet. IP ini bersifat unik pada setiap host yang menggunakan fasilitas internet. Walaupun terdapat IP private, namun intinya host yang menggunakan IP private tetap menggunakan IP publik induk yang digunakan. Dengan kata lain semakin bertambahnya kebutuhan akan pengguna layanan komunikasi internet maka akan semakin bertambah pula kebutuhan ketersediaan IP.

Ketersediaan IP saat ini sudah mulai terbatas karena IPv4 yang hanya berjumlah 32 bit. Jumlah orang di bumi sekitar 7 milyar dan seluruhnya tidak dapat dicukupi dengan jumlah IPv4 tersebut. Selain itu satu orang bisa menggunakan lebih dari satu host pada jaringan internet. Dengan kata lain penggunaan layanan internet melebihi jumlah orang di bumi ini. Dalam memecahkan masalah ini, maka diciptakanlah IPv6 yang berkapasitas 128 bit. Dengan adanya IPv6 ini, ketersediaan jumlah IP di dunia lebih dari cukup.

Kebutuhan teknologi saat ini adalah teknologi yang dapat mendukung mobilitas tinggi. Kebutuhan *mobile* ini juga terdapat pada IPv6 yang disebut sebagai *mobile* IPv6. Tingginya kebutuhan teknologi *mobile* IPv6 ini akan menarik kesempatan *hacker* atau *cracker* untuk melakukan serangan. Serangan akan ditujukan untuk mempengaruhi performansi dari teknologi *mobile* IPv6 ini.

Untuk itu keamanan jaringan pada teknologi *mobile* IPv6 ini sangat dibutuhkan guna mencegah serangan-serangan ini.

Yang melatarbelakangi penggunaan aplikasi FTP pada skripsi ini adalah tingginya penggunaan layanan *mobile* internet untuk mendownload suatu data. Serangan yang dilakukan terhadap aplikasi FTP pada jaringan *mobile* IPv6 ini dapat mempengaruhi transfer time, delay, packet loss, dan throughput-nya selama proses *mobile* download berlangsung.

1.2 Tujuan

Tujuan penulisan skripsi ini adalah untuk menjelaskan prinsip kerja *mobile* IPv6 yang diimplementasikan pada jaringan komputer, kinerja *mobile* IPv6 dengan mengimplementasikan metode *bidirectional* pada aplikasi *File Transfer Protocol* (FTP), menganalisis performansi jaringan *bidirectional mobile* IPv6 yang diserang dengan metode *Distributed Denial of Service* pada aplikasi FTP, dan menganalisis pengaruh besar paket serangan *Distributed Denial of Service* terhadap buruknya performansi jaringan ini dengan aplikasi FTP.

1.3 Metodologi penelitian

Metodologi penelitian yang digunakan dalam penulisan skripsi ini adalah sebagai berikut.

1. Metode studi literatur

Dalam metode ini, sumber dicari melalui media internet atau buku-buku yang diobservasi baik *e-book* maupun buku cetak yang berkaitan dengan *mobile* IPv6, *bidirectional tunneling*, *Distributed Denial of Service* dan hal-hal yang penting untuk penulisan skripsi ini.

2. Metode diskusi

Dalam metode ini, sumber dicari dengan berdiskusi dengan pembimbing tugas akhir dan orang-orang yang ahli dengan hal-hal penting mengenai materi bahasan skripsi ini.

3. Perancangan jaringan

Dalam metode ini, jaringan dirancang untuk pengukuran dan analisis performansi aplikasi FTP dengan jaringan *bidirectional mobile* IPv6 yang diserang dengan metode *Distributed Denial of Service*.

4. Pengukuran dan analisis

Dalam metode ini, pengukuran dan analisis performansi serangan *Distributed Denial of Service* pada aplikasi FTP dengan *bidirectional mobile IPv6* dilakukan dengan parameter transfer time, delay, packet loss, dan throughput.

1.4 Pembatasan masalah

Batasan masalah dalam penulisan skripsi ini adalah sebagai berikut.

1. Pemahaman konsep dan sistem kerja *mobile IPv6* dengan metode *bidirectional*.
2. Pemahaman bentuk FTP yang diimplementasikan pada jaringan *mobile IPv6*.
3. Pembahasan efek yang dihasilkan apabila FTP pada *mobile IPv6* dengan metode *bidirectional tunneling* yang diserang dengan metode *Distributed Denial of Service*.
4. Analisis performansi jaringan *bidirectional mobile IPv6* dengan aplikasi FTP yang diserang dan besar paket data serangan dengan parameter transfer time, delay, packet loss, dan throughput. Analisis dilakukan dengan perbandingan ketika jaringan *bidirectional mobile IPv6* dengan aplikasi FTP diserang dengan variasi tiga besar paket data serangan *Distributed Denial of Service*.

1.5 Sistematika penulisan

Penulisan skripsi ini dilakukan dengan urutan yang memiliki bahasan masing-masing untuk memudahkan pembahasan. Bahasan tersebut adalah sebagai berikut.

1. BAB 1 Pendahuluan

Bab ini berisi tentang latar belakang, tujuan, pembatasan masalah, metodologi penulisan, dan sistematika penulisan.

2. BAB 2 *Mobile Internet Protocol* versi 6

Bab ini berisi tentang gambaran mengenai *IPv6*, *mobile IPv6*, *bidirectional tunneling*, FTP, metode serangan *Distributed Denial of Service*, dan semua hal penting yang berkaitan dengan bahasan skripsi ini.

3. BAB 3 Konfigurasi dan Implementasi Aplikasi FTP pada Jaringan *Bidirectional Mobile IPv6* serta Serangannya

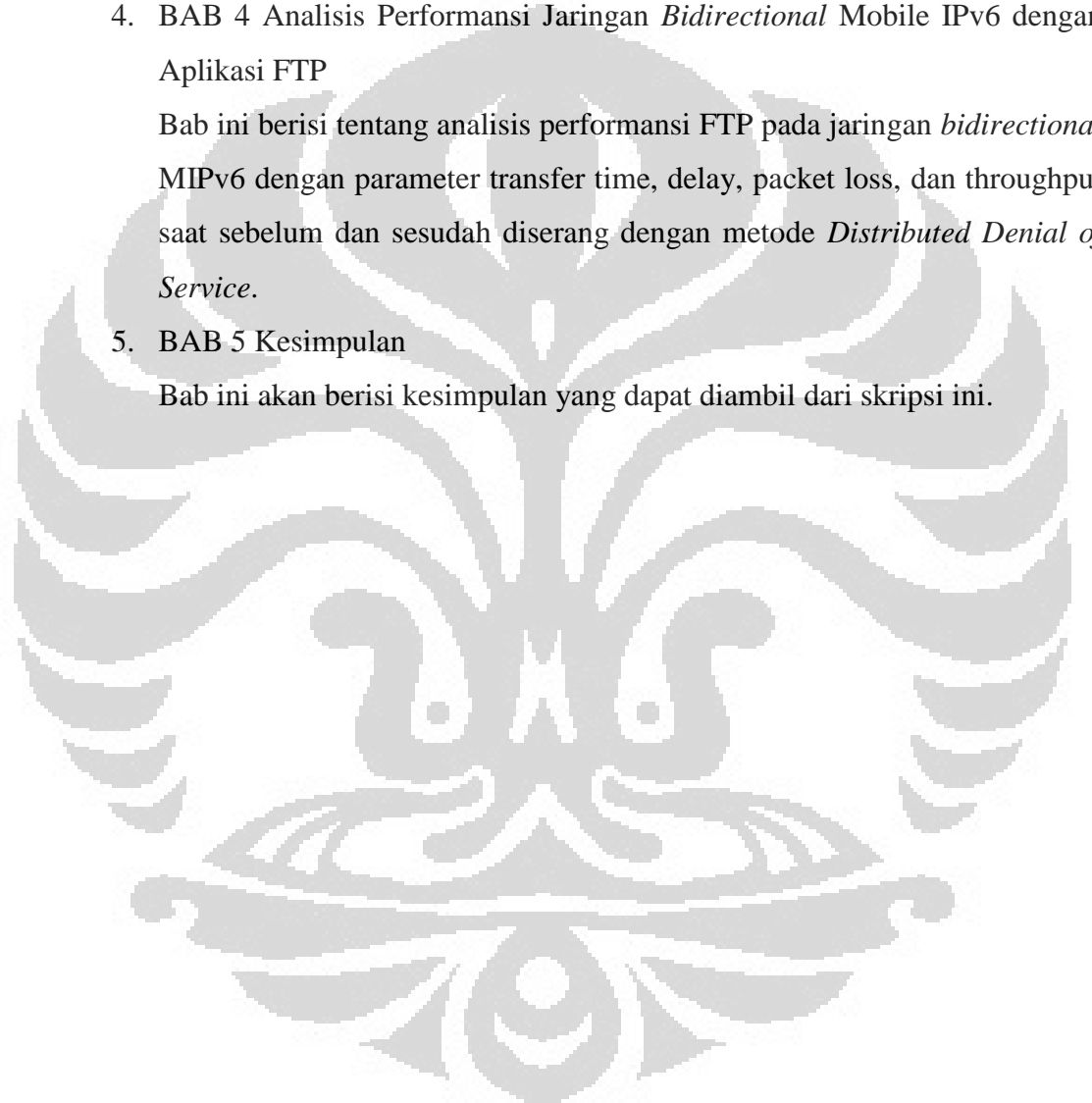
Bab ini berisi tentang model jaringan *bidirectional mobile IPv6* dengan komponen-komponennya, FTP yang diimplementasikan dalam jaringan *mobile IPv6* tersebut serta serangan-serangan yang menjadi skenario dari skripsi ini.

4. BAB 4 Analisis Performansi Jaringan *Bidirectional Mobile IPv6* dengan Aplikasi FTP

Bab ini berisi tentang analisis performansi FTP pada jaringan *bidirectional MIPv6* dengan parameter transfer time, delay, packet loss, dan throughput saat sebelum dan sesudah diserang dengan metode *Distributed Denial of Service*.

5. BAB 5 Kesimpulan

Bab ini akan berisi kesimpulan yang dapat diambil dari skripsi ini.



BAB 2

MOBILE INTERNET PROTOCOL VERSI 6

2.1 IPv6

Seiring dengan meningkatnya kebutuhan akan internet dan keterbatasan jumlah alamat IPv4 maka IETF (*Internet Engineering Task Force*) mulai memikirkan cara menanggulangi masalah akan protokol ini sejak tahun 1990. Kegiatan yang dilakukan IETF ini berkembang ke arah protokol yang dikenal dengan nama IPv6 sampai saat ini. Memperbanyak alamat dan memperluas kemampuan merupakan suatu motivasi dalam pengembangan protokol baru ini. Hal-hal yang menjadi bahan pertimbangan dalam pengembangan IPv6 ini adalah peningkatan *packet handling*, penambahan skalabilitas dan durabilitas berupa penambahan ketersediaan alamat IP dan lama penggunaan alamat IP tersebut di masa mendatang, peningkatan QoS, dan *integrated security*.

IPv6 menyediakan fitur-fitur sebagai berikut.

- a. Besar alamat yang dimiliki adalah 128 bit – fitur ini berguna untuk memperbanyak ketersediaan alamat IP.
- b. Format header yang lebih disederhanakan – fitur ini berguna untuk meningkatkan *packet handling*.
- c. Meningkatkan komponen pendukung untuk ekstensi dan opsi – fitur ini berguna untuk menambah skalabilitas, durabilitas, dan juga memiliki fungsi sama untuk meningkatkan *packet handling*.
- d. Kapabilitas flow labeling – fitur ini berguna sebagai mekanisme QoS.
- e. Kapabilitas authentication dan privacy – fitur ini berguna untuk *integrated security*.

2.1.1 Pengalamatan IPv6

Pengalamatan IPv6 akan lebih rumit dibandingkan dengan IPv4 karena IPv6 berjumlah 128 bit. Selain itu tidak hanya angka yang ditampilkan dalam pengalamatan IPv6 ini, tetapi juga terdapat huruf. Huruf tersebut merupakan representasi dari heksadesimal. Heksadesimal ini menjadi perbedaan pada IPv6 dibandingkan dengan IPv4 yang menggunakan desimal. 128 bit alamat IPv6 tersebut akan dibagi masing-masing menjadi 16 bit heksadesimal dan dipisahkan dengan titik dua (:). Contoh dari alamat IPv6 dalam bentuk biner adalah sebagai berikut.

```
00100000000000010000110110111000111111111111111111111111011101101
10111110111011111111111011101101101111101110111111111111011101101
```

Alamat biner tersebut akan dipisahkan masing-masing 16 bit, sehingga hasilnya adalah sebagai berikut.

```
0010000000000001 0000110110111000 1111111111111111 0000000000000000
1011111011101111 1111111011101101 1011111011101111 1111111011101101
```

Setelah dipisahkan, 16 bit biner tersebut akan dikonversi menjadi heksadesimal dan dipisahkan kembali dengan titik dua (:). Hasilnya adalah sebagai berikut.

```
2001:0db8:ffff:0000:beef:feed:beef:feed
```

Dalam penulisan alamat IPv6 ini, angka nol di awal 4 bit heksadesimal tersebut dapat disederhanakan dengan menghilangkannya. Selain itu apabila 4 bit heksadesimal tersebut terdiri dari 4 angka nol, blok tersebut dapat diisi dengan 1 angka nol. Apabila contoh diatas disederhanakan kembali, maka hasilnya adalah sebagai berikut.

```
2001:db8:ffff:0:beef:feed:beef:feed
```

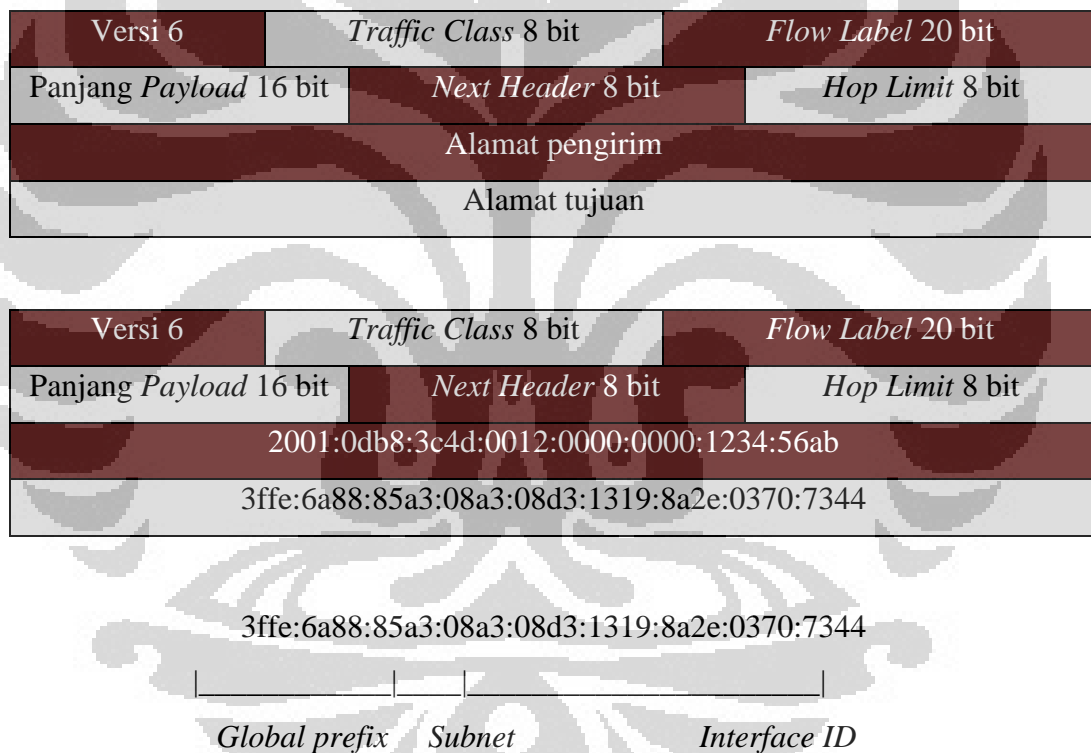
Satu angka nol pada blok 4 bit heksadesimal juga dapat lebih disederhanakan lagi dengan menghilangkan angka nolnya dan dapat diubah dengan menggunakan dua buah tanda titik dua (::). Apabila contoh diatas disederhanakan kembali, maka hasilnya adalah sebagai berikut.

2001:db8:ffff::beef:feed:beef:feed

Selain itu juga apabila blok IPv6 bernilai nol semua dan berapapun jumlah bloknnya yang bernilai nol secara berurutan, maka nol tersebut bisa disedrehanakan hanya dengan dua buah tanda titik dua (::). Contohnya adalah sebagai berikut.

2001:0:0:0:0:0:0:0 menjadi 2001::

Struktur IPv6 terdiri dari tiga bagian besar, yaitu *global prefix*, *subnet*, dan *interface ID*. Alamat yang digunakan ini menggunakan format hexadecimal yang berarti dalam penyusunannya akan terdiri dari 16 bit hexadecimal seperti yang ditunjukkan pada Gambar 2.1 berikut.



Gambar 2.1 Format header IPv6

Berikut ini adalah penjelasan mengenai bagian dari IPv6 paket header sesuai dengan Gambar 2.1.

a. Versi

Bagian ini adalah 4 bit data yang menunjukkan versi dari protocol.

b. *Traffic Class*

Bagian ini adalah 8 bit data yang digunakan oleh *source* dan router untuk mengetahui paket berada pada traffic class yang sama. Setiap paket akan dibedakan berdasarkan prioritas.

c. *Flow Label*

Bagian ini adalah 20 bit data yang digunakan sebagai label untuk menunjukkan aliran data.

d. Panjang *Payload*

Bagian ini adalah 16 bit data yang menunjukkan panjang dari paket data.

e. *Next Header*

Bagian ini adalah 8 bit data yang menunjukkan jenis header.

f. *Hop Limit*

Bagian ini adalah 8 bit data yang menunjukkan jumlah hop untuk masing-masing node untuk meneruskan paket. *Hop limit* ini akan terus berkurang satu tiap melewati node dan jika bernilai nol setelah berkurang maka paket dibuang.

g. Alamat pengirim

Bagian ini adalah 128 bit data yang menunjukkan alamat *source* dari paket.

h. Alamat tujuan

Bagian ini adalah 128 bit data yang menunjukkan alamat tujuan dari paket.

IPv6 memiliki enam tipe alamat yang berbeda, yaitu *Unicast*, *Global Unicast address*, *Link-local address*, *unique local address*, *Multicast*, dan *Anycast*. Penjelasan masing-masingnya adalah sebagai berikut.

a. *Unicast*

Paket dari satu alamat sumber akan dikirimkan dan diterima hanya oleh satu interface. Hal ini berarti komunikasi dilakukan dengan point-to-point.

b. *Global Unicast address*

Global Unicast address merupakan metode *unicast* yang dapat memberikan komunikasi antar komputer secara luas dalam internet dengan basis IPv6.

c. *Link-local address*

Alamat ini sama seperti alamat private pada IPv4 yang berarti komunikasi dilakukan pada jaringan lokal yang berbasis IPv6 dalam satu subnet.

d. *Unique local address*

Alamat ini bukan merupakan alamat untuk di routing namun alamat ini bersifat unik dan tidak *overlap*. Alamat ini mengizinkan komunikasi melalui site ke *multiple local network*.

e. *Multicast*

Alamat ini mengizinkan paket yang dikirimkan dari alamat IPv6 sumber ke banyak tujuan.

f. *Anycast*

Alamat ini mirip dengan multicast namun perbedaan yang menonjol adalah pada paketnya yang hanya akan dikirimkan ke satu alamat tujuan. *Anycast* ini bertujuan untuk mengirimkan paket ke alamat tujuan yang terdekat dari suatu kelompok atau dengan kata lain alamat ini mendukung komunikasi *one-to-one of many*.

Berikut ini adalah pembagian rentang alamat special dalam IPv6 yang sudah ditetapkan secara global.

- 0:0:0:0:0:0:0:0

Alamat ini sama dengan :: dan 0.0.0.0 pada IPv4. Alamat ini juga merupakan alamat sumber dari suatu *host* ketika menggunakan konfigurasi *stateful*.

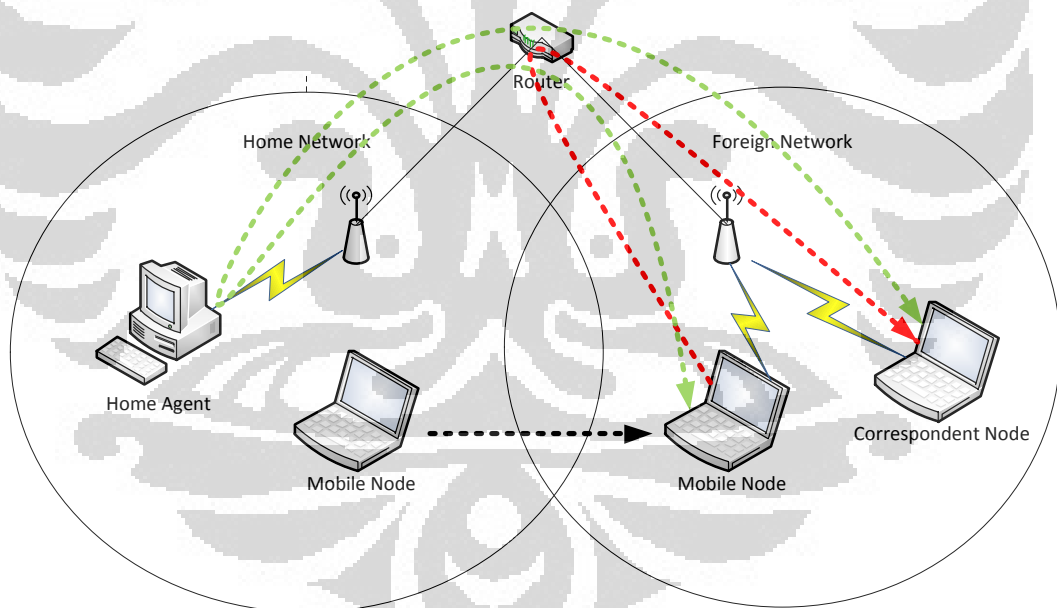
- 0:0:0:0:0:0:0:1
Alamat ini sama dengan ::1 dan juga 127.0.0.1 pada IPv4. Alamat ini merupakan alamat *local host*.
- 0:0:0:0:0:192.168.5.122
Bentuk alamat ini merupakan bentuk pencampuran IPv4 dengan IPv6.
- 2000::/3
Alamat ini merupakan rentang alamat yang ditetapkan sebagai *global unicast address*.
- FC00::/7
Alamat ini merupakan rentang alamat yang ditetapkan sebagai *unique local unicast address*.
- FE80::/10
Alamat ini merupakan rentang alamat yang ditetapkan sebagai *link-local unicast address*.
- FF00::/8
Alamat ini merupakan rentang alamat yang ditetapkan sebagai *multicast address*.
- 3FFF:FFFF::/32
Alamat ini merupakan rentang alamat yang ditetapkan dengan tujuan untuk contoh atau dokumentasi.
- 2001:0DB8::/32
Alamat ini juga merupakan rentang alamat yang ditetapkan dengan tujuan untuk contoh atau dokumentasi.
- 2002::/16
Alamat ini digunakan untuk system transisi 6to4. Struktur ini berguna untuk mentransmisikan paket IPv6 melalui jaringan IPv4 tanpa harus mengkonfigurasi *explicit tunnel*.

IPv6 dapat dikonfigurasi secara otomatis maupun manual. Untuk konfigurasi otomatis terdapat dua cara, yaitu *stateless* dan *statefull*. Pada

konfigurasi otomatis *statefull* jarak antar IP yang diberikan pada host ditentukan oleh sebuah server sedangkan *stateless* tidak membutuhkan server namun perlu mengkonfigurasinya router untuk pembagiannya.

2.2 Mobile IPv6

Mobile IPv6 merupakan komunikasi suatu perangkat baik perangkat *mobile* maupun perangkat komputer dari suatu node yang memungkinkan untuk terhubung dari satu jaringan (*Home Network*) ke jaringan lainnya (*Foreign Network*) dengan mempertahankan alamat IP yang sama. Perangkat yang terhubung dari jaringan satu ke jaringan lainnya akan terhubung secara otomatis. *Mobile IPv6* juga merupakan protokol yang berisi set pesan-pesan dan proses-proses dalam penetapan hubungan antar node yang berdekatan. Protokol yang dimaksud adalah *Neighbor Discovery*. *Neighbor Discovery* ini menggantikan menambahkan beberapa fungsi dari ARP, ICMP *Router Discovery*, dan ICMP *redirect* pada IPv4. Gambar 2.2 berikut ini merupakan contoh dari *mobile IP*.



Gambar 2.2 Mobile IP

Beberapa proses yang dijalankan oleh *Neighbor Discovery* adalah sebagai berikut.

a. *Router Discovery*

Proses ini merupakan proses host dalam mencari router-router pada sebuah sambungan.

b. *Prefix Discovery*

Proses ini merupakan proses host dalam mencari prefix-prefix jaringan pada sambungan lokal yang dituju.

c. *Parameter Discovery*

Proses ini merupakan proses host dalam mencari parameter operasi tambahan. Dalam parameter tersebut juga terdapat MTU dan hop limit default untuk paket yang keluar.

d. *Address autoconfiguration*

Proses ini merupakan proses pengalamatan IP pada interface secara otomatis.

e. *Neighbor Unreachable detection*

Proses ini merupakan proses node dalam mendeteksi layer IPv6 dari node tetangga tidak lagi menerima paket-paket.

f. *Duplicate Address Detection*

Proses ini merupakan proses node dalam mendeteksi alamat yang digunakan belum pernah atau sedang digunakan oleh node lainnya.

Terdapat beberapa komponen penting yang mendukung proses *mobile* IPv6, yaitu.

a. *Home Address*

Komponen ini merupakan alamat yang diberikan kepada perangkat *mobile* pada saat node berada pada *Home Network* dan *Foreign Network*.

b. *Home Agent (HA)*

Komponen ini merupakan suatu perangkat router atau komputer yang berada pada *Home Network*. Komponen ini berfungsi untuk menjaga registrasi dan alamat *Mobile Node* pada saat keluar dari *Home Link*. Hal ini bertujuan agar paket-paket yang dikirimkan ke

Home Address dari *Mobile Node* tersebut dapat diarahkan ke alamat *Mobile Node* yang digunakan pada saat berada diluar *Home Link*.

c. *Home Network* (HN)

Komponen ini merupakan jaringan yang memberikan prefix *home subnet* pada perangkat *mobile*.

d. *Foreign agent* (FA)

Komponen ini merupakan perangkat router yang berfungsi untuk menyimpan informasi *Mobile Node* yang melewati jaringannya. Dalam informasi tersebut juga terdapat informasi *care of address*.

e. *Foreign network* (FN)

Komponen ini merupakan jaringan dimana *Mobile Node* berada diluar *Home Network*.

f. *Mobile Node* (MN)

Komponen ini merupakan suatu titik perangkat dengan IPv6 yang dapat berpindah koneksi. Komponen berfungsi untuk mengetahui informasi lokasi dari *home address* atau alamat dari *home address* yang sedang digunakan saat ini dan node IPv6 yang lain yang sedang terhubung dengan MN.

g. *Care of address* (CoA)

Komponen ini merupakan alamat yang dipakai ketika perangkat *mobile* terhubung dengan *Foreign Network*. CoA juga merupakan perpaduan dari *prefix foreign subnet* dan *interface ID* yang ditentukan oleh *Mobile Node*. MN dapat memiliki banyak CoA, tetapi hanya satu saja CoA yang terdaftar sebagai CoA utama dengan home agent. MN akan mengirimkan binding update yang berisi CoA yang baru ke *Home Agent* agar *Home Agent* dapat menghubungkan MN antara *home address*-nya dengan CoA-nya.

h. Correspondent node

Komponen ini merupakan suatu titik dimana MN yang dapat saling berkomunikasi pada saat berada pada *Home Network* dan *Foreign Network*. CN ini dapat dikatakan sebagai *Mobile Node* dan juga sebagai node biasa.

i. Agent advertisement

Komponen ini merupakan informasi dari *Mobile Node* agar dapat terhubung dengan *Home Agent*.

Terdapat beberapa layanan pendukung *mobile IPv6*. Layanan tersebut adalah sebagai berikut.

a. *Agent Solicitation*

Merupakan layanan yang diminta dari *Home Agent*, *Foreign Agent*, dan *Access Point* oleh *Mobile Node* yang terdiri dari permintaan link untuk mengetahui apakah ada paket yang hilang namun masih memiliki CoA yang berlaku.

b. *Registration*

Merupakan layanan pendaftaran CoA bagi mobile node ketika menjauhi *Home Agent*, sehingga *Home Agent* mengetahui keberadaan *Mobile Node* dan meneruskan paket data.

c. *Encapsulation*

Merupakan layanan penumpangan IP datagram mobile node dengan header IP lain yang terdiri dari CoA. IP datagram tersebut tidak akan hilang dan tidak terproses seluruhnya ketika penumpangan.

d. *Decapsulation*

Merupakan layanan pemisah header IP pada paket *incoming*, sehingga datagram yang ditumpangi dapat diakses dan dikirimkan ke tujuan.

Mobile IPv6 ini bekerja dengan kemungkinan memiliki dua alamat IP pada *Mobile Node*. IP pada home addressnya merupakan alamat IP tetap dalam *mobile IPv6* ini. Sedangkan IP CoA merupakan alamat bersifat sementara pada saat *Mobile Node* berada pada luar *Home Address*. *Home Agent* bertugas dalam penyimpanan informasi tetap tentang *Mobile Node*. Sedangkan *Foreign Agent* bertugas dalam penginformasian alamat sementara dan menyimpan informasi tentang node jaringan seluler yang mengunjunginya.

Home Network bertugas untuk terus menyampaikan paket yang dikirimkan ke *Home Agent* dengan menggunakan routing IP. Paket selalu dialihkan oleh

Home Agent dengan mengambil IP CoA dari *table look-up*. Lalu *Home Agent* bertugas untuk menambahkan header IP yang baru pada pake IP yang asli. *Mobile IP* ini tidak perlu diatur secara *manual* oleh pengguna secara terus menerus untuk mempertahankan koneksinya.

Terdapat dua metode agar *Mobile Node* dapat menerima dan mengirim data ke *Correspondent Node* pada saat *Mobile Node* tidak berada pada *Home Network*, yaitu *bidirectional tunneling* dan *route optimization*.

Mobile IP juga memiliki kelebihan dan kekurangan. Kelebihan *mobile IP* adalah sebagai berikut.

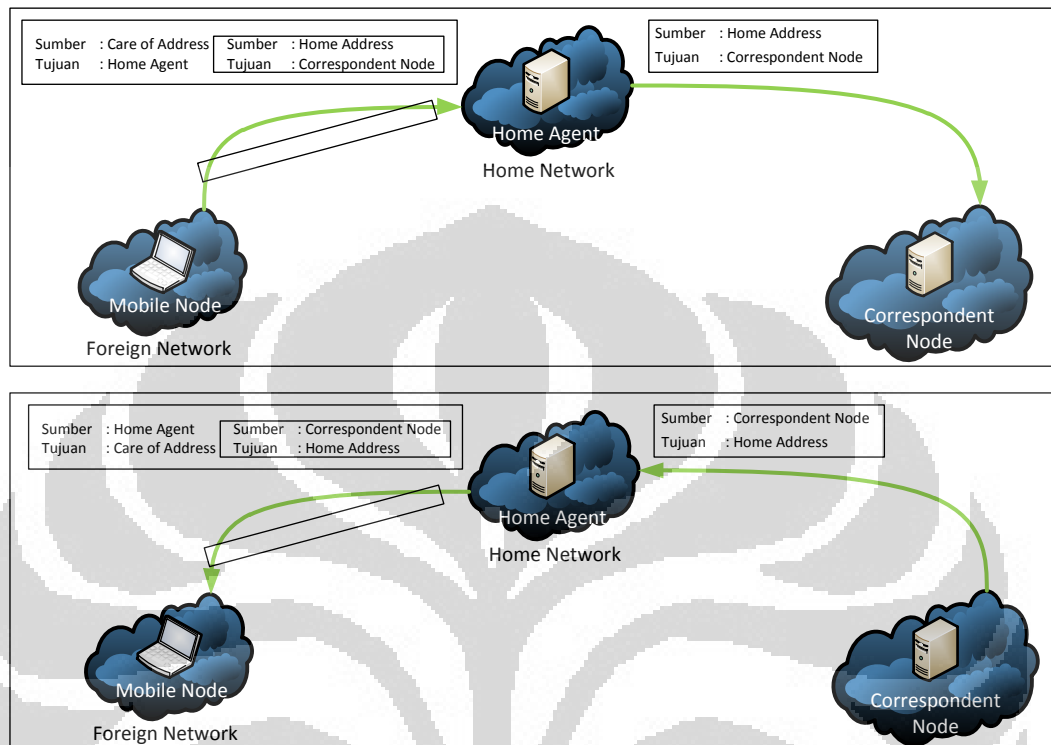
- a. Memberikan kemudahan dalam penggunaan perangkat *mobile* dimana saja.
- b. Memberikan kemudahan pada pengguna perangkat *mobile* untuk terhubung ke internet tanpa memerlukan IP yang statis melainkan IP dinamis.
- c. Memberikan kemudahan untuk mengakses internet pada tempat yang jauh selama tetap menggunakan router setup maupun modem.

Kekurangan *mobile IP* adalah menjadi kurang efektif pada saat ketersediaan internet kurang merata untuk setiap wilayah. Hal ini berpengaruh besar jika pengguna perangkat *mobile* dari kota besar yang ketersediaan internetnya jauh lebih besar berpindah dan tetap ingin terhubung ke internet di kota kecil yang ketersediaan internetnya terbatas.

2.2.1 Bidirectional Mobile IPv6

Bidirectional merupakan salah satu metode untuk menyalurkan paket IPv6 pada *mobile IP* dari CN ke MN. Tunnel ini digunakan pada saat CN tidak memiliki binding untuk *Mobile Node* atau CN tidak mendukung *mobile IPv6*. Hal ini memungkinkan MN untuk tetap terhubung meskipun tidak berada di *Home Network* dan CN tidak dapat memadai untuk *mobile IPv6*. Pada saat pengiriman paket, contohnya dari CN ke MN, alamat pada header paket akan diset sebagai alamat home dari MN dan diarahkan dengan menggunakan metode routing IPv6. Kemudian paket tersebut akan di-intercept dan ditunnel dari HA ke MN. Begitu

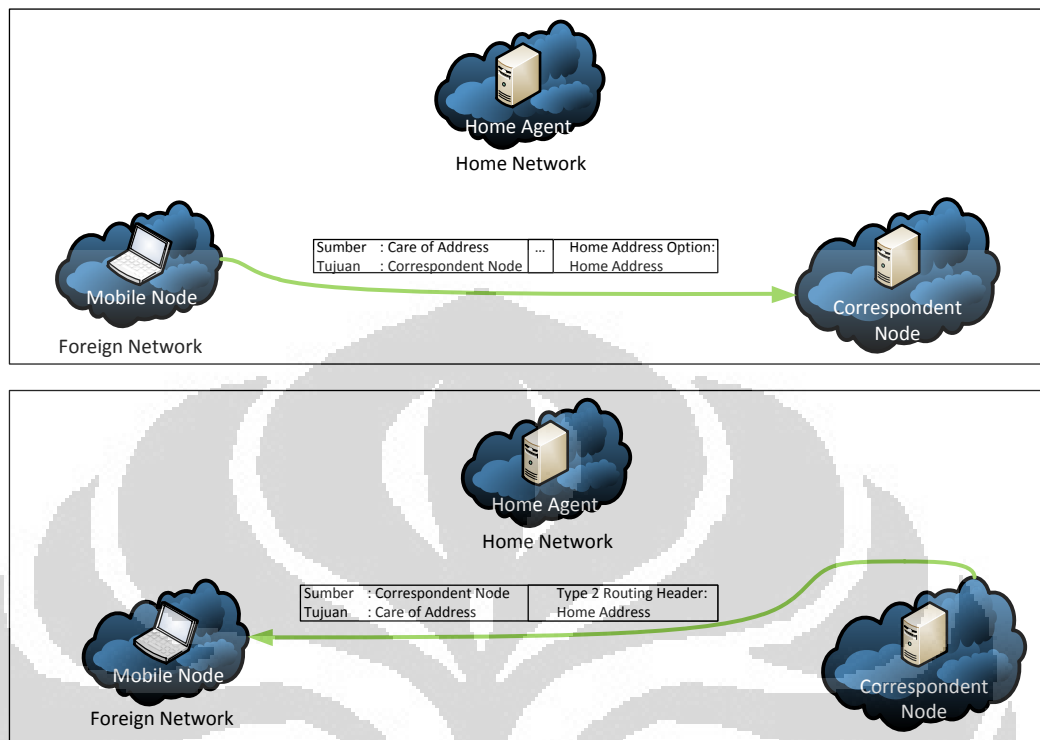
juga sebaliknya jika MN yang ingin mengirimkan paket ke CN pasti melalui HA, seperti yang ditunjukkan pada Gambar 2.3.



Gambar 2.3 Bidirectional tunneling

Proses yang dilakukan pada *bidirectional* ini yang pertama adalah MN akan terhubung ke jaringan *foreign* (FN) dan ingin mendapatkan CoA. Proses selanjutnya MN akan mengirimkan binding update ke HA dan HA akan menggunakan pencarian proxy dari tetangganya dengan proxy ARP untuk menghadirkan ulang MN di home networknya. Paket atau traffic yang selalu ditujukan ke MN akan dienkapsulasi dalam tunnel IPv6-to-IPv6 dan nantinya akan dikirimkan ke CoA dari MN. Tunnel mode ini sangat tidak optimal apabila MN berada jauh dari HN karena semua traffic harus melalui HA. Dalam hal ini peran paket handling tambahan diperlukan pada HA dan MN dalam menunjang traffic tersebut.

2.2.2 Route Optimization Mobile IPv6

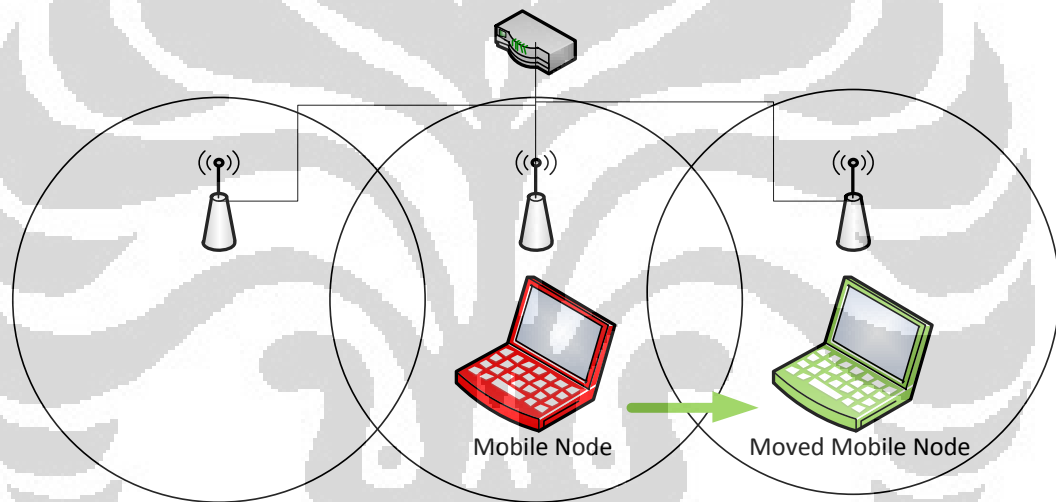


Gambar 2.4 *Route optimization tunneling*

Route optimization juga merupakan salah satu metode untuk menyalurkan paket IPv6 pada *mobile IP* dari CN ke MN. *Route optimization* ini membutuhkan dukungan dari MN dalam registrasi binding update terhadap CN. Pada saat MN berpindah ke jaringan lain dan registrasi CN sudah selesai maka paket-paket antar MN dan CN dapat terhubung langsung tanpa harus melalui HA seperti yang terlihat pada Gambar 2.4 diatas. Ketika terjadi pengiriman paket ke beberapa tujuan tertentu, CN akan mengoreksi binding yang tertahan yang kemudian akan dimasukkan ke dalam alamat paket tujuan. Apabila binding yang tertahan tersebut terdeteksi, node akan menggunakan ripe dari header routing IPv6 yang baru untuk mengarahkan paket ke MN. Pengarahan tersebut dilakukan dengan cara CoA menandai binding tersebut. Dengan adanya paket yang dirouting ini maka CoA mengizinkan untuk melakukan komunikasi terpendek. Hal ini mengakibatkan congestion pada HA dan home link pada MN akan hilang. Selain itu juga *route optimization* ini dapat mengurangi potensi gagalnya paket yang diteruskan dari HA.

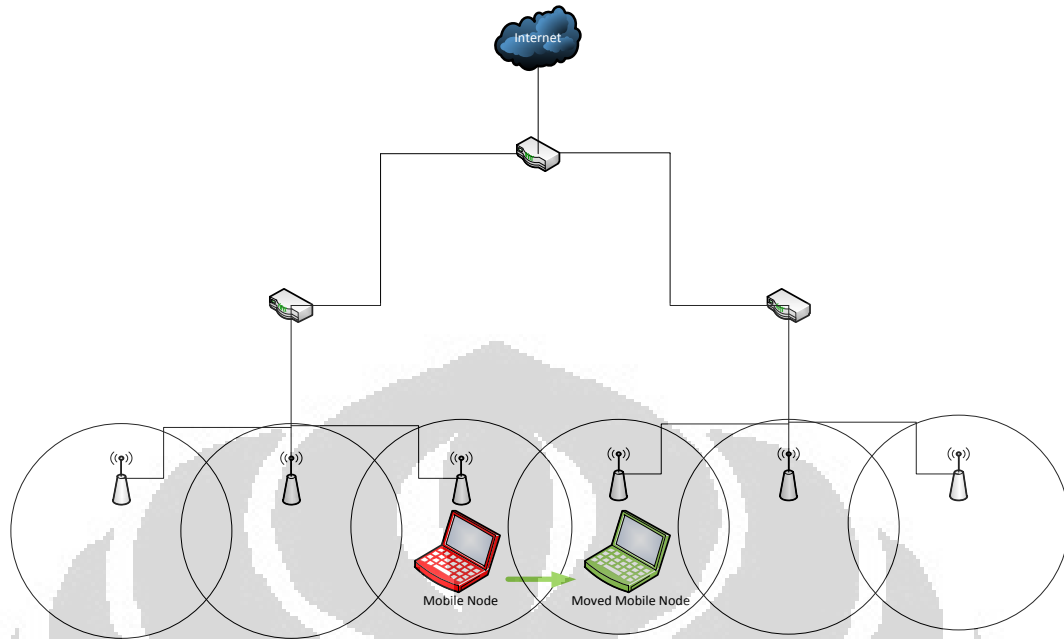
2.2.3 Handover Mobile IPv6

Handover merupakan proses yang dilakukan pada MN ketika berpindah dari suatu jaringan nirkabel ke jaringan nirkabel lainnya. *Handover* ini terdiri dari dua bagian besar, yaitu *horizontal handover* dan *vertical handover*. *Horizontal handover* merupakan handover yang dilakukan pada jaringan yang sama. Dengan kata lain handover ini terjadi perubahan pada layer data link saja dan tidak mengubah alamat IP. *Handover* ini dilakukan ketika MN berpindah ke AP WLAN lain yang masih berada pada IP *access router* yang sama. Dalam hal ini AP WLAN sebelum dan sesudah berpindahnya MN berada pada *Extended Service Set (ESS)* yang sama. *Horizontal Handover* ini dapat dilihat pada Gambar 2.5 berikut ini.

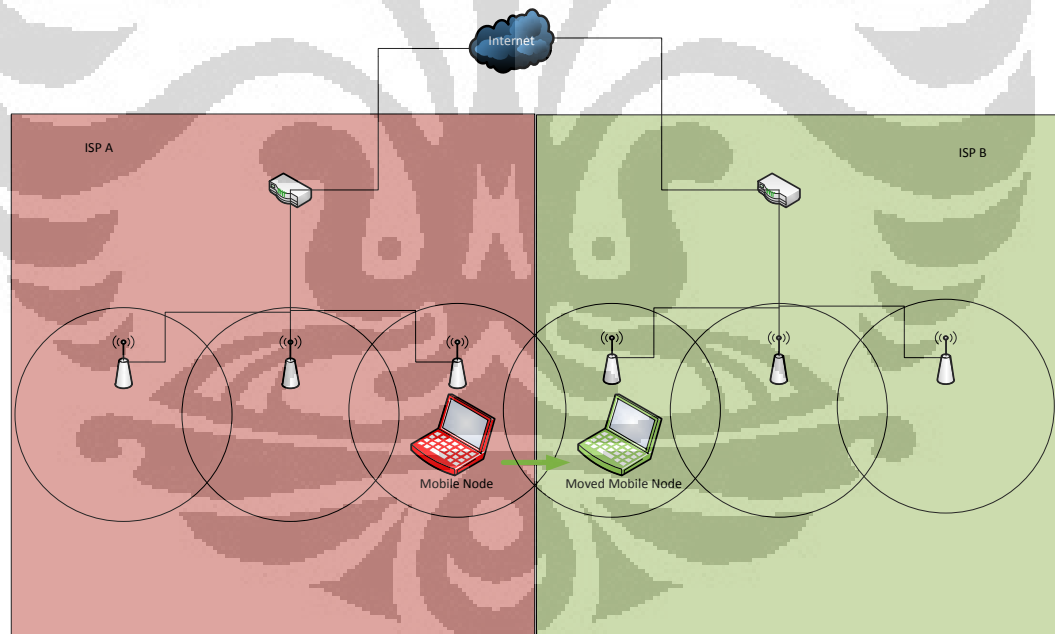


Gambar 2.5 Horizontal Handover

Sedangkan *vertical handover* merupakan *handover* yang terjadi saat MN berpindah access point yang berbeda ESS. Proses handover ini dapat terjadi pada ISP yang sama maupun yang berbeda. Vertical handover pada ISP yang sama dapat dilihat pada Gambar 2.6, sedangkan *vertical handover* pada ISP yang berbeda dapat dilihat pada Gambar 2.7 berikut ini.



Gambar 2.6 Vertical handover dengan ISP yang sama



Gambar 2.7 Vertical handover dengan ISP yang berbeda

Terdapat beberapa syarat untuk melakukan *handover* pada *mobile IPv6*. Syarat yang dibutuhkan pada handover ini hampir sama dengan *autoconfiguration*

pada saat IPv6 melakukan booting ke suatu jaringan. Perbedaan dari keduanya adalah sebagai berikut.

- MN dapat mendeteksi bahwa MN sudah berpindah ke suatu jaringan lain.
- Pada saat proses berjalan, MN harus mengirimkan informasi kepada HA dan CN yang berisi informasi lokasi barunya.
- *Handover* harus dilakukan dengan cepat agar dapat mengurangi potensi *packet loss* dan *packet delay*.

Syarat atau prosedur yang harus dipenuhi pada *mobile* IPv6 adalah sebagai berikut.

1. Deteksi perpindahan

MN diharuskan untuk dapat mendeteksi tentang keberadaan dirinya pada jaringan tertentu, apakah MN masih berada di *Home Network* atau sudah berpindah ke *Foreign Network*. Yang harus dilakukan MN adalah melakukan *Neighbor Unreachability Detection* (NUD) secara sekuensial dengan tujuan untuk mengetahui apakah *Current Access Router* (CAR) masih terjangkau dalam dua arah atau tidak. Jika CAR tersebut tidak dapat dijangkau maka MN harus mengirimkan *router solicitation* untuk menemukan router yang baru.

2. *Router Discovery*

Pada proses ini, MN akan menerima *router advertisement* dari NAR atau *New Access Router*. MN juga akan terus mengirimkan *router solicitation* jika CAR masih tidak terjangkau dan akan menerima *solicited advertisement* dari NAR yang dikirimkan secara sekuensial.

3. Konfigurasi CoA

MN harus mengkonfigurasi dirinya dengan alamat IPv6 yang baru sesuai dengan jaringan yang baru dikunjunginya. Konfigurasi alamat IPv6 tersebut dapat dilakukan dengan dua cara, yaitu.

a. *Stateless auto-configuration address*

Konfigurasi ini mengizinkan MN untuk melakukan konfigurasi alamat IP secara otomatis dengan menggabungkan prefix NAR dengan alamat MAC NIC.

b. Stateful configuration

Konfigurasi ini menggunakan prinsip kerja DHCPv6 agar dapat mengintrik dan mendokumentasikan penggunaan alamat IPv6.

4. *Duplicate Address Detection*

Setelah MN berpindah ke jaringan yang baru maka MN harus melakukan DAD untuk CoA yang didapatkan dari konfigurasi *stateless* dan *stateful*. Proses ini dilakukan dengan tujuan agar tidak terjadi duplikasi alamat IPv6 pada jaringan tersebut. Jika terdapat node yang memiliki alamat yang sama seperti CoA maka akan terjadi hal seperti berikut.

- Node yang memiliki alamat yang sama tersebut akan mendapatkan pesan *neighbor solicitation* dan akan merespon dengan *neighbor advertisement*. Selain itu juga node tersebut akan memberitahukan alamatnya kepada MN.
- MN yang sebenarnya akan menerima *neighbor solicitation* juga dari node yang alamat IP-nya sama tersebut yang juga melakukan proses DAD.

Proses DAD ini akan memberikan informasi kepada MN bahwa terdapat node lain yang menggunakan alamat yang sama dengan CoA sehingga salah satu dari mereka harus mengganti alamat IP-nya. Kemungkinan terjadinya duplikasi alamat IP ini dapat dikurangi apabila menggunakan konfigurasi *stateless*. Hal ini dikarenakan karena *stateless* yang menggabungkan antara prefix jaringan dengan alamat MAC yang bersifat unik.

5. Otentikasi dan Otorisasi

MN yang berpindah ke jaringan lain juga harus melakukan proses AAA atau *Authentication And Authorization* agar dapat mengakses ke jaringan yang baru tersebut. Proses ini membutuhkan interaksi

secara dua arah atau handshake di antara MN, server lokal, dan home server MN.

6. Registrasi CoA

Pada saat MN menerima CoA dan diizinkan untuk dapat mengakses jaringan tersebut, MN akan mengirimkan informasi kepada HA tentang lokasi yang baru. Selama koneksi MN terputus dengan jaringan sebelumnya atau terputus dengan *Previous Router Access* (PAR) hingga MN mengirimkan informasi mengenai lokasi barunya kepada HA, maka semua paket yang dikirimkan MN akan hilang dan MN juga tidak dapat mengirimkan paket ke CN manapun. Untuk itu MN harus mendaftarkan CoA-nya kepada HA dengan mengirimkan *Binding Update*. Kemudian HA akan merespon dengan mengirimkan binding acknowledgement. Setelah proses ini berjalan maka HA dapat men-tunnel paket yang ditujukan ke home address MN ke lokasi barunya.

7. *Binding Update*

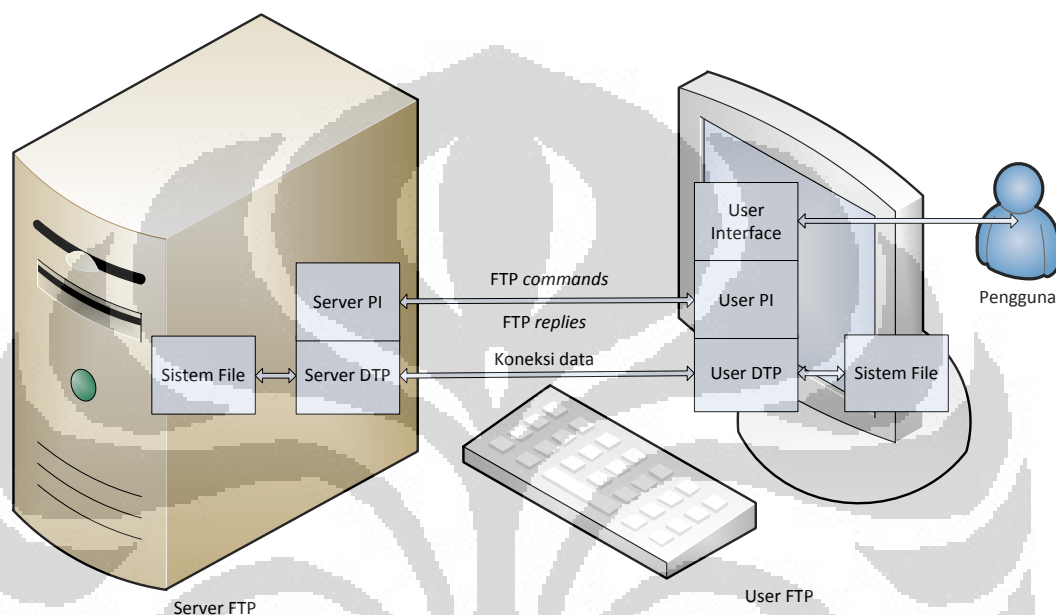
MN harus mengirimkan informasi ke semua CN mengenai lokasi barunya dan juga mengenai keterjangkauannya melalui CoA yang baru tersebut. Hal ini dilakukan dengan cara mengirimkan *Binding Update* ke semua CN.

2.3 *File Transfer Protocol*

File Transfer Protocol merupakan kepanjangan dari FTP. FTP ini merupakan suatu protokol yang berfungsi untuk tukar menukar data atau file antar dua host pada TCP/IP. FTP ini bukan hanya sebagai protokol tetapi juga sebagai program. Pada saat FTP sebagai protokol maka FTP ini digunakan oleh suatu aplikasi, sedangkan pada saat FTP sebagai program maka FTP ini dijalankan oleh pengguna secara manual untuk mengoperasikan tugas-tugas filenya. Transfer file dapat disediakan oleh protokol ini melalui FTP server yang telah dilog oleh kita secara langsung atau telnet. FTP ini juga menggunakan protokol telnet dalam mengatur sambungannya.

FTP menggunakan port 20 atau 21 dalam port TCP yang memiliki fungsi penunjang. Port 21 berfungsi sebagai port control yang mengizinkan koneksi

antara klien dan server, mengizinkan perintah FTP yang dikirimkan dari klien untuk sampai ke server, dan mengizinkan dalam pengiriman respon perintah FTP tersebut dari server. Port 20 berfungsi untuk membentuk koneksi antara klien dan server dalam transfer data saat pengunduhan dan penggugahan.



Gambar 2.8 Model dari FTP

Gambar 2.8 menjelaskan mengenai protokol user yang sedang menafsirkan kontrol koneksi yang diikuti dengan protokol telnet. Dalam penafsirannya tersebut, perintah FTP diterjemahkan oleh user-PI dan kemudian dikirimkan ke server melalui control koneksi untuk diproses lebih lanjut. User juga dapat melakukan control koneksi dengan FTP server secara langsung dari TAC terminal, kemudian menerjemahkan perintah FTP tersebut melalui proses yang dilakukan klien FTP. Informasi berupa perintah standar FTP direspon oleh server dikirim ke user-PI melalui control koneksi.

Perintah FTP terdiri dari beberapa komponen untuk koneksi data, seperti port data, mode transfer, tipe representasi, dan struktur dan juga perintah untuk operasi dasar system file, seperti penyimpanan, penghapusan, dan lain sebagainya.

User-DTP bertugas untuk hanya mendengarkan port data tertentu, kemudian server mulai membuat data koneksi dan transfer data sesuai dengan parameter tertentu yang sudah ditentukan. Dalam hal ini port data tidak perlu untuk diperhatikan.

FTP memiliki dua jenis mode dalam membuat koneksi, yaitu mode aktif dan mode pasif. Penjelasan keduanya adalah sebagai berikut.

a. Mode aktif

Kerja mode ini diawali dengan mengatur server FTP agar dapat memiliki sambungan dengan klien. Server akan menunggu port dinamis yang dibuka oleh klien, kemudian klien akan mengirimkan perintah PORT tersebut. Perintah tersebut berisi port number dinamis dari klien yang berisi control steam. Kemudian klien akan menunggu balasan dari server. Server akan merespon kemudian akan membuat koneksi data pada port sumber sesuai perintah dari klien ke port 20 milik server.

Untuk melakukan modus aktif ini terdapat beberapa port yang harus dibuka sesuai dengan firewall server side. Port tersebut adalah sebagai berikut.

- Port 21 pada server FTP dari mana pun yang terjadi pada saat klien meminta koneksi.
- Port 21 pada server FTP ke port 1023 yang terjadi pada saat server merespon port control klien.
- Port 20 pada server FTP ke port 1023 yang terjadi saat server mulai membuat koneksi data dengan port data milik klien.
- Port 20 pada server FTP ke port 1023 yang terjadi ketika klien mengirimkan data atau file ke port data milik server.

b. Mode pasif

Kerja mode ini tidak diawali dengan server FTP yang menunggu klien FTP untuk mengirimkan informasi mengenai port transfer data, melainkan server mengirimkan perintah PASV dan alamat IP server ke klien. Perintah PASV dan

alamat IP dari server ini bertujuan untuk membuat koneksi dengan port dinamis sumber milik klien dan juga efektif untuk klien yang berada di balik firewall. Dari segi keamanan, mode PASV biasanya dinon-aktifkan pada server FTP oleh admin.

Mode pasif ini juga membutuhkan port yang harus dibuka untuk menunjang prosesnya. Port tersebut sesuai dengan firewall server side adalah sebagai berikut.

- Port 21 pada server FTP dari mana pun yang terjadi pada saat klien mulai membuat koneksi.
- Port 21 pada server FTP ke port 1023 yang terjadi pada saat server merespon port control klien.
- Port 1023 pada server FTP yang terjadi saat server mulai membuat koneksi data dengan port data yang ditentukan secara acak milik klien.
- Port 1023 pada server FTP yang terjadi ketika server mengirimkan data atau file ke port data milik klien.

Pada dasarnya, FTP dalam melakukan pengiriman data bersifat clear text yang tidak dienkripsi terlebih dahulu. Hal ini menyebabkan FTP kurang aman karena data dapat di-sniffing dengan protocol analyzer sehingga username, password, data yang sedang dikirimkan, dan perintah-perintah yang dikirimkan dapat terlihat jelas. Oleh karena itu FTP dikembangkan agar dienkripsi terlebih dahulu, seperti SFTP yang berbasis SSH atau FTPS yang melalui SSL.

Parameter-parameter yang digunakan dalam pengukuran QoS dari FTP ini adalah sebagai berikut.

a. **Transfer time**

Transfer time merupakan parameter yang menunjukkan waktu keseluruhan yang dibutuhkan oleh file dari FTP server ke FTP client atau sebaliknya. Perhitungan transfer time dimulai ketika FTP client me-request ke FTP server hingga pengiriman file selesai. Transfer time ini dipengaruhi oleh throughput pada

jaringan. Semakin besar throughput maka akan semakin kecil transfer time-nya.

b. Delay

Delay merupakan parameter yang menunjukkan waktu yang dibutuhkan ketika paket dikirimkan hingga paket sampai ke tujuan. Delay ini dapat dihitung dengan cara membagi transfer time dengan jumlah paket dalam file tersebut.

c. Packet Loss

Packet loss merupakan parameter yang menunjukkan paket-paket yang hilang atau tidak sampai ke tujuan.

d. Throughput

Throughput merupakan parameter yang menunjukkan besarnya atau banyaknya paket data yang dapat diterima setiap detiknya. Pada skripsi ini satuan throughput yang digunakan adalah MBps.

2.4 Keamanan Jaringan pada *Mobile IP*

Sistem yang sudah berbasis *mobile* akan rentan terhadap gangguan baik dalam bentuk serangan, pencurian data rahasia, dan lain sebagainya. Untuk itu keamanan jaringan pada *mobile IP* menjadi komponen penting yang harus diperhatikan. Serangan sering terjadi pada layer network dan juga data link. Jenis serangan yang dilakukan pada bahasan skripsi ini adalah dengan menggunakan metode *Denial of Service (DoS)*.

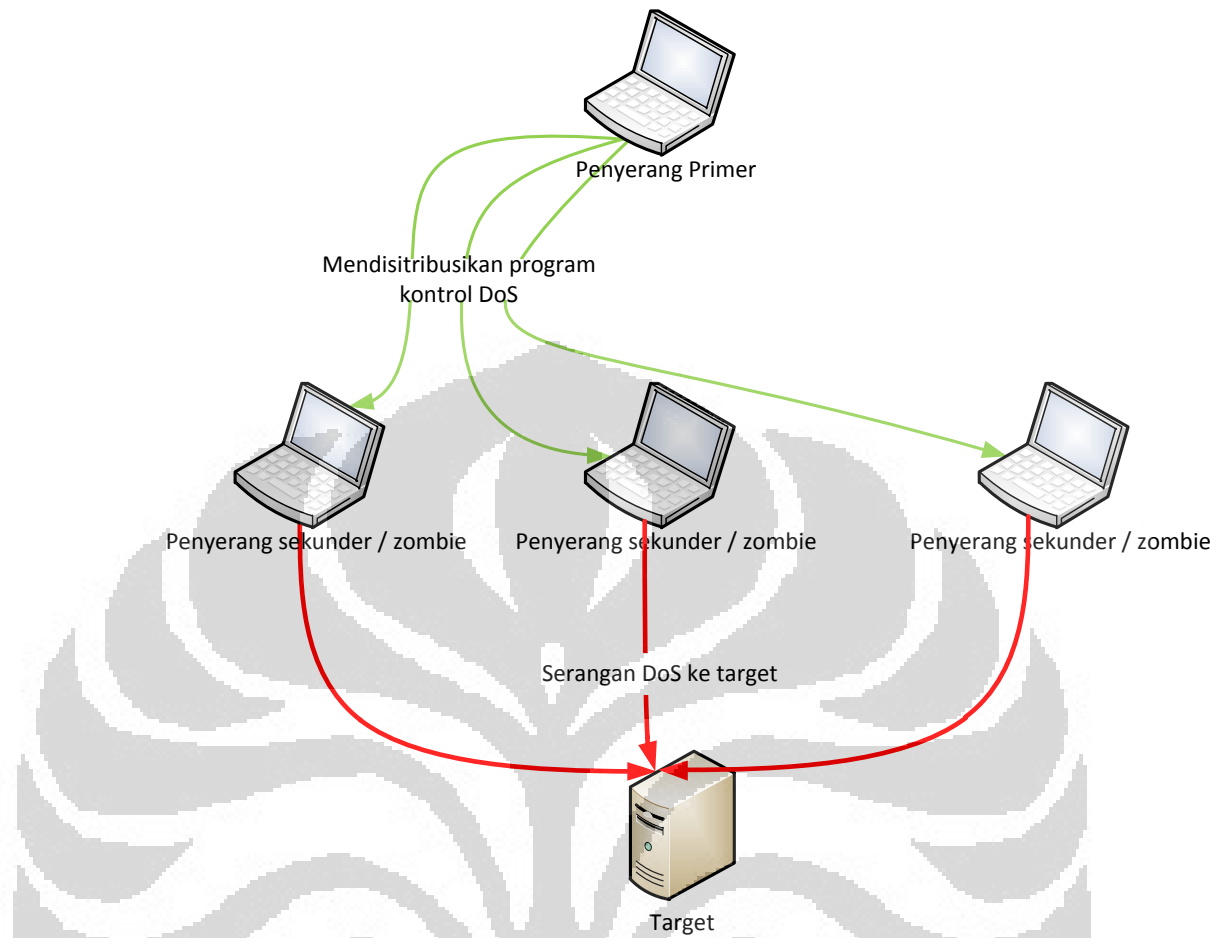
DoS merupakan serangan yang digunakan untuk menguasai sumber dari suatu jaringan. Akibat yang ditimbulkan dari serangan ini adalah pihak yang diserang tidak dapat mengakses jaringan yang diinginkan. Dibutuhkan suatu access point pada rancangan ini untuk dijadikan sebagai jembatan lalu lintas jaringan, sehingga pihak yang berhak atas jaringan dapat melakukan otentikasi dan mengakses jaringan. Dalam hal ini penyerang dapat mengirim suatu frame ke access point tersebut. Serangan pada *access point* dilakukan dengan mem-*flooding* dengan paket data untuk menginterupsi jaringan dari pihak yang sah tersebut.

Penyerang juga dapat mengirimkan *spoofed binding update* sehingga dapat menaikkan traffic yang tidak diinginkan pada jaringan tersebut. Pertama kali penyerang biasanya mencari situs yang memiliki data stream yang berat dan kemudian menghubungkan ke jaringan tersebut. Lalu penyerang dapat mengirim BU ke CN dan mengatakan untuk mengalihkan arbitrary node lokasi baru penyerang. Arbitrary node ini kemudian akan di-*boom* dengan banyak paket yang tidak penting. Selain itu juga penyerang dapat melakukan *spoof* BU untuk mengalihkan data stream ke alamat acak dari prefix jaringan sehingga jaringan yang dimaksud mengakses data yang salah.

Terdapat banyak teknik pada metode serangan DoS ini, namun yang digunakan dalam skripsi ini adalah *Distributed Denial of Service*. Berikut ini adalah penjelasan teknik serangan tersebut.

2.4.1 *Distributed Denial of Service*

Distributed Denial of Service merupakan serangan yang kerjanya dengan melakukan serangan DoS yang terkoordinasi melalui beberapa komputer. Dengan kata lain DoS dilakukan dengan satu komputer sedangkan DDoS dilakukan dengan lebih dari satu komputer. Penyerang primer pada dasarnya hanya terdiri dari satu komputer kemudian penyerang utama tersebut mendistribusikan metode serangannya ke komputer-komputer pasif yang menjadi penyerang-penyerang sekunder. Penyerang-penyerang sekunder ini akan menjadi zombie-zombie. Kemudian zombie-zombie ini akan dapat dikontrol untuk melancarkan serangan terhadap target yang ditentukan. Bentuk penguat serangan metode ini adalah adanya zombie-zombie yang membantu dalam serangan DoS ke target. Gambaran tentang DDoS akan ditampilkan pada Gambar 2.9 berikut ini.



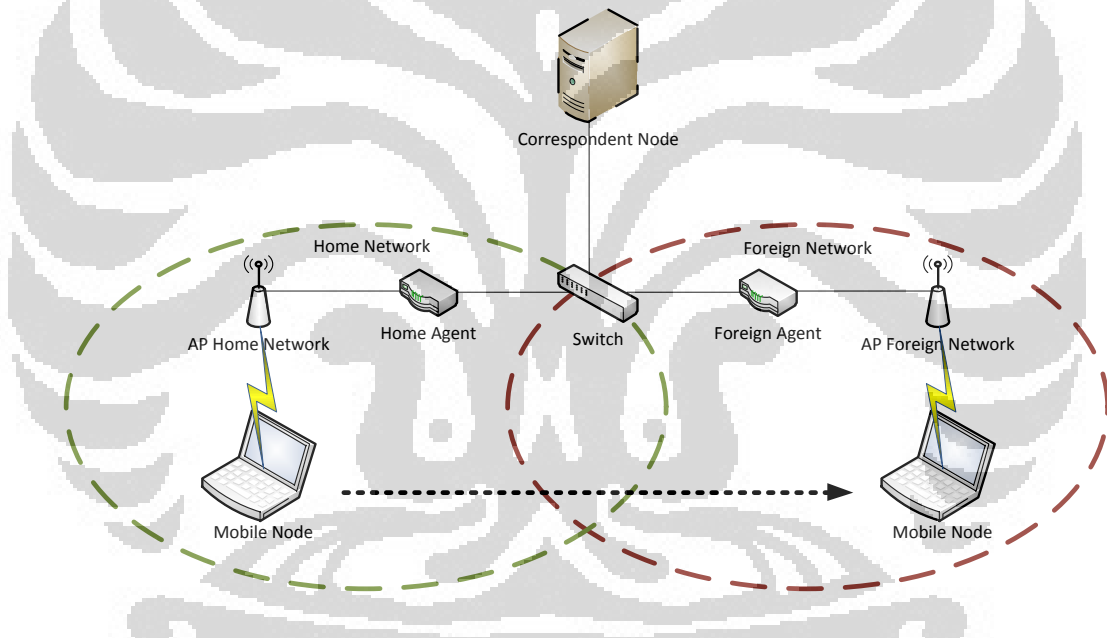
Gambar 2.9 Distributed Denial of Service

BAB 3

KONFIGURASI DAN IMPLEMENTASI APLIKASI FTP PADA JARINGAN *BIDIRECTIONAL MOBILE IPv6* SERTA SERANGANNYA

3.1 Topologi Jaringan

Dalam rancangan jaringan topologi jaringan dengan menggunakan topologi vertical. Topologi ini akan menerapkan *bidirectional mobile IPv6* dengan aplikasi FTP yang akan diserang dengan dua macam serangan yang telah disebutkan sebelumnya. Berikut ini merupakan Gambar 3.1 yang menjelaskan tentang topologi yang akan digunakan.



Gambar 3.1 Gambar rencana topologi jaringan

Dalam topologi ini dibutuhkan 4 (empat) buah laptop, 3 (tiga) buah PC, 2 (dua) buah *access point*, dan 1 (satu) buah *switch*. Perangkat-perangkat tersebut memiliki fungsi sebagai berikut ini.

- 1 Laptop digunakan sebagai *Mobile Node*.
- 3 Laptop digunakan sebagai penyerang sekunder *Distributed Denial of Service*.

- c. 1 PC digunakan sebagai *Home Agent* dan 1 PC digunakan sebagai *Foreign Agent*.
- d. 1 PC digunakan sebagai *Correspondent Node* diantara *Home Agent* dan *Foreign Agent*.
- e. 1 *Access point* digunakan sebagai penghubung nirkabel pada *Home Agent*, dan 1 *Access point* lagi digunakan sebagai penghubung nirkabel pada *Foreign Agent*.
- f. 1 *Switch* digunakan sebagai penghubung antara *Home Agent*, *Foreign Agent*, dan *Correspondent Node*.

3.2 Spesifikasi Sistem

3.2.1 Spesifikasi Hardware

Spesifikasi perangkat yang digunakan dalam perancangan jaringan bidirectional *mobile IPv6* ini adalah sebagai berikut.

1. *Correspondent Node / FTP Server*

Correspondent Node ini menggunakan sebuah PC sebagai FTP server.

Processor : Intel® Dual-Core™ CPU E6300 @2.80 GHz

Memori : 2 GB

Harddisk : 320 GB

2. *Home Router*

Router yang digunakan adalah sebuah PC yang difungsikan sebagai

Router yang dikonfigurasi agar mendukung *mobile IPv6* dan dapat menghubungkan perangkat-perangkat pada jaringan tersebut. PC ini

memiliki dua fungsi, yaitu sebagai *Home Router* dan *Home Agent*.

Processor : Intel® Dual-Core™ CPU E6300 @2.80 GHz

Memori : 2 GB

Harddisk : 320 GB

3. *Foreign Router*

Router yang digunakan adalah sebuah PC yang difungsikan sebagai

Router yang dikonfigurasi agar mendukung *mobile IPv6* dan dapat

menghubungkan perangkat-perangkat pada jaringan tersebut. PC ini memiliki dua fungsi, yaitu sebagai *Foreign Router* dan *Foreign Agent*.

Processor : Intel® Dual-Core™ CPU E6300 @2.80 GHz

Memori : 2 GB

Harddisk : 320 GB

4. *Access Point*

Access Point yang digunakan tanpa harus menggunakan spesifikasi tertentu. *Access Point* ini digunakan untuk menghubungkan *Mobile Node* dengan router di *Home Network* dan *Foreign Network*.

Tipe : TP-Link Wireless-G Access Point [TL-WA730RE]

Data Rates : 150 Mbps

6. *Switch*

Switch digunakan untuk menghubungkan *Home Agent*, *Foreign Agent* dan *Correspondent Node* / FTP Server.

Tipe: TP-LINK-TL-SF1005D

Port: 5-ports/10/100/Mbps

7. *Mobile Node*

Mobile node menggunakan laptop yang mendukung teknologi wireless.

Processor : Intel® Core 2 Duo T6600 @2.20 GHz

RAM : 4 GB

Harddisk : 320 GB

Wireless : Intel® WiFi Link 5100 AGN

8. Penyerang *Distributed Denial of Service*

Penyerang menggunakan tiga buah laptop untuk melakukan serangan *Distributed Denial of Service*.

- Laptop 1

Processor : Intel (R) Core i5

RAM : 4GB

Harddisk : 750 GB

- Laptop 2

Processor : Intel® Dual-Core™ CPU E6300 @2.80 GHz

Memori : 2 GB

Harddisk : 320 GB

- Laptop 3

Processor : Intel® Core 2 Duo T6600 @2.20 GHz

RAM : 2 GB

Harddisk : 320 GB

3.2.2 Spesifikasi Software

Software yang digunakan untuk mendukung perancangan jaringan bidirectional mobile IPv6 ini adalah sebagai berikut.

a. Sistem Operasi Linux Ubuntu 12.04 LTS

Sistem operasi ini penting digunakan karena mudah untuk dikonfigurasi dalam mendukung jaringan *mobile* IPv6 karena kernelnya yang dapat digunakan untuk bermacam-macam modul konfigurasi. *Software* lainnya yang mendukung perencanaan topologi jaringan ini dan program untuk serangannya membutuhkan spesifikasi linux.

b. Sistem Operasi Linux Ubuntu 13.04 LTS (Raring Ringtail)

Untuk beberapa perangkat menggunakan system operasi ini karena beberapa masalah dengan *driver* yang tidak mendukung. Perangkat yang menggunakan system operasi ini adalah *Home Agent* dan laptop untuk serangan *Distributed Denial of Service*.

c. UMIP (Linux Mobile IPv6 Daemon)

UMIP merupakan perangkat lunak yang digunakan untuk membuat konfigurasi pada *Home Agent*, *Correspondent Node*, dan *Mobile Node* untuk menciptakan jaringan *mobile* IPv6. Konfigurasi ini lah

yang digunakan untuk membedakan penggunaan *bidirectional tunneling* dan *route optimization*.

d. RADVD (*Router Advertisement Daemon*)

RADVD merupakan perangkat lunak yang berfungsi dalam pengiriman informasi yang berisi *router advertisement*. RADVD ini harus dipasang pada perangkat yang memiliki fungsi sebagai router. Dalam hal ini *Home Agent* dan *Foreign Agent* yang harus dipasang RADVD yang berfungsi juga sebagai router. Ketika *Mobile Node* meminta *router solicitation* pada *Home Agent* dan *Foreign Agent* ini maka router tersebut dapat memberikan IP kepada *Mobile Node*.

e. Wing FTP Server

Wing FTP Server ini merupakan suatu aplikasi untuk membuat FTP server. Aplikasi ini terpasang dalam bentuk aplikasi web. Aplikasi ini mendukung beberapa fungsi FTP, HTTP, FTPS, HTTPS, dan SFTP. Aplikasi ini dipasang di server yang ditentukan kemudian harus membuat domain untuk memberikan user-user yang didaftarkan sebagai hak akses. Setelah konfigurasi selesai maka client cukup mengakses alamat IP dari server tersebut.

f. Wireshark

Wireshark merupakan perangkat lunak yang berfungsi untuk memantau *traffic* pada jaringan tertentu melalui *interface* yang ditentukan. Wireshark ini membaca paket-paket data yang dikirim dan diterima melalui *interface* yang ditentukan tersebut.

g. *Multi-Generator (MGEN) Traffic Generator*

Perangkat lunak ini berfungsi untuk membuat jaringan lokal sesuai dengan jaringan sebenarnya dengan berbagai bentuk *traffic* yang ditentukan.

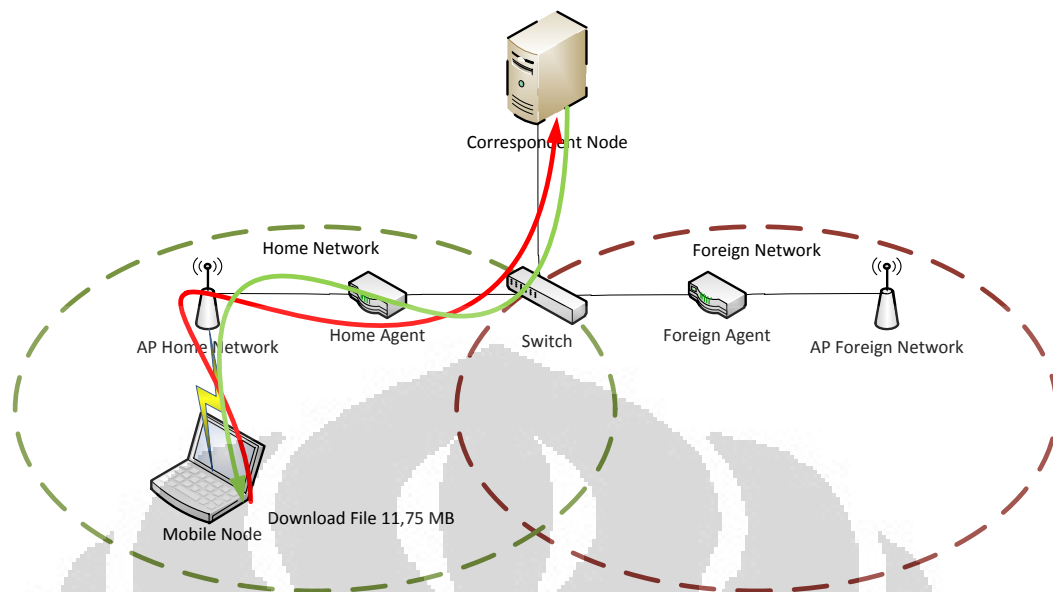
h. Xenotix Hash DoS *Tester*

Perangkat lunak ini digunakan untuk melakukan bentuk penyerang berupa *flood* paket data dengan ukuran dan *thread* yang dapat ditentukan ke tujuan penyerangan. Minimum besar paket data *flood* pada perangkat ini adalah 200KB. Perangkat ini dapat dikategorikan sebagai perangkat untuk melakukan serangan *Denial of Service* dan apabila perangkat ini didistribusikan ke beberapa komputer maka perangkat ini juga dapat dikategorikan sebagai perangkat untuk melakukan serangan *Distributed Denial of Service*. Aplikasi ini dapat mengakibatkan jaringan aksesnya sibuk dan penggunaan CPU-nya mencapai 100%. Perangkat ini juga memiliki fitur infinite loop untuk terus mengirimkan paket data yang ditentukan.

3.3 Skenario Penyerangan

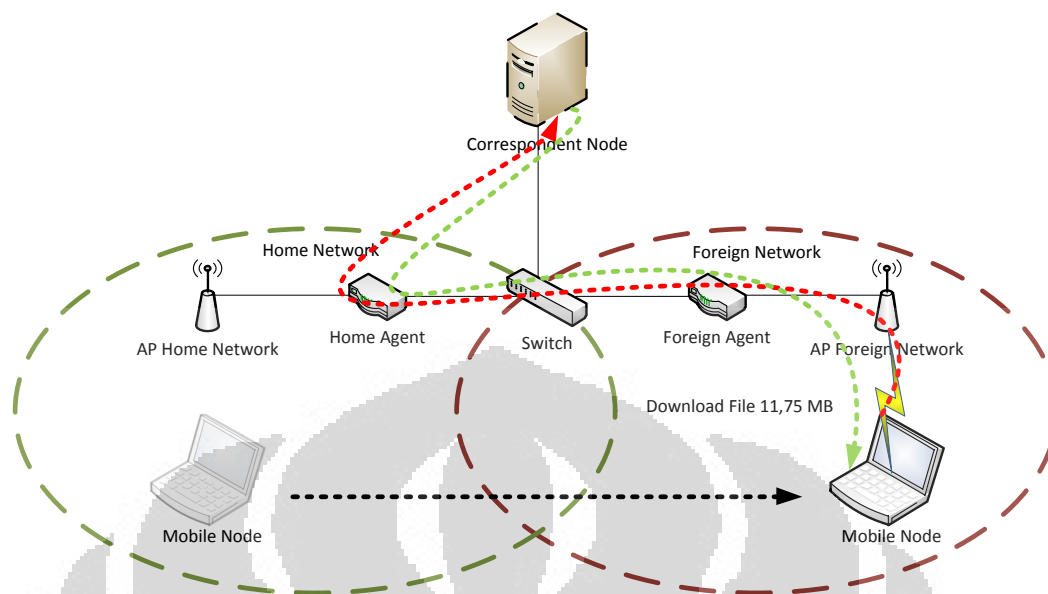
3.3.1 Skenario Pertama

Pada skenario ini jaringan dikonfigurasi dengan *bidirectional tunneling*. *Mobile Node* akan berada pada *Home Network* dan akan melakukan download data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Kemudian *Mobile Node* memantau jaringan pada interface WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan sebanyak 10 kali. Pada skenario ini server belum diserang. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.2 berikut ini.



Gambar 3.2 *Mobile Node* pada saat di *Home Network*

Kemudian *Mobile Node* akan berpindah ke *Foreign Network* dan akan melakukan download data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Kemudian *Mobile Node* memantau jaringan pada interface WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan sebanyak 10 kali. Pada skenario ini server belum diserang. Bentuk topologi percobaan ini dijelaskan pada Gambar 3.3 berikut ini.

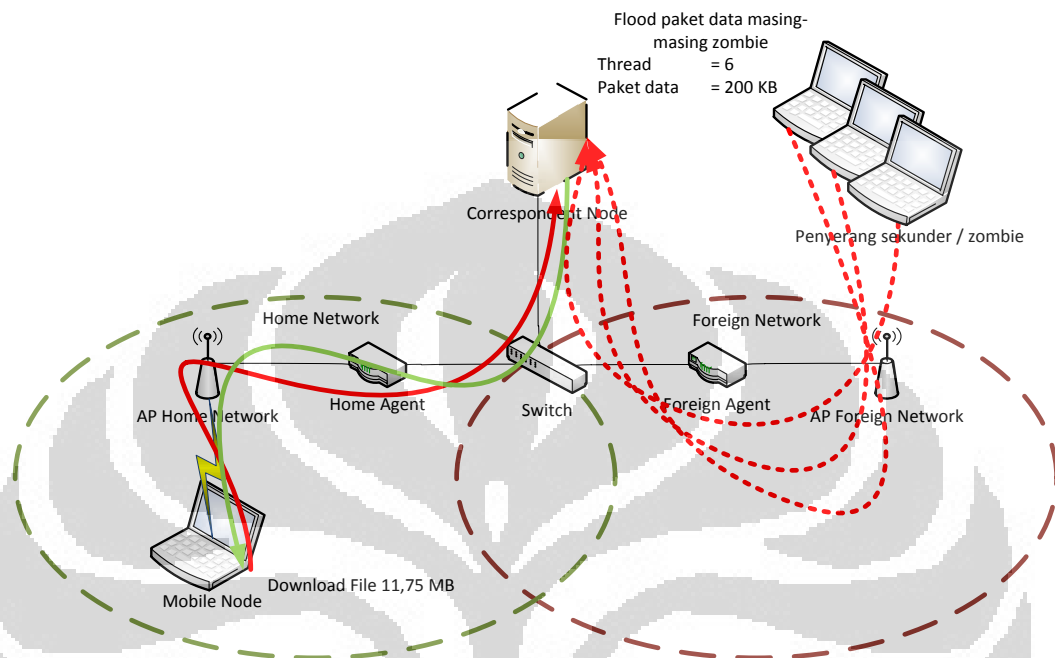


Gambar 3.3 *Mobile Node* saat berpindah ke *Foreign Network*

3.3.2 Skenario Kedua

Pada skenario ini *Mobile Node* akan berada pada *Home Network* dan akan melakukan download data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Selama mendownload file, FTP server atau *Correspondent Node* akan diserang dengan *Distributed Denial of Service*. Serangan ini menggunakan tiga buah laptop yang telah didistribusikan perangkat yang sudah siap dipakai untuk menyerang ke FTP server. Besar paket data masing-masing laptop untuk melakukan *flooding* adalah sebesar 200KB dengan besar *thread* 6. Besar *thread* dibuat 6 karena pengunduhan file sebesar itu di jaringan ini sekitar 15 sampai 16 detik dan jika diakumulasikan pada tiga laptop tersebut jumlah *thread* akan menjadi 18. Dengan 18 *thread* tersebut proses penyerangan tidak terdapat jeda untuk pengiriman *thread* berikutnya selama proses pengunduhan dimulai hingga selesai. Penyerang akan terhubung dari *Foreign Network*. Kemudian *Mobile Node* memantau jaringan pada *interface* WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan

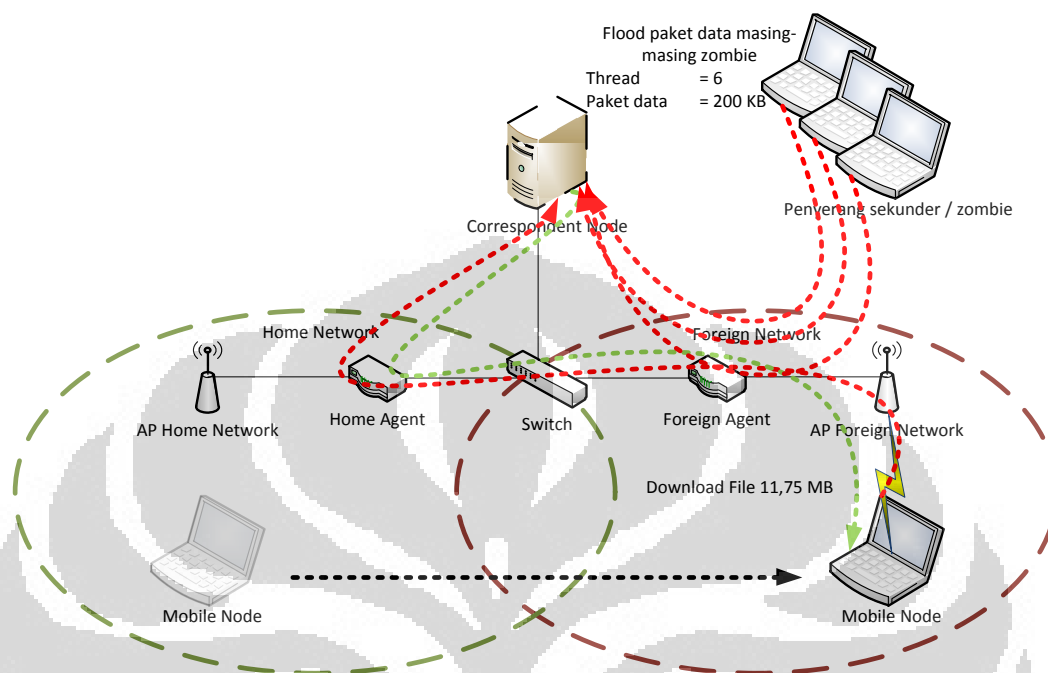
sebanyak 10 kali. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.4 berikut ini.



Gambar 3.4 Mobile Node pada saat di Home Network dan diserang dengan DDoS 200KB

Pada skenario ini *Mobile Node* akan berpindah ke *Foreign Network* dan akan melakukan *download* data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Selama mendownload file, FTP server atau *Correspondent Node* akan diserang dengan *Distributed Denial of Service*. Serangan ini menggunakan tiga buah laptop yang telah didistribusikan perangkat yang sudah siap dipakai untuk menyerang ke FTP server. Besar paket data masing-masing laptop untuk melakukan *flooding* adalah sebesar 200KB dengan besar *thread* 6 juga. Penyerang akan terhubung dari *Foreign Network*. Kemudian *Mobile Node* memantau jaringan pada *interface* WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan

ini dilakukan sebanyak 10 kali. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.5 berikut ini.

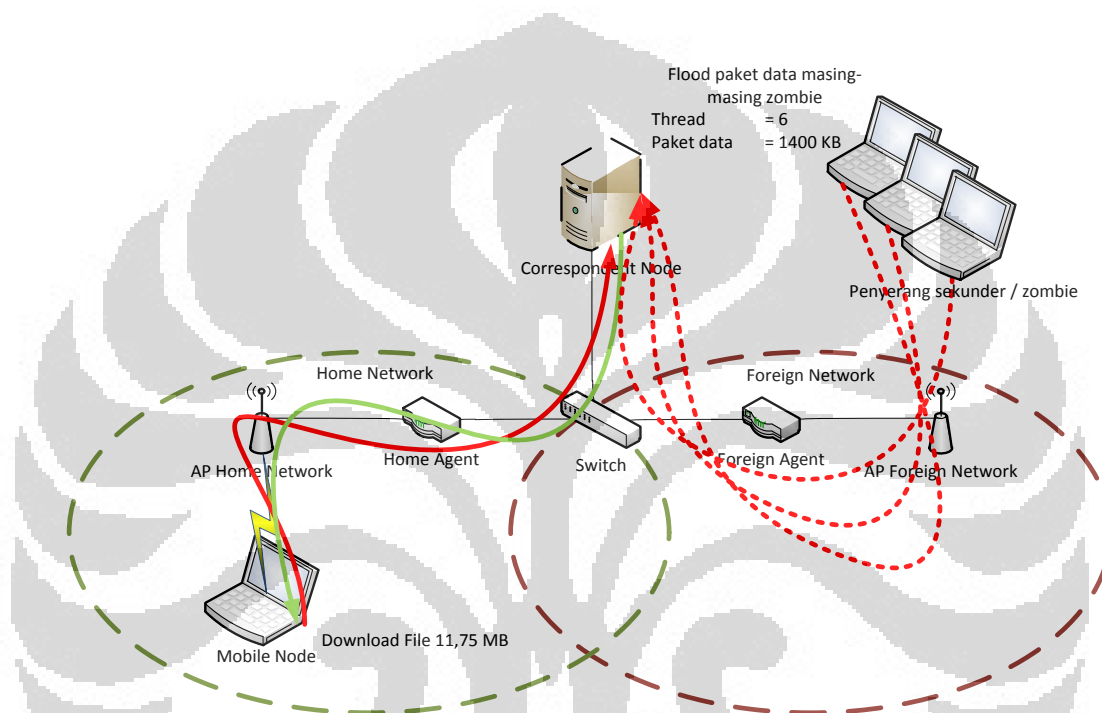


Gambar 3.5 Mobile Node saat pindah ke Foreign Network dan diserang dengan DDoS 200KB

3.3.3 Skenario Ketiga

Pada skenario ini Mobile Node akan berada pada *Home Network* dan akan melakukan download data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Selama mendownload file, FTP server atau *Correspondent Node* akan diserang dengan *Distributed Denial of Service*. Serangan ini menggunakan tiga buah laptop yang telah didistribusikan perangkat yang sudah siap dipakai untuk menyerang ke FTP server. Besar paket data masing-masing laptop untuk melakukan *flooding* adalah sebesar 1400KB dengan besar *thread* 6. Besar *thread* dibuat 6 karena pengunduhan file sebesar itu di jaringan ini sekitar 15 sampai 16 detik dan jika diakumulasikan pada tiga laptop tersebut jumlah *thread* akan menjadi 18. Dengan 18 *thread* tersebut proses penyerangan tidak terdapat jeda untuk pengiriman *thread* berikutnya selama proses pengunduhan dimulai hingga selesai. Penyerang akan terhubung dari

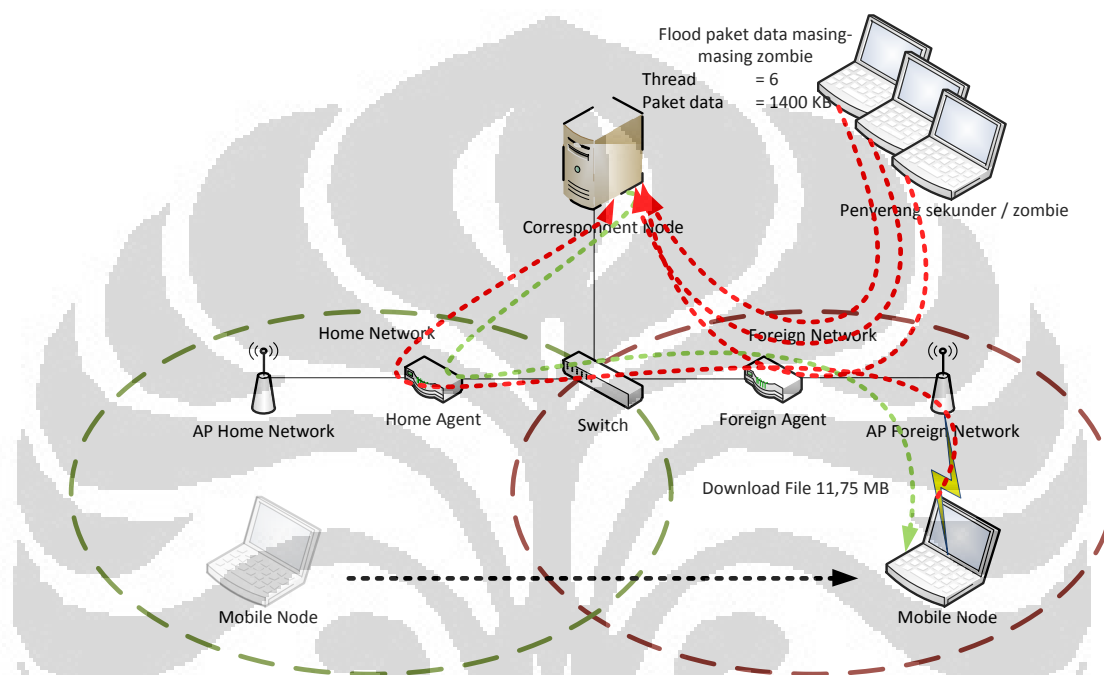
Foreign Network. Kemudian *Mobile Node* memantau jaringan pada *interface* WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan sebanyak 10 kali. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.6 berikut ini.



Gambar 3.6 Mobile Node pada saat di Home Network dan diserang dengan DDoS 1400KB

Pada skenario ini *Mobile Node* akan berpindah ke *Foreign Network* dan akan melakukan *download* data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Selama mendownload file, FTP server atau *Correspondent Node* akan diserang dengan *Distributed Denial of Service*. Serangan ini menggunakan tiga buah laptop yang telah didistribusikan perangkat yang sudah siap dipakai untuk menyerang ke FTP server. Besar paket data masing-masing laptop untuk melakukan *flooding* adalah sebesar 1400KB dengan besar *thread* 6 juga. Penyerang akan terhubung dari *Foreign Network*. Kemudian *Mobile Node* memantau

jaringan pada *interface* WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan sebanyak 10 kali. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.7 berikut ini.

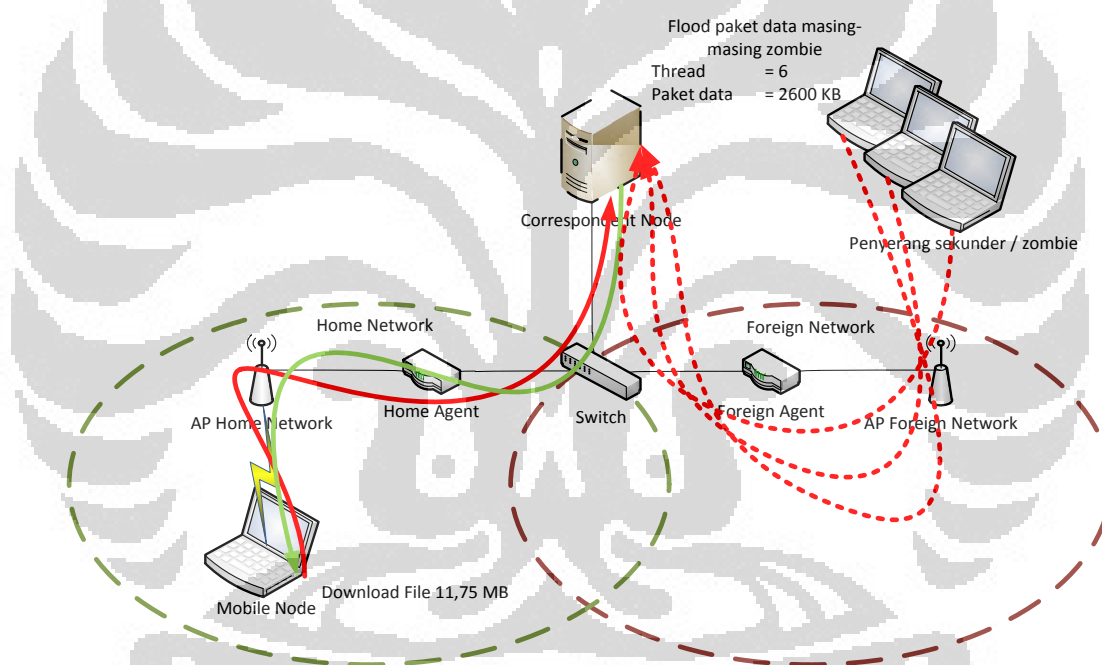


Gambar 3.7 Mobile Node saat pindah ke Foreign Network dan diserang dengan DDoS 1400KB

3.3.4 Skenario Keempat

Pada skenario ini Mobile Node akan berada pada *Home Network* dan akan melakukan download data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Selama mendownload file, FTP server atau *Correspondent Node* akan diserang dengan *Distributed Denial of Service*. Serangan ini menggunakan tiga buah laptop yang telah didistribusikan perangkat yang sudah siap dipakai untuk menyerang ke FTP server. Besar paket data masing-masing laptop untuk melakukan *flooding* adalah sebesar 2600KB dengan besar *thread* 6. Besar *thread* dibuat 6 karena pengunduhan file sebesar itu di jaringan ini sekitar 15

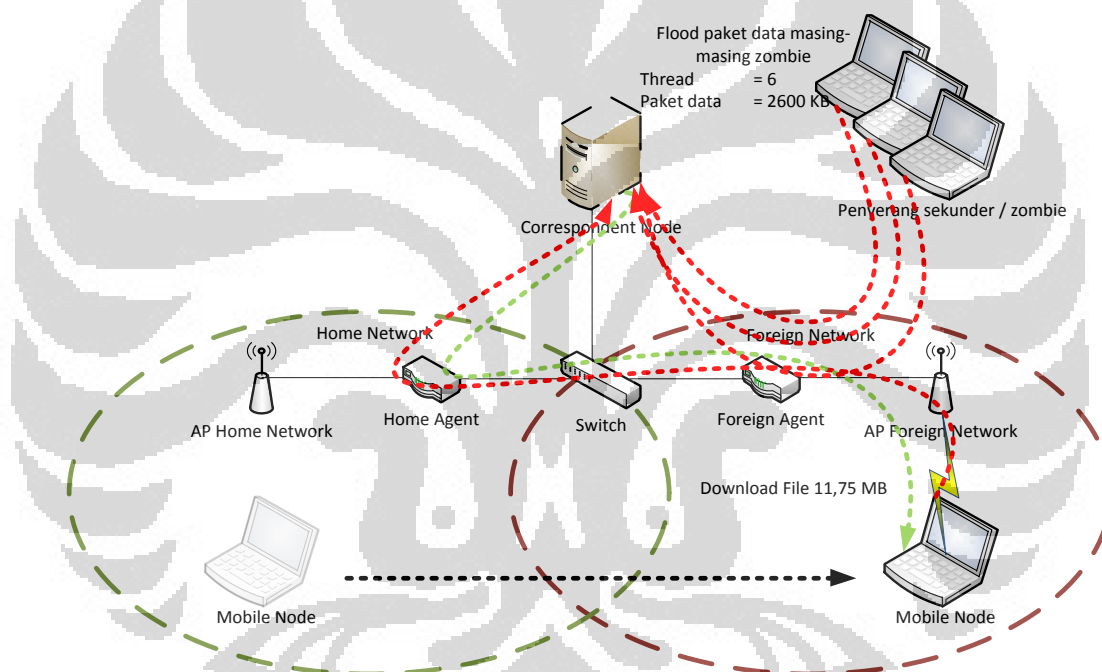
sampai 16 detik dan jika diakumulasikan pada tiga laptop tersebut jumlah *thread* akan menjadi 18. Dengan 18 *thread* tersebut proses penyerangan tidak terdapat jeda untuk pengiriman *thread* berikutnya selama proses pengunduhan dimulai hingga selesai. Penyerang akan terhubung dari Foreign Network. Kemudian *Mobile Node* memantau jaringan pada *interface* WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan sebanyak 10 kali. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.8 berikut ini.



Gambar 3.8 Mobile Node pada saat di Home Network dan diserang dengan DDoS 2600KB

Pada skenario ini *Mobile Node* akan berpindah ke *Foreign Network* dan akan melakukan *download* data dari FTP server atau *Correspondent Node* yang besarnya 11,75 MB hingga selesai. Selama mendownload file, FTP server atau *Correspondent Node* akan diserang dengan *Distributed Denial of Service*. Serangan ini menggunakan tiga buah laptop yang telah

didistribusikan perangkat yang sudah siap dipakai untuk menyerang ke FTP server. Besar paket data masing-masing laptop untuk melakukan *flooding* adalah sebesar 2600KB dengan besar *thread* 6 juga. Penyerang akan terhubung dari *Foreign Network*. Kemudian Mobile Node memantau jaringan pada *interface* WLAN0 dengan menggunakan Wireshark. Wireshark yang digunakan akan dibuat untuk menyaring paket TCP yang dikirimkan dari alamat FTP server atau *Correspondent Node*. Percobaan ini dilakukan sebanyak 10 kali. Bentuk topologi perobaan ini dijelaskan pada Gambar 3.9 berikut ini.



Gambar 3.9 Mobile Node saat pindah ke Foreign Network dan diserang dengan DDoS 2600KB

3.4 Pembuatan Sistem

Topologi yang akan digunakan pada skripsi ini harus dikonfigurasi lagi sedemikian rupa sehingga dapat mendukung mobile IPv6. Semua perangkat pada skripsi ini diinstal sistem operasi Ubuntu. Berikut ini adalah proses-proses yang dibutuhkan untuk menciptakan lingkungan mobile IPv6.

3.4.1 Instalasi Kernel

Pada topologi ini, perangkat menggunakan sistem operasi Ubuntu 12.04 dan beberapa menggunakan sistem operasi Ubuntu 13.04 karena beberapa alasan masalah driver. Untuk dapat mendukung fitur *mobile* IPv6 maka perlu dipasang kernel 3.8.2. Untuk instalasi kernel ini dibutuhkan file `linux-3.8.2.tar.bz2` dan `linux-3.8.2.tar.sign`. File tersebut dapat didownload dari situs `kernel.org` dan juga harus diletakkan pada direktori `/usr/src`. Kemudian kernel di verifikasi secara online kemudian kita masuk ke direktori `linux-3.8.2` tersebut. Pada direktori ini, konfigurasi dilakukan dengan masuk ke `menuconfig` dari kernel linux tersebut dan mengaktifkan beberapa opsi yang dibutuhkan untuk mendukung *mobile* IPv6. Setelah konfigurasi selesai, kernel siap untuk diekstraksi dan diinstal ke dalam sistem operasi termasuk modul dan header-nya. Setelah selesai ekstraksi dan instalasi maka sistem harus di *reboot*. Masuk ke header kernel 3.8.2 untuk menggunakan kernel yang baru terinstal.

3.4.2 Instalasi UMIP dan RADVD

Dalam instalasi UMIP dilakukan dengan penyusunan beberapa kode-kode pada paket pendukung yang terdapat pada UMIP tersebut agar dapat tercipta jaringan *mobile* IPv6. Untuk proses instalasinya dibutuhkan beberapa perangkat lunak tambahan, yaitu `autoconf`, `automake`, `bison`, `flex`, `libssl-dev`, `indent`, `ipsec-tools`, dan `radvd`. Kemudian UMIP tersebut diinstal di direktori `/usr/src/`. UMIP dapat diperoleh dengan mendownload atau melakukan `git clone` pada website `umip.org`. Setelah itu masuk ke direktori `umip` dan proses `autoreconf` serta instalasi dilakukan didalam direktori tersebut.

3.4.3 Instalasi Wing FTP Server

Wing FTP Server dapat didownload pada website resminya di `wftpserver`. Setelah instalasi selesai untuk masuk kedalam konfigurasi Wing FTP Server, buka alamat local host dengan port 5466 melalui web

browser di komputer server. Kemudian login dengan user dan password yang sesuai saat proses penginstallan.

Setelah itu domain harus dibuat dan daftarkan beberapa user dan password sebagai klien yang diizinkan untuk mengakses FTP server tersebut. Pada pembuatan domain, masukkan alamat IPv6 server sebagai Bind IP Address. Bind IP Address pada aplikasi ini adalah untuk alamat akses ke server dari klien.

Pada saat mendaftarkan user, arahkan setiap user ke direktori yang ditentukan pada FTP server sebagai direktori penyimpanan maupun pengunduhan. Setelah selesai maka FTP server dapat diakses dari mana saja yang dapat terhubung ke FTP server melalui web browser dengan memasukkan alamat IP dari FTP server tersebut. Dalam skripsi ini FTP server yang dipakai adalah Correspondent Node.

3.4.4 Rekayasa Trafik

Untuk melakukan rekayasa trafik, perangkat lunak yang digunakan adalah MGEN. Perangkat lunak ini bersifat open source sehingga dapat membuat pola trafik pada jaringan secara bebas. Dalam instalasi MGEN, dibutuhkan sebuah server untuk melakukan balasan paket yang dikirimkan dari klien dan klien tersebut akan mendengarkan koneksi. Klien juga berperan untuk merespon dan menerima paket-paket yang dikirimkan.

MGEN diproses dengan menjalankan command line. Pada command line tersebut terdapat IPv6, input script file, dan output log file. IPv6 pada command line ini digunakan untuk menunjukkan jenis IP yang digunakan, yaitu IPv6. Input script file digunakan untuk perintah-perintah untuk membuat rekayasa trafik yang dijalankan pada MGEN. Output log file merupakan catatan dari perintah-perintah yang dijalankan.

MGEN ini dijalankan pada Home Agent, Foreign Agent, dan Correspondent Node. Setiap node harus memiliki masing-masing script file. Home Agent dikonfigurasi agar mengirimkan pesan UDP dari port 5001 sebanyak 32 pesan per detik dengan ukuran 8192 byte ke port 5001 Foreign Agent. Foreign Agent juga dikonfigurasi agar mengirimkan pesan

UDP dari port 5001 sebanyak 32 pesan per detik dengan ukuran 8192 byte ke port 5001 Home Agent. Correspondent Node dikonfigurasi agar dapat mendengarkan kiriman pesan UDP di port 5002 dari Foreign Agent dan mendengarkan permintaan sambungan. Correspondent Node juga dikonfigurasi agar dapat mendengarkan kiriman pesan TCP di port 8000 dari Home Agent. Foreign Agent mengirimkan paket UDP sebanyak 32 pesan per detik sebesar 8192 byte dan Home Agent mengirimkan pesan TCP sebanyak 1 pesan per detik sebesar 5242880 byte.

3.4.5 Konfigurasi Node

Setiap node harus dilakukan konfigurasi tambahan lagi untuk mendukung berjalannya jaringan *mobile* IPv6 ini. Konfigurasi tambahan untuk setiap node adalah sebagai berikut.

1. Home Agent

Pada *Home Agent* terdapat dua interface yang menghubungkan antara Home Network dan jaringan untuk ke *switch*. *Interface* eth1 digunakan untuk *access point* yang menghubungkan *Home Agent* dengan *Home Network*. *Interface* eth0 digunakan untuk menghubungkan *Home Agent* dengan jaringan untuk ke *switch*. Alamat eth0 adalah 2001:db8:ffff:100b::11/64 dan alamat eth1 adalah 2001:db8:ffff:100a::1/64. Kedua *interface* ini dikonfigurasi terlebih dahulu. Kemudian untuk dapat berkomunikasi dengan *Foreign Network* maka *Home Agent* dikonfigurasi dengan *static route* ke jaringan tersebut melalui *interface* masukannya.

Pada *Home Agent* harus ada beberapa file konfigurasi untuk mendukung *mobile* IPv6. File tersebut adalah *mip6d.conf*, *setkey.conf* dan *radvd.conf*. File-file tersebut harus dikonfigurasi agar berjalan secara otomatis saat *Home Agent* melakukan *booting up*.

2. *Foreign Agent*

Pada *Foreign Agent* terdapat dua *interface* yang menghubungkan antara *Foreign Network* dan jaringan untuk ke *switch*. *Interface* eth1 digunakan untuk *access point* yang menghubungkan *Foreign Agent* dengan *Foreign Network*. *Interface* eth0 digunakan untuk menghubungkan *Foreign Agent* dengan jaringan untuk ke *switch*. Alamat eth0 adalah 2001:db8:ffff:100b::12/64 dan alamat eth1 adalah 2001:db8:ffff:100c::1/64. Kedua *interface* ini dikonfigurasi terlebih dahulu. Kemudian untuk dapat berkomunikasi dengan *Home Network* maka *Foreign Agent* dikonfigurasi dengan *static route* ke jaringan tersebut melalui *interface* masukannya.

Pada *Foreign Agent* tidak dibutuhkan file *mip6d.conf* namun hanya diperlukan file *radvd.conf*. File *radvd.conf* tersebut harus dikonfigurasi agar berjalan secara otomatis saat *Foreign Agent* melakukan *booting up*.

3. *Mobile Node*

Pada *Mobile Node*, konfigurasi *interface* hanya dilakukan pada *interface* wlan0 saja karena pada topologi ini *Mobile Node* terhubung secara nirkabel. *Mobile Node* harus ada file *mip6d.conf* dan *setkey.conf*. File tersebut harus dikonfigurasi agar berjalan secara otomatis saat *Mobile Node* melakukan *booting up*. Alamat IP akan otomatis didapatkan sesuai dengan konfigurasi yang terdapat pada konfigurasi *mip6d.conf* dan saat berpindah jaringan akan muncul *iptnl1* sesuai dengan alamat IP dari *Home Address*-nya.

4. *Correspondent Node*

Pada *Correspondent Node*, konfigurasi *interface* hanya dilakukan pada *interface* eth0 saja. Alamat IP-nya adalah 2001:db8:ffff:100b::13 dan ini adalah alamat akses ke server. Node ini tidak perlu file-file konfigurasi seperti node lainnya karena node ini hanya sebagai koresponden.

BAB 4

ANALISIS PERFORMANSI JARINGAN *BIDIRECTIONAL MOBILE IPv6* DENGAN APLIKASI FTP

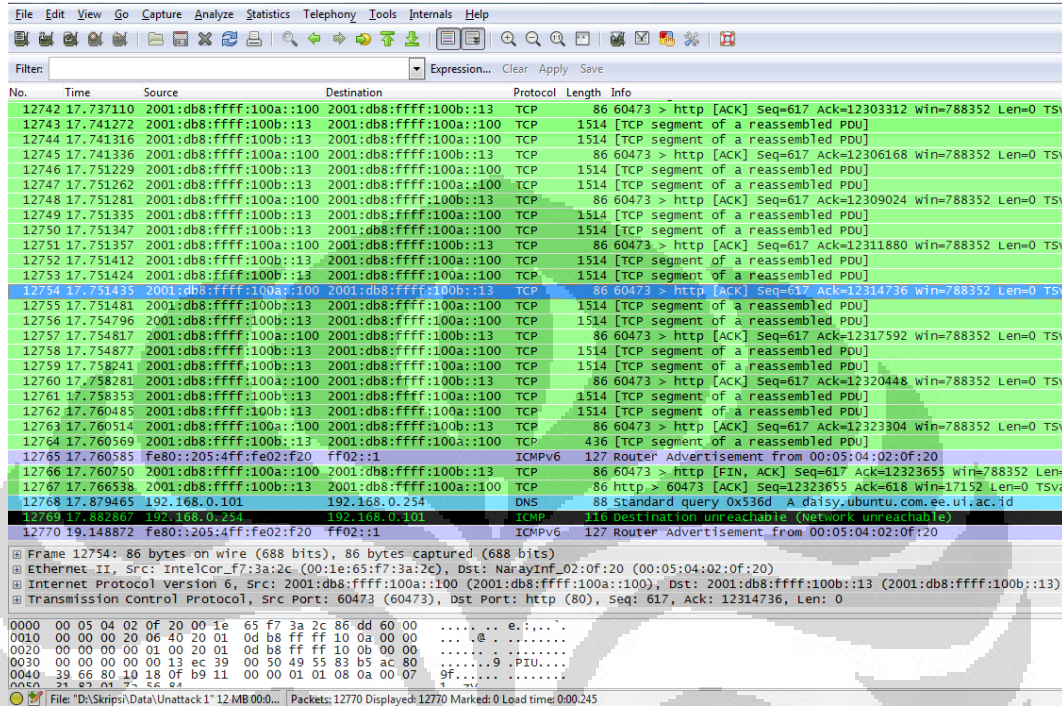
4.1 Pengujian Parameter Performansi

Berdasarkan topologi jaringan *bidirectional mobile IPv6* pada skripsi ini maka akan diuji dan diukur parameter performansi dari aplikasi FTP pada jaringan tersebut. Pada skenario-skenario yang telah dijelaskan pada bab III, *Mobile Node* akan mengunduh file yang terdapat pada *Correspondent Node* atau FTP server yang besarnya 11.75 MB. Ekstensi file tersebut adalah format *.tar.gz*. Performansi diukur mulai dari pengunduhan dimulai hingga pengunduhan selesai dilakukan.

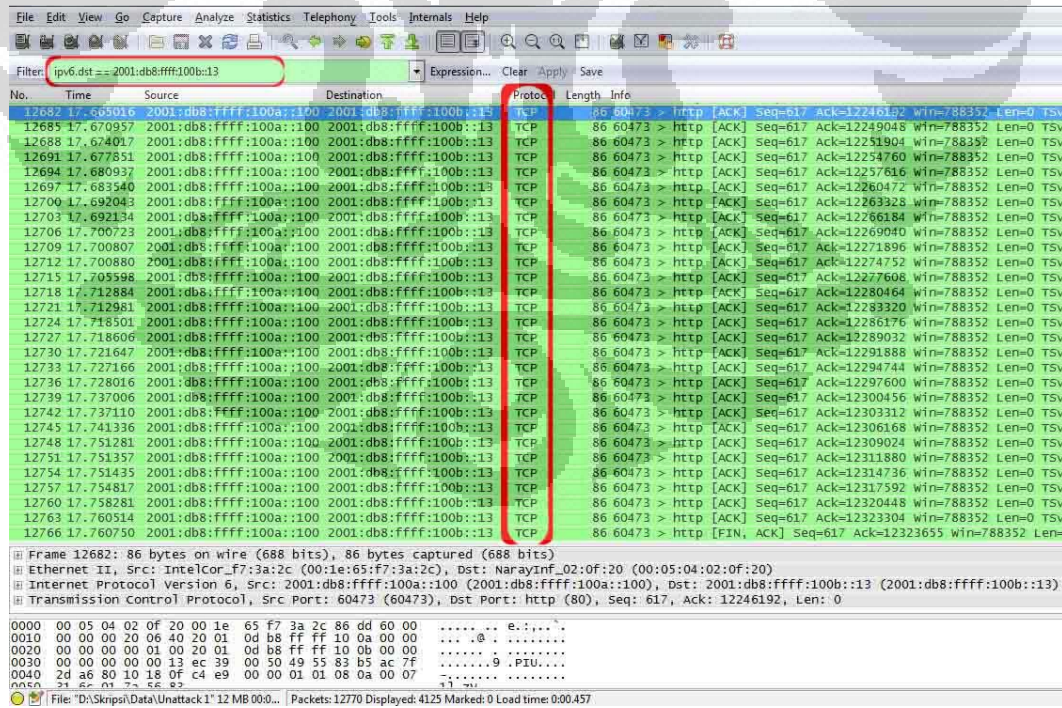
Pengukuran performansi akan dilakukan pada *Mobile Node* dengan menggunakan Wireshark. Pada dasarnya pengukuran hanya dilakukan dengan dua pengukuran, yaitu pengukuran pada saat *Mobile Node* mengunduh file dengan keberadaan di *Home Network* dan pada saat *Mobile Node* mengunduh file dengan keberadaan di *Foreign Network*. Kedua pengukuran tersebut menggunakan *tunneling* yang sama, yaitu *bidirectional tunneling*. Kemudian kedua pengukuran tersebut akan terbagi lagi dengan keadaan jaringan yang sedang diserang. Jadi pengukuran pada saat *Mobile Node* mengunduh file sebelum diserang, setelah diserang *Distributed Denial of Service* dengan variasi besar paket data serangan sesuai bab III dengan keberadaan di *Home Network* dan berpindah di *Foreign Network*.

Pengukuran akan dilakukan sebanyak 10 kali pada setiap skenario yang ditentukan agar mendapatkan nilai yang valid. Wireshark akan digunakan untuk menangkap paket data selama proses pengunduhan file dari *Correspondent Node* ke *Mobile Node* berlangsung. Dari hasil yang didapatkan dari Wireshark, data dapat dianalisis sesuai dengan parameter yang digunakan, yaitu transfer time, delay, packet loss, dan throughput. Wireshark ini tidak hanya menangkap lalu lintas paket data yang berasal dari *Correspondent Node*, tetapi seluruh paket-paket yang melalui jaringan yang keluar masuk interface tersebut seperti yang

ditampilkan pada Gambar 4.1. Untuk mendapatkan paket-paket yang hanya berasal dari *Correspondent Node* maka dibutuhkan filter paket seperti yang ditampilkan pada Gambar 4.2.



Gambar 4.1 Hasil Wireshark sebelum di-filter



Gambar 4.2 Hasil Wireshark setelah di-filter

Filter akan dilakukan untuk menyaring paket-paket yang dikirimkan dari *Correspondent Node* sehingga alamat IP sumber di-filter di alamat 2001:db8:ffff:100b::13. Alamat tersebut merupakan alamat dari *Correspondent Node* atau FTP server. Karena Wing FTP server merupakan aplikasi FTP yang berbasis web yang dapat diunduh melalui web browser maka protokol yang bekerja di atasnya merupakan TCP. Sehingga filter dilakukan pula pada TCP.

Setelah paket-paket data sudah disaring sesuai dengan keinginan, parameter-parameter pengukuran untuk dianalisis dapat dilihat melalui *summary*. *Summary* ini mencakup seluruh data statistik dari paket-paket data yang tertangkap oleh Wireshark ini. Dari *summary* ini, parameter transfer time, delay, packet loss, dan throughput dapat dihitung. Nilai yang dilihat adalah nilai yang tertera pada kolom displayed karena ini merupakan hasil statistik sesuai dari filter yang telah dilakukan. Transfer time dapat dilihat pada baris *Between first and last packet* dengan satuan detik. Delay dapat dihitung dengan cara transfer time dibagi dengan jumlah paket. Packet loss dapat dilihat dari paket-paket yang berwarna hitam yang ter-capture saat wireshark sudah difilter. Sedangkan throughput pada Wireshark memiliki tiga satuan yang ditampilkan, yaitu Avg.packets/sec, Avg.bytes/sec, dan Avg.Mbit/sec. Dalam skripsi ini, satuan throughput yang digunakan adalah Avg.bytes/sec. Contoh dari *summary* ditampilkan pada Gambar 4.3 berikut ini.

File

Name: D:\Skripsi\Data\Unattack 1
 Length: 13605073 bytes
 Format: Wireshark/tcpdump/... - libpcap
 Encapsulation: Ethernet
 Packet size limit: 65535 bytes

Time

First packet: 2013-05-24 02:56:52
 Last packet: 2013-05-24 02:57:11
 Elapsed: 00:00:19

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	65535 bytes

Display

Display filter: ipv6.src == 2001:db8:ffff:100b::13
 Ignored packets: 0

Traffic	Captured	Displayed	Marked
Packets	12770	8623	0
Between first and last packet	19.149 sec	16.848 sec	Transfer Time
Avg. packets/sec	666.880	511.823	
Avg. packet size	1049.391 bytes	1512.365 bytes	
Bytes	13400729	13041121	
Avg. bytes/sec	699818.188	774062.729	Throughput
Avg. MBit/sec	5.599	6.193	

Gambar 4.3 Summary dari Wireshark

4.2 Mekanisme Serangan

Mekanisme serangan dengan menggunakan perangkat Xenotic Hash DoS Tester yang didistribusikan ke tiga buah laptop. Serangannya adalah dengan flooding paket data. Paket data akan divariasikan menjadi 200KB, 1400KB, dan 2600KB. Laptop-laptop tersebut akan flooding sesuai paket data yang ditentukan tersebut ke alamat IP dari FTP server atau *Correspondent Node*. Flooding dilakukan secara bersamaan oleh ke tiga laptop tersebut. Dengan flooding paket data tersebut akan diamati parameter performansi dari jaringan *bidirectional mobile IPv6* dengan aplikasi FTP ini berupa transfer time, delay, throughput, dan packet loss.

4.3 Analisis Parameter Performansi

4.3.1 Analisis Transfer Time

Transfer time merupakan waktu keseluruhan yang dibutuhkan file dari FTP server ke FTP client. Pada skripsi ini, transfer time berarti waktu yang dibutuhkan hingga file selesai diunduh dari *Mobile Node*. Transfer time ini juga dipengaruhi oleh besarnya throughput pada jaringan. Semakin besar throughputnya maka semakin kecil pula transfer timenya. Analisis data dengan parameter transfer time ini dilakukan pada saat *Mobile Node* berada di *Home Network* dan mengunduh file, kemudian pindah ke *Foreign Network* dan mengunduh file kembali. Pengukuran tersebut juga dilakukan pada saat *Correspondent Node* atau FTP server sebelum dan sesudah diserang. Untuk perhitungan persentase kenaikan transfer time adalah sebagai berikut.

$$\mu_T = \frac{TT_{(Sesudah\ diserang)} - TT_{(Sebelum\ diserang)}}{TT_{(Sebelum\ diserang)}} \times 100\%$$

μ_T = Persentase kenaikan transfer time (%)

$TT_{(Sesudah\ diserang)}$ = Transfer time sesudah diserang (detik)

$TT_{(Sebelum\ diserang)}$ = Transfer time sebelum diserang (detik)

a. Transfer time di *Home* dan di *Foreign Network* sebelum diserang

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Kemudian *Mobile Node* akan dipindahkan ke *Foreign Network*. Di *Foreign Network* juga *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Data transfer time dari 10 kali pengunduhan tersebut ditampilkan pada Tabel 4.1 berikut ini.

Tabel 4. 1 Transfer time pada *Home* dan *Foreign Network* sebelum diserang

Pengujian ke-	Transfer Time di <i>Home Network</i> (detik)	Transfer Time di <i>Foreign Network</i> (detik)
1	16.85	23.33
2	16.26	29.59
3	16.42	30.54
4	23.67	21.93
5	16.37	22.76
6	21.27	22.41
7	15.13	26.96
8	18.39	25.35
9	17.68	23.34
10	15.25	26.09
Rata-rata	17.73	25.23

Berdasarkan Tabel 4.1 terlihat perbedaan transfer time pada saat *Mobile Node* berada di *Home Network* dengan *Mobile Node* saat berada di *Foreign Network*. Besar data yang diunduh adalah sama, namun perbedaan transfer timenya cukup besar. Hal ini dikarenakan *tunneling* pada topologi jaringan mobile IPv6 yang dipakai pada skripsi ini adalah *bidirectional tunneling*. Transfer time di *Foreign Network* lebih lama 42.30%

dibandingkan dengan transfer time di *Home Network*. Transfer time lebih lama pada saat di *Foreign Network* dibandingkan *Home Network* karena dengan *bidirectional tunneling* tukar menukar data antara *Mobile Node* dengan *Correspondent Node* harus selalu melalui Home Agent.

b. Transfer time di *Home Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali dengan keadaan FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data transfer time dari 10 kali pengunduhan dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.2 berikut ini.

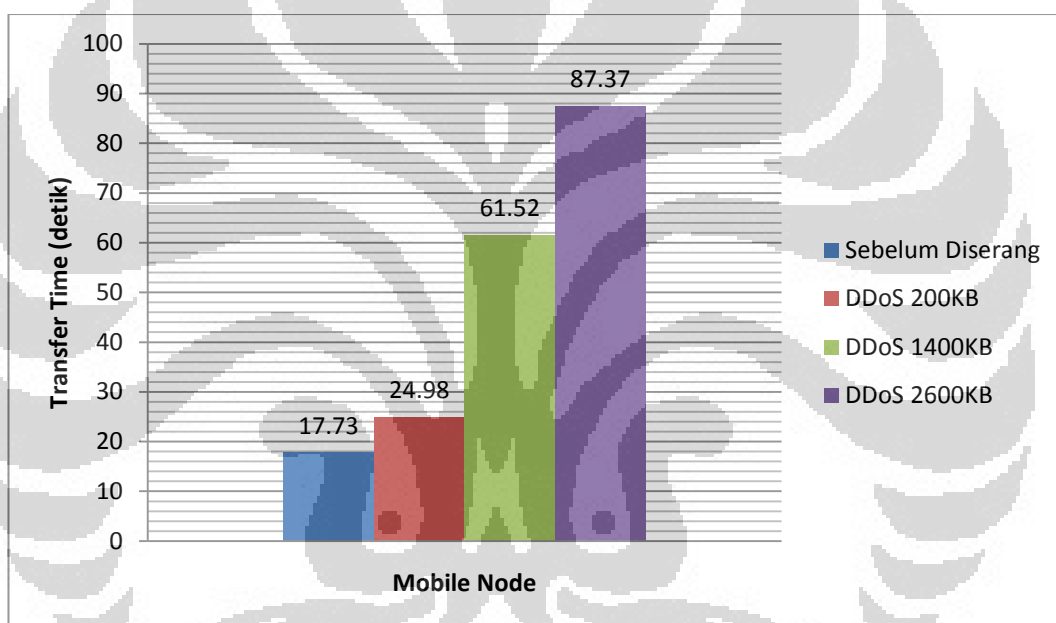
Tabel 4. 2 Transfer time pada *Home Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Transfer Time di <i>Home Network</i> (detik)	Transfer Time saat di-DDoS 200KB (detik)	Transfer Time saat di-DDoS 1400KB (detik)	Transfer Time saat di-DDoS 2600KB (detik)
1	16.85	25.79	88.31	84.51
2	16.26	24.07	48.38	76.33
3	16.42	22.78	59.99	69.66
4	23.67	23.54	54.12	71.93
5	16.37	24.98	79.36	64.71
6	21.27	27.79	55.62	80.58
7	15.13	25.84	47.58	125.73
8	18.39	22.56	70.18	96.93
9	17.68	22.58	56.39	107.82
10	15.25	29.84	55.25	95.47
Rata-rata	17.73	24.98	61.52	87.37

Berdasarkan Tabel 4.2 terlihat perbedaan transfer time pada saat *Mobile Node* berada di *Home Network* dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan. Besar data yang diunduh adalah sama, namun perbedaan transfer timenya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat transfer time lebih lama 40.89% dibandingkan transfer time pengunduhan di *Home Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat transfer time lebih lama 246.98% dibandingkan transfer time pengunduhan di *Home Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat transfer time lebih lama 392.78% dibandingkan transfer time pengunduhan di *Home Network* sebelum diserang. Semakin besar paket data serangan

maka semakin lama pula transfer time yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

Gambar 4.4 berikut ini akan menampilkan grafik perbandingan rata-rata transfer time dari *Mobile Node* saat mengunduh file di *Home Network* sebelum dan diserang dengan DDoS 3 variasi besar paket data serangan.



Gambar 4.4 Grafik perbandingan transfer time di *Home Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

c. Transfer time di *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berpindah ke *Foreign Network* dan terhubung dengan *access point Foreign Network* yang terhubung pada *interface eth1 Foreign Agent*. Kemudian *Mobile Node* akan mengunduh file file.tar.gz dari *Correspondent Node* atau FTP server sebanyak 10 kali dengan keadaan

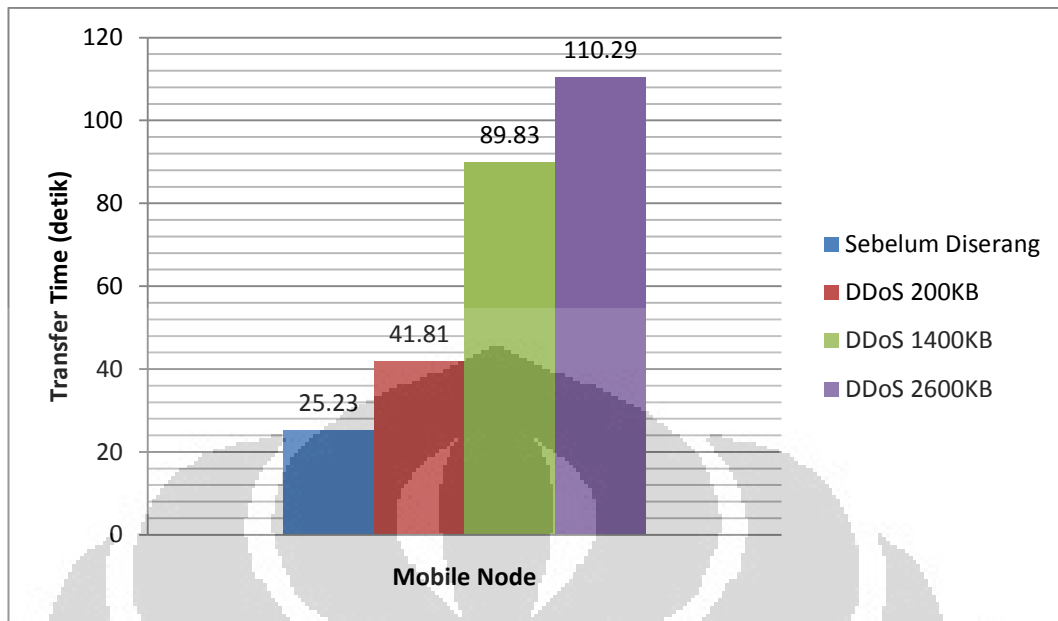
FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data transfer time dari 10 kali pengunduhan dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.3 berikut ini.

Tabel 4. 3 Transfer time pada *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Transfer Time di <i>Foreign Network</i> (detik)	Transfer Time saat di-DDoS 200KB (detik)	Transfer Time saat di-DDoS 1400KB (detik)	Transfer Time saat di-DDoS 2600KB (detik)
1	23.33	31.82	103.96	117.33
2	29.59	30.16	103.21	120.32
3	30.54	43.46	86.12	137.1
4	21.93	52.85	70.84	119.82
5	22.76	32.56	88.8	128.39
6	22.41	40.99	72.73	116.71
7	26.96	48.09	104.37	99.66
8	25.35	49.46	80.9	85.55
9	23.34	37.8	95.82	94.91
10	26.09	50.89	91.6	83.19
Rata-rata	25.23	41.81	89.83	110.29

Berdasarkan Tabel 4.3 terlihat perbedaan transfer time pada saat *Mobile Node* berada di *Foreign Network* dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan. Besar data yang diunduh adalah sama, namun perbedaan transfer timenya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat transfer time lebih lama 65.71% dibandingkan transfer time pengunduhan di *Foreign Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat transfer time lebih lama 256.04% dibandingkan transfer time pengunduhan di *Foreign Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat transfer time lebih lama 337.14% dibandingkan transfer time pengunduhan di *Foreign Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula transfer time yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

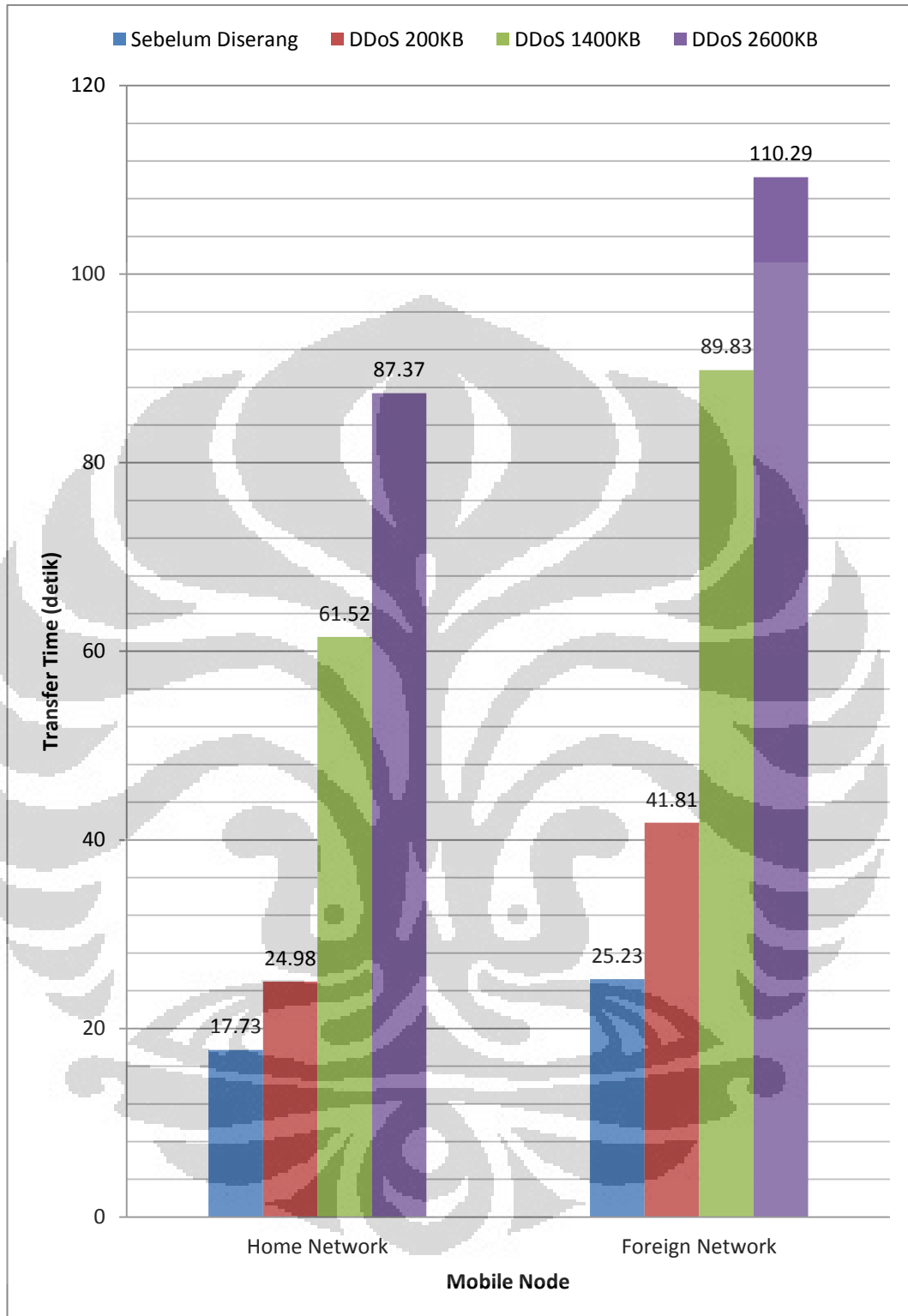
Gambar 4.5 berikut ini akan menampilkan grafik perbandingan rata-rata transfer time dari *Mobile Node* saat mengunduh file di *Foreign Network* sebelum dan diserang dengan DDoS 3 variasi besar paket data serangan.



Gambar 4.5 Grafik perbandingan transfer time di *Foreign Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

d. Perbanding transfer time dari seluruh keadaan

Pengujian untuk transfer time pengunduhan jaringan *bidirectional mobile IPv6* ini telah dilakukan dengan berbagai skenario. Untuk perbandingan lebih terlihat maka perlu penggabungan seluruh grafik data transfer time dari berbagai skenario tersebut. Gambar 4.6 berikut ini akan menampilkan perbandingan transfer time dari seluruh keadaan pengujian.



Gambar 4.6 Grafik perbandingan transfer time seluruh keadaan sebelum dan sesudah diserang

Dari Gambar 4.6 diatas terlihat transfer time di *Foreign Network* memiliki nilai yang lebih tinggi dibandingkan dengan di *Home Network* saat setelah diserang. Hal ini dikarenakan transfer time di *Foreign Network* sebelum diserang pun sudah lebih tinggi dibandingkan dengan di *Home Network*. Dengan ditambahkan serangan maka transfer time pada jaringan ini pun akan semakin bertambah. Pada grafik pun terlihat bahwa semakin besar paket data serangan DDoS maka semakin besar pula transfer time-nya. Hal ini juga dikarenakan paket data serangan mengacaukan dan membuat jaringan *mobile* ini menjadi lebih sibuk dibandingkan sebelumnya. Dari grafik tersebut juga dapat dilihat perbandingan persentase peningkatan transfer time paket data serangan 200KB dengan 1400KB berbeda dengan paket data serangan 1400KB dengan 2600KB. Hal ini dikarenakan dengan proses penyerangan ini harus melibatkan kedua belah pihak antara penyerang dan yang diserang. Semakin besar paket data yang digunakan untuk menyerang maka semakin berat proses bagi penyerang untuk dapat mengirimkan flood paket data tersebut hingga sampai ke target dan berat pula proses bagi yang diserang untuk dapat paket tersebut diterima. Dengan demikian flood paket data membutuhkan waktu yang lebih lama untuk mengirimkan flood paket-paket selanjutnya karena harus menunggu proses pengiriman flood paket-paket sebelumnya hingga selesai. Interval antar flood paket-paket akan menjadi lambat dan tidak tetap dengan semakin besarnya paket data serangan tersebut. Hal inilah yang menyebabkan perbandingannya tidak terlalu signifikan antara paket data serangan 1400KB dengan 2600KB.

4.3.2 Analisis Delay

Delay merupakan waktu keseluruhan yang dibutuhkan ketika paket dikirimkan dari FTP server hingga paket sampai ke FTP client. Analisis data dengan parameter delay ini dilakukan pada saat *Mobile Node* berada di *Home Network* dan mengunduh file, kemudian pindah ke *Foreign Network* dan mengunduh file kembali. Pengukuran tersebut juga dilakukan pada saat

Correspondent Node atau FTP server sebelum dan sesudah diserang. Untuk perhitungan persentase kenaikan delay adalah sebagai berikut.

$$\mu_D = \frac{D_{(Sesudah\ diserang)} - D_{(Sebelum\ diserang)}}{D_{(Sebelum\ diserang)}} \times 100\%$$

μ_D	= Persentase kenaikan delay (%)
$D_{(Sesudah\ diserang)}$	= Delay sesudah diserang (milidetik)
$D_{(Sebelum\ diserang)}$	= Delay sebelum diserang (milidetik)

a. Delay di Home dan di Foreign Network sebelum diserang

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Kemudian *Mobile Node* akan dipindahkan ke *Foreign Network*. Di *Foreign Network* juga *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Data delay dari 10 kali pengunduhan tersebut ditampilkan pada Tabel 4.4 berikut ini.

Tabel 4. 4 Delay pada *Home* dan *Foreign Network* sebelum diserang

Pengujian ke-	Delay di <i>Home Network</i> (milidetik)	Delay di <i>Foreign Network</i> (milidetik)
1	1.95	2.69
2	1.91	3.45
3	1.92	3.57
4	2.77	2.54
5	1.91	2.64
6	2.49	2.61
7	1.75	3.11
8	2.16	2.95
9	2.07	2.71
10	1.76	3.04
Rata-rata	2.07	2.93

Berdasarkan Tabel 4.4 terlihat perbedaan delay pada saat *Mobile Node* berada di *Home Network* dengan *Mobile Node* saat berada di *Foreign Network*. Besar data yang diunduh adalah sama, namun perbedaan delay-nya cukup besar. Hal ini dikarenakan *tunneling* pada topologi jaringan mobile IPv6 yang dipakai pada skripsi ini adalah *bidirectional tunneling*. Delay di *Foreign Network* lebih lama 41.55% dibandingkan dengan delay di *Home Network*. Delay lebih lama pada saat di *Foreign Network* dibandingkan *Home Network* karena dengan *bidirectional tunneling* tukar menukar data antara *Mobile Node* dengan *Correspondent Node* harus selalu melalui *Home Agent*.

b. Delay di *Home Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali dengan keadaan

FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data delay dari 10 kali pengunduhan dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.5 berikut ini.

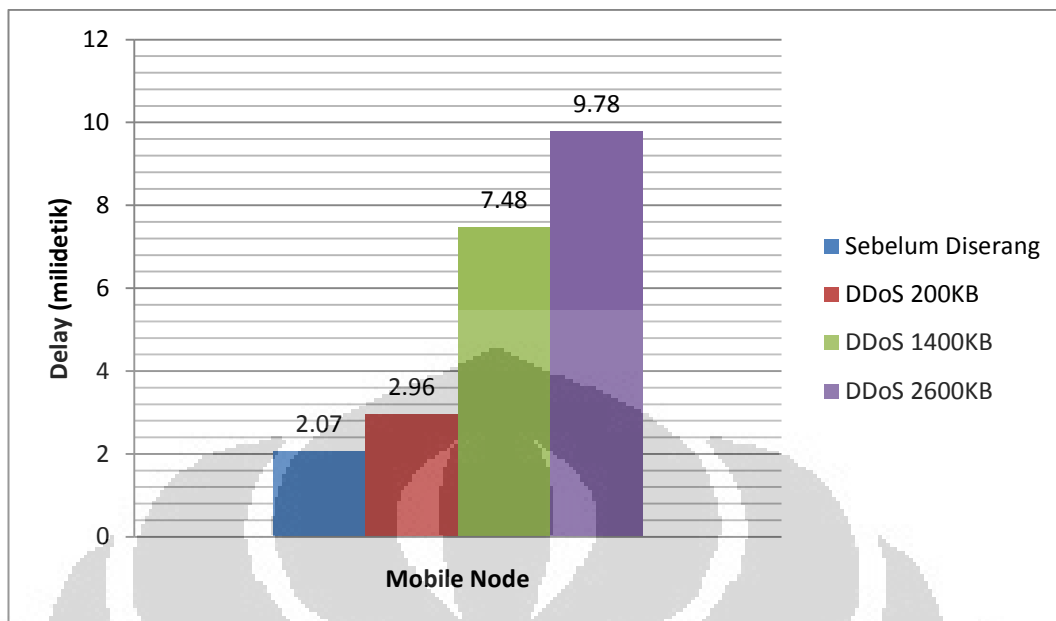
Tabel 4. 5 Delay pada *Home Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Delay di <i>Home Network</i> (milidetik)	Delay saat di-DDoS 200KB (milidetik)	Delay saat di-DDoS 1400KB (milidetik)	Delay saat di-DDoS 2600KB (milidetik)
1	1.95	3.07	10.29	9.86
2	1.91	2.82	5.6	9.36
3	1.92	2.65	7.26	8.32
4	2.77	2.79	8.26	8.59
5	1.91	2.93	9.5	7.59
6	2.49	3.29	6.74	9.43
7	1.75	3.2	5.53	14.95
8	2.16	2.65	8.48	11.34
9	2.07	2.65	6.64	12.72
10	1.76	3.51	6.46	5.69
Rata-rata	2.07	2.96	7.48	9.78

Berdasarkan Tabel 4.5 terlihat perbedaan delay pada saat *Mobile Node* berada di *Home Network* dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan. Besar data yang diunduh

adalah sama, namun perbedaan delay-nya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat delay lebih lama 42.99% dibandingkan delay pengunduhan di *Home Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat delay lebih lama 261.35% dibandingkan delay pengunduhan di *Home Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat delay lebih lama 372.46% dibandingkan delay pengunduhan di *Home Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula delay yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

Gambar 4.7 berikut ini akan menampilkan grafik perbandingan rata-rata delay dari *Mobile Node* saat mengunduh file di *Home Network* sebelum dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan.



Gambar 4.7 Grafik perbandingan delay di *Home Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

c. Delay di *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berpindah ke *Foreign Network* dan terhubung dengan *access point Foreign Network* yang terhubung pada *interface eth1 Foreign Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali dengan keadaan FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data delay dari 10 kali pengunduhan

dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.6 berikut ini.

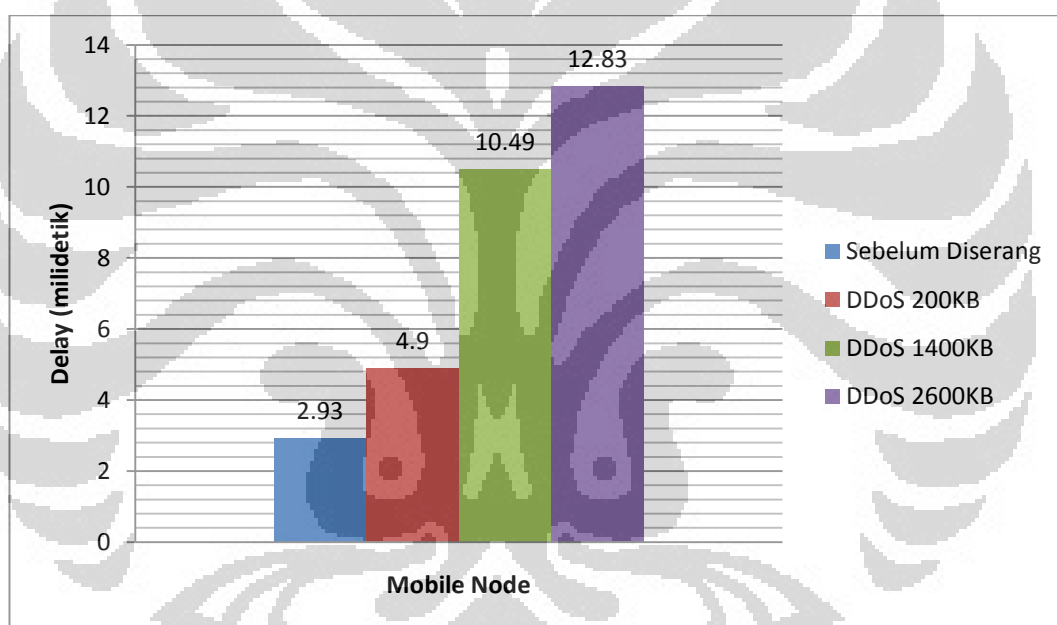
Tabel 4. 6 Delay pada *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Delay di <i>Foreign Network</i> (milidetik)	Delay saat di-DDoS 200KB (milidetik)	Delay saat di-DDoS 1400KB (milidetik)	Delay saat di-DDoS 2600KB (milidetik)
1	2.69	3.8	12.17	13.57
2	3.45	3.53	11.99	13.91
3	3.57	5.05	10.04	16.03
4	2.54	6.18	8.23	14.17
5	2.64	3.87	10.26	15.03
6	2.61	4.85	8.71	13.54
7	3.11	5.69	12.07	11.56
8	2.95	5.77	9.4	9.91
9	2.71	4.33	11.22	10.95
10	3.04	5.95	10.77	9.63
Rata-rata	2.93	4.9	10.49	12.83

Berdasarkan Tabel 4.6 terlihat perbedaan delay pada saat *Mobile Node* berada di *Foreign Network* dan diserang dengan *Distributed Denial of Service* 3 variasi data paket serangan. Besar data yang diunduh adalah sama, namun perbedaan delay-nya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat delay lebih lama 67.23% dibandingkan delay pengunduhan di *Foreign Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat delay lebih lama 258.02% dibandingkan delay pengunduhan di *Foreign Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat delay lebih lama 337.88% dibandingkan delay

pengunduhan di *Foreign Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula delay yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

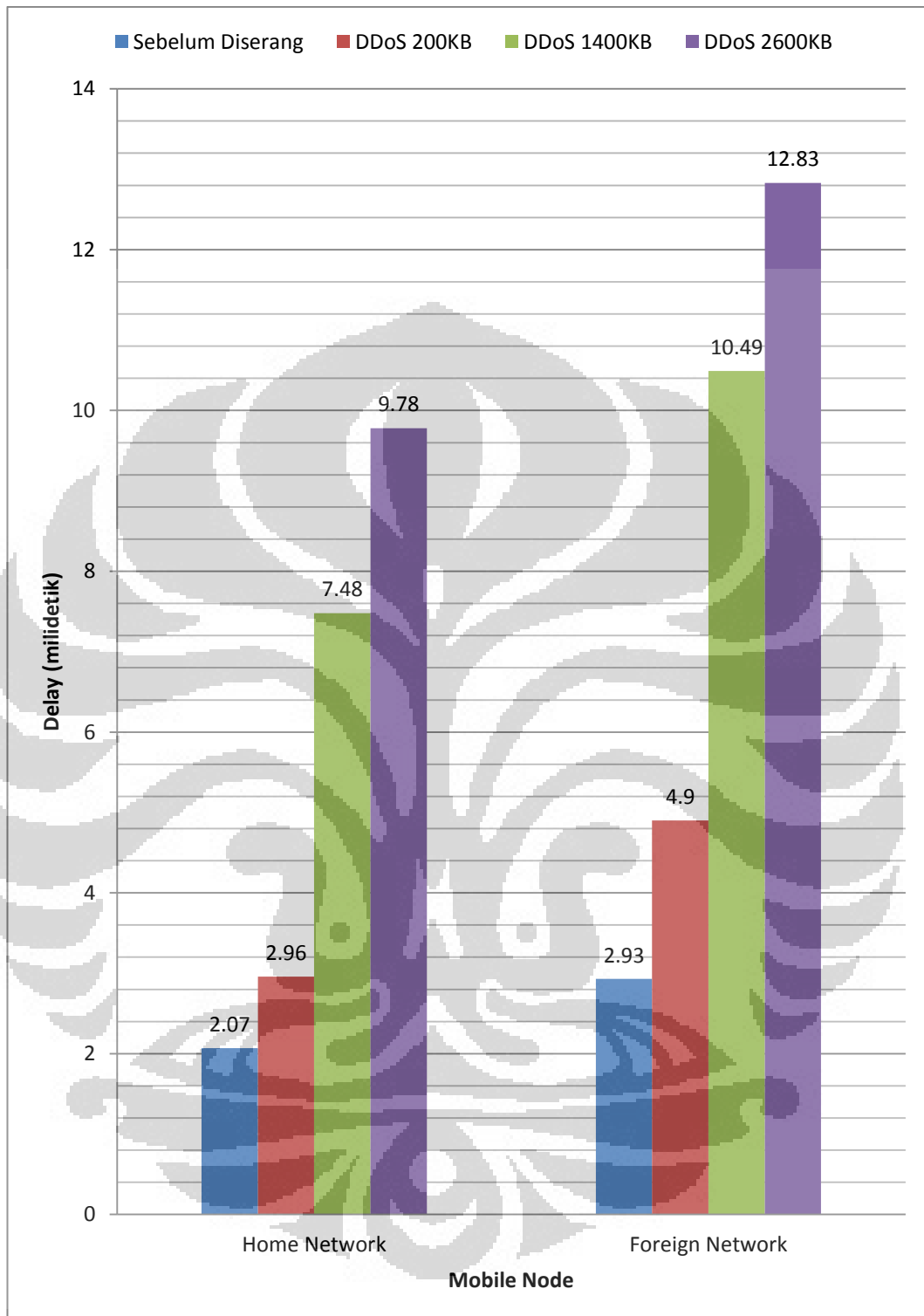
Gambar 4.8 berikut ini akan menampilkan grafik perbandingan rata-rata delay dari *Mobile Node* saat mengunduh file di *Foreign Network* sebelum dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan.



Gambar 4.8 Grafik perbandingan delay di *Foreign Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

d. Perbandingan delay dari seluruh keadaan

Pengujian untuk delay pengunduhan jaringan *bidirectional mobile IPv6* ini telah dilakukan dengan berbagai skenario. Untuk perbandingan lebih terlihat maka perlu penggabungan seluruh grafik data delay dari berbagai skenario tersebut. Gambar 4.9 berikut ini akan menampilkan perbandingan delay dari seluruh keadaan pengujian.



Gambar 4.9 Grafik perbandingan delay seluruh keadaan sebelum dan sesudah diserang

Dari Gambar 4.9 di atas terlihat delay di *Foreign Network* memiliki nilai yang lebih tinggi dibandingkan dengan di *Home Network* saat setelah diserang. Hal ini dikarenakan delay di *Foreign Network* sebelum diserang pun sudah lebih tinggi dibandingkan dengan di *Home Network*. Dengan ditambahnya serangan maka delay pada jaringan ini pun akan semakin bertambah. Pada grafik pun terlihat bahwa semakin besar paket data serangan DDoS maka semakin besar pula delay-nya. Hal ini juga dikarenakan paket data serangan mengacaukan dan membuat jaringan *mobile* ini menjadi lebih sibuk dibandingkan sebelumnya. Dari grafik tersebut juga dapat dilihat perbandingan persentase peningkatan delay paket data serangan 200KB dengan 1400KB berbeda dengan paket data serangan 1400KB dengan 2600KB. Hal ini dikarenakan dengan proses penyerangan ini harus melibatkan kedua belah pihak antara penyerang dan yang diserang. Semakin besar paket data yang digunakan untuk menyerang maka semakin berat proses bagi penyerang untuk dapat mengirimkan flood paket data tersebut hingga sampai ke target dan berat pula proses bagi yang diserang untuk dapat paket tersebut diterima. Dengan demikian flood paket data membutuhkan waktu yang lebih lama untuk mengirimkan flood paket-paket selanjutnya karena harus menunggu proses pengiriman flood paket-paket sebelumnya hingga selesai. Interval antar flood paket-paket akan menjadi lambat dan tidak tetap dengan semakin besarnya paket data serangan tersebut. Hal inilah yang menyebabkan perbandingannya tidak terlalu signifikan antara paket data serangan 1400KB dengan 2600KB.

4.3.3 Analisis Throughput

Throughput merupakan besarnya atau banyaknya paket data yang dapat diterima dalam satuan waktu oleh FTP client dari FTP server. Analisis data dengan parameter throughput ini dilakukan pada saat *Mobile Node* berada di *Home Network* dan mengunduh file, kemudian pindah ke *Foreign Network* dan mengunduh file kembali. Pengukuran tersebut juga dilakukan pada saat

Correspondent Node atau FTP server sebelum dan sesudah diserang. Untuk perhitungan persentase penurunan throughput adalah sebagai berikut.

$$\mu_{Tp} = \frac{Tp_{(Sebelum\ diserang)} - Tp_{(Sesudah\ diserang)}}{Tp_{(Sebelum\ diserang)}} \times 100\%$$

- μ_{Tp} = Persentase penurunan throughput (%)
 $Tp_{(Sesudah\ diserang)}$ = Throughput sesudah diserang (milidetik)
 $Tp_{(Sebelum\ diserang)}$ = Throughput sebelum diserang (milidetik)

a. Throughput di *Home* dan di *Foreign Network* sebelum diserang

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Kemudian *Mobile Node* akan dipindahkan ke *Foreign Network*. Di *Foreign Network* juga *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Data throughput dari 10 kali pengunduhan tersebut ditampilkan pada Tabel 4.7 berikut ini.

Tabel 4. 7 Throughput pada *Home* dan *Foreign Network* sebelum diserang

Pengujian ke-	Throughput di <i>Home Network</i> (KBps)	Throughput di <i>Foreign Network</i> (KBps)
1	774.06	560.336
2	791.85	438.92
3	786.01	424.1
4	545.08	595.82
5	789.9	573.55
6	606.94	578.66
7	863.68	485.84
8	698.89	512.45
9	731.88	557.79
10	856.62	497.23
Rata-rata	744.49	522.47

Berdasarkan Tabel 4.7 terlihat perbedaan throughput pada saat *Mobile Node* berada di *Home Network* dengan *Mobile Node* saat berada di *Foreign Network*. Besar data yang diunduh adalah sama, namun perbedaan throughput-nya cukup besar. Hal ini dikarenakan tunneling pada topologi jaringan *mobile IPv6* yang dipakai pada skripsi ini adalah *bidirectional tunneling*. Throughput di *Foreign Network* lebih kecil 29.82% dibandingkan dengan throughput di *Home Network*. Throughput lebih kecil pada saat di *Foreign Network* dibandingkan *Home Network* karena dengan *bidirectional tunneling* tukar menukar data antara *Mobile Node* dengan *Correspondent Node* harus selalu melalui *Home Agent*.

b. Throughput di *Home Network* dengan serangan **Distributed Denial of Service**

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari

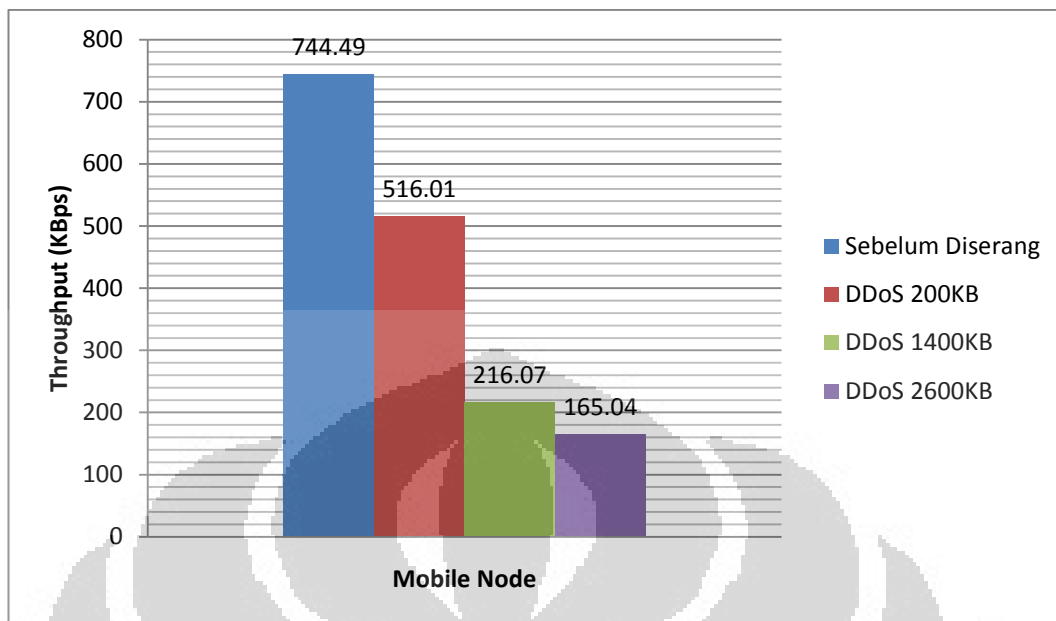
Correspondent Node atau FTP server sebanyak 10 kali dengan keadaan FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data throughput dari 10 kali pengunduhan dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.8 berikut ini.

Tabel 4. 8 Throughput pada *Home Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Throughput di <i>Home Network</i> (KBps)	Throughput saat di-DDoS 200KB (KBps)	Throughput saat di-DDoS 1400KB (KBps)	Throughput saat di-DDoS 2600KB (KBps)
1	774.06	494.85	146.85	153.29
2	791.85	535.9	270.02	161.11
3	786.01	571.1	208.22	181.64
4	545.08	540.79	238.84	176.23
5	789.9	515.23	159.17	199.34
6	606.94	459.07	224.24	160.53
7	863.68	472.42	273.27	100.99
8	698.89	570.07	178.41	133.28
9	731.88	570.1	227.62	118.68
10	856.62	430.58	234.05	265.31
Rata-rata	744.49	516.01	216.07	165.04

Berdasarkan Tabel 4.8 terlihat perbedaan throughput pada saat *Mobile Node* berada di *Home Network* dan diserang dengan *Distributed Denial of Service* 3 variasi data paket serangan. Besar data yang diunduh adalah sama, namun perbedaan throughput-nya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat throughput lebih kecil 34.72% dibandingkan throughput pengunduhan di *Home Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat throughput lebih kecil 70.98% dibandingkan throughput pengunduhan di *Home Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat throughput lebih kecil 77.83% dibandingkan throughput pengunduhan di *Home Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula throughput yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

Gambar 4.10 berikut ini akan menampilkan grafik perbandingan rata-rata throughput dari *Mobile Node* saat mengunduh file di *Home Network* sebelum dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan.



Gambar 4.10 Grafik perbandingan throughput di *Home Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

c. Throughput di *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berpindah ke *Foreign Network* dan terhubung dengan *access point Foreign Network* yang terhubung pada *interface eth1 Foreign Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali dengan keadaan FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data throughput dari 10 kali pengunduhan

dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.14 berikut ini.

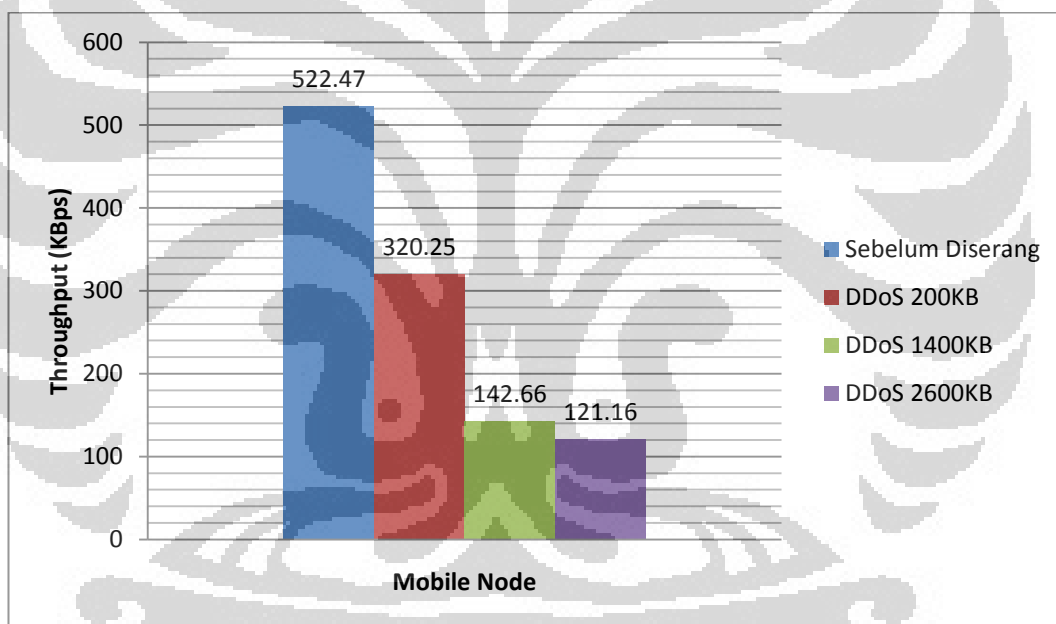
Tabel 4. 9 Throughput pada *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Throughput di <i>Foreign Network</i> (KBps)	Throughput saat di-DDoS 200KB (KBps)	Throughput saat di-DDoS 1400KB (KBps)	Throughput saat di-DDoS 2600KB (KBps)
1	560.336	397.87	124.25	111.41
2	438.92	428.41	125.98	108.63
3	424,1	299.24	150.46	94.27
4	595.82	244.56	183.55	106.67
5	573.55	390.09	147.27	100.48
6	578.66	311.43	173.29	111.68
7	485.84	265.63	125.08	130.86
8	512.45	262.03	160.54	152.6
9	557.79	348.99	95.82	137.91
10	497.23	254.25	140.39	157.06
Rata-rata	522.47	320.25	142.66	121.157

Berdasarkan Tabel 4.9 terlihat perbedaan throughput pada saat *Mobile Node* berada di *Foreign Network* dan diserang dengan *Distributed Denial of Service* 3 variasi data paket serangan. Besar data yang diunduh adalah sama, namun perbedaan throughput-nya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat throughput lebih kecil 38.7% dibandingkan throughput pengunduhan di *Foreign Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat throughput lebih kecil 72.69% dibandingkan throughput pengunduhan di *Foreign Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat throughput lebih kecil

76.81% dibandingkan throughput pengunduhan di *Foreign Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula throughput yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

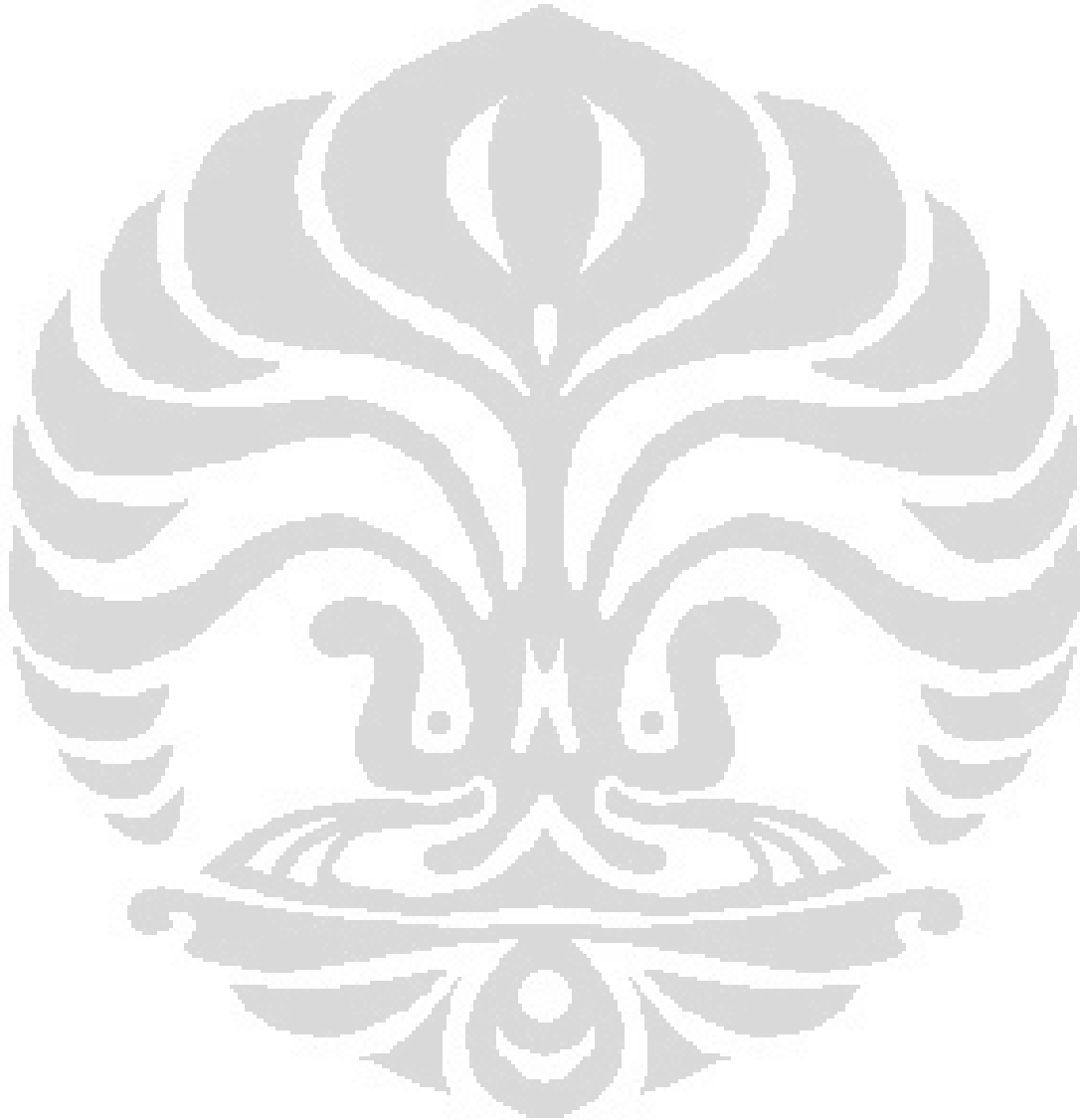
Gambar 4.11 berikut ini akan menampilkan grafik perbandingan rata-rata throughput dari *Mobile Node* saat mengunduh file di *Foreign Network* sebelum dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan.

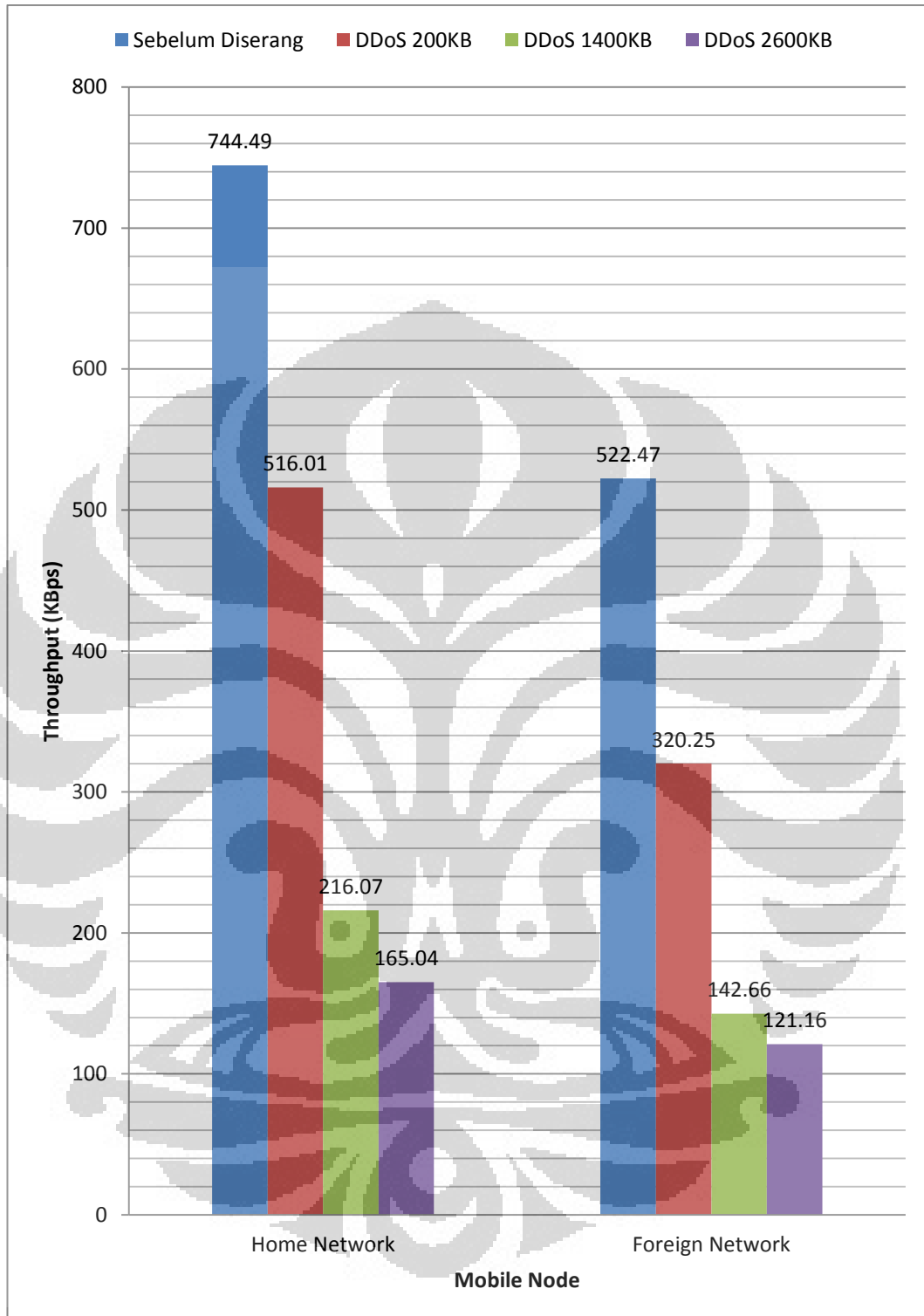


Gambar 4.11 Grafik perbandingan throughput di *Foreign Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

d. Perbandingan throughput dari seluruh keadaan

Pengujian untuk throughput pengunduhan *jaringan bidirectional mobile* IPv6 ini telah dilakukan dengan berbagai skenario. Untuk perbandingan lebih terlihat maka perlu penggabungan seluruh grafik data throughput dari berbagai skenario tersebut. Gambar 4.12 berikut ini akan menampilkan perbandingan throughput dari seluruh keadaan pengujian.





Gambar 4.12 Grafik perbandingan throughput seluruh keadaan sebelum dan sesudah diserang

Dari Gambar 4.12 diatas terlihat throughput di *Foreign Network* memiliki nilai yang lebih kecil dibandingkan dengan di *Home Network* saat setelah diserang. Hal ini dikarenakan throughput di *Foreign Network* sebelum diserang pun sudah lebih kecil dibandingkan dengan di *Home Network*. Dengan ditambahnya serangan maka throughput pada jaringan ini pun akan semakin bertambah. Pada grafik pun terlihat bahwa semakin besar paket data serangan DDoS maka semakin besar pula throughput-nya. Hal ini juga dikarenakan paket data serangan mengacaukan dan membuat jaringan *mobile* ini menjadi lebih sibuk dibandingkan sebelumnya. Dari grafik tersebut juga dapat dilihat perbandingan persentase penurunan throughput paket data serangan 200KB dengan 1400KB berbeda dengan paket data serangan 1400KB dengan 2600KB. Hal ini dikarenakan dengan proses penyerangan ini harus melibatkan kedua belah pihak antara penyerang dan yang diserang. Semakin besar paket data yang digunakan untuk menyerang maka semakin berat proses bagi penyerang untuk dapat mengirimkan flood paket data tersebut hingga sampai ke target dan berat pula proses bagi yang diserang untuk dapat paket tersebut diterima. Dengan demikian flood paket data membutuhkan waktu yang lebih lama untuk mengirimkan flood paket-paket selanjutnya karena harus menunggu proses pengiriman flood paket-paket sebelumnya hingga selesai. Interval antar flood paket-paket akan menjadi lambat dan tidak tetap dengan semakin besarnya paket data serangan tersebut. Hal inilah yang menyebabkan perbandingannya tidak terlalu signifikan antara paket data serangan 1400KB dengan 2600KB.

4.3.4 Analisis Packet Loss

Packet Loss merupakan banyaknya paket yang hilang selama pengiriman dari FTP server ke FTP client. Analisis data dengan parameter packet loss ini dilakukan pada saat *Mobile Node* berada di *Home Network* dan mengunduh file, kemudian pindah ke *Foreign Network* dan mengunduh file kembali. Pengukuran tersebut juga dilakukan pada saat *Correspondent Node* atau FTP server sebelum

dan sesudah diserang. Untuk perhitungan persentase kenaikan packet loss adalah sebagai berikut.

$$\mu_{PL} = \frac{PL_{(Sesudah\ diserang)} - PL_{(Sebelum\ diserang)}}{PL_{(Sebelum\ diserang)}} \times 100\%$$

μ_{PL} = Persentase kenaikan packet loss (%)

$PL_{(Sesudah\ diserang)}$ = Packet loss sesudah diserang

$PL_{(Sebelum\ diserang)}$ = Packet loss sebelum diserang

a. Packet loss di Home dan di Foreign Network sebelum diserang

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Kemudian *Mobile Node* akan dipindahkan ke *Foreign Network*. Di *Foreign Network* juga *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali. Data packet loss dari 10 kali pengunduhan tersebut ditampilkan pada Tabel 4.11 berikut ini.

Tabel 4. 10 Packet loss pada *Home* dan *Foreign Network* sebelum diserang

Pengujian ke-	Packet loss di <i>Home Network</i>	Packet loss di <i>Foreign Network</i>
1	13	39
2	10	3
3	5	14
4	24	2
5	1	39
6	3	52
7	0	25
8	5	8
9	10	46
10	0	51
Rata-rata	7.1	27.9

Berdasarkan Tabel 4.11 terlihat perbedaan packet loss pada saat *Mobile Node* berada di *Home Network* dengan *Mobile Node* saat berada di *Foreign Network*. Besar data yang diunduh adalah sama, namun perbedaan packet loss-nya cukup besar. Hal ini dikarenakan *tunneling* pada topologi jaringan mobile IPv6 yang dipakai pada skripsi ini adalah *bidirectional tunneling*. Packet loss di *Foreign Network* lebih banyak 292.96% dibandingkan dengan packet loss di *Home Network*. Packet loss lebih banyak pada saat di *Foreign Network* dibandingkan *Home Network* karena dengan *bidirectional tunneling* tukar menukar data antara *Mobile Node* dengan *Correspondent Node* harus selalu melalui *Home Agent*.

b. Packet loss di *Home Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berada pada *Home Network* dan terhubung dengan *access point Home Network* yang terhubung pada *interface eth1 Home Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari

Correspondent Node atau FTP server sebanyak 10 kali dengan keadaan FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data packet loss dari 10 kali pengunduhan dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.12 berikut ini.

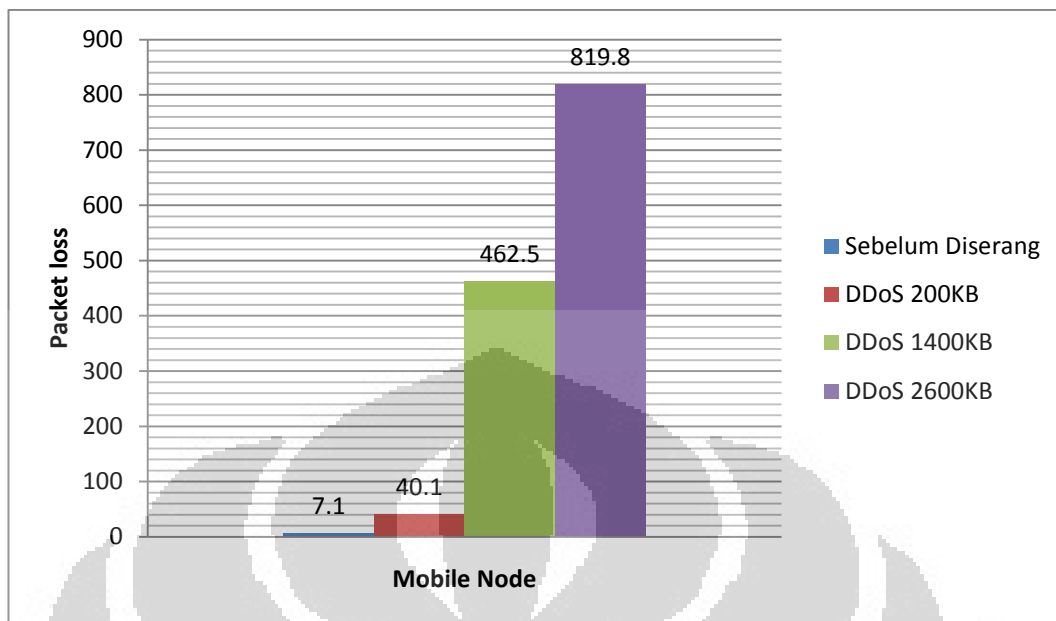
Tabel 4. 11 Packet loss pada *Home Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Packet loss di <i>Home Network</i>	Packet loss saat di-DDoS 200KB	Packet loss saat di-DDoS 1400KB	Packet loss saat di-DDoS 2600KB
1	13	26	486	504
2	10	10	110	836
3	5	8	477	413
4	24	78	374	743
5	1	24	624	981
6	3	35	500	788
7	0	111	543	1383
8	5	10	611	1246
9	10	9	389	848
10	0	90	511	456
Rata-rata	7.1	40.1	462.5	819.8

Berdasarkan Tabel 4.12 terlihat perbedaan packet loss pada saat *Mobile Node* berada di *Home Network* dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan. Besar data yang

diunduh adalah sama, namun perbedaan packet loss-nya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat packet loss lebih banyak 464.79% dibandingkan packet loss pengunduhan di *Home Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat packet loss lebih banyak 6414.08% dibandingkan packet loss pengunduhan di *Home Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat packet loss lebih banyak 11446.48% dibandingkan packet loss pengunduhan di *Home Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula packet loss yang dihasilkan. Hal ini dikarenakan dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

Gambar 4.13 berikut ini akan menampilkan grafik perbandingan rata-rata packet loss dari *Mobile Node* saat mengunduh file di *Home Network* sebelum dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan.



Gambar 4. 13 Grafik perbandingan packet loss di *Home Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

c. Packet loss di *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengambilan data untuk keadaan seperti ini dilakukan ketika *Mobile Node* berpindah ke *Foreign Network* dan terhubung dengan *access point Foreign Network* yang terhubung pada *interface eth1 Foreign Agent*. Kemudian *Mobile Node* akan mengunduh file *file.tar.gz* dari *Correspondent Node* atau FTP server sebanyak 10 kali dengan keadaan FTP server diserang dengan *Distributed Denial of Service*. Tiga laptop telah didistribusikan program untuk melakukan serangan flood paket data, sehingga tiga komputer tersebut menyerang bersamaan. Paket data untuk serangan divariasikan, yaitu 200KB, 1400KB, dan 2600KB. Masing-masing variasi besar paket data untuk serangan dilakukan sebanyak 10 kali pengujian. Serangan menggunakan thread yang berjumlah sama pada setiap variasi, yaitu 6 thread tiap laptop yang didistribusikan program untuk melakukan serangan. Laptop-laptop tersebut terhubung dengan jaringan pada *Foreign Network*. Data packet loss dari 10 kali pengunduhan dengan keadaan FTP server diserang dengan *Distributed Denial of Service* ditampilkan pada Tabel 4.6 berikut ini.

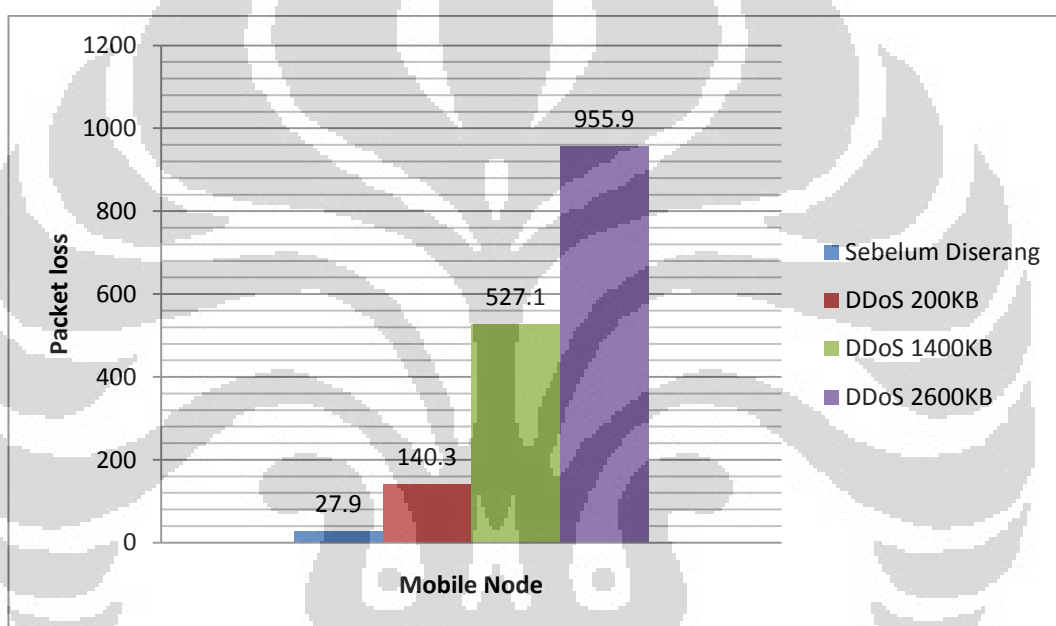
Tabel 4. 12 Packet loss pada *Foreign Network* dengan serangan *Distributed Denial of Service*

Pengujian ke-	Packet loss di <i>Foreign Network</i>	Packet loss saat di-DDoS 200KB	Packet loss saat di-DDoS 1400KB	Packet loss saat di-DDoS 2600KB
1	39	138	478	1384
2	3	86	639	1247
3	14	11	680	982
4	2	137	504	849
5	39	140	624	837
6	52	251	611	789
7	25	187	331	744
8	8	107	340	625
9	46	146	524	1250
10	51	200	540	852
Rata-rata	27.9	140.3	527.1	955.9

Berdasarkan Tabel 4.13 terlihat perbedaan packet loss pada saat *Mobile Node* berada di *Foreign Network* dan diserang dengan *Distributed Denial of Service* 3 variasi data paket serangan. Besar data yang diunduh adalah sama, namun perbedaan packet loss-nya cukup terlihat. DDoS dengan besar paket data serangan 200KB dari tiga komputer dan masing-masing 6 thread membuat packet loss lebih banyak 402.87% dibandingkan packet loss pengunduhan di *Foreign Network* sebelum diserang. DDoS dengan besar paket data serangan 1400KB dari tiga komputer dan masing-masing 6 thread membuat packet loss lebih banyak 1789.25% dibandingkan packet loss pengunduhan di *Foreign Network* sebelum diserang. Sedangkan DDoS dengan besar paket data serangan 2600KB dari tiga komputer dan masing-masing 6 thread membuat packet loss lebih banyak 3326.16% dibandingkan packet loss pengunduhan di *Foreign Network* sebelum diserang. Semakin besar paket data serangan maka semakin lama pula packet loss yang dihasilkan. Hal ini dikarenakan

dengan paket data serangan yang besar maka bandwidth pada penjaluran *Mobile Node* dengan *Correspondent Node* dipenuhi trafik serangan yang besar juga sehingga jaringan akan dikacaukan dan lebih sibuk dibandingkan sebelumnya.

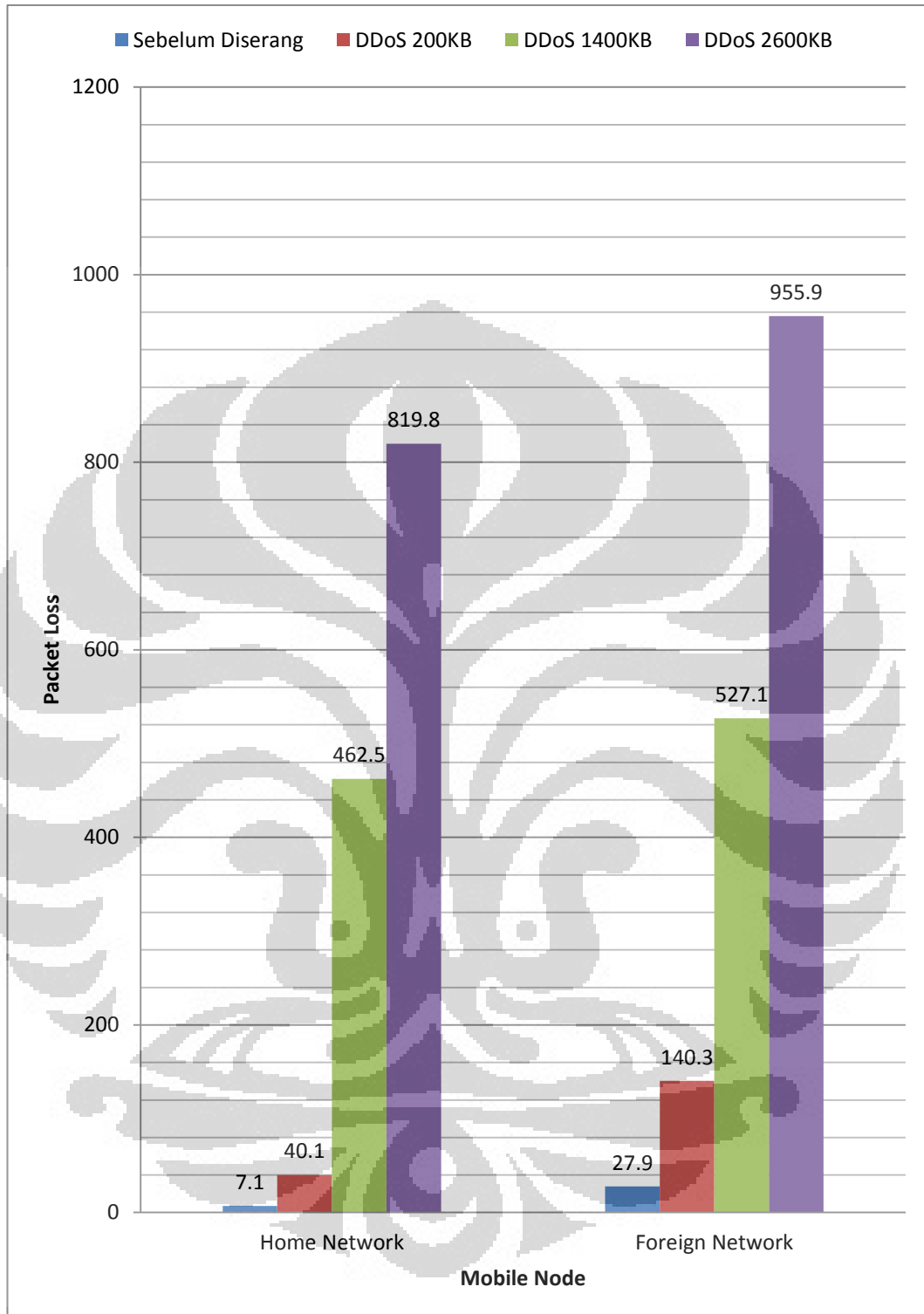
Gambar 4.14 berikut ini akan menampilkan grafik perbandingan rata-rata packet loss dari *Mobile Node* saat mengunduh file di *Foreign Network* sebelum dan diserang dengan *Distributed Denial of Service* 3 variasi besar paket data serangan.



Gambar 4. 14 Grafik perbandingan packet loss di *Foreign Network* sebelum dan sesudah diserang dengan *Distributed Denial of Service*

d. Perbandingan packet loss dari seluruh keadaan

Pengujian untuk packet loss pengunduhan jaringan *bidirectional mobile IPv6* ini telah dilakukan dengan berbagai skenario. Untuk perbandingan lebih terlihat maka perlu penggabungan seluruh grafik data packet loss dari berbagai skenario tersebut. Gambar 4.15 berikut ini akan menampilkan perbandingan packet loss dari seluruh keadaan pengujian.



Gambar 4. 15 Grafik perbandingan packet loss seluruh keadaan sebelum dan sesudah diserang

Dari Gambar 4.15 diatas terlihat packet loss di *Foreign Network* memiliki nilai yang lebih tinggi dibandingkan dengan di *Home Network* saat setelah diserang. Hal ini dikarenakan packet loss di *Foreign Network* sebelum diserang pun sudah lebih tinggi dibandingkan dengan di *Home Network*. Dengan ditambahnya serangan maka packet loss pada jaringan ini pun akan semakin bertambah. Pada grafik pun terlihat bahwa semakin besar paket data serangan DDoS maka semakin besar pula packet loss-nya. Hal ini juga dikarenakan paket data serangan mengacaukan dan membuat jaringan *mobile* ini menjadi lebih sibuk dibandingkan sebelumnya. Dari grafik tersebut juga dapat dilihat perbandingan persentase peningkatan packet loss paket data serangan 200KB dengan 1400KB berbeda dengan paket data serangan 1400KB dengan 2600KB. Hal ini dikarenakan dengan proses penyerangan ini harus melibatkan kedua belah pihak antara penyerang dan yang diserang. Semakin besar paket data yang digunakan untuk menyerang maka semakin berat proses bagi penyerang untuk dapat mengirimkan flood paket data tersebut hingga sampai ke target dan berat pula proses bagi yang diserang untuk dapat paket tersebut diterima. Dengan demikian flood paket data membutuhkan waktu yang lebih banyak untuk mengirimkan flood paket-paket selanjutnya karena harus menunggu proses pengiriman flood paket-paket sebelumnya hingga selesai. Interval antar flood paket-paket akan menjadi lambat dan tidak tetap dengan semakin besarnya paket data serangan tersebut. Hal inilah yang menyebabkan perbandingannya tidak terlalu signifikan antara paket data serangan 1400KB dengan 2600KB.

BAB 5

KESIMPULAN

Berdasarkan hasil pengujian serta analisis performansi aplikasi FTP pada topologi jaringan *bidirectional mobile* IPv6 ini yang diserang maka dapat disimpulkan bahwa:

1. Transfer time di *Home Network* sebelum diserang lebih cepat 42.30% dibandingkan di *Foreign Network*. Di *Home Network* saat diserang DDoS 200KB, 1400KB, dan 2600KB kenaikannya adalah 40.89%, 246.98%, dan 392.78%. Sedangkan di *Foreign Network* kenaikannya adalah 65.71%, 256.04%, dan 337.14%.
2. Delay di *Home Network* sebelum diserang lebih cepat 41.55% dibandingkan di *Foreign Network*. Di *Home Network* saat diserang DDoS 200KB, 1400KB, dan 2600KB kenaikannya adalah 42.99%, 261.35%, dan 372.46%. Sedangkan di *Foreign Network* kenaikannya adalah 67.23%, 258.02%, dan 337.88%.
3. Throughput di *Home Network* sebelum diserang lebih besar 29.82% dibandingkan di *Foreign Network*. Di *Home Network* saat diserang DDoS 200KB, 1400KB, dan 2600KB penurunannya adalah 34.72%, 70.98%, dan 77.83%. Sedangkan di *Foreign Network* adalah 38.7%, 72.69%, dan 76.81%.
4. Packet loss di *Home Network* sebelum diserang lebih banyak 292.96% dibandingkan di *Foreign Network*. Di *Home Network* saat diserang DDoS 200KB, 1400KB, dan 2600KB kenaikannya adalah 464.79%, 6414.08%, dan 11446.48%. Sedangkan di *Foreign Network* kenaikannya adalah 402.87%, 1789.25%, dan 3326.16%.
5. Transfer time, delay, throughput, dan packet loss yang didapatkan memiliki perbedaan persentase antara paket data serangan 200KB dengan 1400KB dan 1400KB dengan 2600KB karena semakin besar paket data serangan maka semakin lama pengiriman flood paket data akibat pemrosesan yang semakin berat juga pada penyerang dan target. Hal tersebut yang menyebabkan perbedaan persentase flood paket data 1400KB dengan 2600KB tidak terlalu signifikan dibandingkan 200KB dengan 1400KB meskipun masing-masing memiliki kesamaan selisih flood paket data 1200KB.

DAFTAR REFERENSI

- [1] Cisco Systems, Inc. *Cisco IOS IP Configuration Guide*. San Jose: Cisco Systems, Inc., 2006.
- [2] kumarasamy, Saravanan, dan Dr.R.Asokan. *DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS DETECTION MECHANISM*. Kongu: IJCSEIT, 2011.
- [3] Lammle, Todd. *CCNA Cisco Certified Network Associate Study Guide 6th Edition*. Indiana: Wiley Publishing, Inc., 2007.
- [4] MALEKIAN, Reza, dan Abdul Hanan ABDULLAH. *Bidirectional and RO Methods for Analysis of Stream-Intensive Applications over Mobile IP Network*. Johor: PRZEGLĄD ELEKTROTECHNICZNY (Electrical Review), ISSN 0033-2097, R. 88 NR 3b/2012, 2012.
- [5] Moravejosharieh, Amirhossein, Hero Modares, dan Rosli Salleh. *Overview of Mobile IPv6 Security*. Kota Kinabalu: IEEE Conference Publications Page(s): 584 - 587, Intelligent Systems, Modelling and Simulation (ISMS), 2012 Third International Conference on, 10.1109/ISMS.2012.9 , 2012.
- [6] Pilihanto, Atik. *A Complete Guide on IPv6 Attack and Defense*. The SANS Institute, 2011.
- [7] Postel, J., dan J. Reynolds. *FILE TRANSFER PROTOCOL (FTP)*. Oktober 1985. <http://www.ietf.org/rfc/rfc959.txt> (diakses Mei 2013).
- [8] Specht, Stephen M., dan Ruby B. Lee. *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures*. International Workshop on Security in Parallel and Distributed Systems, 2004.
- [9] Sudanthi, Sudha. *Mobile IPv6*. SANS Institute InfoSec Reading Room, 2003.

LAMPIRAN 1

KONFIGURASI KERNEL DAN UMIP

1.1 Pengunduhan kernel

```

# cd /usr/src/
# wget http://www.kernel.org/pub/linux/kernel/v3.x/linux-3.8.2.tar.bz2

# wget http://www.kernel.org/pub/linux/kernel/v3.x/linux-3.8.2.tar.sign
# bunzip2 linux-3.8.2.tar.bz2
# gpg --keyserver wwwkeys.pgp.net --recv-keys 0x6092693E
# gpg --verify linux-3.8.2.tar.sign
gpg: Signature made Sun Mar  3 23:04:31 2013 CET using RSA key ID 6092693E
gpg: Good signature from "Greg Kroah-Hartman (Linux kernel stable release signing key) [...]"

# tar xf linux-3.8.2.tar
# ln -s /usr/src/linux-3.8.2/ /usr/src/linux
# cd linux-3.8.2/

# apt-get install libncurses5-dev

# make menuconfig

General setup
--> Prompt for development and/or incomplete code/drivers [CONFIG_EXPERIMENTAL]
--> System V IPC [CONFIG_SYSVIPC]

Networking support [CONFIG_NET]
--> Networking options
--> Transformation user configuration interface [CONFIG_XFRM_USER]
--> Transformation sub policy support [CONFIG_XFRM_SUB_POLICY]
--> Transformation migrate database [CONFIG_XFRM_MIGRATE]
--> PF_KEY sockets [CONFIG_NET_KEY]
--> PF_KEY MIGRATE [CONFIG_NET_KEY_MIGRATE]
--> TCP/IP networking [CONFIG_INET]
--> The IPv6 protocol [CONFIG_IPV6]
--> IPv6: AH transformation [CONFIG_INET6_AH]
--> IPv6: ESP transformation [CONFIG_INET6_ESP]
--> IPv6: IPComp transformation [CONFIG_INET6_IPCOMP]
--> IPv6: Mobility [CONFIG_IPV6_MIP6]
--> IPv6: IPsec transport mode [CONFIG_INET6_XFRM_MODE_TRANSPORT]
--> IPv6: IPsec tunnel mode [CONFIG_INET6_XFRM_MODE_TUNNEL]
--> IPv6: MIPv6 route optimization mode [CONFIG_INET6_XFRM_MODE_ROUTEOPTIMIZATION]
--> IPv6: IPv6-in-IPv6 tunnel [CONFIG_IPV6_TUNNEL]
--> IPv6: Multiple Routing Tables [CONFIG_IPV6_MULTIPLE_TABLES]
--> IPv6: source address based routing [CONFIG_IPV6_SUBTREES]

```

```
File systems
--> Pseudo filesystems
    --> /proc file system support [CONFIG_PROC_FS]

# make
# make install
# make modules_install
# make headers_install
```

1.2 Penginstalan UMIP

```
# apt-get install autoconf automake bison flex libssl-dev indent
ipsec-tools radvd

$ cd /usr/src/
$ git clone git://git.umip.org/umip.git
$ cd umip/

$ autoreconf -i
$ CPPFLAGS='-isystem /usr/src/linux/usr/include/' ./configure --
enable-vt
$ make
# make install
```

1.3 Program init.d mip6d

```
#!/bin/sh

# Copyright (C) 2006, 2007 USAGI/WIDE Project. All rights reserved.
# Adapted by Martin Andre <andre@hongo.wide.ad.jp>
# Further modified by Arnaud Ebalard <arno@natisbad.org>

### BEGIN INIT INFO
# Provides:          mip6d
# Required-Start:   $network $syslog
# Required-Stop:    $network $syslog
# Should-Start:     $local_fs
# Should-Stop:      $local_fs
# Default-Start:    2 3 4 5
# Default-Stop:     0 1 6
# Short-Description: Start/Stop MIPv6 Daemon (UMIP)
# Description:      (empty)
### END INIT INFO

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

DESC="UMIP daemon"
NAME=mip6d
MIP6D=/usr/sbin/mip6d
MIP6D_CONF=/etc/mip6d.conf
MIP6D_DEBUG_LOG=/var/log/mip6d.log
PIDFILE=/var/run/mip6d.pid
FORCE_IPV6_FORWARDING="no"
RUN="no"

. /lib/lsb/init-functions

DIETIME=1

# Include defaults if available
```

```

if [ -f /etc/default/$NAME ] ; then
    . /etc/default/$NAME
fi

if [ "x$RUN" != "xyes" ] ; then
    log_failure_msg "$NAME disabled, please adjust the configuration
to your needs"
    log_failure_msg "and then set RUN to 'yes' in /etc/default/$NAME
to enable it."
    exit 1
fi

if [ ! -e $MIP6D_CONF ]; then
    log_failure_msg "ERROR: $MIP6D_CONF does not exist."
    log_failure_msg "    See mip6d.conf(5) for configuration file
syntax and"
    log_failure_msg "    sample configuration elements."
    log_failure_msg "    => $DESC will not be started"
    exit 0
fi

if [ ! -x $MIP6D ]; then
    log_failure_msg "ERROR: While trying to start $DESC, found its
binary was"
    log_failure_msg "    missing ($MIP6D)."
    log_failure_msg "    => $DESC will not be started"
    exit 0
fi

if [ ! -e /proc/sys/net/ipv6 ]; then
    log_failure_msg "ERROR: In-kernel IPv6 is required for $DESC to
work."
    log_failure_msg "    => $DESC will not be started."
    exit 0
fi

set -e

MIP6D_OPTS="-c ${MIP6D_CONF}"
if [ "x"$MIP6D_DEBUG_LOG" != x"" ]; then
    MIP6D_OPTS="${MIP6D_OPTS} -l ${MIP6D_DEBUG_LOG}"
fi

post_war_cleaning()
{
    # clean-up XFRM (BCE/BUL)
    for t in sub main; do
        ip xfrm policy flush ptype ${t} > /dev/null 2>&1 || true
    done

    for p in esp ah comp route2 hao; do
        ip xfrm state flush proto ${p} > /dev/null 2>&1 || true
    done

    # clean-up tunnel device
    tnls=`ifconfig -a | awk '/^ip6tnl/ { print $1 }'`
    for tnl in $tnls; do
        ip -6 tunnel del $tnl > /dev/null 2>&1 || true
    done

    # clean-up neighbor cache

```

```

    devices=`ip link 2>&1 | grep '^[0-9]' | awk '{print $2}' | sed -e
's/:$//'\`
    for dev in $devices; do
        ip neigh flush dev $dev > /dev/null 2>&1 || true
    done

    return 0
}

case "$1" in
start)
    echo -n "Starting MIP6D: "
    PID=x`pgrep -f $MIP6D || true`
    if [ "${PID}" != "x" ] ; then
        echo "failed (already started)."
        exit 0
    fi
    if [ x"$FORCE_IPV6_FORWARDING" = x"yes" ]; then
        echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
    fi
    start-stop-daemon --start --quiet --exec ${MIP6D} --
${MIP6D_OPTS}
    echo "done."
    ;;
stop)
    echo -n "Stopping MIP6D: "
    PID=x`pgrep -f $MIP6D || true`
    if [ "${PID}" = "x" ] ; then
        echo "done (none found)."
        exit 0
    fi

    # Be nice ...
    HOW=""
    pkill -f ${MIP6D}
    sleep $DIETIME

    # Hum, you did not understand. Louder ...
    PID=x`pgrep -f $MIP6D || true`
    if [ "${PID}" != "x" ] ; then
        pkill -TERM -f ${MIP6D} || true
        sleep $DIETIME
        PID=x`pgrep -f $MIP6D || true`
        if [ "${PID}" != "x" ] ; then
            post_war_cleaning
        fi
        HOW=" (TERMinated)"
    fi

    # Ok, go to hell ...
    PID=x`pgrep -f $MIP6D || true`
    if [ "${PID}" != "x" ] ; then
        pkill -KILL -f ${MIP6D} || true
        sleep $DIETIME
        post_war_cleaning
        HOW=" (KILLed)"
        exit 0
    fi

    echo "done.${HOW}"

```

```
;;

reload)
    echo -n "Reloading MIP6D: "
    pkill -HUP -f ${MIP6D} || true
    echo "done."
    ;;

restart|force-reload)
    $0 stop
    $0 start
    ;;

status)
    status=" NOT"
    PID=x`pgrep -f $MIP6D || true`
    if [ "${PID}" != "x" ] ; then
        status=""
    fi
    echo "${DESC} (${NAME}) is${status} running."
    exit 0
    ;;

*)
    N=/etc/init.d/$NAME
    echo "Usage: $N {start|stop|restart|force-reload|status}" >&2
    exit 1
    ;;
esac
exit 0
```

LAMPIRAN 2

KONFIGURASI *HOME AGENT* & *HOME ROUTER*

2.1 Konfigurasi Interface *Home Agent*

```
# ifconfig eth1 inet6 add 2001:db8:ffff:100a::1/64
# ifconfig eth0 inet6 add 2001:db8:ffff:100b::11/64
```

2.2 Konfigurasi static routing

```
# ip route add 2001:db8:ffff:100c::/64 via 2001:db8:ffff:100b::12
```

2.3 Konfigurasi beberapa fungsi pada *home router*

```
# iwconfig eth1 mode ad-hoc essid homenet enc off
# echo "1" > /proc/sys/net/ipv6/conf/eth1/forwarding
# echo "0" > /proc/sys/net/ipv6/conf/eth1/autoconf
# echo "0" > /proc/sys/net/ipv6/conf/eth1/accept_ra
# echo "0" > /proc/sys/net/ipv6/conf/eth1/accept_redirects
# iwconfig eth0 mode ad-hoc essid homenet enc off
# echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
# echo "0" > /proc/sys/net/ipv6/conf/all/autoconf
# echo "0" > /proc/sys/net/ipv6/conf/all/accept_ra
# echo "0" > /proc/sys/net/ipv6/conf/all/accept_redirects
```

2.4 Konfigurasi *mip6d.conf* pada *Home Agent*

```
NodeConfig HA;

# Set DebugLevel to 0 if you do not want debug messages
DebugLevel 10;

# Replace eth1 with the interface connected to the home link
Interface "eth1";

DoRouteOptimizationCN disabled;

# Binding information
BindingAclPolicy 2001:db8:ffff:100a::100 allow;
DefaultBindingAclPolicy deny;

# Enable IPsec static keying
UseMnHaIPsec enabled;
KeyMngMobCapability disabled;

# IPsec Security Policies information
IPsecPolicySet {
    HomeAgentAddress 2001:db8:ffff:100a::1;
    HomeAddress 2001:db8:ffff:100a::100/64;

    # All MH packets (BU/BA/BERR)
    IPsecPolicy Mh UseESP 10;
    # All tunneled packets (HoTI/HoT, payload)
    # IPsecPolicy TunnelPayload UseESP 11;
    # All ICMP packets (MPS/MPA, ICMPv6)
    # IPsecPolicy ICMP UseESP 15 16;
}
```

2.5 Konfigurasi setkey.conf

```

# IPsec Security Associations
# HA address: 2001:db8:ffff:100a::1;
# MR HoAs:    2001:db8:ffff:100a::100/64;

# Flush the SAD and SPD
flush;
spdflush;

# MN1 -> HA transport SA for BU
add 2001:db8:ffff:100a::100 2001:db8:ffff:100a::1 esp 0x11
    -u 11
    -m transport
    -E 3des-cbc "MIP6-011--12345678901234"
    -A hmac-sha1 "MIP6-011--1234567890" ;

# HA -> MN1 transport SA for BA
add 2001:db8:ffff:100a::1 2001:db8:ffff:100a::100 esp 0x12
    -u 12
    -m transport
    -E 3des-cbc "MIP6-012--12345678901234"
    -A hmac-sha1 "MIP6-012--1234567890" ;

# MN1 -> HA tunnel SA for any traffic
add 2001:db8:ffff:100a::100 2001:db8:ffff:100a::1 esp 0x13
    -u 13
    -m tunnel
    -E 3des-cbc "MIP6-013--12345678901234"
    -A hmac-sha1 "MIP6-013--1234567890" ;

# HA -> MN1 tunnel SA for any traffic
add 2001:db8:ffff:100a::1 2001:db8:ffff:100a::100 esp 0x14
    -u 14
    -m tunnel
    -E 3des-cbc "MIP6-014--12345678901234"
    -A hmac-sha1 "MIP6-014--1234567890" ;

# MN1 -> HA transport SA for ICMP (including MPS/MPA)
add 2001:db8:ffff:100a::100 2001:db8:ffff:100a::1 esp 0x15
    -u 15
    -m transport
    -E 3des-cbc "MIP6-015--12345678901234"
    -A hmac-sha1 "MIP6-015--1234567890" ;

# HA -> MN1 transport SA for ICMP (including MPS/MPA)
add 2001:db8:ffff:100a::1 2001:db8:ffff:100a::100 esp 0x16
    -u 16
    -m transport
    -E 3des-cbc "MIP6-016--12345678901234"
    -A hmac-sha1 "MIP6-016--1234567890" ;

```

2.6 Konfigurasi radvd.conf

```
# Home Agent radvd configuration file
# Replace eth1 with the interface connected to the home link
interface eth1
{
    AdvSendAdvert on;
    MaxRtrAdvInterval 3;
    MinRtrAdvInterval 1;
    AdvIntervalOpt on;
    AdvHomeAgentFlag on;
    AdvHomeAgentInfo on;
    HomeAgentLifetime 1800;
    HomeAgentPreference 10;

    # Home Agent address
    prefix 2001:db8:ffff:100a::1/64
    {
        AdvRouterAddr on;
        AdvOnLink on;
        AdvAutonomous on;
    };
};
```



LAMPIRAN 3

KONFIGURASI *FOREIGN ROUTER*

3.1 Konfigurasi Interface *Foreign Agent*

```
# ifconfig eth0 inet6 add 2001:db8:ffff:100b::12/64
# ifconfig eth1 inet6 add 2001:db8:ffff:100c::1/64
```

3.2 Konfigurasi *static routing*

```
# ip route add 2001:db8:ffff:100a::/64 via 2001:db8:ffff:100b::11
```

3.4 Konfigurasi beberapa fungsi pada *foreign router*

```
# iwconfig eth1 mode ad-hoc essid visitnet enc off
# echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
# echo "0" > /proc/sys/net/ipv6/conf/all/autoconf
# echo "0" > /proc/sys/net/ipv6/conf/all/accept_ra
# echo "0" > /proc/sys/net/ipv6/conf/all/accept_redirects
```

3.5 Konfigurasi *radvd.conf*

```
# Foreign Agent radvd configuration file
# Replace eth1 with the interface connected to the home link
interface eth1
{
    AdvSendAdvert on;
    MaxRtrAdvInterval 3;
    MinRtrAdvInterval 1;
    AdvIntervalOpt on;
    AdvHomeAgentFlag on;
    AdvHomeAgentInfo on;
    HomeAgentLifetime 1800;
    HomeAgentPreference 10;

    # Home Agent address
    prefix 2001:db8:ffff:100c::1/64
    {
        AdvRouterAddr on;
        AdvOnLink on;
        AdvAutonomous on;
    };
};
```

LAMPIRAN 4

CORRESPONDENT NODE

4.1 Konfigurasi Interface *Correspondent Agent*

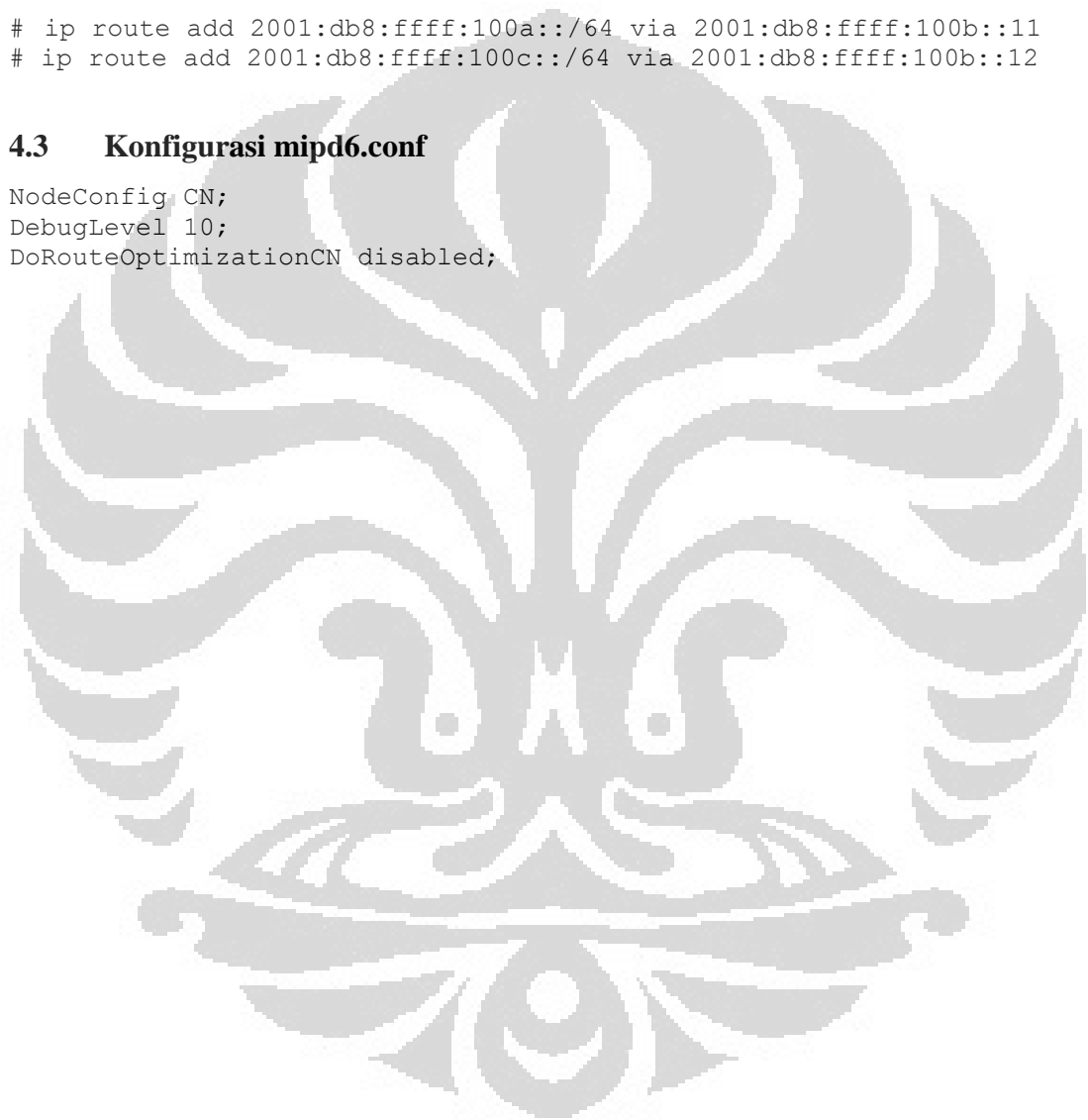
```
# ifconfig eth2 inet6 add 2001:db8:ffff:100b::13/64
```

4.2 Konfigurasi *static routing*

```
# ip route add 2001:db8:ffff:100a::/64 via 2001:db8:ffff:100b::11  
# ip route add 2001:db8:ffff:100c::/64 via 2001:db8:ffff:100b::12
```

4.3 Konfigurasi *mipd6.conf*

```
NodeConfig CN;  
DebugLevel 10;  
DoRouteOptimizationCN disabled;
```



LAMPIRAN 5

MOBILE NODE

5.1 Konfigurasi mip6d.conf

```

NodeConfig MN;

# Set DebugLevel to 0 if you do not want debug messages
DebugLevel 10;

# Enable the optimistic handovers
OptimisticHandoff enabled;

# Specifies an interface and options associated with AP
Interface "wlan0";

    # Controls whether MN sends Mobile Prefix Solicitations
    # to the HN
    SendMobPfxSols enabled;

    # Indicated if the Acknowledge bit should be set in BU sent
    # to CN
    UseCnBuAck enabled;

# Disable RO with other MNs (it is not compatible
# with IPsec Tunnel Payload)
DoRouteOptimizationMN disabled;

# The Binding Lifetime (in sec.)
MnMaxHaBindingLife 60;

# List here the interfaces that you will use
# on your mobile node. The available one with
# the smallest preference number will be used.
Interface "wlan0" {
    MnIfPreference 1;
}

# Replace eth0 with one of your interface used on
# your mobile node
MnHomeLink "wlan0" {
    HomeAgentAddress 2001:db8:ffff:100a::1;
    HomeAddress 2001:db8:ffff:100a::100/64;
}

# Enable IPsec static keying
UseMnHaIPsec enabled;
KeyMngMobCapability disabled;

# IPsec Security Policies information
IPsecPolicySet {
    HomeAgentAddress 2001:db8:ffff:100a::1;
    HomeAddress 2001:db8:ffff:100a::100/64;

    # All MH packets (BU/BA/BERR)
    IPsecPolicy Mh UseESP 11 12;
    # All tunneled packets (HoTI/HoT, payload)
    IPsecPolicy TunnelPayload UseESP 13 14;
}

```

```
# All ICMP packets (MPS/MPA, ICMPv6)
IPsecPolicy ICMP UseESP 15 16;
}
```

5.2 Konfigurasi beberapa fungsi *mobile node*

```
# echo 0 > /proc/sys/net/ipv6/conf/wlan0/forwarding
# echo 0 > /proc/sys/net/ipv6/conf/wlan0/autoconf
# echo 1 > /proc/sys/net/ipv6/conf/wlan0/accept_ra
# echo 1 > /proc/sys/net/ipv6/conf/wlan0/accept_redirects
```

