

**TUGAS AKHIR – KI141502**

**IMPLEMENTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) UNTUK MENGATASI BLACK HOLE DAN WORM HOLE ATTACK PADA KOMUNIKASI V2V DI LINGKUNGAN VANETS**

**TITIES NOVANINDA OVARI**

**NRP 5113100083**

Dosen Pembimbing I

Dr. Radityo Anggoro, S.Kom., M.Sc.

Dosen Pembimbing II

Henning Titi Ciptaningtyas, S.Kom., M.Kom.

Jurusan Teknik Informatika

Fakultas Teknologi Informasi

Institut Teknologi Sepuluh Nopember

Surabaya 2017

***[Halaman ini sengaja dikosongkan]***



**TUGAS AKHIR – KI141502**

**IMPLEMENTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) UNTUK MENGATASI BLACK HOLE DAN WORM HOLE ATTACK PADA KOMUNIKASI V2V DI LINGKUNGAN VANETS**

**TITIES NOVANINDA OVARI**

**NRP 511310003**

**Dosen Pembimbing I**

**Dr. Radityo Anggoro, S.Kom., M.Sc.**

**Dosen Pembimbing II**

**Henning Titi Ciptaningtyas, S.Kom., M.Kom.**

**Jurusan Teknik Informatika**

**Fakultas Teknologi Informasi**

**Institut Teknologi Sepuluh Nopember**

**Surabaya 2017**

***(Halaman ini sengaja dikosongkan)***

****

**UNDERGRADUATE THESES – KI141502**

**ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) IMPLEMENTATION TO OVERCOME BLACK HOLE AND WORM HOLE ATTACK IN V2V COMMUNICATION OF VANETS**

**TITIES NOVANINDA OVARI**

**NRP 5113100083**

**First Advisor**

**Dr. Radityo Anggoro, S.Kom., M.Sc.**

**Second Advisor**

**Henning Titi Ciptaningtyas, S.Kom., M.Kom.**

**Department of Informatics**

**Faculty of Information Technology**

**Sepuluh Nopember Institute of Technology**

**Surabaya 2017**

***(Halaman ini sengaja dikosongkan)***

# LEMBAR PENGESAHAN

**IMPLEMENTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM UNTUK MENGATASI BLACK HOLE DAN WORM HOLE ATTACK PADA KOMUNIKASI V2V DI LINGKUNGAN VANETS**

**TUGAS AKHIR**

Diajukan Untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

pada

Bidang Studi Komputasi Berbasis Jaringan

Program Studi S-1 Jurusan Teknik Informatika

Fakultas Teknologi Informasi

Institut Teknologi Sepuluh Nopember

Oleh:

**TITIES NOVANINDA OVARI**

**NRP: 5113100083**

Disetujui oleh Pembimbing Tugas Akhir:

1. Dr. Radityo Anggoro, S.Kom., M.Sc. .....................

(NIP. 198410162008121002) (Pembimbing 1)

1. Henning Titi Ciptaningtyas, S.Kom., M.Kom. .....................

(NIP. 198407082010122004) (Pembimbing 2)

**SURABAYA**

**MARET, 2017 *[Halaman ini sengaja dikosongkan]***

**IMPLEMENTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) UNTUK MENGATASI BLACK HOLE DAN WORM HOLE ATTACK PADA KOMUNIKASI V2V DI LINGKUNGAN VANETS**

|  |  |  |
| --- | --- | --- |
| **Nama Mahasiswa** | **:** | **TITIES NOVANINDA OVARI** |
| **NRP** | **:** | **5113100083** |
| **Jurusan** | **:** | **Teknik Informatika FTIF-ITS** |
| **Dosen Pembimbing 1** | **:** | **Dr. Radityo Anggoro, S.Kom., M.Sc.** |
| **Dosen Pembimbing 2** | **:** | **Henning Titi Ciptaningtyas, S.Kom., M.Kom.** |

# Abstrak

Vehicular Ad-hoc Network (VANET) merupakan teknologi yang mendukung pertukaran data antar kendaraan di jalan raya. VANET menggunakan jaringan *wireless* berbasis ad-hoc yang memungkinkan terjadi serangan, seperti *Black hole* dan *Worm hole attack*. *Black hole attack* adalah serangan yang dilakukan suatu *malicious node* dengan menjatuhkan paket data yang diterima, sedangkan *Worm hole attack* dilakukan dengan mengubah isi paket data. Kedua serangan ini dapat mempengaruhi performa *routing protocol* yang digunakan dalam komunikasi antar kendaraan.

Kedua serangan tersebut dapat diatasi jika tiap *node* dapat mendeteksi jika ada *malicious node* di sekitarnya, sehingga tiap *node* tersebut tidak meneruskan paket data ke *malicious node*. *Black hole attack* dapat dideteksi dengan melakukan pemantauan terhadap arus pertukaran data pada tiap *node*, sedangkan *Worm hole attack* dapat dideteksi dengan menggunakan *digital signature*. Tugas akhir ini mengimplementasikan Elliptic Curve Digital Signature Algorithm (ECDSA) sebagai algoritma *digital signature* yang dilampirkan pada tiap paket data.

Pada tugas akhir ini didapatkan *routing protocol* yang menerapkan pemantauan arus pertukaran data dan *digital signature* pada tiap paket data yang dikirimkan mempunyai performa yang lebih baik jika dihadapkan dengan *Black hole* dan *Worm hole attack* dibandingkan dengan *routing protocol* yang tidak menerapkannya.

**Kata kunci: ECDSA, *Black hole attack*, *Worm hole attack*, VANET.**

**ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM IMPLEMENTATION TO OVERCOME BLACK HOLE AND WORM HOLE ATTACK IN V2V COMMUNICATION OF VANETS**

|  |  |  |
| --- | --- | --- |
| **Student’s Name** | **:** | **TITIES NOVANINDA OVARI** |
| **Student’s ID** | **:** | **5113100083** |
| **Department** | **:** | **Teknik Informatika FTIF-ITS** |
| **First Advisor** | **:** | **Dr. Radityo Anggoro, S.Kom., M.Sc.** |
| **Second Advisor** | **:** | **Henning Titi Ciptaningtyas, S.Kom., M.Kom.** |

# *Abstract*

*Vehicular Ad-hoc Network (VANET) is a technology enabling data exchange between vehicular on roads, in order to support Intelligent Transportation System. VANET use an ad-hoc base wireless network that can be attacked by several attacks, such as Black hole attack and Worm hole attack. Black hole attack is an attack conducted by dropping data packet that has been received, meanwhile Worm hole attack conducted by tampering the data packet. Both attacks can affect the performance of the routing protocol used in vehicular communication.*

*Both attacks can be overcome if each node can detect the malicious node around them, so they do not forward the data packet to malicious node. Black hole attack can be detected by recording the data packet exchange traffic in each node, meanwhile Worm hole attack can be detected by attaching digital signature on each data packets that will be sent. This thesis implements Elliptic Curve Digital Signature Algorithm (ECDSA) as the digital signature algorithm attached to each data packets that will be sent.*

*In this thesis, it is obtained that the routing protocol which applies data packet exchange traffic recording and the digital signature on each packet that will be sent has better performance than the routeing protocol which does not.*

***Keywords: ECDSA, Black hole attack, Worm hole attack, VANET.***

**KATA PENGANTAR**



Alhamdulillahirabbil’alamin, segala puji bagi Allah SWT, yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul “**IMPLEMENTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) UNTUK MENGATASI BLACK HOLE DAN WORM HOLE ATTACK PADA KOMUNIKASI V2V DI LINGKUNGAN VANETS**”. Tugas Akhir ini merupakan salah satu syarat dalam menempuh ujian sidang guna memperoleh gelar Sarjana Komputer. Dengan pengerjaan Tugas Akhir ini, penulis bisa belajar banyak untuk memperdalam dan meningkatkan apa yang telah didapatkan penulis selama menempuh perkuliahaan di Teknik Informatika ITS.

Selesainya Tugas Akhir ini tidak terlepas dari bantuan dan dukungan beberapa pihak, sehingga pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Allah SWT dan Nabi Muhammad SAW.
2. Keluarga penulis yang selalu memberikan dukungan doa, moral, dan material yang tak terhingga kepada penulis sehingga penulis dapat menyelesaikan Tugas Akhir ini.
3. Bapak Dr. Radityo Anggoro, S.Kom., M.Sc. dan Ibu Henning Titi Ciptaningtyas, S.Kom., M.Kom.selaku dosen pembimbing penulis yang telah membimbing dan memberikan motivasi, nasehat dan bimbingan dalam menyelesaikan tugas akhir ini.
4. Bapak Darlis Herumurti, S.Kom., M.Kom. selaku kepala jurusan Teknik Informatika ITS.
5. Seluruh dosen dan karyawan Teknik Informatika ITS yang telah memberikan ilmu dan pengalaman kepada penulis selama menjalani masa studi di ITS.
6. Ibu Eva Mursidah dan Ibu Sri Budiati yang selalu mempermudah penulis dalam peminjaman buku di RBTC.
7. Teman-teman seperjuangan RMK NCC/KBJ, yang telah menemani dan menyemangati penulis.
8. Teman-teman administrator NCC/KBJ, yang telah menemani dan menyemangati penulis selama penulis menjadi administrator, menjadi rumah kedua penulis selama penulis berkuliah.
9. Teman-teman angkatan 2013, yang sudah mendukung penulis selama perkuliahan.
10. Sahabat penulis yang tidak dapat disebutkan satu per satu yang selalu membantu, menghibur, menjadi tempat bertukar ilmu dan berjuang bersama-sama penulis.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kekurangan sehingga dengan kerendahan hati penulis mengharapkan kritik dan saran dari pembaca untuk perbaikan ke depan.

Surabaya, Maret 2017

# DAFTAR ISI

LEMBAR PENGESAHAN 5

Abstrak 7

*Abstract* 9

DAFTAR ISI 13

DAFTAR GAMBAR 17

DAFTAR TABEL 21

BAB I PENDAHULUAN 23

1.1 Latar Belakang 23

1.2 Rumusan Masalah 24

1.3 Batasan Permasalahan 24

1.4 Tujuan 24

1.5 Manfaat 25

1.6 Metodologi 25

1.6.1 Penyusunan Proposal Tugas Akhir 25

1.6.2 Studi Literatur 25

1.6.3 Implementasi Sistem 26

1.6.4 Pengujian dan Evaluasi 26

1.6.5 Penyusunan Buku 27

1.7 Sistematika Penulisan Laporan 27

BAB II TINJAUAN PUSTAKA 29

2.1 VANET (Vehicular Ad hoc Network) 29

2.2 AODV (Ad hoc On-Demand Distance Vector) 30

2.3 ECDSA (Elliptic Curve Digital Signature Algorithm) 32

2.4 *Black hole Attack* 33

2.5 *Worm hole Attack* 34

2.6 NS-2 (Network Simulator-2) 35

2.6.1 Instalasi 36

2.6.2 *Trace File* 36

2.7 OpenSSL 38

2.8 SUMO (Simulation of Urban Mobility) 39

2.9 OpenStreetMap 39

2.10 AWK 40

3. BAB III PERANCANGAN 41

3.1 Deskripi Umum 41

3.2 Perancangan Skenario Mobilitas 42

3.2.1 Perancangan Skenario Mobilitas *Grid* 43

3.2.2 Perancangan Skenario Mobilitas *Real* 44

3.3 Perancangan Simulasi pada NS-2 46

3.4 Perancangan Metrik Analisis 48

3.4.1 *Packet Delivery Ratio* (PDR) 48

3.4.2 Rata-rata *End to End Delay* (E2E) 48

3.4.3 *Routing Overhead* (RO) 49

3.5 Perancangan Modifikasi pada *Protocol* AODV 49

BAB IV IMPLEMENTASI 51

4.1 Implementasi Skenario Mobilitas 51

4.1.1 Skenario *Grid* 51

4.1.2 Skenario *Real* 55

4.2 Implementasi Modifikasi pada *Protocol* AODV 57

4.2.1 Modifikasi Makefile 57

4.2.2 Modifikasi *Packet Header* 58

4.2.3 Penambahan Evaluasi pada Tiap *Node* 59

4.2.4 Implementasi ECDSA 61

4.2.5 Modifikasi Pemilihan *Node* 62

4.3 Implementasi Simulasi pada NS-2 62

4.3.1 Implementasi *Black hole Attack* 63

4.3.2 Implementasi *Worm hole Attack* 65

4.4 Implementasi Metrik Analisis 67

4.4.1 Implementasi *Packet Delivery Ratio* (PDR) 67

4.4.2 Implementasi Rata-rata *End to End Delay* (E2E) 69

4.4.3 Implementasi *Routing Overhead* (RO) 70

BAB V HASIL UJI COBA DAN EVALUASI 73

5.1 Lingkungan Uji Coba 73

5.2 Hasil Uji Coba 73

5.2.1 Hasil Uji Coba Skenario *Grid* 74

5.2.2 Hasil Uji Coba Skenario *Real* 80

BAB VI KESIMPULAN DAN SARAN 87

6.1 Kesimpulan 87

6.2 Saran 87

DAFTAR PUSTAKA 89

LAMPIRAN 91

A.1 Kode Skenario NS-2 91

A.2 Kode Fungsi AODV::recvHello 93

A.3 Kode Fungsi AODV::recvRequest 93

A.4 Kode Fungsi AODV::sendRequest 98

A.5 Kode Skrip AWK *Packet Delivery Ratio* 103

A.6 Kode Skrip AWK Rata-rata *End to End Delay* 103

A.7 Kode Skrip AWK *Routing Overhead* 104

BIODATA PENULIS 105

***[Halaman ini sengaja dikosongkan]***

# DAFTAR GAMBAR

Gambar 2.1 Ilustrasi komunikasi pada VANET [4] 8

Gambar 2.2 Ilustrasi pencarian rute *routing protocol* AODV [6] 9

Gambar 2.3 Ilustrasi kurva pada ECDSA [7] 10

Gambar 2.4 Ilustrasi *Black hole attack* [9] 12

Gambar 2.5 Ilustrasi *Worm hole attack* [10] 13

Gambar 2.6 Perintah untuk menginstall *dependency* NS-2 14

Gambar 2.7 Baris kode yang diubah pada *file* ls.h 14

Gambar 2.8 Logo OpenSSL [15] 16

Gambar 2.9 Logo SUMO [12] 17

Gambar 2.10 Logo OpenStreetMap [13] 18

Gambar 3.1 Diagram rancangan simulasi 21

Gambar 3.2 Alur pembuatan skenario mobilitas *grid* 23

Gambar 3.3 Alur pembuatan skenario mobilitas *real* 25

Gambar 3.4 Pseudocode modifikasi *protocol* AODV 29

Gambar 4.1 Perintah netgenerate 31

Gambar 4.2 Hasil *generate* peta *grid* 32

Gambar 4.3 Perintah randomTrips 32

Gambar 4.4 Perintah duarouter 33

Gambar 4.5 File skrip sumocfg 33

Gambar 4.6 Simulasi pergerakan kendaraan 34

Gambar 4.7 Perintah SUMO 34

Gambar 4.8 Perintah traceExporter 35

Gambar 4.9 Ekspor peta dari OpenStreetMap 35

Gambar 4.10 Perintah netconvert 35

Gambar 4.11 Hasil konversi peta *real* 36

Gambar 4.12 Modifikasi Makefile 38

Gambar 4.13 Daftar *library* OpenSSL yang digunakan 39

Gambar 4.14 Perubahan struktur *packet header* 39

Gambar 4.15 Pengaktifan *hello packet* 40

Gambar 4.16 Inisialisasi variabel 40

Gambar 4.17 Konfigurasi lingkungan simulasi 43

Gambar 4.18 Potongan kode untuk menugaskan *node* sebagai *Black hole attacker* 44

Gambar 4.19 Potongan kode untuk mengenali *Black hole attacker* 44

Gambar 4.20 Inisialisasi variabel malicious 44

Gambar 4.21 Potongan kode untuk melakukan *drop* paket 45

Gambar 4.22 Potongan kode *Black hole attacker* mengirim paket *reply* 45

Gambar 4.23 Potongan kode untuk menugaskan *node* sebagai *Worm hole attacker* 46

Gambar 4.24 Potongan kode untuk mengenali *Worm hole attacker* 46

Gambar 4.25 Inisialisasi variabel worm 46

Gambar 4.26 Potongan kode untuk mengirim paket *reply* dan memodifikasi paket yang diterima 47

Gambar 4.27 Pseudocode untuk menghitung PDR 48

Gambar 4.28 Perintah pengeksekusian skrip awk PDR 48

Gambar 4.29 *Output* skrip awk PDR 48

Gambar 4.30 Pseudocode untuk menghitung E2E 49

Gambar 4.31 Perintah pengeksekusian skrip awk E2E 50

Gambar 4.32 *Output* skrip awk E2E 50

Gambar 4.33 Pseudocode untuk menghitung RO 50

Gambar 4.34 Perintah pengeksekusian skrip awk RO 51

Gambar 4.35 *Output* skrip awk RO 51

Gambar 5.1 Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 30 *node* 54

Gambar 5.2 Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 40 *node* 54

Gambar 5.3 Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 50 *node* 55

Gambar 5.4 Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 30 *node* 56

Gambar 5.5 Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 40 *node* 56

Gambar 5.6 Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 50 *node* 57

Gambar 5.7 Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 30 *node* 58

Gambar 5.8 Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 40 *node* 58

Gambar 5.9 Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 50 *node* 59

Gambar 5.10 Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 30 *node* 60

Gambar 5.11 Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 40 *node* 60

Gambar 5.12 Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 50 *node* 61

Gambar 5.13 Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 30 *node* 62

Gambar 5.14 Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 40 *node* 62

Gambar 5.15 Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 50 *node* 63

Gambar 5.16 Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 30 *node* 64

Gambar 5.17 Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 40 *node* 64

Gambar 5.18 Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 50 *node* 65

***[Halaman ini sengaja dikosongkan]***

# DAFTAR TABEL

[Tabel 2.1 Tabel detail penjelasan *trace file* AODV 37](#_Toc484054935)

[Tabel 3.1 Parameter lingkungan simulasi dengan skenario 48](#_Toc484054936)

[Tabel 5.1 Spesifikasi perangkat yang digunakan 74](#_Toc484054937)

***[Halaman ini sengaja dikosongkan]***

# 

# BAB I PENDAHULUAN

## Latar Belakang

Vehicular Ad-hoc Network (VANET) merupakan salah satu teknologi yang saat ini banyak dikembangkan di berbagai negara. Terdapat beberapa area riset dalam teknologi VANET, diantaranya adalah *routing protocol* dan sekuritas [1]. Fokus pada *routing protocol* adalah untuk memenuhi kebutuhan mengenai penentuan rute dari *source node* ke *destination node* dengan jangka waktu sesingkat mungkin dan akurasi rute yang optimal, sedangkan sekuritas berfokus pada ketercapaian dan autentikasi paket dalam pertukaran paket. Skenario serangan yang memungkinkan terjadi pada jaringan VANET adalah *Black hole* dan *Worm hole attack.*

*Black hole attack* merupakan serangan dimana *malicious node* selalu melakukan *drop* pada paket yang diterimanya dan membalas pada *source node* seolah paket sudah diterima oleh *destination node*. Sedangkan *Worm hole attack* memiliki banyak variasi serangan, salah satunya dengan mengubah isi dari paket yang diterimanya.

Dalam beberapa tahun terakhir terdapat penelitian terkait metode untuk mengatasi *Black hole* maupun *Worm hole attack* pada jaringan VANET, salah satunya adalah penerapan *evaluation system* dan *digital signature* pada *routing protocol* GPSR.

Pada penelitian kali ini akan dilakukan cara untuk mengatasi *Black hole* dan *Worm hole attack* dengan menggunakan *evaluation value* yang didapatkan melalui *forward-backward* evaluation dan implementasi *Elliptic Curve Digital Signature Algorithm* (ECDSA) sebagai algoritma digital signature pada *routing protocol* AODV.

Dikemudian hari dapat dihasilkan routing protocol yang cukup efektif dalam mengatasi serangan dalam jaringan VANET, sehingga didapatkan *routing protocol* yang aman dan *reliable* untuk komunikasi antar kendaraan.

## Rumusan Masalah

Tugas akhir ini mengangkat beberapa rumusan masalah sebagai berikut:

1. Bagaimana cara mendeteksi *malicious node* yang melakukan *Black hole* dan *Worm hole attack*?
2. Bagaimana cara mengimplementasikan ECDSA untuk mengatasi *Black hole* dan *Worm hole attack*?
3. Bagaimana perbandingan performa *routing protocol* AODV ketika terdapat *malicious node* yang melakukan *Black hole* dan *Worm hole attack* sebelum dan sesudah ECDSAditerapkan?

## Batasan Permasalahan

Permasalahan yang dibahas pada tugas akhir ini memiliki batasan sebagai berikut:

1. Simulator yang digunakan adalah simulator NS2.
2. *Routing protocol* yang digunakan adalah *routing protocol* AODV.
3. Algoritma *digital signature* yang digunakan adalah algoritma ECDSA.

## Tujuan

Tujuan dari tugas akhir ini adalah sebagai berikut:

1. Dapat mendeteksi *malicious node* yang melakukan *Black hole* dan *Worm hole attack* pada lingkungan VANET dengan *routing protocol* AODV.
2. Dapat mengimplementasikan ECDSA untuk mengatasi *Black hole* dan *Worm hole attack* yang terjadi di lingkungan VANET dengan *routing protocol* AODV.
3. Menganalisa perbandingan performa *routing protocol* AODV ketika terdapat *malicious node* yang melakukan *Black hole* dan *Worm hole attack* sebelum dan sesudah ECDSA diterapkan.

## Manfaat

Manfaat dari hasil pembuatan tugas akhir ini adalah sebagai berikut:

1. Memberikan manfaat di bidang VANET terutama pada area riset sekuritas dengan mendapatkan performa *routing protocol* yang relatif stabil meskipun terdapat *malicious node* yang melakukan *Black hole* dan *Worm hole attack* pada lingkungan VANET.
2. Menerapkan ilmu yang dipelajari selama kuliah di Teknik Informatika ITS agar dapat berguna bagi orang banyak.

## Metodologi

Tahapan-tahapan yang dilakukan dalam pengerjaan tugas akhir ini adalah sebagi berikut:

### Penyusunan Proposal Tugas Akhir

Tahap awal tugas akhir ini adalah menyusun proposal tugas akhir. Pada proposal, berisi tentang deskripsi pendahuluan dari tugas akhir yang akan dibuat. Proposal juga berisi tentang garis besar tugas akhir yang akan dikerjakan sehingga memberikan gambaran untuk dapat mengerjakan tugas akhir sesuai dengan *timeline* yang dibuat. Gagasan untuk mengatasi *Black Hole* dan *Worm Hole attack* pada komunikasi V2V di lingkungan VANETs.

### Studi Literatur

Pada tahap ini dilakukan untuk mencari informasi dan studi literatur apa saja yang dapat dijadikan sebagai referensi untuk membantu pengerjaan tugas akhir ini. Tahap ini merupakan tahap untuk memahami semua metode yang akan dikerjakan, sehingga memberi gambaran selama pengerjaan tugas akhir. Informasi didapatkan dari buku dan literatur yang berhubungan dengan metode yang digunakan. Informasi yang dicari adalah *Black Hole* dan *Worm Hole attack*, dan ECDSA*.* Tugas akhir ini juga mengacu pada literatur jurnal dengan judul “*Secure and Efficient Protocol for Position-based Routing in VANET”* [2].

### Implementasi Sistem

Implementasi merupakan tahap untuk mengimplementasikan metode-metode yang sudah diajukan pada proposal Tugas Akhir. Untuk membangun algoritma yang telah dirancang sebelumnya, implementasi dilakukan dengan menggunakan NS-2 sebagai *Network Simulator*, bahasa C/C++ sebagai bahasa pemrograman, dan OpenSSL sebagai *library* untuk mengimplementasikan ECDSA.

### Pengujian dan Evaluasi

Pada tahap ini algoritma yang telah disusun diuji coba dengan melakukan *generate* skenario *grid* dan skenario *real* yang kemudian diberikan *malicious node* dalam jumlah tertentu dan melakukan serangan tertentu. Kemudian dari skenario tersebut akan didapatkan data uji *packet delivery ratio* (PDR), rata-rata *end to end delay* (E2E), dan *routing overhead* (RO). Dari data uji tersebut, dilakukan analisa untuk membandingkan performa *routing protocol* yang telah dimodifikasi dengan *routing protocol original*.

### Penyusunan Buku

Pada tahap ini disusun buku sebagai dokumentasi dari pelaksanaan tugas akhir yang mencangkup seluruh konsep, teori, implementasi, serta hasil yang telah dikerjakan.

## Sistematika Penulisan Laporan

Sistematika penulisan laporan tugas akhir adalah sebagai berikut:

* + 1. Bab I. Pendahuluan

Bab ini berisikan penjelasan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi, dan sistematika penulisan dari pembuatan tugas akhir.

* + 1. Bab II. Tinjauan Pustaka

Bab ini berisi kajian teori dari metode dan algoritma yang digunakan dalam penyusunan tugas akhir ini. Secara garis besar, bab ini berisi tentang VANET, AODV, ECDSA, *Black Hole attack*, *Worm Hole attack*, OpenSSL, OpenStreetMap, SUMO, NS-2, dan AWK*.*

* + 1. Bab III. Perancangan Perangkat Lunak

Bab ini berisi pembahasan mengenai perancangan dari metode ECDSA untuk mengatasi *Black Hole* dan *Worm Hole attack* pada komunikasi V2V di lingkungan VANETs menggunakan NS-2 sebagai *simulator*.

* + 1. Bab IV. Implementasi

Bab ini menjelaskan implementasi ECDSA untuk mengatasi *Black Hole* dan *Worm Hole attack* pada komunikasi V2V di lingkungan VANETs menggunakan NS-2 sebagai *simulator.*

* + 1. Bab V. Pengujian dan Evaluasi

Bab ini berisikan hasil uji coba dari implementasi ECDSA untuk mengatasi *Black Hole* dan *Worm Hole attack* pada komunikasi V2V di lingkungan VANETs menggunakan NS-2 sebagai *simulator*. Pengujian dilakukan dengan skenario yang di*generate* oleh SUMO untuk mendapatkan data uji PDR, E2E, dan RO yang nantinya akan dianalisa menggunakan skrip awk dan dilakukan perbandingan performa *routing protocol*.

* + 1. Bab VI. Kesimpulan dan Saran

Bab ini merupakan bab yang menyampaikan kesimpulan dari hasil uji coba yang dilakukan, masalah-masalah yang dialami pada proses pengerjaan tugas akhir, dan saran untuk pengembangan solusi ke depannya.

* + 1. Daftar Pustaka

Bab ini berisi daftar pustaka yang dijadikan literatur dalam tugas akhir.

* + 1. Lampiran

Dalam lampiran terdapat kode program secara keseluruhan.

# BAB II TINJAUAN PUSTAKA

Bab ini berisi pembahasan mengenai teori-teori dasar yang digunakan dalam tugas akhir. Teori-teori tersebut diantaranya adalah *Elliptic Curve Digital Signature Algorithm*, dan beberapa teori lain yang mendukung pembuatan tugas akhir. Penjelesan ini bertujuan untuk memberikan gambaran secara umum terhadap program yang dibuat dan berguna sebagai penunjang dalam pengembangan riset yang berkaitan.

## VANET (Vehicular Ad hoc Network)

VANET merupakan bentuk dari *wireless ad hoc network* untuk menyediakan komunikasi antar kendaraan dan *roadside equipment* terdekat. VANET muncul sebagai teknologi baru untuk mengintegrasikan kemampuan *wireless network* baru dengan kendaraan. Tujuan utama VANET adalah untuk menyediakan *ubiquitos connectivity* kepada *mobile user* ketika berada di jalan raya dan komunikasi antar kendaraan yang efisien menuju *Intelligent Transportation System* [3].

VANET merupakan pengembangan dari MANET (Mobile Ad hoc Network). Pada VANET maupun MANET, *node* yang bergerak bergantung pada *ad hoc routing protocol* untuk menentukan bagaimana mengirim pesan kepada tujuan. Perbedaan antara VANET dan MANET terletak pada kecepatan *node*. Pada VANET, *node* bergerak dengan kecepatan yang relatif tinggi. Hal tersebut merupakan sebuah tantangan dan memiliki peranan penting dalam menentukan desain jaringan seperti apakah yang akan dibuat.

Terdapat dua jenis *node* yang tergabung dalam VANET, yaitu RSU (*Road-side Unit*) dan OBU (*On-Board Unit*) [4]. Oleh karena itu terdapat dua tipe komunikasi dalam VANET, yaitu antara kendaraan dengan kendaraan, yang biasa disebut dengan komunikasi V2V dan antara kendaraan dengan RSU, yang biasa disebut dengan komunikasi V2I seperti pada Gambar 2.1.



Gambar . Ilustrasi komunikasi pada VANET [4]

Agar komunikasi antar *node* pada VANET dapat berjalan dengan baik, diperlukan sebuah *routing protocol* yang dapat beradaptasi dengan karakteristik VANET. Pada Tugas Akhir ini, penulis menggunakan *routing protocol* AODV yang dimodifikasi untuk menambahkan aspek sekuritas sehingga dapat mengatasi serangan yang memungkinkan terjadi pada VANET, yaitu *Black hole* dan *Worm hole attack*. Implementasi VANET dilakukan pada NS-2 dan dilakukan pengujian performa menggunakan skrip awk.

## AODV (Ad hoc On-Demand Distance Vector)

AODV merupakan *routing protocol* yang umum digunakan di MANET dan telah diaplikasikan juga di VANET. Pada AODV, rute dibuat hanya ketika diminta oleh *node* asal (*source node*). Metode penemuan rute AODV berdasarkan pada *routing table* yang menyimpan rute terhadap beberapa *node*. *Source node* akan menyebarkan paket *route request* (RREQ) ke tiap *neighbor*-nya yang akan mengirimkan paket RREQ juga ke tiap *neighbor*-nya, begitu seterusnya hingga mencapai *node* tujuan (*destination node*).

Ketika paket RREQ mencapai *destination node* atau *node* yang mengetahui rute ke *destination node*, paket *route replay* (RREP) akan dikirimkan kembali ke *source node* melalui *reverse route*. AODV menggunakan sequence number untuk mendapatkan informasi rute yang paling update dan mencegah *routing loop* [5]. Ilustrasi pencarian rute *routing protocol* AODV dapat dilihat pada Gambar 2.2.



Gambar . Ilustrasi pencarian rute *routing protocol* AODV [6]

Sebagai contoh pencarian rute, ilustrasi pada gambar 2.2.1 menggambarkan bagaimana *node* asal, yaitu *node* A mencari rute untuk menuju *node* destination yaitu *node* J. *Node* A mengirimkan RREQ kepada semua *neighbor*nya dan diteruskan oleh *node* *neighbor* hingga mencapai *node* J. Kemudian *node* J mengirimkan RREP melalui rute terdekat yang telah dibuat.

*Routing protocol* AODV termasuk ke dalam *routing protocol* yang bersifat reaktif, artinya *node* hanya akan mencari rute jika diminta (*on demand*). Sehingga *routing protocol* AODV dinilai memiliki performa yang relatif baik jika diterapkan pada lingkungan VANET yang memiliki karakteristik yaitu *node* bergerak dengan kecepatan tinggi.

Pada Tugas Akhir ini, penulis menggunakan *routing protocol* AODV sebagai algoritma *routing protocol* yang digunakan untuk mengimplementasikan lingkungan VANET beserta skenario serangannya.

## ECDSA (Elliptic Curve Digital Signature Algorithm)

*Elliptic Curve Digital Signature Algorithm* (ECDSA) merupakan varian dari *Digital Signature Algorithm* (DSA) yang beroperasi pada grup *elliptic curve*. Untuk mengirim pesan yang tertandatangani dari node asal ke node tujuan, keduanya sepakat pada parameter domain *elliptic curve*. Pengirim memiliki *key pair* yang terdiri dari *private key* (sebuah *integer* kurang dari n yang dipilih secara acak, dimana n merupakan urutan dari kurva, sebuah parameter domain *elliptic curve*) dan *public key* (G adalah *generator point*, sebuah parameter domain *elliptic curve*) [7]. Ilustrasi kurva dapat dilihat pada Gambar 2.3.



Gambar . Ilustrasi kurva pada ECDSA [7]

ECDSA merupakan salah satu algoritma *digital signature* yang umum digunakan selain RSA. Tingkat kemanan ECDSA dinilai cukup baik digunakan dalam jaringan. Di samping itu, ECDSA membutuhkan tempat yang lebih sedikit dibandingkan dengan RSA. Untuk tingkat keamanan yang sama, ECDSA memiliki ukuran *signature* dan *public key* yang lebih kecil [8]. Sehingga jika akan ditambahkan pada *packet header*, tidak akan terlalu membebani dengan menambah ukuran paket yang akan dikirimkan.

Pada Tugas Akhir ini, penulis menggunakan ECDSA sebagai algoritma *digital signature* yang diterapkan untuk menjaga keaslian paket yang dikirimkan. Dengan menjaga keaslian paket, *Worm hole attack* yang melakukan penyerangan dengan memodifikasi paket dapat diatasi.

## *Black hole Attack*

*Black hole attack* terjadi saat terdapat *malicious node* yang menunggu mendapatkan paket RREQ dari *neighbor*-nya. Namun ketika sudah mendapatkan paket RREQ, *malicious node* tersebut membalas seolah-olah dia memiliki rute terpendek menuju *destination node*. Sehingga *source node* akan meneruskan dengan mengirim paket data ke *destination node* melalui *malicious node* tersebut. Ketika mendapatkan paket data dari *source node*, *malicious node* tersebut tidak meneruskan paket data ke *destination node*, tetapi melakukan *drop* terhadap paket data yang diterima. Sehingga paket data tersebut tidak mencapai *destination source*-nya dan *malicious node* tidak memberi tahu *source node* jika paket datanya tidak mencapai *destination node* [2]*.* Ilustrasi *Black hole attack* dapat dilihat pada Gambar 2.4.



Gambar . Ilustrasi *Black hole attack* [9]

Pada Tugas Akhir ini, *Black hole attack* dilakukan sebagai skenario untuk menilai performa *routing protocol* dalam mengatasi serangan yang memungkinkan terjadi pada komunikasi V2V di lingkungan VANET.

## *Worm hole Attack*

*Worm hole attack* terdiri dari 2 fase yang dilancarkan oleh satu atau lebih *malicious node*. Pada fase pertama, *malicious node* mencoba mengumpan *node neighbor*-nya agar mengirimkan paket melalui dirinya. Pada fase kedua, *malicious node* tersebut memanfaatkan paket data yang diterimanya sesuai keinginannya, salah satunya dengan mengubah isi paket data [2]. Worm hole attack dapat diilustrasikan seperti pada Gambar 2.5.



Gambar . Ilustrasi *Worm hole attack* [10]

Pada Tugas Akhir ini, *Worm hole attack* dilakukan sebagai skenario untuk menilai performa *routing protocol* dalam mengatasi serangan yang memungkinkan terjadi pada komunikasi V2V di lingkungan VANET.

## NS-2 (Network Simulator-2)

NS-2 merupakan sebuah discrete event simulator yang didesain untuk membantu penelitian pada bidang jaringan komputer. Pengembangan NS dimulai pada tahun 1989 sebagai sebuah varian dari REAL network simulator, pada tahun 1995 pengembangan NS didukung oleh DARPA melalui VINT project di LBL, Xerox PARC, UCB dan USC/ISI. NS kemudian memasuki versi dua pada tanggal 31 Juli 1995. Saat ini pengembangan NS didukung oleh DARPA melalui SAMAN dan NSF melalui CONSER beserta peneliti lainnya termasuk ACIRI [11].

NS-2 dinilai lebih stabil untuk melakukan simulasi lingkungan VANET jika dibandingkan dengan versi terbarunya, yaitu NS-3.

Pada Tugas Akhir ini, NS-2 digunakan untuk melakukan simulasi lingkungan VANET beserta dengan skenario serangan yang memungkinkan terjadi, yaitu *Black hole* dan *Worm hole attack*. *Trace file* yang dihasilkan oleh NS-2 juga digunakan sebagai informasi untuk mengukur performa *routing protocol*.

### Instalasi

NS-2 membutuhkan beberapa package yang harus sudah terinstall sebelum memulai instalasi NS-2. Untuk menginstall *dependency* yang dibutuhkan dapat dilakukan dengan *command* berikut:

sudo apt-get install build-essential autoconf automake libxmu-dev

Gambar . Perintah untuk menginstall *dependency* NS-2

Setelah menginstall *dependency* yang dibutuhkan, ekstrak *package* NS-2 dan ubah baris kode ke-137 pada *file* ls.h di folder linkstate menjadi seperti berikut:

void eraseAll(){**this->**erase(baseMap::begin(), baseMap::end()); }

Gambar . Baris kode yang diubah pada *file* ls.h

Install NS-2 dengan menjalankan perintah ./install pada folder NS-2.

### *Trace File*

*Trace file* merupakan *file* hasil simulasi yang dilakukan oleh NS-2 dan berisikan informasi detail pengiriman paket data. *Trace file* digunakan untuk menganalisis performa *routing protocol* yang disimulasikan.

Tabel . Tabel detail penjelasan *trace file* AODV

|  |  |  |
| --- | --- | --- |
| Kolom ke- | Penjelasan | Isi |
| 1 | *Event* | s : *sent*  r : *received*  f : *forwarded*  D: *dropped* |
| 2 | *Time* | Waktu terjadinya *event* |
| 3 | ID *Node* | \_x\_ : dari 0 hingga banyak *node* pada topologi |
| 4 | *Layer* | AGT : *application*  RTR : *routing*  LL : *link layer*  IFQ : *packet queue*  MAC : MAC  PHY : *physical* |
| 5 | *Flag* | --- : Tidak ada |
| 6 | *Sequence Number* | Nomor paket |
| 7 | Tipe Paket | AODV : paket *routing* AODV  cbr : berkas paket CBR (*Constant Bit Rate*)  RTS : *Request To Send* yang dihasilkan MAC 802.11  CTS : *Clear To Send* yang dihasilkan MAC 802.11  ACK : MAC ACK  ARP : Paket *link layer address resolution protocol* |
| 8 | Ukuran | Ukuran paket pada *layer* saat itu |
| 9 | Detail MAC | [a b c d]  a : perkiraan waktu paket  b : alamat penerima  c : alamat asal  d : IP *header* |
| 10 | *Flag* | -------- : Tidak ada |
| 11 | Detail IP *source*, *destination*, dan *nexthop* | [a:b c:d e f]  a : IP *source node*  b : *port* *source node*  c : IP *destination node* (jika -1 berarti *broadcast*)  d : *port destination node*  e : IP *header* ttl  f : IP *nexthop* (jika 0 berarti *node* 0 atau *broadcast*) |

## OpenSSL

OpenSSL adalah sebuah proyek open source yang menyediakan toolkit protokol Transport Layer Security (TLS) dan Secure Socket Layer (SSL). OpenSSL juga merupakan library yang umum digunakan untuk keperluan kriptografi. OpenSSL toolkit terlisensi di bawah lisensi Apache, yang bisa didapatkan secara gratis untuk tujuan komersial maupun non-komersial [15].

Pada tugas akhir ini, penulis menggunakan OpenSSL untuk mengimplementasikan ECDSA yang digunakan sebagai algoritma *digital signature* dalam mengatasi skenario serangan yang diberikan.



Gambar . Logo OpenSSL [15]

## SUMO (Simulation of Urban Mobility)

Simulation of Urban Mobility atau disingkat SUMO merupakan simulasi lalu lintas jalan raya yang *open source*, *microscopic*, dan *multi-modal*. Sumo mensimulasikan bagaimana permintaan lalu lintas yang terdiri dari beberapa kendaraan berjalan pada jalan raya yang telah ditentukan. Simulasi SUMO dapat menunjukkan beberapa topik manajemen lalu lintas dalam skala besar. SUMO murni *microscopic*, yang artinya setiap kendaraan dimodelkan secara eksplisit, memiliki rutenya sendiri, dan bergerak secara individu dalam jaringan [12].

Pada Tugas Akhir ini, penulis menggunakan SUMO untuk men*generate* skenario VANET, peta area simulasi, dan pergerakan *node* sehingga menyerupai keadaan sebenarnya lalu lintas yang ingin disimulasikan.



Gambar . Logo SUMO [12]

## OpenStreetMap

OpenStreetMap merupakan proyek kolaboratif untuk membuat sebuah peta dunia yang dapat dengan bebas disunting oleh siapapun. OpenStreetMap digunakan sebagai data peta pada berbagai *website*, aplikasi *mobile*, dan *hardware device*. OpenStreetMap dibangun oleh komunitas pembuat peta yang berkontribusi dan mengelola data mengenai jalan raya, kafe, stasiun kereta api, dan sebagainya di seluruh dunia [13].



Gambar . Logo OpenStreetMap [13]

Pada Tugas Akhir ini, penulis menggunakan OpenStreetMap untuk mendapatkan peta sebenarnya guna melakukan simulasi dengan skenario *real*.

## AWK

AWK merupakan sebuah bahasa pemrograman yag didesain untuk *text-processing* dan biasanya digunakan sebagai alat ekstrasi data dan pelaporan. AWK bersifat *data-driven* yang berisikan kumpulan perintah yang akan dijalankan pada data tekstural baik secara langsung pada *file* atau digunakan sebagai bagian dari *pipeline* [14].

Pada tugas akhir ini, penulis menggunakan AWK untuk memproses data yang diberikan oleh NS-2 agar mendapatkan analisis mengenai *packet delivery ratio*, *end to end delay*, dan *routing overhead*.

# BAB III PERANCANGAN

Bab ini membahas mengenai perancangan implemetasi sistem yang dibuat pada Tugas Akhir. Bagian yang akan dijelaskan pada bab ini berawal dari deskripsi umum, perancangan skenario, hingga alur dan implementasinya.

## Deskripi Umum

Pada Tugas Akhir ini penulis akan mengimplementasikan *routing protocol* AODV yang dimodifikasi dengan menambahkan proses evaluasi untuk mengatasi *Black hole* dan *Worm hole attack*. Proses evaluasi pertama dilakukan dengan cara merekam keluar masuknya paket dalam suatu node. Proses evaluasi kedua dilakukan dengan mengimplementasikan ECDSA sebagai algoritma *digital signature* untuk memvalidasi keaslian paket yang diterima. Diagram rancangan simulasi dapat dilihat pada Gambar 3.1.



Gambar . Diagram rancangan simulasi

*Routing protocol* AODV yang telah dimodifikasi tersebut kemudian disimulasikan menggunakan skenario dari SUMO. Simulasi yang dilakukan akan menghasilkan *trace file*, yang kemudian dianalisis menggunakan AWK untuk mendapatkan *packet delivery ratio*, *average end to end delay*, dan *routing overhead.* Analisis tersebut dapat mengukur performa *routing protocol* AODV yang telah dimodifikasi dibandingkan dengan *routing protocol* AODV sebelum dimodifikasi.

## Perancangan Skenario Mobilitas

Perancangan skenario mobilitas dimulai dengan *generate* area simulasi, pergerakan *node*, implementasi pergerakan *node*, dan memilih *node* yang akan dijadikan *attacker*. Dalam Tugas Akhir ini, terdapat dua macam area simulasi yang akan digunakan. Diantaranya adalah peta *grid* dan peta *real*. Peta *grid* yang dimaksud adalah bentuk jalan berpetak-petak sebagai contoh jalan berpotongan yang sederhana. Peta *grid* digunakan sebagai simulasi awal VANET karena lebih seimbang dan stabil. Peta *grid* didapatkan dengan menentukan panjang dan jumlah petak area menggunakan SUMO. Sedangkan yang dimaksud peta *real* adalah peta asli yang digunakan sebagai area simulasi. Peta *real* didapatkan dengan mengambil area yang dimaksudkan sebagai area simulasi dari OpenStreetMap. Pada Tugas Akhir ini, peta *real* yang diambil penulis adalah salah satu area di Surabaya.

### Perancangan Skenario Mobilitas *Grid*

Perancangan skenario mobilitas *grid* diawali dengan merancang luas area peta *grid* yang dibutuhkan. Luas area tersebut bisa didapatkan dengan cara menentukan terlebih dahulu jumlah titik persimpangan yang diinginkan pada peta *grid*, sehingga dari jumlah persimpangan tersebut dapat diketahui berapa banyak petak yang dibutuhkan. Dengan mengetahui jumlah petak yang dibutuhkan, dapat digunakan untuk menentukan panjang tiap petak sehingga mendapatkan luas area seperti yang diinginkan. Misalkan luas area yang dibutuhkan adalah 1000 m x 1000 m. Dengan 11 titik persimpangan, maka akan didapatkan 10 petak. Dengan begitu panjang tiap petak untuk mendapatkan luas area 1000 m x 1000 m adalah 100 m.

Peta *grid* yang telah ditentukan luas areanya tersebut kemudian dibuat dengan menggunakan tools SUMO yaitu netgenerate. Selain titik persimpangan dan panjang tiap petak *grid*, dibutuhkan juga pengaturan kecepatan kendaraan dalam pembuatan peta *grid* menggunakan netgenerate ini. Peta *grid* yang dihasilkan oleh netgenerate akan memiliki ekstensi .net.xml. Peta *grid* ini kemudian digunakan untuk membuat pergerakan *node* dengan *tools* SUMO yaitu randomTrips dan duarouter.

Skenario mobilitas *grid* dihasilkan dengan menggabungkan *file* peta *grid* dan *file* pergerakan *node* yang telah di*generate*, yang akan menghasilkan *file* dengan ekstensi .xml. Selanjutnya, untuk dapat menerapkannya pada NS-2 file skenario mobilitas *grid* yang berekstensi .xml dikonversi ke dalam bentuk file .tcl. Konversi ini dilakukan menggunakan *tools* traceExporter. Alur pembuatan skenario *grid* dapat dilihat pada Gambar 3.2.



Gambar . Alur pembuatan skenario mobilitas *grid*

### Perancangan Skenario Mobilitas *Real*

Perancangan skenario mobilitas *real* diawali dengan memilih area yang akan dijadikan simulasi. Pada Tugas Akhir ini, penulis menggunakan peta dari OpenStreetMap untuk mengambil area yang dijadikan model simulasi. Setelah memilih area, unduh dengan menggunakan fitur *export* dari OpenStreetMap. Peta hasil export dari OpenStreetMap ini memiliki ekstensi .osm.

Setelah mendapatkan peta area yang dijadikan simulasi, peta tersebut dikonversi ke dalam bentuk *file* dengan ekstensi .net.xml menggunakan tools SUMO yaitu netconvert. Tahap berikutnya memiliki tahapan yang sama seperti tahapan ketika merancang skenario mobilitas *grid*, yaitu membuat pergerakan *node* menggunakan randomTrips dan duarouter. Kemudian gabungkan *file* peta *real* yang sudah dikonversi ke dalam *file* dengan ekstensi .net.xml dan *file* pergerakan *node* yang sudah di*generate*. Hasil dari penggabungan tersebut merupakan *file* skenario yang berekstensi .xml. *File* yang dihasilkan tersebut dikonversi ke dalam bentuk *file* .tcl agar dapat diterapkan pada NS-2. Alur pembuatan skenario *real* dapat dilihat pada Gambar 3.3.



Gambar . Alur pembuatan skenario mobilitas *real*

## Perancangan Simulasi pada NS-2

Simulasi VANET pada NS-2 dilakukan dengan menggabungkan *file* skenario yang telah dibuat menggunakan SUMO dan *file* skrip tcl yang berisikan konfigurasi lingkungan simulasi. Konfigurasi lingkungan simulasi VANET pada NS-2 dapat dilihat pada tabel

Tabel . Parameter lingkungan simulasi dengan skenario

|  |  |  |
| --- | --- | --- |
| **No.** | **Parameter** | **Spesifikasi** |
| 1. | *Network simulator* | NS-2, 2.35 |
| 2. | *Routing protocol* | AODV |
| 3. | Waktu simulasi | 200 detik |
| 4. | Area simulasi | 1700 m x 1700 m |
| 5. | Banyak kendaraan | 30, 40, 50 |
| 6. | Agen pengirim | *Constant Bit Rate* (CBR) |
| 7. | *Protocol* MAC | IEEE 802.11 |
| 8. | Propagasi sinyal | *Two-ray ground* |
| 9. | *Source/Destination* | Dinamis |
| 10. | Tipe Kanal | *Wireless channel* |

Selain konfigurasi lingkungan simulasi VANET, pada skrip tcl tersebut juga ditambahkan perintah untuk menugaskan *node* yang akan menjadi *attacker* untuk *Black hole attack* maupun *Worm hole attack*.

Agar *node attacker* dapat menjalankan tugasnya melakukan *Black hole attack* atau *Worm hole attack*, ditambahkan beberapa kode untuk melakukan *Black hole attack* dan *Worm hole attack* pada kode routing protocol AODV di NS-2.

Kode yang ditambahkan diantaranya adalah deklarasi variabel pada *file* aodv.h. Kemudian pada *file* aodv.cc ditambahkan kode untuk mengenali *node attacker* dan alur penyerangan. Ketika simulasi NS-2 dijalankan *routing protocol* AODV akan mengenali apakah suatu *node* adalah *Black hole attacker* atau *Worm hole attacker*. Jika *node* tersebut adalah *Black hole attacker*, maka *node* tersebut akan melakukan *drop* pada setiap paket yang diterimanya, sedangkan jika *node* tersebut adalah *Worm hole attacker*, maka *node* tersebut akan mengubah *node* tujuan yang ada pada paket *header*.

## Perancangan Metrik Analisis

Berikut ini merupakan parameter-parameter yang akan dianalisis pada Tugas Akhir ini untuk dapat membandingkan performa dari *routing protocol* AODV yang telah dilakukan modifikasi dan *routing protocol* AODV yang asli:

### *Packet Delivery Ratio* (PDR)

*Packet Delivery Ratio* merupakan perbandingan antara jumlah paket yang diterima dengan jumlah paket yang dikirimkan. *Packet Delivery Ratio* dihitung dengan persamaan 3.1.

|  |  |
| --- | --- |
|  |  |
| (3.1) |

*Packet Delivery Ratio* dapat menunjukkan keberhasilan paket yang dikirimkan. Semakin tinggi *Packet Delivery Ratio*, artinya semakin berhasil pengiriman paket yang dilakukan.

### Rata-rata *End to End Delay* (E2E)

Rata-rata *End to End Delay* merupakan rata-rata dari *delay* atau waktu yang dibutuhkan tiap paket untuk sampai ke *node* tujuan. *Delay* tiap paket didapatkan dari rentang waktu antara *node* asal mengirimkan paket (CBRSentTime) dan *node* tujuan menerima paket (CBRRecvTime). Dari *delay* tiap paket tersebut semua dijumlahkan dan dibagi dengan jumlah paket yang berhasil diterima (recvnum), maka akan didapatkan rata-rata *end to end delay*, yang dapat dihitung dengan persamaan 3.2.

|  |  |
| --- | --- |
|  |  |
| (3.2) |

### *Routing Overhead* (RO)

*Routing Overhead* adalah jumlah paket kontrol *routing* yang ditransmisikan per data paket ke *node* tujuan selama simulasi terjadi. *Routing Overhead* didapatkan dengan menjumlahkan semua paket kontrol *routing* yang ditransmisikan, baik itu paket *route request* (RREQ), *route reply* (RREP), maupun *route error* (RERR). Perhitungan *Routing Overhead* dapat dilihat dengan persamaan 3.3.

|  |  |
| --- | --- |
|  |  |
| (3.3) |

## Perancangan Modifikasi pada *Protocol* AODV

*Routing Protocol* AODV tidak memiliki benteng sekuritas sehingga rentan terjadi serangan, dalam hal ini adalah *Black hole* dan *Worm hole attack*. Modifikasi pada *Routing Protocol* AODV dilakukan dengan adanya penambahan aspek sekuritas guna mengatasi *Black hole* dan *Worm hole attack*. Aspek sekuritas yang ditambahkan adalah dengan mengimplementasikan ECDSA sebagai algoritma *digital signature* untuk menjaga keaslian paket yang diterima. Penerapan evaluasi oleh tiap *node* kepada *node* tetangganya juga dilakukan untuk memilih *node nexthop* yang aman. Alur modifikasi yang dilakukan pada *routing protocol* AODV diwujudkan dalam bentuk *pseudocode*, yang dapat dilihat pada Gambar 3.4.

Gambar . Pseudocode modifikasi *protocol* AODV

**Part I**

if source IP of packet != IP of this node then

counter array of packet received from node n ++

if verify of the signature successful then

counter array of verified packet from node n ++

else

drop packet and return

end if

**Part II**

if neighbor IP != destination IP of packet

counter array of packet sent to node n ++

if eval value of node n > threshold

record node n as nexthop

forward packet

else

forward packet

end if

**Part III**

for i = 1 to the number of neighbors

forward eval [i] = counter array of packet received from node i / counter array of packet send to node i

backward eval [i]= counter array of verified packet from node i / counter array of packet received from node i

eval value [i] = random number \* forward eval [i] + random number \* backward eval [i]

# BAB IV IMPLEMENTASI

Bab ini membahas mengenai implementasi dari perancangan sistem yang telah dijabarkan pada bab sebelumnya.

## Implementasi Skenario Mobilitas

Implementasi skenario mobilitas VANET dibagi menjadi dua, yaitu skenario *grid* yang menggunakan peta jalan berpetak dan skenario *real* yang menggunakan peta hasil pengambilan suatu area di kota Surabaya.

### Skenario *Grid*

Dalam mengimplementasikan skenario *grid*, SUMO menyediakan *tools* untuk membuat peta *grid* yaitu netgenerate. Pada Tugas Akhir ini, penulis membuat peta *grid* dengan luas 1500 m x 1500 m yang terdiri dari titik persimpangan antara jalan vertikal dan jalan horizontal sebanyak 11 titik x 11 titik. Dengan jumlah titik persimpangan sebanyak 11 titik tersebut, maka terbentuk 10 buah petak. Sehingga untuk mencapai luas area sebesar 1500 m x 1500 m dibutuhkan luas per petak sebesar 150 m x 150 m. Berikut perintah netgenerate untuk membuat peta tersebut dengan kecepatan *default* kendaraan sebesar 20 m/s dapat dilihat pada Gambar 4.1.

netgenerate --grid --grid.number=11 --grid.length=150 --default.speed=20 --tls.guess=1 --output-file=map.net.xml

Gambar . Perintah netgenerate

Gambar hasil peta yang telah dibuat dengan netgenerate dapat dilihat pada Gambar 4.2.



Gambar . Hasil *generate* peta *grid*

Setelah peta terbentuk, maka dilakukan pembuatan *node* dan pergerakan *node* dengan menentukan titik awal dan titik akhir setiap *node* secara random menggunakan *tools* randomTrips. Perintah penggunaan *tools* randomTrips untuk membuat *node* sebanyak n *node* dengan pergerakannya dapat dilihat pada Gambar 4.3.

python sumo-0.27.1/tools/randomTrips.py –n map.net.xml –e 30 –l --trip-attributes=”departLane=\”best”\ departSpeed=\”max\” departPos=\”random\_free\”” –o trip.trips.xml

Gambar . Perintah randomTrips

Selanjutnya dibuatkan rute yang digunakan kendaraan untuk mencapai tujuan dari *file* hasil sebelumnya menggunakan *tools* duarouter. Secara *default* algoritma yang digunakan untuk membuat rute ini adalah algoritma dijkstra. Perintah penggunaan *tools* duarouter dapat dilihat pada Gambar 4.4.

duarouter –n map.net.xml –t trip.trips.xml –o route.rou.xml --ignore-errors --repair

Gambar . Perintah duarouter

Untuk menjadikan peta dan pergerakan *node* yang telah di*generate* menjadi sebuah skenario dalam bentuk *file* berekstensi .xml, dibutuhkan sebuah *file* skrip dengan ekstensi .sumocfg guna menggabungkan *file* peta dan rute pergerakan *node*. Isi dari *file* skrip tersebut dapat dilihat pada Gambar 4.5.

<?xml version="1.0" encoding="UTF-8"?>

<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://sumo.dlr.de/xsd/sumoConfiguration.xsd">

<input>

<net-file value="map.net.xml"/>

<route-files value="routes.rou.xml"/>

</input>

<time>

<begin value="0"/>

<end value="200"/>

</time>

</configuration>

Gambar . File skrip sumocfg

*File* .sumocfg disimpan dalam direktori yang sama dengan *file* peta dan *file* rute pergerakan *node*. Untuk percobaan sebelum dikonversi, *file* .sumocfg dapat dibuka dengan menggunakan *tools* sumo-gui. Cuplikan pergerakan kendaraan dapat dilihat pada Gambar 4.6.



Zoom in



Gambar . Simulasi pergerakan kendaraan

Kemudian buat *file* skenario dalam bentuk *file* .xml dari sebuah *file* skrip berekstensi .sumocfg menggunakan *tools* SUMO. Perintah untuk menggunakan *tools* SUMO dapat dilihat pada Gambar 4.7.

sumo –c scenario.sumocfg --fcd-output scenario.xml

Gambar . Perintah SUMO

*File* skenario berekstensi .xml selanjutnya dikonversi ke dalam bentuk *file* berekstensi .tcl agar dapat disimulasikan menggunakan NS-2. *Tools* yang digunakan untuk melakukan konversi ini adalah *traceExporter*. Perintah untuk menggunakan *traceExporter* dapat dilihat pada Gambar 4.8.

python sumo-0.27.1/tools/traceExporter.py --fcd-input=scenario.xml --ns2-mobility-output=scenario.tcl

Gambar . Perintah traceExporter

### Skenario *Real*

Dalam mengimplementasikan skenario *real*, langkah pertama adalah dengan menentukan area yang akan dijadikan area simulasi. Pada Tugas Akhir ini penulis mengambil area jalan sekitar Kertajaya Surabaya. Setelah menentukan area simulasi, ekspor data peta tersebut dari OpenStreetMap seperti yang ditunjukkan pada Gambar 4.9.



Gambar . Ekspor peta dari OpenStreetMap

*File* hasil ekspor dari OpenStreetMap tersebut adalah *file* peta dengan ekstensi .osm. Kemudian konversi *file* .osm tersebut menjadi peta dalam bentuk *file* berekstensi .xml menggunakan *tools* netconvert. Perintah untuk menggunakan netconvert dapat dilihat pada Gambar 4.10.

Gambar . Perintah netconvert

netconvert --osm-files map.osm --output-file map.net.xml

Hasil konversi peta dari *file* berekstensi .osm menjadi *file* berekstensi .xml dapat dilihat menggunakan *tools* sumo-gui seperti yang ditunjukkan pada Gambar 4.11.



Gambar . Hasil konversi peta *real*

Langkah selanjutnya sama dengan ketika membuat skenario mobilitas *grid*, yaitu membuat *node*, asal, dan tujuan *node* menggunakan *tools* randomTrips. Lalu membuat rute *node* untuk sampai ke tujuan menggunakan *tools* duarouter. Kemudian membuat *file* skenario berekstensi .xml menggunakan *tools* SUMO dengan bantuan *file* skrip berekstensi .sumocfg. Selanjutnya konversikan *file* skenario berekstensi .xml tersebut menjadi *file* skenario berekstensi .tcl untuk dapat disimulasikan pada NS-2 menggunakan *tools* traceExporter. Perintah untuk menggunakan *tools* tersebut sama dengan ketika membuat skenario *grid* di atas.

## Implementasi Modifikasi pada *Protocol* AODV

*Routing protocol* AODV merupakan salah satu *routing protocol* yang umum digunakan dalam simulasi VANET. Namun, *routing protocol* ini belum dilengkapi dengan aspek sekuritas sehingga memungkinkan penurunan performa yang cukup drastis ketika terjadi serangan. Beberapa serangan yang memungkinkan terjadi adalah *Black hole* dan *Worm hole attack*.

Pada Tugas Akhir ini dilakukan modifikasi pada *routing protocol* AODV guna menambahkan aspek sekuritas untuk menjaga performa *routing protocol*. Berikut perubahan yang dilakukan pada *routing protocol* AODV:

* Modifikasi *packet header*
* Penambahan evaluasi pada tiap *node*
* Implementasi ECDSA
* Modifikasi pemilihan *node*

Kode implementasi dari *routing protocol* AODV pada NS-2 versi 2.35 berada pada direktori ns-2.35/aodv. Di dalam diretori tersebut terdapat beberapa *file*, diantaranya aodv.cc, aodv.h, dan aodv\_packet.h. Ketiga *file* tersebut akan dimodifikasi untuk dapat mengatasi *Black hole* dan *Worm hole attack* yang telah disebutkan sebelumnya.

Pada bagian ini penulis akan menjelaskan langkah-langkah dalam mengimplementasikan modifikasi *routing protocol* AODV untuk mengatasi *Black hole* dan *Worm hole attack*.

### Modifikasi Makefile

Untuk dapat memanggil dan menjalankan *library* OpenSSL pada NS-2 dilakukan modifikasi pada Makefile. *File* ini terdapat pada direktori ns2.35. Perubahan yang dilakukan pada Makefile ini dapat dilihat pada Gambar 4.12.

LIB = \

-L/home/tities/Documents/TA/ns-allinone-2.35/tclcl-1.20 -ltclcl -L/home/tities/Documents/TA/ns-allinone-2.35/otcl-1.14 -lotcl -L/home/tities/Documents/TA/ns-allinone-2.35/lib -ltk8.5 –

L/home/tities/Documents/TA/ns-allinone-2.35/lib -ltcl8.5 \

**-L/usr/include/openssl -lssl -lcrypto\**

-lXext -lX11 \

-lnsl -ldl \

-lm -lm

Gambar . Modifikasi Makefile

### Modifikasi *Packet Header*

Seperti yang telah dijelaskan pada subbab, aspek sekuritas yang ditambahkan adalah dengan mengimplementasikan ECDSA sebagai algoritma *digital signature* untuk menjaga keaslian paket data. Oleh karena itu diperlukan beberapa variabel untuk menambahkan *digital signature* pada *packet header* yang dikirimkan.

Untuk menambahkan variabel tersebut pada *packet header*, dilakukan modifikasi pada *file* aodv\_packet.h. Variabel-variabel yang ditambahkan diletakkan pada struktur data *packet header request*. Agar dapat menyimpan *public key* dan *digital signature*, diperlukan inisialisasi untuk memanggil *library* OpenSSL. Daftar *library* OpenSSL yang dilibatkan dapat dilihat pada Gambar 4.13.

#include <openssl/sha.h>

#include <openssl/ec.h>

#include <openssl/obj\_mac.h>

#include <openssl/ecdsa.h>

Gambar . Daftar *library* OpenSSL yang digunakan

Kemudian ditambahkan beberapa variabel diantaranya int record, char mdString[SHA256\_DIGEST\_LENGTH\*2+1], EC\_KEY \*eckey, dan ECDSA\_SIG \*signature. Variabel record digunakan untuk mengetahui darimana paket tersebut dikirim atau di*forward*. Variabel ini digunakan pada saat proses evaluasi tiap node yang akan dijelaskan pada subbab, Variabel mdString digunakan untuk menyimpan nilai *hash* dari isi paket. Variabel eckey digunakan untuk menyimpan *public key*, sedangkan variabel signature digunakan untuk menyimpan *digital signature*. Kode implementasi perubahan struktur *packet header* dapat dilihat pada Gambar 4.14.

struct hdr\_aodv\_request {

...

int record;

char mdString[SHA256\_DIGEST\_LENGTH\*2+1];

EC\_KEY \*eckey;

ECDSA\_SIG \*signature;

...

}

Gambar . Perubahan struktur *packet header*

### Penambahan Evaluasi pada Tiap *Node*

Evaluasi pada tiap *node* ini dilakukan untuk dapat mendeteksi *node neighbor* yang kemungkinan melakukan *Black hole attack*. Secara teknis, tiap *node* akan menghitung jumlah paket yang diterima dan jumlah paket yang dikirimkan kepada *neighbor*nya, kemudian dilakukan perbandingan dari hasil jumlah tersebut. Penambahan evaluasi ini diletakkan pada *file* aodv.cc. Untuk dapat melakukan evaluasi ini, terlebih dahulu setiap *node* harus mengetahui siapa saja *node* tetangganya. Oleh karena itu, *hello packet* harus diaktifkan terlebih dahulu. Pengaktifan *hello packet* dapat dilihat pada Gambar 4.15.

**//#ifndef AODV\_LINK\_LAYER\_DETECTION**

htimer.handle((Event\*) 0);

ntimer.handle((Event\*) 0);

**//#endif // LINK LAYER DETECTION**

Gambar . Pengaktifan *hello packet*

Setelah *hello packet* diaktifkan, diperlukan sebuah variabel yang digunakan untuk menyimpan *node neighbor* dari tiap *node* yaitu std::vector<std::vector<int>> myneigh(50). Kode implementasi penyimpanan *node neighbor* ini dilakukan pada fungsi AODV::recvHello dan dapat dilihat pada lampiran A.2.

Kemudian diperlukan beberapa variabel untuk menjumlahkan paket yang diterima oleh *node* a dari *node* b dan paket yang dikirim dari *node* a ke *node* b, serta variabel untuk membandingkan keduanya. Variabel-variabel tersebut diantaranya int kirimdari[50][50], int kirimke[50][50], double forward\_eval[50][50]. Gambaran inisialisasi variabel dapat dilihat pada Gambar 4.16.

std::vector<std::vector<int> > myneigh(50);

int kirimdari[50][50] = {0};

int kirimke[50][50] = {0};

double forward\_eval[50][50] = {0.0};

Gambar . Inisialisasi variabel

Selanjutnya setiap *node* akan menjumlahkan paket yang diterima dari *node* tetangganya setiap kali menerima paket. *Node* tersebut juga akan menjumlahkan paket yang dikirimkan kepada *node* tetangganya setiap akan melakukan *forward*. Kemudian *node* tersebut membandingkan jumlah paket yang diterima dengan jumlah paket yang dikirimkan dan menyimpan nilainya pada variabel forward\_eval. Nilai dari variabel tersebut akan dijadikan bahan evaluasi ketika akan memilih apakah *node* yang akan dijadikan *nexthop node* adalah *node* yang aman. Kode implementasi evaluasi ini diletakkan pada fungsi AODV::recvRequest dan dapat dilihat pada lampiran A.3.

### Implementasi ECDSA

Implementasi ECDSA diletakkan pada *file* aodv.cc. ECDSA digunakan sebagai algoritma *digital signature* untuk menjaga keaslian paket yang diterima oleh suatu *node*. *Malicious node* dapat dideteksi melakukan *Worm hole attack* oleh *node* tetangganya dengan melakukan pengecekan *digital signature* yang sebelumnya telah ditambahkan pada *packet header*. Untuk mengimplementasikan ECDSA ini diperlukan *library* OpenSSL yang dipanggil terlebih dahulu seperti yang ditunjukkan pada Gambar 4.13.

Secara garis besar, implementasi ECDSA ini dibagi menjadi dua tahap yaitu penandatanganan paket yang akan dikirim dan verifikasi *signature* yang ditambahkan pada *packet header*. Tahap penandatanganan paket dilakukan setiap kali *node* akan mengirimkan paket *request*. Kode implementasi penandatanganan paket diletakkan pada fungsi AODV::sendRequest dan dapat dilihat pada lampiran A.4.

Tahap verifikasi *signature* yang ditambahkan pada *packet header* dilakukan setiap kali *node* menerima paket. Beberapa variabel yang dibutuhkan yaitu int verified[50][50], dan double backward\_eval[50][50]. Jika paket lolos verifikasi, maka *counter* untuk paket terverifikasi dari *node* tetangganya akan di*increment* dengan disimpan pada variabel int verified. Namun jika paket tidak lolos verifikasi, maka *counter* tidak akan di*increment*. Jumlah dari *counter* ini dapat digunakan untuk mendapatkan hasil evaluasi oleh suatu *node* dari *node* tetangganya yang disimpan dalam backward\_eval. Nilai dari variabel tersebut juga akan dijadikan bahan evaluasi ketika akan melakukan pemilihan *node*. Kode implementasi verifikasi *signature* ini diletakkan pada fungsi AODV::recvRequest dan dapat dilihat pada lampiran A.3.

### Modifikasi Pemilihan *Node*

Modifikasi pemilihan *node* dilakukan ketika suatu *node* akan memilih *nexthop* untuk memastikan *node* yang akan dijadikan *nexthop* adalah *node* yang aman. Modifikasi ini diletakkan pada *file* aodv.cc. Sebelum *node* memilih *nexthop*, *node* tersebut akan mengakumulasikan nilai forward\_eval dan backward\_eval. Tiap nilai forward\_eval dan backward\_eval dikalikan dengan angka desimal *random* dari 0 sampai 1.

Setelah dikalikan dengan angka *random*, kedua nilai tersebut dijumlahkan dan disimpan pada variabel eval\_value[50][50]. Terdapat nilai *threshold* yang telah ditetapkan untuk membedakan apakah suatu *node* aman untuk dijadikan *nexthop*.

Dalam Tugas Akhir ini, penulis menetapkan nilai *threshold*nya adalah 0.7. Jika nilai eval\_value lebih dari 0.7, *node* tersebut bisa dijadikan *nexthop*. Namun jika sebaliknya, maka *node* tersebut tidak dijadikan *nexthop*. Kode modifikasi pemilihan *node* ini diletakkan pada fungsi AODV::recvRequest dan dapat dilihat pada lampiran A.3.

## Implementasi Simulasi pada NS-2

Implementasi simulasi VANET diawali dengan pendeskripsian lingkungan simulasi pada sebuah *file* tcl. *File* ini berisikan konfigurasi setiap *node* dan langkah-langkah yang dilakukan selama simulasi. Potongan konfigurasi lingkungan simulasi dapat dilihat pada Gambar 4.17.

set val(chan) Channel/WirelessChannel

set val(prop) Propagation/TwoRayGround

set val(netif) Phy/WirelessPhy

set val(mac) Mac/802\_11

set val(ifq) Queue/DropTail/PriQueue

set val(ll) LL

set val(ant) Antenna/OmniAntenna

set val(ifqlen) 50

set val(nn) 30

set val(rp) AODV

set val(energymodel) EnergyModel

set val(initialenergy) 100

set val(lm) "off"

set val(x) 1700

set val(y) 1700

set val(stop) 200

set val(cp) "traffic"

set val(sc) "scenario.tcl"

Gambar . Konfigurasi lingkungan simulasi

Pada konfigurasi dilakukan pemanggilan terhadap *file* traffic yang berisikan konfigurasi *node* asal dan *node* tujuan, serta *file* skenario yang berisi pergerakan node yang telah di*generate* oleh SUMO. Kode implementasi pada NS-2 dapat dilihat pada lampiran

### Implementasi *Black hole Attack*

Selain konfigurasi lingkungan simulasi dan pergerakan *node*, dilakukan juga konfigurasi untuk menugaskan *node* yang akan melakukan *Black hole attack* dan bagaimana *node* tersebut melakukan tugasnya sebagai *attacker*. Konfigurasi dilakukan di beberapa *file*, diantaranya *file* tcl, aodv.h, dan aodv.cc.

Pada *file* tcl, suatu *node* ditugaskan menjadi *Black hole attacker* dengan memberikan tambahan *kode* seperti yang ditunjukkan oleh Gambar 4.18.

$ns\_ at 0.0 "[$node\_(4) set ragent\_] hacker"

Gambar . Potongan kode untuk menugaskan *node* sebagai *Black hole attacker*

Setelah itu, pada *file* aodv.h dilakukan modifikasi dengan menambahkan variabel bool malicious yang digunakan untuk menandai jika suatu *node* adalah *malicious node* yang melakukan *Black hole attack*.

Agar *node* yang ditugaskan menjadi *Black hole attacker* dapat melakukan *Black hole attack*, dilakukan modifikasi pada *file* aodv.cc. Modifikasi pertama yang dilakukan adalah mengenali *attacker* yang telah dideklarasikan di file tcl. Modifikasi ini diletakkan pada fungsi AODV::command, kode untuk mengenali *attacker* dapat dilihat pada Gambar 4.19.

if(strncasecmp(argv[1], "hacker", 6) == 0) {

malicious = true;

return TCL\_OK;

}

Gambar . Potongan kode untuk mengenali *Black hole attacker*

Selanjutnya menginisialisasi variabel malicious diletakkan pada fungsi AODV::AODV, inisialisasi dapat dilihat pada Gambar 4.20.

malicious = false;

Gambar . Inisialisasi variabel malicious

*Black hole attack* dilakukan dengan melakukan *drop* pada setiap paket yang diterima. Untuk dapat melakukan itu, dilakukan modifikasi pada fungsi AODV::rt\_resolve dengan menambahkan kode seperti pada Gambar 4.21.

if (malicious == true ) {

drop(p, DROP\_RTR\_ROUTE\_LOOP);

return;

}

Gambar . Potongan kode untuk melakukan *drop* paket

Selain melakukan *drop* pada paket, *attacker* juga mengirimkan respon kepada *node* asal sehingga *node* asal mengira bahwa paket yang ia kirimkan telah diterima. Untuk dapat melakukan hal tersebut, dilakukan modifikasi pada fungsi AODV::recvRequest dengan menambahkan kode seperti pada Gambar 4.22.

else if (malicious == true) {

seqno = max(seqno, rq->rq\_dst\_seqno)+1;

if (seqno%2) seqno++;

sendReply(rq->rq\_src,

1,

rq->rq\_dst,

seqno,

MY\_ROUTE\_TIMEOUT,

rq->rq\_timestamp);

Packet::free(p);

}

Gambar . Potongan kode *Black hole attacker* mengirim paket *reply*

### Implementasi *Worm hole Attack*

Sama seperti implementasi *Black hole attack*, *file* yang diperlukan untuk konfigurasi antara lain *file* tcl, aodv.h dan aodv.cc. Konfigurasi pertama yang dilakukan adalah dengan menugaskan suatu *node* untuk menjadi *Worm hole attacker* dengan menambahkan kode pada *file* tcl seperti pada Gambar 4.23.

$ns\_ at 0.0 "[$node\_(4) set ragent\_] wormhole"

Gambar . Potongan kode untuk menugaskan *node* sebagai *Worm hole attacker*

Kemudian pada *file* aodv.h dilakukan modifikasi dengan menambahkan variabel bool worm yang digunakan untuk menandai apakah suatu *node* adalah *malicious node* yang melakukan *Worm hole attack*.

Selanjutnya dilakukan modifikasi pada *file* aodv.cc agar *node* dapat melakukan *Worm hole attack*. Sama seperti implementasi *Black hole attack*, hal pertama yang dilakukan adalah mengenali jika suatu *node* ditugaskan melakukan *Worm hole attack* dengan menambahkan kode pada fungsi AODV::command seperti pada Gambar 4.24.

if(strncasecmp(argv[1], "wormhole", 8) == 0){

worm = true;

return TCL\_OK;

}

Gambar . Potongan kode untuk mengenali *Worm hole attacker*

Variabel worm diinisialisasi terlebih dahulu nilainya dengan melakukan modifikasi pada fungsi AODV::AODV seperti yang ditunjukkan pada Gambar 4.25.

worm = false;

Gambar . Inisialisasi variabel worm

*Worm hole attack* dilakukan dengan memodifikasi isi paket oleh *node* yang berada di antara *node* asal dan *node* tujuan. Dalam Tugas Akhir ini, isi paket yang diubah adalah *node* tujuan. Selain mengubah isi paket, *Worm hole attacker* mengirimkan respon kepada *node* asal sehingga *node* asal mengira bahwa paketnya telah tersampaikan dengan aman. Modifikasi untuk mengimplementasikan hal tersebut diletakkan pada fungsi AODV::recvRequest dengan menambahkan kode seperti yang ditunjukkan pada Gambar 4.26.

if(worm == true){

seqno = max(seqno, rq->rq\_dst\_seqno)+1;

if (seqno%2) seqno++;

sendReply(rq->rq\_src,

1,

rq->rq\_dst,

seqno,

MY\_ROUTE\_TIMEOUT,

rq->rq\_timestamp);

rq->rq\_dst = 3;

}

Gambar . Potongan kode untuk mengirim paket *reply* dan memodifikasi paket yang diterima

## Implementasi Metrik Analisis

Simulasi yang telah dijalankan oleh NS-2 menghasilkan keluaran sebuah *trace file* yang berisikan data mengenai apa saja yang terjadi selama simulasi dalam bentuk *plain text*. Dari data *trace file*, dapat dilakukan analisis performa *routing protocol* dengan mengukur beberapa metrik. Pada Tugas Akhir ini, metrik yang akan dianalisis adalah *Packet Delivery Ratio* (PDR), Rata-rata *End to End Delay* (E2E), dan *Routing Overhead* (RO).

### Implementasi *Packet Delivery Ratio* (PDR)

Pada bagian telah ditunjukkan contoh struktur data *event* yang dicatat dalam *trace file* oleh NS-2. Kemudian, pada persamaan telah dijelaskan bagaimana menghitung PDR. Dengan begitu, dilakukan penghitungan PDR melalui bantuan skrip awk. Skrip awk untuk menghitung PDR berdasarkan kedua informasi tersebut dapat dilihat pada lampiran A.5.

Dalam perhitungan PDR, kata kunci yang perlu diperhatikan dari *trace file* adalah *layer* AGT, karena kata kunci tersebut menunjukkan *event* yang bersangkutan dengan paket komunikasi data. Kemudian hitung jumlah paket yang dikirimkan dan paket yang diterima dengan menggunakan karakter pada kolom pertama sebagai *filter*, karena kolom pertama yang menunjukkan *event* yang terjadi dari sebuah paket. Setelah itu nilai PDR dapat dihitung dengan persamaan yang telah dijelaskan. *Pseudocode* untuk menghitung PDR dapat dilihat pada Gambar 4.27.

sent = 0

received = 0

for i = 1 to the number of rows

if in a row contains “s” and AGT then

sent++

else if in a row contains “r” and AGT then

received++

end if

pdr = received / sent

Gambar . Pseudocode untuk menghitung PDR

Contoh perintah pengeksekusian skrip awk untuk menganalisis *trace file* beserta *output*nya dapat dilihat masing-masing pada Gambar 4.28 dan Gambar 4.29.

awk –f pdr.awk s-aodv2.tr

Gambar . Perintah pengeksekusian skrip awk PDR

Gambar . *Output* skrip awk PDR

pdr: xx.xx (float number)

### Implementasi Rata-rata *End to End Delay* (E2E)

Perhitungan E2E telah dijelaskan melalui persamaan. Skrip awk untuk menghitung E2E dapat dilihat pada lampiran A.6.

Dalam perhitungan E2E, langkah yang digunakan untuk mendapatkan E2E hampir sama dengan ketika mencari PDR, hanya saja yang perlu diperhatikan adalah waktu dari sebuah *event* yang tercatat pada kolom ke-2 dengan *filter event* pada kolom ke-4 adalah layer AGT dan *event* pada kolom pertama guna membedakan paket dikirim atau diterima. Setelah seluruh baris yang memenuhi didapatkan, akan dihitung *delay* dari paket dengan mengurangi waktu dari paket diterima dengan waktu dari paket dikirim dengan sayarat memiliki *id* paket yang sama.

Setelah mendapatkan *delay* paket, langkah selanjutnya adalah dengan mencari rata-rata dari *delay* tersebut dengan menjumlahkan semua *delay* paket dan membaginya dengan jumlah paket. *Pseudocode* untuk menghitung rata-rata *end to end delay* dapat dilihat pada Gambar 4.30.

sum\_delay = 0

counter = 0

for i = 1 to the number of rows

counter++

if layer == AGT and event == s then

start\_time[packet\_id] = time

else if layer == AGT and event == r then

end\_time[packet\_id] = time

end if

delay[packet\_id] = end\_time[packet\_id] – start\_time[packet\_id]

sum\_delay += delay[packet\_id]

e2e = sum\_delay / counter

Gambar . Pseudocode untuk menghitung E2E

Contoh perintah pengeksekusian skrip awk untuk menganalisis *trace file* beserta *output*nya dapat dilihat masing-masing pada Gambar 4.31 dan Gambar 4.32.

awk –f e2e.awk s-aodv2.tr

Gambar . Perintah pengeksekusian skrip awk E2E

e2e: xx.xx (float number)

Gambar . *Output* skrip awk E2E

### Implementasi *Routing Overhead* (RO)

Perhitungan RO telah dijelaskan pada persamaan. Skrip awk untuk menghitung RO dapat dilihat pada lampiran A.7.

Seperti yang telah dijelaskan sebelumnya, *routing overhead* merupakan jumlah dari paket kontrol *routing* baik itu RREQ, RREP, maupun RERR. Dengan begitu, untuk mendapatkan RO yang perlu dilakukan adalah menjumlahkan tiap paket dengan *filter event sent* pada kolom pertama dan *event layer* RTR pada kolom ke-4. *Pseudocode* untuk menghitung RO dapat dilihat pada Gambar 4.33.

ro = 0

for i = 1 to the number of rows

if in a row contains “s” and RTR and is not hello packet then

ro++

end if

Gambar . Pseudocode untuk menghitung RO

Contoh perintah pengeksekusian skrip awk untuk menganalisis *trace file* beserta outputnya dapat dilihat masing-masing pada Gambar 4.34 dan Gambar 4.35.

awk –f ro.awk s-aodv2.tr

Gambar . Perintah pengeksekusian skrip awk RO

ro: xxx (integer number)

Gambar . *Output* skrip awk RO

***[Halaman ini sengaja dikosongkan]***

# BAB V HASIL UJI COBA DAN EVALUASI

Bab ini membahas mengenai uji coba dan evaluasi dari skenario yang telah disimulasikan di NS-2.

## Lingkungan Uji Coba

Uji coba dilakukan pada perangkat dengan spesifikasi seperti yang tertera pada tabel 5.1.

Tabel . Spesifikasi perangkat yang digunakan

|  |  |
| --- | --- |
| **Komponen** | **Spesifikasi** |
| **CPU** | Intel(R) Core(TM) i3-3217U CPU @ 1.80 GHz x 2 |
| **Sistem Operasi** | Linux Mint 17.3 Cinnamon 64-bit |
| **Linux Kernel** | 3.19.0-32-generic |
| **Memori** | 1.8 GiB |
| **Penyimpanan** | 26.5 GB |

Pengujian dilakukan dengan menjalankan skenario yang disimulasikan pada NS-2. Dari simulasi tersebut dihasilkan sebuah trace file dengan ekstensi.tr yang akan dianalisis dengan bantuan skrip awk untuk mendapatkan packet delivery ratio, rata-rata end to end delay, dan routing overhead menggunakan kode pada lampiran masing-masing A.5, A.6, dan A.7.

## Hasil Uji Coba

Hasil uji coba dari skenario *grid* dan skenario *real* dapat dilihat sebagai berikut:

### Hasil Uji Coba Skenario *Grid*

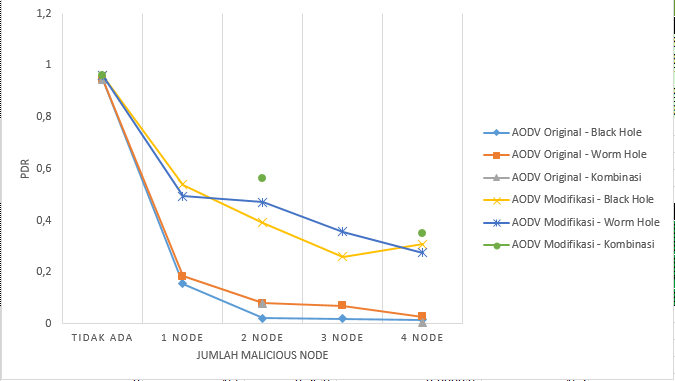
Pengujian pada skenario *grid* digunakan untuk melihat perbandingan *packet delivery ratio*, *rata-rata end to end delay*, dan *routing overhead* antara *routing protocol* AODV *original* dan *routing protocol* AODV yang telah dimodifikasi ketika terjadi serangan *Blackhole*, *Wormhole*, maupun keduanya di satu waktu, dengan kondisi peta yang lebih stabil dan mempunyai kecenderungan persebaran *node* yang merata.

Pengujian dilakukan sesuai dengan perancangan parameter lingkungan simulasi yang dapat dilihat pada tabel 3.1. Selain itu, ditambahkan beberapa *malicious node* dengan beberapa variasi serangan dalam satu skenario.

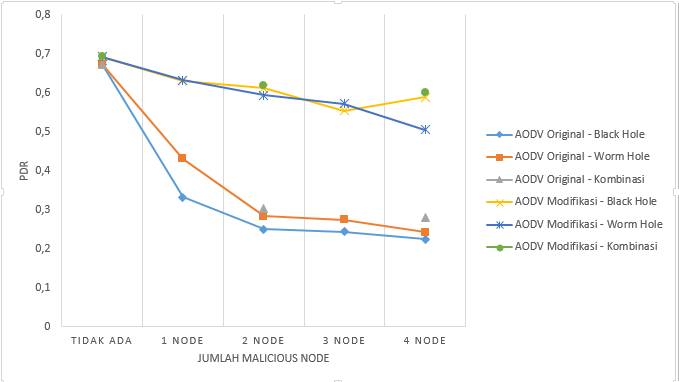
Pengambilan data uji PDR, rata-rata *end to end delay*, dan *routing overhead* dengan luas area 1700 m x 1700 m dan *node* sebanyak 30, 40, dan 50 dilakukan pada kecepatan standar yaitu 20 m/s. Pada skenario 30 *node*, dilakukan variasi serangan dengan jumlah malicious *node* yang bertambah dari 1 *node* hingga 2 *node*. Sedangkan pada skenario 40 dan 50 *node*, jumlah malicious *node* bertambah dari 1 *node* hingga 4 *node*. Pada tiap *malicious node*, ditugaskan untuk menjadi *Blackhole attacker* dan *Wormhole attacker*. Untuk jumlah lebih dari 1 *malicious node*, dilakukan beberapa variasi serangan, yaitu semua *malicious node* melakukan *Blackhole attack*, semua *malicious node* melakukan *Wormhole attack*, dan sebagian melakukan *Blackhole attack*, sedangkan sebagian yang lain melakukan *Wormhole attack*.

Pengujian dilakukan dengan beberapa variasi serangan yang berbeda untuk melihat pengaruh serangan pada performa routing protocol AODV dan seberapa banyak *malicious node* beserta variasi serangannya yang dapat diatasi oleh *routing protocol* AODV yang telah dimodifikasi.

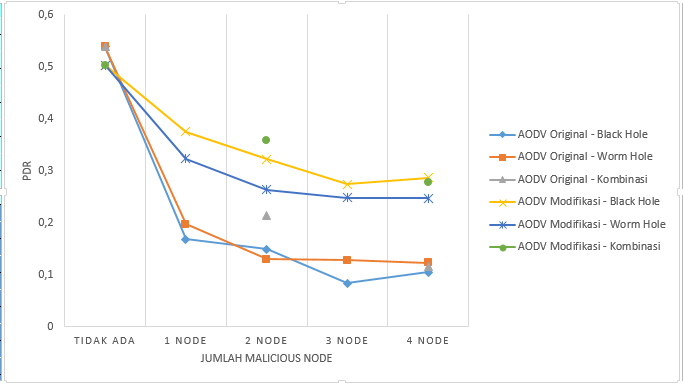
Hasil pengambilan data *packet delivery ratio* (PDR) pada skenario *grid* 30, 40, dan 50 *node* masing-masing dapat dilihat pada Gambar 5.1, Gambar 5.2, dan Gambar 5.3.



Gambar . Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 30 *node*



Gambar . Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 40 *node*

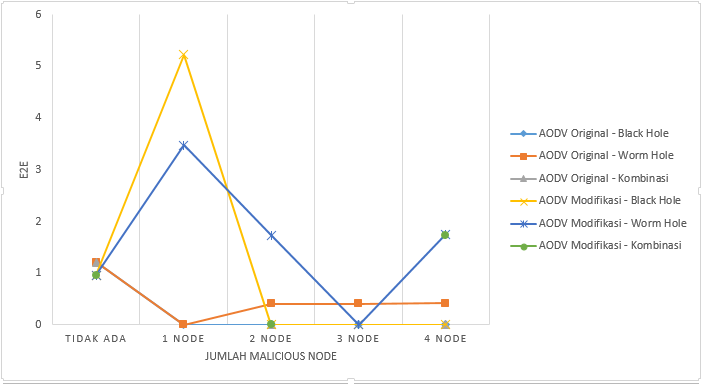


Gambar . Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 50 *node*

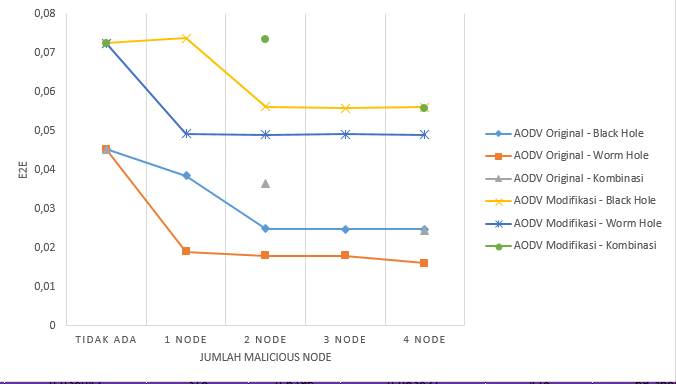
Berdasarkan grafik pada Gambar 5.1, Gambar 5.2, dan Gambar 5.3 dapat dilihat bahwa *routing protocol* AODV yang telah dimodifikasi mampu mengatasi *Black hole*, dan *Worm hole attack* maupun kombinasi keduanya, yang ditunjukkan oleh mampunya *protocol* melakukan *recovery* paket data yang sempat turun drastis akibat terjadinya serangan. Dengan mengimplementasikan beberapa metode yang telah dipaparkan pada bab sebelumnya, *routing protocol* ini mampu melakukan recovey paket data hingga 53,94%.

Jika ketiga grafik tersebut dibandingkan, dapat dilihat bahwa dengan *node* yang lebih banyak, selisih antara paket data yang hilang dan paket data yang di*recovery* menjadi kurang signifkan. Selain kepadatan *node*, letak dan pergerakan *malicious node* juga mempengaruhi performa *routing protocol*. Jika *malicious node* terus bergerak di antara *node-node* yang menjadi rute normal, maka paket data yang dapat di*recovery* menjadi semakin sedikit.

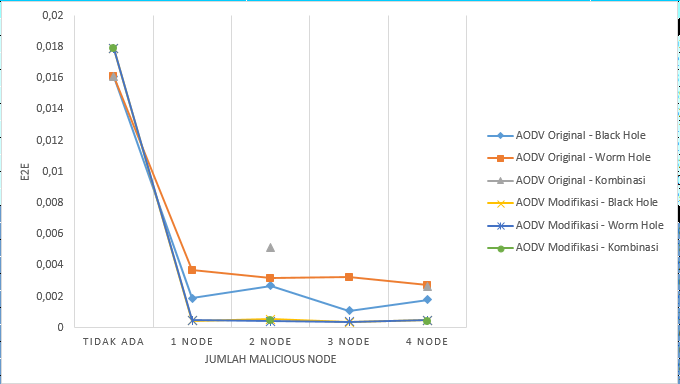
Hasil pengambilan data rata-rata *end to end delay* (E2E) pada skenario *grid* 30, 40, dan 50 *node* dapat dilihat masing-masing pada Gambar 5.4, Gambar 5.5, dan Gambar 5.6.



Gambar . Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 30 *node*



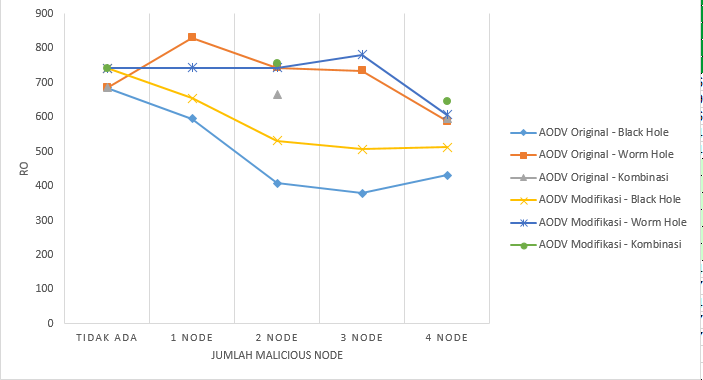
Gambar . Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 40 *node*



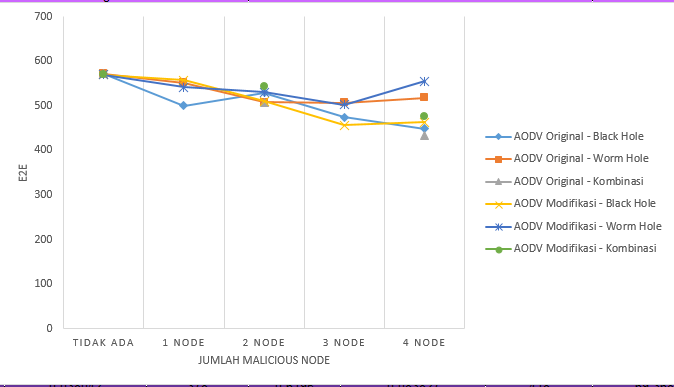
Gambar . Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 50 *node*

Berdasarkan grafik pada Gambar 5.4, Gambar 5.5, dan Gambar 5.6 dapat dilihat bahwa rata-rata *end to end delay* antara *routing protocol* AODV *original* dan AODV yang telah dimodifkasi tidak selalu lebih besar dan tidak selalu lebih kecil. Pada grafik-grafik diatas, *delay* menjadi lebih besar ketika paket yang sampai ke tujuan lebih banyak, begitu pula sebaliknya.

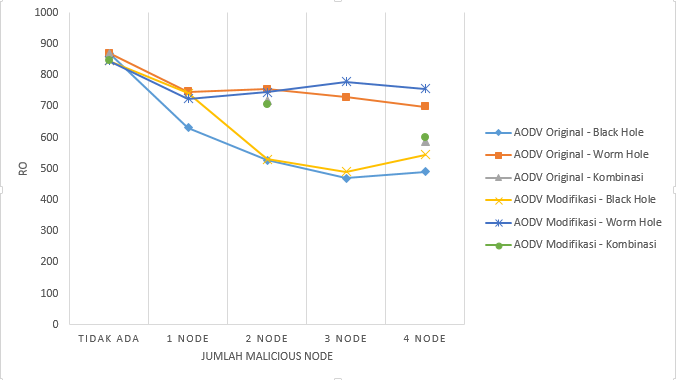
Hasil pengambilan data *routing overhead* (RO) pada skenario *grid* 30, 40, dan 50 *node* dapat dilihat masing-masing pada Gambar 5.7, Gambar 5.8, dan Gambar 5.9.



Gambar . Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 30 *node*



Gambar . Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 40 *node*



Gambar . Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *grid* 50 *node*

Berdasarkan grafik pada Gambar 5.7, Gambar 5.8, dan Gambar 5.9 dapat dilihat bahwa *routing protocol* AODV yang telah dimodifkasi tidak selalu dapat mengatasi *routing overhead* yang disebabkan oleh serangan. Ada di beberapa skenario uji coba saat *routing protocol* ini dapat meredakan *routing overhead*, namun hal tersebut tidak selalu terjadi.

### Hasil Uji Coba Skenario *Real*

Pengujian pada skenario *real* digunakan untuk melihat perbandingan performa *routing protocol* AODV *original* dengan *routing protocol* AODV yang telah dimodifikasi ketika terjadi serangan, dalam hal ini adalah *Black Hole attack* dan *Worm Hole attack*, maupun kombinasi keduanya jika diimplementasikan menggunakan peta nyata dimana persebaran kendaraannya tidak selalu merata. Pengambilan data uji *packet delivery ratio* (PDR), rata-rata *end to end delay* (E2E), dan *routing overhead* (RO) dilakukan pada peta *real* dengan luas area 1700 m x 1700 m pada wilayah perumahan Kertajaya Surabaya.

Hasil pengambilan data PDR pada skenario *real* 30, 40, dan 50 *node* dapat dilihat pada Gambar 5.10, Gambar 5.11, dan Gambar 5.12.

Gambar . Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 30 *node*

Gambar . Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 40 *node*

Gambar . Grafik PDR terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 50 *node*

Berdasarkan grafik pada Gambar 5.10, Gambar 5.11, dan Gambar 5.12 *routing protocol* AODV yang telah dimodifikasi mampu mengatasi *Black Hole*, dan *Worm Hole attack* maupun kombinasi keduanya dengan ditunjukkan oleh paket data yang dapat di*recovery* selama serangan terjadi. *Routing protocol* AODV yang telah dimodifikasi ini mampu melakukan *recovery* paket hingga 77,57%.

Pada ketiga grafik tersebut, terlihat bahwa pengaruh letak dan pergerakan *malicious node* lebih dominan dibandingkan dengan pengaruh kepadatan kendaraan. Hal ini ditunjukkan dengan kemampuan *recovery* paket pada skenario 40 dan 50 *node* lebih baik dibandingkan dengan skenario 30 *node*.

Hasil pengambilan data E2E pada skenario *real* 30, 40, dan 50 *node* dapat dilihat pada Gambar 5.13, Gambar 5.14, dan Gambar 5.15.

Gambar . Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 30 *node*

Gambar . Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 40 *node*

Gambar . Grafik E2E terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 50 *node*

Berdasarkan grafik pada gambar Gambar 5.13, Gambar 5.14, dan Gambar 5.15 perbandingan rata-rata *end to end delay* antara *routing protocol* AODV yang telah dimodifikasi dengan *routing protocol* AODV original hampir sama dengan ketika diimplementasikan pada skenario *grid*. Namun pada skenario *real* 50 *node*, grafik *rata-rata end to end delay* ketika terjadi serangan terlihat relatif lebih stabil dibandingkan dengan skenario *real* 30 dan 40 *node*.

Hasil pengambilan data RO pada skenario *real* 30, 40, dan 50 *node* dapat dilihat pada Gambar 5.16, Gambar 5.17, dan Gambar 5.18.

Gambar . Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 30 *node*

Gambar . Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 40 *node*

Gambar . Grafik RO terhadap banyak *malicious node* dan variasi serangannya pada skenario *real* 50 *node*

Berdasarkan grafik pada Gambar 5.16, Gambar 5.17, dan Gambar 5.18 perbandingan *routing overhead* antara *routing protocol* AODV yang telah dimodifikasi dengan *routing protocol* AODV *original* hampir sama dengan ketika diimplementasikan pada skenario *grid*. Hal ini menunjukkan bahwa *routing protocol* AODV yang telah dimodifikasi belum mampu untuk dapat selalu mengatasi *routing overhead* ketika terjadi serangan.

# BAB VI KESIMPULAN DAN SARAN

Pada bab ini akan diberikan kesimpulan yang diperoleh dari Tugas Akhir yang telah dikerjakan dan saran tentang pengembangan dari Tugas Akhir ini yang dapat dilakukan di masa yang akan datang.

## Kesimpulan

Kesimpulan yang diperoleh dari hasil uji coba dan evaluasi Tugas Akhir ini adalah sebagai berikut:

* + 1. Pengimplementasian ECDSA dan evaluasi pada tiap *node* dapat mengatasi *Black Hole* dan *Worm Hole attack* maupun kombinasi keduanya.
    2. Kemampuan *routing protocol* untuk memperbaiki *packet delivery ratio* (PDR) dapat mencapai 53,94% pada skenario *grid* dan 77,57% pada skenario *real*.
    3. Pengimplementasian ECDSA dan evaluasi pada tiap *node* tidak selalu dapat mengatasi *routing overhead* yang disebabkan oleh serangan.
    4. Kepadatan lalu lintas, letak dan pergerakan *malicious node* dapat mempengaruhi performa *routing protocol*.

## Saran

Saran yang diberikan dari hasil uji coba dan evaluasi Tugas Akhir ini adalah sebagai berikut:

1. Dapat dilakukan metode lain atau menambahkan metode lagi untuk dapat mengatasi *routing overhead* yang disebabkan oleh serangan.
2. Pengimplementasian Elliptic Curve Digital Signature Algorithm dan evaluasi pada tiap *node* dapat dilakukan pada *routing protocol* lain, seperti GPSR, DSR, dsb.
3. Pengimplementasian *digital signature* untuk memvalidasi keaslian paket dapat dilakukan dengan menggunakan algoritma *digital signature* yang lain.
4. Dapat dilakukan penambahan metode guna meningkatkan aspek sekuritas pada *routing protocol* untuk mengatasi variasi *Wormhole attack* yang lain, seperti *Out of Band Wormhole attack*, maupun variasi lain yang dilakukan oleh dua *malicious node* yang bekerja sama.

# DAFTAR PUSTAKA

[1] Y. Liu, J. Bi, and J. Yang, “Research on Vehicular Ad Hoc Networks,” in *2009 Chinese Control and Decision Conference*, 2009, pp. 4430–4435.

[2] J. Hou, J. Liu, L. Han, and J. Zhao, “Secure and efficient protocol for position-based routing in VANETs,” in *2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment*, 2012, pp. 142–148.

[3] Y. Wang and F. Li, “Vehicular Ad Hoc Networks,” in *Guide to Wireless Ad Hoc Networks*, S. Misra, I. Woungang, and S. C. Misra, Eds. Springer London, 2009, pp. 503–525.

[4] C. Sommer and F. Dressler, *Vehicular Networking*. Cambridge University Press, 2014.

[5] S. Bitam, A. Mellouk, and S. Zeadally, “HyBR: A Hybrid Bio-inspired Bee swarm Routing protocol for safety applications in Vehicular Ad hoc NETworks (VANETs),” *J. Syst. Archit.*, vol. 59, no. 10, Part B, pp. 953–967, Nov. 2013.

[6] J. Jamal, “Routing Protocols in MANETs,” *Eexploria*, 18-Sep-2012. .

[7] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, “Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach,” in *2009 International Conference on Future Computer and Communication*, 2009, pp. 16–20.

[8] Acevpn, “Elliptic Curve IPSEC IKEv2 VPN Service - Next Gen Security,” *Acevpn.com*, 03-Jun-2014. .

[9] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” *Hum.-Centric Comput. Inf. Sci.*, vol. 1, no. 1, p. 4, Nov. 2011.

[10] “ResearchGate,” *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/51956520\_Different\_types\_of\_attacks\_in\_Mobile\_ADHOC\_Network. [Accessed: 23-May-2017].

[11] “The Network Simulator - ns-2.” [Online]. Available: http://www.isi.edu/nsnam/ns/. [Accessed: 13-Apr-2017].

[12] “Sumo\_at\_a\_Glance - SUMO - Simulation of Urban Mobility.” [Online]. Available: http://www.sumo.dlr.de/userdoc/Sumo\_at\_a\_Glance.html. [Accessed: 13-Apr-2017].

[13] “OpenStreetMap,” *OpenStreetMap*. [Online]. Available: https://www.openstreetmap.org/about. [Accessed: 13-Apr-2017].

[14] “AWK,” *Wikipedia*. 29-Apr-2017.

[15] “/index.html.” [Online]. Available: https://www.openssl.org/. [Accessed: 13-Apr-2017].

[16] A. Robbins, *Effective Awk Programming: Text Processing and Pattern Matching*. O’Reilly Media, Inc., 2001.

# 

# LAMPIRAN

## A.1 Kode Skenario NS-2

set val(chan) Channel/WirelessChannel;

set val(prop) Propagation/TwoRayGround;

set val(netif) Phy/WirelessPhy;

set val(mac) Mac/802\_11;

set val(ifq) Queue/DropTail/PriQueue;

set val(ll) LL;

set val(ant) Antenna/OmniAntenna;

set val(ifqlen) 50;

set val(nn) 30;

set val(rp) AODV;

set val(energymodel) EnergyModel;

set val(initialenergy) 100;

set val(lm) "off";

set val(x) 1700;

set val(y) 1700;

set val(stop) 200;

set val(cp) "traffic2";

set val(sc) "scenario30.tcl";

set ns\_ [new Simulator]

set tracefd [open s-aodv230.tr w]

set namtrace [open s-aodv230.nam w]

$ns\_ trace-all $tracefd

$ns\_ namtrace-all-wireless $namtrace $val(x) $val(y)

Agent/AODV set num\_nodes $val(nn)

set topo [new Topography]

$topo load\_flatgrid $val(x) $val(y)

create-god $val(nn)

set chan\_1\_ [new $val(chan)]

$ns\_ node-config -adhocRouting $val(rp) \

-llType $val(ll) \

-macType $val(mac) \

-channel $chan\_1\_ \

-ifqType $val(ifq) \

-ifqLen $val(ifqlen) \

-antType $val(ant) \

-propType $val(prop) \

-phyType $val(netif) \

-topoInstance $topo \

-agentTrace ON \

-routerTrace ON \

-macTrace ON \

-movementTrace ON \

for {set i 0} {$i < $val(nn)} {incr i} {

set node\_($i) [$ns\_ node]

}

source $val(cp)

source $val(sc)

for {set i 0} {$i < $val(nn)} {incr i} {

$ns\_ initial\_node\_pos $node\_($i) 100

}

for {set i 0} {$i < $val(nn)} { incr i} {

$ns\_ at $val(stop) "$node\_($i) reset"

}

$ns\_ at 200.01 "puts \"end simulation\" ; $ns\_ halt"

proc stop {} {

global ns\_ tracefd namtrace

$ns\_ flush-trace

close $tracefd

close $namtrace

}

$ns\_ run

## A.2 Kode Fungsi AODV::recvHello

void AODV::recvHello(Packet \*p) {

struct hdr\_aodv\_reply \*rp=HDR\_AODV\_REPLY(p);

AODV\_Neighbor \*nb;

nb = nb\_lookup(rp->rp\_dst);

if(nb == 0) {

nb\_insert(rp->rp\_dst);

}

else {

nb->nb\_expire = CURRENT\_TIME + (1.5 \* ALLOWED\_HELLO\_LOSS \* HELLO\_INTERVAL);

}

myneigh[(int)rp->rp\_dst].push\_back(index);

Packet::free(p);

}

## A.3 Kode Fungsi AODV::recvRequest

Void AODV::recvRequest(Packet \*p) {

struct hdr\_ip \*ih = HDR\_IP(p);

struct hdr\_aodv\_request \*rq = HDR\_AODV\_REQUEST(p);

aodv\_rt\_entry \*rt;

int function\_status = -1;

char string[SHA256\_DIGEST\_LENGTH];

strcpy(string,(char \*)&rq->rq\_type);

strcat(string,(char \*)&rq->rq\_bcast\_id);

strcat(string,(char \*)&rq->rq\_dst);

strcat(string,(char \*)&rq->rq\_dst\_seqno);

strcat(string,(char \*)&rq->rq\_src);

strcat(string,(char \*)&rq->rq\_src\_seqno);

SHA256((unsigned char\*)&string, strlen(string), (unsigned char\*)&hash);

char mdString[SHA256\_DIGEST\_LENGTH\*2+1];

for(int i = 0; i < SHA256\_DIGEST\_LENGTH; i++)

sprintf(&mdString[i\*2], "%02x", (unsigned int)hash[i]);

int verify\_status = ECDSA\_do\_verify(ucstr(mdString), strlen(mdString), rq->signature, rq->eckey);

const int verify\_success = 1;

if (verify\_success != verify\_status){

function\_status = -1;

}

else{

verified[rq->record][index]+=1;

function\_status = 1;

}

if(rq->rq\_src == index) {

fprintf(stderr, "%s: got my own REQUEST\n", \_\_FUNCTION\_\_);

Packet::free(p);

return;

}

if (id\_lookup(rq->rq\_src, rq->rq\_bcast\_id)) {

#ifdef DEBUG

fprintf(stderr, "%s: discarding request\n", \_\_FUNCTION\_\_);

#endif // DEBUG

Packet::free(p);

return;

}

id\_insert(rq->rq\_src, rq->rq\_bcast\_id);

aodv\_rt\_entry \*rt0;

rt0 = rtable.rt\_lookup(rq->rq\_src);

if(rt0 == 0) {

rt0 = rtable.rt\_add(rq->rq\_src);

}

rt0->rt\_expire = max(rt0->rt\_expire, (CURRENT\_TIME + REV\_ROUTE\_LIFE));

if ( (rq->rq\_src\_seqno > rt0->rt\_seqno ) ||

((rq->rq\_src\_seqno == rt0->rt\_seqno) &&

(rq->rq\_hop\_count < rt0->rt\_hops)) ) {

rt\_update(rt0, rq->rq\_src\_seqno, rq->rq\_hop\_count, ih->saddr(),max(rt0->rt\_expire, (CURRENT\_TIME + REV\_ROUTE\_LIFE)) );

if (rt0->rt\_req\_timeout > 0.0) {

rt0->rt\_req\_cnt = 0;

rt0->rt\_req\_timeout = 0.0;

rt0->rt\_req\_last\_ttl = rq->rq\_hop\_count;

rt0->rt\_expire = CURRENT\_TIME + ACTIVE\_ROUTE\_TIMEOUT;

}

assert (rt0->rt\_flags == RTF\_UP);

Packet \*buffered\_pkt;

while ((buffered\_pkt = rqueue.deque(rt0->rt\_dst))) {

if (rt0 && (rt0->rt\_flags == RTF\_UP)) {

assert(rt0->rt\_hops != INFINITY2);

forward(rt0, buffered\_pkt, NO\_DELAY);

}

}

}

rt = rtable.rt\_lookup(rq->rq\_dst);

if(rq->rq\_dst == index) {

#ifdef DEBUG

fprintf(stderr, "%d - %s: destination sending reply\n",index, \_\_FUNCTION\_\_);

#endif // DEBUG

seqno = max(seqno, rq->rq\_dst\_seqno)+1;

if (seqno%2) seqno++;

sendReply(rq->rq\_src, 1, index, seqno, MY\_ROUTE\_TIMEOUT, rq->rq\_timestamp);

Packet::free(p);

}

else if (malicious == true) {

seqno = max(seqno, rq->rq\_dst\_seqno)+1;

if (seqno%2) seqno++;

sendReply(rq->rq\_src, 1, rq->rq\_dst, seqno, MY\_ROUTE\_TIMEOUT, rq->rq\_timestamp);

Packet::free(p);

}

else if (rt && (rt->rt\_hops != INFINITY2) && (rt->rt\_seqno >= rq->rq\_dst\_seqno) ) {

assert(rq->rq\_dst == rt->rt\_dst);

sendReply(rq->rq\_src, rt->rt\_hops + 1, rq->rq\_dst, rt->rt\_seqno,(u\_int32\_t) (rt->rt\_expire - CURRENT\_TIME), rq->rq\_timestamp);

rt->pc\_insert(rt0->rt\_nexthop);

rt0->pc\_insert(rt->rt\_nexthop);

#ifdef RREQ\_GRAT\_RREP

sendReply(rq->rq\_dst, rq->rq\_hop\_count, rq->rq\_src, rq->rq\_src\_seqno,(u\_int32\_t) (rt->rt\_expire - CURRENT\_TIME), rq->rq\_timestamp);

#endif

Packet::free(p);

}

else {

ih->saddr() = index;

ih->daddr() = IP\_BROADCAST;

rq->rq\_hop\_count += 1;

if(worm == true){

seqno = max(seqno, rq->rq\_dst\_seqno)+1;

if (seqno%2) seqno++;

sendReply(rq->rq\_src, 1, rq->rq\_dst, seqno, MY\_ROUTE\_TIMEOUT, rq->rq\_timestamp);

rq->rq\_dst = 4;

}

backward\_eval[rq->record][index] = (double)verified[rq->record][index]/(double)kirimdari[rq->record][index];

rq->record = index;

for(int i=0; i < (int)myneigh[index].size(); i++){

if((int)rq->rq\_dst != (int)myneigh[index][i]){

kirimke[(int)myneigh[index][i]][index] += 1;

forward\_eval[(int)myneigh[index][i]][index] =(double)kirimdari[(int)myneigh[index][i]][index]/(double)kirimke[(int)myneigh[index][i]][index];

}

eval\_value[(int)myneigh[index][i]][index] = (double) rand()/(double) RAND\_MAX \* forward\_eval[(int)myneigh[index][i]][index] + (double) rand()/(double) RAND\_MAX \* backward\_eval[(int)myneigh[index][i]][index];

if(eval\_value[(int)myneigh[index][i]][index] > 0.7){

if (rt) rq->rq\_dst\_seqno = max(rt->rt\_seqno, rq->rq\_dst\_seqno);

}

}

}

forward((aodv\_rt\_entry\*) 0, p, DELAY);

}

}

## A.4 Kode Fungsi AODV::sendRequest

void

AODV::sendRequest(nsaddr\_t dst) {

Packet \*p = Packet::alloc();

struct hdr\_cmn \*ch = HDR\_CMN(p);

struct hdr\_ip \*ih = HDR\_IP(p);

struct hdr\_aodv\_request \*rq = HDR\_AODV\_REQUEST(p);

aodv\_rt\_entry \*rt = rtable.rt\_lookup(dst);

assert(rt);

if (rt->rt\_flags == RTF\_UP) {

assert(rt->rt\_hops != INFINITY2);

Packet::free((Packet \*)p);

return;

}

if (rt->rt\_req\_timeout > CURRENT\_TIME) {

Packet::free((Packet \*)p);

return;

}

if (rt->rt\_req\_cnt > RREQ\_RETRIES) {

rt->rt\_req\_timeout = CURRENT\_TIME + MAX\_RREQ\_TIMEOUT;

rt->rt\_req\_cnt = 0;

Packet \*buf\_pkt;

while ((buf\_pkt = rqueue.deque(rt->rt\_dst))) {

drop(buf\_pkt, DROP\_RTR\_NO\_ROUTE);

}

Packet::free((Packet \*)p);

return;

}

#ifdef DEBUG

fprintf(stderr, "(%2d) - %2d sending Route Request, dst: %d\n", ++route\_request, index, rt->rt\_dst);

#endif // DEBUG

rt->rt\_req\_last\_ttl = max(rt->rt\_req\_last\_ttl,rt->rt\_last\_hop\_count);

if (0 == rt->rt\_req\_last\_ttl) {

ih->ttl\_ = TTL\_START;

}

else {

if (rt->rt\_req\_last\_ttl < TTL\_THRESHOLD){

ih->ttl\_ = rt->rt\_req\_last\_ttl + TTL\_INCREMENT;

}

else {

ih->ttl\_ = NETWORK\_DIAMETER;

rt->rt\_req\_cnt += 1;

}

}

rt->rt\_req\_last\_ttl = ih->ttl\_;

rt->rt\_req\_timeout = 2.0 \* (double) ih->ttl\_ \* PerHopTime(rt);

if (rt->rt\_req\_cnt > 0)

rt->rt\_req\_timeout \*= rt->rt\_req\_cnt;

rt->rt\_req\_timeout += CURRENT\_TIME;

if (rt->rt\_req\_timeout > CURRENT\_TIME + MAX\_RREQ\_TIMEOUT)

rt->rt\_req\_timeout = CURRENT\_TIME + MAX\_RREQ\_TIMEOUT;

rt->rt\_expire = 0;

#ifdef DEBUG

fprintf(stderr, "(%2d) - %2d sending Route Request, dst: %d, tout %f ms\n",

++route\_request,

index, rt->rt\_dst,

rt->rt\_req\_timeout - CURRENT\_TIME);

#endif

ch->ptype() = PT\_AODV;

ch->size() = IP\_HDR\_LEN + rq->size();

ch->iface() = -2;

ch->error() = 0;

ch->addr\_type() = NS\_AF\_NONE;

ch->prev\_hop\_ = index;

ih->saddr() = index;

ih->daddr() = IP\_BROADCAST;

ih->sport() = RT\_PORT;

ih->dport() = RT\_PORT;

rq->rq\_type = AODVTYPE\_RREQ;

rq->rq\_hop\_count = 1;

rq->rq\_bcast\_id = bid++;

rq->rq\_dst = dst;

rq->rq\_dst\_seqno = (rt ? rt->rt\_seqno : 0);

rq->rq\_src = index;

seqno += 2;

assert ((seqno%2) == 0);

rq->rq\_src\_seqno = seqno;

rq->rq\_timestamp = CURRENT\_TIME;

rq->record = index;

char string[SHA256\_DIGEST\_LENGTH];

strcpy(string,(char \*)&rq->rq\_type);

strcat(string,(char \*)&rq->rq\_bcast\_id);

strcat(string,(char \*)&rq->rq\_dst);

strcat(string,(char \*)&rq->rq\_dst\_seqno);

strcat(string,(char \*)&rq->rq\_src);

strcat(string,(char \*)&rq->rq\_src\_seqno);

SHA256((unsigned char\*)&string, strlen(string), (unsigned char\*)&hash);

char mdString[SHA256\_DIGEST\_LENGTH\*2+1];

for(int i = 0; i < SHA256\_DIGEST\_LENGTH; i++)

sprintf(&mdString[i\*2], "%02x", (unsigned int)hash[i]);

strcpy(rq->mdString,mdString);

int function\_status = -1;

rq->eckey = EC\_KEY\_new();

if (NULL == rq->eckey){

function\_status = -1;

}

else{

EC\_GROUP \*ecgroup= EC\_GROUP\_new\_by\_curve\_name(NID\_secp192k1);

if (NULL == ecgroup){

function\_status = -1;

}

else{

int set\_group\_status = EC\_KEY\_set\_group(rq->eckey,ecgroup);

const int set\_group\_success = 1;

if (set\_group\_success != set\_group\_status)

{

function\_status = -1;

}

else{

const int gen\_success = 1;

int gen\_status = EC\_KEY\_generate\_key(rq->eckey);

if (gen\_success != gen\_status){

function\_status = -1;

}

else{

rq->signature = ECDSA\_do\_sign(ucstr(mdString), strlen(mdString), rq->eckey);

if (NULL == rq->signature){

function\_status = -1;

}

else{

function\_status = 1;

}

}

}

EC\_GROUP\_free(ecgroup);

}}

for(int i=0; i < (int)myneigh[index].size(); i++){

if((int)rq->rq\_dst != (int)myneigh[index][i]){

kirimke[(int)myneigh[index][i]][index] += 1;

}}

Scheduler::instance().schedule(target\_, p, 0.);

}

## A.5 Kode Skrip AWK *Packet Delivery Ratio*

BEGIN {

sendLine = 0;

recvLine = 0;

fowardLine = 0;

}

$0 ~/^s.\* AGT/ {

sendLine ++ ;

}

$0 ~/^r.\* AGT/ {

recvLine ++ ;

}

$0 ~/^f.\* RTR/ {

fowardLine ++ ;

}

END {

printf "cbr s:%d r:%d, r/s Ratio:%.4f, f:%d \n", sendLine, recvLine, (recvLine/sendLine),fowardLine;

}

## A.6 Kode Skrip AWK Rata-rata *End to End Delay*

BEGIN{

sum\_delay = 0;

count = 0;

}

{

event = $1;

type = $4;

packet\_id = $6;

time = $2;

count++;

if(type == "AGT" && event == "s"){

start[packet\_id] = time;

}

else if(type == "AGT" && event == "r"){

end[packet\_id] = time;

}

if(end[packet\_id] != 0){

delay = end[packet\_id] - start[packet\_id];

sum\_delay += delay;

}

}

END{

printf("Average end to end delay : %lf \n",sum\_delay/count);

}

## A.7 Kode Skrip AWK *Routing Overhead*

BEGIN {

ro = 0;

}

$0 ~/^s.\* RTR/ {

if($23 != "(HELLO)"){

ro++ ;

}

}

END {

printf("Routing Overhead : %d\n",ro);

}

# BIODATA PENULIS