

**TUGAS AKHIR – KI141502**

**IMPLEMENTASI ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) UNTUK MENGATASI BLACKHOLE DAN WORMHOLE 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 BLACKHOLE DAN WORMHOLE 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 BLACKHOLE AND WORMHOLE 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 BLACKHOLE DAN WORMHOLE 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 BLACKHOLE DAN WORMHOLE 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 Blackhole dan Wormhole attack. Blackhole attack adalah serangan yang dilakukan suatu malicious node dengan menjatuhkan paket data yang diterima, sedangkan Wormhole 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. Blackhole attack dapat dideteksi dengan melakukan pemantauan terhadap arus pertukaran data pada tiap node, sedangkan Wormhole 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 Blackhole dan Wormhole attack dibandingkan dengan routing protocol yang tidak menerapkannya.*

***Kata kunci: ECDSA, Blackhole attack, Wormhole attack, VANET.***

**ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM IMPLEMENTATION TO OVERCOME BLACKHOLE AND WORMHOLE 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 Blackhole attack and Wormhole attack. Blackhole attack is an attack conducted by dropping data packet that has been received, meanwhile Wormhole attack conducted by tampering the data packet. Both attacks can affect the performance of the routeing 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. Blackhole attack can be detected by recording the data packet exchange traffic in each node, meanwhile Wormhole 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 routeing 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, Blackhole attack, Wormhole 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 BLACKHOLE DAN WORMHOLE 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 v

Abstrak vii

*Abstract* ix

DAFTAR ISI xiii

DAFTAR GAMBAR xvii

DAFTAR TABEL xix

DAFTAR KODE SUMBER xxi

BAB 1 BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 2

1.3 Batasan Permasalahan 2

1.4 Tujuan 2

1.5 Manfaat 3

1.6 Metodologi 3

1.6.1 Penyusunan Proposal Tugas Akhir 3

1.6.2 Studi Literatur 3

1.6.3 Implementasi Perangkat Lunak 4

1.6.4 Pengujian dan Evaluasi 4

1.6.5 Penyusunan Buku 4

1.7 Sistematika Penulisan Laporan 5

BAB 2 BAB II TINJAUAN PUSTAKA 7

2.1 Citra Digital 7

2.2 Forensik Digital 7

2.3 Forensik Citra Digital 8

2.4 *Copy Move* 8

2.5 Python 9

2.6 Anaconda 10

2.7 OpenCV 11

2.8 Matplotlib 11

2.9 NumPy 12

2.10 SciPy 12

2.11 PyQt 13

2.12 JSON 13

2.13 Variance 14

2.14 Mean Squared Error 14

2.15 Convolution 14

2.16 Canny Edge Detection 15

BAB 3 BAB III PERANCANGAN PERANGKAT LUNAK 17

3.1 Data 17

3.1.1 Data Masukan 17

3.1.2 Data Keluaran 19

3.2 Dekripsi Umum Sistem 20

3.3 Modifikasi *Expanding Block Algorithm* 23

3.4 Metode Filter 23

3.4.1 *Averaging Filter* 23

3.4.2 *Median Filter* 23

3.5 Perancangan Antarmuka 24

BAB 4 BAB IV IMPLEMENTASI 27

4.1 Lingkungan Implementasi 27

4.2 Implementasi 27

4.2.1 Kelas Block Container 28

4.2.1.1 Detail Atribut Kelas Blok Container 28

4.2.2 Inisialisasi File 29

4.2.3 Inisialisasi Threshold 30

4.2.4 Pembuatan *Overlapping Block* 31

4.2.5 Pembuatan Grup 32

4.2.6 Pembuatan Bucket 33

4.2.7 Calculate Statistic 33

4.2.8 Find Overlap Block 34

4.2.9 Find Connection 35

4.2.10 Bucket Process 35

4.2.11 Build Copy-Move Image 37

4.2.12 Create Mask 38

4.2.13 Write Mask 39

4.2.14 Build Edge Copy-Move Image 39

4.2.15 Mean Squared Error 40

4.2.16 Similarity 41

4.2.17 Pembuatan Antarmuka 42

BAB 5 BAB V HASIL UJI COBA DAN EVALUASI 45

5.1 Lingkungan Pengujian 45

5.2 Data Pengujian 45

5.3 Preprocessing citra 48

5.4 Skenario Uji Coba 48

5.4.1 Skenario Uji Coba 1 51

5.4.2 Skenario Uji Coba 2 52

5.4.3 Skenario Uji Coba 3 53

5.4.4 Skenario Uji Coba 4 54

5.4.5 Skenario Uji Coba 5 55

5.4.6 Skenario Uji Coba 6 56

5.4.7 Skenario Uji Coba 7 57

5.4.8 Skenario Uji Coba 8 58

5.4.9 Skenario Uji Coba 9 59

5.4.10 Skenario Uji Coba 10 60

5.4.11 Skenario Uji Coba 11 61

5.4.12 Skenario Uji Coba 12 62

5.4.13 Skenario Uji Coba 13 63

5.4.14 Skenario Uji Coba 14 64

5.4.15 Skenario Uji Coba 15 65

5.5 Evaluasi Umum Skenario Uji Coba 66

BAB 6 BAB VI KESIMPULAN DAN SARAN 68

6.1 Kesimpulan 68

6.2 Saran 68

BAB 7 DAFTAR PUSTAKA 69

BAB 8 LAMPIRAN 70

8.1 Kumpulan Kode Sumber 70

BAB 9 BIODATA PENULIS 79

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

# DAFTAR GAMBAR

Gambar 2.1 Contoh Copy-Move Citra 9

Gambar 2.2 Logo Python 10

Gambar 2.3 Logo Anaconda 10

Gambar 2.4 Logo OpenCV 11

Gambar 2.5 Logo Matplotlib 11

Gambar 2.6 Logo NumPy 12

Gambar 2.7 Logo SciPy 12

Gambar 2.8 Logo Qt 13

Gambar 2.9 Logo JSON 13

Gambar 3.1 Contoh citra *copy-move* 17

Gambar 3.2 Contoh kunci jawaban citra *copy-move* 18

Gambar 3.3 Contoh keluaran citra terdeteksi *copy-move* 19

Gambar 3.4 Overlapping Block 2 x 2 20

Gambar 3.5 Proses Pengurutan Blok dan Penempatan ke Buckets 21

Gambar 3.6 Desain Tampilan Antarmuka 24

Gambar 4.1 Antarmuka Awal Dijalankan 44

Gambar 4.2 Antarmuka Masukan Data 44

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

# DAFTAR TABEL

[Tabel 4.1 Lingkungan Implementasi Perangkat Lunak 27](#_Toc470245388)

[Tabel 4.2 Atribut Kelas Blok Container 28](#_Toc470245389)

[Tabel 5.1 Spesifikasi Lingkungan Pengujian 45](#_Toc470245390)

[Tabel 5.2 Threshold a 48](#_Toc470245391)

[Tabel 5.4 Confusion matrix uji coba 1 51](#_Toc470245392)

[Tabel 5.5 Confusion matrix uji coba 2 52](#_Toc470245393)

[Tabel 5.6 Confusion matrix uji coba 3 53](#_Toc470245394)

[Tabel 5.7 Confusion matrix uji coba 4 54](#_Toc470245395)

[Tabel 5.8 Confusion matrix uji coba 5 55](#_Toc470245396)

[Tabel 5.9 Confusion matrix uji coba 6 56](#_Toc470245397)

[Tabel 5.10 Confusion matrix uji coba 7 57](#_Toc470245398)

[Tabel 5.11 Confusion matrix uji coba 8 58](#_Toc470245399)

[Tabel 5.12 Confusion matrix uji coba 9 59](#_Toc470245400)

[Tabel 5.13 Confusion matrix uji coba 10 60](#_Toc470245401)

[Tabel 5.14 Confusion matrix uji coba 11 61](#_Toc470245402)

[Tabel 5.15 Confusion matrix uji coba 12 62](#_Toc470245403)

[Tabel 5.16 Confusion matrix uji coba 13 63](#_Toc470245404)

[Tabel 5.17 Confusion matrix uji coba 14 64](#_Toc470245405)

[Tabel 5.18 Confusion matrix uji coba 15 65](#_Toc470245406)

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

# DAFTAR KODE SUMBER

[Pseudocode 3.1 Contoh Threshold Config 19](#_Toc470245407)

[Pseudocode 4.1 Kode Program Kelas Blok Container 28](#_Toc470245408)

[Pseudocode 4.2 Kode Program Inisialisasi File 30](#_Toc470245409)

[Pseudocode 4.3 Kode Program Inisialisasi Threshold 31](#_Toc470245410)

[Pseudocode 4.4 Kode Program Overlapping block 31](#_Toc470245411)

[Pseudocode 4.5 Kode Program Pengurutan Blok 31](#_Toc470245412)

[Pseudocode 4.6 Kode Program Pembuatan Grup 32](#_Toc470245413)

[Pseudocode 4.7 Kode Program Pembuatan Bucket 33](#_Toc470245414)

[Pseudocode 4.8 Kode Program Perhitungan Statistik 34](#_Toc470245415)

[Pseudocode 4.9 Kode Program Pengecekan Overlap 35](#_Toc470245416)

[Pseudocode 4.10 Kode Program Pengekan Connection 35](#_Toc470245417)

[Pseudocode 4.11 Kode Program Memproses Setiap Bucket 37](#_Toc470245418)

[Pseudocode 4.12 Kode Program Membangun Gambar Copy-Move 38](#_Toc470245419)

[Pseudocode 4.13 Kode Program Membuat Gambar Mask 39](#_Toc470245420)

[Pseudocode 4.14 Kode Program Menempelkan Mask Ke Gambar 39](#_Toc470245421)

[Pseudocode 4.15 Kode Program Membuat Edge Pada Gambar 40](#_Toc470245422)

[Pseudocode 4.16 Kode Program Menghitung Mean Squared Error 41](#_Toc470245423)

[Pseudocode 4.17 Kode Program Menghitung Kemiripan 41](#_Toc470245424)

[Pseudocode 4.18 Kode Program Menjalankan Deteksi 43](#_Toc470245425)

# 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. 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 *Blackhole* dan *Wormhole attack.*

*Blackhole 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 *Wormhole attack* memiliki banyak variasi serangan, salah satunya dengan mengubah isi dari paket yang diterimanya.

Dalam beberapa tahun terakhir terdapat penelitian terkait metode untuk mengatasi *Blackhole* maupun *Wormhole 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 *Blackhole* dan *Wormhole 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 *Blackhole* dan *Wormhole attack*?
2. Bagaimana cara mengimplementasikan ECDSA untuk mengatasi *Blackhole* dan *Wormhole attack*?
3. Bagaimana perbandingan performa *routing protocol* AODV ketika terdapat *malicious node* yang melakukan *Blackhole* dan *Wormhole 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 *blackhole* dan *wormhole attack* pada lingkungan VANET dengan *routing protocol* AODV.
2. Dapat mengimplementasikan ECDSA untuk mengatasi *blackhole* dan *wormhole attack* yang terjadi di lingkungan VANET dengan *routing protocol* AODV.
3. Menganalisa perbandingan performa *routing protocol* AODV ketika terdapat *malicious node* yang melakukan *blackhole* dan *wormhole 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 *Blackhole* dan *Wormhole 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. Prosposal juga berisi tentang garis besa tugas akhir yang akan dikerjakan sehingga memberikan gambaran untuk dapat mengerjakan tugas akhir sesuai dengan *timeline* yang dibuat. Gagasan untuk menganalisa dan mengidentifikasi pemasuan citra terhadap serangan *copy-move* menggunakan metode *expanding block algorithm*[1].

### 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 *expanding block algorithm*, dan metode-metodestatistika seperti mean dan variance seta metode-metode untuk melakukan pengolahan gambar atau *Image Processing* seperti *Blur, Sharpen, Edge Detection*[6]*.* Tugas akhir ini juga mengacu pada literatur jurnal dengan judul “*An efficient expanding block algorithm for image copy-move forgery detection”* yang diterbitkan pada tahun 2013[1].

### Implementasi Perangkat Lunak

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 suatu perangkat lunak yaitu Python versi 2.7 sebagai bahasa pemrograman utama dengan distribusi package Anaconda dan PyCharm Professional 2016.2.3 sebagai IDE.

### Pengujian dan Evaluasi

Pada tahap ini algoritma yang telah disusun diuji coba dengan menggunakan data uji coba yang ada. Data uji coba tersebut diuji coba dengan menggunakan suatu perangkat lunak dengan tujuan mengetahui kemampuan metode yang digunakan dan mengevaluasi hasil tugas akhir dengan jurnal pendukung yang ada. Hasil evaluasi juga mencakup kompleksitas dari kemampuan masing-masing metode tersebut dalam mendeteksi serangan *copy-move*.

### 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 forensik digital, forensik citra digital, *copy-move*, Mean, Variance, Mean Squared Error dan Qt*.*

* + 1. Bab III. Perancangan Perangkat Lunak

Bab ini berisi pembahasan mengenai perancangan dari metode *expanding block*  yang digunakan untuk menedeteksi pemalsuan citra pada serangan *copy-move* dan perancangan GUI menggunakan Qt.

* + 1. Bab IV. Implementasi

Bab ini menjelaskan implementasi yang berbentuk *Pseudocode* yang berupa *Pseudocode* dari metode *expanding block algorithm.*

* + 1. Bab V. Pengujian dan Evaluasi

Bab ini berisikan hasil uji coba dari metode *expanding block algorithm* yang digunakan untuk menedeteksi pemalsuan citra pada serangan *copy-move* yang sudah diimplementasikan pada *Pseudocode*. Uji coba dilakukan dengan menggunakan dataset citra yang memiliki kualitas rendah dengan ukuran 512 x 512 dengan memiliki.Hasil evaluasi mencakup perbanding masing-masing data masukan dan filter atau *image processig*.

* + 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 tabel-tabel data hasil uji coba dan 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*.

## 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*.

## 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*).

## *Blackhole Attack*

*Blackhole 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.*

## *Wormhole Attack*

*Wormhole 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.

## 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.

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

## 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.

## 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.

## 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*. 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*.

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

# 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 *Blackhole* dan *Wormhole 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

*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

### 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

## 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

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

Agar *node attacker* dapat menjalankan tugasnya melakukan *Blackhole attack* atau *Wormhole attack*, ditambahkan beberapa kode untuk melakukan *Blackhole attack* dan *Wormhole 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 *Blackhole attacker* atau *Wormhole attacker*. Jika *node* tersebut adalah *Blackhole attacker*, maka *node* tersebut akan melakukan *drop* pada setiap paket yang diterimanya, sedangkan jika *node* tersebut adalah *Wormhole attacker*, maka *node* tersebut akan mengubah *node* tujuan yang ada pada paket *header*. Diagram alur pembuatan simulasi penyerangan dapat dilihat pada gambar

## 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

*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 dan *node* tujuan menerima paket. Dari *delay* tiap paket tersebut akan didapatkan rata-rata *end to end delay*, yang dapat dihitung dengan persamaan

### *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

## Perancangan Modifikasi pada *Routing Protocol* AODV

*Routing Protocol* AODV tidak memiliki benteng sekuritas sehingga rentan terjadi serangan, dalam hal ini adalah *Blackhole* dan *Wormhole attack*. Modifikasi pada *Routing Protocol* AODV dilakukan dengan adanya penambahan aspek sekuritas guna mengatasi *Blackhole* dan *Wormhole 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

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

# 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

Gambar hasil peta yang telah dibuat dengan netgenerate dapat dilihat pada gambar

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

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

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

*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

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

*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

### 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

*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

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

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.

Untuk melihat percobaan pergerakan *node* pada *file* .sumocfg dapat dengan menggunakan tools sumo-gui seperti pada gambar

## Implementasi Modifikasi pada *Routing 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 *Blackhole* dan *Wormhole 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 *Blackhole* dan *Wormhole attack* yang telah disebutkan sebelumnya.

Pada bagian ini penulis akan menjelaskan langkah-langkah dalam mengimplementasikan modifikasi *routing protocol* AODV untuk mengatasi *Blackhole* dan *Wormhole 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

### 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 struct 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

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 diforward. 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

### Penambahan Evaluasi pada Tiap *Node*

### Implementasi ECDSA

### Modifikasi Pemilihan *Node*

## Implementasi Simulasi pada NS-2

### Implementasi *Blackhole Attack*

### Implementasi *Wormhole Attack*

## Implementasi Metrik Analisis

Simulasi yang telah dijalankan oleh NS-2 menghasilkan keluaran sebuah *tracefile* yang berisikan data mengenai apa saja yang terjadi selama simulasi dalam bentuk *plain text*. Dari data *tracefile*, 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 *tracefile* 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.

Dalam perhitungan PDR, kata kunci yang perlu diperhatikan dari *tracefile* 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

Contoh perintah pengeksekusian skrip awk untuk menganalisis *tracefile* beserta outputnya dapat dilihat masing-masing pada gambar dan

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

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

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

Contoh perintah pengeksekusian skrip awk untuk menganalisis *tracefile* beserta outputnya dapat dilihat masing-masing pada gambar dan

### Implementasi *Routing Overhead* (RO)

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

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

Contoh perintah pengeksekusian skrip awk untuk menganalisis *tracefile* beserta outputnya dapat dilihat masing-masing pada gambar dan

# BAB V HASIL UJI COBA DAN EVALUASI

## Lingkungan Uji Coba

## Hasil Uji Coba

### Hasil Uji Coba Skenario *Grid*

### Hasil Uji Coba Skenario *Real*

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

# BAB VI KESIMPULAN DAN SARAN

## Kesimpulan

## Saran

# DAFTAR PUSTAKA

[1] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, “An efficient expanding block algorithm for image copy-move forgery detection,” *Inf. Sci.*, vol. 239, pp. 253–265, Aug. 2013.

[2] F. J, S. D, and L. J, “Detection of copy-move forgery in digital images,” *Proc Digit. Forensic Res. Workshop*, Aug. 2003.

[3] C. S. Lin, C. C. Chen, and Y. C. Chang, “An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection,” in *2015 International Conference on Intelligent Networking and Collaborative Systems*, 2015, pp. 228–231.

[4] A. Langille and M. Gong, “An Efficient Match-based Duplication Detection Algorithm,” in *The 3rd Canadian Conference on Computer and Robot Vision (CRV’06)*, 2006, pp. 64–64.

[5] J. A. Redi, W. Taktak, and J.-L. Dugelay, “Digital image forensics: a booklet for beginners,” *Multimed. Tools Appl.*, vol. 51, no. 1, pp. 133–162, Jan. 2011.

[6] “OpenCV: Morphological Transformations.” [Online]. Available: http://docs.opencv.org/trunk/d9/d61/tutorial\_py\_morphological\_ops.html. [Accessed: 14-Dec-2016].

[7] “Numpy and Scipy Documentation — Numpy and Scipy documentation.” [Online]. Available: https://docs.scipy.org/doc/. [Accessed: 15-Dec-2016].

[8] “PyQt/Tutorials - Python Wiki.” [Online]. Available: https://wiki.python.org/moin/PyQt/Tutorials. [Accessed: 15-Dec-2016].

[9] “4.3. Preprocessing data — scikit-learn 0.18.1 documentation.” [Online]. Available: http://scikit-learn.org/stable/modules/preprocessing.html#preprocessing. [Accessed: 15-Dec-2016].

# LAMPIRAN

## Kumpulan Kode Sumber

|  |
| --- |
| **from** PyQt5.QtGui **import** \* **from** PyQt5.QtCore **import** \* **from** PyQt5.QtWidgets **import** \* **import** json,subprocess  **class** CopyMoveGUI(QMainWindow):  **def** \_\_init\_\_(self):  super(CopyMoveGUI, self).\_\_init\_\_()  self.initUI()  self.centerWindow()   **def** initUI(self):  self.setWindowTitle(**"Copy Move Detection"**)  self.setFixedSize(800, 600)  self.createAction()  self.createMenuBar()   self.centralWidget = QWidget()   *#group input* self.groupInput = QGroupBox(self.centralWidget)  self.groupInput.setGeometry(QRect(10, 0, 401, 541))  self.groupInput.setTitle(**"Input"**)   self.inputGambar = QLabel(self.groupInput)  self.inputGambar.setGeometry(QRect(20, 30, 361, 201))  self.inputGambar.setText(**"No Image"**)   self.pilihInputGambar = QPushButton(self.groupInput)  self.pilihInputGambar.setGeometry(QRect(300, 240, 80, 25))  self.pilihInputGambar.setText(**"Pilih Gambar"**)  self.pilihInputGambar.clicked.connect(self.openImage)   self.line = QFrame(self.groupInput)  self.line.setGeometry(QRect(0, 270, 401, 16))  self.line.setFrameShape(QFrame.HLine)  self.line.setFrameShadow(QFrame.Sunken)   self.inputGambarKunci = QLabel(self.groupInput)  self.inputGambarKunci.setGeometry(QRect(20, 290, 361, 201))  self.inputGambarKunci.setText(**"No Image"**)   self.pilihInputGambarKunci = QPushButton(self.groupInput)  self.pilihInputGambarKunci.setGeometry(QRect(259, 500, 121, 25))  self.pilihInputGambarKunci.setText(**"Pilih Gambar Kunci"**)  self.pilihInputGambarKunci.clicked.connect(self.openKeyImage)   *#group threshold config* self.groupThreshold = QGroupBox(self.centralWidget)  self.groupThreshold.setGeometry(430, 20, 351, 171)  self.groupThreshold.setTitle(**"Threshold Config"**)   self.vlWidThresold = QWidget(self.groupThreshold)  self.vlWidThresold.setGeometry(QRect(10, 30, 331, 131))  self.vltThreshold = QVBoxLayout(self.vlWidThresold)  self.vltThreshold.setContentsMargins(11,11,11,11)  self.vltThreshold.setSpacing(6)   self.pval = QLabel(self.vlWidThresold)  self.pval.setText(**"pVal : "**)  self.vltThreshold.addWidget(self.pval)  self.blocksize = QLabel(self.vlWidThresold)  self.blocksize.setText(**"Block Size : "**)  self.vltThreshold.addWidget(self.blocksize)  self.blockdistance = QLabel(self.vlWidThresold)  self.blockdistance.setText(**"Block Distance : "**)  self.vltThreshold.addWidget(self.blockdistance)  self.totalbucket = QLabel(self.vlWidThresold)  self.totalbucket.setText(**"Total Bucket : "**)  self.vltThreshold.addWidget(self.totalbucket)  self.minarea = QLabel(self.vlWidThresold)  self.minarea.setText(**"Min Area : "**)  self.vltThreshold.addWidget(self.minarea)   self.pilihInputThreshold = QPushButton(self.groupThreshold)  self.pilihInputThreshold.setGeometry(QRect(250, 130, 80, 25))  self.pilihInputThreshold.setText(**"Pilih Config"**)  self.pilihInputThreshold.clicked.connect(self.openThrehsold)   *#group option* self.groupOption = QGroupBox(self.centralWidget)  self.groupOption.setGeometry(QRect(430, 210, 351, 101))  self.groupOption.setTitle(**"Option"**)   self.filter = QLabel(self.groupOption)  self.filter.setGeometry(QRect(10, 30, 54, 17))  self.filter.setText(**"Filter : "**)   self.filterCombo = QComboBox(self.groupOption)  self.filterCombo.setGeometry(QRect(10, 60, 331, 25))  listFilter = [**"None"**,**"Averaging"**,**"Median"**,**"Bilateral"**]  self.filterCombo.addItems(listFilter)  self.filterCombo.currentIndexChanged.connect(self.getFilter)   *#start and result folder* self.buttonStart = QPushButton(self.centralWidget)  self.buttonStart.setGeometry(QRect(690, 320, 91, 25))  self.buttonStart.setText(**"Mulai Deteksi"**)  self.buttonStart.clicked.connect(self.startDetection)   self.buttonResult = QPushButton(self.centralWidget)  self.buttonResult.setGeometry(QRect(550, 320, 121, 25))  self.buttonResult.setText(**"Lihat Folder Hasil"**)  self.buttonResult.clicked.connect(self.openResultDir)   *#group log* self.groupLog = QGroupBox(self.centralWidget)  self.groupLog.setGeometry(QRect(430, 350, 361, 201))  self.groupLog.setTitle(**"Log"**)   self.logOutput = QTextEdit(self.groupLog)  self.logOutput.setGeometry(QRect(0, 20, 361, 181))   self.setCentralWidget(self.centralWidget)   *#Process Detection* self.process = QProcess(self)  self.process.readyReadStandardOutput.connect(self.stdoutReady)  self.process.readyReadStandardError.connect(self.stderrReady)  self.process.started.connect(**lambda**: self.buttonStart.setEnabled(False))  self.process.finished.connect(**lambda**: self.buttonStart.setEnabled(True))   **def** getFilter(self,i):  **print** i  self.filterChoice = str(i)   **def** append(self, text):  cursor = self.logOutput.textCursor()  cursor.movePosition(cursor.End)  cursor.insertText(text)  *#self.logOutput.ensureCursorVisible()* **def** stdoutReady(self):  text = str(self.process.readAllStandardOutput())  **print** text.strip()  self.append(text)   **def** stderrReady(self):  text = str(self.process.readAllStandardError())  **print** text.strip()  self.append(text)   **def** startDetection(self):  self.argv = [**"/media/sudirahanif/Kuliah/TA/Program/TugasAkhir.py"**,self.imageFile,self.thresholdFile,self.filterChoice]  self.process.start(**'/home/sudirahanif/anaconda2/bin/python'**,self.argv)    **def** openResultDir(self):  *#subprocess.Popen(["xdg-open", "/media/sudirahanif/Kuliah/TA/Hasil"])* subprocess.Popen([**"explorer"**, **"."**])   **def** openThrehsold(self):  fileName, \_ = QFileDialog.getOpenFileName(self, **"Open File"**, QDir.currentPath(), **"JSON (\*.json)"**)  self.thresholdFile = fileName  **if** fileName:  **with** open(fileName, **'rb'**) **as** file:  data = json.load(file)  minArea = data[**'threshold'**][**'minArea'**]  blockSize = data[**'threshold'**][**'blockSize'**]  numBuckets = data[**'threshold'**][**'numBuckets'**]  pVal = data[**'threshold'**][**'pVal'**]  blockDistance = data[**'threshold'**][**'blockDistance'**]  self.pval.setText(**"pVal : "**+str(pVal))  self.blocksize.setText(**"Block Size : "**+str(blockSize))  self.blockdistance.setText(**"Block Distance : "**+str(blockDistance))  self.totalbucket.setText(**"Total Bucket : "**+str(numBuckets))  self.minarea.setText(**"Min Area : "**+str(minArea))   **def** openImage(self):  fileName, \_ = QFileDialog.getOpenFileName(self, **"Open File"**, QDir.currentPath(), **"Images (\*.png \*.jpg)"**)  self.imageFile = fileName  **if** fileName:  image = QImage(fileName)  **if** image.isNull():  QMessageBox.information(self, **"Image Viewer"**, **"Cannot load %s."** % fileName)  **return  else**:  self.inputGambar.setPixmap(QPixmap.fromImage(image))  self.inputGambar.setScaledContents(True)   **def** openKeyImage(self):  fileName, \_ = QFileDialog.getOpenFileName(self, **"Open File"**, QDir.currentPath(), **"Images (\*.png \*.jpg)"**)  self.imageFileKey = fileName  **if** fileName:  image = QImage(fileName)  **if** image.isNull():  QMessageBox.information(self, **"Image Viewer"**, **"Cannot load %s."** % fileName)  **return  else**:  self.inputGambarKunci.setPixmap(QPixmap.fromImage(image))  self.inputGambarKunci.setScaledContents(True)    **def** centerWindow(self):  frameGm = self.frameGeometry()  screen = QApplication.desktop().screenNumber(QApplication.desktop().cursor().pos())  centerPoint = QApplication.desktop().screenGeometry(screen).center()  frameGm.moveCenter(centerPoint)  self.move(frameGm.topLeft())   **def** createMenuBar(self):  self.fileMenu = QMenu(**"&File"**, self)  self.fileMenu.addAction(self.exitAct)   self.helpMenu = QMenu(**'&Help'**, self)  self.helpMenu.addAction(self.aboutAct)  self.helpMenu.addAction(self.aboutActQt)   self.menuBar().addMenu(self.fileMenu)  self.menuBar().addMenu(self.helpMenu)   **def** createAction(self):  self.exitAct = QAction(**"&Keluar"**, self, shortcut=**"Ctrl+Q"**, triggered=self.close)  self.aboutAct = QAction(**"Tentang &Penulis"**, self, triggered=self.about)  self.aboutActQt = QAction(**"Tentang &Qt"**, self,triggered=QApplication.instance().aboutQt)   **def** about(self):  QMessageBox.about(self, **"Tentang Tugas Akhir"**,**"<p>Hanif Sudira - 5113100184</p>""<p>Teknik Informatika ITS 2013</p>"**)  **if** \_\_name\_\_ == **'\_\_main\_\_'**:  **import** sys  app = QApplication(sys.argv)  CopyMove = CopyMoveGUI()  CopyMove.show()  sys.exit(app.exec\_()) |

Kode Sumber . Antarmuka Aplikasi

# BIODATA PENULIS

******Hanif Sudira merupakan anak dari pasangan Bapak Syamsul Bahar dan Ibu Roslinda. Lahir di Padang pada tanggal 22 April 1995. Penulis menempuh pendidikan formal dimulai dari TK Aisyah (2000-2001), SDN 29 Ganting Utara Padang Timura (2001-2007), SMPN 12 Padang (2007-2010), SMAN 10 Padanga (2010-2013) dan S1 Teknik Informatika ITS (2013-2017). Bidang studi yang diambil oleh penulis pada saat berkuliah di Teknik Informatika ITS adalah Berbasis Jaringan (KBJ). Penulis aktif dalam organisasi seperti Himpunan Mahasiswa Teknik Computer-Informatika (2014-2016) dan KMI (2014-2015). Penulis juga aktif dalam berbagai kegiatan kepanitiaan yaitu SCHEMATICS 2014 divisi NPC dan SCHEMATICS 2014 NPC. Penulis juga pernah kerja praktik di Tokopedia periode Juli – Agustus 2016.. Penulis dapat dihubungi melalui email: [sudirahanif@gmail.com](mailto:sudirahanif@gmail.com).