

Protokol Routing pada VANET: Taksonomi dan Analisis Perbandingan antara DSR, AODV, dan TORA

Rosida Nur Aziza¹, Puji Catur Siswipraptini², Rizqia Cahyaningtyas³

^{1,2,3}Jurusan Teknik Informatika STT-PLN Jakarta
Jl. Lingkar Luar, Duri, Kosambi, Cengkareng, Jakarta Barat 11750
e-mail : ¹rosida@sttpln.ac.id

ABSTRAK

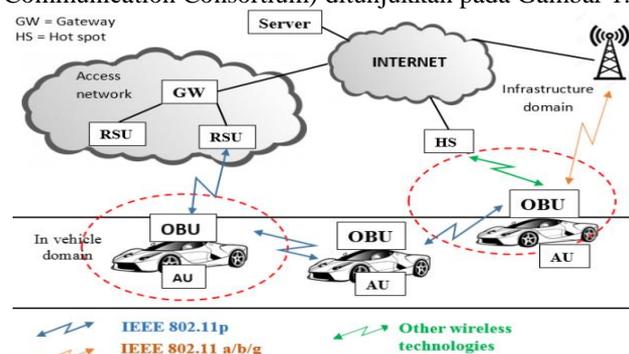
VANET yang merupakan bagian dari MANET adalah teknologi yang memungkinkan komunikasi nirkabel antar berbagai kendaraan yang bergerak atau antara kendaraan dengan unit komunikasi yang terdapat di sepanjang jalan. VANET dikembangkan untuk mendukung ITS dalam meningkatkan keselamatan di jalan raya dan efisiensi lalu lintas. Jaringan ad-hoc ini juga dirancang untuk memungkinkan pertukaran pesan-pesan peringatan antar kendaraan untuk meningkatkan keselamatan penumpang dan informasi-informasi lain terkait dengan aplikasi dan layanan VANET. Untuk mewujudkan hal tersebut, ada beberapa hal yang perlu dipertimbangkan supaya VANET dapat beroperasi dengan baik. Hal-hal tersebut antara lain masalah keterbatasan bandwidth, keamanan, skalabilitas, protokol kendali akses media (MAC) dan mekanisme routing. Ada beberapa karakteristik khusus dari VANET yang perlu diperhatikan oleh protokol routing, antara lain : mobilitas node yang tinggi, jumlah dan kepadatan node yang tidak tetap, dan topologi jaringan yang terus berubah. Diperlukan protokol routing tertentu untuk mewujudkan komunikasi yang handal, kontinu dan tanpa batas antar node pada VANET. Secara garis besar, protokol routing pada VANET dikelompokkan menjadi dua: kelompok protokol yang berdasarkan posisi kendaraan dan kelompok yang berdasar pada topologi jaringan. Tulisan ini akan membahas mengenai protokol routing DSR, AODV, TORA dan menjelaskan bagaimana ketiga protokol reaktif ini menjalankan mekanisme routing pada VANET. Kelebihan dan kekurangan dari ketiga protokol tersebut juga akan dianalisis dengan didukung oleh beberapa hasil simulasi dari penelitian-penelitian yang telah dilakukan sebelumnya.

Kata kunci: VANET, protokol routing untuk VANET, DSR, AODV, TORA.

1. PENDAHULUAN

Jaringan Ad-hoc Vehicular atau VANET (*Vehicular Ad-hoc Network*) adalah jaringan dengan *node-node* berupa kendaraan-kendaraan yang *mobile*. Kendaraan tersebut dapat berkomunikasi dengan kendaraan lainnya, maupun dengan berbagai piranti komunikasi yang ada di sepanjang jalan raya. VANET ini merupakan bagian dari MANET (*Mobile Ad-hoc Network*), namun *node-node* pada VANET memiliki tingkat mobilitas yang lebih tinggi.

VANET, secara garis besar, tersusun dari dua bagian yaitu bagian yang *mobile* dan bagian yang tetap. Kelompok yang pertama meliputi kendaraan dan berbagai alat komunikasi *mobile*, termasuk piranti navigasi. Bagian kedua adalah piranti-piranti pendukung komunikasi VANET, yang dapat berupa titik akses, *gateway*, dan lain sebagainya. Titik akses pada VANET dikenal dengan istilah *Road Side Unit* (RSU). RSU ditempatkan di lokasi-lokasi strategis di sepanjang jalan, misalkan di persimpangan jalan atau pada lampu lalu lintas. Berdasarkan referensi dari C2C-CC (*Car2Car-Communication Consortium*), setiap kendaraan yang menjadi bagian atau *node* dari VANET dilengkapi dengan teknologi khusus yang dikenal sebagai *On Board Unit* (OBU) dan *Application Unit* (AU). OBU bertindak sebagai terminal sekaligus router *wireless*. Dalam jaringan vehicular ini, OBU dapat dianggap sebagai *node* yang bergerak dan RSU adalah *node* yang diam (Liang et al, 2015). Adapun contoh arsitektur dari VANET menurut referensi C2C-CC (*Car-2-Car Communication Consortium*) ditunjukkan pada Gambar 1.



Gambar 1 Arsitektur VANET berdasar C2C-CC

Ada beberapa karakteristik VANET yang mempengaruhi perancangan protokol-protokol yang sesuai untuk VANET, yaitu (Almalag et al., 2013), (Daas et al., 2012), (Rana et al, 2014):

a. Jumlah Node

Jumlah dan kepadatan *node* pada VANET bervariasi. Jumlah *node* bisa sangat besar di daerah perkotaan pada jam sibuk. Namun jumlah *node* VANET bisa sangat sedikit di daerah pedesaan dengan jumlah mobil yang dilengkapi kemampuan komunikasi sangat terbatas. Protokol MAC harus mampu bekerja dengan baik pada kedua keadaan tersebut.

b. Mobilitas node yang tinggi

Kendaraan sebagai *node* dari VANET dapat bergerak dengan kecepatan tinggi, lebih dari 100 km/jam. Hal ini sering menyebabkan diskoneksi antar *node*. Jika, dimisalkan, suatu kendaraan yang melaju kencang berkomunikasi dengan kendaraan yang berjalan lambat, maka *link* komunikasi yang terbentuk akan berumur pendek. Hubungan akan terputus karena jarak yang memisahkan kedua *node* tersebut semakin besar. Protokol MAC harus dapat bekerja baik dengan umur *link* komunikasi yang singkat.

c. Topologi jaringan yang berubah-ubah

Karena *node-node* VANET memiliki mobilitas tinggi, maka topologi jaringan VANET yang terbentuk juga terus-menerus mengalami perubahan.

d. Topologi jaringan yang dapat diprediksi

Walaupun *node-node* VANET banyak bergerak, namun pergerakannya dibatasi oleh topologi jalan raya yang dilaluinya.

e. Ketersediaan informasi lokasi

Informasi lokasi dari *node* yang diberikan oleh GPS dapat mengurangi waktu pengiriman data dan meningkatkan *throughput* jaringan. Selain itu, informasi posisi dan kecepatan *node-node* melaju juga dapat membantu memperkirakan pola mobilitas dari *node-node* tersebut.

f. Metode komunikasi

Metode yang digunakan untuk pengiriman pesan dari pengirim ke penerima adalah *broadcast*.

g. Lingkungan komunikasi yang berbeda

VANET memiliki dua tipe lingkungan komunikasi yang berbeda, yaitu: lingkungan trafik jalan raya (*highway*) dan lingkungan trafik perkotaan. Tipe yang pertama lebih sederhana dibandingkan tipe trafik di perkotaan.

h. Tidak memiliki pusat pengendali

Node-node pada VANET dapat saling terhubung dan berkomunikasi tanpa adanya pengendalian yang terpusat.

i. Sumber tenaga/batere yang tak terbatas

Dibandingkan *node-node* MANET yang memiliki daya listrik terbatas, *node* VANET memiliki daya yang tidak terbatas. Batere dari kendaraan yang melaju mampu menyediakan daya terus-menerus untuk mengaktifkan peralatan komunikasi *node* tersebut.

Berdasarkan karakteristik-karakteristik di atas, maka diperlukan mekanisme *routing* tertentu yang sesuai untuk lingkungan VANET. Terdapat tiga protokol *routing* untuk VANET yang akan dibahas dan dianalisis pada tulisan ini. Studi perbandingan dilakukan berdasarkan hasil-hasil simulasi dan penelitian sebelumnya.

2. LANDASAN TEORI

2.1 Arsitektur VANET

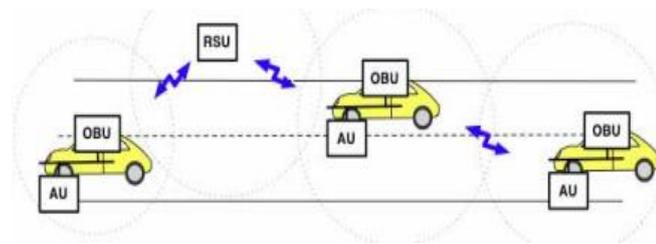
Arsitektur VANET tidak seragam. Contoh arsitektur yang ditunjukkan pada Gambar 1 merupakan referensi dari C2C-CC, yaitu kelompok utama penggagas komunikasi vehicular di benua Eropa. Bab ini akan membahas lebih lanjut mengenai arsitektur VANET.

2.2 Komponen Utama

Menurut *draft* dari C2C-CC, komponen penyusun VANET terdiri dari 3 domain berbeda, yaitu: *in-vehicle*, *ad-hoc*, dan infrastruktur. Domain *in-vehicle* meliputi komponen yang terletak di dalam kendaraan, yaitu *on-board unit* (OBU) dan *application unit* (AU). Jumlah AU dalam suatu kendaraan bisa lebih dari satu. AU dapat berupa bagian dari kendaraan yang secara permanen terhubung ke OBU atau berupa laptop, PDA, atau game pad yang terhubung dengan OBU secara dinamis. Koneksi antara AU dan OBU dapat melalui kabel, *bluetooth*, WUSB, maupun UWB.

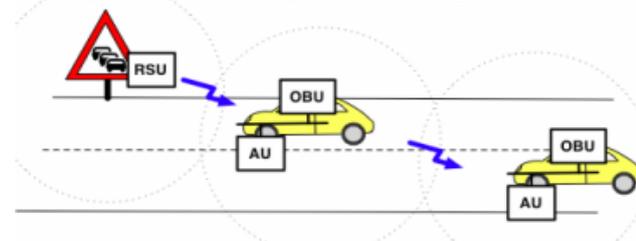
Domain kedua adalah domain *ad-hoc*. Domain ini terdiri dari kendaraan-kendaraan yang telah dilengkapi dengan OBU dan unit-unit komunikasi pendukung di sepanjang jalan (RSU). Tugas utama dari RSU adalah sebagai berikut:

- 1) Memperluas rentang komunikasi dari jaringan dengan mengirimkan kembali informasi ke OBU-OBU yang berada dalam wilayahnya.



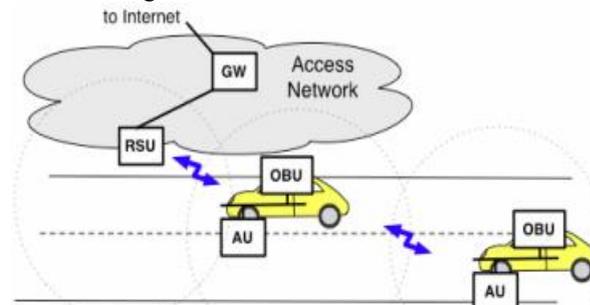
Gambar 2 RSU memperluas penyebaran informasi

- 2) Bisa menjalankan aplikasi-aplikasi pendukung keselamatan di jalan raya, pengendali persimpangan jalan, lampu lalu lintas virtual, sekaligus bertindak sebagai sumber dan penerima informasi.



Gambar 3 RSU sebagai sumber informasi

- 3) Menyediakan hubungan ke internet bagi OBU-OBU,



Gambar 4 RSU sebagai penyedia akses Internet

- 4) Bekerja sama dengan RSU-RSU lain untuk meneruskan informasi yang terkait dengan keselamatan jalan raya.

OBU dari beberapa kendaraan akan membentuk jaringan nirkabel ad-hoc (MANET). OBU-OBU yang terhubung secara nirkabel akan langsung dapat saling berkomunikasi tanpa adanya koordinasi secara terpusat. Jika tidak ada koneksi langsung, protokol *routing* untuk VANET memungkinkan komunikasi secara *multi-hop*, yaitu data diteruskan dari satu OBU ke OBU lainnya hingga ke tujuan. OBU dan RSU dapat dianggap sebagai *node-node* dari VANET. RSU dapat terhubung dengan jaringan infrastruktur komunikasi sehingga RSU dapat terhubung dengan Internet. Hal ini memungkinkan berbagai AU yang terhubung pada suatu OBU untuk berkomunikasi dengan host-host di Internet. Seperti ditunjukkan pada Gb.1, OBU dapat juga terhubung ke Internet melalui Hot Spot (HS). Apabila tidak tersedia RSU dan HS, OBU dapat memanfaatkan teknologi komunikasi lain untuk aplikasi yang tidak berhubungan dengan keselamatan lalu lintas, misalnya menggunakan GSM, GPRS, UMTS, 4G, dan lain sebagainya.

Domain infrastruktur pada VANET mengacu pada berbagai piranti pendukung terlaksananya komunikasi lainnya yang ada di sepanjang jalan.

2.3 Arsitektur Komunikasi

Ada empat tipe komunikasi pada VANET, yaitu komunikasi *In-vehicle*, *Vehicle-to-vehicle (V2V)*, *Vehicle-to-road infrastructure (V2I atau V2R)*, dan *Vehicle-to-broadband (V2B)* (Liang et al., 2015). Komunikasi *In-vehicle* menyediakan berbagai informasi yang berhubungan dengan kejadian di dalam suatu kendaraan, misalnya: kecepatan dan posisi kendaraan, informasi apakah pengemudi mengantuk atau mengalami kelelahan.

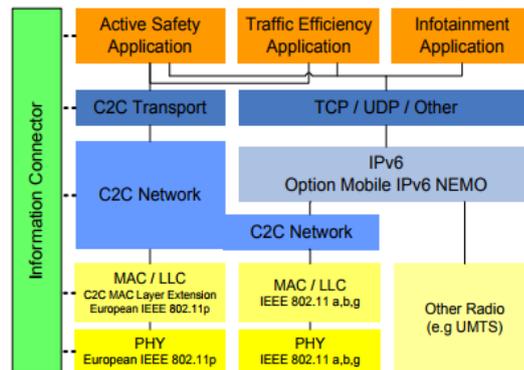
Komunikasi V2V mengatur bagaimana kendaraan-kendaraan dapat saling bertukar informasi dan pesan peringatan yang berhubungan dengan lalu lintas.

Komunikasi V2I menghubungkan kendaraan dengan berbagai perangkat infrastruktur, termasuk RSU. V2I memungkinkan pengemudi menerima informasi tentang kondisi lalu lintas, cuaca, dan informasi lain dari sensor yang tergabung dalam VANET secara *real time*.

Tipe komunikasi V2B menghubungkan kendaraan dengan jaringan *wireless broadband*, seperti 3G/4G. Dari gambar 1 di atas, dapat diketahui bahwa komunikasi V2V dilaksanakan menggunakan standar *wireless* atau protocol yang khusus dikembangkan untuk VANET, seperti IEEE 802.11p. Sedangkan, komunikasi dari kendaraan ke RSU atau ke perangkat infrastruktur jaringan yang lain dapat dilakukan menggunakan berbagai teknologi *wireless* lain yang tersedia saat ini.

2.4 Arsitektur Protokol pada VANET

Arsitektur protokol untuk komunikasi di VANET, menurut usulan C2C-CC, ditunjukkan pada Gb.5. Sisi kanan menunjukkan tumpukan protokol komunikasi dengan standar TCP/IP. Tumpukan sisi kiri adalah protokol-protokol C2C untuk pengiriman data atau informasi khusus untuk VANET. Lapisan *C2C Transport* bertugas menyediakan transfer data yang handal dari pengirim ke penerima. Lapisan *C2C Network* bertanggung jawab untuk melaksanakan fungsi *routing*, yaitu menentukan rute yang harus dilewati suatu data atau informasi melewati lebih dari satu jaringan. Lapisan *network* ini menyediakan komunikasi nirkabel *multihop* berdasarkan pengalamatan geografis dan *routing*.



Gambar 5 Arsitektur Protokol VANET menurut C2C

Aplikasi yang didukung oleh VANET dapat dikelompokkan menjadi aplikasi terkait keselamatan lalu lintas (*safety applications*) dan aplikasi lainnya (*non-safety applications*). Data dari aplikasi yang tidak terkait dengan keselamatan lalu lintas dikirimkan melalui set protokol yang ada di sisi kanan, yaitu melalui protokol TCP/UDP dan Ipv6. Lapisan MAC dan fisik yang digunakan untuk data dari aplikasi ini adalah standar WLAN IEEE 802.11 a, b, dan g.

Data dari aplikasi yang terkait dengan keselamatan dikirimkan melalui tumpukan lapisan protokol di sebelah kiri. Lapisan *C2C transport* melaksanakan beberapa tugas, antara lain *data multiplexing/ demultiplexing*, menyediakan hubungan *connection-oriented* berbasis *unicast*, pengiriman data yang handal yang sesuai untuk pengiriman data terkait keselamatan lalu lintas, dan menggabungkan data dari aplikasi yang berbeda dalam satu paket tunggal dan mengirimkannya ke sisi tujuan. Untuk lapisan MAC dan fisik, pengiriman data dari aplikasi terkait keselamatan menggunakan protokol IEEE 802.11p. Dari gambar 5, dapat dilihat bahwa aplikasi keselamatan yang tidak kritis juga dapat menerima dan mengirimkan data melalui IEEE 802.11 a/b/g atau teknologi komunikasi nirkabel lainnya, misal UMTS. Terakhir, module IC (*Information Connector*) berfungsi menyediakan mekanisme pertukaran data dari berbagai lapisan pada tumpukan protokol yang ada.

Standar IEEE 802.11p, seperti disebutkan pada paragraf di atas, dikembangkan oleh grup IEEE 802.11 untuk komunikasi antar kendaraan yang bergerak (V2V), maupun kendaraan dengan infrastruktur (V2I) dan beroperasi pada daerah frekuensi 5.850-5.925 MHz (US). Spektrum tersebut dibagi menjadi 8 kanal, 1 kanal 5 MHz untuk *guard band* dan 7 kanal untuk transmisi masing-masing sebesar 10 MHz. Dari ketujuh kanal tersebut, 1 kanal difungsikan sebagai kanal kendali (*Control Channel, CCH*) dan 6 kanal untuk kanal servis (*Service Channel, SCH*). CCH atau kanal 178, seperti ditunjukkan pada Gambar 3, digunakan untuk mengirim pesan-pesan kendali. Kanal 172,174, 176, 180,182,184 digunakan sebagai kanal SCH. Kanal nomor 172 dan 184 digunakan untuk pengiriman pesan-pesan penting yang berhubungan dengan keselamatan. Pasangan kanal 174-176 dan 180-182 dapat digunakan bersama sebagai kanal berukuran 20 MHz, yaitu kanal nomor 175 dan kanal 181 (Teixeira, 2014). Pembagian frekuensi yang digunakan untuk standar ini ditunjukkan pada Gambar 6.

Frequency (MHz)	5850	5855	5865	5875	5885	5895	5905	5915	5925
Channel number	Guard band	172	174	176	178	180	182	184	
			175			181			
Channel usage		SCH	SCH	SCH	CCH	SCH	SCH	SCH	

Gambar 6 Alokasi penggunaan frekuensi untuk komunikasi vehicular menurut IEEE 802.11p

3. HASIL DAN PEMBAHASAN

3.1 Protokol Routing untuk Jaringan Ad-Hoc

Mekanisme routing pada jaringan vehicular bertanggung jawab menjaga supaya pertukaran informasi, mengenai topologi jaringan dan kondisi tiap jalur (link state), antar node yang sebagian besar mobile dapat berlangsung terus-menerus. Informasi tersebut diperlukan untuk menentukan rute terbaik dan memelihara jalur komunikasi yang terbentuk antar sepasang node pada jaringan. Jadi, protokol routing di VANET merupakan kunci untuk terbentuknya komunikasi antar kendaraan yang handal, kontinyu, dan aman.

Ada beberapa tantangan yang dihadapi oleh protokol routing di lingkungan VANET. Tantangan tersebut muncul karena beberapa karakteristik khusus yang dimiliki oleh jaringan vehicular ini. Tantangan pertama adalah kerusakan jalur komunikasi akibat node-node yang terus bergerak keluar masuk jaringan. Adanya kesulitan untuk mempertahankan suatu rute karena perubahan topologi dan kepadatan kendaraan yang berubah-ubah. Hal ini dapat mengakibatkan throughput yang rendah dan routing overhead yang lebih tinggi. Adanya masalah hidden terminal, yaitu problem yang muncul jika terdapat terminal atau node yang di luar jangkauan beberapa node yang lain. Hidden terminal dapat menyebabkan pesat penerimaan paket data yang rendah. Gedung-gedung tinggi di daerah perkotaan juga dapat menimbulkan interferensi, seperti routing loop dan pengiriman data ke arah yang salah, sehingga dapat memperbesar delay (Venkatesh, 2014). Selain itu, protokol routing juga harus memperhatikan jenis aplikasi pada VANET. Aplikasi yang menyangkut keselamatan berlalu-lintas memerlukan protokol routing yang mampu menjamin waktu pengiriman yang tepat (strict time delay).

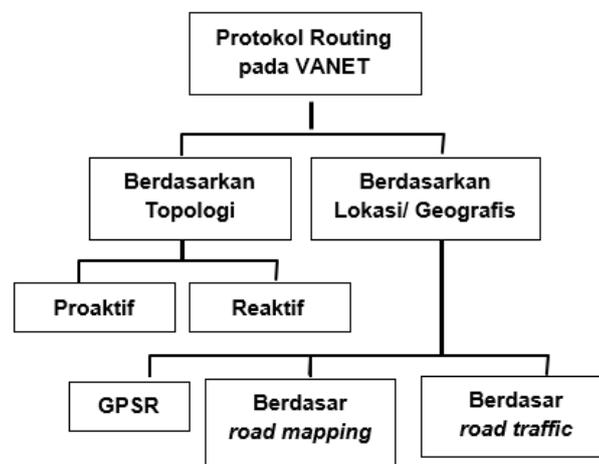
Bedasarkan penjelasan di atas, maka protokol routing yang dikembangkan untuk lingkungan VANET perlu memiliki kemampuan-kemampuan sebagai berikut:

- 1) mampu membentuk rute secara dinamis dan mempertahankan rute selama proses komunikasi,
- 2) mampu menemukan rute alternatif jika ada jalur yang putus,
- 3) mampu menentukan jalur optimal untuk mengurangi waktu untuk perutean,
- 4) mampu menyediakan banyak jalur dalam suatu jaringan untuk menghindari kemacetan data (congestion),
- 5) mampu bekerja dengan baik di lingkungan jalan raya (highway) dan perkotaan (urban) dengan kondisi trafik yang padat, maupun sepi.

3.2 Taksonomi Routing pada VANET

Protokol *routing* untuk VANET dibagi menjadi beberapa kelompok. Pengelompokan tersebut tidak seragam. Gaikwad et al., Seliem, dan Erritali mem-bagi protokol *routing* untuk VANET menjadi dua kelompok, yaitu: protokol yang berdasarkan topologi jaringan dan protokol berdasarkan posisi dari kendaraan. Venkatesh et al. mengelompokkan protokol *routing* untuk jaringan vehicular ini menjadi 4 bagian, sedangkan S. Rana et al. membaginya menjadi 5 kelompok, yaitu: kelompok protokol berdasarkan topologi jaringan, posisi kendaraan, *geocast*, *cluster*, dan *broadcast*.

Salah satu taksonomi atau pengelompokan protokol *routing* menjadi dua bagian dapat ditunjukkan pada Gambar 7. Protokol *routing* berdasarkan topologi menggunakan informasi *link* yang terdapat pada tabel *routing* di jaringan untuk meneruskan paket dari pengirim ke penerima. Kelompok ini dibagi menjadi protokol *routing* proaktif dan reaktif. *Node* dengan protokol *routing* yang reaktif menggunakan tabel *routing* untuk menyimpan informasi *routing* dan informasi lain mengenai *node-node* yang terhubung dengannya. Apabila terdapat perubahan topologi jaringan, setiap *node* yang terhubung ke jaringan tersebut harus memperbaharui tabel *routing*-nya. Protokol proaktif sebagian besar menggunakan algoritma jalur terpendek untuk menentukan rute yang dipilih (S. Rana et al, 2014). Contoh dari protokol *routing* proaktif adalah protokol FSR (*Fisheye State Routing*) dan OLSR (*Optimized Link State Routing*).



Gambar 7 Contoh Taksonomi Protokol Routing pada VANET

Kelompok protokol yang reaktif merupakan protokol *on-demand*, yaitu protokol akan memulai proses pencarian rute jika permintaan dari suatu *node* untuk berkomunikasi dengan *node* lainnya. Dibandingkan dengan kelompok proaktif, protokol ini menghasilkan lebih sedikit *overhead* karena rute yang dipertahankan hanya rute yang sedang digunakan untuk pengiriman data. Contoh protokol yang masuk kelompok ini adalah AODV (*Ad Hoc On Demand Distance Vector*), DSR (*Dynamic Source Routing*), dan TORA (*Temporally Ordered Routing Algorithm Protocol*) (Erritali& Ouahidi, 2013).

Kelompok protokol *routing* geografis melakukan mekanisme *routing* berdasarkan posisi geografis *node-node*. Untuk melaksanakan mekanisme *routing* secara geografis, tiap *node* harus dilengkapi dengan piranti penentu lokasi, seperti GPS. Asumsi yang berlaku adalah bahwa setiap *node* mengetahui posisinya, posisi dari *node-node* tetangga, dan posisi dari *node* yang dituju (Gaikwad et.al., 2016). Lokasi geografis dari *node-node* diketahui berdasarkan informasi-informasi pendek (*beacon*) yang dikirimkan oleh *node-node* tersebut pada interval waktu tertentu.

Pada protokol GPSR (*Greedy Perimeter Stateless Routing*), tiap *node* mengirimkan secara periodis pesan (*beacon*) yang berisi alamat dan lokasi (x, y) masing-masing ke *node-node* di sekitarnya (Kakarla et al, 2011). Apabila suatu *node* tidak menerima pesan *beacon* dalam jangka waktu tertentu dari salah satu *node* tetangganya, maka router GPSR akan menganggap *node* tetangga tersebut di luar jangkauan dan akan menghapusnya dari tabel *routing*. Algoritma *Greedy* diperlukan untuk menentukan *node-node* tetangga dalam suatu jaringan. *Node* pada protokol ini menggunakan algoritma *Greedy* dan meneruskan (*forward*) paket data ke *node* tetangga yang paling dekat dengan tujuan.

Kelompok protokol *routing* geografis yang lain mendasarkan keputusan *routing* -nya pada keadaan jalan sesuai peta (*road mapping*). Contoh dari protokol ini adalah GSR (*Geographic Source Routing*) dan GPCR (*Greedy, Perimeter Coordinator Routing*). GSR beroperasi berdasarkan pada posisi geografis dan informasi topologi jalan. Jadi, *node* sumber yang akan mengirimkan data ke suatu kendaraan akan menghitung jalur *routing* terpendek ke tujuan menggunakan informasi geografis yang diperoleh dari peta jalan. GPCR adalah protokol yang merupakan kombinasi dari GPSR dan penggunaan peta digital. Selain berdasarkan peta, terdapat protokol-protokol *routing* yang berbasis kondisi trafik, seperti pada protokol A-STAR. Protokol ini melakukan *routing* berdasarkan trafik dan karakteristik dari jalan. Pembobotan dilakukan berdasarkan kapasitas dari jalan.

Pada pengelompokkan protokol *routing* yang lain, terdapat kelompok protokol berbasis *cluster* dan protokol berbasis *broadcast*. Pada protokol berbasis *cluster*, jaringan dibagi menjadi beberapa kelompok (*cluster*). Tiap kelompok terdiri dari beberapa *node* yang memiliki karakter sama, misalnya persamaan kecepatan gerak dan persamaan arah. Tiap kelompok memiliki kepala yang bertanggung jawab mengatur komunikasi di dalam dan keluar dari *cluster*. Contoh dari protokol ini adalah CBR (*Cluster Baser Routing*) dan CBLR (*Cluster Based Location Routing*). Selanjutnya adalah protokol-protokol yang menggunakan metode pengiriman *broadcast*. Metode pengiriman ini menggunakan mekanisme *flooding* untuk menyebarkan informasi ke semua *node* pada suatu jaringan. Contoh dari kelompok ini adalah protokol SRB (*Secure Ring Broadcast*) dan BROADCAST (S. Rana et al., 2014).

Beberapa persamaan dan perbedaan dari protokol-protokol *routing* untuk VANET dari berbagai kelompok ditunjukkan oleh tabel 1 dan tabel 2 berikut. Protokol-protokol yang mewakili kelompok protokol *routing* VANET yang berbeda dibandingkan menurut mekanisme *routing* dan *forwarding* yang dilakukan, skenario, besarnya *overhead* untuk pengendalian, kebutuhan akan peta digital, pemberitahuan posisi *node*, dan pengelompokkan dalam jaringan (*clustering*).

Tabel 1 Perbandingan Protokol-protokol Routing (Mekanisme Routing, Mekanisme Forwarding, Skenario, Overhead)

Protocol	Routing Mechanism	Forwarding Strategy	Scenario	Control Overhead
FSR	Unicast	Multi-hop	Urban	High
OLSR	Broadcast	Multi-hop	Urban	High
AODV	Unicast Multicast	Store & Forwarding	Urban	Low
DSR	Unicast	Multi-hop	Urban	Low
TORA	Unicast Multicast	Multi-hop	Urban	
GPSR	Unicast	Greedy	Both	Medium
GSR	Unicast	Greedy	Urban	Medium
GPCR	Unicast	Greedy	Urban	Medium

A-STAR	Unicast	Greedy	Urban	-
CBLR	Cluster Based	Multi-hop	Urban	Low
SRB	Broadcast	Store & forwarding	Highway	High

Tabel 2 Perbandingan Protokol-protokol Routing (Kebutuhan akan Peta Digital, Posisi, dan Clustering)

Protocol	Digital Map Required	Position Verification	Clustering
FSR	No	No	No
OLSR	No	No	No
AODV	No	No	No
DSR	No	No	No
TORA	No	No	No
GPSR	Yes	Yes	No
GSR	Yes	Yes	No
GPCR	Yes	Yes	No
A-STAR	Yes	Yes	No
CBLR	Yes	-	Yes
SRB	No	No	No

3.3 Protokol AODV, DSR, dan TORA

Protokol AODV, DSR dan TORA adalah protokol *routing* yang berbasis topologi dan bersifat reaktif. Ketiga protokol ini, pada bab 6 akan dibandingkan kinerjanya dan dianalisis manakah yang memberikan kinerja yang lebih baik di lingkungan VANET. Bab ini akan menjelaskan secara singkat ketiga protokol tersebut.

3.4 DSR (*Dynamic Source Routing*)

Protokol ini merupakan protokol *routing* yang memiliki *overhead* yang rendah, tapi mampu menyesuaikan dengan perubahan yang terjadi pada jaringan. DSR menentukan dan membentuk rute jika ada permintaan dan dirancang untuk bekerja pada jaringan ad-hoc multihop tanpa adanya kendali terpusat. Protokol ini tidak memerlukan pesan *routing* yang periodik, penginderaan status jalur komunikasi, paket untuk mendeteksi *node-node* tetangga, sehingga dapat mengurangi kebutuhan *bandwith* untuk *overhead*, menghindari proses perbaruan *routing* yang besar, dan lebih menghemat daya baterai (Khandakar, 2012). DSR menggunakan *source routing* dengan informasi rute atau urutan *node* lengkap yang tercantum pada *overhead*.

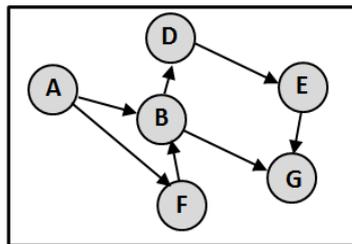
Protokol DSR terdiri dari dua mekanisme utama, yaitu mekanisme pencarian rute (*route discovery*) dan mekanisme untuk memelihara rute (*route maintenance*) (Johnson et al, 2003). Kedua mekanisme tersebut beroperasi dengan mode "*on demand*". Mekanisme pencarian rute dilakukan apabila terdapat suatu *node* (S) yang akan mengirimkan data ke *node* tujuan (D) dan S belum memiliki rute dasar (*source route*) ke D. Sedangkan *route maintenance* adalah mekanisme yang memungkinkan *node* S mendeteksi adanya perubahan pada topologi jaringan ketika menggunakan rute dasar ke D. Apabila terdapat suatu jalur pada rute ke D yang tidak sapat digunakan, maka *route maintenance* akan menyimpulkan bahwa rute dasar menuju ke D terputus dan S dapat menggunakan rute lain menuju D, atau mengaktifkan mekanisme pencarian rute untuk menentukan rute baru ke D.

3.5 AODV (*Ad-hoc On-demand Distance Vector*)

AODV adalah protokol *routing* reaktif yang dapat digunakan untuk mendukung komunikasi unicast atau multicast. Protokol ini tidak menyimpan informasi rute yang lengkap, melainkan hanya informasi *node* yang harus dituju pada lompatan berikutnya. Sama dengan DSR, protokol ini juga terdiri dari dua mekanisme utama, yaitu: mekanisme pencarian rute dan pemeliharaan rute. Pesan RREQ (*Route Request*) dan RREP (*Route Reply*) digunakan untuk pencarian rute. *Node* yang akan mengirimkan data akan menyebarkan paket RREP ke *node-node* di sekitarnya untuk menemukan *node* tujuan. Jadi, paket RREQ digunakan untuk mengawali pembentukan rute menuju tujuan.

Terdapat beberapa informasi yang ada pada paket RREQ, antara lain: alamat *node* sumber/pengirim dan alamat *node* penerima, pencacah *hop*, *source sequence number*, *destination sequence number*, dan *broadcast ID*. Pencacah *hop* atau lompatan berfungsi sebagai pencatat jumlah lompatan setiap dilakukan pengiriman paket RREQ. *Broadcast ID* adalah identitas dari paket RREQ. Nilai ID ini akan bertambah setiap kali *node* sumber mengirimkan RREQ. Langkah-langkah pencarian rute pada AODV yang lengkap adalah sebagai berikut (Pradana et al., 2017):

- 1) Jika suatu *node* sumber (S) membutuhkan suatu rute menuju *node* tujuan (D), tahap awal yang dilakukan oleh *node* sumber adalah menyebarkan paket *route request* (RREQ) menuju *node* tetangganya, seperti ditunjukkan pada Gambar 8.



Gambar 8 Contoh Penyebaran Pesan RREQ

- 2) Apabila *node* yang menerima RREQ memiliki informasi rute menuju D, maka *node* tersebut akan mengirim paket RREP kembali menuju *node* sumber melalui *reverse path* yang diciptakan RREQ setiap kali *flooding* dilakukan. Namun, jika *node* tersebut tidak memiliki informasi rute menuju D, maka *node* tersebut akan menyiarkan ulang pesan RREQ ke *node* di sekitarnya.
- 3) *Node* yang menerima RREQ dengan nilai alamat sumber dan nilai *broadcast ID* yang sama dengan RREQ yang diterima sebelumnya, akan mempertahankan RREQ yang sudah diterima di awal dan membuang RREQ baru.
- 4) Ketika sebuah *node* yang memiliki informasi rute menuju D menerima RREQ, maka *node* tersebut akan melakukan perbandingan antara nilai *destination sequence number* yang telah dimiliki dengan *sequence number* yang ada pada RREQ. Jika *sequence number* pada *node* lebih besar atau sama dengan yang ada di RREQ, maka *node* akan mengirim paket RREP menuju S. Jika *sequence number* pada RREQ lebih kecil, maka pesan RREQ akan diteruskan ke *node* lain.
- 5) Jika terdeteksi adanya kerusakan rute, mekanisme *route maintenance* akan mengirimkan paket *route error* (RERR) menuju S dan *node* sumber akan kembali menyebarkan paket RREQ.
- 6) Informasi masa aktif rute akan diberikan oleh *node* antara yang menerima RREQ. Informasi untuk perutean dari sumber (S) ke D akan dihapus jika waktu aktifnya telah habis.

3.6 TORA (*Temporally Ordered Routing Algorithm*)

Protokol TORA bekerja menggunakan algoritma yang berusaha membangun DAG (*Directed Acyclic Graphs*) yang berorientasi tujuan. Protokol ini termasuk kelompok algoritma *link reversal*. Pada dasarnya, TORA melaksanakan 3 tugas sebagai berikut: pembentukan rute dari sumber ke tujuan, pemeliharaan rute, dan penghapusan rute yang tidak terpakai. Ketiga tugas tersebut terlaksana dengan penggunaan paket QRY, UPD, dan CLR.

Pertama-tama, DAG dibentuk antara *node* sumber dan *node* tujuan. Jika ada jalur yang putus, maka diperlukan perhitungan ulang DAG untuk menentukan rute yang baru. Jika jaringan terbagi, maka diperlukan penghapusan rute. DAG adalah graf berarah tanpa siklus. DAG pada TORA berakar pada tujuan (*destination oriented*). Semua jalur yang ada pada graf tersebut berujung pada tujuan sehingga akan dihasilkan banyak rute ke tujuan.

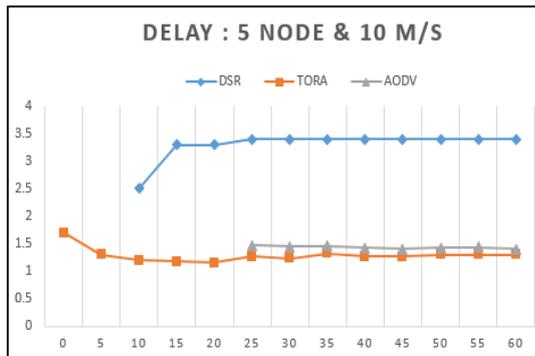
3.7 Perbandingan

Pada bab ini, kinerja dari protokol AODV, DSR, dan TORA akan dibandingkan berdasarkan penelitian-penelitian yang telah dilakukan oleh Saeed et al. (2017), Pradana dkk. (2017), Erritali & Ouahidi (2013), dan Khandakar (2012). Perbandingan antar protokol dilakukan dengan menggunakan bantuan perangkat lunak *Network Simulator*. Model pergerakan *node* yang dipilih adalah *random/random waypoint* untuk mewakili lingkungan yang menyerupai VANET. Jumlah *node* dan kecepatan gerak *node* diubah-ubah untuk melihat kinerja masing-masing protokol pada kondisi yang berbeda-beda.

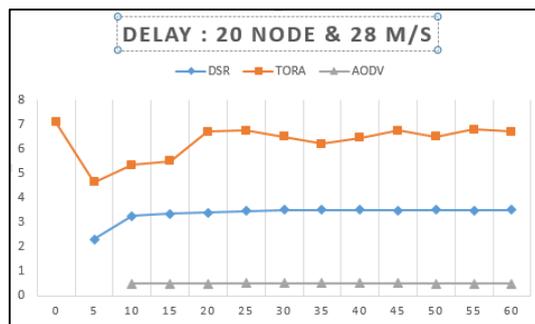
Perbandingan antar protokol tersebut dilihat dari hasil pengamatan terhadap *packet delivery ratio* (PDR), *end to end delay*, *routing load*, *packet loss percentage* (PLP), dan debit. PDR adalah rasio jumlah paket yang diterima dengan

jumlah paket yang dikirimkan. *End to end delay* adalah waktu yang diperlukan suatu paket data melintasi jaringan dari sumber ke tujuan. PLP adalah perbandingan antara paket yang gagal sampai tujuan per jumlah paket yang dikirim oleh suatu *node* (dalam persen) dan *routing load*. Debit mengacu pada pesat transfer data pada suatu saat tertentu dalam bit per detik atau bps (Erritali, 2013).

Grafik-grafik pada gambar 9,10,11,12 mengacu pada penelitian oleh Erritali dan Ouahidi. Beberapa protokol yang dirancang untuk jaringan *ad-hoc* dibandingkan berdasarkan *routing traffic*, pesat transfer data pada suatu waktu (debit), dan *delay*. Sumbu x pada grafik menunjukkan waktu dalam menit. Jumlah node dalam pelaksanaan simulasi bervariasi, yaitu: 5, 20, 40 dengan kecepatan *node* 10 m/det (36 km/jam) dan 28 m/det (100,8 km/jam). Jumlah *node* 5 mewakili jaringan dengan kepadatan rendah, 20 untuk kepadatan sedang, dan 40 untuk kepadatan tinggi.

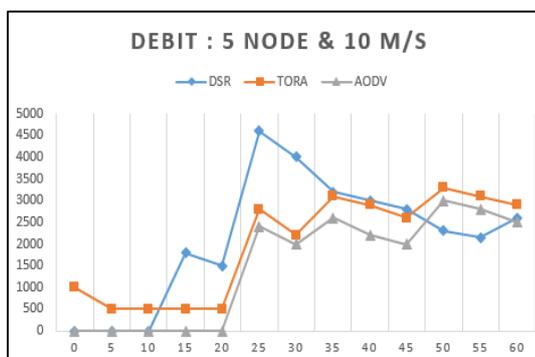


Gambar 9 Grafik Delay dengan 5 Node dan Kecepatan 10 m/s (Satuan mdetik)

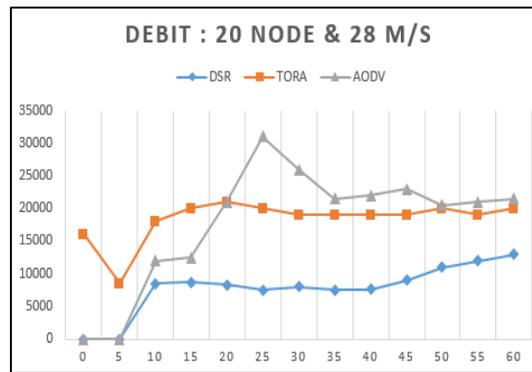


Gambar 10 Grafik Delay dengan 20 Node dan Kecepatan 28 m/s (Satuan mdetik)

Berdasarkan grafik pada gambar 9, terlihat bahwa waktu pengiriman paket (*delay*) untuk jaringan dengan kepadatan rendah dan mobilitas rendah bernilai stabil untuk protokol DSR, TORA, dan AODV. DSR memerlukan *delay* tertinggi, yaitu sekitar 3,5 mdetik. Protokol TORA menunjukkan kinerja yang lebih baik dibandingkan AODV dan DSR, dengan nilai *delay* di bawah 1.5 mdetik. Nilai *delay* yang dihasilkan protokol TORA menjadi di jaringan yang lebih padat dengan mobilitas tinggi.

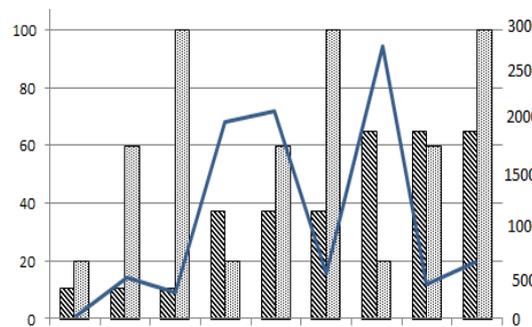


Gambar 11 Grafik Debit dengan 5 Node dan Kecepatan 10 m/s (Satuan bit/det)

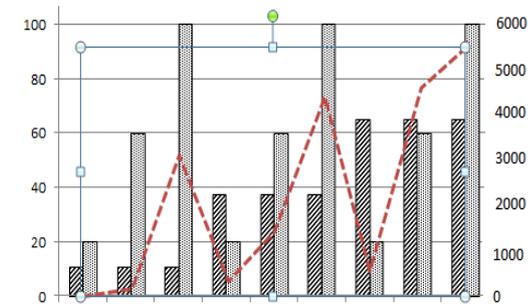


Gambar 12 Grafik Debit dengan 20 Node dan Kecepatan 10 m/s (Satuan bit/det)

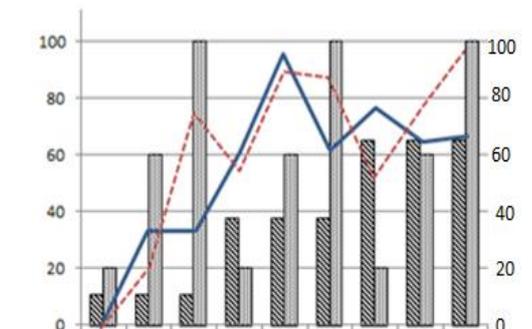
Dari gambar 11 dapat dilihat bahwa untuk jumlah *node*=5 dan kecepatan=10 m/det, pesat transter yang bisa dicapai DSR lebih tinggi dibandingkan protokol TORA. Debit dari DSR dapat mencapai 4700 bps. Namun nilai debit yang dihasilkan oleh DSR menjadi rendah seiring dengan kenaikan kepadatan jaringan. Pada gambar 12, nilai pesat transfer tertinggi yang dicapai oleh DSR adalah 10000 bps, sedangkan TORA dan AODV masing-masing memiliki pesat atau debit sampai sekitar 20000 bps dan 30000 bps.



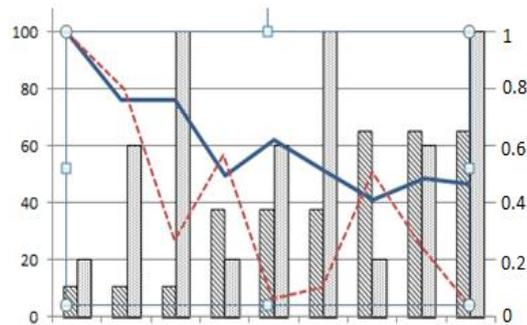
Gambar 13 Grafik Average End to End Delay (ms) vs Density & Average Speed (Mobility) – AODV



Gambar 14 Grafik Average End to End Delay (ms) vs Density & Average Speed (Mobility) – DSR



Gambar 15 Grafik Packet Loss Percentage vs Density & Average Speed (Mobility)



Gambar 16 Grafik Packet Delivery Ratio vs Density & Average Speed (Mobility)

4. KESIMPULAN

Di simpulkan penelitian ini yaitu:

1. VANET sebagai jaringan ad-hoc nirkabel dengan *node* yang memiliki mobilitas tinggi dan berbagai karakteristik khusus lainnya memerlukan mekanisme *routing* tertentu yang mampu bekerja mempertahankan komunikasi antar *node* dengan baik.
2. Protokol DSR, AODV dan TORA adalah protokol yang akan membentuk koneksi hanya jika ada *node* yang akan mengirimkan data. Ketiganya merupakan protokol yang berbasis topologi, jadi isi tabel *routing* mengikuti perubahan topologi dalam jaringan.
3. Berdasarkan penelitian, protokol TORA pada jaringan dengan jumlah *node* sedikit dan kecepatan gerak yang rendah menghasilkan *delay* yang paling sedikit. Untuk kondisi jaringan yang padat dan kecepatan tinggi, *delay* dari protokol TORA menjadi lebih besar dibandingkan DSR dan AODV.
4. Dari sisi pesat transfer atau debit, protokol DSR menghasilkan kinerja yang terbaik pada jaringan dengan jumlah *node* sedikit. Kinerja tersebut menurun seiring dengan kepadatan jaringan yang bertambah.

DAFTAR PUSTAKA

- [1] Almalag, M.S., M.C. Weigle, S. Olariu. (2013). *MAC Protocols for VANET. Mobile Ad-hoc Net-working: Cutting Edge Directions*, 2nd ed. New Jersey: IEEE Press. pp 599-618.
- [2] Bijan, P., M. Ibrahim, dan M.A.N. Bikas. (2011). *VANET Routing Protocols: Pros and Cons*. International Journal of Computer Applications, Vol. 20, No.3, April 2011: 28-34.
- [3] CAR-2-CAR Communication Consortium Manifesto. (2017). http://elib.dlr.de/48380/1/C2C-CC_manifesto_v1.1.pdf
- [4] Dass, R., R. Sangwan, I. Girhdar. (2012). *Vehicular Ad Hoc Networks*. International Journal of Advanced Trends in Computer Science and Engineering, Vol. 1, No.4, September - October 2012: 121-129.
- [5] Erritali, M. dan B.E. Ouahidi. (2013). *Performance Evaluation of Ad-hoc Routing Protocols in VANETs. IJACSA Special Issue on Selected Papers from Third International Symposium on Automatic Amazigh Processing: 33-38*.
- [6] Gaikwad, S.K., A.R. Deshmukh, S.S. Dorle. (2016). *A Survey of Routing Protocols for Vehicular Ad-hoc Networks. International Journal of Computer Applications, Vol. 139, No.1, April 2016: 34 – 37*.
- [7] Johnson, D., D. A. Maltz, and Y. C. Hu. (2003). *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*. IETF Internet Draft, work in progress, April 2003.
- [8] Kakarla, J., S.S. Sathya, B.G. Laxmi, Ramesh B.B. (2011). *A Survey on Routing Protocols and Its Issues in VANETs. International Journal of Computer Applications, Vol.28, No.4, August 2011: 38 – 44*.
- [9] Khandakar, A. (2012). *Step by Step Procedural Comparison of DSR, AODV, and DSDV Routing Protocol*. International Conference on Computer Engineering and Technology (ICCET 2012), IPCSIT Vol.40: 36. Singapor: IACSIT Press.
- [10] Liang, W., Z. Li, H. Zhang, S. Wang, R. Bie. (2015). *Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends*. International Journal of Distributed Sensor Networks, Vol. 2015, Article ID 475303.
- [11] Pradana, P.D., R. M. Negara, F. Dewanta. (2017). *Evaluasi Performnsi Protokol Routing DSR dan AODV pada Simulasi Jaringan VANET untuk Keselamatan Transportasi dengan Studi Kasus Mobil Perkotaan*. E-Proceeding of Engineering, Vol. 4, No.2, Agustus 2017: 1996-2004.
- [12] Rana, S., S. Rana, dan K.C. Purohit. (2014). *A Review of Various Routing Protocols in VANET*. International Journal of Computer Applications, Vol.96, No. 18, June 2014: 28.
- [13] Raw, R.S., M. Kumar, N. Singh. (2013). *Security Challenges, Issues, and Their Solutions for VANET*. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013: 96-105.

- [14] Saeed, N., R.U. Amin, A.S. Malik, M.K. Kasi, dan B. Kasi. (2017). *Performance Evaluation of AODV, DSDV and DSR Routing Protocols in Unplanned Areas*. Technical Journal University of Engineering and Technology Taxila, Vol. 22, No. I-2017: 143-150.
- [15] Seliem, H.M. (2014). *Ad-Hoc on Demand Distance Vector (AODV) Routing Protocol for V2V Communication*. Thesis submitted for the Degree of Master of Science in Computer and Information Sciences Ain Shams University.
- [16] Stallings, W. (2011). *Komunikasi Data dan Komputer*. Jakarta: Penerbit Salemba Infotek.
- [17] Teixeira, F.A., V.F. e Silva,, J.L.Leoni, J.F. Mace-do, J.M.S.Nogueira. (2014). *Vehicular Networks Using IEEE 802.11p Standard: An Experimental Analysis*. Vehicular Communications 1 (2014): 91-96.
- [18] Toutoh J., J.G. Nietoo, dan E. Alba. (2012). *Intelligent OLSR Routing Protocol Optimization for VANETs*. IEEE Transactions on Vehicular Technology.
- [19] Venkatesh, A. Indra, dan R. Murali. (2014). *Routing Protocols for Vehicular Adhoc Networks (VANETs): A Review*. Journal of Emerging Trends in Computing and Information Sciences, Vol.5, No.1, Januari 2014: 25.