

PENGARUH SERANGAN KEAMANAN PADA VANET TERHADAP PERFORMANSI JARINGAN

Alfon Sera¹⁾, Linna Oktaviana Sari²⁾

¹⁾Mahasiswa Program Studi Teknik Elektro ²⁾Dosen Teknik Elektro

Laboratorium Telekomunikasi

Program Studi Teknik Elektro S1, Fakultas Teknik Universitas Riau

Kampus Bina Widya Jl. HR. Soebrantas Km 12,5 Simpang Baru, Panam,
Pekanbaru 28293

Email: alfon.sera@student.unri.ac.id

ABSTRACT

Information and communication technology developing are very rapidly, because human needs keep growing. Human safety in driving is one of the important factors in technological development. VANET is communication between vehicles, so that it can be used as a smart traffic information system. The VANET network is an ad-hoc network that does not have a fixed infrastructure and the rapidly changing network topology VANET is vulnerable to various attacks. Analysis of AODV routing protocol using 150 nodes with no attack and with blackhole attack scenario. This research uses Network Simulator 2 and SUMO software to make a model of node mobility. The results show that the network simulated without attack has 99.56% PDR value the PDR value with blackhole attack is 0%. In conclusion, VANET network performance is otherwise influential towards blackhole attack because, the difference value between no attack PDR value & blackhole attack PDR value is so significant.

Keywords : VANET, AODV, Blackhole, PDR.

1. Pendahuluan

Teknologi informasi dan komunikasi berkembang sangat pesat, hal ini terjadi karena kebutuhan umat manusia yang terus berkembang. Keamanan dan keselamatan manusia dalam berkendara menjadi salah satu faktor penting perkembangan teknologi. *Wireless*, teknologi yang terus mengalami peningkatan karena memiliki kelebihan dan tidak memerlukan banyak perangkat dalam pengaplikasiannya, mendukung mobilitas perangkat dan pertukaran informasi dengan cepat.

VANET merupakan versi terbaru pada jaringan dan merupakan pengembangan dari MANET (*Mobile Ad hoc Network*). Tujuan dasar VANET adalah untuk mendukung komunikasi antar kendaraan sehingga dapat digunakan sebagai sistem informasi trafik lalu lintas cerdas. Komunikasi ini dapat dilakukan langsung antar kendaraan (*Vehicle to Vehicle*) dan antara kendaraan-infrastruktur (*Vehicle to Infrastructure*).

Serangan ini tidak luput pada VANET karena VANET menggunakan media *wireless* yang diaplikasikan pada kendaraan, hal ini sangat mempengaruhi keselamatan saat berkendara bagi pengemudi maupun penumpang.

Penelitian tentang jaringan VANET ini sudah banyak diterbitkan didalam jurnal maupun skripsi. Pada jurnal Kshama, dkk pada tahun 2016 menganalisa efek dari hilangnya paket di jaringan karena serangan *blackhole* dan *grayhole* dan juga mengusulkan teknik deteksi yang secara kompeten mendeteksi kedua serangan dalam jaringan. Dalam penelitian ini simulasi menggunakan simulator NS-2. (Kshama dkk, 2016)

Jurnal Firdaus Nutrihadi, dkk, penelitian ini yang diteliti yaitu performa skema VANET yang dihasilkan oleh *mobility generator* SUMO dan *Vanetmobisim*. Penelitian ini menggunakan NS-2 sebagai simulator VANET dengan protokol reaktif

AODV sebagai *routing protocol* (Firdaus Nutrihadi dkk, 2016)

Penelitian jurnal Raj Bala 2015, menganalisa kinerja protokol routing AODV dan GPSR dalam VANET dalam berbagai skenario di kondisi lalu lintas yang berbeda sehubungan dengan *Packet Delivery Ratio* dan *Average Delay End-to-End*. Simulasi dilakukan menggunakan NS-2.35 dan dikombinasikan dengan VanetMobiSim dimana bahwa AODV bekerja lebih baik di PDR (Raj Bala, 2015)

Berdasarkan latar belakang dan penelitian-penelitian yang sudah ada, maka dilakukan penelitian mengenai analisa Pengaruh Serangan Keamanan pada VANET Terhadap Performansi Jaringan. pengaruh berupa serangan *blackhole* yang disimulasikan dengan *software* NS-2. NS-2 adalah *software* simulasi jaringan yang bersifat *Open Source* yang banyak digunakan dalam mempelajari struktur dinamik dari jaringan komunikasi. Simulasi dari jaringan nirkabel dan protokol (seperti algoritma *routing*, CBR, TCP, dan UDP). Proses simulasi ini dilakukan untuk mengetahui nilai dari *Quality of Service* (QoS) dimana QoS tersebut adalah nilai *packet delivery ratio*.

2. Landasan Teori

2.1. VANET

Vehicular Ad hoc Networks) VANET merupakan jenis jaringan *adhoc* yang dibentuk oleh penggunaan radio jarak dekat yang dipasang pada kendaraan pribadi, dan kendaraan umum. Jaringan ini melibatkan komunikasi *Vehicle-to-Vehicle* (V2V) dan *Vehicle-to-Infrastructure* (V2I), bertujuan untuk meningkatkan keselamatan mengemudi dan manajemen lalu lintas sementara menyediakan driver dan penumpang dengan akses Internet.

Ada empat tipe komunikasi pada VANET komunikasi *In-vehicle*, *Vehicle-to-vehicle* (V2V), *Vehicle-to-road infrastructure* (V2I atau V2R), dan *Vehicle-to-broadband* (V2B) (Rosida, 2016).

1. *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

2. *Vehicle-to-vehicle* (V2V)

mengatur bagaimana kendaraan-kendaraan dapat saling bertukar informasi yang berhubungan dengan lalu lintas

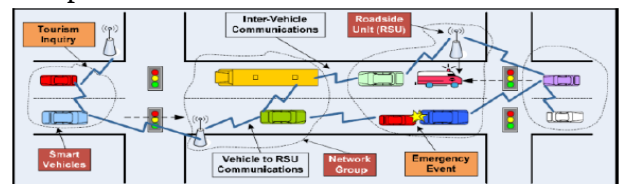
3. *Vehicle-to-road infrastructure* (V2I)

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.

4. *Vehicle-to-broadband* (V2B)

menghubungkan kendaraan dengan jaringan wireless broadband, seperti 3G/4G.

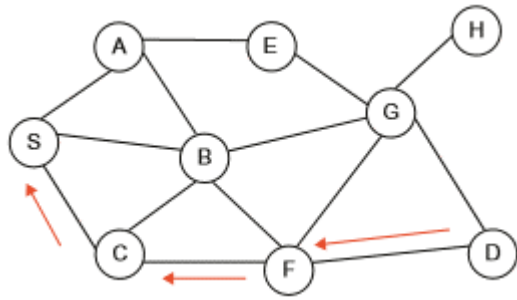
Komunikasi V2V menggunakan standar wireless atau protocol yang khusus dikembangkan untuk VANET, seperti IEEE 802.11p.



Gambar 2.1. Komunikasi jaringan VANET
(Dr. Al-Sakib Khan Pathan, 2011)

2.2. *Ad-hoc On Demand Distance Vector* (AODV)

AODV merupakan salah satu jenis reactive routing yang dirancang khusus untuk jaringan mobile ad hoc. AODV routing protocol memiliki adaptasi cepat untuk kondisi dinamik link, pemrosesan yang rendah dan overhead memori, pemanfaatan jaringan rendah, dan menentukan unicast rute ke tujuan dalam jaringan ad hoc. Selama koneksi rute pengiriman ke penerima telah *valid*, AODV tidak melakukan pencarian lagi dan akan tetap pada rute ini selama mereka dibutuhkan. Dalam proses penentuan jalur, AODV membutuhkan pesan-pesan RREQ (*Route Request*), RREP (*Route Reply*), dan RERR (*Route Error*)



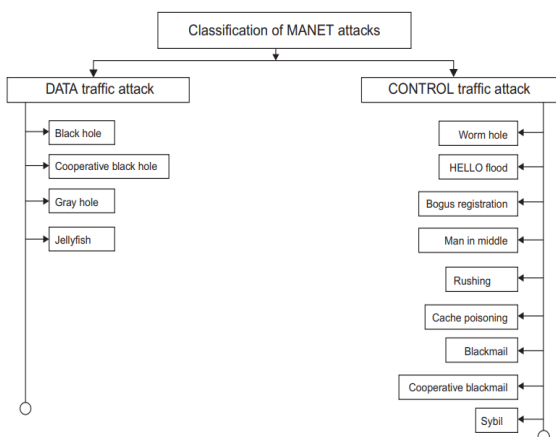
Gambar 2.2. Kinerja *Routing Protocol* AODV.(Dr. Al-Sakib Khan Pathan, 2011)

2.3. SUMO (*Simulation of Urban*)

SUMO adalah salah satu *tools* untuk *mobility generators* yang digunakan untuk simulasi VANET. SUMO merupakan *software* simulasi lalu lintas *open source* yang dirancang untuk menangani *mobility* pada jaringan dengan jalur luas. Fitur utama SUMO mengatur pergerakan kendaraan (*node*), perbedaan jenis kendaraan, multijalur, dan lain-lain.

2.4. Jenis Serangan pada VANET

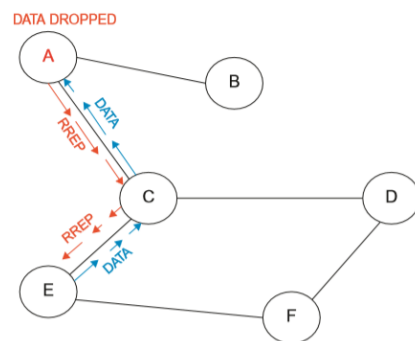
Serangan diklasifikasikan atas dasar sumber serangan, yaitu, serangan internal atau eksternal, dan berdasarkan aksi serangan yaitu, serangan pasif atau aktif. Karena penyerang dapat memanfaatkan jaringan baik secara internal, eksternal atau sebagai serangan aktif atau pasif menyerang jaringan. Ada dua jenis serangan utama yaitu, serangan lalu lintas DATA dan serangan CONTROL lalu lintas.



Gambar 2.3. Klasifikasi Serangan pada MANET

2.4. Serangan *Blackhole*

Dalam serangan *blackhole*, sebuah *node* penyerang menggunakan *routing protocol* untuk mempublikasikan dirinya sendiri memiliki rute terpendek ke *node* tujuan. *Node* penyerang ini mempublikasikan ketersediaan rute baru tanpa mengecek tabel *routing*nya. Dalam serangan ini, *node* penyerang selalu memiliki aksesibilitas dalam membalas permintaan rute sehingga menyesuaikan paket data dan membuang paket.



Gambar 2.4. Serangan *Blackhole* (Biswas & Ali, 2007)

2.5. *Quality of Service* (QoS)

Quality of Service (QoS) merupakan permasalahan tentang *internet* yang mendiskusikan tentang kualitas suatu jaringan. Dengan ini kualitas jaringan dapat diukur menjadi suatu karakteristik jaringan yang akan dicapai.

Pengukuran QoS ini akan dilakukan menggunakan script ber-ekstensi *.awk* yang data diambil dari output ekstensi *.tr* yang di dapat setelah di olah di NS2 . Berikut parameter yang akan diuji adalah *packet delivery ratio*.

- ***Packet Delivery Ratio***

Packet delivery ratio merupakan Packet data yang sukses diterima di *node* tujuan dengan total paket data yang dikirimkan oleh *node* sumber. PDR dapat menunjukkan tingkat keberhasilan sebuah protokol *routing* karena semakin tinggi nilai PDR salah satunya disebabkan oleh berhasilnya sebuah protokol *routing* dalam melakukan pencarian dan pemeliharaan rutenya. (Forouzan ., 2017).

4. Hasil dan Pembahasan

4.1. Pengukuran *Packet Delivery Ratio* Tanpa Seragan

Untuk dapat mengukur *packet delivery ratio*, diperlukan pengiriman paket data yang berhasil di terima dengan jumlah packet yang telah dikirim pada jaringan. Untuk dapat menggolah hasil dari PDR digunakan NS-2 *output* dari out.tr kemudian di analisa dengan *script* .awk yang menghasilkan informasi QoS yang dibutuhkan.

```
alfon@HP-G42:~/Documents$ awk -f analysis.awk out.tr
No_of_Packets_Sent      227
No_of_Packets_Received  226
Packet_Delivery_Ratio:  99.56 %
Control_Overhead:       91
Normalized_Routing_Overhead: 40.27 %
Delay:                   0.01 Seconds
Throughput:              21.46 Kbps
Packet_Dropping_Ratio:  0.44 %
```

Gambar 4.1 Tampilan hasil pengukuran pada jaringan VANET dengan script .awk

4.2. Pengukuran *Packet Delivery Ratio* dengan Seragan *Blackhole*

Pada gambar 4.1 terlihat bahwa semua *node* yang telah dirancang terhubung, dengan hasil PDR 99,56% hal ini disebabkan karna *node* bergerak dan ini menggunakan sistem *wireless* sehingga ada *packet drop*

```
Sorting Lists ...DONE!
alfon@HP-G42:~/Documents/Hasil/Seragan/blackhole$ awk -f analysis.awk out.tr
No_of_Packets_Sent      300
No_of_Packets_Received  0
Packet_Delivery_Ratio:  0.00 %
Control_Overhead:       69
Normalized_Routing_Overhead: 1nf %
Delay:                   -nan Seconds
Throughput:              0.00 Kbps
Packet_Dropping_Ratio:  100.00 %
```

Gambar 4.2 Hasil pengukuran dengan serangan *blackhole*

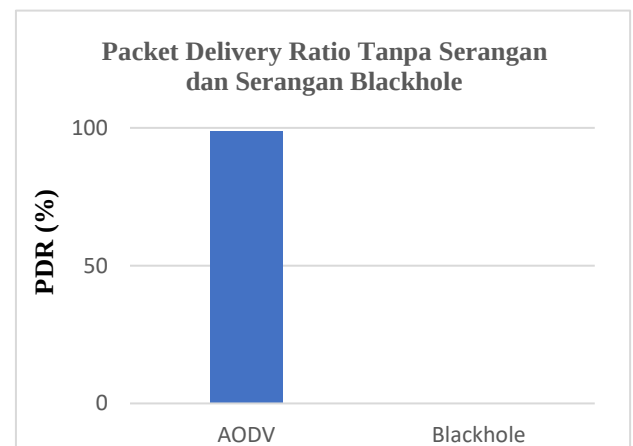
Gambar 4.2 merupakan tampilan hasil performansi dari serangan *blackhole* di terminal. Hasil ini bisa diakses setelah menjalankan simulasi dan telah diolah menggunakan *script* .awk. Hasil diatas merupakan hasil dari pengukuran jaringan VANET dengan serangan untuk mencari *packet delivery ratio* pada jaringan.

Pengukuran PDR pada jaringan VANET untuk melihat nilai perubahan performansi dari jaringan VANET tanpa serangan dengan jaringan VANET dengan serangan *blackhole*. Adapun tabel 4.1 memperlihatkan PDR dari jaringan VANET.

Tabel 4.1 *Packet Delivery Ratio*

Tanpa Seragan	Seragan Blackhole
99.56 %	0%

Pada tabel diatas terlihat bahwa nilai pada jaringan VANET tanpa serangan adalah 99,56%. Sedangkan dengan serangan 0% nilai PDR pada jaringan. Untuk melihat perbedaan nilai PDR tanpa serangan dan dengan serangan *blackhole* dapat dilihat pada gambar 4.1.



Gambar 4.1. Hasil PDR Tanpa Seragan dengan Seragan *Blackhole*

5. Kesimpulan

Hasil simulasi nilai *packet delivery ratio* jaringan VANET tanpa serangan menunjukkan nilai yang sangat baik yaitu 99,56%. Jika nilai PDR dibandingkan dengan nilai PDR dengan serangan *blackhole* di jaringan VANET, maka nilai PDR dengan serangan *blackhole* dengan hasil 0%. Jadi dapat disimpulkan bahwa serangan *blackhole* sangat mempengaruhi performansi jaringan pada VANET.

Ini terjadi karna sifat dari serangan *blackhole* adalah menerima packet data asli kemudian membuang seluruh packet yang telah diterimanya.

Daftar Pustaka

- Pathan, A.S.K. ed., 2016. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press.
- Jurnal, R.T., 2016. Jaringan Ad-hoc Vehicular (Vanet): Tinjauan Tentang Arsitektur, Karakteristik, Aplikasi, Dan Protokol Medium Access Control (Mac). *Petir*, 9(1), pp.28-37.
- Fazeldehkordi, E., Amiri, I.S. and Akanbi, O.A., 2016. –Research Methodology.
- Bala, R. and Krishna, C.R., 2015, February. Scenario based performance analysis of AODV and GPSR routing protocols in a VANET. In *Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on*(pp. 432-437). IEEE.
- Nutrihadi, F., 2016. Studi Kinerja VANET Scenario Generators: SUMO dan VanetMobisim untuk Implementasi Routing Protocol AODV menggunakan Network Simulator 2 (NS-2). *Jurnal Teknik ITS*, 5(1).