TESIS

EVALUASI KINERJA VANET DENGAN PENGARUH SERANGAN *MALICIOUS NODE* BERDASARKAN PARAMETER QOS

Disusun Oleh:

Naufal Faiz Alfarizi

20206052001

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2022

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1195/Un.02/DST/PP.00.9/06/2022

Tugas Akhir dengan judul : EVALUASI KINERJA VANET DENGAN PENGARUH SERANGAN MALICIOUS NODE BERDASARKAN PARAMETER QOS

yang dipersiapkan dan disusun oleh:

Nama : NAUFAL FAIZ ALFARIZI, S.T, MTCNA
Nomor Induk Mahasiswa : 20206052001
Telah diujikan pada : Senin, 27 Juni 2022
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Ir. Muhammad Taufiq Nuruzzaman, S.T. M.Eng., Ph.D.
SIGNED

Valid ID: 62bac80b776fa

Penguji I

Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom.
SIGNED

Valid ID: 62baac3e81ba2

Penguji II

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.
SIGNED

Valid ID: 62ba8a45d34eb

Yogyakarta, 27 Juni 2022
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 62ba022ad86a4

SURAT PERNYATAAN KEASLIAN / BEBAS PLAGIASI

Yang bertanda tangan dibawah ini:

Nama Mahasiswa	: Naufal Faiz Alfarizi
NIM	: 20206052001
Program Studi	: Informatika (S2)
Fakultas	: Sains dan Teknologi

Menyatakan dengan sesungguhnya bahwa laporan tesis saya yang berjudul: **"EVALUASI KINERJA VANET DALAM PENGARUH SERANGAN MALICIOUS NODE BERDASARKAN PARAMETER QOS"** adalah hasil karya pribadi yang tidak mengandung plagiarisme dan tidak berisi materi yang dipublikasikan atau ditulis orang lain, kecuali bagian – bagian tertentu yang penulis ambil sebagai acuan dan tata cara yang diberikan secara ilmiah.

Jika terbukti pernyataan ini tidak benar, maka penulis siap mempertanggung jawabkan sesuai hukum yang berlaku.

Yogyakarta, 27 Juni 2022

Yang menyatakan,

Naufal Faiz Alfarizi

NIM. 20206052001

Universitas Islam Negeri Sunan Kalijaga

SURAT PERSETUJUAN TUGAS AKHIR

Hal : Persetujuan Tugas Akhir
Lamp : -

Kepada Yth.,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta

Assalamualaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa naskah tesis Saudara:

Nama	:	Naufal Faiz Alfarizi
NIM	:	20206052001
Judul Tesis	:	Evaluasi Kinerja VANET dalam Pengaruh Serangan *Malicious Node* Berdasarkan Parameter QoS

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Program Studi Magister Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta untuk diujikan dalam rangka memperoleh gelar Magister Informatika.

Waalaikumsalam wr. wb.

Yogyakarta, 16 Juni 2022
Pembimbing,

Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Phd.
NIP. 19791118 200501 1 003

ABSTRAK

Teknologi jaringan *adhoc* sangat rentan terhadap berbagai jenis serangan seperti node jahat atau *Malicious Node*. Serangan *Malicious Node* terbagi atas beberapa jenis seperti dalam penelitian ini melibatkan *Malicious Node* dengan jenis *Blackhole Attack* dan *Wormhole Attack* pada model jaringan VANET yang merupakan jenis teknologi komunikasi data untuk kendaraan yang menggunakan teknologi nirkabel secara *adhoc*. Serangan *Blackhole* memberi dampak meningkatnya jumlah *packet drop* sedangkan, serangan *Wormhole* memberi dampak meningkatnya *delay* pada saat proses pendistribusian *packet* dengan dibuktikan dari nilai *Throughput*, *End to End Delay*, *Jitter* dan *Packet Loss Ratio*. Penelitian ini dilakukan dengan menggunakan SUMO untuk membuat VANET *simulation* dengan konsep *urban simulation area*, NS3 untuk membuat *Network Simulator* dan menggunakan parameter QoS berdasarkan *standard* TIPHON sebagai evaluasi dari kinerja VANET yang dipengaruhi oleh *Malious Node*.

Kata Kunci: VANET, *Malicious*, *Blackhole*, *Wormhole*, QoS, TIPHON.

MOTTO

“Gue ini tipe orang yang tidak pernah mempersiapkan sesuatu tapi selalu menyelesaikannya dengan sempurna.” – Onic Udil, 2020.

KATA PENGANTAR

Bissmillahirahmanirrahim,

Assalamualaikum warahmatullahi wabarakatuhu

Puji dan syukur kehadirat Allah SWT yang telah memberikan ridha dan hidayah-Nya serta kekuatan, Kesehatan dan kesabaran. Sehingga penulis dapat menyelesaikan tesis yang berjudul "**EVALUASI KINERJA VANET DALAM PENGARUH SERANGAN MALICIOUS NODE BERDASARKAN PARAMETER QOS".**

Dalam penyusunan dan penyelesaian naskah tesis ini, penulis menyadari bahwa terdapat banyak semangat dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan kali ini penulis menyampaikan terimakasih dan penghargaan kepada:

1. Ibu Dr. Khurul Wardati, M,Si, selaku dekan fakultas SAINTEK UIN Sunan Kalijaga.
2. Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T, selaku Kaprodi Magister Informatika dan dosen penguji 2.
3. Bapak Dr. Agung Fatwanto, S.Si., M.Kom, selaku dosen pembimbing akademik.
4. Bapak Muhammad Taufiq Nuruzzaman, S.T., M.Eng., Ph.d, selaku dosen pembimbing tesis.
5. Ibu Dr. Ir. Shofwatul 'Uyun, S.T., M.Kom, selaku dosen penguji 1.

Terimakasih juga saya sampaikan kepada seluruh Dosen Magister Informatika yang selama ini telah banyak memberikan ilmu dan wawasan yang berguna. Semangat penulis dalam menyelesaikan naskah tesis ini juga tidak lepas dari dukungan keluarga dan rekan – rekan oleh karena itu dalam kesempatan ini penulis juga mengucapkan terimakasih kepada seluruh keluarga besar terutama orang tua saya yang telah mendoakan dan memotivasi saya sehingga dapat menyelesaikan tugas akhir ini dan tidak lupa saya mengucapkan mengucapkan terimakasih kepada rekan – rekan Magister Informatika Angkatan 2020 atas kekeluargaan yang diberikan selama ini.

Akhir kata, penulis sangat mengharapkan kritik dan saran yang dapat membangun karena naskah tesis ini sangat jauh dari kata sempurna. Semoga Allah meridhoi Langkah kita, Aamiin. Demikian laporan ini penulis susun, semoga dapat dikembangkan dan dimanfaatkan sesuai dengan kapasitasnya dan Semoga Allah SWT senantiasa mencurahkan ilmu pengetahuan yang bermanfaat bagi seluruh umat dan memberikan petujuk di jalan-Nya.

Wassalamualaikum warahmatullahi wabarakatuhu

Yogyakarta, 27 Juni 2022

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Quality of Service (QoS) merupakan sebuah metode pengukuran yang dapat digunakan untuk menentukan kualitas dari kinerja jaringan VANET Ketika sedang mengalami serangan dari *Malicious Node* seperti *Blackhole attack dan Wormhole Attack*. Serangan *Blackhole* adalah sejenis serangan *Denial of Service* (Dos) pada jaringan *Adhoc.* Serangan ini terbagi menjadi dua macam yaitu serangan yang hanya dilakukan oleh satu node penyerang dan serangan *collaborative blackhole* yang dilakukan oleh lebih dari satu node penyerang. Serangan *blackhole* menjadi berbahaya karena memberikan informasi pada node sumber bahwa ia memiliki rute tercepat untuk menuju node tujuan, sehingga node sumber mengirimkan paketnya melalui node *black hole*. Kemudian secara diam – diam node *black hole* membuang paket yang diterimanya dengan menyamarkan dirinya layaknya sebuah node normal (Istiqomah et al., 2018). Sedangkan, Serangan *Wormhole* merupakan bagian dari *Malicious Node* yang dapat membahayakan kinerja dari jaringan *adhoc*. *Wormhole* merupakan suatu serangan pada jaringan dengan terdapat satu atau lebih *Wormhole* node yang saling terhubung dan bekerja sama untuk menyerang lalu lintas jaringan (Jenefer and Vydeki, 2013). Node *attacker* tersebut memiliki jarak yang cukup jauh antar *node attacker* satu dengan node *attacker* yang lainnya

dan setiap node *attacker* tersebut mengirimkan paket yang diterima dari node biasa ke node *attacker* lainnya menggunakan *wormhole tunnel*. Dengan *tunnel* tersebut antar node *attacker* satu dan node *attacker* lainnya hanya memiliki nilai satu hop meskipun memiliki jarak yang cukup jauh dan terlihat memiliki jalur yang lebih pendek dibandingkan dengan melewati jalur yang seharusnya. Dengan demikian dampak yang diberikan dari serangan *wormhole* tentunya dapat berpengaruh terhadap *end to end delay* pengiriman paket dari node sumber ke node tujuan.

Vehicular Adhoc Network (VANET) adalah teknologi komunikasi data untuk kendaraan. Jaringan VANET merupakan jaringan yang menggunakan teknologi nirkabel (*wireless*) secara *adhoc (Sampetoding et al., 2020).* Tentunya serangan *Malicious Node* ini akan sangat berbahaya jika paket yang dikirmkan adalah sebuah paket yang berisi informasi – informasi penting karena VANET apabila sudah diimplementasikan pada setiap kendaraan dapat mengurangi resiko kecelakaan. VANET sangat berperan pada perkembangan teknologi *Intelligent Transportation System* (ITS) dalam menyediakan aplikasi keamanan dan kenyamanan bagi para pengendara jalan. Oleh karena itu, diperlukan sebuah pengujian mengenai kinerja VANET Ketika dalam pengaruh *Malicious Node* seperti *Blackhole Attack* yang dapat menyebabkan *packet drop* berlebih dan *Wormhole Attack* yang dapat menyebabkan peningkat *delay*.

Dengan demikian, penelitian terkait evaluasi diambil mengenai kinerja VANET dengan pengaruh *Malicious Node Attack* berdasarkan QoS. Penelitian tersebut termasuk dalam *experiment*. Pada penelitian ini, Penulis menggunakan Sumo sebagai generator skema VANET yang

kemudian dilakukan analisis terkait *mobility node* dengan menggunakan *Network Simulator*-3. *Network Simulator* merupakan sebuah perangkat lunak yang dapat digunakan untuk melakukan simulasi jaringan komputer terkait dengan topologi yang digunakan dan bagaimana proses komunikasi pada suatu jaringan sedang berlangsung. *Network Simulator* juga dapat digunakan pada jaringan kabel dan komunikasi jaringan *wireless* atau tanpa kabel dan hasil yang didapat kemudian dilakukan evaluasi kinerja jaringan dengan menggunakan teknik QoS. Parameter dalam QoS yang diujikan untuk melakukan evaluasi kinerja VANET dalam mengatasi serangan *Malicious Node* pada jalur komunikasi antar node adalah *throughput*, *end to end delay*, *jitter* dan *packet loss ratio*.

Pada skenario yang dibuat dalam evaluasi dari kinerja VANET dengan pengaruh *Malicious Node Attack* berdasarkan QoS yaitu dengan simulasi model jaringan VANET menggunakan *routing protocol* AODV yang dipengaruhi oleh *Malicious Node* seperti *Blackhole Attack* dan *Wormhole Attack* serta untuk komunikasi antar kendaraan yang digunakaan yaitu lingkungan perkotaan dengan IEEE 802.11p yang termasuk kedalam WAVE. Metriks pengujian berdasarkan parameter QoS memiliki performasi berupa *Throughput*, *End to End Delay*, *Jitter* dan *Packet loss ratio*. Tujuan utama dari QoS untuk menyampaikan informasi dari hasil pengujian yang dilakukan terkait evaluasi dari kinerja VANET Ketika dalam pengaruh *Malicious Node*.

B. RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah bagaimana melakukan evaluasi terkait kestabilan kinerja dari VANET dalam menghadapi serangan *Malicious Node* yang diujikan dengan menggunakan parameter yang telah ditentukan dalam QoS berdasarkan *standard* TIPHON?

C. BATASAN MASALAH

Batasan masalah merupakan ruang lingkup dari permasalahan yang dibatasi dalam penelitian Evaluasi Kinerja VANET Dengan Pengaruh Serangan *Malicious Node* Berdasarkan Parameter QoS. Adapun Batasan masalah yang sudah ditetapkan dalam penelitian ini, antara lain:

1. Teknologi jaringan *Adhoc* yang digunakan dalam penelitian ini adalah *Vehicular Adhoc Network* (VANET) dengan pengaruh serangan *Malicious Node* seperti *Blackhole Attack* dan *Wormhole Attack.*
2. Parameter yang diujikan dengan menggunakan QoS sesuai dengan *standard* TIPHON adalah *throughput, end to end delay*, *jitter* dan *packet loss* ratio.
3. Penelitian ini termasuk dalam penelitian *Experimental*.
4. Penelitian ini hanya menggunakan *routing protocol Adhoc On-Demand Distance Vector* (AODV).
5. Hanya melakukan pengujian berdasarkan parameter QoS untuk mengevaluasi kestabilan kinerja dari teknologi jaringan VANET.

D. TUJUAN PENELITIAN

Berdasarkan rumusan masalah dan Batasan masalah diatas, maka tujuan dari penelitian ini adalah melakukan Evaluasi dari kinerja jaringan VANET ketika dalam pengaruh serangan *Malicious Node* Berdasarkan indeks dari parameter QoS. Dari evaluasi tersebut didapatkan hasil terkait kestabilan kinerja dari teknologi VANET dalam mengatasi serangan *Malicious Node*.

E. MANFAAT PENELITIAN

Dalam hasil penelitian yang telah dilakukan, diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan gambaran terkait simulasi teknologi jaringan *Adhoc* seperti VANET ketika dalam pengaruh serangan *Malicious Node*.
2. Mendapatkan informasi terkait perbandingan kondisi normal dan kondisi Ketika mendapat serangan *Malicious Node*.
3. Dapat memberikan hasil terkait tingkat kestabilan kinerja dari VANET dalam pengaruh serangan *Malicious Node.*
4. Dapat digunakan sebagai acuan oleh *network engineer* dalam pengimplementasian teknologi jaringan *Adhoc* sesuai dengan *environment* nya melalui evaluasi dari kinerja dari VANET ketika kondisi normal ataupun kondisi dalam serangan *black hole.*

F. KEASLIAN PENELITIAN

Penelitian yang berkaitan dengan Evaluasi Kinerja VANET Dengan Pengaruh Serangan *Malicious Node* Berdasarkan Parameter QoS yang dilakukan dengan menggunakan metode *experimental* sejauh pengamatan yang telah dilakukan dengan mempertimbangkan tinjauan pustaka, penelitian tersebut belum pernah dilakukan.

BAB V

PENUTUP

A. KESIMPULAN

Dari hasil evaluasi kinerja pada simulasi jaringan VANET yang dipengaruhi oleh serangan *Malicious Node* dapat diperoleh kesimpulan bahwa Serangan *Malicious Node* dengan jenis *Blackhole Attack* terbukti dapat menyebabkan peningkatan yang signifikan pada p*acket loss ratio* karena sifat dari *Blackhole Attack* dapat membuat node palsu hal tersebut yang dapat membuat *packet* data hilang. Dengan menggunakan scenario variasi penambahan node serangan tentunya juga memberikan pengaruh lebih pada kinerja simulasi jaringan VANET dengan menghasilkan nilai rata – rata QoS pada parameter *Packet Loss Ratio* yaitu 1 dengan indeks QoS Jelek. Sedangkan, Serangan *Malicious Node* dengan jenis *Wormhole Attack* juga terbukti menyebabkan nilai *end to end delay* yang tinggi. Hal ini disebabkan oleh cara *Wormhole Attack* bekerja dengan membuat *private channel* agar *packet* yang dikirimkan dari node sumber ke node tujuan tidak terjadi secara *direct* namun, melalui kolaborasi antar node *wormhole* terlebih dahulu. Tentunya dengan menggunakan skenario penambahan node serangan dengan sifat kolaborasi pada model serangan *wormhole* dapat menghasilkan nilai rata – rata QoS pada parameter *End to End Delay* yaitu 2,8 dengan indeks QoS sedang.

Serangan *Malicious Node* dengan jenis *Blackhole Attack* dan *Wormhole Attack* secara keseluruhan tentunya memiliki pengaruh besar terhadap kinerja jaringan VANET yang telah diukur dengan

menggunakan parameter QoS berdasarkan standard TIPHON. Hasil yang didapatkan dari setiap parameter yang diukur seperti *Throughput, End to End Delay, Jitter dan Packet Loss Ratio* menunjukan nilai rata – rata hasil akhir 2,6 dengan indeks QoS sedang pada pengaruh serangan *Blackhole*. Sedangkan. Rata – rata hasil akhir pada pengaruh serangan *Wormhole* 2,5 dengan indeks QoS sedang.

B. SARAN

Dalam proses Evaluasi Kinerja Vanet dengan Pengaruh Serangan *Malicious Node* penulis hanya menggunakan dua jenis serangan yaitu *Blackhole Attack* dan *Wormhole Attack* pemilihan model serangan tersebut merupakan sebuah pembuktian dengan metode *experiment* menggunakan SUMO dan *Network Simulator* 3 yang memiliki tujuan agar memperoleh data dari kedua karakteristik serangan tersebut karena memiliki *impact* besar yang berbeda pada setiap segment parameter QoS. Harapan pada peneliti selanjutnya dapat menambahkan hasil pembuktian dari ragam model serangan *Malicious Node* seperti *Flooding Attack, Jellyfish Attack* dan *Replay Attack* yang tentunya memiliki karakteristik serangan yang berbeda. Sehingga dengan adanya *experiment* terhadap model serangan *Malicious Node* lebih banyak dapat memperbanyak data terkait dampak dari model serangan *Malicious Node* dan memiliki tingkat keunikan yang beragam.

DAFTAR PUSTAKA

Agustin, A.T., Akbar, D.R., Risqiwati, D., 2019. Analisis kinerja jaringan VANET dengan model propagasi free space dan two ray ground pada routing AODV. Jurnal Repositor 1, 69–78. https://doi.org/10.22219/repositor.v1i2.10

Ahmed, Md.T., Rubi, A.A., Rahman, Md.S., Rahman, M., 2021. Red-AODV: A Prevention Model of Black Hole Attack for VANET Protocols and Identification of Malicious Nodes in VANET. IJCNA 8, 524–537. https://doi.org/10.22247/ijcna/2021/209985

Al-Shabi, M.A., 2020. Evaluation the Performance of Maodv and Aodv Protocols in Vanets Models. International Journal of Computer Science and Security 14, 12–24.

Aprianto Budiman, M. Ficky Duskarnaen, Hamidillah Ajie, 2020. Analisis Quality Of Service (QOS) Pada Jaringan Internet Smk Negeri 7 Jakarta. Jurnal Pendidikan Teknik Informatika dan Komputer 4, 32–36. https://doi.org/10.21009/pinter.4.2.6

Ar, A.H., Trisnawan, P.H., Siregar, R.A., 2019. Kinerja Protokol Routing Aodv Terhadap Serangan Wormhole Pada Jaringan Mobile Ad Hoc Network (Manet). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 3, 8746–8753.

Aziza, R.N., Siswipraptini, P.C., Cahyaningtyas, R., 2017. Protokol Routing Pada Vanet: Taksonomi dan Analisis Perbandingan Antara DSR, AODV, Dan TORA. JURNAL ILMIAH FIFO 9, 98–109. https://doi.org/10.22441/fifo.2017.v9i2.002

Bandung, Y., Z.R, A., Suhardi, 2006. Metoda Real Time Flow Measurement (RTFM) untuk Monitoring QoS di Jaringan NGN. Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia 3, 454–460.

Bilstrup, K., Uhlemann, E., Strom, E.G., Bilstrup, U., 2008. Evaluation of the IEEE 802.11p MAC Method for Vehicle-to-Vehicle Communication, in: 2008 IEEE 68th Vehicular Technology

Conference. Presented at the 2008 IEEE 68th Vehicular Technology Conference (VTC 2008-Fall), IEEE, Calgary, Canada, pp. 1–5. https://doi.org/10.1109/VETECF.2008.446

Eichler, S., 2007. Performance Evaluation of the IEEE 802.11p WAVE Communication Standard, in: 2007 IEEE 66th Vehicular Technology Conference. Presented at the 2007 IEEE 66th Vehicular Technology Conference, IEEE, Baltimore, MD, USA, pp. 2199–2203. https://doi.org/10.1109/VETECF.2007.461

Hadi, M.Z.S., Amran, H., R, N.P., 2011. Analisis Performansi Routing AODV pada Jaringan VANet. The Electronic Engineering Polytechnic Institute of Surabaya 2, 65–75.

Harry Saptarini, N.G.A.P., Hidayat, R.A., Ciptayani, P.I., 2019. AJARINCODE : Aplikasi Pembelajaran Bahasa Pemrograman Berbasis Web. Jurnal Sains Terapan Teknologi Informasi 10, 21–23. https://doi.org/10.46964/justti.v10i2.106

Istiqomah, T., Siregar, R.A., Kartikasari, D.P., 2018. Implementasi Serangan Black Hole pada Mobile Ad-Hoc Network dengan Pergerakan Dinamis Terstruktur menggunakan Protokol Dynamic Source Routing. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 2, 7262–7270.

Jenefer, F.A., Vydeki, D., 2013. Performance Analysis of Mobile Ad Hoc Network in the Presence of Wormhole Attack. International Journal of Advanced Computer Engineering and Communication Technology 2, 13–18.

Jiang, Y., Tham, C.-K., Ko, C.-C., 2000. Challenges and Approaches in Providing QoS Monitoring £. Network Operations and Management Symposium 2, 1–15.

Krajzewicz, D., Erdmann, J., Behrisch, M., Bieker, L., 2012. Recent Development and Applications of SUMO – Simulation of Urban MObility. International Journal on Advances in Systems and Measurements 5, 128–137.

Mukmin, C., Negara, E.S., 2019. Analisis Kinerja Redistribusi Routing Protokol Dinamik (Studi Kasus : RIP, EIGRP, IS-IS). Kumpulan jurnaL Ilmu Komputer 6, 284–292. https://doi.org/10.20527/klik.v6i3.262

Nutrihadi, F., 2016. Studi Kinerja Vanet Scenario Generators: Sumo Dan Vanetmobisim Untuk Implementasi Routing Protocol Aodv Menggunakan Network Simulator 2 (Ns-2). Jurnal Teknik Institut Teknologi Sepuluh November 5, 19–24. https://doi.org/10.12962/j23373539.v5i1.14307

Patel, B.B., Thaker, C.S., Jani, N.R., 2013. Analysis and Implementation of Malicious Node in AODV Routing Protocol. Computer Engineering and Intelligent Systems 4, 91–97.

Pattnaik, O., Pattanayak, B.K., 2017. Performance Analysis of MANET and VANET based on Throughput Parameter. International Journal of Applied Engineering Research 12, 7435–7441.

Pradana, P.D., Negara, R.M., Dewanta, F., 2017. Evaluasi Performansi Protokol Routing DSR Dan AODV Pada Simulasi Jaringan Vehicular Ad-Hoc Network VANET untuk Keselamatan Transportasi dengan Studi Kasus Mobil Perkotaan. e-Proceeding of Engineering 4, 1996–2003.

Rahardjo, I.A., Anggoro, R., Arunanto, F.X., 2017. Studi Kinerja 802.11P pada Protokol Ad Hoc On-Demand Distance Vector (AODV) di Lingkungan Vehicular Ad Hoc Network (VANET) Menggunakan Network Simulator 2 (NS-2). Jurnal Teknik ITS 6, 163–167. https://doi.org/10.12962/j23373539.v6i1.21994

Rathore, N.C., Verma, S., Tomar, R.S., Tomar, G.S., 2010. CMAC: A cluster based MAC protocol for VANETs, in: 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM). Presented at the 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM),

IEEE, Krackow, Poland, pp. 563–568. https://doi.org/10.1109/CISIM.2010.5643514

Ratnasih, R., Ajinegoro, R.M.N., Perdana, D., 2018a. Analisis Kinerja Protokol Routing Aomdv Pada Vanet Dengan Serangan Rushing. Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, dan Teknik Elektronika 6, 232–243. https://doi.org/10.26760/elkomika.v6i2.232

Ratnasih, R., Perdana, D., Wulandari, T., Pratama, M.I., 2018b. Performance Analysis of Reactive Routing Protocol on VANET with Wormhole Attack Schemeaper. INFOTEL 10, 138. https://doi.org/10.20895/infotel.v10i3.384

Rendro, D.B., Aji, W.N., Serang, J.R., Km, C., Drangong, T., 2020. Analisis Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP (Studi Kasus: SMK N 1 Kota Serang). Jurnal Pengembangan Riset dan Observasi Rekayasa Sistem Komputer 7, 108–115.

Rezkinanda, N., Anggoro, R., 2017. Pengembangan Protokol Multicast AODV dengan Memperhitungkan Jarak Euclidean Berdasarkan Posisi, Kecepatan dan Delay Transmisi pada VANET. JUTI: Jurnal Ilmiah Teknologi Informasi 15, 152–161. https://doi.org/10.12962/j24068535.v15i2.a611

Rosida Nur Aziza, R.N.A., 2019. Jaringan Ad-Hoc Vehicular (Vanet) : Tinjauan Tentang Arsitektur, Karakteristik, Aplikasi, Dan Protokol Medium Access Control (Mac). Jurnal Pengkajian dan Penerapan Teknik Informatika 9, 28–37. https://doi.org/10.33322/petir.v9i1.188

Sampetoding, E.A.M., Natalin, M., Manapa, E.S., Yoga, V., Ardhana, P., 2020. Studi Literatur: Cara Kerja Keamanan Internet dan Kerentanan dengan TCP/IP dan DNS. SainTech Inovation Journal 3, 66–73.

Sasongko, J., 2009. Network Simulator dan Network Animator menggunakan Cygnus Windows dalam Windows XP. Jurnal Teknologi Informasi DINAMIK 14, 60–69.

Tanaya, I.P.K.Y., Primananda, R., Nurwarsito, H., 2019. Analisis Dampak Serangan Black Hole terhadap Kinerja Protokol AODV dan DYMO pada MANET (Mobile Ad-Hoc Network). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer 3, 3131–3139.

Tassia, S.E., 2019. Implementasi Routing Terdistribusi pada Mobile AD HOC Networks (MANETS) untuk Sistem Komunikasi Taktis. Jurnal Teknologi Sistem Informasi dan Aplikasi 2, 1–8. https://doi.org/10.32493/jtsi.v2i1.2191

Utami, P.R., 2020. Analisis Perbandingan Quality Of Service Jaringan Internet Berbasis Wireless Pada Layanan Internet Service Provider (ISP) Indihome dan First Media. Jurnal Ilmiah Teknologi dan Rekayasa 25, 125–137. https://doi.org/10.35760/tr.2020.v25i2.2723

Wardhana, R., 2020. Pemodelan Multi-Layer Multihop Routing Protocol Pada Jaringan Wireless Sensor Network. Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer 15, 59–65. https://doi.org/10.30872/jim.v15i1.3315

Wulandari, R., 2016. Analisis Qos (Quality of Service) Pada Jaringan Internet (Studi Kasus : Upt Loka Uji Teknik Penambangan Jampang Kulon – Lipi). Jurnal Teknik Informatika dan Sistem Informasi 2, 162–172. https://doi.org/10.28932/jutisi.v2i2.454

Yusuf, M., Anggoro, R., 2017. Analisis perbandingan wireless network standard 802.11a dan 802.11p berdasarkan protokol dynamic source routing di lingkungan vehicular ad hoc networks. Jurnal Ilmiah Teknologi Sistem Informasi 3, 75–82. https://doi.org/10.26594/register.v3i2.1040