SIMULASI DAN ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV (*AD-HOC ON DEMAND DISTANCE VECTOR*) DAN OLSR (*OPTIMIZED LINK STATE ROUTING)* TERHADAP SERANGAN *WORMHOLE* PADA JARINGAN MANET

Muhammad Ramadhan[1], Ida Nurcahyani[2]
Jurusan Teknik Elektro, Universitas Islam Indonesia
Jl Kaliurang KM 14.5 Yogyakarta, Indonesia
[1]14524022@students.uii.ac.id
[2]ida.nurcahyani@uii.ac.id

***Abstrak*—MANET (*Mobile Ad Hoc Network*) merupakan jaringan yang teridiri atas kumpulan *node* yang bersifat dinamis, karena setiap *node* bergerak secara bebas. Selain itu, MANET juga dapat dibuat dengan mudah tanpa menggunakan infrastruktur jaringan yang tetap seperti *base station,* sehingga MANET menjadi rentan terkena serangan. Salah satu serangan yang mungkin terjadi adalah *wormhole attack*. Serangan *wormhole* merupakan serangan yang sangat jahat dapat merusak jaringan MANET efeknya dapat merubah topologi jaringan, dan menyebabkan salah dalam pengiriman informasi *routing*. Pemilihan *routing protocol* yang tepat dapat meminimalkan dampak dari serangan *wormhole*. Penelitian ini dibuat untuk membandingkan manakah yang lebih baik kinerjanya diantara *routing protocol* AODV dan OLSR dalam meminimalkan dampak dari serangan *wormhole*. Hasil dari penelitian ini menunjukan bahwa OLSR lebih baik kinerjanya dibandingkan dengan AODV dari beberapa nilai QoS seperti *throughput, delay*, dan *packet loss*.**

Kata Kunci : MANET,AODV,OLSR,*Wormhole Attack*

I. PENDAHULUAN

Perkembangan teknologi nirkabel yang sangatlah pesat dapat memenuhi kebutuhan masyarakat akan akses informasi yang *real time*, dapat diandalkan, dan fleksibel. Muncullah teknologi baru yang bisa disebut dengan MANET (*Mobile Ad hoc Network*). Kehadiran MANET sendiri merupakan sebuah jaringan nirkabel yang menghubungkan *node* satu ke *node* lainnya dan bersifat hanya sementara sehingga dapat dikatakan tidak tetap. *Routing* protokol merupakan pengaturan *node* untuk meneruskan paket dari *node* satu ke *node* lainnya, sehingga pada jaringan MANET dibutuhkan *routing protocol* yang tepat untuk membantu *node* mengirimkan paket data secara cepat dan efisien. Pada jaringan MANET ada beberapa macam *routing protocol* yaitu reaktif, proaktif, dan *hybrid*. Protokol yang akan dibahas adalah protokol *proaktive* dan protokol *reactive.* Protokol proaktif berfungsi *meng-update rute* secara berkala, sedangkan protokol reaktif berfungsi untuk mencari *rute* apabila ada permintaan. Ada beberapa protokol dari kelas reaktif dan proaktif, salah satunya adalah AODV dan OLSR. *Wormhole attack* merupakan serangan yang sangat jahat pada jaringan MANET dimana ada dua penyerang yang saling terhubung dengan kecepatan tinggi. Efek serangan *wormhole* adalah dapat merubah topologi jaringan, dan menyebabkan salah dalam pengiriman informasi *routing*.

II. TINJAUAN PUSTAKA

Perbandingan protokol routing AODV dan OLSR pada MANET yang ditulis oleh Wahyu Edi Saputra [4]. Membuktikan bahwa perbandingan kelas protokol *routing reactive* dan *proactive*, kinerja OLSR lebih baik dibandingkan dengan AODV dengan menggunakan skenario pengujian pertambahan *node* dan parameter yang dibandingkan yaitu *delay*, *throughput*, dan *packet delivery ratio*. Hasil OLSR lebih baik kinerjanya dibandingkan dengan AODV.

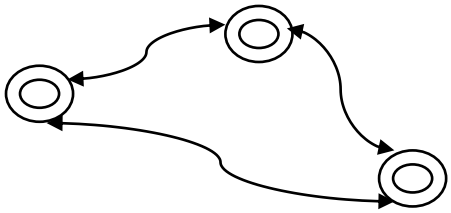
Perbandingan protokol *routing* DSR dan GRP pada MANET yang ditulis oleh Fitri Amalia [8]. Membuktikan bahwa perbandingan kelas protokol *routing proactive*, dan *reactive*, kinerja GRP lebih baik dibandingkan dengan DSR dengan menggunakan skenario pengujian pertambahan node dan parameter yang dibandingkan yaitu *throughput*, *delay*, *load*, *media access delay*, *data dropped*, dan *network load.* Hasil GRP lebih baik kinerjanya dibandingkan dengan DSR.

III. Dasar Teori

MANET (*Mobile Ad Hoc Network*) merupakan sebuah jaringan nirkabel yang dibentuk dari banyak *node* yang tidak memiliki *router* tetap [11]. *Node* berfungsi juga sebagai *router* yang dapat berkontribusi dalam memberikan informasi ke setiap *node* pada jaringan.

Oleh karena itu, *node* pada jaringan MANET dapat berfungsi maksimal harus diberikan *routing* agar

node dapat menjalankan proses pencarian *rute* dan data bisa efisien dan dinamis.

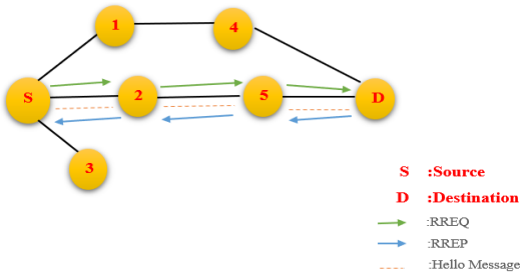


Gambar 1. Jaringan MANET.

Routing protocol merupakan pengaturan *node* untuk pencarian rute tersingkat untuk mengirimkan paket data menuju alamat yang dituju. Pada jaringan MANET ada 3 kelas *routing protocol* yaitu reaktif, proaktif, dan *hybrid*. Pada penelitian ini protokol *routing* yang digunakan hanya reaktif dan proaktif.

Protokol *reactive* merupakan *routing* yang berfungsi untuk membentuk rute jika suatu saat n*ode* meminta dibuatkan rute untuk pengiriman pesan.

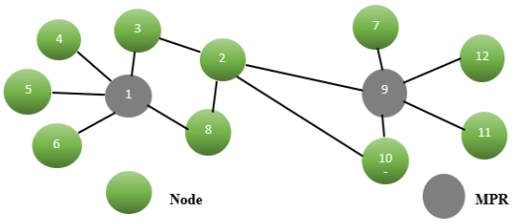
AODV (*Ad-Hoc on Demand Distance Vector)* merupakan sebagian protokol *routing* yang bersifat reaktif. Protokol AODV, *rute* dari *node* satu ke *node* lain akan dibuat jika *source node* menginginkan adanya permintaan pengiriman paket ke *node* tujuan yang dipilih. Protokol *routing* AODV akan melakukan *Route discovery* dengan menyebarkan *Route Request* (RREQ) ke semua *node* yang bertetanggan dengan *node* sumber. Setelah itu n*ode* tetangga mengirimkan RREQ ke *node* tetangga lagi hingga berakhir di *node* tujuan. *Node* tujuan akan membalas pesan RREQ dengan *Route Reply* (RREP) [13].



Gambar 2. Proses Pencarian *rute* AODV.

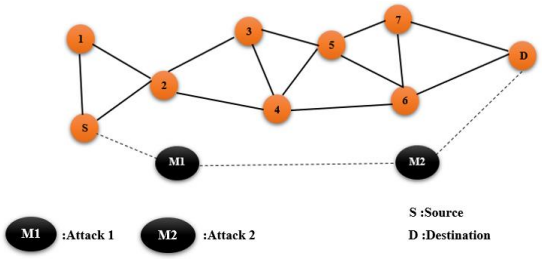
Routing protocol proaktif merupakan *routing* yang berfungsi *meng-update* informasi secara berkala.

OLSR (*Optimized Link State Routing)* merupakan protokol *routing* yang bersifat *proaktif.* Keunggulan OLSR dapat menemukan jalur di antara dua *node* yang berada di dalam jaringan dengan waktu yang sangat singkat, namun OLSR juga dapat menghabiskan sumber daya dalam proses pemilihan *node Multi Point Relay* (MPR) [14]. OLSR menggunakan 2 jenis pesan kontrol, yaitu pesan *hello* dan *Topology Control* (TC). Fungsi pesan *hello* adalah untuk menemukan informasi tentang kondisi *link* dan *node* tetangga. Pesan *hello* hanya mengirimkan sejauh 1 *hop*, sedangkan pesan TC dikirim secara *broadcast* ke seluruh jaringan. Pesan TC kegunaannya adalah menyebarkan informasi tentang *node* tetangga yang ditetapkan oleh MP. Pesan TC disebarkan secara periodik [4].



Gambar 3. *Packet Transmission Using* MPR.

Wormhole Attack adalah serangan yang sangat jahat pada jaringan MANET dimana ada dua penyerang yang saling terhubung dengan kecepatan tinggi [3]. Serangan ini dapat membuat kerusakan besar pada *ad-hoc network* yang telah terbentuk. Serangan *wormhole* dapat dilakukan dengan satu node, tetapi pada umumnya dilakukan untuk dua atau lebih penyerang. Efek serangan *wormhole* adalah dapat merubah topologi jaringan, dan menyebabkan salah dalam pengiriman informasi *routing*.



Gambar 4. *Wormhole Attack*.

Packet loss merupakan banyaknya jumlah paket yang terbuang saat proses pengiriman paket didalam suatu jaringan. Rumus untuk menghitung nilai *packet loss* adalah :

$$Packet\ loss = \left(\frac{\text{paket yang dikirim} - \text{paket yang diterima}}{paket\ \ yang\ dikirim}\right) X\ 100 \quad (3.1)$$

Throughput merupakan kecepatan dalam mentransfer data dikalkulasikan dalam *bit per second*. Rumus untuk menghitung nilai *throughput* adalah :

$$Throughput = \frac{\text{jumlah data yang dikirim}}{waktu\ pengiriman\ data} \quad (3.2)$$

Delay merupakan rata-rata waktu yang dibutuhkan untuk mengirimkan paket dari pengirim ke tujuan. Rumus untuk menghitung nilai *Delay* adalah :

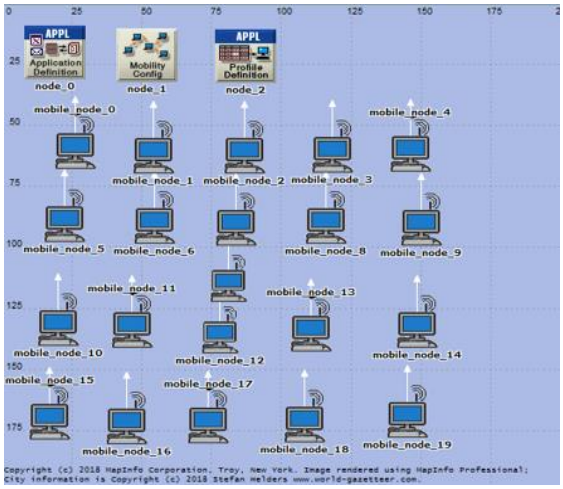
$$Delay = \frac{Total\ Delay}{Total\ packet\ received} \quad (3.3)$$

IV. Metode Penelitian

Konfigurasi jaringan MANET pada tugas akhir ini menggunakan *project* dengan OPNET MODELER 14.5. Perancangan simulasi menggunakan 2 skenario yaitu tanpa serangan dan menggunakan serangan *wormhole* dengan jenis *traffic* FTP *high load* dan luas 200 m * 200 m. Tugas akhir ini memiliki susunan yang berbeda pada setiap protokol *routing* AODV dan OLSR. Setelah perancangan dibuat langkah selanjutnya adalah menentukan analisa QoS yang meliputi parameter *throughput*, *delay* dan *packet loss*. Hasil perbandingan dari kedua protokol AODV dan OLSR simulasi akan dijadikan analisa yang nantinya akan ditarik sebuah kesimpulan yang menunjukan hasil kinerja dari simulasi yang telah dikerjakan.

Tabel 2. Spesifikasi Skenario Tanpa Serangan.

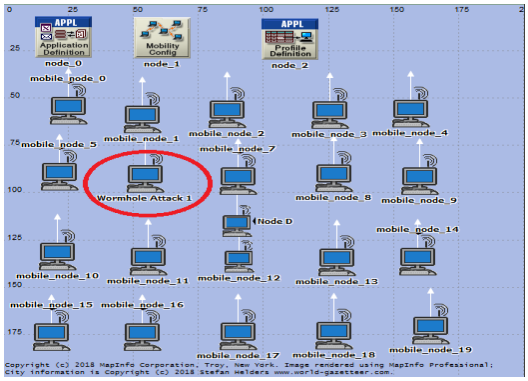
No	PARAMETER	NILAI
1.	*Technology* Jaringan	802.11b
2.	Luas Area	200X200 meter
3.	Jumlah *Node*	21 *Node*
4.	Jenis Pergerakan *Node*	*Random Waypoint*
5.	Data *Rate*	11 Mbps
6.	Aplikasi Layanan	FTP
7.	Jenis *Traffic* Aplikasi	*High load*



Gambar 5. Skenario Tanpa Serangan

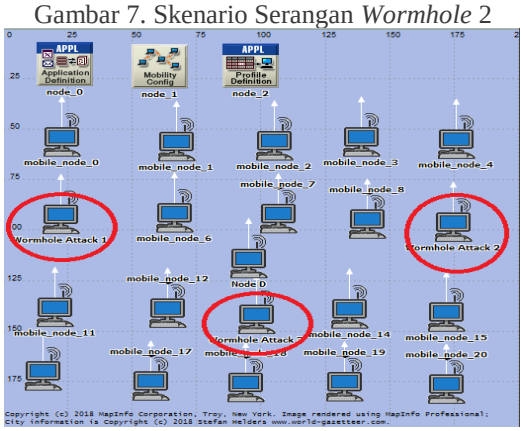
Tabel 3. Spesifikasi Serangan *Wormhole*

No	PARAMETER	NILAI
1.	*Technology* jaringan	802.11b
2.	Luas Area	200X200 meter
2.	Jumlah *Node*	18 *Node*
3.	Jenis Pergerakan *Node*	*Random Waypoint*
4.	Data *Rate*	11 Mbps
5.	Aplikasi Layanan	FTP
6.	Jenis *Traffic* Aplikasi	*High load*
7.	Jumlah *node Wormhole*	*1, 2, dan 3 Attacker node* + 1 *Node* D



Gambar 6. Skenario Serangan *Wormhole* 1

Gambar 7. Skenario Serangan *Wormhole* 2



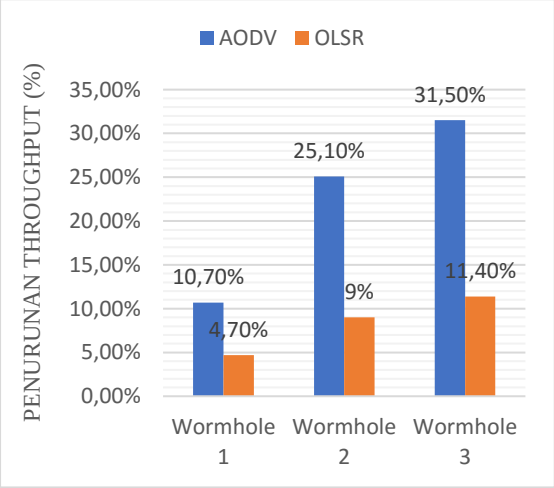
Gambar 8. Skenario Serangan *Wormhole* 3

Setelah hasil dari simulasi didapatkan kemudian dibandingkan dengan parameter QoS oleh pihak telekomunikasi internasional, sehingga jika kinerja yang dihasilkan belum sesuai standar maka perlu dilakukan perancangan kembali jaringannya, jika kinerja protokol routing sudah sesuai standar langkah selanjutnya menganalisis dan menarik sebuah kesimpulan.

V. HASIL DAN ANALISIS

Tabel 4. Nilai rata-rata Penurunan *Throughput*

Routing Protocol	*Wormhole* 1	*Wormhole* 2	*Wormhole* 3
AODV	10,7%	25,1%	31,5%
OLSR	4,7%	9%	11,4%



Gambar 9. Grafik Penurunan *Throughput*

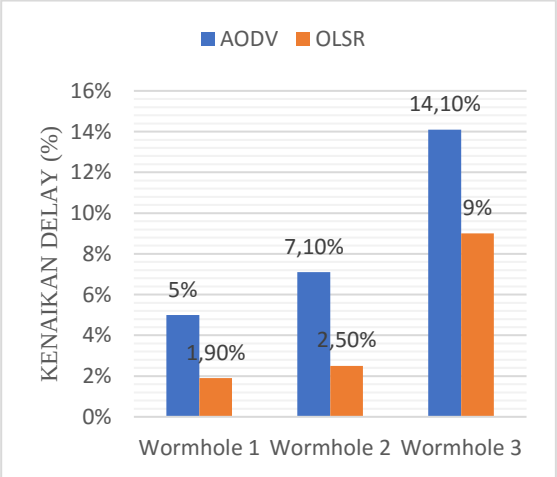
Dari hasil keluaran nilai *Throughput*, *routing protocol* AODV dan OLSR memiliki kemampuan dalam mentransfer paket data yang berbeda. Semakin besar nilai *throughput* maka semakin baik nilainya.

Pada protokol AODV percobaan tanpa serangan menghasilkan nilai sebesar 287,09 *kbit/s*. Sedangkan untuk protokol OLSR menghasilkan nilai sebesar 773,36 *kbit/s*. Nilai rata-rata *throughput* pada OLSR lebih tinggi dibandingkan dengan AODV, hal ini disebabkan dari beberapa faktor yaitu OLSR menggunakan pesan *hello* dan pesan *topology control* (TC) dalam penyebaran paket, sedangkan protokol AODV hanya menggunakan pesan *hello* saja [4].

Selanjutnya pada percobaan serangan *wormhole*, untuk protokol routing AODV penurunan nilai *throughput*nya sebesar 25,1%. Sedangkan protokol OLSR penurunan nilai *throughput*nya sebesar 9%. Dimana adanya serangan *wormhole* sangat berpengaruh bagi jaringan MANET yang membuat tidak stabil dan dapat mengakibatkan *throughput* turun. Efek serangan wormhole adalah dapat membuat perubahan topologi jaringan, dapat merubah pengiriman pesan yang normal, dan menyebabkan salah dalam pengiriman informasi *routing*.

Tabel 5. Nilai rata-rata Kenaikan *Delay*

Routing Protocol	*Wormhole* 1	*Wormhole* 2	*Wormhole* 3
AODV	5%	7,1%	14,1%
OLSR	1,9%	2,5%	9%



Gambar 10. Grafik Kenaikan *Delay*

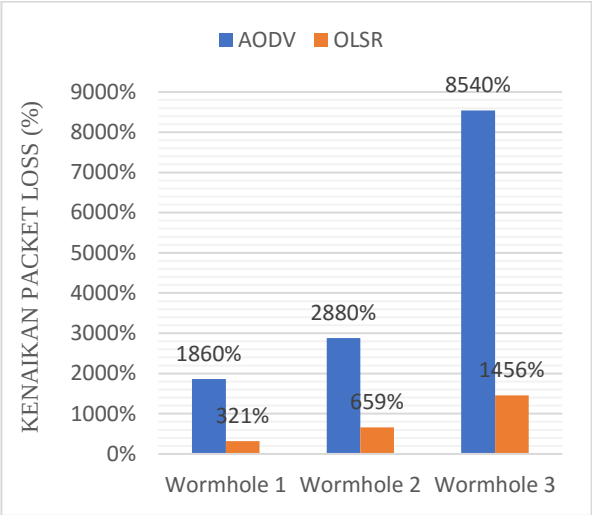
Dari hasil keluaran nilai *Delay*, *routing protocol* AODV dan OLSR memiliki kemampuan dalam mengirim paket data yang berbeda hingga sampai ke tujuan.

Protokol AODV percobaan tanpa serangan menghasilkan nilai *delay* sebesar 0.704 *ms*. Sedangkan protokol OLSR menghasilkan nilai *delay* sebesar 0,362 *ms*. Lebih besar protokol AODV dibandingkan dengan OLSR. Hal ini disebabkan dari beberapa faktor yaitu protokol AODV bekerja secara *on demand*, dimana pencarian rute sesuai dengan permintaan pengiriman paket secara *hop by hop* sehingga membutuhkan waktu yang ekstra untuk mencapai tujuan. Berbeda dengan protokol OLSR yang bekerja secara *link state*, dimana *rute* sudah tersedia sehingga tidak membutuhkan waktu yang lama untuk mencapai tujuan [4]. Meski begitu kedua protokol AODV dan OLSR dikategotikan sangat baik nilai *delay*nya yang terdapat pada standar TIPHON [15].

Selanjutnya pada percobaan serangan *wormhole*, untuk protokol routing AODV nilai *delay*nya mengalami peningkatan sebesar 7,1%. Sedangkan protokol OLSR nilai *delay*nya mengalami peningkatan sebesar 2,5%. Serangan *wormhole* dapat membuat jaringan tidak stabil yang dapat mempengaruhi nilai *delay*.

Tabel 6. Nilai rata-rata Kenaikan *Packet loss*

Routing Protocol	*Wormhole* 1	*Wormhole* 2	*Wormhole* 3
AODV	1860 %	2880 %	8540 %
OLSR	321 %	659 %	1456 %



Gambar 11. Grafik Kenaikan *Packet loss*

Dari hasil keluaran nilai *Packet loss*, *routing protocol* AODV dan OLSR saat terjadi serangan, paket banyak yang dibuang sehingga serangan *wormhole* dapat membuat jaringan tidak stabil yang dapat mempengaruhi nilai *packet loss.*

Dari hasil keluaran *packet loss*, protokol AODV percobaan tanpa serangan menghasilkan *packet loss* sebesar 0,05%. Sedangkan protokol OLSR menghasilkan *packet loss* sebesar 0,37%. Hal ini disebabkan dari masing-masing protokol memiliki kinerja yang berbeda. Protokol AODV tanpa serangan lebih baik dibandingkan dengan protokol OLSR. Tetapi masih dikategorikan sangat baik menurut standar TIPHON [15].

Selanjutnya pada serangan *wormhole* hasil keluaran yang dihasilkan pada *routing* OLSR mengalami kenaikan sebesar 659%. Sedangkan pada protokol AODV kenaikannya sebesar 2880%. Dimana saat terjadi serangan paket banyak yang dibuang, sehingga serangan *wormhole* dapat membuat jaringan tidak stabil yang dapat mempengaruhi nilai *packet loss*. OLSR lebih baik dibandingkan dengan AODV.

Tabel 7. Hasil Keseluruhan

Parameter	Tanpa Serangan		*Wormhole* 1		*Wormhole* 2		*Wormhole 3*	
	AODV	OLSR	AODV	OLSR	AODV	OLSR	AODV	OLSR
Throughput	287,09	773,36	10,7%	4,7%	25,1%	9%	31,5%	11,4%
Delay	0,704	0,362	5%	1,9%	7,1%	2,5%	14,1%	9%
Packet loss	0,05%	0,37%	1860%	321%	2880%	659%	8540%	1456%

VI. KESIMPULAN

Pada penelitian ini protokol OLSR lebih baik kinerjanya dibandingan dengan AODV dari beberapa aspek penelitian *throughput*, *delay*, dan *packet loss*. Dari hasil saat sebelum dan sesudah serangan *wormhole* protokol OLSR lebih baik dalam meminimalkan dampak dari serangan *wormhole* pada jaringan MANET. Dampak dari serangan *wormhole* dapat membuat kerusakan dalam jaringan MANET sehingga kinerja dari kedua protokol terhambat dalam pengiriman paket.

DAFTAR PUSTAKA

[1] R. M. N. Muhammad Irfan Denatama, Doan Perdana, “Analisis Perbandingan Kinerja Protokol Routing DSDV dan OLSR untuk Perubahan Kecepatan Mobilitas pada Standar IEEE 802.11ah." Univ Telkom,” 2016.

[2] D. Imawan, “Analisis Kinerja Pola-Pola Trafik pada Beberapa Protokol Routing dalam Jaringan Manet." Institut Teknologi Sepuluh Nopember,” pp. 1–9, 2009.

[3] M. Susanto, “Evaluasi Protokol untuk Mendeteksi Wormhole Attack dengan Menggunakan Global Positioning System (GPS)," ITB, 2013.

[4] W. E. Seputra, Sukiswo, and A. A. Zahra, “Perbandingan Kinerja Protokol AODV dengan OLSR pada MANET,” *J. Jur. Tek. Elektro, Fak. Tek. Univ. Diponegoro, Semarang, Indones.*, pp. 1–7, 2011.

[5] A. P. Rai, V. Srivastava, and R. Bhatia, “Wormhole Attack Detection in Mobile Ad Hoc Networks,” Institute of Technology and Management, Gwalior (M.P), India vol. 2, no. 2, pp. 174–179, 2012.

[6] P. M. and N. Chavhan, “A Survey on Security Issues to Detect Wormhole Attack

in Wirelss Sensor Network," G.H. Raisoni College od Engineering, Nagpur, India," vol. 2, no. 4, pp. 37–50, 2012.

[7] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs," *Procedia Comput. Sci.*, vol. 56, no. 1, pp. 384–390, 2015.

[8] A. Fitri Amillia, Marzuki, "Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) dan Geographic Routing Protocol (GRP) pada Mobile Ad Hoc Network (MANET)," UIN Sultan Syarif Kasim, Riau vol. 12, no. 1, pp. 9–15, 2014.

[9] D. V. Silaban, S. N. Hertiana, and A. Mulyana, "Simulasi dan Analisis Perbandingan Performansi Jaringan MANET (Mobile Ad Hoc Network) untuk Aplikasi Video Menggunakan Routing Protocol AODV (Ad Hoc On-Demand Distance Vector) dan OLSR (Optimized Link State Routing)," Universitas Telkom vol. 4, 2010.

[10] M. H. Y. H.Ghayvat, S.Pandya, S.V.Shah, "Advanced AODV Approach for Efficient Detection and Mitigation of Wormhole Attack in MANET," SEAT,Massey University, Palmerston North,NZ. 2014.

[11] K. Purwoko, "Analisis Kinerja Routing Protocol AODV dan OLSR Pada Jaringan Wireless Mesh," Univ Mercu Buana 2012.

[12] E. H. Harahap, "Analisis Performansi Protokol AODV (Ad Hoc On Demand Distance Vector) dan DSR (Dynamic Source Routing) terhadap Active Attack Pada MANET (Mobile Ad Hoc Network) Ditinjau dari QoS (Quality Of Service)," *Tugas Akhir Telkom Univ.*, vol. 34, no. 1, p. 9, 2014.

[13] R. F. Sari, A. Syarif, and B. Budiardjo, "Analisis Kinerja Protokol Routing Ad Hoc On-Demand Distance Vector (AODV) pada Jaringan Ad Hoc Hybrid Perbandingan Hasil Simulasi dengan NS-2 dan Implementasi pada Testbed dengan PDA," Universitas Indonesia vol. 12, no. 1, pp. 7–18, 2008.

[14] A. Pradesh, "A Quantitative Study and Comparison of AODV , OLSR and TORA Routing Protocols in MANET' Department of Information Technology, LITAM, India," *J. Comput. Sci.*, vol. 9, no. 1, pp. 364–369, 2012.

[15] S. A. Cedex, "Telecommunication and Internet Protocol Harmonization Over Network (TIPHON); Ganeral Aspects of Quality of Service (Qos)," *ETSI*, vol. 2.1.1, pp. 1-37, 1999.