

ABSTRAK

Vehicular Ad Hoc Network (VANETs) merupakan sebuah jaringan *mobile Ad Hoc* terbuka yang disusun oleh komunikasi timbal balik antara kendaraan dan *access point* tetap. Setiap *node* dalam satu jaringan memiliki pergerakan dan fitur yang bersifat *random* (berubah-ubah). *Vehicular Ad Hoc Network* (VANETs) adalah jaringan nirkabel yang dinamis dimana *node* bergerak secara acak tanpa infrastruktur apapun.

VANET adalah jaringan terbuka dan media komunikasi tanpa mekanisme keamanan. Jadi, ada banyak *node* serangan berbahaya pada VANETs. Salah satu permasalahan yang ada pada jaringan VANET adalah adanya serangan *blackhole*. Serangan *blackhole* adalah salah satu ancaman keamanan di mana lalu lintas tidak ditransmisikan ke *node* tujuan tetapi akan *redirect* ke *node* yang benar-benar tidak ada dalam jaringan untuk *drop* lalu lintas. Oleh karena itu, ketergantungan terhadap protokol *routing* yang adaptif dan efektif terhadap lingkungan jaringan menjadi hal yang diprioritaskan. Dalam tugas akhir ini untuk skema mobilitas menggunakan ONE *Simulator* dan analisis menggunakan *software* NS-2.

Dapat disimpulkan bahwa kinerja jaringan dengan menggunakan *routing protocol* AODV, OLSR, dan ZRP pada model mobilitas *freeway based on map* banyaknya jumlah *node*, besar *packet size*, dan perubahan kecepatan berpengaruh terhadap performansi QoS. Pada kondisi tanpa serangan *blackhole*, performansi *delay* OLSR adalah yang paling baik, nilai rata-rata *delay* untuk semua skenario adalah 4.3552 ms. Untuk performansi *throughput*, PDR, dan *total packet drop* AODV adalah yang paling tinggi. Rata-rata nilai *throughput* untuk semua skenario 24.398 kbps, PDR untuk semua skenario sebesar 98.19%, *Total packet drop* untuk semua skenario 43.552 *packet* atau 44 *packet*. Serangan *blackhole* menyebabkan penurunan performansi QoS. Penurunan *delay* AODV yang paling berbahaya, rata-rata penurunan performansi *delay* pada AODV untuk semua skenario adalah 96.825 ms. untuk *throughput* dan PDR OLSR dan ZRP penurunan performansi melebihi 50%. Dan penurunan kinerja *total packet drop* paling tinggi adalah ZRP. Rata-rata penurunan untuk semua skenario adalah 1249.1 *packet* atau 1250 *packet*. Pencegahan serangan *blackhole* menggunakan algoritma IDS untuk Performansi *delay* meningkat 72.682%, Performansi *throughput* terjadi kenaikan 2.14 kbps, performansi PDR meningkat 11.13%. Performansi *total packet drop* meningkat 274 *packet*.

Kata kunci : ONE *Simulator*, NS-2, VANET, *Blackhole*, AODV, OLSR, ZRP, IDS.