ABSTRAK

Vehicular Ad-hoc Network (VANET) merupakan jaringan *Ad-hoc* pada lingkungan kendaraan dengan node (*vehicle*) yang merupakan *router* yang bergerak dengan kecepatan tinggi. Hal ini menyebabkan VANET memiliki topologi yang berubah-ubah dengan waktu yang sangat singkat. Oleh karena itu, VANET rentan akan serangan dari luar dengan menyerang *routing protocol* yang digunakan. *Routing protocol* jika terserang oleh *malicious node* akan menyebabkan terganggunya fungsi dari *routing protocol* tersebut, dimana dapat menyebabkan paket data hilang saat pengiriman, bahkan dapat menyebabkan terjadinya kecelakaan pada komunikasi VANET. Salah satu jenis *routing protocol* pada VANET yang rentan akan serangan yaitu *reactive routing protocol.* Oleh karena itu, untuk mengatasi celah keamanan tersebut digunakanlah *Intrusion Detection System* sebagai pencegahan serangan. Tugas akhir ini menganalisis perbandingan performansi pada protokol *routing Ad-hoc On-Demand Distance Vector* (AODV) dengan skenario simulasi perubahan jumlah node sebanyak 30, 50, 70, dan 90 dan kecepatan node 70, 80, 90, 100 km/jam dengan tipe serangan *Denial of Service* yang digunakan *Blackhole* dan *Grayhole* tanpa dan dengan *Intrusion Detection System* disimulasikan dengan *Network Simulator* 2 (NS2) dengan pemodelan mobilitas node menggunakan *ONE Simulator*. Simulasi ditinjau dari parameter *Quality of Service* (QoS) : *packet delivery ratio*, *end to end delay*, dan *throughput.*

Berdasarkan hasil simulasi menunjukkan bahwa protokol *routing* AODV pada model mobilitas *freeway* dengan skenario perubahan jumlah node dan kecepatan node mempengaruhi performansi QoS yang dihasilkan. Pada skenario tanpa serangan dengan pengaruh perubahan jumlah node bahwa semakin banyak jumlah node dalam jaringan maka performansi *throughput, delay*, dan PDR akan naik. Sedangkan dalam skenario pengaruh perubahan kecepatan node, semakin cepat node bergerak dalam suatu jaringan maka performansi *throughput* dan PDR akan semakin turun, sedangkan *delay* akan naik. Pada skenario penambahan serangan *Blackhole* dan *Grayhole* menyebabkan penurunan performansi protokol routing AODV. Sehinga untuk menanggulangi serangan tersebut digunakan IDS sebagai pencegah serangan. Dengan adanya penambahan IDS pada sistem akan mengurangi dampak serangan dengan menaikkan performansi protokol *routing* dari keadaan terserang.

Kata kunci: VANET, reactive routing protocol, AODV, DSR, IDS, Blackhole, Greyhole, packet delivery ratio, end to end delay, dan throughput.