BAB I

PENDAHULUAN

1.1 Latar Belakang

VANET (*Vehicular Ad Hoc Network*) merupakan jaringan ad-hoc bergerak yang memungkinkan kendaraan melakukan komunikasi antara satu dengan lainnya tanpa ada infrastruktur yang tetap. Jaringan Ad-hoc mempunyai arsitektur yang terdesentralisasi dan algoritma pada jaringan ad-hoc bergantung pada keikutsertaan node yang kooperatif pada jaringan VANET. Sehingga pembuatan keputusan pun bersifat desentralisasi, hal ini dapat digunakan oleh penyerang untuk melakukan serangan. Serangan tersebut bertujuan untuk mengacaukan algoritma kooperatif yang berjalan [1]. Hal tersebut membuat jaringan VANET rentan terhadap serangan yang dapat menyebabkan masalah kecil bahkan besar pada jaringan. Selain itu, hal ini dapat menimbulkan ancaman keamanan jaringan yang dapat memperburuk fungsi atau layanan jaringan [2]. Diantara seluruh tantangan yang ada, keamanan jaringan pada VANET kurang diperhatikan selama ini. Paket data pada VANET mengandung informasi kritis dan perlu dipastikan bahwa paket ini tidak dimasuki atau dimodifikasi oleh penyerang. Masalah keamanan jaringan tidak serupa dengan komunikasi jaringan secara umum. Ukuran dari jaringan, mobilitas, relevansi geografis, dan hal lainnya membuat implementasi ini sulit dan berbeda dari keamanan jaringan lainnya [3].

Pada penelitian sebelumnya yang dilakukan oleh Nisha, dkk. [4] serangan *black hole* dapat menyebabkan *packet delivery fraction* menjadi 10% - 40%, tetapi ketika ada penambahan algoritma IDS, naik kembali menjadi 90% - 98%. Algoritma IDS ini mempunyai keuntungan yaitu tidak membutuhkan penambahan *overhead* dan sedikit modifikasi dari AODV. Penelitian yang dilakukan oleh *Hepikumar* [5] mengenai simulasi serangan *jellyfish* menggunakan *routing* protokol AODV pada jaringan MANET. Hasil dari simulasi tersebut didapat bahwa serangan *jellyfish* mempengaruhi kinerja jaringan dengan meningkatkan *end-to-end delay* dan *jitter.*

Berdasarkan penelitian terkait sebelumnya, dapat ditarik kesimpulan bahwa serangan *black hole* dan *jellyfish* dapat ditanggulangi dengan melakukan modifikasi

pada protokol *routing* yang digunakan yaitu AODV. Karena pada serangan tersebut dilakukan modifikasi pesan RREP yang mengganggu proses *routing.* Dimana pesan RREP dipalsukan sehingga seolah-olah *malicious node* memiliki *routing* tercepat dan terbaru.

Pada tugas akhir ini dilakukan penelitian keamanan jaringan pada VANET terhadap serangan DoS dengan algoritma tambahan pada protokol *routing* AODV. AODV merupakan salah satu protocol routing yang sederhana dan efisien dan akan berfungsi saat diperlukan (*on-demand*). Pada routing AODV digunakan pesan RREQ (*route request*), RREP (*route reply*) dan RRER (*route error*) untuk melakukan *route discovery* dan *route maintenance* [6].

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, maka dirumuskan beberapa rumusan masalah yang dibahas pada tugas akhir ini yaitu:

1. Bagaimanakah proses pembuatan model dan skenario kendaraan pada lingkungan VANET?
2. Bagaimanakah performansi jaringan VANET dengan protokol *routing* AODV sebelum dan setelah mendapat serangan *black hole* dan *jelly fish?*
3. Bagaimanakah perbandingan performansi AODV pada VANET dengan skenario penambahan jumlah *node* dan kecepatan *node* dalam kondisi normal, dengan serangan *black hole* dan *jelly fish* dan penambahan IDS sebagai algoritma proteksi terhadap parameter uji yaitu *packet delivery ratio*, *throughput* dan *end-to-end delay.*

1.3 Batasan Masalah

Untuk memperjelas pembahasan tugas akhir ini perlu dibuat pembatasan masalah. Pembatasan masalah yang dilakukan dalam tugas akhir ini yaitu:

1. Simulasi kendaraan sudah menggunakan standar VANET yaitu IEEE 802.11p.

2. Pergerakan kendaraan disimulasikan pada jalan *highway* dimana tidak memperhitungkan adanya lampu merah, kemacetan, dan *obstacle*.
3. Peta diambil dari *www.openstreetmap.org.* pada daerah yang sudah ditentukan yaitu Tol Jakarta – Cikampek KM 47 sampai dengan 54.
4. Mobilitas *node* pada simulasi menggunakan mobilitas *Map Based Movement*
5. *Routing protocol* yang akan dianalisis adalah AODV.
6. Pemodelan traffic yang digunakan adalah *Constant Bit Rate* (CBR) dan menggunakan *User Datagram Protocol* (UDP) sebagai *transport agent*.
7. Transmisi paket dalam simulasi hanya berasal dari satu *node* sumber.
8. Ukuran setiap paket 512 *bytes.*
9. *Node* penyerang hanya berasal dari satu *node.*
10. Aspek parameter uji yang diukur hanya parameter performansi QoS, yaitu *throughput*, *end-to-end delay* dan *packet delivery ratio.*
11. Tidak dibahas IP *Address* untuk setiap *node.*

1.4 Tujuan Penelitian

Tujuan dari pembuatan tugas akhir ini adalah:

1. Menyimulasikan jaringan VANET dengan *routing protocol* AODV.
2. Menganalisis dan membandingkan performansi jaringan VANET dengan *routing protocol* AODV sebelum dan setelah mendapat serangan *black hole* dan *jellyfish.*
3. Menganalisis kinerja *routing protocol* AODV pada keadaan normal, dalam serangan *black hole* dan *jelly fish* dan setelah ditambahkan algoritma IDS, dalam dua skenario berbeda berdasarkan parameter uji yang telah ditentukan.

1.5 Metodologi Penelitian

Metodologi penelitian pada tugas akhir ini adalah sebagai berikut:

1. Studi Literatur

   Pada tahap ini dilakukan proses pembelajaran teori dan pengumpulan berbagai literature berupa jurnal, buku, referensi dan sumber-sumber lainnya yang berkaitan dengan jaringan VANET, AODV, serangan black hole, serangan jelly fish dan algoritma IDS.

2. Identifikasi masalah dan perancangan skenario simulasi

   Pada tahap ini dilakukan identifikasi permasalahan berdasarkan hasil studi literatur. Pada tahap ini dilakukan peninjauan kembali masalah terhadap setiap metode, pemodelan simulasi yang akan dibangun dan hal-hal yang perlu dilakukan untuk mendukung proses simulasi agar berjalan sesuai dengan yang diharapkan.

3. Desain simulasi

   Pada tahap ini dilakukan perancangan model simulasi dengan menggunakan Network Simulator 2 sebagai perangkat lunak penunjang yang berjalan pada Linux Ubuntu 12.04 LTS. Kemudian, dirancang skenario untuk menghasilkan nilai-nilai parameter yang dapat dijadikan pembanding untuk melihat performansi AODV pada kondisi normal, dalam serangan DOS dan dengan penambahan algoritma IDS.

4. Pengujian dan analisis

   Pada tahap ini dilakukan proses pengujian simulasi pada Network Simulator 2 dan pengambilan data. Hasil dari simulasi berupa data dan grafik dari setiap skenario dan parameter. Selanjutnya hasil dari simulasi tersebut akan dibandingkan dengan kondisi normal, dalam serangan DOS dan dengan penambahan algoritma IDS yang kemudian menghasilkan kesimpulan dari penelitian ini.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini adalah sebagai berikut:

1. BAB I PENDAHULUAN

   Bab ini berisi uraian mengenai latar belakang pembuatan tugas akhir, perumusan masalah, batasan masalah, tujuan penelitian, hipotesis penelitian, metodologi penelitian, sistematika penulisan dan jadwal rencana penelitian.

2. BAB II LANDASAN TEORI

   Bab ini membahas seluruh konsep dasar yang berkaitan dengan penelitian diantaranya yaitu VANET, AODV, serangan *black hole,* serangan *jelly fish,* IDS dan paremeter uji yang digunakan seperti *packet delivery ratio*, *end-to-end delay,* dan *throughput.*

3. BAB III PEMODELAN SISTEM DAN SIMULASI

   Bab ini membahas tentang perancangan simulasi dan kebutuhan dari sistem. Hasilnya dituangkan ke dalam suatu sistem pemodelan secara terstuktur. Kemudian dilanjutkan ke tahap simulasi.

4. BAB IV ANALISIS HASIL SIMULASI

   Bab ini berisi penguji hasil simulasi yang kemudian dianalisis dengan menggunakan beberapa parameter uji untuk melihat performansi dari *routing protokol*.

5. BAB V KESIMPULAN DAN SARAN

   Bab ini berisi kesimpulan dari penulisan Tugas Akhir dan saran untuk pengembangan penelitian selanjutnya.

1.7 Jadwal Rencana Penelitian

Jadwal rencana pelaksanaan penelitian Tugas Akhir ini adalah sebagai berikut:

Tabel 1.1 Jadwal Rencana Penelitan Tugas Akhir

No	Kegiatan	Februari 2017				Maret 2017				April 2017				Mei 2017				Juni 2017				Juli 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Mengumpulkan segala sumber informasi terkait penelitian																								
2	Simulasi																								
3	Analisis data hasil simulasi																								
4	Perbaikan dan penyelesaian Buku																								
5	Sidang Tugas Akhir																								