1. PENDAHULUAN

1.1. Latar Belakang

Vehicular Ad Hoc Network (VANET) adalah jaringan wireless berbasis *ad hoc* yang merupakan kategori khusus dari *Mobile Ad Hoc Network* (MANET), ditandai dengan mobilitas tinggi [24]. Jaringan berbasis *ad hoc* terus mengalami perkembangan yang signifikan hingga saat ini karena kelebihannya yang dapat diimplementasikan tanpa adanya dukungan dari infrastruktur terpusat.

Terdapat dua tipe komunikasi pada VANET: *vehicle-to-vehicle* (V2V), yang di mana dalam hal transmisi data antara kendaraan tanpa menggunakan infrastruktur yang tetap, dan *vehicle-to-infrastructur* (V2I), yang dimana kendaraan mengirim dan menerima data ke/dari *Road Side Unit* (RSU) [2]. VANET membantu para pengendara untuk berkomunikasi dan berkoordinasi antara mereka sendiri untuk menghindari situasi yang berbahaya melalui komunikasi antara kendaraan (V2V) [21]**.**

VANET merupakan jaringan nirkabel, oleh karena itu VANET rentan terhadap suatu serangan. Berbagai serangan keamanan seperti *Denial of Service* (DoS), *Sybil attack, Blackhole attack,* dan serangan dengan tujuan tertentu, tidak hanya mengganggu privasi *driver* tetapi serangan tersebut dapat juga membahayakan keselamatan dari pengendara tersebut [25].

VANET membutuhkan suatu *routing* protokol untuk menentukan rute atau jalur yang diperlukan untuk sampai ke *node* tujuan. *Secure Ad-Hoc On-Demand Distance Vector* (SAODV) dan *Authenticated Routing for Ad-Hoc Network* (ARAN) adalah jenis protokol yang merupakan pengembangan dari protokol *Ad-Hoc On-Demand Distance Vector* (AODV) dan *Dynamic Source Routing* (DSR) [6][22]. Pada AODV dan DSR, semua node yang berada pada jaringan *ad-hoc* akan berpartisipasi dalam pembentukan rute dan meneruskan pesan. Karena kerentanan akan suatu serangan yang terjadi pada AODV maupun DSR, digunakanlah SAODV dan ARAN. Dampak serangan yang dilakukan akan berkurang dikarenakan SAODV menggunakan *hash* dan *digital signature* yang akan menjamin *authentication* dan *integrity* [8]. Sedangkan ARAN menggunakan mekanisme *public key cryptographic* yang menjamin *authentication* dan *integrity* [16]. Dengan begitu, komunikasi antar node dapat berlangsung lebih terjamin keamanannya karena antar node dapat percaya satu dengan lain ketika melakukan komunikasi.

Pada tugas akhir ini akan dianalisa performansi protokol *routing* SAODV dan ARAN dengan salah satu *node* telah terdampak serangan *blackhole* pada saat antar kendaraan saling berkomunikasi. Serangan tersebut ditempatkan pada posisi yang strategis pada topologi jaringan dan dengan tujuan untuk menggangu komunikasi antar kendaraan. Performansi akan dilihat berdasarkan beberapa parameter yang dapat membantu analisis terhadap fungsionalitas protokol *routing*, yaitu *packet delivery ratio* (PDR), *average end-to-end delay, packet loss ratio, routing overhead, convergence time,* dan *normalized routing load*. Hasil dari analisis dapat dijadikan pertimbangan dalam penggunaan protokol *routing* terbaik dalam kondisi tersebut.

1.2. Rumusan Masalah

Permasalahan yang diangkat dalam penyusunan tugas akhir ini yaitu:

1. Bagaimana mensimulasikan protokol *routing* SAODV dan ARAN pada jaringan VANET.
2. Bagaimana tipe serangan *Blackhole* menyerang pada mekanisme protokol *routing* SAODV dan ARAN dalam mengganggu performansi keduanya.
3. Bagaimana mensimulasikan trafik dan model mobilitas VANET pada lingkungan *highway*.
4. Bagaimana perbandingan performansi protokol *routing* SAODV dan ARAN dalam skenario sesudah terjadinya serangan seperti *Blackhole* pada pengaruh perubahan kecepatan node dan jumlah node berdasarkan parameter yang telah ditentukan agar mengetahui perfomansi dari kedua protokol *routing* yang memiliki fitur keamanan.

1.3. Tujuan Penulisan

Tujuan dari penulisan tugas akhir ini adalah menganalisis performansi protokol *routing Secure Ad-Hoc On-Demand Distance Vector* (SAODV) dan *Authenticated Routing for Ad-Hoc Network* (ARAN) yang memiliki fitur keamanan dalam mekanisme pencarian rutenya pada skenario setelah terjadinya serangan seperti *Blackhole* dengan pengaruh perubahan kecepatan node dan jumlah node berdasarkan parameter *packet delivery ratio* (PDR), *average end-to-end delay*, *packet loss ratio*, *routing overhead*, *convergence time,* dan *normalized routing load*. Serangan dilakukan untuk menguji apakah bentuk komunikasi antar kendaraan akan terganggu atau tidak terhadap serangan tersebut.

1.4. Hipotesis

1. Kedua *routing protocol* SAODV dan ARAN dapat menghindari serangan *blackhole* dikarenakan fitur keamanan yang kedua *routing protocol* tersebut miliki.
2. Performansi *routing* secara keseluruhan pada SAODV akan lebih baik dari pada ARAN, dikarenakan pada ARAN terdapat *Certificate Authority* (CA) yang dapat membuat *header packet* akan semakin besar.

1.5. Batasan Masalah

Sejumlah permasalahan yang dibahas pada tugas akhir ini dibatasi ruang lingkup pembahasannya, yaitu:

1. Jaringan nirkabel yang digunakan adalah *Vehicular Ad Hoc Network* (VANET)
2. Komunikasi yang dibangun adalah komunikasi antar kendaraan (V2V).
3. Protokol routing yang digunakan adalah SAODV dan ARAN.
4. Trafik yang digunakan adalah *Constant Bit Rate* (CBR) pada protokol UDP.
5. Simulasi mobilitas VANET dilakukan berdasarkan skenario lingkungan *Highway*.
6. Simulasi pengujian jaringan menggunakan NS-2.

7. Analisis kinerja jaringan didasarkan pada *packet delivery ratio* (PDR), *average end-to-end delay*, *packet loss ratio*, *routing overhead*, *convergence time,* dan *normalized routing load.*
8. Tipe serangan yang digunakan adalah *Blackhole*.
9. Tidak membahas bagaimana protokol Tesla bekerja.
10. Pada simulasi NS-2 menggunakan *random seed* (dengan maksud menggambarkan kenyataan tingkah laku trafik).

1.6. Sistematika Penulisan

Penyusunan tugas akhir ini dilaksanakan berdasarkan rencana berikut:

1. Tahap Studi Literatur

   Pada tahap ini dilakukan proses pembelajaran, pendalaman teori, dan konsep dari teknologi yang digunakan, serta pengumpulan informasi terkait yang diperoleh dari literatur, paper, jurnal, artikel-artikel untuk mendukung dalam penyusunan tugas akhir ini

2. Tahap Perancangan Model Sistem

   Pada tahap ini dilakukan analisis kebutuhan dan perancangan sistem yang digunakan dalam analisis.

3. Tahap Simulasi Sistem dan Pengumpulan Data

   Pada tahap ini dilakukan simulasi skenario VANET dengan menggunakan protokol SAODV dan ARAN dalam menghindari suatu kemacetan pada skenario sebelum dan sesudah serangan *Blackhole* terjadi dengan pengaruh perubahan kecepatan node dan jumlah node berdasarkan parameter *packet delivery ratio* (PDR), *average end-to-end delay*, *packet loss ratio*, *routing overhead*, *convergence time*, dan *normalized routing load*. Dilanjutkan dengan pengujian jaringan NS-2 berdasarkan skenario tersebut, hingga masuk ke tahap pengumpulan data untuk dianalisis dan diolah.

4. Tahap Mengolah dan Menganalisis

   Pada tahap ini dilakukan analisis terhadap beberapa data yang didapat pada tahap simulasi sesuai dengan parameter yang telah ditentukan, lalu ditarik suatu kesimpulan dari hasil data yang telah dianalisis tersebut mengenai performansi.

5. Kesimpulan dan Saran

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