BAB 2
TINJAUAN PUSTAKA

2.1 Studi Literatur

Salah satu penelitian pada VANET yang telah dilakukan oleh Elsa Mustikawati, Doan Perdana, dan Ridha Muldina Negara [10] menganalisis pengaruh dari serangan *blackhole* pada jaringan VANET. Penulis menambahkan IDS yang dapat meningkatkan kinerja parameter QoS seperti PDR, *throughput*, dan *delay end-to-end* dibanding dengan kondisi diserang. Hasil yang diperoleh nilai rata-rata PDR pada serangan *blackhole* berkurang, dan nilai *throughput* saat terkena serangan berkurang serta *delay* saat terkena serangan nilai juga berkurang.

Selanjutnya penelitian yang dilakukan oleh Badreddine Cherkaoui, Abderrahim Beni-Hssane, dan Mohammed Erritali [11] menyatakan bahwa penulis melakukan penelitian pada jaringan VANET dengan memanggil kendaraan *Ad-hoc* jaringan. Tujuan pembuatan jaringan komunikasi jenis ini adalah menangani lalu lintas dan memastikan mengemudi dengan aman dan menyampaikan beberapa informasi bermanfaat kepada pengguna. Untuk menjamin hal tersebut penulis harus mengamankan komunikasi dengan memprediksi serval masalah. Salah satu masalah tersebut adalah serangan *blackhole*. Penulis menggunakan metode berdasarkan *control* proses statistik. Pada penelitian ini simulasi menggunaka NS-2, untuk analisis menggunakan parameter *packet loss ratio* (PLR). Hasil yang diperoleh PLR di atas antara batas grafik maka komunikasi di anggap normal dan tidak ada serangan *blackhole*.

Dalam Penelitian yang dilakukan Salim Lachdhaf, Mohammed Mazouzi, Mohamed Abid [12] penulis menyatakan mobilitas *node* dari koneksi di jaringan telah membuat VANET rentan terhadap banyak ancaman. *Blackhole attack, gray hole attack, worm hole attack, dan sybil hole attack* adalah ancaman keamanan dimana *node* menghadirkan dirinya sedemikian rupa ke *node* lain yang memiliki jalur terpendek. Penulis melakukan pendekatan yang efisien untuk mendeteksi dan menghilangkan *blackhole attack* di kendaraan *ad-Hoc Networks* VANET. Solusi yang di usulkan diimplementasikan pada *routing protocol* AODV. *Routing protocol* AODV merupakan strategi dapat mendeteksi baik serangan *blackhole* tunggal maupun *cooperative blackhole* pada awal fase penemuan rute. Dalam mengevaluasi solusi menggunakan simulator NS-2. Analisis menggunakan *packet delivery ratio, dan delay end-to-end*. Hasil yang di peroleh dibandingkan dengan *routing protocol* AODV dimana pada *packet delivery ratio* menunjukkan 85% dan AODV berada 85% yang berarti nilai yang sama dimana tidak ada terdeteksi serangan. Pada *delay end-to-end* menunjukkan penundaan ujung ke ujung sama dengan AODV yaitu 40% menunjukkan adanya serangan *blackhole.*

Rand S. Majeed dan Mohammed A. Abdala [13] penulis melakukan beberapa mekanisme untuk meningkatkan keamanan *protocol routing* AODV terhadap serangan *blackhole*. Pada penelitian ini menggunakan simulator NS 2 yang meliputi skenario efek serangan, skenario dibawah efek *blackhole*, skenario dengan penerapan solusi yang sesuai. IDS-AODV, RAODV yang merupakan modifikasi dari algoritma AODV dan AntNet digunakan untuk menghilangkan efek *blackhole*. Analisis yang digunakan dalam simulasi menggunakan *routing protocol* AODV. Hasil yang diperoleh jumlah paket yang menurun, meningkat dengan meningkatkan jumlah *node* penyerang *blackhole*, IDS-AODV meningkatkan kinerja perutean AODV *protocol* di bawah pengaruh serangan *blackhole* yaitu mendeteksi dan mencegah simpul dari peretasan, dan algoritma AntNet memiliki perbandingan efisiensi paling kecil dengan IDS-AODV dalam kasus serangan *blackhole* karena berhubungan dengan jumlah *node* yang kecil dimana jumlah *node* meningkat efisiensi dalam pemecahannya masalah serangan akan berkurang.

Ratnasih, Riski Muktiarto Nugroho Ajinegoro dan Doan Perdana [14] penulis melakukan analisis kinerja *protocol routing* AOMDV pada VANET dengan serangan *Rushing*. Pada penelitian tersebut penulis menggunakan skenario perubahan kecepatan *node* dan variasi jumlah *node* serangan dengan menggunakan parameter *throughput, end to end delay* dan *packet delivery ratio*. Hasil yang diperoleh pada perubahan kecepatan, performansi QoS AOMDV memiliki nilai yang *fluktuatif* (lancar). Hal ini terjadi karena faktor jumlah *node* serangan, mobilitas, serta *traffic* yang ada pada jaringan AOMDV tersebut dan pada kondisi adanya serangan *rushing* performansi QoS AOMDV pada skenario perubahan jumlah *node* penyerang memiliki nilai yang *fluaktif* juga dimana nilai performansi QoS berada pada titik terendah ketika kondisi jaringan memiliki 3 *node* penyerang. Hal ini dipengaruhi oleh banyak faktor seperti posisi, mobilitas dan *traffic* yang ada pada jaringan tersebut.

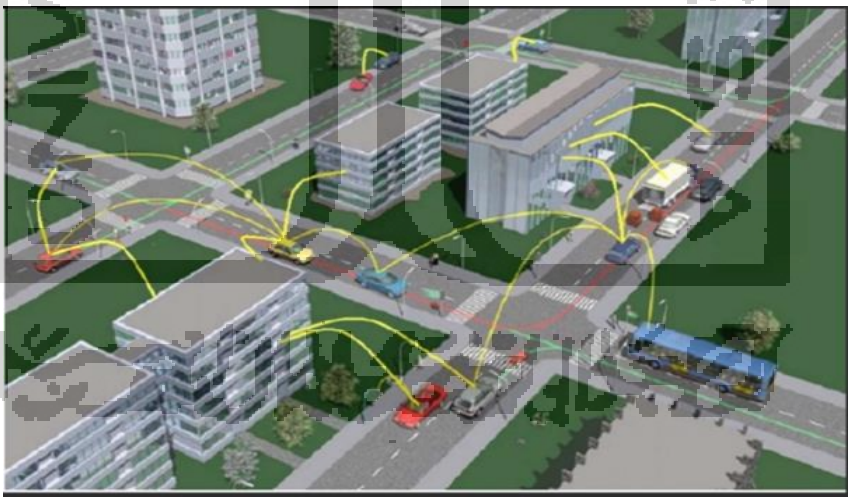
Pada studi literatur dijelaskan bahwa dari beberapa penelitian yang dilakukan, para penulis mengklaim serangan *blackhole* dapat mengurangi kinerja pada jaringan VANET. Penelitian jaringan VANET saat sesudah terkena serangan *blackhole* dengan menggunakan *routing protocol* AODV sudah pernah dilakukan dan di ambil kesimpulan bahwa kinerja jaringan VANET menurun saat sesudah terkena serangan *blackhole*. Namun pada penelitian tersebut belum ada melakukan perbandingan dampak serangan *blackhole* menggunakan skenario penambahan jumlah *node* dan perubahan kecepatan *node* dengan menggunakan *Network Simulator-3*. Oleh sebab itu, penulis mencoba untuk melakukan penelitian mengenai perbandingan saat sebelum dan setelah terkena serangan *blackhole* dengan menggunakan skenario yang berbeda seperti mengubah jumlah *node*, kecepatan *node* dengan parameter QoS seperti *throughput, delay* dan *packet delivery ratio*.

2.2 Tinjauan Teori

Jaringan *Ad Hoc* merupakan salah satu jenis jaringan *Wireless Local Area Network* (WLAN) terdiri dari sekumpulan *node* yang dapat berkomunikasi satu sama lain secara langsung tanpa melibatkan *node* perantara seperti *access point. Node* pada jaringan *Ad Hoc* bersifat dinamis dan dapat berubah-ubah. *Node-node* pada jaringan *Ad Hoc* bukan hanya berfungsi sebagai pengirim dan penerima informasi tetapi juga berfungsi sebagai pendukung jaringan seperti *router.* Dengan demikian diperlukan adanya *routing protocol* dalam jaringan *Ad Hoc* untuk menunjang proses kirim terima antar *node-node* nya.

2.2.1 *Vehicular Ad-hoc Network (VANET)*

VANET adalah jaringan *Ad-hoc* yang tidak memiliki pengetahuan tentang topologi jaringan yang berada di sekitar mereka. Setiap *node* hanya mengirimkan pengumuman kehadirannya dan menyadari keberadaan *node* tetangganya secara otomatis dengan menggunakan *broadcasting packets*, untuk menemukan *node* tetangga yang terdekat, dibutuhkan *routing protocol*. *Mode* komunikasi pada VANET dapat di klarifikasikan menjadi dua kategori yaitu, kendaraan ke kendaraan(V2V) dan kendaraan ke infrastruktur jalan(V2I) berada pada *node* atau kendaraan dengan perangkat keras di pinggir jalan atau disebut *Road Side Unit* (RSU) [15]. Pada Gambar 2.1 menunjukkan proses kinerja jaringan VANET.



Gambar 2.1 Jaringan VANET

Tujuan akhir VANET adalah untuk memberikan konsep konektivitas dimana-mana antara orang-orang yang mengemudi dijalan. VANET dibentuk oleh kendaraan jalan yang dilengkapi dengan beberapa sensor nirkabel, perangkat posisi dan peta. Pada VANET kedaraan diizinkan untuk berkomunikasi dengan unit sisi jalan. VANET mendapat cakupan karena menyediakan banyak aplikasi seperti keselamatan lalu lintas, akses internet, hiburan, dan pembayaran tol

otomatis. Karakteristik dari VANET ialah pesan tidak dapat dikirim secara langsung ke tujuan, pesan pasti akan di alihkan oleh *node* yang lain di antara *node* mereka. Pada VANET *node* tidak dapat bergerak ke semua arah karena jalan-jalan dan bangunan di jalan mereka [16].

2.2.2 *Routing protocol*

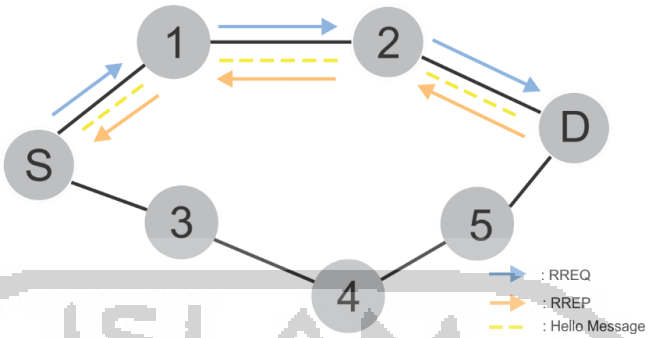
Routing protocol merupakan standarisasi yang melakukan kontrol bagaimana sebuah *node* dapat meneruskan paket diantara perangkat komputasi. *Routing protocol* layaknya sebuah router yang berkomunikasi dengan perangkat lain untuk menyebarkan informasi serta mengijinkan pemilihan rute diantara dua *node* dalam jaringan. Pada jaringan *Ad-hoc* setiap *node* akan memiliki kemampuan layaknya router yang meneruskan pesan antar *node* di sekitarnya maka di perlukan *routing protocol* untuk membantu tiap-tiap *node* [17]**.** Dalam jaringan *Ad-hoc* tidak ada topologi tetap karena *node*-nya bersifat *mobile* jadi kehilangan jalur sangat dimungkinkan. Oleh karena itu, *routing protocol* yang dinamis sangat di butuhkan karena dapat bekerja jika *node* sumber membutuhkan rute menuju *node* tujuan. *Routing protocol* reaktif meliputi *Ad-hoc On Demand Distance Vector* (AODV).

2.2.3 *Ad-hoc On Demand Vector (AODV)*

Ad Hoc On-Demand Distance Vector (AODV) merupakan salah satu jenis *routing protocol* yang termasuk kedalam kategori reaktif *routing protocol*. AODV merupakan *routing protocol* yang dirancang untuk jaringan bergerak *Ad-hoc* dan membuat jalur dengan menggunakan rute permintaan. Apabila *node* menginginkan rute ke tujuan yang belum memiliki rute maka ia akan mengirim paket permintaan rute ke seluruh jaringan. *Node* yang menerima paket ini memperbarui informasinya untuk *node* sumber dan mengatur penunjuk ke *node* sumber dalam tabel rute [8]**.**

Ketika ada permintaan dari *node* sumber AODV akan mulai bekerja untuk menemukan jalur yang terbaik menuju *node* tujuan. AODV akan melakukan penemuan rute untuk menyebarkan *route request* (RREQ) kepada semua *node* yang ada di sekitar *node* sumber. Untuk menghindari pesan yang sama maka, saat menyebarkan RREQ dikirim juga *ID Broadcast* dan nomor urutan. Penyebaran RREQ akan terus berlanjut sampai menuju *node* tujuan. Setelah RREQ sampai pada tujuan maka tugas *node* tujuan adalah memberikan balasan *route replay* (RREP). Jalur yang dipilih adalah jalur yang pendek dan biaya yang rendah dari jalur lainnya. Mekanisme AODV dapat dilihat pada Gambar 2.2 dalam proses pengiriman *routing* AODV akan mengirimkan pesan HALLO untuk menghindari perubahan topologi dan menyebabkan jalur yang menuju *node* tujuan terputus, maka suatu *node* akan mengirimkan pesan *route error* (RRER) menuju *node*

sumber. Setelah *node* sumber menerima RRER, maka *node* sumber melakukan penemuan rute kembali untuk mencari jalur lainnya menuju *node* tujuan [17].

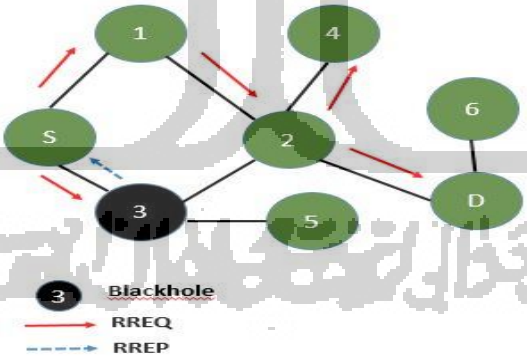


Gambar 2.2 Proses pencarian rute AODV

Keuntungan *routing protocol* AODV adalah banyak mengurangi jumlah rute pesan di jaringan dan karena *bandwidth* yang efisien sehingga mengkonsumsi lebih sedikit daya baterai. Sedangkan kekurangan *routing protocol* AODV adalah beberapa paket RREP dalam menanggapi paket RREQ tunggal dapat menyebabkan biaya *overhead control* besar dan apabila *node* tidak memiliki nomor urut tujuan terbaru dapat menyebabkan data yang masuk basi [18].

2.2.4 *Blackhole Attack*

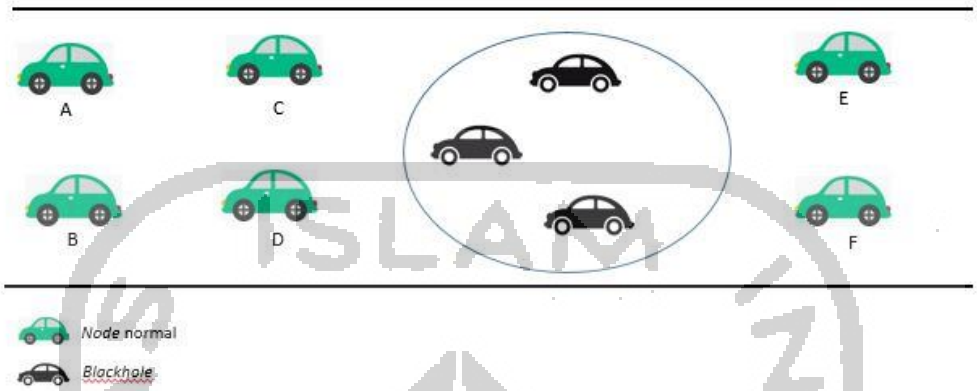
Pada serangan *blackhole*, *node* penyerang memperoleh rute yang di inginkan dengan menyatakan pada *node* sumber ia memiliki rute terpendek untuk mencapai *node* tujuan. Gambar 2.3 menunjukkan proses *node blackhole*.



Gambar 2.3 Mekanisme *node blackhole*

Node blackhole setelah menerima paket RREQ , *node* penyerang mengirimkan paket RREP palsu ke *node* sumber tanpa melihat informasi tentang *node* tujuan. *Node* penyerang memanipluasi RREP dengan memberikan nomor urutan palsu dengan menyatakan *node* penyerang memiliki rute terpendek. Pada nilai nomor urutan *node* tujuan yang tinggi dan paket RREP pertama kali di terima oleh *node* sumber. *Node* sumber akan menolak paket RREP yang dikirimkan oleh *node* lain meskipun memiliki rute yang benar. Sehingga rute antara *node* sumber

dan *node* penyerang akan terbentuk serta *node* sumber mengirimkan paket kepada *node* penyerang. *Node* penyerang kemudian akan membuang paket yang diterima. Menunjukkan mekanisme *node blackhole* melakukan *dropping* data dengan melakukan manipulasi pada *node* normal dengan menyatakan memiliki rute terpendek.



Gambar 2. 4 *Blackhole attack* pada kondisi nyata

Pada Gambar 2.4 menggambarkan serangan *blackhole*. *Blackhole* terbentuk oleh sejumlah *node* berbahaya, yang menolak untuk mengirimkan pesan yang diterima dari mobil asli, yaitu C dan untuk mobil E dan F. Dalam serangan *blackhole*, *node* berbahaya menggunakan *routing protocol* untuk menyatakan bahwa dirinya memiliki jalur terpendek ke *node* tujuan atau sebagai paket yang ingin menghadang. *Blackhole* menyatakan ketersediaan jalur yang tepat tanpa memeriksa tabel routing. Dengan cara ini *node* penyerang akan selalu sedia dalam membalas permintaan rute untuk menghadang paket data.

Gambar 2.4 menunjukkan bagaimana masalah *blackhole* muncul disini *node* C akan mengirim data ke *node* F dan memulai proses penemuan rute. Jadi jika *node blackhole* adalah *node* berbahaya maka *node* akan mengklaim bahwa ia memiliki rute aktif untuk tujuan tertentu segera setelah menerima paket RREQ. *Node* serangan kemudian akan mengirimkan respon ke *node* C sebelum *node* lain. Dengan cara ini *node* C akan berpikir bahwa ini adalah rute yang aktif dan rute aktif selesai. *Node* C akan mengabaikan semua balasan *node* lain, kemudian akan mulai pengiriman paket data ke *node blackhole* dengan cara ini semua paket data akan hilang di konsumsi.

2.2.5 *Quality of service (QoS)*

QoS didesain untuk membantu *user (client)* menjadi lebih produktif dengan memastikan *user* mendapatkan perfomansi yang handal dari aplikasi-aplikasi berbasis jaringan. Kemampuan QoS mengacu pada jaringan untuk menyediakan layanan yang lebih baik pada lalu lintas jaringan

tertentu melalui teknologi yang berbeda-beda. Tujuan QoS ialah untuk memenuhi kebutuhan layanan yang berbeda dengan menggunakan infrastruktur yang sama. Perfomansi QoS mengacu pada tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data didalam suatu komunikasi. Perfomansi adalah kumpulan dari beberapa parameter yaitu, *throughput, packet deliery ratio,* dan *delay*.

a. *Delay* adalah waktu yang digunakan untuk mengirimkan data dari pengirim menuju penerima dihitung dalam satuan waktu, *delay* dapat dipengaruhi oleh banyak hal seperti jarak, media yang digunakan, gangguan pada jaringan. Untuk menghitung jumlah *delay*, menggunakan rumus yang ditunjukkan pada persamaan (2.1) sebagai berikut :

$$Delay = \frac{delaySum}{rxPacket} \qquad (2.\ 1)$$

Keterangan :

DelaySum = Waktu paket tiba

RxPacket = Paket yang diterima

b. *Throughput* yaitu kecepatan transfer data efektif yang diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang di amati pada tujuan selama jarak waktu tertentu dibagi dengan durasi jarak waktu tersebut [19]. Jumlah bit yang berhasil diterima dalam selang waktu tertentu, semakin tinggi nilai *throughput*, maka perfomansi protokolnya semakin baik juga [14]. Untuk menghitung jumlah *throughput*, menggunakan rumus yang ditunjukkan pada persamaan (2.2) sebagai berikut :

$$Throughput = rxBytes\ /\ (Timelast\ rxPacket - Timefirst\ TxPacket) \qquad (2.\ 2)$$

Keterangan :

RxPacket = Paket yang diterima (*bytes*)

Timelast rxPacket = Waktu terakhir paket diterima

Timefirst TxPacket = Waktu pertama pengiriman paket

c. *Packet delivery ratio* adalah rasio antara jumlah data yang dikirimkan dengan data yang diterima. Untuk menghitung jumlah PDR, menggunakan rumus yang ditunjukkan pada persamaan (2.3) sebagai berikut :

$$Packet\ delivery\ ratio = \frac{Jumlah\ data\ yang\ diterima}{Jumlah\ data\ yang\ dikirim}\ \text{x}\ 100\% \qquad (2.\ 3)$$