BAB I

PENDAHULUAN

1.1 Latar Belakang

Sebuah jaringan *ad-hoc mobile* atau MANET adalah kumpulan perangkat mobile yang digunakan untuk berkomunikasi secara nirkabel tanpa otoritas jaringan terpusat atau terstruktur. Perangkat mobile dapat dengan mudah berkomunikasi dengan perangkat lain dengan meneruskan paket atas diri mereka sendiri. MANET adalah jaringan yang fleksibel pada perangkat mobile atau node dapat yang dengan mudah dapat bergabung dan meninggalkan jaringan. Konektivitas *mobile node* melalui saluran nirkabel menggunakan routing Hop demi Hop. Node dapat menjadi *router* untuk menemukan rute meneruskan paket ke node lain dalam jaringan. MANET memiliki beberapa karakteristik khusus seperti media yang terbuka, topologi yang dinamis, kurangnya pemantauan pusat dan manajemen, algoritma yang sederhana, tidak ada mekanisme pertahanan yang jelas. Dalam sistem jaringan yang terbuka MANET mudah terkena berbagai jenis serangan. Salah satunya adalah serangan *black hole*. Serangan *black hole* adalah sejenis serangan *Denial of Service(DoS)* pada MANET. Dalam serangan ini, node berbahaya menyatakan memiliki rute terbaik untuk node tujuan selama proses pencarian rute. Setiap kali menerima pesan RREQ, node bermasalah tersebut segera mengirimkan sebuah RREP palsu ke node sumber. Node sumber pertama menerima RREP palsu dari node berbahaya sebeum menerima RREP dari node lain. Namun, ketika node sumber mulai mengirim paket data ke tujuan dengan menggunakan rute ini, node berbahaya tidak meneruskan paket yang dikirimkan oleh node sumber melainkan menjatuhkannya.

Untuk menghindari dampak dari *black hole* pada MANET, beberapa pendekatan yang pernah diusulkan berdasarkan pada monitoring lalu lintas jaringan oleh setiap node untuk mendeteksi node yang bermasalah, dan kemudian mengambil tindakan yang tepat untuk menghindari efek negatif dari perilaku yang terjadi. Masalah utama yang timbul pada

saat terjadi serangan *black hole* adalah bagaimana untuk mendeteksi *black hole*, sambil menghindari sebanyak mungkin diagnosa yang salah, seperti RREP palsu.

Dalam simulasi ini penulis mengusulkan mekanisme *watchdog* yang mengintegrasikan teknik dari *Bayesian filtering*. Mekanisme *watchdog* ini berperan sebagai bagian perangkat lunak yang mengumpulkan dan menganalisa lalu lintas jaringan untuk mendeteksi suatu serangan. Dalam konteks ini, mekanisme *watchdog* bertujuan memantau aktivitas node dalam jaringan untuk mendeteksi perilaku yang merugikan jaringan.

1.2 Rumusan Masalah

Rumusan masalah adalah pertanyaan yang harus dicari jawabannya melalui pengumpulan dan analisis data. Adapun rumusan masalah yang akan dibahas dalam penelitian kali ini adalah.

a. Bagaimana membuat simulasi serangan *Black Hole* pada MANET menggunakan ns2 2.35?
b. Bagaimana kerja mekanisme *watchdog* pada proses deteksi serangan *Black Hole*?

1.3 Batasan Masalah

Pembatasan Masalah adalah usaha untuk menetapkan batasan dari masalah penelitian yang akan diteliti. Batasan masalah ini bertujuan untuk mengidentifikasi faktor mana saja yang termasuk dalam ruang lingkup masalah penelitian dan faktor mana saja yang tidak termasuk dalam ruang lingkup masalah penelitian. Batasan masalah pada penelitian ini dibatasi pada beberapa hal sebagai berikut.

a. Jumlah *node* yang digunakan 20 *node*.
b. Menggunakan NS2-3.5.
c. Menggunakan Ubuntu 12.04
d. Sistem keamanan yang digunakan adalah keamanan *watchdog*.

e. Karakteristik protokol routing yang digunakan pada penelitian ini adalah AODV.

1.4 Tujuan

Tujuan skripsi ini adalah melakukan simulasi serangan *black hole* pada MANET dan mengkaji performansinya. Beberapa tujuan yang ingin dicapai dari skripsi ini adalah sebagai berikut :

a. Mengkaji serangan *Black Hole* pada MANET.
b. Mengkaji keamanan jaringan menggunakan mekanisme keamanan *watchdog.*
c. Membandingan performansi pengiriman paket pada jaringan yang diserang oleh *Black Hole* dengan dan tanpa mekanisme *watchdog.*
d. Mengkaji simulasi sebuah serangan *Black Hole* dan mekanisme keamanan *Watchdog* menggunakan NS2 pada Ubuntu.

1.5 Manfaat

Manfaat penelitian merupakan dampak dari tercapainya tujuan dan terjawabnya rumusan masalah secara akurat. Manfaat yang didapat dari penelitian ini adalah sebagai berikut:

a. Bagi penulis mendapatkan manfaat dari pengetahuan yang diperoleh selama menempuh pendidikan di bangku perkuliahan khususnya mengenai jenis serangan *DOS* pada *MANET.*
b. Bagi mahasiswa mendapatkan manfaat mengenai pemahaman akan pengamanan terhadap serangan *Black Hole*.
c. Bagi pembaca mendapatkan manfaat berupa informasi mengenai mekanisme keamanan terhadap serangan *Black Hole* untuk menjadikannya sebagai referensi tambahan serta pengembangan lebih lanjut.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini mengenai MANET, AODV, serangan *Black Hole*, mekanisme keamanan *watchdog*.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang proses dan metode yang digunakan dalam peranrancangan jaringan, perancangan serangan *Black Hole* dan mekanisme keamanan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil dari serangkaian simulasi yang telah dibuat serta analisa hasil simulasi yang telah dibuat.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan kesimpulan dari penelitian yang telah dilakukan serta saran-saran yang berguna bagi pengembangan system.