1. Pendahuluan

1.1 Latar Belakang

Mobile Ad Hoc Network (MANET) yaitu sebuah jaringan *wireless* yang terdiri dari mobile-mobile node yang tidak memiliki infrastruktur. Jaringan ini merupakan salah satu mode jaringan *wireless ad hoc* akan tetapi node-node atau user pada jaringan ini bersifat mobile. Node bebas datang dan meninggalkan jaringan, node juga bebas bergerak atau diam pada posisinya MANET bisa terbentuk dari sekumpulan *node* yang menggunakan antarmuka nirkabel (*wireless interface*) mereka untuk melakukan komunikasi antara satu *node* dengan *node* yang lainnya. Untuk melakukan komunikasi tersebut maka node tersebut menggunakan protokol routing untuk memilih jalur terbaik untuk pengiriman pesan dari alternatif route yang dihasilkan dan diterima oleh node sumber [1]. Banyak algoritma protokol routing yang telah dikembangkan, antara lain AODV, DSDV, DSR, TORA

Protokol routing *Ad hoc on-demand distance vector* (AODV) banyak digunakan sebagai Protokol *routing* ini mengacu kepada protokol *routing* DSDV dengan penambahan fungsi broadcast untuk meminta *route*. Protokol ini mampu menangani perubahan topologi dan bebas dari looping *route*. Ketika suatu *route* dibutuhkan oleh suatu *node*, maka *node* tersebut akan mem-*broadcast* pesan *"route request"* ke semua *link*. Respon dari pesan tersebut kemudian dikirim balik oleh *node* penerima atau intermediate *node* yang berisi *route* baru untuk ke *node* tujuan [2].

Protokol routing AODV memiliki beberapa kelemahan, antara lain yaitu mudah disusupi penyerang. Tipe penyerangan yang banyak dan mungkin dilakukan pada AODV adalah Serangan Blackhole dan Wormhole. biasanya terjadi pada protokol routing reaktif. Karakteristik Blackhole attack dan wormhole attack adalah dropping paket, sehingga banyak paket yang hilang ketika node penerima menerima jumlah paket tertentu, tentu hal tersebut sangat mengganggu komunikasi dalam jaringan MANET [16]. Karena hal tersebut maka diperlukan suatu mekanisme pertahanan terhadap blackhole dan wormhole pada protokol routing AODV. Skema pertahanan yang dilakukan dengan memodifikasi mekanisme routing AODV dengan fungsi-fungsi tambahan untuk meng-*handling* terhadap serangan tersebut [15].

1.2 Perumusan Masalah

Berdasarkan latar belakang, maka dapat dirumuskan beberapa masalah yaitu:

a. Bagaimana *Wormhole Attack* dan *Blackhole Attack* menyerang pada mekanisme routing protocol pada MANET
b. Bagaimana Algoritma modifikasi AODV diterapkan untuk mengatasi serangan *Blackhole attack* dan *Wormhole attack* pada MANET
c. Menganalisis algoritma modifikasi AODV untuk mempertahankan performansi jaringan MANET dari serangan blackhole dan wormhole

1.3. Batasan Masalah

Dalam implementasi tugas akhir ini dibatasi oleh beberapa hal, sebagai berikut:

a. Protokol routing yang dimodifikasi adalah AODV
b. Serangan jaringan yang dipilih adalah *Blackhole* dan *Wormhole attack*, karena banyak menyerang pada jaringan MANET dengan protokol AODV
c. Serangan yang dilakukan hanya berasal dari satu node
d. Pengujian terfokus pada seberapa resisten modifikasi AODV yang dilakukan terhadap *blackhole attack* dan *wormhole attack*
e. Pengujian resistensi modifikasi AODV dilakukan dengan waktu simulasi yang bervariatif serta mengubah-ubah pergerakan node
f. Paremeter-parameter pengujian yang dianalisis adalah *average end to end delay* dan *packet loss*
g. Dalam pengujian Tugas Akhir ini hasil pengujian terfokus pada faktor *blackhole attack* dan *wormhole* attack, sedangkan penyebab menurunnya performansi karena antrian penuh / buffer penuh diabaikan, akan dijelaskan pada sub bab 4.3.4.1

1.4 Tujuan

Tujuan yang ingin dicapai dalam tugas akhir ini, yaitu :

a. Mensimulasikan penyerangan Wormhole dan Blackhole pada jaringan berbasis *mobile ad-hoc*
b. Mengimplementasikan algoritma modifikasi AODV untuk menghadapi Blackhole attack dan wormhole attack
c. Menganalisis kehandalan algoritma modifikasi AODV untuk mengatasi Blackhole attack dan Wormhole attack dengan parameter pengujian *packet loss*, *Average end to end delay*.
d. Menganalisis efektifitas algoritma modifikasi AODV dalam faktor waktu simulasi yang diperbesar (jika waktu diperbesar maka jumlah paket yang dikirim juga makin besar) dan kecepatan mobility node yang diperbesar.

1.5 Hipotesis

Algoritma modifikasi AODV mampu dalam mengatasi serangan *Blackhole* maupun *Wormhole* dalam jumlah *node* banyak maupun sedikit serta maksimum mobility yang kecil maupun besar dan memulihkan peformansi *routing* AODV (kembali seperti sebelum terserang *Attacking*)

1.6 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan adalah :

a. Studi Literatur, yaitu dengan mempelajari literatur-literatur yang ada sesuai dengan permasalahan meliputi konsep dari routing, protocol routing pada w*ireless*, Jenis-jenis serangan pada jaringan *wireless*, tentang NS-2 sebagai simulatornya
b. Analisa kebutuhan sistem dan perancangan skenario simulasi yaitu melakukan analisa terhadap model simulasi yang akan dibangun
c. Simulasi sistem dengan menggunakan NS-2 sebagai *network simulator* dengan modul *wireless*
d. Analisis hasil, yaitu menganalisi hasil pengujian dengan parameter pengujian *Packet loss, Average end to end delay*
e. Pembuatan laporan, melakukan pelaporan hasil pengerjaan Tugas Akhir berupa analisis sistem yang dibangun beserta dokumentasinya.