BAB III

METODE PENELITIAN

3.1 Rancangan Penelitian

Skipsi ini dilakukan sebuah simulasi keamanan yang telah diterapkan sebelumnya oleh tim Kanika Lakhani. Dengan menggunakan dua buah skenario yaitu saat mekanisme *watchdog* belum terpasang dan mekanisme *watchdog* sudah terpasang, dua buah skenario tersebut untuk membandingkan tingkat efektifitas parameter performansi yang terdiri dari *throughput, delay* dan *packet loss.* Berikut ini adalah alur rancangan penelitian yang dilakukan :

Gambar 3.1 Diagram Alur Rancangan Penelitian

3.1.1 Studi Literatur

Tahap ini melakukan persiapan kebutuhan sistem dan aplikasi yang akan digunakan serta pengumpulan konsep dan metode dari berbagai sumber seperti jurnal, makalah dan artikel ilmiah serta buku.

3.1.2 Spesifikasi Kebutuhan Penelitian

Perancangan penelitian berupa persiapan *hardware* dan *software* yang akan digunakan dalam penelitian. Antara lain :

a. Hardware

Hardware yang digunakan pada penelitian ini adalah sebuah laptop Lenovo Ideapad tipe U310 dengan kelengkapan spesifikasi seperti pada tabel 3.1 :

Tabel 3.1 Spesifikasi sistem laptop

Processor	Intel® Core ™ i3- 3217U
CPU	2.40 GHz
RAM	4 GB
HDD	500 GB

b. Software

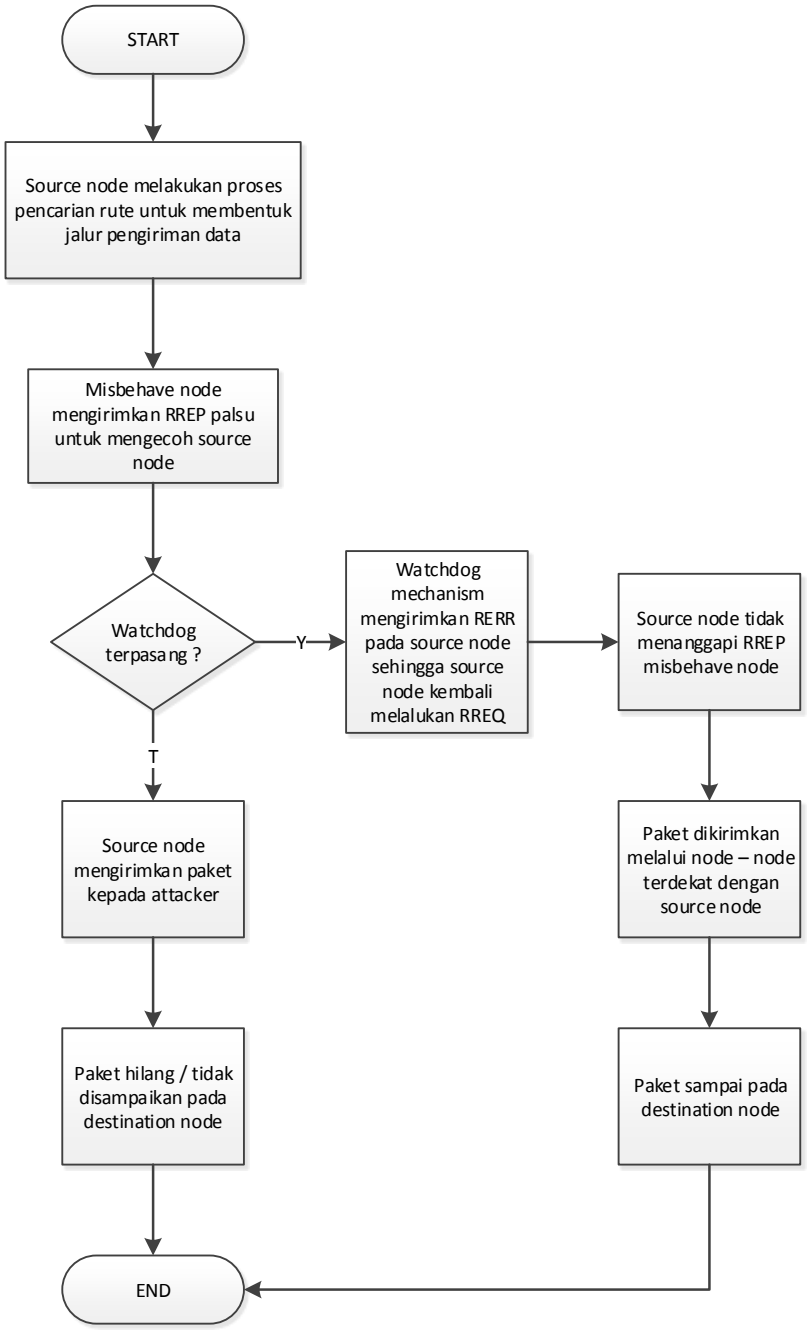
Berikut ini merupakan *software* atau perangkat lunak yang digunakan dalam penelitian :

a. Ubuntu 14.04 LTS
b. Virtualbox
c. Ubuntu 14.04
d. NS2 (*Network Simulator 2*)

3.2 Rancangan Sistem

3.2.1 Diagram Alur Sistem

Adapun penjelasan mengenai desain sistem kebutuhan dapat dilihat pada Gambar 3.2 di bawah ini, sebuah diagram alur penerapan rancangan program yang akan diujikan.



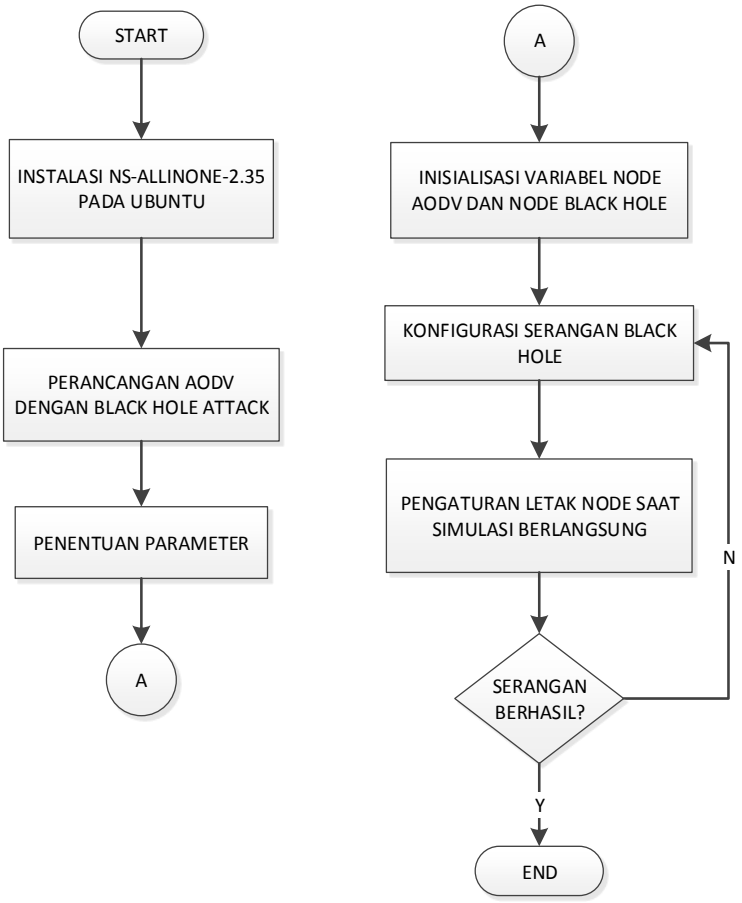
Gambar 3.2 Diagram alur rancangan program

Topologi yang digunakan merupakan jenis topologi dinamis dimana pergerakan *routing protocol* AODV merupakan pergerakan *routing* secara acak dan berubah – ubah

dalam beberapa waktu. Topologi yang diimplementasikan terbagi dua topologi ialah topologi tanpa mekanisme *Watchdog* seperti pada Gambar 2.9 dan topologi dengan mekanisme Watchdog seperti pada Gambar 2.10 di BAB 2.

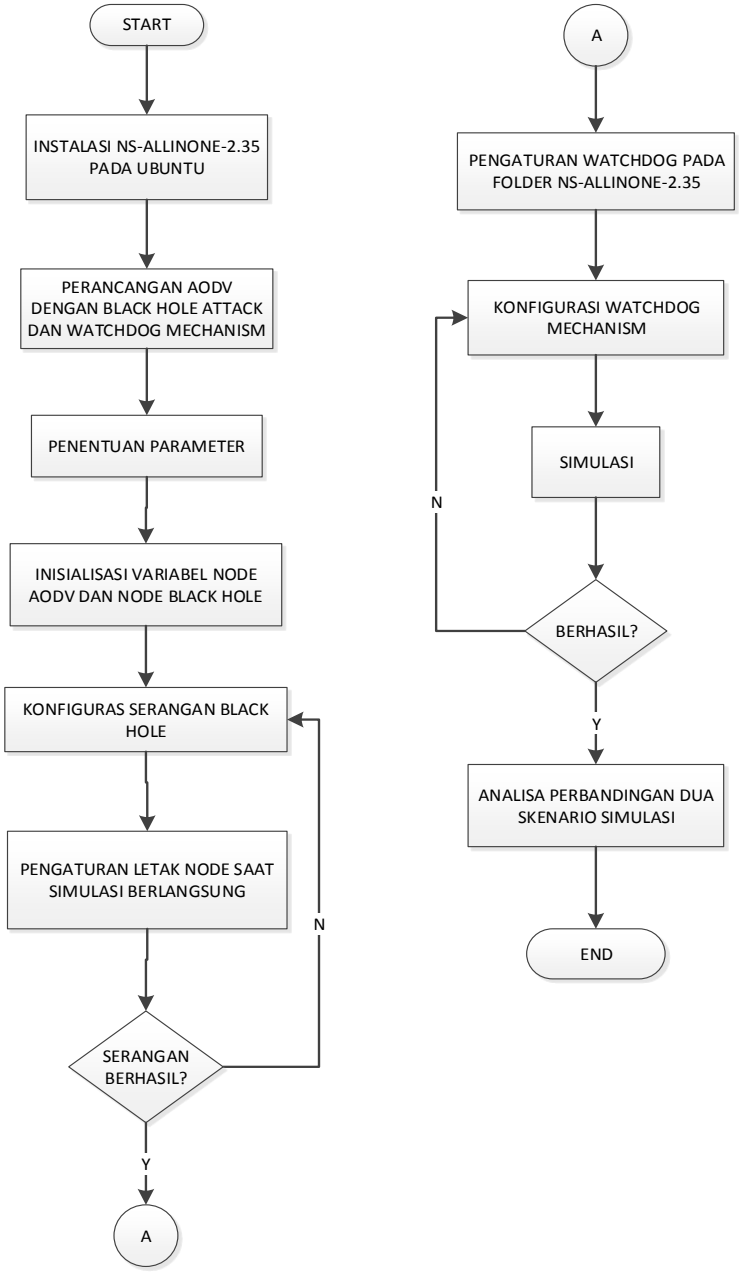
3.2.2 Instalasi Kebutuhan Simulasi

Pada bagian ini menjelaskan tentang desain instalasi program. Proses instalasi program berlangsung bertahap dan dilakukan secara terpisah dengan instalasi Serangan *black hole* (Gambar3.5) terlebih dahulu dilanjutkan dengan instalasi Mekanisme *watchdog* (Gambar 3.6).



Gambar 3.3 Diagram alur instalasi Serangan *black hole*

Proses pemasangan *Black Hole Attack* pada Gambar 3.3 menggunakan sebuah berkas *patch* yang dipasang dalam folder ns-allinone-2.35. Selanjutnya dilakukan konfigurasi untuk penyesuaian informasi agar dapat membaca pergerakan data yang telah ditentukan. Begitu juga dengan pemasangan Mekanisme *watchdog* pada Gambar 3.4, sebuah berkas *patch* dalam folder ns-allinone-2.35 setelah konfigurasi Serangan *black hole*.



Gambar 3.4 Diagram alur instalasi Mekanisme *watchdog*

3.3 Pembahasan dan Hasil

Uji coba simulasi dilakukan pada *network simulator 2.35* yang telah dipasang pada Ubuntu 12.04 di virtualbox. Penerapan dua skenario dijelaskan sebagaia berikut:

a. Skenario 1 – Serangan *Black Hole*

Parameter :

val(nn)	20	val(x)	800
Rp	AODV	val(y)	541
val(ifqlen)	50	time finish	20.0

Keterangan:

Val(nn) : jumlah node yang ditentukan pada simulasi

Rp : protokol routing

Val(x) dan val (y): luas bidang pada simulasi

Val(ifqlen) : variable maksimum pada file Tcl di simulasi

Time finish : waktu pengiriman paket

Prinsip Kerja :

Saat simulasi berlangsung, *node* sumber akan menyebarkan proses pencarian rute untuk memulai pengiriman paket. Sebuah *node* yang diidentifikasikan sebagai *Black Hole* akan melakukan RREP pada *node* sumber dan melakukan serangan dengan *drop packet*. Dari sini dapat dihitung jumlah paket yang hilang, waktu *delay* dan paket yang berhasil terkirim. Jika jumlah paket hilang lebih besar dibanding paket terkirim, maka serangan *Black Hole* berhasil dilakukan.

b. Skenario 2 – Mekanisme *watchdog*

Parameter :

val(nn)	20	val(x)	800
Rp	AODV	val(y)	541
val(ifqlen)	50	time finish	20.0

Keterangan:

Val(nn) : jumlah node yang ditentukan pada simulasi

Rp : protokol routing

Val(x) dan val (y): luas bidang pada simulasi

Val(ifqlen) : variable maksimum pada file Tcl di simulasi

Time finish : waktu pengiriman paket

Prinsip Kerja :

Mekanisme *watchdog* yang telah terpasang pada NS2 akan melakukan kerjanya ketika serangan *Black Hole* terjadi. Hal ini dapat dilihat dari pergerakan proses pengiriman paket yang langsung mencari rute baru tanpa melewati *node* berbahaya. Saat jumlah paket yang terkirim akan lebih besar dari jumlah paket yang hilang. Ini dikarenakan *watchdog* telah menemukan keberadaan *node* berbahaya dan mengabarkan pada *node* lain untuk membuat rute baru tanpa melewati *node* berbahaya.

Berdasarkan pengawasan Bayesian penelitian ini menerapkan sebuah pengawas Bayesian yang kolaboratif berdasarkan pada mekanisme pesan-lewat di setiap pengawas individu yang memungkinkan reputasi yang baik. Setiap simpul berjalan dan berkolaborasi dengan pengawas untuk mengumpulkan semua informasi reputasi agar mendapatkan nilai-nilai α dan β 'untuk setiap node tetangga. Hal yang mendasari pendekatan ini adalah bahwa jika pengawas Bayesian bekerja dengan baik untuk mendeteksi *Black*

Hole, sekelompok gabungan pengawas Bayesian akan mampu melakukan deteksi lebih cepat dan lebih akurat.

Demikian pula untuk pengawas bayesian, pengawas Bayesian kolaboratif hanya mendengar jaringan untuk mengumpulkan informasi tentang paket yang dikirim dan diterima. Selain itu, memperoleh α dan β nilai untuk seluruh lingkungan nya. Nilai-nilai ini sama dengan nilai yang diperoleh oleh pengawas bayesian dengan pengamatan yang sama, hal ini disebut "informasi tangan pertama" atau "reputasi langsung". Secara berkala, pengawas berbagi informasi dengan node terdekat, dan disebut "informasi tangan kedua" atau "reputasi tidak langsung". Dalam implementasi ini, reputasi tidak langsung dimodulasi menggunakan parameter δ. Setiap kali diperlukan, setiap simpul menjalankan penghitungan pengawas bayesian kolaboratif.

Penggunaan kelas layanan atau tipe komunikasi berupa CBR (*Constant Bit Rate*) yang bekerja sebagaimana layaknya, atau mengemulasikan sebuah saluran fisik, tidak membutuhkan pengecekan *error* atau kontrol aliran data dan tanpa gangguan *jitter* (variasi *delay* antar paket yang terjadi pada jaringan). Jika didapat perbedaan seperti yang diharapkan maka penelitian simulasi skripsi ini dinyatakan berhasil sesuai dengan konsep yang diterapkan sebelumnya.

3.3.1 Performansi

Parameter yang digunakan untuk perbandingan adalah sebagai berikut :

a. Throughput

Throughput adalah laju data aktual per satuan waktu, bisa disebut juga sebagai *bandwith* dalam kondisi yang sebenarnya. Namun, *bandwith* lebih bersifat tetap sementara *throuhput* sifatnya dinamis tergantung proses yang sedang terjadi dengan satuan yang digunakan adalah Bps (*Bits per second*). Rumus menghitung *throughput* yaitu :

$$Throughput = received\_Data * 8/DataTransmissionPeriod \quad (1)$$

b. Delay

Delay adalah jeda waktu antara paket pertama dikirim dengan paket yang diterima oleh tujuan. Rumus *delay* yaitu :

$$Delay = \left(\frac{waktu\ terima\ paket - waktu\ kirim\ paket}{paket\ yang\ diterima}\right) \qquad (2)$$

c. Packet Loss

Packet Loss adalah banyaknya paket yang hilang selama proses pengiriman paket berlangsung. Rumus *packet loss* yaitu :

$$Packet\ Loss = \frac{Packet\ Drop}{Packet\ Sent} \times 100\% \qquad (3)$$

3.3.2 Analisa Simulasi

Pada bagian ini menjelaskan bagaimana dua simulasi akan dilakukan, yaitu :

a. Serangan *Black Hole*

Jumlah node : 20 *node*

Luas area : 800 x 541

Tujuan : Penerapan serangan *Black Hole* pada AODV, tingkat keberhasilan serangan dilihat dari parameter yang telah disebutkan di atas.

b. Mekanisme *Watchdog*

Jumlah node : 20 *node*

Luas area : 800 x 541

Tujuan : Penerapan mekanisme keamanan *watchdog* yang mampu menangkap keberadaan *node* berbahaya. Sehingga dapat mencegah hilangnya paket yang dikirim pada saat proses pengiriman berlangsung.

Dari kedua simulasi di atas akan ditemukan nilai perbandingan sesuai dengan parameter yang dianalisa untuk penentuan keberhasilan mekanisme keamanan *watchdog* terhadap serangan *black hole* pada protokol *routing* AODV dalam MANET.