BAB I Pendahuluan

1.1 Latar Belakang

Seiring dengan perkembangan zaman di era digital kebutuhan manusia untuk berkomunikasi semakin meningkat. Seperti kebanyakan orang saat ini perangkat yang digunakan adalah perangkat *handphone* yang digunakan untuk berkomunikasi via suara, data dan sebagainya. Teknologi komunikasi yang digunakan saat ini lebih di dominasi dengan penggunaan data internet baik dalam layanan *Voice Over, Video Stream*, dan lain lain Seperti yang sudah ketahui layanan-layanan semacam itu menggunakan jaringan UDP sebagai *background* jaringanya.

Teknologi UDP sendiri bukan teknologi yang amat baru. Teknologi ini sudah banyak digunakan dan di aplikasikan dalam kehidupan sehari-hari. Teknologi ini juga sudah didukung dengan berbagai macam *routing* protokol yang mendukung berjalan dengan baiknya teknologi ini, seperti *AODV, AOMDV,* dll. *Routing* protokol menjadi *support system* yang sangat berpengaruh dalam berjalananya jaringan ini oleh karena itu pemilihan *routing* menjadi faktor penting dalam sebuah jaringan. Namun dengan semakin banyak yang menggunakan UDP sebagai *background* jaringan, semakin banyak pula rentan jaringan ini mendapatkan serangan.

Kejahatan atau serangan yang mungkin dan sering terjadi pada layanan *mobile* berbasis UDP ini adalah *Distributed Denial of Service* (DDoS). Serangan ini akan menbanjiri jaringan yang ada dengan data, dan bila terus berlangsung lama dengan jumlah *flooder* semakin banyak dan terdistribusi maka performansi jaringan semakin lama akan semakin menurun dan tidak menutup kemungkinan hinggal menonaktifkan jaringan tersebut.

Selain serang *DDoS* ada juga serangan yang tidak kalah berbahaya yaitu serangan *rushing attack*, serangan ini adalah serangan yang mengirimkan transmisi yang lebih besar berupa RREQ untuk mendapat prioritas jalur. Oleh karena itu pada penelitian tugas akhir ini akan membuktikan serangan manakah yang lebih berbahaya pada jaringan UDP. Kedua serangan ini akan diimplementasikan pada NS2 sebagai simulator dengan *wireless comunication* dan masing-masing skenario memiliki 30 *node*.

1.2 Perumusan Masalah

Adapun perumusan masalah pada Tugas Akhir ini sebagai berikut:

1. Bagaimana mengimpelementasikan *DDoS* pada jaringan UDP?

2. Bagaimana mengimplementasikan *Rushing Attack* pada jaringan UDP?
3. Bagaimana hasil pembuktian serangan *DDoS* atau *Rushing Attack* yang lebih berbahaya ?

1.3 Tujuan

Tujuan yang akan dicapai dari pengerjaan Tugas akhir ini adalah:

1. Melakukan *DDoS* pada jaringan UDP dengan *AODV routing.*
2. Melakukan *Rushing Attack* pada jaringan UDP dengan *AODV routing.*
3. Membuktikan serangan *DDoS* atau *Rushing Attack* yang lebih berbahaya.

1.4 Batasan Masalah

Adapun batasan masalah selama pengerjaan Tugas Akhir ini sebagai berikut :

1. Protokol yang digunakan merupakan jaringan UDP.
2. Metode Serangan *Distributed Denial of Service* (DDoS).
3. Metode Serangan *Rushing Attack*.
4. *Routing* yg digunakan AODV.
5. Simulator yang digunakan untuk simulasi adalah NS2.
6. Jumlah *node* pengujian terdapat 30 *node*.
7. Penyerang terus bertambah dari 1 hingga 10 *attacker*
8. Besar paket data adalah 1024.
9. Waktu simulasi 100 detik.
10. Parameter yang di gunakan send packet , receive packet , average throughput , packet delivery ratio.
11. Node yang digunakan tidak bergerak.
12. Menggunakan AWK untuk mendapatkan hasil pengujian.