ABSTRAK

Teknologi internet pada saat ini berkembang dengan pesat, begitu pula ancaman serangan kepada pengguna internet yang semakin banyak. Salah satu ancaman yang sedang marak terjadi *yaitu Distributed Denial of Service* (DDoS), DDoS merupakan jenis *Anomaly Traffic* yang menyebabkan pengguna tidak dapat mengakses internet sebagaimana mestinya.

Dalam mendeteksi serangan anomaly, terdapat dua metode yaitu metode *signature* dan metode *anomaly based*. Pada penelitian ini metode yang digunakan adalah metode *anomaly based* yang tidak menggunakan basis data untuk mendeteksi serangan anomali, metode ini bekerja dengan pengenalan pola sebagai mana karakteristik anomali yang dapat berubah-ubah polanya sehingga memungkinkan mendeteksi jenis serangan-serangan baru. Namun kelemahan *anomaly based* memiliki *false detection* yang tinggi bila tidak dibuat dengan baik.

Pada Tugas Akhir ini telah dibangun sistem deteksi anomali dengan menggunakan metode *traffic anomaly based*. Mahalanobis *distance* dan algoritma CART digunakan untuk deteksi anomali dan fungsi revisi *belief* pada konsep BDI. Pada penelitian ini digunakan distribusi poison sebagai pengelompokan data pada saat pengujian sistem, hal ini dilakukan agar sistem yang dibangun nantinya dapat diterapkan di dalam kehidupan nyata. Dengan menggunakan parameter DR, FPR, dan ACC pada setiap pengujian, rata-rata hasil yang dihasilkan pada setiap pengujian sebesar μDR = 80.36%, μFPR = 0.0008%, dan μACC = 99.89%.

Kata kunci : Deteksi anomali, Mahalanobis, CART, fungsi revisi *belief*, distribusi poisson, BDI