

ABSTRAK

Seiring berkembangnya teknologi internet sekarang ini, semakin banyak muncul jenis serangan ataupun ancaman terhadap sebuah komputer atau *server* dalam sebuah jaringan, salah satu contohnya berupa *anomaly traffic*. Beberapa macam tipe *anomaly traffic* pada komputer dalam sebuah jaringan internet seperti *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS) atau *flashcrowd*. Oleh karena itu, dibutuhkan adanya suatu sistem deteksi untuk mendeteksi dan mengenali setiap *anomaly traffic* tersebut.

Pada penelitian Tugas Akhir ini mengembangkan sistem deteksi berbasis statistik menggunakan *Multivariate Correlation Analysis* (MCA). MCA menggunakan teknik representasi *Triangle-Area-Map* (TAM) untuk mendeskripsikan hubungan antar setiap fitur trafik dengan menghitung jarak satu buah nilai fitur terhadap nilai fitur yang lain untuk setiap fitur hasil ekstraksi. Data hasil pengolahan MCA dianalisis menggunakan *Mahalanobis Distance* untuk digunakan sebagai data referensi atau observasi.

Proses pendeteksian terhadap data yang diobservasi berbasis *threshold* dari data referensi dan proses klasifikasi anomali menggunakan *Mahalanobis Distance* dan *Cosine Distance* untuk menghitung besar jarak antara nilai fitur TAM trafik yang diobservasi dengan TAM trafik acuan. Pengujian sistem dilakukan dengan melakukan pengukuran tingkat keakuratan algoritma, berdasarkan hasil keluaran sistem dengan parameter *Detection Rate* (DR), *False Positive Rate* (FPR) dan *Accuracy* (ACC).

Kata Kunci : *anomaly traffic, DDoS, flashcrowd, multivariate correlation analysis, triangle-area-map, mahalanobis distance, cosine distance*