ABSTRAK

Sistem deteksi berdasarkan anomali trafik adalah suatu sistem keamanan jaringan yang berfungsi untuk mengetahui adanya keanehan atau gangguan dalam sebuah jaringan komputer. Terdapat beberapa contoh jenis anomali trafik diantaranya adalah *Denial of Service* (DoS), *Distributed Denial of Services* (DDoS) dan sebagainya. Dimana setiap anomali memiliki ciri – ciri yang berbeda sehingga akan menimbulkan sebuah pola anomali. Oleh karena itu perlu adanya sistem deteksi anomali trafik yang dapat menangani dan menangkap pola yang dibentuk oleh anomali trafik tersebut.

Pada penelitian Tugas Akhir ini digunakan salah satu teknik dalam deteksi anomali trafik yaitu *clustering based* dengan menggunakan Algoritma Denstream. Algoritma Denstream merupakan salah satu algoritma *clustering* berbasis *density* yang biasa digunakan untuk pengolahan *Data Stream*. Dalam penelitian Tugas Akhir memiliki fokus untuk melakukan modifikasi pada proses *update micro-cluster*.

Hasil dari penelitian ini, algoritma Denstream modifikasi memiliki perfomansi yang baik dalam mendeteksi anomali trafik, dan juga algoritma Denstream modifikasi dapat memproses semua *micro-cluster* tanpa ada yang dihilangkan. Hal itu dapat ditunjukkan dengan pengujian yang dilakukan dengan dataset DARPA 1998, dimana nilai rata-rata parameter *Purity* rata-rata 97.07%.

Kata Kunci : anomali trafik, ddos, *clustering*, algoritma Denstream, *update micro-cluster*