ABSTRAK

Sistem Deteksi serangan berdasarkan anomali trafik dengan metode *clustering* algoritma *Denstream* adalah suatu sistem keamanan jaringan Komputer yang berfungsi untuk mengetahui adanya gangguan-gangguan pada jaringan komputer dengan cara mendeteksi gangguan-gangguan tersebut berdasarkan pola-pola anomali yang ditimbulkan. Serangan *Distributed Denial of Services* (DDoS) adalah salah satu contoh jenis serangan yang dapat mengganggu trafik pada jaringan komputer, serangan jenis ini memiliki suatu ciri khas, dimana dalam setiap serangannya akan mengirimkan sejumlah paket data secara terus-menerus kepada target serangannya. Dengan menggunakan metode deteksi anomali, serangan DDoS dapat dideteksi dengan mengidentifikasi pola-pola anomali yang ditimbulkan.

Pada penelitian Tugas Akhir ini digunakan salah satu teknik dalam deteksi anomali trafik yaitu *clustering based*. Algoritma *Denstream* merupakan salah satu algoritma *clustering* berbasis *Density* yang dapat digunakan pada *Data Stream* Kemudian, fokus penelitian Tugas Akhir ini adalah Menyesuaikan algoritma *Denstream* pada proses *generating cluster* secara periodik.

Hasil dari penelitian ini, algoritma Denstream modifikasi memiliki perfomansi yang baik dalam mendeteksi anomali trafik. Hal itu dapat ditunjukkan dengan pengujian yang dilakukan dengan dataset DARPA 1998, dimana nilai Purity rata-rata sebesar 98.02 %.

Kata Kunci : anomali trafik, ddos, *clustering*, algoritma *Denstream, Density, generating cluster*