# ABSTRAK

*Anomaly traffic* merupakan suatu kejadian dimana seorang pengguna internet tidak dapat mengakses internet sebagai mana mestinya, hal tersebut bisa dikarenakan karena peningkatan *traffic* secara drastis (Flash Crwod) atau telah terjadinya serang (DoS maupun DDoS) oleh pihak yang tidak menginginkan user untuk melakukan akses *internet*. DDoS merupakan sebuah serangan dimana salah satu jenis serangan dilakukan dengan membanjiri *traffic target* menggunakan pesan "PING" sehingga *target* tidak dapat terkoneksi dengan baik. Sedangkan Flash Crowd merupakan keadaan suatu *traffic* meningkat tetapi bertahap (tidak seperti DDoS) karena bencana alam, promosi produk, dan lain-lain.

Ada dua metode untuk melakukan deteksi *anomaly* yaitu dengan *signature* dan *anomaly based*. Metode *Signature* menggunakan database dalam pengenalan suatu *anomaly*, sehingga jika terdapat *anomaly* baru tidak akan terdeteksi. Sedangkan, *Anomaly* tidak menggunakan *database* tetapi menggunakan pembelajaran pola yang terjadi, sehingga jika terdapat *anomaly* baru bisa terdeteksi. Sehingga pada Tugas Akhir, menggunakan metode *anomaly based* sebagai metode deteksi.

Dalam Tugas Akhir ini menerapkan metode *Clustering* dengan menggunakan Algoritma Modified K-Means dengan *Timestamp Initialization* pada *Sliding Window*. Hasil yang diperoleh berupa sebuah metode pendeteksian *anomaly traffic* dengan *detection rate* yang tertinggi 96.06% dan *false positive rate* terkecil 0.75% dari pengujian beberapa *dataset*.

Kata kunci : *Anomaly traffic*, *Clustering*, K-Means, *Timestamp Initialization*, *Sliding Window*.