BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir *interconnection network* atau internet mengalami perkembangan yang pesat. Internet adalah jaringan yang terdiri dari milyaran komputer yang ada di seluruh dunia, dengan menggunakan internet semua orang dapat mengakses banyak informasi yang telah disediakan. Dengan adanya perkembangan internet banyak orang melakukan penyalahgunaan internet. Jenis serangan yang umum dilakukan adalah *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) [1].

Denial of Service (Dos) merupakan suatu bentuk serangan *flooding* yang bertujuan membuat suatu sumber (*resource)* yang dimiliki suatu komputer target habis dan tidak dapat memberikan layanan kepada pengguna yang sah. *Distributed Denial of Service* (DDoS) adalah salah satu jenis serangan DoS yang menggunakan banyak host penyerang baik itu menggunakan komputer yang di dedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi zombie untuk menyerang sebuah host target dalam sebuah jaringan. Target serangan dalam DoS dan DDoS adalah *bandwidth,* dimana *bandwidth* dalam sebuah jaringan tersebut akan dibuat penuh dan sumber daya komputasi pada server maupun node jaringan habis akan sumber daya dan akhirnya *crash* atau *down* sehingga tidak dapat lagi memberikan *service* jaringan.

Oleh karena itu, diperlukan suatu sistem untuk mendeteksi *(Intrussion Detection System)* anomali trafik di jaringan komputer. Salah satu teknik deteksi yang dapat digunakan untuk mendeteksi anomali trafik yaitu *clustering based* yang merupakan metode dalam data mining . Pada Tugas Akhir ini, algoritma *clustering* Denstream yang merupakan algoritma berbasis *density* digunakan untuk melakukan

proses deteksi. Kemudian, fokus penelitian Tugas Akhir ini adalah untuk melakukan modifikasi pada proses *update micro-cluster*. Dengan teknik *clustering based*, maka dilakukan proses penganalisaan data ke dalam struktur kelompok-kelompok data yang memiliki kesamaan berdasarkan jenis anomali trafik (normal dan serangan *DDoS*) dengan algortima Denstream yang digunakan.

1.2 Perumusan Masalah

Clustering adalah metode penganalisaan data, yang sering dimasukan sebagai salah satu Metode *Data Mining*, sebuah proses untuk mengelompokan data ke dalam beberapa *cluster* atau kelompok sehingga data dalam satu *cluster* memiliki tingkat kemiripan yang maksimum dan data antar *cluster* memiliki kemiripan yang minimum. Implementasi *clustering* dapat diterapkan di berbagai bidang.

Salah satu metode *clustering* adalah *density-based clustering*. *Density-based clustering* [2] merupakan algoritma yang berdasarkan kerapatan suatu data dan mengelompokannya menjadi beberapa *cluster*. *density-based clustering* diciptakan untuk menemukan *cluster* yang berbentuk acak dan terdapat banyak *noise* didalamnya. Beberapa algoritma yang termasuk *Density-based clustering : DBSCAN (Density-based Spatial Clustering of Application with Noise)* [3] , *OPTICS(Ordering Point to Identify the Clustering Structure)* [4], *DENCLUE(Density-based Clustering)* [2] . Namun masih terdapat kekurangan pada *density-based clustering* yaitu ketika jenis data yang akan di*cluster* merupakan jenis data stream maka *density-based clustering* akan sulit dalam penentuan *cluster* karena sifat ketidakpastian dari data stream yang menyebabkan sulitnya penentuan kerapatan pada suatu *cluster*.

Penelitian Tugas Akhir ini menggunakan algoritma Denstream untuk melakukan proses deteksi *(Intrussion Detection System)* terhadap anomali trafik pada jaringan komputer. Fokus penelitian ini yaitu melakukan modifikasi pada proses *update micro-cluster* yang terdapat pada dataset dalam algoritma *clustering* Denstream. Pada penelitian ini proses *update micro-cluster* dilakukan dengan

mengetahui *weight* dari sebuah *p-micro-cluster*, *weight* tersebut adalah salah satu parameter yang mempengaruhi apakah sebuah *p-micro-cluster* langsung dihapus atau akan dihitung ulang. Penghitungan ulang *p-micro-cluster* inilah yang akan mempengaruhi hasil dari deteksi anomali trafik menggunakan algoritma Denstream.

Dengan penelitian yang dilakukan, maka algoritma Denstream yang digunakan diharapkan dapat mengefektifkan proses *update micro-cluster* dan memiliki tingkat keakuratan algoritma / *benchmarking* algoritma tinggi dengan parameter *Purity* dan hasil analisis dengan menggunakan tabel konvolusi .

Berdasarkan uraian diatas, maka masalah yang akan dibahas pada penelitian Tugas Akhir ini, sebagai berikut :

1. Perancangan sistem deteksi anomali trafik menggunakan algoritma *clustering* Denstream.
2. Penerapan modifikasi pada proses *update micro-cluster* untuk menangani proses perhitungan *weight p-micro-cluster* dalam algoritma *clustering* Denstream.
3. Proses *Prepocessing* untuk mendapatkan fitur dari dataset yang digunakan untuk kemudian diolah dalam sistem deteksi anomali trafik menggunakan algoritma Denstream.
4. Analisis modifikasi pada proses *update micro-cluster* dan performansi algoritma Denstream dalam proses deteksi anomali trafik.

1.3 Tujuan

Tugas Akhir mengenai analisis sistem deteksi menggunakan algoritma *clustering* Denstream dengan modifikasi pada proses *update micro-cluster* memimiliki beberapa tujuan, yaitu :

1. Merancang sistem deteksi anomali trafik menggunakan algoritma *clustering* Denstream.

2. Proses *Prepocessing* untuk mendapatkan fitur dari dataset yang digunakan kemudian diolah dalam sistem deteksi anomali trafik menggunakan algoritma Denstream.
3. Menerapkan modifikasi pada proses *update micro-cluster* dalam algoritma Denstream.
4. Analisis hasil metode modifikasi pada proses *update micro-cluster* serta performansi algoritma Denstream dalam proses deteksi anomali trafik dengan parameter *Purity*.

1.4 Batasan Masalah

Berikut merupakan hal-hal yang dibatasi dalam penelitian Tugas Akhir ini :

1. Membahas tentang sistem deteksi anomali trafik *(Intrussion Detection System)*.
2. Membahas tentang metode yang digunakan untuk melakukan proses deteksi anomali trafik.
3. Metode yang digunakan yang adalah algortima *cluster*ing Denstream.
4. Melakukan modifikasi pada proses *update micro-cluster* dalam perhitungan *p-micro-cluster*.
5. Analisis dilakukan dengan menggunakan tools / software berbasis java (javascript programming).
6. Menggunakan dataset DARPA 1998 *real time* yang sudah terekam (ter-*capture*) berupa *network log connection* untuk trafik normal dan serangan DDoS.
7. Tidak membahas mengenai pencegahan *(prevention)* terhadap serangan yang ada pada jaringan.

1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang digunakan adalah:

a. Studi literatur, yaitu mempelajari literatur-literatur yang ada sesuai dengan permasalahan yang akan dibahas meliputi, konsep deteksi anomali trafik *(Intrussion Detection System)*, teori serangan *flooding traffic (DDoS)* dan konsep *preprocessing*, teori *density based clustering*, konsep algoritma *clustering* Denstream, konsep *micro-cluster*, dan teori mengenai uji perfomansi menggunakan parameter *Purity*.

b. Analisis terhadap kebutuhan dan pemodelan sistem untuk proses deteksi anomali trafik.

c. Perancangan dan analisis menggunakan tools untuk sistem deteksi anomali trafik.

d. Uji performansi dan analisis hasil penelitian.

e. Pembuatan laporan dari hasil penelitian.

1.6 Sistematika Penulisan TA

Adapun sistematika penulisan pada Tugas Akhir ini adalah :

BAB I PENDAHULUAN

Berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Berisi tentang penjelasan mengenai deteksi anomali trafik *(Intrussion Detection System)*, penjelasan mengenai serangan *flooding traffic* (DDoS), penjelasan mengenai *density based clustering*, konsep algoritma *clustering* Denstream dan *micro-cluster*, penjelasan mengenai parameter uji.

BAB III PERANCANGAN SISTEM

Berisi tentang perancangan sistem yang akan dibangun.

BAB IV PENGUJIAN DAN ANALISIS

Berisi tentang pengujian performansi dan analisis hasil penelitian.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari hasil penelitain yang dilakukan dan rekomendasi untuk penelitian berikutnya.