Perancangan dan Analisis Deteksi Anomaly Berbasis Clustering Menggunakan Algoritma Modified K-Means dengan Random Initialization pada Landmark Window

Design and Analysis Of Clustering Based Anomaly Detection Using Modified K-Means Algorithm With Random Initialization On Landmark Window

Made Indra Wira Pramana[1], Yudha Purwanto[2], Fiky Yosef Suratman[3]
[1,2,3] Universitas Telkom
[1]indrawp@students.telkomunivesity.ac.id, [2]omyudha@telkomuniversity.ac.id, [3]fysuratman@telkomuniversity.ac.id

Abstrak

Seiring perkembangan internet, terdapat gangguan dalam jaringan yang dapat menganggu layanan, salah satunya adalah Distributed Denial of Service (DDoS) yang merupakan serangan dengan tujuan menghilangkan hak ases sehingga dapat memberi dampak yang merugikan bagi user dan service provider. Fenomena lain adalah Flash Crowds yang memiliki kemiripan dengan DDoS, namun Flash Crowds tidak dikategorikan sebagai serangan karena memiliki ciri yang berbeda. Flash Crowds biasanya terjadi saat terdapat sebuah berita besar atau peluncuran produk baru sehingga permintaan akses meningkat namun terjadi secara gradual. Metode yang dapat digunakan dalam mendeteksi anomaly dalam jaringan adalah Intrusion Detection System (IDS), agar dapat mengenali jenis anomaly baru, maka IDS dapat dibangun anomaly-based salah satunya dengan memanfaatkan unsupervised learning clustering sehingga tidak memerlukan database dalam perancangannya. Algoritma dalam teknik clustering dipilih algoritma K-Means yang memiliki ruang modifikasi dan pengembangan yang luas. Algoritma K-Means yang digunakan dalam penelitian ini dimodifikasi dengan Random Initialization dan dikombinasikan dengan Landmark Window sehingga menghasilkan cluster yang optimal ditinjau dari parameter Detection Rate (DR), Accuracy (ACC), dan False Positive Rate (FPR).

Kata kunci : Network, Anomaly, Clustering, K-Means, Random Initialization, Landmark Window.

Abstract

In Internet, Distributed Denial of Service (DDoS) is one of many form of attack which is popular nowadays. DDoS's affect user access right by preventing user from accessing certain information, thus giving disadvantage to the user and service provider. Similar to DDoS's effect is phenomenon so-called Flash Crowds which is categorized as anomaly because it occurs on product launching or big news which is happened naturally due to increasing of number of access gradually.

Detecting network anomaly can be done using Intrusion Detection System (IDS). To make sure the IDS recognize latest anomaly type, IDS could be built in anomaly-based by using unsupervised learning clustering which need no database.

Algorithm used in building the IDS is K-Means algorithm which can be modified and developed in many possible way. K-Means Algorithm will be using Random Initialization and combined with Landmark Window to create optimal cluster and will be reviewed by several parameter, Detection Rate (DR), Accuracy (ACC), and False Positive Rate (FPR).

Keywords : Network, Anomaly, Clustering, K-Means, Random Initialization, Landmark Window.

1. Pendahuluan

Jaringan komunikasi internet merupakan jaringan komunikasi digital yang telah menjadi bagian dalam kehidupan sehari-hari. Aktifitas dalam internet sangat beragam, jutaan akses datang tiap harinya melalui internet. Menurut statistik dalam [1] sebanyak 42% dari populasi di dunia adalah pengguna internet. Aktifitas yang terjadi dalam internet bukan saja aktifitas legal seperti yang biasa kita lakukan, namun terdapat juga aktifitas illegal. Salah satu aktifitas illegal yang sering terjadi adalah denial-of-service.

Denial-of-service (DOS) merupakan aktifitas penyerangan jaringan yang dilakukan dengan usaha menghilangkan hak akses user. Serangan DoS biasanya dilakukan secara masif, aktifitas ini biasa disebut *Distributed denial-of-service* (DDoS). DDoS dilakukan dengan mengirimkan sebuah perintah dari perangkat pelaku atau *attacker*, perintah dikirmkan ke perangkat yang telah diinfeksi dengan *malware*, perangkat ini disebut *botnet*, *botnet* yang menerima perintah dari *attacker* akan mengirimkan paket *request* dalam jumlah banyak atau berukuran besar ke korban atau *victim* tertentu sehingga perangkat *victim* akan mengalami *crash*

dan tidak dapat beroperasi secara normal. DDoS merupakan pelanggaran pada etika penggunaan internet karena dianggap memaksa pengguna kehilangan haknya. DDoS biasa terjadi pada pesaing bisnis, website, dan kompetisi *online game.*

Selain DDoS, terdapat sebuah fenomena dalam *internet* yang memiliki efek serupa, fenomena ini disebut *flash crowds. Flash crowds* terjadi akibat pembajiran *traffic* pada sebuah server yang biasanya terjadi saat terdapat sebuah berita yang fenomenal. Efek yang ditimbulkan oleh *flash crowds* adalah server yang tidak dapat melayani user akibat banyaknya user yang mengantri dalam jaringan sehingga waktu pelayanan jaringan menjadi melambat. Jika dilihat dari sisi pengguna, efek DDoS dan *flash crowds* memiliki kemiripan, namun faktanya keduanya memiliki fitur yang membedakan satu sama lain.

Pendekatan secara analitik dalam deteksi *flash crowds* dan serangan DDoS dapat dilakukan dengan membangun *Intrusion Detection System* (IDS) dengan metode data mining. Salah satu teknik yang umum digunakan dalam data mining adalah clustering, dengan menggunakan clustering, analisa *traffic* dapat digunakan untuk mendeteksi *flash crowds* dan serangan DDoS. Sistem kerja clustering adalah mengelompokkan data ke dalam sebuah kelompok yang memiliki kemiripan atau biasa disebut *cluster*, setiap *cluster* memiliki titik tengah yang disebut *centroid.* Algoritma yang digunakan dalam penelitian ini adalah algoritma K-Means [2] yang dimodifikasi dengan *max chain initialization* dan diterapkan pada *landmark window* [3] untuk memastikan tingkat presisi dan akurasi dari clustering.

2. Dasar Teori

IDS biasa digunakan dalam mendeteksi serangan yang terjadi dalam jaringan. Penerapan IDS dapat dilakukan dengan dua metode :

a. *Signature based* : Menggunakan *database* yang menyimpan pola-pola serangan, memiliki tingkat deteksi yang tinggi namun *database* harus selalu diperbarui untuk memastikan IDS dapat mengenali serangan jenis baru.
b. *Anomaly based* : Tidak menggunakan *database*, serangan dikenali lewat pola *anomaly* dalam jaringan, sehingga dapat mengenali serangan jenis baru.

Membangun IDS dengan teknik data mining yang dapat mendeteksi DDoS pernah dilakukan dalam [4] dengan hasil *detection rate* yang baik, namun IDS masih terbatas dalam mendeteksi DDoS. Penelitian lain yang menggunakan teknik data mining adalah [5] dan [6], keduanya menggunakan fitur tertentu sehingga IDS yang dibangun dapat mengenali DDoS. Penelitian ini bertujuan membangun IDS yang dapat mengenali *flash crowds* dan DDoS, sehingga perlu dilakukan pengenalan pola sebelumnya. *Flash crowds* terjadi saat jumlah akses user meningkat, namun yang membedakan dengan DDoS adalah serangan ini terjadi secara gradual, saat mencapai puncaknya, *traffic* akan terlihat mulai menurun karena *server* mulai kesulitan melayani permintaan akses yang berlebihan. Pada DDoS, serangan dilakukan dalam satu perintah, sehingga kenaikan secara statistik akan terlihat instan dan stabil pada saat puncaknya yang menandakan jumlah paket yang dikirimkan tidak mengalami perubahan.

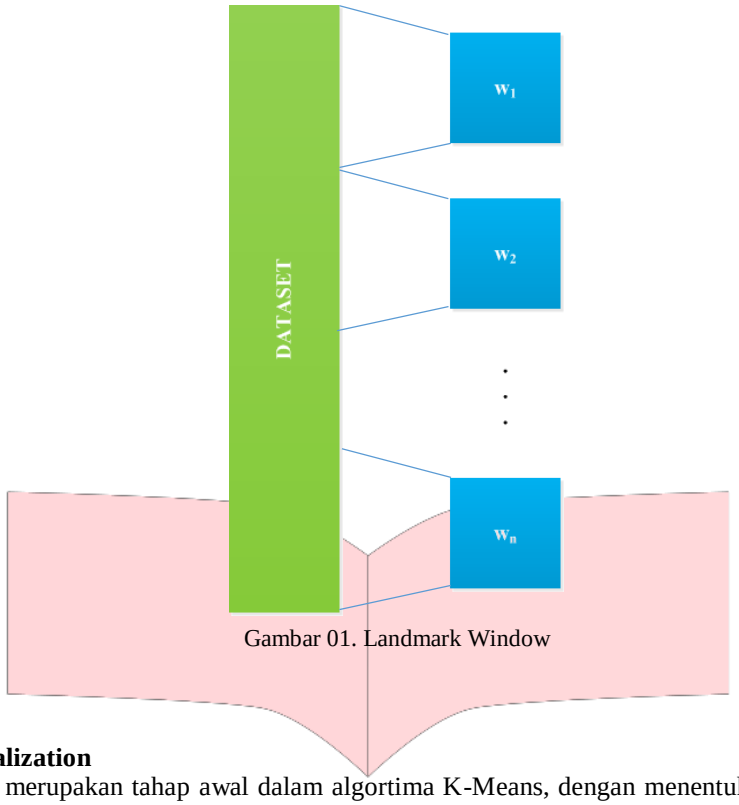
2.1. K-Means

Algoritma yang digunakan dalam membangun IDS adalah K-Means, algoritma ini merupakan algoritma data mining yang populer digunakan [2]. Algoritma K-Means mengelompokan data berdasar kemiripan fitur numerik yang dihitung menggunakan *Euclidiean Distance* (1). Data yang memiliki kemiripan akan dikelompokan dalam sebuah cluster, akan dipilih sebuah centroid sebagai titik tengah cluster yang merupakan nilai rata-rata dari seluruh data dalam cluster tersebut. Algoritma ini bekerja dengan memetakan data ke dalam *d* dimensi, kemudian data diukur ke tiap *centroid* yang diinisialisasi dan ditetapkan sebagai anggota dari cluster terdekat, proses ini dilakukan hingga setiap data menjadi anggota tepat satu cluster, kemudian nilai-rata rata cluster dihitung dan dijadikan *centroid* cluster tersebut, proses ini berulang hingga *centroid* tidak lagi mengalami perubahan.

$$d(x,y) = d(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \qquad (1)$$

2.2. Landmark Window

Dalam membentuk cluster, dibutuhkan fitur yang menggambarkan kemiripan antar data. Teknik Windowing digunakan untuk meningkatkan presisi dan akurasi dalam clustering. Dengan mengolah data per bagian, akan didapatkan hasil clustering yang optimal. Windowing juga berguna agar sistem dapat bekerja dalam *data stream* yang memiliki aliran data yang tidak dapat diprediksi sehingga tidak perlu menunggu data selesai diterima untuk memprosesnya. Landmark Window memproses *x* jumlah data dalam satu *w* window, jumlah data tergantung range *r* yang telah ditentukan sebelumnya. Jumlah data yang diproses dalam window akan selalu berjumlah sama dengan *r* yang ditentukan. Illustrasi kerja Landmark Window dapat dilihat pada Gambar 1.



Gambar 01. Landmark Window

2.3. Max Chain Initialization

Initialization merupakan tahap awal dalam algortima K-Means, dengan menentukan *k* sebagai jumlah *centroid* yang akan diinisialisasi, akan dibentuk *k* jumlah cluster secara acak, teknik ini disebut *Random Initialization.* Penelitian ini memodifikasi *Initialization* yang biasa digunakan dalam K-Means dengan metode yang dapat menentukan nilai *k* sebagai jumlah maksimum *centroid* yang akan diinitialisasi. Hal ini memungkinkan banyak jumlah cluster yang terbentuk, tidak menutup kemungkinan cluster yang terbentuk lebih kecil dari nilai *k* yang telah ditentukan. Pada keadaan tertentu, *centroid* yang diinisialisasi dapat menjadi cluster kosong yang tidak memiliki anggota, dalam algoritma Modified K-Means, cluster yang tidak beranggota akan dihapus.

Karena algoritma Modified K-Means menggunakan teknik Windowing, maka *centroid* tiap *window* akan disimpan untuk digunakan dalam *window* selanjutnya, hal ini dilakukan untuk memastikan jika *data* pada *window* sebelumnya dan *window* saat ini memiliki kemiripan, titik tengahnya tidak berubah secara signifikan. Algoritma Modified K-Means dapat dilihat pada Algortima 1.

Algoritma 1 : *Modified K-Means* (*dataset, k, r*)

```
1: Pilih dataset
2: Masukkan k sebagai jumlah initialization
3:  repeat
4:    Proses x data per r pada w_n
5:    if c pada w_{n-1} ≠ 0, do
6:      Bentuk k-c cluster secara acak
7:    else
8:      Bentuk k cluster secara acak
9:    end if
10:   repeat
11:     for 1 to x do
12:       Hitung jarak x_n ke centroid
13:       Tetapkan x_n ke centroid terdekat
14:     end for
15:   until centroid tidak berubah
16:   Hapus c_kosong
17:   w_n ← w_{n+1}
18: until semua data diproses
```

2.4. Dataset

Penelitian ini menggunakan *dataset* yang telah banyak digunakan dalam penelitian serupa. *Dataset* yang digunakan adalah KDD Cup 1999 [7] untuk *dataset* normal, DARPA 1998 [8] untuk *dataset* DDoS, dan World Cup 1998 [9] untuk *dataset flash crowds.* Untuk menguji metode IDS yang dirancang, dilakukan simulasi

dengan menggunakan bahasa pemrograman Java. *Dataset* yang digunakan adalah *dataset* yang telah dilakukan *preprocessing* sehingga siap untuk dianalisa menggunakan algoritma.

2.5. Parameter Uji

Sistem diuji menggunakan dataset yang telah ditentukan, tingkat ketepatan teknik clustering dilihat dari hasil algoritma membedakan antara traffic normal dan traffic lainnya. Sebagai parameter uji, dataset diberikan label pada setiap traffic tergantung jenis traffic tersebut. Pada tiap cluster dihitung jumlah jenis traffic yang paling banyak di dalamnya, maka label cluster tersebut adalah traffic tersebut. Misalkan sebuah cluster memiliki 50 anggota dengan 40 traffic normal dan 10 traffic DDoS, maka cluster tersebut adalah cluster normal. Pelabelan pada dataset tidak akan berpengaruh pada kinerja algoritma, hal ini dikarenakan teknik clustering yang dilakukan dalam penelitian ini hanya mengukur kemiripan data berdasarkan fitur yang bersifat numerik. Dengan membandingkan label cluster dengan label anggota cluster, dapat dilakukan analisa matching matrix seperti pada Tabel 1.

Tabel 1. Matching matrix

	Terdeteksi	**Tidak Terdeteksi**
***Traffic* Serangan**	True positive	False negative
***Traffic* Normal**	False positive	True negative

Jika terdapat kesalahan pengelompokan yang menyebabkan traffic serangan berada pada cluster normal, maka kondisi ini disebut False Negative (FN), sedangkan kondisi jika traffic normal berada pada cluster normal disebut True Negative (TN). Analisa serupa juga berlaku pada cluster serangan, jika traffic normal berada dalam cluster serangan maka kondisi ini disebut False Positive (FP) dan pada kondisi traffic serangan disebut True Positive (TP). Dengan analisa berdasar matching matrix, digunakan tiga parameter sebagai evaluasi performa algoritma Modified K-Means.

2.5.1. Detection Rate

Detection Rate (DR) merupakan parameter yang menilai tingkat presisi sebuah sistem. DR berhubungan dengan random error, semakin tinggi nilai DR maka semakin baik sistem deteksi yang digunakan. DR diformulasikan pada (2).

$$DR = \frac{TP}{(TP + FN)} \quad (2)$$

2.5.2. False Positive Rate

False Positive Rate (FPR) merupakan parameter yang menunjukan rata-rate kesalahan deteksi pada sebuah sistem. Tingginya nilai FPR bisanya disebabkan oleh noise atau kesalahan konfigurasi pada sistem. Semakin rendah nilai FPR maka semakin baik sistem dalam membedakan antara serangan dan normal. FPR diformulasikan pada (3).

$$FPR = \frac{FP}{(FP + TN)} \quad (3)$$

2.5.3. Accuracy

Accuracy (ACC) merupakan parameter penilai akurasi sebuah sistem deteksi. Berbeda dengan DR, ACC berhubungan dengan systematic error. Semakin tinggi nilai ACC, maka semakin akurat sistem yang digunakan. ACC diformulasikan pada (4).

$$ACC = \frac{TP + TN}{(\sum$$ (4)

3. Pembahasan

Preprocessing dilakukan pada *dataset* DDoS untuk memastikan data yang diolah relevan dengan *dataset* yang digunakan dalam penelitian. Fitur yang digunakan dapat dilihat pada Tabel 2. Algoritma Modified K-Means dapat dilihat pada Algoritma 2. Dataset dalam penelitian ini diberi label untuk mempermudah analisa hasil akhir yang didapatkan.

Tabel 2. Ekstraksi fitur

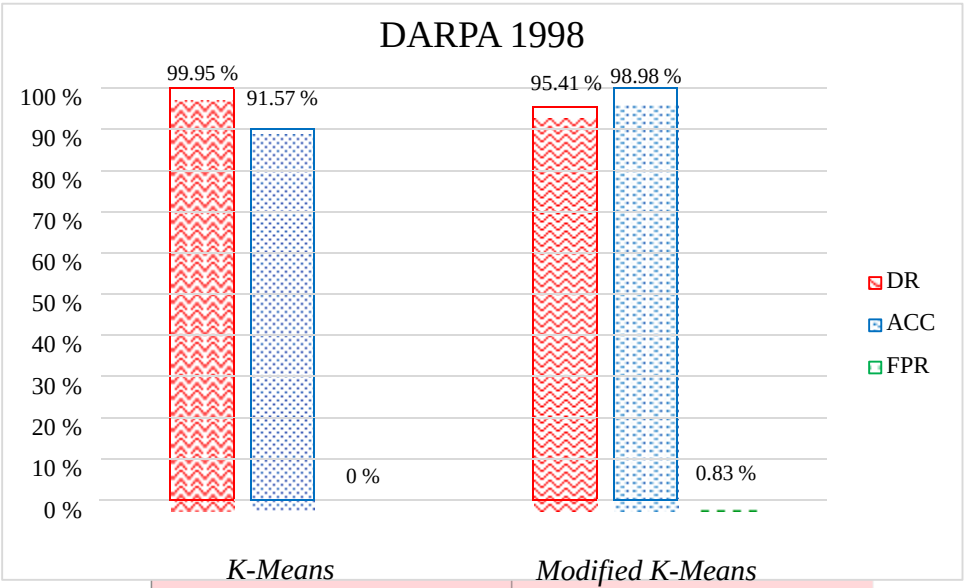
Nama Fitur	Jenis Koneksi	Penjelasan
Count	-	Jumlah *traffic* dalam satu window
IP_source	IP Source dan IP Destination sama	Jumlah *traffic* dari IP Source ke IP Destination yang sama
Protocol		Jumlah protocol yang sama
SYN		Jumlah *traffic* "SYN"
ACK		Jumlah *traffic* "ACK"
Port_Out		Jumlah *traffic* menuju ke port out yang sama
Length		Jumlah *traffic* dengan length yang sama
Different_Source	IP Destination sama	Jumlah *traffic* dengan IP Source berbeda
New_IP	-	Jumlah kemunculan IP baru

Algoritma 2 : *Modified K-Means* (*dataset, k, r*)

1: Pilih *dataset*
2: Masukkan *k* sebagai jumlah *initialization*
3: ***repeat***
4: Proses *x data* per *r* pada w_n
5: ***if*** *c* pada $w_{n-1} \neq 0$, ***do***
6: Bentuk *k-c cluster* secara acak
7: ***else***
8: Bentuk *k cluster* secara acak
9: ***end if***
10: ***repeat***
11: ***for*** 1 to *x* **do**
12: Hitung jarak x_n ke *centroid*
13: Tetapkan x_n ke *centroid* terdekat
14: ***end for***
15: ***until*** *centroid* tidak berubah
16: Hapus c_{kosong}
17: $w_n \leftarrow w_{n+1}$
18: ***until*** semua *data* diproses

3.1. DDoS Dataset

Sebelum diproses, dilakukan *preprocessing* pada *dataset* DARPA 1998 karena *dataset* ini masih berupa *raw data*. Aplikasi untuk *preprocessing* dibuat dalam penelitian ini dengan pengkhususan berdasar pada karakteristik *traffic* DDoS sehingga hasil yang didapat dari *dataset* ini lebih baik dari hasil sebelumnya. Pengujian dilakukan pada *dataset* normal dan *dataset* serangan menghasilkan hasil uji yang bervariasi. Hasil pengujian dan perbandingan algoritma pada *dataset* DARPA 1998 dapat dilihat pada Gambar 2.

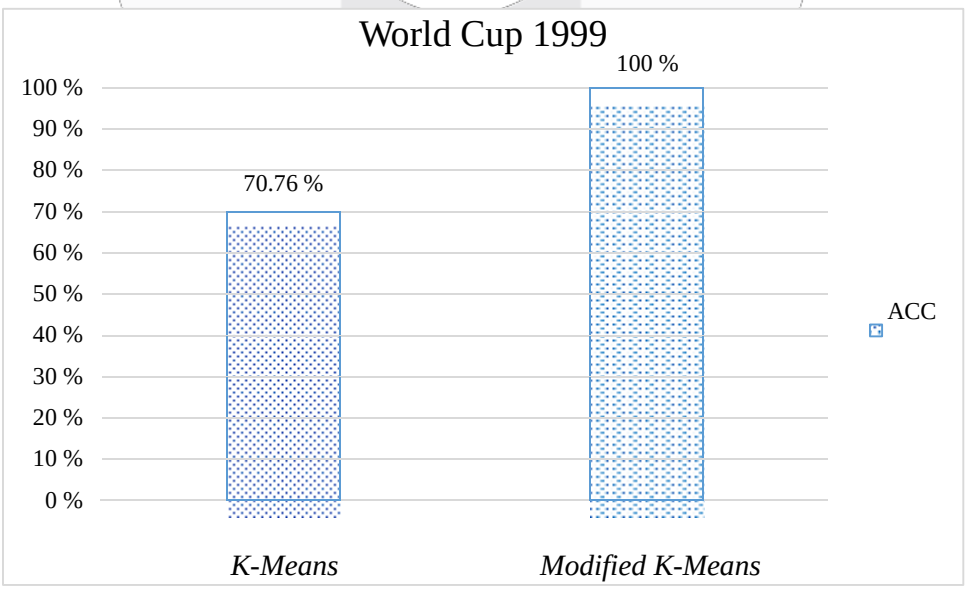


Gambar 2. Hasil pengujian pada DDoS *Dataset*

Pada *dataset* DARPA 1998, setiap pengujian dilakukan dengan menggunakan *input* yang sama, *r*=50 dan *k*=50 sehingga didapat hasil yang presisi dan akurat. Pengujian berulang-ulang pada dataset tidak mengubah hasil secara signifikan, walaupun algoritma menggunakan *random initialization.* Meskipun memiliki tingkat presisi dan kesalahan deteksi yang lebih baik, algoritma *K-Means* dasar memiliki tingkat akurasi yang lebih rendah karena pengenalan *traffic* serangan lebih sulit dilakukan jika pengolahan data dilakukan dalam satu kali penghitungan. Kedua algoritma memberikan hasil yang baik dengan menggunakan teknik *preprocessing* yang dibangun. Hal ini membuktikan bahwa jenis serangan DDoS tertentu memiliki fitur khusus yang mencirikannya, dengan memanfaatkan pola yang dibentuk, membedakan antara *traffic* normal dan *traffic* DDoS dapat dilakukan dengan mudah.

3.2. Flash Crowds Dataset

Skenario pengujian dan analisis pada *dataset* World Cup 1998 dilakukan dengan memberi *label* pada *dataset* sehingga lebih mudah untuk mendapatkan hasil akhir. *Dataset* ini hanya memuat dua jenis *traffic* yaitu, *traffic* normal dan *traffic flash crowds*, pelabelan *flash crowds* dilakukan pada saat *traffic* mulai menunjukan kenaikan jumlahnya. Pada pengujian dataset digunakan panjang *r*=50, namun untuk memastikan kerja algoritma, jumlah *k* divariasikan, dengan asumsi jika algoritma bekerja baik, maka *traffic flash crowds* dan *traffic* normal akan berada dalam satu *cluster* yang sama, sehingga tidak akan membentuk *cluster* dengan jumlah lebih dari satu. Jika terbentuk *cluster* yang hanya beranggotakan *traffic flash crowds*, maka *cluster* ini dianggap sebagai kesalahan deteksi.



Gambar 3. Hasil pengujian pada *Flash Crowds Dataset*

4. Kesimpulan

a. *Random Initialization* pada *K-Means* tidak mempengaruhi tingkat DR, FPR, dan ACC secara signifikan pada hasil *clustering*.

b. *Preprocessing* yang dibangun memiliki peran penting dalam mengenali serangan DDoS sehingga dapat menghasilkan hasil yang optimal dinilai dari ketiga parameter uji.

c. Penerapan *Landmark Window* meningkatkan tingkat presisi dan akurasi dalam perancangan sistem untuk membedakan antara *traffic* normal, DDoS, dan *traffic flash crowds*.

d. Algoritma *Modified K-Means* layak digunakan sebagai *intrusion detection system*, dalam hal ini *traffic* berupa seragan DDoS dan *flash crowds*

Daftar Pustaka

[1] Miniwatts Marketing Group, "The Internet Big Picture : Internet Usage Statistics," Miniwatts Marketing Group, 30 June 2014. [Online]. Available: http://www.internetworldstats.com/stats.htm.

[2] X. Wu, V. Kumar, J. Quinlan, J. Ghosh, Q. Yang, H. Motoda, G. J. McLachlan, A. Ng, B. Liu, P. S. Yu, Z.-H. Zhou, M. Steinbach, D. J. Hand and Steinberg, "Top 10 algorithms in data mining," 2007.

[3] P. S. and O.P.Vyas, "Data Stream Mining: A Review on Windowing," *Global Journal of Computer Science and Technology Software & Data Engineering*, vol. 12, no. 11, 2012.

[4] G. Munz, S. Li and G. Carle, "Traffic Anomaly Detection Using K-Means Clustering," in *GI/ITG-Workshop MMBnet*, Hamburg, Germany, 2007.

[5] R. Zhong and G. Yue, "DDoS Detection System Based on Data Mining," in *Second International Symposium on Networking and Network Security*, Jinggangshan, P. R. China, 2010.

[6] S. Kandula, D. Katabi, M. Jacob and A. Berger, "Surviving Organized DDoS Attacks That Mimic Flash Crowds," in *2nd Symposium on Networked Systems Design & Implementation*, 2005.

[7] L. M, "UCI Machine Learning Repository," University of California, Irvine, School of Information and Computer Sciences, 2013. [Online]. Available: http://archive.ics.uci.edu/ml.

[8] MIT Lincoln Laboratory, "DARPA Intrusion Detection Evaluation," [Online]. Available: www.ll.mit.edu/ideval/data/.

[9] P. Danzig, J. Mogul, V. Paxson and M. Schwartz, "WorldCup98," ACM SIGCOMM, [Online]. Available: http://ita.ee.lbl.gov/html/contrib/WorldCup.html.