Journal of Al Azhar University-Gaza *(Natural Sciences)*, **2015, 17** : **35-54**

Detecting DDoS Attack Using A Multilayer Data Mining techniques

Tawfiq S. Barhoom , Heba S. Albiltaje

Faculty of Information Technology
Islamic University of Gaza
tbarhoom@iugaza.edu

Received 9/2/2015 *Accepted* 20/5/2015

Abstract:

Detection Distributed Denial of Service Attack (DDoS) becomes a crucial process for the commercial organization that using the internet these days. Different approaches have been adopted to process traffic information collected by a monitoring stations to distinguish the misbehaving of malicious traffic of DDoS attacks in Intrusion Detection Systems (IDS).. In this paper, we present multi-clustering method called "MCDDM" detect a real-world DDoS attacks collected from "CAIDA UCSD " DDoS Attack 2012 Dataset" and normal traffic traces from "CAIDA Anonymized Internet Traces 2014 Dataset" using combination of (k-means ,K-fast means , K-medoid) data mining clustering techniques. "MCDDM" method are used to effectively detect new DDoS attack from unlabeled dataset . The Result of experiments shows that the "MCDDM" method perform better than the cluster method if they used lonely in term of Davies Bouldin Index the proposed solution obtains very low Davies Bouldin Index (-0.666) .

Keywords: Intrusion Detection, Distributed Denial of Service (DDoS), data mining, Clustering, Unsupervised Anomaly Detection.

Introduction:

Availability is one of the three main components of computer security, along with confidentiality and integrity. One of the major threats to cyber security is Distributed Denial-of-Service (DDoS) attack .In which the victim network element(s) are bombarded with high volume of fictitious attacking packets originated from a large number of Zombies. The aim of the attack is to overload the victim and render it incapable of performing normal transactions the proposed solution tries to prevent DDoS. [5][7] two different approaches are by far dominant in current research community and commercial detection systems: signature-based detection and anomaly detection. Despite being opposite in nature, both approaches share a common downside: they rely on the knowledge provided by an expert system, usually a human expert, to do the job. On the one hand, signature-based detection systems [2][4] are based on an extensive knowledge of the particular characteristics of each attack, referred to as its "signature". Such systems are highly effective to detect those well-known attacks which they are programmed to alert on. However, they cannot defend the network against new attacks, simply because they cannot recognize what they do not know. In addition, building new signatures involves manual inspection by human experts, which is not only very expensive and prone to errors, but also introduces an important latency between the discovery of a new attack and the construction of its signature. In a network scenario where new attacks are constantly appearing, such a manual process imposes a serious bottleneck on the defense capabilities of the network.

On the other hand, anomaly detection [3][6] relies on the existence of normal-operation traffic instances to build a baseline-profile, detecting anomalies as traffic activities that deviate from it. Such an approach permits to detect new kinds of network attacks not seen before, because these will naturally deviate from the constructed baseline. Nevertheless, anomaly detection requires training to construct normal-operation profiles, which is time-consuming and depends on the availability of purely anomaly-free traffic datasets. Labeling traffic as anomaly-free is expensive and hard to achieve in the practice, since it is difficult to guarantee that no anomalies are hidden inside the collected traffic. Additionally, it is not easy to maintain an accurate and up-to-date normal-operation profile, particularly in a dynamic and

evolving context where new services and applications are constantly emerging.

Motivated by the limitations of knowledge-based approaches, a new research area has emerged in the last years, based on a diametrically opposite philosophy for detection of anomalous traffic events: Unsupervised Anomaly Detection. Instead of relying on a previously acquired knowledge on the characteristics of network attacks or on the baseline-traffic behavior, unsupervised detection uses data-mining techniques to extract patterns and uncover similar structures "hidden "in unlabeled traffic of unknown nature (attack or normal operation traffic).

I. DDoS Attacks Detection Problem

With the increased usage of computer networks, security becomes a critical issue. A network intrusion by malicious or unauthorized users can cause severe disruption to networks. Therefore the development of a robust and reliable network intrusion detection system (IDS) is increasingly important. Traditionally, signature based automatic detection methods have been widely used in intrusion detection systems. When an attack is discovered, the associated traffic pattern is recorded and coded as a signature by human experts, and then used to detect malicious traffic. However, signature based methods suffer from their inability to detect new types of attack. Furthermore the database of the signatures is growing as new types of attack are being detected, which may affect the efficiency of the detection.

Other methods have been proposed using machine learning algorithms to train on labelled network data, i.e., with instances pre-classified as being an attack or not [1][4]. These methods can be classified into two categories: misuse detection and anomaly detection. In the misuse detection approach, the machine learning algorithm is trained over the set of labelled data and automatically builds detection models. Thus, the detection models are similar to the signatures described before. Nonetheless these detection methods have the same weakness as the signature based methods in that they are vulnerable against new types of attack. In contrast, anomaly detection approaches build models of normal data and then attempt to detect deviations from the normal model in observed data.

Consequently these algorithms can detect new types of intrusions because these new intrusions, Nevertheless these algorithms require a

set of purely normal data from which they train their model. If the training data contains traces of intrusions, the algorithm may not detect future instances of these attack because it will assume that they are normal.

In most circumstances, labelled data or purely normal data is not readily available since it is time consuming and expensive to manually classify it. Purely normal data is also very hard to obtain in practice, since it is very hard to guarantee that there are no intrusions when we are collecting network traffic.[2] Major advantage of unsupervised detection techniques is that they do not need attack-free training data.

To address these problems, we proposed an unsupervised anomaly detection based on multi-clustering method . It makes two assumptions about the data.

- *Assumption 1* The majority of the network connections are normal traffic. Only X% of traffic are malicious.
- *Assumption 2* The attack traffic is statistically different from normal traffic.

II. Related works

Many recent researches in the last few years have been proposed and presented about "DDoS Detection" domain based on data mining as an efficient way to improve the security of networks, Two different approaches are by far dominant in current research community and commercial detection systems: signature-based detection and anomaly detection. The anomaly detection is supervised Anomaly Detection and Unsupervised Anomaly Detection.

Several researches proposed method in supervised anomaly detection area Yang et al. [8] propose to detect DDoS attacks using decision trees and grey relational analysis. The detection of the attack from the normal situation is viewed as a classification problem. They use 15 attributes, which not only monitor the incoming/outgoing packet/byte rate, but also compile the TCP, SYN, and ACK flag rates, to describe the traffic flow pattern. The decision tree technique is applied to develop a classifier to detect abnormal traffic flow. They also use a novel traffic pattern matching procedure to identify traffic flow similar to the attack flow and to trace back the origin of an attack based on this similarity.

This technique has one advantage and one limitations, Their system could detect DDoS attacks with the false positive ratio about 1.2–2.4%, false negative ratio about 2–10% as an advantage , and find the

attack paths in traceback with the false negative rate 8–12% and false positive rate 12–14% as a limitation . Thw et al.[19] proposed system presents a classification scheme based on extracted features by using UCLA data set. The various packet features which exhibit DDoS attack natures in traffic are extracted from traffic data. Then, a data mining capability based on K-Nearest Neighbor approach combined with the proposed detection algorithm and classification algorithm is developed for attack detection. the system can correctly detect 94.87% for normal traffic and 98.87% for attack traffic. It incorrectly classified traffic in 5.13% for normal class and 1.13% for attack class. Nguyen et al. [3] develop a method for proactive detection of DDoS attacks by classifying the network status. They break a DDoS attack into phases and select features based on an investigation of DDoS attacks. Finally, they apply the k-nearest neighbor (KNN) method to classify the network status in each phase of DDoS attack. **Selvakumar** et al.[9] proposed a DDoS classification algorithm" NFBoost", it differs from the existing methods in weight update distribution strategy, error cost minimization, and ensemble output combination method, but resembles similar in classifier weight assignment and error computation. Their proposed NFBoost algorithm is achieved by combining ensemble of classifier outputs and Neyman Pearson cost minimization strategy, for final classification decision. Publicly available datasets such as KDD Cup, CONFICKER worm, UNINA traffic traces, and UCI Datasets were used for the simulation experiments. NFBoost was trained and tested with the publicly available datasets and their own SSE Lab SSENET 2011 datasets. Detection accuracy and Cost per sample were the two metrics used to analyze the performance of the NFBoost classification algorithm and were compared with bagging, boosting, and AdaBoost algorithms. From the simulation results, it is evident that NFBoost algorithm achieves high detection accuracy (99.2%) with fewer false alarms. Cost per instance is also very less for the NFBoost algorithm compared to the existing algorithms. NFBoost algorithm outperforms the existing ensemble algorithms with a maximum gain of 8.4% and a minimum gain of 1.1%.

This technique has the advantages the detection accuracy is high and the false alarm is fewer .but its limitation come from it use an old public dataset to test their method. , **Karimazad** et al.[16] proposed propose an anomaly-based DDoS detection method based on the

various features of attack packets, obtained from study the incoming network traffic and using of Radial Basis Function (RBF) neural networks to analyze these features. they evaluate the proposed method using their owned simulated network and UCLA Dataset. The results show that the proposed system can make real-time detection accuracy better than 96% for DDoS attacks. This technique has an advantages the system can filter the attack traffics quickly and forward the normal traffics simultaneously. and one limitations as this is shown that the proposed method can successfully identify DDoS attacks but in low detection rates. **Mihui** et al.[11] proposed a combined data mining approach for the DDoS attack detection of the various types, that is composed of the automatic feature selection module by decision tree algorithm and the classifier generation module by neural network. For proving the practical detection performance of their approach, they gathered the real network traffic in the normal case and the attack case. they mounted the most powerful DDoS attack changing attack types, so they could get the attack traffic of various types. this technique has an advantages they used the NetFlow data as the gathering data, because the analysis per flow is useful in the DDoS attack detection. Because the NetFlow provides the abstract information per flow, we don't need the extensive pre-processing, different with the tcpdump . And the limitations they couldn't gather the many attack runs because the DDoS attack could severely affect their network, **Khamruddin** et al.[12] proposed approach routers collectively try to mitigate the DDoS attack on the server. There are three steps in the proposed approach, initially, for attack detection and classification destination router (which is attached to the victim) monitors continuously the traffic pattern. Second, once the attack is detected destination router tries to balance the load using the NAT (Network Address Translator). Third, whenever the attack is detected to mitigate different types of attacks, the signature is pushback to upstream routers so that the upstream routers start monitoring the traffic and apply the mitigation mechanism depending on type of attack detected.

This technique has an advantages they reduce the traffic on the victim machine so that the legitimate users get the services from destination machine.

Other researcher proposed methods in unsupervised anomaly detection:, **Zhong** et al.[13] presents a DDoS attack detection method

based on data mining algorithm. FCM cluster algorithm and Apriority association algorithm used to extracts network traffic method and network packet protocol status method. The threshold is set for detection method , From the analysis of DDoS attacks in the experiment, it is found that this system has a high detection efficiency, the detection rate reach more than 97%.

This technique has an advantages This method could receive the currently normal network traffic method with data mining algorithm. Once network traffic appears abnormal, this method could detect the packets maintaining in abnormal traffic duration. In this way the system load will be greatly reduced and its real-time can be improved. this system is able to effectively detect DDoS attacks in real time, **Lee** et al. [14] propose a method for proactive detection of DDoS attacks by exploiting an architecture consisting of a selection of handlers and agents that communicate, compromise and attack. The method performs cluster analysis. The authors experiment with the DARPA 2000 Intrusion Detection Scenario Specific Dataset to evaluate the method. The results show that each phase of the attack scenario is partitioned well and can detect precursors of a DDoS attack as well as the attack itself, **Meera** et al.[15] alternative clustering approach is presented to perform robust unsupervised detection of attacks. The main idea is to combine the clustering results provided by multiple independent partitions of the same set of flow. The combination of multiple evidence on flow groupings adds robustness to the process of separating malicious from normal operation traffic. Automatic characterization and updating of attacks is used to find out the variation of flow. **Pedro** et al.[16] presented a robust multi-clustering-based detection method and evaluated its ability to detect and characterize standard network attacks without any previous knowledge, using packet traces from two real operational networks. In addition, they have shown detection results that outperform previous proposals for unsupervised detection of attacks, providing more evidence of the feasibility of an accurate knowledge-independent detection system**. Kingsly** et al.[17] proposed approach in unsupervised anomaly detection in the application of network intrusion detection. The new approach, fpMAFIA, is a density-based and grid-based high dimensional clustering algorithm for large data sets. It has the advantage that it can produce clusters of any arbitrary shapes and cover over 95% of the data set with appropriate values of

parameters. they provided a detailed complexity analysis and showed that it scales linearly with the number of records in the data set. They have evaluated the accuracy of the new approach and showed that it achieves a reasonable detection rate while maintaining a low positive rate., **YANG** et al.[18] proposed Another unsupervised detection mechanism is where normal anomaly patterns are built over the network traffic dataset that uses subtractive clustering, and at the same time the built Hidden Markov Method correlates the observation sequences and state transitions to predict the most probable intrusion state sequences. The unsupervised anomaly detection approach proposed in should be capable of reducing false positives by classifying intrusion sequences into different emergency levels, **Cuixiao** et al.[20] a mixed intrusion detection system (IDS) method is designed. First, data is examined by the misuse detection module, then abnormal data detection is examined by anomaly detection module. In this method, the anomaly detection module is built using unsupervised clustering method, and the algorithm is an improved algorithm of K-means clustering algorithm and it is proved to have high detection rate in the anomaly detection module. Other researcher proposed methods in Semi-Supervised Anomaly Detection area . **Hari** et al.[10] presented A hybrid intrusion detection system that combines k-Means and two classifiers: K-nearest neighbor and Naïve Bayes for anomaly detection is presented , The presented method selects the important attributes and removes the irredundant attributes based on entropy based feature selection. This algorithm has been used on the KDD-99 Dataset; the system detects the intrusions and further classify them into four categories: Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L) and probe and the experimental results reduce the false alarm rate. **Palnaty** et al.[21] proposed and developed an algorithm called JCADS. The JCADS works based on the text similarities using Jaccord's Coefficient. Initially the dataset tuples are categorized based on the protocol and service used by the session. Because the attributes are categorical, the method is able to distinguish the protocol, service based clusters.The process improved the classification accuracy at the first stage. In the second stage, value similarities are measured on the Euclidian distance measure to form the clusters. The proposed two stage process, highly improved system to get the high accuracy. The experimental results show that, the use of two stage approach is the best way to cluster the intrusion attacks.

The categorical clustering (semi-supervised),and the numerical distance in two stage clustering process is the essential for the intrusion clustering. The JCADS proved that multi-level attribute clustering improves the accuracy for intrusion detection systems. We conclude that the protocol،and services attribute values plays major role in the clustering process intrusion datasets

III. The Proposed Methodology

1. Data Collection

The real-world DDoS attacks are collected from [23]"The CAIDA DDoS Attack 2012 Dataset". In this data set, the anonymized traffic were included a Distributed Denial of Service (DDoS) attack on August 04, 2012 for one hour time and size 21 GB [23]. Anonymized traffics was collected as DDoS attack traffic to-victim (including the attack traffic) and from-victim (including responses to the attack from the victim). DDoS traces block the victim (target server) by consuming the computing resources on the server and all of the bandwidths of the network connecting the server to the internet. On the other hand, the normal traffic traces are collected from "The CAIDA Anonymized Internet Traces 2014 Dataset". This dataset contains anonymized passive traffic from "Equinix-Chicago' OC192 link [22].

***2. Data Preprocessing*:** We use the datasets from [22] [23],

- Open each data set using Wireshark version 1.10.6.
- convert the dataset to .xlsx to be suitable for rapidminar.
- Merge the datasets according to the parentage of the attacks on the normal dataset in three cases

Cases of experiments

For 20000,5000,10000 dataset record three cases is done as follow:

- Case 1: (10% attacks,90% normal).
- Case 2: (20% attacks,80% normal).
- Case 3: (30% attacks,70% normal).

a summarization of these cases is shown in Table 1,

Tabel.1 **Cases of experiments**

Case #	20000 Record		5000 Record		10000 Record		Output
	Normal 90%	Attack 10%	Normal 80%	Attack 20%	Normal 70%	Attack 30%	
1 (4 Exp)	19000	100	18000	2000	16000	4000	2 custer "attack, or Normal"
2 (4 Exp)	3500	1500	4000	1000	4500	500	
3 (4 Exp)	9000	1000	8000	2000	7000	3000	

a) First case (10% attacks,90% normal)

Dataset used in this case is composed of 20000,5000,10000 profiles, where contained

- 1000 attacks profile and 19000 normal profile .
- 500 attacks profile and 4500 normal profile.
- 1000 attacks profile and 9000 normal profile

Table 2: Experiments results of case 1

Method	20000 Record			5000 Record			10000 Record		
	cluster0	**cluster1**	**Davies Bouldin**	**cluster0**	**cluster1**	**Davies Bouldin**	**cluster0**	**cluster1**	**Davies Bouldin**
KFM	15065	4935	-0.347	3349	1651	-0.252	7144	2856	-0.542
KM	15065	4935	-0.347	3349	1651	-0.252	7144	2856	-0.542
KD	16145	3855	-0.322	4082	918	-0.339	7904	2099	-0.494
MCDDM	16305	3695	-0.356	4120	880	-0.341	7154	2846	-0.551

b) Second case (20% attacks,80% normal)

Dataset used in this case is composed of 20000,5000,10000 profiles, where contained

- 200 attacks profile and 18000 normal profile .
- 1000 attacks profile and 4000 normal profile.
- 2000 attacks profile and 8000 normal profile

Table 3 Experiments results of case 2

Method	20000 Record			5000 Record			10000 Record		
	cluster 0	cluster 1	Davies Bouldin	cluster 0	cluster 1	Davies Bouldin	cluster 0	cluster 1	Davies Bouldin
KFM	15388	4612	-0.441	3639	1361	-0.301	7451	2549	-0.565
KM	15388	4612	-0.441	3639	1361	-0.301	7451	2549	-0.565
KD	16420	3580	-0.387	4082	918	-0.339	7073	2927	-0.544
MCDDM	15400	4600	-0.443	4237	703	-0.342	7466	2534	-0.570

c) Third case (30% attacks,70% normal)

Dataset used in this case is composed of 20000,5000,10000 profiles, where contained

- 4000 attacks profile and 16000 normal profile .
- 1500 attacks profile and 3500 normal profile.
- 3000 attacks profile and 7000 normal profile .

Table 4 Experiments results of case 3

Method	20000 Record			5000 Record			10000 Record		
	cluster 0	cluster 1	Davies Bouldin	cluster 0	cluster 1	Davies Bouldin	cluster 0	cluster 1	Davies Bouldin
KFM	15908	4092	-0.336	3893	1107	-0.315	8086	1910	-0.634
KM	15908	4092	-0.336	3893	1107	-0.315	8086	1910	-0.634
KD	16960	3040	-0.312	4142	858	-0.342	8195	1805	-0.644
MCDDM	15922	4078	-0.339	4342	658	-0.355	8174	2856	-0.666

4. Detecting DDoS Attack Using A Multilayer Data Mining techniques "MCDDM" (The Our Proposed Method)

The main objective of this research is to propose a new method of DDoS detection. To achieve this, we used combination of clusters as integration to be able to adapt with new DDoS attacks , and to achieve better Davies–Bouldin index.

Also, we try to overcome the drawbacks of the existing methods used in previous and related researches. For that, we propose "MCDDM" methods for DDoS detection based on multi clustering to detect new DDoS attacks from unlabeled data.

To achieve the objective of this research, we propose the following steps shown in Figure 1:

Step I: Collecting datasets normal dataset and DDoS attacks dataset .

Step II: Merge datasets according to attacks percentage , The purpose of this merger is to evaluate the performance of "MCDDM" methods .

Step III: For each case, we apply the "MCDDM" methods as follows :

a) Apply K-mean cluster in the first step to build KM method , and tested it. This step will produce output (cluster 1,cluster 0) (attacks/normal)
b) Apply K-fast Mean cluster in the second step on the same dataset to build KFM method , and tested it , this step will produce output (cluster 1,cluster 0) (attacks /normal).
c) Apply K-Mididod cluster in the second step on the same dataset to build KD method , and tested it , this step will produce output (cluster 1,cluster 0) (attacks /normal).

Step IV: We combined the three outputs from previous steps to generate the final output for all methods .

Step V: Extraction results to evaluate clusters performance by using the final Davies–Bouldin index .

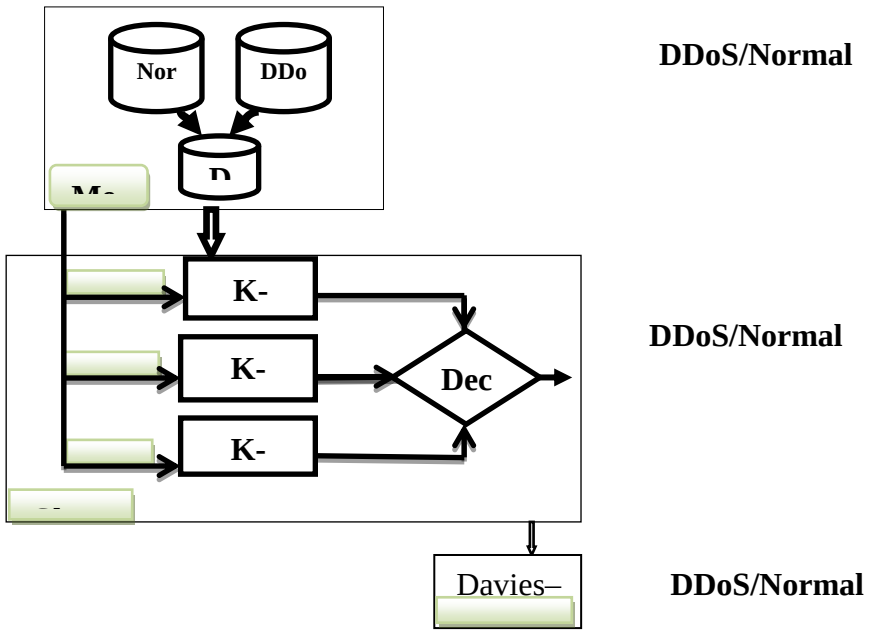

Figure 1: General view of "MCDDM" method

5. Evaluate the "MCDDM" method

Performance evaluation of the "MCDDM" model is one of the most important tasks in our research. When a clustering result is evaluated based on the data that was clustered itself, this is called internal evaluation. These methods usually assign the best score to the algorithm that produces clusters with high similarity within a cluster and low similarity between clusters. One drawback of using internal criteria in cluster evaluation is that high scores on an internal measure do not necessarily result in effective information retrieval applications.[14] we use davies_bouldin index that the commonly evaluation measures for clustering method that can be defind as follow:

Davies_Bouldin Index **:** The algorithms that produce clusters with low intra-cluster distances (high intra-cluster similarity) and high inter-cluster distances (low inter-cluster similarity) will have a low Davies–Bouldin index, the clustering algorithm that produces a collection of

clusters with the smallest Davies–Bouldin index is considered the best algorithm based on this criterion.

The Davies–Bouldin index can be calculated by the following formula:

$$DB = \frac{1}{n}\sum_{i=1}^{n} \max_{i \neq j} \left(\frac{\sigma_i + \sigma_j}{d(c_i, c_j)} \right)$$

where n is the number of clusters, c_x is the centroid of cluster x, σ_x is the average distance of all elements in cluster x to centroid c_x, and $d(c_i, c_j)$ is the distance between centroids c_i and c_j. Since algorithms that produce clusters with low intra-cluster distances (high intra-cluster similarity) and high inter-cluster distances (low inter-cluster similarity) will have a low Davies–Bouldin index, the clustering algorithm that produces a collection of clusters with the smallest Davies–Bouldin index is considered the best algorithm based on this criterion.[24] Because the objective of the Davies-Bouldin index and its derivatives is to be minimized, a high negative value indicates a good performance of the index. Those values which are highlighted indicate when the Davies-Bouldin index had the best performance.[24]

6. Experimental Results and Evaluation

We apply sets of experiments scenarios on case 1, 2, and 3 of data sets, the details about these experiments and their result that have achieved presented and explained in this section.

7.Experiment Scenarios and Results

we apply a set of experiments on 3 cases of data sets presented in section 2. In first experiments set, our method is applied on data sets contain 10% DDoS attacks and 90% normal . In second experiments set, the "MCDDM" method is applied on data set contain 20% DDoS attacks and 80% normal. In last experiments set, the "MCDDM" method is applied on data set contain 20% DDoS attacks and 80% normal. The details of these experiments is explained as follows:

a) Experiment Scenario I (10% attacks 90%normal)

In this experiment the datasets is merging as 10 % attacks and 90% normal and the clusters method , we perform 4 experimentation ,Table 5.1 and Figure 2 illustrates experiments results in this case, which show that "MCDDM" method has achieved the best lowest Davies–Bouldin index.

Table 3: Experiments results of case 1

Method	Davies–Bouldin index		
	20000 Record	5000 Record	10000 Record
KFM	-0.347	-0.252	-0.542
KM	-0.347	-0.252	-0.542
KD	-0.322	-0.243	-0.494
MCDDM	-0.356	-0.274	-0.551

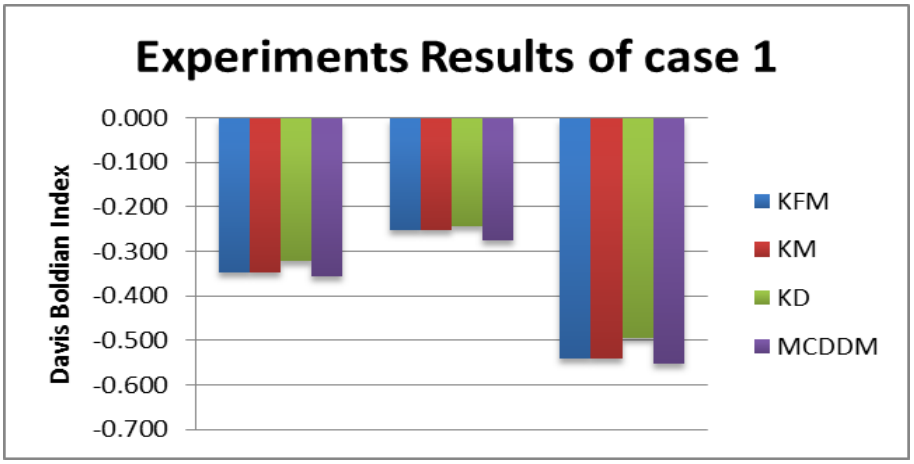

Figure 2: Experiments Results of case 1

b) Experiment Scenario II (20% attacks 80%normal)

In this experiment the datasets is merging as 20 % attacks and 80% normal and the clusters method , we perform 12 experimentation ,Table 4 and Figure 3 illustrates experiments results in this case, which show that "MCDDM" method has achieved the best lowest Davies–Bouldin index.

Table 4: Experiments results of case 2

Method	Davies–Bouldin index		
	20000 Record	5000 Record	10000 Record
KFM	-0.441	-0.301	-0.565
KM	-0.441	-0.301	-0.565
KD	-0.387	-0.339	-0.544

MCDDM	-0.443	-0.342	-0.570

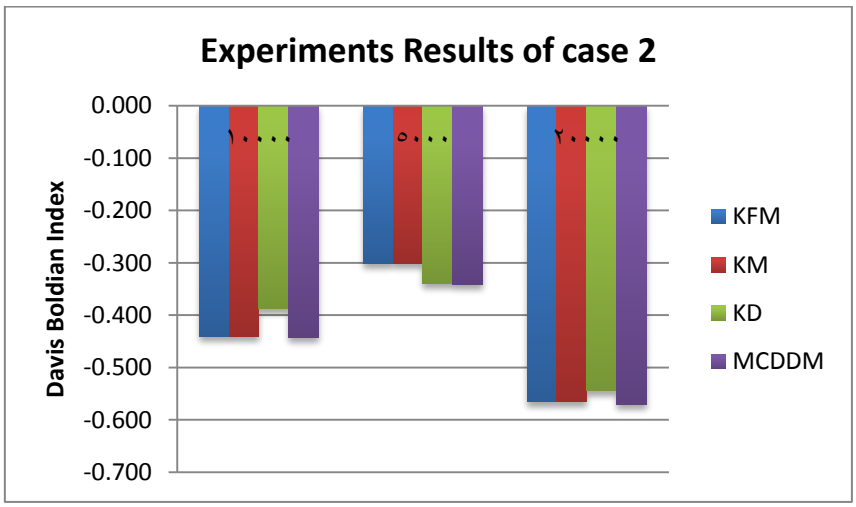

Figure 3: Experiments Results of case 2

c) Experiment Scenario III (30% attacks 70%normal)

In this experiment the datasets is merging as 30 % attacks and 70% normal and the clusters method , we perform 12 experimentation ,Table 5 and Figure 4 illustrates experiments results in this case, which show that "MCDDM" method has achieved the best lowest Davies–Bouldin index.

Table 5: Experiments results of case 3

Method	Davies–Bouldin index		
	20000 Record	5000 Record	10000 Record
KFM	-0.336	-0.315	-0.634
KM	-0.336	-0.315	-0.634
KD	-0.312	-0.342	-0.644
MCDDM	-0.339	-0.355	-0.666

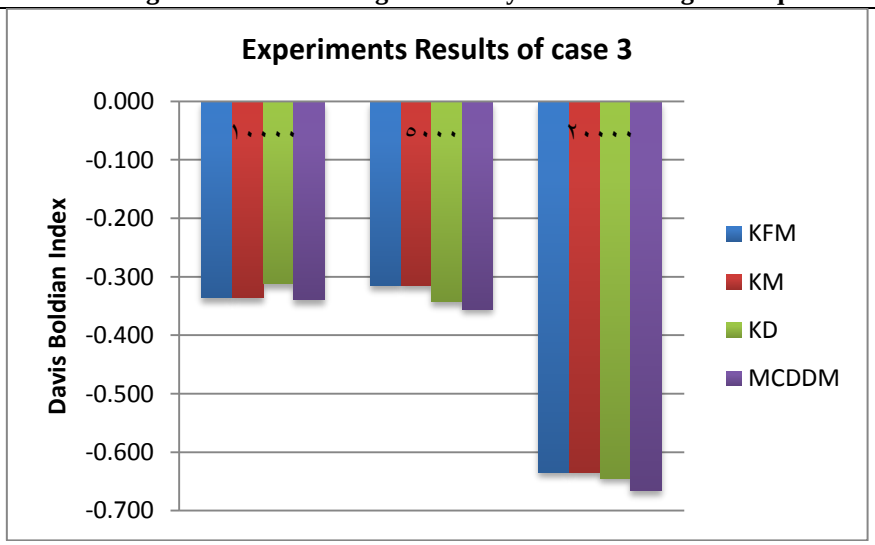

Figure 4: Experiments Results of case 3

We can summarize our experiments results as follows:

a) The experiments on datasets of case 1 achieved the lowest Davies–Bouldin index(-0.374), were in our method.
b) The experiments on datasets of case 2 achieved the lowest Davies–Bouldin index(-0.570), were in our method.
c) The experiments on datasets of case 3 achieved the lowest Davies–Bouldin index(-0.666), were in our model.
d) In general, we can say that our model has achieved good results from the all experiments on datasets of case 1, 2, and 3 where lowest Davies–Bouldin index was (-0.666)

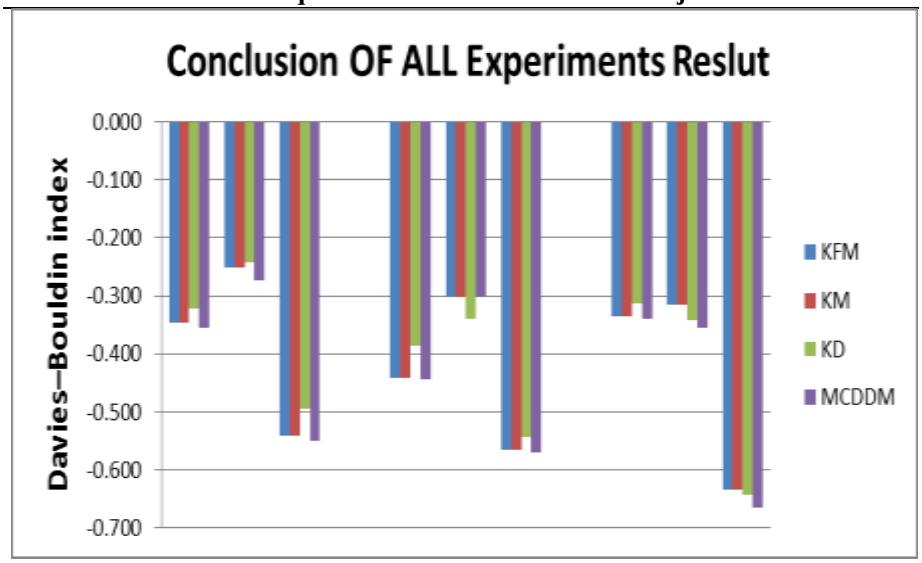

Figure 5: All Experiments Results

IV. Conclusion and Future work

We proposed method which is an adaptive method based on multi clustering that able to be detecting DDoS attacks. The purpose of used multi clustering was to obtain reduce Davies–Bouldin index to evaluate "MCDDM" method, as shown in figure 5 We can concluded that "MCDDM" method achieved the best results for performance measurements which are Davies–Bouldin index

V. Future Work Directions:

The future work direction of this dissertation can be summarized on the following points:

- Evaluate the proposed method with other attacks such as (DoS, Worm).
- Try to build method by a hyper of clustering methods and classification method to build the method to detect DDoS attacks.

References

Cuixiao Z ; Guobing Z ; Shanshan S," A Mixed Unsupervised Clustering-based Intrusion Detection Method ",3rd International Conference on DOI: 10.1109/WGEC.2009.72, 2009 .

David, Z.," Peer to peer botnet detection based on flow intervals and fast flux network capture". MSc Thesis, University of Victoria, Heritage, Canada.2012.

Hari, O. and K. Aritra." A hybrid system for reducing the false alarm rate of anomaly intrusion detection system". Proc, the 1st International Conference on Recent Advances in Information Technology, 2012.

Javitz, H. S. & Vadles, A. (1993), The NIDES statistical component: Description and justification Technical report, SRI International.

Khamruddin Md, Rupa Ch. "A Rule Based DDoS Detection and Mitigation Technique", NIRMA UNIVERSITY INTERNATIONAL CONFERENCE ON ENGINEERING, NUiCONE,2012.

Kingsly L.," Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters", NICTA Victoria Laboratory Department of Computer Science and Software Engineering The University of Melbourne,2005.

Lee, K., Kim, J., Kwon, K. H., Han, Y., and Kim,S, " DDoS attack detection method using cluster analysis. Expert Systems with Applications", 2008.

Lee, W. & Stolfo, S. (1998), Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX.

Lemos, R.." Web worm targets white house", 2001. CNET News. http://news.cnet.com/2100-1001-270272.html.

McCue, A. "Revenge' hack downed US port systems",. 2003. ZD- Net News. http://www.zdnet.co.uk/news/security-management/2003/10/07/revenge-hack-downed-us-port-systems-39116978/.

Meera R ," Detection & Deletion of DDOS Attacks Using Multi-clustering Algorithm",2014.

Mihui K. and Hyunjung H, "A Combined Data Mining Approach for DDoS Attack Detection",2008.

Nguyen, H.-V. and Choi, Y(2010)." Proactive detection of DDoS attacks utilizing k-NN classifier in an Anti- DDoS framework", International Journal of Electrical,Computer, and Systems Engineering, 4, 247–252, 2010.

Palnaty, R.P.; Rao, a. "JCADS: Semi-supervised clustering algorithm for network anomaly intrusion detection systems", Advanced

Computing Technologies (ICACT), 15th International Conference on, On page(s): 1 – 5,2013.

Pedro H, Johan M, Philippe O. "Unsupervised Network Intrusion Detection Systems: Detecting the Unknown without Knowledge.", Computer Communications, Elsevier, 2012.

Selvakumar S. and Arun Raj Kumar P.," Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems",Computer Communications Jornal, Volume 36 Issue 3, February, Pages 303-319,2013.

Source: http://en.wikipedia.org/wiki/Intrusion_detection_system, (2013, December), [Online].

Thw T, Thandra P," Analysis of DDoS Detection System based on Anomaly Detection System", International Conference on Advances in Engineering and Technology (ICAET'2014) March 29-30, 2014.

Tseng, H. R., Yang, W., and Jan, R. H. "DDoS detection and traceback with decision tree and grey relational analysis", International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136,2011.

YANG, C., DENG, F., YANG, H.," An Unsupervised Anomaly Detection Approach using Subtractive Clustering and Hidden Markov Method". Communications and Networking in China, 2007. CHINACOM '07. Second International Conference on , vol., no., pp.313-316, 22-24 Aug. 2007.

Zhong , Yue." DDoS Detection System Based on Data Mining", Proc.the Second International Symposium on Networking and Network Security,2010.

http://www.caida.org/data/passive/passive_2013_dataset.xml

http://www.caida.org/data/passive/ddos-20130804_dataset.xml.

Carlos J., Thomas R.," New Version of Davies-Bouldin Index for Clustering Validation Based on Cylindrical Distance", in Proc. Chilean Computer Conference 2013.