Journal of Computer Science 10 (10): 2037-2046, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.2037.2046 Published Online 10 (10) 2014 (http://www.thescipub.com/jcs.toc)

REVIEW CLUSTERING MECHANISMS OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

Wesam Bhaya and Mehdi Ebady Manaa

College of Information Technology, University of Babylon, Babylon, Iraq

Received 2014-03-15; Revised 2014-05-03; Accepted 2014-06-26

ABSTRACT

Distributed Denial of Service attacks (DDoS) overwhelm network resources with useless or harmful packets and prevent normal users from accessing these network resources. These attacks jeopardize the confidentiality, privacy and integrity of information on the internet. Since it is very difficult to set any predefined rules to correctly identify genuine network traffic, an anomaly-based Intrusion Detection System (IDS) for network security is commonly used to detect and prevent new DDoS attacks. Data mining methods can be used in intrusion detection systems, such as clustering k-means, artificial neural network. Since the clustering methods can be used to aggregate similar objects, they can detect DDoS attacks to reduce false-positive rates. In this study, a review of DDoS attacks using clustering data mining techniques is presented. A review illustrates the most recent, state-of-the art science for clustering techniques to detect DDoS attacks.

Keywords: Network Security, Distributed Denial of Service (DDoS), Data Mining

1. INTRODUCTION

Information has become an organization's most precious asset upon which they have increasingly become dependent. The widespread use of e-commerce has increased the necessity of protecting the system to a very high extent (Kiran, 2008).

DDoS attacks have become a hot research topic, because they can lead to a loss of confidence and privacy and could lead to illegal actions taken against an organization. DDoS attacks make use of many different hosts that compromised by the attacker to send useless packets to the target in a short time, which may consume the target's resources, making them unavailable for normal operations (Jieren *et al*., 2009).

This attack is one of the main threats that the internet is facing which causes corrupted for information and loss of data integrity, confidentiallity and avaliability for organizations. Hence, losing any factor of security criteria Confidentially, Integrity and Availability (CIA) can cause significant harm in business for the organization assets such as loss customer confidence, contract damages, regulatory fines and restrictions, or a reduction in market reputation. In the worst case, a failure to control or protect information could lead to significant financial losses or regulatory restrictions on the ability to conduct business. The detection of intrusion on information stored in networks is increasingly as crucial aspect of system defense and for this reason the intrusion detection has become an integral part of the information security process (Kiran, 2008).

There are two general approaches in intrusion detection: Misuse Intrusion Detection (MID) or signature-based and Anomaly Intrusion Detection (AID). Misuse detection is based on the pattern matching to hunt for signature detection from known attacks. However, AID construction the normal usage behavior profile, named historical or long-term behavior profile from the network traffic which use later for attack possibility detection (Jun and Ming, 2005). The summarization of the DDoS attack based on Intrusion Detection System (IDS) is illustrated in **Fig. 1**.

Corresponding Author: Wesam Bhaya, College of Information Technology, University of Babylon, Babylon, Iraq

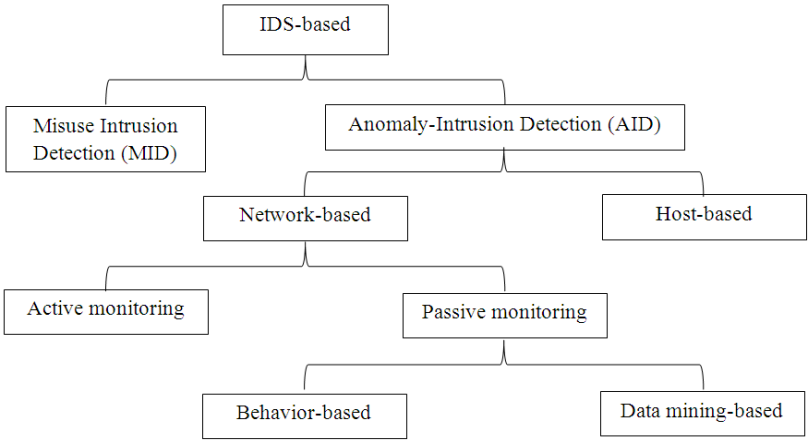

Fig. 1. Summarization of DDoS attack detection strategies

Data mining approach comes to help into DDoS detection. Since, this approach is working well on extracting wide range of features from the network flow; It could be used in the process of distinguishing attack traffic from the common legitimate traffic.

In this study, a review of DDoS attack detection clustering mechanisms is presented to illustrate the last art-of-science techniques and studying their performance criteria to detect such attack. The reminder of this study is as follow. Section 2 discusses the theoretic review of DDoS attack and architecture. Section 3 focuses on classification of DDoS attack. Section 4 discusses the characteristics and literature reviews of DDoS attacks. Performance comparison based on clustering methods is discussed in section 5 and section 6 is illustrated the other detection methods.

2. DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

Distributed Denial of Service attack (DDoS) is one of the main threats that the internet is facing and the defence of this attacks has become a hot research topic. The DDoS attack makes use of many compromised hosts to send a lot of useless packets to the target in short time of invalid access which will consume the target's resources and causes outage of server operation (Junaid *et al*., 2013).

These kinds of attacks have posed an immense threat to the internet. Many researchers have been developing to detect this kind of attack which results in not only the advance of network security system, but also constantly attack tools improved adept attackers in order to evade these security mechanisms (David, 2012).

DDoS attack is considered the worst one in the Internet where multiple of compromised computers are being used. These computers are called zombies. **Figure 2** below illustrates architecture of DDOS attack.

In a hierarchical scheme of **Fig. 2**, an attacker performs the following steps by (Keunsoo *et al*., 2007):

- The attacker indirectly achieves access for the agents through the handlers. Handlers are chosen in the first step by the attacker which has security vulnerabilities and intrude them by gaining access right
- The attacker chooses network-handlers and agents as many as possible
- network-connected systems (handlers and agents) are located outside the victim's and attacker's network
- The attacker is compromised hosts by scanning the hosts which have security vulnerabilities to install attack type in a specific attack time. ICMP is usually used in this step
- The function of agents is sending a large number of useless packets to a victim simultaneously. The agents generate some types of DDoS attack traffic among TCP, UDP and ICMP types
- The victim or related network is jeopardized and the service availability is shutdown under some types of DDoS attack heading to this victim
- In most times, the attacker uses spoofing IP and random port to attack the victim, which causes the difficulty of attacker detection using indirect architecture as shown in **Fig. 2**

In addition to all steps, the DDoS attack is easier to carry out with genuine packets, more harmful, hard to be traced due to attacker spoofed IP and difficult to prevent and its threat is more serious (Keunsoo *et al*., 2007).

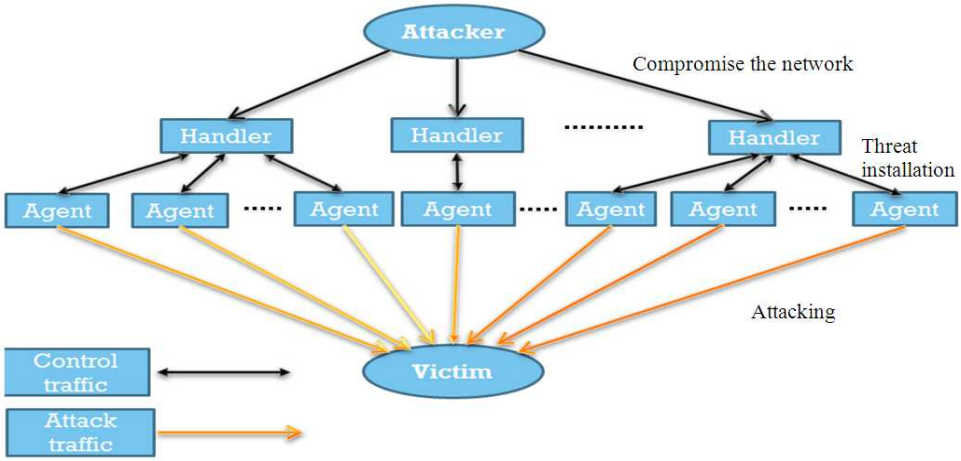

Fig. 2. Architecture of Distributed Denial of Service (DDoS) attack

3. CLASSIFICATION OF DDOS ATTACK

There is no general DDoS classification model because there is no theory of DDoS attack.Some researchers are classified DDoS attack in a broadly scheme as below (Ghazali and Rosilah, 2011; Sung-Ju *et al*., 2013).

3.1. Attack on Bandwidth

UDP/ICMP flooding attacks, which makes the network link congestion or overloading by sending a lot of UDP/ICMP and SYN-flooding packets. Mehdi and Angela (2012) is illustrated the main detection schemes of SYN-flooding attack.

Distributed Reflected Denial of Service (DRDoS), it sends a large number of forged requests to large number of computer using spoofing of Internet Protocol (IP) address. All replies to these requests will send to the targeted victim such as an organization server.

3.2. Attack of Host Resource

These attacks are used to slow the service availability on the web server. It tries to keep many connections to the target web server open and hold them as long as possible and some other attacks of this kind send a large amount of requests to the victims' website to disable it. Some types are Slowlories DoS HTTP and HTTP GET Flooding attack. In HTTP Flooding attack, the attacker sends a large number of HTTP flood attack simultaneously from multiple computers (bots machines). This attack repeatedly request to download the target site's pages (HTTP GET flood) and resulting in denial of service condition.

3.3. Attack on System/Application Weakness

Ping of Death is one kind of this type which can cripple network resources based on a flaw in the TCP/ IP suite. The maximum size for a packet is 65, 535 bytes. If one sender were to send a packet larger than this size, the receiving computer would ultimately crash from confusion.

In the **Table 1** below, some types of early (D) DoS attacks anonymous is illustrated from the year 1998-2012 (Radware, 2013).

According to (Radware, 2013), the attack type's evolution toward the target is classified in 2011 as 56% of cyber-attacks were targeted at applications; 46% at the network. **Figure 3** illustrates this classification.

4. CLUSTERING WORK ON DDOS METHODS

Data mining is the discovery of models for data. A model, however, can be of these models (Anand and Jeffrey, 2012):

- Statistical model: It attempts to extract information that was not supported by the data
- Machine-learning models: It uses the data as a training set, to train an algorithm of one of the many types used by machine-learning algorithms, such as Bayes nets, support-vector machines, decision trees, hidden, Markov models and many others

Data mining clustering is the unsupervised technique that uses to group together the similar items to extract new knowledge from a largely data set. Clustering technqiue is separating dissimilar items according to some defined dissimilarity measure among data items themselves.

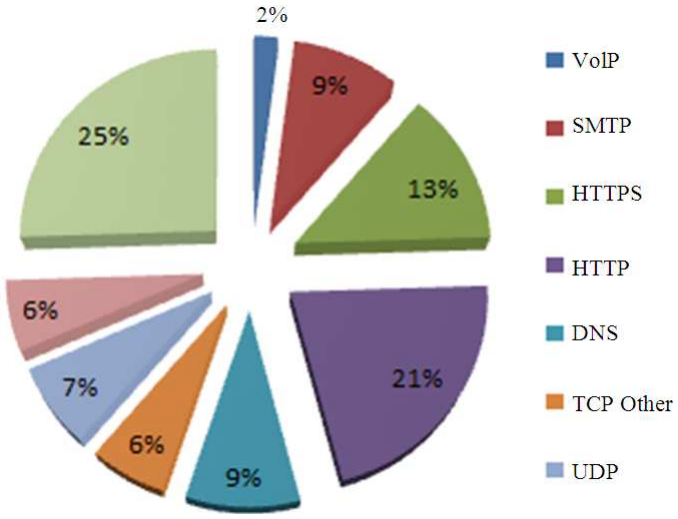

Fig. 3. DDoS attack classification based on applications percentage

Table 1. The history of anonymous DDoS attack

	Timeline		
Item no.	Time stage	years	Description
1.	Early days	1988	Morris worm, AOL's punters
2.		1996	First SYN flood
3.		1997-1998	Smurf attacks; First DDoS tools-Teardrop, Boink, Bonk, WinNuke
4.		1999	Trinoo, Tribe Flood Network, Stacheldraht, Shaft University of Minnesota taken down
5.	Democratization of DoS tools	2000	FBI site taken down, Seattle's Oz.net down, Attacks on eBay, Yahoo, Etrade, Buy.com, Amazon, Excite.com, CNN
6.		2002	Attack on Internet's DNS Root servers Dos reflected tools
7.	Political agenda and criminal extortion	2003	MyDoom attacks 1M computers, Attacks on ClickBank and Spamcop, Worm blaster, Attack on Al-Jazeera website during Iraq war
8.		2007	Attacks on Estonia Attacks on online game servers
9.		2008	Attacks on Georgian government sites
10.		2009	Attacks on UltraDNS, Register.com, the Pirate Bay
11.		2009	Attacks South Korean and American websites + Washington Post, NYSE
12.		2009	Attacks on Iranian Government websites
13.	Hacktivists, the	2009	Attacks on Facebook, Twitter, Google
14.	rise of anonymous	2010	Operation Payback, Avenge Wikileaks' Assange
15.		2011-2012	Operation Tunisia, Operation Sony, Operation Syria, Operation MegaUpload, Operation Russia, Operation India, Operation Japan

Clustering algorithms are classified in five main categories (Jiawei and Micheline, 2006), see the **Fig. 4.**

The hierarchical clustering are methods start with each point in its own cluster. Clusters are combined based on their closeness, using one of many possible definitions of "close."

The partitioning clustering are methods involve point assignment. Initial points are chosen randomly or in some order and each point in a state space is assigned to the cluster into which it best fits based on similirty distacne. On the other hand, Statistics model-based methods attempt to find the best fit of the data to the hypnosis model that was not supported by the data.

The density-based methods are developed based on the notation of density. The key idea is to continue growing the given cluster as long as the density (the number of objects or data points) in the "neighborhood" exceeds some threshold.

The Grid-based methods are performed in a fast processing time, where the object space quantizes into a

finite number of cells that form a grid structure (on the quantized space).

Table 2-5 are described the main characteristics of the partitioning, hierarchical, density-based and Grid-based clustering methods. The main characteristics are briefly defined in these tables. More details for input parameters and other characteristics are mentioned in (Jiawei and Micheline, 2006).

The problem of detection malicious network traffic and promptly trigger alerts such as DDoS attacks has been widely studied in the last decade and is still of high interest. Data mining algorithms have been developed to detect the DDoS attacks using classification and clustering algorithms. In the following sub-sections, we provide a literature review of the main schemes that use the data mining algorithms in detection of DDoS attacks.

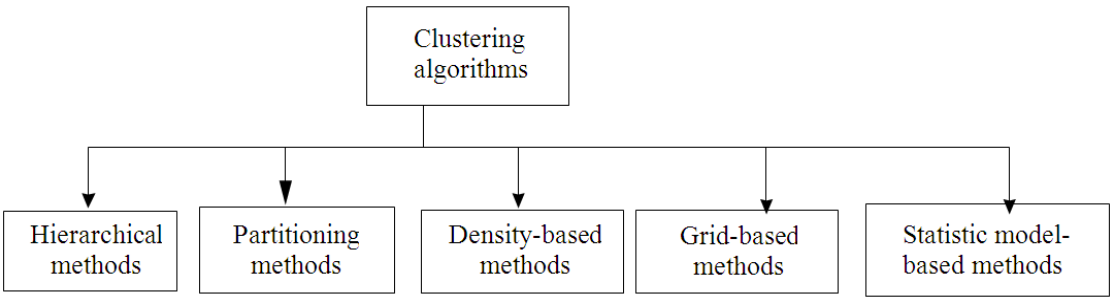

Fig. 4. Main categories of clustering data mining algorithms

Table 2. Characteristics of partitional clustering algorithm

Clustering method	Data type	Complexity	Geometry	Outliers, noise	Input parameters	Outputs
k-mean	Numerical	O(nkt)[a]	spherical-shaped clusters	No	K and data	Center of clusters, where K≤n
k-mediod	Categorical	O(n)	Non- convex shapes	No	K and data	Modes of clusters
PAM[b]	Numerical	O (k (n −k)^2)	Non- convex shapes	No	K and data	Medoids of clusters
CLARA[c]	Numerical	O (ks^2+k (n-k))	Non- convex shapes	No	K	Medoids of clusters
CLARANS[d]	Numerical	O (n^2)	Non- convex shapes	No	(maxneighbor) and (numlocal)	Medoids of clusters

[a](nk) are the total number of objects and the total number of cluster respectively
[b](PAM): Partitioning around medoids
[c](CLARA): Clustering large applications
[d](CLARANS): Clustering Large Applications based on Randomized search
[e](maxneighborand numlocal) are themaximum number of neighbors examined and the number of local minima obtained respectively

Table 3. Characteristics of hierarchical clustering algorithm

Method	Data Type	Complexity	Geometry	Outliers, noise	Input parameters	Outputs
BIRCH[f]	Numerical	O(n)	spherical- shaped clusters	Yes	Radius of clusters, branching factor	CF = (number of points in the cluster N, linear sum of the points in the cluster LS, the square sum of N data SS) points
ROCK[g]	Categorical	O(n^2+nm$_m$m$_a$ +n^{2}logn)[h]	Arbitrary shapes	Yes	No. of clusters	Assignment of data values to clusters
CURE[i]	Numerical	O(n^{2}logn)	Arbitrary shapes	Yes	No. of clusters, number of clusters representatives	Assignment of data values to clusters

[f](BIRCH): Balanced Iterative Reducing and Clustering Using Hierarchies
[g](ROCK): Robust Clustering using links)
[h]M$_m$ and m$_a$ are the maximum and average number of neighbors, respectively and n is the number of objects
[i](CURE): (Clustering Using Representative)

Table 4. Characteristics of density clustering algorithm

Method	Data type	Complexity	Geometry	Outliers, noise	Input parameters	Outputs
DBSCAN[j]	Numerical	O(nlogn)	Arbitrary shapes	Yes	Cluster radius ε, minimum number of objects ξ	Assignment of data values to clusters
OPTICS	Numerical	O(nlogn)	Arbitrary shapes	Yes	smallest cluster radius ε, minimum number of objects ξ	Assignment of data values to clusters
DENCLUE[k]	Numerical	O(nlogn)	Arbitrary shapes	Yes	Cluster radius σ, minimum number of objects ξ	Assignment of data values to clusters

[j](DBSCAN): (Density-based spatial clustering of applications with noise)
[k](DENCLUE): DENsity-based clustering

Table 5. Characteristics of grid-based clustering algorithm

Method	Data type	Complexity	Geometry	Outliers, noise	Input parameters	Outputs
Wave-cluster	Special data	O(n)	Arbitrary shapes	Yes	Wavelets, the number of grid cells for each dimension, the number of application of wavelet transform	Clustered objects
STING (statistical information grid)	Special data	O(K)	Arbitrary shapes	Yes	Number of objects in a cell	Clustered objects

4.1. Detection Using Data Mining Statistics-Based Methods

A model based on the multiple principal component analysis is proposed by (Sangjae *et al*., 2011). The profiling of normal web browsing behaviors and its reconstruction error is used as a criterion for detecting DDoS attacks. The proposed method is experimentally confirmed with various types of new App-DDoS attacks.

David (2012) stated in his thesis two different strategies, in one, network flow is examined based on metrics of potential botnet traffic and it shows the detection results of botnets with only data from a small time interval of operation. For the second technique, a similar strategy to identify botnets based on their potential fast flux behavior is presented. The obtained results show a good percent to detect DDoS attack.

In the network misbehavior DDoS detection packets using statistical method, (Maryam *et al*., 2011) exploits some statistical method features for the incoming traffic and design a system based on statistic-based method using entropy to decide whether the attack is occurred. The simulation results show that the proposed method can detect DDoS attacks efficiently.

4.2. Detection Using Hierarchical Clustering Methods

Researches of hierarchical clustering method are limited to detect and classify the DDoS attacks. Taxonomy is needed to identify and classify existing attacks tools and their late editions and should be scalable to deal with new attacks.

Jian *et al*. (2006) proposed a novel and abstract method for describing DDoS attacks with the characteristic tree, tree-tuple and introduced an original, formalized taxonomy based in similarity and hierarchical clustering method. The tests and evaluations of this method have performed in a serious of experiments with 12 real DDoS attack tools and calculate the similarities between new attack class and each of the old class. This study can be used as an automated plug-in tool to aid in rapid response to DDoS attack.

Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm is proposed by (Mansouri *et al*., 2013). To preserve the energy consumption in WSN nodes, an energy-preserving solution to detect compromised nodes in WSN is introduced to analyzes the traffic inside a cluster and sends warning to the cluster heads whenever abnormal behavior is detected in Wireless Sensor Network (WSN) environment. This solution is used to mitigate the DoS attack which causes the degradation in the overall Quality of Service (QoS). The proposed method is dynamic as the Cnode are periodically elected among ordinary on each atomic cluster.

Yu *et al*. (2007) reported a Distributed Change-point Detection (DCD) architecture using Change Aggregation Trees (CAT). Abrupt traffic changes

across multiple network domains at the earliest time are detected. Early detection of DDoS attacks minimizes the flooding damages to the victim systems serviced by the provider. The system is built over attack-transit routers, which work together cooperatively. The results show 98% detection accuracy with only 1% false-positive alarms.

Ward's minimum variance method is employed as a hierarchic linkage rule to detect the DDoS attack by (Keunsoo *et al*., 2007). The proposed method consists of further two main steps; the first step is using entropy to find useful detection parameters which is commonly used to extract these parameters. In the second step, the cluster analysis is used to detect the DDoS attack phases. The results show each phase of the attack scenario is partitioned well. Furthermore, an entropy-based approach is used also in detection of DDoS attack in IEEE 802.16 based network as shown in (Maryam *et al*., 2011).

4.3. Detection Using Data Mining Partitioning clustering Methods

Adopting unsupervised clustering techniques using k-means clustering which distinguishes normal traffic behavior from malicious network activity has been proposed by (Walter *et al*., 2009). The proposed method shows the effectiveness in performance in a test-bed web server under several attacks techniques.

A hybrid intrusion detection system that combines k-Means and two classifiers: K-nearest neighbor and Naïve Bayes for anomaly detection is presented by (Hari and Aritra, 2012). 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 Data set; 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.

Analyzing the fundamental features of DDoS attack is an important task to find the relevant features to detect of such attacks. Chi-Square and information gain feature selection mechanisms for selection the important attributes is proposed by (Manjula *et al*., 2011). Navies Bayes, C4.5, SVM, KNN, K-means and Fuzzy c-means clustering are developed for efficient detection of the selected attributes to detect DDoS attacks. The results show that the Fuzzy c-means clustering gives better accuracy in identifying the attacks.

Development of alert classification system to classify False Positive and True Positive related to DDoS using Fuzzy Inference System (FIS) is proposed by (Subbulakshmi *et al*., 2010). FIS is help in eliminating the false positive.

To overcome the supervised strategies using the signature-based detection or supervised-learning techniques, an unsupervised approach using DBSCAN to detect and characterize network anomalies, without relying on signature, statistical training, or labeled traffic is introduced by (Johan *et al*., 2011). Detection and characterization performance of the unsupervised approach is extensively evaluated with real traffic from two different data-sets.

Many researchers have been developed to detect DDoS attacks using the clustering methods such as k-means on wireless WAN. Vishal *et al*. (2012) adopted new solution for security against DDoS in enterprises and campuses by using clustering techniques in wireless traffic dataset for detection CTS-based DoS attacks in 802.11 WLANs. The k-means clustering technique is able to achieve high detection rates and low false positive rates.

On the other hand, a hybrid technique that is combination of both entropy of network features and support vector machine is compared with individual methods is adopted by (Basant and Namita, 2012). DARPA intrusion detection evaluation dataset is used in order to evaluate the methods. Anomalies is detected by using entropy which capable of identifying attacks in network in good results.

5. THE PERFORMANCE COMPARISON OF DDOS ATTACK USING CLUSTERING METHODS

In this section, performance evaluation is illustrated regarding the CPU Time, memory consumption, False Positive (FP), False Negative (FN) and accuracy detection based on the reviewing and studding of these algorithms. The behavior of DDoS attack is varied from one phase (attack time) to final phase (shut down of victim's resources). The comparison in **Table 6** is important when the adopting of DDoS avoidance strategy in real time is required.

Table 6. Performance comparison of clustering method

Category	Method	CPU Time	Memory Consumption	FP	FN	Accuracy Detection	Limitation
Partitional methods	k-means	Flexible	Flexible	High	High	Flexible	sensitive to shape and outliers of clusters
	k-Mediod	Low	Low	High	High	Flexible (for some type of data)	Sensitive to cluster shape and outlier
	PAM	Low	Low	Flexible	Flexible	Flexible (for small data set)	Sensitive to cluster shape and outlier
	CLARA	Low	Low	Flexible	Flexible	Flexible (for large data set)	Sensitive to cluster shape and outlier
	CLARANS	High	Flexible	Low	Low	High	Sensitive to cluster shape and outlier
Hierarchical	BIRCH	Flexible	utilizes storage efficiently	Low	Low	High	Sensitive to shape cluster
methods	ROCK	High	Flexible	Low	Low	High	Sensitive to shape cluster
	CURE	High	High	Low	Low	Excellent	Ignore cluster interconnectivity
	Chameleon	Flexible	High (for large data scale)	Low	Low	Excellent	NA
Density-based methods	DBSCAN	Flexible	Flexible	Low	Low	Excellent Sensitive to	Cluster radius ε, minimum number of objects ξ
	OPTICS	Flexible	Flexible	Low	Low	Excellent	Time needed for cluster order in real life application
	DENCLUE	Low	Low	Low	Low	Excellent	density parameter σ and noise threshold ξ,
Grid-Based	Wave-cluster	Low	Low	Low	Low	Excellent	NA
method	STING	Low	Low	Low	Low	flexible	The output cluster is Isothetic

6. OTHER DETECTION SCHEMES

DDoS attack is detected and clustered using schemes of neural network and Fuzzy-logic schemes. One of the most popular neural network methods are Self-Organization Maps (SOMs). With SOMs, several units are competing for the current object to perform the clustering. The winning or active unit is selected where its weight vector is closest to the current object. SOMs assume that there is some topology or ordering among the input objects and that the units will eventually take on this structure in space. Design and implement systems based on SOM clustering method to detect and classify DDoS attack has been broadly used in the recent topics (Kumar and Selvakumar, 2011; Dusan *et al*., 2012), (Hoque *et al*., 2013).

Fuzzy logic was adopted by many researches to cluster and to design and implement the clustering method for DDoS attack. Fuzzy logic helps is appropriate for nonlinear systems and helps in solving the systems which have elements of uncertainly (Ma, 2010). DDoS cluster based on fuzzy mechanisms are adopted in a recent trends of security work (Stavros *et al*., 2012; Kumar and Selvakumar, 2012).

Simulation work is presented to mitigate DDoS attack in the wireless environment. Ribeiro *et al*. (2014) evaluated the simulation work based on throughput metric which is well known metric when the evaluation of work is needed. Visualization charts is shown with a good results to realize the normal traffic from attack. Justification of using this metric is illustrated, where the increasing in the simulation host can decrease the throughput metric.

7. CONCLUSION

Reviewing and studying the architecture of DDoS attack is considered a crucial step to deploy the appropriate mechanism to detect this attack in the early launching stage before the attacker overwhelming the legitimate applications on the internet. Data mining cluster analysis was adopted by many researches to detect and cluster the DDoS attack. Performance comparison is evaluated as the ultimate goal is to promote real-time avoidance strategy against DDoS attack.

8. REFERENCES

Anand, R. and D.U. Jeffrey, 2012. Mining of Massive Datasets. 1st Edn, Cambridge, New York, ISBN-10: 978-1-107-01535-7, pp: 398.

Basant, A. and N. Mittal, 2012. Hybrid approach for detection of anomaly network traffic using data mining techniques. Proc. Technol., 6: 996- 1003. DOI: 10.1016/j.protcy.2012.10.121

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

Dusan, S., N. Vlajic and A. An, 2012. Detection of malicious and non-malicious website visitors using unsupervised neural network learning. Applied Soft Comput., 13: 698-708. DOI: 10.1016/j.asoc.2012.08.028

Ghazali, K.W.M. and R. Hassan, 2011. Flooding distributed denial of service attacks-a review. J. Comput. Sci., 7: 1218-1223.

Hari, O. and K. Aritra, 2012. A hybrid system for reducing the false alarm rate of anomaly intrusion detection system. Proceedings of the 1st International Conference on Recent Advances in Information Technology, 15-17, IEEE Xplore Press, Dhanbad, India, pp: 131-136. DOI: 10.1109/RAIT.2012.6194493

Hoque, N., M.H. Bhuyan, R.C. Baishya, D.K. Bhattacharyyaa and J.K. Kalitab *et al*., 2013. Network attacks: Taxonomy, tools and systems. J. Netw. Comput. Applic., 40: 307-324.DOI: 10.1016/j.jnca.2013.08.001i

Jian, K., Y. Zhang and J.B. Ju, 2006. Classifying DDoS attacks by hierarchical clustering based on similarity. Proceedings of the 5th International Conference on Machine Learning and Cybernetics, Aug. 13-16, IEEE Xplore Press, Dalian, China, pp: 2712-2717. DOI: 10.1109/ICMLC.2006.258931

Jiawei, H. and M. Kamber, 2006. Data Mining: Concepts and Techniques. 2nd Edn., San Francisco, CA. ISBN-10: 13978-1-55860-901-3, pp: 772.

Jieren, C., J. Yin, C. Wu, B. Zhang and Y. Liu *et al*., 2009. DDoS attack detection method based on linear prediction model. Emerg. Intell. Comput. Technol. Applic., 5754: 1004-1013. DOI: 10.1007/978-3-642-04070-2-106

Johan, M., P. Casas and P. Owezarski, 2011. Sub-space clustering and evidence accumulation for unsupervised network anomaly detection. Proceedings of the 3rd International Conference on Traffic Monitoring and Analysis, Apr. 27, Springer Berlin Heidelberg, pp: 15-28. DOI: 10.1007/978-3-642-20305-3-2

Jun, Z. and M.Z. Hu, 2005. Intrusion detection of DoS/DDoS and probing attacks for web services. Proceedings of the 6th International Conference on Advances in Web-Age Information Management, Oct. 11-13, Springer, Berlin Heidelberg, pp: 333-344. DOI: 10.1007/11563952-30

Junaid, A., P. Townend and J. Xu, 2013. A novel intrusion severity analysis approach for clouds. Future Gener. Comput. Syst., 29: 416-428. DOI: 10.1016/j.future.2011.08.009

Keunsoo, L., J. Kim, K.H. Kwon, Y. Han and S. Kim *et al*., 2007. DDoS Attack detection method using cluster analysis. Expert Syst. Applic., 34: 1659-1665. DOI: 10.1016/j.eswa.2007.01.040

Kiran, S., 2008. Exploring a novel approach for providing software security using soft computing systems. Int. J. Security Applic., 2: 51-58.

Kumar, P.A.R. and S. Selvakumar, 2012. Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Comput. Commun., 36: 303-319. DOI: 10.1016/j.comcom.2012.09.010

Kumar, P.A.R. and S. Selvakumaras, 2011. Distributed denial of service attack detection using an ensemble of neural classifier. Comput. Commun., 34: 1328-1341. DOI: 10.1016/j.comcom.2011.01.012

Ma, Y., 2010, System for attack recognition based on mining fuzzy association rules. Proceedings of the International Conference on Computer Design and Application, Jun. 25-27, IEEE Xplore Press, Qinhuangdao, China, pp: 129-133. DOI: 10.1109/ICCDA.2010.5541136

Manjula, S., A. Jose, S. Divakar and R. Subramanian, 2011. Degumming rice bran oil using phospholipase-A_1. Eur. J. Lipid Sci. Technol., 113: 658-664. DOI: 10.1002/ejlt.201000376

Mansouri, D., L. Mokdad, J. Ben-othman and M. Ioualalen, 2013. Detecting DoS attacks in WSN based on clustering technique. Proceedings of the International Conference on Wireless Communications and Networking. Apr. 7-10, IEEE Xplore Press, Shanghai, China, pp: 2214-2219. DOI: 10.1109/WCNC.2013.6554905

Maryam, S., N. Movahhedinia and B.T. Ladani, 2011. An entropy based approach for DDoS attack detection in IEEE 802.16 based networks. Proceedings of the 6th International Conference on Advances in Information and Computer Security, Nov. 8-10, Springer, Berlin Heidelberg, pp: 129-143. DOI: 10.1007/978-3-642-25141-2-9

Mehdi, E.M. and A. Amphawan, 2012. Review of syn-flooding attack detection mechanism. Int. J. Distributed Parallel Syst., 3: 99-117. DOI: 10.202/1202.1761.pdf

Radware, 2013. DDoS survival handbook. knowledge center-radware security web site.

Ribeiro, A.C., A.R. Pinto, G.F.D. Zafalon, D.F. Pigatto and K.C. Branco *et al*., 2014. An approach to mitigate denial of service attacks in IEEE 802.11 networks. J. Comput. Sci., 10: 128-137.

Sangjae, L., G. Kim and S. Kim, 2011. Sequence-order-independent network profiling for detecting application layer DDoS attacks. EURASIP J. Wireless Commun. Netw., 50: 1-9. DOI: 10.1186/1687-1499-2011-50

Stavros, N.S., V. Katos, S.K. Alexandros and B.K. Papadopoulos, 2012. Real time DDoS detection using fuzzy estimators. Comput. Secuirty, 31: 782-790. DOI: 10.1016/j.cose.2012.06.002

Subbulakshmi, T., S.M. Shalinie, C.S. Reddy and A. Ramamoorthi, 2010. Detection and classification of DDoS attacks using fuzzy inference system. Proceedings of the 3rd International Conference, Jul. 23-25, Springer Berlin Heidelberg, Chennai, India, pp: 242-252. DOI: 10.1007/978-3-642-14478-3_25

Sung-Ju, K., B.C. Kim and J.Y. Lee, 2013. DDoS analysis using correlation coefficient based on kolmogorov complexity. Proceedings of the 8th International Conference, GPC and Colocated Workshops, May 9-11, Springer Berlin Heidelberg, pp: 443-452. DOI: 10.1007/978-3-642-38027-3_47

Vishal, R., B.R. Tamma, B.S. Manoj and M. Sarkar, 2012. On detecting CTS duration attacks using K-means clustering in WLANs. Proceedings of the IEEE International Conference on Advanced Networks and Telecommuncations Systems, Dec. 16-19, IEEE Xplore Press, Bangalore, pp: 90-95. DOI: 10.1109/ANTS.2012.6524235

Walter, C., G. Monti, G. Moro and M. Ramilli, 2009. Network attack detection based on peer-to-peer clustering of SNMP data. Lecture Notes of the Institute for Computer Sciences. Social Informat. Telecommun. Eng., 22: 417-430. DOI: 10.1007/978-3-642-10625-5-26

Yu, C., K. Hwang and W. Ku, 2007. Collaborative detection of DDoS attacks over multiple network domains. IEEE Trans. Parallel Distributed Syst., 18: 1649-1662. DOI: 10.1109/TPDS.2007.1111