A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification

Dr. ABBASS ASOSHEH, NAGHMEH RAMEZANI
Information Technology Department
Tarbiat Modares University
Jalal Ale Ahmad, PO BOX: 14115-111
Tehran-IRAN
asosheh@modares.ac.ir, ramezani_n@modares.ac.ir

Abstract: -A Distributed denial of service (DDoS) attack uses multiple machines operating in concern to attack a network or site. It is the most important security problem for IT managers. These attacks are very simple organized for intruders and hence so disruptive. The detection and defense of this attack has specific importance among network specialists. In this paper a new and smart taxonomy of DDoS attack and defense mechanism will be introduced. The attacks taxonomy is introduced using both known and potential attack mechanisms. It comprises all types of attacks and provides a comprehensive point of view for DDoS attacks. We introduce a useful tool that can be employed to a sophisticated selection defense method for DDoS attacks. Furthermore a smart taxonomy method of DDOS attacks will be proposed to help selection an appropriate defense mechanism. This method uses some features of DDOS attacks and classifies it to several clusters by K-mean algorithm and labels each cluster with a defense mechanism. If an IDS detects a DDOS attack, proposed system extract attack features and classify it by KNN (K-Nearest-Neighbor) to determine the cluster in which it belongs to. The defense mechanisms taxonomy is using the currently known approaches. Also the comprehensive defense classification will help to find the appropriate strategy to overcome the DDoS attack.

Key-Words: - DDoS attack, Defense mechanism, Taxonomy, Detection, Smart Classification

1 Introduction

Denial of service attacks are rapidly increasing threats for productivity and the profitability of the internet. DDoS attacks are relatively simple, very powerful technique to attack Internet resources and services. It is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack called primary victim, while the compromised systems used to launch the attack are often called the secondary victims. The use of secondary victims in a DDoS attack provides the ability to wage a much larger and more disruptive attack while remaining anonymous. The secondary victims actually perform the attack and so make it more difficult to track down the real intruder for network forensics.

A highly flexible and distributed defense is the only solution to cope against this threat. During last few years, several high scale attacks had been launched to target profile internet site. It is necessary to understand all aspects of DDoS attacks and deployed defense mechanisms to make an effective defense up. Some classifications have been proposed for DDoS attacks and defense mechanisms. In [1], it classified DDoS in two main branches based on vulnerability: bandwidth depletion and resource depletion attacks. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim.

A resource depletion attack is designed to tie up the victim resources to make the system unable to process legitimate service request. Various classification criteria are indicated in bold type: Degree of Automation, Exploited Vulnerability, Attack Rate Dynamics and Impact [2]. The Level of Computerization, attack networks, Oppressed vulnerability, Influence of DDoS attack, attack Intensity dynamics taxonomy have been presented in [3].

In [4], Authors classified DDoS attacks by Congestion based, anomaly based and source based techniques and defense is classified by destination network filtering and source work filtering. In [5] authors present classification of denial-of-service

attacks according to the type of the target (e.g. firewall, Web server, router), a resource that the attack consumes (network bandwidth, TCP/IP stack) and the exploited vulnerability (bug or overload). This classification focuses more on the actual attack phase. A realistic model of DDoS simulation and experimentation has been proposed a formalized and scalable taxonomy in [6]. In [7] authors introduced a framework for classifying denial of service (DOS) attacks based on header content, transient ramp-up behavior and novel techniques such as spectral analysis.

Some taxonomy for defense mechanisms has been proposed, too. Three categories of DDoS countermeasures introduced in [1]. Firstly, prevention of the setup of the DDoS attack network, including preventing secondary victims and detecting and neutralizing handlers.

Secondly, dealing with a DDoS attack while it is in progress, including detecting or preventing, mitigating or stopping, and deflecting the attack. The post-attack category which involve network forensic discussed for the third. Other defense classification is based on activity level and location [2] and on submissive defense mechanism, active defense mechanism, action and defense deployment position [3]. None of the mentioned DDoS taxonomies are comprehensive. Also the proposed classifications for defense mechanism are not effective to deploy for suitable defense mechanism selection.

In this paper we will introduce a new comprehensive taxonomy for DDoS attack and defense mechanism. Also a new taxonomy method of DDoS attacks will be introduced. It classifies DDoS Attacks to several clusters. Then each cluster is labeled with a defense mechanism. If an IDS detects a DDOS attack, proposed system extract attack features and classify it to determine the cluster in which it belongs to. Obviously, this method can help us to choice a suitable defense mechanism against a new detected DDOS attack.

The rest of this paper is organized as follows: the new proposed taxonomy of DDoS will discuss in section 2. In section 3, the taxonomy of defense mechanisms will propose. In section 4, we will propose a smart classification framework. This paper will be concluded in section 5 and finally provide an overview of future work.

2 New taxonomy for DDoS attacks

There are a wide variety of DDoS attacks. To make an effective defense, it is highly recommended to know the classified nature of attacks. We describe the attacks and classify these attacks into eight classes. Eight features will be deployed in new taxonomy for DDoS attacks. They are as architecture, degree of automation, impact, vulnerability, attack rate dynamics, scanning strategy, propagation strategy and packet content which will be described in the following in details.

2.1 Architecture base

Agent-Handler Model: This typical model consists of attacker, handler, agent, and target network. The handlers are software packages located throughout the Internet that the attacker uses to communicate with the agents. The agent software exists in compromised systems that will eventually carry out the attack. The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents [1].

Reflector Model: this model consists of attacker, handler, agent, and reflector. The scenario of this type of attack is the same as that of typical DDOS attacks up to a specific stage. The attackers have control over handlers, which, in turn, have control over agents. The difference in this type of attack is that agents are led by handlers to send a stream of packets with the victim's IP address as the source IP address to other uninfected machines, known as *reflectors*, exhorting these machines to connect with the victim. A reflector is any host that responds to requests, for example a web server that responds to TCP SYN requests with a SYN-ACK reply, or any host that responds to ICMP echo requests with ICMP echo replies. Any host can be used as a reflector by spoofing the the victim’s IP address in the source field of the request, tricking the reflector into directing its response to the victim. Reflectors can also be used as amplifiers by sending packets to the broadcast address on the reflector network, soliciting a response from every host on the LAN [30, 31].

IRC-Based Model: This model is similar to above models except that instead of using a handler program installed on a network server, an IRC (Internet Relay Chat) communication channel is used to connect the client to the agents. According to the communication mechanism has been

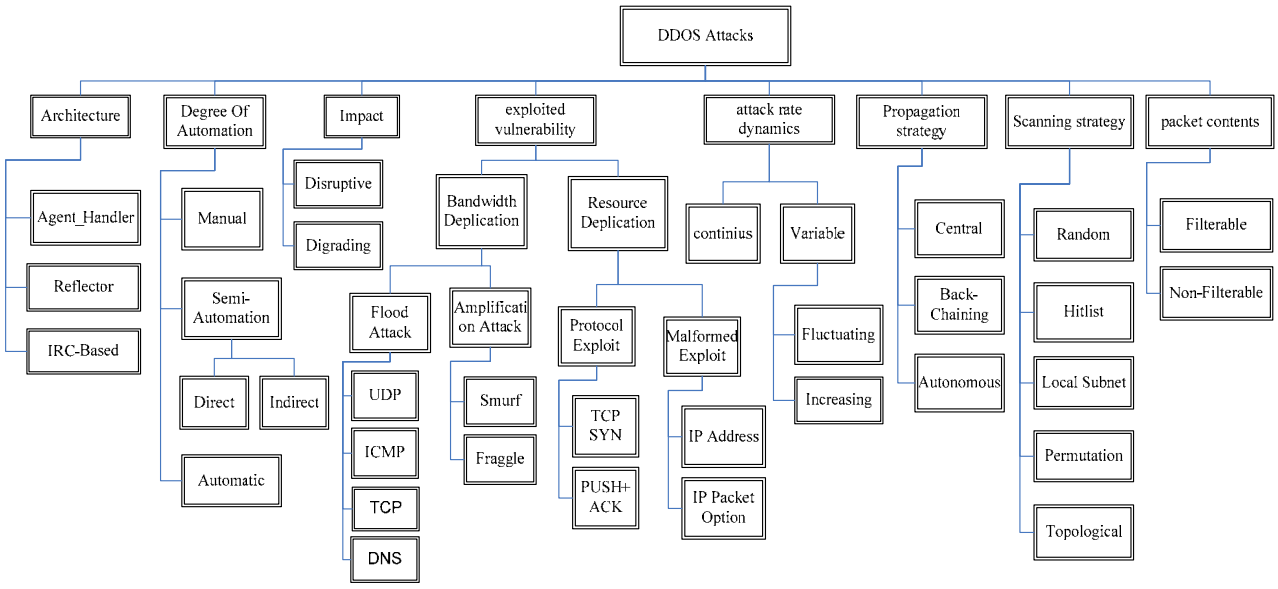

Fig.1 DDoS attacks Classification

deployed between agent and handler machines, there are two types of attacks [1, 18].

2.2 Degree of automation base

Manual: The attacker scanned remote machines for vulnerabilities, broke into them and installed the attack code, and then commanded the onset of the attack.

Semi-Automatic: The intruder deploys automated scripts to investigate and compromise the target machines for installation of the attack code. The handler machines will be employed to specify the attack type, the victim's address and then order the onset of the attack to agents who send packets to the victim. Attacks with direct and indirect communication are different. In direct one, the agent and handler machines need to know each other's identity in order to communicate. This is achieved by hard-coding the IP address of the handler machines in the attack code that is later installed on the agent. In indirect one, an attacker controls the agents using IRC communications channels. Thus, discovery of a single agent may lead no further than the identification of one or more IRC servers and channel names that used by the DDoS network.

Automatic: Automatic DDoS attacks additionally automate the attack phase to avoid any communication needs between attacker and agent machines. The time of the onset of the attack, attack type, duration and victim's address is preprogrammed in the attack code.

2.3 Impact base

Disruptive: In this class the entire of the bandwidth will be cutoff and so it is known as disorderly attack.

Degrading: If DDoS attack causes the partial bandwidth consumption, it is said to be degrading attack. It is hard to detect because of slowly cutoff legitimate bandwidth.

2.4 Vulnerability base

Bandwidth depletion: In this class, attacker sends unwanted traffic to target network. Flood and amplification methods are the well known method in this line. A flood attack involves zombies sending large volumes of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth and preventing access by legitimate users. Flood attacks have been launched using TCP, UDP, ICMP and DNS packets and so on. An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, by that all systems in the subnet receive from the broadcast address and so send a reply to the victim system. Smurf and Fraggle are examples of these attacks.

Resource depletion: In this attack the attacker sends packets which misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users. In protocol exploit attacks a

specific feature or implementation bug of some protocol will be employed at the victim in order to consume excess amounts of its resources. The TCP SYN and PUSH+ACK are examples of these attacks. However, in Malformed Packet Attacks, attacker instructs the zombies to send incorrectly formed packets to the victim system in order to crash it. Examples include malformed IP address and OPTION field in IP packet.

2.5 Attack rate dynamic base

Continuous: The agent machines after getting the onset order will generate the attack packets with full force. Detection is so simple in this attack.

Variable: Variable rate attacks are more cautious in their engagement. The attack rate will be changed to avoid detection and response. According to the rate change mechanism, there are two types of attacks, increasing and fluctuation. In increasing, attacks have a gradually increasing rate lead to a slow exhaustion of victim's resources. A state change of the victim could be so gradual that its services degrade slowly over a long period time and so delaying detection of the attack. In Fluctuating, attacks have a fluctuating rate adjust the attack rate based on the victim's behavior, occasionally relieving its effect to avoid detection.

2.6 Scanning strategy base

Random: During random scanning each compromised host probes random addresses in the IP address space. This potentially creates a high traffic volume since many machines probe the same addresses. Code Red (CRv2) used this method [19].

*Hitlist:*A machine that perform hitlist scanning, probes all addresses from an externally supplied list. When it detects the vulnerable machine, it sends one half of the initial hitlist to the recipient and keeps the other half. This technique allows a great propagation speed and no collisions during the scanning phase.

Topological: Topological scanning uses the information on the compromised host to select new targets. All email worms use this method. *Permutation*: During permutation scanning, all compromised machines share a common pseudo-random permutation of the IP address space; each IP address is mapped to an index in this permutation. A machine begins scanning by using the index computed from its IP address as a starting point. Whenever it sees an already infected machine, it chooses a new random start point.

Local Subnet: Local subnet scanning can be added to any of the previously described techniques to preferentially scan for targets that reside on the same subnet as the compromised host that used local subnet scanning.

2.7 Propagation strategy base

Central: In this method the attack code resides on a central server or set of servers. After compromising the agent machine, the code is downloaded from the central source through a file transfer mechanism. Li0n worm used this central propagation [20].

Back-chaining: In this method the attack code is downloaded from the machine that was used to exploit the system. The infected machine then becomes the source for the next propagation step. Ramen worm used this method [21].

Autonomous: This method avoids the file retrieval step by injecting attack instructions directly into the target host during the exploitation phase. Warhol worm used autonomous method [22].

2.8 Packet content base

Filterable: Filterable attacks use bogus packets or packets for non-critical services of the victim's operation, and thus it can be filtered by a firewall. Examples of such attacks are a UDP flood attack or an ICMP request flood attack on a Web server.

Non-filterable: Non-filterable attacks use packets that request legitimate services from the victim. Thus, filtering all packets that match the attack signature would lead to an immediate denial of the specified service to both attackers and the legitimate clients. Examples are a HTTP request flood targeting a Web server or a DNS request flood targeting a name server.

3 New taxonomy for DDoS defense mechanism

There is currently no comprehensive method to protect against all known forms of DDoS attacks. Also, many derivative DDoS attacks are continually being developed by attackers to bypass each new countermeasure employed.

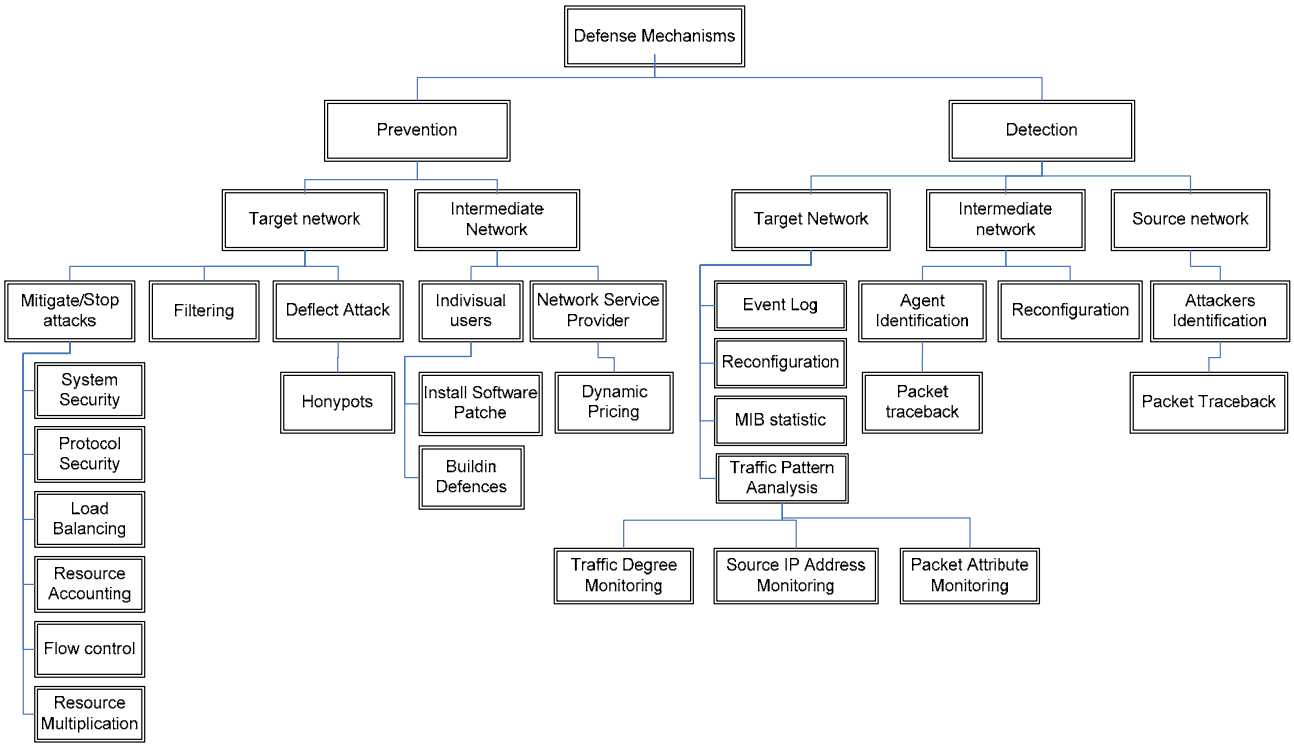

Fig.2 DDoS defense Classification

The proposed taxonomy of defense mechanism is based on human thinking logic to defense. Fig. 2 shows this classification. All defense mechanism has been divided to two categories: prevention and detection.

Moreover it must determine where the defense has to be deployed. DDoS attacks have several features that hinder their successful detection and defense: 1) DDoS attacks generate a large volume flow to overwhelm the target network. 2) It is difficult to distinguish attack packets from legitimate packets. 3) Most DDoS attacks use spoofed IP addresses [28]. 4) The large number of attacking machines and the use of source IP address spoofing make the trace back difficult or impossible besides. 5) Although the router performs the ingress filtering, a lot of spoofing packets can pass it because some DDoS tools provide the several spoofing levels in order to pass the ingress filtering router. 6) The distributed nature of the attacks calls for a distributed response, but cooperation between administrative domains is hard to achieve [29].

In the following the new taxonomy for DDoS defense will be described in details.

3.1 Prevention mechanism

The best option to defend against DDoS attacks is prevention. In this approach researchers try to stop attack in start. Several preventing mechanisms have been proposed [23, 24, and 25]. The prevention can be done in *target network* or *intermediate network*. Target network*:* is one that the attack organized for denial of that. *Security mechanisms* increase the overall security of the system, guarding against illegitimate accesses to the machine, removing application bugs and updating protocol installations to prevent intrusions and misuse of the system. The *protocol security* mechanisms address the problem of bad protocol design. Many protocols contain operations that are cheap for the client but expensive for the server. Classic misuse example is the TCP SYN attack that can increase bandwidth on critical connections to prevent them to go down in an attack. *Load balancing* can improve both normal performances as well as mitigate a DDoS attack.

Additionally, providers can replicate servers and provide additional failsafe protection if some go down during a DDoS attack. *Flow control* is another technique proposed to prevent servers from going down. The Max-min Fair server-centric router throttle method sets up routers that access a server

with logic to adjust incoming traffic to levels that will be safe for the server to process. *Resource multiplication* mechanisms provide an abundance of resources to counter DDoS threats. The straightforward example is a system that deploys a pool of servers with a load balancer and installs high bandwidth links between itself and upstream routers. *Resource accounting* mechanisms restrict the access of each user to resources based on the privileges of the user and his behavior. Such mechanisms guarantee fair service to legitimate well-behaving users [9, 10]. *Filtering* refers to the scanning of IP packet headers leaving a network and checking to see if they meet certain criteria. If the packets pass the criteria, they are routed outside of the sub network from which they originated. Otherwise, the packets will not be sent. Firewall is important tool in this area. *Deflect method* serve to pervert attacks from hitting the systems. It protects as well as serves as a means for gaining information about attackers by storing a record of their activity and learning what types of attacks and software tools has been using. Honeypots intentionally set up with limited security to be an enticement approach for an intruder's attack.

One of the best methods to prevent DDoS attacks is to prevent themselves from participating in the attack for the secondary victim systems (intermediate network). This requires a heightened awareness of security issues and prevention techniques from all Internet users. Secondary victims would be prevented from becoming infected with the DDoS agent software; these systems must continually monitor their own security. They should check the system status to make sure that no agent programs have been installed on their systems and also they are not indirectly sending agent traffic into the network. Because of the de-centralized Internet, and different hardware and software platforms variety, it is quite difficult for users to implement the right Protective measures such as anti-Trojan software. Network users should have enough resources to afford protective measures and the knowledge of the right protections method selection. *End user* can provide defense against malicious code insertion through buffer overflow violations by installing software patches and built in mechanisms in the core hardware and software of computing systems.

Another strategy is for network *service providers* and network administrators to add dynamic pricing to network resource usage. If providers choose to charge differently for the use of different resources, they would be better able to identify legitimate users.

3.2 Detection and defense:

This approach uses attacks signatures or learning normal behavior of network to detect attacks. Many intrusion detection systems are written based on this approach and used data mining and artificial intelligence techniques. It can be employed to detect attacks in target network or intermediate network.

In Target network, the goal is to detect attack in network that attack organized for. With monitoring the traffic degree any *traffic pattern* changed could be detected and by monitoring the IP address and other field the usage pattern of resources can be detected. Also we are able to defend by using filtering, load balancing and access control. Some attacks scenarios are known. Therefore we can detect attacks by analysis existent *log files* in systems and servers and comparison the result by known scenarios or normal pattern (event analysis). *MIB information analysis* is another method to identify when a DDoS attack is occurring. MIB data includes parameters that indicate different packet and routing statistics. Identifying statistical patterns in different parameters during a DDoS attack looks promising for possibly mapping ICMP, UDP, and TCP packet statistical abnormalities to a specific attack [32, 33]. This approach could provide methods to identify when a DDoS attack is happened and how to adjust network parameters to compensate for the unwanted traffic [8]. *Reconfiguration* mechanisms change the topology of the target network to either add more resources to the target network.

In intermediate network, the goal is to detect intermediate systems to prevent from participating in the attack. *Agent identification* mechanisms provide the victim with information about the identity of the machines that are performing the attack. Agent identification uses trace back techniques [12, 13, 14, and 15] that enabling the usage of the source address field for agent identification. *Reconfiguration* mechanisms change the topology of the intermediate network to isolate the attack machines.

Source network mechanism has been used to detect and defend against attackers [16, 26]. *Attacker's identification* uses trace back techniques to find attacker by source address of IP packet.

Detection at the side of the target network is more practical but can hardly produce an alarm at

the early stage of a DDoS attack because abnormal deviation can only be easily found until the DDoS attack turns to the final stage. Furthermore, it is difficult for target side to take efficient response after DDoS is detected due to numerous malicious packets aggregating at this side.

Defense at the intermediate network has two main advantages: Detection is more hidden since it is deployed apart from attacking path and it has little vulnerability to DDoS attack. But, Detection at intermediate network has several challenges. On the one hand, accurate detection is not easy to achieve since the abnormal signature is distributed in a backscatter way. On the other hand, defense at innocent side is deployed far from the victim side and detection effect depends on the number of participant of Internet Service Providers (ISPs).

4 Smart Classification Framework

Obviously, each kind of DDOS attack has different impact on network traffic. It is important to detect each kind of attack and deployed an effective defense mechanism against it. In [6], the basic idea of the taxonomy is to use Hierarchical Clustered method to classify various DDoS attacks based on similarity. It extracts features of DDoS attacks and builds a Binary Weighted Tree based on these features. To each attack, they record one's information about the path it passed in the tree using a sequence of three-tuple, and each three-tuple is (name, code, and weight).

We propose a framework that automates detection of each kind of DDoS attacks and choose a suitable defense mechanism against it. Fig.3 shows our proposed framework.

Clustering is the process of grouping the data into classes or clusters, so thet objects within a cluster have high similarity in comparison to one another but are very dissimilar to objects in other cluster. Dissimilarities are assessed based on the attribute values describing the object.

All tuples will be distinguished in k cluster by clustering algorithm and each cluster is labeled with a defense mechanism. If an intrusion detection system (IDS) detects a DDOS attack, the system extracts features of attack and generates a tuple for it. Also it classifies new tuple or attack by a classifier (for example k-nearest-neighbor) to determine the cluster in which it belongs to. The new attack is assigned the most similar cluster.

Data classification is a two step process. In the first step, a classifier is built describing a predetermined set of data classes and a model based on this set of data. This is the learning step. In the second step, the model is used for classification.

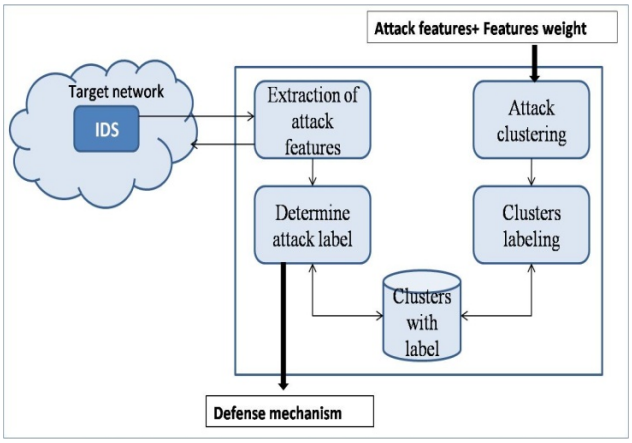

Fig.3 Smart Classification Framework

The Attacks features and features' weights are inputs of the smart system. *Attack clustering* module maps all attacks in an N-dimensional space and runs a clustering algorithm on attacks to make them distinguishable in k clusters. After that the *cluster labeling* module labels these clusters with an appropriate defense mechanism. The labeled clusters are saved into a file. It is supposed that the target or victim network contains an intrusion detection system (IDS) which is a type of security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). IDS send alarm to smart system as soon as possible on detection of DDOS attack. *Extraction of attack features* module extracts detected attack features from target network and determines detected attack label by *determine attack label* module. This module does its duty by a classifier. The specified label is suitable defense mechanism for the attack. The attack and its label are saved into a file. Clusters labeling run clustering on updated attacks file periodically and update attacks file.

The proposed framework is explained with an example. K-mean and k-nearest-neighbor (KNN) are considered as selected clustering algorithm and classification method, respectively.

K-mean is one of the oldest and most widely used clustering algorithms. K-mean defines a

prototype in terms of a centroid, which is usually the mean of group of points, and is typically applied to objects in a continuous n-dimensional space. In K-mean we first choose K initial centroids, where K is a user specified parameter, namely the number of clusters desired. Each point is then assigned to the closest centroid, and each collection of points assigned to a centroid is a cluster. The centroid of each cluster is then updated based on the points assigned to the cluster [34, 35].

Nearest-neighbor classifiers are based on learning by analogy, that is, by comparing a given new tuple with known tuples that are similar to it. The known tuples are described by N attributes. Each tuple represents a point In an N-dimensional space. in this way, all of the known tuples are stored in an N-dimensional pattern space. When given an unknown tuple, a k-nearest-neighbor classifier searches the pattern space for the k known tuples that are closest to the unknown tuple. These k known tuples are the k nearest neighbor of the unknown tuple. For k-nearest-neighbor classification, the unknown tuple is assigned the most common class among its k nearest neighbors. When k=1, the unknown tuple is assigned the class of the known tuple that is closest to it in pattern space [34, 35].

The following steps will be done based on proposed framework.

Step1: Select features of DDOS attacks that are detectable for IDS. Label each feature with Fi (0<i<N and N is number of features).

Step2: Assign a weight to each feature and label it W_i. This weight should be assigned by network security experts.

Step3: Assign value to each feature. These values can be zero or 1. Label feature F_i's value with V_i.

Step4: Assign an N-tuple to each attack as follows: (M is Number of known attacks)

$Attack_j = (W_1*V_1, W_2*V_2, \ldots, W_N*V_N)$, $1<j<M$

Step5: All known attacks will be mapped into an N-dimensional space. In other words, each attack is a point in N-dimensional space.

Step6: Run K-mean algorithm on these points (attacks). K, number of clusters can be equal to the number of defense mechanisms.

Step7: Label each cluster by appropriate defense mechanism.

Step8: As a DDoS attach is detected by an IDS, will be classified by K-nearest-neighbor (KNN) algorithm to determine which cluster it belongs to.

5 Conclusion

Exact recognition of DDoS attacks and selection the proper strategy in defense against these attacks is so important. The proposed taxonomy for the DDoS attacks comprised eight futures of it as architecture, degree of automation, impact, vulnerability, attack rate dynamics, scanning strategy, propagation strategy and packet content. Also the defense mechanism explained in two main categories: prevention and detection.

However in this paper a general classification of DDoS attacks and the ways to deal with them, in a comprehensive research on the DDoS attacks and ways to deal with them, is given. The defense mechanism is so useful in the selection of a proper strategy in defense against DDoS attacks. We also proposed a smart classification framework to automate detection of each kind of DDoS attacks and choosing an appropriate defense mechanism. The proposed framework is explained with an example. K-mean and k-nearest-neighbor (KNN) are considered as selected clustering algorithm and classification method, respectively.

6 Future works

Obviously, there are various kinds of DDOS attacks which have different impact on network traffic. Paper [36] proposed 44 statistical features, which are estimated only from the packet headers. Each attack impacts on some specific features. So, one of the important tasks which can be done in the following is to determine affected features by each attack. This work help detect an attack by checking its especial features based on proposed framework in this paper.

References:

[1] S. Specht, M. and R. B. Lee., *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures*. Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004, pp.543-550.

[2] J. Mirkovic, J. Martin, et al., *A Taxonomy of DDoS Attacks and DDoS Defence Mechanisms*, Computer Science Department, University of California, 2002.

[3] U. Tariq, M. Hang, and et al., *A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques.,* ADMA LNAI 4093, 2006 pp.1025-1036.
[4] L. Chen, T. Longstaff, K. Carley*, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, Computers and Security, 2004.
[5] F. Kargl, J. Maier and M. Weber, *Protecting web servers from distributed denial of service attacks*, In Proceedings of 10th International World Wide Web Conference, 2001.
[6] J. Kang, Y. Zhang, and et al., *A Formalized Taxonomy of DDoS Attacks based on Similarity*, ISI 3975, 2006, pp. 717-719.
[7] A. Hussain, J. Heidemann, C. Papadopoulos, *A Framework for Classifying Denial of Service Attacks*, ACM, 2003, pp.99-110
[8] B. Joao, D. Cabrera, and et al. ,*Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables – A Feasibility Study*, Integrated Network Management Proceedings, 2001, pp. 609-622.
[9] A. Juels and J. Brainard, *Client puzzles: A cryptographic countermeasure against connection depletion attacks*, In Proceedings of the 1999 Networks and distributed system security symposium (NDSS'99), 1999.
[10] F. Lau, S. H. Rubin, and et al., *Distributed denial of service attacks*, In Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, 2000.
[11] A. C. Snoeren, C. Partridge, and et al., *Hash-Based IP Traceback*, In Proceedings of ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2001.
[12] D. X. Song and A. Perrig, *Advanced and authenticated marking schemes for IP Traceback*, IEEE Infocom, 2001.
[13] D. Dean, M. Franklin and A. Stubblefield, *An algebraic approach to IP Traceback*, In Proceedings of the 2001 Network and Distributed System Security Symposium, February 2001.
[14] S. M. Bellovin, *ICMP traceback messages, Internet draft*, http://search.ietf.org/internetrafts/draft-ietf-itrace-01.txt, Oct. 2001.
[15] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, *Practical network support for IP Traceback*, In Proceedings of 2000 ACM SIGCOMM Conference, Aug. 2000.
[16] T. M. Gil and M. Poleto, *MULTOPS: a datastructure for bandwidth attack detection*, In Proceedings of 10th Usenix Security Symposium, August 2001.
[17] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, R. Morris, *Resilient Overlay Networks*,In Proceedings of 18th ACM SOSP, October 2001.
[18] Distributed Denial of Service attacks and theirdefenses:http://www.lancs.ac.uk/postgrad/pissias/net sec /DDoS/
[19] D. Moore, *The spread of the code red worm (crv2),*http://www.caida.org/analysis/security/coderedd/coderedv2_analysis.xml.
[20] CERT Coordination Center, *erkms and l*i0n worms, http://www.cert.org/incident_notes/IN-2001- 03.html
[21] CERT Coordination Center*, Ramen worm*, http://www.cert.org/incident_notes/IN-2001-01. html
[22] N. Weaver, *Warhol Worm*; http://www.cs. berkeley.edu/~nweaver/ warhol.html
[23] Tripwire, *Tripwire for servers*, http://www. tripwire.com/products/servers/
[24] McAfee, *Personal Firewall*, http://www. mcafee.com/myapps/firewall/ov_firewal l.asp
[25] Cisco, *Strategies to protect against distributed denial of service attacks*, http://www.cisco.com/warp /public/707/newsflash.html
[26] Mananet, *Reverse Firewall*, http://www.cs3-inc.com/ps_rfw.html
[27] Information Sciences Institute, *Dynabone*, http://www.isi.edu/dynabone/.
[28] G. Zhang, M. Parashar, *Cooperative Mechanism against DDOS Attacks,* the Applied Software Systems Laboratory, Department of Electrical and Computer Engineering, Rutgers University, 2005.
[29] K. Mihui, K. Chae, *Detection and Identification Mechanism against Spoofed,* Springer-Verlag Berlin Heidelberg, 2004, pp. 673–682.
[30] A. Hussain, J. Heidemann, *A Framework for Classifying Denial of Service Attacks,* SIGCOMM, ACM, 2003, pp.99-110.
[31] V. A. Kumar, *Sophistication in distributed denial-of-service attacks on the Internet,* CURRENT SCIENCE, VOL. 87, NO. 7, 10 October, 2004, pp.885-888.
[32]R. Jalili, F. Imani-Mehr, *Detection of Distributed Denial of Service Attacks Using Statistical Pre-Prossesor and Unsupervised Neural Network*", ISPEC, Springer-Verlag Berlin Heidelberg, 2005, pp.192-203

[33] M. Li, J. Liu, and D. Long, *Probability Principle of Reliable Approach to detect signs of DDOS Flood Attacks* , PDCAT, Springer-Verlag Berlin Heidelberg, 2004, pp.596-599.
[34] J. Han, M. Kamber, *Data Mining Concepts and Techniques* ,Elsevier Inc., 2006.
[35] P. Tan, N., M. Steinbach, *Introduction to Data Mining*, Pearson Education, Inc., 2006.
[36] G. Dimitris, T. Ioannis, and D. Evangelos, *Feature Selection for Robust Detection of Distributed Denial of service Attacks using Genetic Algorithm*, SETN, Springer-Valag Berlin Heidelberg, 2004, pp.276-281.