ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 2, Issue 7, July 2013*

# A Survey on Defense Mechanisms countering DDoS Attacks in the Network

Dileep Kumar G[1], Dr CV Guru Rao[2], Dr Manoj Kumar Singh[3], Dr Satyanarayana G[4]

Asst Professor, Dept of Computer Science & Engg, SR Engineering College, Warangal, India [1]
Professor, Dept of Computer Science & Engg, SR Engineering College, Warangal, India [2]
Asst. Professor, Dept of Computing, Adama Science & Technology University, Adama, Ethiopia [3]
Assoc. Professor, Dept of Computing, Adama Science & Technology University, Adama, Ethiopia [4]

**Abstract**: Distributed Denial of Service attacks disrupts the availability of a service or resource in the internet. A substantial no of Distributed DoS attacks potential have to severely decrease backbone availability and which enable it to virtually detach a network from the net. As a result of the seriousness of the problem many defense methods have been proposed to combat these attacks. We present an extensive survey of DDoS detection methods as published in technical papers. The paper also highlights the open issues, research challenges and possible solutions. The purpose of the paper is usually to put some order into the existing defense methods, to ensure that a greater perception of DDoS attacks methods may be accomplished and subsequently better efficient and effective algorithms, techniques and procedures to combat these attacks could also be developed.

**Keywords**: Agent, Attacker, Denial of Service, Defense Mechanisms.

## I. INTRODUCTION

Denial of service attack programs are about for several years. The sources of single source attacks are countered easily by many existing defense mechanisms. These can be easily de-activated with improved tracking techniques. However, with the massive development of the net over the past, a progressively numerous vulnerable systems have become available to attackers. Attackers can hire these vulnerable hosts to launch an attack. A distributed denial of service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resources [1-2]. A DDoS attack occurs when the attacker uses many computers to launch a coordinated DoS attack against one or more victims.

According to the CERT/CC, the primary DDoS attacks occurred in 1999. In February 2000, one of the first major DDoS attacks was waged against yahoo.com, eCommerce, EBay and Amazon. This attack kept these off the web for about 2 hours and caused damage of 1.7 billion dollars. Another DDoS attack occurred in October 2002 against the 13 root servers that provide the DNS service to internet users around the world. If all 13 servers were to go down, there would be unfortunate problems accessing the web. Although the attack only lasted for an hour and the effects were hardly noticeable to the typical Internet user, it caused seven of the thirteen root servers to stop working. If unchecked, more powerful DDoS attacks might probably disable essential internet services in minutes [3].

DDoS attacks follow two kinds of architectures: the Agent-Handler architecture and the Internet Relay Chat (IRC) architecture. The Agent-Handler architecture for DDoS attacks is comprised of clients, handlers, and agents [4]. At first, the attacker builds a network of computers by discovering vulnerable hosts and uses them to produce the volume of traffic needed. Next, attacker will install attack tools on the compromised hosts of the attack network. The hosts running these attack tools are known as Handlers which works under the control of attacker. The hosts that have been infected by the attack tools look for other vulnerable hosts and install on them the same attack tool. The Agents are compromised hosts that are running an attack tool and also responsible for generating a stream of packets towards the intended victim. The users of the agent systems will be unaware of the situation.

In the IRC-based architecture, an IRC communication channel is used to connect the clients to the agents. IRC ports can be used for sending commands to the agents. The disadvantage of this architecture is that an attacker can hide his presence. An example includes Low Orbit Ion Cannon (LOIC) [5]. It has two versions: binary and web-based. It allows clients to connect remotely via the IRC protocol and to be a part of a system of victims. Among these two architectures, the Agent Handler architecture is commonly found in use in the literature.

The survey begins in Section II with the introduction of generic architectures of DDoS defense mechanisms classified based on locality of deployment. Section III discusses various methods for DDoS attack detection. Section IV discusses open issues and challenges faced by many researches.

## II. DEFENSE ARCHITECTURES

DDoS defense schemes can be divided into 3 classes based on the locality of deployment: victim-end, source-end, and intermediate network defense mechanisms. All of these approaches have their own benefits and downsides.

### A. *Source-end defense mechanisms*

A generic architecture of source-end defense schemes is shown in Figure 2. The choking component is used to impose rate limit on outgoing connections. The Detection engine compares each incoming and outgoing traffic statistics with some predefined traditional profiles.

It is best defense for detecting and stopping a DDoS attack at the source end which prevents the chance of flooding on the victim side and also in the whole network. This approach has two disadvantages: 1) it is difficult to detect DDoS attack at the source end because the sources are widely distributed and a single source behaves almost similarly as in normal traffic. 2) the difficulty of deploying system at the source end.

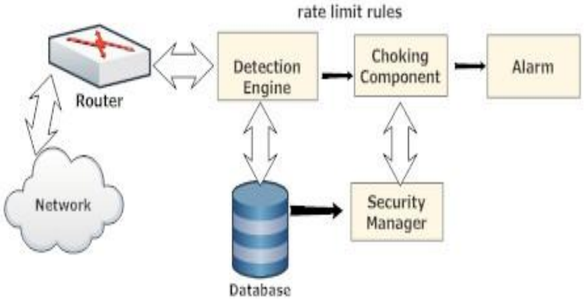

Fig 1: Architecture for source-end DDoS mechanism

### B. *Victim-end defense mechanisms*

Victim-end defense mechanisms are usually used in the routers of victim networks. A generic architecture of such schemes is shown in Figure 1. Here the detection engine is employed to detect attack either online or offline. The database stores data concerning about known attack signatures of normal behaviour. The security manager is responsible for updating attack signatures when the ascertained behaviour becomes available and also checks for any crucial events such as false alarms.

It is simple to detect DDoS attacks in victim routers due to the high rate of resource utilization. But it is very important to secure the network resources as used by Web Servers which provides services to the network users. This approach has two disadvantages: 1) victim resources typically get weak and the flow can’t be stopped on far side victim routers, 2) attacks can be detected only when it reaches the victim.

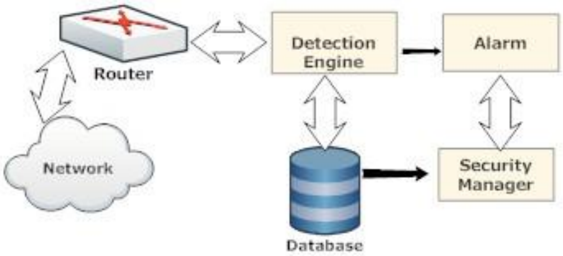

Fig 2: Architecture for victim-end DDoS Defense mechanism

### C. *Intermediate network defense mechanisms*

The intermediate network defense scheme balances the trade-offs between detection accuracy and attack bandwidth consumption, the main issues in source-end and victim-end detection approaches. Figure 3 shows a generic architecture of the intermediate network defense scheme which can be used in any network router. Such a scheme is usually cooperative in nature and also the routers share their observations with other routers. Like a source-end scheme, these schemes also impose rate limits on connections passing by the router when scrutiny with hold on normal profiles.

In this approach, detection and traceback of attack sources are simple because of cooperative operation. Routers can form an overlay mesh to share their observations [8]. One main drawback of this approach is deployability. All other routers on the network need to employ this detection scheme in order to achieve full detection accuracy. Obviously, full practical implementation of this scheme is extremely tough by reconfiguring all the routers on the Internet.

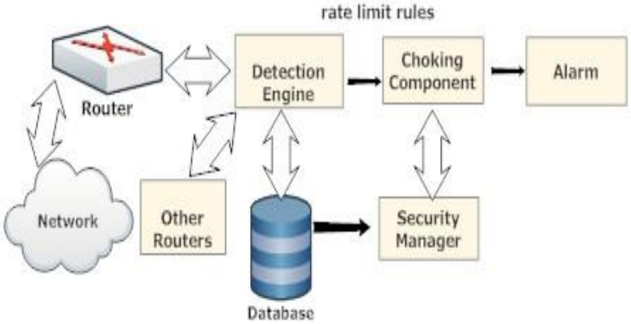

Fig 3: Architecture for intermediate network based DDoS mechanism

## III. RELATED WORK

In this particular section, we tend to present an outline of existing literature on DDoS attack defense mechanisms. These methods are based on the architectures mentioned above. We tend to discuss these schemes without considering their practical deployability in tangible networks. Recent trends show that soft computing approaches have been used heavily for DDoS attack detection. Ensembles of classifiers have also performed satisfactorily with high detection rates. We classify methods for DDoS attack detection into four major classes as shown in Figure 4.

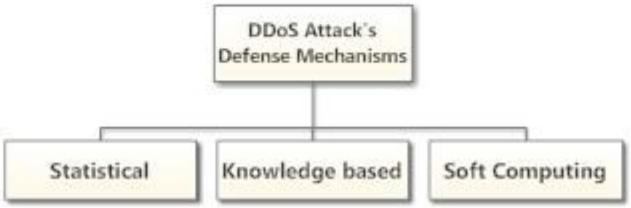

Fig 4: Classification of DDoS Attack detection methods

### A. *Statistical Methods*

Statistical properties of normal and attack patterns could be exploited for detection of DDoS attacks. A statistical inference test is applied to see whether any new instance belong to statistical model of normal traffic. Instances that won't comply with the learnt model are classified as anomalies.

A very famous DDoS defense scheme is D-WARD [6]. A D-WARD system is installed on source router that acts as gateway between the source network and the internet. It identifies an attack based on continuous watching of two-way traffic between the two networks. D-WARD compares the collected statistics with predefined model of normal traffic periodically. If the comparison result shows that there is the possibility of a DDoS attack, D-WARD will impose a rate limit on the suspicious outgoing flow for this peer. Each flow record kept by D-WARD contains statistics on three types of traffic: TCP, UDP and ICMP. This method offers a decent detection rate and also reduces DDoS attack traffic significantly.

Chen [7] presents two-sample t-test for DDoS Attacks. It confirms the normal distribution by obtaining statistics for normal SYN Arrival Rate. This method identifies an attack by computing difference a) between the number of SYN and ACK packets, and b) between incoming SAR and normal SAR. The proposal uses two statistical tests to identify malicious traffic. Firstly, it compares the differences involving the overall means of the incoming traffic arrival rate and the normal traffic arrival rate. If the difference is significant, it concludes that the traffic may include flooding attack packets. One drawback of this approach is that the low-rate attack traffic may pass the arrival rate test and make the backlog queue full. Then it compares the two groups that contain different numbers of SYN and ACK packets. If there is a significant difference, it witnesses that the attack traffic is mixed into the current traffic.

Akella et al. [8] proposed methods for an ISP network. In this mechanism, each router detects traffic anomalies using stream sampling algorithms. With this approach: 1) it is possible to profile normal traffic accurately, 2) identify anomalies with low false positive and false negative rates at the router, 3) be cost effective in terms of memory consumption and per packet computation, and 4) Routers can exchange data with one another to gather responses from all different routers concerning suspicions and based on them decide whether or not traffic aggregate is an attack or is normal.

### B. *Knowledge based Methods*

In this type of method, attack events are checked against predefined patterns of attack. General features of known attacks are formulated to identify actual occurrences of attacks. Examples of these approaches embody Expert systems, self organizing maps, signature analysis, and state transition analysis. Gil and Poletto [9] present a heuristic along with a data structure called MULti-Level Tree for Online Packet Statistics (MULTOPS), which monitor certain traffic characteristics used by routers to detect and eliminate DDoS attacks. It is a tree of nodes which contains packet rate statistics for subnet prefixes at different aggregation levels. Expansion and contraction of the tree happens inside a predefined memory size. The router using MULTOPS detects bandwidth attacks by the presence of a significant difference between packet rates about to and coming from the attacker.

Thomas et al. [10] present client-legitimacy-based DDoS filtering scheme known as **NetBouncer.** It is deployed near the victim side and it tries to detect legitimate clients. A NetBouncer device maintains a large legitimacy list of clients that have been proved to be legitimate. If packets are received from a client (source) not on the legitimacy list, a NetBouncer device will proceed to administer a variety of legitimacy tests to challenge the client to prove its legitimacy. If a client can pass these tests, it is added to the legitimacy list and subsequent packets from the client are accepted till a particular legitimacy window expires. The legitimacy of a client expires after a certain interval.

Wang et al. [11] proposed a formal method of modeling DDoS attacks using Augmented Attack Tree (AAT). They used AAT based attack detection algorithm. This model captures the attack patterns and the corresponding state transitions on the primary victim server. Limwiwatkul and Rungsawang [12] propose to find DDoS attack signatures by analyzing the TCP/IP packet header against predefined rules and distinguishing normal and abnormal traffic. They focus on TCP/IP, ICMP, and UDP flooding attacks.

Zhang and Parashar [13] propose a distributed approach to detect DDoS attacks. This approach detects and stops DDoS attacks independently in the intermediate network. A communication mechanism is used to exchange data about network attacks between the independent detection nodes to aggregate data about the overall network attacks. The individual defense nodes obtain approximate data about global network attacks and can stop them more effectively and accurately. Lu et al. [14] describe DDoS system which analyses the traffic at edge routers of an ISP Network. This approach can detect and identify attack packets without modifying existing IP forwarding mechanisms at routers accurately.

Dogawon seo et al. [15] proposes Probabilistic Filter Scheduling (PFS), to efficiently defeat DDoS attacks and to satisfy the necessary properties. In PFS, filter routers identify attack paths using probabilistic packet marking, and maintain filters using a scheduling policy to maximize the defense effectiveness. Experiment Results show that PFS achieves 44% higher effectiveness than other filter-based approaches.

### *C. Soft Computing Methods*

Soft computing is a general term for describing a collection of optimization and processing techniques that are tolerant of imprecision and uncertainty. Jalili et al. [16] introduce SPUNNID, a DDoS attack detection system based on statistical pre-processor and unsupervised artificial neural nets. The statistical pre-processing techniques are used to extract features from the traffic, and an unsupervised neural net used to research and classify traffic patterns as either a DDoS attack or normal.

Karimazad and Faraahi [17] propose an anomaly based DDoS detection method. The attack packets are analysed using Radial Basis Function (RBF) neural networks. The method can be applied to edge routers of victim networks. Seven featured Vectors are used to activate an RBF neural network at each time window. The RBF neural network classifies data to be either normal or attack. If the incoming traffic is recognized as attack traffic, then the source IP addresses of the attack packets are sent to the Filtering Module and also the Attack Alarm Module for further actions. Otherwise, if the traffic is normal, it is sent to their destinations.

Gavrilis and Dermatas [18] also present a detector for DDoS attacks based on estimated statistical features in short-time window analysis of incoming data packets in public networks. Statistical descriptors are used to describe the behavior of the DDoS attacks. An accurate classification is achieved using RBF neural networks. Wu et al. [19] propose to detect DDoS attacks using grey relational analysis and decision trees. They use fifteen attributes which monitor the in/out packet/byte rate and also compile the TCP, SYN, and ACK flag rates, to describe the traffic pattern. The decision tree technique develops a classifier to detect abnormal traffic flow. They also use a novel traffic pattern matching technique to spot traffic flow like the attack flow and to trace back the origin of an attack based on this similarity.

Nguyen and Choi [20] develop a mechanism that classifies the network status. They divide a DDoS attack into phases and choose features based on an investigation of DDoS attacks. Finally, they apply the k-nearest neighbor (KNN) method to classify the network status in every phase of DDoS attack. A method presented in [21] detects DDoS attacks based on a fuzzy estimator using mean packet inter-arrival times. It detects the suspected host and traces the IP address to drop packets within 3 second detection windows.

Lately ensembles of classifiers have been used for DDoS attack detection. An ensemble of classifiers has been used by [22] for this purpose where a Resilient Back Propagation (RBP) neural network is chosen as the base classifier. They tried to improve the performance of the base classifier.

An effective defense system to guard network servers, network routers, and client hosts from changing into handlers, zombies, and victims of DDoS flood attacks is given in [23]. The NetShield system protects any IP-based public network on the Internet. It uses preventive and deterrent controls to remove system vulnerabilities on victims. Adaptation techniques are used to launch protocol anomaly detection and provide corrective intrusion responses. The NetShield system enforces dynamic security policies. NetShield is particularly tailored for protecting network resources against DDoS attacks.

Chen et al. [24] present a comprehensive framework for DDoS attack detection known as DDoS Container. It works in inline mode to examine and manipulate traffic in real time. DDoS container will do inspection on data streams and correlates attack events in different sessions. It terminates a session when it detects an attack. Rahmani et al. [25] discuss an entropy analysis of multiple traffic distributions for DDoS attack detection. They observed the time series of IPflow numbers and aggregate traffic sizes are statistically dependant. The occurrence of an attack will affects this dependence and causes a rupture in the time series for joint entropy values. The results show that this method can lead to more accurate and effective DDoS detection.

A low rate DDoS attack has vital ability to hide its traffic because of its similarity with normal traffic. Xiang et al. [26] propose two metrics: i) generalized entropy metric, and ii) information distance metric for detecting low rate DDoS attacks. An attack is identified by measuring the distance between legitimate traffic and attack traffic. The generalized entropy metric is more effective than the metric in [27]. Additionally, the information distance metric outperforms the favoured Kullback-Leibler divergence approach. The approach reported in [28] analyses DDoS and flash crowd characteristics and provides an effective way to distinguish between the two in VoIP networks. The authors validate the method by simulation. A wavelet transformation and probability theory based network anomaly detection approach is projected in [29]. The approach is able to identify known as well as unknown attacks. Zhong and Yue [30] present a DDoS attack detection model which extracts a network traffic model and a network packet protocol status model and sets the limit for the detection model. Captured network traffic values are clustered based on the k-means clustering algorithm to build initial threshold values for network traffic. All captured packets are used to build the packet protocol status model using the Apriori and FCM [31] algorithms. Whenever the current network traffic is over the threshold value, the network packet protocol status is tested to detect abnormal packets. If there are no abnormal packets, the current network traffic is clustered again by the k-means module to build a new threshold value model.

A two-stage automated system is projected in [32] to detect DDoS attacks. It combines traditional change point detection approach with a novel one [33]. The authors check the system using a set of publicly available attack-free traffic traces. Gupta et al. [34] use ANN to count the number of slaves or zombies in a DDoS attack. They use sample data to coach a feed-forward neural network which is generated using the NS-2 network simulator. A port-to-port specific traffic in a router known as IF flow is introduced in [35]. A very important feature of IF flow is that it can amplify the attack to normal traffic ratio. A Recursive Least Square (RLS) filter is employed to predict IF flows. Next, a statistical method using a residual filtered process is used to detect anomalies. The authors applied the method to three types of traffic: IF flows, input links and output links in a router to compare the anomaly detection results using ROC curves. Experiment results show that IF flows are more powerful than other two input links and output links for DDoS attack detection.

Cheng et al. [36] propose the IP Address Interaction Feature (IAI) algorithm considering interactions among addresses, abrupt traffic changes, many-to-one asymmetries among addresses, distributed source IP addresses and target addresses. The algorithm describes the important characteristics of network flow states. Next, a SVM (Support Vector Machine) classifier is applied to classify the state of current network flows in order to identify the DDoS attacks. Experimental results show that the IAI based detection approach can distinguish between normal and abnormal flows and also help to identify quick and correct attack flows when the attacking traffic is hidden. This approach has higher detection of attacks and lower false alarm rates when compared to other competing techniques.

The method presented in [37] will determine flooding attacks in real time and can also assess the intensity of the attackers based on fuzzy reasoning. Firstly, the method analyse network traffic time series using Schwarz information criterion (SIC) and discrete wavelet transform to find the change point of the Hurst parameters resulting from DDoS flood attack. Next, it will do the identification and assessment of the DDoS attacks based on an intelligent fuzzy reasoning mechanism. The Test results demonstrate that the method could detect DDoS flood attack intelligently and effectively. Zhang et al. [38] present a CPR (Congestion Participation Rate) based approach to detect low-rate DDoS (LDDoS) attacks using flow level network traffic. A flow with higher CPR value leads to LDDoS and consequent dropping of the packets. The authors evaluate the mechanism using ns2 simulation; tested experiments and Internet traffic trace and claim that the method can detect LDDoS flows effectively. In [39], a mathematical model is presented to provide gross evaluation of the benefits of DDoS defense based on dropping of attack traffic. Simulation results and tested experiments are used to validate the model. In the same work, the authors also consider an autonomic defense mechanism based on CPN (Cognitive Packet Network) protocol and establish it to be capable of tracing back flows coming into a node automatically.

## IV. OPEN ISSUES AND CHALLENGES

Many strategies for DDoS detection have been reported in the literature, however only a couple of them are applied in a real network environment and work effectively. Designing and implementing a perfect and sensible DDoS defense system is really difficult. An ideal DDoS defense mechanisms should have the following characteristics: effective, transparent to existing Internet infrastructure, low performance overhead, invulnerable to attacks aim at defense system, incremental deployable and no impact on the legitimate traffic.

| Type of Classifier | Authors | Title of Paper | Objective |
|---|---|---|---|
| Statistical | Mikoviac et al. | Attacking DDoS at source | A D-WARD system identifies an attack based on continuous watching of two-way traffic between the two networks. |
| | Chen C.L | A new detection method for distributed denial service of attacks traffic based on statistical tests | Presents two sample test for DDoS attacks. |
| | Akella et al. | Detecting DDoS Attacks on ISP networks | Detects traffic anomalies using sampling algorithms |
| Knowledge based | Gil et al. | A data structure for bandwidth attack detection | A Data Structure, MULTOPS monitors the traffic characteristics used by routers. |
| | Thomas R et al. | NetBouncer: Client-legitimacy based higher performance DDoS filtering | Presents DDoS filtering scheme NetBouncer which maintains a list of legitimate clients. |

| | | | |
|---|---|---|---|
| | Wang J et al. | Augmented attack tree modeling of distributed denial of services and tree based attack detection method | Propose a model using Augmented Attack Tree. |
| | Limwiwatkul L et al. | Distributed denial of service detection using TCP/IP header and traffic measurement analysis | Finds attack signatures by analyzing TCP/IP header. |
| | Zhang G et al. | Coperative defense against DDoS Attacks | Propose distributed approach for detecting and stopping attacks independently in intermediate network. |
| | Lu et al. | Robust and efficient detection of DDoS Attacks for large-scale internet | Analyze the traffic at edge routers of an ISP network. |
| | Dongwon Seo et al. | Probabilistic Filter Scheduling against Distributed denial of service attacks | Propose Probabilitistic filter scheduling detect attacks |
| Soft Computing | Jalili R et al. | Detection of Distributed denial of service attacks using statistical pre-processor and unsupervised neural networks | Introduce SPUNNED, system based on statistical preprocessor and unsupervised artificial neural network. |
| | Karimazad R et al. | An anomaly based method for DDoS attacks detection using RBF neural networks | Propose an anomaly detection system which analyses attacks using Radial Basis Function neural networks. |
| | Garvilis D et al. | Real time detection of distributed denial of service attacks using RBF networks and statistical features | Present detector for DDoS attacks based on estimated statistical features. |
| | Wu Y C et al. | DDoS detection and traceback with decision tree and grey relational analysis | Detects attacks using grey relational analysis and decision trees. |
| | Nguyen et al. | Proactive detection of DDoS attacks utilizing K-NN classifier in an Anti-DDoS framework | Develop a mechanism that classifies the network status. |
| | Shiaeles S N et al. | Real-time DDoS detection using fuzzy estimators | Detects attacks based on fuzzy estimators. |
| | Kumar P A R et al. | Distributed denial of service attack detection using an ensemble of neural classifier | An essemble of classifier used which uses Resilient Back Propagation |
| | Hwang K Dave et al. | NetShield: Protocol anomaly detection with data mining against DDoS attacks | Propose a NetShiled system that protects any IP based public network. |
| | Chen Z et al. | An inline detection and prevention framework for distributed denial of service attacks | Present a framework known as DDoS Container. |
| | Rahmani H et al. | Joint entropy analysis model for DDoS detection | Discuss an entropy analysis of multiple traffic distributions. |
| | Xiang Y et al. | Low rate DDoS attacks detection and traceback by using new information metrics. | Propose a two stage metric for detecting attacks. |
| | Shannon et al. | A mathematical theory of communication | Propose a metric for DDoS attacks. |
| | Jeyanthi N et al. | An entropy based approach to detect and distinguish DDoS Attacks from flash crowds in VOIP networks | Analyze the traffic in VOIP networks. |
| | Li M et al. | A new approach for detecting DDoS attacks based on wavelet analysis | Use wavelet transformation probability theory. |
| | Zhong R et al. | DDoS detection system based on data mining | Present a model which extracts a network traffic model and network status model. |

| | | | |
|---|---|---|---|
| | Agarwal R et al. | Fast algorithms for mining association rules in large databases | Use Data mining algorithms for detecting DDoS attacks. |
| | Dainotti R et al. | A cascade architecture for DoS attack detection based on wavelet transform | Present a system which combines traditional change point with novel one. |
| | Gupta B et al. | ANN based scheme to predict number of zombies in DDoS attack | Use ANN to count no of slaves and zombies in DDoS attacks. |
| | Yan R et al. | A new way to detect DDoS attacks within single router | Present an IPFlow which amplifies an attack to normal traffic ratio. |
| | Cheng J et al. | DDoS attack detection using IP address feature interaction | Propose an IP address Interaction Feature Algorithm. |
| | Xia Z et al. | Enhancing DDoS flood attack detection via intelligent fuzzy logic | Determines flooding attack and also access intensity of the attackers. |
| | Zhang C et al | FLow level detection and filtering of low rate DDoS | Present Congestion Participation rate to detect low rate attacks. |
| | Gelenbe E et al. | A self-aware approach to denial of service defense | Present mathematical model which provides gross evaluation of DDoS defense methods. |

Table1: Survey of papers

The main challenges that any DDoS defense scheme should overcome to become ideally usable are given below.

1. More emphasis must be given to speed over accuracy of detection because faster detection scheme usually consumes higher processing power which can also affects detection accuracy.
2. Real time detection of low rate DDoS attacks with detection accuracy high and low false alarm could be a challenging task, since such traffic follows the normal traffic distribution.
3. Real time DDoS detection systems are expected to be scalable for use in high speed real networks.
4. Developing a combined approach based on both supervised and unsupervised approaches with the capability of detecting both known and unknown attacks real time or near real time is of utmost necessity.
5. Accurate segregation of high-rate DDoS attack traffic from normal flash crowds with minimum resource consumption or low false alarm rate in real-time or near real-time is a challenging task.
6. Transparency to existing Internet infrastructure is incredibly important in terms of deployment. So, a DDoS defense scheme should be deployable in real networks.
7. High speed traffic analysis for detecting DDoS attacks is a difficult task. A defense scheme capable of real time detection should perform well with high speed traffic.
8. Real time updation of network statistics and quick identification of randomized spoofed IP addresses are challenges.
9. A DDoS defense mechanism aiming to give a near real time solution may have to be based on an incremental clustering algorithm to segregate the attack from normal traffic. This requires an appropriate proximity measure that works sensibly, quickly and reliably.
10. The detection method should be dependent on a minimum number of input parameters if not independent of parameters and should also be based on a minimum no of traffic parameters or features.

## V. CONCLUSION

In this paper, we have presented an overview of DDoS defense schemes and at last open issues and challenges. Practically designing and implementing a DDoS defense is incredibly difficult. While developing a DDoS defense scheme, the issues discussed in this paper need to be deliberated and considered with due seriousness. The comparison of the existing detection mechanisms shows that the majority schemes are not capable of fulfilling all the requirements for real time network defense. Different performance parameters have to be balanced against each other finely and fitly.

## REFERENCES

[1] Peng, T., Leckie, C., and Ramamohanarao, K. (2007) Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Survey, 39, 3:1–3:42.

[2] Lin, S. and Chiueh, T. C. (2006) A survey on solutions to distributed denial of service attacks. Technical Report TR201, Department of Computer Science, State University of New York, http://www.ecsl.cs.sunysb.edu/tr/TR201.pdf.

[3] CERT Coordination Center, Denial of Service attacks, Available from http://wwww.cert.org/tech_tips/denial_of_service.html

[4] Specht, S. M. and Lee, R. B. (2004) Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems, San Francisco, California, USA, 15-17 September, pp. 543–550. ISCA.

[5] Batishchev, A. M. (2004). LOIC(Low Orbit Ion Cannon). http://sourceforge.net/projects/loic/.

[6] Mirkoviac, J., Prier, G., and Reiher, P. (2002) Attacking DDoS at the source. Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS.

[7] Chen, C. L. (2009) A new detection method for distributed denial-of-service attack traffic based on statistical test. Journal of Universal Computer Science, 15, 488–504.

[8] Akella, A., Bharambe, A., Reiter, M., and Seshan, S. (2003) Detecting DDoS attacks on ISP networks. Proceedings of the Workshop on Management and Processing of Data Streams, San Diego, CA, 8 June, pp. 1–2. ACM.

[9] Gil, T. M. and Poletto, M. (2001) MULTOPS: a datastructure for bandwidth attack detection. Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 13-17 August 3.USENIX Association Berkeley.

[10] Thomas, R., Mark, B., Johnson, T., and Croall, J. (2003) NetBouncer: Client-legitimacy-based highperformance DDoS filtering. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington, DC, 22-24 April, pp. 111–113. IEEE CS, USA.

[11] Wang, J., Phan, R. C. W., Whitley, J. N., and Parish, D. J. (2010) Augmented attack tree modeling of distributed denial of services and tree based attack detection method. Proceedings of the 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July, pp. 1009–1014. IEEE CS.

[12] Limwiwatkul, L. and Rungsawang, A. (2004) Distributed denial of service detection using TCP/IP header and traffic measurement analysis. Proceedings of the IEEE International Symposium Communications and Information Technology, Sapporo, Japan, 26-29 October, pp. 605–610. IEEE CS.

[13] Zhang, G. and Parashar, M. (2006) Cooperative defence against DDoS attacks. Journal of Research and Practice in Information Technology, 38, 1–14. [42] Lu, K., Wu, D., Fan, J., Todorovic, S., and Nucci, A. (2007) Robust and efficient detection of DDoS attacks for large-scale internet. Computer Networks, 51, 5036– 5056.

[14] Lu, K., Wu, D., Fan, J., Todorovic, S., and Nucci, A (2007) Robust and efficient detection of DDoS attacks for large-scale internet. Computer Networks, 51, 5036– 5056.

[15] Dongwon Seo, Heejo Lee and Adrian Perrig, “PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks”, 36th Annual IEEE Conference on Local Computer Networks( LCN 2011), pages 9-17.

[16] Jalili, R., Imani-Mehr, F., Amini, M., and Shahriari, H. R. (2005) Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks. Proceedings of the Internationational conference on information security practice and experience, Singapore, 11-14 April, pp. 192–203.

[17] Karimazad, R. and Faraahi, A. (2011) An anomalybased method for DDoS attacks detection using rbf neural networks. Proceedings of the International Conference on Network and Electronics Engineering, Singapore, pp. 44–48. IACSIT Press.

[18] Gavrilis, D. and Dermatas, E. (2005) Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. Computer Networks and ISDN Systems, 48, 235–245.

[19] Wu, Y. C., Tseng, H. R., Yang, W., and Jan, R. H. (2011) DDoS detection and traceback with decision tree and grey relational analysis. International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136.

[20] 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.

[21] Shiaeles, S. N., Katos, V., Karakos, A. S., and Papadopoulos, B. K. (2012) Real time DDoS detection using fuzzy estimators. Computers & Security, 31, 782–790.

[22] Kumar, P. A. R. and Selvakumar, S. (2011) Distributed denial of service attack detection using an ensemble of neural classifier. Computer Communication, 34, 1328–1341.

[23] Hwang, K., Dave, P., and Tanachaiwiwat, S. (2003) NetShield: Protocol anomaly detection with datamining against DDoS attacks. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, 8-10 September, pp. 8–10. Springer-verlag.

[24] Chen, Z., Chen, Z., and Delis, A. (2007) An inline detection and prevention framework for distributed denial of service attacks. Comp. J., 50, 7–40. [45] Lee, K., Kim, J., Kwon, K. H., Han, Y., and Kim, S. (2008) DDoS attack detection method using cluster analysis. Expert Systems with Applications, 34, 1659–1665.

[25] Rahmani, H., Sahli, N., and Kammoun, F. (2009) Joint entropy analysis model for DDoS attack detection. Proceedings of the 5th International Conference on Information Assurance and Security -

[26] Xiang, Y., Li, K., and Zhou, W. (2011) Low rate DDoS attacks detection and traceback by using new information metrics. IEEE Transactions on Information Forensics and Security, 6, 426–437.

[27] Shannon, C. E. (1948) A mathematical theory of communication. Bell system technical journal, 27, 397–423.

[28] Jeyanthi, N. and Iyengar, N. C. S. N. (2012) An entropy based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks. International Journal of Network Security, 14, 257–269.

[29] Li, M. and Li, M. (2009) A new approach for detecting DDoS attacks based on wavelet analysis. Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17-19 October, pp. 1–5. IEEE.

[30] Zhong, R. and Yue, G. (2010) DDoS detection system based on data mining. Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher.

[31] Agrawal, R. and Srikant, R. (1994) Fast algorithms for mining association rules in large databases. Proceedings of the 20th International Conference on Very Large Data Bases, Santiago de Chile, Chile, 12-15 September, pp. 487–499. Morgan Kaufmann.

[32] Dainotti, A., Pescap´e, A., and Ventre, G. (2009) A cascade architecture for DoS attacks detection based on the wavelet transform. Journal of Computer Security, 17, 945–968.

[33] Haar, A. (1910) Zur Theorie der orthogonalen Funktionensysteme. Mathematische Annalen, 69, 331–371.

[34] Gupta, B. B., Joshi, R. C., and Misra, M. (2012) ANN based scheme to predict number of zombies in DDoS attack. International Journal of Network Security, 14, 36–45.

[35] Yan, R., Zheng, Q., Niu, G., and Gao, S. (2008) A new way to detect DDoS attacks within single router. Proccedings of the 11th IEEE Singapore International Conference on Communication Systems, Guangzhou, China, 19-21 November, pp. 1192–1196. IEEE CS.

[36] Cheng, J., Yin, J., Liu, Y., Cai, Z., and Wu, C. (2009) DDoS attack detection using IP address feature interaction. Proceedings of the 1st International Conference on Intelligent Networking and Collaborative Systems, Barcelona, Spain, 4-6 November, pp. 113–118. IEEE CS.

[37] Xia, Z., Lu, S., Li, J., and Tang, J. (2010) Enhancing DDoS flood attack detection via intelligent fuzzy logic. Informatica (Slovenia), 34, 497–507.

[38] Zhang, C., Cai, Z., Chen, W., Luo, X., and Yin, J. (2012) Flow level detection and filtering of low-rate DDoS. Computer Networks, 56, 3417–3431.

Gelenbe, E. and Loukas, G. (2007) A self-aware approach to denial of service defense. Computer Networks, 51, 1299–1314.