Countermeasures against Distributed Denial of Service
A Literature Review

Manish Gupta, Gayathri Gopalakrishnan, and Raj Sharman
School of Management
State University of New York
Buffalo, NY, USA
{mgupta3, g5, rsharman}@buffalo.edu

Abstract—A distributed denial-of-service (DDoS) attack is carried out by simultaneously by compromised systems against targets causing system and service unavailability. Regardless of industry and size, companies worldwide are increasingly becoming target of DDoS attacks. The sophistication and intensity of these attacks are exponentially rising due to increase in number of compromised systems, unpatched vulnerabilities and increased business impact. The paper reviews more than 200 research articles in the area of DDoS, of which 142 present countermeasures and mitigation against DDoS. The paper develops an ontological framework to classify the proposed mitigation methods under three layers of defense-in-depth – prevent, detect and respond. Research done each of these 3 pillars are further conceptualized based on underlying design and security principles. The paper also proposes alternate classification schemes based on placements of target components, while presenting qualitative analyses on research activities on DDoS

Keywords—distributed denial of service, botnets, availability, network attack, traffic detection, bandwidth consumption, resource exhaustion

I. INTRODUCTION

An application server can provide many services to the clients. There are multiple users who access the system simultaneously. Regular service is provided when clients can access the service without any interruption. A service can be delayed due to various reasons. One reason could be that the resources of the server are insufficient (server features may not be designed well) or there could be flaws within the system. A denial of service happens when a client is denied of the access to a particular system or denied information or any service from a system. Then the question may arise whether the denial of service can be intentional or unintentional. It may happen in both ways. Imagine a situation when a disaster occurs; the service may be interrupted till the time the backups are restored. This is an example of an external factor which would interrupt the service. The internal factors can be due to reasons mentioned earlier like insufficient care given to details while designing the service architecture.

An intentional attack can be influenced by several factors like monetary gains, competence or it can be politically motivated. An attacker may adopt several ways to interrupt the services. An attacker can either directly attack the source with many requests or utilize the bandwidth of the communication channel. A good detection mechanism will look for balancing the server load at the same time keep a watch on the utilization of resources. A good defense mechanism will try to mitigate the attack as well to make sure the legitimate clients are served. But good security policies can help preventing the attacks most of the time although they cannot be completely avoided.

A distributed denial of service happens when there are multiple points of attack sources. The attacker can form the army of vulnerable systems in network to attack the server. A potential impact is business may find loss of revenue due downtime and a trace back is difficult due to innocent servers used as attackers. There can be attacks where IPs are spoofed as well. Typically, the DDoS attacks can be executed with these major components-an attacker, a proper mechanism, the victim/target server and the innocent intermediate servers. In case of DDoS, the bots or zombies participate in the attack unintentionally. This paper reviews literature on countermeasure suggested to mitigate risks from DDoS attacks and classifies these countermeasures in an ontological framework. A review of 142 papers provided key insights to categorize them using a 3-layered defense in depth model. The paper categorizes each paper into one of the categories. This provides a complete and holistic view of research on DDoS protection. We also compared our work against other review and survey papers on similar topic and found our contribution is unique and novel in terms of coverage and in ontological development. The details of each of the papers have not been included in this research due to lack of space. The contributions of the paper can help researchers and practitioners alike understand how DDoS protection research has evolved over last decade or more to be better informed in their decisions.

II. PRELIMINARIES

1. DDoS Attack

The DDoS attack is planned strategically. DDoS is not an uncommon event for more than a decade. The motivation could be malevolent aiming at the destruction of the entire system. It can be monetary gains or even politically motivated. Attacks against banking industry can be really devastating. The DDoS attacks start with initiating control on systems that can act as command and control servers. The command and control servers can give command to other vulnerable systems identified by scanning process. An army is formed in order to
launch the attack. A specific time is decided in order to launch the attack. This will ensure that all the nodes send packets to the target at the same time duration thus causing congestion at the bandwidth or the server memory level. The attacks may last for hours. The aftermath can be the target can be crashed due to overload and the service provided will be temporarily disrupted. The resilience depends on the timely identification of attack, tracing the attack or blocking the illegitimate traffic caused by the attack.

There is a continuous research process which aims at saving the business owners from negative and worst consequences of these attacks. There are many successful and innovative result oriented methodologies but there are few which may not have succeeded in the real world but can be a strong weapon in the future if they can be molded well.

There are some unique features to the DDoS attacks. They are distributed in nature. The impact is much high compared to an attack from a single source. Within a short span of time they can cause much disruption to the system. Over the years much paper has researched on DDoS attacks as well. But are they covering DoS defense as well? To answer this question, we need to look whether the defense mechanisms take into account the distributed nature of the attacks. Some of the common techniques to detect DDoS attacks are tracing the source, statistical analysis on the flow of traffic and detection of self-similarity in the attack traffic. Many of these apply for DoS as well. Although there can be an overlap, there are few defense mechanisms that can be unique to DDoS like analysis on similarity based on source information as there is only one source of attack in case of DoS.”.

2. **State of System**

A system can be visualized to have the following states. In healthy state, a system can provide services to its clients without any failure. A proactive measure can help the system retain its normal behavior. Figure 1 shows states of a network system. An attack traffic will cause disturbances in the normal performance of the client. The load is unbalanced. When a system detects an attack and knows how to mitigate, it moves to the defense state. On applying policies and recovering activities, system can move back to healthy state. While an attack happens, the survivability of system depends on its resilience. If the resilience is less, then the system may go to exhausted state. Several activities like clearing memory buffer, etc. would be required to regain a balanced state.

### III. LITERATURE REVIEW

The following sources are used to collected the papers

1) ACM Digital Library
2) IEEE Xplore
3) ScienceDirect – Elsevier
4) Google Scholar

The keywords used to search are ‘Distributed Denial of service’, ‘Distributed Denial of service attacks and defense’.

The number of papers have increased over the last decade especially a high peak can be observed from 2011 to 2012 and 2013. This proves the fact that much focus is being given recently to defending against DDoS attacks. The attacks are really common with rented bots being available in the market. The Figure 2 shows this trend. The Figure 3 above shows the number of conference proceedings and journals in each year. The papers collected are broadly classified into defense techniques, Survey papers, DDoS Analysis and DoS.
The defense techniques include the papers that focus on one or the other kind of mechanisms against DDoS discussed later in the paper. The defense techniques are classified and the papers are categorized accordingly. These papers usually observe a particular aspect of the attack traffic and then use this aspect to detect and track the attacks. Majority of the papers have simulated the techniques described using simulation tools like NS-2 or other experimental set ups. Table 1 shows this distribution. The practical aspects of implementation are not fully discussed in many of these papers. The survey papers have classified the defense techniques. There has been many base of classification. The third section of papers include those papers which cover the impact of DDoS attacks, the possibility of attacks on few architectures, simulation mechanisms for studying and analyzing the defense techniques. These papers also include different types of attacks, evolution of attacks. Few papers that completely focus on Denial of Service are also collected.

IV. CLASSIFICATION SCHEME

A good classification scheme helps in analyzing the current trends of the research in the field. The classification scheme presented in this paper takes into account different aspects of the defense technique. The classification is based on an extensive review of collection of DDoS papers. All activities done to protect against DDoS can be broadly classified into three types – based on the action performed – Prevention techniques, Detection techniques and Reaction or responses. Although the mechanisms can be classified, they are a continuous process. An organization needs to do continuous improvement on these areas in order to sustain in the world of threats and attacks. Figure 4 shows the classification that we came up with based on literature review. The following sections discuss each of these categories (boxes), using the same numbering scheme as Figure 4.

<table>
<thead>
<tr>
<th>Type of papers</th>
<th>Number of papers collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Techniques</td>
<td>142</td>
</tr>
<tr>
<td>Survey papers</td>
<td>16</td>
</tr>
<tr>
<td>Analysis on DDoS</td>
<td>23</td>
</tr>
<tr>
<td>Papers focusing on DoS</td>
<td>20</td>
</tr>
</tbody>
</table>

The following sections discuss each of these categories (boxes), using the same numbering scheme as Figure 4.

1. Prevent

Any proactive measure fall under prevention category. These can include stringent security policies that can even protect the system from intrusions, denial of service or any malware activities. The research in prevention techniques require more attention compared to the detection techniques as the attacks can be stopped earlier without much resource wastage. These types of techniques require immense knowledge of attacks, botnet formation and vulnerability detection in networks.

1.1. Tightened Security

The kind of prevention mechanisms are more into securing own systems or using stringent policies by ISP networks. Some of the key aspects in these papers are focused on security policies by ISPs (internet service providers) or

![Fig. 4. Classification of DDoS Countermeasures](attachment:fig4.png)
segmenting the network into domain and apply token systems. The concept is more focused to security in individual systems or network domains. The more secure systems are, the attackers find it difficult to capture vulnerable systems.

1.2. Prevent Botnet Formation

A DDoS attack is launched using bots or zombies. Attackers search for vulnerable systems. In case the systems are vulnerable enough to install a malware then they are used as C&C servers (Command and Control Servers). These C&C servers in turn command other zombies to perform the attack. The papers that focus on preventing botnet formation cover key concepts like preventing systems from being botnets, developing botnet detection strategies, etc. For example, building a tool to detect if a computer is a bot depending on the traffic flow. The key idea is that vulnerability of the system must not be exploited to form an army of bot network.

1.3. Source Verification

In source verification methods, the hosts or routers try to verify the source of the attack. The host ensures that the connection set up is attempted by a human and not a bot. These mechanisms use the packet header information and see if the packet can be trusted. In application level, the users can be sent a text based question or CAPTCHA puzzle to verify their authenticity. These type of mechanisms checks for the authenticity of a packet by checking its source. The packets may follow a certain path or contain unique ID that can be verified.

2. Detect

The alarm of DDoS has to be within shortest time possible and as accurate as it can be. A good separation from the legitimate packets is desired. This ensures that legitimate clients are served during attack.

2.1. Anomaly Based

Anomaly means deviation from a normal behavior. These type of defense mechanisms record the behavior of traffic and perform monitoring in order to detect any anomaly. Anomaly can be either volume based or content based.

2.1.1 Rate Anomaly

Statistical analysis/Computational

Some of the defense mechanisms apply methods like probabilities, entropy variations, etc. They use information like flow rate, source and destination IPs, traffic volume, open connections, time series data to analyze and then detect an attack. The papers usually suggest algorithms that can be implemented in router or victim and more of a comparison from a predicted behavior. These papers cover techniques that use neural networks, chaos theory or fuzzy logic to detect an anomaly. Based on the previous learning (when there is no attack), these mechanisms can be used to detect any deviation from normal behavior. A set of fuzzy rules can be built on data that are captured during normal traffic flow.

2.1.2 Volume Anomaly

A volume anomaly can be detected when there is an unusual volume of traffic in the network or in the servers. The papers that use volume anomaly as detection mechanism look at the packet counts, traffic congestion at edge routers or unusually large number of packets to a particular server. The main idea is that there can be large number of packets or heavy packets (with large packet length) in the traffic during an attack time.

2.1.2.1 Server Load

The papers that cover these type of anomaly detection look at the resource consumption in the server side. During an attack, much memory will be utilized due to large number of incoming packets. The flow may be less but the packet lengths could be high. The papers look in to those factors that can be detected in the server. For example, a regulator can be placed on the server side to check the traffic that are having much resource consumption.

2.1.2.2 Network Congestion

A network congestion can be detected locally or globally. Routers can detect for an anomaly and share the information with other routers. The bandwidth of the communication channel to the victim may be consumed due to the attack traffic. During an attack, areas of high network congestion can be identified based on the traffic flow rates.

2.1.3 Veracity Anomaly

These type of defense mechanisms check the source information of packet and see if they are legitimate. The veracity anomaly based techniques are much closely related to the reaction (traceback) mechanisms.

2.1.4 Other Anomaly

The content anomaly detection mechanisms look for any deviation in the packet contents. These can be the packet behavior or access behavior. A user can access for documents that are not commonly accessed.

2.1.4.1 Access Behavior

An access behavior may be recorded for the clients based on their common access behavior. This may include the way the users access the documents or requests that have heavy packets as replies or request for documents that are not commonly accessed. The papers that cover this type of mechanisms include the papers that compute the connection scores of the clients. The defense mechanisms to detect application layer attacks can be categorized here. An example would be frequency of page visits compared to normal behavior.

2.1.4.2 Incomplete Connections/Probing

Every protocol has a sequence of activities/rules and all the network components need to adhere with those rules. During an attack, it can be noticed that some of the packets or
connection requests do not completely obey these rules. These type of mechanisms look for such activities by the clients and detect DDoS attack. The symmetric behavior of protocols is used as the base to detect any suspicious behavior.

Incomplete connections

The type of mechanisms that check for incomplete connections are usually at the server side. For example, incomplete HTTP requests can be checked. In TCP SYN attack, the zombies do not reply for the SYN ACK acknowledgement (When a server receives a SYN packet, it replies with a SYN ACK and expects ACK packet from the client to complete the connection). Some mechanisms also check if the packets are paired. For example, if for every TCP SYN packet, there is an ACK packet. These methods are usually found in router level.

Probing

The papers under this category check for the legitimacy of packets by probing the delay in network or validating the membership in P2P networks.

2.2 Similarity Based

It can be observed that the attacks can be similar in nature either due to the fact that they are planned to be active at the same time, request for same information or originate from similar source. These type of defense mechanisms look for similarity in traffic features or packet requests.

Clustering

The papers classified under this category utilize the clustering to group the traffic that are similar. The main concept behind this is that the attack traffic can be similar to each other. Some of the similarities could be size of the packets, the interval of the packets.

Correlation

These mechanisms look into similarity but use other correlation techniques like regression analysis to look for any correlation in time series of traffic.

3. React

After detecting an attack, the system need to take necessary actions to mitigate the attack. The reaction can be either traceback or filtering (mitigate the attack traffic) or creating an overlay or a ring or shield.

3.1 Traceback

The traceback mechanisms trace back the source of the path. These mechanisms could be based on the packet marking, static path of the packets or checking path fingerprint. For example, the TTL field (Time to Live) can be used to count the number of hops crossed by the packet. This information can be used to estimate the source of the packet. The papers under this category look into techniques to trace the source of the packets using either identifiers, information that can be added in headers of the packet or without any marking on the header. An example of the latter could be when an attack is detected, routers can collaborate, communicate and share the information about the packets send to victim. Irrespective of the type of method used, main idea is to trace back the source of the attack.

3.1.1 With Marking

The traceback mechanisms that use marking requires changes in the packet header. Marking helps to determine the path of the packet.

3.1.2 Traceback without marking

The traceback mechanisms can also work without any modification in the packet header fields. These are usually based on locally detected traffic rates by routers.

3.2 Filtering/Mitigation/Rate Limiting

Filtering can be done based on thresholds or attack signatures. Filtering can be performed at edge routers or firewalls. Some of the papers look into the concept of rate limiting at the routers. When an attack is detected, the routers can share information about the attack signature. Thus the traffic towards to the victim can be filtered. Rate limiting is performed in order to reduce the traffic rate. The mechanisms can use statistical analysis before performing rate limiting. The common idea behind these papers are to limit the traffic flow toward the victim and save it from exhaustion.

3.3 Overlay network

A packet needs to travel through the network domain to reach the server. A secure overlay can be used to detect an illegitimate traffic. Agents can be placed in the network to detect any anomaly behavior. The papers that cover this concept discuss about placing a virtual tunnel in the domain or a collaborative mechanism by routers to look for any attackers. A common pattern would be collaboration rather than an autonomous system or a security policy.

V. ALTERNATE CLASSIFICATION SCHEME

1. Placement of the mechanisms

An alternate way to classify the attacks is based on placement of the defense mechanism. The defense technique can be either work independently or can work collaboratively with other nodes in the network. The attack can be detected earlier when the system is near the source but more accurate detection can happen near the victim as the server.
VI. COMPARISON WITH OTHER SURVEYS

We reviewed literature for other similar undertakings on literature review studies and we found several papers. But they have very different focus and coverage than our study. Next we present some of these studies with discussion on their coverage to express differences with our approach.

(Silva, Silva, Pinto & Raquel, 2013) [1]

This paper is a comprehensive survey of research done on botnets during 1999 - 2011. There were 205 papers reviewed in this study. The paper covers definition of botnet, few botnets, and major components of a botnet, characteristics, lifecycle and architecture of botnets. The paper also covers few of the detection mechanisms classified as honeynet-based, intrusion detection systems. IDSs are classified into signature-based and anomaly-based. Anomaly based can be classified into host-based and network-based (active monitoring or passive monitoring).

(Zargar, Joshi & Tipper 2013) [2]

The authors of this study collected 149 papers from 1994 to 2012. The motivation behind hackers are summarized, then the classification of the attacks (network/transport level and application level), botnet architecture and then types of defense mechanisms are covered. The paper points out the need for a comprehensive distributed and collaborative defense solution and also give an insight of the metrics that can be used to evaluate the defense techniques. Other topics include the cyber insurance policies and implementing a new type of mechanism. Types of attacks - 1) Network/transport level DDoS attacks - a) Flooding attacks b) Protocol exploitation flooding c) Reflection-based flooding d) amplification based flooding 2) Application level - a) Reflection/amplification based flooding b) HTTP flooding-session flooding, request flooding, asymmetric attacks, slow request/response attacks Types of Botnets- IRC-based, Web-based, P2P-based Types of defense mechanisms- source-based, destination-based, network-based and hybrid.

(Kumar & Sharma, 2013) [3]

This paper discusses about different security issues in cloud and the different types of attacks found in the cloud based on 21 papers published between 1999 and 2013. Some of the attacks seen in web can be - SQL Injection attacks, Cross Site Scripting attacks, Man in the Middle Attack, DNS attack, sniffer attacks, issues caused by reused IP addresses, BGP Prefix addresses, DoS, Backdoor attacks, cookie poisoning, DDoS, CAPTCHA breaking. The defense mechanisms of DDoS can be classified according to three aspects - detection, identification and filtration. IDS can be categorized into host based, network based, distributed and hybrid. The paper has also discussed about few mechanisms - 1) Collaborative peer-to-peer architecture to defend against DDoS attacks 2) Intrusion detection in the cloud 3) Cloud based attack Defense System (CLAD) 4) Confidence Based Filtering 5) Cloud based Intrusion Detection System 6) Approach based on SOA (Service Oriented Architecture).

( Beitollahi & Deconinck, 2012) [4]

The paper classifies the DDoS defense techniques into source-end, core-end, Victim-end, distributed defense techniques based on literature review of 78 papers published between 1996 and 2012. The defense techniques can be classified into survival, proactive or reactive based on reaction time. Different types of detection techniques include sequential change point detection, wavelet analysis, neural networks, and statistical techniques. Few of the survival techniques are multiple proxy servers, enlarging backlog queue, changing the timeout for connection requests or a combination of multiple techniques. The proactive techniques can be ingress/egress filtering, route-based distributed packet filtering, D-WARD, Internet indirection infrastructure, Secure overlay services, collaborative detection. Few of the reactive techniques are pushback, K-MaxMin, Hop count filtering, Anit-DDoS, traceback techniques, DeICOM, Divide and Conquer Strategy, Client-puzzle protocols, CAPTCHA puzzles, sharing beliefs, refector attack detection and SYN cookies.

(Mansfield-Devine, 2011) [5]

This article has covered the DDoS attacks, the attack motivation and the type of attacks derived from 14 studies conducted between 2007 and 2011. Summarized results for different factors like DDoS based on type of attacks, affected...
sites, country of attack sources and the mitigating mechanisms. A comprehensive summary is provided based on the data collected from different sources for the year 2011.

(Rejimol & Thomas, 2012) [6]

This study argues that the attacks can be classified into bandwidth depletion and resource depletion. Bandwidth depletion attacks are of two types - Flood attack and amplification attacks. There were 14 papers reviewed that were published between 2001 and 2011. Resource depletion attacks are of two types - Protocol Exploit attacks and Malformed packet attacks. Mitigation methods can be classified into different types - a) Network based - provide protection of network or its servers and isolate certain portions of traffic. b) Signature based - if some packets are malicious, then other packets with same signature are discarded. c) Server side mitigation - modify the server settings like scan TCP queue and drop half open connections. d) Client centric methods - puzzles and resource pricing schemes. This paper focuses on mitigation near server. Few of the mitigation methods are – using Swarm Network, Mitigation of TCP SYN flooding with IP spoofing, Adaptive history-based IP Filtering, Probabilistic approach and HCF method.

(Mirkovic & Reiher, 2004) [7]

This literature review paper suggests, based on degree of automation, the DDoS attacks can be classified as Manual, semi-automatic (with direct or indirect communications) and automatic. This paper reviewed 76 papers published between 1997 and 2003. Based on the exploited weakness, they can be classified into semantic and brute-force attacks. Based on source address validity, they can be classified into either spoofed (again classified as routable or non-routable and spoofing techniques) and Valid. The attack rate can be constant or variant (increasing or fluctuating). Attacks are also classified as characterizable (filterable or non-filterable) or non characterizable. Other basis for classification is persistence of agent set, victim type and impact on victim. The DDoS defense mechanisms are classified into preventive or reactive. Attack prevention involves securing target using system security and protocol security. DoS prevention can be resource accounting or resource multiplication. The detection strategies can be pattern, anomaly based or third party. Based on cooperation degree, the techniques are either autonomous, cooperative or interdependent. The deployment location can be either victim, intermediate or source network. Response strategy can be agent identification, rate limiting, filtering and reconfiguration.

VII. CONCLUSION

The breadth and intensity of threats to an organization in today’s age is increasing at an unprecedented rate. There are types of attack which exploit vulnerabilities on non-target systems (botnet) to use in an attack. DDoS uses similar attack vector has been around for many decades. This has been a constant threat to business continuity and service availability. This research looked at extant literature review for analyzed and proposed mitigation controls and countermeasures against DDoS attacks. A review of 142 papers provided key insights to categorize them using a 3-layered defense in depth model. The paper categorizes each paper into one of the categories. This provides a complete and holistic view of research on DDoS protection. We also compared our work against other review and survey papers on similar topic and found our contribution is unique and novel in terms of coverage and in ontological development. The details of each of the papers have not been included in this research due to lack of space. The contributions of the paper can help researchers and practitioners alike understand how DDoS protection research has evolved over last decade or more to be better informed in their decisions.

REFERENCES