Chapter 16
Cooperative Mechanisms for Defending Distributed Denial of Service (DDoS) Attacks

Prachi Gulihar and B. B. Gupta

Abstract Distributed denial of service (DDoS) attack is one of the biggest challenges faced by the Internet community today. DDoS attack attempts to disrupt the availability of resources to the legitimate users by overwhelming the network and server resources. In this chapter, we discuss the importance of cooperative mechanisms over the centralised ones and various existing cooperative techniques to defend against DDoS attack. We also discuss their major drawbacks. The major disadvantage of centralised defence mechanism is single point of failure when the central kingpin node itself comes under attack. What we realise is that although these techniques have been developed, they are rarely deployed in the real world because the researchers have long ignored the economic incentive part in the working of cooperative DDoS mechanisms. Due to lack of incremental payment structures, the cooperation between the nodes fails. Sometimes the payment structures are non-existent, and in some cases, the payment structure is in place, but the incentives are not lucrative enough for the nodes to share their resources. The DDoS attack scenario can be divided into attack phase, detection phase and response phase. When the attacker machines perform in cooperation, then for the defence mechanism to be strong, it should also be in cooperation. This work gives an overview of the existing cooperative defence mechanisms at different layers of the Open Systems Interconnection (OSI) model and an overview of mechanism using third party for any of these three phases.

Keywords Distributed denial of service (DDoS) attack · Defence mechanisms · Cooperative third-party defence schemes

P. Gulihar (✉) · B. B. Gupta
Department of Computer Engineering, National Institute of Technology Kurukshetra, Kurukshetra, India

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_16

1 Introduction

Distributed denial of service (DDoS) [1] attack is one of the biggest challenges faced by the Internet community today. They are performed by the slave machines which are a part of the botnet army and act on the commands of the master machine whose motive is to exhaust network and server resources like bandwidth and storage so that its services become unavailable to the legitimate clients. The largest reported DDoS attack was of volume 400 Gpbs in the year 2014 [2]. Since then, the DDoS attacks are growing in volume. Their efficiency and implementation techniques have become more sophisticated day by day, making it a big challenge for the security professionals. Recently, the study of economics of Internet has emerged as a fast emerging field of study for cyber defence. The workstations being distributed across the network along with the users having varied interests have made this study very important from the information security and policy designing point of view. The main purpose of any framework design is to keep up with the security standards of confidentiality, integrity and availability without being an overburden on the deployer.

The concept of "tragedy of the commons" plays an important role in distributing the limited resources of the Internet. In this, the users because of their own self-interest destroy the collective interest of a community sharing the resource. A sustainable pricing strategy is the one which is able to cater to the competitive advantage of different network providers offering the same set of services but on varied prices. A pricing mechanism will help in differentiating the services offered to the users, but another important task is of fixing the incentives. The pricing strategy plays a very important role in facilitating varied kinds of QoS requirements. Security professionals have realised that while designing any security mechanism, it is vital to keep in consideration the "theory of mind" which explains the way the attackers and benign users take decision to deceive or remain loyal to the system.

Distributed denial of service attacks are the ones in which the attacker gains control of the system by exploiting its vulnerabilities. In this manner, the attacker is able to compromise several machines which then together form an army of zombies who act as slave machines. The attacker or the master machine then commands the slave machines to begin the attack either by sending malicious packets to the victim's address or by flooding exhausting the connectivity bandwidth and server resources. When the attacker's target is connection bandwidth, then the attack takes place in network and transport layer, whereas when the target is on exhausting the server resources, then the attack takes place on the application layer. Figure 16.1 explains how distributed denial of service attack differs from the denial of service attack in a way that the former attack involves the execution of the attack by the coordination of numerous zombie machines and Internet connections whereas the latter only involved a single machine and a single connection in control of the attacker [3]. When the attacker performs the attack, it is doing that with the collaborative efforts of hundreds and thousands of machines; then why not defend

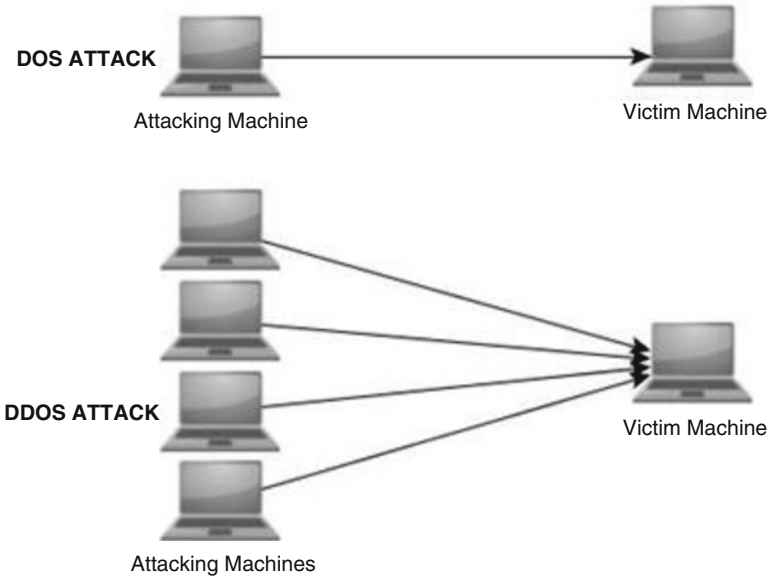


Fig. 16.1 DoS vs DDoS attack

the system in the similar way by achieving collaboration between several nodes which are ready to pool their resources in exchange for some economic incentive?

When combating DDoS attacks, the industry and the academia have always ignored the economic incentive part of the problem which has been the key aspect in defeating DDoS attacks. Incentives are the cornerstones of the race of humans. The problem is that although there are many distributed cooperative defence mechanisms, still the systems are being victims of DDoS attacks. This is because no solution has been able to lure ISPs to pool their free cache memories in order to perform collaborative defence. They have been rarely deployed on the Internet because their payment structure is either non-existent or it lacks an incremental pattern. This has led to failure of cooperation. Another closely related challenging problem is the deployment of the distributed solutions because detection and responses are scattered at different locations.

The DDoS attack defence mechanisms can be classified by the strategy used to detect the attack. It can be classified as anomaly-based, pattern-based and third-party detection. In pattern-based attack detection technique, the signatures of known attacks are stored in the database, and then the traffic is matched with the signatures stored; if the signature matches, then the DDoS attack is successfully detected. The main drawback of this approach is its vulnerability to zero-day attacks. Every now and then new attacks are launched and new viruses are made, so if the stored database is not updated in real time, then the system is bound to surpass many new attack types. In anomaly-based attack detection technique, an ideal model is defined,

and the incoming traffic is then compared with that ideal model. If the deviations go beyond the defined acceptable limits, then the attack is detected. The advantage of this technique over pattern detection is that here the system can be trained to detect the new types of malicious traffic.

2 Motivation

The Internet Service Providers (ISPs) are facing a problem of increased volumes of illegitimate traffic. The main purpose of this malicious traffic is to exhaust the limited network resources like storage and bandwidth. The level of resources required to maintain the network performance falls short, and the quality of service (QoS) provided by the network degrades rapidly. A very large volume of malicious traffic is produced by misbehaving users who either knowingly or unknowingly launch flooding distributed denial of service attacks from their systems. Congestion control mechanisms are executed at network level to prevent the traffic from reaching its peak value by throttling mechanism. Throttling means regulating the rate of traffic being transferred over a network link to prevent it from collapsing due to traffic overload.

But this mechanism fails to maintain the required level of QoS. The ability of DDoS attack to generate massive volumes of unwanted traffic has made it one of the biggest threats the Internet is vulnerable to [4]. The main targets of DDoS attack are the websites. They attack the benign user's ability to access the website or server [5]. The primest marks of DDoS attack which went on for 2 days can be traced back to the year 1999 [6]. Since then, a lot of DDoS detection techniques and response strategies have been developed. A more advanced kind of DDoS attack is known as amplification attacks like Domain Name Server (DNS) amplification attack, NTP amplification attack, etc. in which these servers play the role of reflectors and create a stronger attack. In these attacks, the servers are not attacked directly, but instead these multiple servers are used to generate large traffic against small requests which is directed towards the spoofed IP address provided by the attacker who sent the request to these servers. The response data is used as unwanted traffic. As observed [7], there are two main characteristics because of which the DDoS defence mechanisms have been unable to provide reliable protection. First is the inability to distinguish between the malicious and benign traffic. There is no such mechanism which efficiently differentiates the traffic with minimum collateral damage to the legitimate requests. Second, DDoS attack sources are distributed across different sites which is why it becomes very difficult to trace them.

The reasons for failure of security in any system are twofold. First is the poor design and second is the poor incentive. Although the design part has been widely explored, the incentive part remains naïve. Computer systems are failing because the group of people responsible to protect them does not suffer from complete setbacks on failure. Just as the mathematics concepts came as a boon for security industry in the form of cryptography 25 years back, the same goes for theory of

microeconomics now. The problem of incentives being misaligned has led to several frauds in the banking industry [8]. Construction and development of systems that promote fair behaviour among the users is a must to maintain the security standards and lower the system failure rates. The innovative concept of online auctions as a reputation system has motivated the researchers to explore more such options. This feedback mechanism gave a vent to the free riding problem faced by eBay [9]. A striking example of economic analysis was shown in January 2005 when the power of online music sharing shifted from music vendors to individual publishers [10].

3 Research Objective

This chapter presents various aspects of the security from DDoS attacks. This chapter gives a comprehensive view of how DDoS attack has evolved and the security challenges around it. Moreover, we have also presented various taxonomies on the types of DDoS attacks, the taxonomies of their defence mechanisms. This chapter also discusses in detail various payment structures and economic incentive schemes in the Internet. We conclude the chapter by discussing some of the existing research evaluation parameters. The main objective should be able to design a cooperative DDoS defence mechanism suitable for the Internet. However, the task is challenging due to the lack of degree of cooperation in network entities. The key factor to be considered while dealing with cooperative defence schemes is the motive of collateral profit which shall motivate the participating entities. For this, a multi-level defence scheme which combines anomaly-based and volume-based filtering of attack traffic using client puzzles as Proof of Work (PoW) which is further extended by using effective economic incentive scheme on the existing payment structures of the Internet will be beneficial like a DDoS mitigation framework which works in cooperation by proposing a solution to prevent DDoS attacks by transferring the risk to some third-party network entity like underutilised cache servers in the Internet by providing iterative economic incentives.

4 Statistics

The largest reported DDoS attack was of volume 400 Gpbs in the year 2014 [11]. Since then, the DDoS attacks are growing in volume. Their efficiency and implementation techniques are getting more sophisticated day by day, making it a big challenge for the security professionals. Figure 16.2 shows the distribution of various kinds of DDoS attacks the systems are prone to. The volumetric DDoS attack type is the most common one with 65% of the attacks being the volumetric attacks. They are performed by the slave machines which are a part of botnet and act on the commands of the master machine. The volumetric attacks are done by floods like User Datagram Protocol (UDP) floods, Internet Control.

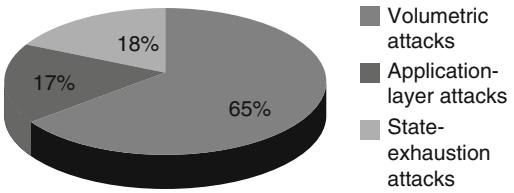


Fig. 16.2 Types of DDoS attacks

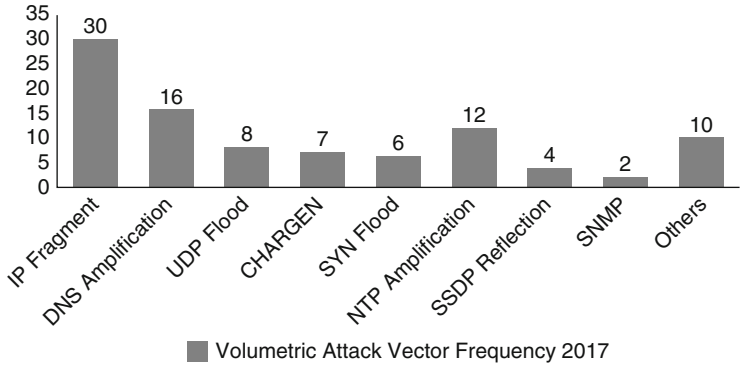


Fig. 16.3 DDoS attack vectors recorded

Message Protocol (ICMP) floods, etc. The second popular attacks are the state exhaustion attacks standing at 18%. This type of DDoS attack is also known as protocol attack because it exploits the vulnerability present in network protocols. Ping of Death exploiting buffer overflow has most instances in state exhaustion attacks.

The next kind of attacks are the application layer attacks standing at 17%. HTTP flood is the most popular kind in this subset. Figure 16.3 shows the various volumetric attack types prevalent in the year 2017 [12]. They include both infrastructure and application attack vectors. The percentage share of IP fragmentation is the most at 30 percent followed by amplification attack done using Domain Name Servers (DNS). A jump of 69 percent was recorded from August 2017 to December 2017 peaking in September. Probably the reason is that any person having a computer and Internet access is now able to generate volumetric DdoS attack from its location. The other vectors shown in the graph include PUSH, POST and GET floods.

5 Taxonomy of DDoS Attacks

The first kind of DDoS attack exploits the vulnerabilities in the network protocol and software [13]. And the second kind of DDoS attack focuses on exhausting the network resources by generating huge volumes of attack traffic. This kind of attack is known as flooding attack which is further divided into two types: simple

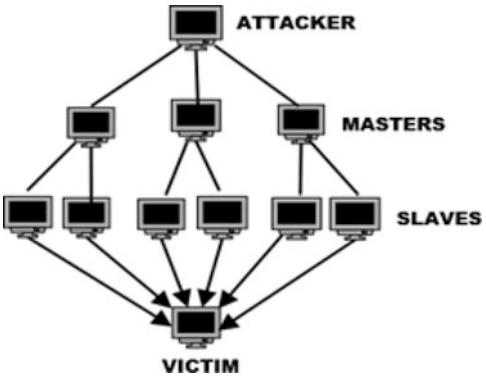


Fig. 16.4 Master slave model

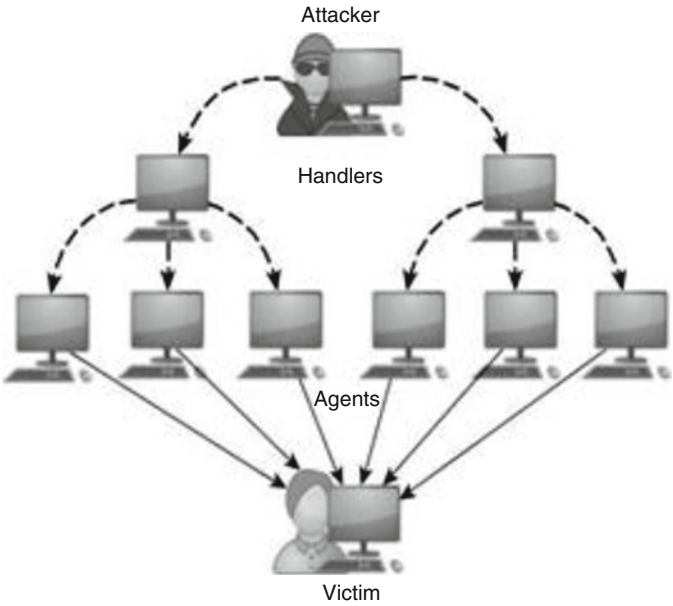


Fig. 16.5 IRC model of DDoS attack network

DDoS attack and amplified DDoS attack. Amplified DDoS attack is harder to defend because the sources of attacks are not traceable. In simple DDoS attack, an attacker makes an army of several zombie machines by exploiting the vulnerabilities in them as shown in Fig. 16.4. In amplified DDoS attacks, the use of reflectors is made. For example, a DNS server, web server and Network Time Protocol (NTP) server can behave as reflector nodes. They all return response packets based on the request packet. A DDoS network is comprised of attackers, agents, victim and control messages whose flow is denoted by dotted arrows in Fig. 16.5. It is via control messages that the attacker conveys the commands to the zombie army.

5.1 Architecture of DDoS Attack Network

The DDoS attack network is of three types [14]: agent-handler model, IRC and reflector-based model. The agent-handler model has three components: attacking machine, zombie machine and the agents. The attacker sends control messages to other zombie machines commanding them to send malicious traffic to the victim node. The Internet Relay Chat (IRC) model is the one in which the zombie machines are replaced by handlers. The function of handlers is to flood the victim on the command of the attacker machine.

5.2 Reflector-Based Flooding Attack

Figure 16.6 explains the reflector-based architecture of the DDoS attack. In this attack lies a big difference from the traditional DDoS attack scenario: the use of reflectors. A reflector is a kind of server which responds the client with the replies

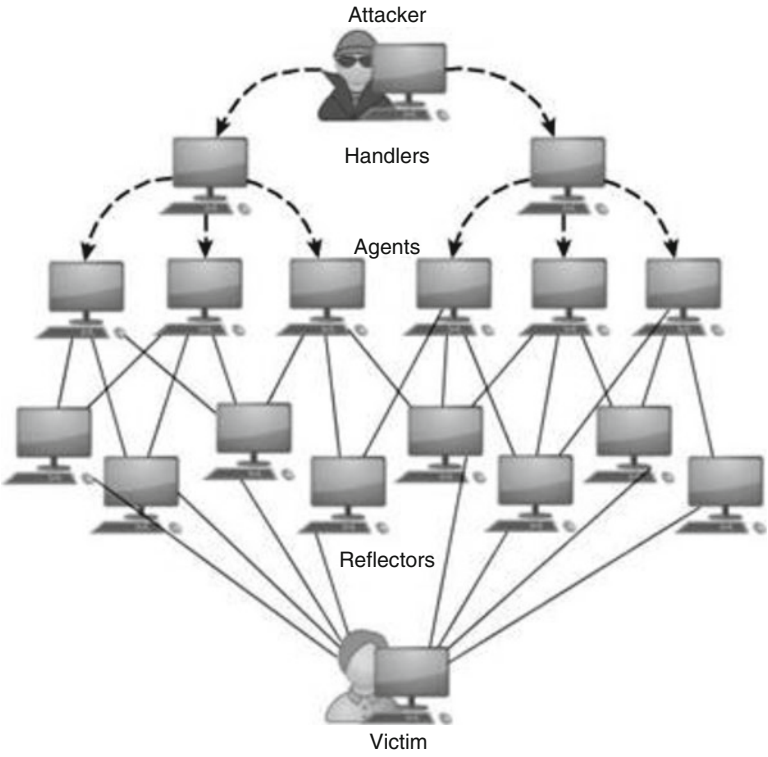


Fig. 16.6 Reflector model of DDoS attack network

in accordance with the queries received. The reflector-based DDOS attack is always diffused across the network and may further be of two types: amplified or non-amplified. Not all reflectors serve as amplifiers [15]. Reflectors are able to generate the attack traffic by catering to legitimate requests only.

5.3 IP Spoofing Based

IP Spoofing is the fundamental technique used in almost all kinds of DDoS attacks. It is done to prevent the location of the attacker from getting revealed. In the IP header, there is a field for source address, which is changed by the agent machines. In the reflecting DDOS attack, the attacking agent replaces its source address by the IP address of the victim machine. These victim machines may be existent or non-existent. For a DDoS attack to be successful, it is better to use existent IP addresses so that they can pass through ingress filtering defence mechanism. If the number of zombie machines in the attacker's army is large in count, then DDOS flooding attack can be performed without spoofing the IP address. This becomes more untraceable if the chain of zombie machines is spread across different geographical regions. The flooding-based DDoS attacks are broadly classified into direct attacks and reflector attacks [16].

5.4 Direct Flooding Attack

In direct flooding type DDoS attack, the architecture remains as of simple DDoS attack. The agent machine sends packets like Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and ICMP directly to the victim machine, and the reply generated by the victim instead of going to the attacking machine goes to the IP address which the attacker had spoofed in the IP header. In the reflector flooding mechanism, the attacker spoofs its IP address as that of the victim. It then sends query packets to the reflector server, but the reply packets instead of coming to the attacking machine are diverted to the victim machine. The following are some typical flooding attacks.

5.5 Smurf Attack

This attack is also known as ICMP echo flooding attack. It aims to exhaust the bandwidth of the victim machine by sending multiple echo reply packets. This attack can also make use of amplifiers. The ICMP messages are used to get the status of the nodes in path. The amplifier will broadcast echo request message to the

hosts in its subnet. So if its subnet is comprised of 100 nodes, then the victim will be getting echo reply message from 100 nodes. This is called amplification effect [17].

5.6 TCP SYN Attack

TCP SYN flood [18] is a kind of direct DDoS attack. In this attack, the attacker attacks the ability of the victim machine to accept any new TCP connections by leaving them in open state due to incomplete handshake protocol execution. In setting up of a TCP connection, the client initiates by sending TCP SYN packet to the server which replies with TCP SYN-ACK packet. The third step is when the client who requested the TCP connection sends back TCP ACK packet to the server, hence completing the three-way handshake. The server has only limited number of TCP connections; the attacker exploits this vulnerability and sends numerous TCP SYN packets without sending TCP ACK packets for the earlier requested connections, hence leaving open connections. This inhibits the server's ability to accept any TCP connection requests from the legit users.

5.7 UDP Flood Attack

UDP flooding DDoS attack aims at exhausting the bandwidth resource of the victim machine by diverting numerous UDP packets to it. The attacks which target the bandwidth are not completely curbed by increasing the bandwidth links of the victim machine; only its resistance can be increased. UDP protocol is a connectionless protocol. In a UDP flood attack, the victim receives numerous UDP packets at different ports. The victim machine then checks for the application on that port; finding none it replies back the sender with Destination Unreachable message packet. Due to absence of any kind of negotiation, spoofing a packet becomes much easier. Figure 16.7 explains the basic difference.

5.8 DNS Amplification Attack

Any network protocol which generates a reply to the query can be used in reflector flooding attack. But what empowers this characteristic is the technique of amplification. An amplifier is used to broadcast the query packet to all the servers in its range which aids the attacker to generate a bigger response to a small request as shown in Fig. 16.8. This way the volume generated as reply to the query becomes multi-fold, and using the technique of IP spoofing, this response is diverted to the victim machine which gets overburdened and hence cannot serve legitimate requests

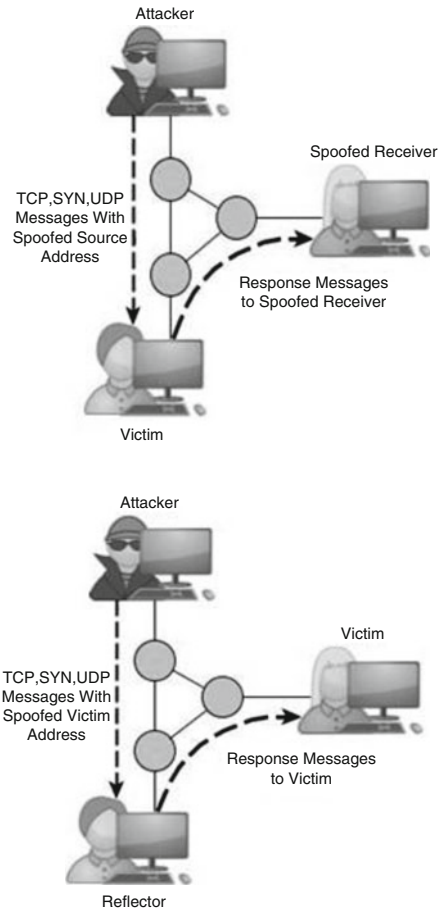


Fig. 16.7 Direct vs reflective flooding mechanism

making the DDoS attack successful. Figure 16.9 illustrates the attack mechanism. The largest on record DDoS attack is caused by DNS amplification. The ratio of query to reply of DNS server is 1:70, whereas for NTP server, it ranges from 1:20 to 1:200.

DNS amplification attack is a recent type of reflector-based DDoS flooding attack. Complicated interaction mechanisms exist between clients and name servers. On comparing the smurf amplification attack with DNS amplification attack, one must notice the significant difference in their attacking mechanisms. In smurf attack, the echo request messages are broadcasted to multiple hosts in the subnet using amplifiers, because of which the amplification effect is achieved, whereas in DNS amplification, the server itself magnifies the volume of traffic diverted to the victim machine by generating larger response packets to very small query packets. Smurf attack performs flooding by generating multiple replies to a request, whereas DNS amplification generates a single big reply. This helps the attackers in getting more

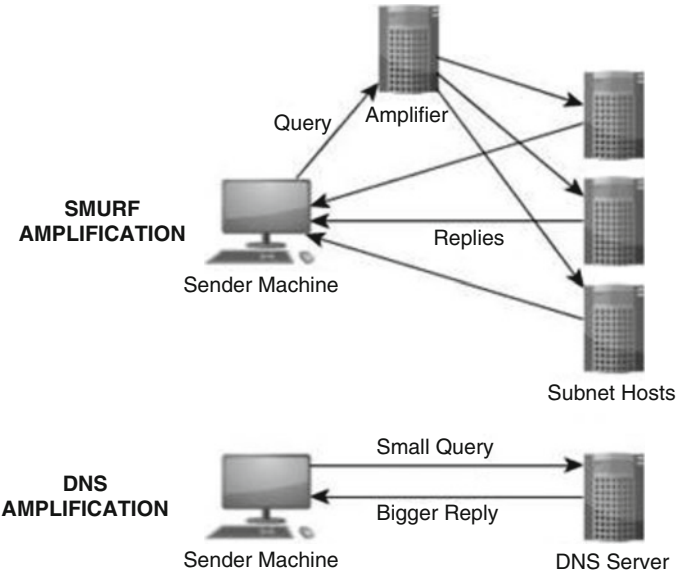
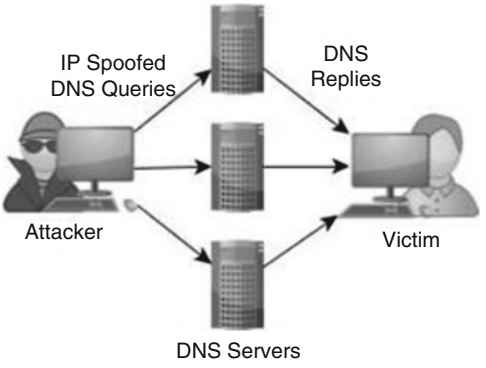


Fig. 16.8 Smurf vs DNS amplification

Fig. 16.9 DNS amplification attack



work done in doing less efforts which is why this is a very popular and hard to defend flooding DDoS attack caused by DNS servers as amplifiers.

6 Taxonomy of Cooperative DDoS Defence Mechanisms

We can categorise DDoS defence mechanisms in two categories: centralised and distributed. This depends on whether the defence mechanism phases, detection, mitigation and response, are deployed at the same location or different locations. In the centralised mechanisms, the whole DDoS defence mechanism is either set up at

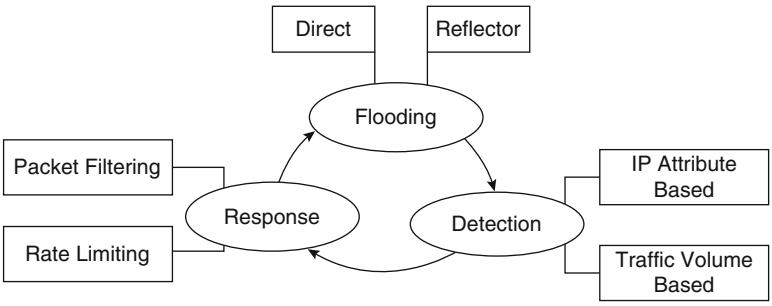


Fig. 16.10 DDoS attack scheme

source, destination or the intermediate network. But in centralised mechanisms, the detection might take place at the victim node, mitigation at the intermediatory nodes and response at the source of the attack traffic generation. This means that the whole process is scattered at various locations in the Internet, but to successfully combat against the DDoS attack, all these parties need to work together in collaboration with one another [19].

In this write-up, the focus is on several cooperative defence mechanisms available, but first we explain the need of such mechanisms when centralised ones are already in place. Figure 16.10 explains the action cycle. In centralised systems, the main issue is single point of failure. It means the whole of the defence system can crash if the only site where all its components are deployed comes under attack. The cooperative system is able to solve this problem by having multiple nodes in action for defence at different locations. These nodes have similar functionalities, so even if the nodes in one location are compromised, still we have numerous set of nodes in place to defend the victim site. Secondly, Internet does not have any central control authority over its autonomous systems, so a defence model which does not have a central authority in control will prove beneficial.

6.1 Pushback and Packet Marking

Chen and Park [20] proposed a cooperative mechanism by combining the techniques of pushback messages and packet marking. It is called Attack Diagnosis (AD) in which the victim machine first detects the DDoS attack and then sends AD commands to the upstream routers in the network. It is a reactive defence mechanism. It makes use of AD-enabled routers which then start marking each packet deterministically with the interface information it is passing through. The victim machine then uses this attached interface information to trace back the source of malicious packets.

The AD-related commands are authenticated using the Time To Live (TTL) field of the IP packet header. AD scheme is ineffective when the DDoS attack

is performed at a large scale, so there exists an extension to AD which is called Parallel Attack Diagnosis (PAD). AD can stop the traffic from single router at a time, whereas PAD diagnoses and stops the traffic from multiple routers simultaneously.

6.2 IP Traceback and Port Marking

Chen et al. [21] have proposed one more distributed DDoS mechanism based on the concept of router port marking and packet filtering. These are presented as two modules used. The function of router port marking module is to mark the packets probabilistically by appending router's interface port number to the packets. It is a six-digit number which is locally unique. When the victim machine is flooded with the malicious packets, then it makes use of this appended information to trace back the source of the malicious packets.

The function of packet filtering module comes next which then filters the malicious incoming packets at the upstream routers. This mechanism has low computation and communication overheads. But it has two limitations. Firstly, as there is no authentication used, the attackers can forge the marking fields so that their actual location is never revealed. Secondly, although this technique effectively traces back the IP, it fails to identify the master behind the DDoS attack who is in control of the army of zombies or compromised machines.

6.3 Signature-Based Defence

Papadopoulos et al. [22] proposed Coordinated Suppression of Simultaneous Attacks (COSSACK) mechanism. It uses a software system called watchdog which is built on the edge routers. It is based on a critical set of assumptions like existence of attack signatures, edge router's capability to filter packets on the basis of these signatures and continuous connection availability. The watchdog software does ingress and egress filtering on the edge routers to stop DDoS attack flow, and it also sends multicast notifications to the source side. It is unable to withstand DDoS attack traffic generated from the legacy networks that have not deployed COSSACK.

6.4 Capability-Based Defence

Anderson et al. [23] have proposed distributed defence mechanisms based on the capabilities. In these mechanisms, firstly the sender has to obtain the rights to send from the receiver. These rights are kind of short-term contracts, tokens or authorisations. To understand this better, we can understand it through an analogy of sticking the postage stamp onto the letter before posting. The only difference here

is that the postage stamp is bought from the post office whereas the sending rights will be obtained directly from the receiver. Another analogy will be of receiver defining the window size beforehand in sliding window protocol of data link layer. The major drawback of this scheme is that the capability setup channel is not secure. These mechanisms always have to be kept active, hence increasing the processing and memory overheads.

6.5 Datagram-Based Defence

Argyraki et al. [24] proposed an alternative to capability-based filtering mechanism which is datagram filtering mechanism in which instead of denying all the traffic by default, only the traffic that is denied is identified as malicious. This is called Active Internet Traffic Filtering (AITF). In this, the receiver is able to contact the misbehaving senders and ask them to stop. Every ISP polices its misbehaving nodes, or else they are at a risk of losing connectivity to the victim machine which may be an important point of access. So there lies as strong incentive for the participating ISPs to cooperate. AITF is affordable to be deployed by the ISPs because it preserves the receiver's bandwidth at per-connection cost. The legitimacy of the traffic is verified using three-way handshake which may not be completed because the handshake packets and the DDoS attack traffic are flowing through the same flooded link. This mechanism also has several deployment issues because it is not relying on edge routers for actual filtering. The routers used are placed in the middle of the network.

6.6 Anomaly-Based Defence

Liu et al. [25] proposed another distributed defence mechanism against network and transport layer DDoS attacks, namely StopIt. In this mechanism, each receiver installs a network filter which blocks the undesirable traffic. It makes use of Passport mechanism proposed by Liu for authentication purpose. It has made use of looped and third generation of telecom networks in its architecture. Every autonomous system has a StopIt server for sending and receiving StopIt requests. A filter is installed at the source and the filter requests are exchanged among the peer nodes. In this mechanism, the StopIt server can be attacked with packet floods and filter requests if the requests are allowed from neighbouring autonomous systems also. Moreover, StopIt mechanism needs complex detection mechanisms which make it hard to deploy.

6.7 Volume-Based Defence

Walfish et al. [26] proposed a distributed DDoS defence mechanisms to prevent application layer level attacks. In this paper, the concept of defence by offence is followed. It encourages the honest clients to speak up by increasing the volume of benign traffic it sends to the server being targeted by DDoS attack. This ensures that the percentage of bandwidth captured by the good clients is increased, hence out-crowding the one flooded by the attacker. In this work, it is not explained how will the server detect the attack. Speak-up mechanism is applicable only in session flooding attacks and not in request flooding or asymmetric attacks.

6.8 Hybrid Defence

Yu. et al. [27] proposed a Defense and Offense Wall (DOW) scheme. This is an extension to the speak-up work by Walfish et al. with addition of anomaly detection method. The anomaly detection method used is based on K-means clustering approach to detect asymmetric, request flooding and session flooding attacks. It has explained the mechanism using two models: the detection model and the currency model. The former's function is to drop suspicious packets, while the latter's function is to encourage the increase in session rates by legitimate clients. The major drawback of this mechanism is that it is too resource consuming to be implemented.

7 Literature Review

Mahajan et al. [28] proposed a distributed DDoS defence mechanism called Aggregate-based Congestion Control (ACC). Aggregates are a part of the network traffic which is identified as malicious. It is characterised by source IP addresses or destination ports. In this mechanism, the router detects the aggregates which are overloading its bandwidth rather than the IP sources. On detection of such samples, the router sends pushback message to the upstream routers in the network and then sends a rate limit. From then on, if the traffic from those upstream routers exceeds that rate limit, then the packets are dropped and multiple pushback messages are sent. This technique fails to be effective when the attack traffic is uniformly distributed in the network (Tables 16.1 and 16.2).

Mirkovic et al. [29] proposed a distributed framework called DEFensive Cooperative Overlay Mesh (DEFCOM). This framework supports information and service exchange among the cooperating nodes in the system. They have shown a distributed defence framework architecture of heterogeneous defence nodes which collaborate and cooperate with each other and work as a team to combat DDoS attack. By heterogeneous, what is meant is that all the defence nodes do not share the same

Table 16.1 Application layer cooperative DDoS defence mechanisms

Name of scheme	Author	Scheme description	Limitations
Aggregate congestion control and pushback (2002)	R. Mahajan et al.	ACC rate limits the aggregates rather than IP sources	Not effective against uniformly distributed attack sources
Attack Diagnosis and parallel AD (2005)	R. Chen, J.M. Park	Combines pushback and packet marking	AD is not effective against large-scale attacks
TRACK (2006)	R. Chen et al.	Combines IP traceback, packet marking and packet filtering	Not effective for attack traceback
Passport (2008)	X. Liu, A. Li, X. Yang, D. Wetherall	Makes use of symmetric key cryptography to put tokens on packets that verify the source	Attackers may get capabilities from colluders
			It only prevents the hosts in one AS from spoofing the IP addresses of other ASs
DEFensive Cooperative Overlay Mesh (2003)	J. Mirkovic et al.	Defence nodes collaborate and cooperate together	Classifier nodes require an inline deployment
			Unable to handle attacks from legacy networks
Stateless Internet Flow Filter (2004)	A. Yaar et al.	Capability-based mechanism	Always active
			Processing and memory costs overheads
StopIt (2011)	X. Liu, X. Yang, Y. Lu	Novel closed control and open service architecture for filters to be installed	Vulnerable to attacks in which attacker floods the router
			Needs complex verification/authentication mechanisms
			Challenging to deploy and manage in practice

functionality, like nodes near the victim will do the detection best, and the nodes near the source will cater to the response technique.

In this mechanism, the attack alerts from the generator nodes are flooded into the network after which the rate limits are sent to the upstream routers. From then on, all the resource requests that are sent to the downstream routers are first classified, and the malicious packets are dropped. This works in a P2P network scenario, just proper rate limits for both upstream and downstream routers need to be defined, and simultaneously the classifier nodes are at work to differentiate malicious traffic and benign traffic. The main disadvantage of this framework is that this is not compatible with the old or legacy networks, so if a large portion of the network is a legacy network, then the classifier nodes which are deployed in-line malfunction.

Table 16.2 Application layer cooperative DDoS defence mechanisms

Name of scheme	Author	Scheme description	Limitations
Active Internet Traffic Filtering (2009)	K. Argyraki, D.R. Cheriton	Misbehaving sources are policed by their own ISPs	Several deployment issues If the flooded link is outside victim's AS, the three-way handshake may not be completed
Speak-up (2002)	M. Walfish et al.	Encourages the good clients to out-crowd the bad ones	Not applicable against request flooding and asymmetric attacks
Defense and Offense Wall (2005)	J. Yu et al.	Encouragement method with anomaly detection	Very resource consuming to be implemented
CAPTCHA (2003)	L.V. Ahn et al.	Differentiates DDoS flooding bots from humans	More delay for legitimate users Disables web crawler's access to websites
Admission control and congestion control (2002)	M. Srivatsa et al.	Port hiding	Requires a challenge server which can be the target of DDoS attacks

Li et al. [30] addressed the drawback of the capability-based mechanism scheme by adding secure authentication systems to capability-based mechanisms. They called it a Passport system which uses symmetric-key cryptography to encrypt the tokens before appending them to packets being sent. This allows the routers in path to verify that the source address is genuine. Using this technique, the ISPs can protect their own addresses from being forged, so such schemes offer stronger incentive as compared to other filtering schemes.

This mechanism is vulnerable to colluding attacks in which the attackers get the capabilities from the cheating nodes or they can eavesdrop the packets of the node is honest. Another limitation of this scheme is that although the attackers cannot spoof the IP address of host belonging to other autonomous system, it can easily spoof the IP of some other host in the same autonomous system.

Kandula et al. [31] tried to differentiate the DDoS flooding done by humans and bots. They employed a mechanism called Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). Although it is a good technique to differentiate robots and humans, the main disadvantage is that it requires the users to solve different puzzles to pass the authentication test having text and pictures which becomes an annoying task for the users.

Srivatsa et al. [32] proposed an admission control and congestion control scheme which limits the number of clients being served simultaneously. It works on the principle of port hiding which hides the port number on which the service requests are accepted, hence making the port invisible to the illegitimate clients. Then congestion control is performed to allocate more resources to good or legitimate set of clients.

8 Performance Evaluation Metrics

Although there is no any standard set of measurements used by the research community, the performance evaluation metrics for volumetric DDoS attack defence strategy can be divided into two according to the level of attack traffic experienced. The first category of the metrics is the ones which measure the performance evaluation under high traffic load, and the second one measures the performance under low traffic load. Some commercial products [33] also exist to measure the performance by evaluating a variety of results of the defence technique. They are discussed below.

8.1 Detection Rate

It measures the number of attacks that are detected from the number of attacks actually performed by the attacker.

8.2 False Positive Rate

It measures the number of times the legitimate user traffic is wrongly detected as DDoS attack traffic. A similar parameter is true negative which detects the attack even when it is absent. Similarly, false negative denotes the inability to find the malicious traffic.

8.3 Ratio Between Detection Rate and False Positive Rate

This metric is generated using Receiver Operating Characteristic (ROC) curves over detection rate and false positive rate. ROC curves are widely used to calculate the sensitivity and specificity of the evaluation parameters.

8.4 Failure Rate

It is an application layer level metric [34] which is calculated by finding the ratio of number of requests which go unresponded by the victim to the total number of requests received by the victim.

8.5 Average Latency

It is a measure of application level performance. It is the average of the time delays experienced between the sender initiating the request and the receiver receiving the response message at different instances.

8.6 Throughput

The throughput directly indicates the performance of any defence mechanism. It is the total amount of data transmitted in a unit time.

8.7 Bandwidth

It is the aggregate level of performance measure [35]. Bandwidth denotes the amount of traffic a link can carry under various states like normal state and attack state.

8.8 Malicious Packet Drop Rate

DDoS defence scheme on packet level aims to lower the volume of malicious packets by selectively dropping them from the whole traffic received. It reflects the capability of any defence mechanism to control the flooding traffic. It is calculated as the ratio of number of packets dropped before reaching the victim to the total number of packets destined for the victim.

8.9 Benign Packet Drop Rate

The main purpose of DDoS defence scheme is to maintain the level of QoS for the benign user traffic. The motive is to be able to forward as many benign packets as possible by preventing the bandwidth to collapse due to congestion. It is calculated as the ratio of number of benign packets dropped before reaching the victim to the total number of packets destined for the victim.

Adjusting the parameters of performance estimation is an important task. Selection of appropriate parameters to judge the performance of any scheme in the network depends on certain rules like the changes in the attack tragic load should be separated into two cases: first, when the variation in traffic rate is very slow

and, second, when the attack traffic is changing at a rapid rate. The parameters of legitimate data traffic should be collected from the victim side when it is not under any kind of attack; then only a comparative analysis can be done when the developed scheme is enforced.

9 Conclusion

On analysis of various DDoS detection, mitigation and response frameworks, the common challenge faced by each one of them is to quicker the detection rate with sustainability of QoS for benign users. In all these techniques, the DDoS defence mechanism can be broken down into three parts: detection, mitigation and response. The mechanisms developed are not only victim-end defence or source-end defence mechanisms but a combination of both across the network. The backbone of these hybrid mechanisms remains a highly effective cooperative mechanism to ensure stable and rigid communication. So studying the incentive and payment structure used in any scheme from economic point of view is important. Like, Internet is comprised of several cache servers which may not be fully utilised and these unused cache capacities can be utilised in cooperative DDoS defence. The traffic flood can be diverted to these multiple servers each handling only a fraction of attack traffic, thus preventing congestion from the attack flood. This resource is already existing and will incur meagre costs to the parties involved, but management of network resources is one of the most essential issues of Internet. The heuristic techniques of optimisation have always been the backbone in solving economic engineering problems, and so the main task of the mechanisms like double auction is not only to increase the utility of free cache resources but also to promote sustainable individual profits in the long run.

10 Scope for Future Research

In the future research, the evaluation of these defence schemes on different topologies of Internet will be helpful in deployment of these mechanisms in broader technical areas. For any detection technique developed, setting the value of threshold is very important. Optimisation of threshold parameter for any network is an important research area. Inclusion of statistical features for calculating threshold value will enhance its precision. Timely detection of end of DDoS attack is also an important research area having future scope. In fighting against any kind of cyber attack, data plays a very crucial role. The recovery of the legitimate traffic should be very quick and must ensure integrity.

Over the past years, the research area of Internet economics has generated many useful works having an interdisciplinary approach. Long unknown things to the security professionals like incentives and market failure are now taken into

consideration before designing any payment structure. The work being carried out in Internet domain field has spread across various other domains like algorithmic design, security and warfare, interconnected networks and dependability economics of these complicated networks. Psychology has proved to be an important consideration while developing practical schemes for Internet pricing. It gives a deeper understanding of fundamental user behaviour which helps in making the scheme more usable and secure.

References

1. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069.
2. Srivastava, A., Gupta, B. B., Tyagi, A., Sharma, A., & Mishra, A. (2011). A recent survey on DDoS attacks and defense mechanisms. In *Advances in parallel distributed computing* (pp. 570–580). Berlin: Springer.
3. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53.
4. Xu, K., Zhang, Z.-L., & Bhattacharyya, S. (2005). Reducing unwanted traffic in a backbone network. In *Steps to reducing unwanted traffic on the internet workshop (SRUTI)* (p. 915). Berkeley, CA: USENIX Association.
5. CERT Coordination Center. (2007, March). *Denial of service attacks*. Retrieved from http://www.cert.org/techtips/denial of service.html
6. Garber, L. (2000). Denial-of-service attacks rip the internet. *Computer, 33*(4), 12–17.
7. CERT Coordination Center. (2007, March). *CERT advisory CA-98.01 smurf IP denial-of-service attacks*. Retrieved from http://www.cert.org/advisories/CA-1998-01.html
8. Liu, X., Li, A., Yang, X., & Wetherall, D. (2008). *Passport: Secure and adoptable source authentication*. Renton, WA: USENIX.
9. Argyraki, K., & Cheriton, D. R. (2009). Scalable network-layer defense against internet bandwidth-flooding attacks. *IEEE/ACM Transactions on Networking (ToN), 17*(4), 1284–1297.
10. Liu, X., Yang, X., & Lu, Y. (2008). To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. In *ACM SIGCOMM computer communication review* (Vol. 38(4), pp. 195–206). New York: ACM.
11. Retrieved March 21, 2018, from https://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/
12. Retrieved March 21, 2018, from https://www.akamai.com/us/en/about/news/press/2017-press/akamai-releases-third-quarter-2017-state-of-the-internet-security-report.jsp
13. Molsa, J. (2006). *Mitigating denial of service attacks in computer networks*. PhD thesis, Helsinki University of Technology, Espoo, Finland.
14. Specht, S. M., & Lee, R. B. (2004). Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In *ISCA PDCS* (pp. 543–550).
15. Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review, 31*(3), 38–47.
16. Chang, R. K. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Communications Magazine, 40*(10), 42–51.
17. CERT Coordination Center. (2007). *CERT advisory CA-98.01 smurf IP denial-of-service attacks*. Retrieved March, 2007, from http://www.cert.org/advisories/CA-1998.01.html

18. Mölsä, J. (2006). *Mitigating denial of service attacks in computer networks*. Espoo: Helsinki University of Technology.
19. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069.
20. Chen, R., & Park, J. M. (2005). Attack diagnosis: Throttling distributed denial-of-service attacks close to the attack sources. In *Proceedings of the 14th International Conference on Computer Communications and Networks, ICCCN 2005* (pp. 275–280). Piscataway, NJ: IEEE.
21. Chen, R., Park, J. M., & Marchany, R. (2006). TRACK: A novel approach for defending against distributed denial-of-service attacks. In *Technical Report TR ECE—O6–02*. Blacksburg, VA: Department of Electrical and Computer Engineering, Virginia Tech.
22. Papadopoulos, C., Lindell, R., Mehringer, J., Hussain, A., & Govindan, R. (2003). Cossack: Coordinated suppression of simultaneous attacks. In *Proceedings: DARPA information survivability conference and exposition, 2003* (Vol. 1, pp. 2–13). Los Alamitos, CA: IEEE.
23. Anderson, T., Roscoe, T., & Wetherall, D. (2004). Preventing internet denial-of-service with capabilities. *ACM SIGCOMM Computer Communication Review, 34*(1), 39–44.
24. Argyraki, K., & Cheriton, D. R. (2009). Scalable network-layer defense against internet bandwidth-flooding attacks. *IEEE/ACM Transactions on Networking (ToN), 17*(4), 1284–1297.
25. Liu, X., Yang, X., & Lu, Y. (2008). To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. In *ACM SIGCOMM Computer Communication Review* (Vol. 38(4), pp. 195–206). New York: ACM.
26. Walfish, M., Vutukuru, M., Balakrishnan, H., Karger, D., Karger, D., & Shenker, S. (2006). DDoS defense by offense. In *ACM SIGCOMM Computer Communication Review* (Vol. 36(4), pp. 303–314). New York: ACM.
27. Yu, J., Li, Z., Chen, H., & Chen, X. (2007). A detection and offense mechanism to defend against application layer DDoS attacks. In *Third International Conference on Networking and Services, 2007. ICNS* (pp. 54–54). Piscataway, NJ: IEEE.
28. Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V., & Shenker, S. (2002). Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review, 32*(3), 62–73.
29. Mirkovic, J., Robinson, M., & Reiher, P. (2003). Alliance formation for DDoS defense. In *Proceedings of the 2003 workshop on New security paradigms* (pp. 11–18). New York: ACM.
30. Li, A., Yang, X., & Wetherall, D. (2008). *Passport: Secure and adoptable source authentication*. Renton, WA: USENIX.
31. Kandula, S., Katabi, D., Jacob, M., & Berger, A. (2005). Botz-4-sale: Surviving organized DDoS attacks that mimic flash crowds. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2* (pp. 287–300). Berkeley, CA: USENIX Association.
32. Srivatsa, M., Iyengar, A., Yin, J., & Liu, L. (2008). Mitigating application-level denial of service attacks on Web servers: A client-transparent approach. *ACM Transactions on the Web (TWEB), 2*(3), 15.
33. Hussain, A., Schwab, S., Thomas, R., Fahmy, S., & Mirkovic, J. (2006, June). DDoS experiment methodology. In *Proceedings of DETER Community Workshop* (pp. 8–14).
34. Ko, C., Hussain, A., Schwab, S., Thomas, R., & Wilson, B. (2006, June). Towards systematic IDS evaluation. In *Proceedings of DETER Community Workshop* (pp. 20–23).
35. Feibel, W. (2000). *The network press encyclopedia of networking*. San Francisco, CA: Sybex.