Journal of Network and Computer Applications 58 (2015) 165–179

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing

Alireza Shameli-Sendi [a,*], Makan Pourzandi [b], Mohamed Fekih-Ahmed [c], Mohamed Cheriet [c]

[a] School of Computer Science, McGill University, Montreal, Canada
[b] Ericsson Security Research, Ericsson, Montreal, Canada
[c] Synchromedia Lab, Ecole de Technologie Superieure (ETS), University of Quebec, Montreal, Canada

ARTICLE INFO

Article history:
Received 23 May 2015
Received in revised form
17 July 2015
Accepted 29 September 2015
Available online 9 October 2015

Keywords:
Distributed Denial of Service (DDoS)
DDoS detection
DDoS mitigation
Defense system
Cloud computing
Software-Defined Networking (SDN)

ABSTRACT

Cloud computing has a central role to play in meeting today's business requirements. However, Distributed Denial-of-Service (DDoS) attacks can threaten the availability of cloud functionalities. In recent years, many effort has been expended to detect the various DDoS attack types. In this survey paper, our concentration is on how to mitigate these attacks. We believe that cloud computing technology can substantially change the way we respond to a DDoS attack, based on a number of new characteristics, which were introduced with the advent of this technology. We first present a new taxonomy of DDoS mitigation strategies to organize the work. Then, we go on to discuss the main features of existing DDoS mitigation strategies and explain their functionalities in the cloud environment. Afterwards, we show how the existing DDoS mechanisms fit into the network topology of the cloud. Finally, we discuss some of these DDoS mechanisms in detail, and compare their behavior in the cloud. Our objective is to show how these characteristics bring a novel perspective to existing DDoS mechanisms, and so give researchers new insights into how to mitigate DDoS attacks in the cloud computing.

Contents

* Corresponding author.
E-mail addresses: alireza.shameli-sendi@cs.mcgill.ca (A. Shameli-Sendi), makan.pourzandi@ericsson.com (M. Pourzandi), mohamed.fekih.ahmed@synchromedia.ca (M. Fekih-Ahmed), mohamed.cheriet@etsmtl.ca (M. Cheriet).

http://dx.doi.org/10.1016/j.jnca.2015.09.005
1084-8045/

1. Introduction

Cloud computing has a central role to play in meeting today's business requirements. Following the lead of early cloud providers (Amazon, Google, IBM, etc.), organizations such as banks, corporations, hospitals, and medical centers have begun to rely on cloud services. However, DDoS attacks can be a major threat to the availability of these services (Zissis and Lekkas, 2012; Subashini and Kavitha, 2011; Bhadauria et al., 2011; Zhang et al., 2012). According to the Cooperative Association for Internet Data Analysis (CAIDA), over 5000 DDoS attacks occur on the Internet every week (Zargar et al., 2013).

DDoS attacks, as the name implies, involve a large number of distributed hosts generating traffic that is directed at a selected target (Huici and Handley, 2007). Attack vectors can be categorized into two groups (Ranjan et al., 2009; Walfish et al., 2010; Spyridopoulos et al., 2013), brute-force and semantic. Brute-force attacks, also known as "flooding attacks", focus on bandwidth consumption by invoking vast numbers of bogus requests, aggregating the traffic of a large number of distributed hosts, and overwhelming the target (Argyraki and Cheriton, 2009). These targets can be applications, hosts, or infrastructure. An example of a brute-force application attack would be a large number of SSH login attempts on all elements of a provider's network (McPherson, 2010). A brute-force attack, because of its distributed nature, can be massive. The biggest botnets currently hold over a million bots, and estimates of the number of bots involved in any particular DDoS range from a few thousand to upwards of 10,000 (NetworkWorld, 2009).

In contrast, semantic attacks, also known as "vulnerability attacks", focus on resource starvation by exploiting protocol weaknesses (Mirkovic and Reiher, 2004). The latest trend is to carry out an application-level attack, based on HTTP, HTTPS, or DNS, for example. This type of attack does not cause major congestion, but it is harder to detect and so more challenging to fight. A semantic attack attempts to exploit a weakness, rather than exhausting bandwidth/resources, and generally targets a protocol or an application. A DDoS on a protocol does not necessarily involve the characteristic of flooding by massive amounts of traffic. A well-known example would be the TCP SYN attack, which exploits the allocation of a connection context in the server (Moore et al., 2006; Argyraki and Cheriton, 2009).

As Fig. 1 illustrates, the DDoS defense life-cycle consists of four phases: *prevention*, *monitoring*, *detection*, and *mitigation*. In the prevention phase, appropriate security appliances are put in place at different locations to secure services and data against DDoS attack. In the monitoring phase, tools are deployed to gather useful host or network information to follow the execution of the system. The detection phase involves analysis of the systems that are running, in order to find the source of malicious traffic or malicious attempts to cause DDoS (Abliz, 2011; Shin et al., 2013). The final phase, mitigation, completes the defense life-cycle by evaluating the severity of the attack and selecting the right response (Shameli-Sendi and Dagenais, 2013) at the right time (Shameli-Sendi et al., 2012). In the mitigation phase, a response system selects appropriate countermeasures to effectively handle a DDoS attack or slow down the malicious clients (Walfish et al., 2010).

Existing defense mechanisms against DDoS attacks have limited success because they cannot meet the considerable challenge of achieving simultaneously efficient detection, effective response, acceptable rate of false alarms, and the real-time transfer of all packets (Zargar et al., 2013; PC World, 2013). Prevention and poor detection alone have resulted in huge financial losses to leading businesses around the world (Alomari et al., 2012). Strategies and heuristics for DDoS detection have been researched extensively (Yu et al., 2009). In real world, it is not possible to detect attacks with 100% accuracy (Yu et al., 2012). Therefore, there is a need to concentrate on more efficient mitigation mechanisms. The cloud by its very nature is more exposed to DDoS attack, but it also provides us with additional means to protect applications against DDoS attacks. Therefore, in this work, we mean by DDoS detection the implementation of mechanisms designed to identify the source of malicious traffic or malicious flows, and we define DDoS mitigation as the implementation of mechanisms designed to eliminate the malicious traffic.

Several taxonomies of DDoS defense techniques have been proposed in the literature (Zargar et al., 2013; Geng et al., 2002; Wood and Stankovic, 2004; Mirkovic and Reiher, 2004; Peng et al., 2007; Abliz, 2011). Mirkovic and Reiher (2004) and Zargar et al. (2013)) propose taxonomies for classifying DDoS attacks and defense techniques, while Peng et al. (2007) propose a taxonomy

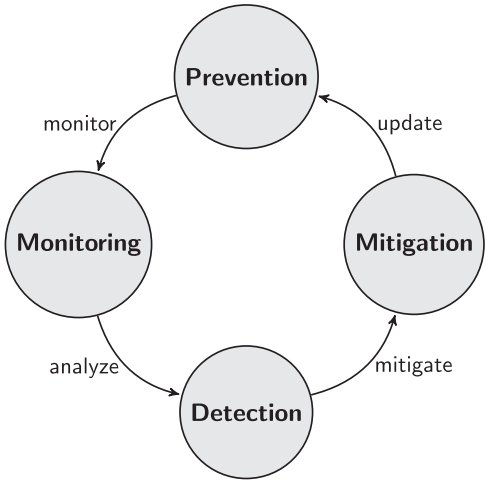

Fig. 1. Defense life-cycle.

for identifying the impact of different types of DDoS attacks. Abliz (2011) presents a taxonomy of a number of defense mechanisms and provides suggestions to address the shortcomings of some defense frameworks. In this paper, we concentrate on DDoS mitigation techniques and how effective they are against such attacks in the cloud. Research and development on frameworks for DDoS defense in the cloud environment are still at an early development stage (Yu et al., 2014). Our work differs from other similar works, in that it concentrates on the ways in which cloud computing is exposed to DDoS attacks and how the essential characteristics of cloud computing can add a new dimension to DDoS defense. DDoS mitigation in Data Center Networks (DCNs) has long been a goal of network security research and industrial community. DDoS protection implementation is not limited to only the cloud providers. It must be implemented end-to-end, from user's equipment through the access and core network to the servers running in the cloud. In this paper, we consider all different DDoS mitigation mechanisms and attempt to map them to different locations in the network, as well as how these various mechanisms can be affected by the characteristics of the cloud.

The main contributions of this survey are the following: first, we provide a taxonomy of the DDoS mitigation strategies applied in cloud computing; second, we extensively review the literature on DDoS mitigation in cloud computing; third, we provide a comprehensive discussion about deploying DDoS mitigation strategy in the cloud; and finally, we provide suggestions for eliminating the current weaknesses of DDoS mitigation and defense mechanisms.

The rest of this paper is organized as follows: In Section 2, the boundaries and scope of the survey are introduced and a methodology to extract the literature is illustrated. In Sections 3 and 4, we present a taxonomy of DDoS prevention and detection techniques respectively. In Section 5, we present our new taxonomy of DDoS mitigation mechanisms for cloud computing. A review of recently developed DDoS mitigation mechanisms for cloud computing is presented in Sections 6 and 7. Section 8 provides a general representation of our proposed deployment strategy of DDoS mitigation mechanisms. In Section 9, we provide some discussion about the current weaknesses of DDoS mitigation and defense frameworks and how they can be remedied by future research. Finally, in Section 10, we present our conclusions.

2. Scope and assumptions of the survey

2.1. Inclusion and exclusion criteria

This paper covers conference papers, journal papers, and doctoral dissertations. Other publication forms such as magazines or newspapers were not included. A total of 98 papers from 2001 to May 2015 were obtained and reviewed. Papers were found via computerized search of the information security risk assessment. The papers were searched according to the online databases: Science Direct, IEEE Xplore, Springer Link Online Libraries, ACM Digital Library, Wiley InterScience, and Ingenta Journals. The papers were carefully reviewed to select those that considered DDoS defense models as the core part. In this paper, the approaches which presented a new and genuine DDoS defense approaches based on a concrete and scientific research approach are selected. The reviewed DDoS mitigation approaches are classified based on proposed taxonomy. They are filtered based on novelty, strong content, and aligning with cloud specific characteristics.

2.2. Methodology

The previous widely accepted classifications for DDoS mitigation were often based around filtering and rate-limiting. These classifications could not answer the following questions to classify the DDoS mitigation approaches: (1) whether multiple nodes cooperate to mitigate the DDoS attack or not? (2) whether the defense strategy is dynamic (adapted to the attack) or static, (3) does the mitigation mechanism adjust the defense architecture respect to the DDoS attack severity? (4) is the network services or topology reconfigured in mitigation process?. In this paper, we will introduce a new classification which will remove many ambiguities created by previous classification. To reach a new taxonomy of DDoS mitigation mechanisms for deployment in the cloud, we went through comprehensive studying of 98 papers and observing the characteristics of the DDoS attacks and those of the cloud environment. At the time of writing, we are not aware of any other classification which could answer all the questions mentioned above.

3. DDoS prevention

Prevention involves the implementation of a set of defenses, practices, and configurations prior to any kind of DDoS attack, with the aim of reducing the impact of such an attack. The following broad categories can be used to classify most DDoS prevention approaches.

3.1. Over provisioning

Until recently, this approach, which is based on preventing an attack on a site by preparing in advance for far more traffic than would be expected during normal operation, was the main prevention mechanism used, although now, with the increasing size of DDoS attacks, this is clearly not sustainable (e.g. in 2009, Arbor reported the largest DDoS to be around 49 Gbps; in 2013, the largest attack was in size, to 300 Gbps, CloudFlare, 2014; and the average DDoS size went from 1.5 Gbps in 2012 to 3.5 Gbps in 2013).

3.2. Modifying scheduling algorithms

The aim of this approach is to favor legitimate traffic over malicious traffic. For example, Ranjan et al. (2006) propose a mechanism for suspicion assignment and scheduler for DDoS-resilient. This framework maps suspicion value into its scheduling decision. The suspicion assignment mechanism uses the arrivals, request arrivals, and workload profiles sessions as input. Then, two scheduling policies were proposed: Least Suspicion First and Proportional to Suspicion Share. Notably, tests have shown that suspicion-aware policies reduce the impact on response time of a DDoS attack to 0.1 s, as opposed to 10 s with suspicion-agnostic policies.

3.3. QoS and resource accounting

The aim of resource accounting is to keep track of resources (e.g. network bandwidth, processor time) across protected domains (Mirkovic and Reiher, 2004). It is useful in preventing DDoS attacks, since we require guaranteed bandwidth, priority, and QoS under a DDoS attack (Goldstein et al., 2008). These resources are protected using QoS mechanisms, such as traffic shaping, scheduling, and congestion avoidance, to enforce traffic class priorities and guarantee fair service to legitimate users. Typically, the objective is to control metrics like dropped packets, delay, and jitter (Mirkovic et al., 2009; Matrawy et al., 2005). QoS

is not a universal solution, however, as the attackers could target gold-class clients, which is where these threats to network use hurt the most.

4. DDoS detection

The next step in defense life-cycle, after DDoS attack prevention, is attack detection. Attack detection algorithms can be categorized into two main groups: *signature-based* and *behavior-based*.

4.1. Signature-based detection

In the signature-based detection technique, the captured traffic is compared with well-defined attack patterns (Douligeris and Mitrokotsa, 2004). This technique may be useful to extract the communication between attackers and their "zombie" computers (Peng et al., 2007). This technique will be ineffective if the communication is encrypted.

4.2. Behavior-based detection

The main idea here is to define what is normal behavior for the traffic, based on the traffic pattern (Shiaeles et al., 2012), so that any deviation from that behavior can be considered to be malicious (Chen et al., 2007). Generally, thresholds are set to make the deviation more configurable and adaptable to different conditions. Normal behavior can be defined based on the following:

- *Comparing forward and reverse traffic:* The traffic is measured in both directions, i.e. uplink traffic and downlink traffic (Gil and Poletto, 2011; Mirkovic et al., 2002). The two should be proportional. If they are not, this is interpreted as an downloading large files in a repetitive way. The disadvantage of this approach is that stealth attacks based on legitimate traffic cannot be detected.
- *Statistics on connections characteristics:* The statistics for different destinations (Liu and Chang, 2011), for example, the number of connection setups and teardowns per second, the duration of sessions, and the number of sessions involving clients, can be used. In Kompella et al. (2004) and Wang et al. (2002), statistics on TCP session setups and teardowns are monitored and used to define abnormal behaviors.
- *Aggregate traffic behavioral monitoring:* The incoming or outgoing traffic from a network node is divided into different traffic aggregates and analyzed to detect patterns (Kuzmanovic and Knightly, 2003). The meant traffic should share the same attribute, for example HTTP, encryption, or UDP connection.
- *Flow traffic behavioral monitoring:* The flow of traffic on the network is monitored, in order to enable fine-grained control of the behavior of different flows (Mahajan et al., 2002). The machine learning algorithms are used to learn the normal behavior of network traffic and then detect the abnormal behaviors (Kline et al., 2008; Bernaille and Teixeira, 2007).

5. Taxonomy of DDoS mitigation mechanisms

To draw up a taxonomy of DDoS mitigation mechanisms for deployment in the cloud, we observe the characteristics of the DDoS attacks and those of the cloud environment. In this section, we briefly introduce our DDoS mitigation mechanisms taxonomy, and in the next section, we discuss each element of this taxonomy in detail, as well as the existing DDoS mitigation approaches in relation to the proposed taxonomy. As Figs. 2 and 3 illustrate, we base our taxonomy on two concepts: mitigation tactic and mitigation strategy. We define these two concepts as follows:

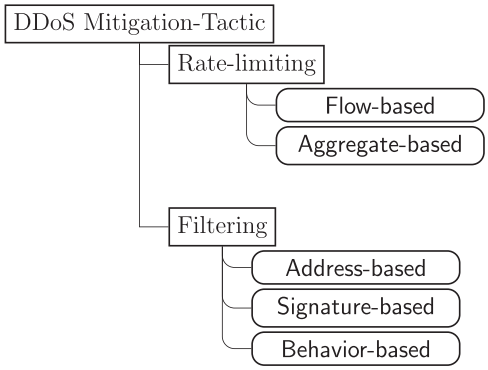

Fig. 2. A taxonomy of mitigation tactics against DDoS attack.

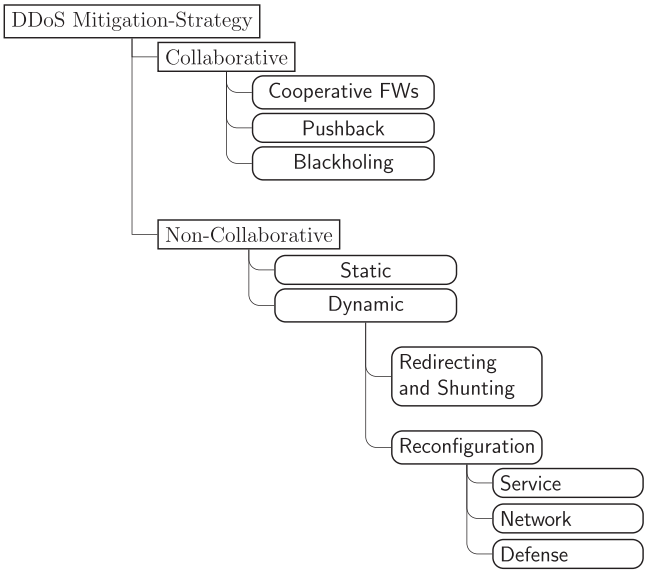

Fig. 3. A taxonomy of mitigation strategies against DDoS attack.

Definition 1 (Mitigation tactic). A mitigation tactic is a local approach implemented in one network component.

There are two categories of mitigation tactic: rate-limiting and filtering. Mitigation tactics will be explained in more detail in the next section.

Definition 2 (Mitigation strategy). A mitigation strategy describes the overall strategy deploying different means at different locations of the network in order to mitigate attacks.

There are two categories of mitigation strategy:

- *Collaborative*: Multiple nodes cooperate to mitigate the DDoS attack and defend the victim effectively. We can distinguish three cooperative defense mechanisms: Firewall, Pushback, and Blackholing.
- *Non-collaborative*: There is no collaboration between services, security appliances, or network elements though these strategies still involve several nodes in the network. This strategy can be dynamic or static. A dynamic strategy acts like an adaptive model, in that the mitigation mechanism automatically adjusts the defense architecture with respect to the DDoS attack severity. In this case, we can either reconfigure the services, security appliances, or network elements, or redirect the traffic to a center to be cleaned. In contrast, in static approaches, the defense mechanisms are not adapted to the attack.

Table 1
Classification of existing DDoS mitigation approaches in cloud based on proposed taxonomy.

Approach	Mitigation strategy	Strategy model	Mitigation tactic	Network		Protection point		
				Traditional	SDN-based	Source-end	Core	Victim-end
Robinson et al. (2003)	Collaborative	Cooperative Firewalls	Rate-limiting	√		√		
Dubendorfer et al. (2005)	Non-Collaborative	Static	Filtering	√		√		
Mirkovic et al. (2005)	Collaborative	Cooperative Firewalls	Rate-limiting	√		√		
Chu et al. (2010)	Non-Collaborative	Static	Rate-limiting		√		√	
Braga et al. (2010)	Non-Collaborative	Static	Filtering		√		√	
Suh et al. (2010)	Non-Collaborative	Static	Rate-limiting		√		√	
Sathyanarayana (2011)	Collaborative	Pushback	Rate-limiting		√	√		
Lua and Yow (2011)	Non-Collaborative	Network Reconfiguration	Filtering	√				√
Yao et al. (2011)	Non-Collaborative	Static	Filtering		√	√		
Dou et al. (2012)	Non-Collaborative	Static	Filtering	√				√
NEC and Radware (http://www.nec.com/en/global/prod/pflow/images_documents/GartnerReport_2013.pdf)	Non-Collaborative	Redirecting & Shunting	Filtering	√				√
Yu et al. (2014)	Non-Collaborative	Service and Defense (hybrid) Reconfiguration	Filtering	√				√
Shin et al. (2013b)	Non-Collaborative	Defense Reconfiguration	Filtering		√		√	
Zargar and Joshi (2010, 2013)	Collaborative	Cooperative Firewalls	Rate-limiting		√	√	√	
Lee et al. (2013)	Collaborative	Pushback	Rate-limiting		√	√		

The strategy needs to be supported in at least one node that does some form of policy enforcement. For example, a threshold-based rate-limiting approach can be implemented in a static or a dynamic way. Similarly, a filtering based on an IP address tactic can be used as a tactic by various cooperating firewalls, or in a pushback or blackholing strategy.

Cloud, SDN, and DDoS protection: Software-Defined Networking (SDN) has been a new paradigm for the network virtualization in which the control and data planes of a network switch are separated form each other (McKeown et al., 2008), the idea being to physically pull the control plane function away from the switch and move it to a PC-based application. Thus, the SDN paradigm allows us to deploy a range of control functions from a single control platform. The control functions can be access control, routing, or virtual machine migration in a variety of contexts (e.g. enterprises, data-centers, WANs) (Jarraya et al., 2014; Koponen et al., 2010; Mehdi et al., 2011). SDN enables dynamic configuration of an entire network using logically centralized control brain in an open approach. This flexibility is beneficial for cloud DCNs, which are made up of numerous virtual switches/routers, computing nodes, and virtual user machines. In short, the SDN paradigm offers the authors of complex network security applications a way to dramatically simplify their designs, particularly in the area of DDoS defense (Shin et al., 2013a; Jafarian et al., 2012; Fonseca et al., 2012; Lara et al., 2014). Our proposed taxonomy is independent of any approach to computer networking. But, SDN is extensively used in collaboration with virtualization in the cloud context (Drutskoy et al., 2013). As we will see in the next sections, where the most relevant research works with respect to the taxonomy presented, SDN makes it much more efficient in answering DDoS at run-time (Vizvary and Vykopal, 2014). This is why we believe SDN is so important in the DDoS mitigation for the cloud and special attention has been paid to SDN in the following sections.

In continuation, we focus on the most relevant research works with respect to the taxonomy presented in Figs. 2 and 3. Section 6 briefly describes the DDoS mitigation tactics and reviews some of the related works. Then, Section 7 briefly presents the most significant mitigation strategies and compares the most relevant reviewed works based on the proposed taxonomy.

6. DDoS mitigation tactics

There are two categories of mitigation tactic: rate-limiting and filtering.

6.1. Rate-limiting

This is the most common way to mitigate a DDoS attack, and perhaps one of the most efficient. It does so by discarding a fraction of the incoming attack packets, in order to reach a manageable number (Molsa, 2004). There are two rate-limiting models (Mirkovic et al., 2003): flow and aggregate:

- *Flow rate-limiting*: This approach considers the individual flows and limits the traffic flows transmission rate to a level below a predetermined rate for each one of those individual flows (Chen et al., 2004).
- *Aggregate rate-limiting*: This approach is based on restricting the bandwidth consumption for aggregate traffic. The aggregate traffic can be based on source/destination application or address, transport protocol or other criteria. For example, Mahajan et al. (2001) propose to rate limit based on a specific protocol (e.g. TCP) or traffic pattern. Another example can be to use the application traffic type (e.g. the HTTP protocol) for defining aggregate traffic, i.e. application traffic exceeding a predefined threshold is rate-limited. The application traffic can be defined through traffic analysis or using the “type of service” field in the IP header (Price, 2002).

6.2. Filtering

This is the most basic approach to mitigating a DDoS attack, and involves eliminating attack traffic. Note that the use of pure filtering mechanisms in transit routers is dependent on the application environment. Filtering can be applied without a problem in an enterprise, however its use for the benefit of the general public can be subject to legal constraints.

Static filters are often used in commercial solutions (Cisco Anomaly Guard, 2007) as a first line of defense. Dynamic rules are only applied when an anomaly is detected in a zone (defined as the network subnets to be defended against DDoS attacks). The resource costs of filtering vary according to the type of filtering. Filtering based on an IP (or MAC) address can be very efficient, and can be performed in line cards with minimal impact from the point of view of resources (El Defrawy et al., 2007). There are three filtering models: address, signature, and behavior.

- *Address-based filtering*: This approach is based on 5-tuple filtering (Source IP address, Source Port, Destination IP address, Destination Port, Protocol) (Gupta and McKeown, 2001), or on the MAC address. It is a quick, simple, and effective, technique for dropping attack traffic aimed at a victim.
- *Signature-based filtering*: This is the most commonly used method of filtering attacks. It is based on the predefinition of signatures that can recognize malicious traffic. The traffic is then analyzed to detect binary or text patterns that match the signatures of DDoS attacks, and, if they do, the attack traffic is dropped (Jiang and Liu, 2003). The efficiency of this approach depends on the update rate for the signatures and the availability of the signature. Because of the changing nature of the attacksvirus polymorphism and metamorphism (Polychronakis et al., 2009), finding the appropriate signatures can become more and more challenging, which makes keeping the date-based malware signature up to date a difficult task. Moreover, a high update rate can decrease performance dramatically, because of the number of interruptions it causes in the routing process.
- *Behavior-based filtering*: This approach looks for detours from a pre-defined normal behavior. There are numerous methods for achieving this, such as data mining, artificial neural networks, and artificial immunological systems (Scepanovic, 2011).

7. Mitigation strategies

In this section, we describe in more detail the mitigation strategies as presented in our taxonomy and discuss the most relevant works classified according to the used strategy. Table 1 presents a comparison of the most relevant works in accordance with the mitigation strategy, the mitigation tactic, the network architecture, and the protection point. Two categories are considered for the network architecture: traditional networking and SDN. The protection point of defense deployment can be the edge router on the attacker side (source-end defense), the routers on the path (core defense), or the edge router on the victim side (victim-end defense).

7.1. Collaborative strategy

Depending on the type of cooperation and our network security architecture, this mitigation strategy can be categorized as Firewalls, Pushback, or Blackholing cooperative defense.

7.1.1. Firewall cooperative defense

The main idea here is to position a number of firewalls in the cloud, and have them communicate and work together to stop a DDoS attack from the nearest available firewall node. In this model, a firewall broadcasts its security policy to the surrounding firewalls (Sterne et al., 2001; El-Soudani and Eissa, 2003).

El-Soudani and Eissa (2003) propose a firewall cooperative defense protocol for traditional networks. The group of firewalls is divided into two sections: Defender Firewalls (DFWs) and Assistant Firewalls (AFWs). A defender firewall is connected to the target network and is responsible for inspecting every incoming packet. If a violation occurs, the DFW broadcasts its security policy to the surrounding firewalls (AFWs) to stop the attacker as close to the source as possible.

Mirkovic et al. (2005) and Robinson et al. (2003) moved away from isolated defense architectures and introduced a distributed framework, DEFCOM, to enable collaboration among all defense nodes. It relies on cooperation between heterogeneous nodes in overlay networks to mount an effective defense. They classify the defense nodes based on their performance. For example, the detection and response defense nodes are most effective near the victim and the source of the attack respectively. In this framework, the rate-limiting tactic has been used to drop malicious packets.

Zargar and Joshi (2010, 2013) propose a distributed and collaborative defense mechanism, called DiCodefense, for detecting and responding to the DDoS flooding attacks. This approach is a hybrid defense, deployed at multiple points, including sources, destinations, and networks. They introduce what they call a DiCoTraM monitoring component, which is used to monitor traffic flows on each Autonomous System (AS), and mitigate the high attack volume closer to the source of attack. Their central Task Assignment Servers (TASs) are responsible for monitoring coordination and distribution among all the routers in each AS. The mitigation decision is made by the DiCoRes component, which responds by distributing the defense against the reported flows by rate-limiting at individual routers in each AS.

7.1.2. Pushback cooperative defense

In this case, the collaboration is between routers (Ioannidis and Bellovin, 2011; Mahajan et al., 2002; Peng et al., 2002). The term “pushback” refers to the fact that a security appliance or network element pushes the information about malicious traffic to other security or network devices. The receiving devices are generally ahead of the source of the malicious traffic in the communication path to the target (Chen et al., 2004). Information such as congestion signature, bandwidth limit, and expiration time is sent to upstream routers in order to rate-limit the traffic closest to the source as possible.

Sathyanarayana (2011) demonstrates that SDN can be leveraged to mitigate DDoS attacks efficiently using the pushback technique with their Frenetic mechanism. Two daemons are implemented in the OpenFlow controller: a pushback daemon and a rate-limiter daemon. The use of the OpenFlow controller prevents pushback messages from being sent by the routers, and all communications are handled by the central controller. The pushback messages are the (defense) rules that would be added to the switches by the controller. The “Preferential Dropping phase of the Pushback” mentioned by Ioannidis and Bellovin (2011) is implemented in this work, in which anomalous nodes are removed first from the flow table of the switch next to the victim, and then successively on all the switches, one after the other, from the victim node to the malicious node.

Lee et al. (2013) propose a collaborative defense model, called coDef, against large scale link-flooding attacks. CoDef consists of two complementary mechanisms: collaborative routing and collaborative rate control. They introduce a specialized server, called the route controller, into each participating AS, which has complete knowledge of the network topology by participating in the intra-domain routing protocol (i.e. IGP). The route controller is implemented in an SDN architecture. In collaborative routing, a congested router sends a congestion notification message to its route controller. Then, a reroute control message is exchanged between route controllers placed in individual ASs to instruct the source ASs to reroute their traffic, which relieves congestion at that router. The collaborative rate control mechanism helps us to distinguish between bot-contaminated and uncontaminated ASs. In this case, a router that is subject to a flooding attack sends rate-control requests to all the ASs to establish the service priorities of their out-going flows (i.e. high-priority flows, low-priority flows, and flows to be filtered).

7.1.3. Blackholing cooperative defense

Also referred to as blackhole filtering, this is a quick and simple technique for dropping attack traffic at the routing level. It forwards the malicious traffic to a virtual interface known as Null0 (Glenn, 2003; Tanase, 2003; Morrow and Gemberling, 2003; Marques et al., 2003). Traffic routed to Null0 is essentially dropped and in case of heavy traffic, the rest of the network remains stable (Tanase, 2003). Blackholing is a cooperative defense mechanism, as it involves DDoS detection mechanisms and routers. These mechanisms instruct the routers to blackhole traffic from the various bots.

7.2. Non-collaborative-static strategy

The static strategy is neither collaborative nor reconfigurable. The mitigation appliance has already been configured, and we only apply a mechanism to mitigate attack when a detection component detects a DDoS.

Chu et al. (2010) propose an OpenFlow-based DDoS defender to realize the autonomic self-defense concept. This approach is an aggregate-based rate-limiting mitigation strategy in which a DDoS defender monitors all the flows of an OpenFlow switch and detects the DDoS attack via volume counting. They consider two static thresholds for this mechanism. The first is 3000 packets every five seconds. Once the traffic has passed this threshold, the second threshold is activated to verify 800 packets per second 5 times over. When these two thresholds meet, the controller realizes that a DDoS attack is occurring, and drops incoming packets until the system registers a return to normal traffic volume.

Suh et al. (2010) propose their Content-Oriented Networking Architecture (CONA), which figures out what content is being requested and can launch a countermeasure against resource-exhausting attacks like DDoS. The architecture is based on an OpenFlow Switch on the NetFPGA platform, which was first proposed by Naous et al. (2008). This architecture performs very well in terms of flow processing and insertion rate. The proposed model captures the packets containing the content name, extracts the requested content from the packet fields, and then it concatenates them. Finally, a flow limiter blocks the DDoS attack flows by limiting the rate of arrival of content request messages.

Braga et al. (2010) propose a lightweight method based on traffic flow features for DDoS attack detection and mitigation. They use an unsupervised artificial neural network, Self-Organizing Maps (SOM), trained with those features. The approach retrieves traffic data for predetermined time intervals, and then it classifies network packets (as either malicious or not) using Self-Organizing Maps. The information is extracted first from the flow entries of all OpenFlow tables by the NOX controller and then transferred to a classifier module to be analyzed. Three main modules are implemented as OpenFlow-enabled application extending the NOX controller: Flow Collector, Feature Extractor, and SOM Classifier.

The Flow Collector module periodically sends requests to all OpenFlow switches' tables. The Feature Extractor module is responsible for extracting important features for attack detection. The Classifier module parses and analyzes the collected informations and finally alerts the matching flows corresponding to DDoS flooding attack. The proposed framework is scalable, so, old module can be updated and new modules can easily added to address other vulnerabilities. The Classifier module analyzes whether the information from the Feature Extractor module can determine legitimate or DDoS flooding attack. The proposed approach can be updated in order to detect new types of attacks.

Dou et al. (2012) propose a Confidence-Based Filtering (CBF) approach for cloud computing. The model generates a nominal profile in the non-attack period. Each packet is then evaluated based on different correlation factors. This evaluation results in a score for each packet defining whether it must be considered malicious or not. The malicious packets are consequently discarded. Correlation characteristics are used to detect malicious flows. First, six single attribute candidates are selected (protocol type, total length, source IP address, flag, time to live (TTL), and destination port number). Then, these six attributes are paired (no two pairs the same), resulting in 15 attribute pairs. The profile is built through measures in small time intervals. The CBF method counts the number of times the 15 attribute pairs appear. These numbers of appearances in turn define the confidence values which are used to score the packets. The packets going beyond the discarding threshold are considered as malicious and then discarded.

Dubendorfer et al. (2005) propose an adaptive traffic control service for DDoS attack mitigation which delegates partial network management capabilities to network tenants using adaptive traffic processing device as an extension to the data plane. The authors compare reactive and proactive mitigation, and point out the drawbacks of reactive mitigation in the face of a reflector DDoS attack, as well as the benefits of the proactive approach. For this, they chose proactive mitigation in overlay networks and built a defense system based on distributed control delegation to the network tenants based on their own address IP. Their model can accommodate a distributed firewall; for example, it can filter traffic close to the source of the attack and has a traceback service for the entire network.

Yao et al. (2011) propose Virtual source Address Validation Edge (VAVE), which extends the SDN NOX controller to check flow entries on the virtual switches. The NOX controller consists of on-demand filtering, validation, and rule adaptor mechanisms designed to prevent a DDoS attack. They use OpenFlow devices to form a protection zone to validate the incoming packet from outside, and redirect the traffic to the controller to take decisions using the VAVE modules.

7.3. Non-collaborative-dynamic strategy

7.3.1. Redirecting and shunting

In redirecting and shunting strategy, instead of the traffic being dropped, it is sent out to a different physical interface (Gonzalez et al., 2007). A data scrubber residing on the alternate data path can then filter out the attack traffic and send the clean traffic to the customer. Recently, the SDN has been used to redirect suspect traffic to these scrubbing centers (Radware, 2013; OpenContrail, 2014).

Several commercial solutions are based on this approach. For example, Riverhead Guard and Cisco Guard are data scrubbers that use this technique to prevent DoS/DDoS attacks. The Cisco DDoS mitigation solution redirects DDoS traffic to the Cisco Guard appliance, which is in charge of cleaning the traffic and forwarding the legitimate traffic to the destination (Cisco Anomaly Guard data sheet, 2007). Alternatively, the traffic can be sent to the cloud to be cleaned and then returned to the target. Verisign is proposing to use this approach (http://www.verisigninternetdefensenetwork.com).

Recently, new solutions have been developed in the industry for a comprehensive and cost-effective solution for SDN hardware DDOS attacks at the core router (http://www.nec.com/en/global/prod/pflow/images_documents/GartnerReport_2013.pdf). The attack detection mechanism is a behavior-based detection algorithm, which compares recently collected tenant network actions to the usual behavior. The algorithm needs to recognize both expected behavior and any serious deviation in that behavior. In case of a DDoS attack, traffic is diverted to the DDoS mitigation device for cleaning, and then the clean traffic is forwarded to its original destination. The proposed model considers response deactivation over time, as the defense system confirms that there is no attack traffic, at which point it alerts the controller to redirect the traffic to its normal path.

7.3.2. Reconfiguration

The reconfiguration strategy changes the topology or defense mechanism of the victim or the intermediate network, in order to prevent the DDoS attack (Mirkovic, 2003). Depending on the level of reconfiguration, this mitigation strategy can be categorized as service reconfiguration, network reconfiguration, or defense reconfiguration:

- *Service reconfiguration*: This strategy can be classified into two categories: (1) service cloning, and (2) service regeneration. In a service cloning strategy, new instances of the service are created in different locations, and then flows are distributed among them (Yau et al., 2005). Service cloning works well in the cloud, since it can pool a large amount of resources to handle a rapid increase in service demand and clone VMs very quickly (Yu et al., 2014; Peng et al., 2012; Armbrust et al., 2009). In contrast, service regeneration tries to fix service vulnerabilities, and then neutralizes the attacker's control of compromised services. It can prevent future attacks that have the same vulnerabilities (Wang, 2005).
- *Network reconfiguration*: In this strategy, network topology is reconfigured to prevent a DDoS attack by providing alternative routes via many IP addresses assigned to protected resources, or via alternative gateways (Cai, 2008; Lua and Yow, 2011). Unlike the service reconfiguration approach, in which extra resources are allocated, in this approach, the network topology is changed. For example, the VM location may be changed from one data center (DC) to another in which location information exposed by attacks is invalid.
- *Defense reconfiguration*: This strategy offers the following two options: (1) the defense system configuration is altered; or (2) the capacity of the defense system is increased. With the first option, the defense system is connected to the victim network. In this case, a default defense mechanism is considered for a cloud application or service. Then, as the volume of DDoS attack packets increases, the defense mechanism is automatically reconfigured to be more robust in the face of the attack. With the second option, as with the service reconfiguration strategy, the defense system (e.g. virtual firewall) can be cloned to mitigate the attack when a new instance of the service is created in a different location (Yu et al., 2014).

Yu et al. (2014) present a service reconfiguration mitigation approach to counter DDoS attacks for individual cloud customers. The main idea is when under attack use the elastic nature of the cloud to clone new service VMs in order to continue providing service to the legitimate users. Simultaneously, new IPSes are

cloned through out the system to filter the malicious traffic. To summarize, no matter how efficient the detection and filtering algorithms are, there remains the task of allocating sufficient resources to address the attack, which this model achieves using queueing theory, based on its estimation of the resource demands and QoS required to support legitimate users commensurate with strength of the attack.

Also, Yu et al. (2014) present a defense reconfiguration mitigation approach considering multiple parallel IPSs, in addition to service reconfiguration mitigation, to take into account the rate of the DDoS attack. To identify the malicious traffic and guarantee the QoS, multiple parallel IPSes are cloned. The number of IPSes and service VMs is decreased when the malicious DDoS traffic reduces. This model, with its IPS activation and deactivation capability, is the only elastic defense system that has been proposed to date.

Lua and Yow (2011) propose a network reconfiguration mitigation based on an intelligent fast-flux swarm network. When under attack, the network is reorganized in order to provide the maximum availability for servers and clients. This fast-flux technique has been used in DNSs to marshal a large number of nodes, in order to greatly enhance the availability of a particular resource. As a result, an attacker must target more than one IP address. A parallel optimization algorithm, for example the Intelligent Water Drop, is used to constantly reconfigure the swarm network (Shah-Hosseini, 2009).

Shin et al. (2013b) present a defense reconfiguration framework called FRESCO. Fresco framework is provided with an application development environment to help prototyping of detection and mitigation security modules. The framework is based on Openflow. These modules are combined into security services that can be efficiently deployed to produce complex network defense applications. FRESCO framework provides the developers with an API to access network flows and statistics. It then mitigates the attack by pushing new flow constraint rules to the controller.

8. Mitigation deployment

A new taxonomy of DDoS mitigation strategies to combat DDoS attacks in cloud computing has been proposed in this paper. Figure 4 depicts a general representation of the deployment scenario for the described DDoS mitigation strategies, which is based on a simple 3-tier cloud computing architecture. The discussion in this section is based on the deployment of a simple 3-tier web application in the cloud computing architecture. Actually, to better describe the possible deployment, we consider a 3-tier web application and how it could be deployed in the cloud. We then use this scenario as an illustrative example to show the possible deployment of DDoS mitigation mechanisms.

Note that we describe the deployment scenario in this section for purely informative purposes, our main goal being to help the reader to better grasp the deployment options, and not to provide guidelines or an exhaustive study. The access and aggregation networks connect cloud tenants to the core network that have high capacity to process tenants' packets to different cloud service providers. In Table 2, we show the possible deployment locations for mitigating a DDoS attack in cloud computing for each strategy, in order to better explain the deployment scenario depicted in Fig. 4.

Access, aggregation, and core networks DDoS mitigation deployments: Generally, the access and aggregation networks connect cloud tenants to the core network that have high capacity to carry tenants' traffic to different cloud service providers. Even though, the large cloud service providers support high bandwidth traffic inside their data centers, the bandwidth at core network is often much higher than the traffic inside the data center. From security point of view, it is important to eliminate the DDoS traffic as early as possible in the access, aggregation and core networks. Based on our literature study, the filtering and rate limiting are the principal means used in these networks. The rate-limiting and filtering mitigation tactics are positioned all over the architecture, and can be deployed in all routers, switches, and firewalls (FWs). In some deployments, it is possible additionally for the network operators to deploy the scrubbing centers. The scrubbing center is a cleaning station where inter/intra-network traffic is analyzed and malicious DDoS packets are removed. The traffic is typically redirected using Domain Name Servers (DNSs) or Border Gateway Protocol (BGP) routers, where the attack mitigation strategy drops attack traffic and returns clean traffic to the network for delivery.

Cloud service provider DDoS mitigation deployments: Generally, the access to the cloud service provider data center is protected by

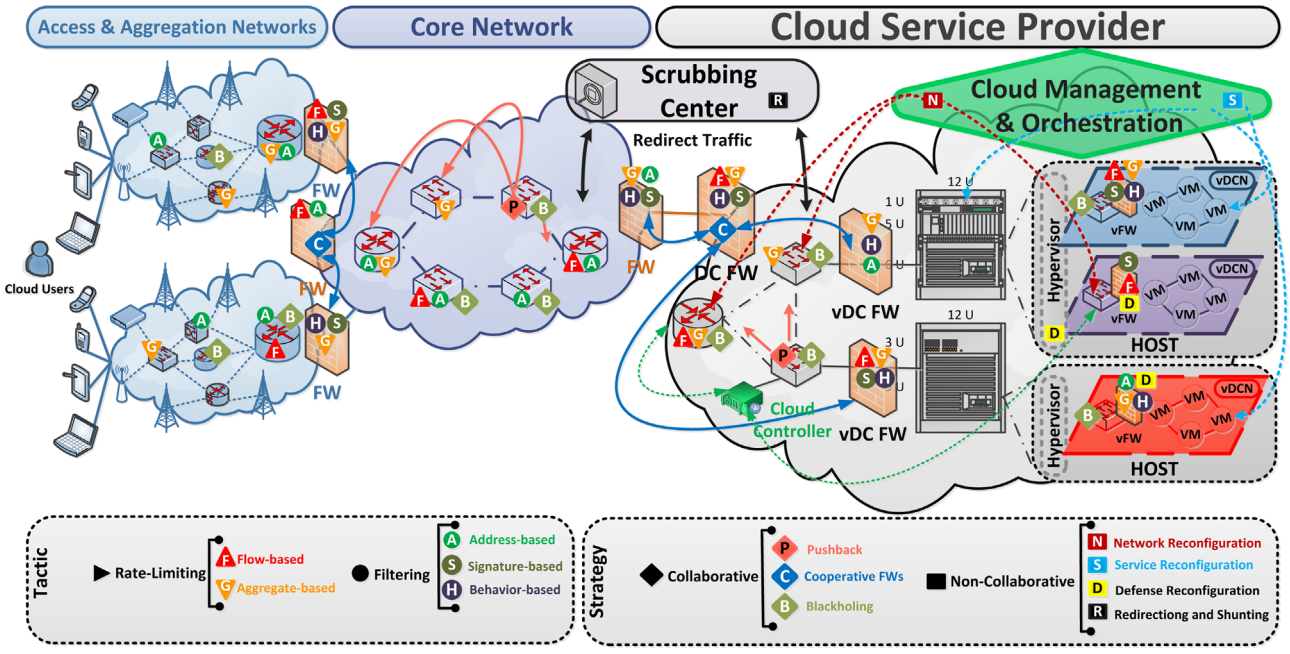

Fig. 4. General representation of different mitigation strategies against DDoS attacks in cloud computing.

Table 2
DDoS mitigation deployment location in cloud computing.

DDoS Mitigation	Models	Access, Aggr. & Core Networks				Cloud Service Provider							
											Hosts		
		Routers	Switches	FWs	Scrubbing Center	Routers	Switches	FWs	Scrubbing Center	Cloud Mgmt & Orch.	virtual Switches	virtual FW	Hypervisor
Rate-limiting	Flow	√	√	√		√	√	√			√		√
	Aggregate	√	√	√		√	√	√			√		√
Filtering	Address	√	√	√		√	√	√				√	√
	Signature			√					√			√	√
	Behavior			√					√			√	√
Non-Collaborative	Network Reconfiguration	√	√			√	√			√	√		
	Service Reconfiguration									√			
	Defense Reconfiguration									√		√	√
	Redirecting & Shunting				√				√	√			
Collaborative	Pushback	√	√			√	√			√			
	Cooperative FWs			√				√		√			
	Blackholing	√	√			√	√			√	√		

Table 3
Summary of advantages and disadvantages of DDoS mitigation tactics.

Mitigation tactic	Advantages	Disadvantages
Rate-limiting	• Easy to deploy and provision across network nodes • Flexible through dynamic threshold setting • Useful when detection has many false positives	• Coarse grain filtering also hitting legitimate traffic • Cannot completely eliminate the malicious traffic
Filtering	• Easy to deploy and provision across network node • Flexible through adding and removing addresses	• Cannot distinguish between malicious and legitimate traffic associated to the same sources • Difficult to detect all malicious addresses

FWs. FWs are placed between external networks and internal virtual data centers (VDCs) and cloud service provider infrastructure to filter and drop unauthorized traffic. In today's large data centers, up to 75% of traffic can be between different servers inside the data center, i.e. east–west traffic (Juniper, 2011). Therefore, a DDoS attack inside these large data centers is a possibility. We then assume that virtual FWs are placed between hypervisors and virtual networks in addition to the entrance to each virtual data center to protect tenants' VMs and eliminate malicious traffic as early as possible. As all these security appliances are in the same administrative domain, collaborative mitigation can be now implemented through cooperation between these security appliances. Additionally, the deployment of these different security appliances is orchestrated by cloud management, which, through knowledge of network topology and orchestration capabilities, can deploy different DDoS mitigation mechanisms in different places in the cloud service provider's infrastructure. Furthermore, the cloud management can orchestrate reconfiguration mitigation strategies leveraging the predefined work-flows to deploy adequate DDoS mitigation mechanisms.

9. Discussion

9.1. DDoS mitigation strategies and tactics: advantages and disadvantages

The advantages and disadvantages of each DDoS mitigation tactic and strategy are summarized in Tables 3 and 4 respectively.

As far as mitigation tactics are concerned, rate-limiting and filtering can be efficiently implemented through access rules inserted into routers or FWs; however, they prevent the DDoS attack in different ways. Rate-limiting is easy to deploy and provision across network nodes, and is flexible, through dynamic threshold setting. Rate-limiting is used when the DDoS detection algorithm is congestion-based, and legitimate traffic cannot be precisely distinguished from attack traffic (Chen et al., 2004). Since the congestion-based DDoS detection algorithm yields many false positives, applying rate-limiting to the traffic would be preferable to using the filtering approach (Abliz, 2011).

Filtering, like rate-limiting, is easy to deploy and flexible enough, through adding/removing addresses or updating the detection algorithm, to cover new kinds of attacks (e.g. improving the classifier in behavior-based detection, or adding a new signature in signature-based detection). So, in fact, filtering works better with a DDoS detection algorithm that detects attacks by verifying packet headers (Chen et al., 2004). However, the disadvantage of this tactic is that it cannot distinguish between malicious and legitimate traffic associated with the same sources. In practice, it is challenging to use, as it has difficulty detecting all malicious addresses or attack types.

A collaborative mitigation strategy has a distributed DDoS prevention architecture. Its distributed nature makes it more resilient to DDoS attacks. The great advantage of this strategy, if it is applied properly, is that it contains the attack close to the attack sources. Pushback cooperative defense creates a new requirement for routers, which is to support a protocol that enables communication between two routers so that they can coordinate the rate-limiting or filtering tactics. Their deployment depends on the ability of the downstream router to determine what fraction of the

Table 4
Summary of advantages and disadvantages of DDoS mitigation strategies.

Mitigation strategy	Strategy model	Advantages	Disadvantages
Collaborative	Cooperative Firewalls, Push-back, Blackholing	• Containing the attack close the attack sources	• Difficult to put in place the collaboration
		• Considering distributed mitigation architecture (robust against attack)	• Difficult to put in place trust and secure interactions between different domains • Dependent on network topology
	Static	• Easy to deploy and put in place	• Inability to automatically adjust the defense architecture based on severity of DDoS attack
Non-Collaborative	Reconfiguration (Service, Network, Defense)	• Efficient defense as it is elastic	• Deploy at victim side
		• Distributed solution therefore more reliable as it could create instances in different DCs • Scalable solution as it could divide the attack into smaller chunks	• Need for some orchestration and precise information about resources and network topology in order to put in place the defense mechanisms
	Redirecting and Shunting	• Shield completely the target	• More difficult to put in place

attack traffic comes from up-stream routers. Except for the case of simple point-to-point connections between routers, when the router can only see which line cards the traffic is coming from and not the corresponding routers, then there is a need for additional mechanisms to find out how much attack traffic is being sent over by upstream routers. Unfortunately, pushback can inflict collateral damage when the attackers are co-located with the legitimate users and the filtering rules are not precise enough to filter only bad traffic. In addition, the expiration time of the rate-limiting tactic must be carefully managed to avoid affecting the legitimate traffic of an unsuspecting victim of a botnet. The main disadvantage of pushback is that all routers upstream must implement it, if it is to be effective against a large-scale DDoS. Also, it is difficult to implement in practice. Moreover, core routers have little incentive to deploy pushback. In general, collaborative mitigation is completely dependent on network topology, and it is difficult to establish the collaboration. Another limitation of this approach is the difficulty of establishing secure connections between routers from different domains. The cloud environment changes this picture in a major way, as different routers can be controlled and managed by cloud orchestration mechanisms, which SDN helps us to implement.

Non-collaborative strategies can be static or dynamic. A static strategy is easy to deploy, since all mitigation appliances have already been configured and we only apply rate-limiting or filtering to mitigate an attack when an attack occurs. Moreover, it can either be a source-end, a core defense, or a victim-end defense. The main disadvantage of the static strategy is that it is non-adaptive. The mitigation mechanism does not have the ability to automatically readjust the defense architecture respect to the severity of a DDoS attack.

A dynamic strategy acts like an adaptive model, as the mitigation mechanism can automatically readjust the defense architecture with respect to the DDoS attack severity. Dynamic strategies can be classified into two groups: (1) reconfiguration; and (2) redirecting and shunting. A reconfiguration mitigation strategy is an efficient model, since it leads to an elastic defense. The clear advantage of the reconfiguration mitigation strategy in the cloud environment is that it provides a distributed solution, which makes it more reliable as it can create instances in different DCs. In terms of disadvantages, this strategy needs some orchestration, along with precise information about resources and network topology in order to put the defense mechanisms in place. Also, it cannot be applied to all scenarios, and sometimes it is not possible to reconfigure it, because of deployment or resource constraints.

Redirecting and shunting mitigation shields the target completely, so that it does not see any malicious traffic. This means that its resources are not consumed to fight the attack. Another advantage of this model is that it outsources the work to the security providers who can aggregate more resources to fight a DDoS attack.

9.2. Evaluation of existing proposals

In the following we enumerate some of significant characteristics for DDoS mitigation strategies and discuss them in the context of cloud computing:

Static defense: The current DDoS mitigation approaches are often based on static defense postures, i.e. hardware-type security appliances with predefined security capabilities deployed in predefined places in the network topology. The dynamic mechanisms such as cooperative firewalls (Section 7.1.1) and reconfiguration (Section 7.3.2) are considered in only few references. Pushback approach is more widely cited (see Section 7.1.2) though both cooperative defense and pushback have been considered unrealistic because the various security appliances, e.g. firewalls or routers, were controlled by different administrative authorities (Ioannidis and Bellovin, 2011; Mahajan et al., 2002; Peng et al., 2002; Sathyanarayana, 2011; Lee et al., 2013). The practical difficulty of establishing any degree of cooperation between these authorities was cited as the major obstacle beyond technical reasons. However, in the cloud computing context, many of these firewalls and routers inside and at the edge of the data centers are now under the same administrative control, i.e. cloud service provider. Therefore, cooperation between these security appliances can now be enforced through cloud service provider orchestration and management components making cooperative defense mechanisms now a viable solution.

On the contrary, the blackholing and redirecting have received wide coverage and many industry wide implementations of these latters are available. To the best of our knowledge, we have not seen any industry implementation of cooperative firewalls or pushback approaches.

We can also see from Table 1 that, although cooperative firewalls have been proposed in Zargar and Joshi (2010, 2013), Mirkovic et al. (2005), and Robinson et al. (2003), cooperative virtual firewalls have not yet received much attention (we have not found any reference to any virtual proposal). The ease of creation of the virtual firewalls inside the same virtual data center by the cloud service provider opens new opportunity for deploying cooperative firewalls at will in different points in the data center. In light of changes highlighted above, the cooperative defense mechanisms should receive renewed interest in the cloud computing context and deserve receiving more attention.

Strongly dependent on deployment location in network topology: The current approaches strongly depend on where the DDoS defense mechanisms are deployed in the network topology. We see three types of location: source-end defense (e.g. the edge router) closer to the attacker side, the core defense (e.g. core router), and victim-end defense (e.g. the edge router) closer to the victim side (Douligeris and Mitrokotsa, 2004; Singh et al., 2013; Dubendorfer et al., 2005; Mirkovic, 2003). Source-end defense systems are often inaccurate, since the source of the attacks can be spoofed or distributed in different domains in order to hide the sources (the volume of traffic from any one source may not be significant to permit differentiation between legitimate and malicious traffic) (Seo et al., 2013; Oikonomou et al., 2006). Core defense needs complete coverage, since a single location cannot capture all attacks. In addition, the high volume of traffic in these nodes needs large DDoS mitigation deployments which are costly.[1] Victim-end defense suffers from high flood rate, and is itself vulnerable to DDoS attacks. These drawbacks motivate a decentralized and collaborative approach (Zargar et al., 2013; Singh et al., 2013; Shi et al., 2005). The cloud environment by its flexible, scalable and elastic nature is a perfect fit for deploying distributed nodes deployed throughout the data center. However, a distributed and collaborative DDoS defense system requires many message exchanges between these nodes, and suffers from high overhead and delays in detection and response (El-Soudani and Eissa, 2003).

As we have seen in Table 1, the majority of existing traditional mitigation frameworks are of the victim-end defense type. The reason for this is that all the traffic can be easily observed on the victim side, which maximizes detection accuracy (Oikonomou et al., 2006). The advent of SDN gives us a new paradigm, offering a dramatically simplified design for complex network security applications, especially in fighting DDoS (Shin et al., 2013a; Jafarian et al., 2012; Fonseca et al., 2012; Lara et al., 2014). SDN-based solution using middle boxes created dynamically (Qazi et al., 2013; Anderson et al., 2012; Rajagopalan et al., 2013; Sekar et al., 2012; Shin et al., 2013a; Fayazbakhsh et al., 2013) with DDoS mitigation mechanisms using SDN as described in OpenContrail (2014) and DDoSDefense4all (2013) can deal with attacks in source and core networks very efficiently.[2] This architecture makes it easier to efficiently capture and analyze data collected at a single point, and provides great flexibility in terms of adding (defense) rules to SDN switches, and removing them from the switches. SDN also gives a new perspective to pushback mechanisms (collaborative mitigation). As a matter of fact, since the SDN controller is in charge of many switches in the network, it can filter the malicious traffic closest to the source, thereby eliminating any difficulties that arise due to the collaboration between different switches (OpenContrail, 2014; DDoSDefense4all, 2013).

Note that east–west traffic in today's data centers is as important as north–south traffic, sometimes even more, which means that counteracting internal DDoS attacks beyond data center gateways in a (virtual) data centers should be a high priority. A strategy based on dynamic creation of virtual security appliances in different real or virtual network topology orchestrated by cloud management can be a promising approach to prevent internal attacks.

Application context-free: None of the defense mechanisms referred in this study are application context-aware, i.e. there is no means for adapting DDoS defense mechanisms to the type of applications, or further more for adapting the defense to the type of attacks on the target application. This approach contributes to a one-size-fits-all type of approach where DDoS defense mechanisms are deployed independently from the applications they need to protect or attacks on them. This generic approach is not efficient and resource consuming. In the contrary, the cloud provides necessary means to implement an application aware defense through deployment at run time, dynamic modifications of defense mechanisms or security policy composition/decomposition (Shin et al., 2013a,b; Qazi et al., 2013; Anderson et al., 2012; Rajagopalan et al., 2013; Sekar et al., 2012; Fayazbakhsh et al., 2013). This defense can be adapted for each application deployed in the cloud. Therefore, the cloud based DDoS defense mechanism can explore new mitigation strategies to protect against different DDoS attack types for different application types instead of a uniform and generic approach for all applications running in the cloud.

Application context-free: Even though, the application context is used more and more often when it comes to DDoS attack detection and prevention, the defense mechanisms for mitigation are often not application context-aware, i.e. there is no means for adapting DDoS mitigation mechanisms to the type of applications, or further more for adapting the defense to the type of attacks on the target application. This approach contributes to a one-size-fits-all type of approach where DDoS mitigation mechanisms are deployed independently from the applications they need to protect or attacks on them. This generic approach is not efficient and resource consuming. In the contrary, the cloud provides necessary means to implement an application aware defense through deployment of application aware mitigation mechanisms at run time, dynamic modifications of defense mechanisms to tune in the mitigation to the specific attack on specific components of the application or through security policy composition/decomposition (Shin et al., 2013a,b; Qazi et al., 2013; Anderson et al., 2012; Rajagopalan et al., 2013; Sekar et al., 2012; Fayazbakhsh et al., 2013). This defense can be adapted for each application deployed in the cloud. Further, as this is already the case for scaling in/out of the applications deployed in the cloud, one can imagine the deployment of pre-defined work flows for deploying dynamically DDoS mitigation mechanisms targeting specific components of the applications. Therefore, the cloud based DDoS defense mechanism can explore new mitigation strategies to protect against different DDoS attack types for different application types instead of a uniform and generic approach for all applications running in the cloud.

Network/service/defense reconfiguration: As described in Section 7.3.2, the reconfiguration of networks/defense/service is a new and efficient way of addressing DDoS attacks. The cloud management of virtual resources (e.g. network, computing, storage) makes it possible to easily reconfigure at run time the network/service/defense to meet the specific threat posed by the DDoS attacks (Yu et al., 2014; Lua and Yow, 2011; Shin et al., 2013b). Therefore, the reconfiguration in the cloud context takes much more central role than in the hardware deployments.

End-to-end DDoS defense: At the end, pervasive DDoS mitigation mechanisms, i.e. end-to-end defense from access point up to the servers running in the cloud, are often not considered. This scenario has become interesting for the servers running in data centers installed in Telecom operators network. In this latter, the access network, core network, and data centers are managed by the same administrative authorities. Further, the Telecom networks characterized by a strong identification of different users combined with the end-to-end control described above can drastically improve the mitigation of DDoS attacks close to the sources.

[1] Note that the high costs are to be considered as major obstacles for their deployments by ISPs.

[2] An extension of these mechanisms by cloud service providers can easily extend these works to be considered for victim-end defense.

10. Conclusion

Recently, the number and the volume of DDoS attacks have been increased rapidly. The cloud by its open nature is exposed to DDoS attacks. At the same time, ever changing nature and type of DDoS attacks has made the appropriate and efficient detection and response to these attacks a challenging task. Many research activities concentrate on DDoS detection though recent experience and the repetitive occurrences of DDoS attacks have shown that DDoS detection has its limits. Therefore, in addition to the research on DDoS detection, there is need for additional research on more efficient DDoS mitigation strategies in order to create a stronger defense.

A comprehensive survey of DDoS mitigation techniques for cloud computing has been presented in this paper. The key finding of this work is that SDN has brought a new perspective to DDoS mitigation in the cloud. The new aspects have been embraced by academic research on two main directions: first, more efficient implementations of known techniques. These implementations use SDN centralized control to better implement rate limiting and filtering techniques or to steer suspect traffic into security appliances to be analyzed and cleansed. Second, SDN has helped us to enhance the collaborative approaches such as push backs in SDN switches. We consider though that the cloud flexibility and the usage of SDN in cloud environment can bring more DDoS mitigation strategies. Cloud and SDN combined allow reconfiguration at run time of virtual services, networks, and defense mechanisms. This opens new directions in the research and makes possible new strategies in the cloud significantly different from the existing DDoS mitigation defense approaches deployed today.

Based on our study, we believe that further research can be conducted in the following areas: (i) *Adequate defense*: creating context-aware defense mechanisms in the cloud based on the application security attributes and profiles. Virtual security appliances advent and their fast on demand deployment in the cloud open the door to deploy application specific security mechanisms for different virtual data centers, or even further extend this to further deploy specific security mechanisms per virtual applications based on new attacks targeting these applications. (ii) *Elastic defense system*: the orchestration capabilities of the cloud bring the possibility of activating, scaling up and down, and scaling in and out the appropriate security mechanisms according to the rate of attack or cloud risk tolerance. In addition, the cloud creates the possibility of dynamically and automatically re-configuring virtual data centers in order not only to duplicate or clone the services in the same data centers or different data centers but also to re-organize the virtual networks to re-direct the suspect traffic. (iii) *Cloud-based defense system*: the possibility for the defense mechanisms to be orchestrated by the cloud management among different virtual data centers in order to consolidate different security mechanisms making DDoS attack mitigation more efficient and economic but also benefiting from the possibility of sharing different security mechanisms specialized hardware among different cloud tenants.

Acknowledgments

This work is partly funded by Natural Sciences and Engineering Research Council of Canada Research Chair on Sustainable Smart Eco-Cloud, NSERC-950-229052, and by the NSERC CRDPJ 424371-11: ECOLOTIC Sustainable and Green Telco-Cloud. In addition, the authors would like to thank Dr. Mats Näslund at Ericsson Sweden Research and Dr. Yosr Jarraya at Ericsson Canada Research for their constructive comments and helpful feedback.

References

Abliz M. Internet denial of service attacks and defense mechanisms. University of Pittsburgh, Department of Computer Science, Technical report. TR-11-178; 2011.
Alomari E, Manickam S, Gupta BB, Karuppayah S, Alfaris R. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. Int J Comput Appl 2012;49(7):24–32.
Anderson JW, Braud R, Kapoor R, Porter G, Vahdat A. xOMB: extensible open middleboxes with commodity servers. In: Proceedings of the eighth ACM/IEEE symposium on architectures for networking and communications systems; 2012. p. 49–60.
Argyraki K, Cheriton DR. Scalable network-layer defense against internet bandwidth-flooding attacks. IEEE/ACM Trans Netw 2009;17(4):1284–97.
Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, et al. Above the clouds: a Berkeley view of cloud computing. Berkeley: EECS Department, University of California. Technical report UCB/EECS-2009-28; 2009.
Bernaille L, Teixeira R. Early recognition of encrypted applications. In: Proceedings of the eighth passive and active measurement conference (PAM'07); 2007.
Bhadauria R, Chaki R, Chaki N, Sanyal S. A survey on security issues in cloud computing, CoRR 2011, arxiv:abs/1109.5388.
Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. In: 2010 IEEE 35th conference on local computer networks (LCN); 2010.
Cai Y. A ddos defense mechanism with topology reconfiguration. J Eng Comput Archit 2008;2(1):65–78.
Chen LC, Longstaff TA, Carley KM. Characterization of defense mechanisms against distributed denial of service attacks. Comput Secur 2004;23(8):665–78.
Chen Y, Hwang K, Ku WS. Collaborative detection of ddos attacks over multiple network domains. IEEE Trans Parallel Distrib Syst 2007;18(12):1649–62.
Chu Y, Tseng M, Chen Y, Chou Y, Chen Y. A novel design for future on-demand service and security. In: The 12th IEEE international conference on communication technology (ICCT); 2010.
Cisco Anomaly Guard data sheet ⟨http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6235/product_data_sheet0900aecd80220a7c.html⟩; 2007 [accessed July 2015].
Cisco Anomaly Guard ⟨http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6235/product_data_sheet0900aecd80220a7c.html⟩; 2007 [accessed July 2015].
CloudFlare ⟨https://www.cloudflare.com/ddos⟩; 2014 [accessed July 2015].
DDoS-Defense4all ⟨https://wiki.opendaylight.org/images/d/d1/Defense4All_Proposal_Overview_-_130718.pdf⟩; 2013 [accessed July 2015].
Denial of service protection in a programmable network. ⟨http://www.nec.com/en/global/prod/pflow/images_documents/GartnerReport_2013.pdf⟩; 2013 [accessed July 2015].
Dou W, Chen Q, Chen J. A confidence-based filtering method for DDoS attack defense in cloud environment. Future Gener Comput Syst 2012;29(7):1838–50.
Douligeris C, Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Comput Netw 2004;44(5):643–66.
Drutskoy D, Keller E, Rexford J. Scalable network virtualization in software-defined networks. IEEE Internet Comput 2013;17(2):20–7.
Dubendorfer T, Bossardt M, Plattner B. Adaptive distributed traffic control service for DDoS attack mitigation. In: The 19th IEEE international on parallel and distributed processing symposium; 2005.
El Defrawy K, Markopoulou A, Argyraki K. Optimal allocation of filters against DDoS attacks. In: Information theory and applications workshop; 2007. p. 140–9.
El-Soudani MM, Eissa MA. Cooperative defense firewall protocol. In: Security and privacy in the age of uncertainty; 2003. p. 373–84.
Fayazbakhsh SK, Sekar V, Yu M, Mogul JC. FlowTags: enforcing network-wide policies in the presence of dynamic middlebox actions. In: Proceedings of the second ACM SIGCOMM workshop on hot topics in software defined networking; 2013. p. 19–24.
Fonseca P, Bennesby R, Mota E, Passito A. A replication component for resilient OpenFlow-based networking. In: Network operations and management symposium (NOMS); 2012. p. 933–9.
Geng X, Huang Y, Whinston AB. Defending wireless infrastructure against the challenge of DDoS attacks. Mob Netw Appl 2002;7(3):213–23.
Gil TM, Poletto M. MULTOPS: a data-structure for bandwidth attack detection. In: Proceedings of 10th Usenix security symposium; 2001.
Glenn M. A summary of dos/ddos prevention, monitoring and mitigation techniques in a service provider environment. SANS Institute; 2003.
Goldstein M, Reif M, Stahl A, Breuel T. High performance traffic shaping for DDoS mitigation, In: Proceedings of the 2008 ACM CoNEXT conference; 2008.
Gonzalez JM, Paxson V, Weaver N. Shunting: a hardware/software architecture for flexible, high-performance network intrusion prevention. In: Proceedings of the 14th ACM conference on computer and communications security; 2007. p. 139–49.
Gupta P, McKeown N. Algorithms for packet classification. IEEE Netw 2001;15(2):24–32.
Huici F, Handley M. An edge-to-edge filtering architecture against DoS. ACM SIGCOMM Comput Commun Rev 2007;37(2):39–50.
Ioannidis J, Bellovin SM. Pushback: router-based defense against DDoS attacks. In: Proceedings of NDSS; 2011.
Jafarian JH, Al-Shaer E, Duan Q. Openflow random host mutation: transparent moving target defense using software defined networking. In: Proceedings of the first workshop on hot topics in software defined networks; 2012. p. 127–32.

Jarraya Y, Madi T, Debbabi M. A survey and a layered taxonomy of software-defined networking. IEEE Commun Surv Tutor 2014;16(1).
Jiang B, Liu B. High-speed discrete content Sensitive pattern match algorithm for deep packet filtering. In: Proceedings of the 2003 international conference on computer networks and mobile computing; 2003. p. 149–56.
Juniper. Network fabrics for the modern data center; 2011.
Kline J, Nam S, Barford P, Plonka D, Ron A. Traffic anomaly detection at fine time scales with bayes nets. In: The third international conference on internet monitoring and protection; 2008. p. 37–46.
Kompella RR, Singh S, Varghese G. On scalable attack detection in the network. In: Proceedings of IMC 2004; 2004. p. 187–200.
Koponen T, Casado M, Gude N, Stribling J, Poutievski L, Zhu M, et al. Onix: a distributed control platform for large-scale production networks. In: The symposium on operating systems design and implementation (NSDI); 2010.
Kuzmanovic A, Knightly EW. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In: Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications; 2003. p. 75–86.
Lara A, Kolasani A, Ramamurthy B. Network innovation using openflow: A survey. IEEE Communications Surveys & Tutorials 2014;16(1):493–512.
Lee SB, Kang MS, Gligor VD. CoDef: collaborative defense against large-scale link-flooding attacks. In: Proceedings of the ninth ACM conference on emerging networking experiments and technologies; 2013. p. 417–28.
Liu HI, Chang KC. Defending systems against tilt DDoS attacks. In: The sixth international conference on telecommunication systems, services, and applications (TSSA); 2011. p. 22–7.
Lua R, Yow KC. Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network. IEEE Netw 2011;25(4):28–33.
Mahajan R, Floyd S, Wetherall D. Controlling high-bandwidth flows at the congested router. In: Proceedings of the ninth international conference on network protocols; 2001. p. 192–201.
Mahajan R, Bellovin S, Floyd S, Paxson V, Shenker S. Controlling high bandwidth aggregates in the network. ACM Comput Commun Rev 2002;32(3).
Mahajan R, Bellovin S, Floyd S, Ioaannidis J, Paxson V, Shenker S. Aggregate-based congestion control. Comput Commun Rev 2002;32(3).
Mahajan R, Bellovin SM, Floyd S, Ioannidis J, Paxson V, Shenker S. Controlling high bandwidth aggregates in the network. ACM SIGCOMM Comput Commun Rev 2002;32(3):62–73.
Marques P, Sheth N, Raszuk R, Greene B, Mauch J, McPherson D. Dissemination of flow specification rules. The internet engineering task force, Internet-drafts; 2003.
Matrawy A, van Oorschot PC, Somayaji A. Mitigating network denial-of-service through diversity-based traffic management. In: Applied cryptography and network security; 2005. p. 104–21.
McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, et al. OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput Commun Rev 2008;38(2):69–74.
McPherson D. 5th Edition of the worldwide infrastructure security report by Danny McPherson ⟨http://asert.arbornetworks.com/2010/01/5th-edition-of-the-world wide-infrastructure-security-report⟩; 2010 [accessed July 2015].
Mehdi SA, Khalid J, Khayam SA. Revisiting traffic anomaly detection using software defined networking. In: Proceedings of recent advances in intrusion detection; 2011.
Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput Commun Rev 2004;34(2):39–53.
Mirkovic J, Prier G, Reiher P. Attacking DDoS at the source. In: Proceedings of 10th IEEE international conference on network protocols; 2002. p. 312–21.
Mirkovic J, Prier G, Reiher P. Source-end DDoS defense. In: The second IEEE international symposium on network computing and applications; 2003. p. 171–8.
Mirkovic J, Robinson M, Reiher P, Oikonomou G. Distributed defense against DDOS attacks. University of Delaware CIS Department technical report CIS-TR-2005-02; 2005.
Mirkovic J, Hussain A, Fahmy S, Reiher P, Thomas RK. Accurately measuring denial of service in simulation and testbed experiments. IEEE Trans Dependable Secure Comput 2009;6(2):81–95.
Mirkovic J. D-WARD: source-end defense against distributed denial-of-service attacks [Ph.D. thesis]. University of California Los Angeles; 2003.
Molsa J. Effectiveness of rate-limiting in mitigating flooding DOS attacks. In: International conference on communications, internet, and information technology; 2004. p. 155–60.
Moore D, Shannon C, Brown DJ, Voelker GM, Savage S. Inferring internet denial-of-service activity. ACM Trans Comput Syst 2006;24(2):115–39.
Morrow C, Gemberling B. How to allow customers to blackhole their own traffic ⟨http://www.twdx.net/CustomerBlackHole/⟩; 2003 [accessed July 2015].
Naous J, Erickson D, Covington GA, Appenzeller G, McKeown N. Implementing an openflow switch on the netfpga platform. In: Proceedings of the fourth ACM/IEEE symposium on architectures for networking and communications systems (ANCS'08); 2008. p. 1–9.
NetworkWorld. America's 10 most wanted botnets ⟨http://www.networkworld.com/news/2009/072209-botnets.html⟩; 2009 [accessed July 2015].
Oikonomou G, Mirkovic J, Reiher P, Robinson M. A framework for a collaborative DDoS defense. In: The 22nd computer security applications conference; 2006. p. 33–42.
OpenContrail. DDoS ⟨http://www.sdncentral.com/channel/juniper/⟩; 2014 [accessed July 2015].
PC World. ⟨http://www.pcworld.com/article/2035407/ddos-attacks-have-increased-in-number-and-size-this-year-report-says.html⟩; 2013 [accessed July 2015].
Peng T, Leckie C, Ramamohanarao K. Defending against distributed denial of service attacks using selective pushback. In: Proceedings of the ninth IEEE international conference on telecommunications (ICT); 2002. p. 411–29.
Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput Surv 2007;39(1).
Peng C, Kim M, Zhang Z, Lei H. Vdn: virtual machine image distribution network for cloud data centers. In: INFOCOM; 2012. p. 181–9.
Polychronakis M, Anagnostakis KG, Markatos EP. An empirical study of real-world polymorphic code injection attacks. In: USENIX workshop on large-scale exploits and emergent threatsm; 2009.
Price PD. Toward an internet service provider (ISP) centric security approach [M.Sc. thesis]. Naval Postgraduate School; 2002.
Qazi ZA, Tu CC, Chiang L, Miao R, Sekar V, Yu M. SIMPLE-fying middlebox policy enforcement using SDN. In: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM; 2013. p. 27–38.
Radware ⟨http://www.radware.com/⟩; 2013 [accessed July 2015].
Rajagopalan S, Williams D, Jamjoom H, Warfield A. Split/merge: system support for elastic execution in virtual middleboxes. In: NSDI; 2013. p. 227–40.
Ranjan S, Swaminathan R, Uysal M, Knightly E. DDoS-resilient scheduling to counter application layer attacks under imperfect detection. In: Proceedings of 25th IEEE International Conference on Computer Communications; 2006. p. 1–13.
Ranjan S, Swaminathan R, Uysal M, Nucci A, Knightly E. DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. IEEE/ACM Trans Netw 2009;17(1):26–39.
Robinson M, Mirkovic J, Michel S, Schnaider M, Reiher P. DefCOM: defensive cooperative overlay mesh. In: DARPA information survivability conference and exposition; 2003. p. 101–2.
Sathyanarayana SM. Software defined network defense [M.Sc. thesis]. University of Pennsylvania; 2011.
Scepanovic S. Mitigating DDoS attacks with cluster-based filtering [M.Sc. thesis]. Aalto University; 2011.
Sekar V, Egi N, Ratnasamy S, Reiter MK, Shi G. Design and implementation of a consolidated middlebox architecture. In: NSDI; 2012. p. 323–36.
Seo D, Lee H, Perrig A. APFS: adaptive probabilistic filter scheduling against distributed denial-of-service attacks. Comput Secur 2013;39:366–85.
Shah-Hosseini H. The intelligent water drops algorithm: a nature-inspired swarm-based optimization algorithm. Int J Bio-Inspired Comput 2009;1(1):71–9.
Shameli-Sendi A, Dagenais M. ARITO: cyber-attack response system using accurate risk impact tolerance. Int J Inf Secur 2013, . http://dx.doi.org/10.1007/s10207-013-0222-9.
Shameli-Sendi A, Ezzati-Jivan N, Jabbarifar M, Dagenais M. Intrusion response systems: survey and taxonomy. Int J Comput Sci Netw Secur 2012;12(1):1–14.
Shi W, Xiang Y, Zhou W. Distributed defense against distributed denial-of-service attacks. In: Distributed and parallel computing; 2005. p. 357–62.
Shiaeles SN, Katos V, Karakos AS, Papadopoulos BK. Real time DDoS detection using fuzzy estimators. Comput Secur 2012;31(6):782–90.
Shin S, Yegneswaran V, Porras P, Gu G. AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks. In: Proceedings of the 2013 ACM SIGSAC conference on computer & communications security; 2013a. p. 413–24.
Shin S, Porras P, Yegneswaran V, Fong M, Gu G, Tyson M. FRESCO: Modular composable security services for software-defined networks. In: Proceedings of the 20th annual network and distributed system security symposium (NDSS); 2013b.
Shin S, Xu Z, Gu G. EFFORT: a new host-network cooperated framework for efficient and effective bot malware detection. Comput Netw 2013;57(13):2628–42.
Singh K, Kaur N, Nehra D. A comparative analysis of various deployment based ddos defense schemes. In: Quality, reliability, security and robustness in heterogeneous networks; 2013. p. 606–16.
Spyridopoulos T, Karanikas G, Tryfonas T, Oikonomou G. A game theoretic defense framework against DoS/DDoS cyber attacks. Comput Secur 2013;38:39–50.
Sterne D, Djahandari K, Wilson B, Babson B, Schnackenberg D, Holliday H, et al. Autonomic response to distributed denial of service attacks. In: Recent advances in intrusion detection; 2001. p. 134–49.
Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 2011;34(1):1–11.
Suh J, Choi H, Yoon W, You T, Kwon T, Choi Y. Implementation of a content-oriented networking architecture (CONA): a focus on ddos countermeasure. In: European NetFPGA developers workshop; 2010.
Tanase M. Closing the floodgates: DDoS mitigation techniques ⟨http://www.symantec.com/connect/articles/closing-floodgates-ddos-mitigation-techniques⟩; 2003 [accessed July 2015].
Verisign internet defense network ⟨http://www.verisigninternetdefensenetwork.com⟩; 2013 [accessed July 2015].
Vizvary M, Vykopal J. Future of DDoS attacks mitigation in software defined networks. In: Monitoring and securing virtualized networks and services; 2014. p. 123–7.
Walfish M, Vutukuru M, Balakrishnan H, Karger D, Shenker S. DDoS defense by offense. ACM Trans Comput Syst 2010;28(1).
Wang H, Zhang D, Shin KG. Detecting SYN flooding attacks. In: Proceedings of IEEE INFOCOM 2002; 2002. p. 1530–9.
Wang J. Tolerating denial-of-service attacks—a system approach [Ph.D. thesis]. University of California; 2005.

Wood AD, Stankovic JA. A taxonomy for denial-of-service attacks in wireless sensor networks. In: Handbook of sensor networks: compact wireless and wired sensing systems; 2004. p. 739–63.

Yao G, Bi J, Xiao P. Source address validation solution with OpenFlow/NOX architecture. In: The 19th IEEE international conference on network protocols (ICNP); 2011. p. 7–12.

Yau DK, Lui J, Liang F, Yam Y. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. IEEE/ACM Trans Netw 2005;13(1):29–42.

Yu J, Fang C, Lu L, Li Z. A lightweight mechanism to mitigate application layer DDoS attacks. In: Scalable Information Systems; 2009. p. 175–91.

Yu S, Guo S, Stojmenovic I. Can we beat legitimate cyber behavior mimicking attacks from botnets? In: Proceedings of the INFOCOM; 2012.

Yu S, Tian Y, Guo S, Wu D. Can we beat ddos attacks in clouds? IEEE Transactions on Parallel and Distributed Systems 2014;25(9):2245–54.

Zargar ST, Joshi J. A collaborative approach to facilitate intrusion detection and response against DDoS attacks. In: The sixth international conference on collaborative computing: networking, applications and worksharing (CollaborateCom); 2010. p. 1–8.

Zargar ST, Joshi J. DiCodefense: distributed collaborative defense against DDoS flooding attacks. In: IEEE symposium on security and privacy; 2013.

Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. IEEE Commun Surv Tutor 2013; 99:1–24.

Zhang C, Cai Z, Chen W, Luo X, Yin J. Flow level detection and filtering of low-rate DDoS. Comput Netw 2012;56(15):3417–31.

Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst 2012;28(3):583–92.