DOI: 10.21917/ijct.2016.0207

ECONOMIC DENIAL OF SUSTAINABILITY ATTACK ON CLOUD – A SURVEY

A. Somasundaram
Department of Computer Applications, Sree Saraswathi Thyagaraja College, India
E-mail: somasundaram.a@gmail.com

Abstract

Cloud computing is a promising technology aims to provide reliable, customized and quality of service computation environments for cloud users in terms of Software as a Service-SaaS , Plat- form as a Service-PaaS and Infrastructure as Service-IaaS, which is provided on the pay per use basis. Cloud computing enables services to be deployed and accessed globally on demand with little maintenance by providing QoS as per service level agreement (SLA) of customer. However, due to elasticity of resources, cloud systems are facing severe security problems. One of the most serious threats to cloud computing is EDoS (economic Distributed Denial of Service) aims to consume the cloud resource by attacker and impose financial burden to the legitimate user, where integrity, availability and confidentiality of the cloud services are never compromised but affects the accountability which leads to inaccurate billing. Since the billing models of cloud services may not be mature enough to properly account for an EDoS attack. These paper surveys, the different techniques that generate, detect and mitigate the EDoS Attack on Cloud.

Keywords:

EDoS, SaaS, PaaS, IaaS, SLA, Cloud Computing, Security

1. INTRODUCTION

Cloud computing is an integrations of computing technologies employed to facilitate on-demand services and applications to the consumers through the internet. Cloud offers several features like multi-tenancy (shared resources), massive scalability, elasticity, pay as you go, and self-provisioning of resources to serve the customers efficiently [2]. Organizations are migrating businesses into the cloud, so that they can rent the cloud services for use on a subscription or pay-per-use model instead of building their own infrastructures.

In spite of these huge potential advantages, security is the most fundamental issue for fastening the adoption of the cloud for many business and mission critical computations [3,4]. There are several types of attacks which harm the resources and services of cloud environment and lead to compromise their SAL. An SLA ensures that the consumer's expectation should be satisfied. SLA includes in terms of QoS, availability, reliability and performance, the billing methods, service cost and the penalty terms [22]. Based on SLA, cloud resources are provided to customer in restricted or unrestricted mode. The resource consumption (e.g. RAM, disk storage) and the computing power are billed to the client.

One of the crucial attacks which compromise the availability of the resource is Distributed Denial of Service (DDoS). Denial of service (DoS) attack is an effort by a single machine, namely, an attacker to make a target (server or network) unavailable to its customers, by absorbing all available bandwidth and disrupting access for legitimate customers and partners. DDoS attack consists of highly damageable attacks to collapse or degrade the quality of service in hardly unexpected manner [5].

Distributed Denial of Service (DDoS) attacks target web sites, hosted applications or network infrastructures by absorbing all available bandwidth and disrupting access for legitimate customers and partners.

The EDoS in cloud are due to the DDoS attack, where the service to the legitimate user is never restricted. But the service provider who is using cloud will incur a debilitating bill by using highly elastic (auto-Scaling) capacity to unwittingly serve a large amount of undesired traffic in order to maintain the QoS as per the SLA. This leads to Economic Denial of Sustainability (EDoS) [1].Therefore making it no longer viable for a company to affordability use or pay for their cloud based infrastructure. This kind of attack is also called as Fraudulent Resource Consumption (FRC) attack [10].

It was found in an experiment, by sending 1000 requests/second with 1000 Megabits/second data transfer on a web-service hosted on Amazon CloudFront for 30 days incurred an additional cost of $42,000 to the cloud user[25]. In a similar experiment, this incurred the additional cost to the customer, by an attacker just sending one web request (size of 320KB) per minute for one month, which accumulates total 13GB of data transfer [26].

In another experiment conduced, web server cluster running on extra-large instance at Amazon EC2 was targeted with an EDoS attack and shown that bills are rising on the basis of number of requests and deployment of additional resources[6].

2. EDOS ATTACK

EDoS attack supposes to be mitigated before it triggers the billing mechanism of the cloud service provider. Since the resources and services utilized by the customer are charged as per the SLA. If the DDoS attack is not properly addressed, then the attacker consumes the cloud resources and the cost is finally paid by the legitimate user. But the legitimate user doesn't have any idea that other person (attacker) is taking the services actually meant for him [6].

EDoS attack can be called as HTTP and XML based DDoS attack. EDDoS attack is generated at application layer by utilizing HTTP and XML based attack traffic. Coercive Parsing attack is one of the X- DoS (XML Based Denial of Service) attacks which use a continuous sequence of open tags so that the CPU usage on an Axis2 web server becomes exhausted. HTTP Flooder is type of HTTP-DoS attack (HTTP Based Denial of Service) that starts up 1500 threads so that it can send randomized HTTP requests to the victim web server to exhaust its communication channels [7]. In the above example, increased requests may look like normal activity since the EDoS attack traffic is just above the normal activity threshold and below the DDoS attack threshold. The Fig.1 shows the EDoS operations and its counter measures.

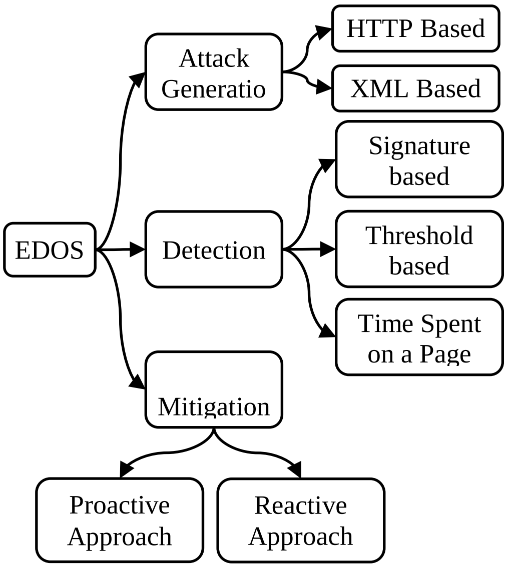

Fig.1. EDOS Operations

3. ATTACK GENERATION

The EDoS attack executing at the application layer by generating large number of fake requests to the Cloud Server to consumption of Cloud resource. The EDoS attack can be generated by using botnets or cloud originated DDoS attacks.

Index Page Based EDoS on Infrastructure Cloud-Index page of any website is available freely without any authentication credentials so employing bulky and concurrent HTTP-GET requests to index page of a website to generate resource consumption overhead on server [14]. These attacks consumes good amount of bandwidth and leads to heavy economic loss to the cloud user.

Web-Bugs - A Web Bug is embedded in a spam-email of legitimate user's browsers will generate an HTTP-GET Request to attack the Cloud Server [13]. These intelligent attacks are planned by constructing bots behaving like a real user based on the web service flow and behavior.

YO-YO ATTACK - Exploiting the auto-scaling mechanism to perform an efficient attack that impacts the cost of a service and the response time of standard users [15]. This is also called as Reduction of Quality (RoQ) attack. It cycles between two phases repeatedly: In the on-attack phase, the attacker sends a short burst of traffic that causes the auto-scaling mechanism to perform a scale up. In the off-attack phase, the attacker stops sending the excess traffic.

Coercive Parsing attack-It manipulates the WebService Request when a Simple Object Access Protocol (SOAP) is parsed to it so that it can transform the content to make it accessible to applications. Coercive Parsing attack uses a continuous sequence of open tags so that the CPU usage web server becomes exhausted [7]. The Table.1 summarizes the various EDoS generation techniques in Cloud environment.

4. ATTACK DETECTION

EDOS attack imposes exhaustive computation tasks to the server on the Cloud by exploiting its system vulnerability or flooding it with huge amount of useless packets. This causes serious damages to the services running on the Cloud server. EDoS detection aims to identify the suspicious traffic pattern which will consume the billable resources of the Cloud.

EDoS attacks are specific to Cloud service and are not easy to detect because cloud services doesn't have any mechanism to provide the correlation between requests and successful transactions [9].

Table.1. Summary of EDoS Generation Techniques

Sl. No	Taxonomy	Method	Type of Attack	Target Resource	Impact	Exploiting Resource	Countermeasure
1	Index Page Based EDoS	HTTP-GET flood	Flood Based	Index Page of any Website	Performance degradation and financial loss	auto-scaling mechanism	IPA Defender (Based on Human Browsing Behavior)
2	Web-Bugs	Spam – Email with Web-Bugs	Reflective	any Website/ Small and medium size business with limited web hosting budget	Financial loss	Metered Bandwidth	Not Addressed
3	Yo-Yo Attack	Cycle between on-attack phase and off-attack phase	Reflective	Increase the CPU utilization and scale up VMs	Reduction of Quality and cost of service	auto-scaling mechanism	Not Addressed
4	Coercive Parsing attack	X-DOS	Flood Based	Increase the CPU utilization	affect the availability	Oversized / incomplete SOAP messages	Cloud Protector

Attack detection systems are based on monitoring the traffic transmitted over the protected networks to provide quality services with minimum delay in response.

The attack can be detected based on various metrics such as pattern in web access behavior of a client, session duration and thresholds based filtering. Patterns are recognized from web access logs or request headers of each transaction. The specific pattern to identify in the log, is decided by attack traces and other past historic behaviors [24]. The Table.2 shows the comparison of EDoS attack detection techniques in Cloud.

Table.2. Summary of EDoS Detection Techniques

Methodology	Technique used	Comparison item	Pros	Cons
Flow Based	Signature based detection	Detection of varietal attack	High accuracy for previously known attacks	High false positive rate for unknown attacks
User behavior-based detection	Time Spent on a Page (TSP) based Detection	The learning process of all site	Simple method to differentiate legitimate traffic from attack.	Supports only SaaS kind of service
Statistical Approach	Threshold-based detection	Error rate	Fast attack detection	Time consuming process to generate priori knowledge

Signature-based detection: It detects traffic anomalies by looking for patterns that match signatures of known anomalies. It’s based on a firewall, which is working as a filter. It receives the request from the client, and redirected to a Puzzle-Server. The Puzzle-Server sends a puzzle to the client, who either sends a correct or false answer of the puzzle. If the answer is correct, the server will send a positive acknowledgment to the firewall which will add the client to its white list and will forward the request to the protected server to get services. Otherwise, the firewall will receive a negative acknowledgment and put the client in its black list [6].

Time Spent on a Page (TSP) based Detection: Time Spent on a Web Page (TSP) defined as time spent on viewing a web page. The TSP of the attack traffic differs from the mean TSP of a web page. This deviation of TSP from the mean is calculated taking the exponential distribution of the TSPs and the calculated value is used to detect the surreptitious behavior [11].

Threshold-based detection: The threshold is used to differentiate between normal traffic and abnormal traffic in the network. Dynamic threshold value is based on training or priori knowledge of the network activity, after that the threshold is selected [17].

5. ATTACK MITIGATION

EDoS mitigation schemes can be classified into two categories; reactive and proactive solutions. Reactive solutions systems are waiting the attack to occur then try to mitigate its impacts. It works in three steps First step, use traffic monitoring to identify attacks in progress. The second step triggered the sequence to locate the source of attack. In the third step, mitigation methods are implemented to eliminate or reduce the impact of the attack. The proactive solution is provided treating the source of packets before reaching to the secured server [23]. The filtering systems are considered as reactive solutions. However, Overlay-based techniques are considered as proactive solutions. There are many mechanisms available to mitigate EDoS attacks. Few of these methods are discussed in this section. The Table.3 shows the comparison between EDoS mitigation mechanisms.

Secure Overlay Services (SOS): SOS architecture consists of a set of nodes which are classified into four groups. The first group is the Secure Overlay Access Points (SOAP), while the second collection is the overlay nodes which connect SOAP nodes with the third group .i.e., Beacon nodes. The last group is the Secret Servlets. It reduces the possibility of harmful attacks by “performing intensive filtering near protected network edges”, and by “introducing randomness and anonymity into the architecture, making it difficult for an attacker to target nodes along the path to a specific SOS-protected destination” [27].

EDoS Shield: This mechanism has two main components, the cloud verifier node and virtual firewall. Firewall does the packet filtering based on the White list and Black list method. The service provider uses CAPTCHA (Graphic turning test) to identify that the request is coming from a legitimate user or from a malicious machine [18]. If request is coming from an attacker (machine) then request is add in black list and we block the request i.e. request cannot pass through virtual firewall. Otherwise request passes through virtual firewall and starts the service in cloud infrastructure. The limitation of this scheme is that the time delay, due to Turing test performed on every incoming request

Enhanced EDoS-Shield: This is used to mitigate the EDoS attacks originating from spoofed IP addresses [19]. When user registers into cloud for the first time, the request goes to Verifier node and TTL value is recorded related to source IP address. When user sends request, the Verifier node check the request against source IP address and corresponding TTL value rang. If both values match, then requester is added to white list and request pass through virtual firewall. Otherwise added in a black list and request is blocked at virtual firewall. This method fails to find the attacker with-in network vulnerability to IP spoofing.

sPoW: self-verifying Proof of Work (sPoW) is a On Demand Cloud based and application layer mitigation scheme. The main function of this method is to filter the attack traffic before it start over committing of resources. It transforms the network level traffic to distinguishable traffic that can be filtered using pattern matching. In second phase it sends crypto puzzles to client to resolve by brute force method. Here client solves a sPoW puzzle to discover a hidden channel to communicate with the serve [20]. This framework requires high computation power to solve crypto-puzzles for client, which can create overheads on the machine to brute force harder puzzles, which makes this method not suitable for mobile devices.

Table.3. Summary of EDoS Mitigation Techniques

Solution	Methodology	Approach	Pros	Cons
Secure Overlay Services (SOS)	combination of secure overlay tunneling, hashing and Filtering	Proactive	Reduce the probability of successful attacks	Priori client information required Requires new routing protocols.
EDoS Shield	Virtual firewall and authentication	Reactive	Protects against the direct source EDoS attacks	Delay due to tuning test performed on every incoming packet.
Enhanced EDoS-Shield	Identifies spoofed IP addresses	Reactive	Prevents infinite looping of packet in the network	Difficult to identify the source of attack Fails to find the attacker with-in network
Self-verifying Proof of Work (sPoW)	Packet Filtering	Reactive	Real time response Offers network-level and application-level protection	Requires high computation power to solve puzzles. Not viable to mobile devices
In-Cloud Scrubber Service	Puzzle generation and Verification	Proactive	Detects network-layer attacks	end-to-end latency
Digital signature based architecture	Public Key and private Key	Reactive	Highly Scalable	Delay in response
Vivin Sandar and Shenai Framework	firewall and Third party authentication	Reactive	The grouping of attack help to identify the attacks of similar pattern	Time delay at puzzle server and verifier node Legitimate user blacklisted if failed to answer the puzzle
Enhanced EDoS Mitigation system	Packet filtering by testing the first packet	Reactive	Provides load balancing Ensures the entry of legitimate users	Does not protect against the internals attacks.
Damask	Software defined network	Proactive	High accuracy rate	Communication Overhead. Computation Cost

In-Cloud Scrubber Service: Generates and verifies the Client puzzle (crypto puzzle) to authenticate the clients. The generated puzzle solved by the consumer by brute force method. Cloud-service is switched between normal and suspected modes, it depend on server and network bandwidth. During the normal mode, the incoming requests will be immediately directed to cloud-service and otherwise it will be directed to In-Cloud Scrubber Service for verification process during the suspected mode. The limitation of this technique is that Client-puzzles provide weak access guarantees to customer/users [21].

Digital signature based architecture: This framework used to differentiate the legitimate user from the attacker. The client request goes to cloud infrastructure and it is verified at verifying node using public key infrastructure (PKI). Request is send to certify authority (CA) to check that request is coming from legitimate user or an attacker. Certify authority tries to decrypts the request with his private key. If request is decrypted by CA private key, it proves that it’s coming from a legitimate user; otherwise it is originated from an attacker. If request is coming from legitimate user, it is passed through the firewall and is forwarded to cloud infrastructure for service while other requests are blocked [26].

Vivin Sandar and Shenai Framework: This framework is based on firewall. It receives the request from the client, and redirected to a Puzzle-Server. The Puzzle-Server sends a puzzle to the client, who either sends a correct or false answer of the puzzle. If the answer is correct, the server will send a positive acknowledgment to the firewall which will add the client to its white list and will forward the request to the protected server to get services. Otherwise, the firewall will receive a negative acknowledgment and put the client in its black list [6].

An Enhanced EDoS Mitigation System: This system tests the legitimacy of the request by testing the first packet from the source of requests during each session to distinguish the human user from the botnet. The test is done by the verifier node(s), which use the Graphical Turing Test (GTT) in verifying the packets. After that, the users' requests will be examined by the IPS device. If IPS detects malware in the contents of packets, the source IP address will be placed in the Malicious List. The last layer of the monitoring process tools will be done by the Reverse Proxy (RP) which performs several tasks including detecting the suspicious users who try to overwhelm the system by sending a huge amount of requests without drawing the attention of the previous monitoring layers. If there are suspicious users detected, the client puzzle server will send a crypto puzzle to them to delay their requests [28].

Damask: This is based on Software-Defined Networking. The DaMask architecture has three layers, network switches, network controller, and network applications. The main functions of the DaMask are DDoS detection and reaction. There are two separate modules in the DaMask, DaMask-D, a network attack detection system, and DaMask-M, an attack reaction module. It requires little effort from the cloud provider which means few changes are required from the current cloud computing service architecture [29].

6. CONCLUSIONS

Cloud computing, making the revolution in IT market, but the security and maintaining the service level agreement is the crucial challenge to the Cloud Service Provider. EDOS Attack is very specific to the cloud environment. For cloud computing to uphold its renown, the EDOS attack must be addressed properly. If EDOS in not mitigated properly, then it makes financial burden to the cloud users. This paper emphasized the various mechanisms available to EDOS attack generation, detection and mitigation techniques in the Cloud environment. More robust techniques are required to detect and mitigate the EDOS attack effectively.

REFERENCES

[1] M. Naresh Kumar, P. Sujatha, V. Kalva, R. Nagori, A. Katukojwala and M. Kumar, "Mitigating Economic Denial of Sustainability (edos) in Cloud Computing using In-Cloud Scrubber Service", *Proceedings of International Conference on Computational Intelligence and Communication Networks*, pp. 535-539, 2012.

[2] Tim Mather, Subra Kumaraswamy and Shahed Latif, "*Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*", O'Reilly, 2009

[3] Y. Chen, V. Paxson and R.H. Katz, "Whats New about Cloud Computing Security", Technical Report, EECS Department, University of California, 2010.

[4] John Viega, "Cloud Computing and the Common Man", *Computer*, Vol. 42, No. 8, pp. 106-108, 2009.

[5] Qi Chen, Wenmin Lin, Wanchun Dou and Shui Yu, "CBF: A Packet Filtering method for DDoS Attack Defense in Cloud Environment", *Proceedings of the 9th International Conference on Dependable, Autonomic and Secure Computing*, pp. 427-434, 2011.

[6] S. Vivin Sandar and Sudhir Shenai, "Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks", *International Journal of Computer Applications*, Vol. 41, No. 20, pp. 11-16, 2012.

[7] Ashley Chonka, Yang Xiang, Wanlei Zhou and Alessio Bonti, "Cloud Security to Protect Cloud Computing against HTTP-DoS and XML-DoS Attacks", *Journal of Network and Computer Applications*, Vol. 34, No. 4, pp. 1097-1107, 2011.

[8] S.V. Sandar and S. Shenai, "Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks", *International Journal of Computer Applications*, Vol. 41, No. 20, pp. 11-16, 2012.

[9] Rational Survivability, Available at: http://www.rationalsurvivability.com/blog/2009/01/a-couple-of-follow-ups-on-the-edos-economic-denial-of-sustainability-concept

[10] J. Idziorek, M. Tannian and D. Jacobson, "Detecting Fraudulent use of Cloud Resources", *Proceedings of 3rd ACM Workshop on Cloud Computing Security*, pp. 61-72, 2011.

[11] Anusha Koduru, Tulasi Ram Neelakantam and S. Mary Saira Bhanu, "Detection of Economic Denial of Sustainability Using Time Spent on a Web Page in Cloud", *Proceedings of IEEE International Conference on Cloud Computing in Emerging Markets*, pp. 1-6, 2013 .

[12] Joseph Idziorek and Mark Tannian, "Exploiting Cloud Utility Models for Profit and Ruin", *Proceedings of IEEE International Conference on Cloud Computing*, pp. 33-40, 2011.

[13] Armin Slopek and Natalija Vlajic, "Economic Denial of Sustainability (EDoS) Attack in the Cloud using Web-Bugs", *Proceedings of 17th International Symposium on Research in Attacks, Intrusions and Defenses*, 2014.

[14] Bhavna Saini and Gaurav Somani, "Index Page based EDoS Attacks in Infrastructure Cloud", *Proceedings of 2nd International Conference on Recent Trends in Computer Networks and Distributed Systems Security*, pp. 382-395, 2014.

[15] Mor Sides, Anat Bremler-Barr and Elisha Rosensweig, "Yo-Yo Attack-Vulnerability in Auto-Scaling Mechanism", *Proceedings of Conference on Special Interest Group on Data Communication*, pp. 103-104, 2015.

[16] Joseph Idziorek and Mark Tannian, "Exploiting Cloud Utility Models for Profit and Ruin", *Proceedings of the International Conference on Cloud Computing*, pp. 33-40, 2011.

[17] Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom and Tai-Myoung Chung, "Multi-Level Intrusion Detection System and Log Management in Cloud Computing", *Proceedings of the 13th International Conference Advanced Communication Technology*, pp. 552-555, 2011

[18] Mohammed H. Sqalli, Fahd Al-Haidari and Khaled Salah, "EDoS Shield-A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing", *Proceedings of 4th International Conference on Utility and Cloud Computing*, pp. 49-56, 2011.

[19] Fahd Al-Haidari, Mohammed H. Sqalli and Khaled Salah, "Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses", *Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1167-1174, 2012.

[20] Soon Hin Khor and Akihiro Nakao, "Spow On-Demand Cloud-based eDDoS Mitigation Mechanism", *Proceedings of 5th Workshop on Hot Topics in System Dependability*, pp. 1-6, 2009.

[21] M. Naresh Kumar, P. Sujatha, V. Kalva, R. Nagori, A.K. Katukojwala and M. Kumar, "Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing Using In-cloud Scrubber Service", *Proceedings of 4th International Conference on Computational Intelligence and Communication Networks*, pp. 535-539, 2012.

[22] L. Wu and R. Buyya, "Service Level Agreement (SLA) in Utility Computing Systems", Technical Report, pp. 1-27, 2010.

[23] Bernd Grobauer, Tobias Walloschek and Elmar Stocker, "Understanding Cloud Computing Vulnerabilities Security and Privacy", *IEEE Security and Privacy*, Vol. 9, No. 2, pp. 50-57, 2011.

[24] Jelena Mirkovic, Gregory Prier and Peter Reiher, "Attacking DDoS at the Source", *Proceedings of 10th IEEE International Conference on Network Protocols*, pp. 1-10, 2002.

[25] Amazon Cloud Front and S3 maximum cost, Available at: http://www.reviewmylife .co.uk/blog /2011/05/19/amazon-cloudfront-and-s3-maximum-cost/.

[26] Joseph Idziorek and Mark Tannian, "Exploiting Cloud Utility Models for Profit and Ruin", *Proceedings of IEEE International Conference on Cloud Computing*, pp. 33-40, 2011.

[27] Mohit Kumar and Nirmal Roberts, "A Technique to Reduce the Economic Denial of Sustainability (EDoS) Attack in Cloud", *Proceedings of 4th International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 571-574, 2013.

[28] Angelos D. Keromytis, Vishal Misra and Dan Rubenstein, "SOS: Secure Overlay Services", *Proceedings of International Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 61-72, 2002.

[29] Wael Alosaimi and Khalid Al-Begain, "An Enhanced Economical Denial of Sustainability Mitigation System for the Cloud", *Proceedings of 2nd International Conference on Next Generation Mobile Apps, Services and Technologies*, pp. 19-25, 2013.

[30] Bing Wang, Yao Zheng, Wenjing Lou and Y. Thomas Hou, "DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking", *Computer Networks*, Vol. 81, No. C, pp. 308-319, 2015.