A Survey on Discovery of Distributed Denial of Service Attacks in Cloud

Tayebe Shokatpour[1] and Reza Ravanmehr[2] *

**[1] Computer Engineering Department, Central Tehran Branch, Islamic Azad University
Tehran, Iran**

[2] Computer Engineering Department, Central Tehran Branch, Islamic Azad University

Tehran, Iran

Abstract

Cloud computing is a paradigm which involves delivering hosted services over the internet and is predicted as the next generation of information technology architecture whose high potentiality enhances efficiency and reduces the costs. Although cloud computing is still considered as a young field, it has to deal with challenges such as security, performance, accessibility and so forth. Cloud services can be vulnerable to Distributed Denial of Service (DDoS), which is one of the most common and damaging forms of attack on the cloud. Therefore, detecting and encountering security attacks on the cloud are of considerable importance. The present study aims to introduce DDoS and its classifications, and assess effective parameters in detection of these attacks. Finally, prevention methods have been classified and then, analyzed in the cloud.

Keywords: *Cloud Computing, Cloud Security Attacks, Flooding Attacks, Denial of Service (DoS), Distributed Denial of Service (DDoS).*

1. Introduction

Cloud computing is a computing model based on huge computer networks such as internet. According to NIST (National Institute of Standards and Technology) [1],Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It means that elastic, scalable and on-demand IT resources are delivered through internet which is a cloud hosting provider.

Security is regarded as the top nine challenge, as mentioned in [2]. Users of Cloud Computing worry about their businesses' information and critical IT resources which are vulnerable to be attacked. Nevertheless, concerns on performance and availability are below the security. Users of Cloud Computing systems may face many threats to their individual data. For example, internal threats, external threats, service disruption, multi-tenancy, portability, etc.

SOAP (wrapping attack), malware-injection, flooding attack and data stealing can be named among serious attacks on the security of cloud computing. Flooding attack and data stealing have been also observed in cluster and grid computing. Flooding attack is a form of Denial of Service (DoS) attack in which an attacker sends a succession of requests to a target's system to bring the network or system down by flooding it with large amounts of traffic. It occurs when a service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.

Using many computers or internet connections, Distributed Denial of Service (DDoS) attack involves flooding the target resource in order to prevent it from responding to legitimate traffic and make it unavailable to users. In such attacks, the perpetrators will send large numbers of packets with the fake source address to appear to be the address of the victim; therefore, the network's bandwidth or CPU is quickly used up, preventing legitimate packets from getting through to their destination.

In Section 2, a classification of DDoS is presented. Its effective parameters in DDoS detection and type of datasets are respectively introduced in Sections 3 and 4. Also prevention methods have been classified in Section 5. Finally, an analysis has been made between Section 5's methods.

2. Classification of DDOS Attacks

Denial of Service (DoS) is a dangerous and relatively new internet attack which aims to make a machine or network resource unavailable to its intended users and disable its

* *Corresponding author*

doi:10.20943/01201503.101108

computing system. DDoS is harder to deal with because it comes at a different rate from distributed sources. This section presents a classification of DDoS attacks, see Fig. 1.

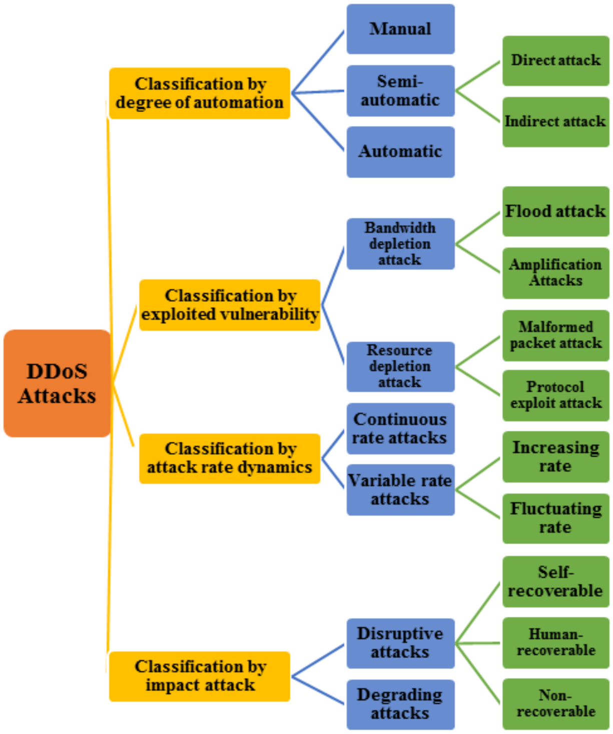

Fig. 1 Classification of DDoS attacks.

2.1 Classification by degree of automation

Based on the degree of automation, attacks can fall into three types: manual, semi-automatic and automatic DDoS attacks [3]. 1) Manual attacks: The attacker scanned remote machines for vulnerabilities, broke into them and installed the attack code, and then commanded the onset of the attack [3]. 2) Semi-automatic attacks: In these attacks, the attacker deploys automated scripts for scanning and compromise of those machines and installation of the attack code. They then use handler machines to specify the attack type and the victim's address and to command the onset of the attack to agents, who send packets to the victim [3]. 3) Automatic attacks: Automatic DDoS attacks additionally automate the attack phase, thus avoiding the need for communication between attacker and agent machines. The time of the onset of the attack, attack type, duration and victim's address is preprogrammed in the attack code. It is obvious that such deployment mechanisms offer minimal exposure to the attacker, since he is only involved in issuing a single command – the start of the attack script [3].

2.2 Classification by exploited vulnerability

Distributed Denial of Service attacks exploit different strategies to deny the service of the victim to its clients. Based on the vulnerability that is targeted during an attack, we can differentiate between bandwidth depletion and resource depletion attacks. 1) Bandwidth depletion attacks can be characterized as flood attacks and amplification attacks. a) Flood attacks: In a flood attack, zombies send a large volume of traffic to a victim system, so as to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth, thereby preventing access by an authorized user. b) Amplification attacks: In amplification attack, the attacker or the zombies send messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system [4]. 2) Resource depletion attacks can fall into malformed packet attacks and protocol exploit attacks. a) Malformed packet attacks: A malformed packet attack is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash it [4]. b) Protocol exploit attacks: They exploit a specific feature or implementation bug of some protocol installed at the victim in order to consume excess amounts of its resources [3].

2.3 Classification by attack rate dynamics

Depending on the attack rate dynamics DDoS attacks can be divided in continuous rate and variable rate attacks. Continuous rate attacks comprise attacks that after the onset of the attack are executed with full force and without a break or decrement of force. This sudden packet flood disrupts the victim's services quickly, and thus leads to attack detection. Variable rate attacks are more cautious in their engagement, and they vary the attack rate to avoid detection and response. Based on the rate change mechanism we differentiate between attacks with increasing rate and fluctuating rate [3, 5].

2.4 Classification by impact of attack

Based on the impact of a DDoS attack, we can divide DDoS attacks to disruptive and degrading attacks [3, 5]. Disruptive attacks lead to the complete denial of the victim's service to its clients. These attacks fall into three self-recoverable, human-recoverable and non-recoverable attacks. The goal of degrading attacks is to consume some portion of a victim's resources. This has as an effect the delay of the detection of the attack and at the same time a great damage on the victim.

doi:10.20943/01201503.101108

3. Effective parameters in DDoS detection

Based on the above mentioned issues, defense methods can be compared according the following parameters in Table 1.

Table 1: Effective parameters in DDoS attack detection

Effective parameters in attack detection		
Time-dependent parameters	Real-time or non-real time	
	Throughput [7, 8].	
	Request response time [7, 8].	
	Delay in detection /response	One-way delay [9]
		Request-response delay [9,10]
		Delay variation [9,10]
Quantitative parameters	Defense strength [6, 7].	Accuracy
		Sensitivity or true positive rate
		Specificity or true negative rate
		Precision or positive predictive value
		False positive rate
		False negative rate
	Request dropping probability [8, 9].	
	Throughput	
	Delay in detection/response	
Qualitative parameters	Defense strength	
	Scalability	
	Unknown attacks detection	
	Availability	
	System performance degradation	
	Passive, reactive or proactive mechanisms	
	Holistic defense [11].	
	Implementation complexity [11].	
	Usability [11].	
	Deployment location [11].	

1) *Real-time (R) or non-real time (N):* A defense mechanism with real-time detection enjoys a good performance in high speed traffics. Offline methods in high speed traffics face problems due to the generated overhead by delay in processing. It causes failure or lower speed in detection.

2) *Scalability:* A scalable defense mechanism can effectively handle its attack detection and response duties even if both the number of attackers and the amount of attack traffic increases.

3) *Unknown attacks detection:* New attacks detection is challenging for defense systems. The observed methods are not capable of detecting the unknown attacks.

4) *Defense strength:* The strength of a defense mechanism can be measured by various metrics depending on how well it can prevent, detect, and stop the attacks. These metrics could be defined based on the decision or prediction that each defense mechanism makes [6, 7].

a) *Accuracy:* Ratio of the correct outcomes of the defense mechanism (true positives and true negatives) over the total outcomes of the defense mechanism.

$$((TP+TN))/ ((P+N)). \qquad (1)$$

b) *Sensitivity or true positive rate:* Ratio of true positives over total desired positive outcomes.

$$TP/ ((FN+TP)). \qquad (2)$$

c) *Specificity or true negative rate:* Ratio of true negatives over total desired negative outcomes.

$$TN/ ((TN+FP)). \qquad (3)$$

d) *Precision or positive predictive value (PPV):* Ratio of true positives over the total positive outcomes of the defense mechanism.

$$TP/ ((FP+TP)). \qquad (4)$$

e) *Reliability or False positive rate:* Ratio of false positive outcomes of the defense mechanism over total positive outcomes of the defense mechanism.

$$FP/ ((FP+TN)). \qquad (5)$$

f) *False negative rate:* Ratio of false negative outcomes of the defense mechanism over total negative outcomes of the defense mechanism.

$$FN/ ((TP+FN)). \qquad (6)$$

5) *Request response time:* It refers to the average response time of each successful HTTP. The response time will increase with the increase of attack rate since those bad HTTP requests also consume the processing capacity of (DDoS defense system) nodes. When the bad requests are filtered at network-layer, the average response time will decrease dramatically [7, 8].

6) *Availability:* The signs of DDoS attack can be abnormal consumption of server resources such as memory and bandwidth that can be caused lack of access.

7) *Request dropping probability:* Low level of request dropping probability is more appropriate [8, 9].

8) *Throughput:* It stands for the client's request per second or the average end-to-end throughput of a legitimate client who sends one request per second to download a file of 100 Kbytes. The client of directly accessed base server will suffer from high request dropping probability and large response time. High levels of throughput ought to be more appropriate [7, 8].

9) *Delay in detection/response*

a) *One-way delay [9]*

doi:10.20943/01201503.101108

b) Request-response delay [9,10]

c) Delay variation (Jitter) [9,10]

10) System performance degradation: Defense mechanism causes system performance degradation such as memory storage and lack of CPU cycles.

11) Passive, reactive or proactive: Mechanisms which prevent attacks from happening or take actions only after the DDoS attacks are launched.

12) Holistic defense: The defense mechanism which considers all the required tasks in order to stop the DDoS attacks, i.e., both detection and response [11].

13) Implementation complexity: One of the important metrics to compare defense mechanisms is their implementation complexity. The best defense mechanisms in this classification are those that are easy and feasible to implement [11].

14) Usability: The interface that mechanisms provide to their users should be as user-friendly as possible [11].

15) Deployment location: Deployment location is another metric to compare various defense mechanisms. Each location has its own benefits and disadvantages which makes one mechanism better than the other [11].

4. Type of Datasets

All methods must be tested and analyzed, so the best way is to use dataset. Table 2 depicts type of datasets that to be using for testing.

Table 2: Type of Datasets

Type of Datasets	Description	Dataset and tools
Benchmark Datasets	Only a few benchmark intrusion datasets are publicly available but they are not for DDoS attacks.	KDDcup99 intrusion data set [24], DARPA Intrusion Detection Data Sets [25]
Simulated Datasets	Simulate the environment using available tools.	ns2 [26], Qualnet[27], OMNeT++ [28], CloudSim [29]
Private Datasets	The best approach for testing any intrusion detection system or DDoS attack detection method is to create a real network test bed with a large number of host and network components.	

5. DDoS defense mechanisms

DDoS flooding attacks waste a lot of resources (e.g., processing time, space, etc.) on the paths that lead to the targeted machine; hence, the ultimate goal of any DDoS defense mechanism is to detect them as soon as possible and stop them as near as possible to their sources. Fig. 2 depicts defense mechanisms divided into two groups. We classify the defense mechanisms against two types of DDoS flooding attacks. The first criterion for classification is the location where the defense mechanism is implemented (i.e., Deployment location). We classify the defense mechanisms against network/transport-level DDoS flooding attacks into four categories: source-based, destination-based, network-based, and hybrid (a.k.a. distributed) and the defense mechanisms against application-level DDoS flooding attacks into two categories: destination-based, and hybrid (a.k.a. distributed) based on their deployment location [11]. The second criterion for classification is the point of time when the DDoS defense mechanisms should act in response to a possible DDoS flooding attack. Based on this criterion we classify DDoS flooding attacks into three categories (i.e., three points of defense against the flooding attack): before the attack (attack prevention), during the attack (attack detection), and after the attack (attack source identification and response) [12].

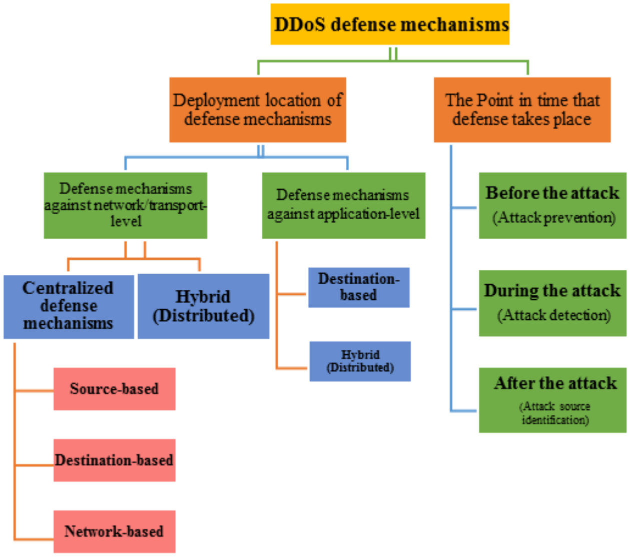
DDoS defense mechanisms
Deployment location of defense mechanisms
The Point in time that defense takes place
Defense mechanisms against network/transport-level
Defense mechanisms against application-level
Before the attack (Attack prevention)
Centralized defense mechanisms
Hybrid (Distributed)
Destination-based
During the attack (Attack detection)
Hybrid (Distributed)
After the attack (Attack source identification)
Source-based
Destination-based
Network-based

Fig. 2 A taxonomy of defense mechanisms against DDoS flooding attacks.

5.1 Source-based mechanisms

Source-based mechanisms are deployed near the sources of the attack to prevent network customers from generating DDoS flooding attacks. These mechanisms can take place

doi:10.20943/01201503.101108

either at the edge routers of the source's local network or at the access routers of an Autonomous System (AS) that connects to the sources' edge routers. Various source-based mechanisms have been designed to defend against DDoS flooding attacks at the source; some of the major ones are Ingress/Egress filtering at the sources' edge routers [13].

5.2 Destination-based mechanisms

In the destination-based defense mechanisms, detection and response is mostly done at the destination of the attack (i.e., victim). These mechanisms can closely observe the victim, model its behavior and detect any anomalies. Some of the major destination-based DDoS defense mechanisms are as follows: IP Traceback mechanisms [14] and packet filtering mechanisms [15].

5.3 Network-based mechanisms

These mechanisms are deployed inside networks and mainly on the routers of the ASs [16]. Detecting attack traffic and creating a proper response to stop it at intermediate networks is an ideal goal of this category of defense mechanisms.

5.4 Hybrid (Distributed) mechanisms

In most of the previously discussed categories of DDoS flooding defense mechanisms (source-based, destination-based, and network-based), there is no strong cooperation among the deployment points. Furthermore, detection and response is mostly done centrally either by each of the deployment points (e.g., source-based mechanisms) or by some responsible points within the group of deployment points (e.g., network-based mechanisms). Hence, we call these categories of DDoS defense mechanisms centralized.

As opposed to centralized defense mechanisms, hybrid defense mechanisms are deployed at (or their components are distributed over) multiple locations such as source, destination or intermediate networks and there is usually cooperation among the deployment points. For instance, detection can be done at the victim side and the response can be initiated and distributed to other nodes by the victim. For example, TRACK combines IP traceback, packet marking, and packet filtering [17]. TRACK is composed of two components: router port marking module and packet filtering module [17].

5.5 Before the attack (attack prevention)

The best point in time to stop a DDoS attack is at its launching stage. In other words, attack prevention is the best DDoS defense solution. The prevention mechanisms can be deployed at the attack sources, intermediate networks, destinations or a combination of them. Most of the prevention mechanisms aim to fix security vulnerabilities. There are some general prevention mechanisms that should be employed almost everywhere (e.g., servers, hosts, and intermediate networks). Employing local filters to block attack flows before their bombardment is another important category of the prevention mechanisms against DDoS attacks [15].

5.6 During the attack (attack detection)

The next step in defending against DDoS attacks is attack detection, which happens during the attack. The detection mechanisms can also be deployed at sources, intermediate networks, and destinations. There are various mechanisms to detect DDoS attacks such as spectral analysis, statically-based methods, machine learning, and intrusion detection system as mentioned in [17, 18, 19, and 20].

5.7 After the attack (attack source identification and response)

After a DDoS attack is detected, the defense system should identify the source of the attack and block the attack traffic. Today, most of the DDoS response mechanisms cannot completely prevent or stop DDoS attacks. There are two main categories for most of the after the attack mechanisms: attack source identification [14] and initiating a proper response [15].

6. Survey and Analysis of DDoS defense mechanisms

Defense mechanisms against DDoS flooding attacks have been qualitatively compared in this section, see Table 3. Then, some defense methods have been evaluated in the cloud, see Table 4.

Table 3: Qualitative comparison of defense mechanisms against DDoS flooding attacks

Effective parameters in attack detection	***Centralized***			***Distributed***
	Source-base	Destination-base	Network-base	Hybrid (distributed)
Defense strength (Accuracy)	Low	High	Low	Medium
Scalability	Low	Low	Medium	Medium-high
System performance	Medium	Good	Medium	Poor-medium
Implementation complexity	Low	Low	Medium	Medium-high
Holistic defense	No	No	No	Yes

An ideal comprehensive DDoS defense mechanism must have specific features to combat DDoS flooding attacks both in real-time and as close as possible to the attack sources. More nodes in the Internet should be involved in preventing, detecting, and responding to DDoS flooding attacks (i.e., Hybrid (Distributed) defense). As we discussed earlier, the detection accuracy is high at the victim side but it is not robust; victims cannot tolerate high volume of DDoS traffic. Stopping the attacks at the source could be the best response option but it is very difficult. Furthermore, the collateral damage is high at intermediate networks because there is not enough memory to profile the traffic. Therefore, centralized mechanisms in which, all the defense components (i.e., prevention, detection, and response) are deployed at the same place, are not practical against DDoS flooding attacks.

Cloud trace back model (CTB) can reduce vulnerabilities by being located before the Web Server, in order to place a Cloud Trace Back Mark (CTM) tag within the CTB header. As a result, all service requests are first sent to the CTB for marking, thereby effectively removing the service provider's address and preventing a direct attack. If an attack is discovered or was successful at bringing down the web server, the victim will be able to recover and reconstruct the CTM tag and as a result reveal the identity of the source [21].

CBF (Confidence-Based Filtering) method [22] is based on mining the correlation patterns, which refer to some simultaneously appeared characteristics in the legitimate packets. These patterns are mainly in network and transport layer. But in this method no fixed number of single attributes is defined that has to be selected. Apart from this problem a database is also maintained at the server side which uses the 3-dimensional array storing strategy due to which the processing speed of the server is slow down. In enhanced CBF packet filtering method, CBF is modified so that utilization of storage at the victim side is reduced and the processing speed of the server will be increased. It reduces the overhead of the server by calculating the confidence value of the packet at the packet header itself and then storing the value in the optional field of the IPV4 packet header.

By using a decision tree classification mechanism, Intrusion Detection System (IDS) is adopted as CLASSIE [23]. CLASSIE's rule set has been built up over time to identify the known HDoS (HTTP DDoS) and X-DoS (XML DDoS) messages. Upon detection of HX-DoS message, CLASSIE drops the packet which matches the rule set. After examined by the CLASSIE, then the packets are subjected to marking.

Table 4: Evaluation of some defense mechanisms against DDoS flooding attacks in the cloud

Mechanism	**Advantages**	**Disadvantages**	**Effective detection parameters**
Cooperative IDSs	-Increasing confidence in proportion to an ordinary IDS	-Consuming more computing time in proportion to an ordinary IDS	System performance: low Scalability: medium
Cloud trace back model (CTB)	-Overcoming direct DDoS attacks -Identifying the attacker in a successful attack	-The model's performance is dependent upon the efficiency of neural net and data set accuracy -Collecting data set is difficult for the neural net	Defense strength: medium
Confidence-based filtering	-Low storage capacity for the profile in normal mode -High speed of filtering attack packets -Reducing the overhead of the server	-The accuracy of this model is less than other models.	System performance: high Defense strength: low
CLASSIE	-Detecting HX-DoS attacks -Reducing false positive rate of the attacks -Reducing the overhead of the server	-Detecting the attacks at application-level	System performance: high
Filtering tree	-Filtering the attacks at various levels -Using the concept of entropy	-Detecting the attacks at application-level	Implementation complexity: medium-high
Information theory based metrics	-Easy deployment and decrease of negative rate	-Probability of information loss due to entropy compression	Implementation complexity: low

7. Conclusions

Organizations are accelerating their paces in developing cloud computing systems and take more advantages from this facility; however there are always security issues for the information being exchanged. Each kind of disruption in offering services causes disconnection and ruins the organization’s reputation. The gaol of this study is to present a classification of DDoS and its effective parameters in attack detection. Section 5 dealt with the defense mechanisms against DDoS attacks. Finally, the mechanisms were analyzed.

Therefore, centralized mechanisms which are deployed at a central location cannot be efficacious to overcome DDoS attacks. Security mechanisms are required to coordinate different distributed components and prevent suspect customers from generating flooding attacks.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST special publication 800-145, National Institute of Standards and Technology, October 2009.

[2] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security and privacy in cloud computing: A Survey", IEEE Computer Society, Sixth International Conference on Semantics Knowledge and Grids, 2010.

[3] J. Mirkovic, J. Martin and P. Reiher, "A taxonomy of DDoS attacks and DDoS defense mechanisms," Computer Science Department, University of California, 2002.

[4] M. Chhabra1, B. Gupta1 and A. Almomani, "A novel solution to handle DDOS attack in MANET," SciRes Journal of Information Security, vol. 4, no. 3, 2013, pp. 165-179.

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Computer Networks The International Journal of Computer and Telecommunications Networking, Elsevier, vol 44, Issue 5, 2004, pp 643–666.

[6] C. Modi, D. Patel, B. Borisanya, A. Patel and M. Rajarajan, "A novel framework for intrusion detection in cloud," in Proc. 15th Int. Conf. Security of Information and Networks, ACM, 2012, pp. 67-74.

[7] S.Pu, "Choosing parameters for detecting DDoS attack," in Proc. Int. Conf. Wavelet Active Media Technology and Information Processing (ICWAMTIP), IEEE, 2012, pp. 239-242.

[8] P. Du and A. Nakao, "DDoS defense as a network service," in Proc. Network Operations and Management Symposium (NOMS). IEEE, 2010, pp. 894–897.

[9] J. Mirkovic, S. Fahmy, P. Reiher , R. Thomas, A. Hussain, S. Schwab, and C. Ko, "Measuring impact of DoS attacks," in Proc. the DETER Community Workshop on Cyber Security Experimentation, 2006.

[10] P. Jayashree, K.S. Easwarakumar , B. Gokul and S. Harishankar, "Providing QoS as a means for defending DoS attacks in active networks," in Proc. 16th Int. Conf. on Advanced Computing and Communications ADCOM, IEEE, 2008, pp. 406-409.

[11] S. T. Zargar, J. Joshi and D. Tipper, "A survey of defense mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," Communications Surveys & Tutorials, IEEE, vol.15, no.4, 2013, pp.2046-2069.

[12] V.T.L. Ling, "Adaptive Response System for Distributed Denial of Service attacks," Ph.D. Thesis, Imperial College London, August 2008.

[13] P. Ferguson, and D. Senie, "Network ingress filtering: defeating Denial of Service attacks that employ IP source address spoofing," Internet RFC 2827, 2000.

[14] A. John, and T. Sivakumar, "DDoS: Survey of traceback methods," International Journal of Recent Trends in Engineering ACEEE (Association of Computer Electronics & Electrical Engineers), vol. 1, no. 2, May 2009.

[15] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using Hop-Count filtering," IEEE/ACM Trans. On Networking, vol. 15, no. 1, 2007, pp.40-53.

[16] A. T. Mizrak, S. Savage, and K. Marzullo, "Detecting compromised routers via packet forwarding behavior," IEEE Network, 2008, pp.34-39.

[17] R. Saad, F. Nait-Abdesselam and A. Serhrouchni, "A collaborative peer-to-peer architecture to defend against DDoS attacks," 33rd IEEE Conference on Local Computer Networks LCN, 2008, pp. 427-434.

[18] S. Roshke, F. Cheng and C. Meinel, "Intrusion detection in the cloud," In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 729-734.

[19] H.A. Kholidy, F. Baiardi, "CIDS: A framework for intrusion detection in cloud systems," In Ninth International Conference on Information Technology-New Generation, 2012, pp. 379-385.

[20] A.M. Lonea, D.E. Popescu and H. Tianfield, "Detecting DDoS attacks in cloud computing environment," Journal of Computers Communications & Control., vol. 8, no. 1, 2013, pp. 70-78.

[21] B. Joshi, A. Vijayan and B. Joshi, "Securing cloud computing environment against DDoS attacks," International Conference In Computer Communication and Informatics (ICCCI), IEEE, 2012, pp. 1-5.

[22] P. Negi, A. Mishra and B.B. Gupta, "Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment," International Journal of Computer Science Issues (IJCSI) 10, no. 2, 2013.

[23] E.Anitha and S.Malliga, "A packet marking approach to protect cloud environment against DDoS attacks," International Conference Information Communication and Embedded Systems (ICICES), IEEE, 2013, pp. 367-370.

[24] "KDDcup99 intrusion data set," http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, January 30, 2014.

[25] "DARPA Intrusion Detection Data Sets," http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/, February 2, 2015.

[26] "ns2 ," http://www.isi.edu/nsnam/ns/, January 12, 2014.

[27] "Qualnet," https://www.ee.iitb.ac.in/~prakshep/IBMA_lit/manual/manual244.html, February 2, 2014.

doi:10.20943/01201503.101108

[28] "OMNeT++," http://www.omnetpp.org, January 30, 2014.

[29] "Cloudsim," http://www.cloudbus.org/cloudsim, January 30, 2014.

Tayebe Shokatpour received her B.Sc. degree in computer engineering in 2011, respectively from Alzahra University, Iran. She has studied M.Sc. degrees in computer engineering in Islamic Azad University, Central Tehran Branch from 2013. Her research interests include cloud computing, cloud security attacks, distributed denial of service (DDoS).

Reza Ravanmehr graduated in computer engineering from Shahid Beheshti University in Iran. After that he gained the M.Sc. and Ph.D. both from Islamic Azad University, Science and Research branch in computer engineering. His main research interests are distributed/parallel systems, Large Scale Data Management systems and Context
Awareness/Pervasive Computing. He is the faculty member of computer engineering department in Islamic Azad University, Central Tehran Branch from 2001.

doi:10.20943/01201503.101108