Simulation-Based Study of Distributed Denial of Service Attacks Counteract in the Cloud Services

WAEL ALOSAIMI, MAZIN ALSHAMRANI AND KHALID AL-BEGAIN
Faculty of Computing, Engineering and Science
University of South Wales
Pontypridd, Wales, CF37 1DL
UNITED KINGDOM
{wael.alosaimi, mazin.alshamrani, k.begain}@southwales.ac.uk

Abstract: - Network availability is threatened by the traditional Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The risk is much increased with the emergence of the new computing paradigm of cloud computing. In this era, DDoS attacks can threaten the cloud sustainability by hitting its pricing model exploiting the cloud scalability feature. Therefore, a new phenomenon is emerged as a result of launching DDoS attacks against the cloud customers. It is called Economic Denial of Sustainability (EDoS). It is no more than an economic version of DDoS attack sharing its mechanism but different in the final aim. In order to defeat DDoS and EDoS attacks, the filtering firewalls can play main role in this regard. This paper is an extended version of a previous work that invented by the authors which introduced a new technique to mitigate the impacts of such attacks depending on the firewall features in managing a verification process to maintain the targeted system. The proposed framework is known as Enhanced DDoS- Mitigation System (Enhanced DDoS-MS). The firewalls characteristics are evaluated using OPNET simulation tool. The results showed that the firewall is effective in mitigating the DDoS impacts by limiting the response time, throughput, server load, and the traffic sent and received under attack. The paper also suggests using an active test bed for evaluating the proposed framework in a real manner.

Key-words: - cloud computing, Firewall, Distributed Denial of Service attacks, DDoS, Economic Denial of Sustainability, EDoS.

1 Introduction

Cloud computing has main concerns that can affect its attractiveness to the new customers and threaten the survival of its current customers. These concerns are mainly security related concerns which are physical, policy-related, legal, and technical security risks. Actually, the availability is a chief factor which needs to be maintained to ensure the cloud sustainability. Its importance lies in providing the cloud services in all times with no shortage affecting the services accessibility. This feature can be harmed by attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and Economic Denial of Sustainability (EDoS). DoS and DDoS attacks are common attacks that affect the traditional networks and the cloud networks. However, these attacks in the cloud implementation can affect the victims, which are the cloud providers and customers, economically by hitting the customers' bills exploiting the cloud computing scalability. This phenomenon harms the cloud clients immediately and the cloud providers in the long run.

This paper enhances the previous work of the authors [1] by measuring more parameters to evaluate the effectiveness of the firewall in mitigating the DDoS attacks. It starts with studying the characteristics of these attacks in terms of the nature, the launching methods, and a selective set of the existing solutions. The solution of such attack must be a proactive technique in order to protect the targeted system. In this study, an evaluation of the Enhanced DDoS-Mitigation System (Enhanced DDoS-MS), which is developed as an attempt to encounter the DDoS attacks proactively, is presented focusing on the chief function that the firewall can perform to achieve the protection objectives. The firewall is working as a filter for the received packets by the targeted network according to predetermined rules which are designated by the network managers to alleviate the consequences of DDoS and EDoS attacks. The evaluation is performed using the OPNET simulation tool.

The paper is organised as the following: an overview of cloud computing will be presented in the first section. After that, Denial of Service attack will be defined, Distributed Denial of Service attacks will be classified into two main types, and the Economic Denial of sustainability concept will be explained. The proposed framework will be described after that and its evaluation will be presented in terms of the simulation setup and the achieved results.

2 Cloud Computing

Cloud computing is a new technological model which involves providing its users with applications and services over the Internet in an on-demand base. These services are owned by cloud service providers that have distributed massive data centers [2]. Scalability, elasticity, flexibility, on-demand, metered services, and the large pool of resources are valuable features of cloud services and applications [3]. The cloud consumers can decrease their infrastructure and expenditure costs, limiting the technical overheads, and boosting their storage capacity [4]. Cloud services are provided as either infrastructure as a Service (IaaS), or software as a Service (SaaS), or platform as a Service (PaaS). Their deployment models can be classified into private, public, and hybrid cloud based on the type of customers that can access them [5]. Despite the valuable services that the cloud offers to its users, there are some risks that may threaten the cloud users and cloud providers. These threats are classified by [6] into policy and organisational risks such as compliance risk [7], physical security issues [8][9][10][7], technical risks such as Distributed Denial of Service (DDoS) [11][12], and legal issues such as data breach [7][13][14] and data deletion [6][15]. From the list of the cloud security threats, the DDoS attack is a persistent risk that did not mitigated appropriately. Moreover, it is becoming more harmful by exploiting its pricing model (pay-as-you-use) to affect the cloud customers and providers. In the next section, the three versions of DoS attacks will be clarified.

3 Denial of Service Attacks

In this paper, the Denial of Service attacks will be divided into three types taken in the consideration their nature and effects in the cloud computing environment. This includes:

3.1 Denial of Service (DoS)

The Denial of Service (DoS) attack affects the availability of network resources or services by preventing genuine users from accessing the network assets. The principal of this attack is explained by [16] who stated that computing power of the web page that is hosted by a cloud server is not limited. However, they determined three types of threats can flood this service. The first type is consuming the system resources. The second type is wasting the communication link by repeating download a large file from the server, while the third type is employing the SQL injections and password guessing attacks [16].

The flooding attacks can be launched from botnet, viruses or open DoS tools in order to overwhelm a web page or the hosting server or even the whole network [17]. The malicious users launch such attacks by sending a huge amount of bogus requests to the servers in order to consume their processing power and flood the network bandwidth. In such case, the legitimate users will be unable to access the network services although they are authenticated [18].

3.2 Distributed Denial of Service (DDoS)

The DDoS attack is a DoS attack that is generated by many distributed sources at the same time [11]. The attackers use worms and viruses in order to infect the devices that will be used in the attack without trigger their owners intention. The adversary aims to build a network of these compromised machines to be under his control so he can manage each one of them to infect other devices in order to augment the number of attack sources. These devices are called bots and their network is called botnet. The attacker can use this botnet to launch several types of attacks including DDoS attacks. Currently, tools such as TFN can be used to launch DDoS attacks [19].

There are many solutions have been proposed to encounter the DDoS attacks including:

- Overlay-based mitigation techniques that employ distributed firewalls and hide the protected system's identity
- Push-back methods that use routers close to the sources for filtering purposes
- Trace-back techniques that mark the malicious packet and trace its source

- Filtering methods that depend on attack patterns or a threshold value

However, the current countermeasures are either applying methods increase the legitimate users' response time or neglecting the sources' initial verification [19].

According to [20], the main DDoS attacks are SYN flooding attack, Smurf attack, ICMP flooding attack, and Ping of Death. Attacks can be generated to affect networks on different layers such as network, transport, or application layers. [21] classified the DDoS flooding attacks based on the attack protocol level into two main categories:

1. Network/transport-Layer DDoS flooding attacks: These are the attacks that are generated usually using ICMP, UDP, and TCP protocol packets. This kind of attacks can be classified into the following four sub-categories [22][23]:
   1.1. Bandwidth Flooding Attacks: Adversaries affect the connectivity of the legitimate client by overwhelming the target system bandwidth. Examples of this kind of attacks are UDP flood and ICMP flood [24].
   1.2. Protocol Exploitation Flooding Attacks: TCP SYN flood, TCP SYN-ACK flood, and RST/FIN flood are examples of this type of attacks where adversaries can implement bugs on some protocols of the target system or exploit particular features of these protocols [24].
   1.3. Reflection-Based Flooding Attacks: The attacker in this type sends bogus requests such as ICMP echo requests to the reflectors. As a result, the reflectors reply to the victim server and overwhelm its resources [23, 22].
   1.4. Amplification-Based Flooding Attacks: An example of such attacks is Smurf attack when the adversary sends requests with spoofed IP addresses in a reflection manner to a big number of reflectors exploiting the IP packet broadcast feature. This process is called amplification. Actually, the botnets are used in the reflection and the amplification techniques [23, 22].
2. Application-Layer DDoS flooding attacks: These attacks are more dangerous than the lower-layers flooding attacks as they consume less bandwidth and mimic the legitimate traffic so they are more difficult to be detected. They focused on overwhelming the target system's resources such as its CPU and/or memory. The applications that can be affected by these attacks include HTTP, DNS, and Session Initiation Protocol (SIP). The Application-layer attacks can be classified into the following categories:
   2.1. Reflection/Amplification-BasedFlooding Attacks: The used techniques in the application layer are the same of their counterparts in the network/transport layers. However, DNS protocol can be exploited to launch reflection as well as amplification attacks. In this case, the adversaries create small DNS queries with spoofed IP addresses that can launch a huge volume of traffic that is forwarded to the victim server directly to overwhelm it. Another example of this kind of attacks is the VoIP flooding. It involves sending spoofed VoIP packets through SIP by a large number of attackers. The targeted VoIP server needs to differentiate the genuine VoIP connections from the bogus ones. This process exhausts a large amount of resources. Moreover, VoIP flooding can flood a network with packets that arrive with dynamic or static source IP addresses. Hence, the VoIP flooding attack mimics the traffic coming from huge VoIP servers if the source IP addresses are static and as a result it will be very complicated to be detected [21][22][23].
   2.2. HTTP Flooding Attacks: Three types of attacks can be considered under this category:
      2.2.1. Session Flooding Attacks: An obvious example of such attacks is the HTTP GET/POST flooding attack. In this attack, the victim server's resources are overwhelmed

by attackers who launch a huge volume of valid HTTP requests.

2.2.2. Slow Request Attacks: The attacker in this type creates sessions that have high workload requests. An example of this kind of attacks is Slowloris attack which employs a limited number of computers to shut down the victim server by sending partial HTTP requests that are raised rapidly, updated slowly, opened continuously. The attack does not reach to the end before rendering the victim server inaccessible because all available sockets are engaged in responding to the requests [21].

2.2.3. Slow Reading Attacks: These attacks use a mechanism which is reading the response slowly rather than sending the requests slowly. The attacker exploits the feature of the TCP protocol that preserves open connections even if there is no information exchange. So, the adversary renders a huge number of server connections open and as a result floods the server [21].

3.3 Economic DDoS

The DDoS attack in the cloud computing environment can affect its victims economically. Therefore, the term Economic Denial of Sustainability (EDoS) is presented by [26]. The EDoS attack can be defined as a flooding attack that exploits the cloud elasticity feature to harm its metered-services which adopted by the cloud server [27]. EDoS mechanism is the same of DDoS attack but with different objective. While DDoS aims to overwhelm the network resources in order to shut down the server, EDoS works on overwhelming the customers' bills forcing them to withdraw from the cloud services reaching to harm the cloud industry in the long term. The huge amount of bogus requests will be delivered to the cloud to get its services based on the cloud scalability. However, the problem will be in the increased charges in cloud cost [28]. As a result, the customers will find the costs of cloud services are much higher than their counterparts in on-premise base. Therefore, they may withdraw from the cloud causing a huge loss in the providers' side. This may render the cloud industry itself profitless as it depends on the small and medium enterprises more than individuals [29][30].

Based on what is clarified above, the solution of such threats should be a technical technique that is implemented on the customer's side to protect it from DDOS attacks and protect the cloud provider from EDoS attacks in a proactive manner. Next section will present some of the current methods that are proposed to encounter DDoS and EDoS attacks.

4 Existing Mitigation Method

There are many methods proposed for tackling DDoS attacks such as CLAD, SOS, WebSOS, and Fosel. The Secure Overlay Services (SOS) is proposed by [31]. It hides the location of the protected server and uses overlay techniques to render the received packets pass through distributed nodes before accessing the targeted server. However, it prevents the legitimate users from accessing the targeted servers [32] and it can fail to encounter the attacks that are generated from spoofed IP addresses or from any internal node.

WebSOS is another solution that uses the same architecture of SOS beside using Graphic Turing test (CAPTCHA) to distinguish the man-kind users from botnets in order to strength the verification process [32]. However, it still increases the end-to-end latency and it has the same overlay networks drawback that is determined by [33] which lies in assuming that the list of users are known in advance. Therefore, it cannot be effective in the current internet settings.

[34] have proposed a proactive method that is called Filtering by Helping an Overlay Security Layer (Fosel). It employs specific filters (Fosel filters) that allow only the packets which are approved by green nodes and reject the others in order to protect the targeted system. In this way, it prevents the attacks that are generated by spoofing IP addresses. However, Fosel did not verify the received packets. This renders the whole architecture exposed to several attacks that threaten the target.

Cloud-Based Attack Defense System (CLAD) is another solution that protects the web server from flooding attacks by offering a network security service that works on a large cloud infrastructure that forms a super computer. Hence, the cloud infrastructure can embraces and overcomes any flooding attack in the network level against the CLAD nodes that work as web proxies [35]. This technique is evaluated by [30] who stated that the limitation of CLAD lies in increasing the end-to-end latency because all received packets must access the overlay system in order to reach to the target server. Moreover, it cannot be valid on large businesses or public networks [28, 33].

From the economic effects perspective, there are a number of techniques have been developed to encounter the EDoS attacks such as EDoS-Shield framework [28], Enhanced EDoS-Shield framework [36], Sandar and Shenai framework [37], and In-Cloud eDDoS Mitigation Web Service (Scrubber Service) technique [30]. However, these solutions are either increasing the end-to-end latency by verifying all received packets or inspecting only the first packet from any source without further tests leading to weak protection of the system. This status motivated the author to design a new framework that can fill this gap. The proposed framework will be presented in the following section.

5 The Enhanced DDoS-MS Framework

The above evaluation shows that the existing solutions still have limitations with regard to encounter DDoS and EDoS attacks. Maintaining the cloud features such as scalability and elasticity besides providing the required security with limiting the end-to-end latency must be the main aim for any suggested solution to solve such problem. Therefore, a new framework is proposed to fill this gap by including the strong aspects of the existing solutions and strengthen the weak ones. It is a proactive technique that is implemented in the customers' side to protect them from DDoS attacks and proactively protect them and their cloud providers from EDoS attacks. The framework is called Enhanced DDoS-Mitigation System (Enhanced DDoS-MS).

It consists of a firewall, a Verifier Node (VN), a client puzzle server, an Intrusion Prevention System (IPS) device, and a Reverse Proxy (RP) in front of the protected servers as shown in Fig.1.

The firewall is the main part of this framework. In general, the firewall is a network component that is used as a packet filter placed at the edge of a network that is connected to the internet [38][39].It controls the packets access process by intercepting every packet that is transferred between a specific network and the internet, testing the packet headers fields, and deciding to accept the packet or discard it based on two factors [39]:

1. The packet headers fields values.
2. A specific security policy that is prepared by the firewall designers to define filtering rules.

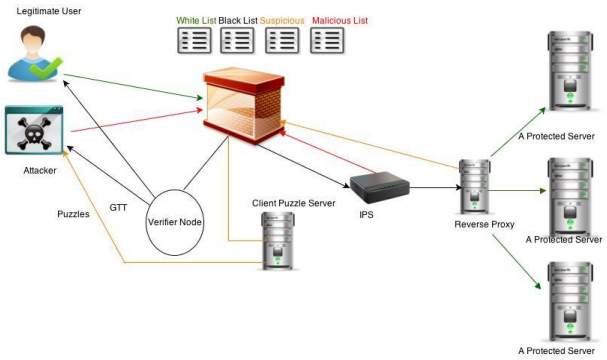

Fig.1 Enhanced DDoS-MS Architecture

Based on these rules, the firewall takes actions on the received and sent packets. A rule minds a set of network fields such as the source and destination IP addresses, the source and destination ports, the protocol type, and the determined action. The decision of accepting or denying packets by the firewall is a result of matching or not matching the packet header data with the rule network field [40]. In this framework, the firewall controls the whole protection process and the logical flow of the received packets. It receives the packets that come from any source and takes a decision of either allowing them to pass through or dropping them. The decision is based on the results of the verification test that is conducted by the VN and the monitoring process that are carried out by the remaining parts of the framework. The VN verifies the source of packets by using Graphic Turing test (CAPTCHA) that can detect the bots. The human user can easily pass the test while it is impossible for the zombies to do such. The failed users are considered as black list users. The IPS inspects the packets' payload in order to detect any malicious components using Deep Packet Inspection (DPI)

technology. The sources of malicious packets are considered as malicious users. The Reverse Proxy (RP) server is used to perform three tasks. These are hiding the location of the target servers, controlling the load balance between the target servers and monitoring the traffic rate to discover any possible DDoS attacks that are launched against the protected servers. The detection can be performed by assigning a predestined threshold value for the number of requests generating from any user in a specific time [41]. The sources of such attempts to overwhelm the server are considered as suspicious users.

The client puzzle server is used to rate limit the suspicious users who are detected by the RP. To achieve this, it uses crypto puzzles to be sent to this set of users in order to consume resources and time in their side. The firewall has four lists for the sources of packets depending on the result of the verification and monitoring processes. These lists are white, black, suspicious, and malicious lists. The Enhanced DDOS-MS idea is to verify the first packet of any user by the VN which uses CAPTCHA in testing the packets sources. Then, the IPS and the RP will monitor the remaining packets.

If a user passed the CAPTCHA test, then his IP address will be placed into the white list with the packet header TTL value. So, any packet comes from this user will be passed through the firewall to the protected server while its TTL value is not changed. The change in the TTL value leads to delete the IP address from the white list. On the other hand, if a user failed to pass the CAPTCHA test, then his IP address will be registered in the black list with TTL value and timestamp. Moreover, the current packet will be dropped and any new packet from the same user will be dropped unless it arrives with different TTL value or out of its previous timestamp. In such case, the IP address will be deleted from the black list.

The malicious packet will be detected by the IPS and its source IP address will be placed into the malicious list. As a result, any new packet from the same source will be dropped. Lastly, the RP will detect any attempt to exhaust the protected server. Thus, the attempt's source will be placed into the suspicious list so the new packets from the same source will be forwarded to the client puzzle server for further verification and delay. From the above mechanism, it is obvious that the legitimate user will avoid CAPTCHA tests after passing the verification process of his first packet. Therefore, he will be able to get his required services even if the server is under attack with minimum latency. This ability will not be affected unless the user sends malicious packets or clean packets but with different TTL values or tries to overwhelm the protected server. It is assumed that the packets that are arrived to the firewall have static source IP addresses and they are not fragmented, thus their TTL values will not be changed according to the different routes the fragmented packets can use to reach to the destination.

6 Simulation Setup

OPNET simulation tool provides the required related system components to setup and workout with different scenarios for this research study based on simulation models that support providing reliable outcomes for this study. OPNET is classified as Discrete Event Simulation (DES) tool that offers precise and realistic implementations for different applications. Furthermore, OPNET can evaluate the performance of different supported frameworks with the existence of large number of nodes in very reliable implementations. Therefore, it been chosen to conduct the simulation efforts in this study evaluation.

In Fig.2, the system design is shown where the Server is accessible by users from the internal network and connected with an IP Cloud for other users through the Cloud and with different applications. The Attacker is influencing the users' devices that connected to switch 1 (S1) where all the devices are infected. The Attacks on these devices will flood the Server with the traffic requests for the HTTP applications and initiate large number of applications on the Server. The Legitimate HTTP clients are connected with switch 2 (S2) and all connected users in this zone are not affected by the Attacker actions. Furthermore, this design considered the Firewall on its design to protect the Server from the DDoS attacks using a specified protection policy for HTTP applications that will applied on the protected scenarios on the simulated models. The access from the IP Clouds to the Server has limited affect over the Server performance and as it provides a background traffic for normal network access.

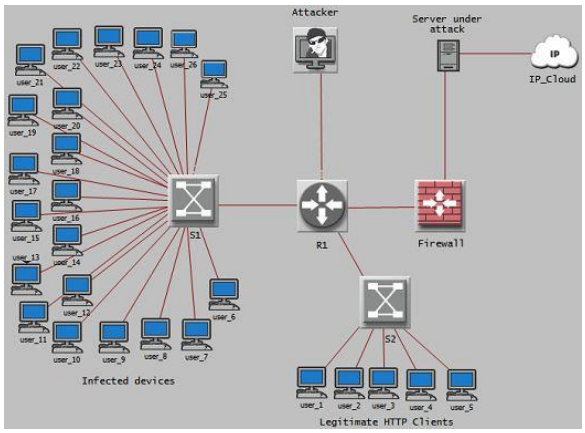

Fig.2 System design and implementation for a server under attack with the configured network system in OPNET

The implementation of this evaluation study were on OPNET Modeler v17.5 and considered four scenarios based on the introduced design at Fig.2 with regard to the identified simulation parameters given in Table 1. The first scenario considered the basic implementation for the network systems represented in Fig.2 without an active Firewall configuration where no assign for scheduled attacks in the system. This scenario examines the best case implementation of the assigned network system without DDoS issues in the Server. The second scenario considered the network system with the existence of the Firewall and without active attacks in the network system. This scenario examines the network efficiency with the existence of the Firewall component to check the network system overhead that may added to the system with its effect on the network performance. The third scenario considered a network system with the existence of the Firewall under active attacks where no security policies had assigned on the Firewall. This scenario examines the efficiency issues that could result with the existence of the Firewall without the implementation of the network protection policy on the Firewall which represents the worst case as the network performance is affected with serious level of DDoS attacks. The fourth scenario considered the implementations of the network system with an active policy system on the Firewall that preventing the infected traffic generated by the infected users which represents the protected scenario from the DDoS attacks of the implemented system. The results of these implemented scenarios will be compared and studied in terms of the performance and protection efficiency throughout this research study.

System Setup			
No. of Simulations	4	**Simulation Seed Number**	128
Simulation Duration:		30 Minutes = 1800 Seconds	
No. of Infected Devices:	21	**No. of Legitimate Users:**	5
Main Implemented Applications		web browsing (HTTP)	

Table 1 Simulation Parameters in OPNET

7 Results Evaluation

The evaluation study for the implemented scenarios considers different performance measurements for HTTP applications that identified in the network system which implemented in Fig.2. In this paper, we focused on the performance parameters on the Server side that assigned for HTTP applications in terms of traffic volume which generated with the assigned users, and the application response time over the simulation time line.

7.1 Number of Requests received by the Server for HTTP applications

For the implemented HTTP applications for web browsing, the users are trying to access the Server during the simulation time where the attacker is affecting the users based on the identified scenarios. Fig.3 shows the average volume of request traffic received by the Server from the users in the network system for HTTP applications in bytes per second. All the scenarios considered about 75 seconds at the beginning of the simulation for the system setup time for the users connection within the network system. The representations of the best effort scenarios has shown an ideal traffic volume for average HTTP requests (150 to 350 bytes/seconds) that received by the Server where no assigned attacks been considered over the implemented system.

On the other hand, the largest volume for the average HTTP requests has 300 to 550 bytes/second as shown in the scenario with active attacks without an active policy on the Firewall for the increased volume of HTTP requests. However, with the implementation of Firewall policy, the volume of HTTP requests received by the Server has reduced to a level between 250 to 380 bytes/second which is close to the optimum level of the received traffic.

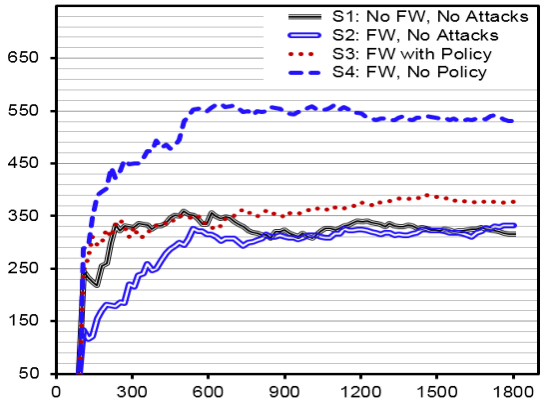

Fig.3 Average number of traffic requests received by the Server from users for HTTP applications in bytes/second

7.2 Response time for HTTP applications

The average response time for HTTP applications that initiated between the system users and HTTP Server reflects the performance level of the implemented DDoS prevention system as shown in Fig.4. The shortest average response time is between 80 to 90 ms with the scenario that has no assigned attacks and no Firewall where this value is increased and reached to average time between 100 and 128 ms with the second scenario with the Firewall representation. The average response time reached between 120 to 140 ms with the third scenario that represents firewall existence with no policy under attack. However, with the implementation of the Firewall policy, the average response time for HTTP applications has reduced to a level from 110 to 125 ms. The reduction in the average response time has enhanced the performance level of HTTP applications in the implemented system as a result of applying the Firewall prevention policy over the flooded traffic.

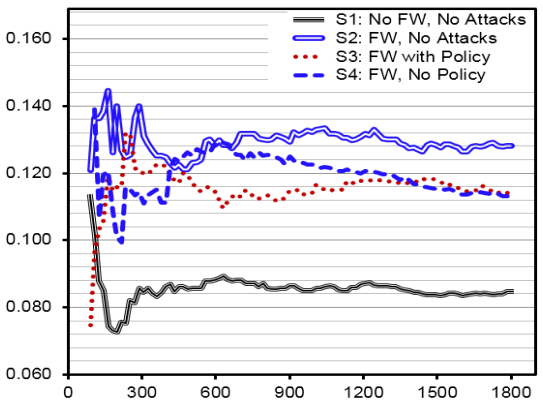

Fig.4 Average response time for HTTP applications initiatedbetween users and HTTP Server in millisecond/second

7.3 Server Performance

Another parameter that affects the performance level of the implemented DDoS prevention system is the evaluation of the Server performance with the loaded tasks which have been executed per second. The Server is operating in the best effort conditions where no DDoS attacks are implemented where the average load level on the Server is between 5 to 18 tasks/sec. On the other hand, with the scenario that has implemented attacks without any configured policy on the Firewall, the average load level is between 13 to 33 tasks/sec. Furthermore, the evaluation shows that when applying the policy constrains on the Firewall, the average load level on the Server has enhanced to be between 7 to 27 tasks/sec as shown in Fig.5.

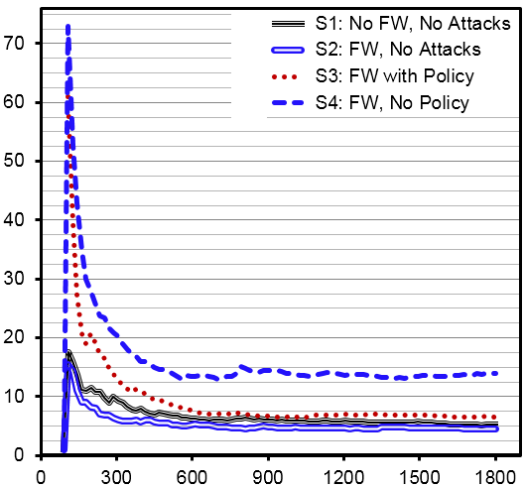

Fig.5 Average load on the Server for HTTP applications in tasks/second

7.4 Server Traffic Sent

Fig.6 shows that the average of HTTP packets that sent from the Server through the Firewall with a policy is very close to the optimal scenarios that have no attacks. This average is between 40 and 52 Kilo Bytes per Second (KB/Sec). On the other hand, implementing the prevention system without an active policy in the Firewall permits more packets to access the Firewall and leave the network. The average in this case has increased dramatically to reach up to approximately 80 KB/Sec and settle between this maximum value and 70 KB/Sec during the rest of the simulation period. This reflects the performance level of the implemented prevention system without the policy that leads to increase the required work from the Server and the Firewall under attacks. This result is exactly what the

adversaries intend to perform reaching to deny the access for the legitimate users. However, implementing the policy decreased the amount of traffic that can be pass through the Firewall in order to protect the system from the Denial of Service attacks to be between 35 and 53 Kilo Bytes per Second (KB/Sec).

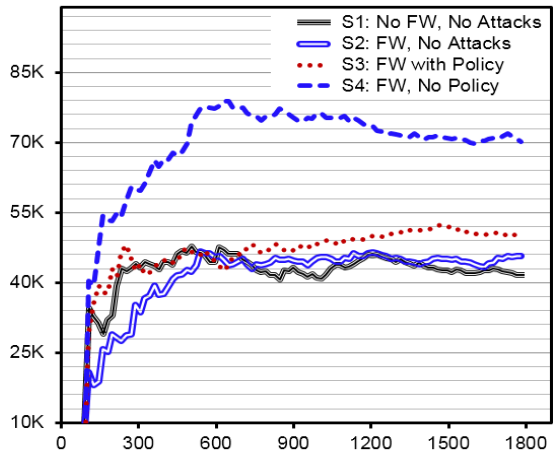

Fig.6 Average HTTP packets sent from server in Kilo Bytes per Second (KB/Sec)

7.5 The average throughput for HTTP packets that are transferred between the Firewall and the Server

The average throughput for HTTP packets that are transferred between the Firewall and the Server represents the role that the Firewall can play in protecting the Server from being exhausted and therefore unable to respond to the legitimate users' requests. Fig.7 proves that using a specific policy with the Firewall minimises the load in the network links to a level which is very close to the normal situations (with no attacks). The evaluation in the figure is performed in the link between the Firewall and the Server. To illustrate the Figure, the attacks against the Server increase the consumption of the network bandwidth dramatically by exchanging data with a rate between 500 and 550 Kilo bits per Second (Kb/Sec) when a standard Firewall is implemented. On the other hand, the average rate of such exchange has decreased to be in a level between 300 and 325 Kb/Sec. Thus, it is obvious that developing a proper policy and implementing it into the Firewall can enhance the effectiveness of the prevention scheme against the DoS attacks.

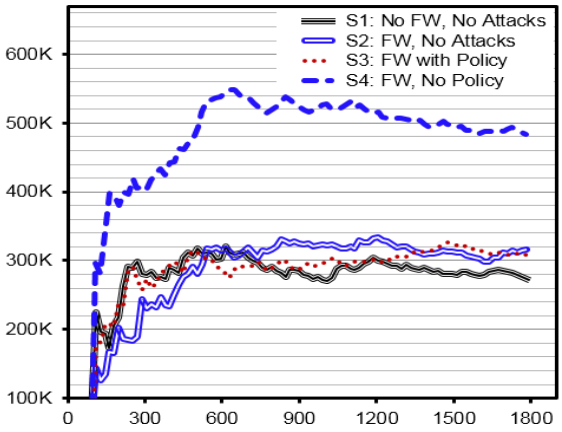

Fig.7 Average throughput for HTTP packets in Kilo bits per Second (Kb/Sec)

7.6 Infected Devices Throughput

The average throughput for HTTP packets that are initiated from the infected devices reflects the performance level of the implemented prevention system with and without policy under attacks. Fig.8 shows that applying the policy in countering these malicious requests causes a little difference from using a standard Firewall. The highest average throughput increases with a sharp escalation until reaching to 445 packets per second (pps) without policy and 418 pps with the Firewall policy after 7 minutes of the setup as a result of connectivity initiation between different components for HTTP applications. After that, the system becomes stable and the average throughput decreased to a level between 220 and 205 pps respectively. This reduction proves the effectiveness of the Firewall in general and the proposed Firewall with policy in particular against the malicious requests that try to access the protected server.

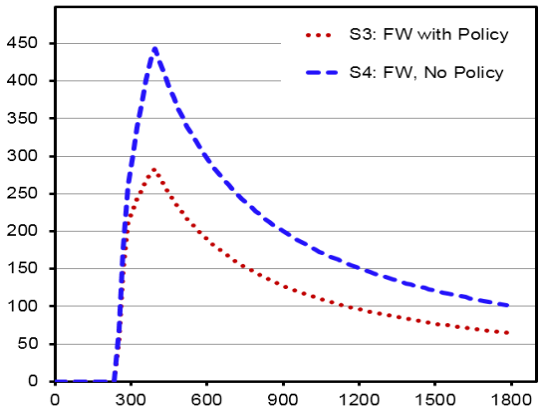

Fig.8 Average throughput for HTTP packets initiated from the infected devices in packets per second (pps)

7.7 Legitimate Clients Throughput

The average throughput for HTTP packets that initiated from the legitimate clients' machines reflects the performance level of the implemented prevention system with and without Firewall policy. Fig.9 shows that applying the policy enhances the prevention system's performance by decreasing the bandwidth consumption even in the case of benign users. While applying the policy leads the throughput reach to 20 pps, the absence of such policy fails to decrease the throughput from its maximum value which is about 28 pps. From Fig.8 and Fig.9, it is obvious that the attack has a great impact on the network bandwidth consumption. The throughput for legitimate clients is between 20 and 28 packets per second with and without policy respectively. On the other hand, it counted by hundreds of packets per second and reaching to be 10 times with Firewall policy (220 pps) and 20 times without the policy (445 pps).

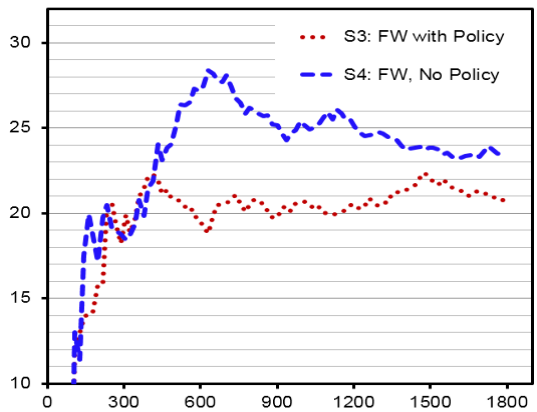

Fig.9 Average throughput for HTTP packets initiated from legitimste clirnts in packets per second (pps)

8 Future Works

Further work in this project involves evaluation of the Enhanced DDoS-MS as well as improvement the framework and includes a number of situations that were not covered in the current version, such as:

1. Involving dynamic IP addresses of the resources of packets and performing the required modification on the design of the proposed framework to embrace this change.
2. Including the case of packet fragmentation. In this case, the TTL value will be affected. Therefore, the framework needs to deal with the ID field in order to trace the various fragmented packets of the sent request.
3. Selecting additional packets for further random verification in order to enhance the framework robustness.
4. Embracing the new trend, Bring Your Own Device (BYOD) into the scope of the proposed method to investigate its impacts in amplifying the DDoS attacks from the inner customer's network.

Moreover, the framework will be evaluated in an active test bed to prove its correctness and effectiveness.

9 Conclusion

DDoS attacks are still threatening all types of networks from the traditional networks to the cloud networks. Therefore, counteracting them and mitigating their impacts need an intensive evaluation of the existing countermeasures and working on improve them. Therefore, the authors introduced the Enhanced DDoS-MS as a new solution for solving such issues. The proposed method relies mainly on the firewall characteristics which are assessed in a simulated environment. This evaluation shows that the firewall is effective in mitigating the DDoS attacks' impacts. Applying more complex scenarios against the Enhanced DDoS-MS solution is a future task besides validating it in a genuine test bed environment.

References:

[1] W. Alosaimi, M. Alshamrani, and K. Al-Begain, "Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 60–65.

[2] J. Rittinghouse, J, and Ransome, "Cloud Computing: Implementation, Management, and Security," USA: Taylor and Francis Group, LLC, 2010.

[3] D. Raths, "Cloud Computing: Public-Sector Opportunities Emerge.," 2008. [Online]. Available: http://www.govtech.com/gt/articles/387269. [Accessed: 25-Jan-2012].

[4] M. A. Vouk, "Cloud Computing – Issues , Research and Implementations," *J. Comput. Inf. Technol.*, vol. 16, no. 4, pp. 235–246, 2008.

[5] H. Steve, "Cloud Computing Made Clear," *Bus. Week*, vol. 59, no. 1, 2008.

[6] ENISA, "Cloud Computing Risk Assessment," *European Network and Information Security Agency*, 2009. [Online]. Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

[7] A. Sangroya, S. Kumar, J. Dhok, and V. Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments," *ICISTM*, pp. 255–265, 2010.

[8] D. Sitaram and G. Manjunath, "Cloud Security Requirements and Best Practices," in *MOVING TO THE CLOUD: Developing Apps in the New World of Cloud Computing*, USA: Elsevier, 2012, p. 309.

[9] C. Fortinet, "Network and physical security in the cloud," in *Asia Cloud Forum*, 2011.

[10] T. Aslan, "Cloud physical security considerations," *IBM Cloud*, 2012. [Online]. Available: http://thoughtsoncloud.com/index.php/2012/02/cloud-physical-security-considerations/. [Accessed: 15-Feb-2013].

[11] B. Raju, P. Swarna, and M. Rao, "Privacy and Security issues of Cloud Computing," *Int. J.*, vol. 1, no. 2, pp. 128–136, 2011.

[12] A. Khan, N. Fisal, and S. Hussain, "Man-in-the-Middle Attack and Possible Solutions on Wimax 802 . 16j," in *International Conference on Recent and Emerging Advance Technologies in Engineering (iCREATE 2009)*, 2009, no. iCREATE.

[13] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," in *Grid Computing Environments Workshop*, 2008, pp. 1–10.

[14] S. Kuyoro, F. Ibikunle, and O. Awodele, "Cloud Computing Security Issues and Challenges," *Int. J. Comput. Networks*, vol. 3, no. 5, pp. 247–252, 2011.

[15] E. Slack, "How do you know that 'Delete' means Delete in Cloud Storage?," 2011. [Online]. Available: http://www.storage-switzerland.com/Articles/Entries/2011/8/16_How_do_you_know_that_Delete_means_Delete_in_Cloud_Storage.html. [Accessed: 14-Apr-2012].

[16] C. Lin, C. Lee, and C. Chen, "A Detection Scheme for Flooding Attack on Application Layer Based on Semantic Concept " 2010.

[17] T. Yatagai, T. Isohara, and I. Sasase, "Detection of HTTP-GET Flood Attack Based on Analysis of Page Access Behavior," in *Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 2007, pp. 232–235.

[18] W. Liu, "Research on DoS Attack and Detection Programming," in *2009 Third International Symposium on Intelligent Information Technology Application*, 2009, pp. 207–210.

[19] Y. Choi, J. Oh, J. Jang, and J. Ryou, "Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention," in *Proceedings of the Second IEEE International Conference on Information Technology Convergence and Services (ITCS)*, 2010, pp. 1–6.

[20] S. S. Chopade, K. U. Pandey, and D. S. Bhade, "Securing Cloud Servers Against Flooding Based DDOS Attacks," in *2013 International Conference on Communication Systems and Network Technologies*, 2013, pp. 524–528.

[21] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[22] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–54, 2004.

[23] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Networks*, vol. 44, no. 5, pp. 643–666, 2004.

[24] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surv.*, vol. 39, no.

1, pp. 1–42, 2007.

[25] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Comput. Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004.

[26] C. Hoff, "Cloud Computing Security: From DDoS (Distributed Denial Of Service) to EDoS (Economic Denial of Sustainability)," *Rational Survivability*, 2008. [Online]. Available: http://rationalsecurity.typepad.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-service-to-edos-economic-denial-of-sustaina.html. [Accessed: 27-Sep-2012].

[27] S. Khor and A. Nakao, "DaaS: DDoS Mitigation-as-a-Service," in *2011 IEEE/IPSJ International Symposium on Applications and the Internet*, 2011, no. 2, pp. 160–171.

[28] M. Sqalli, F. Al-Haidari, and K. Salah, "EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing," in *2011 Fourth IEEE International Conference on Utility and Cloud Computing*, 2011, pp. 49–56.

[29] C. Hoff, "A Couple Of Follow-Ups On The EDoS (Economic Denial Of Sustainability) Concept," *Rational Survivability*, 2009. [Online]. Available: http://www.rationalsurvivability.com/blog/2009/01/a-couple-of-follow-ups-on-the-edos-economic-denial-of-sustainability-concept/. [Accessed: 26-Jan-2013].

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

[31] A. Keromytis, V. Misra, and D. Rubenstein, "SOS : Secure Overlay Services," in *SIGCOMM*, 2002, pp. 61–72.

[32] W. Morein, A. Stavrou, D. Cook, A. Keromytis, V. Misra, and D. Rubenstein, "Using graphic turing tests to counter automated DDoS attacks against web servers," in *Proceedings of the 10th ACM conference on Computer and communication security - CCS '03*, 2003, pp. 8–19.

[33] K. Lakshminarayanan, D. Adkins, A. Perrig, and I. Stoica, "Taming IP Packet Flooding Attacks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 1, pp. 45–50, 2004.

[34] H. Beitollahi and G. Deconinck, "FOSeL: Filtering by Helping an Overlay Security Layer to Mitigate DoS Attacks," *2008 Seventh IEEE Int. Symp. Netw. Comput. Appl.*, pp. 19–28, Jul. 2008.

[35] P. Du and A. Nakao, "DDoS defense as a network service," *2010 IEEE Netw. Oper. Manag. Symp. - NOMS 2010*, pp. 894–897, 2010.

[36] F. Al-Haidari, M. Sqalli, and K. Salah, "Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses," in *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 1167–1174.

[37] V. Sandar and S. Shenai, "Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks," *Int. J. Comput. Appl.*, vol. 41, no. 20, pp. 11–16, Mar. 2012.

[38] S. Y. Ameen, S. W. Nourildean, and I. Ntroduction, "Firewall and VPN Investigation on Cloud," *Int. J. Comput. Sci. Eng. Surv.*, vol. 5, no. 2, pp. 15–25, 2014.

[39] H. B. Acharya and M. G. Gouda, "Firewall verification and redundancy checking are equivalent," in *Proceedings - IEEE INFOCOM*, 2011, pp. 2123–2128.

[40] E. S. Al-Shaer and H. H. Hamed, "Discovery of policy anomalies in distributed firewalls," *Proc. - IEEE INFOCOM*, vol. 4, pp. 2605–2616, 2004.

[41] C.-H. Lin, J.-C. Liu, and C.-C. Lien, "Detection Method Based on Reverse Proxy against Web Flooding Attacks," *2008 Eighth Int. Conf. Intell. Syst. Des. Appl.*, pp. 281–284, Nov. 2008.