© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Identification and Avoidance of DDoS Attack for Secured Data Communication in Cloud

G. Divya AP/CSE, Archana S, Dhanalakshmi S, Divya D
Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

Distributed Denial of Service (DDoS) attack in a client server environment would collapse the entire system, but as far as cloud is concern it is not that effective but still it will try to disturb the regular activity of the system. We deploy multiple Intrusion Prevention System (IPS) to monitor the activity of the users and filter the request based on the behaviour and forwards to the corresponding servers through cloud server. Every server would have allocated certain space in cloud server. IPS monitors the activity of the users to avoid DDoS attacks. This system ensures the detection and avoidance of DDoS attack in the cloud server. Few DDoS attacks are listed and monitored. The behaviour patterns are 1.Continuous and same request from single user in a point of time,2.Different query from the same user within a period of time,3.Different queries from different users but from same IP, 4. Request of huge sized file beyond the permitted. Based on these patterns user behaviour is monitored therefore DDoS attack is avoided in cloud.

Keywords: Cloud computing, Distributed denial-of-service attack detection and avoidance, multiple Intrusion Prevention System (IPS)

I. INTRODUCTION

Cloud computing is a recent trending in IT that where computing and data storage is done in data centres rather than personal portable PC's. It refers to applications delivered as services over the internet as well as to the cloud infrastructure – namely the hardware and system software in data centres that provide this service. The sharing of resources reduces the cost to individuals. The best definition for Cloud is defined in [2] as large pool of easily accessible and virtualized resources which can be dynamically reconfigured to adjust a variable load, allowing also for optimum scale utilization. Distributed Denial-of-Service (DDoS) is an especially potent type of attack on Web availability, capable of severely degrading the response-rate and quality at which Web-based services are offered. An emerging and increasingly more prevalent set of DDoS attacks are the so-called application-layer or Layer-7 attacks that mimic a Flash Crowd event. A DDoS attack is a distributed, cooperative and large-scale attack. It has been widely spread on wired or wireless networks. In the early research about DDoS defence, Yau et al.[7] treated DDoS attacks as a problem of resource management.

Recent researches [8], [9], [10] have further demonstrated that the essential issue of DDoS attack and defense is a competition for resources, the one who possesses more resources in the battle is the winner.

II. METHODS AND MATERIAL

A. Cloud Server Deployment

Cloud Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain all the User information to authenticate the User when are login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Cloud Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job. The Request of all the Users will process by the Resource Assigning Module. To communicate with the Client and with the other modules of the Cloud Network, the Cloud Server will establish connection between them. For this Purpose we are going to create a User Interface Frame. Also the Cloud Service Provider will send the User Job request to the Resource Assign Module in Fist in First out (FIFO) manner.

a) Deployment of Multiple IPS

In this system we implement multiple IPS which is intrusion protection system that is used to protect the user form the attacks. In existing system they were using single IPS to scan the query of a cloud user [7]. Here multiple IPS is deployed to monitor the user query so that it easily finds the denial of attack. Cloud Servers is a cloud infrastructure service that allows users to deploy one to hundreds of cloud servers instantly and create advanced, high availability architectures.In general, the number of benign users is stable, and we suppose the virtual IPS and virtual server have been allocated sufficient resources, and therefore the quality of service (QoS) is satisfactory to users.

b) DDoS from Single User

DDoS is a type of DoS attack where multiple compromised systems which are usually infected with virus are used to target a single system causing a Denial of Service (DoS) attack [5]. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. In a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more[12][14]. This effectively makes it impossible to stop the attack simply by blocking a single IP address is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

c) DDOS from Multiple User from same IP

To launch a *DDoS* attack, malicious *users* first build a network of computers that a large *number of* compromised hosts to probe and check the *same* addresses in period of time, the spreading rate reduces because the *number of* the new *IP* .In this multiple users will be login in the same IP address and send query so it will see the account and it will lead to overload on the sever. In out proposed we monitor the query coming from multiple user from the same IP. We analysis IP address to find the DDOS attack.To the best of our knowledge, this paper is an early feasible work on defeating DDoS attacks in a cloud environment.

d) Attacks Filtering Model

We present a probabilistic packet *filtering* (PPF) mechanism to defend the Web server against Distributed Denial-of-Service (DDoS) *attacks*. In the attack filtering model we implement the requested huge sized file beyond the permitted. Based on these patterns user behavior is monitored DDOS attack is avoided in cloud.In order to estimate our resource demands and QoS for benign users in a DDoS battle, we employ queueing theory to undertake performance evaluation due to its extensive deployment in could performance analysis, such as in [19], [20], [21].Various distributions of Linux are supported, and each user space allocation with different band width is allocated so they utilizes within the bandwidth.

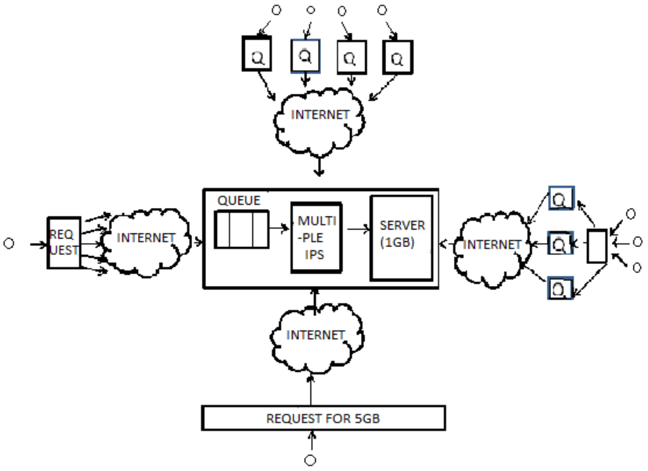

Figure 1: Cloud hosted server under different behaviour patterns of DDoS attack

In this paper, we propose a practical dynamic resource allocation mechanism to confront DDoS attacks that target individual cloud customers. In general, there is one or several access points between a cloud data center and the Internet. Similar to firewalls, we place our Intrusion Prevention System (IPS) at these locations to monitor incoming packets. When a cloud hosted server is under a DDoS attack, the proposed mechanism will automatically and dynamically allocate extra resources from the available cloud resource pool, and new virtual machines will be cloned based on the image file of the original IPS using the existing clone technology [17], [18]. All IPSs will work together to filter attack packets out, and guarantee the quality of service (QoS) for benign users at the same time. When the volume of DDoS attack packets decreases, our mitigation system will automatically reduce the number of its IPSs, and release the extra resources back to the available cloud resource pool.

As aforementioned, the essential issue to defeat a DDoS attack is to allocate sufficient resources to mitigate attacks no matter how efficient our detection and filtering algorithms are. In order to estimate our resource demands and QoS for benign users in a DDoS battle, in this system we employ queueing theory to undertake the performance evaluation due to its extensive deployment in could performance analysis, such as in [19], [20], [21]. We therefore do not involve specific DDoS detection methods, and do not involve too many business issues which may be caused by our mitigation proposal.With the proposed system in place, we believe most DDoS attacks can be defeated, if not all attacks. This will make cloud customers more confident in shifting their businesses to cloud platforms.

B. The contributions of this paper are summarized as follows

We point out that DDoS attacks do threaten individual cloud customers. However, by taking advantage of the cloud platform, we can overcome DDoS attacks, which is difficult to achieve for noncloud platforms. To the best of our knowledge, this paper is an early feasible work on defeating DDoS attacks in a cloud environment. We propose a dynamic resource allocation mechanism to automatically coordinate the available resources of a cloud to mitigate DDoS attacks on individual cloud customers. The proposed method benefits from the dynamic resource allocation feature of cloud platforms, and it is easy to implement.

We establish a queueing theory based model to estimate the resource allocation against various attack strengths. Real-world data set based analysis and experiments help us to conclude that it is possible to defeat DDoS attacks in a cloudenvironment with affordable costs.

C. DDOS Attack Mitigation in Clouds

In this section, we propose a mechanism to dynamically allocate extra resources to an individual cloud hosted server when it is under DDoS attack. In Fig.1.The IPS is used to protect the specific server of the hosted service. All packets of benign users go through the queue,pass the IPS and are served by the server. In general, the number of benign users is stable, and we suppose the virtual IPS and virtual server have been allocatedsufficient resources, and therefore the quality of service (QoS) is satisfactory to users. When a DDoS attack occurs against the hosted virtual server, alarge number of attack packets are generated by botnets, and pumped to queue Q. In order to identify these attack packets and guarantee the QoS of benign users, we have to invest more resources to clone multiple IPSs to carry out the task. We propose to clone multiple parallel IPSs to achieve the goalthe number of IPSs we need to achieve our goal depends on the volume of the attack packets. As discussed previously, the attack capability of a botnet is usuallylimited, and the required amount of resources to beat the attack is usually not very large. In general, it is reasonable to expect a cloud can manage its reserved or idle resources to meet demand.

D. Virtualization Layer (SVL) in Cloud Infrastructure

The Secure model for Virtualization Layer (SVL) protects cloud environment from threats and attacks. In this model is attempted to find a way to improve the attack identification and mechanism to avoid system failure and increase the virtualization security.

The Secure model for Virtualization Layer (SVL) uses cloud architecture which build IaaS on Virtual Machines (VMs) and it workload are usually integrated from the guest OS and the user processes. Virtual Machine Monitor (VMM) is introduced which provides techniques and methods for securing VMs.This method is usually based on IDS/IPS in combination with Access Control List (ACL) and Service-Level Agreement (SLA).The main concept of these models is to build a hierarchical isolate-defeat mechanism, which protect the whole virtualization against malicious activities, identify without preventing legitimate operations from continuous activities. Instead of implementing normal model for cloud infrastructure, we propose a new layer for virtualization, which is called Virtualization Basement (V-Basement). This layer divides virtualization into two separate monitored components. This will improve the feasibility of applying security procedures. It is necessary to specify IDS for each data flow source based on its application. This source allows for lightweight IDSs, instead of huge resource-consuming IDSs.

E. Cryptographyfor Cloud Infrastructure

This standard specifies the AES algorithm, a symmetric block cipher that can process data blocks of 16 bits, using cipher keys with lengths of 16, 192, and 216 bits. The AES algorithm may be used with three different key lengths referred to as “AES-16”, “AES-192”, and “AES-216”. AES algorithm uses a round function, which is composed of four different byte-oriented transformations: 1) byte substitution using a substitution table (S-box), 2) shifting rows of the State array by different offsets, 3) mixing the data within each column of the State array, and 4) adding a Round Key to the State.

In main AES architecture is centrally controlled by both hardware and software components. Decryption of this model is depending upon the designing rule mechanism which is called Substitution Permutation Networking (SPN). Advanced Encryption standard has blocks with fixed length of 16 bits and these allowed key size is 16,192 or 216 bits, new research has evolved that multiple key size can be allocated to the block which could be 32 bits with the least capacity of 16 bits and its key size may be extended with no fixed length is announced. Its whole operations are based on 4X4 matrix of the bytes with finite field calculations, especially designed for the purpose of simple calculations. AES specifies the repetition numbers for convert the input to the normal readable text. An input provided by the user undergoes several steps of processing according to the encryption algorithm which is encryption key provided. Numbers of repetitions are depending on the level of the algorithm and nature used as the base of system. Rounds are depending on the schedule of the algorithm provided by the AES key.

AES Process

We start by looking at the overall structure of the AES cipher algorithm. In AES, the block size is 16 bits and the key size can be 16bits, 192bits or 216 bits. Consider DES algorithm, the cipher consists of a basic operation called "round" which is repeated a number of times.

In the case of AES is based on a design principle called "Substitution-Permutation Networks (SPN)" which state that the cipher is composed of a series of substitutions and permutations one after each another.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text.

The numbers of cycles of repetition are as follows:
10 cycles of repetition for 16-bit keys.
12 cycles of repetition for 192-bit keys.
14 cycles of repetition for 216-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

In AES structure was known as the AES state, which is simply an arrangement of the block state in a 4x4 matrix. Most of the AES operations can be described as operations in the finite field, which gives AES a quite neat algebraic description state. However, they will look at it as a byte operation.

The basic blocks of the AES cipher consists as follow:

Sub Bytes - A non-linear substitution step where each byte is replaced with another

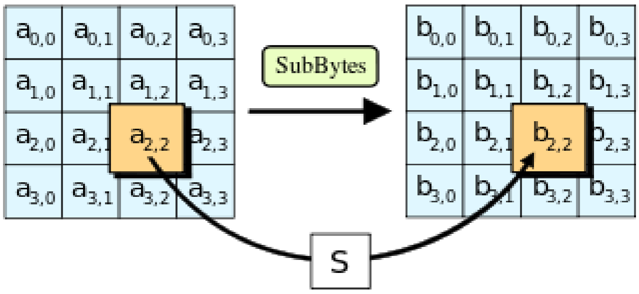
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
S
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Figure. 2: .Replacement of SubByte by shifting rows in AES cipher

In Fig.2 Shift Rows – A transposition step where the last three rows of the state are shifted cyclically a certain number of steps. It Fig.3 Mix Column - A mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey -The subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule. Each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

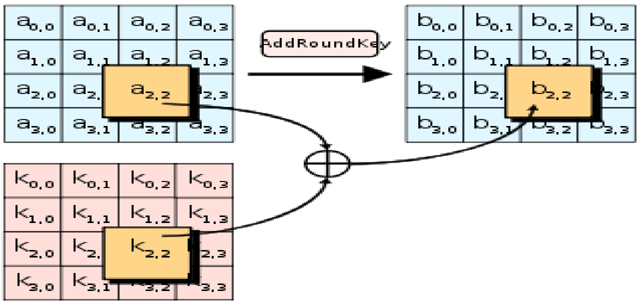

Figure 3: Replacement of SubByte by mixing column in AES cipher

AES encryption consists of the following step:

Initial round:
AddRoundKey
Rounds
R-1 rounds:
Sub Bytes
Shift Rows
Mix Columns
AddRoundKey
Final round:
Sub Bytes
Shift Rows
AddRoundKey

So, we have an initial AddRoundKey step, which mixes input data with the 0th round key. Then, R-1 (9, 11 or 13) identical rounds take place, and at the end a final round is applied.

F. DDoS Attack Mitigation in Cloud Environment

We propose a mechanism which is dynamically allocate an extra resource to an individual cloud hosted server, when it is under DDoS attack identified.

In cloud environment, we examine the features of a cloud hosted virtual server in nonattack scenario. A cloud hosted service includes a server host and intrusion prevention system (IPS) and also include buffer for incoming Cloud hosted server in a nonattack scenario. The IPS is used to protect the specific host server of the service. All packets of beginning users go through the queue and pass the IPS and are served by the server host. In general, the number of begin users is stable, and we propose a virtual IPS and virtual server have been allocated for sufficient resources, so that the quality of service (QoS) is satisfactory to users. When a DDoS attack occurs against by the hosted virtual server, botnets generated a large number of attack packets, and pumped to queue Q. In order to detect these attack packets and QoS of benign users. We propose to clone multiple parallel IPSs to achieve our goal which was depends on the volume of the attack packets.

a) DDoS Mitigation Algorithm for Cloud Environment

In this section, we propose a related algorithm for the mitigation strategy.

DDoS Detection Methods

In this section, we discuss about detection of DDoS defense in cloud infrastructure which is especially depends on the resources no matter which defense methods we are using. Therefore, in our mitigation algorithm, we focus on the resource management aspect of detection method.

In the algorithm, we first analysis the arrival patterns in nonattack for a protected server, and then extract the parameters α and β. Moreover, we also identify the resources for the current intrusion prevention system (IPS), RIPS, or available idle resources RC of the cloud environment. When a DDoS attack is detected by the original IPS, we then clone another IPS which is based on the image of the original IPS, and then calculate the average time for the current status. If $Ta(t,m) > Tn$, then we clone one more available IPS for the filtering task. As the battle continues until we find $Ta(t,m) < Ta(t,m-1)$, finally it is time to reduce one IPS and then release the resources back to the cloud infrastructure available resource pool.

b) System Modeling and Analysis

In this section, we discuss about how to model the system in general, and then establish an executable mathematical model to detect the resource demands on various attack strengths using queuing theory for mitigation method.

General System Modeling

In general, we implement a black box system and then observe its input and output with respect to the time (t).We denote the input and output as m (t) and n (t), and the black box system function as g (t) .We implement a relationship among these three functions as follows:

$$n(t) = m(t) * g(t) \tag{1}$$

Where * is the convolution operation.

In order to find solutions for the output, and for many cases, we map m(t) and g(t) into another domain using different transform techniques,(i.e.)Laplace-transform, Z-transform.

The Laplace transform of input m(t) is defined as follows

M(s) =integral (m(t) e^-st dt) (2)

Similarly, we can obtain G(s) from g(t). Let N(s) be the Laplace transform of n(t), and we obtain N(s) through the following equation

N(s) = M(s) . G(s) (3)

Once N(s) is in place, we can calculate n(t) using the inverse Laplace transforms,

n(t) = 1/2(pi)i integral(N(s) e^st ds) (4)

In our case, m(t) represents the arrival distribution, g(t) is the system service distribution. In the queuing theory, system can be modeled as G=G=p, namely, general arrival distribution and general service rate distribution. However, for this general model, the analysis will be very complex. For ex, we cannot obtain M(s) and G(s) from m(t), g(t) most of the time, and we cannot obtain n(t) even if N(s) is in place sometime.

III. RESULTS AND DISCUSSION

A. Performance Evaluation

In this section, we evaluate the performance of theproposed dynamic resource allocation method for DDoS mitigation in a cloud from various perspectives. We first study the performance for nonattack scenarios, then investigate the performance of the proposed mitigation method against an on-going DDoS attack, and then estimate the cost for the proposed mitigation methods. First of all, we summarize the key statistics of DDoS attacks in a global scenario from highly referred literature [6], [8], and present them in Table 1.A cloud usually has profound resources. We use the Amazon EC2 as an example and show the related data in Table 2.

TABLE 1
Key Statistics of DDoS Attacks

Feature	*Attack duration [8]*	*Attack rate [8]*	*Sources per attack session[6]*
Value	5 minutes	500 request/s	Around 1000

TABLE 2
Estimated Key Resources of Amazon EC2

Resource	*servers* *Bandwidth*
Value	500,000 1Gb/Instance

Based on Tables 1 and 2, we can conclude that it is not possible to deny the service of a cloud data center as a data center possesses profound resources against the attack capability of a DDoS attack.

On the other hand, we are interested in observing the workload of individual web sites for our following experiments. In order to obtain this data,we observed two popular web sites (one news web site and one e-business web site) of a data center of a major ISP. We counted the requests for each web site every 30 seconds for a day. We processed the data and present the number of requests in seconds in Fig. 2. From these results, we can see that the requests for a popular web site are usually less than 10 requests per second. It is generally unwise to reserve too many idle resources as it becomes costly. For the news web site, we suppose the owner reserves resources for a maximum need of 10 requests per second. As Moore et al. [8] indicated, the average attack rate is 500 requests or packets per second. This means a web site faces 50 times the workload of its maximum capacity.

It is not difficult to conclude that a DDoS attack is highly likely to be successful. This confirms our claim that a DDoS attack is still a critical threat to individual cloud hosted services. As discussed previously, we use average time in system as a metric for our performance evaluation in the following experiments. Therefore, let us firstly explore the average time in system for nonattack cases, which is modelled as an M/M/1 queue. We want to know the impact on the average time in a system from different arrival rates under different service rates.we obtained the results of experiments shown in Fig. 3. These results indicated that when an IPS server is heavily loaded, e.g., μ=10 (therefore, $\rho n \rightarrow 1$ when $\lambda \rightarrow 10$), Tn increases in an exponential way. On the other hand, when the IPS server's workload is suitable, e.g.,μ= 15 (therefore, $\rho n \rightarrow$ 2/3 when $\lambda \rightarrow 10$), This relatively stable for various arrival rate λ. From this experiment, we know that the workload of an IPS should be kept within a suitable range. If it is too low, say $\rho n <$ 0:5, then we waste some capability of the system. On the other hand, if it is too high, say $\rho n \rightarrow 1$, then we degrade the quality of service for benign users. We summarize this in the following observation.

a) Observation 1

We prefer the busy rate as high as possible under the condition that the average time in system is acceptable.

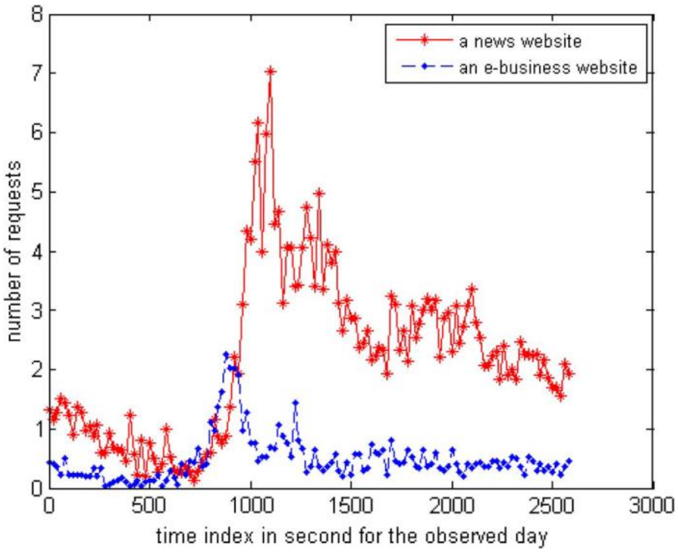

Figure 4: Requests per second for two popular web sites of a major ISP data center.

Secondly, we studied the performance when a DDoS attack was ongoing. As previously discussed, we have multiple IPS servers in this case, and the model is M/M/m. For the system of multiple IPS servers, π0is an important element, and is also involved in the calculation of other items. We expect a good understanding of π0against the number of duplicated servers (m) for a given busy rate.

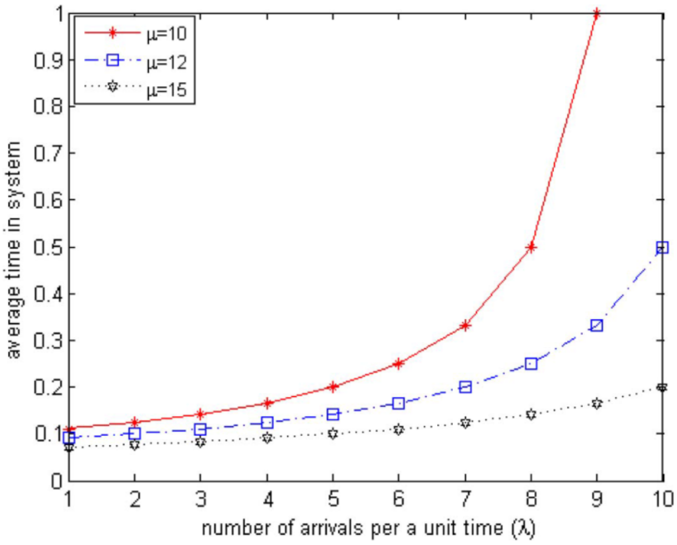

Figure 5: Average time in system against arrival rate under different service rates for nonattack cases.

The experiment results are shown in Fig. 4. In contrast to π0, ρmþ is also important to us because it is a critical point where incoming packets have to wait for service, which is expressed and the experimental results are shown in Fig. 5. The results indicate that: 1) for a given number of duplicated IPS servers, the higher ρ is, the less probability of packet queueing; 2) for a given ρ, the probability of packet queueing decreases when there are more duplicated servers (this is intuitively straightforward). From this perspective, we obtain the following observation.

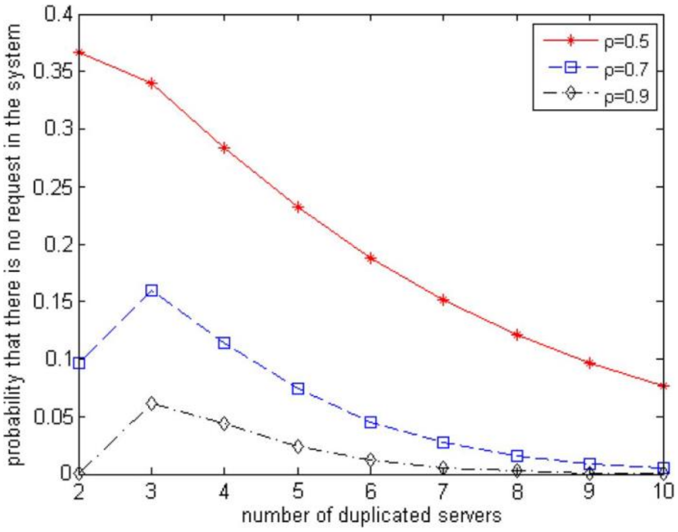

Figure 6: Relationship between π0 and the number of duplicated IPS servers for a given busy rate.

b) Observation 2

In order to reduce the queuing probability, we prefer the busy rate to be high. We note there is a contradiction between observation 1 and observation 2. Intuitively, there should exist equilibrium for the busy rate that balances the needs from both sides. However, this is beyond the scope of this paper, and will be an avenue for future research. To evaluate the performance of the proposed mitigation method, we desperately want to know how we can beat an on-going DDoS attack using minimum resources. In other words, how can we hold equation under the constrains. In the following experiments, we set the service rate of the original IPS as μ=10, therefore, there are three variables, λ (arrival rate for nonattack cases), r (attack strength as defined before), and m (number of duplicated IPSs), which have an impact on our results. In order to match our previous experiments, we conduct three experiments for λ= 5; 7; and 9, respectively. For a given λ, we observe the variation of f(r,m). The results are shown in Figs. 6a, 6b, 6c, which show complete information about the metric f(r,m). As previously discussed, if f(r,m) <0, this means the average time in system for the proposed method is greater than that of nonattack cases, namely, the quality of service for benign users in an attack case is worse than they expect. In order to guarantee the QoS, we need to keep f(r,m) ≥ 0, which is of more interest to us. Therefore, we repeat the threesimulations and only display the f(r,m) ≥ 0 parts, asshown in Figs. 6a.1, 6b.1, 6c.1, respectively. When f(r,m) < 0, this means benign users enjoy an even better QoS than they had in nonattack cases. This occurs by the cloud service provider investing more resources into the service.

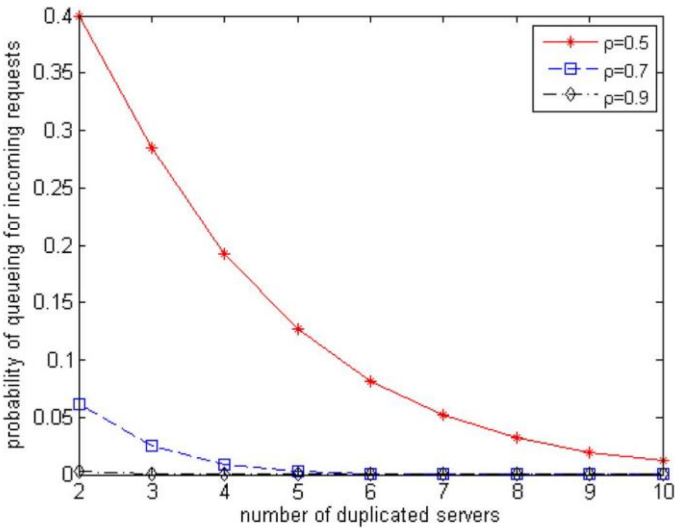

Figure 7: Relationship between ρmþ and the number of duplicated IPS servers for a given busy rate.

From the results of Figs. 6a.1, 6b.1, 6c.1, we find thesolution space is roughly divided into two parts: the right hand part (low r and high m part) and the left hand part. Obviously, the right hand part is not what we expectbecause it requires a large amount of resources (represented by m) for a low attack strength case (represented by r). CSPs prefer to minimize their investment of resources, namely, to make sure f(r,m)→ 0 any time.

Based on Figs. 6a.1, 6b.1, 6c.1, we extract the critical points of f(r,m)→ 0, and demonstrate them in Fig. 7. The relationship between r and m in Fig. 7 looks linear. However, this is not true. We therefore list some of the numerical results in Table 3 for readers' reference. In order to estimate the financial cost ofmitigating DDoS attacks using our proposed strategy, we use Amazon EC2 as an example. Currently, the prices of Amazon EC2 Pricing for Standard On-Demand Instances. We take the default setting of a small Linux instance in our following calculation. We suppose the legitimate traffic volume is 10 requests per second based on our real-world data set (refer to Fig. 2). At the same time, based on DDoS attack characteristics (refer to Table 1), we take the attack rate as 500 requests per second. Therefore, the attack strength is 50. Under different normal workloads (measured by busy rate), we need different numbers of duplicated IPSs to carry out the mitigation task.

By combing all these parameters, we obtained a monetary cost in terms of duration of attacks as shown in Fig. 8. We should note that a long time and high volume DDoSattack is very rare. For example, Moore et al. [8] have indicated that the average attack duration is around 5 minutes, and the rate of a repeat attack is quite low.This may contributed by a few reasons. First of all, long time DDoS attacks will expose botnets to defenders, and therefore, bots will be removed by network administrators.

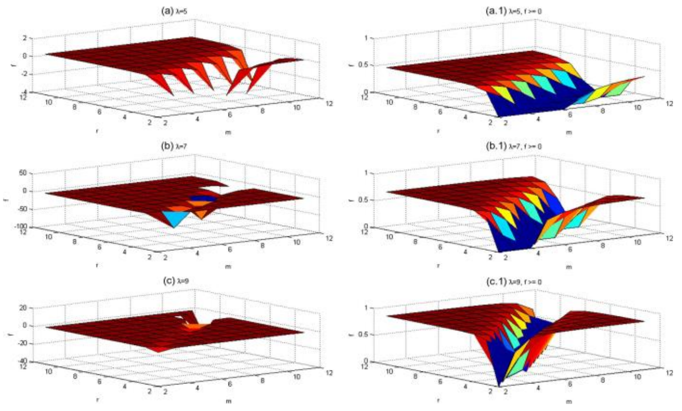

Figure 8: Performance of defense systems under DDoS attack (compared to nonattack cases) with a different number of duplicated IPSs m, different attack strength r, and different arrival rate λ (with fixed service rate μ= 10). (a) Function f with λ= 5, (a.1) function f ≥0 with λ=5. (b) function f with ρ ¼ 7, (b.1) function f ρ 0 with λ=7. (c) function f ≥0 with λ=9, (c.1) function f ≥ 0 with λ= 9.

Secondly, it is hard for attackers to organize a large number of active bots to carry out lengthy attacks, e.g., time zones have an impact on the number of active bots [12].

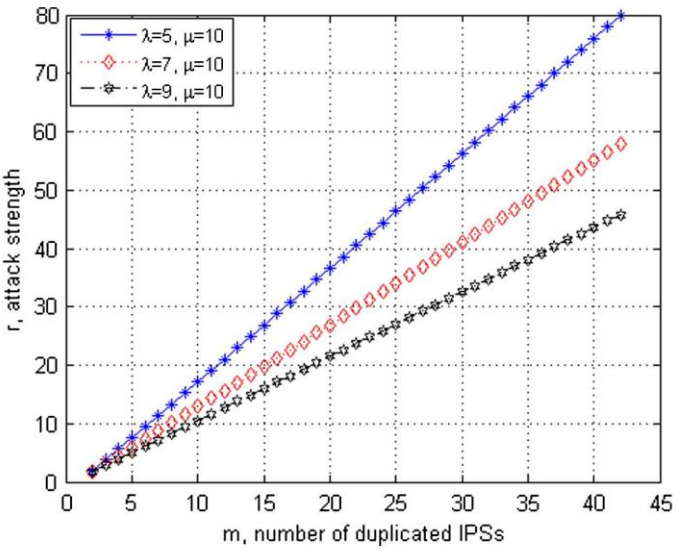

Figure 9: Relationship between attack strength r and minimum number of duplicated IPSs to guarantee QoS for benign users.

In order to have a straight concept of the monetary cost, we list some of the numerical results from Fig. 8

From Table 5, we can see the defense cost for most DDoS attacks on a victim is less than US$1 per month if the attackhappens every fortnight based on the observation of [8]. A dedicated attack for 1 day or 1week costs defenders around US$50 or US$350, respectively. We note that this kind of lengthy attack occurs with a low probability as they can be easily found by CSPs, and subsequent actions can be taken to terminate them. Based on these results, we claim that the proposed mitigation strategy is practical and feasible.

IV. CONCLUSION and FUTURE WORK

Many researchers have found that there are many security issues in cloud computing. The surveys focus on various threats for the cloud environment like abuse of cloud computing resources, insecure APIs, etc. In this paper we found out that the DDoS attacks are the major threat in cloud environment and acts as a effective tool for cyber criminals to shutdown individual cloud customers. Because of this we design a strategy for dynamic allocation of resources and to avoid brute force attack through Intrusion Prevention System to defeat the attack and provide Quality of Service (QoS).

Future Work

Current clouds are considered to be distributed systems, and a cloud is usually a composite of a number of data centers. A cloud customer is generally hosted by one data center. The problem arises if a data center runs out of reserved resources during abattle against a DDoS attack; the question remains how touse the reserved resources of other data centers to beat the ongoing attack, defeat the attacks, and at the same time guaranteeing the quality of service for benign users.

As future work, we firstly attempt to improve the M/M/m model to a more general model, such as the M/G/m model for better performance. Secondly, to explore what to be done if a cloud data center runs out of resources during a battle. In future collaborative resource sharing will be used in majority in this case this system can designed to ensure the security in proper manner and attack should be detected and avoided in the data packet shared between the service providers. Thirdly, we would like to discover whether it is possible for attackers to rent the resources of a cloud to carry out their attacks on servers hosted by the same or other clouds and to find out whether there is any other possible behaviour of DDoS attacks which would affect the cloud customers. Finally, real cloud environment tests for the proposed method are expected in the near future which makes cloud environment usage safe.

V. REFERENCES

[1] J. Francois, I. Aib, and R. Boutaba, ‘‘Firecol, a Collaborative Protection Network for the Detection of Flooding ddos Attacks,’’IEEE/ACM Trans. Netw., vol. 20, no. 6, pp. 168-1641, Dec. 2012.

[2] C. Peng, M. Kim, Z. Zhang, and H. Lei, ‘‘Vdn: Virtual Machine Image Distribution Network for Cloud Data Centers,’’ in Proc.INFOCOM, 2012, pp. 161-169.

[3] S. Subashini and V. Kavitha, ‘‘A Survey on Security Issues in Service Delivery Models of Cloud Computing,’’ J. Netw. Comput.Appl., vol. 34, no. 1, pp. 1-11, Jan. 2011.

[4] G. Carl et al., “Denial-of-service attack-detection techniques,” IEEE Internet Comput., vol. 10, no. 1, pp. 82–89, Jan./Feb. 2006.

[5] 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. 1-3, 2007.

[6] M.A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, ‘‘My Botnetis Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging,’’ in Proc. 1st Conf. HotBots, 2007, p. 5.

[7] D.K.Y. Yau, J.C.S. Lui, F. Liang, and Y. Yam, ‘‘DefendingAgainst Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles,’’ IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 29-42, Feb. 2005.

[8] D. Moore, C. Shannon, D.J. Brown, G.M. Voelker, and S. Savage, ‘‘Inferring Internet Denial-of-Service Activity,’’ ACM Trans. Comput. Syst., vol. 20, no. 2, pp. 115-139, May 2006.

[9] S. Ros, F. Cheng, and C. Meinel, “Intrusion Detection in the Cloud,” 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 729–734, Dec. 2009.

[10] “Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach.” Ying Xuan Dept. of Comput. & Inf. Sci. & Eng., Univ. of Florida, Gainesville, FL, USA Incheol Shin ; Thai, M.T. ; Znati, T.

[11] U. Tupakula, V. Varadharajan, and N. Akku, “Intrusion Detection Techniques for Infrastructure as a Service Cloud,” 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, pp. 744–751, Dec. 2011.

[12] J. Idziorek, M. Tannian, and D. Jacobson, ‘‘Insecurity of Cloud Utility Models,’’ IT Prof., vol. 15, no. 2, pp. 18-23, Mar./Apr. 2012.

[13] S. L. and Z. L. and X. C. and Z. Y. and J. Chen, S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, “Virtualization security for cloud computing service,” in International Conference on Cloud and Service Computing (CSC), 2011, pp. 174–179.

[14] Q. Wang, K. Ren, and X. Meng, ‘‘When Cloud Meets Ebay: Towards Effective Pricing for Cloud Computing,’’ in Proc.INFOCOM, Mar. 2012, pp. 936-944.

[15] A. Shevtekar, K. Anantharam, and N. Ansari, “Low rate TCP Denial-of-Service attack detection at edge routers,” IEEE Commun. Lett.,vol. 9, no. 4, pp. 363–365, Apr. 2005.

[16] Y. Chen, K. Hwang, and W.-S. Ku, “Collaborative detection of DDoSattacks over multiple network domains,” IEEE Trans. Parallel Distrib.Syst., vol. 16, no. 12, pp. 1649–1662, Dec. 2007.S. Yu and W. Zhou, “Entropy-Based collaborative detection of DDoSattacks on community networks,” in Proc. 6th IEEE Int. Conf. PervasiveComputing and Communications (PerCom 2008), 2008, pp.566–571.

[17] R.Wartel, T.Cass, B.Moreira, E. Roche, M. Guijarro, S.Goasguen, and U.Schwickerath, ‘‘Image Distribution Mechanisms in Large Scale Cloud Providers,inProc.CloudCom, 2010, pp.112 117.

[18] J. Zhu, Z. Jiang, and Z. Xiao, ‘‘Twinkle: A Fast Resource Provisioning Mechanism for Internet Services,’’ in Proc. INFOCOM, 2011, pp. 802-810.

[19] H. Khazaei, J.V. Misic, and V.B. Misic, ‘‘Performance Analysis of Cloud Computing Centers using m/g/m/m+r Queuing Systems,’’ IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 5, pp. 936-943, May 2012.

[20] H. Khazaei, J.V. Misic, V.B.Misic, and S. Rashwand, ‘‘Analysis of a Pool Management Scheme for Cloud Computing Centers,’’

IEEE Trans.Parallel Distrib. Syst.,vol.20, no.5, pp. 849-861,May 2013.

[21] H. Sun, J. C. S. Lui, and D. K. Y. Yau, “Defending against low-rate TCP attacks: Dynamic detection and protection,” in Proc. IEEE Int.Conf. Network Protocols (ICNP 2004), 2004, pp. 196–205.

[22] H. Sun, J. C. S. Lui, and D. K. Y. Yau, “Defending against low-rate TCP attacks: Dynamic detection and protection,” in Proc. IEEE Int.Conf. Network Protocols (ICNP 2004), 2004, pp. 196–205.

[23] Dagon, C. Zou, and W. Lee, ‘‘Modeling Botnet Propagation using Time Zones,’’ in Proc. 13th NDSS, 2006, pp. 1-16.