|| Volume 3 || Issue 5 || May 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

An Effective DDoS Defence Framework Using Network Function Virtualization

Shelke Shivani[1], Supekar Dhanashri [2], Satav Vishakha[3] ,Hande Shubhangi[4] Asst. Prof. M.D.Ingle[5]
Student, Jayawantrao Sawant College Of Engineering, Handewadi, Hadapsar, Pune-28, India

Abstract: **Destructive Distributed Denial of Service (DDoS) attacks is one of the top security concerns as the DDoS attacks volumes are increasing constantly.DDos is high profile attack.Among them the SYN Flood attack is the most common type.Other attack are UDP flood,ICMP (Ping) flood,SYN flood,Ping of Death,HTTP flood.Conventional DDoS defense solutions may not be preferable since they demand highly capable hardware resources which induces high cost and long deployment cycle.The emerging of Network Function Virtualization (NFV) technology introduces new opportunities to decrease the amount of proprietary hardware that is needed to launch and operate network services.Also existing solution are not network interoperable.They requires specific hardware In this paper, we propose a DDoS defense mechanism named DDfence which facilitates a "domain-helps-domain" collaboration network among NFV-based domain networks. DDfence allows domain networks to help each other in handling large volume of DDoS attacks through resource sharing. Specifically compatible. The resource sharing mechanism is modeled as a multi-leader-follower Stackelberg game. In this game all domains have a degree of control to maximize their own utility. The resource supplier domains determine the amount of resource to each requesting peer based on optimizing a reciprocal-based utility function. On the other hand, the resource requesting domains decide the level of demand to send to the resource supplier domains in order to reach sufficient support.In this paper we are using maven.moven is build automation tool.**

Keywords—*: DDoS Attacks ,HybridCloud SoftwareDefined Networking ,Network Virtualization, scalability , security , Denial of Service*

I INTRODUCTION

Distributed Denial of Service (DDoS) attacks have a history of about 25 years up to now since the first ping flooding attack appeared in 1989 . In order to avoid detection, DDoS attacks are usually launched by botnets, which are groups of zombies remotely controlled by attackers. Zombies are usually coded to use spoofed source addresses and each address is only used to send part of the attack traffic. These techniques make DDoS attacks hard to detect and defend. Distributed Denial of Service (DDoS) attacks have been a growing problem for computer networks and Internet users.They utilize a variety of techniques of flooding, amplification, protocol exploiting, and malformed packets. DDoS attacks become more advanced with the use of zombie hosts and reflectors to hide the attacker's traces. Malicious network packets look very similar to normal traffic [3]. Distributed denial-of-service (DDoS) attacks make online services unavailable by overwhelming victims with traffic from multiple attackers. How to effectively and quickly detect DDoS attacks is one of the most important problems for network measurement. Since DDoS attackers are by nature distributed across the whole network, coordinated networkwide monitoring is necessary for efficient DDoS detection[15]. For example, on October 21,2002, an attacker flooded the root DNS servers with traffic in an effort to deprive the Internet of the DNS name lookup service (which would have paralyzed the majority of In ternet applications). Only five out of thirteen root servers were able to withstand the attack Previously, DDoS attacks had shut down several large Internet sites, such as Yahoo! and eBay[4]. experimental results demonstrate that our proposed solution can effectively reduce the attack flow to the target server, and therefore our solution mitigates DDoS attacks[7]. The defense mechanism leverages the flexible feature of NFV that allows the implementation of network functions dynamically according to the requirements.

There are many ways of DDoS, such as UDP flooding attacks, Smurf attacks and SYN flooding attacks and so on. And the SYN flooding attack is one of the most widely used ways. Using the inherent defect of the TCP/IP protocol, it is concealed and destructive but simple to use. In order to detect the SYN flooding attacks, many methods have been proposed. SYN cookie method is based on the TCP sever. It enhances the three-way handshake protocol by calculating a cookie according to the SYN segment, when the sever sends back the SYN/ACK segment. This is in fact to verify legality of the ACK segment. This mechanism can remove the backlog queue in original TCP, but the complex process of calculating and verifying may become another disadvantage against high-rated traffic DDoS attacks, researchers have taken two distinct approaches: *router-based* and host-based. The router-based approach installs defense

mechanisms inside IP routers to trace the source(s) of attack or detect and block attacking traffic. However, these router-based solutions require not only router support, but also coordination among different routers and networks, and wide-spread deployment to reach their potential.In contrast to the router-based approach, the host-based approach can be deployed immediately. Moreover, end systems should have a much stronger incentive to deploy defense mechanisms than network service providers[13].

In this paper, we present a new approach for defending against DDoS attacks that DDefence, a collaborative DDoS diminution network system which facilitates a "domain-helps-domain" collaboration network. In this network, a domain can direct excessive traffic to other trusted external domains for DDoS filtering. The filtered clean traffic will be forwarded back to the targeted domain. Specifically, we focus on the resource allocation problem when multiple requesters ask for help. We design a fair and incentive-compatible resource allocation method which provides an effective collaborative DDoS defense with inherent reciprocal ecosystem. The resource allocation scenario is further modeled into a multi-leader-follower Stackelberg game by formalizing a two-level utility functions for resource requesters and suppliers. More specifically, the resource provider domains determines how much resource to allocate to each requesters, and resource requester domains decide how much resource to request from each provider. We study the optimal strategies of all players and derive a Nash equilibrium for the Stackelberg game. Our experimental results demonstrate that our proposed solution can effectively reduce the DDoS attack flow to the targeted server, and the resource allocation is fair and provides incentive for domains to maximally help other domains in need. The contributions of this paper include: 1) A novel collaborative DDoS defense network based on network function virtualization technology. 2) A dynamic resource allocation mechanism for domains so that the system is fair, efficient, and incentive-compatible. 3) A multi-leader-follower Stackelberg game model to study the resource allocation results of network domains. 4) An evaluation of our proposed solutions using simulation to verify that the proposed solution is effective, fair, and incentive compatible.

BACKGROUND AND RELATED WORK

In this section we will briefly discuss the previous DDoS attack techniques and DDoS defense using network softwarization technologies.

DDos Attack Techniques:

DDoS attacks can be divided into two categories: IP spoofing and attacks based on real IP addresses. When an attack is formed by using IP spoofing techniques, duplicate source IPs are used to hide the true IP address of the attackers. An example of such type of attack is SYN Floods . Almost DDoS attacks based on real source IPs utilize botnets as attacking source. A bot master orchestrates a large number of compromised devices in the Internet to flood the target. However, the attacking bot nodes can be detected and blacklisted so that the overall cost of using bot nodes is much higher than the spoofing-based attacks. Therefore the botnet based attack typically generates only a small percentage of the entire attacking stream.On the other hand, the IP spoofing-based DDoS attacks,such as SYN Floods, can effectively hide the true identities of attacking nodes and also require much less resources to launch the attacks. For SYN Floods, the attacker fabricates a large number of TCP SYN packets using spoofed source IPs to initiate hand-shakings with the victim, which overflows the backlog on the victim to prevent legitimate SYN requests from being processed.

DDoS attacks are generated to the web server. Attack scripts created using traffic generation tool used to attack the web server are HTTP flooding, session flooding, TCP flooding and UDP flooding. The HTTP packets may be HTTP-valid or HTTP-invalid packets. HTTP-valid packets are used to request the inline objects like number of pages and resources from the server. HTTP-invalid packets are used to flood the victim. In session flooding attack, attacker requests more number of connections to the server. Sockets are completely utilized by the session flooding attack, so service is unavailable to legitimate user. In TCP flooding, attacker requests connection to the server to create half open connection, but in UDP packets there is no response. In this network,there is Node deployment function for deploying number of nodes.after deploying the number of nodes there is function for creating clusters and randomly select the cluster head in distributed network by using by using cluster detection.After the selection of cluster head there is next process for resource allocation to each node by using specific algorithm that will be briefly discuss in algorithm section.In a network there is a process for helping the nodes for identify which node is hacked by attacker.these process is happened by using another algorithm.These overall network is sensing data from the users.

DDoS Defense using Network Softwarization Technologies:

NFV is gaining growing attention from both academia and industry due to its potential for cost reduction and operational efficiency. The main idea of NFV is to replace dedicated network appliances, such as hardware-based routers and firewalls, with software that runs on commercial off-the-shelf servers .A network based on NFV can achieve much lower cost and much higher flexibility compared to a traditional computer network. Based on ETSI NFV ISG, the NFV architecture is composed of three key elements.

1) Network Function Virtualization Infrastructure (NFVI):NFVI is composed of the commercial-off-the-shelf hardwareand the abstractions of the computing, storage and networkresources.The abstraction is achieved through a virtualizationlayer based on hyperviser, which decouples the virtual resources from the underlying physical resources.

2) Virtual Network Functions (VNF): A VNF is a virtualized functional block within a network infrastructure that has well defined external interfaces and functional behavior. Examples of VNFs include virtualized residential gateway, virtualized firewall, and virtualized load balancer. VNFs can be realized through virtual machines.

3) NFV Management and Orchestration (NFV MANO): NFV MANO performs the orchestration and lifecycle managementof NFVI resources and VNFs. It is in charge of theoperations of the VNFs such as the configuration of the VNFsand the infrastructure these functions run on. It covers threefunctional blocks: NFV Orchestrator, VNF Managers, andVirtualized Infrastructure Manager. NFV MANO also interacts with the (NFV external) business support systems (OSS/BSS) landscape, which allows NFV to be integrated into an already existing network-wide management landscape. The defense network is an NFV network consisting of dynamically allocated virtualized network functions (VNFs). In the physical layer, we have one product server which provides online service to customers from the Internet, and three commodity servers which are connected to each other. Each commodity server hosts virtual machines to realize different virtual network functions, such as dispatcher, switches, and agents. The dispatcher is the gateway for packets to the virtual filtering system. This agents act as filters for attack traffic. The VNFs are organized in a way so that attack flows will be handled by filtering agents

II EXISTING SYSTEM

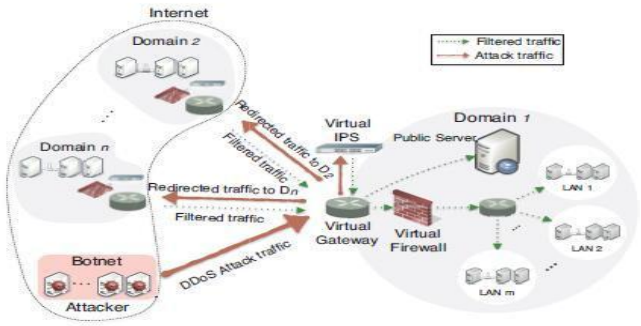


Fig. 2. A case study of collaborative DDoS defense

In DDoS attack detection using matching pursuit algorithm, distributed denial of service attacks are threat to the internet. In this paper TCP SYN flood attacks are identified by using matching pursuit algorithm. Dictionaries are created using K-SVD algorithm from attack traffic and normal traffic of training data. Matching pursuit algorithm uses the created dictionary and match the current traffic and detect attacks in the network.

In Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, in this paper, DDOS attacks identify based on entropy metric and the information distance metric. Algorithm checks traffic and measuring difference between legitimate traffic and attacked traffic.In An alert analysis approach to DDoS attack detection, in this paper system generate large number of false alert when it finds attacks in network and DDOS attack detection by using alert correlation. The alert correlation process is useful for identify and analyze multistep attacks. in detecting dos and ddos attacks by using an intrusion detection and remote prevention system, in this paper system uses intrusion detection and identify the intrusion and based on intrusion system detect the ddos attacks.in ddos attack detection using packet size interval, in this paper attacks detect by using packet size. system continuous checks packet size and identify difference of packet size between legitimate traffic and attack traffic.in machine learning based ddos attack detection from source side in cloud, system collects statisticalinformation from cloud server and virtual machine and prevents network packets to send outside the network. in experiment result checks nine machine learning algorithm performances and 99.7% four kind of ddos attacks detected.

III PROPOSED SYSTEM

Node Deployment:

In Node deployment stage, the specific number of node which is given by user deployed in jung simulation. we also called node as a domain. To identify DDOS attack, first of all we need to create network.

Cluster Head Selection:

In cluster Head selection stage, The network is divided into four cluster and each cluster has its own cluster head. cluster head selection is based on node energy, distance from base station and energy required for transmitter and reciever.

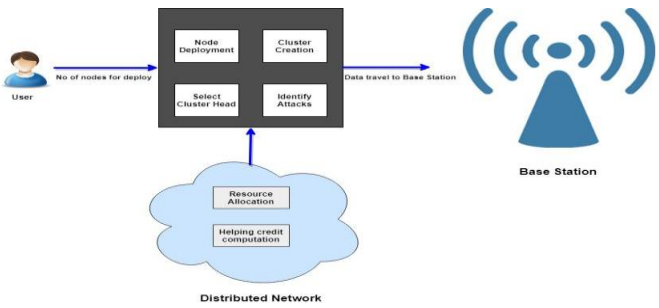
Resource Allocation:

a node contains processor, RAM and hardware components and these components we called as a resources. neighbour node sends help request for resources and resouce allocation algorithm identify how much resouces required for perform certain task.resource allocation technique is most useful when balanced the load in network.

DDOS attack detection:

While attacking perticular network, attacker first of all change it's IP by using virtual private network and it is also called as IP spoofing. our system holds DHCP IP list and if attackers IP is different then we identify given user is attacker. when attacker launches DDOS attack in network then lot of traffic generated. our system identify which domain or node send lot of traffic in network and detect attacks.

IV System Architecture:



V MathematicalModel:

Input : No of nodes

Let, S be a system, S= { N, C, CH, B, U , H}, where,

1. Deploy Sensor nodes.. N= { N1, N2, ..., Nn }, N is set of all deployed sensor nodes.

2. Cluster formation. C= { C1, C2, ..., Cn }, C is a set of all clusters.

3. **Select the Cluster Heads** that is aggregator for Each Clusters. CH= { CH1, CH2, ..., CHn }, CH is a set of all cluster heads.

4. **Create Base Station**. B= { B1, B2, ..., Bn }, B is a set of all base stations.

6. **Optimal Resource Allocation for Domain** u: This algorithm describes the algorithm for each domain u to find the optimal resource allocation given requested amount and past credit

U= { Nu, Hu, Ru, ru , u}

Nu = the set of neighbors of domain u that are trusted by domain u

Hu = helping credits for all neighbors of domain u

Ru = requested helping resource needed by the neighbors of domain u

ru = the total available resource for domain u

u = Utility function

7. **Seek Help by Node u** : In this step first of all identify it's trusted neighbors, then its helping domain help to solve DDos

attack and after solving attacks then given helping nodes credits updated.

H = {v. Au , Nu}

v= v computes resource offer

Au = required helping resource needed for domain u during DDoS attack

Nu = Update neighbors' helping credits periodically Δt

Output = Identify DDos Attack.

Algorithm

Node deployment**:**

for i to n

iteration

Randomly choose x and y coordinate to ith node with specified range by using random() method

plot ith node in cluster area.

Cluster Head Selection :

Energy Calculation, Etx (k; d) = Eelec * K+ ∈amp * k * d n

ERx(k) = Eelec * k

d: Distance for neighboring sensor node.

∈amp: Energy required for the transmitter amplifier.

Eelec: Energy consumed for driving the transmitter or receiver circuitry.

highest energy node assigned as cluster head-

Resouce Allocation**:**

when multiple sensor node sends data to cluster head then managing all request is not possible so for handling request we provide resources of near by nodes.

collect all x and y coordinates of sensor node as well as cluster head in particular cluster by using jung getX() and getY() function.

calculate distance between sensor node to cluster head. distance = clusterhead x - sensor x + clusterhead y - sensor y.

sort array of distance by using red black Binary search tree (It provides lowest time complexity for searching and sorting).

collect four lowest distance sensor node in cluster.

each neighbor node has some capacity to handle request.

if request come then sort neighbors based on capacity and choose highest capacity neighbors

while request assigned to neighbors then we deduct request capacityin neighborscapacity.

neighbors Resource capacity = neighbors Resource capacity - request capacity

Go to previous step until request comes

VI LITERATURE SURVEY

CAAMP: Completely Automated DDoS AttackMitigation Platform in Hybrid Clouds

Distributed Denial of Service (DDoS) attacks areone of the main concerns for online service providers becauseof their impact on cost/revenue and reputation. This paper presents Completely Automated DDoS Attack Mitigation Platform (CAAMP), a novel platform to mitigate DDoS attackson public cloud applications using capabilities of software defined infrastructure and network function virtualization techniques.When suspicious traffic is identified, CAAMP deploys a copy of the application's topology on-the-fly (a shark tank) on an isolated environment in a private cloud. It then creates a virtual network that will host the shark tank. Software defined networking (SDN) controller programs the virtual switches dynamically to redirect the suspicious traffic to the shark tank until final decision is made. If traffic is proved to be non-malicious, SDN controller installs flow rules on the switches to redirect the traffic back to the original application. Thus, CAAMP autonomically protects applications against potential DDoS threats and lowers the false positives associated with common detection mechanisms by leveraging resources from a private cloud.

SDNShield: Towards More Comprehensive Defense against DDoS Attacks on SDN Control Plane

While the software-defined networking (SDN) paradigm is gaining much popularity, current SDN infrastructure has potential bottlenecks in the control plane, hindering the network's capability of handling on-demand, fine-grained flow level visibility and controllability. Adversaries can exploit these vulnerabilities to launch distributed denial-of-service (DDoS) attacks against the SDN infrastructure. Recently proposed solutions either scale up the SDN control plane or filter out forged traffic, but not both. We propose SDN Shield, a combined solution towards

more comprehensive defense against DDoS attacks on SDN control plane. SDN Shield deploys specialized software boxes to improve the scalability of ingress SDN switches to accommodate control plane workload surges. It further incorporates a two stage filtering scheme to protect the centralized controller. The first stage statistically distinguishes legitimate flows from forged ones, and the second stage recovers the false positives of the first stage with in-depth TCP handshake verification. Prototype tests and dataset-driven evaluation results show that SDNShield maintains higher resilience than existing solutions under varying attack intensity.

A Pi2HC Mechanism against DDoS Attacks

Distributed Denial of Service (DDoS) attacks pose a major threat to today's cyber security. Defense against these attacks is complicated by source IP address spoofing. The Path Identification (Pi) mechanism is a promising technique to defend against DDoS attacks with IP spoofing. In the Pi scheme, each router marks forwarding packets to generate particular identifiers corresponding to different paths, which can be used to distinguish between malicious packets and legitimate ones. To improve the previous Pi scheme, we suggest that the victim record not only the Pi mark of each packet but also its hop count (HC). Thus the victim can use the <Pi, HC> tuple to identify and discard malicious packets instead of Pi more effectively. By theoretical analysis and simulations based on actual Internet topologies, we demonstrate our scheme, Pi2HC, outperforms previous Pi. We also show that Pi2HC is robust against spoofed initial Time-to-Live (TTL) values by sophisticated attackers.

A Real-time Method for Detecting Internet-wide SYN Flooding Attacks

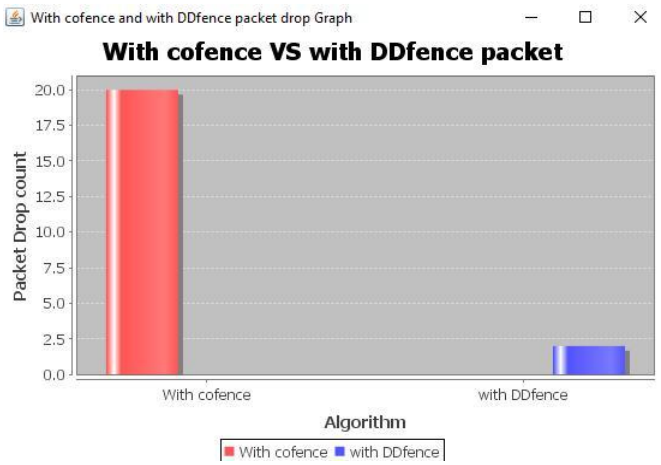
Reports show that DDoS attacks are ubiquitous on the Internet and may jeopardize networks' stable operation. In order to understand the nature of this threat and further to enable effective control and management, a whole picture of the Internet-wide attacks is a necessity. Traditional methods use darknets to this end. However, with the IPv4 address space exhaustion, darknets become hard to acquire. In this paper, we seek to detect Internet-wide attacks using a live network. In particular, we focus on the most prevalent SYN flooding attacks. First, a complete attack scenario model is introduced according to the positions of the attacker, the victim and the attacking address. Then, after discussing the features of all scenarios, an algorithm named WSAND is proposed to detect Internet-wide SYN flooding attacks using Netflow data. In order to evaluate it, the algorithm is deployed at 28 main PoPs (Points of Presence) of the China Education and Research Network (CERNET) and the total internal address space is up to 200 /16 blocks. A large quantity of Internet-wide SYN flooding attacks detected in March 2014 is discussed in detail. With the help of the detected attacks, a case study of detecting an internal zombie is presented.

An SDN-Supported Collaborative Approach for DDoS Flooding Detection and Containment-Tommy Chin, Xenia Mountrouidou,2011

We have presented the implementation of a collaborative detection and containment mechanism of network attacks. Our approach is unique to use a synergistic monitoring, detection and mitigation strategy to realize the full capabilities of SDN.The experimentation on GENI has shown that our solution is scalable to process a high volume of traffic and large scale attacks. The alerting, detection, and mitigation in our system are proven robust through experimentation. Furthermore, the total time required for this collaborative system to detect and contain an attack is low. Thus, this solution can potentially be deployed in a real system where such an attack is detected and mitigated in time before legitimate users start to suffer. We are working to apply this collaborative approach to other security applications, including detection and mitigation of covert channels and other attacks. Our goal is to develop a systematic methodology along this line of work.

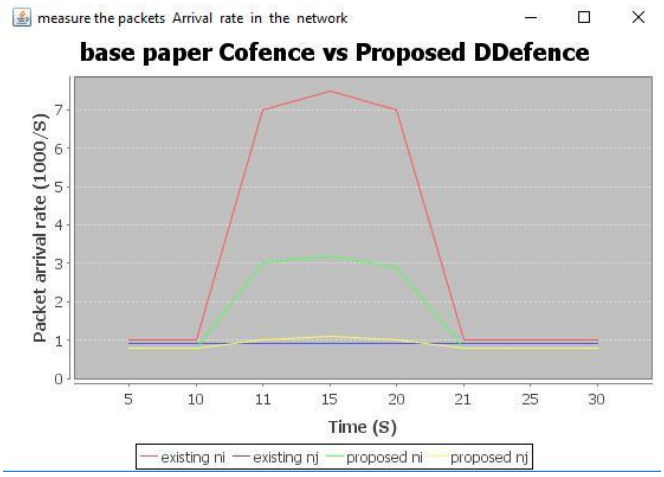
VII RESULT ANALYSIS

Without Cofence Vs with Ddfence packet drop count



Our results show that compared to Cofence,Packet drop count decreases with Ddfence.

Measure the packets arrival rate in the network



Packets Arrival Rate increases with Ddfence as we have assigned credit to every node to forward packets to cluster head Packets dropping rate decreases with Ddfence compared to Cofence

VIII FUTURE WORK

Through proposed history based characterization yield reasonable performance against DDos attacks ,yet sneaky attackers can falsely train our history to treat attacker's sources as legitimate ones. As per literature , deviation in traffic cluster entropy can be effectively used to estimate number of attack sources. The estimate number of attack source cn act as minimum threshold to find attack source from the history matrix iteratively.

DDos attacks are launched using well coordinated and highly organized attack networks .The ISPs are also required to work in tandem for designing technical and economic model to achieve cooperation, in order to fight against the menace of DDos attack collaborativety.

As easy availability of user friendly attack tools and their source codes provide flexibility to attack create a variety of new attacks by error and trial. It is almost impossible to predict all attack variations and design defenses that will work for all cases. So the long term goal should be to design bug free code and fix the security holes in existing system as early as possible.

The number of DDos defense technique developed in recent past has grown in number but not in quality in number of. The clear-cut proof for the same is growing number of DDos incidents against popular sites. In order to strengthen the quality of research in the field ,scalable test bed and freely accessible benchmarked attack dataset must be available to the researchers.

IX CONCLUSION

Purpose of this paper is the Defence ,it is Effective network used to defend against DDOS based on Network Virtualization technology, domain network cause excessive traffic to other collaborating element under DDos attack for filtering. So use focus on the resource allocation mechanism they determine one domain how much resource provide and should offer to the requester , so resource distributed easily fairly with incentives. To make the resource allocation optimized ,we using the stakelberg game model for collaboration. We Proposed a QOS framework to make a collaboration fair under when domain network agree with. Evaluation result demonstrate the collaborating DDos defence can reduce impact from the attack and proposed resource allocation mechanism can give as to desing goal. In order to make our credit evaluation process more fair and effective we will include the impact of link bandwidth into our credit evaluation process

REFERANCES

[1] Arbor ddos detection and protection. http://security.arbornetworks.com/protection, Last Visit: December 2016.

[2] Y. Xu and Y. Liu. Ddos attack detection under sdn context. In IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, pages 1–9, April 2016.

[3] Biggest internet attack in history threatens critical systems. http://www.ibtimes.co.uk/biggest-internet-attack-history-threatenscritical-infrastructure-450969, Last Visit: December 2016.

[4] W. Ding, W. Qi, J. Wang, and B. Chen. Openscaas: an open servicechain as a service platform toward the integration of sdn and nfv. IEEENetwork, 29(3):30–35, May 2015.

[5] ETSI NFV ISG. Network Functions Virtualization White Paper 3:Network Operator Perspectives on Industry Progress. In SDN andOpenFlow World Congress, Oct. 2014.

[6] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey. Bohatei: Flexible andelastic ddos defense. In 24th USENIX Security Symposium (USENIXSecurity 15), pages 817–832, Washington, D.C., 2015. USENIX Association.

[7] P. Ferguson and D. Senie. Network ingress filtering: Defeating denialof service attacks which employ ip source address spoofing (bcp 38) .http://tools.ietf.org/html/rfc2827.

[8] C. J. Fung and B. McCormick. Vguard: A distributed denial of serviceattack mitigation method using network function virtualization. InNetwork and Service Management (CNSM), 2015 11th InternationalConference on, pages 64–70. IEEE, 2015.

[9] R. Greenwell, X. Liu, and K. Chalmers. Semantic description of cloudservice agreements. In Science and Information Conference (SAI), 2015,pages 823–831, July 2015.

[10] W. Ding, W. Qi, J. Wang, and B. Chen. Openscaas: an open servicechain as a service platform toward the integration of sdn and nfv. IEEENetwork, 29(3):30–35, May 2015.

[11] ETSI NFV ISG. Network Functions Virtualization White Paper 3:Network Operator Perspectives on Industry Progress. In SDN andOpenFlow World Congress, Oct. 2014.

[12] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey. Bohatei: Flexible andelastic ddos defense. In 24th USENIX Security Symposium (USENIXSecurity 15), pages 817–832, Washington, D.C., 2015. USENIX Association.

[13] P. Ferguson and D. Senie. Network ingress filtering: Defeating denialof service attacks which employ ip source address spoofing (bcp 38).http://tools.ietf.org/html/rfc2827.

[14] C. J. Fung and B. McCormick. Vguard: A distributed denial of serviceattack mitigation method using network function virtualization. InNetwork and Service Management