Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective

K.C. Okafor
Dept. of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Imo State, Nigeria

Joy Anulika Okoye
Dept. of Electrical and Electronic Engineering, Odumegwu Ojukwu University Uli, Anambra State, Nigeria

Gordon Ononiwu
Dept. of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Imo State, Nigeria

ABSTRACT

A previous work on Airport Information Resource Management System (AIRMS) established that sophisticated attacks in the form of Denial of Service (DoS), Distributed DoS (DDoS), and related attacks are becoming the most effective schemes used by cyber terrorists on such enterprise systems. Similarly, a novel Smart Green Energy Management Distributed Cloud Computing Network (SGEM-DCCN) was developed as an extension to the work. Interestingly, the DCCN could be shut down by malicious attackers while running its renewable energy management cloud service. Consequently, this work presents a security model designed to improve the security architecture in a mission-critical DCCN running Enterprise Energy Tracking Analytic Cloud Portal (EETACP). As a result of the EETACP DCCN vulnerability to DoS attacks, this work employed a core OpenFlow gateway firewall to pre-empt DDoS attacks and subsequently mitigate such destructive vulnerabilities in the network. In this case, Vulnerability Bandwidth Depletion DDoS Attack (VBDDA) was detected using Cisco Nexus 9000 firewall as an embedded network device with support for Virtual DDoS protection in the DCCN threat mitigation design. Also, security Quality of Service (QoS) profiling was employed to ascertain the network behavior in terms of resource utilization and query response times. For DDoS traffic flows, the network metrics were compared under simulated firewall scenarios involving Cisco Application Policy Infrastructure Controller (Cisco APIC), Cisco Nexus 9000 Series multilayer Switches and Cisco Application Virtual Switch (AVS). It was concluded that with a robust firewall in place, VBDDA will be mitigated in DCCN infrastructure. This offers protection and reliability in the Smart Green Energy Management System architecture.

General Terms

Distributed Cloud Computing, Modelling & Simulation, Security Architecture, Smart Green, Design Algorithms.

Keywords

Bandwidth Depletion, Cloud Datacenters, Smart Green, Vulnerability Attacks, Threat, QoS Profiling, DCCN, OpenFlow Firewall, Riverbed Modeller.

1. INTRODUCTION

1.1 Background Study

A DoS attack is a malicious attempt to make a server or a network resource unavailable to users usually by temporarily interrupting or suspending the services of a host connected to the Internet. It is aimed at disrupting the normal function of a specific website or service. It is planned and coordinated with the goal of ensuring that an entire web service is unavailable to the valid users. In a DDoS attack, by taking advantage of security vulnerabilities, an attacker could take control of the entire network system by using multiple systems to launch the attack. This forces a vulnerable system to send huge amounts of data to the entire network making the web service to be unavailable to the valid users. This is the case with a previous work on AIRMS.

Basically, Distributed Denial-of-Service (DDoS) attack is considered as a major threat to cloud computing Smart Green Energy Management System (CC-SGEMS) which offers on-demand load profiling and Demand Side Management (DSM) services. Attackers could compromise vulnerable energy users (hosts), called zombies, on the network and deploy attack tools on them. These zombies can together form a Botnet that could generate large amount of distributed attack packets targeting at the backend servers under the control of the attackers [1]. This attack will block the legitimate access to the servers, exhaust their resources such as network bandwidth, computing power and even lead to great financial losses [2].

With the plans of deploying SGEMS architecture in the Nigerian environment, DCCN DoS attack must be addressed to maximize its potentials. For the SGEMS in context, the DCCN service provider will be charged with the responsibility of providing EETACP services to end users. This comes with its peculiar challenges especially for EETACP services uptime. This is because the service providers will struggle under intense pressure to monitor, prevent, and mitigate DDoS attacks directed toward their infrastructure [3].

For the DCCN network service provider, network security remains a very vital consideration since any loophole can cause active disaster. According to [4], enterprise customers and service providers increasingly want their critical assets to be protected from large DDoS attacks and other security threats. Some forms of network attacks seen on daily basis include direct attacks, remote controlled attacks, reflective attacks, worms, and viruses. But specific attacks directed at the service provider's infrastructure could be very destructive and cause wide spread outages.

A secure network infrastructure sets the foundation for efficient service delivery, but there are approximately three major branches of DDoS research yet to be fully addressed such as attack detection [5], [6], attack filtering [7], [8], and attack traceback [9], [10]. From the perspective of attack filtering as a branch of DDoS research, attacks filtering is usually based on the point of protection. They include: source-initiated, path-based and victim-initiated [7]. In the SGEMS architecture, to harness DSM, billing and consumption profiling for end users, adequate security reinforcement at the gateway demilitarized zone will facilitate mitigation of

VBDDA in the DCCN. Hence, under this condition, an efficient renewable energy cloud solution would remain sustainable. The emphasis of this paper is on victim-initiated area, which filters incoming attack packets from victim side i.e. DCCN server cluster domain. In this regard, availability is one of the three main components of DCCN security, along with confidentiality and integrity [11].

1.2 Research Contributions

EETACP service and several other services are now being shared and provisioned in the DCCN platform which elastic cloud environment providing unlimited capabilities. The effect of DDoS attacks could render SGEMS/EETACP project [4] grounded, apart from degrading its QoS (refer to Appendix 1). In view of this challenge, this paper aims at proposing a holistic approach to securing DCCN to facilitate return on investment in the SGEMS/EETACP DCCN. Consequently, the main motivation of this paper is to explore, and evaluate the significant effects of DDoS attacks against a newly developed DCCN. It is believed that only by better understanding the effects and consequences of these attacks, can sensible and effective counter measures be possibly developed.

In context, the key contributions of this work are highlighted as follows:

- To provide an extensive review on state of the art in the DoS research area, various attack mechanisms, while identifying a more practical taxonomy for DoS attack and its defence mechanisms.
- To show a DoS/DDoS attack mitigation approach in DCCN which hosts EETACP service.
- To show the functionality of OpenFlow security firewall.

Consequently, this research will summarily achieve the following:

i. Use of Stateful packet Inspection OpenFlow Application Configuration Interface (SPI-OACI) for the DCCN protection while carrying out the security QoS profiling using selected metrics.

ii. A developed vulnerability bandwidth and memory attack model for the cloud based network.

The rest of the paper is organized as follows. Section 2, focused on threat dimensions and related security proposals. Section 3 presented the research methodology. Also, the security architecture, characterization of Vulnerability Bandwidth Depletion DDoS Attack (VBDDA), SPI-OACI allocation model, security architectural components, and SPI-OACI DDoS mitigation procedure were addressed in section 3. Section 4 explained the experimental system design, detailing the simulation/validation setup with Riverbed Modeller 17.5. Section 5 discussed the results while Section 6 summarized the key outcomes of the research.

2. LITERATURE REVIEW

2.1 Classical Theories on Attacks

In [12], some popular types of DoS attacks that work against current TCP/IP-based cloud based internet were enumerated. This section contextualizes these attack/threat dimensions.

2.1.1 DDoS Reflection Attacks

This type involves three parties namely [13]: the attacker, a victim host, and a set of secondary victims (reflectors). The goal of the attacker is to use the reflectors to overwhelm the victim host with traffic. To do so, a reflection attack uses IP packets with unreal addresses. Here, the attacker replaces its own source addresses with the address of its intended victim, and sends these packets to the secondary victims. Responses to such packets are not routed back to the attacker; rather it overwhelms the victim instead. To be effective, these attacks use some form of amplification optimization, (i.e., the amount of data used by the attacker to perform the attack is significantly smaller than the amount of data received by the victim [13]. However, SPI-OACI routers incorporate a useful suppression feature such that whenever an SPI-OACI router/firewall overhears a content packet on a broadcast interface for which it has a current entry with the incoming interface, it caches the content and flushes the entry as anomaly traffic.

2.1.2 DDoS Bandwidth Depletion

Basically, in a typical coordinated DDoS attack, attacker-controlled zombies flood their victims with IP traffic in order to saturate their network resources [12]. The intended aim is to make the victims unreachable by other users or network interface as well as to generally inhibit victims’ ability to communicate. Normally, such attacks are carried out via TCP, UDP or ICMP and rely on sending a stream of packets to the victim at the maximum data rate. Similarly, in bandwidth depletion attacks, the requested content is dynamic, and all interests are routed to content servers, thus consuming bandwidth and router/firewall utilization cycle state. Also, if generating dynamic content is expensive (i.e. have overhead), the targeted content network servers might waste significant computational resources. A perfect example of this type of attack is one targeted to a web server that allows site-wide searches: each zombie issues an interest that requests the victim server to search its entire site for a random string.

2.1.3 DDoS Prefix Hijacking and Black-holing

In a prefix hijacking attack [14], a misconfigured, compromised or malicious Autonomous System (AS) advertises invalid routers so as to motivate other ASs to forward their traffic to it. This usually results in the term referred to as black-holing [13] whereby all traffic sent to the malicious AS is simply discarded. This attack is effective in IP networks, since, once routing information is infected, it is difficult for routers to detect, and recover from the problem. While countermeasures have been proposed in [15], this remains a serious threat to the current cloud based network data centers.

2.1.4 Domain Name Service Poisoning

In the current cloud Internet, DNS servers translate human-readable names to the corresponding IP address and vice-versa. For performance reasons, DNS servers usually store the output of previous requests in their cache. There is a well-known attack, called DNS cache poisoning [16], which allows the attacker to insert corrupted entries in a DNS server’s cache in order to control the server responses for a set of DNS names. The author in [17] opined that best countermeasure against this attack is the use of the DNS Security Extensions protocol, i.e. DNSSEC [17]. This is gradually gaining acceptance on the cloud domain.

Having discussed these forms, there are still some current variations of the earlier discussed DoS attacks that could be used against DCCN if not well secured. Meanwhile, it should be noted that there are two key features that distinguish current Internet routers from the proposed SPI-OACI counterparts. They are: (1) Pending Interest State (PIT) entries needed to perform content routing and (2) the use of content caches. This work describes the two classes of extended DDoS attacks – Interest Flooding and Content/Cache Poisoning. These are briefly discussed below.

2.1.5 DDoS Interest Flooding

Currently, layer 3 routing of content is performed using Pending Interest State (PIS) entries established by interests [12]. In this context, the name of each incoming content packet is used to look up the Pending Interest Table (PIT) and identify a corresponding entry. The attacker can take advantage of this state to mount an effective DoS attack; hence referred to as interest flooding. In this type of attack, the attacker (normally controlling a set of possibly geographically distributed zombies) generates a large number of closely-spaced interests, aiming to (a) overwhelm (PITs) in routers, in order to prevent them from handling legitimate interests, and/or (b) swamp the targeted content producer(s). Since DCCN SPI-OACI interests has source address and are secured (e.g., signed) by design, this makes it possible to determine the attack originator(s) and take targeted countermeasures.

There are three identified types of interest flooding attacks based on the type of content requested: i.) Existing or static, ii.) Dynamically-generated and iii.) Non-existent (i.e., unsatisfiable interests). In any case, the attacker uses zombies to generate a large number of interests requesting content from targeted hosts or cluster producers. Attacks in (i) and (iii) are mostly aimed at the network infrastructure, while attack (ii) affects both network and application-layer functionalities. The direct outcome of this attack type is that the production server wastes resources to satisfy malicious rather than legitimate interests. The impact on routers varies with their distance from the targeted content producer/server. The third type of attacks involves the issuing of unsatisfactory interests for non-existent content by zombies. Such interests cannot be collapsed by routers, and are routed to the targeted content servers. The latter can quickly ignore such interests without incurring significant overhead. However, such interests will linger and take up space in router memory until they eventually expire. It must be stated that the layer 3 routers are usually the primary victims for this type of attack.

2.1.6 DDoS Content and cache Poisoning

There are DDoS attacks that target content servers, routers, access points, etc. In this case, the attacker's aim is to engender the routers to forward and cache corrupted or unreal data packets (ie. invalid packet signature or generated with wrong private key). The effect is that valid users are prevented from accessing legitimate content.

2.2 Related Research Efforts

Various works in the context of threats and attacks in datacenter network security systems are reviewed in this section. The intent is to ascertain the extent of security research in similar network architectures.

The authors of [18] proposed self-aware networks and a defense against DoS attacks. The work presented an overview of the existing proposals on both detection of such attacks and defense against them. Also, a generic framework of DoS protection based on the dropping of probable illegitimate traffic, with a mathematical model which can measure the impact of both attack and defense on the performance of a network was presented. The authors validated their work with simulation results and experimental measurements in a Storage Area Network (SAN) environment.

In [19], Internet scale DoS attack with a survey on its theoretical underpinnings and experimental applications was carried out. A comparison on the different types of DoS attacks was discussed. The work detailed the DDoS classifications as well as their application domain.

In [20], the authors proposed a mathematical model for a low-rate DoS attacks against application servers (LoRDAS) attack. Their model was used to evaluate the performance of LoRDAS by relating it to the configuration parameters of the attack and the dynamics of network and victim. The model is validated by comparing the performance values given against those obtained from a simulated environment.

In [21], Secure Overlay Services (SOS) architecture was proposed to provide reliable communication between clients and a target under DoS attacks. The SOS architecture employs a set of overlay nodes arranged in three hierarchical layers that controls access to the target. They proposed an SOS architecture that could proactively prevents denial of service (DoS) attacks, which works toward supporting emergency services. Their goal was to allow communication between a confirmed user and a target. Similarly, the work in [22] proposed a composite DoS attack model that combines bandwidth exhaustion, filtering and memory depletion models for a more real representation of similar cyber-attacks. On the basis of their introduced model, different experiments were done. They showed the main dependencies of the influence of attacker and victim's properties on the success probability of denial of service attack. The concept of the composite model was explained where an incoming traffic is blocked because of insufficient bandwidth. In this case, the remaining part of traffic could be blocked by its filtering system.

Other works on threats and attacks with emphasis on evaluation analysis of DoS traffic have been studied in [22], [23]. This paper observed that existing works in literature regarding cyber security vis-à-vis DoS and other schemes have not explored embedded Stateful Packet Inspection (SPI) based on OpenFlow Application Centric Infrastructure (OACI) for securing enterprise systems and their networks such as SGEMS architecture. In fact, works on DoS attack and defense mechanisms are relatively inappropriate in the context of cloud computing for real time renewable management. This work believe that the DCCN architecture should: (1) be resilient to existing DoS/DDoS attacks, or at least limit their effectiveness, (2) anticipate new attacks that take advantage of its philosophies, and (3) incorporate basic defences in its design.

To the best of our knowledge, there has been no scientific and systematic assessment of how DCCN fares with respect to DoS attacks in the presence SPI-OACI and Non SPI-OACI contexts considering VBDDA. Such assessment is believed to be both timely and very important. While SPI-OACI in DCCN appears to be quite efficient in terms of content distribution between valid and invalid traffic entities, it is clear that a comprehensive consideration of security attacks DCCN will eradicate VBDDAs as a case study. Hence, this work adopted Application Centric Infrastructure (ACI) which have support for OpenFlow paradigms, Network Address Translation (NAT), Quality of Service (QoS), IP Security (IPSec), Secure Sockets Layer (SSL) VPN, and an embedded DDoS thereby improving end-to-end network security infrastructure of the SGEMS DCCN at large.

3. SYSTEM DESIGN APPROACH

3.1 System Formulation

First, SGEMS architecture was developed using data obtained from the DCN of University of Nigeria Nsukka, galaxy backbone and swift networks. From these networks, the security setup of these networks makes VBDDA very feasible as they basically uses the basic access control configuration on generic routers. From the findings of the study, the DCCN core backend was built with cluster servers which are protected by the Cisco 9000 SPI-OACI. This was meant to satisfy the security architecture of the DCCN running EETACP service. The SPI-OACI firewall architecture was used to formulate an efficient security interface for the proposed DCCN. The key approach used was the Discrete Event Modelling using object palette tree from Riverbed Modeller 17.5. In this case, the work used OpenFlow firewall as a security hardware interface for thin clients connected to the DCCN server cluster. This creates security framework that is transparently provisioned for users once connected to the internet. It also has control logic which monitors all forms of traffic going into the server clusters.

Besides, the DCCN servers was configured to use the cloud service coordinator which serve as an active interface between the valid users, cloud brokers and the Virtual Machine (VM) instances. The VMs are dynamically interconnected to form a logic topology that mirrors a physical infrastructure. In DCCN, the emulated attacker carries out flood attacks on the target server clusters with massive ICMP/IGMP messages, to consume the bandwidth of the target. In real world, is easy to launch this attack with attack tools such as *hping*, though this is no longer a common attack used by the hackers because the victim can disable this attack by directly filtering and dropping the ICMP/IGMP packets at the network edge.

The major issue investigated in context is the security layout of traffic flow into the DCCN perimeter of defence where malicious attackers seek to hijack the network via the victim imitated DDoS attacks. To understudy the QoS behavior, a VBDDA (ie direct attack such as ICMP/IGMP Flood attack and UDP Flood attack) was then characterized while carrying out a QoS profiling on the network. Another actively harmful VBDDA is the reflection attack technique also known as Distributed Reflection Denial of Service (DRDoS). This exploits the requested responses of the routers and servers (reflectors), in order to reflect the attack traffic as well as hide the attack source. When these attacks are successfully executed, they use up the network bandwidth resource of the target. In this regard, by introducing using OpenFlow Stateful Packet Inspection (SPI) implemented in Cisco IOS firewall [23], this offered a new attack tracking and control paradigm.

Hence, using the simulated SPI-OACI firewall, the DCCN infrastructure supporting the EEATCP platform on clustered backend servers was protected against VBDDA. Failure to achieve this will lead to network collapse and quality of service hijack on the cloud network.

3.2 Vulnerability Bandwidth Depletion DDoS Attack (VBDDA)

A Vulnerability Bandwidth Depletion DDoS Attack (VBDDA) occur when an attacker X_n consumes all available bandwidth by generating a large number of packets directed to the cloud based network such as DCCN. ICMP ECHO packets or disruptive malware could be used as the attack payload. This could also result from an attacker comprising any vulnerable system and using it to launch an attack to the compute backend server cluster. The properties of an attack as explained previously could be used to ascertain its effect on QoS. In [22], a good mathematical expression for calculating the success of DoS attack using the known data on the attacks, normal flow and other properties of the victim is described but this paper models the security QoS metrics for VBDDA using the SPI-OACI approach. In this case, when a DDoS/ DRDoS resource depletion attacks occur~~s~~, this will facilitate an attacker sending packets that misuse network protocol communications or sending malformed packets that tie up network resources so that none are left for legitimate users or the server backend at large. Active memory is usually exhausted, and thus no new queries can be stored and served in the intervening devices or nodes. It has been observed that memory depletion DDoS attacks are the most common because of noticeable effect on an operational networks. For memory depletion DDoS attacks models, using the simplified ingest loss model G(N)/G/m(0) [24], helps to estimate the success of the SYN flooding attack when average attack flow, the average storage time of open-state connections and buffer size are known. As part of the security design of the DCCN [25], this work considered a bandwidth exhaustion and memory depletion contexts which basically allows fractional analysis of every DoS or DDoS attack.
Now, from Figure 3, vulnerability bandwidth exhaustion and memory depletion DDoS attacks on victim nodes are tackled by the SPI-OACI filtering capability. Incoming illegitimate traffic is blocked because of anomaly detection of SPI-OACI thereby filtering the illegitimate packet while maintaining open connections.

Let SPI-OACI bandwidth exhaustion probability be given as B_p, the probability of filtering legitimate traffic as $\mathrm{Fn_P}$ and memory depletion probability as M_P. A Stateful attack probability $\mathrm{S_P}$ can be calculated as the probability of blocking legitimate traffic at least in one of these three device variables, viz: bandwidth exhaustion, filtering or memory depletion [24]:

$$S_p = \sum_{i=0}^{n} \langle 1 - (1 - B_p) * (1 - F_{np}) * (1 - M_p) \rangle \qquad (1)$$

For estimating bandwidth exhaustion probability B_{bP} in SPI OACI, the use of stochastic bandwidth exhaustion model was adopted [26] which is given by Equ. (2)

$$B_{b_p} = \left(\frac{\rho^k}{k!}\right) \Big/ \sum_{i=0}^{k} \left(\frac{\rho^i}{i!}\right) \qquad (2)$$

Where

$\rho = {(S_{Ba} + S_{Bn})}/{T}$. This is also given by:

$\rho = {(I_a * \lambda_{Ba} + I_n * \lambda_{Bn})}/{T}$

.K = Number of open channels

$\mathrm{S_{Ba}}$ = Attack traffic (bps)

$\mathrm{S_{Bn}}$ = Normal traffic (bps)

T = Channel bandwidth (bps)

$\mathrm{I_a}$ = Average Query Size of the Attack (b)

$\mathrm{I_n}$ = Average Query Size of the legitimate users (b)

λ_{B_a}= Average arrival rate attack queries (qps)

λ_{B_n}= Average rate of legitimate queries (qps)

It was assumed that the SPI-OACI filtering system has two properties: the probability of filtering and dispatching legitimate traffic $\boldsymbol{Fn_P}$ and the probability of filtering and dropping attack traffic $\boldsymbol{Fa_P}$. These properties show the part of legitimate and attack traffics that are blocked on average using filters.

To estimate incoming traffic, these properties were considered in Figure 3 to address attack probabilities and memory depletion.

Considering the bandwidth exhaustion model, this work assumed that both legitimate and attack traffic has the same distribution in time as the overall incoming data. After passing the bandwidth exhaustion model, the rate of incoming traffic will be reduced to λ_{Fa} and λ_{Fn} such that Equ. (3) and (4) holds

$$\lambda_{Fa} = \lambda_{Ba} . (1 - B_p) \tag{3}$$

$$\lambda_{Fn} = \lambda_{Bn} . (1 - B_p) \tag{4}$$

Now, the SPI-OACI filtering system must block traffic equally at every instant of time. It is reasonable to say that incoming legitimate traffic $\boldsymbol{\lambda_n}$ and attack traffic $\boldsymbol{\lambda_a}$ could change in size only but not in its distribution as perceived by the SPI-OACI firewall. The extent to which traffic size will be reduced depends on filtering properties of the abnormal or illegitimate traffic probability and normal or legitimate traffic probabilities given in Equ 5 and 6.

$$\lambda_{\mathrm{Mn}} = \lambda_{Bn} . (1 - P_{Fn}) \tag{5}$$

$$\lambda_{\mathrm{Ma}} = \lambda_{Ba} . (1 - P_{Fa}) \tag{6}$$

In the DCCN, another identified type of DDoS attack model is the memory depletion model as previously observed. To represent this kind of the DDoS attack, this work leveraged the SYN flooding attack model [27] which could serve as a more general DDoS attack types. This model is given by Equ. (7).

$$P_m = \left[\frac{\sigma^M}{M!}\right] \Big/ \textstyle\sum_{i=0}^{M} \frac{\sigma^i}{i!} \tag{7}$$

Where

$\sigma = \lambda M_a * t_a + \lambda M_n * t_n$

$\mathrm{t_a}$ = Averageprocessing time of the attack query (s);

M = Buffer size of the SPI firewall

$\mathrm{t_n}$ = Averageprocessing time of the legitimate query (s).

Equ (2) can be used to model a typical ping of death traffic where an illegitimate attack with about 250GBps traffic flow hijacks a network. A typical case scenario was found in [28]. This was an online context illustrating a typical DDoS attack which represented a 250GBps DDoS attack designed to crash the web based service. This can be eradicated with SPI OACI.

3.3 SPI-OACI Security Architecture/Components

The SPI-OACI security gateway controller was used for securing the DCCN against VBDDA. The major device adopted for the implementation is the Cisco Nexus 9000 firewall [29] which is network embedded, and has a virtual DDoS protection capacity. There are two distinct components in the SPI-OACI security model viz: The Traffic Anomaly Detector (TAD) and the Guard Alert Trigger (GAT). Both of these works together to deliver complete DDoS protection for virtually any environment. While the SPI-OACI Traffic Anomaly Detector (STAD). The function is to act as an early warning system, provides in-depth analysis of the most complex DDoS attacks and passively monitors network traffic while looking for any deviation from normal or baseline behavior that indicates a DDoS attack. The SPI-OACI Guard (SG) when notified that a network link or device is under DDoS attack, diverts the normal traffic destined for the target while discarding the abnormal traffic. The traffic is then subjected to a concurrent five-stage analysis and filtering processes. These are designed to remove all malicious traffic while allowing legitimate packets to get to the DCCN backend servers without any interruption. The architectural components of the SPI-OACI comprises viz: verification, analysis, and enforcement techniques shown in Figure 1. These were used as steps for identifying and separating malicious traffic from legitimate traffic. The purification process consists of the following, viz: Filtration of suspicious DDoS flows, active verification of packets entering the system, anomaly recognition which monitors all traffic that was not stopped by the filter or the active verification modules and compares it to baseline behavior recorded over time, looking for deviations that would identify the source of malicious packets. Protocol analysis which processes flows that the anomaly recognition marks as suspicious and rate limiting which provides another enforcement option and prevents misbehaving flows from overwhelming the target while more detailed monitoring is taking place. The module performs per-flow traffic shaping, penalizing sources that consume too many resources (for example, bandwidth or connections) for too long a period.

3.4 SPI-OACI DDoS Mitigation Procedure

As explained previously, Riverbed OpenFlow software was used to implement Figure 1. By enabling the SPI-OACI firewall, the following were monitored in the DCCN cloud network viz: link consumption of computational resources, disruption of configuration information, disruption of state information, disruption of physical network, disruption of the communication media between the firewall and its backend servers. The Figure offers a complete DDoS protection solution based on the principles of detection, diversion, verification, and forwarding to help ensure total protection and mitigation. When a DDoS attack is launched against the DCCN firewall, the cluster server network is protected by the flow (as shown in Figure 1) thereby maintaining business continuity. In this case, the recursive SPI-OACI allow the creation of specific Access Control List (ACL) bypass for only the desired traffic, as defined by an inspection list consisting of only the protocols that are explicitly permitted by an organization’s network security access policy. By analyzing and filtering the illegitimate traffic flows from the legal traffic flows packets prevents malicious traffic from impacting QoS performance while allowing legitimate transactions to complete appropriately.

The SPI-OACI solution shown in Figure 1 provides complete protection against all types of DDoS attacks (VBDDA). Figure 2 shows the SPI-OACI Optimal allocation model which is used for effective and robust security layer considering the various compute resources in DCCN. The main component is the OpenFlow application configuration infrastructure discussed in section 3.5. The advantages include:

i. Growth: Scalability to network growth in respect of computing infrastructures. The solution offers a scalable option that eliminates any single points of failure and does not impact the performance or reliability of the existing network components
ii. Intelligence: Active mitigation capabilities that rapidly detect attacks and separate malicious traffic from legitimate traffic.
iii. Latency: It delivers a rapid DDoS response that is measured in seconds.
iv. Deployment ease: It can be easily deployed adjacent to critical routers and switches. But the key features of the SPI-OACI or Cisco APIC include:

- The capability to build and enforce application-centric network policies.
- An open standards framework, with the support of northbound and southbound application program interfaces (APIs).
- Integration of third-party Layer 4-7 services, virtualization, and management.
- Scalable security for multitenant environments.
- A common policy platform for physical, virtual, cloud based computing integration.

Figure 1 shows the proposed DCCN security algorithm with the traffic flowing between interacting systems via an SPI-OACI firewall.

3.5 OpenFlow Application Configuration Infrastructure

To achieve a robust security for the DCCN using Figure 1 flowchart, an OpenFlow Application Configuration Infrastructure (OACI) was adopted. This enables a holistic approach to managing firewall, network, server, storage, and application resources within a cloud data center and across multiple data centers. The foundation devices of OACI are the Cisco Application Policy Infrastructure Controller (Cisco APIC) and Cisco Nexus 9000 Series devices [30]. In the SGEMS DCCN, the security policy controlled environment, this Cisco APIC was used. This automates and centralizes policies that apply to all layers of the network stack. It was used a secure, programmable environment that anticipates application requirements and rapidly deliver the network infrastructure onto which the EETACP applications is deployed at large scale with high security and full visibility. In the design, this integrates into cloud environments easily, and enables consistently secure policies for both physical and virtual workloads defense mechanisms.

3.6 Description of Firewall Optimal Allocation Framework

In the server clusters, the Cisco APIC northbound integration allowed for easy interfacing into DCCN environment. In addition, the southbound communication enables the APIC to manage the entire DCCN. Consequently, the SPI-OACI enables the DCCN to deliver secure, programmable, policy-based, agile cloud infrastructure to its deployment.

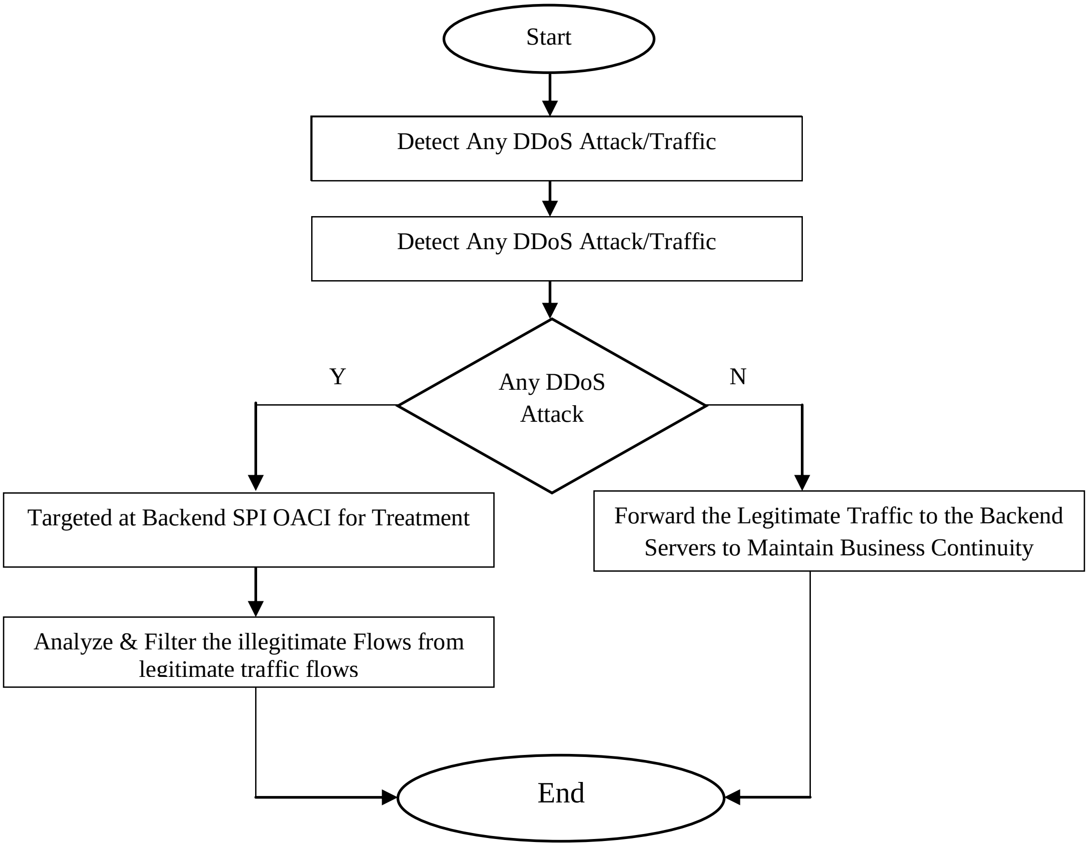

Start
Detect Any DDoS Attack/Traffic
Detect Any DDoS Attack/Traffic
Y
Any DDoS Attack
N
Targeted at Backend SPI OACI for Treatment
Forward the Legitimate Traffic to the Backend Servers to Maintain Business Continuity
Analyze & Filter the illegitimate Flows from legitimate traffic flows
End

Fig 1: Recursive SPI-OACI flow model for VBDDA

The allocation model explains the operation of a high-level Optimal Allocation Framework (OAF) shown in Figure 2 which helps to manage traffic at the firewall gateway. This creates a look up table for the inputs (ie. topology file, normal traffic file, DoS traffic file) and a description of the defense mechanism (DCCN VictimID, excluded nodes, service time penalty, number of defenders). The output comprises the optimal allocation control of firewall against VBDDA. The performance of bandwidth allocation based on the QoS metrics for the network users in the DCCN is monitored. A few parameters referring to the precision of the numerical computations are reflected (number of iterations and buffer sizes). The functional components of Figure 2 are explained next. Essentially, this isolates the background processes that runs in Figure 3 discussed next.

i. Normal traffic file **n**: This text file contains all information for the DCCN normal traffic in steady state. Each line in the file represents a flow of normal traffic with the format being: Unique ID of the flow / node sequence in the flow's path starting from the source to the destination server measured in packets/s or Kbits/sec.

ii. DoS traffic file **d:** This file contains all information for the DDoS traffic in steady state, with each line representing a flow of DoS traffic.

iii. Topology file $\mathbf{T_f}$: The topology network information is fed to the firewall either as a text file which is converted to a fixed topology array or directly as a hard coded array (N is the number of nodes in the topology).

iv. VictimID $\mathbf{A_v}$**:** This is the node ID of the DCCN victim in the scenario i.e. node that the defense system is set to protect.

v. Measured NodeID $\mathbf{M_n}$. This is the node ID used to measure the QoS metrics. Essentially, the SPI-OACI device measures and captures both the normal and the DoS incoming rates for all nodes in a given topology. Optimal allocation is used here for precise packet filtering by the defenders.

vi. Service time penalty $\mathbf{S_p}$: Packet filtering task can affect efficiency at processing and forwarding packets, hence service time penalty is a positive value which represents the increase of the average service time per packet for a specific defence task.

vii. Number of defenders $\mathbf{N_d}$: The SPI-OACI device is designed to suggest the optimal allocation for protecting the network. The number is usually greater than 0.

viii. Average packet size in Kbits/s or packets/ sec, number of iterations, buffer sizes and QoS metrics are computation variables for an operational scenario.

Considering Figure 2, to better appreciate the problem of DDoS in Figure 7 (where there are security vulnerabilities), Let the victim device (firewall, servers, client computer$\boldsymbol{\beta}$) receive packets from both attackers X_1 and X_2, in a normal network with cloud destination server clusters [24]. There could be limited resources which are to be protected in the cloud environment against possible cyber terrorists. Algorithm 1 illustrates a functional traffic event monitoring.

Algorithm 1: DCCN Security with SPI-OACI in DCCN

```
% Define all the network and traffic parameters
Read $\varphi, \beta, \gamma$;
DDoS attack = VBDDA =0
Set definitions for DCCN Defence Parameters;
Set definitions for SPI-OACI at the DCCN gateway;
Set definitions for SPI-OACI  QoS the DCCN gateway;
Set counter = 0;
Start checking legitimate and illegitimate traffic;
If traffic = legitimate, then Traffic = pass (1)
Else if traffic = DDoS attack, then Traffic = fail (0)
Call firewall optimal allocation ()
    Detect and flush Traffic (0);
Estimate QoS metrics for Traffic (1) and Traffic (0) in
DCCN
If Traffic QoS = Above threshold, then ++
If Traffic QoS = Below threshold, then Pause & Exit;
Goto  firewall optimal allocation ();
End;
```

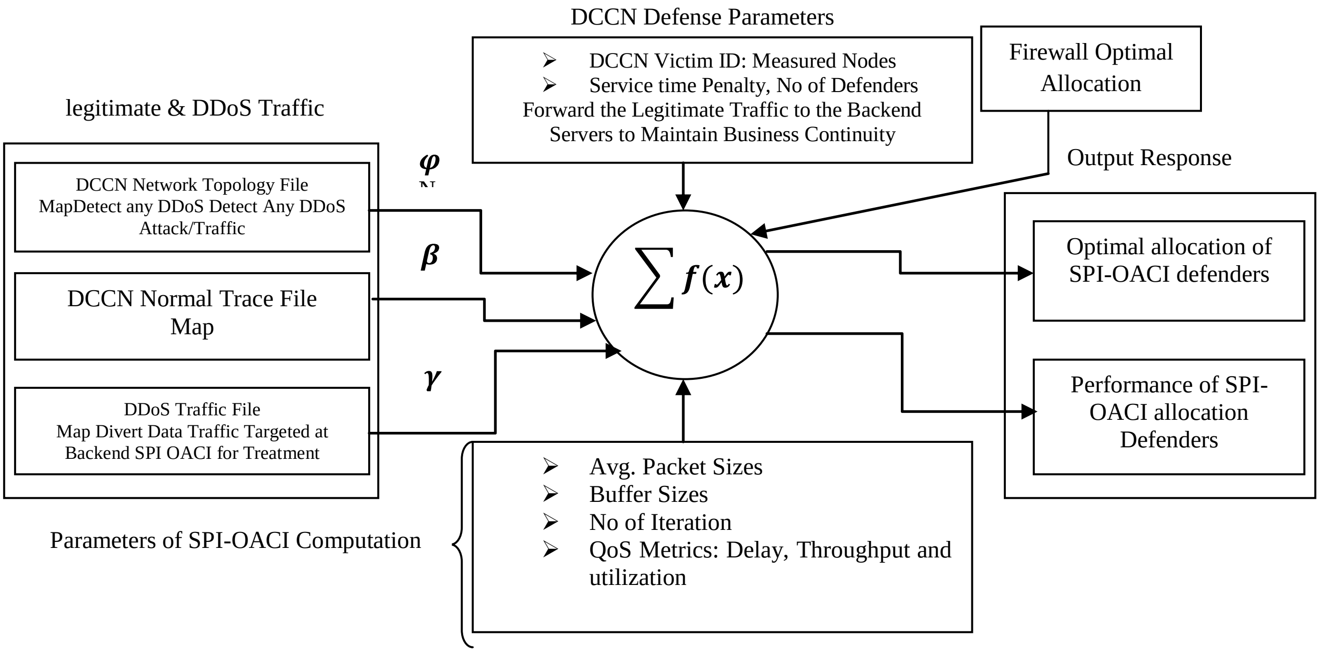

DCCN Defense Parameters
DCCN Victim ID: Measured Nodes
Service time Penalty, No of Defenders
Forward the Legitimate Traffic to the Backend Servers to Maintain Business Continuity
Firewall Optimal Allocation
legitimate & DDoS Traffic
Output Response
DCCN Network Topology File MapDetect any DDoS Detect Any DDoS Attack/Traffic
DCCN Normal Trace File Map
DDoS Traffic File Map Divert Data Traffic Targeted at Backend SPI OACI for Treatment
φ
β
γ
∑ f(x)
Optimal allocation of SPI-OACI defenders
Performance of SPI-OACI allocation Defenders
Avg. Packet Sizes
Buffer Sizes
No of Iteration
QoS Metrics: Delay, Throughput and utilization
Parameters of SPI-OACI Computation

Fig 2: A Model for DCCN SPI-OACI Optimal Allocation Firewall Mechanism

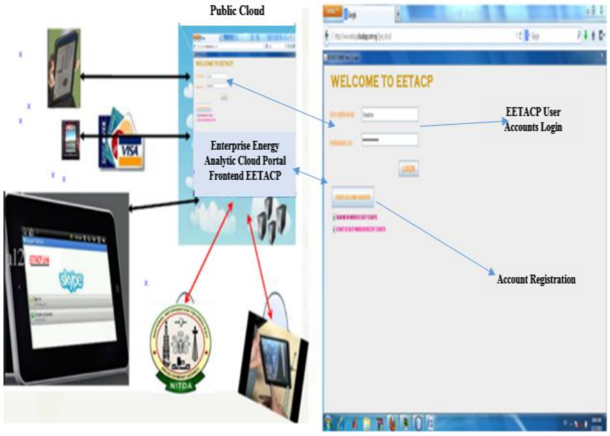

Public Cloud
Enterprise Energy Analytic Cloud Portal Frontend EETACP
WELCOME TO EETACP
EETACP User Accounts Login
Account Registration
NITDA

Fig 3: User interfaces on DCCN EETACP Application

This work will discuss the proposed DDoS mitigation response model against VBDDA considering the level of differentiation between normal and attack packets next. Some of the system assumptions made include:

1. The OpenFlow SPI device and server clusters for DCCN which is targeted by a DDoS attack (the victim nodeID) has the ability to detect or to be informed about the attack, based on an OpenFlow localized SPI detection scheme. The entire server upstream from the firewall up to the source(s) of the attack will never experience the ongoing threat.
2. The firewall device node will react by verifying and dropping DDoS packets which are probabilistically considered to be part of the attack while allowing normal flows.
3. The DDoS attack itself can produce buffer overflows and saturation of network resources such as CPU capacity, due to the inability of the nodes or routers to handle the resulting heavy packet traffic.

The SPI OpenFlow detection scheme is perfect, so that both detection failures and wrong packet droppings are impossible. Though imperfections could be possible both with regard to the detection of the DDoS attack as a whole, and the identification of the packets that belong to this attack. Thus, for any packet that flows in the network, the exact probability of correct identification as being an attacking packet, and a probability of wrong alarm must be considered. In this work, the DDoS attack packets will clearly identify and dropped while the normal or non-attacking packets will be correctly identified.

3.7 Analytical Model for DDoS Mitigation

This work formulated a mitigation model to analyze the impact of DDoS protection on the proposed EETACP DCCN performance using probabilities of active detection (DDoS attacks) and false detection (normal traffic). In the model, DDoS packet flows are identified with a degree of realistic probability and are smartly dropped. The layer 3 (network) packet network consists of *N* server nodes ***i_0, i_1, ……N.***

At any node *I,* the arrival traffic is the aggregate of normal valid flows. A possibility of invalid (DDoS) flows could be inclusive such that $n= (n_1, n_2, n_3,\ldots\ldots\ldots n_{j,}\ \ldots\ldots\ldots .n_l\ (n))$ and $d = (\ d_1,d_2,d_3\ldots\ldots\ldots dj,\ldots\ldots\ldots d_L(d))$ are the shortest distances/path followed by a normal and a DDoS flow respectively.

Let *L(n)* = the path length of flow n, and j denote the generic position of nodes inside the path. The total traffic rate λ_i arriving externally to node i is node composed of two realistic paths viz:

$$\lambda_i= \sum_n \lambda_{i,n}^n + \sum_d \lambda_{i,d}^d \tag{8}$$

Where

$\lambda_{i,n}^n$ is the normal non-DDoS incoming traffic rate belonging to normal flow n

$\lambda_{i,d}^d$ is the arrival rate of DDoS packets belonging to flow d.

Any traffic that node I perceives as DDoS traffic is dropped at the ingress point. Hence, a fractional degree f_{i_n} of normal traffic (probability of false detection) and a fraction of DDoS traffic d_{i_d} (probability of correct detection) will be dropped as it arrives to the SPI-OACI.

If the node's DDoS detection mechanism is perfect, $f_{i,_n} = 0$ and $d_{i_{,d}} = 1$.

Once a packet is admitted into SPI-OACI node, it is queued and forwarded based on its server destination address. Each server is modelled as a single server queue with service times s_i representing both the time taken to process the packet in the firewall node and the actual transmission dispatch time. The traffic intensity parameter ρ_i is then given by

$$\rho_i = \left[s_i \sum_n I_{i,n}^n\ (1-f_{i,_n})\right] + \left[\sum_d I_{i,d}^d\ (1-d_{i,_d})\right] \tag{9a}$$

Where for node I, $I_{i,n}^n$ is the arriving traffic rate of the normal flow n, and $I_{i,d}^d$is the traffic arriving rate of a DDoS flow d.

Since DDoS attacks will tend to dominate the SPI firewall or even the server node packet processing and dispatch capabilities, packets will be lost by the node with the probabilityL_i.

Assuming piossion arrivals for incoming traffic and let the buffer overflow Bf account for loss probability, this is then modelled using M/M/1 composite queue with finite buffer capacity [24]. The assumption of piossion arrivals, exponential piossion servers, and FIFO queue of limited capacity remains valid.

Using the expression in [28], the loss probability is obtained as

$$L_i= \rho_i^{\beta i}\ \frac{1-\rho_i}{1-\rho_i^{\beta i+1}} \tag{9b}$$

Where βi= Buffer size of the firewall node i

At this point, the following generalizations are deemed necessary in this modelling.

- Any traffic that is correctly or mistakenly thought to be DDoS traffic is dropped at the ingress point of the SPI device.
- Any traffic which effectively enters node ingress is precisely filtered and all droppings are independent.

Hence, the traffic equation for the cloud based network system is given by Equ 10.

$$I_{n_{j,n}}^n = \lambda_{n_{1,n}}^n \prod_{l=0}^{j-1}((1-L_{n_l}))\ (1-f_{n_{l,n}}))$$

$$I_{d_{j,d}}^d = \lambda_{d_{1,d}}^d \prod_{l=0}^{j-1}((1-L_{d_l}))\ (1-d_{d_{l,d}})) \tag{10}$$

Where L_{n_0}= L_{d_0} = $f_{n_{0,n}}$= $d_{d_{0,d}}$= 0

The above model characterizes the fact that, at the SPI firewall, an incoming packet may be dropped due to correct or mistaken identification as a DDoS packet or due to buffer overflow when the firewall node is overloaded. All the packets which enter the buffer queue successfully and are not dropped are eventually sent to the cloud backend server cluster nodes.

Equation 10 relates input rate arrivals to the node's buffer overflow or loss probabilities L_i which in turn depend on the traffic rates. Numerically. Equ. 10 could be obtained numerically via non-linear iteration.

Now, the good throughput G_i at node i is given by

$$G_i = \sum_n I_{i,n}^n \, (1 - L_{n_i}) \, (1 - f_{i_{,n}}) \qquad (11)$$

Equ. 11 is non-linear because the loss probabilities due to buffer overflows depends on the other flows from the network. The evaluation of the DDoS attack impact using various sizes of DDoS flows greater than 2500 packets/Sec as a distributed attack could be handled by the SPI OACI. These models were used in Section IV for the system implementation and analysis.

Figure 6 depicts the interfaces for legitimate users on the DCCN. The front end runs as EETACP http service via the internet web browser. The cloud broker and the cloud service coordinator are responsible for ensuring user to DCCN server cluster communication.

4. EXPERIMENTAL DESIGN

Discrete event modelling of the OpenFlow SPI-OACI based DCCN was implemented using Riverbed Modeller 17.5 [31]. The modeler software served as the tool for predicting, measuring, modelling, and analyzing the system performance. In the work, the performance of the DCCN cloud network was determined by network attributes that are affected by the various components such as network media, nodes, clients, servers, server applications. The modelling was based on the Discrete Event Modelling development cycle discussed in [32]. It involves capturing the system of interest, determining the entities and their attributes, defining the object statistics, establishing link consistence tests for the identified scenarios and running the simulation. Afterwards, the results are viewed and while carrying out evaluation on the trace files. The process took the previous discussion into account. The specification of the System of Interest (SoI), i.e. DCCN SPI-OACI was achieved with the cyber effect and attacker node library in Figure 4. On completion of the discrete event specification, model-checking is used to validate its properties. In this regard, after model-checking, the behaviour of system considering both normal and illegitimate traffic was analysed. Once satisfied with the simulation results, analysis of results was carried out.

As shown in Figure 4, the OpenFlow firewall comprises the time event generator and the set attribute blocksets of the Riverbed tool taking cognizance of Equs (8), (9) and (10). An in-coming traffic is decoupled to the SPI firewall (SPI-OACI device) with its look up table. This is the core of the threat mitigation. Recall that the foundation devices of DCCN are the Cisco Application Policy Infrastructure Controller (Cisco APIC), Cisco Nexus 9000 Series multilayer Switches and Cisco Application Virtual Switch (AVS). But the Cisco APIC in this work serves as a single point of automation and management in the DCCN. This allows for building fully automated and multi-tenant DCCN with scalability. In this work, the main function of Cisco APIC is to offer policy authority and resolution methods for the DCCN. A Cisco Nexus 9000 Series multilayer Switch connected to APIC was logically configured for firewalling the DCCN servers.

A characterization of the Cisco 9000 router firewall as an embedded network device with support for Virtual DDoS protection was considered in the DCCN threat mitigation strategy shown in Fig 4. In this case, the clients connect to the client gateway on a separate VLAN network interfaces (AVS). The SPI-OACI firewall from Nexus 9000 was placed adjacent to the client gateway which facilitates on-demand protection on the backend server systems. This was positioned so as to concurrently protect multiple potential LAN server network cluster and WAN bandwidth.

For the security QoS profiling, the system response metrics (i.e. SPI-OACI delay, throughput and utilization) in cloud based network will be analyzed. Using the models outlined above for the composite DDoS attack, different situations were examined. The purpose of the QoS profiling via a DDOS experiments was to distinguish the influence of different attack properties on the success of the DDoS attack and how the SPI firewall can normalize the attack scenario and protect the DCCN.

For the analysis of simulation experiments, standard situation parameters were chosen as detailed in Table 1 whose parameter are derived from [20] while implementing the system using Riverbed Modeller version 17.5 [32]. From Table 1, the analysis of the network leveraged the following phases considering known vulnerabilities:

i. Capture packet traces when the DCCN http service is running normally to build a baseline for QoS study. These traces are captured using the application characterization environment in riverbed Modeller.
ii. Importing the capture files to create a representation of the application's transactions called an application task for further analysis.
iii. After creating the application task, the following operations are carried out over the captured traffic traces:

- Viewing and editing the captured packet traces on different windows.
- Performing application level analysis by measuring the components of the QoS metrics in terms of throughput, delay and utilization.

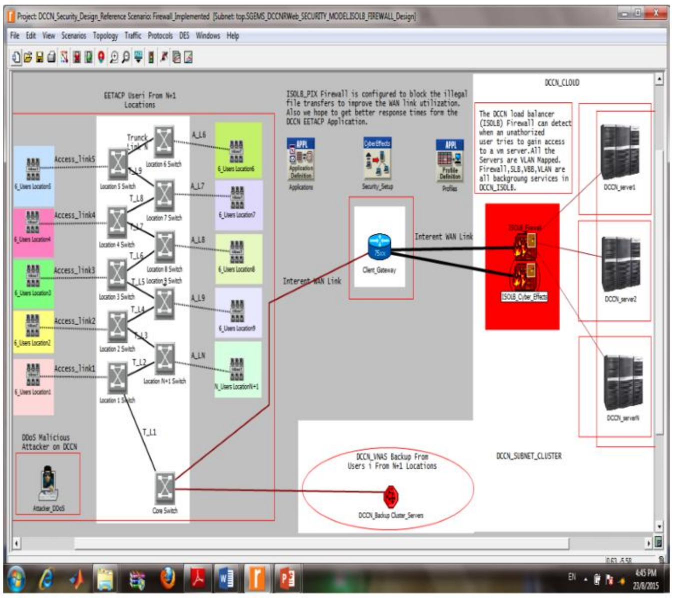
Table 1: Experimental design Parameters [20]

SN	Parameters	Specifications
1	No of Attacks	3 [From DDoS Attacker]

2	Attack Profile	2(Infect &Confirm);
		Decrease IP forward rate;
		Increase IP Forward rate

3	Start time	Uniform
4	Local Scripts	Nil
5	Remedies	SPI-OACI (Scan &Clean all)
6	Model	Cyber-Ethernt4-Slip8-gtwy-adv (Cisco 9000)
7	Name	ISOLB-Cyber Effects
8	No of Users	Init =600,Final =N+1
9	Location Map	Access link =10, Final = N+1;

		Truck link =10
10	No of Switch	12
11	No of Servers	9 with 20 Mbps normal traffic (100 queries per second by 200 bits in each).
12	No of Client gateway	1 (75xxxxxxx Series)
13	No of backup sites	1
14	Attack Traffic	10 Mbps attack traffic (50000 queries per second by 200 bits in each).
15	Bandwidth	2 Channels with 100 Mbps bandwidth each;
16	SPI firewall Filter	Uses filter that filter VBDDA attack via DDoS and DRDoS queries.
17	Query Time	Legitimate query takes 200 ms to execute
18	Attack Query	Execution takes 2000 ms.
19	Firewall Type	Cisco 9000 router firewall
20	SPI firewall buffer capacity	2500 and can hold information of 50 connections.



Project: DCCN_Security_Design_Reference Scenario: Firewall_Implemented [Subnet: top.SGEMS_DCCNRWeb_SECURITY_MODEL.ISOLB_FIREWALL_Design]

ISOLB_PIX Firewall is configured to block the illegal file transfers to improve the WAN link utilization. Also we hope to get better response times form the DCCN EETACP Application.

The DCCN load balancer (ISOLB) Firewall can detect when an unathorized user tries to gain access to a vm server.All the Servers are VLAN Mapped. Firewall,SLB,VBB,VLAN are all backgroung services in DCCN_ISOLB.

Fig 4: DCCN Security Testbed

5. DISCUSSION AND RESULT ANALYSIS

From Figure 4, the analysis focused on the security QoS profiling given the possibility of VBDDA in DCCN. The SPI-OACI proposal in this work has similar security implication to the OpenFlow security appliance initiative for forensic spyware robots in [34]. Though the concern in this work is the security vulnerability in layer 3. In the validation phase of this work, a comparative study was focused on both normal and illegitimate traffic flow via SPI-OACI into the DCCN server cluster. The SPI-OACI firewall device was actively used to check for VBDDA, memory attacks, as well as legitimate traffic flows. The intent is to form an initial baseline for a comparative evaluation. After developing Figure 7, some selected network QoS metrics were evaluated to ascertain the influence of the SPI-OACI procedure However, the difficulty of carrying out an exhaustive set of experiments in real environments, involving production DCCN servers and real traffic must be noted at this point. This fact, together with the exhibited performance by current simulation tool, gives way to accepting DEVS software tool as valid framework for experimentation. The DCCN security evaluation considered both vulnerable or attackers DDoS traffic and legitimate traffic as depicted in Figure 4. In this case, the work introduced a two case scenario for SPI-OACI firewall and non SPI-OACI firewall implementations. Figure 5 explained the DCCN security influence on link utilization under active usage.

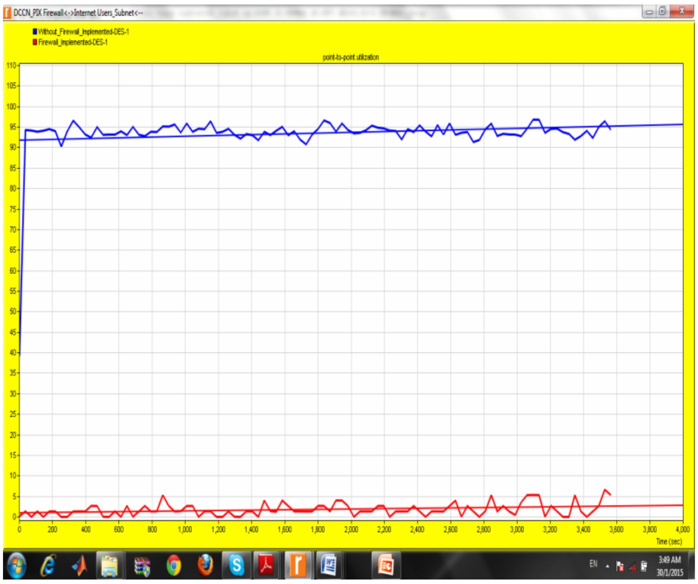


Fig 5: A Plot of DCCN SPI-OACI Point to Point Utilization of WAN Link

Recall that Recall that the EETACP application on the server was emulated with a heavy http service in the Modeller environment. As observed in the OpenFlow firewall design, the low utilization (**5%**) of the link was as a result of the activity of OpenFlow firewall that blocks unauthorized activities on the DCCN, thereby facilitating lower bandwidth link utilization as shown in Figure 5. This is not the case, when the SPI-OACI firewall was isolated. It was observed that the utilization was very high (**95%**) in a scenario without OpenFlow firewall. This is as a result of the non-monitoring or filtering of unauthorized user activities which constitute a major drain on the network link, thereby causing the system to have a very high utilization response. As such, for an improved performance of the DCCN, the need for a Pix firewall is very indispensable. Figure 6 shows the DCCN security influence on query response time. As expected, the presence of the Pix firewall improved the database (DB) response time by **12.4%.** This demonstrated that with lower link utilization, the average delay on the link will be lower also.

By isolating the firewall device, the response time delay of 87.06% was observed. This is very high, implying that malicious activities as well as unnecessary transaction on the network will increase the system delay and adversely affect the network performance.

From the DCCN security analysis, it could be deduced that low link resource utilization will result to high resource conservation (processor, memory, I/Os, disk, etc.) while a high link resource utilization will result to low resource conservation. The discrete event methodology used, assesses the performance of DCCN firewall under VBDDA. In this case, the DCCN OpenFlow firewall is shown as an effective security strategy for the proposed DCCN as represented in Figure 7.

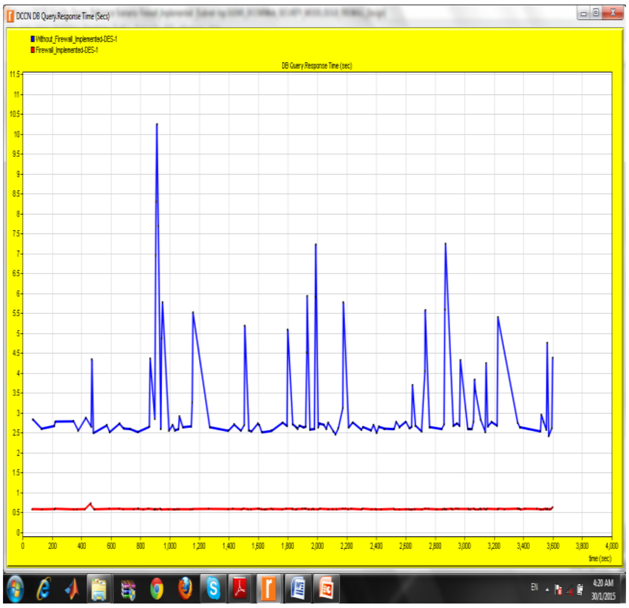


Fig 6: Plot of DCCN SPI-OACI Firewall Response times

Fig 7: Experimental DCCN EETACP Server Testbed

6. CONCLUSION

This paper has dealt with security QoS metrics of a DCCN which is the network support of Smart Green Energy Management System (SGEMS). In the work, traffic flow into DCCN cloud network system could be hijacked by attackers. The VBDDA executed by malicious cyber criminals collapse an entire network setup. In this regard, bandwidth exhaustion, memory depletion, CPU power drain and application crashing were the identified DDoS strategies that could be used by these cyber terrorist to halt the operation of an enterprise system such as SGEMS. In the proposed DCCN, Stateful Packet Inspection based on OpenFlow Application Configuration Infrastructure firewall scheme was presented as a comprehensive solution. Mathematical characterization of the VBDDA and DDoS mitigation procedure were discussed. Using Cisco Nexus 9000 firewall as an embedded network device, the security QoS metrics under protective and non-protective firewalls were analyzed. It was concluded that the absence of a robust security firewall technology can adversely affect the network QoS and expose the SGEMS DCCN to various forms of DoS attacks. It was concluded that with a robust firewall in place, VBDDA will be mitigated in DCCN infrastructure.

In conclusion, the Open Flow virtual Appliance research, AIRMS and the current Spine leaf DCNs will benefit immensely from the deployment of Cisco Application Policy Infrastructure Controller (Cisco APIC), Cisco Nexus 9000 Series multilayer Switches and Cisco Application Virtual Switch (AVS) infrastructures as these facilitates satisfactory QoS provisioning, scalability and security in distributed cloud based networks.

7. ACKNOWLEDGMENTS

This research was carried out as an extended work on Distributed Cloud Computing Network for SGEMS EETACP project commissioned by the Department of Electronic Engineering, University of Nigeria Nsukka. This paper has been partly presented at the IEEE CyberAbuja, 2015, conference in Nigeria. A modification was made in the context of DCCN as against the AIRMS context and Spyware robot.

8. REFERENCES

[1] W.Dou, Q.Chen, J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment", Future Generation Computer Systems 29 (2013) 1838–1850, Elsevier SciVerse ScienceDirect

[2] T. Peng, C. Leckie, K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems, ACM Comput. Surv. 39 (1) (2007) 3.

[3] White paper-How to prevent DDOS attacks in a Service Provider Environment, Available Online: http://www.reply.eu/Documents/10943_img_SYTR12_Prevent_DDoS_attacks.pdf,Retrived 23rd, August, 2015

[4] K.C. Okafor, F.N.Ugwoke, Obayi.I A.A, O.U Oparaku,"The Impact of Distributed Cloud Computing Initiatives (DCCI) on Green Energy Management Using Cronbach's Alpha Test", International Journal of Advanced Scientific and Technical Research, India. Issue 4, Volume 4, July-August 2014, Pp.853-865. Available online on http://www.rspublication.com/ijst/index.html ISSN 2249-9954.

[5] A. Chonka, J. Singh, W. Zhou, Chaos theory based detection against network mimicking DDoS attacks, IEEE Commun. Lett. 13 (9) (2009) 717–719.

[6] H. Liu, M.S. Kim, Real-time detection of stealthy DDoS attacks using timeseries decomposition, in: Communications (ICC), 2010 IEEE International Conference, 2010.

[7] Y. Kim, W.C. Lau, M.C. Chuah, H.J. Chao, Packetscore: a statistics-based packet filtering scheme against distributed denial-of-service attacks, IEEE Trans. Dependable Secure Comput. 3 (2) (2006) 141–155.

[8] F. Soldo, A. Markopoulou, K. Argyraki, Optimal filtering of source address prefixes: models and algorithms, in: Proc. IEEE INFOCOM, 2009.

[9] M.T. Goodrich, Probabilistic packet marking for large-scale IP traceback, IEEE/ACM Trans. Netw. 16 (1) (2008) 15–24.

[10] S. Yu, W. Zhou, R. Doss, W. Jia, Traceback of DDoS attacks using entropy variations, IEEE Trans. Parallel Distrib. Syst. 22 (3) (2011) 412–425.

[11] Mehmud Abliz, Internet Denial of Service Attacks and Defense Mechanisms", University of Pittsburgh Technical Report, No. TR-11-178, March 2011, Pages 1-50.

[12] P. Gasti, G. Tsudik, E. Uzun, L. Zhang, "DoS & DDoS in Named-Data Networking",

[13] F.N.Ugwoke, K.C.Okafor, V.C.Chijindu, "Security QoS Profiling against Cyber Terrorism in Airport Network Systems", To appear in the 6th IEEE Cyber Abuja Conference, Abuja, Nigeria, 23-24 Nov.2015.

[14] H. Ballani, P. Francis, and X. Zhang. A Study of Prefix Hijacking and Interception in the Internet. SIGCOMM Comput. Commun. Rev., 37(4):265–276, August 2007.

[15] M. Lad, D.Massey, D. Pei, Y.Wu, B.Zhang, L. Zhang. Phas: a prefix hijack alert system. USENIX Security, August 2006.

[16] D.Dagon, M. Antonakakis, K.Day, X.Luo, C.P. Lee, and W. Lee. Recursive DNS architectures and vulnerability implications. In Network and Distributed System Security Symposium (NDSS09), 2009.

[17] The DNSSEC Protocol. http://tools.ietf.org/html/rfc2535.

[18] G. Loukas, "Defence Against Denial of Service in Self-Aware Networks", PhD thesis, Intelligent Systems and Networks Group Dept. of Electrical & Electronic Engineering Imperial College London.

[19] B.Kurar , R.Tahboub, "Internet Scale DoS Attacks", In International Journal of Applied Mathematics ,Electronics and Computers, IJAMEC, 2015, 3(2), Pp.83–89.

[20] G.M.Fernández, J. E. Díaz-Verdejo, and PG.Teodoro, "Mathematical Model for Low-Rate DoS Attacks Against Application Servers", IEEE Transactions On Information Forensics And Security, Vol. 4, No. 3, September 2009, Pp.519-529. DOI: 10.1109/TIFS.2009.2024719 · Source: IEEE Xplore

[21] S.S. Chowriwar ,M.S. Mool, P.P.Sabale, S.S. Parpelli, N.Sambhe, "Mitigating Denial-of-Service Attacks Using Secure Service Overlay Model", International Journal of Engineering Trends and Technology (IJETT) – Volume 8 Number 9- Feb 2014.

[22] SimonaRamanauskaitė, Antanas Čenys, "Composite Dos Attack Model", System Engineering, Computer Technology, 2012 4(1): 20–26 doi:10.3846/mla.2011.05 Pp.20126

[23] Cisco IOS Firewall Design Guide, 2005, Cisco Systems Inc

[24] Huang, Q.; Kobayashi, H.; Liu, B. 2003a. Analysis of a new form of distributed denial of service attack, in Conference of Information Science and Systems. The Johns Hopkins University, 2003, March 12–14.

[25] K.C.Okafor "A Model for Smart Green Energy Management Using Distributed Cloud Computing Network", Ph.D. Thesis, Dept. of Electronic Engineering, University of Nigeria Nsukka, 2015.

[26] Specht, S. M.; Lee, R. B, "Distributed denial of service: Taxonomies of attacks, tools and countermeasures", in International Conference Parallel and Distributed Computing Dydtems. San Francisco, 2004, 15–17.

[27] Ramanauskaitė, S., "Modeling of SYN flooding attacks", Jaunųjųmoks lininkųdarbai 2010, 26(1), 331–335.

[28] Online: https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

[29] Online: http://www.arbornetworks.com/.

[30] Cisco Application Centric Infrastructure May 2014, Cisco Systems Inc.

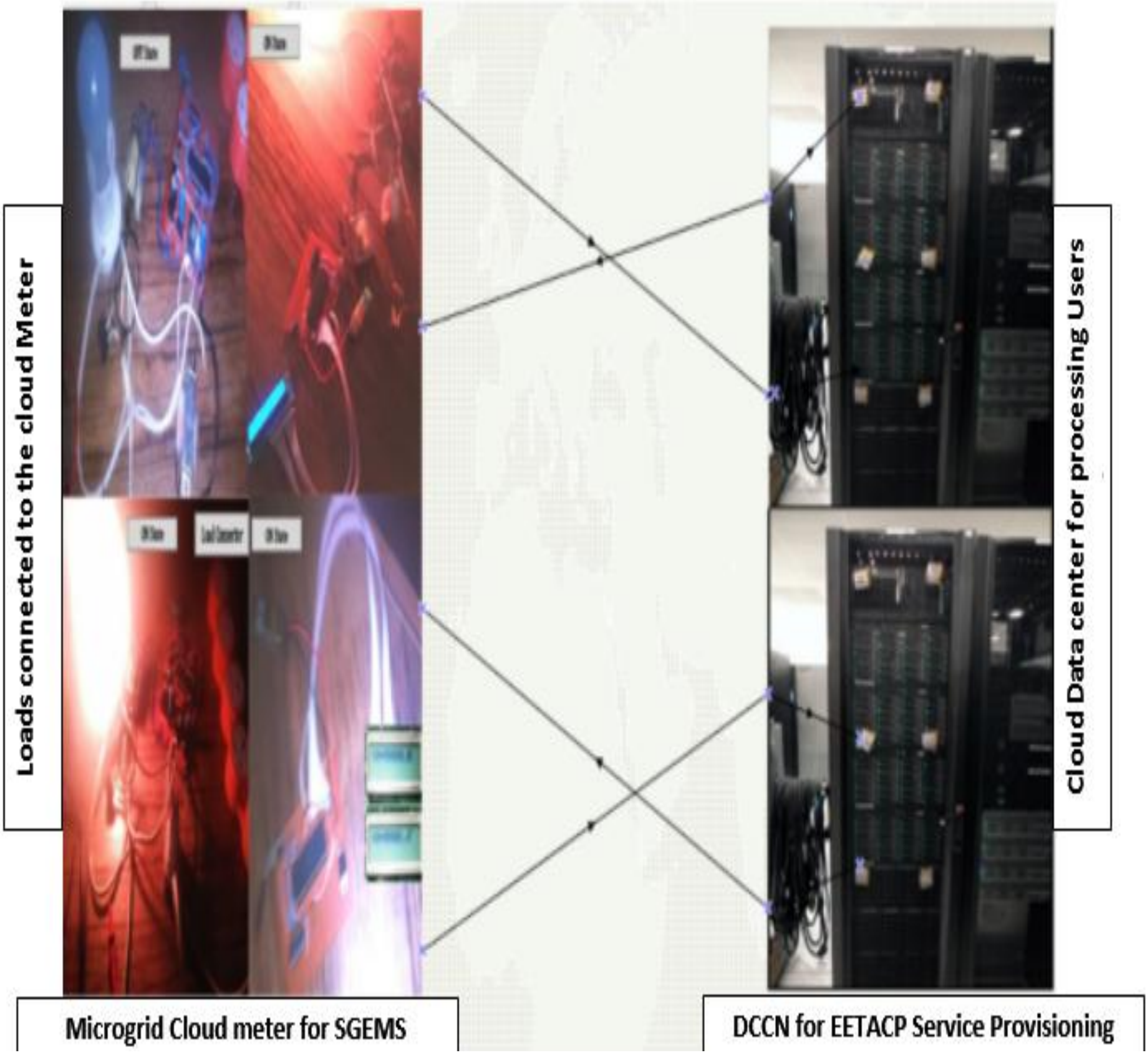
[31] Riverbed Modeler Academic Edition release17.5 PL6.https://splash.riverbed.com/.../riverbed-modeller academic- edition-release, June 11, 2014.

[32] C.C. Udeze, K.C. Okafor, & C.C. Okezie, "MATLAB SimEvent: A Process Model Approach for Event-Based Communication Network Design (A Case for Reengineered DCN)", Journal of Basic and Applied Sciences, 2(5), (2012), 5070–5080.

[33] http://www.colasoft.com/capsa/network_bandwidth_analyzer.php. Retrieved, 9th August, 2015.

[34] I.E. Achumba, K.C, Okafor, G.N.Ezeh, U.Diala, "OpenFlow Virtual Appliance: An Efficient Security Interface for Cloud Forensic Spyware Robot" In International Journal of Digital Crime and Forensics (IJDCF), July 2015, Vol. 7, No. 2, Pp.31-52., USA

9. APPENDIX 1: COMPLETE SGEM/DCCN EETACP PROJECT


Loads connected to the cloud Meter
Cloud Data center for processing Users
Microgrid Cloud meter for SGEMS
DCCN for EETACP Service Provisioning