Security QoS Profiling Against Cyber Terrorism in Airport Network Systems

F.N.Ugwoke[1], K.C.Okafor[2], V.C.Chijindu[3]
[1]Dept. of Computer Science, Michael Okpara University of Agriculture, Umudike, Umuahia, Nigeria
[2]Dept. of Electrical Electronic Engineering, Federal University of Technology, Owerri, FUTO, Nigeria
[3]Dept. of Electronic Engineering, University of Nigeria, Nsukka, Nigeria
[1]ndidi.ugwoke@gmail.com, [2]kennedy.okafor@futo.edu.ng, vincent.chijindu@unn.edu.ng

***Abstract*—Attacks on airport information network services in the form of Denial of Service (DoS), Distributed DoS (DDoS), and hijacking are the most effective schemes mostly explored by cyber terrorists in the aviation industry running Mission Critical Services (MCSs).This work presentsa case for Airport Information Resource Management Systems(AIRMS) which is a cloud based platform proposed for the Nigerian aviation industry. Granting that AIRMS is susceptible to DoS attacks, there is needed to develop a robust counter security network model aimed at pre-empting such attacks and subsequently mitigating the vulnerability in such network. Existing works in literature regarding cyber security DoS and other schemes have not explored embedded Stateful Packet Inspection (SPI) based on OpenFlow Application Centric Infrastructure (OACI) for securing critical network assets. As such, SPI-OACI was proposed to address the challenge of Vulnerability Bandwidth DepletionDDoS Attacks (VBDDA). A characterization of the Cisco 9000 router firewall as an embedded network device with support for Virtual DDoS protection was carried out in the AIRMS threat mitigation design. Afterwards, the mitigation procedure and the initial phase of the design with Riverbed modeller software realized. For the security Quality of Service (QoS) profiling, the system response metrics (i.e.SPI-OACI delay, throughput and utilization) in cloud based network were analysed only for normal traffic flows. The work concludes by offering practical suggestion for securing similar enterprise management systems running on cloud infrastructure against cyber terrorists.**

Keywords—Attacks; Cloud Datacenters; DoS; DDoS; Vulnerabilities; AIRMS; Mitigation Techniques; Aviation Industry)

II. INTRODUCTION

As the human population grows, malicious cyber-criminals grow in a proportional status. These entities tend to launch attacks for various reasons yet to be justified. With respect to post September 9/11 attack, the United States aviation security Transportation Security Administration (TSA) has placed focus on security checkpoints and unearthing potential threats through bomb-sniffing technology, terrorist watch lists, increased use of in-flight security officers, full-body-scanners, behavioral detection officers, positive baggage matching, and hardened cockpit doors [1], [2]. More so, a variety of airport security techniques are currently available, and more are at the developmental stage. The most popular security schemes on aviation systems architectures includes: Intruder Detection Systems (IDS), Biometrics, Enhanced Body Scanners (EBS), X-ray technologies, Smart Phone Applications (SPAs), blackholing, router filtering, and firewalls.Because sophisticated DDoS attacks are defined byanomalous behaviour at layers 3 and 4, existing approaches are not optimized for DDoS detection or mitigation as they are not reliable, cost effective, and scalable.

Again, the technological components of aviation security systems such as biometrics and access control, flight tracking and information display systems (FIDS), Air Traffic Control (ATC), passenger screening, baggage tracking and inspection, networks and web Services and radio communication [3] have gained strong advocacy in the past with still various degree of inefficiencies. Since airport information systems infrastructures could be complex and are derived from a seemingly untraceable number of sources, by developing an intelligent cloud based network infrastructure, a mitigating technique for dealing with DoS attack will ensure that the AIRMS is undisrupted.

Hence, this work adopted Application Centric Infrastructure (ACI) which supports 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. This research is still ongoing, but the intended contributions are as follows:

i. To use SPI-OACI for the AIRMS cloud based network while carrying out the security QoS profiling using selected metrics.
ii. To develop the vulnerability bandwidth and memory attack model for the cloud based AIRMS network.

This paper will only address the above while providing the roadmap for future work. The rest of the paper is organized as follows. Section II; focus on threat dimensions, and airport security models/architectures. In Section III; a description of the airport network model was made. Also, characterization of Vulnerability Bandwidth Depletion DDoS Attack (VBDDA), SPI-OACI security architectural components, and SPI-OACI DDoS mitigation procedure were presented. Section IV presented the system design detailing the experimental setup and results analysis. Section V; presents the conclusions, recommendations and future work.

III. RELATED WORKS

A. *Threats Dimensions*

Globally, threats such as nuclear, biological and chemical attacks exist [4]. However; these physical threats are not the only security challenges facing the Nigeria. At large, everybody is concerned with the emerging technological threats to critical cyberspace infrastructures. With the globalization incidence, the Nigerian government is now tending towards the use of e-governance i.e. using interconnected computer systems to manage public services such as smart cities, smart grid energy systems, coordinate public transportation logistics, e-payment systems, and leverage similar technologies for a variety of services that will promote economic growth for the huge populace.

However, a state-sponsored attack could be launched to either deny certain services, steal information, or to take control and hijack such system. In the aviation context, this is referred to as cyber terrorism. For Instance, on June 22, 2015, hackers forced polish airline to cancel flights and this adversely affected the 1400 passengers [5]. Similarly, for the past two years, a team of Iranian hackers has compromised computers and networks belonging to more than 50 organizations from 16 countries, including airlines, defense contractors, universities, military installations, and hospitals. The hackers used common SQL injection, spear phishing or watering hole attacks to gain initial access to one or more computers of a targeted organization. They then used privilege escalation exploits and other tools to compromise additional systems and move deeper inside its network [6]. The aviation network systems if not well secured will suffer from emerging attacks and threats.

The author in [7] outlined the cyber security threats facing airports and revealed the potential vectors that might be used in an attack as well as the tactics for securing known vulnerabilities. It was noted that several threats could be focused on external airport operations, such as external airport or airline websites, concession point-of-sale, credit card transaction information, and passenger's wireless devices. However, the overall impact of cyber attacks on systems external to airport operations is little when compared to attacks on systems required to perform internal airport operations.

In this context, the potential targets within an airport internal network include: access control and perimeter intrusion systems, e-Enabled aircraft systems, radar systems, wireless and wired network systems, and network-enabled baggage systems [7].Unfortunately, a variety of vulnerabilities occur within cyberspace because of humans, hardware, software, and connection points that provide access to such systems. The United States Computer Emergency Readiness Team (US-CERT) [8] has provided a high level overview of cyber vulnerabilities for control systems. These include the following vulnerabilities: wireless access points, network access points, unsecured SQL databases, poorly configured firewalls, interconnected peer networks with weak security, and several others.

Similarly, the National Institute of Standards and Technology (NIST) [9] has published a guide called Risk Management Guide for Information Technology Systems which shows a multi-step system analysis which network experts can use to assess network vulnerabilities, measure the potential of each vulnerability occurring with respect to the threat's source, motivation, and actions, whilst developing recommendations and documentation to counteract the vulnerabilities found within the assessment. In their report, vulnerabilities from the perspective of the potential consequence(s) of an exploited vulnerability is presented in three folds: loss of integrity, loss of availability, and loss of confidentiality. Loss of integrity occurs when access is gained and one can no longer guarantee that data has not been modified. Loss of availability occurs when a system is no longer operational or loses effectiveness.

Finally, loss of confidentiality "refers to the protection of information from authorized disclosure. Furthermore, NIST provides three levels to measure vulnerabilities: high, medium, and low. Ultimately, the assessment in [7] which is similar in nature to [8] and [9], settles on four components within an airport that are vulnerable to cyber attack. They include: the network, the device, the application, and the back-end system. Each of these requires a different approach to security. But by focusing on process, culture, staffing, and training, security of such systems can be guaranteed [10].

B. *Related Research Efforts*

Various works in the context of threats and attacks in airport security are reviewed in this section. The intent is to ascertain the extent of security research in AIRMS as well as the computing networks.

- *Airport Security Models/Architecture*

A selected highlight of works on Airport Transport management systems, security, frameworks and models is presented below. In [11], the authors presented a risk-based Airport model that consists of 5A's (Accounting, Authorization, Authentication, Auditing and Administration). Case study approach was used while an application method of the risk-based Airport model to the cyber security environment. This paper in [12] focused on key Airside Management Information Systems (AMIS) which could be used to facilitate the airport and airline operations. These are required to process aircraft, passengers, and air cargo. They involve the ticketing of air travelers, ground movement of aircraft and vehicles, flight procedures of aircraft within airport airspace, and scheduling and managing of boarding and gate equipment, and weather updates. Their AMIS proposal covered include: Gate Management System, Aircraft Fuelling System, Air Traffic Control (ATC) System, Weather Monitoring System, Airfield Lighting System, and Automatic Vehicle Identification (AVI) System. This study used naturalistic inquiry to elicit data related to the classification and use of AMIS. In [13], the author proposed a violation and vulnerability diagram of a cyber-exercise scenario based on Air Traffic Management infrastructures (ATM) incidents and showed how Vulnerability and Violation (V2) diagrams can identify interactions between malware and degraded modes of operation. Their initial results revealed the underlying

vulnerabilities that exist across safety-critical transportation infrastructures.

In [14], the authors discussed the US FAA's National Airspace System (NAS) model, and summarize the need, background, ongoing developments and research efforts on cyber-security standards and best practices at U.S. airports with special emphasis on cyber security education and literacy.Cyber Threats to Internal Airport Operations and related vulnerabilities were also presented.

The whitepaper in [15] presented an introduction to cyber security in air traffic management, including the cyber threats and risks and motives of threat actors, as well as some considerations to managing cyber risks and implementing a cyber security programme. In addition, the ATM information standards, framework for cyber security, and some practical guidance to conducting a cyber risk assessment and managing the cyber security risks to systems, assets, data and capabilities in ATM were detailed.

- *Existing DoS Attack Models*

In this section, a concise explanation of DDoS is given with the review on various research efforts. A denial of service (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. In context, DDoS attacker attempts to prevent legitimate administrators from accessing information or services. By targeting the AIRMS (computers and its network connection), an attacker may be able to prevent access from the airport application services that rely on the affected computer network. 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.

The work in [16] proposed self-aware networks and a defense against denial of service 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, witha mathematical model which can measure the impact of both attack and defense on the performance of a network were presented. The work was validated with simulation results and experimental measurements in a SAN environment.

In [17], 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 were discussed as shown in figure 1. The work detailed the classifications as well as the application domain. In [18], 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 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 [19], secure overlay services (SOS) architecture was proposed to provide reliable communication betweenclients 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. Their proposed SOS architecture that proactively prevents denial of service (DoS) attacks, which works toward supporting emergency services. Their goalwas is to allow communication between a confirmed user and a target.

Similarly, the work in [20] 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 were an incoming traffic is blocked because of insufficient bandwidth. In this case, the remaining part of traffic can be blocked by its filtering system. This is efficiently carried out using the proposed SPI OACI. This will also block anything left after filtering by creating an insufficient place in the buffer devoted to store open connections for the cyber attackers.

Apart from the generalized DoS classification given in Fig1, a comprehensive cyber-based threat to Air Traffic Management is shown in Fig 2. The Possible DDoS traffic types include: HTTP Header, HTTP POST Flood, HTTP POST Request, HTTPS Post Flood, HTTPS POST Request, HTTPS GET Flood, HTTPS GET Request, HTTP GET Flood, HTTP GET Request SYN Flood (TCP/SYN), UDP Flood, ICMP Flood, MAC Flood.

However, there two identified mitigation approaches for any large scale DoS/DDoS attacks, viz:

- Using firewall device at layer 4 and 7. This can be optimized for flow and deep inspections. In this case, the DoS protections include: Screen, session limits, and SynCookie.
- Using Router device at layer 3 and 4. This can be optimized for packet inspection and flow inspection. In this case, the DoS protections include: Line-rate ACLs, and Tare Limits.

This work combines the effectiveness of both approaches to offer an efficient security solution for AIRMS. By addressing the above attacks, bandwidth depletion and memory exhaustion in the network infrastructure is eradicated.

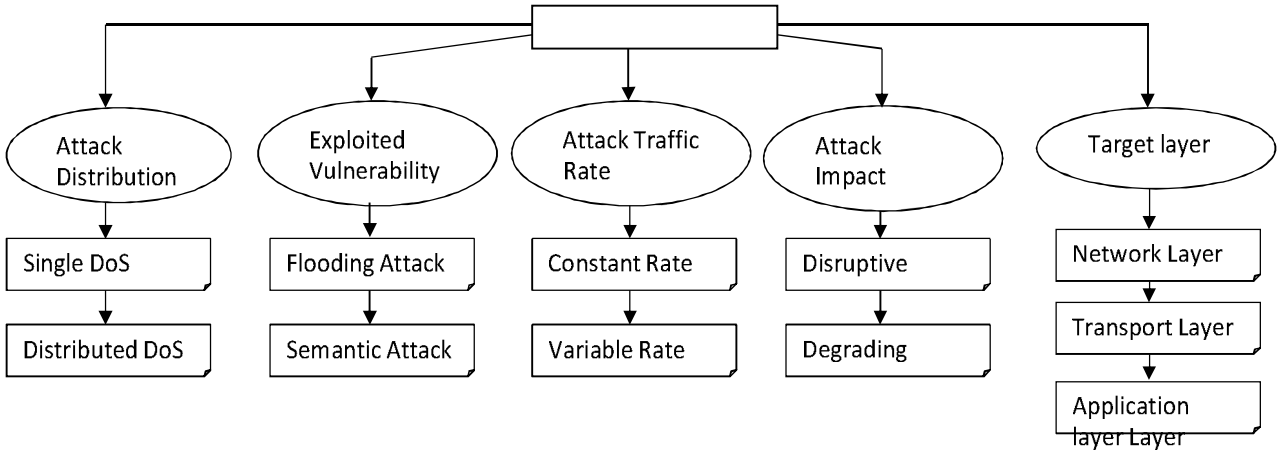

Fig. 1: DoS Attack Classification [17]

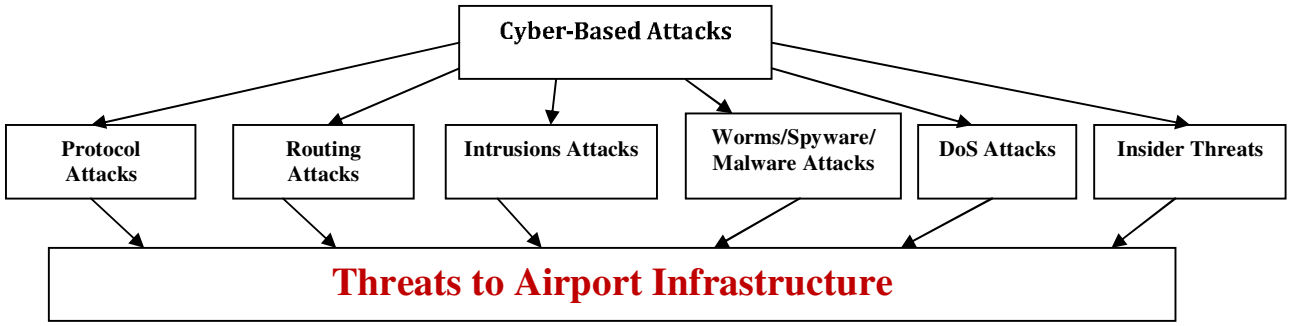

Fig. 2: Cyber-Based threats to Airports [21]

Other works on threats and attacks with emphasis on evaluation analysis of DoS traffic have been studied in [22],[23]. Existing works in literature regarding cyber security DoS and other schemes have not explored embedded Stateful Packet Inspection (SPI) based on OpenFlow Application Centric Infrastructure (OACI) for securing critical network architecture. This work seeks to address this research gap.

IV. Proposed AIRMS Network Model

Generally, many security algorithm computations exhibit a trade off between execution time and quality of service. For example, a firewall SPI OACI encoder can often track packets more quickly if proper configuration is made to drop only illegitimate traffic. This is generally summarized as Deep Packet Flow Inspection (DPFI) shown in Fig 3. All the network traffic inputs into the SPI-OACI processing are mapped into a clean vector $A_{gm.}$

This ensures that the monitoring servers are well secured.

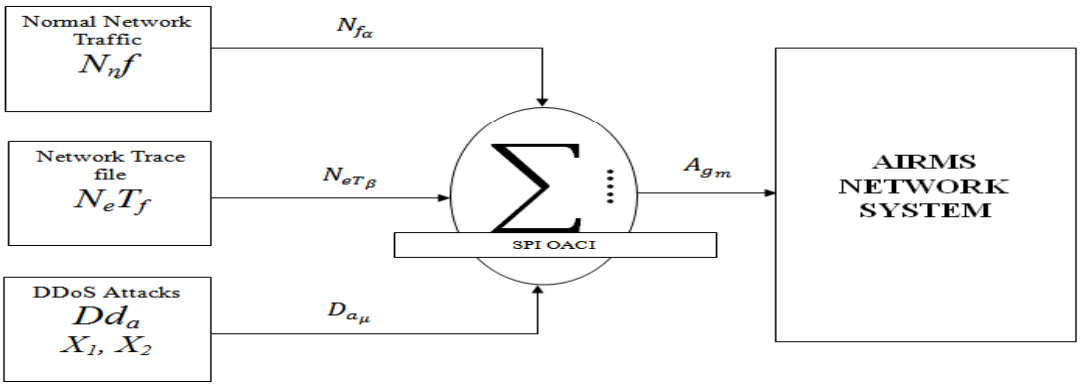

Fig. 3: Proposed System Architecture of cloud based Airport System

Fig 3 shows the proposed airport management system with information flowing between interacting systems via an SPI-OACI firewall. The management system runs on a cloud environment. The infrastructures and platforms supporting the AIRMS are interfaced on the cloud. The use of airport backend servers and high end monitoring servers via the airport fixed wireless infrastructure is shown in the proposed architecture. Also, maintenance services inside and outside the airport systems are enabled via e-devices. The security enforcement must find optimizations that appropriately balance quality of service and performance of the cloud network.

It must be stated that theproposed system architecture of cloud based airport system as shown in Fig 3 evolved from an initial work carried out in Distributed Cloud Computing Network (DCCN) [24]. The major issue investigated in context is the security layout of traffic flow into the AIRMS perimeter of defencewhere malicious attackers seek to hijack the AIRMS via DDoS attacks.This paper will present Vulnerability Bandwidth Depletion DoS Attack (VBDDA) characterizations that will facilitate QoS profiling with ease. This will help security designers and network architect to identify promising optimization benchmarks in such networks.

Interestingly, cyber terrorists represented by the attackers (see Fig 3) have the sole aim of exploiting the AIRMS via the backend servers. In this regard, an introduction of optimal allocation usingstateful Packet Inspection implemented in Cisco IOS firewall [25] will suffice. Some of the functions of the SPI include:

i. It provides a per-application control mechanism across network perimeters,as well as within networks through the Transparent Firewall capability. The SPI sets precedence for Context-Based Access Control (CBAC) which improves Access Control List (ACL) immensely.

ii. It enhances security for TCP and UDP applications by scrutinizing several attributes of data connection. The inspection enginetracks the state and context of network connections to secure traffic flow.

iii. It protects against packet-injection attacks by checking several components of TCP and UDP sessions. Source and destination IP address and port numbers must match, as well as TCP sequence number. Other attributes are checked as well, such as TCP window size, reducing the likelihood of buffer overrun attacks.

iv. It provides support for several complex, advanced services such as streaming protocols, IP voice, and other complex services that require detailed scrutiny to support additional data and media channels.

v. It provides DoS detection and prevention against some popular attack modes, such as SYN (synchronize/start) flooding, portscans, and packet injection.

From Fig. 3, when the SPI firewall detects unusually high rates of new connections, it issues an alert message, and resets excessive half open TCP connections to prevent system resource depletion. It tracks connections by destination address and port pairs to control undesired activity and reduce impact on hosts on the protected network that are under attack from malicious activity originating outside the firewall. Essentially, the SPI monitors several attributes in TCP connections, UDP sessions,

and Internet Control Message Protocol (ICMP) dialogue to ensure that the only traffic allowed through a firewall ACL is the return traffic for dialogue that was originated on the private side of the firewall. The OpenFlow ACI [26] is now the state of art for large scale configurations. This work opines that DoS and DDoS attacks just as in [20] can be modeled at the session rather than at the package level. Using Poisson process with arrival rate to characterize this scenario gives a better platform to study DoS types and their mitigation approach.

A. *Characterization of Vulnerability Bandwidth Depletion DoS Attack (VBDDA)*

Now, a Vulnerability Bandwidth DepletionDDoS Attack (VBDDA) could occur when an attacker $X_n$consumes all available bandwidth in Fig 3by generating a large number of packets directed to the cloud based network. ICMP ECHO packets or disruptive malware could be used. This could also result from an attacker comprising any vulnerable system and using it to launch an attack to the compute server center.

The properties of an attack could be used to ascertain its effect on QoS. While the work in [20] presented a mathematical expression of calculating the success of DoS attack using theknown data on the attacks, normal flow and other properties of the victim this work models the security QoS metrics using the SPI OACI approach. When a DDoS resource depletion attacks occurs, this will facilitate an attacker sending packets that misuse network protocol communications or sending malformed packets that tie up network resources sothat 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 Engest loss model G(N)/G/m(0) [27], this helps to estimate the success of the SYN flooding attackwhen average attack flow, the average storage time of open-state connections and buffer size areknown. This work considered a bandwidth exhaustion and memory depletion contexts which basically allows fractional analysis of every DoS or DDoSattack.

Considering Fig. 3, when analyzing a DDoS attack, vulnerability bandwidth and memory depletion DDoS models as well as for the SPI OACI filtering properties of the system are very vital. Incoming illegitimate traffic can be blocked because of insufficient bandwidth configured in SPI OACI while correctly filtering a legitimate packet. Anything left after filtering can be blocked by an insufficient place in the buffer devoted to store open connections. Let SPI OACI bandwidth exhaustion probability be given as B_p,the probability of filtering legitimate traffic as Fn_P and memory depletion probability as M_P. A stateful attack probability 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 [20]:

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

For estimating bandwidth exhaustion probability Bb_P in SPI OACI, the use of stochastic bandwidth exhaustion model was adopted [28] which is given by

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

Where

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

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

$K = Numberofopenchannels$

$S_{Ba} = Attacktraffic\ (bps)$

$S_{Bn} = Normaltraffic\ (bps)$

$T = Channelbandwidth(bps)$

$I_a = AverageQuerySizeoftheAttack\ (b)$

$I_n = AverageQuerySizeofthelegitimateusers\ (b)$

λ_{Ba}= *Average arrival rate attack queries (qps);*

λ_{Bn}= *Arrival rate of legitimate user queries (qps).*

It was assumed that the SPI OACI filtering system has two properties: the probability of filtering and dispatching legitimate traffic $\boldsymbol{Fn_P}$andthe 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 Fig 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 λFa and λFnsuch that Equ 3 and 4 holds

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

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

Now, the SPI OACI filtering system must block traffic equally at every instant of time. It is reasonable to say that incoming legitimate traffic λ_n and attack traffic λ_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 abnormal or illegitimate traffic probability and normal or legitimate traffic probabilities given in Equ 5 and 6.

$$\lambda_{Mn} = \lambda_{Bn} \cdot (1 - P_{Fn}) \quad (5)$$

$$\lambda_{Ma} = \lambda_{Ba} \cdot (1 - P_{Fa}) \quad (6)$$

In the AIRMS, another identified type of DDoS attack model is the memory depletion model. To represent this kind of the DDoS attack, this work leveraged the SYN flooding attack model [29] which can serve as a more general DDoS attack types. This model is given by Equ 7.

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

Where

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

t_a = $Averageprocessing\ time\ of\ the\ attack\ query\ (s)$; $M = Buffer\ size\ of\ the\ SPI\ firewall$

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

Equation 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 case based scenario was found in [30]. 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.

B. SPI-OACI Security Architectural Components

This work will use the SPI-OACI security model for securing the AIRMS against VBDDA. The major device is adopted for the implementation is the Cisco ASR 9000 firewall [31] 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. Both of these works together to deliver complete DDoS protection for virtually any environment. An in-depth discussion is presented below.

- SPI-OACI Traffic Anomaly Detector (STAD): This acts as an early warning system. It provides in-depth analysis of the most complex DDoS attacks and passively monitors network traffic while looking for any deviation from normal or baseline behaviour that indicates a DDoS attack.
- SPI-OACI Guard (SG): When an attack is identified, the STAD alerts the SG, providing detailed reports as well as specific alerts to quickly react to the threat. For instance, the model can examine and deduce that the rate of UDP packets from a single source IP is out of range, even if overall thresholds are not exceeded. The SG is the heart beat of AIRMS cloud network DDoS detection. It represents a high-performance DDoS attack-mitigation device that could be deployed upstream at either the cloudservice provider data center or at the perimeter of the AIRMS to protect both the network and data center resources.

When the SG is notified that a network link or device is under DDoS attack traffic destined for the target is diverted to active treatment and possible packet discard as shown in Fig 7. In this case, the traffic is then subjected to a concurrent five-stage analysis and filtering process designed to remove all malicious traffic whileallowing legitimate packets to get to the AIRMS backend servers without any interruption.

Considering Fig. 3, the architectural components of the SPI OACI (see Fig 4) comprises the following, viz: verification, analysis, and enforcement techniques. This was used to identify and separate malicious traffic from legitimate traffic (See section III). This purification process consists of five modules or steps:

- Filtering: This block includes both static and dynamic DDoS filters. Static filters block the non-essential traffic from reaching the backend servers under attack. They are user-configurable, and come with preset default values. Dynamic filters are inserted by the other modules based on observed behaviour and detailed analysis of traffic flows, delivering real-time updates that either increase the level of verification applied to suspicious flows or block sources and flows that have been verified as malicious.
- Active verification: This block verifies that packets entering the system have

not been compromised. The SG uses numerous unique, patent-pending source-authentication mechanisms to stop spoofed packets from reaching the backend servers. The active verification module also has several mechanisms to help ensure proper identification of legitimate traffic, virtually eliminating the risk of valid packets being discarded.

- Anomaly recognition: This block monitors all traffic that was not stopped by the filter or the active verification modules and compares it to baseline behaviour recorded over time, looking for deviations that would identify the source of malicious packets. The basic principle behind the operation of this module is that the pattern of traffic originating from an attacker daemon residing at a source differs dramatically from the pattern generated by legitimate sources during normal operation. This principle is used to identify the attack source and type, as well as to provide guidelines for blocking traffic or performing more detailed analysis of the suspected data.
- Protocol analysis: This block processes flows that anomaly recognition finds suspicious in order to identify application-specific attacks, such as HTTP error attacks. It then detects any misbehaving protocol transactions, including incomplete transactions or errors.
- Rate limiting: This block 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.

In context, between any DDoS attacks, the SG will be in learning mode, passively monitoring traffic patterns and flow for each of the different resources it protects to understand normal behavior and establish a baseline profile. This information is later used to fine-tune policies for recognizing and filtering both known and unknown attacks in real-time network activity.

C. SPI OACI DDoS Mitigation Procedure

An outline of the cloud security counter DDoS flowchart was detailed while showing the initial phase of the design with Riverbed OpenFlow software in this work. By enabling the SPI OACI firewall, the following were monitored in the AIRMS 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 back end servers. The flow chart in Fig 4offers 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 AIRMS firewall, the cluster server network is protected by the flow as shown in Fig 4thereby maintaining business continuity. Some of the technical highlights of the SPI OACI firewall include:

- Provision of a granular firewall engine
- Provision for authentication proxy which offers a per-host access control mechanism
- Its application Inspection features additional protocol conformance while checking the network policy controls
- Greater deployment flexibility, reduce implementation timelines

It is known that common single-connection services such as Point of Presence, Telnet, Microsoft Remote Procedure Call, and other simple protocols are usually inspected by the generic capability of TCP, UDP, and ICMP inspection. However, using these inspection capabilities is simple to implement, but can limit Stateful Packet Inspection's granularity (i.e any traffic that was allowed to leave through a firewall was allowed to return because inspection created an Access Control List (ACL) can bypass entry for that traffic). However, the recursive SPI OACI can allow the creation of specific 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.

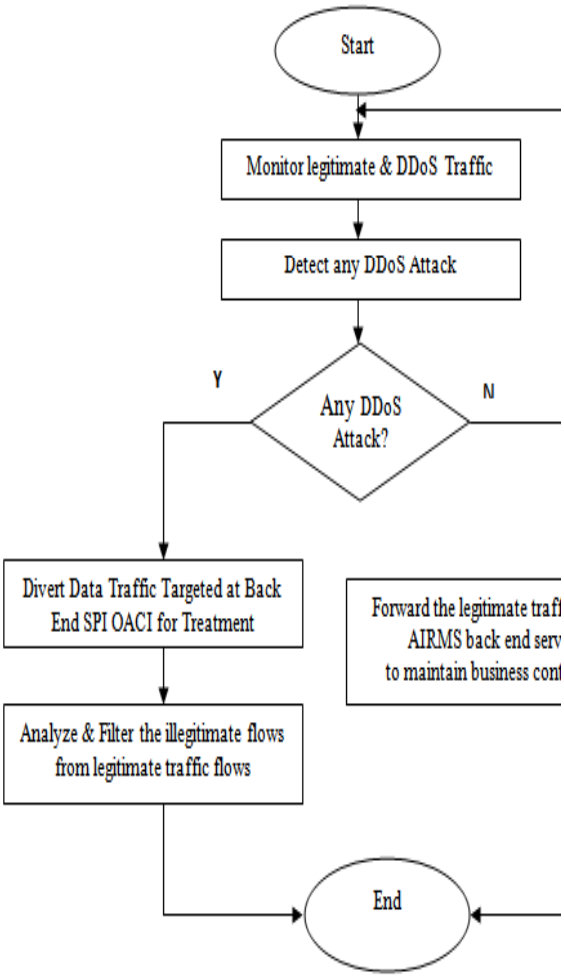

Fig. 4: A Proposed Recursive SPI OACI flow model

By analysing and filtering the illegitimate traffic flows from the legal traffic flows packets, this will prevent malicious traffic from impacting QoS performance while allowing legitimate transactions to complete appropriately.

D. Recursive SPI OACI Advantages

The SPI OACI solution shown in Fig 4 provides complete protection against all types of DDoS attacks including VBDDA as discussed in section III. 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.

V. SYSTEM DESIGN

A. Experimental Design

In this paper, the core of the threat mitigation proposal is the SPI OACI device. The foundation devices of SPI-OACI are the Cisco Application Policy Infrastructure Controller (Cisco APIC) and Cisco Nexus 9000 Series multilayer Switches configured for firewalling the AIRMS servers. A characterization of the Cisco 9000 router firewall as an embedded network device with support for Virtual DDoS protection was considered in the AIRMS threat mitigation proposal. Considering Fig 3, the SPI OACI was placed adjacent to a switch on a separate VLAN network interface, helping enable on-demand protection on the backend monitoring 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 analysed. 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 AIRMS. For the analysis of simulation experiments, standard situation parameters were chosen as detailed below [20] while implementing the system using Riverbed Modeller version 17.5 [32]. Table 1 shows the security cloud network design parameters.

Table 1: Experimental design Parameters

SN	Parameters	Specifications
1	Normal Traffic	20 Mbps normal traffic (100 queries per second by 200 bits in each).
2	Attack Traffic	10 Mbps attack traffic (50000 queries per second by 200 bits in each).
3	Bandwidth	2 Channels with 100 Mbps bandwidth each;
4	SPI firewall Filter	Uses filters that filter 20% of the attack and 2% of legitimate user's queries.
5	Query Time	Legitimate query takes 200 ms to execute

6	Attack Query	Execution takes 2000 ms.
7	Firewall Type	Cisco 9000 router firewall
8	SPI firewall buffer capacity	2500 and can hold information of 50 connections.

The modeler software served as the tool for predicting, measuring, modeling, and analyzing the system performance. In the work, the performance of the AIRMS cloud network was determined by network attributes that are affectedby the various components such as network media, nodes, clients, servers, server applications. From Table 1, the analysis of the network leveraged the following phases:

i. Capture packet traces when the AIRMS 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.

B. Analysis of Results

This study focused only on the security QoS profiling under normal traffic flow via the SPI OACI firewall device. The intent is to form an initial baseline for a comparative study in a future research. After proposing the model, some selected network QoS metrics were evaluated to ascertain the applicability of the SPI OACI. However, the difficulty of carrying out an exhaustive set of experiments in real environments, involving production AIRMS 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 this kind of software tool as valid framework for experimentation. The metrics for security QoS profiles is presented next.

- *Security QoS Profile 1: Point-to-Point Throughput*

In context, this is defined as the probability for a legitimate user to acquire a free position in the service queue during an observation period. It is related to the amount of time during which at least one free position in the service queue is available. It can serve as a measure of the efficiency considering the valid traffic pattern into the server. With the pseudo traffic generation event tool, normal traffic was generated by the configuration manager considering a typical http request on the AIRMS servers via the SPI OACI. The variable request speed not exceeding 25requests/secs was used.

Fig. 5 shows the throughput verification results. A scan be seen from the figure, the actual measured values follow a linear response for all the legitimate requests made to the server via the firewall device. The maximum value is about 8700packets/sec representing 96.66% of correctly delivered packets with respect to the trace back time which is determined by the maximum hop count between the sever and the firewall. The implication is that reliability is guaranteed besides securing the server clusters from cyber attacks.

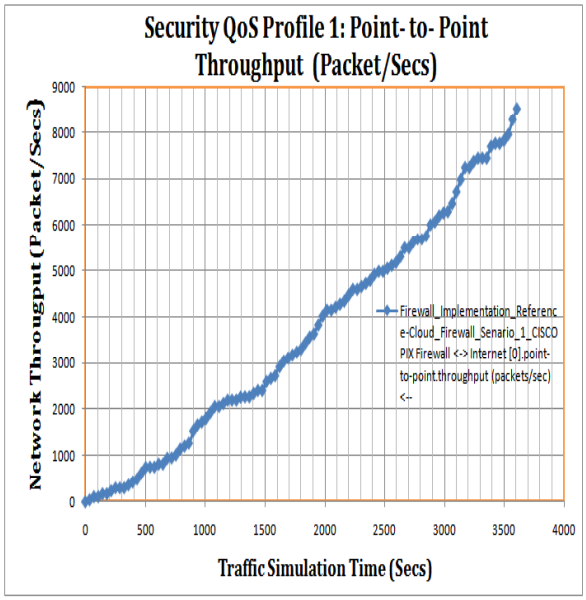

Fig. 5: Normal Traffic flow throughput (Packets/sec)

- *Security QoS Profile 2: Point-to-Point Resource Utilization*

Network utilization is the ratio of current network traffic to the maximum traffic that the port can handle [33]. It indicates the bandwidth use in the network. While high network utilization indicates the network is busy, low network utilization indicates the network is idle or less busy. When network utilization exceeds the threshold under normal condition, it will cause low transmission speed, intermittence, request delay and so on. It is know that

networks of different architectures have different theoretical peaks under general conditions. Ensuring that there is no packet loss when network utilization reaches a certain value is a basic concern.

For most networks 50% network utilization can be considered as high efficiency. By monitoring network utilization, this can aid understand whether the network is idle, normal or busy. It also helps us to set proper benchmark and troubleshoot network failures. In this research, utilization is the reciprocal of resource availability (which is the ratio between the number of legitimate user requests served by the server, and the total number of requests sent by these users). The aim of the DDoS attack is to minimize the availability of the service by increasing resource utilization beyond some specified thresholds. This task can be achieved by minimizing the client success probability, which reduces the probability of a legitimate user acquiring a position in the queue. Fig. 6 shows a 15% resource utilization response from the AIRMS network. An interesting behavior was observed by disabling the SPI OACI device. A 70% differential in the resource utilization was evidenced. In this case, the sudden transition from 15% to over 85% utilization response shows the influence of a possible Synflood DDoS attack which will normally lead to very high link bandwidth, memory and CPU utilization cycles. Fig 6 shows the measurement results in this regard. As can be seen from the figure, it shown that over a prolonger DDoS attack, the network can come to a halt.

However, by re-enabling the firewall device, the effective resource utilization was restored.

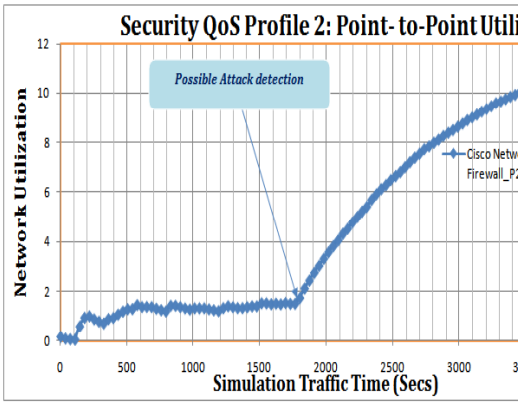

Fig. 6: Biased normal traffic flow Utilization Response

- Security QoS Profile 3: Point-to-Point Delay

This work used delay interchangeably with latency. The delay of the network specifies how long it takes for a bit or byte of data to transverse across the network from point *A* to point *B*. It is typically measured in multiples or fractions of seconds. As shown in Fig 7, the latency of the firewall device including the network delay during the normal traffic flow is about 87.5% (0.875secs). The effect is basically negligible in the context of AIRMS. However, the concern in network latencies is on how to reduce it to the barest minimum.

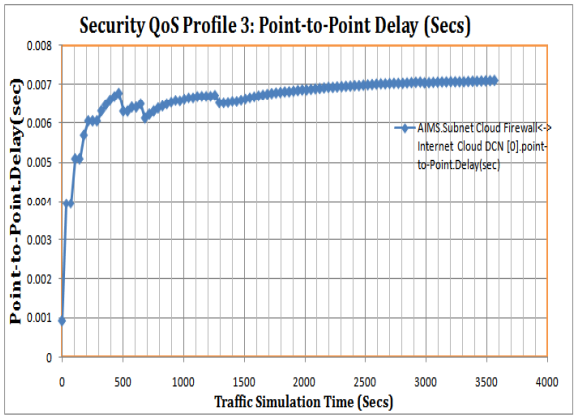

Figure 7: Normal Traffic flow delay response

Another security QoS profile deduced from the work is the effect of resource utilization on the network throughput. Essentially, an increase in utilization leads to higher throughput response. However, beyond a certain utilization threshold, the network throughput becomes very unstable leading to TCP incast collapse. The congestion caused by DDoS Incast has the effect of increasing the latency observed by the application and its users. The detrimental effect on TCP throughput caused by network congestion via incast communication patterns makes its imperative to guard against DDoS traffic at all times. All the observations made in tis phase of the work only depict the scenario for normal traffic flow via the SPI OACI device.

VI. CONCLUSION AND FUTURE WORK

This paper has dealt with security QoS metrics for legitimate traffic flow in an AIRMS cloud network system. Bandwidth exhaustion, memory depletion, CPU power drain and application crashing are the identified DDoS strategies used by cyber terrorist. In the Proposed AIRMS, 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 9000 router firewall as an embedded network device and the design parameters in table 1, the security QoS metrics under normal traffic flow was analyzed. It was concluded that

the absence of a robust security firewall technology can adversely affect the network QoS and expose the network to various forms of DoS attacks. R&D is currently underway on the use of SPI OACI traceback device to track down the sources ofDDoS attacks on Enterprise cloud based services like EETACP, AIRMS, etc. The roadmap for future works involves: i) Completing the design phase of AIRMS for production use, ii) applying the proposed SPI-OACI approach in DCCN smart portal [24] against various forms of DoS attacks and iii) comparing various mitigation models with the proposed SPI-OACI proposal.

In practical context, the mitigation model of the AIRMS cloud network can be enhanced by using these preventive steps as recommended for SPI-OACI based deployment. These are stated below.

- Employing SPI rate-limiting in OpenFlow firewalls which encompasses the routers, load balancers and other network perimeter devices.
- Enabling TCP SYN cookie protection.
- Testingdeployed applications and the network architecture for DoS vulnerabilities and fix them.
- Conduct regular configuration audits on the perimeter devices.
- Using updated software/firmware
- Employing updated Anti-virus and regularly checks for malware, bots on existing physical machines.
- Employing multiple hybrid cloud providers for redundancy.
- Maintaining a smart backup site for quick switch over.
- Installing and configuring network SPI-OACI monitoring systems which can use its SG to trigger an alert any time any DDoS hits the network.
- Engaging network security experts to manage the network professionally

ACKNOWLEDGEMENTS

This research was carried out as an extended work on Security of Distributed Cloud Computing Network for SGEMS EETACP project commissioned by the Department of Electronic Engineering, University of Nigeria Nsukka. We would like to express our gratitude to Engr. Prof. O.U.Oparaku for his guidance and support.

References

[1] C. C. Mann, "Smoke screening", *Vanity Fair*. (2011, December 20). Retrieved from http://www.vanityfair.com/culture/features/2011/12/tsa-insanity-201112.

[2] R. W. Poole, Jr., "Toward risk-based aviation security policy", *International Transport Forum*. (2008, December 11), Retrieved from http://www.internationaltransportforum.org/jtrc/discussionpapers/DP200823.pdf

[3] https://researchedsolution.wordpress.com/2012/02/27/protecting-airport-information-systems-against-cyber-attacks/

[4] P. K. Kerr, "Nuclear, biological, and chemical weapons and missiles: Status and trends", *Congressional Research Service. The Library of Congress* (CRS Report for Congress), (2008, February 20). Retrieved from http://www.fas.org/sgp/crs/nuke/RL30699.pdf

[5] http://www.cbsnews.com/news/hackers-force-poland-lot-airlines-to-cancel-and-delay-flights/June 22, 2015, retrieved on August 1st, 2015

[6] https://www.google.com/search?q=ranian+hackers+compromised+airlines%2C+airports%2C+critical+infrastructure+firms&ie=utf-8&oe=utf-8-IDG_News_Servicel Dec 2, 2014, retrieved on August 1st, 2015

[7] D. Nessi, "Are you exposed? The perils of a connected world", *Airports Council International – North America*, (2011, October 17). Retrieved from http://www.aci-na.org/sites/default/files/nessi-areyouexposed-bit.pdf

[8] Overview of cyber vulnerabilities. (n.d.). US-CERT (United State Computer Emergency Readiness Team). Retrieved from http://www.us-cert.gov/control_systems/csvuls.html

[9] G. Stoneburner, A. Goguen, and F. Alexis, "Risk management guide for information technology systems", *National Institute of Standards and Technology* (NIST), , (2002, July). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[10] D. Swan, "Assessing Primary Cyber Threats to an International Airport's Critical Information Systems", University of Maryland University College.

[11] Yong-Suk Kang, Yang-Ha Chun, Yong-Tae Shin and Jong-Bae Kim, "A Study of the Airport Model Based on Security Risk", International Journal of Software Engineering and Its Applications Vol. 8, No. 11, 2014, Pp. 67-74 http://dx.doi.org/10.14257/ijseia.2014.8.11.06.

[12] A. Marks and K. Rietsema, "Airport Information Systems—Airside Management Information Systems", In Intelligent Information Management", vol. 6, may 2014, pp. 149-156 in SciRes. http://www.scirp.org/journal/iimhttp://dx.doi.org/10.4236/iim.2014.63016

[13] C. W. Johnson**,** **"**Preparing for Cyber-Attacks On Air Traffic Management Infrastructures: Cyber-Safety Scenario Generation",

[14] K.Gopalakrishnan1, M.Govindarasu, Doug W. Jacobson, and B. M. Phares, "Cyber Security For Airports", International Journal for Traffic and Transport Engineering, vol. 3, no. 4, 2013, pp. 365 – 376,DOI: http://dx.doi.org/10.7708/ijtte.2013.3(4).02.

[15] Whitepaper- CANSO Cyber Security and Risk Assessment Guide,CANSO civil air navigation services organisation, June 2014.

[16] 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.

[17] B. Kurar , R. Tahboub, "Internet Scale DoS Attacks", In International Journal of Applied Mathematics, Electronics and Computers, IJAMEC, vol 3, no. 2, 2015, pp.83–89.

[18] G. M. Fernández, J. E. Díaz-Verdejo, and P. G. 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*

[19] 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),* vol. 8, no. 9, Feb 2014.

[20] S. Ramanauskaitė, A. Čenys, "Composite Dos Attack Model", System Engineering, Computer Technology, vol. 4, no. 1, 2012, pp. 20–26 doi:10.3846/mla.2011.05 Pp.20126

[21] M. Montanari, R. H. Campbell, K. Sampigethaya, and M. Li, "A security policy framework for eEnabled fleets and airports", *Systems Software Research Group at University of Illinois at Urbana-Champaign*. 2011, Retrieved from http://srg.cs.uiuc.edu/srg/sites/default/files/montanari_ieeeaerospace_2011.pdf.

[22] Y. Jiang, K. Zheng, Y. Yang, S.Luo, "Evaluation Model for DoS Attack Effect in Softswitch Network", Communications and Intelligence Information Security (ICCIIS), 2010 International Conference on 13-14 Oct. 2010, pp. 88 – 91

[23] A. Aissani, "Queueing Analysis for Networks Under DoS Attack", Computational Science and Its Applications – ICCSA 2008Lecture Notes in Computer Science Volume 5073, 2008, pp 500-513 .

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

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

[26] Cisco Application Centric Infrastructure May 2014Cisco Systems Inc.

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

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

[29] S. Ramanauskaitė, "Modeling of SYN flooding attacks", *Jaunųjųmoks lininkųdarbai,* vol 26, no. 1, Pp. 331–335.

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

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

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

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