Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique

T.Siva[#1], E.S.Phalguna Krishna[#2]

[#1] *M. Tech Department of CSE &,JNTUA*
[#2] *Asst. Professor., Department of CSE & JNTUA*
Sree Vidyanikethan Engineering college ,Thirupathi,Chittoor Dist.,A.P.,INDIA

***Abstract*— Cloud computing security is sub-domain of computer security, network security, and information security. It refers to a broad set of security policies, technologies, and flow controls deployed to protect data, applications, and the associated infrastructure resources of cloud computing. There are a number of security issues/concerns associated with cloud computing .We provide security to cloud resources by Denial of Service (DoS) attacks and their related sub-domains. Application Denial of service (ADoS) attacks comes under DDOS attacks these are concentrate on SaaS in cloud computing. In this we present different types of cloud based DDOS Attacks and their solutions, also give most dangerous Application DoS attacks scenario and their remedy mechanisms, Introduce new port hopping i.e True Random Number Generation(TRNG) Based Port Hopping in cloud computing request/response environment. In previous port hopping by using Pseudo Random number Generation (PRNG) over comes the disadvantage of prediction of the port hopping sequence and is periodic in nature. Finally overcome/prevent the ADOS attack by using TRNG.**

***Keywords*— Cloud computing, Denial of Service (DoS) attacks, Application DoS attacks, Port Hopping, Pseudo Random number Generation (PRNG), True Random Number Generation (TRNG).**

I. Introduction

Today's network environment denial of service attacks focus on specific application service instead of entire web application. In cloud environment more infrastructure resources are present, A hacker doesn't need to attack your entire infrastructure anymore. They can simply choose the most resource-intensive application that you're running on the cloud and use simple low-bandwidth attacks to take out your access to that service. General attacks present in Network environment are also impact role in cloud environment. This paper is organized as in session II Cloud Architecture for client communicating with cloud services, in session III Cloud Services vulnerabilities, in session IV Formal methods of cloud DoS attacks, in session V some Solutions of Formal DoS attacks in cloud, in session VI Protocols used in cloud in Session VII Latest and most Dangerous ADoS attacks, in session VIII Preferred solutions and their pros and cons in session and in session IX conclusion is given.

II. CLOUD ARCHITECTURE FOR CLIENT COMMUNICATING WITH CLOUD SERVICES

The Cloud Computing Architecture of a cloud comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, and their externally visible properties, and relationships between them. Cloud architecture typically involves multiple cloud components communicating with each other over a loose coupling cloud mechanism such as a messaging queue format. Elastic provisioning impact implies on intelligence in the use of tight or loose coupling of cloud resources, services, middleware, and software components [2].

Front end: The front end of the cloud computing system comprises of set of client devices (or it may be a computer network also) and some applications are needed for accessing the cloud computing system resources. All the cloud computing systems do not give the same interface look and feel to users. Web service applications like electronic mail programs use some existing web browsers such as Firefox, Chrome,Microsoft's internet explorer or Apple's Safari and so on. Other types of systems have some unique applications which provide network access to its clients.

Back end: Back end refers to some physical components. In cloud computing, the back end interface is cloud itself which may encompass various computer systems, data storage systems and different application servers. Groups of this all infrastructures make a whole cloud computing system environment. Theoretically, cloud computing system can include practically any type of web application program such as video games to applications for data pree-processing, software products development and entertainment things. Usually, every application would have its individual dedicated server for services.

In order to include the components of our security architecture in a concept of a cloud computing environment, Based on mainly three cloud service models:
(a) Cloud software as the service (SaaS), (b) cloud platform as a service (PaaS), and (c) cloud infrastructure as a service (IaaS). More precisely, clients do not access servers directly and they do not trigger server applications directly through some network connections. Users in fact access certain cloud components (request brokers) and those cloud components

distribute requests to individual servers, as appropriate. This approach mainly indicates that, in addition to different application servers, one distinctive service of a cloud is a “Service Dispatcher”, in this we called Applications Access Point (AAP) Server. AAP is service level dispatcher, i.e. it distributes different service requests into a cloud to individual application servers present in cloud infrastructure, based on types of requests and other processing parameters. This is another cloud service in a cloud, in this we called Services Publishing and Dispatching (SPD) Server. This server is mainly based on the standard concept of the UDDI Server, as specified by OASIS, i.e. it is the server used for publishing and discovery of cloud application services.

Clients may access cloud services through a variety of communication protocols, as shown in Figure 2.Usually, it is used to be Internet and HTTP (Web access) access protocol. But, with the different recent advances of mobile and wireless technologies and networks the scope of communication protocols is much wider compare to existing one. Clients now a days may access a cloud services using SMS messages, GPRS data channel access, through Wi–Fi access, Bluetooth access, RFID access and even some proprietary communication access protocols. Therefore, in order to be able to accept requests coming through different types of communication access protocols, a cloud needs in front of it and facing various communication networks another service provider. This is communication services provider, in this document called *Communication Access Point (CAP)[3]*.

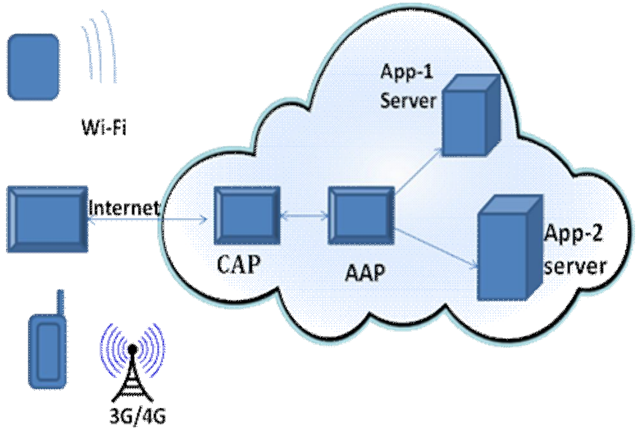

Figure 1.Different ways of connecting cloud services.

We have extended functional components and architecture of a could computing environment, shown in Figure 1, with the following additional security components and services:

Security Access Point

The first component that is needed an extension of the functional architecture is *Security Access Point (SAP).* That is cloud server providing front end security services. The first service, which is important before any access to a cloud is allowed, to access authorizied *authentication of users.*

Security Infrastructure Servers

Three security servers are security infrastructure servers already mentioned in the previous section: IDMS Server, PDP Server, and CA Server. Since cloud should also support different open access services, even by users being registered in other cloud services, binding between IDMS Servers located in cooperating clouds must be performed as a prerequisite for federated secure cloud architecture.

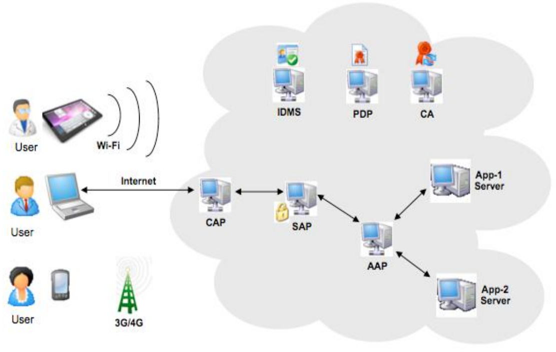

Figure 2. Additional security components and services

Besides binding of IDMS servers, in case of multiple cloud services, federation must also be established between authorization access policies. Finally, CA is standard Certificate Authority Server in cloud. For the purpose of scaling, CA Server must be linked into a large scale Public Key Infrastructure (PKI).

III. CLOUD SERVICES VULNERABILITIES

Hypervisor Holes[4]

In a virtualized cloud services environment, each client has a Virtual Machine that is running client specific applications. As the operating system (OS) of cloud provider is running multiple VMs concurrently, it is a challenging task in cloud to manage the entire VMs in cloud recently; however different black hat hackers and other security experts have discovered security holes in some hypervisor implementations in cloud. Hypervisors are getting more and more common, and growing in deployment in everything from data center systems to embedded consumer electronics goods. But, as their deployment process increases, more security concerns come into cloud service play platform, including a variety of cloud attack methods and the direct consequences of a compromised hypervisor.

XML Signature

SOAP (Simple Object Access Protocol) is an XML based protocol consists of mainly three parts: an envelope, Defines what is in the message and how to process that message, a set of encoding rules for expressing instances of application defined different data types, and a convention for representing cloud procedure calls and request/responses. Setting up a virtual machine to send spam mails is just one example what an attacker can do using the legitimated user’s identity and charging his account .

Malware Injection Attack

In this attack the adversary creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and adds it to the Cloud service system. Then, the adversary has to trick the Cloud service system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the attacker. If this succeeds, the Cloud service system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. Such an attack could be a major hindrance to bank applications in the cloud as malicious applications taking its place could swindle the bank's clients.

Denial of Service

When the Cloud Computing operating system notices the high workload on the flooded service in cloud, it will start to provide more computational power to cope with the additional workload. Thus, the cloud server hardware boundaries for maximum workload to process do no longer hold time. In that sense, the Cloud system is trying to work against the attacker (by providing more cloud computational power), but actually to some sorts supports the attacker by enabling him to do most possible damage on a cloud service's availability, starting from a single flooding attack entry point in the cloud system.

IV. FORMAL METHODS OF CLOUD DOS ATTACKS (TYPES OF DOS ATTACKS AND THEIR ATTACK SCENARIOS)

In computing, a *denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack)* is an attempt to make a machine or network resource unavailable to its intended users.

Methods of attack

a. ICMP flood

A smurf attack is one particular variant of a flooding DoS attack on the public Internet access. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine in the netowork. The network then serves as a smurf amplifier attack. In such an attack, the cloud perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim machine. The network's bandwidth is quickly used up, preventing legitimate data packets from getting through to their destination system.

b. SYN flood

A SYN flood occurs when a host sends a flood of TCP/SYN data packets, often with a forged sender IP address. Each of these packets is handled like a connection request, causing the cloud server to spawn a half-open connection request, by sending back a TCP/SYN-ACK data packet (Acknowledge), and waiting for a request packet in response from the sender IP address (response to the ACK Packet). However, because the sender IP address is forged, the response from other machines never comes. These half-open connections saturate the number of available connections the server is able to make the resources, keeping it from responding to authorized/legitimate requests until after the attack ends.

c. Teardrop attacks

A Teardrop attack involves sending mangled IP fragments with overlapping, over sized payload data packets to the target machine. This can crash/damages various operating systems and their resources because of a bug in their TCP/IP fragmentation re-assembly code.

d. Low-rate Denial-of-Service attacks

The Low-rate DoS (LDoS) attack exploits TCP's slow-time scale dynamics of retransmission time out (RTO) mechanisms to reduce TCP throughput delay. Basically, an attacker can cause a TCP flow to repeatedly enter a RTO state by sending high rate, but short duration bursts of a system, and repeating periodically at slower RTO time stamp scales. The TCP packet throughput at the attacked node will be significantly reduced while the attacker will have low average rate making it difficult to be detected the system.

e. Permanent denial-of-service attacks

A permanent denial-of-service (PDoS) attacks, also known loosely as phlashing, is a type of dos attack that damages a cloud system so badly that it requires replacement or reinstallation of hardware reaources. Unlike in the distributed denial-of-service attack, a PDoS attack exploits cloud security flaws which allow remote administration on the management interfaces of the victim's hardware resources, such as routers, printers, or other networking hardware resources. The attacker uses different vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware cloud image a process which when done legitimately is known as *flashing attack*. This therefore called "bricks" the device, rendering it unusable for its original intent purpose until it can be repaired or replaced by another one.

f. Application-level floods

Various DoS causing exploits attacks such as buffer overflow can cause server running software to get confused and resources like fill the disk space or consume all available memory or CPU time.

Other kinds of DoS rely primarily on brute force attacks, flooding the target system with an overwhelming flux of packets, over saturating its connection bandwidth or depleting the target's system resources. A "banana attack" is another particular type of DoS attack. It involves redirecting outgoing messages from the client back onto the client system, preventing outside access sys resources, as well as flooding the client with the sent packets.

g. *Reflected / Spoofed attack*

A distributed reflected denial of service attack (DRDoS) involves sending forged requests of some type to a very large number of computer systems that will reply to the requests. Using Internet Protocol IP address spoofing, the source IP address is set to that of the targeted victim machines, which means all the replies will go to (and flood) the target system.

V. SOLUTIONS OF FORMAL CLOUD DDOS ATTACKS

a. *Prevention and response*

Defending against the Denial of Service attacks mainly involves the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate/authorized and allow traffic that they identify as legitimate/authorized.

b. *Firewalls*

Firewalls can be setup to have simple rules such to allow or deny access protocols, ports or IP addresses. In the case of a simple attack coming from a small number of unusual IP addresses for instance, one could put up a simple rule in its cloud authentication system to drop all incoming traffic from those attackers network.

c. *Switches*

Most switches have some rate-limiting and Access Control List capability. Some switches provide reasonable automatic and/or system-wide rate limiting, deep packet inspection, traffic shaping, delayed binding (TCP splicing), and Bogon filtering (bogus IP filtering) to detect and remediate denial of service attacks through automatic rate filtering mechanisms and WAN Link failover and balancing mechanisms.

d. *Routers*

Similar to switches, routers have some rate-limiting and ACL capability. They, too, are manually set rules and regulations. Most routers can be easily overwhelmed under DoS attack scenario. Cisco IOS has different features that prevent flooding messages.

e. *Application front end hardware*

Application front end hardware is intelligent hardware device placed on the network before traffic reaches the servers side. It can be used on networks in conjunction with routers and switches. Cloud Application front end hardware resources analyzes data packets as they enter the network system, and then identifies them as based on priority, regular, or dangerous. There are more than 25 bandwidth management vendors available in cloud environment.

f. *IPS based prevention*

Intrusion-prevention systems (IPS) are effective if the attacks have different signatures associated with them. However, the trend among the different attacks is to have legitimate content of packets but bad intent. Intrusion-prevention systems work on content recognition cannot block behavior based DoS attacks.

g. *Blackholing and sinkholing*

With this blackholing, all the traffic to the attacked DNS or IP address packets are sent to a "black hole" (null interface, non-existent serve). To be more efficient and avoid affecting of network infrastructure connectivity, it can be managed by the ISP systems.

Sink holing routes to a valid IP address which analyzes network traffic and rejects bad ones. Sink holing is not that much of efficient for most severe server side attacks.

VI. PROTOCOLS USED FOR CLOUD COMPUTING

Security implemented by provider - Not A Protocol Based Solution!.

-Isolation among the resources of different tenants
- • Hypervisor
- • Storage
- • Network (VLAN)

- Restrict administrator privileges on hosting systems Strong cloud authentication, cloud authorization, and cloud identity management

-Interfaces for direct cloud client-controlled audits are implemented in cloud service points.

-Engage third-party auditors in cloud services.

Mechanisms implemented by client side

– Cryptographically protect the data/Information
- • Encryption
- • Integrity protection

– Remote auditing

Client must trust provider ...

Introduction to Cloud Trust Protocol

The Cloud Trust Protocol (CTP)[5] is the mechanism by which cloud service consumers/clients (also known as “cloud users” or “cloud service owners”) ask for and receive information/data about the elements of transparency as applied to cloud service providers and owners. The primary purpose of the CTP and the elements of transparency is to generate fully evidence based confidence that everything that is claimed to be happening in the cloud is indeed happening as described, and nothing else in the cloud. This is a classic application of the definition of digital trust policy. And, assured of such evidence based, cloud consumers become liberated to bring more sensitive and valuable business functions to the cloud services, and reap even larger amount of payoffs. With the CTP cloud consumers are provided a way to find out important pieces of information concerning the compliance, cloud security, cloud privacy, cloud integrity, and cloud operational security history of service elements being performed “in the cloud”.

VII. LATEST AND MOST DANGEROUS ADOS ATTACKS

Application DoS attacks exploit flaws in the application design and implementation to prevent legitimate access to the victim’s different services. They represent a suitable subset of potential attacks on such cloud applications,they are aimed specifically at disrupting the operation rather than the subverting application service controls[6].

• *The attacks will typically unable to detectable or preventable by existing entire price security monitoring solutions:* Since the attacks do not consume an unreasonable amount of Bandwidth and in could networks, in many cases, be indistinguishable from normal network traffic.

• *Application attacks are efficient:* The attacker may not need as much resource system at their disposal to successfully complete the attack. Application level attacks target bottlenecks and resources limitations within the application and no need many compromised “zombie” systems or a large amount of bandwidth malicious data packets .

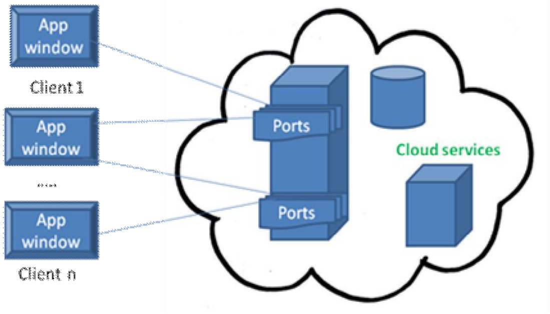

Figure 3: Application Dos attacks scenario.

Fig 3 Represent Application Dos attack scenario in this client communicates through different port numbers with cloud services. In the above scenario each application window uses different ports if we are using single port at any client ideal time attacker may do attacks on those open ports.This type of attacks known as Application denial of service attacks.

To overcome this type of attacks we are frequently change the protocol port numbers.

• *Application attacks are harder to trace back:* Application level attacks normally use HTTP or HTTPS as their transport layer protocols. Proxy servers can therefore be used to obfuscate the true origin of the cloud attacker, and the many are available for an attacker to redirect his malicious traffic to cloud network.

VIII. PREFERRED SOLUTIONS AND THEIR PROS AND CONS

When considering network based applications, are particularly weak point in this cloud context is that they commonly provide some open port(s) for cloud service communication, making themselves targets for cloud DoS attacks. Attackers that have the ability of eavesdropping messages exchanged by the application can identify open ports and launch directed attacks to those open/ideal ports as opposed to blind attacks that can be launched to arbitrary ports, even by non-eavesdropping adversaries.This problem was also posed earlier in the literature and a simple and useful approach was proposed,

namely, *port-hopping*. The application parties communicate via ports that change port numbers periodically change over time, according to a pre calculated pattern known by both the sender and receiver, such as a (pseudo)random sequence with common seed.

Badishi et al. propose an ack-based port-hopping [7] protocol focusing on the communication only between two parties(client-server), modeled as cloud sender and cloud receiver. The cloud receiver sends back an acknowledgment for every data message received from the sender sending data message, and the sender uses these acknowledgments as signals to change the destination port numbers of its messages. Since this protocol is acknowledgement based port hopping, For this time synchronization is not necessary in this cloud services and users.

Badishi et al. also propose a solution that reinitializes [7] the protocol between the cloud services and users. With reinitializing time to time, the cloud sender and cloud receiver can use new seed value for each time of the pseudorandom function to generate different port number sequences, so that the port number sequence used for communication is changed time to time (periodically).

Lee and Thing propose another port-hopping scheme [8] for the client-server mode here we taken as cloud server and user. In their mechanism, time is divided into discrete time interval slots. The cloud clients and the cloud server share a pseudorandom function to compute which port should be used in a certain time slot and how the port is changed frequently based on time interval. This scheme shows the basic idea of the time-based port hopping, but still it is based on synchronized clock values.

Similar as port hopping, Srivatsa et al. Propose a client transparent approach in cloud. This approach uses JavaScript to embed cloud authentication code into the TCP/IP layer of the networking stack, so the cloud messages with invalid authentication code will be filtered by the cloud server’s firewall access control list.

Port hopping with true random number based port hopping: High-speed network environment necessitates lightweight mechanisms for differentiating between valid traffic and the attacker’s packets in the cloud network. The main challenge in presenting such a solution is to exploit existing packet-filtering mechanisms in a way that allows fast processing of packets but is complex enough so that the attacker cannot efficiently craft packets that pass the filters. A protocol that controls DoS attacks by adversaries that can eavesdrop packets and (with some delay) adapt their attacks accordingly. The cloud protocol uses only available efficient cloud packet filtering mechanisms based mainly on IP IP addresses and port numbers. This protocol avoids the use of fixed ports for cloud communication and instead performs “pseudo random port hopping” mechanisms. We model the underlying cloud packet filtering services and define measures for the capabilities of the cloud adversary and for the success rate of the protocol. Using this, provide a novel rigorous analysis of the impact of DoS on an end-to-end protocol and show that protocol provides effective cloud DoS prevention for realistic attack and deployment scenarios.

PRNG Port hopping Disadvantages:

-PRNGs generate random numbers based on mathematical formulae or precalculated list, so attacker can esily predict or know the random numbers.
-*Deterministic:G*iven sequence of numbers may be reproduced later date if know the starting point in the sequence.
-PRNGs are *periodictable*, which means that the sequence will eventually repeat at any point itself .

TRUE RANDOM NUMBER GENERATORS extract different randomness from physical phenomena and introduce it into a computer system. Imagine this is a die properly connected to a computer system for different random number generation, but typically people interested to use a physical phenomenon that is easier to connect to a computer than a die is. The physical phenomenon can be very simple, like the little variations in mouse movements [9] or in the amount of time between keystrokes. In practical implementation, however, you have to be careful about which source you choose. For example, it can be tricky to use keystrokes in this similar fashion, because keystrokes are often buffered by the computer's operating system, meaning that several keystrokes of keyboard are collected before they are sent to the processing program waiting for generating random numbers. To a program waiting for the keyboard keystrokes, it seem as the keys were pressed almost simultaneously, and there may not be generate a lot of randomness there after all.

However, there are many other ways to get true randomness into computer system. A really good physical phenomenon for generation of random number is to use is a radioactive source generation. The points in time at which a radioactive source decays are completely unpredictable by any another person or device, and they can quite easily be detected and fed into a computer, avoiding the use of any buffering mechanisms in the operating system.

Another suitable implementable physical phenomenon is atmospheric noise, which is quite simple and easy to pick up with a normal radio sources. Also use background noise released from an office or any other laboratory source, but you'll have to watch out for different patterns. The fan from computer system might contribute to the background noise generation, and since the fan is a rotating device in the physical environmnet, chances are the noise it produces won't be as random as atmospheric noise.

A. ***Characteristic***	B. ***PRNG***	C. ***TRNG***
D. *Periodicity*	E. *Periodic*	F. *Aperiodic*
G. *Determinism*	H. *Deterministic*	I. *Nondeterministic*
J. *Efficiency*	K. *Excellent*	L. *Poor*

Table 1.Comparison of PRNGs and TRNGs

The above table represent the difference between the Pseudo Random Number Generation and True Random Number Generation based on some characteristics.

IX. CONCLUSION

In this we give different types of Denial of Service attacks in cloud computing environment and their existing solutions these remedy methods are taken from normal client server network environment. We briefly give the most dangeourous attack i.e. How Application Denial of service attack present in cloud environment and their attacks scenarios and different port hopping techniques like Pseudo Random Number Generation(PRNG), these port hopping techniques are taken from client-server network environment if we implement then attackers can predict the random sequences and also introduce new unpredictable True Random Number Generation (TRNG) port hopping in cloud computing environment.

REFERENCES

[1] Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas “*Mitigating Distributed Denial of Service Attacks in Multiparty Applicationsin the Presence of Clock Drifts*” Ieee Transactions On Dependable And Secure Computing, Vol.9, No.3, May/June 2012.

[2] https://cloudsecurityalliance.org/research/ctp/

[3] SETECS®, Inc. “Security Architecture for Cloud Computing Environments” White Paper– February 1, 2011.

[4] Anand Mukundan Bina Bhaskar “Security in Cloud Computing - Vulnerabilities, Challenges, Models and path ahead”

[5] IBM Research – Zurich Christian Cachin “*Protocols for Secure Cloud Computing*” April 2011.

[6] Stephen de Vries “A Corsaire White Paper:Application Denial of Service (DoS) Attacks”1 April 2004.

[7] G. Badishi, A. Herzberg, and I. Keidar, “*Keeping Denial-of-Service Attackers in the Dark*,” IEEE Trans. Dependable and Secure Computing, vol. 4, no. 3, pp. 191-204, July-Sept. 2007.

[8] H. Lee and V. Thing, “*Port Hopping for Resilient Networks*,” Proc. IEEE 60th Vehicular Technology Conf. (VTC2004-Fall), vol. 5,pp. 3291-3295, 2004.

[9] Wang Xingyuan, Qin Xue, and Teng Lin “A Novel True Random Number Generator Based on Mouse Movement and a One-Dimensional Chaotic Map” 26 October 2011.