Attack Analysis & Bio-Inspired Security Framework for IP Multimedia Subsystem

Aliya Awais , Muddassar Farooq ,M Younus Javed
College of Electrical & Mechanical Engineering
National University of Sciences & Technology
Rawalpindi, Pakistan
aliya.awais@gmail.com, muddassar.farooq@udo.edu ,myjaved@ceme.edu.pk

ABSTRACT

This paper analyzes the security vulnerabilities and requirements of IP Multimedia Subsystem(IMS), particularly the impact of Denial-of-Service(DoS) and Distributed DoS(DDoS) attacks on the IMS. We propose and develop an intelligent Bio-inspired, self-defending security framework for the IMS and Next Generation all-IP Networks. Our proposed framework will complement the existing authentication and encryption mechanisms to protect infrastructure nodes and subscribers against the attacks launched by the malicious nodes in the network. This framework is expected to become a cardinal component which can be integrated into any IMS converged network infrastructure to provide defense against wide variety of attacks particularly DoS and DDoS attacks.

Categories and Subject Descriptors

C.2.2 [**Computer Systems Organization**]: Computer Communication Networks—*Network Protocols*[Applications]; C.2.0 [**Computer Systems Organization**]: Computer Communication Networks—*Security and protection*

General Terms

Experimentation, Security

Keywords

Artificial Immune Systems, IP Multimedia Subsystem, Network Security

1. INTRODUCTION

The IMS is a standard for the Next Generation Networks (NGNs) defined by the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP) [1] and 3GPP2 [1] and is inherently capable of media services.

IMS can be defined as a global, access independent, standards based IP connectivity and service control architecture that enables various types of multimedia services to end-users, using common internet-based protocols [5]. IMS architecture makes it possible to establish peer-to-peer IP communications with all types of clients with the requisite quality of service. In addition to the session management, IMS architecture also addresses functionalities that are necessary for complete service delivery, for example, registration, security, billing, media control and roaming. IMS is still being defined and there are still many open issues within the IMS architecture [6]. The 3GPP IMS standardization is ongoing, and yet there is no commercial deployment of IMS within the operators' networks [5].

Most of the issues regarding the security for IMS, like authentication, encryption, confidentiality and reliability, are standardized by the 3GPP release 5 that provide security at the first level in IMS networks [2]. However, the possibility of malicious attacks or service abuse by crafty attackers has increased significantly with the advent of new access technologies and devices. In this study, we show that attackers can penetrate into the network through security trap doors by breaking the first level of security to misuse network resources and services. The breach of the first level of security also means that they can not only steal the subscriber's confidential information, but also can damage the network operator's resources and assets [7]. In this study, we propose an in-built security monitor that can detect and stop the attacks that target IMS networks.

A further insight into the security loopholes in the IMS framework requires a layered based logical view of the IMS core. IMS layered architecture allows the services and common functions to be reused for multiple applications and access types. The layer-based logical view will help in localizing the causes of vulnerabilities to a handful of modules/components. This will simplify the task of devising a security framework to counter the vulnerabilities in a robust and reliable manner. IMS framework can be viewed as a stack that consists of the following three layers [5].

- The *application layer* contains applications and multimedia content servers and provides services of that particular application along with its control logic to the end users.
- The *control layer* comprises of servers that are required for doing critical functions which include, but are not limited to, call setup, modification, release and call session control function (CSCF).
- The *transport layer* consists of routers and switches both at the edge access networks and at backbone networks.

This layered structure makes IMS an open communication architecture rather than a monolithic and closed architecture. This layered architecture decouples the service delivery components from the physical network making it possible for services to be independent of the network over which they are delivered.

IMS functional elements communicate via standard reference points instead of the classical way of via interfaces.

GECCO '08 July 12–16, 2008, Atlanta, Georgia, USA.
ACM 978-1-60558-131-6/08/07.

Unlike an interface where any device can communicate to a particular element, a reference point is a well-defined set of rules that associate two functions of the communicating elements. Regardless of the reference point types, all IMS signaling and communications are based on IP protocol. Likewise, IMS information streams can be divided into three types: *control stream*, *media stream* and *management stream*. A malicious node/user can modify one of these streams to launch a number of effective attacks that can play havoc with the normal operations of the IMS network [13].
In this paper, we present the security framework for IMS and implement two security systems. The first system is a Bio-inspired Artificial Immune System (AIS) and the second system is a signature based cryptology algorithm. Our results show that AIS based solution provides good detection accuracy which low overheads. Although, crypto-based solution gives 100% detection rate but has high memory and computational overhead which makes it unsuitable for IMS users.
The rest of the paper is organized as follows. Section 2 describes the IMS security requirement, attack simulation and performance. In Section 3, we present the security framework for IMS and components of the security framework. Classification techniques for attack detection are explained in Section 4. Testbed and discussion on results are described in Section 5. In Section 6, we present the related work. We finally conclude the paper with an outlook to our future work.

2. IMS SECURITY REQUIREMENT

Functional entities separated by IP reference points provide a number of benefits in IMS in terms of application flexibility, reuse of common components and interoperability. However, this architecture also has its own set of drawbacks. Most importantly, distribution of IMS core network functions to different entities in an IP network provides greater number of opportunities for an attacker to break-in the IMS core. Therefore, IMS network is not only open for known IP-based vulnerabilities but also to a completely new set of IMS applications based vulnerabilities. The vulnerabilities are unique and real-time. These vulnerabilities include, but are not limited to, IMS framework-related vulnerabilities, session initiation protocol (SIP) vulnerabilities, media plane related vulnerabilities, authentication and encryption protocol vulnerabilities, Voice-over-IP (VoIP)/video/messaging/Push-to-talk-over-Cellular (PoC) spam and service abuse of IMS applications like VoIP, video, PoC, messaging, presence and conferencing [2]. We have identified eight different aspects in which our proposed IMS security framework must provide security. These include *access control*, *authentication*, *non-repudiation*, *data confidentiality*, *communication security*, *data completeness*, *availability* and *privacy*.
We can cater for all above-mentioned aspects if we secure the three types of information streams (control, media and management) which are transmitted over the IMS network. In Table 1, we have mapped different types of attacks that can be launched in the IMS network to different IMS components and streams. Every type of attack is the representative of a broader class of attacks.

Attacks Simulation and Performance: In typical DoS and DDoS attacks on an IMS network, large number of random or control messages are simultaneously sent from a single or multiple malicious nodes to overwhelm network's resource. The legitimate nodes can no longer communicate or use network services like Domain Name Server (DNS) or P-CSCF. IMS specifies IPSec as the preferred form of core-level network-layer security protocol; therefore, once tunnels are established with the packet data gateway (P-CSCF), the crafty attacker can readily launch huge floods of traffic, up to $10,000$ messages per second, which is equivalent to the traffic from 10 million subscribers.
Generally, malicious node(s) in DoS or DDoS attacks abuse or exploit vulnerabilities in the networking protocols. Relevant examples are ICMP SMURF attack, TCP-SYN flood, and UDP flood. The flood of messages is beyond the processing capability of the target host, thereby quickly exhausting its resources and denying services to its legitimate users. The nature of these flood attacks is very similar to what can be launched in other classical data networks, but the impact is much more devastating. The types of floods which are most damaging to IMS networks include Internet Key Exchange (IKE) floods, which are possible even before setting up the IPSec tunnel. SIP floods such as *register request floods* and *presence update floods* are also possible. These attacks can be easily launched using publicly available tools.
1-ICMP Flood Attack:
In SMURF attack, ICMP echoes a request to the broadcast address with the victim's address as source.
2-UDP Flood Attack:
In UDP floods, bandwidth is exhausted by sending large number of bogus UDP packets. Figure 2 and 2 show the impact of spoofed UDP flood attack on different components of IMS framework. It has significant impact on S-CSCF as it maintains the signaling path and provides applications support to the user. Any attack on this component will affect the availability of services to user for which he/she has subscribed. Since I-CSCF is needed when a device first tries to register with a P-CSCF which performs SIP registration, charging and resource utilization generation of Charging Data Records (CDR), and acts as a Topology Hiding Inter-working Gateway (THIG). A DoS attack on I-CSCF will not only affect user registration but also will be damaging for an operator's resources and assets, as it affects user charging who are already registered to the operator's network for different services.
3-TCP Flood Attack:
The most common form of DDoS attacks is TCP-SYN attacks. In these attacks, various malicious nodes distributed in the network, floods the victim node, running a TCP server, by sending TCP-SYN packets with forged source addresses. Consequently, the server allocates resources for the request. The connection state is maintained till timeout. As a result, the resources of the victim node are exhausted resulting in denial of service to legitimate nodes running TCP clients. This makes the protection even more difficult.
4-SIP Flood Attack:
DoS attack against a SIP system can occur through registration hijacking, proxy impersonation, message tampering, and session tear down. Strong authentication is rarely used, therefore, SIP processing components must trust and process SIP messages from possible attackers. DoS can take the form of malformed packets, manipulating SIP states, and simple flooding, such as a REGISTER or INVITE flood.

3. SECURITY FRAMEWORK FOR IMS

Now we propose our Bio-inspired, Artificial Immune System (AIS) based self-defending framework, AIS-IDP (Intru-

Table 1: Mapping of Attacks to IMS domains and streams

Attack name	IMS Layer Mapping	IMS Component Affected	Information Stream	Attack Type OSI Layer Mapping	Protocol
Presence Update Fuzzing	Session	P-CSCF,I/S-CSCF	Control, Management	Application Layer	SIP
IMS Register request Flood	Application,Session	I/S-CSCF,HSS	Control, Management	Application Layer	SIP
UDP Flood	Session	P-CSCF,I/S-CSCF	Control, Management	Transport Layer	UDP
TCP SYN Flood based DDoS attack	Session	P-CSCF,I/S-CSCF	Control, Management	Transport Layer	TCP
ICMP Flood	Session	P-CSCF,I/S-CSCF	Control, Management	Network Layer	ICMP

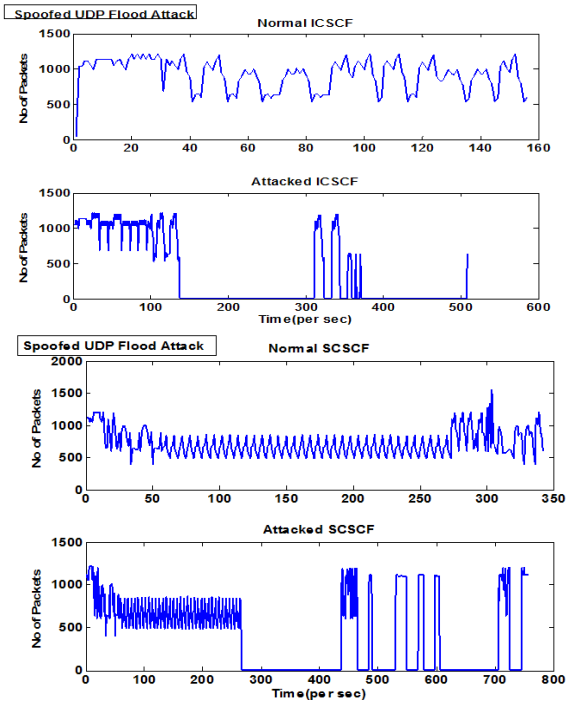

Figure 1: Spoofed UDP flood attacks

sion Detection & Prevention System) for IMS and Next Generation all-IP networks. Our goal is to design a generic security framework which is based on the principles of AIS. AIS have been extensively used for intrusion detection and prevention. An interested reader may find more applications in [8]. An important design consideration for the proposed framework is that it should have the ability to be integrated into the IMS core. Therefore, it will not only detect a majority of attacks but would also protect a user and the operator's assets, the network resources from misuse and other vulnerabilities resulting from previously unknown attacks. IMS network mostly consists of a number of handheld embedded devices such as cell phones and PDAs which are complexity-constrained. To this end, we show that our proposed AIS-IDP has much lower computational complexity then other solutions. Therefore, our proposed AIS-IDP would be an ideal solution for such complexity-constrained devices. The proposed solution will be deployed at the Home Subscriber Server (HSS), IMS Core (Proxy/Interrogating/ Serving Call State Control Functions (P/I/S-CSCF)), applications and media servers to monitor the network traffic in real-time. Figure 2 shows the framework for the proposed AIS-IDP.

IMS and NGN suffer from a unique set of vulnerabilities previously unknown in the data communications community [13]. A unique class of attack protocols namely *fuzzing* is a legitimate method of testing software systems for bugs. Malicious users, however, employ this same methodology to exploit vulnerabilities in a target system resulting in failures like application delays, information leaks, or even system crashes.

Our approach (AIS-IDP) follows the opposite philosophy, called *anomaly detection*. In anomaly detection systems, information collected about *normal* is used to differentiate anomalous activities from normal ones. Anomaly detection systems model the benign behavior of a system. Any deviation of the system from this behavior is an indication of an attack. Due to this, such schemes are able to detect previously unknown attacks. AIS provide an ideal framework to design and develop a real-time classification system for anomaly detection [8]. We believe that an anomaly based AIS paradigm will give us several key advantages. These include the flexibility to detect novel attacks, the formulation of a response to counter them and adaptation of its behavior via online learning.

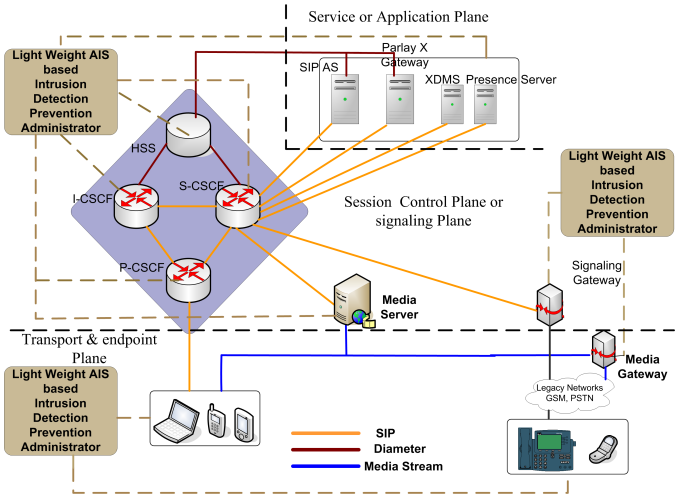

Figure 2: Framework of AIS-IDP

Components of AIS-IDP: A secure IMS framework must be able to counter the malicious attacks originated by the nodes within the network or being launched by the

external network entities. The security module must be able to analyze both packet's header and payload in real-time and maintain service transparency and at the same time must not degrade the performance of the IMS network. The key objective is to control/secure access to the IMS network and to protect its core and the underlying infrastructure. The secure access within the IMS framework is envisioned to allow only authenticated traffic to pass through different entities of the IMS core. Every user must be authenticated and a secure connection must be established between the user and the IMS network. However, protecting the rest of the IMS infrastructure demands protecting the network peering borders, IMS elements and protocols from intrusions. A light-weight AIS-IDP will provide an integrated solution against all types of attacks on IMS infrastructure with low computational complexity. We now briefly provide an overview of our proposed AIS-IDP and discuss its components. Figure 3 shows the functionality of our proposed system. AIS based solution needs to learn the normal behavior of a network host by analyzing the network traffic passing through it. During the learning phase, AIS-IDP collects "self-antigens", which define the *normal* state of the system. By the end of learning phase, a detector database is populated to be used in the protection phase. The detectors in the detector database only match to the "non-self" antigens. Due to stringent complexity and memory constraints, the size of the detector database must be small. The small detector database size would also reduce the search time during the protection phase because we need to match the network traffic with the detector database during the protection phase. The size of the database is variable and is mostly of the order of a few kilobytes. The detector database is shown at the top of Figure 3.

1-Network Layer 3 learning/detection module: The IMS network must be able to thwart flood, sweep, scan, malformed packets, spoofing and fragmentation attacks against IP, ICMP, IGMP protocols at the network layer of OSI reference model. If no anomaly is detected at this layer then the packet is handed over to the upper layer (i.e. Transport layer 4) for further processing (see Figure 3).

2-Transport Layer 4 learning/detection module: The IMS network must be able to prevent flood, sweep, scan, malformed packets, spoofing and fragmentation attacks against the UDP and TCP protocols. TCP-SYN flood based DDoS attacks are launched in the session layer of the IMS layered architecture and are mapped to the transport-layer of the OSI reference model (see Table 1). The Transport layer AIS-IDP module detects these different types of attacks at the transport layer of the OSI reference model and accordingly secures different components of the IMS network. If the packet is not detected as anomalous at this layer, then the packet is handed over to the application layer for further processing (see Figure 3).

3-Application Layer learning/detection module: Our proposed AIS-IDP enables the IMS network to have flow isolation to ensure that proper bandwidth and priority is given to a particular application flow. As a result, it can protect against theft of service within the application flows (i.e., user cannot receive streaming video bandwidth while only paying for streaming audio). This module detects all such types of attacks including DoS/DDoS, sweep, scan, malformed packets, spoofing, and fragmentation attacks against SIP, RTP, RTSP and IKE protocols by matching it with the detector database. If this filter also does not detect any anomaly, then the packet is allowed to propagate further to upper layer or respective application (see Figure 3).

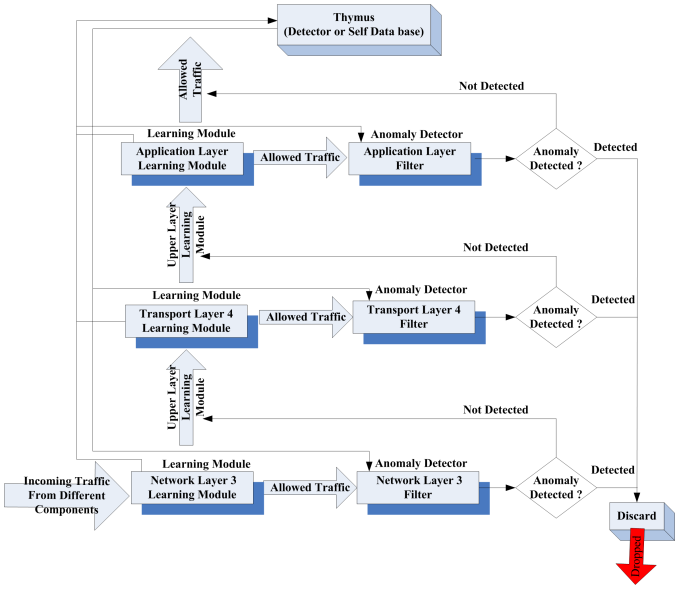

Figure 3: Packet processing in the protection phase of AIS-IDP

4. CLASSIFICATION TECHNIQUES FOR DOS AND DDOS ATTACK DETECTION

In the following subsections we compare two classification techniques for DoS and DDoS attack detection. First technique is our proposed AIS-IDP and the second technique is a classical cryptology based algorithm which uses signature based detection. We give an overview, parametrization and implementation details of the implemented schemes.

4.1 Artificial Immune System utilizing Negative Selection

Negative Selection was proposed by Forrest et al. [9] and derives inspiration from the adaptive immune system [8]. Lymphocytes (detectors) mature in thymus and undergo the negative selection. Only those lymphocytes survive the negative selection phase which do not match any self-antigens presented in the thymus (learning phase). The antigen representation is `<client ip, client port,server ip, server port, protocol>`. Further, we have used the Hamming distance matching rule. The matured lymphocytes have the ability to distinguish between the *self* and *non-self* antigens (see [8] for more details). AIS provides an ideal paradigm for designing, developing, implementing and realizing lightweight security framework which has relatively small overheads. Moreover, AIS does not put additional signature bytes in the packet's header or in its payload.

AIS-IDP Operations: Operation of AIS-IDP consists of two phases: *learning* and *protection*.

In the learning phase, the network is assumed to be free of *non-self* antigens and AIS-IDP defines *self* by profiling the normal behavior of the monitored system. AIS-IDP has a learning phase of 60 seconds. Algorithm 1 shows the learning

Table 2: Overhead Comparison of AIS-IDP and Signature based algorithm

Component Name	Normal Traffic AIS-IDP	Attacked Traffic AIS-IDP	Normal Traffic Signature based Algorithm	Attacked Traffic Signature based Algorithm
S-CSCF	144226 bytes (342 sessions)	171543 bytes (757 sessions)	157906 bytes (342 sessions)	207879 bytes (757 sessions)
I-CSCF	248138 bytes (156 sessions)	295297 bytes (508 sessions)	255625 bytes (156 sessions)	319681 bytes (508 sessions)
UE	60704 bytes (150 sessions)	64836 bytes (453 sessions)	67904 bytes (150 sessions)	86580 bytes (453 sessions)

Table 3: Detection Results for AIS

Component ID	Component Name	FP Rate (%)	TP Rate (%)
1	S-CSCF	1.7	98.3
2	I-CSCF	2.8	97.2
3	P-CSCF	6.1	93.9
4	HSS	3.3	96.7
5	UE1	7.7	92.3
6	UE2	7.8	92.2

second to run on a Pentium IV 1.83 GHz with core2 duo processor. The time required to create and verify 342 traffic signatures is 326.2000 seconds.

6. RELATED WORK

In this section, we briefly discuss the related work in the field of IMS security and Bio-inspired security systems. IMS security has received little attention, however, several research groups have started working in this field. In [7], authors have proposed the design and architecture of Intrusion Detection and Prevention (IDP) Supervisor for IMS and Next Generation all-IP Networks at IMS playground [3] and 3GB (Third Generation and beyond) Testbed [6] of FOKUS Fraunhofer in Germany. The products available in the market for intrusion detection and research work done are not specific to IMS and all-IP networks which is an emerging standard for Next Generation Mobile Networks. They are typically suitable for some specific network, application or environment such as Ethernet, Wireless Network or ad hoc network.

Bio-inspired techniques have been extensively used in the domain of network security. In [9] Hofmeyer et al proposed the general framework, ARTIS, based on the principles of negative selection, which was applied to computer intrusion detection system called LISYS (light-weight intrusion detection system). In [11],[12] the authors have proposed a security framework using principles of Artificial Immune System (AIS) for a nature inspired routing protocol called Beehive. In [10], the authors have used the danger theory inspired AIS for SYN scan detection.

7. FUTURE WORK & CONCLUSIONS

In this paper, we proposed a security framework for IMS. We presented the architecture of AIS for DoS and DDoS attacks on various layers of IMS. Our results show that the AIS-IDP provides very good detection accuracy with relatively lesser memory and computational overheads as compared to the signature based scheme. This makes AIS-IDP an ideal candidate to be integrated into the IMS framework. Our future work focuses on a comprehensive security solution for IMS and NGN all-IP networks to give protection at all layers. We want to extend this work to include different intelligent traffic features that would improve the performance of AIS in terms of detection accuracy. We also want to extend this work and compare the results of negative selection based AIS with other Bio-inspired techniques such as danger theory based AIS and machine learning schemes such as one-class Support Vector Machines (SVM).

8. REFERENCES

[1] Third Generation Partnership Project (3GPP), www.3gpp.org. 3GPP2,www.3gpp2.org.

[2] 3GPP Technical Specification of Security:http://www.3gpp.org/ftp/Specs/html-info

[3] IMS Playground: www.fokus.fraunhofer.de/ims

[4] Open IMS Core Testbed, http://www.openimscore.org

[5] Poikeselka, Mayer, Khartabil, Niemi, “The IMS IP Multimedia Concepts and Services”, Second Edition, 2006 Jhon Wiley & Sons, LTD.

[6] T. Magedanz, D. Witaszek, K. Knuettel, “The IMS Playground @ Fokus - An Open Testbed for NextGeneration Network Multimedia services”, Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005.

[7] M.Sher, T.Magedanz, “Secure Service Provisioning Framework (SSPF) for IP Multimedia System and Next Generation Mobile Networks”, 3rd International Workshop in Wireless Security Technologies, London, U.K., IWWST’05 Proceeding (101-106), April 2005.

[8] Leandro N. de Castro and Jonathan Timmis,”Artificial Immune Systems: A New Computational Intelligence Approach”,Springer,2002.

[9] Steven A. Hofmeyr and S. Forrest,”Architecture for an Artificial Immune System”, Evolutionary Computation Journal, pp. 443-473, 2000.

[10] J. Greensmith and U. Aickelin, “Dendritic Cells for SYN Scan Detection”, ACM GECCO, pp 49-56, 2007.

[11] N. Mazhar and M. Farooq,”BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc”, 6th International Conference on Artificial Immune Systems, Brazil, 2007.

[12] H.F.Wedde, C. Timm, and M. Farooq,”Beehiveais: A simple,efficient, scalable and secure routing framework inspired by artificial immune systems”, In PPSN, pages 623-632,2006.

[13] Kotapati,Liu,Sun,LaPorta,”Taxonomy of Cyber Attacks on 3G networks”,The Pennsylvania State University Park.

[14] J. Viega, Matt Massier, and Pravir Chandra, “Network Security with OpenSSL”, O’Reilly & Assoc., Inc, 2002.

[15] Juels and Brainard, “A Cryptographic Defense Against Connection Depletion Attacks”, RSA Laboratories.

[16] T. Fawcett,”ROC Graphs: Notes and Practical Considerations for Researchers”,TR (HPL-2003-4), HP Labs, USA.