SIP based Service QoS Parameters Impact Analysis According to DoS based Attack Rate

Hongbin Yim*, Jinwoo Hyun*, Hwankuk Kim**, Jaeil Jung*
Department of Electronics and Computer Engineering*, Applied Security Technology Team**
Hanyang University*, Korea Information Security**
17 Haengdangdong, Sungdonggu, Seoul*, 78 Garakdong, Songpagu, Seoul**
South Korea

Abstract: Telephone centric communication world was changed into Internet centric world and telephone network has been developing into IP based Internet telephony. Additionally, there are various applications according to Internet development and many Internet users want to be guaranteed a quality of service. However, DoS (Denial of Service) based attack was appeared a few years ago and attacks an enterprise server, a domain name server and a commercial network using the Internet vulnerability. The damage caused by DoS attack is increasing dramatically.

DoS based attack attacks the network and system resource to consume the whole capacity of network or system in a short period and the network or system cannot provide a VoIP (Voice over IP) or multimedia service to legitimate users. Finally, the service provider cannot provide an IP based real time multimedia service and cannot satisfy the requirement of multimedia users.

In this paper, we analyze the QoS (Quality of Service) parameters impact of SIP based application such as VoIP service according to DoS based attack rate using a simulation tool.

Key-Words: DoS, SIP, VoIP, QoS, Attack pattern, QoS parameter, Attack rate

1 Introduction

Converged services of broadcast and communication such as packet based Internet telephony and video on demand (VoD) are spread according to increase of interests for the next generation network. Telephone centric communication world was changed into Internet centric information and communication world and telephone network has been developing into IP based Internet telephony. Additionally, various applications have been appeared due to Internet development and many Internet users want to be guaranteed a quality of service.

Nowadays, Internet based VoIP technology is highlighted due to increase the number of Internet users and popularity of the Internet service.

However, DoS based attack was appeared a few years ago and attacks an enterprise server, a domain name server and a commercial network using the Internet vulnerability. The damage caused by DoS attack is increasing dramatically. DoS based attack can consume the whole capacity of network and system resources in a short period and the networks or systems cannot provide a VoIP or multimedia services to legitimate users. In recently, various multimedia services such as VoIP and VoD cannot be provided smoothly because of attack. IP based multimedia service cannot provide a real time characteristic and cannot satisfy the requirement of multimedia users caused by these kinds of problems.

In this paper, we research the relationship among the QoS parameters through QoS parameter impact analysis according to DoS based attack rate when DoS based attack is occurred.

This paper is organized as follows. Section 2 gives the related work and shows some DoS based attack patterns for the SIP application. Section 3 gives the QoS parameters and requirements of SIP application that are suggested by international standard. Section 4 shows a simulation environment, attack scenario, simulation results and the analysis of the simulation results. At the end of this paper, we give a conclusion and a future work.

2 Related Work

2.1 DoS based attack patterns

Many papers have been published about a DoS attack as increase of interests for the DoS based attack.

Mark Collier et al.[1] classify the DoS attack into 3 categories such as implementation flaw DoS, Flood DoS and Application DoS and define the DoS attack technique in an aspect of signaling and media. They suggest an attack defense scheme through the monitoring at the firewall to drop the malicious or illegal packets. This is a general attack defense algorithm against DoS attack so using a firewall and dropping the malicious packets is not an efficient defense algorithm against SIP application specific attack.

Andreas Steffen et al.[2] suggest an encryption algorithm using authentication, S/MIME, SRTP and IPsec. In other words, these kinds of defense algorithm is focused on proactive defense techniques to prevent attacks such as an eavesdropping, a session hijacking and a session tear down before attacking. These kinds of defenses are not a proper method against SIP application specific attack.

Dimitris Geneiatakis et al.[3] classify the SIP based attack into DoS based attack and privacy intrusion attack. Therefore, the defense algorithm is data encryption algorithms and this paper does not mention about maintaining a quality of service through the response against the attack.

A. H. Muhamad Amin et al.[4] simulate the performance measurement of VoIP QoS parameters on the Ethernet and wireless LAN environments. This paper use a H.323 and SIP as a signaling protocol and compare these two signaling protocols in terms of jitter and packet loss ratio. SIP protocol has a larger jitter than a H.323 protocol and these two signaling protocols have almost same packet loss ratio. The value of VoIP QoS parameters such as delay and jitter increase in case of applying the PPTP or IPsec algorithm for signaling protocols and this methods can degrade the quality of service. This paper compares two signaling protocol that is applied the encryption algorithms in terms of delay and jitter. However, this paper does not perform the analysis when the attack is occurred for the other components of SIP application such as a SIP proxy server or SIP application terminals.

Son et al.[5] simulate the flow based multimedia QoS monitoring in terms of throughput, delay, jitter and packet loss using an IPFIX(IP Flow Information eXpert). The authors analyze the video and audio streaming parameters through the simulation. The parameters such as throughput, delay, jitter and packet loss vary linearly according to the bandwidth. However, these results come from a simulation so an error of measurement can be occurred if it applies to the real network. Additionally, if the bandwidth decreases dramatically, the multimedia quality can be decreased exponentially and the service cannot be provided due to exhausting of the network or system resources.

As we mentioned in this subtitle, almost DoS based attack defense mechanisms are focused on the monitoring and applying the encryption algorithms. However, we cannot find out the variation of QoS parameters according to the DoS based attack patterns and attack rate. Therefore, we define the three attack patterns and find out relationship among the QoS parameters according to the three attack patterns and attack rate through analyzing the variation of SIP application QoS parameters.

2.2 DoS based attack patterns of SIP application

DoS attack is defined as service users are not provided a service by Internet service provider anymore due to exhausting of network or system resources. In the case of VoIP service, DoS attack interrupts the entire Internet service or normal operation of a specific VoIP service. Fig 1 shows the example of DoS attack.

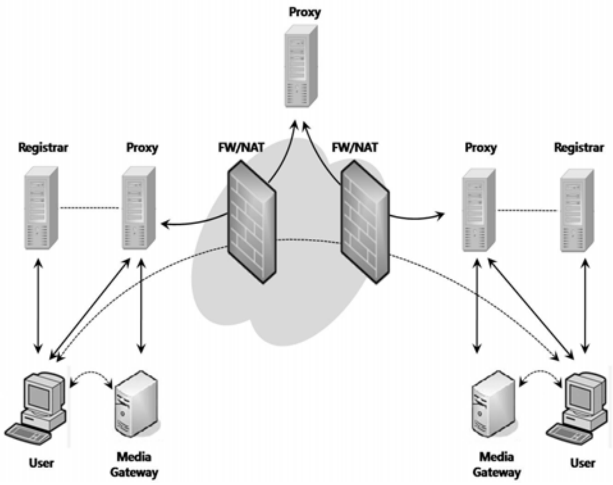

Fig 1. The example of DoS attack

DoS attack for SIP application is classified into three categories such as invite flooding, registration flooding and RTP flooding [6]. Invite flooding and registration flooding attack is similar to TCP SYN flood attack on the IP network.

Registration flood attack exhausts the resource of the SIP proxy server or registrar system as sending a lot of registration packet to request a connection. RTP flooding attack is a kind of attack using a voice or media related RTP packets that are modified the RTP header and payload by the attacker. The attacker sends a lot of modified RTP packets to the victim such as VoIP phone software to increase the call execution time and degrade the quality of the call.

In this paper, we measure and analyze the impact of QoS parameters that is affected by the attack traffic for the SIP proxy server, router and terminal according to attack patterns and attack rate.

3 The analysis of SIP application QoS

In general, Delay, jitter and packet loss are used as SIP based QoS parameters. However, it is difficult for real users to find out the relationship among the QoS parameters about SIP based application quality. In this section, we research the international standard of SIP application QoS parameters.

3.1 The research on SIP application QoS parameters

There are SIP application QoS parameters such as delay, jitter, packet loss rate. However, these parameters can be measured by UDP protocol QoS parameter measurement method.

In the case of SIP application, MOS (Mean Opinion Score) and R value are used as SIP application QoS parameters. MOS is a voice quality metric in an aspect of users and is defined as Table 1.

Table 1 MOS evaluation level

MOS level	Service quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

However, MOS method is depend on the subject view of the users and it varies by the judgement of the users about the quality and it has much time to do the same simulation at all cases. To solve this problem, ITU-T G.107 suggests the objective measurement method known as E-Model[7].

E-Model is suggested by ITU-T G.107. E-Model is a computational model that is measured by network delay and impairment. E-Model has a range of R value from 0 to 100 that is calculated using network delay and impairment. Fig 2 shows the mapping relationship between MOS and R value.

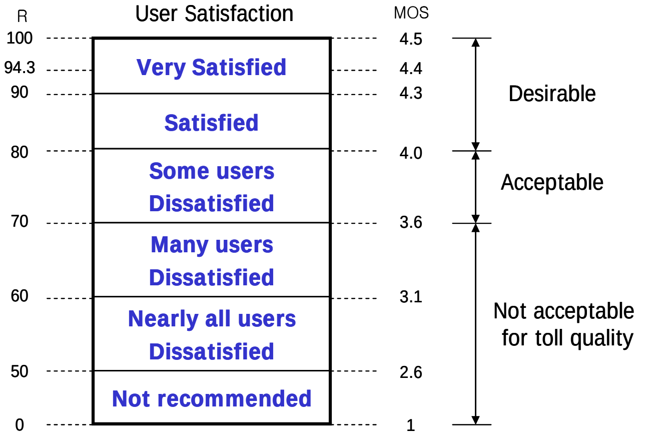

Fig 2 MOS Voice Quality Classes

3.2 The relationship between R value and satisfaction of users

R value is defined as equation 1.

$$R = (R_0 - I_s) - I_d - I_e + A \quad (1)$$

The description of parameters of R value are as follows.

- o R_0 : The basic signal-to-noise ratio. The default value of this parameter is 100.
- o I_s : The factor Isis the sum of all impairments which may occur more or less simultaneously with the voice transmission.
- o I_d : the impairment factor representing all impairments due to delay of voice signals
- o I_e : The values for the Equipment Impairment Factor Ie of elements using low bit rate codecs are not related to other input parameters. They are depending on subjective mean opinion score test results as well as on network experience.
- o A : Due to the specific meaning of the advantage factor A, there is no relation to all other transmission parameters.

The R_0 , I_s and A of the parameters have no relation with voice quality because these parameters is not a impairment due to transmission on the IP network. Therefore, the degree of the quality impairment is decided by I_d and I_e. R_0, I_s and A follow the default value of ITU-T G.107. The default value of R_0, I_s and A is 94.2, 1 and 0 respectively.

Table 2 shows the mapping relation between MOS and R value derived from the equation 1 and Fig 2[8][9].

Table 2 The relationship between R value and the satisfaction of users

R value	Quality level	MOS	satisfaction of users
$90 \le R < 100$	Best	4.34 ~ 4.5	very satisfied
$80 \le R < 90$	High	4.03 ~ 4.34	satisfied
$70 \le R < 80$	Medium	3.60 ~ 4.03	some users dissatisfied
$60 \le R < 70$	Low	3.10 ~ 3.60	many users dissatisfied
$50 \le R < 60$	Poor	2.58 ~ 3.10	nearly all users dissatisfied

4 Simulation

In this section, we analyze the SIP application QoS parameter using a simulation tool.

The background of this simulation is as follows.

It is difficult to make an attack situation on the real network environment. If the attack traffic is generated, the network components are affected by the attack traffic not only simulation testbed but also the components of the real network. Additionally, we can make a scalable network using a simulation tool. The real network testbed is restrict to the number of node that can be attached and we can estimate that the impact of the QoS variation by the mapping of simulation results and real test results.

4.1 Simulation environment and scenario

We use the Qualnet 4.5 tool for this simulation and the simulation environment according to the network components is as Table 3.

This simulation has 2 VoIP connections. One is the single domain connection and the other is multi-domain connection. Each case has 3 different attack scenarios according to attack model such as RTP flooding attack, invite flooding attack and registration flooding attack. In this simulation, attack rate increase from 2,000 packets per second to 8,000 packets per second for every attack model. The victim is the router and terminal for the RTP flooding attack model. In case of invite and registration flooding attack, the victim is SIP proxy server.

Table 3 Network component of simulation

Component	Number of components
Attackers	8
Single domain connection	1
Multi-domain connection	1
RTP Flooding attack period(Scenario 1)	50sec~130sec
INVITE/REGISTRATION attack period(Scenario 2)	50sec~130sec
Terminal attack period (Scenario 3)	50sec~130sec
VoIP application execution period	60sec~240sec

4.2 Simulation results

From fig 3 to fig 6 shows the delay, jitter, MOS and R value graph respectively when router is attacked. The single domain connection is not affected by the router attack. However, the connection between domains is affected by the attack. As the attack rate increases from 2,000 packets per second to 7,000 packets per second, the connection between domains is not failed until the resource of router is consumed totally by the attack traffic. However, the connection between domains is failed at the rate of 8,000 packets per second.

In the case of router attack, VoIP QoS parameters of the connection between domains are affected by the attack greatly and the delay is 3 times than that of single domain connection.

MOS graph is very similar with R value graph in the all cases of this simulation because the relationship between MOS and R value is mapping according to E-model.

MOS and R value can be calculated using the delay according to equation 1.

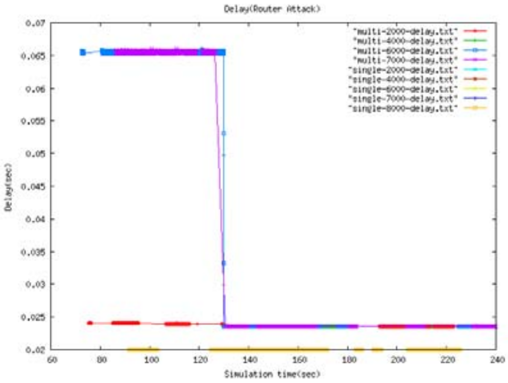

Fig 3 Delay graph of router attack

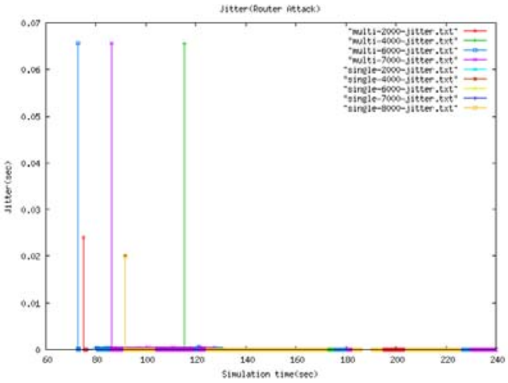

Fig 4 Jitter graph of router attack

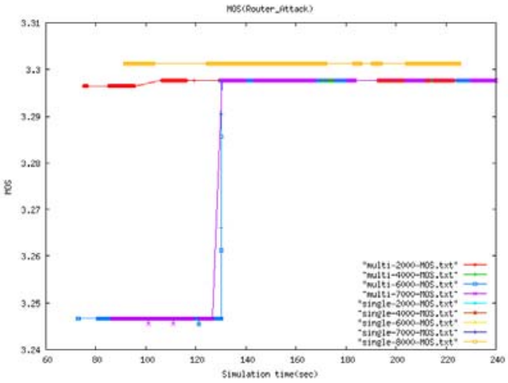

Fig 5 MOS graph of router attack

From fig 7 to fig 10 shows the delay, jitter, MOS and R value graph respectively when SIP proxy server is attacked. In the case of SIP proxy server attack, the connection between domains is failed at the rate of 8,000 packets per second. This result is very similar with the case of router attack. However, the delay of the router attack is greater than that of SIP proxy server attack in the attack period. This means QoS parameter is not affected by SIP proxy server attack because the RTP packets are transmitted by the router after call setup.

In this case, the difference of delay between the single domain connection and multi-domain connection is small because SIP proxy server is used for only call setup. This difference of delay is caused by the path length between domains. In this case, there is no problem to set up the call until the attack traffic reaches the threshold of call processing rate of SIP proxy server. However, if the attack traffic overwhelms the threshold of call processing rate of SIP proxy server then VoIP connection is failed.

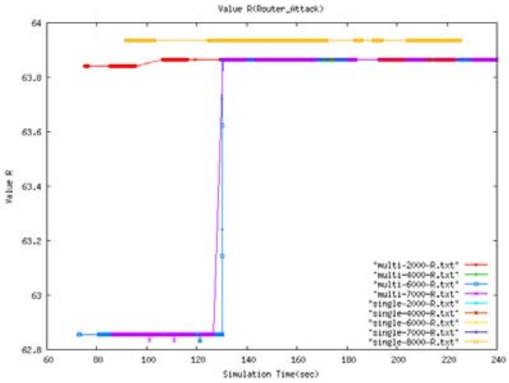

Fig 6 R value graph of router attack

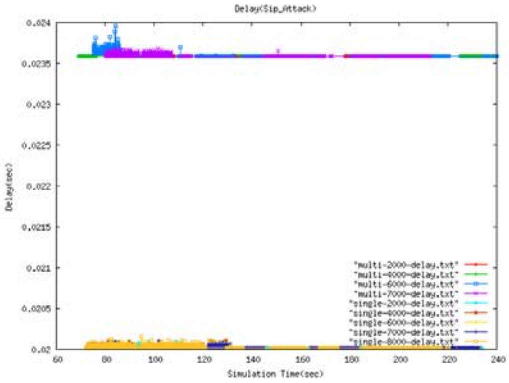

Fig 7 Delay graph of SIP proxy attack

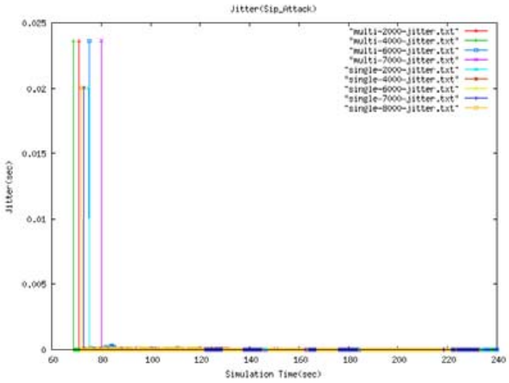

Fig 8 Jitter graph of SIP proxy attack

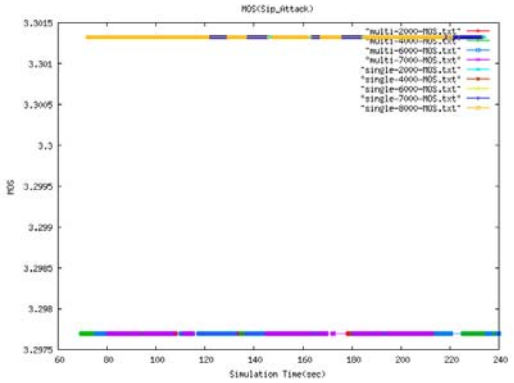

Fig 9 MOS graph of SIP proxy attack

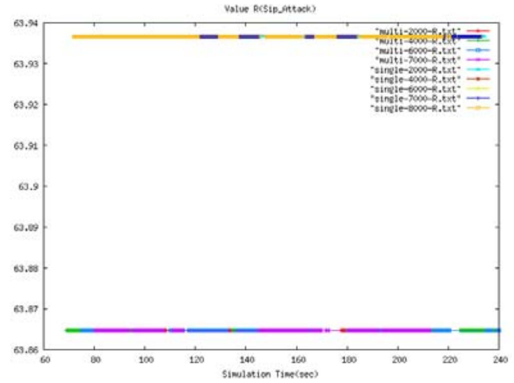

Fig 10 R value graph of SIP proxy attack

From fig 11 to fig 14 shows the delay, jitter, MOS and R value graph respectively when terminal such as UA is attacked. The victim of the attack is the terminal that belongs to the multi-domain connection in this simulation environment. In this case, the other terminals are not affected by the attack except the victim. The delay of the victim terminal increase over 140ms and this delay is not proper the interactive application such as VoIP service. Moreover, the multi-domain connection is failed at the attack rate of 3,000 packets per second and this rate is less than half of the other attack rate such as router or SIP proxy server attack for the connection failure.

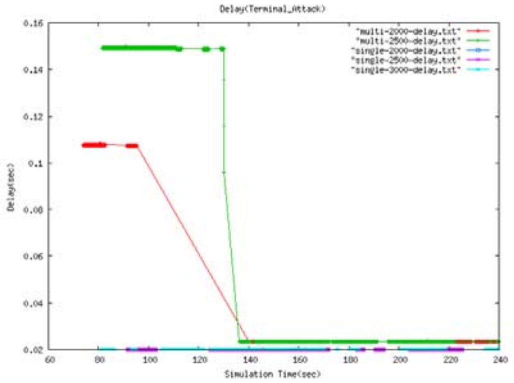

Fig 11 Delay graph of terminal attack

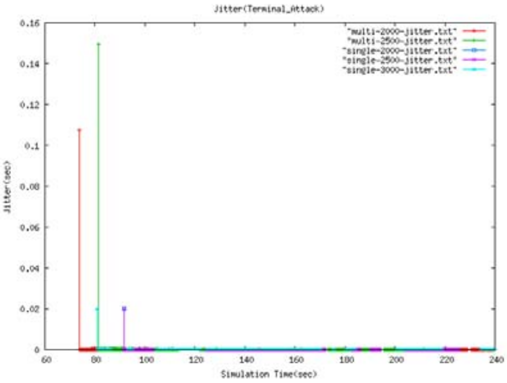

Fig 12 Jitter graph of terminal attack

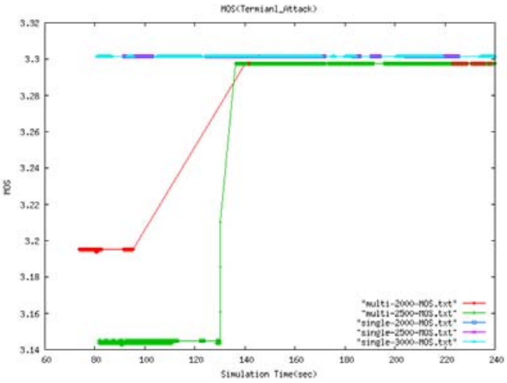

Fig 13 MOS graph of terminal attack

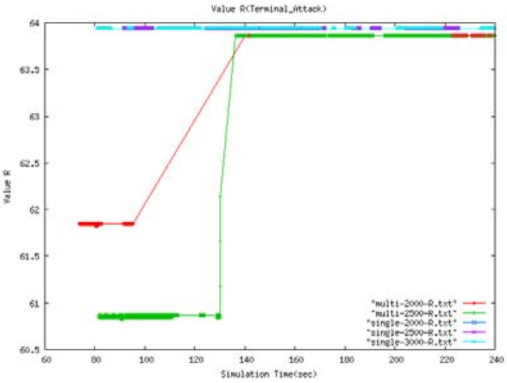

Fig 14 R value graph of terminal attack

4.3 Analysis of Simulation results

In the case of router attack, the delay and jitter increase greater than that of SIP proxy server attack because router transmits the RTP packet between VoIP terminals such as user agent after call setup.

The terminal attack scenario is most sensitive by the attack rate among three scenarios.

In the case of SIP proxy server attack, it can disturb the call setup between terminals after attack traffic reaches the threshold of SIP call processing rate. However, QoS parameters are not affected by the SIP proxy server attack after call setup.

5 Conclusion

In this paper, we analyze the QoS impact according to DoS based attack rate through three scenarios such as invite flooding attack, registration flooding attack and RTP flooding attack.

When the attack occurs for the router, SIP proxy server and terminal, we consider the VoIP QoS parameters such as delay, jitter, MOS and R value according to increase attack rate. In conclusion, terminal attack is most sensitive by DoS based attack and SIP proxy server attack is least sensitive for the VoIP service after call setup is completed.

In the case of router attack and SIP proxy server attack, router and SIP proxy server can provide service until the resource is exhausted by the attack traffic. However, delay is varied greatly in the case of router attack.

In the future, we will analyze the VoIP QoS parameters impact if the intrusion prevention system is applied to the network to prevent the DoS based attack traffic. Moreover, we will research the intrusion response algorithm to minimize the QoS parameters impact by the DoS based attack.

Acknowledgement

This work was supported by the IT R&D program of MKE/IITA. [2008-S-028-01, The Development of SIP-Aware Intrusion Prevention Technique for protecting SIP-base Application Services]

References:

[1] Mark Collier, Voice Over IP(VoIP) Denial of Service(DoS), *Proceedings of the IEEE*, Vol.90, No.9, 2002, pp.1495-1517.

[2] Andreas Steffen, Daniel Kaufmann, Andreas Stricker, SIP Security, *E-Science and Grid, Ad-hoc network*, Verlag, 2004, pp.397-410.

[3] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, S. Gritzalis, SIP security mechanisms: a state-of-the-art review, *Proceedings of the Fifth International Network Conference(INC 2005)*

[4] A.H.Muhamad Amin, VoIP Performance Measurement Using QoS Parameters, *International Conference on Innovations in Information Technology 2005*

[5] Mark Collier, Basic Vulnerability Issues for SIP Security, *Research Report 2005*

[6] Son et al., Flow-level QoS Monitoring of Multimedia Streaming Traffic with IPFIX, KNOM 2007

[7] ITU-T G.107

[8] ITU-T G.1010

[9] ITU-T Y.1541

[10] ITU-T P.800.1