

# 보안관리를 위한 SIP 시험 시뮬레이터 설계 및 구현\*

장 성 만\*\* · 길 민 욱\*\*\* · 이 극\*\* · 김 귀 남\*\*\*\*

## 요 약

차세대 VoIP 통신망 운영에 있어서 시급히 해결해야할 문제점 중 하나가 통신보안에 관련된 부분이다. SIP 기반의 망을 운영 및 프로토콜 스택을 개발한 후에는 일반적인 기능 시험을 비롯하여 보안성 기능 시험을 위한 시험 시나리오의 생성, 시험 환경의 구축, 적합성 시험 기술 등에 대한 연구 및 개발이 필요하다. 따라서 본 논문에서 개발하고자 하는 부분은 SIP를 적용시 보안관리의 기초로 삼기위한 SIP 보안시험 환경 개발 및 SIP 시험 프로그램을 개발하는 것이다.

## Design and Implementation of SIP Testing Simulator for Security Management

Sung-Man Jang\*\* · Min Wook Kill\*\*\* · Geuk Lee\*\* · Kuinam J. Kim\*\*\*\*

### ABSTRACT

One of the most important part in next generation VoIP is security management. When we develop a protocol stack based on SIP (Session Initiation Protocol), it is necessary to develop test scenario, test environment, adaptation test technology for security test of the system. In this paper, we design and implement security test environment and test program for SIP. This system also can be used as a fundamental system when someone develop a communication system based on SIP.

\* 본 논문은 2003년 한남대학교 교비연구비 지원으로 이루어진 연구 결과입니다.

\*\* 한남대학교 컴퓨터공학과

\*\*\* 문경대학 인터넷정보계열

\*\*\*\* 경기대학교 정보보호기술공학과

## 1. 서 론

VoIP(Voice over IP)는 데이터 통신을 위하여 사용하고 있는 인터넷에서 기존의 공중전화망과 같은 서비스를 구현해 보려는 시도로부터 시작되었다.

VoIP를 구현하기 위한 다양한 프로토콜 중에서 SIP(Session Initiation Protocol)의 특징은 웹과 연동해 다양한 인터넷의 기능을 활용할 수 있다는 점이다. 따라서 SIP를 사용하게 되면 인터넷을 활용해 통신환경을 제어할 수 있을 뿐만 아니라 다양한 부가기능을 실현할 수 있게 된다[1].

이러한 인터넷 기반의 통신 시스템 환경에서의 보안성 문제가 심각하며 특히, 통신보안의 보호 문제는 정보통신 사회의 선결과제가 된다. 따라서, SIP에 적합한 보안관리를 위한 기능 시험이 요구된다.

본 논문에서는 SIP 기반의 네트워크에서의 보안 문제와 관련하여 SIP 보안관리를 위한 시험 시뮬레이터를 개발하고자 한다. SIP 시스템 자체의 보안관리 기능에만 초점을 맞추며, 기존의 네트워크 구성 요소인 방화벽 우회 또는 NAT(Network Address Translator) 통과 등의 문제는 다루지 않는다.

본 연구에서는 SIP 기반 네트워크 환경에 적합한 보안관리 모델을 다루며, 시뮬레이터를 이용하여 SIP 보안 성능을 검증한다.

본 연구의 2장 관련연구에서는 SIP에 대하여 살펴보고 3장에서는 SIP 시험 시뮬레이터 구성 제안 및 설계한다. 4장에서 시뮬레이터 구성을 바탕으로 시험 시나리오를 작성하며, 끝으로 5장에서 결론을 맺는다.

## 2. SIP 개요

SIP는 IETF에서 1997년에 Internet Draft 1.0 버전으로 제안되어 1999년에 RFC2543 표준으로

공식으로 채택되었다.

VoIP 구현을 위해 주로 사용되는 프로토콜은 현재 가장 많이 쓰이는 ITU-T에서 제시한 H.323과 IETF의 SIP은 매우 간단한 텍스트 기반의 응용계층 제어 프로토콜로서, 하나 이상의 참가자들이 함께 세션을 만들고, 수정하고 종료할 수 있게 한다. 이러한 세션들에는 인터넷을 이용한 원격회의, 전화, 면회, 이벤트 통지, 인스턴트 메시징 등이 포함된다. SIP는 H.323이 갖고 있는 이러한 문제점을 보완하면서 웹에서 사용되는 프로토콜 및 멀티캐스티 망에서 사용되던 세션 제어 및 표현 프로토콜을 이용하여 매우 간단하고 인터넷에 친화적인 이용자들이 쉽게 사용할 수 있도록 개발된 프로토콜이다[2].

### 2.1 SIP 프로토콜 구성 요소

SIP는 프로토콜의 관점에서 텍스트 기반의 프로토콜이며 헤더 필드는 HTTP(Hypertext Transfer Protocol)와 유사하다. 메시지는 두 가지 종류이며 클라이언트에서 시작된 요청(request) 메시지와 서버로부터 응답(response) 메시지이다. SIP는 클라이언트들이 호출을 시작하면 서버가 그 호출에 응답을 하는 클라이언트/서버 구조에 기반을 두고 있다.

메시지는 헤더(header)와 바디(body)로 구성되며 텍스트 문자로 작성된다. 헤더는 SIP 제어 정보를 포함하며, 바디는 호 설정 시에는 오디오 및 비디오 코덱과 같은 양측의 능력을 협상하기 위한 정보를 SDP(Session Description Protocol) [3] 형식으로 기술한다[4]. 바디는 다양한 멀티미디어 정보를 포함할 수 있으며 바디 정보는 SIP 헤더인 "content-type"에서 MIME(Multipurpose Internet Mail Extension) 형식으로 표시한다. 메시지 교환은 HTTP와 동일하게 요청/응답(Request/Response) 형태로 이루어진다. 헤더와 바디는 공백라인으로 구분된다. 기본적인 클라이언트의

요청 메시지는 6가지이며, 서버측의 응답 메시지는 숫자로 그 의미를 나타낸다. 요청/응답 메시지의 의미는 아래 <표 1>과 같다[5].

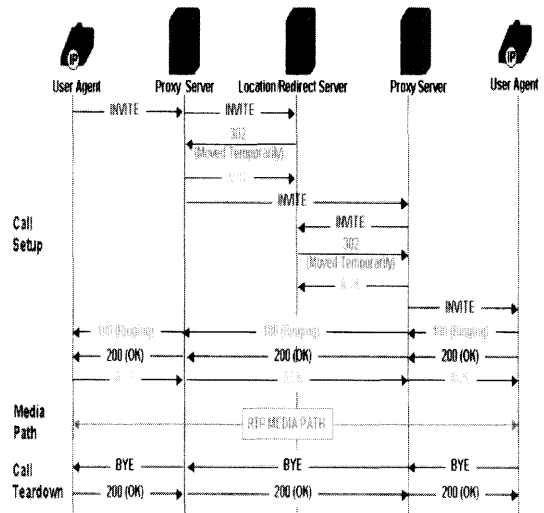
<표 1> SIP 요청/응답 메시지

요청 메시지		응답 메시지	
메시지	의 미	메시지	의 미
INVITE	호 요청	1xx	호의 현재 상태 (Informational)
ACK	INVITE에 대한 최종 응답	2xx	성공(Success)
BYE	호 해지	3xx	클라이언트의 호 설정 요청에 대해 SIP 서버가 착신측의 위치정보를 클라이언트에게 전송(Redirection)
CANCEL	호 설정 도중 호 해지	4xx	클라이언트 에러 (Client Error)
OPTIONS	능력치 (Capability) 정보 요청	5xx	서버 에러 (Server Error)
REGISTER	위치정보 등록, 삭제, 수정	6xx	서버측 지원 불가 (Global Failure)

### 2.2 SIP 구성 요소

SIP 구성 요소는 크게 사용자 에이전트와 서버로 이루어져 있다. 사용자 에이전트는 송신자 기능을 수행하는 사용자 에이전트 클라이언트(UAC : User Agent Client)와 수신자 기능을 수행하는 사용자 에이전트 서버(UAS : User Agent Server)로 분류된다[6]. SIP 서버는 프록시(proxy) 서버, 리다이렉트(redirect) 서버, 등록(registrar) 서버, 로케이션(location) 서버, 게이트웨이(gateway)로 구분된다. 프록시 서버는 UAC로 전달받은 SIP 요청 메시지를 상대방 UAS로 전달하기 위해 경로상의 다른 SIP 서버로 요청 메

시지 전달을 수행한다. 리다이렉트 서버는 UAC의 SIP 요청 메시지를 수신하면 상대방 UAS와 연결되기 위한 서버의 주소를 UAC에게 알려줌으로써 UAC가 직접 다음 서버에 요청 메시지를 보낼 수 있도록 한다[7]. 등록 서버는 도메인 네임 서비스(DNS)와 비슷하게 각 SIP 서버의 위치를 알려주는 기능과 사용자의 위치 정보를 등록 및 갱신하는 역할을 수행한다. 로케이션 서버는 SIP 서버 및 사용자의 위치를 찾는 기능을 수행한다[8]. 게이트 웨이는 인터넷의 패킷망과 공중전화망의 회선교환망간의 변환을 담당한다. 아래(그림 1)은 SIP의 각 구성 요소 및 구성 사용자간의 호 설립 절차를 나타낸다[9].



(그림 1) SIP 구성 요소 및 호 설립 절차

### 3. SIP 시험 시뮬레이터 설계 및 구현

본 논문에서 개발하고자 하는 부분은 SIP를 사용하는 네트워크에서 에이전트 시험 환경 개발 및 SIP 사용자 에이전트 시험 프로그램을 개발하는 것이다. 또한 이들 각 SIP 사용자 에이전트에 대한 시험 시나리오 개발과 시험하고자 하는 기능을 정의하고 테스트 베드를 구축하고 SIP

사용자 에이전트 기능을 시험하는 소프트웨어를 포함한다.

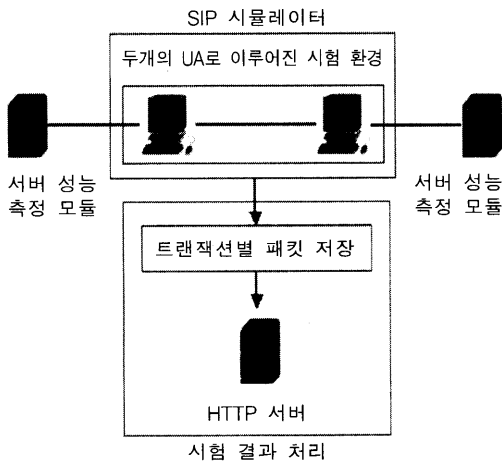
테스트 표준은 SIP RFC3261 표준 문서를 기준으로 작성되었다.

SIP 프로토콜 시험 시뮬레이터는 리눅스(Linux) 운영체제를 바탕으로 하였으며, SIP 프로토콜이 랜 환경에서 실행될 경우의 서버 성능 분석 모듈은 솔라리스(Solalis)를 기반으로 작성되었다.

### 3.1 RFC3261 표준 문서에 따른 테스트 플랜 개관

SIP 표준은 비교적 잘 정의되어져 있으며, 여기에 따른 몇몇 개의 사용 가능한 무료 사용자 에이전트(User Agent)가 개발 되어있다. 이러한 SIP와 상호 운영가능한 사용자 에이전트를 표준 문서에 따른 시험 계획을 설계한다. 이런 특징은 정량적으로 측정 가능한 실증 시험을 실시할 수 있는 기반이 된다.

### 3.2 Web-based SIP 프로토콜 시험 시뮬레이터 구조(모듈 구성 요소)



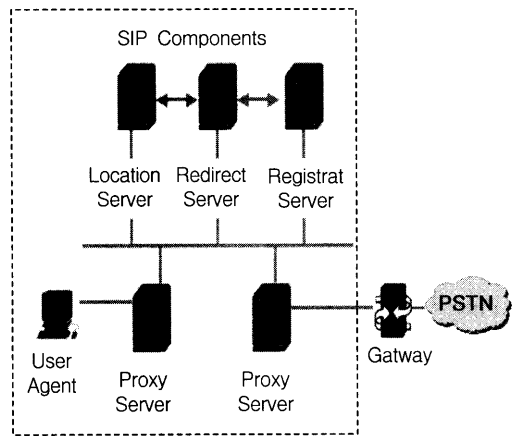
(그림 2) 시뮬레이터 전체 구조

SIP 시험 시뮬레이터는 사용자 에이전트의 성능을 검증하기 위한 구조로 되어 있다. 단순한 콘솔상의 모니터링을 넘어서 HTTP 서버에서 넘겨주는 정보를 웹 브라우저를 이용하여 각 수행단위별로 손쉽게 확인할 수 있도록 하였다. 또한 사용자 에이전트 실행시의 서버의 성능 측정을 하여 서버의 수용 능력을 측정 할 수 있다. 이를 위해 간단한 HTTP 서버를 구현하였으며, 성능 측정 도구를 구현하였다. 망 구성은 두 개의 사용자 에이전트로 구성하였으며, 각 사용자 에이전트의 부하를 측정하기 위한 성능 측정 도구를 각각 탑재하였다. 전체적인 구조는 아래 (그림 2)과 같다.

## 4. 시험 시나리오

SIP 사용자 에이전트를 시험함에 있어서 시뮬레이터와 Test를 구성함은 다음과 같이 간략히 나타낼 수 있다.

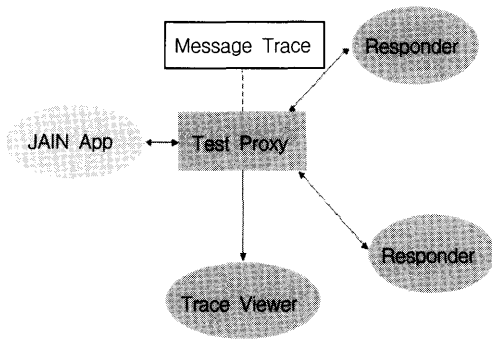
예를 들어 아래와 같이 SIP의 구성 요소가 분산된 구조의 SIP 사용자 에이전트 테스트 망이 있다고 가정하자(그림 3).



(그림 3) 분산된 SIP 망 구조

본 망을 TEST 하기 위해서는 SIP 구성 요소

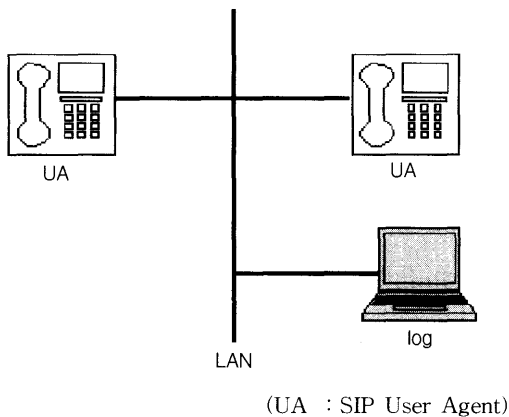
가 실제로 필요할 것이다. 또한 각 구성 요소간의 인터페이스가 필요하다. 하지만, 본 시뮬레이터를 이용 아래와 같이 설정, 각각에 대한 SIP 사용자 에이전트 동작 및 상태, 스트레스 시험 등을 확인할 수 있다(그림 4).



(그림 4) SIP 시뮬레이터 도식도

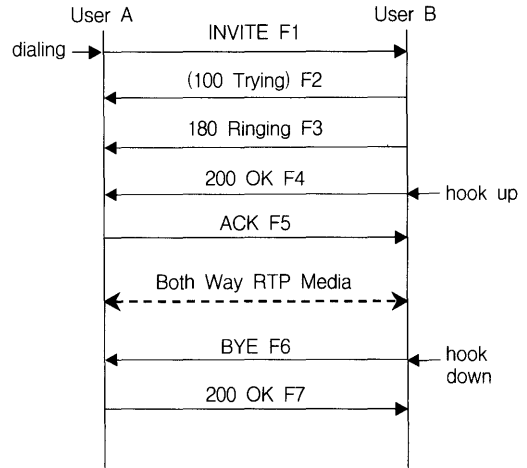
#### 4.1 사용자 에이전트간의 메시지 전송 시험

이 영역의 시험은 두 개의 사용자 에이전트들간의 정확한 연결 설정을 검증한다. 이 시험을 위한 환경 설정은 랜 환경에서 SIP 송·수신 에이전트 호스트와 에이전트간의 전송되는 모든 메시지를 기록하고 저장하기 위한 시험 호스트로 구성된다(그림 5).



(그림 5) UA-to-UA 시험환경

이를 위한 간단한 호 설정 절차는 아래 그림과 같다(그림 6).



(그림 6) UA간의 호 설정 흐름

#### 4.2 호 초기화 시험(Call Initiation)

송신자는 UDP 초대(INVITE) 메시지를 수신자에게 전송하여 호를 초기화시킨다. 초대 메시지를 받은 수신자는 호를 허락할 경우 송신자에게 UDP를 이용하여 200 OK를 보낸 후에 ACK 메시지를 송신자에게 전송한다. 송신자의 초대 메

〈표 2〉 호 초기 설정 시험

Via field	송·수신자 패킷이 Via field의 표준형식을 만족는가?
To, From field	송·수신자 패킷이 To, From field의 표준형식을 만족는가?
Content-Type	Content-Type 헤더가 미디어 정보를 지정하고 있는가?
request line	request line 표준형식을 만족하는가?
CSeq	CSeq가 포함되어 있고 CSeq 숫자 뒤에 INVITE 태그를 포함하는가?
Call-ID	Call-ID가 송·수신자 양쪽에 포함되어 있는가?

시지 내부의 SDP는 코덱의 종류를 알려준다. 만약 수신자가 송신자가 제공한 코덱을 수용할 수 있으면 200 OK를 돌려준다.

이 시험은 코덱을 이용한 미디어의 교환까지 양 사용자 에이전트간에 이루어진 경우에만 완전한 연결이 성립된 것이다.

이 과정에서 이루어진 패킷은 위의 항목을 만족하여야 한다.

#### 4.2.1 송신자 측에서의 호 종료시험(Call Termination by Sender)

호의 설립이 정상적으로 이루어진 후에 송신자 측에서 호를 종료하는 상황을 가정한다. 송신자는 UDP BYE 메시지로 연결 해제 의사를 알린다. 이 메시지를 받은 수신자는 200 OK 메시지를 송신자에게 전송하여 호를 종료하게된다. 호가 종료되면 미디어 교환(음성)은 더 이상 일어나지 않는다.

이 과정에서 이루어진 패킷은 다음 항목을 만족하여야 한다.

〈표 3〉 송신자 측에서의 호 종료시험

6 Call-ID	BYE 메시지 내의 Call-ID 숫자는 연결 초기 INVITE와 동일해야 한다.
CSeq	BYE 메시지 내의 CSeq 숫자는 연결 초기 INVITE 보다 커야한다.
CSeq method tag	BYE 메시지 내의 CSeq method tag는 BYE이어야 한다.
To, From field	연결 초기 INVITE 메시지 내의 To, From field와 같아야 한다.
BYE	BYE 메시지는 Via field를 포함해야 한다.

#### 4.2.2 수신자 측에서의 호 종료시험(Call Termination by Receiver)

호의 설립이 정상적으로 이루어진 후에 수신

자 측에서 호를 종료하는 상황을 가정한다. 수신자는 UDP BYE 메시지로 연결 해제 의사를 알린다. 이 메시지를 받은 송신자는 200 OK 메시지를 송신자에게 전송하여 호를 종료하게된다. 호가 종료되면 미디어 교환(음성)은 더 이상 일어나지 않는다.

이 과정에서 이루어진 패킷은 다음 항목을 만족하여야 한다.

〈표 4〉 수신자 측에서의 호 종료시험

Call-ID	BYE 메시지 내의 Call-ID 숫자는 연결 초기 INVITE와 동일해야한다.
CSeq method tag	BYE 메시지 내의 CSeq method tag는 BYE이어야 한다.
To field	연결 초기 INVITE 메시지 내의 From field와 같아야 한다.
From field	연결 초기 INVITE 메시지 내의 To field와 같아야 한다.
BYE	BYE 메시지는 Via field를 포함해야 한다.
URI	BYE 메시지내의 URI 요청은 INVITE 메시지의 From field와 같아야 한다.

#### 4.2.3 호 연결 거부 시험(Call Rejection)

수신자 측에서 호 연결 수락을 거부한 경우를 가정한다. 수락 거부는 600 또는 400 클래스(class)의 응답을 송신자에게 전송한다. 이 메시지를 받은 송신자는 수신자에게 ACK 메시지를 전송하여 호 연결 수락이 거부되었음을 인식하게 되고 미디어 교환은 일어나지 않게 된다.

〈표 5〉 호 연결 거부 시험

Call-ID	Call-ID 숫자는 연결 초기 INVITE와 동일 해야한다.
To, From field	To, From field는 연결 초기 INVITE와 동일해야한다.
CSeq	CSeq 숫자는 연결 초기 INVITE와 동일 해야한다.

이 과정에서 이루어진 패킷은 위의 항목을 만족하여야 한다.

#### 4.2.4 호 전환(Call Redirection)

수신자 측에서 호 전환이 일어난 경우를 가정한다. 수신자는 송신자에게 300 클래스의 응답을 전송한다. 이 메시지를 받은 송신자는 ACK 메시지로 수신자에게 응답한다. 이 후에 송신자가 호 전환이 이루어졌음을 인식하고 완전한 연결이 성립되지 않았으므로 미디어 교환은 일어나지 않는다.

#### 4.2.5 TCP를 이용한 호 설정

여기서는 UDP 대신 TCP를 이용하여 송·수신자간에 호를 설정하는 것을 가정한다.

이 과정에서 이루어진 패킷은 다음 항목을 만족하여야 한다.

〈표 6〉 TCP를 이용한 호 설정

Via Field	Via Field는 SIP/1.4/TCP로 명시한다.
port	TCP 연결을 위해 수신자는 송신자가 지정한 포트로 응답한다.
request	request는 재전송되지 않는다.

#### 4.2.6 호 재 설정 능력 시험

호의 설립이 완전하게 이루어진 후에 호를 재 설립할 필요가 있을 경우를 가정한다. 송신자가 현재 연결된 호에 사용되고 있는 미디어 등을 재 설정하고자 하는 경우에 이용되며 송신자는 수신자의 가능한 미디어 종류를 알고 있다고 가정한다. 송신자는 INVITE 메시지를 수신자에게 재 전송한다. 만약 수신자가 변경된 호를 수용할 능력이 있는 경우 200 OK를 송신자에게 전송한다. 그렇지 않으면 400 클래스의 메시지를 전송하여 기존의 미디어를 계속 사용하여 호를 유지한다. 이 시험은 사용자 에이전트가 미디어를 호

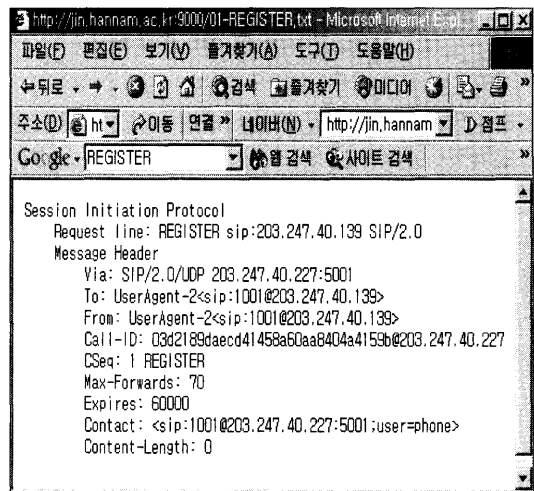
가 설립된 중간에 변경할 수 있는지를 검증한다.

〈표 7〉 호 재 설정 능력 시험

INVITE	송신자는 새로운 INVITE를 생성하여 수신자에게 전송한다.
CSeq	새로운 INVITE는 원래의 INVITE CSeq 숫자보다 커야한다.
SDP	SDP 내의 버전 번호는 증가되어야 한다. SDP는 새로운 페이로드 유형 숫자(payload type number)를 가진 새로운 미디어 코덱을 지시해야 한다.
200 OK 또는 400 클래스 응답	수신자가 호 재 설정을 수락할 경우 200 OK 전송, 그렇지 않으면 400 클래스의 메시지를 전송한다.
ACK	송신자는 수신자에게 ACK를 전송한다.

#### 4.2.7 시험 결과 화면

사용자 에이전트는 사용자의 요청에 따라 SIP 메시지를 생성하고 처리하여 호 연결이 가능하도록 하는 기능을 수행한다. 인터넷 상에서 유연하고 다양한 응용서비스 개발과 이동성, 개인화, 다양한 단말과 시스템에 적용 가능한 것이 특징인 SIP는 아직 초보적인 시스템 개발 수준에 있다.



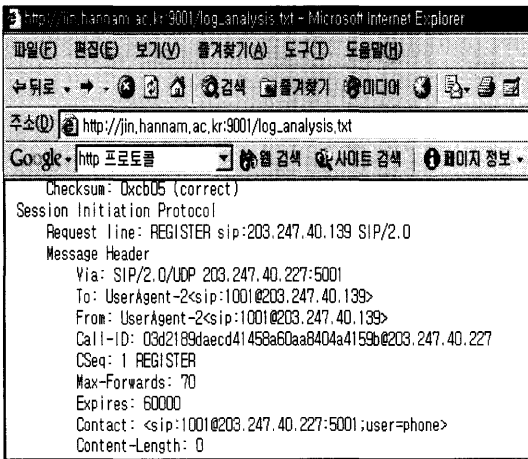
(그림 7) REGISTER

따라서 SIP 기반에서 개발 가능한 다양한 응용 분야가 존재함을 고려할 때 상호 호환성을 보증하는 표준 검증이 병행되어야 할 것이다.

위의 화면(그림 7)은 이러한 표준을 검증하기 위한 시험 결과이다.

#### 4.2.8 동작 과정

아래 그림은 구현된 리눅스 웹서버로 접속하여 패킷을 분석한 파일을 불러오는 화면이다.



(그림 8) 시뮬레이션 실행화면

### 5. 결론 및 향후 연구과제

SIP 프로토콜 시험 시뮬레이터는 SIP 기반 네트워크 환경에서의 보안 운영성을 검증하기 위한 시스템이다. 이에 따라 표준 시험 문서를 개발하였으며, 각 시험 절차를 정의하였다. 시험 절차에 따른 실험 결과는 간단한 웹 서버를 제작하여 서버의 콘솔상이 아닌 웹브라우저를 이용하여 편리하게 검증 결과를 확인 할 수 있도록 하였다.

현재 인터넷 기반의 음성 서비스와 관련하여 차세대 이동통신망, 지능망, 인터넷이 통합되어 가는 추세에 있으며, 이러한 새로운 네트워크에

서 멀티미디어 제어를 위한 새로운 표준 기술로서 SIP가 연구 개발되고 있는 실정이다. 국내에서도 많은 업체들이 표준을 적용하기 위한 노력을 하고 있으나, 외국에 비하여 상대적으로 빠르게 적응하지 못하고 있는 것이 사실이다.

차세대 인터넷 전화 분야에서 콜(call) 시그널링 프로토콜로 인식되고 있는 SIP 프로토콜의 기능과 동작 방식을 알아보고 이를 이용하여 사용자 에이전트들간의 메시지가 표준을 만족하는지를 검증하였다. 사용자 에이전트들간의 메시지는 UDP를 이용하기 때문에 메시지 전송에 대한 신뢰성이 없다. 각 클라이언트는 상대측에서 메시지를 수신하였음을 통보하는 ACK 메시지를 받을 때까지 메시지를 재 전송하게 된다. 만약 사용자 에이전트 구현시 이러한 메시지들을 표준에 따라 정확하게 처리하지 못한다면 상호 운영성을 보장하지 못하게 된다. 따라서 메시지의 정확한 처리의 검증은 반드시 필요하며, 표준을 만족하여야 한다.

SIP 프로토콜의 대부분이 자바 인터페이스와 리눅스를 기반으로 한다. 이에 따라 SIP 시험 시뮬레이터는 리눅스 상에서 개발되었다. 사용자 에이전트뿐만 아니라 SIP의 또 다른 구성 요소인 로케이션 서버, 리다이렉트 서버, 프록시 서버 등에 대한 표준 시험 절차의 개발을 향후 연구과제로 남긴다.

### 참고 문헌

- [1] 개방형컴퓨터 통신 연구회, “인터넷 표준 기술 워크샵”.
- [2] 유승화, “인터넷 전화”, 전자신문사, 2002.
- [3] M. Garcia-Martin, C. Bormann, J. Ott, R. Price, A. B. Roach, “The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling



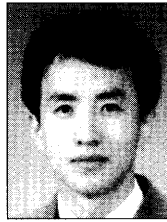
Compression (SigComp)", RFC3485, February 2003.

- [4] Session Initiation Protocol (SIP) Working Group, <http://www.ietf.org/html.charters/sip-charter.html>.
- [5] 이종화, 안상현 "SIP 기반 차세대 응용 기술", 한국정보처리학회지, 제8권, 제2호, pp.28-29, 2001.
- [6] J. Rosenberg, H. Schulzrinne, G. Camarillo et al., SIP : Session Initiation Protocol, RFC 3261, June 2002.
- [7] Henry Sinnreich, Alan B. "Johnston, Internet Communications Using SIP", WILEY, 2001.
- [8] Luan Dang, Cullen Jennings, David Kelly, "Practical VoIP using VOCAL", O'REILLY, 2002.
- [9] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, SIP : Session Initiation Protocol, RFC 2543, March 1999.



**장성만**

2000년 한남대학교 수학과 (이학사)  
 2003년 한남대학교 컴퓨터공학과 (공학석사)  
 2003년~현재 한남대학교 컴퓨터공학과 박사과정



**길민욱**

1989년 한남대학교 전자계산공학과(공학사)  
 1991년 한남대학교 전자계산공학과(공학석사)  
 2000년 한남대학교 전자계산공학과(공학박사)

1997년~현재 문경대학 인터넷정보계열 조교수  
 관심분야 : 정보보호, 보안시스템, 인공지능, 음성인식, 멀티미디어, 유전자 알고리즘



**이극**

1983년 경북대학교 전자과 컴퓨터공학전공(공학사)  
 1986년 서울대학교 컴퓨터공학과(공학석사)  
 1993년 서울대학교 컴퓨터공학과(공학박사)

1988년~현재 과기부 지정 민군겸용 보안공학 연구센터 소장



**김기남**

미국 캔자스대학 수학과(응용수학사)  
 미국 콜로라도 주립대학 통계학과(통계학석사)  
 미국 콜로라도주립대학 기계·산업공학과(기계·산업공학박사)

현재 경기대학교 정보보호기술공학과 주임교수