

VPN을 적용한 인터넷 전화 단말기의 설계에 관한 연구

정회원 유 승 선*, 김 삼 택**, 이 성 가***

Study on Design of Internet Phon(VoIP) using the VPN

Seung-Sun Yoo*, Sam-Tek Kim**, Seung-gi Lee*** *Regular Members*

요 약

인터넷을 이용한 전화(VoIP)의 사용이 전세계적으로 확산 일로에 있으며 이미 여러분야에서 부분적으로 실용화하여 사용되고 있다. 그러나 상대방과의 통화는 그 목적에 따라 비밀을 유지해야 할 필요가 있고 비밀이 보장되어야 한다. 일반적으로 사용되는 일반 전화망(PSTN)은 상대방과 1:1로 회선이 연결되어 도청이 상대적으로 어렵지만 인터넷 망은 무수히 많은 사람들이 동시에 접속이 가능 하므로 상대방과의 통화에 있어 비밀 보장이 어렵다. 따라서 본 연구에서는 개인 통신망(VPN) 프로토콜을 SIP 프로토콜을 탑재한 인터넷 전화기(VoIP)와 접목하여 도청방지용 인터넷 전화기의 새로운 모델을 제안하고, 일반 인터넷 전화기와 성능을 비교 분석하여 실용화의 가능성은 입증한다.

ABSTRACT

The VoIP(Voice over IP) has been worldwide used and already put to practical use in many fields. However, it is needed to ensure secret of VoIP call in a special situation. It is relatively difficult to eavesdrop the commonly used PSTN in that it is connected with 1:1 circuit. However, it is difficult to ensure the secret of call on Internet because many users can connect to the Internet at the same time. Therefore, this paper suggests a new model of Internet telephone for eavesdrop prevention enabling VoIP(using SIP protocol) to use the VPN protocol and establish the probability of practical use comparing it with Internet telephone.

I. 서 론

1980년대 후반 인터넷이 웹(Web)을 통해 일반 대중에게 인식되면서 전 세계를 하나의 통신망으로 연결하는 통신 네트워크로 발전하게 되었다 따라서 이러한 통신망을 기반으로 하는 인터넷은 21세기 현대 사회의 필수적 요인이 되고 있으며 인터넷을 기반으로 하는 산업과 기술이 날로 발전하고 있다 그 중에서도 인터넷을 이용한 음성 전달 기술의 발전으로 인터넷을 이용한 인터넷 전화(VoIP)는 기존의 공중 전화망(PSTN)을 대체할 정도로 빠르게 발전하고 있

다. 또한 인터넷 전화의 사용 비용이 기존의 전화망(PSTN)보다 아주 저렴하다는 장점을 가지고 있으며, 또한 음성뿐만 아니라 인터넷으로 부가되는 모든 서비스를 지금보다 아주 저렴하게 전화기를 통하여 제공 받을 수 있다는 장점이 있어 향후 인터넷 전화는 우리 생활에서 밀접한 통신수단으로 자리를 잡을 것이다. 그러나 이러한 인터넷 전화(VoIP)는 하나의 망에서 일반 대중이 동시에 사용할 수 있는 점 때문에 항상 해커들에 의해서 도청에 무방비 상태로 놓여 있을 수 있다. 따라서 본 연구에서는 인터넷 전화기의 도청을 방지 할 수 있도록 가상사설망(VPN)

* 비맥(주) 기술개발 이사(yss2590@hanmir.com), ** 우송정보대학 컴퓨터정보통신학부 교수(stkim@wsi.ac.kr)

*** 지피텍(주) 대표이사(www2www@empal.com)

논문번호: KICS2004-09-205, 접수일자: 2004년 09월 21일

을 이용한 인터넷 전화 단말기를 개발하였다 SIP 프로토콜 스택을 적용한 인터넷 전화기 단말기에 도청 방지를 위하여 PPTP(Point-to-Point Protocol)를 적용하여 성능을 분석하고 타당성을 입증하였다

II. VPN을 적용한 VoIP 단말기 하드웨어

VPN을 적용한 VoIP 단말기를 구현하기 위하여 [그림 1]과 같이 하드웨어를 설계하였다 [그림 1]에서 보는 바와 같이 본 연구에서 디자인한 하드웨어는 크게 main-board와 sub-board로 구성된다 sub-board는 Processor module로 구성되고 main board는 Audio DSP 부, Ethernet 부, SLAC/SLIC부, Power부 기능 블럭과 인터넷을 연결할 수 있는 2개의 포트와 전화 아날로그 입출력을 할 수 있는 2개의 포트를 갖도록 설계하였다 주요 모듈 상세도는 다음과 같다. [그림 2]는 본 연구에서 설계한 Processor module의 상세도를 나타낸다 [그림 2]에서 보는 바와 같이 본 연구에서 사용한 Main Processor는 모토롤라에서 개발한 50Mhz의 속도를 가진 MPC850을 사용하였다. 그리고 2MB의 FROM과 8MB의 SDRAM을 사용하였다. 또한 mpc850의 이더넷 포트가 연결되어 하나의 RJ45 포트는 인터넷과 연결되고, 또 다른 RJ45 포트는 내부 망에 연결되도록 구성하였다.

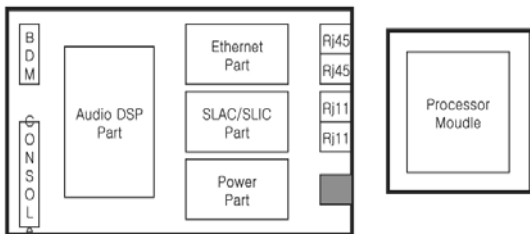


그림 1. 하드웨어 디자인 개념 블럭도

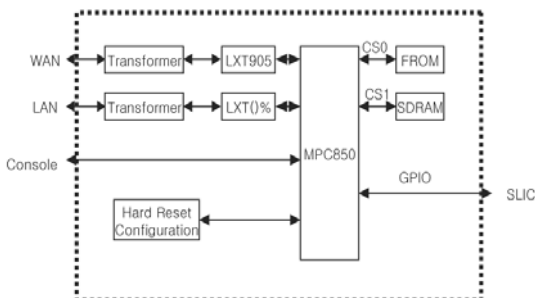


그림 2. 프로세서 모듈 상세도

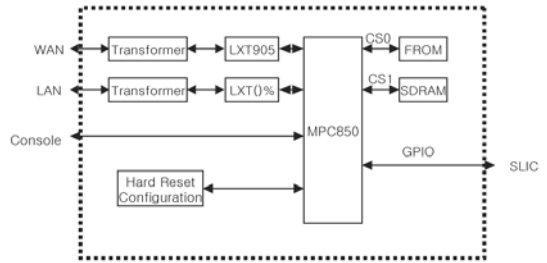


그림 3. 오디오 모듈상세도

그리고 main-board의 오디오 패킷 프로세서 제어를 위하여 사용한 Audio DSP 부의 구성도는 [그림 3]에서 보는 바와 같이 디자인 하였다 Audio 패킷 프로세서는 AudioCodes사에서 개발한 AC4830x-C를 사용하였다. 본 프로세서는 외부에 128Kbytes용량의 메모리인 SRAM (CY7C1021V3-12Z)과 직접 연결하여 사용하며, 16.384Mhz 외부clock을 사용한다.

디지털 오디오를 아날로그 오디오로 아날로그 오디오를 디지털 오디오로 바꿔주기 위해서 [그림 4]와 같이 모토롤라에서 만든 SLAC(모델 MC14LC5480)과 인텔사에서 개발한 RSLIC(모델 HC55185)를 이용하여 SLAC/RSLIC부를 설계하였다. SLAC은 RSLIC로부터 오디오 아날로그를 입력받아서 디지털로 변환하여 오디오 패킷 프로세서(AC4830x-C)에 전달하고 오디오 패킷 프로세서에서 출력된 오디오 디지털 신호를 아날로그로 변환하여 RSLIC으로 전달한다. [그림 5]는 2층 구조로 설계된 VoIP 단말기 하드웨어의 실제 모습을 나타낸다

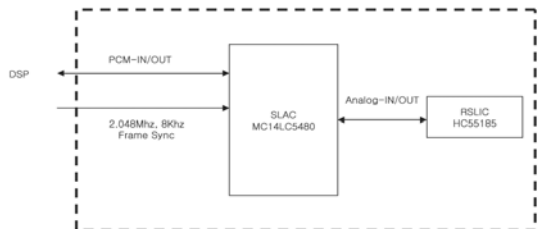


그림 4. SLAC/RSLIC부 상세도



그림 5. VPN을 적용한 VoIP단말기 하드웨어의 모습

III. VPN을 적용한 VoIP 단말기의 프로토콜 스택의 구성

본 연구에서는 인터넷전화(VoIP)의 도청을 방지할 수 있도록 하기 위하여 가상사설망(Virtual Private Network)을 제공하는 프로토콜중의 하나인 PPTP(Point-to-Point Tunneling Protocol)를 기반으로 하고, VoIP기능을 제공하는 SIP(Session Initiation Protocol) 스택을 이용하였다

PPTP는 PPTP 서버와 클라이언트 사이에 터널을 생성하는 기능을 담당하고 서버와 클라이언트 사이의 정보 협상은 PPP를 사용한다. 따라서 본 연구에서 구현에 사용된 각각의 프로토콜의 기능에 대해서 알아본다.

3.1 PPP(Point-to-Point Protocol)

PPP는 PPP링크 상에서 다중 프로토콜 데이터그램(Mult-protocol datagram)을 전송할 수 있는 프로토콜로써 인캡슐레이션(Encapsulation) 기능, PPP링크의 연결과 제어를 담당하는 LCP(Link Control Protocol), 그리고 네트워크 레이어(Network layer)의 협상을 담당하는 NCP(Network Control Protocol)로 나누어진다.

PPP Encapsulation은 PPP Frame에 여러 프로토콜을 실어 나르기 위해서 [그림 6]과 같은 프레임 구조를 가진다 [그림 6]에서 보는 바와 같이 프로토콜 필드와 인포메이션 필드, 패딩필드로 구성된다. 프로토콜 필드는 인포메이션 데이터를 구별하기위한 것으로 1~2 octet이 할당되며, 인포메이션 필드에 사용되는 프로토콜을 명시한다. 그리고 인포메이션 필드는 프로토콜 필드에 해당하는 프로토콜의 데이터로서 최대크기를 MRU(Maximum Receive Unit)라고 하며 기본값으로 1500octets가 할당되고 이 값은 LCP(Link Control Protocol)를 통해서 변경될 수도 있다. 패딩 필드에 사용되는 패딩방법은 각각의 프로토콜에 의해서 결정된다.

LCP는 PPP Link를 설정, 유지, 종료 기능을 담당하는 프로토콜로써 [그림 7]은 LCP 동작에 의해서 나타날 수 있는 상태 천이도이다 [그림 7]에서 보는 바와 같이 Dead는 연결이 시작되기 전과 연결이 끝나고 난 후의 상태로 물리단계(Physical layer)가 준비되면 다음단계로 넘어간다. 설정(Establish) 단계에서는 양 끝단에 Link를 설정하는 것으로 Configuration packet을 교환함으로써 설정된다. 이 단계에서 협상된 Configuration Option의 값에 따라서 Authen-



그림 6. PPP프레임 구조

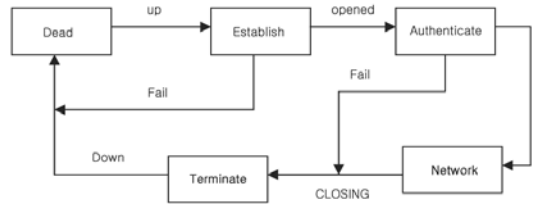


그림 7. LCP 상태 천이도

entication 상태에서 진행될 프로토콜이 결정되거나 생략될 수도 있다.

인증(Authentication)단계는 네트워크 계층의 프로토콜 패킷을 교환하기 전에 PPP Server에게 Client가 자신의 인증을 받기 위해서 수행하는 절차이다. 여기서 사용할 인증 프로토콜은 인증 단계에서 LCP 패킷교환을 통해 미리 정하게 되며 인증이 실패하면 종료(Terminate) 단계로 넘어간다.

네트워크(Network)단계는 NCP 패킷 교환을 통해서 지원되는 네트워크 레이어 프로토콜이 결정되며 해당 프로토콜의 설정 정보를 얻어와 정상적인 네트워크 통신이 가능한 상태가 되도록 한다.

종료(Terminate) 단계에서는 인증단계에서 실패한 경우나 NCP에서 종료를 선택한 경우에 실행되는 단계로서 종료 패킷을 교환함으로써 PPP Link 연결이 종료된다.

NCP는 [그림 7]의 네트워크 상태에 해당하는 프로토콜로서 네트워크 레이어 프로토콜을 설정하는데 사용되는 프로토콜이다. 본 연구에서는 IP 프로토콜을 사용하므로 IPCP(IP Control Protocol)을 사용하여 IP 레이어에 설정해야 하는 정보를 서버로부터 얻어 와서 설정한다. 얻어오는 정보는 대개 자신의 IP 주소와, 네트워크 마스크 기본 게이트웨이 주소 등이 있다.

NCP의 IPCP과정이 정상적으로 끝나면 [그림 6]의 Protocol 필드 값이 0x0021로 결정된다.

3.2 PPTP(Point to-Point Tunneling Protocol)

PPTP는 PPP frame을 IP 데이터그램으로 encapsulation하여 인터넷상에서 전송하는 VPN(Virtual Private Network)의 방법 중의 하나이다. 이 프로토

콜은 PPTP 터널의 생성, 관리, 종료 기능을 담당하는 control connection 메시지라고 하는 TCP 데이터를 사용한다.

PPTP는 PNS (PPTP Network Server)와 PAC (PPTP Access Concentrator)사이의 제어연결(Control connection)부분과 PNS와 PAC사이의 터널링(Tunneling)으로 나눌 수 있다. 먼저 터널링을 하기 전에 PAC와 PNS 사이에 PPTP 제어 연결을 하기 위하여 보내지는 제어 연결 메시지(Control connection message)은 터널의 생성, 관리, 해제의 기능을 수행하며 TCP 세션 위에서 이루어진다 이때 destination port는 1723을 사용한다. 또 Control connection은 PNS, PAC 어느 쪽에서도 시작할 수 있다 그리고 터널링은 끝 단말(End link)의 사용자가 PPP 프레임의 PNS에게 전달하고자 할 때 PAC와 PNS사이의 인터넷 구간을 마치 전용선을 쓰는 것과 같은 효과를 나타낸다. [그림 8]에서 보는바와 같이 PPP 프레임은 GRE헤더(enhanced GRE header)로 인캡슐레이션되고 다시 IP헤더를 붙여서 PAC-PNS구간에서 인터넷을 통하여 전송된다 [그림 9]는 PPTP 클라이언트 내부에서 PPTP 서버에 접속하는 유형에 따라 PPTP 프레임이 생성되는 과정을 나타낸다

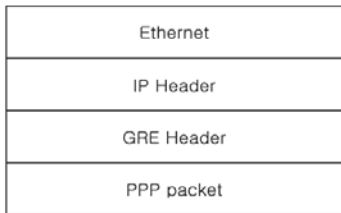


그림 8. PPTP 프레임 구조

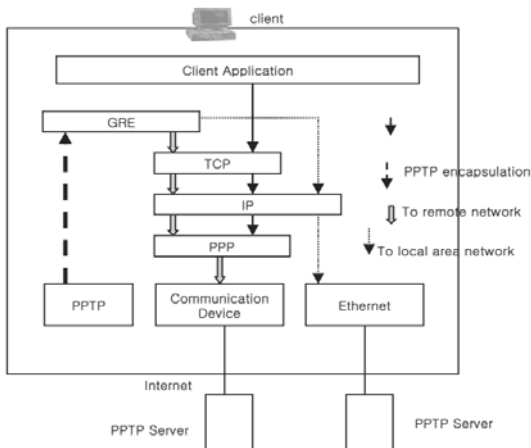


그림 9. PPTP 프레임 생성 과정

2.3 SIP(Session Initiation Protocol) 스택

SIP는 H.323과 마찬가지로 VoIP에서 미디어 세션을 설정, 수정, 종료하는데 사용되는 프로토콜이다 그러나 VoIP의 완전한 기능을 위해서는 SIP 프로토콜 단독으로 사용할 수 없고 다른 프로토콜과 결합해야만 완전한 기능을 수행할 수 있다 가장 기본적으로 필요하고 많이 사용되는 프로토콜의 스택은 [그림 10]과 같다. 그림에서 보는 바와 같이 SIP 프로토콜 스택은 크게 4가지기능으로 분류할 수 있으며 그 각각의 기능은 다음과 같다

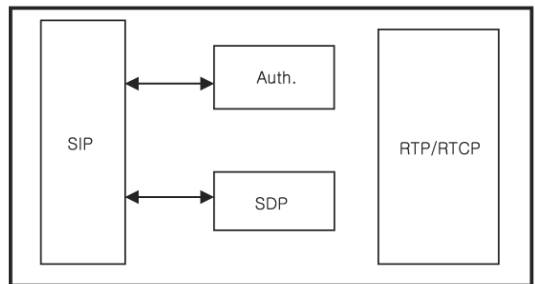


그림 10. SIP 스택 구조

먼저 SIP(Session Initiation Protocol)는 multi-media session을 생성, 수정, 종료하는 프로토콜이며 SDP(Session Description Protocol)는 multi-media session을 설명하는 프로토콜로서 SIP message의 body부분에 포함되어 전달된다. 만약 SIP에서 인증부분을 사용하고자 한다면 Authentication 프로토콜을 사용할 수도 있다 이 두개의 프로토콜을 이용하여 media session을 생성하게 되면, 이 때부터 SDP에 의해서 협상된 media format에 따라서 SIP 메시지 경로와는 별개인 데이터 경로를 통하여 실시간 음성 데이터를 주고받는데 이때 사용되는 것이 RTP(Real-Time Protocol)이다. RTP는 실시간 데이터를 실어 나르는 프로토콜이므로 주로UDP를 통해서 전달된다.

3.4 PPTP를 적용한 VoIP의 통화 시험

본 연구에서는 [그림 11]과 같이 VoIP 서비스 환경을 구성하여 인터넷전화 통화 시험을 하였다. [그림 11]에서 보는 바와 같이 각 VoIP 단말기에는 PPTP Client (PAC)기능이 구현되어 있고 VoIP 프로토콜 중에 하나인 SIP 프로토콜이 구현되어 있다 SIP 프로토콜을 이용해서 VoIP 서비스를 하기 위해서는 기본적으로 Proxy Server(Registrar 기능 포함)

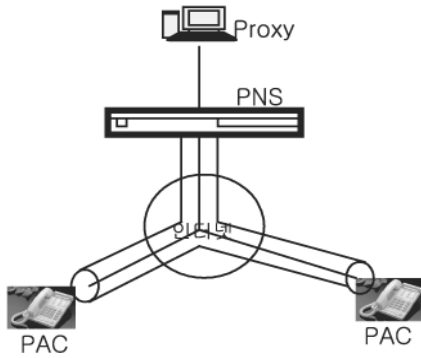


그림 11. VPN을 이용한 인터넷 전화의 서비스 환경 구성도

가 필요하며 이 server는 PPTP Server(PNS)뒤에 사 설망에 연결되어 있다.

먼저 각 PAC(PPTP Network Server)는 시스템이 구동될 때, PNS(PPTP Network Server)와 하나의 Control Connection을 생성한다. Control Connection은 PPTP tunneling을 하기 전에 PPTP 연결을 제어 하기 위해서 설정하는 절차이다 Control Connection을 생성하는 절차는 [그림 12]와 같으며, 그림에서 보는 바와 같이 Control Connection을 생성하기 위해서는 먼저 PAC에서 PNS로 Control Connection을 요청하고 PNS으로 부터 응답을 수신 한 후 외부로 보내는 호(Call)에 대한 설정을 요청한다. PNS로부터 호(Call) 설정에 대한 응답을 수신 한 후 마지막으로 PAC와 PNS가 서로 연결된 Link의 정보를 설정하기 위해서 Set-Link-Info 메시지를 사용하여 Control Connection설정을 완료한다.

Control Connection 설정이 완료가 되면 [그림 13]과 같이 PAC와 PNS사이에 PPP(Point-to-Point Protocol)를 이용하여 Link Configuration을 협상하고 지원할 프로토콜들이 무엇인가를 협상하게 된다 먼저 LCP를 이용하여 PPP Link를 설정하고, 인증 프로토콜을 사용할 것인가 아닌가 만약 사용한다면 어떤 알고리즘을 사용할 것인가를 협상한다 또한 압축알고리즘을 사용할 것인가 아닌가를 협상한다 LCP과정을 통해서 협상된 Option들을 가지고 다음에 적용할 프로토콜이 결정된다 본 연구에서는 인증 프로토콜을 사용하는 것으로 협상을 하였고 CHAP (Challenge Handshake Authentication Protocol)을 사용하기로 했기 때문에 PNS에서 PAC에게 CHAP Challenge 메시지를 보내서 인증을 요청한다 그러면 PAC에서는 PNS로부터 얻은 데이터와 자신의 user-id와 password를 결합하여 CHAP response를 생성하여 응답한다. 그러면 PNS는 수신한 데이터 값이

올바르면 CHAP success 메시지로 응답하여 인증절차를 마치게 된다 또한 LCP의 과정 중에서 압축알고리즘을 사용하겠다고 협상을 하였기 때문에 다음절차는 압축알고리즘으로 어떤 프로토콜을 사용할 것인가를 협상하게 된다 그러면서 동시에 지원할 Network layer의 프로토콜을 협상하게 된다 본 연구에서는 압축알고리즘으로 MPPE를 사용하기로 협상을 하였으며, Stateless Mode를 사용하고, 128bit encryption을 사용하기로 하였다.

Stateless Mode를 선택하게 되면 MPPE(Microsoft Point-To-Point Encryption) packet format의 Coherency Count값이 모든 packet 마다 값이 변하게 설정하여 이전 packet과 별개로 사용되도록 하는 것이다. Network layer는 IP(Internet Protocol)를 사용하기로 하여 IPCP(Internet Protocol Control Protocol)를 사용하여 네트워크 관련 정보를PNS로부터 얻어오게 된다. PAC의 private ip 주소와 private network, private gateway ip 주소등과 같은 정보를 얻어서 PAC의 네트워크 레이어를 설정한다 위의 모든 과정이 끝나면 초기 준비 단계는 완료가 되어 [그림 11]에서 보여주는 모든 장치들이 하나의 VPN으로 연결되는 것이다. 이로써 각 PAC에서 Proxy Server로 접근할 수가 있다 이미 각 PAC에는 Proxy Server의 Private IP가 설정되어 있어서 사설망으로 연결된 뒤에는 Proxy Server에게 자신의 private ip를 이미 할당된 VoIP 전화번호와 함께 등록한다. 등록절차가 완료되면 통화하고자 하는 전화번호로 전화를 걸면 SIP 프로토콜 절차에 따라서 전화 통화가 가능하게 된다 사설망에 연결된 VoIP 단말기들이 서로 전화 통화를 하게 될 때 음성 데이터는 RTP 프로토콜에 의해서 송수신된다. 이 음성 데이터는 caller PAC가 PPTP tunnelling을 통해서 PNS까지 전달 된 후 PNS에서 실제 destination에 해당되는 private ip를 얻어서 다시 PNS가 PPTP tunnelling을 통해서 called PAC로 전달하게 된다. 그 반대의 경우도 마찬가지로 같은 절차에 의해서 전달된다. 본 연구에서 구현한 도청방지용 인터넷전화(VoIP)의 실제로 음성데이터가 전달되는 과정의 각 노드들의 프로토콜의 스택은[그림 14]와 같다. [그림 14]에서 보는 바와 같이 Caller 단말기에 연결되어 있는 전화기에서 음성이 들어오면Audio DSP를 통해서 디지털 음성데이터를 얻게 된다 디지털 음성데이터앞에 RTP header를 붙여서 UDP layer로 내려 보낸다. UDP layer에서는 UDP header를 붙이고 Private IP layer로 전달된다. 사설망 ip를 이용하

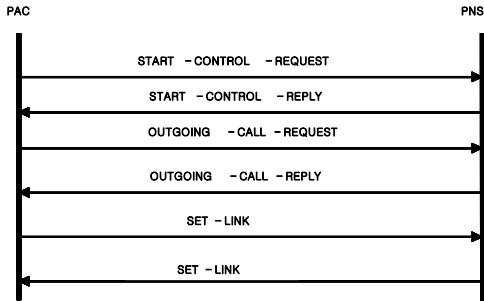


그림 12. PPTP Control Connection 생성 절차

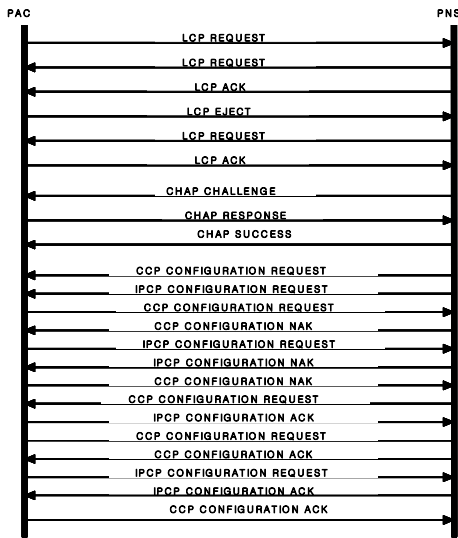


그림 13. PPP module 구동과정

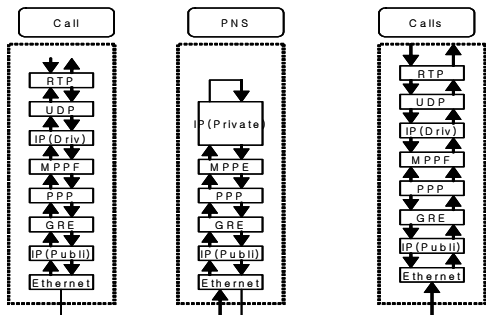


그림 14. 음성 데이터 전송을 위한 프로토콜스택

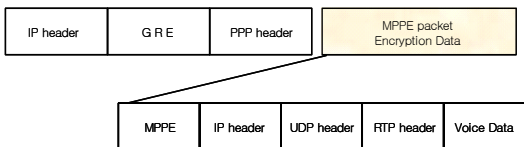


그림 15. 최종 암호화된 음성 데이터를 담은 IP packet format

여 IP header를 붙이고, MPPE(encryption) layer로 보낸다. 이 encryption layer에서는 private IP layer에서 내려온 IP packet을 암호화한 뒤에 MPPE header를 앞에 붙인다. 그리고 PPP layer로 내려 보낸다. PPP layer에서는 PPP header를 붙인 뒤 GRE layer로 보낸다. GRE layer에서는 GRE header로 encapsulation하여 public IP layer로 보내진다. Public IP layer에서는 실제 인터넷에서 통용될 수 있는 Public IP를 가지고 IP header를 붙인다. 최종 IP packet을 ethernet 물리 layer로 보내서 인터넷 망으로 이더넷 프레임을 송신하게 된다 그리고 PNS에서는 caller 단말기에서 보낸 이더넷 프레임을 수신하여 caller 단말기의 역방향(ethernet -> public IP -> GRE -> PPP -> MPPE -> private IP)으로 처리하여 private IP layer에서 최종 목적지를 알아낸다. 최종 목적지에 따라서 called 단말기로 송신하기 위해서 private IP -> MPPE -> PPP -> GRE -> public IP -> ethernet을 통하여 이더넷 프레임을 생성한다. 생성된 이더넷 프레임을 called 단말기로 인터넷을 통하여 송신한다. 또한 called 단말기에서는 PNS로부터 수신된 이더넷 프레임을 caller 단말기의 역방향으로 각 layer로 처리하여 최종 자신에게로 온 음성데이터를 얻어내게 된다 [그림 14]와 같은 프로토콜의 스택을 통해서 외부 인터넷 망으로 송수신되는 이더넷 frame에 encapsulation된 IP Packet의 format은 [그림 15]와 같이 구성되어 있어서 인터넷 망에서 IP packet을 가로챌다 하더라도 실제 중요한 데이터는 encryption되어 있기 때문에 분석할 수가 없게 된다.

IV. 성능 평가

본 연구에서 구현한 VPN(PPTP)을 적용한 인터넷 전화(VoIP)의 성능 평가시험을 하기위하여 기존의 인터넷 전화기의 성능측정시험 방법을 도입하여 시험을 해 보았다. 내부 망 환경에서 주어진 호 패턴(Call Pattern)을 바탕으로 호 연결을 시도했을 때 본 연구에서 개발한 VPN(PPTP)을 적용한 인터넷전화(VoIP)의 호 완료율을 측정하기 위하여 [그림 16]과 같은 시험망을 구성하였다 [그림 16]에서 보는 바와 같이 DUT(Device Under Test, 즉 VoIP 단말기)에서는 directcall, DTMF in band signaling, G.723.1(6.3K)코덱 설정을 하게 된다 또한 directcall을 사용하기 위해서 각 Terminal에 PNS기능을 추가로 구현하였다. HammerIT에서는 [그림 17]에서 보

는 바와 같이 Call length 10초, intercall time 3초, Start to start time 0, 즉 blast call pattern을 가진 호를 24시간 동안 발생시켜 호 완료율을 측정한다 즉 모든 호가 동시에 10초 동안 연결되었다가 끊어지고 3초 후에 다시 10초간 연결되었다 끊는 방법으로 24시간 동안 반복 수행함을 의미한다 그리고 [그림18]은 호 완료 측정을 위한 HammerIT의 시험 스크립트를 나타낸다 그림에서 보는 바와 같이 Place Call은 호의 연결 설정을 의미하고, Confirm Path Stimulus는 tone이나 Voce를 보냄으로써 호를 지정된 시간동안 유지함을 의미한다 그리고 Release Call은 호 연결 해제를 의미한다 본 시험에서는 Call length를 10초로 설정하였다. DUT1와 DUT2 사이에서 tone을 보내고 확인하는데 걸리는 시간이 총 10초가 되지 않으면 DUT1이나 DUT2에서 이러한 행위를 한번 더 수행하게 되어 Call length가 15초 정도 길어 질 수도 있도록 하였다

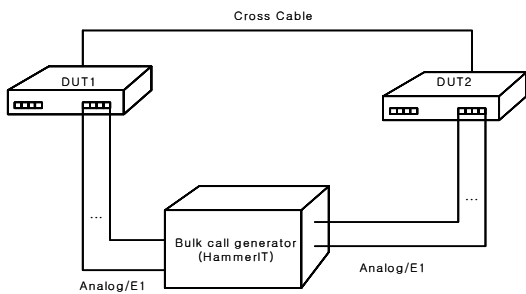


그림 16. 시험 회로망

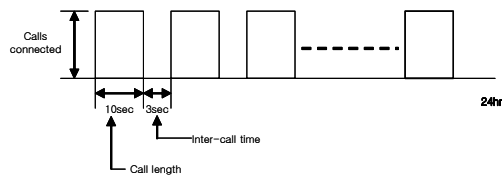


그림 17. HammerIT에서 발생하는 bulk call pattern

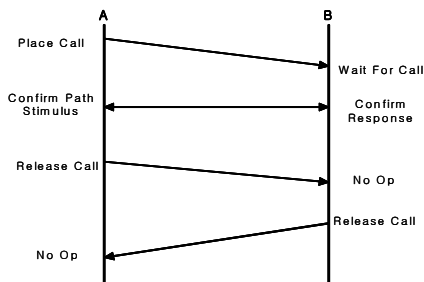


그림 18. 호 완료 측정을 위한 HammerIT의 시험 스크립트

V. 결 론

본 연구에서 구현한 PPTP프로토콜과 SIP프로토콜을 이용한 도청방지용 인터넷전화기의 성능을 측정하기 위하여 Call length를 10초로 설정하였다. [그림 17]에서 보는 바와 같이 A와 B 사이에서 tone을 보내고 확인하는데 걸리는 시간이 총 10초가 되지 않으면 A나 B에서 이러한 행위를 한번 더 수행하게 되어 Call length가 15초 정도 길어 질 수도 있도록 하여 24시간을 운용한뒤에 호 완료율이 100%로 적합 판정을 받았다. 따라서 인터넷 전화기의 최대 단점으로 인식될수 있는 도청을 방지하기 위하여 VPN(Vertural private network)기술을 인터넷 전화기에 접목하여 도청을 방지할 수 있는 토대를 마련하였다. 그러나 본 연구에서 사용된 PPTP 프로토콜은 제어연결(Control Connection)메시지가 암호화가 되지않는다는 점과 인증기능이 없다는 단점으로 중간에서 제어연결메시지를 가로채서 분석이가능함으로 보다 완벽한 암호화(Security)가 이루어 질 수 없다는 단점을 여전히 내포하고 있다. 따라서 향후 보다 완벽한 암호화를 이루기 위해서는 제어연결(Control Connection)메시지가 암호화되어 있고 인증기능이 있는 VPN기능 중 IP sec을 이용하는 것이 바람직하다 할 수 있다.

참 고 문 헌

- [1] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", *RFC 2637*, July 1999
- [2] W. Simpson, "The Point-to-Point Protocol (PPP)", *RFC 1661*, July 1994
- [3] W. Simpson, "PPP LCP Extensions", *RFC 1548*, January 1994
- [4] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", *RFC 1994*, August 1996
- [5] D. Rand, "The PPP Compression Control Protocol (CCP)", *RFC 1962*, June 1996
- [6] G. McGregor, "The PPP Internet Protocol Control Protocol (IPCP)", *RFC 1332*, May 1992
- [7] G. Pall, G. Zorn, "Microsoft Point-To-Point Encryption (MPPE) Protocol", *RFC 3078*,

March 2001

[8] J. Postel, "Internet Protocol", *RFC 760*,
January 1980

유 승 선(Seung Sun Yoo) 정회원
논문 02-27-5A-10 참조

김 삼 택(Sam Tek kim) 정회원



1985년 한남대학교 전자계산학과 졸업(학사)
1987년 중앙대학교 대학원 전자계산학과 졸업(석사)
2005년 중앙대학교 대학원 컴퓨터공학과 졸업(박사)
1990년~1995년 (주) LG 정보

통신 연구소 선임연구원

1995년~현재 우송정보대학 컴퓨터정보통신계열
부교수

<관심분야> 분산컴퓨팅, 이동통신, 네트워크, VoIP

이 성 기(Seong-gi Lee) 정회원



1982년 2월 한국항공대학교 항공통신공학과 졸업
1985년~2003년 10월 현대자동차 제품개발연구소
2003년 전북대학교 대학원 컴퓨터공학과 박사 수료
2004년 1월 (주) 지피텍 대표

이사

<관심분야> 인공지능, 영상처리, 지능제어