논문 2009-2-11

PPTP를 이용한 VoIP 음성보안 단말기 구현

The Implementation of VoIP Terminal using PPTP for Voice Security

김삼택*

Sam-Taek Kim

요 약 음성통화 시 일반적으로 사용되는 공중 전화망은 상대방과 회선이 직접 연결되어 도청이 상대적으로 어렵지만 인터넷망은 동시에 다수가 접근 가능하기 때문에 상대방과 음성 통화에 보안을 유지하기가 쉽지 않다. 그러나 음성통화는 사용 목적에 따라 비밀을 유지하여야 한다. 이러한 인터넷 전화(VoIP)는 인터넷의 특성상 하나의 망에서 일반 대중들이 동시에 사용할 수 있는 점 때문에 항상 해커들에 의해서 도청에 무방비 상태로 놓여 있을 수 있다.
따라서 본 논문에서는 인터넷 전화기의 도청을 방지 할 수 있도록 SIP를 기반으로 하고 가상사설망(VPN)의 PPTP를 적용하여 음성데이터의 전송에 터널링 기법을 사용함으로 사용자 인증과 음성 데이터의 기밀성이 강화된 인터넷 전화 단말기를 개발하고 VoIP 단말기의 통화 품질을 측정하였다.

Abstract Although it is relatively difficult to eavesdrop the commonly used PSTN in that it is connected with direct circuit, it is difficult to ensure the secret of call on Internet because many users can connect to the Internet at the same time. However, it is needed to ensure secret of voice call in a special situation. Due to the fact that many users can connect to the internet at the same time, VoIP can always be in a defenseless state by hackers.
Therefore, in this paper, we have developed the increased voice security internet telephone terminal and measured conversation quality by adopting VPN PPTP based on SIP and using tunnel method in transmitting voice data to prevent eavesdrop of internet telephone.

Key Words : VoIP, IP Telephony, VPN, SIP, PPTP

Ⅰ. 서 론

인터넷 전화는 기존의 공중전화망(PSTN)을 대체할 정도로 빠르게 발전하고 있고 음성 망과 데이터 망이 어떤 형태로든 수렴, 통합하는 방향으로 진화하고 있으며, 이러한 통합망으로 가장 강력히 부상하고 있는 것이 패킷망에서 음성을 수용하는 VoX(Voice over X) 기술이다. 일반적으로 VoIP(Voice over Internet Protocol) 또는 IP 전화는 VoX와 패킷 통합 시장의 하위 영역으로 볼 수 있는데, VoX는 VoIP, VoATM (Voice over ATM), VoFR(Voice over Frame Relay), VoDSL(Voice over DSL) 및 VoCable(Voice over Cable) 등 패킷화 된 음성을 위한 현존하는 차세대 솔루션 전체를 포함하고 있다.[1]

SIP는 기존 VoIP 서비스 뿐 만아니라 다양한 서비스의 콜 시그널링 프로토콜로 멀티미디어 세션에 관련된 호 전환 정책, 주소 변환, 네이밍(naming), 사용자 등록, 다자간 회의, 전송 등의 기능을 제공한다. 또한 SIP는 단순성, 범용성, 확장성, 모듈성 등과 같은 장점을 제공해 주기 때문에 많은 애플리케이션에서 SIP의 특성을 이용

*정회원, 우송대학교 컴퓨터정보통신계열
접수일자 2009.02.23, 수정완료 2009.04.06

하고 있다.[2]

일반적으로 사용되는 일반 전화망(PSTN)은 상대방직접 회선이 연결되어 음성보안에 유리하지만 인터넷 망은 불특정 다수의 접속이 가능 하므로 상대방과의 음성 전달에 보안을 적용하기가 어렵다.

음성뿐만 아니라 인터넷으로 부가되는 모든 서비스를 전화기를 통화여 지금보다 아주 저렴하게 제공 받을 수 있다는 장점을 가지고 있는 인터넷 전화는 인터넷의 특성상 하나의 망에서 일반 대중이 동시에 사용할 수 있는 점 때문에 항상 해커들에 의해서 도청에 무방비 상태로 놓여있다.

본 논문에서는 SIP 프로토콜 스택을 적용한 인터넷 전화 단말기에 도청방지를 위하여 PPP(Point to Point Protocol)와 PPTP(Point-to-Point Tunneling Protocol)를 적용하여 PAC(PPTP Access Concentrator) 기능을 구현하며, 구현 단말기와 기존 VoIP 전화기의 종단간 지연시간을 측정하여 음성품질의 성능을 분석하고 보안기능이 적용된 인터넷 전화기의 종단간 지연시간을 RTT(Round Trip Time)값으로 측정하여 상용화의 문제점을 분석한다.

Ⅱ. 가상 사설 네트워킹(VPN)

가상 사설망(VPN : Virtual Private Network)은 인터넷과 같은 공유 또는 공용 네트워크를 통한 연결을 포함하는 사설 네크워크의 확장으로 통신망 기반시설을 터널링 프로토콜과 보안 절차 등을 사용하여 개별기업의 목적에 맞게 구성한 데이터 네트워크이다. 지점간 터널링 프로토콜인 PPTP은 PPP프레임을 IP 데이터그램으로 캡슐화하여 인터넷 구간을 터널링하는 VPN의 방법 중 하나이다.[3]-[4]

PPP는 PPP링크 상에서 다중 프로토콜 데이터그램(Mulit-protocol datagram)을 전송할 수 있는 프로토콜로써 캡슐화기능, PPP링크의 연결과 제어를 담당하는 LCP(Link Control Protocol), 그리고 네트워크 계층의 협상을 담당하는 NCP(Network Control Protocol)로 나누어진다.[5]

PPTP는 2개의 컴포넌트로 구성 되는데 TCP를 이용하여 PNS(PPTP Network Server)와 PAC(PPTP Access Concentrator)사이의 제어연결(control connection)하는 부분과 터널을 관리하는 부분이다.

제어연결은 터널을 통해서 실어 나르게 되는 세션을 생성, 관리, 해제를 담당하고 터널관리 컴포넌트는 사용자 세션의 PPP 패킷을 실어 나르고, 멀티플렉싱과 디멀티플렉싱을 수행하고 GRE(Generic Routing Encapsulation) 헤더를 이용하여 에러 제어를 수행 한다. 먼저 터널링을 하기 전에 PAC와 PNS사이에 PPTP 제어 연결을 하기 위하여 보내지는 제어 연결 메시지는 터널의 생성, 관리, 해제의 기능을 수행하며 TCP 세션 위에서 이루어진다. 이때 목적지 포트는 1723을 사용한다. 또 제어 연결은 PNS, PAS어느 쪽에서도 시작할 수 있다. 그리고 터널링은 끝 단말(End link)의 사용자가 PPP프레임을 PNS에게 전달하고자 할 때 PAC와 PNS사이의 인터넷 구간을 마치 전용선을 쓰는 것과 같은 효과를 나타낸다. 그림 1은 PPTP 클라이언트 내부에서 PPTP 서버에 접속하는 유형에 따라 PPTP 프레임이 생성되는 과정을 나타낸다.

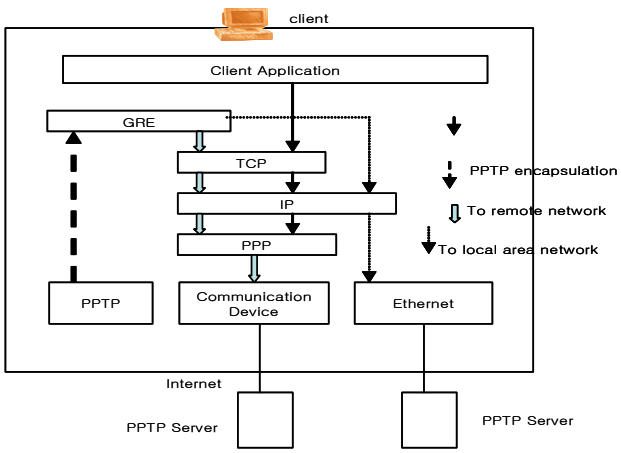

그림 1. PPTP 프레임 생성 과정
Fig. 1. The procedures of producing PPTP frame

Ⅲ. VPN을 적용한 VoIP 단말기 구현

본 논문에서는 인터넷전화의 도청을 방지하기 위해 가상사설망을 제공하는 프로토콜중의 하나인 PPTP 를 기반으로 하고, VoIP기능을 제공하는 SIP 스택을 이용하여 인터넷 전화기를 구현 하였다.

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 결합 해야만 완전한 기능을 수행할 수 있다.

SIP 프로토콜 스택은 크게 4가지기능으로 분류할 수 있으며 각각의 기능은 다음과 같다.

먼저 SIP는 다중 미디어 세션을 생성, 수정, 종료하는 프로토콜이며, SDP(Session Description Protocol)는 다중 미디어 세션을 설명하는 프로토콜로서 SIP 메시지의 몸체 부분에 포함되어 전달된다. 만약 SIP에서 인증부분을 사용하고자 한다면 인증 프로토콜을 사용할 수도 있다. 이 두개의 프로토콜을 이용하여 미디어 세션을 생성하게 되면, 이 때부터 SDP에 의해서 협상된 미디어 포멧에 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 주로 UDP를 통해서 전달된다. VPN을 적용한 VoIP 단말기를 구현하기 위하여 하드웨어는 크게 주 보드(main- board)와 서브 보드(sub-board)로 구성된다.

주 보드는 프로세서 모듈로 구성되고 주 보드는 오디오 DSP 부, 이더넷 부, SLAC/SLIC 부, 전력 부 기능 블럭과 인터넷을 연결할 수 있는 2개의 포트와 전화 아날로그 입/출력을 할 수 있는 2개의 포트를 갖도록 설계하였다. 그림 2는 본 논문에서 설계한 프로세서 모듈의 상세도를 나타낸다. 주 프로세서는 모토롤라에서 개발한 50Mhz의 속도를 가진 MPC850 이다. 그리고 2MB의 FROM과 8MB의 SDRAM을 사용하였다. 또한 MPC850의 이더넷 포트가 연결되어, 하나의 RJ45 포트는 인터넷과 연결되고, 또 다른 RJ45 포트는 내부 망에 연결되도록 구성하였다.

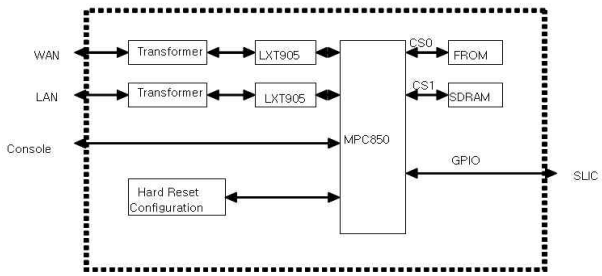

그림 2. 프로세서 모듈 상세도
Fig. 2. processor module spec.

그리고 주 보드의 오디오 패킷프로세서 제어를 위하여 사용한 오디오 DSP부의 구성도는 그림 3에서 보는 바와 같이 디자인 하였다. 오디오 패킷 프로세서는 AudioCodes사에서 개발한 AC4830x-C를 사용하였다. 본 프로세서는 외부에 128Kbytes 용량의 메모리인 SRAM (CY7C1021V3-12Z)과 직접 연결하여 사용하며, 16.384Mhz 외부 클럭을 사용한다.

디지털 오디오를 아날로그 오디오로, 아날로그 오디오를 디지털 오디오로 바꿔주기 위해서 모토롤라사에서 만든 SLAC(모델 MC14LC5480)과 인텔사에서 개발한 RSLIC(모델 HC55185)를 이용하여 SLAC/RSLIC부를 설계하였다.

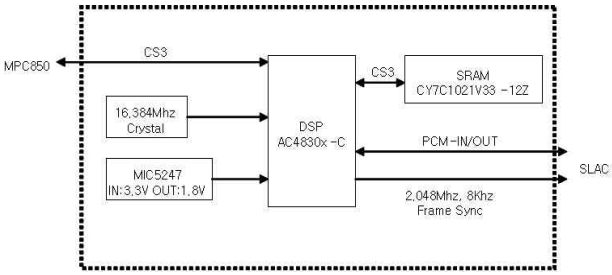

그림 3. 오디오 모듈 상세도
Fig. 3. audio module spec.

SLAC은 RSLIC으로 부터 오디오 아날로그를 입력받아서 디지털로 변환하여 오디오 패킷 프로세서(AC4830x-C)에 전달하고 오디오 패킷 프로세서에서 출력된 오디오 디지털 신호를 아날로그로 변환하여 RSLIC으로 전달한다.

그림 4는 2층 구조로 설계된 VoIP 단말기 하드웨어의 실제 모습을 나타낸다.

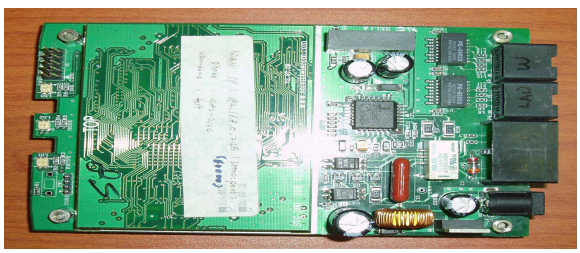

그림 4. VPN을 적용한 VoIP 단말기 H/W
Fig. 4. H/W of VoIp terminal using VPN

Ⅳ. VoIP 단말기의 통화 품질 성능 평가

1. 종단간 지연

본 논문에서 개발된 VPN 기반 VoIP 단말기는 클라이언트 지연 부분에서 PAC과 PNS 사이의 캡슐화 과정이 포함되어 터널링을 통한 음성 패킷을 전달하기 때문에 일반 VoIP 전화기에 비교하여 캡슐화 지연이 추가 된다. VoIP 네트워크에서 종단간의 지연을 어떻게 처리하느냐가 성공적인 VoIP 서비스를 제공하는 중요한 부분이다. 이를 위해 목표 네트워크에 대한 지연을 초래하는 요소들을 대상으로 목표치를 예상하는 것이 중요하다. 단 방향 지연이 120ms ~ 150 ms 정도 되어야 사용자가 만족한 통화 품질을 인식 할 수 있다.[6]

본 논문에서 G.723.1 코덱을 사용한 경우, VoIP를 이용한 음성통화 시에 일반적인 지연을 계산하면 표 1과 같이 예상할 수 있다.[7] 단방향의 전체 예상 지연 시간은 161ms로 본 논문에서는 기존의 VoIP 전화기의 개발 지연시간의 성능평가 기준으로 한다.

ITU-T G.114에서도 단방향 지연이 150ms 이내이면 우수한 통화 품질로 규정하고 있으며, 300ms 이상의 지연은 통화품질에 문제가 있는 것으로 규정하고 있다.[8]

표 1. 단 방향의 전체 지연 예상 시간
Table 1. Total delay time of one way

지연 요소	지연시간
네트워크 인터페이스(1.54Mbps)	1ms
프레이밍(G.723.1 코텍)	30ms
처리 시간(최악의 경우)	10ms
버퍼링(추가적인 버퍼링이 없을 경우)	0ms
패킷화(2프레임/패킷)	30ms
미디어 접근 지연	10ms
라우팅	50ms
지터 버퍼링(one buffer)	30ms
= 단방향의 전체 예상 지연 시간	=161ms

2. 암호화된 음성 데이터 전송을 위한 프로토콜스택

각 VoIP 단말기에는 PPTP 클라이언트(PAC)기능이 구현되어 있고, VoIP 프로토콜 중에 하나인 SIP 프로토콜이 구현되어 있다. SIP 프로토콜을 이용해서 VoIP 서비스를 하기위해서는 기본적으로 프록시 서버 (Registrar 기능 포함)가 필요하며 이 서버는 PPTP 서버(PNS)뒤에 사설망에 연결되어 있다.

본 논문에서 구현한 도청방지용 인터넷전화(VoIP)의 실제로 음성데이터가 전달되는 과정의 각 노드들의 프로토콜 스택은 그림 5와 같다. Caller 단말기에 연결되어 있는 전화기에서 음성이 들어오면 오디오DSP를 통해서 디지털 음성데이터를 얻게 된다. 디지털 음성 데이터 앞에 RTP 헤더를 붙여서 UDP 계층으로 내려 보낸다. UDP 계층에서는 UDP 헤더를 붙이고 Private IP 계층으로 전달된다. 사설망 IP를 이용하여 IP 헤더를 붙이고, MPPE 계층으로 보낸다. 이 암호화 계층에서는 Private IP 계층에서 내려온 IP 패킷을 암호화한 뒤에 MPPE 헤더를 앞에 붙인다. 그리고 PPP 계층으로 내려 보낸다. PPP 계층에서는 PPP 헤더를 붙인 뒤 GRE 계층으로 보낸다. GRE 계층에서는 GRE 헤더로 캡슐화하여 Public IP 계층으로 보내진다. Public IP 계층에서는 실제 인터넷에서 통용될 수 있는 Public IP를 가지고 IP 헤더를 붙인다. 최종 IP 패킷을 이더넷 물리 계층으로 보내서 인터넷 망으로 이더넷 프레임을 송신하게 된다. 그리고 PNS에서는 caller 단말기에서 보낸 이더넷 프레임을 수신하여 caller 단말기의 역방향(이더넷 -> public IP -> GRE -> PPP -> MPPE -> Private IP)으로 처리하여 Private IP 계층에서 최종 목적지를 알아낸다. 최종 목적지에 따라서 called 단말기로 송신하기 위해서 위의 반대로 이더넷 프레임을 생성한다. 생성된 이더넷 프레임을 called 단말기로 인터넷을 통하여 송신한다. 또한 called 단말기에서는 PNS로부터 수신된 이더넷 프레임을 caller 단말기의 역방향으로 각 계층으로 처리하여 최종 자신에게로 온 음성데이터를 얻어내게 된다. 그림 5와 같은 프로토콜의 스택을 통해서 외부 인터넷 망으로 송/수신되는 이더넷 프레임에 캡슐화된 IP 패킷의 형태는 인터넷 망에서 IP 패킷을 가로챈다 하더라도 실제 중요한 데이터는 암호화되어 있기 때문에 분석할 수가 없게 된다.

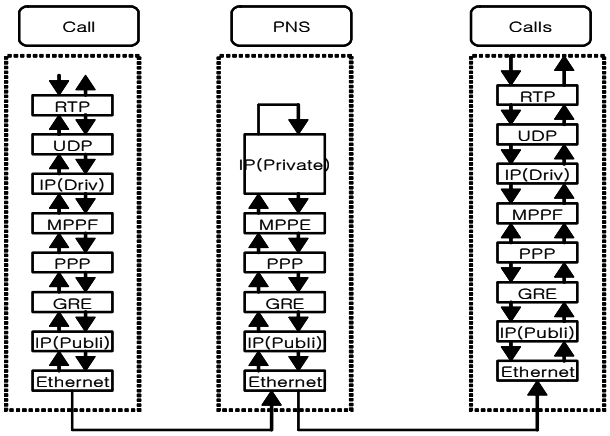

그림 5 음성 데이터 전송을 위한 프로토콜스택
Fig. 5. protocol stack for transmitting voice data

3. VoIP 전화기 통화품질 측정

시험망은 그림 6 에서와 같이 3개의 PAC과 각 로컬네트워크에 프락시 서버, PNS를 라우터로 연결하여 구성하였다. 여기에는 10개의 서브네트워크가 있으며, PNS는 PPTP 서버 부분을 담당하는 곳으로 PAC으로부터 제어연결 설정 요청이 오면 그에 대한 응답을 하여 PAC과 터널을 생성한다. 이미 생성된 터널을 통하여 PAC과 PPP를 이용하여 VPN을 형성한다.

PAC은 PPTP 클라이언트 부분을 담당하는 곳으로 PNS와 터널을 생성하여 사설망의 일원으로 참여한다. 프락시 서버는 SIP 프로토콜을 이용하여 VoIP전화 통화를 위해서 필요한 서버로서 현재 SIP UA들의 정보를 가지고 있다.

PNS는 PPTP 서버 기능이 구현되어 있는 장비로 PAC#1과 PAC#2의 사용자 ID와 비밀번호 정보를 가지고 있으며 VPN을 구성하기 위한 사설 IP pool을 가진다. 또한 2개의 네트워크 인터페이스가 있는데 로컬네트워크 인터페이스는 사설망 구성을 연결하고 외부네트워크 인터페이스는 인터넷망을 연결한다. 또한 1개의 PPTP 인터페이스를 가지고 있고, 외부네트워크 인터페이스를 통해서 수신되는 GRE 패킷을 암호화하여 라우팅 테이블에 의해서 로컬 망이나 또 다른 사설망의 클라이언트에게 전달한다. PAC#1와 PAC#2는 PPTP 클라이언트가 구현되어 있는 VoIP 단말기로 PNS의 공용 IP와 포트번호를 이미 알고 있다. PNS에게 인증을 받기 위한 자신의 사용자 ID와 비밀번호를 가지고 있다.

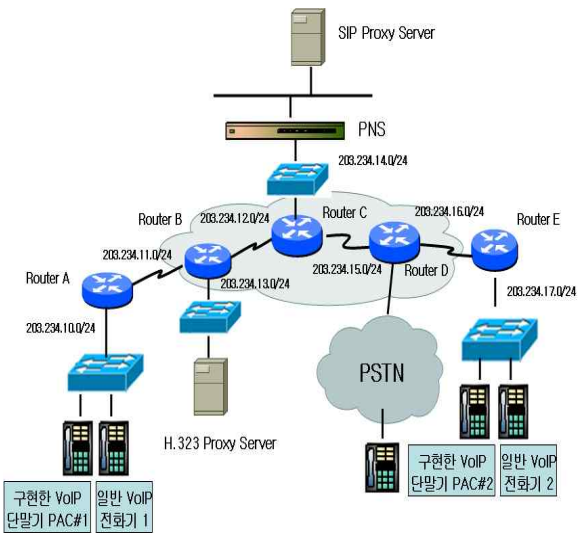

그림 6. VPN 기반의 VoIP 단말기 시험
Fig. 6. VoIP terminal test based on VPN

본 시험에서는 통화 품질의 각 측정 요소 중 가장 큰 영향을 미치는 단 방향 전달지연에 대해 RTT값을 측정하여 본 논문에서 구현한 VoIP 단말기의 음성품질이 전달지연 기준인 150ms에서 200ms 사이에 지연시간이 포함 되는 것을 보이고자 한다. 그러나 암호를 해석해야 하는 PNS는 통화량이 많을 때 집중화 현상이 발생하므로 PNS의 성능은 고려를 하여야 한다.

가. RTP 패킷포맷

SIP에서 사용되는 패킷은 G.723.1 코덱을 사용한 경우 전체 64바이트의 IP 패킷에서 IP 헤더와 옵션을 제외하면 8 바이트의 UDP 헤더와 36 바이트의 RTP 패킷으로 구성된다. RTP패킷은 다시 12바이트의 헤더와 24바이트의 음성 데이터로 구분되고 64바이트는 이 시험에 쓰인 SIP 애플리케이션이 채택하고 있는 G.723.1(6.3K) 코덱이 사용하는 암호화 데이터의 전체 크기이다.

음성압축 코덱 종류에 따라 전송되는 음성 데이터 길이와 IP 패킷에 캡슐화되는 데이터 길이는 다음과 같다.

- G.723.1 => 6.3Kbps, 30ms마다 24bytes씩 전송
- G.729A => 8Kbps, 10ms마다 10bytes씩 전송
- G.723.1의 경우(64bytes)
  private-ip header(20) + UDP header(8) + RTP header(12) + voice data(24)
- G.729A의 경우(50bytes)
  private-ip header(20) + UDP header(8) + RTP header(12) + voice data(10)

나. 캡슐화 지연

VPN의 PPTP 프로토콜을 사용하고 터널링을 구성하여 통화하는 경우는 그렇지 않은 경우와 비교하여 캡슐화 과정을 거치기 때문에 종단간의 지연시간의 차이가 나타날 것이고 그 차이를 조사하고자 한다. 측정 PAC에서 음성패킷을 보내고 네트워크 모니터링 도구인 스니퍼(Sniffer)를 통하여 되돌아오는 시간(Round Trip Time)과 패킷 순서를 측정하여 지연을 측정하였다. 라우팅의 경로상의 차이에서 발생하는 지연을 배제하기위해 VPN을 쓰지 않는 경우에도 같은 경로를 거치도록 시험 환경을 구성하였다.

그림 6 에서와 같이 구현한 VoIP 단말기 PAC #1과 PAC #2의 경로와 같이 일반 VoIP전화기 #1, 일반 VoIP 전화기 #2의 경로를 구성하였다. 그러면 VPN을 적용한

VoIP 전화기와 일반 VoIP 전화기의 차이는 터널링을 위한 캡슐화 오버헤드만 남게 된다. 두 경우의 차이는 RTT 값을 구하면 알 수 있다. 본 시험을 통해 얻은 각 코덱별 RTT 값은 다음 표 2와 같다

시험 결과 VPN을 적용한 VoIP 전화기의 RTT는 표 2에서 보는 것과 같이 데이터의 길이에 따라 5ms ~ 11ms였고 일반 VoIP 전화기의 RTT는 데이터 길이에 따라 1ms ~ 3ms 였다. 즉, VPN을 적용한 인터넷 전화기와 일반 VoIP 전화기와의 지연시간의 차이는 최대 8ms 이하이고, 대부분은 VPN의 터널링을 위한 패킷 캡슐화에 소요되는 시간으로 볼 수 있다. 위의 종단간 지연 시험결과를 종합해 보면 데이터의 길이가 클수록 지연시간의 차이는 증가하는 양상을 보였지만 데이터의 길이가 1000byte를 넘는 경우는 없을 것이고, 일반적으로 하나의 패킷에 1개의 프레임을 전송한다고 했을 때 지연시간의 차이를 보면 4ms 이하이고 최대 7개의 프레임을 한 번에 전송한다고 했을 때에도 최대 데이터 길이는 208byte를 넘지 않고 RTT의 차이는 4ms를 넘지 않았다.

표 2. encryption 대 no-encryption의 RTT 값 비교표
Table 2. RTT data for encryption to no-encryption

데이터길이(바이트)	비 암호화	암호화	차이
64(G.723.1)	1ms	5ms	4ms
50(G.729A)	1ms	5ms	4ms
200(G.711)	1ms	6ms	5ms
88(G.723.1)	1ms	5ms	4ms
112(G.723.1)	1ms	5ms	4ms

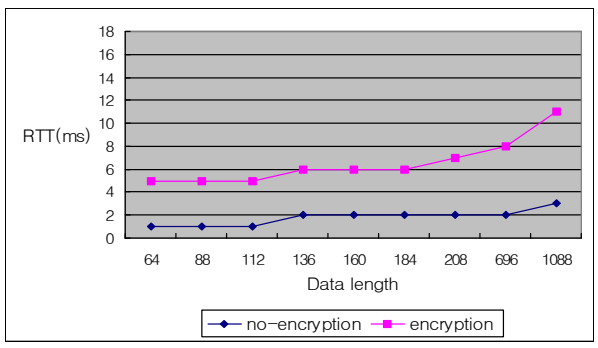

그림 7. G.732.1을 사용한 경우 RTT 값 비교
Fig. 7. RTT data using G732.1

표 1에서와 같이 본 논문에서 기준치로 잡았던 161ms(최악의 경우)에 캡슐화로 인한 지연시간을 합해도 165ms 정도이고, ITU-T의 권고안에서 정한 만족한 통화를 할 수 있는 단 방향 지연의 기준치인 150ms ~ 200ms 안에 있으므로, 기존의 VoIP 일반 전화기와 본 논문에서 제시한 VPN을 적용한 VoIP와의 통화품질의 차이는 무시할 만하다.[6]

또한 인터넷 전화기의 종단간 지연이 150ms 이하 이면 인간의 청력으로는 감지할 수 없는 수준이고 150ms ~ 400ms 이면 통화 가능한 수준이지만 400ms 이상이면 음성의 통신은 심각한 장애가 발생하게 된다.

그림 7은 G.723.1 코덱을 사용한 경우 한 개의 패킷에 들어가는 프레임의수를 증가 시키면서 측정한 RTT 값을 기존의 VoIP 전화기와 비교한 그래프이다.

그림 8은 G.729A 코덱을 사용했을 경우 1개에서 최대 9개의 프레임을 1개의 패킷에 넣어 전송할 경우, 암호화한 경우와 그렇지 않은 경우의 전송지연 차이를 보인 것이다. 위에서 언급했듯이 VPN을 적용한 VoIP 단말기와 일반 VoIP 단말기의 지연시간 차이는 최대 5ms를 넘지 않는다.

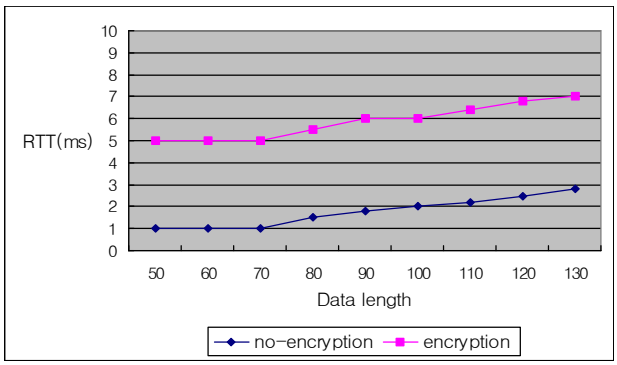

그림 8. G.729A을 사용한 경우 RTT 값 비교
Fig. 8. RTT data using G729A

다. 네트워크 부하

VoIP의 SIP 프로토콜을 이용한 음성 통화 시에 네트워크상에 존재하는 부하에 초점을 두고 하나의 패킷 안에 몇 개 프레임을 전송하는 것이 적절한가를 측정하였다. 하나의 패킷에 한 번에 많은 프레임을 보내어 대기시간이 길어지는 것과 프레임을 적게 보내어 빠른 대기시간을 기대하는 것에 대하여 논의할 여지기 있다. 본 논문에서 사용한 SIP 애플리케이션은 하나의 패킷 안에 64바이트의 프레임을 전송 한다.

그림 9는 하나의 패킷 당 프레임 개수를 다르게 하여 통신하는 동안 구한 네트워크 전체 패킷의 크기에 대한

것인데 PAC과 PNS 사이에 캡슐화로 인해 64 바이트 헤더가 더해지므로, VPN을 적용한 VoIP 단말기를 사용할 경우 하나의 패킷에 몇 개의 프레임을 전송할 지는 중요하다.

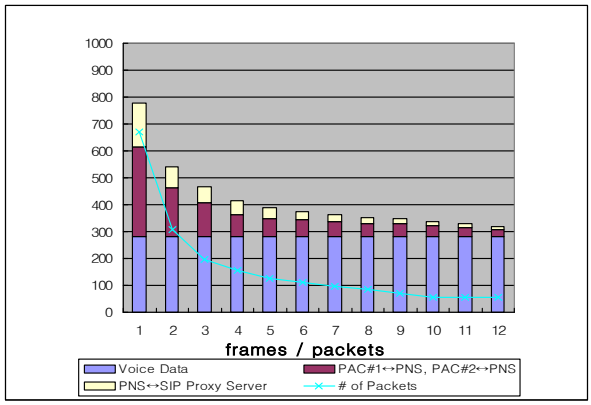

그림 9. 네트워크 부하
Fig. 9. network overload

라. 패킷 당 프레임 수

가장 적합한 패킷 당 프레임수를 얻기 위해 그림 10은 패킷 도달 간격을 도시한 그래프이다. 가운데 2선은 99% 신뢰를 갖는 구간을 이은 것 이고 바깥쪽 2선은 최고와 최악의 경우에 패킷 도달 간격을 그린 것이다

종단간 지연을 160ms ~ 170ms 로 할 때 패킷 당 프레임 개수는 2 ~ 3개가 적합하다.

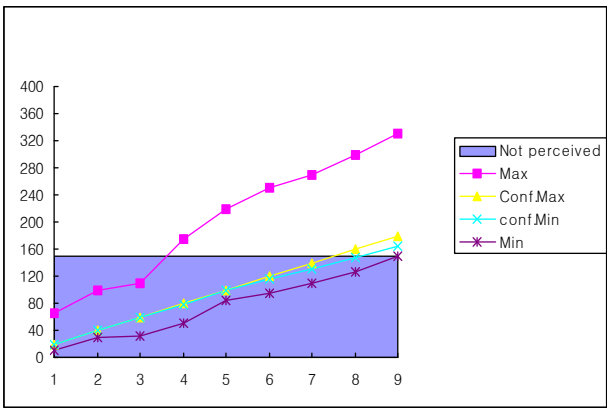

그림 10. 패킷당 프레임 수 변화에 의한 패킷도달 간격
Fig. 10. packet arrival interval by changing number of frame per packet

Ⅶ. 결 론

음성 보안기능이 적용된 인터넷 전화기의 하드웨어를 설계하고, SIP 프로토콜 스택을 구현하여 호 처리를 수행하였으며, 가상 사설망의 프로토콜인 PPTP를 사용하여 터널링 기법으로, 사용자의 ID와 비밀번호를 이용하여 CHAP으로 인증기능과 MPPE, MPPC로 암호화와 압축 기능을 수행 하였다.

구현된 인터넷 전화 단말기의 호 처리율과 보안기능 추가로 음성 품질에 영향을 미칠 종단간 지연시간을 측정하여, ITU-T에서 제안한 종단간 지연시간의 범위인 150mc ~ 200 ms를 만족 하였다.

일반 VoIP 전화기와의 지연시간의 차이는 최대 5ms 이하였다. 대부분은 VPN의 터널링을 위한 패킷 캡슐화에 소요되는 지연시간으로 예상할 수 있고, 평균적으로 지연시간의 차이는 4ms ~ 5ms 이하이므로, 일반 VoIP 전화기와 본 연구에서 제시한 VPN을 적용한 VoIP 전화기와의 통화품질의 차이는 무시할 만하다.

그러나 본 논문에서 사용된 PPTP 프로토콜은 제어연결(Control Connection)메시지가 암호화가 되지 않는다는 점과, 인증기능이 없다는 단점으로 중간에서 제어연결메시지를 가로채서 분석함이 가능하기 때문에 보다 완벽한 암호화(Security)가 이루어 질 수 없다는 문제점을 여전히 내포하고 있다. 그러나 이 문제는 L2TP가 보완하고 있다.

참 고 문 헌

[1] M. Hamdi, et. al., *"Voice Service Interworking for PSTN and IP Networks,"* IEEE Communications Magazine, Vol. 37, No. 5, pp.104-111. May 1999.

[2] D.Kroeselberg, *"SIP security requirements from 3G wireless networks",* Internet Draft, IETF, Jan. 2001. Work in progress.

[3] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999

[4] Ananth Nagarajan, *"Generic Requirements for Provider Provisioned VPN",* IETF Internet Draft Provider Provisioned VPN WG, December, 2002.

[5] W. Simpson, "PPP LCP Extensions", RFC 1548,

January 1994
[6] TIA/EIA/TSB116, V*oice Quality Recommendations for IP Telephony*, March 2001.
[7] A. Percy, *Understanding Latency in IP Telephony*, Brooktroot Technology, pp.34-41 1999.
[8] ITU-T *Recommendation G.114, One-Way Transmission Time*, February 1996.

저자 소개

김 삼 택(정회원)

- 1985년 한남대학교 전자계산학과 학사졸업
- 1987년 중앙대학교 전자계산학과 석사 졸업.
- 2005년 중앙대학교 컴퓨터공학과 박사학위
- 1995년 3월 ~ 2007년 8월 우송정보대학 컴퓨터정보통신계열 교수.
- 2007년 9월 ~ 현재 우송대학교 컴퓨터정보학과 교수

<주관심분야 : 유/무선 네트워킹, VoIP, 모바일 컴퓨팅, ITS>