논문 2010-6-9

VPN 기능을 가진 음성 보안용 IP-PBX 개발

Development of the IP-PBX with VPN function for voice security

김삼택*

Sam-Taek Kim

요 약 오늘날 VoIP 기반의 인터넷 전화 서비스는 일반 사용자의 폭발적인 인기에 따라 사용자의 다양한 요구사항이 증가하고 있는데. 그중 가장 중요한 것은 전화서비스의 음성 보안이다. 음성 통화는 사용 목적에 따라 비밀을 유지하여야 되는데 인터넷 전화는 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 방지할 수 있도록 SIP를 기반으로 하고 가상사설망의 IPsec을 적용하여 음성데이터의 전송에 터널링 기법을 사용함으로 사용자 인증과 음성 데이터의 기밀성이 강화된 VPN IP-PBX를 개발하고 인터넷 교환기의 성능을 측정하였다. 본 음성 보안용 IP-PBX는 문자 메시지 전송, 게이트웨이 기능 등 다양한 부가 서비스를 갖고 소프트폰과 연동 가능하다.

Abstract Today, Internet Telephony Services based on VoIP are gaining tremendous popularity for general user. Therefore a various demands of the user keep up increase, the most important requirements of these is voice security about telephony system. 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 VPN IP-PBX for the voice security and measured conversation quality by adopting VPN IPsec based on SIP and using tunnel method in transmitting voice data to prevent eavesdrop of voice data. This VPN IP-PBX that is connected Soft-phone provide various optional services.

Key Words : VoIP, IP-PBX, IPTelephony ,VPN, SIP, IPsec

Ⅰ. 서 론

최근 개방성을 앞세워 폭발적인 인기를 끌고 있는 VoIP기반의 무료 인터넷 전화 서비스는 일반사용자에게 인터넷폰에 대한 인식을 확산시켰으며, 기존의 음성 통신시장에 새로운 변화를 야기하고 있다. VoIP(Voice over Internet Protocol)는 패킷교환망인 인터넷 상에서 연속성과 실시간성을 가지고 음성정보를 실어 나르는 기술이다. 다양한 응용분야가 가능하지만, 현재는 인터넷폰과 거의 동일한 의미로 사용되고 있다. VoIP 보급은 인터넷 인프라 개선, 음성 코덱 기술의 발달, 국제 표준안 규격에 맞춘 VoIP 장비 및 소프트웨어의 상용화로 인해 확산되었다. 또한, 인터넷에서의 음성서비스를 통해 고객과의 접촉이 쉬어짐에 따라, 기존 통신망 기반의 서비스업체들이 VoIP를 도입하기 시작하였다. 이와 같은 이유로, VoIP 시장은 빠른 속도로 확대되고 있다.[1]

이러한 장점을 가지고 있는 인터넷 전화는 상대방과 회선이 직접 연결되어 도청이 상대적으로 어려운 공중전화망과 달리, 인터넷 망에 동시에 다수가 접근 가능 하므로 상대방과 음성 통화에 보안을 유지하기가 쉽지 않다. 그러나 음성 통화는 사용 목적에 따라 비밀을 유지하여야 한다. 이러한 인터넷 전화는 인터넷의 특성상 하나

*정회원, 우송대학교 컴퓨터정보학과(교신저자)
접수일자 2010.9.2 수정일자 2010.11.22
게재확정일자 2010.12.15

의 망에서 일반 대중들이 동시에 사용할 수 있는 점 때문에 항상 해커들에 의해서 도청에 무방비 상태로 놓여 있을 수 있다.

그러므로 본 논문에서는 SIP 프로토콜 스택을 적용하고 가상사설망을 이용하여 VPN(Virtual Private Network)의 IPSec 프로토콜로 해킹과 도청방지를 할 수 있는, 소프트폰과 연동 가능한 인터넷 교환기를 개발 한다. 본 음성 보안용 IP-PBX는 문자 메시지 전송, 게이트웨이 기능등 다양한 부가 서비스 기능을 수행 한다.

Ⅱ. IP-PBX 시스템

1. 소형 임베디드 IP-PBX 소프트웨어 구성

본 논문에서 개발한 사설망을 이용한 임베디드 IP-PBX의 하드웨어는 그림 1 에서 보는 보는바와 같이 설계하였다. 본 논문에서 개발한 IP-PBX는 WAN(RTL8201) 1포트와 LAN(RTL8306SD) 4포트를 설계하였다. 그리고 인터넷이 단절될 때를 대비하여 백업용으로 FXO(F89010) 1포트를 설계하였으며, FXS(LE88266) 3포트를 두어 일반 전화 3대를 인터넷 전화로 사용할 수 있도록 설계하였다. 이 모든 것을 처리할 수 있는 중앙처리 장치로는 미국 MindSpeed사에서 개발한 32bit 데이터/어드레스 버스를 가지고 있는 M82154를 사용하였다. 본 중앙처리 장치의 데이터 처리 속도는 450MHz이며, 또한 본 중앙처리 장치는 데이터와 네트워크 데이터를 각각 분리 하여 처리 할 수 있는 이중(Dual Prosser)처리가 가능하도록 설계되어, 전화 교환 기능과 공유기능을 불리하여 실행하게 함으로써 CPU 효율성을 높였다. 인터넷 연결이 끊어졌을 때도 통화가 연결 될 수 있도록 하기 위하여 LE87010 1 개를 사용하여 FXO 한 채널을 사용할 수 있도록 설계하였다. 그리고 팩스 또는 일반 전화도 본 장치에 연결하여 인터넷 전화처럼 사용할 수 있도록 하기 위하여 한 개의 모듈에서 FXS 2채널을 연결할 수 있는 LE88266 2개를 사용하여 3채널의 FXS를 설계하였다. 또한 본 장비에 무선 인터넷과 전화를 위해 Wi-Fi 모듈을 붙일 수 있게 설계 하였다. 그리고 본 장치에 4개의 LAN(RJ45)을 연결할 수 있도록 RTL8306SD LAN 스위치 칩을 사용하였다. 이때 사용한 메모리는 64Mbyte용량의 NOR Flash와 역시 64Mbyte용량의 NAND Flash를 사용하였으며, 64Mbyte DDR SDRAM를 사용하였다. 그리고 본 논문에서 사용한 운영체제(Operating System)은 Linux 기반으로 버전 2.6.21를 자체 개발하여 사용하였다. 그림 1은 개발된 부위별 상세 설계도를 나타낸다.

본 논문에서 개발한 임베디드형 IP PBX는 아날로그 전화선을 IP PBX에 연결하기 위하여 4포트를 한 모듈로 하는 FXO, FXO 모듈을 그림 2에서 보는 바와 같이 설계하여 내부에 설치하도록 하였다.

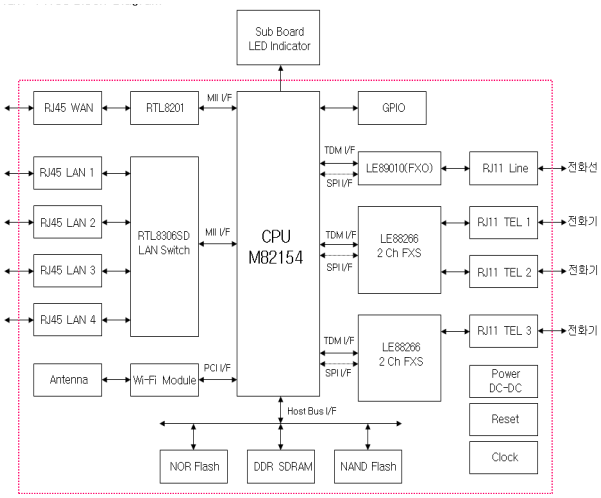

그림 1. IP-PBX 하드웨어 블록 다이어그램
Fig. 1. The block diagram of IP-PBX H/W

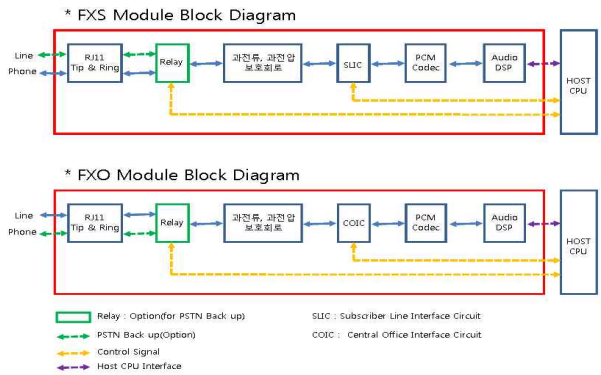

그림 2. FXO, FXS블럭 다이어그램 모듈
Fig. 2. The block diagram module of FXO, FXS

2. 소형 임베디드 IP-PBX 소프트웨어 구성

본 논문에서 구현한 소형 임베디드 IP PBX시스템 단말기의 프로토콜 스택은 그림 3에서 보는바와 같이 구성하였다. 프로토콜 스택은 다음 그림 3에서 보는바와 같이 5레벨로 구성되어 있으며 기본적인 인터넷에 사용되는 프로토콜로 본 논문에서 구현한 단말기 환경구성정보

(Configuration)를 등록하기 위하여 웹(Web)과 텔넷(Telnet)프로토콜을 이용하여 구현하였다. 그리고 IP PBX를 위하여 사설 프로토콜을 정의하여 VoIP 콜을 연결하기 위하여 SIP(Session Initiation Protocol)프로토콜을 사용하였다. 그리고 ADD(Audio Device Driver)와의 보이스(Voice)데이터 통신을 위하여 RTP/RTCP 프로토콜을 구현하여 사용하였다.[2]-[4]

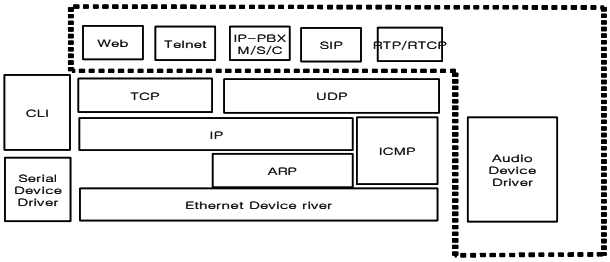

그림 3. 소형 임베디드 IP PBX시스템 프로토콜 스택
Fig. 3. The system protocol stack of small Embeded IP-PBX

본 논문에서 구현한 소형 임베디드 IP PBX시스템의 통신 개념은 그림 4 에서와 같이 본사와 원거리 지사가 일반 전화망(핸드폰, 일반전화)을 연결할 수 있으며, 같은 형태의 단말기에 환경구성정보를 등록하는 값에 따라 마스터, 서버, 클라이언트로 사용할 수 있다. 본사에는 반드시 주소 서버를 갖추고 있어야 하며, 또한 고정 IP를 가지고 있어야하는 마스터로 등록하고 각 지사에는 서버로 등록할 수 있으며, 마스터에는 각 지사의 주소와 해당 서버에 연결 되어 있는 클라이언트의 IP주소와 포트번호가 저장되어 있다. 사설 IP를 가지고 있는 각 서버의 클라이언트와 클라이언트 간에 통화를 원할 때는 해당 서버가 마스터의 도움 없이 자신이 관리하는 콜리의 IP주소와 포트번호의 값을 콜러에게 주어 콜러 클라이언트와 콜리 클라이언트의 호를 연결하게 된다. 그리고 외부의 일반 전화망(PSTN) 또는 핸드폰과의 통화는 마스터 또는 서버를 통해서 연결이 가능 하도록 하였다.[5]-[9]

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. 본 논문에서는 가장 기본적으로 필요하고 많이 사용되는 프로토콜의 스택으로 SIP프로토콜 스택 사용하였으며, 그 스택의 구조는 그림 5와 같다. 그림에서 보는 바와 같이 SIP프로토콜 스택은 크게 3가지의 기능들과 결합하여 사용된다.

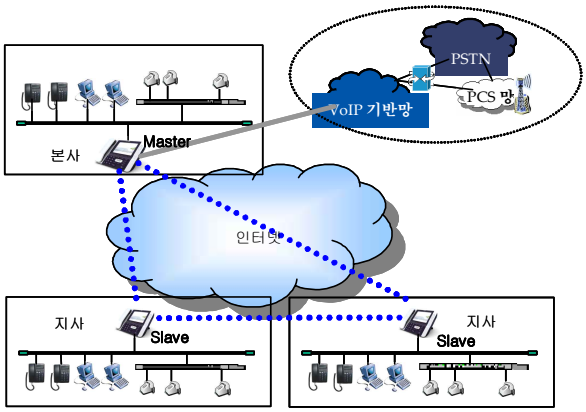

그림 4. 분산형 IP PBX 구성도
Fig. 4. Distributed IP-PBX configuration

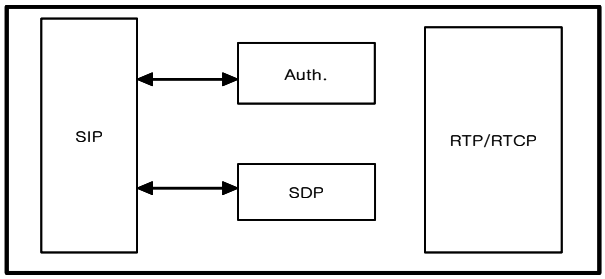

그림 5. SIP 스택 구조
Fig. 5. The structure of SIP stack

III. 침입 및 도청 방지를 위한 VPN 보안

최근에는 VPN 기술이 IPsec(IP Security) 프로토콜로 표준화 되고, 많은 도입 기업에서 VPN 의 보안성과 신뢰성이 검증됨에 따라 원격지 네트워크를 안전하고 효율적인 비용으로 연결할 수 있는 솔루션으로 인정받기 시작하였다. VPN에서 터널링은 외부로부터 어떠한 영향도 받지 않고 안전하게 정보를 전송할 수 있는 가상의 연결로써 사전에 약속한 특별한 프로토콜로 세션을 구성, 타 사용자나 외부로부터 안전하게 보호 받는 기술이다. VPN 프로토콜의 주요 역할은 패킷 캡슐화, 터널 생성 및 관리, 그리고 암화 키 관리등이 있는데, 이러한 대표적인 기술로 PPTP, L2F, L2TP, VTP, IPSec, SSL 등과 같은 다양한 프로토콜이 있다. VPN 터널링 프로토콜은 터널이 형성되고 운영되는 계층(Layer)에 따라 구분된다. 오늘날 대부분의 VPN 터널링 기술은 2계층과 3계층, 그리

고 4계층으로 구현된다. 과거에는 대부분의 VPN 제조사들이 시장 지배력을 강화하기 위하여 고유의 독자적인 터널링 기술을 사용함으로써 동일 벤더 제품 간에 만 호환성을 갖는 폐쇄적인 성격을 갖고 있었다. 현재는 IPSec이나 SSL 등과 같은 표준화된 터널링 기술을 수용하여 이기 종 간 VPN 구성도 가능하게 되었다. OSI 참조모델에서 데이터 링크 계층인 2계층 터널링 기법은 가장 보편적인 형태로 대부분 IPSec 이전의 VPN 기술로 IP나 IPX 패킷을 PPP화 한후, 다시 터널링 프로토콜로 캡슐화 하는 형태를 사용한다.[10]

본 논문에서 사용한 음성 보안 장치로는 가상사설망에 주로 사용하는 IPSec을 구현하였으며, IPSec은 IETF 워킹그룹에 의해 제안되고 표준화(RFC2401 2412)된 보안 프로토콜로 스푸핑이나 스니핑 공격에 취약한 IP 프로토콜의 보안상 문제점을 해결하고 네트워크 계층에서의 보안성을 보장하기 위한 목적으로 개발됐다. IPSec은 데이터 암호화와 인증 및 무결성 서비스를 제공하기 위한 ESP(Encapsulation Security Payload) 헤더와 IP 헤더와 전송 헤더 사이에 위치하는 인증 헤더로 인증 부분을 처리하기 위한 AH 헤더, 그리고 암호화키를 관리하기 위한 IKE, DOI 등 키 관리 부분으로 구성되어 있다. IPSec은 TCP/IP 스택보다 낮은 계층으로, 이 계층은 각 컴퓨터의 보안 정책과 송·수신자가 협상한 보안 결합에 의해 제어된다. 또한 보안 정책은 필터와 보안 규칙들로 정의된다.

V. 통화품질 시험

1. 동시 통화 시험 및 결과

본 연구에서 개발한 소형 임베디드 IP PBX의 성능 중에서 동시 콜을 시험하기 위하여 그림 6에서 보는 바와 같이 시스템을 구성하였다. 본 시험에서 사용된 동시 통화 수를 측정하는데 일반 적으로 많이 이용되는 SPIRENT사에서 개발한 ABACUS 5000모델을 사용하였다. 그림에서 보는바와 같이 ABACUS 5000에 소형 임베디드 IP PBX의 WAN 포트와 LAN 포트를 서로 연결하였다. ABACUS의 slot1은 콜러기능을 담당하여 INVITE를 생성하고 slot2는 콜리기능을 담당하여 INVITE를 수신하면 180, 200을 생성하여 보내게 되어 통화로 생성된다. ABACUS의 콜러에서는 통화로가 생성되면 DTMF를 생성하여 콜리에게 보내어 수신되는 DTMF를 비교하여 정상적인 통화가 이루어지는지를 판단하게 되고, MOS도 계산하게 된다.

1분에 2개의 통화가 생성되도록 메시지를 생성하며, 통화완성율과, 통화품질을 계산하여 통계를 계산한다.

그림 6. 동시통화 수 측정 개념도
Fig. 6. The conceptual diagram of measuring the number of simultaneous telephone calls

본 논문에서는 개발 장비의 동시 콜 성능을 측정하기 위하여 10콜부터 매 5콜 단위로 증가시키며 음성품질(MOS), 패킷 손실, 호 완료율을 측정하였다. 측정결과 패킷 손실률은 그림7 에서 보는바와 같이 0.2%에서 최대 1%까지 나타났으며, 그에 따라서 음성 품질 또한 그림 8에서 보는바와 같이 35콜까지 4.6유지하였으며 동시콜 40콜에서 4.18로 낮아졌다. 그러나 한국통신에서 요구하는 통화 품질 4.0 이상의 범위에는 여전히 존재하고 있었다. 통화 완료율은 그림 9에서 보는바와 같이 30콜까지는 통화 실패 없이 100%의 완료율을 나타났지만 30이상부터 90%대로 떨어졌음을 알 수 있었다 . 따라서 본 장비는 당초 개발 목표로 한 30인 이하의 사용자가 사용할 수 있는 인터넷 교환기로 적당함을 알 수 있다.

그림 7. 패킷 손실률 측정결과
Fig. 7. The measuring results of packet loss

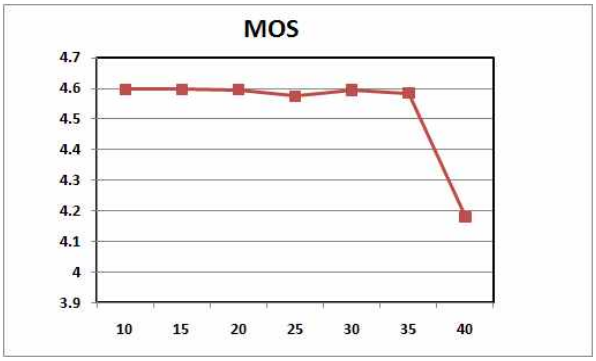

그림 8. 통화 품질 측정결과
Fig. 8. The measuring results of speech quality

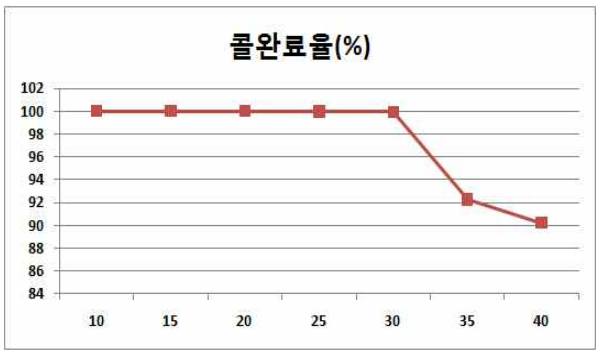

그림 9. 호 완료율 측정 결과
Fig. 9. The measuring results of call completion rate

2. Qos 시험

네트워크 활용도가 증가하면서 안정적인 네트워크 서비스 기반 구축에 대한 요구가 더욱 거세지고 있으며 관리자에게는 최적의 네트워크 운용과 관리를 위한 효율적인 트래픽 제어와 대역폭 관리가 절실하게 필요하다. 결국 서비스의 품질 보장에 대한 다양한 사용자 요구와 효율적인 네트워크 운영을 위한 해결책으로서 QoS는 최적의 솔루션으로 부각되고 있으며 현재의 네트워크 문제를 해소하기 위한 일시적인 대안이 아닌 네트워크의 필수 핵심 요소로 자리매김하고 있다. 따라서 본 논문에서 개발한 임베디드 VPN IP PBX의 QoS를 시험하기 위하여 그림 10과 같이 시스템을 구성하였다. 본 시험을 위해서 SDK 버전 3.4.4을 사용했으며, 시험방법으로는 소형 임베디드 IP PBX의 LAN1~LAN4에 각각 개발된 IP PBX를 1대씩 연결하여 UDP 패킷을 WAN측 1대의 PC로 송신할 수 있도록 구성하였다. 그림 11은 QoS 측정 장면을 나타낸다.

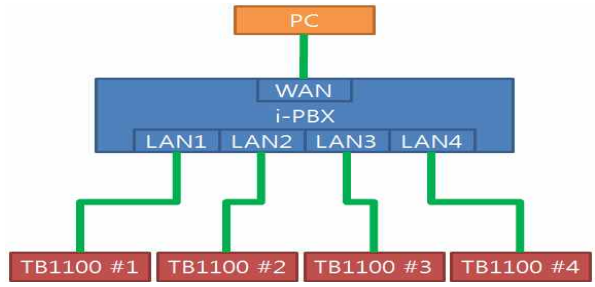

그림 10. QoS 측정 개념도
Fig. 10. The conceptual diagram of measuring Qos

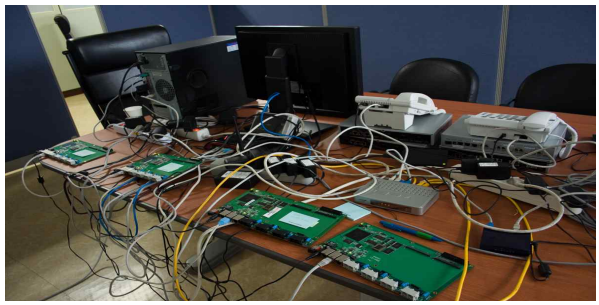

그림 11. QoS 측정 장면
Fig. 11. The actual scene of measuring Qos

3. Qos 시험 결과

본 논문에서 개발한 소형 임베디드 IP PBX의 성능을 아래 표에서 보는바와 같이 3가지 형태로 측정을 하였다. 먼저 본 장비에 QoS를 적용하지 않았을 때는 그림 12에서 보는바와 같이 DSCP(분화된 서비스 코드 포인트=네트워크 트래픽에 서로 다른 수준의 서비스를 할당할 수 있도록 하는 IP 패킷의 한 필드)는 LAN1~LAN4에 0을 입력하였다. 그때 각각의 콜 완료율은 52.1%에서 최대 77.3%까지를 나타남으로 알 수 있듯이 네트워크 데이터의 과다로 호 완료율이 매우 좋지 않음을 알 수 있다. 그리고 LAN3에 ToS 184(가장 높은 우선순위)를 적용한 경우에는 그림 13 에서 보는바와 같이 LAN3에서만 DSCP의 값 46을 입력하였을 때 95.8%로 매우 높은 호 완료율을 나타냈다. 또한 LAN2에 가장 높은 우선순위를 부여하고 LAN1에 그 다음 우선순위를 적용한 경우도 그림에서 알 수 있듯이 가장 우선순위가 높은 LAN2가 가장 높은 호 완료율을 보였으며 그 다음 우선순위에 따라 호 완료율이 높아짐을 알 수 있었다. 마지막으로 LAN4에 가장 높은 우선순위를 부여하고 LAN2와 LAN3에 그 다음 우선순위를 적용한 경우 측정결과는 그림 14에서 보는바와 같이 DSCP는 LAN1 에 0을 입력하고,

LAN2, LAN3에 34입력하였으며, LAN4에 46을 입력하였을 때 우선순위를 적용 받지 않고 LAN1은 12.4%로 매우 낮은 호 완료율을 나타냈고 우선순위가 높을수록 호 완료율이 높아져 가장 우선순위가 높은 LAN4는 98.3%의 높은 호 완료율을 나타냈다.

표 1. QoS 미 적용 시 호 완료율 측정 결과
Table 1. The measuring results of call completion rate on no-Qos

포트	DSCP	호 완료율
LAN1	0	52.1
LAN2	0	45.7
LAN3	0	61.3
LAN4	0	77.3

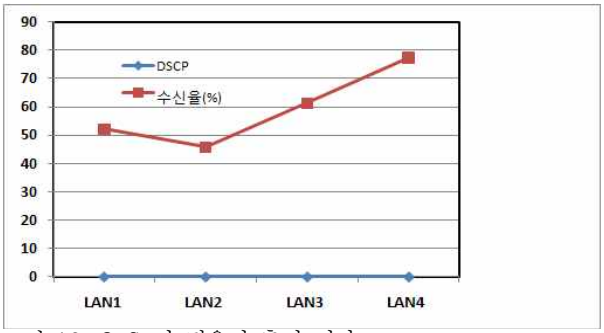

그림 12. QoS 미 적용시 측정 결과
Fig. 12. The measuring results of no-Qos

표 2. LAN3에 ToS 184를 적용한 경우 호 완료율
Table 2. The measuring results of call completion rate on Tos 184 at LAN3

포트	DSCP	호 완료율
LAN1	0	55.4
LAN2	0	43.9
LAN3	46	95.8
LAN4	0	48.8

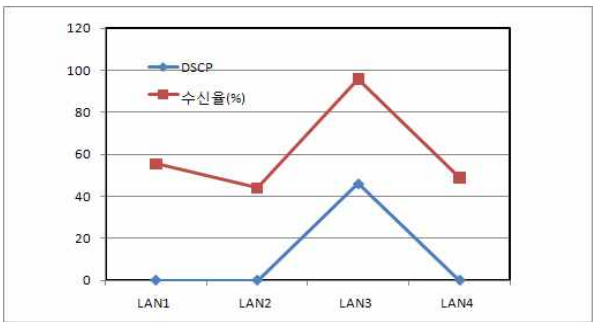

그림 13. LAN3에 ToS 184를 적용한 경우 측정결과
Fig. 13. The measuring results of ToS 184 at LAN3

표 3. LAN2에 가장 높은 우선순위, LAN1에 그 다음 우선순위를 적용한 경우 수신율
Table 3. The measuring results of receiving call rates on the highest priority at LAN2 and LAN1

포트	DSCP	수신율(%)
LAN1	34	64.2
LAN2	46	95.6
LAN3	0	34.8
LAN4	0	27.6

표 4. LAN4에 가장 높은 우선순위, LAN2와 LAN3에 그 다음 우선순위를 적용한 경우 호 완료율
Table 4. The measuring results of receiving call rates on the highest priority at LAN4 and LAN2, LAN3

포트	DSCP	호 완료율
LAN1	0	12.4
LAN2	34	36.4
LAN3	34	53.8
LAN4	46	98.3

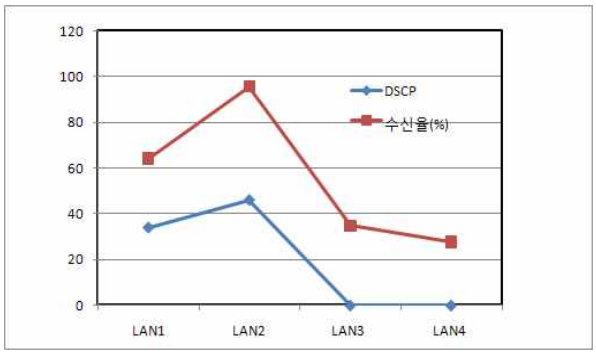

그림 14. LAN2에 ToS 184(가장 높은 우선순위)를 적용한 경우 측정결과
Fig. 14. The measuring results of ToS 184(the highest priority) at LAN2

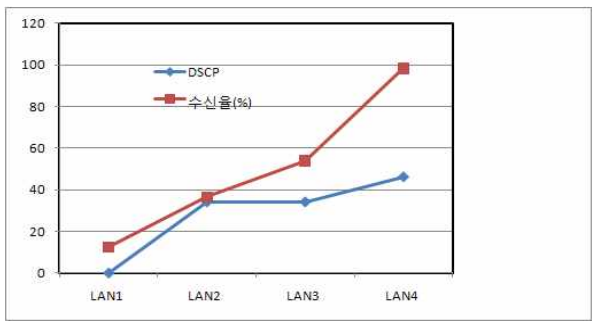

그림 15. LAN4에 가장 높은 우선순위, LAN2와 LAN3에 우선순위를 적용한 경우
Fig. 15. The measuring results of the highest priority on LAN4 LAN3 and LAN2

V. 결 론

본 논문에서 개발한 VPN 기능을 가진 소형 유무선 임베디드 IP 교환기는 IPSec을 이용한 음성 보안 기능을 갖고 소프트폰과 연동 가능하며 Qos 시험결과 우선순위가 높을수록 호 완료율이 높아져 가장 우선순위가 높은 LAN4는 98.3%의 높은 호 완료율을 보였다 .

본 논문의 결과로 기대되는 효과로 먼저 기술적인 측면은 VPN 보안 기능을 적용한 SIP 음성 통신 프로토콜 제작 기술과 P2P IP-PBX 하드웨어 설계 기술을 확보 할 수 있다. 그리고 P2P형 IP-PBX용 실시간 리눅스 운영체제 제작 기술을 확보함으로써 소형 IP-PBX 뿐 만이라 중형, 대형의 IP-PBX 제작 기술 확보에도 커다란 기대 효과를 가져 올 수 있다

참 고 문 헌

[1] 유승선,김삼택,이성기 “VPN을 적용한 인터넷 전화단말기의 설계”, 한국통신학회논문지 v.30

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

[3] "SIP Working Group," http://www.ietf.org/html.charters/sip-charter.html

[4] RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[5] RFC 793 Transmission Control Protocol (TCP)

[6] RFC 768 User Datagram Protocol (UDP)

[7] RFC 2327 Session Description Protocol (SDP)

[8] Allan Sulkin, PBX Systems for IP Telephony : Migrating Enterprise Communications, McGraw-Hill, April 2002.

[9] Harte Lawrence and Flood Robert, Introduction to Private Telephone Systems: KTS, PBX, Hosted PBX, IP Centrex, CTI, IPBX and WPBX, Lightning Source Inc, MAy 2005.

[10] Ananth Nagarajan, *"Generic Requirements for Provider Provisioned VPN"*, IETF Internet Draft Provider Provisioned VPN WG, December, 2002. no. 2A, pp.12-19, 2005.

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>