A Study on VoIP Information Security for Vocie Security based on SIP

Kyung Sung, *Member, KIMICS*

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 eaves-drop 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.

Index Terms—VoIP, SIP, PSTN, Security, PPTP

I. INTRODUCTION

As the internet came to be recognized to the public through Web later in 1980, it has become to develop into a communication network connecting the world. Therefore, the internet on the basis of such a communication network is becoming a necessary factor of modern society in 21st century, and the industry and technology based on the internet are developing day by day. Among them all, Voice over Internet Protocol(VoIP) using the internet by the development of voice transmission technology making use of internet is rapidly developing to the extent that it can replace the existing Public Switched Telephone Network(PSTN). Further the VoIP has an advantage of extraordinary cheapness in a utility rate over the existing PSTN, and it also can provide with rates exorbitantly cheaper than now through the telephone not only for the voice but for all the services the internet is giving, so that it will gain a footing in a way of communication necessary to our daily lives in the future. But there can be a danger of wiretapping by hackers all the time due to the fact that such a VoIP can be used simultaneously by the public in one network. In this study, therefore, in order to prevent the wiretapping by the Internet phone, an Internet phone terminal was developed by using Virtual Private Network(VPN). And it was analyzed for its performance and examined for its validity by applying PPTP(Point-to-Point Protocol) to the Internet phone terminal using SIP protocol stack in order to prevent wiretapping [1].

Manuscript received December 13, 2007.
Kyung Sung is with the Department of Computer Education, Mokwon University, Doan-dong 800, Seo-gu, Daejon, 302-729, Korea

II. VoIP terminal hardware VPN

To bring in VoIP terminal applying VPN, a hardware was designed as the Figure 1 As shown in the Figure 1, the hardware designed in this study is largely composed of main-board and sub-board. The sub-board was composed of processor modules, and the main-board was designed so as to provide two ports connecting the internet to the function bloc like Audio DSP, Ethernet, SLAC/SLIC and Power part and to have two ports possible for telephone analogue input/output. The detailed diagram for main module is as follows. Figure 2 shows the detailed diagram of Processor module in this study used MPC850 with a speed of 50Mhz developed by Motorola as well as 2MB FROM and 8MB SDRAM. And it was made up so that one RJ45 port can be linked to internet and the the other RJ45 port to inside network through a connection of mpc850 ethernet port.

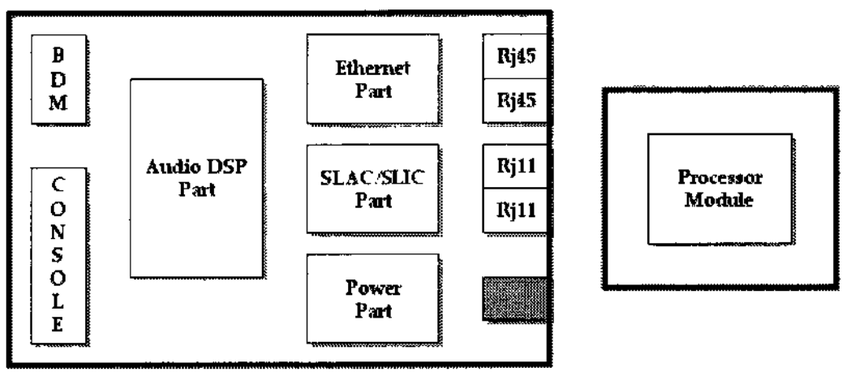


Fig. 1 Hardware design concept block diagram.

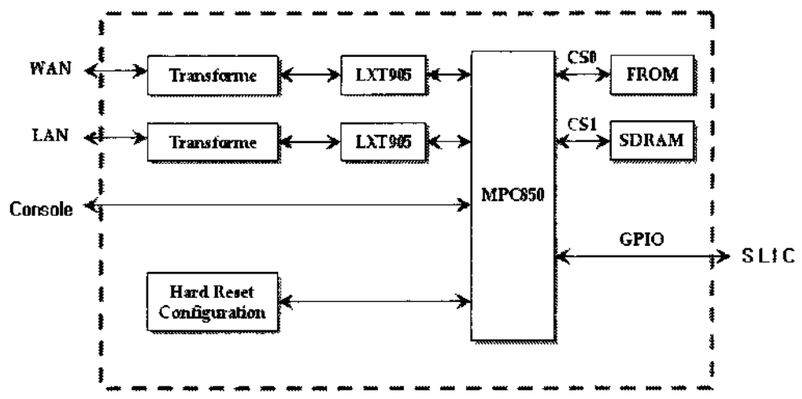


Fig. 2 Detailed diagram of processor moudle.

And configuration diagram of Audio DSP part used for Audio packet processor control for main-board was designed as shown Figure 3. Audio packet processor used AC4830x-C developed by AudioCodes company. This processor is used by directly connecting outside with SRAM (CY7C1021V3-12Z) memory with 128Kbytes capacity and also uses external clock with 16.384Mhz.

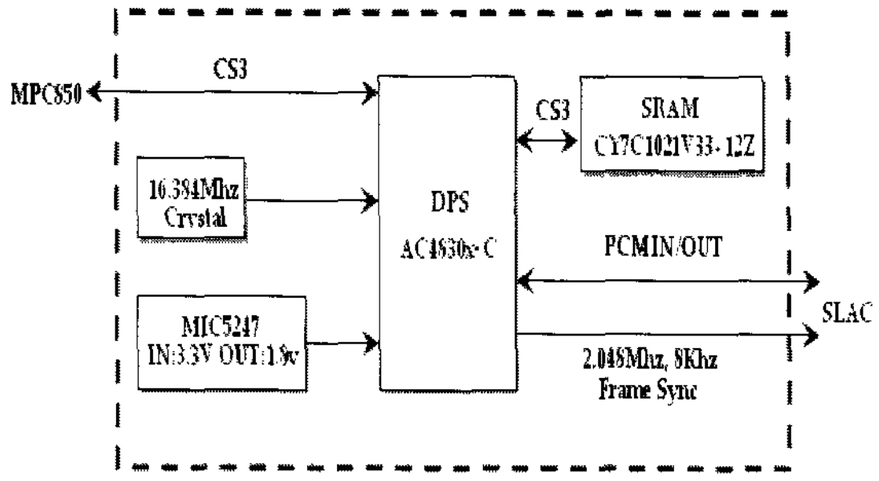


Fig. 3 Detailed diagram of Audio moudle.

In order for Audio to convert from digital to analog, and vice versa, SLAC/RSLIC part was designed by using SLAC(model MC14LC5480) made by Motorola and RSLIC(model HC55185) developed by Intel(see Figure 4). SLAC gets the input of Audio analog from RSLIC, converts into digital and transmits to Audio packet processor(AC4830x-C), and converts Audio digital signal output from Audio packet processor and transmits it to RSLIC. Figure 5 shows an actual figure of VoIP terminal hardware designed as two layers of structure.

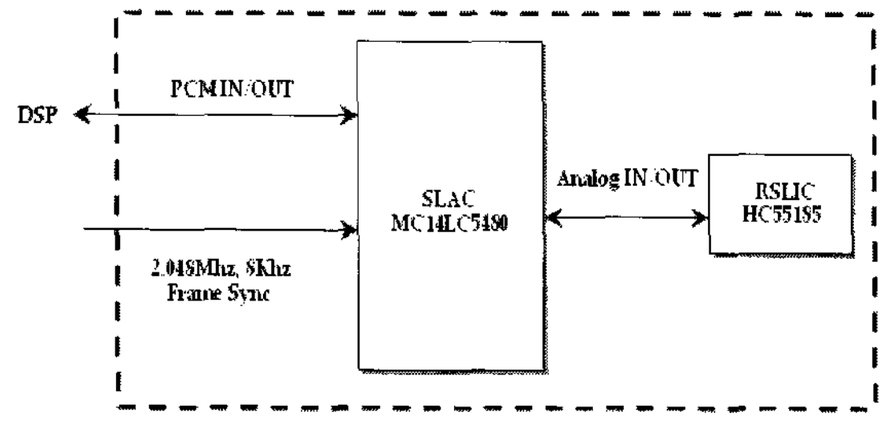


Fig. 4 Detailed diagram of SLAC/RSLIC part.

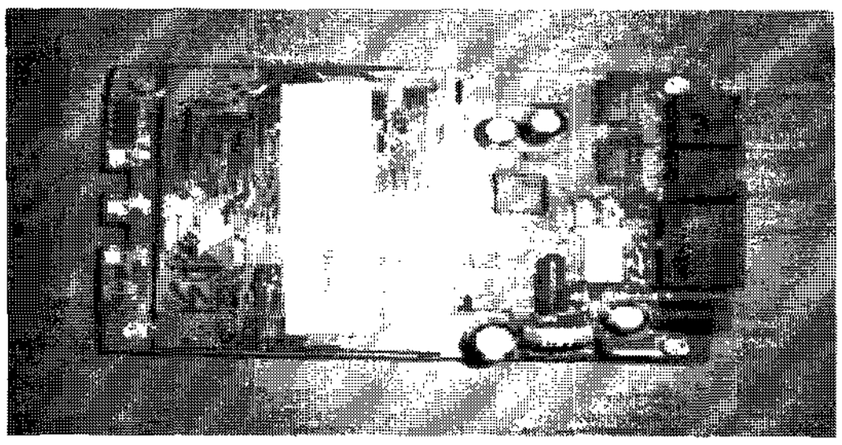


Fig. 5 Figure of VoIP terminal hardware applying VPN.

III. Configuration of VoIP terminal protocol stack applying VPN

This study is based on PPTP (Point-to-Point Tunneling Protocol), one of protocols providing Virtual Private Network in order to prevent VoIP wiretapping and applied SIP (Session Initiation Protocol) stack providing CoIP function. PPTP is in charge of function producing a tunnel between PPTP server and client and PPP is used for information negotiation between server and client. Hence, each protocol function used in this study shall be examined.

A. PPP(Point-to-Point Protocol)

PPP is a protocol to be able to transmit Multi-protocol datagram on PPP link and divided into Encapsulation, LCP(Link Control Protocol) in charge of connection and control of PPP link and NCP(Network Control Protocol) in charge of negotiating Network layer.

PPP Encapsulation has a frame structure as in Figure 6 in order to carry various protocols to PPP Frame. As shown in Figure 6, it comprises protocol field, information field and padding field. Protocol field is for distinguishing the information data, allocated one to two octet and indicates protocol used for information field. And the information field is a protocol data corresponding to protocol field and its maximum sized field is called MRU (Maximum Receive Unit) allocating 1500 octets for its initial value. This value can be changed through LCP(Link Control Protocol). Padding method used for padding field is determined by each protocol.

Fig. 6 Structure of PPP frame

LCP is a protocol in charge of function for Establish, Authentication, Terminate of PPP Link and Figure 7 is a transition diagram that can be come out by LCP operation. As shown in Figure 7, Dead is a mode before and after the connection and if Physical layer is on ready state, it comes to the next step.

The stage of Establish set up the Link of both ends and those are established by exchanging Configuration packet.

The protocol in the Authentication mode can be determined or omitted depending on the value of Configuration Option decided in this stage. Authentication stage is a procedure performed in order for Client to be authenticated from PPP server before exchanging Protocol packet of network layer.

Authentication protocol to be used herein is prearranged through an exchange of LCP packet at the Authentication stage and if authentication failed, it comes to Terminate stage. At the Network stage, network layer protocol to be supported through an exchange of NCP packet is determined and it shall be put in a state possible for normal network communication by getting Establish information of the relevant protocol [3,4,6].

Terminate stage is a process performed in case of failure at the Authentication stage or of selecting Terminate at NCP and PPP Link connection is terminated by exchanging Terminate packets. NCP is a protocol corresponding to the state of network as in Figure 7, which is used for establishing Network Layer Protocol. As this study uses IP protocol, the information established in IP layer is obtained from server by using IPCP(IP Control Protocol) and used for set up. The obtained information includes its IP address, network mask, basic gateway address, etc. on the whole. When IPCP process of NCP is normally finished, Protocol field value as in Figure 6 is determined as 0x0021.

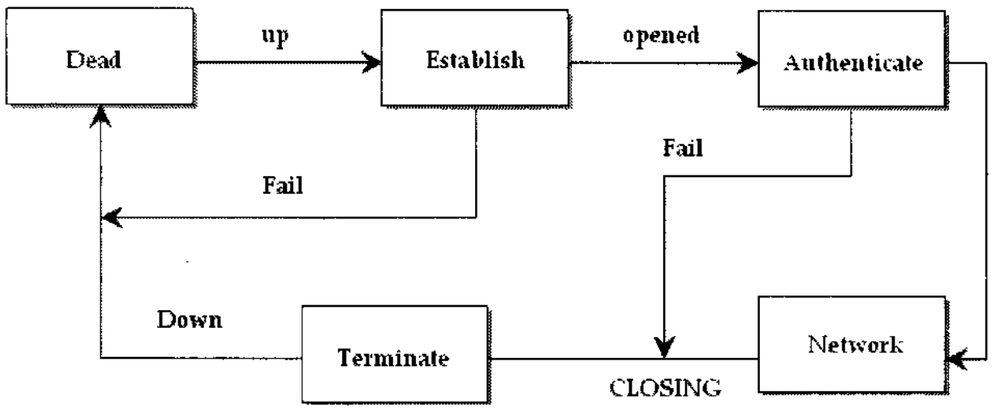


Fig. 7 Transition diagram of LCD mode

B. PPTP(Point to-Point Tunneling Protocol)

PPTP is one of VPN(Virtual Private Network) methods transmitted on internet by encapsulating PPP frame into datagram. This protocol uses TCP data which is called control connection message in charge of function for generation, management and termination of PPTP tunnel.

PPTP can be divided into Control connection part between PNS (PPTP Network Server) and PAC(PPTP Access Concentrator) and Tunneling between PNS and PAC. Control connection massage to be sent for connection of PPTP control between PAC and PNC before tunneling first performs a function of generation, management and release of tunnel and is carried out on TCP session. At this time, destination port uses 1723. And Control connection can start from either PNS or PAS. And tunneling, when a user at End link is going to transmit PPP frame to PNS, shows as same effect as using the exclusive line in a section of internet between PAC and PNS. As shown in Figure 8, PPP frame becomes encapsulation to enhanced GRE header and again is transmitted through ethernet in a section of PAC-PNS by attaching IP header. Figure 9 shows a process of generating PPTP frame depending on patterns of linking to PPTP server inside PPTP client.

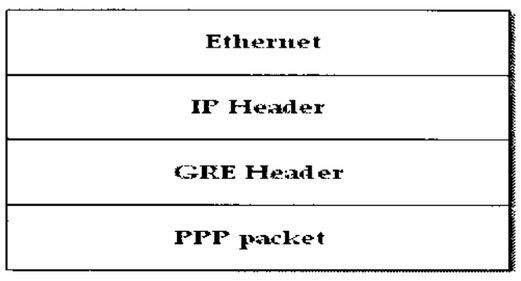


Fig. 8 Structure of PPTP frame

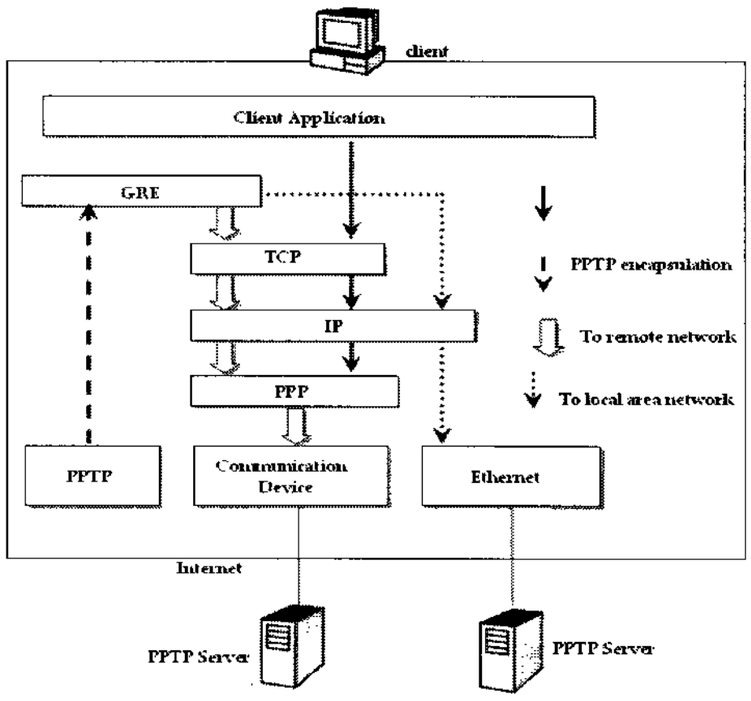


Fig. 9 Process of generating PPTP frame

C. SIP(Session Initiation Protocol) Stack

Like H.323, SIP is a protocol used for establish, modification and termination of media session at VoIP. For complete function of VoIP, however, SIP protocol cannot be used independently but can perform complete function only when it is combined with other protocols. Protocol stack required most basically and most used is shown as in Figure 10. As shown in the figure, SIP protocol stack can be largely classified into four kinds of functions and each function is as follows.

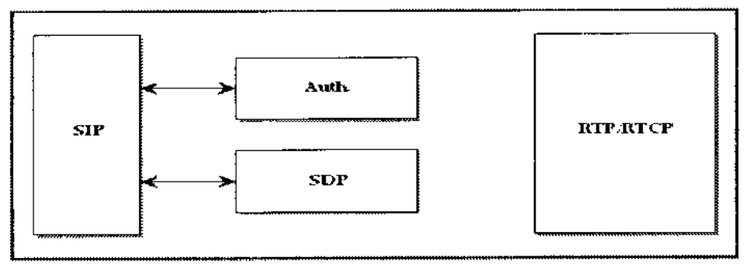


Fig. 10 Structure of SIP stack

First, SIP(Session Initiation Protocol) is a protocol to generate multi-media session, modify and terminate multi-media session, and SDP(Session Description Protocol) is a multi-media session is a protocol to describe multi-media session and is included in and transmitted to body part of SIP message. When using authentication part in SIP, Authentication protocol can be used. When generating media session by using these two protocols, from this time, a real-time data in voice can be exchanged through a different data link from SIP message link depending on media format decided by SDP and what is used at this time is RTP(Real-Time Protocol). RTP is transmitted mostly through UDP because it is a protocol carrying real-time data [2,3,7].

IV. Call test of VoIP applying PPTP

In this study, Internet phone call test was performed as in the Figure 11 by making VoIP service environment. As shown in Figure11, PPTP Client (PAC) function was implemented at each VoIP terminal and SIP protocol which is one of VoIP protocols was also implemented. In order to provide VoIP service by using SIP protocol, Proxy Server(including Registrar function) is required basically and this server is connected with Personal area Network behind PPTP Server(PNS).

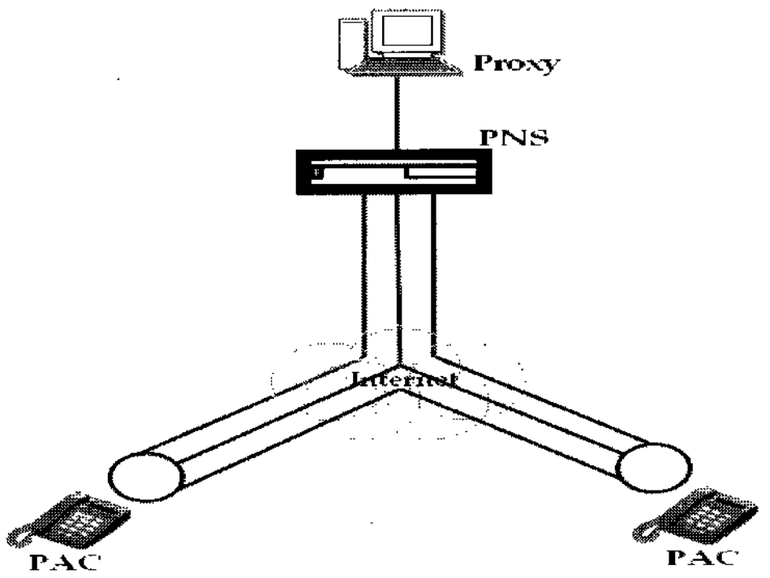


Fig. 11 Configuration of service environment for internet phone using VPN

When operating system first, each PAC(PPTP Network Server) generates PNS(PPTP Network Server) and a single Control Connection. Control Connection is a process of establishing procedure in order to control PPTP connection before PPTP tunneling. The process for generating Control Connection is as in Figure 12, and as shown in the figure, for generating Control Connection, establishing for Call outward is requested after Control Connection from PAC to PNS is requested first and response is received from PNS. After receiving the response about Call Set from PNS, Set-Link-Info message is used lastly to set up the information of Link connected each other with PAC and PNS, and then setting of Control Connection is finished.

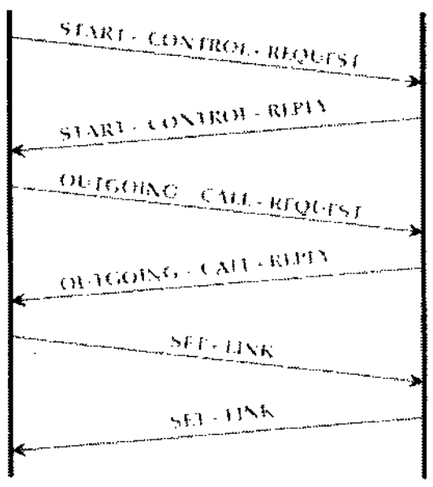


Fig. 12 Procedure of generating PPTP Control Connection

After finishing setup for Control Connection, Link Configuration is negotiated by using PPP(Point-to-Point Protocol) between PAC and PNS as in Figure 13 and which protocol is supported is decided.

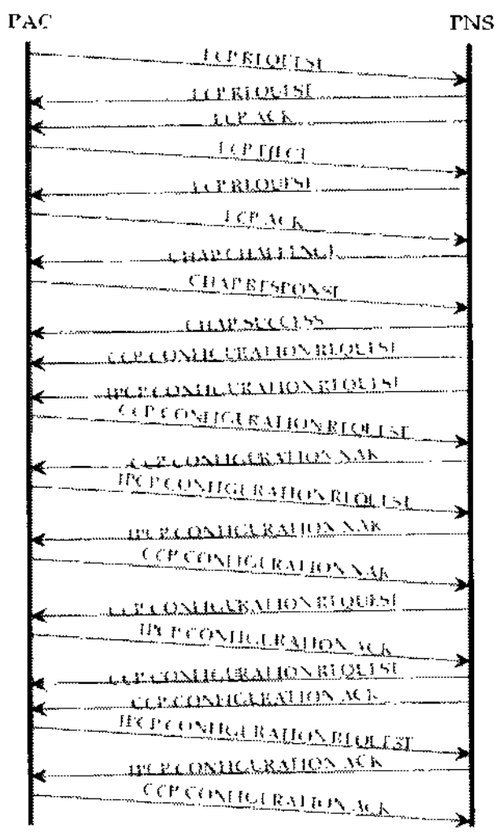


Fig. 13 Operation process of PPP module

First, PPP Link is established by using LCP and it is decided whether authentication protocol will be sued or not. If used, it is decided which algorithm will be used and also whether compressed algorithm will be used or not. The protocol to be applied next is decided with options which were determined through LCP process. As this study decided to use authentication protocol and CHAP(Challenge Handshake Authentication Protocol), authentication is requested by sending CHAP challenge message from PNS to PAC. And then in PAC, CHAP response is generated and replied by combining data obtained from PNS with its own user- id and password. Then if received data is correct, PNS responds by CHAP success message and the authentication process is finished. And because it decided to use compressed algorithm in the process of LCP, it comes to decide which protocol will be used for compressed algorithm for next procedure. At the same time, Network layer protocol to be supported is determined. This study decided to use MPPC as compressed algorithm as well as Stateless Mode and 128bit encryption.

When selecting Stateless Mode, it can be used in a separate way differently from the previous packet, by establishing so as for the value of Coherency Count of MPPE(Microsoft Point-To-Point Encryption) packet format to vary in every packet. IP(Internet Protocol) was to be used for Network layer and information related to network comes to be obtained from PNS by using IPCP(Internet Protocol Control Protocol). PAC network layer is established by obtaining information such as private ip address and private network of PAC, private gateway ip address, etc. When finished all the above procedures, the initial preparatory stage is finished and all the devices shown in Figure 11 is connected to one VPN. In this way, Proxy Server can be approached at each PAC. As Private IP of Proxy Server was already established at each PAC, its private ip with previously allocated VoIP phone number is registered to Proxy Server after connecting through private network. When finishing registration process, phone call is available according to SIP protocol procedure if phone call is made to the number wanted. When VoIP terminals connected to private network make phone call one another, voice data are transmitted/received by RTP protocol. After caller PAC is transmitted to PNS through PPTP tunneling, this voice data obtains private ip corresponding to actual destination in PNS and again PNS is transmitted to called PAC through PPTP tunnelling, and vice versa by the same procedures. The protocol stack of each nodes process that the actual voice data is transmitted inside VoIP implemented for preventing wiretapping in this study is shown as the following Figure 14. If a voice is received from telephone device connected to Caller terminal as shown in Figure 14, digital voice data is obtained through Audio DSP. It is transmitted down to UDP layer by attaching RTP header to the digital voice data. In UDP layer, what is added UDP header is transmitted to private Private IP layer. It is added IP header by using private network ip and transmitted to MPPE(encryption) layer. In this encryption layer, IP packet which came down fro privet IP layer is encrypted and then added in front of MPPE header. And it is sent down to PPP layer. in PPP layer, PPP header is added and sent down to GRE layer. In GRE layer, it is encapsulated to GRE header and sent to public IP layer. In Public IP layer, IP header is added by public IP used commonly is real Internet. Final IP packet is sent to the physical layer of ethernet and ethernet frame

comes to be transmitted by Internet network. And ethernet frame sent from caller terminal is received in PNS and the final destination is found out in private IP layer by processing it in reverse direction of caller terminal (ethernet → public IP → GRE → PPP → MPPE → private IP). in order to transmit it by called terminal depending on final destination, ethernet frame is produced through private IP → MPPE → PPP → GRE → public IP → ethernet. The generated ethernet frame is transmitted through Internet by called terminal. And the called terminal processes ethernet frame received from PNS by each layer in the reverse direction of caller terminal and obtains voice data which finally came to itself. As IP packet format encapsulated to in ethernet frame to be transmitted/received by outside Internet network through protocol stack as in Figure 14 is configurated as in Figure 15, it cannot be analyzed even if IP packet is snatched in Internet network because really important data was encrypted.

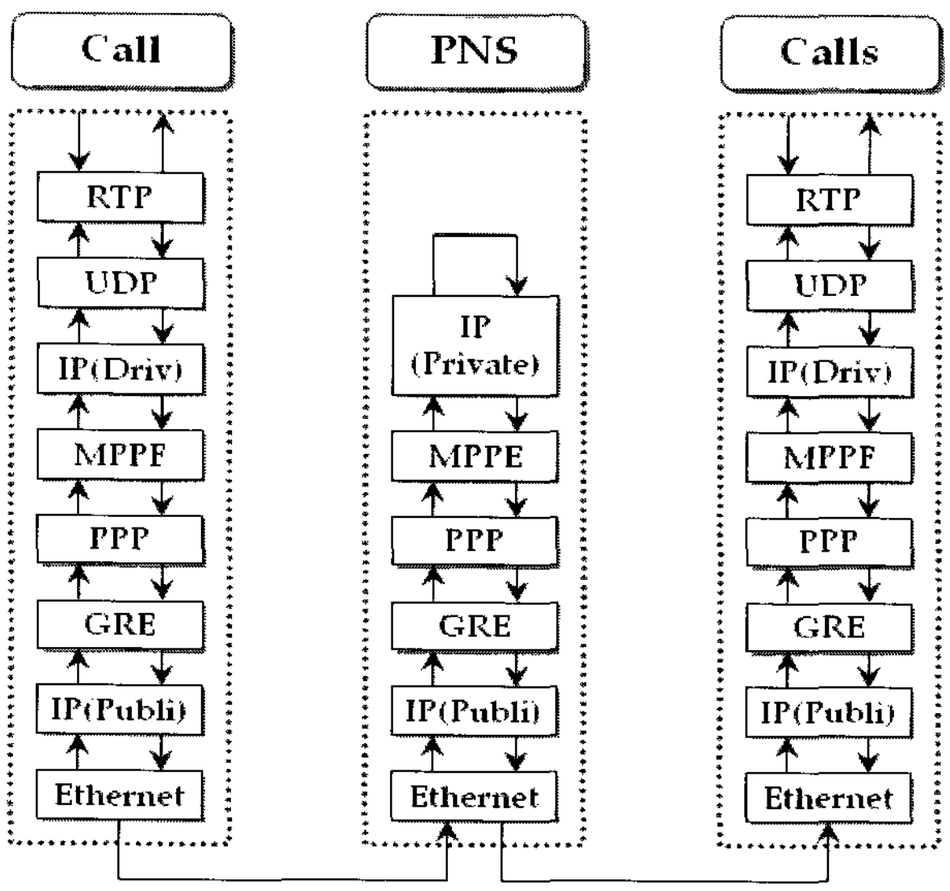


Fig. 14 Protocol stack for transmitting voice data

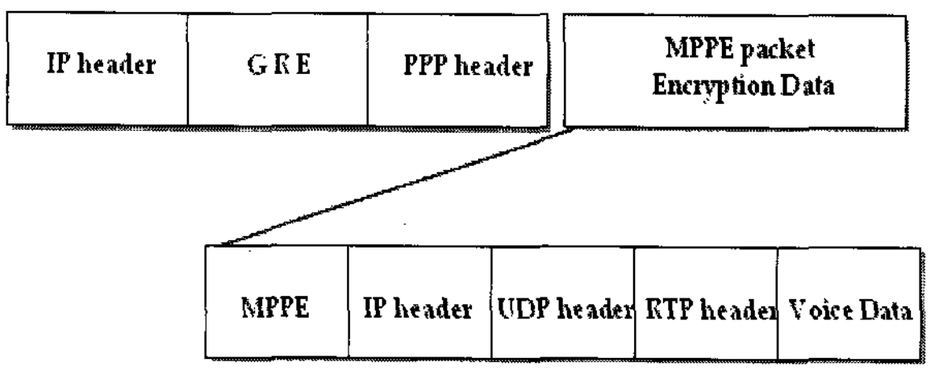


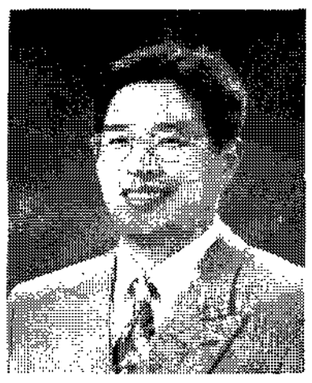
Fig. 15 IP packet format with voice data finally encrypted

IV. CONCLUSIONS

Call length was set up to 10 seconds in order to measure the performance of internet phone call for preventing wiretapping in PPTP and SIP protocol implemented in this study. As shown in [Figure 17], if it does not take 10 seconds in the total call length to send a tone and confirm its call between A and B, this operation can be performed once again in A or B so that Call length can be longer with about 15 seconds. Then, the completion rate of call was 100% receiving its conformance after operating for 24 hours. Thus, VPN(Virtual Private Network) technology was integrated with internet phone call to establish the prevention of wiretapping as the wiretapping can be recognized as the weakest point in the internet phone. However, PPTP protocol used in this study cannot encrypt the Control Connection message and does not have authentication function, hence, complete security cannot be established yet as the Control Connection message can be taken and analyzed in the middle of call. Therefore, Control Connection message should be encrypted in order to make complete security of encryption and it would be better to use IP sec among VPN functions which have the authentication function.

REFERENCES

[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



Kyung Sung
Received a B.S. degree in computer engineering from Mokwon University 1988, and M.S. degree in computer engineering Kyunghee University 1993 and Ph.D. degree in computer engineering from Hannam University 2003. In 2004, he joined the faculty of Mokwon University where he is currently a professor in Department of Computer Education. His research interests Information Security, Neural Network, Web Programming. He is a member of KIMICS, KSII, KMMS and KIAS.