H.323 트래픽 분석 시스템의 개발

이 선 헌[†] · 정 광 수[††]

요 약

최근 다양한 네트워크 환경이 고속으로 발전하면서 화상회의나 VoIP와 같은 고품질의 서비스들이 빠르게 보편화 되어 가고 있다. 오디오, 비디오와 같은 멀티미디어 화상회의 데이터를 인터넷을 통해 전송하기 위한 국제표준인, H.323은 가장 많이 개발되어 상용화된 프로토콜로 다양한 환경을 지원하면서도 성능이 뛰어난 것으로 인식되고 있다. 이러한 환경에서 사용자에게 제공하는 H.323 기반 서비스에 문제가 생기게 될 경우, H.323을 구성하는 프로토콜들의 문제인지, 네트워크 자체의 문제인지를 제대로 분석하는 것이 매우 중요한 기술적 이슈로 대두되고 있다. 이러한 정확한 원인 분석은 H.323 기반의 서비스를 제공하는 네트워크 운영자뿐만 아니라 종단간의 사용자에게도 매우 중요한 서비스 품질의 판단 기준이 되며, 향후 H.323 기반 서비스의 유지 보수에도 많은 도움이 될 것으로 기대할 수 있다. 본 논문은 다양한 네트워크 환경에서의 H.323 기반의 영상 서비스를 가정할 때, H.323 프로토콜의 주요 하위 표준들인 H.245, H.225.0, RTP, RTCP등의 프로토콜을 정확히 분석할 수 있는 통합 분석 시스템인 H.323 Sniffer 개발을 목적으로 한다. 간단한 기능 실험과 성능 분석을 통해 본 논문에서 제안하고, 구현한 분석 시스템이 실제 네트워크 환경에서 서비스되는 H.323 기반 서비스의 상태를 성공적으로 분석하고 이를 통해 발생가능한 문제점의 원인을 판단할 수 있음을 검증하였다.

키워드 : H.323, 멀티미디어 화상회의, VoIP, 프로토콜 분석

Implementation of Analysis System for H.323 Traffic

Sunhun Lee[†] · Kwangsue Chung[††]

ABSTRACT

Recently, multimedia communication services, such as video conferencing and voice over IP, have been rapidly spread. H.323 is an international standard that specifies the components, protocols and procedures that provide multimedia communication services of real-time audio, video, and data communications over packet networks, including IP based networks. H.323 is applied to many commercial services because it supports various network environments and has a good performance. But communication services based on H.323 may have some problem because of current network trouble or mis-implementation of H.323. The understanding of this problem is a critical issue because it improves the quality of service and is easy to service maintenance. In this paper, we implement the analysis system for H.323 protocol which includes H.245, H.225.0, RTP, RTCP, and so on. This system is able to capture, parse, and present the H.323 protocol in real-time. Through the operation test and performance evaluation, we prove that our system is a useful to analyze and understand the problems for communication services based on H.323.

Key Words : H.323, Video Conference, VoIP, Protocol Analyzer

1. 서 론

유.무선 네트워킹 기술의 발전에 따라 전 세계의 통일된 데이터망인 인터넷과의 연계가 가속화 되면서, 오디오, 비디오를 포함한 멀티미디어 데이터를 동일한 IP(Internet Protocol)망을 통해 전송하는 화상회의나 VoIP(Voice over Internet Protocol)와 같은 서비스들에 대한 수요가 빠르게 증가하고 있다. 최선형의 서비스를 제공하는 인터넷 환경에서, 시간에 대한 제약이 존재하는 오디오나 비디오와 같은 멀티미디어 데이터 서비스를 제공하면서 발생하는 통화 품질 감쇄나 지연 등의 QoS(Quality of Service) 문제가 있음에도 불구하고 비용절감, 기존 인프라의 효율적 운용, 관리의 편리성, 데이터 통합에 의한 다양한 응용서비스 제공 등의 효과를 거둘 수 있기 때문에 많은 기업 등에서 큰 관심을 보이고 있는 것이 현실이다[1~3].

화상회의나 VoIP 등의 멀티미디어 통신 서비스를 제공하기 위한 표준화 작업은 ITU-T(International Telecommunications Union-Telecommunication)와 IETF(Internet Engineering Task Force) 기구들을 중심으로 수행되고 있으며, 가장 대표적인 것으로 ITU-T SG16의 H.323과 IETF의 SIP

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성.
지원사업의 연구결과로 수행되었음.
† 준 회 원 : 광운대학교 대학원 전자통신공학과 박사과정
†† 정 회 원 : 광운대학교 전자공학부 교수
논문접수 : 2006년 3월 16일, 심사완료 : 2006년 6월 19일

(Session Initiation Protocol), MGCP(Media Gateway Control Protocol) 등이 있다[3~6]. 이와 같은 통합된 형태의 표준들은 제어 및 시그널링 프로토콜, 게이트웨이 제어 프로토콜, 미디어 전달 프로토콜, 미디어 코딩 기법 등의 기능으로 크게 구분할 수 있다. 특히, H.323은 멀티미디어 데이터를 인터넷 환경과 같은 패킷 교환 방식의 네트워크를 통해 전송하기위한 표준으로, 고품질 비디오를 위한 근거리 네트워킹 기술, 그리고 느린 전송 속도를 가지는 회선을 통해 저주파수 대역의 비디오를 전송하기 위한 표준안 등이 포함되어 있다. 이러한 H.323 표준은 다양한 플랫폼 및 네트워크 환경에 적용이 유연하여 현재 많은 상용화 제품을 이루고 있으며 성공한 국제 표준으로 인식되고 있다[4]. 이미 많은 화상회의 솔루션이나 VoIP 응용들, 그리고 마이크로소프트의 넷미팅(Netmeeting)과 같은 잘 알려진 응용 프로그램들을 통해 일반 사용자들은 H.323 기반의 서비스를 연결된 네트워크 환경에서 쉽게 사용하고 있다. 또한 최근에는 무선 네트워크 환경에서도 H.323 기술을 적용하여 멀티미디어 서비스들의 제공을 시도하고 있다[7].

그러나 아쉽게도 현재의 인터넷 환경에서 H.323 기반의 서비스를 운영하다 보면 의도하지 않은 여러 문제점들을 쉽게 경험할 수 있다. 특히 H.323과 같이, 전체 H.323 표준을 구성하는 여러 복잡하고 다양한 세부 프로토콜들에서 문제가 생길 경우, 그 원인을 발견하고 진단하기가 결코 쉽지 않다. 또한, H.323을 서비스하는 네트워크 관리자와 단말기 간에 문제가 발생할 경우, 빠르고 간단하게 문제를 파악하고 해결할 수 있는 시스템의 필요성은 절실하다[6]. 이러한 상황에서, 간단하게 네트워크 관점에서 H.323 프로토콜의 분석을 통해 문제의 원인을 진단하고 이를 통해 서비스를 개선할 수 있는 기능은 매우 매력적이라 할 수 있다. 본 논문에서는 이러한 H.323 기반의 서비스 제공에서 발생할 수 있는 문제점을 빠르게 분석하고 해결하기 위한, H.323 프로토콜 분석 시스템의 설계 및 구현을 목적으로 한다.

본 논문의 2장에서는 H.323 표준의 세부 내용에 관해 기술하였고, 3장과 4장에서는 본 논문에서 설계하고 구현한 H.323 프로토콜 분석 시스템인 H.323 Sniffer에 대한 설계와 구현 내용, 그리고 간단한 실험을 통한 시스템 성능에 대해 기술하였다. 마지막으로 5장에서는 결론 및 향후 연구 과제에 대해 기술하였다.

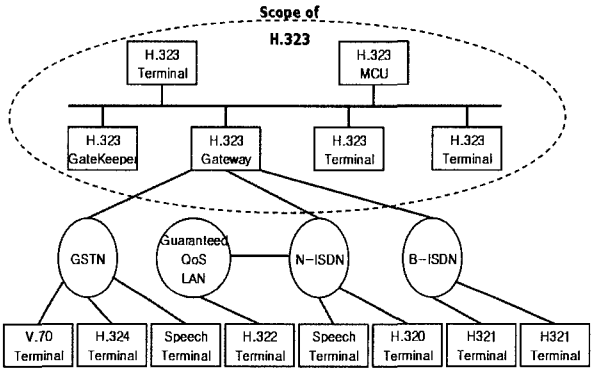
2. H.323 표준

인터넷상에서의 멀티미디어 통신을 위한 세부 프로토콜 표준과 절차를 정의하는 권고로서 ITU-T의 H.323과 IETF의 SIP, 그리고 MGCP가 있다. 본 장에서는 ITU-T의 표준인 H.323 표준에 대한 간단한 설명과, H.323 표준을 구성하는 세부 프로토콜 및 구성 요소, 통신 절차에 대해서 기술하도록 한다.

2.1 H.323의 개요

H.323은 인터넷을 포함한 패킷 기반망에서 오디오, 비디오, 데이터를 지원하는 멀티미디어 통신시스템 표준이다. 현재 VoIP 제품의 많은 수가 H.323에 기반을 두고 구현되어 있는데, 이것은 H.323이 기존 망의 하부구조를 변경하지 않고 멀티미디어 서비스를 사용할 수 있도록 해주고, (그림 2.1)에 나타난 바와 같이 LAN과 GSTN(General Switched Telephone Network), N-ISDN(Narrowband Integrated Services Digital Network), B-ISDN(Broadband ISDN) 등 다른 망과의 상호운용성에 대한 표준도 제공해주기 때문이다. (그림 2.1)과 같이, H.323 표준은 H.323의 구성요소중의 하나인, 게이트웨이를 통해 이종의 네트워크와 상호 운용성을 제공한다.

H.323 표준은 패킷망에서 화상회의나 VoIP와 같은 멀티미디어 서비스를 제공하기 위한 시그널링 및 제어 프로토콜의 사용에 관한 통합 기술이다. H.323 시스템은 터미널, 게이트웨이, 게이트키퍼, 다중점 제어기(MC: Multipoint Controller), 다중점 제어 장치(MCU: Multipoint Control Unit)로 구성되고, 각 구성요소들은 데이터 교환을 통해 통신한다. H.323의 제어 메시지는 신뢰성을 갖춘 TCP (Transmission Control Protocol)를 사용하는 반면, 오디오, 비디오와 같은 데이터는 UDP(User Datagram Protocol)를 사용한다[9].



(그림 2.1) H.323의 상호 운용성

2.1.1 H.323 터미널

H.323 터미널은 실시간 양방향 통신을 지원하는 종단장치로서, 모든 터미널은 필수적으로 시스템 제어 장치, H.225.0 계층, 네트워크 인터페이스, 그리고 오디오 코덱 장치를 포함하며, 비디오와 데이터 서비스는 선택적으로 지원한다. H.323 터미널의 시스템 제어 장치는 채널의 사용과 협상에 대한 능력을 제공하는 H.245와 세션의 설정과 패킷화 과정에 적용되는 표준인 H.225.0을 포함하는 것으로 H.323 터미널의 올바른 동작을 위한 시그널링을 제공한다. 이 장치는 호 제어, 능력 협상, 명령 및 지시 시그널링, 그리고 논리 채널을 개방하고 그 채널의 내용을 설명하는데 이용되는 메시지들을 제공한다. H.225.0은 호 시그널링 및 설정을 위한 Q.931, 터미널과 게이트키퍼 간의 통신 프로토콜인 RAS(Registration, Admission, and Status), 오디오와 비디오 패킷의 전송을 담당하는 RTP/RTCP(Realtime Transport Protocol/Control Protocol) 등을 반드시 지원하여야 한다.

2.1.2 게이트웨이와 게이트키퍼

게이트웨이는 H.245와 Q.931 프로토콜을 사용하여 H.323 터미널이나 LAN 상의 다른 게이트웨이와 WAN 상의 다른 터미널간에 실시간 양방향 통신을 제공하는 종단장치이다. 즉, PSTN(Public Switched Telephone Network), LAN 등의 이종의 네트워크에 연결된 터미널과의 링크를 설정하고자 할 때 필요한 것으로, 다른 네트워크와 연결하지 않을 경우에는 불필요하다. 따라서 게이트웨이는 H.323 종단장치와 다른 형태의 터미널 사이의 변환기능을 수행하며 호 시그널링, 전송 형식, 그리고 통신 절차상의 차이점을 보상해 주어야 한다.

게이트키퍼는 H.323 터미널들에 대한 호 제어 서비스를 제공하는 H.323 실체로 논리적으로는 터미널들과 분리되지만 물리적으로는 터미널, 게이트웨이, MC, MCU 장치에 위치한다. 게이트웨이를 포함하는 LAN은 주소 변경을 위해서 게이트키퍼도 포함해야 한다. 게이트웨이와 마찬가지로 게이트키퍼도 H.323에서 필수적으로 있어야 하는 요소가 아닌, 선택사항이다. 게이트키퍼가 제공해야 하는 서비스는 네 가지 주요 기능 서비스와 네 가지 부가 기능으로 구분할 수 있다. 주요 기능으로는 주소 변환(Address Translation), 수락 제어(Admission Control), 대역폭 제어(Bandwidth Control), 영역 관리(Zone Management)등이 있으며 부가 기능으로는 호 제어 시그널링(Call Control Signaling), 호 권한부여(Call Authorization), 대역폭 관리(Bandwidth Management), 호 관리(Call Management)등이 있다.

2.1.3 MC와 MCU

다중점 제어기, MC는 다중점 회의에서 3개 이상의 터미널들 간의 회의를 지원하기 위한 제어 기능들을 제공한다. MC는 다중점 회의에 참석한 각 터미널들과 능력 협상을 수행하고 변경하는 기능을 포함한다. MC는 터미널, 게이트웨이, 게이트키퍼, 그리고 MCU에 위치할 수 있으며 MCU는 항상 MC를 포함한다.

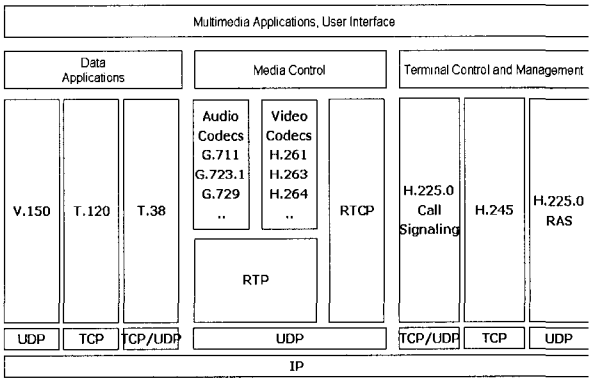
MCU는 세 개 이상의 종단장치 간의 다중점 회의를 제공해주는 장치로서, MC와 다중점 처리기(MP: Multipoint Processors)로 구성된다. MC가 터미널의 공통적인 능력을 정의하기 위해 모든 터미널 간에 수행되는 H.245 협상을 관리하며 멀티캐스트되는 회의 자원을 제어한다면, MP는 다중점 회의에 포함된 터미널들로부터 오디오, 비디오 및 데이터 스트림을 수신하여 각 매체 스트림에 적용된 알고리즘이나 형식의 변경과 같은 스위칭이나 믹싱의 처리과정을 거쳐 해당 터미널에 다시 돌려주는 기능을 담당한다.

2.2 H.323의 프로토콜 구성

본 절에서는 H.323 표준의 핵심 프로토콜들의 주요 구성 및 동작 방법에 대해 기술하고자 한다. H.323은 H.245 세션 제어, H.225.0/Q.931 호 시그널링, H.225.0 RAS 등 세 가지 제어 프로토콜과 RTP/RTCP와 같은 전송 프로토콜을 사용한다. 전체적인 H.323 프로토콜의 구성은 (그림 2.2)와 같다.

2.2.1 H.225.0 호 시그널링

호 시그널링은 종단장치들 간에 호를 설정하고 해제하는데 필요한 기본적인 요구사항이다. H.225.0은 호 시그널링을 위해 기존 ISDN의 호 시그널링인, Q.931 시그널링 프로토콜을 확장한다. 게이트키퍼가 없는 경우, H.225.0 호 시그널링 메시지는 종단장치들 간에 직접 전달된다. 하지만, 게이트키퍼가 있을 경우에는 게이트키퍼를 통해 경유된다. 호 시그널링은 신뢰성을 갖춘 TCP를 사용하여 전달된다[10~11].



(그림 2.2) H.323 프로토콜의 전체 구성

H.225.0의 호 시그널링은 <표 2.1>과 같이 5개의 메시지로 크게 분류되며, 각 메시지에 따라, 필수적인 그리고 선택적인 메시지 속성을 갖는다. 필수적인 메시지만을 사용할 경우, 기본적으로 H.225.0의 호 시그널링은 Call Setup - Call Proceeding - Alerting - Facility - Connect - 데이터 전송 - Call Clearing 의 과정을 거친다.

<표 2.1> H.225.0 호 시그널링 메시지

메시지 분류	속 성	메시지 종류
Call Establishment Msg.	필수 (Mandatory)	Alerting, Connect, Setup
	선택 (Optional)	Call Proceeding, Progress, Setup ACK
Call Clearing Msg.	필수	Release Complete
Call Information Phase Msg.	선택	Resume(ACK), Suspend(ACK), User Information ...
Miscellaneous Msg.	필수	Status
	선택	Information, Notify, Status Inquiry
Q.932 Msg.	필수	Facility
	선택	Hold(ACK, Reject), Retrieve(ACK, Reject)

2.2.2 H.225.0 RAS

H.225.0 RAS 메시지는 종단장치와 게이트키퍼 간의 통신에 사용된다. H.225.0 RAS는 게이트키퍼가 있을 경우에만 필요하다. TCP를 통해 전달되는 H.225.0 호 시그널링과는 달리 H.225.0 RAS는 UDP를 통해 전달되며 다음을 포함한다[10].

a) Gatekeeper discovery : 터미널이 자신의 게이트키퍼를 찾기 위해 사용된다. 게이트키퍼의 전달 주소를 찾아야 하는 종단장치가 GRQ(Gatekeeper Request) 메시지를 멀티캐스트하면, 하나 이상의 게이트키퍼가 게이트키퍼 전달 주소를 포함하는 GCF(Gatekeeper Confirmation) 메시지로 응답함으로써 게이트키퍼를 찾는다.

b) Endpoint registration : 게이트키퍼를 성공적으로 찾았을 경우, 모든 종단장치는 게이트키퍼에 등록하여야 한다. 이것은 게이트키퍼가 자신의 영역에서 호를 라우팅하기 위해 모든 종단장치의 앨리어스(alias) 주소와 전달 주소를 알아야 하기 때문에 필요하다.

c) Endpoint location : 게이트키퍼가 종단장치에 특정한 전달 주소를 배정하기 위해 사용한다. 이것은 게이트키퍼가 앨리어스-전달 주소 데이터베이스를 변경할 때 필요하다.

d) Admissions, Bandwidth Change, Status, Disengage : 게이트키퍼가 수락 제어, 상태 정의, 대역폭 관리 등의 제어 관리기능을 수행할 때 사용된다.

2.2.3 H.245 미디어 제어

H.245는 종단장치들 간에 제어 정보를 교환하기 위한 프로토콜로, RTP/RTCP에 의해 전달되는 모든 미디어 채널의 협상과 설정에 사용된다. H.245 제어는 모든 종단장치에 필수적으로 구현되어야 하며, 다음과 같은 미디어 제어 기능을 제공한다[12].

a) Terminal Capability Exchange : H.323은 서로 다른 송신능력과 수신능력을 종단장치에 제공한다. 각 종단장치는 메시지 내에 미디어 형태, 코덱, 비트율 등과 같은 수신능력과 송신능력을 기록하여 다른 종단장치로 전달한다.

b) Master/Slave Determinations : 한 회의의 MC가 될 수 있는 두 터미널간 또는 양방향 채널의 개방을 시도하는 두 터미널간에 발생하는 충돌을 해소하기 위해 주종 결정 절차가 이용된다. 이 절차에서 두 터미널은 무작위수를 교환하여 주종을 결정한다.

c) Logical Channel Signaling : H.323 오디오와 비디오 논리채널은 단방향 링크이며, 데이터 채널은 양방향 링크이다. 오디오, 비디오 및 데이터 통신을 위해서는 분리된 채널이 필요한데, H.245 메시지는 이러한 채널의 개폐를 제어한다. H.245 제어 메시지는 항상 개방되어 있는 논리채널 0을 사용한다.

d) Conference Control : 통신에 문제가 발생했을 경우 종단장치에 이를 알려주는 기능을 제공한다.

2.2.4 RTP/RTCP

RTP는 오디오 및 비디오 데이터를 실시간으로 송수신하기 위해 H.323에서 사용되는 전송 프로토콜이다. RTP는 UDP를 사용하기 때문에 실시간 서비스를 위한 자원예약이나 QoS를 보장해주지 않는다. 따라서 오버헤드가 적은 대신 데이터를 재전송하지는 않는다. RTP 헤더에 있는 타임스탬프와 시퀀스 번호를 사용하여 오디오와 비디오 데이터 스트림 간의 동기를 맞추고 실시간성을 유지하고 패킷의 손실을 감지한다. RTCP는 데이터 패킷과 동일한 분배 메커니즘을 사용하여 제어 패킷을 주기적으로 전송함으로써 RTP를 이용하는 영상회의에서 QoS를 지원하기 위한 제어 프로토콜이다[13].

2.3 기존의 H.323 프로토콜 분석 시스템

기존의 상용 H.323 프로토콜 분석 시스템은 일반적인 네트워크 프로토콜 분석 시스템과 비슷하게 단순히 해당 프로토콜의 트래픽을 캡쳐하여 프로토콜이 존재하는지의 여부를 알려주게 된다. 이러한 이유는 기존의 상용 분석 시스템의 경우, H.323 프로토콜에 특화되지 않은 범용적인 목적의 네트워크 프로토콜 분석 시스템으로 특히, H.245와 H.225.0은 패킷 포맷이 복잡하여 프로토콜 분석이 쉽지 않기 때문에 정확하고 유용한 분석 정보를 제공하지 못한다.

사용자에게 제공되는 H.323 기반의 서비스의 성능이나 문제가 발생했을 경우, 그 원인을 분석하기 위해서는 단순히 H.323 프로토콜에 해당하는 트래픽이 발생했는지의 여부만으로는 부족하다. 이것은 단순히 네트워크에서 발생 가능한 패킷 손실 여부만을 확인시켜주며 호 시그널링과 같은 제어 메시지 교환이 많은 H.323 기반 서비스의 경우, 제어 메시지의 정확한 전달이나 순서에 대한 분석 정보를 자세하게 제공할 필요가 있다.

다음의 3장에서는 기존의 상용 H.323 프로토콜 분석 시스템의 한계를 극복하여 보다 정확하고 자세한 H.323 프로토콜들의 정보를 제공하는 분석 시스템에 대해 상세히 소개하고자 한다.

3. H.323 프로토콜 분석 시스템 설계 및 구현

본 논문에서 제안한 H.323 프로토콜 분석 시스템은 2장에서 언급한 H.323의 제어 및 시그널링 프로토콜과 전송 프로토콜을 분석하기 위한 시스템이다. 본 장에서는 제안하는 분석 시스템의 구조 및 구현 내용에 대해 기술하고자 한다.

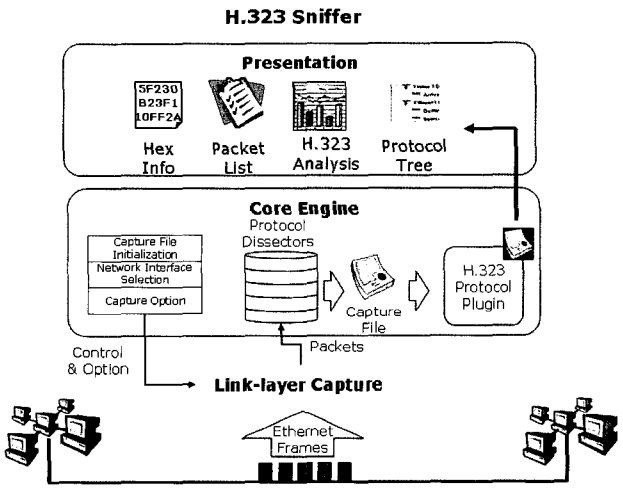
3.1 시스템 설계

본 논문에서 구현한 H.323 프로토콜 분석 시스템을 H.323 Sniffer라 부른다. 기본적으로 H.323 프로토콜뿐만 아니라 범용적인 목적의 다양한 네트워크 프로토콜들을 쉽게 분석하기 위한 구조로 되어있다. 이러한 특징을 위해서 분석하고자하는 프로토콜을 핵심 엔진에 쉽게 추가 할 수 있는 플러그인(plug-in) 구조를 지원하도록 설계하였다.

(그림 3.1)은 구현한 H.323 Sniffer의 전체적인 구조를 보여준다. H.323 Sniffer는 구조적으로 크게 데이터 링크 레이어 정보를 수집하기 위한 Link Layer Capture 모듈과 이러한 프레임 정보를 기반으로 목적이 되는 프로토콜, 즉 H.323

프로토콜을 분석하는 Core Engine, 그리고 이러한 분석 정보를 기반으로 H.323 프로토콜 정보를 분석하고 다양한 방법으로 표현해주는 Presentation 모듈로 구분할 수 있다.

네트워크 인터페이스로부터 패킷 단위로 캡쳐된 데이터들은 Core Engine에서 해당 플러그인에 의해 파싱(parsing)된다. H.323 Sniffer에서는 기본 플러그인으로 H.323 파서(parser)로 설정되어 있으며, 이는 본 논문에서 제안하는 시스템에서 추가적으로 구현한 H.323 플러그인으로, H.323 프로토콜을 기존 분석 시스템과 다르게 보다 정확하고 상세하게 분석한 정보를 사용자에게 제공하게 된다. 해당 파서를 통해 해석된 데이터의 각 필드 및 정보들은 Presentation 모듈에서 바이너리 형태, 계층적 형태, 통계적인 형태로 사용자에게 제공된다. 따라서 H.323 분석 시스템의 Core Engine에서의 H.323 플러그인과 Presentation 모듈의 H.323 프로토콜 분석은 본 논문에서 강조하는 주요 핵심 기능들을 포함하게 된다.



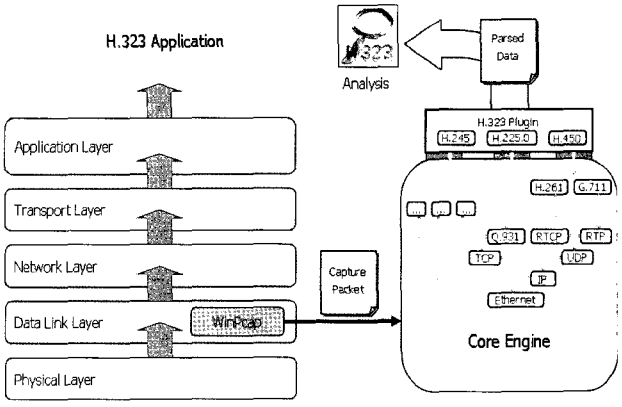
(그림 3.1) H.323 Sniffer의 전체구조

3.2 시스템 구현

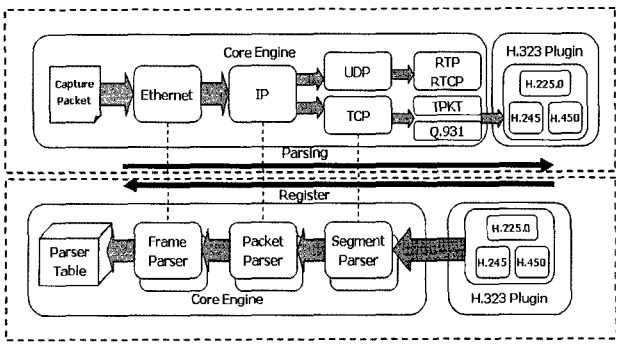
H.323 Sniffer는 종단간의 H.323 기반의 응용프로그램이 동작할 때 동일한 링크에서 같이 동작 시키면서 H.323 데이터를 시스템의 전체 트래픽으로부터 선택적으로 추출하는 방식을 사용한다. 구현한 시스템은 윈도우 운영체제 환경에서 링크 레이어의 패킷을 실시간으로 캡쳐할 수 있는 오픈 소스 라이브러리인 WinPcap을 사용하여 링크 레이어로부터 패킷 단위의 데이터를 추출할 수 있다[14]. 현재 개발된 시스템은 이더넷 프레임에서 정보를 추출하고 있지만 다른 링크 레이어의 정보도 추출이 가능한 구조를 가지고 있다. WinPcap을 이용하여 링크 레이어로부터 추출된 패킷 단위 원시(raw) 데이터는 Core Engine으로 전달된다.

Core Engine에서는 패킷을 파싱하여 정보를 (그림 3.2)와 같이 트리(tree) 구조로 배치하게 된다. Core Engine의 여러 프로토콜의 파서와 플러그인으로 제공되는 H.323 프로토콜 패킷의 파서는 유사한 방식으로 패킷에 대한 파싱을 수행하며 각각의 프로토콜의 파싱 과정이 계층적으로 이루어지게 된다. 즉, WinPcap 라이브러리로부터 캡쳐된 Low-dump 패킷들은 가장 먼저 데이터링크 레벨의 프레임 파서에 의해 파싱이 수행되고, 이후 부분은 상위 레벨의 파서인 IP 패킷 파서에 넘겨지고 순차적으로 상위 레벨의 파서에게 전달이 되는 형태를 가지게 된다. 즉, 하위 레벨의 파서가 파싱을 마친 후, 현재 레벨의 파싱 과정에서 익히게 된 타입이나 포트정보를 바탕으로 H.323 Sniffer 프로그램이 처음 실행될 때 등록된 다양한 프로토콜 파서 테이블 리스트에서 검색을 통해 적절한 파서를 선택한 후, 선택된 상위 레벨의 파서에게 다음의 데이터를 넘겨주게 된다. 각각의 트리 구조는 네트워크 각 계층의 데이터를 파싱하며 최종적으로 H.323을 구성하는 세부 프로토콜을 위한 전용 H.323 분석 모듈이 플러그인 형태로 연결되어 동작하게 된다. H.323 플러그인 모듈을 통해 분석된 패킷은 GUI(Graphic User Interface)를 가진 H.323 Sniffer 프로그램에서 해당 패킷의 정보를 다양한 형태로 사용자에게 제공한다.

(그림 3.3)은 H.323 Sniffer의 Core Engine과 플러그인의 상호 관계를 보다 자세히 나타낸 것이다. 플러그인은 Core Engine에게 자신이 분석하고자 하는 세부 프로토콜에 대한 정보를 미리 등록한다. Core Engine에서 링크 레이어의 프레임에 대한 기본적인 프로토콜 파싱을 수행할 때 플러그인에 의하여 등록된 프로토콜이 발견되면 이것을 해당 플러그인 모듈에게 알리게 된다. H.323에서는 TCP기반의 Q.931



(그림 3.2) Core Engine의 기능



(그림 3.3) Core Engine과 Plugin의 관계

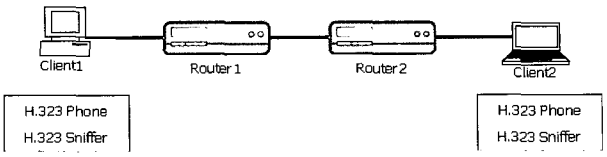
패킷이 Core Engine에서 검출되게 되면 H.323 플러그인에게 알려주어, 이와 관련된 패킷들을 모두 분석하여 H.323 패킷의 정보들을 구성하게 된다. 선택된 H.323 파서를 통해 캡쳐된 패킷의 파싱이 완료된 후, 파싱된 데이터는 H.323 Sniffer 프로그램에 리턴되며 사용자 인터페이스를 통해 다양한 형태로 표현된다.

4. H.323 Sniffer의 동작 및 성능 평가

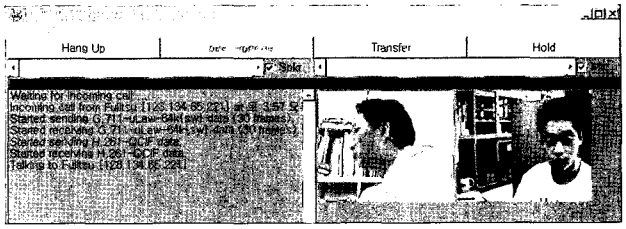
본 장에서는 윈도우 운영체제 환경에서 동작할 수 있도록 구현된, H.323 Sniffer의 동작 및 성능 평가를 위해 실험 환경을 구성하고, H.323 기반의 응용프로그램을 사용하여 구현한 H.323 Sniffer의 다양한 기능을 실험하였다. 또한, 구현한 시스템의 성능 평가와 함께 기존의 상용 프로토콜 분석 도구인 WildPacket사의 EtherPeek와의 분석 능력에 대한 성능 비교를 수행하였다[15].

4.1 실험 환경

(그림 4.1)은 구현한 H.323 Sniffer의 성능 검증을 위한 실험 환경을 보여준다. 유선 네트워크 환경뿐만 아니라 무선 네트워크 환경에서의 실험을 위해 터미널 1은 유선 네트워크에 위치하며, 터미널 2는 무선 네트워크에 위치하도록 설정하였다. 각각의 클라이언트에는 H.323 트래픽을 발생시키기 위한 H.323 Phone 프로그램과 본 논문을 통해 구현한, H.323 Sniffer 프로그램을 실행시키면서 전체적인 동작과 성능에 대한 평가 실험을 수행하였다.



(그림 4.1) 실험 환경

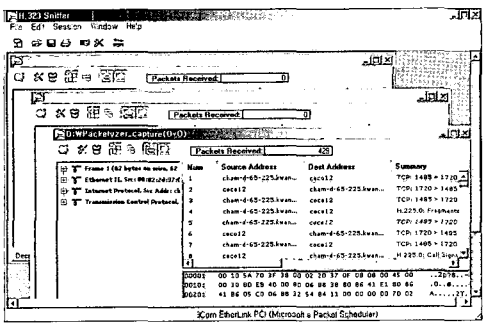


(그림 4.2) H.323 Phone 응용 프로그램

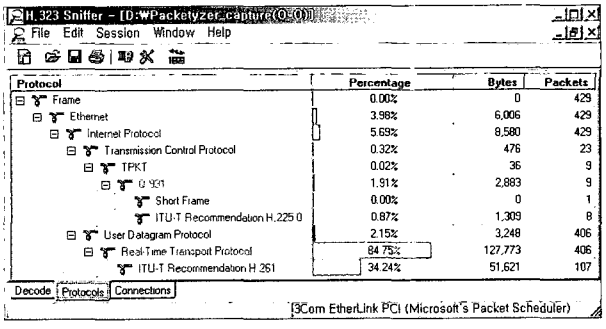
(그림 4.2)는 H.323 Sniffer의 성능 평가 실험에 사용하기 위해 추가적으로 구현한 H.323 Phone 프로그램으로 H.323 프로토콜 스펙을 구현하고 있는 오픈 소스 프로젝트인 OpenPhone 프로그램을 수정하여 구현하였다[16]. 또한, 기존 H.323 호환 화상회의 프로그램과의 호환성 검증을 위해 마이크로 소프트의 윈도우 운영체제에서 기본으로 제공하는 H.323 호환 화상회의 프로그램인 넷미팅(NetMeeting)을 사용하여 실험을 수행하였다[17].

4.2 H.323 Sniffer의 기본 동작

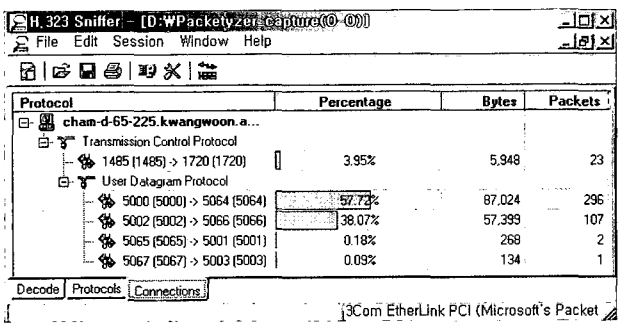
(그림 4.3)은 구현한 H.323 Sniffer의 기본적인 동작 화면이다. (그림 4.3 (a))와 같이 H.323 Sniffer는 기본적으로 여러 상용 프로토콜 분석 도구와 마찬가지로, 멀티 세션을 지



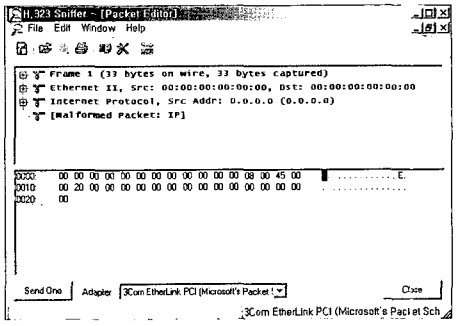
(a) 멀티 세션 기능



(b) 프로토콜 통계

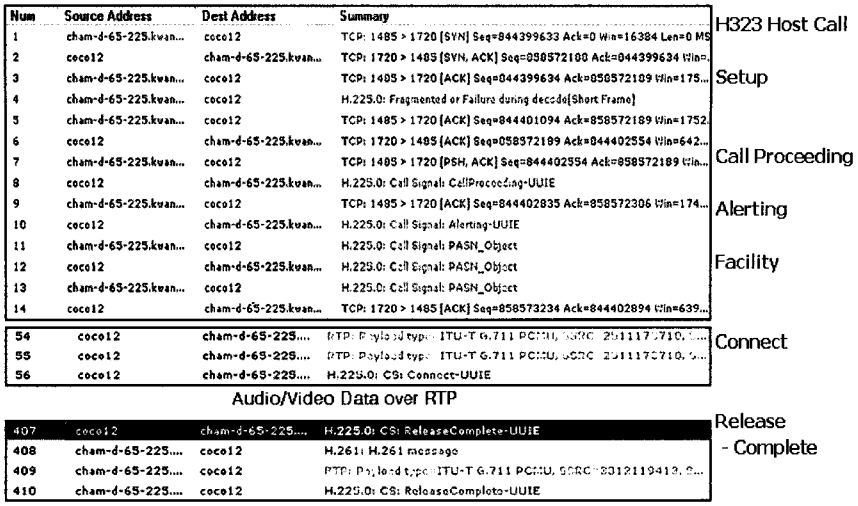


(c) 커넥션 통계



(d) 패킷 편집

(그림 4.3) H.323 Sniffer의 기능



(그림 4.4) H.225.0 메시지의 분석

원하도록 구현되었다. 멀티 세션 기능의 지원으로 세션은 전체 H.323 분석 시스템의 공통된 설정을 적용하지만 각 세션마다 독립적으로 다른 캡쳐 설정값을 적용할 수 있도록 되어 있다. 각각의 세션마다 실시간으로 캡쳐된 패킷의 리스트를 보여주는 부분과 계층적인 트리 형식으로 보여주는 부분, 그리고 패킷의 정보를 16진수 형식으로 보여주는 부분으로 구성된 윈도우를 통해 해당 세션의 캡쳐된 프로토콜을 분석할 수 있는 기능을 제공한다. (그림 4.3 (b))에서 보여지는 프로토콜 통계에서는 해당 세션에서 캡쳐된 각 프로토콜들의 통계를 퍼센티지, 바이트 수, 패킷 수 단위로 보여주며 (그림 4.3 (c))에서의 커넥션 통계에서는 현재 분석 시스템과 커넥션을 맺고 있는 각 시스템과의, 전송 계층에서의 포트(port) 번호에 따른 커넥션의 통계를 마찬가지 퍼센티지, 바이트 수, 패킷 수 단위로 일목요연하게 제공하게 된다. (그림 4.3 (d))는 패킷 편집 기능을 보여주는 것으로 특정 패킷 정보를 임의로 편집하고 이를 다시 H.323 서버나 클라이언트로 전송하여 잘못된 패킷을 디버깅하는 기능을 제공하게 되며, H.323 기반 서비스에서 서버나 클라이언트 시스템에서 생성하는 H.323 트래픽의 문제발생 여부를 효과적으로 검증할 수 있는 기능을 제공하게 된다.

2장에서 설명했듯이, H.323 기반의 화상회의나 VoIP 응용에서 호 시그널링은 종단장치들 간에 호를 설정하고 해제하는데 필요한 기본적인 요구사항으로서 이에 대한 분석은 전체 시스템의 성능에 큰 영향을 미친다. 그러므로 이러한 호 시그널링에 대한 분석 능력은 H.323 프로토콜 분석 시스템에서 가장 중요한 기능이라 할 수 있다.

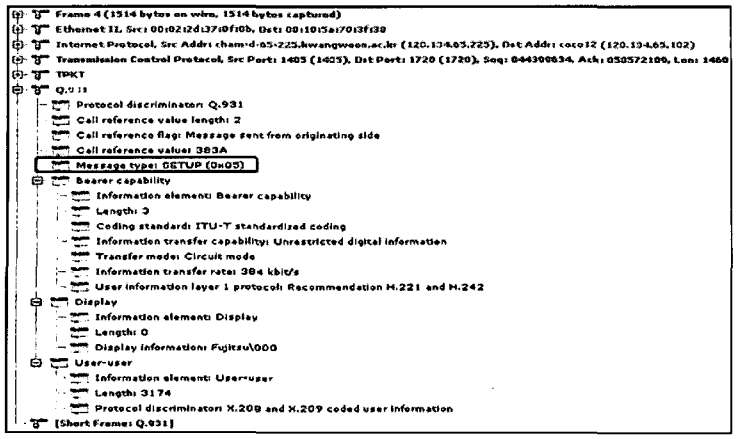
H.323 프로토콜 분석 시스템의 성능을 결정하는 H.225.0의 호 시그널링에 대한 분석 능력을 검증하기 위해서 H.323 기반의 서비스 트래픽을 발생시킨 상태에서, H.323 Sniffer를 통해 호 시그널링 메시지를 캡쳐한 화면을 (그림 4.4)에 나타내었다. 실험을 위해 추가적으로 구현한 H.323 Phone 프로그램은 넷미팅과 같은 일반프로그램과 달리, 2장에서 설명한 H.225.0의 의무적인 호 시그널링 메시지를 모두 발생시킨다. (그림 4.4)에서 확인할 수 있듯이, 구현한 H.323 Sniffer는 H.225.0 호 시그널링 메시지를 모두 성공적으로 캡쳐 및 분석하여 연결된 세션의 각각의 상태를 단계별로 분석하며, 단계에 따라 필수적인 메시지인 Call Setup, Call Proceeding, Alerting, Facility, Connect, Call Clearing을 정확하게 분석하는 것을 확인할 수 있다. 또한, TCP를 통해 전달되는 H.225.0 호 시그널링 메시지의 경우, 논문에서 제안하고 구현한, H.323 프로토콜 플러그인 엔진에 의해 전송계층 이상에서 더 자세한 분석 정보를 제공하는 것을 확인할 수 있다.

(그림 4.5)는 (그림 4.4)의 결과를 보다 자세하게 분석한 결과로서, (a)에서는 H.225.0에서 사용하는 Q.931 패킷의 Setup 메시지의 구조를 각각의 필드 해석을 통해 기존의 상용 H.323 분석 시스템에 비교하여 보다 상세한 정보를 보여주고 있다.

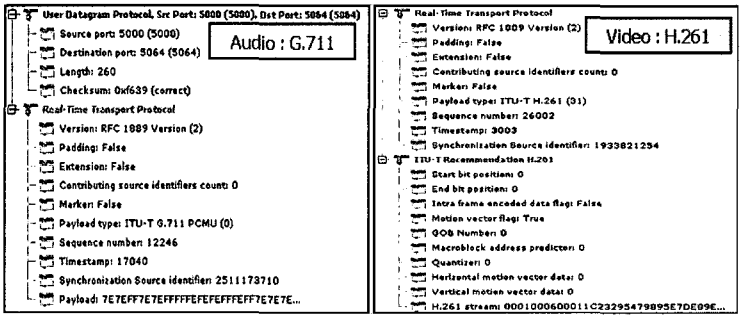
(그림 4.5 (b))와 (c)에서는 RTP를 기반으로 전송되고 있는 실제 멀티미디어 트래픽인 G.711로 인코딩된 오디오 데이터와 H.261로 인코딩된 비디오 데이터에 대한 분석 결과를 나타내고 있으며, 이는 H.323 플러그인이 아닌 추가적으로 구현한 RTP 플러그인에 의한 분석 결과를 보여주고 있다.

4.3 H.323 Sniffer의 성능 비교

본 절에서는 구현한 H.323 Sniffer의 H.323 트래픽에 대한 부가적인 분석 기능에 대해 기술한다. 기존의 상용 트래픽 분석 도구들은 패킷을 캡쳐하고 해당 패킷에 대한 분석 기능과 통계를 보여주는 기본적인 기능만을 제공하고 있다. 본 논문에서 구현한 H.323 Sniffer는 앞선 4장에서의 실험결과에서 확인했듯이, 추가적인 H.323 플러그인 구현을 통해 H.323 시스템에서 가장 중요한 기능인 호 시그널링 과정에 대한 분석을 보다 정확하고 상세히 제공할 수 있었다. 하지만, 단순한 캡쳐 및 분석 기능은 자세한 정보를 제공해 준다는 장점은 제공하지만 여전히 문제점 분석에 대한 편리성을 제공해 주지 못하는 한계를 갖는다. 따라서 이와같은 호



(a) Q.931 Setup 메시지 파싱 결과



(b) G.711 오디오 패킷 (c) H.261 비디오 패킷

(그림 4.5) H.323 Sniffer의 패킷 분석

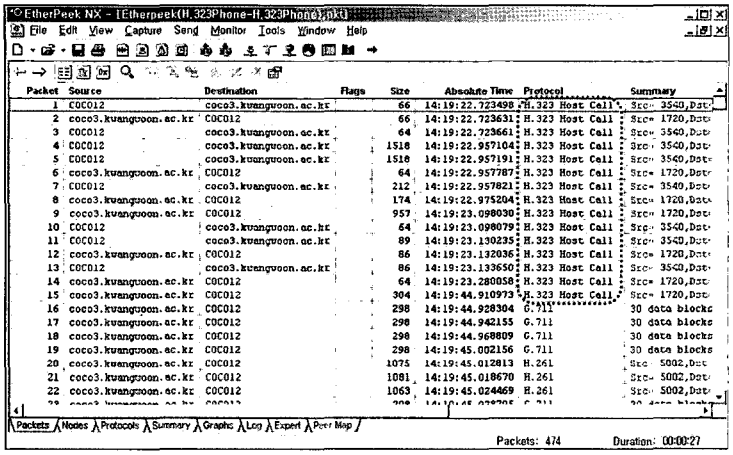
시그널링과 같은 제어메시지의 흐름을 직관적으로 보일 수 있도록 호 시그널링 과정에 대한 흐름도를 추가로 구현하였다. 호 시그널링 과정에 대한 흐름도에서는 H.323 트래픽 세션에 있어서, RTP를 통한 오디오, 비디오 데이터의 흐름이나 부수적인 TCP 패킷의 흐름을 제외한, 커넥션을 맺기까지의 H.225.0 메시지나 H.245 메시지의 흐름이 어떻게 이루어지는지를 순서적으로 보여주게 되며 부수적으로 해당 메시지가 전달되는 시간 정보나 크기, 캡쳐 패킷 리스트에서의 해당 번호에 관한 정보를 제공한다.

(그림 4.6)은 기존의 상용 트래픽 분석 도구인 Wild-Packets의 EtherPeek와 논문에서 구현한 H.323 Sniffer의 성능 비교 결과를 나타낸 것이다. (a)의 결과에서 확인할 수 있듯이, 기존의 트래픽 분석 도구는 H.323 트래픽을 캡쳐하여 단순히 호 시그널링 메시지 여부만을 알려주게 된다. 반면, 논문에서 구현한 H.323 Sniffer는 (그림 4.4)와 (그림 4.5)의 결과에서 확인했듯이 호 시그널링 메시지에 대한 정확한 정보를 제공하며 (그림 4.6)의 (b)와 같이 부가적으로 H.323 트래픽에 대한 호 시그널링 과정의 흐름도를 제공한다. 즉, H.323 Sniffer는 실시간으로 네트워크에서 얻은 H.323 세션의 연결 상태 정보를 분석하여 (그림 4.6)의 (b)와 같은 연결 그래프로 나타냄으로써 사용자들에게 보다 쉬운 분석 기능을 제공한다. 이러한 기능을 통해 H.323 서비스에서 발생하는 문제의 원인을 보다 쉽게 찾을 수 있으며, 이것은 네트워크 운영자와 H.323 터미널 개발자에게 큰 도움이 될 것으로 기대할 수 있다.

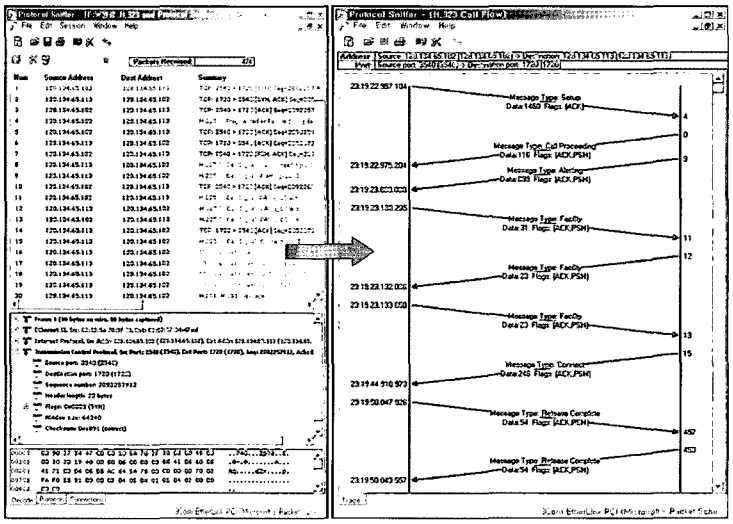
5. 결 론

최근들어 그 수요가 점차 증가하고 있는, 화상회의나 VoIP에 관한 대표적인 국제 표준인 H.323은 다양한 네트워크 환경을 지원한다는 장점과 함께, 기능적으로도 우수한 성능을 가지므로 국내외에서 많이 연구되고 개발되고 있는 통신 프로토콜이다. 하지만 실제로 이러한 H.323을 기반으로 응용프로그램을 구현하여 서비스를 제공하는 시점에서 문제가 생길 경우, 복잡한 H.323 표준의 세부 프로토콜이나 호 처리 및 제어 과정으로 인해 그 원인을 조기에 발견하고 진단하기가 쉽지 않다. 더군다나 H.323 응용 서비스를 제공하는 네트워크나 단말기간에서 복잡한 문제가 발생할 경우, 보다 빠르고 간단하게 문제를 진단할 수 있는 시스템의 필요성은 절실했다.

본 논문은 다양한 네트워크 환경에서 현재 서비스되고 있는 H.323 트래픽의 분석이 가능한 시스템 개발을 목적으로 한다. 논문을 통해 구현한 H.323 트래픽 분석 시스템은 네트워크 관점에서, 서비스되는 H.323 트래픽을 종단간에서 실시간으로 모니터링하며, 이를 기반으로 H.323 표준의 다양한 프로토콜 및 데이터를 분석하는 기능을 제공한다. 실험을 통해 구현한 H.323 Sniffer가 표준 H.323 트래픽을 성



(a) WildPackets의 EtherPeek



(b) H.323 Sniffer

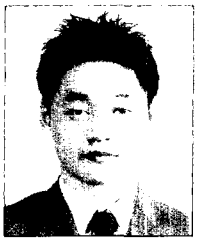
(그림 4.6) H.323 Sniffer의 성능 비교

공적으로 분석할 수 있으며, 기존의 모니터링 도구에서 부족한 기능을 보완하여 보다 빠르고 쉽게 문제점을 파악할 수 있음을 증명하였다.

향후 연구로서, 개발한 H.323 Sniffer에 실제 서비스되는 오디오 및 비디오 데이터의 정성적인 모니터링을 병행하여 사용자에게 제공되는 멀티미디어 서비스의 QoS까지 진단하고 분석할 수 있는 기능을 추가하고자 한다.

참 고 문 헌

[1] 김지영, "VoIP(Voice over Internet Protocol)", 정보통신기술협회, 2000.
[2] 한국정보처리학회, "정보처리학회지", 제8권 제2호, 2001.
[3] 민재홍, 조평동, "VoIP 기술동향", IT Find 기술동향, 2004.
[4] H323 Forum, http://www.h323forum.org/
[5] SIP Forum, http://www.sipforum.org/
[6] N. Greene, M. Ramalho, and B. Rosen, "Media Gateway Control Protocol Architecture and Requirements," IETF RFC 2805, April 2000.
[7] Databeam, "A Primer on the H.323 Series Standard", http://databeam.com/h323/h323.html, May 1998.
[8] Hong Liu, Mouchtaris, "Voice over IP signaling: H.323 and beyond," IEEE Communications Magazine, October, 2000.
[9] ITU-T Recommendation H.323v2, "Packet Based Multimedia Communications System," Geneva, February, 1998.
[10] ITU-T Recommendation H.225.0v2, "Media Stream Packetization and Synchronization on Non-Guaranteed Quality of Service LANs," Geneva, February, 1996.
[11] ITU-T Recommendation Q.931, "ISDN user-network interface layer 3 specification for basic call control," May 1998.
[12] ITU-T Recommendation H.245v2, "Control Protocol for Multimedia Communications," Geneva, February, 1996.
[13] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A transport protocol for real-time applications," IETF, RFC 1889, January, 1996.
[14] WinPcap, http://www.winpcap.org/
[15] WildPackets's EtherPeek, http://www.wildpackets.com/
[16] OpenPhone, http://www.openh323.org/
[17] NetMeeting, http://www.microsoft.com/windows/netmeeting/



이 선 헌

e-mail : sunlee@cclab.kw.ac.kr

2003년 광운대학교 전자공학부(학사)

2005년 광운대학교 대학원 전자통신공학과 (공학석사)

2005년~현재 광운대학교 대학원 전자통신공학과 박사과정

관심분야 : 네트워크 프로토콜, Cross-Layer, 유.무선 비디오 스트리밍

정 광 수

e-mail : kchung@daisy.kw.ac.kr

1981년 한양대학교 전자공학과(학사)

1983년 한국과학기술원 전기 및 전자공학과 (공학석사)

1991년 미국 University of Florida 전기공학과 컴퓨터공학전공(공학박사)

1983년~1993년 한국전자통신연구원 선임연구원

1991년~1992년 한국과학기술원 대우교수

1993년~현재 광운대학교 전자공학부 교수

관심분야 : 인터넷 QoS, 유.무선 비디오 스트리밍, 센서 네트워크