# 공개키기반 사용자인증과 암호화를 적용한 영상회의 시스템 설계 및 구현

정 용 득† · 이 상 훈†† · 전 문 석†††


## 요 약

본 논문에서는 최근 대두되고 있는 화상회의 시스템에 대하여 사용자 인증 및 암호화를 지원하는 공개키 기반 인증서기반의 영상회의 시스템을 설계, 구현하고 이에 대하여 기술한다. 공개키 기반 인증서를 사용함으로써 영상회의 참여자에 대한 인증을 강화하며, 대칭키 시스템을 이용하여 영상회의 정보를 보호함으로써 여러 가지 악의적인 접근을 차단할 수 있다. 본 논문에서는 국내 공인인증 규격에 따르는 인증서를 적용한 트랜스포트 계층 보안 프로토콜을 구현하고, 미디어 암호화를 위하여 대칭키 암호화 알고리즘인 DES, 3DES, AES등을 적용할 수 있도록 영상회의 시스템을 설계 구현하였다. 본 논문은 사용자 인증 및 영상회의에 대한 정보를 보호하기 위하여 대칭키로서 트랜스포트 계층을 보안하는 것과 사용자의 불법 인증을 방지하기 위하여 공개키 기반의 인증 시스템을 두어 사용자의 신원을 확보할 수 있다. 암호화를 위한 세션 키의 분배는 P2P일 경우 IKE 방식의 키 분배 프로토콜을 사용하며, 1 : N 등 다자간 사용자일 경우 공개키 기반의 암호화 키 분배 방식을 따라 보안 프로토콜에 의하여 안전하게 분배된다.


# Design and Implementation of Public key-based Video Conference System for Authentication and Encryption

Yong-Deug Jung† · Sang-Hun Lee†† · Moon-Seog Jun†††


## ABSTRACT

This paper describes the design and implementation of the video conferencing system using public key infrastructure which is used for user authentication and encryption. Public key infrastructure reinforces the authentication process for conference participant, and the symmetric key system blocks malicious access to information and protect conference control information. This paper shows the implementation of the transportation layer secure protocol in conformity with Korea public key authentication algorithm standard and symmetric encryption algorithm (DES, 3DES and AES) for media stream encryption. In this paper, we deal with two ways of protecting information : transportation layer secure protocol secures user authentication process and the conference control information; while public key-based authentication system protects personal information of users when they connect to the network. When distributing the session keys for encryption, Internet Key Exchange is used for P2P communication, and secure protocol is employed for 1 : N multi-user communication in the way of distributing the public key-based encryption key.


**키워드 : 영상회의(Video Conferencing), PKI, Certification, TCP, H.323**

## 1. 서 론

영상회의 표준 규격은 크게 ITU-T(International Telecommunication Union Telecommunication Standardization Sector)와 IETF(Internet Engineering Task Force)를 중심으로 개발되어 왔다. 그 중 H.323[3]은 ITU-T에서 제안된 영상회의 표준 규격으로서 QoS가 보장되지 않는 인터넷 환경에서 운용되는 프로토콜이며, 차세대 이동통신 환경에서도 채택될 예정인 영상회의 프로토콜 중 하나이다. H.323의 내부구성은 호 설정에 관련하는 H.225[5], 각종 제어신호를 주고받는 H.245[7], 비디오 코덱과 오디오 코덱으로 구성되어 있으며, 마이크로소프트사의 NetMeeting을 비롯한 많은 제품들이 H.323 프로토콜을 표준으로 개발되었다.

H.323 영상회의에서 보안 취약점은 구현기술과 적용 환경에 따라서 차이가 있지만 가장 중요한 점을 요약하면 다음과 같다. 첫째, 참여자들에 대한 인증이 필요하다. 일정한 자격을 소유한 사람들만 영상회의에 참여할 수 있는 상업용 시스템에서는 더욱 민감한 문제가 아닐 수 없다. 둘째, 영상회의에 대한 제어 정보와 미디어에 대한 기밀성이 제공되어야 한다. 제어 정보가 노출될 경우에는 영상회의 중에 어떤

※ 본 논문은 숭실대학교 교내지원비에 의한 것임.
† 정 회 원 : 대한무역투자진흥공사 차장
†† 준 회 원 : 숭실대학교 대학원 컴퓨터학부
††† 종신회원 : 숭실대학교 정보과학대학 교수
논문접수 : 2004년 6월 17일, 심사완료 : 2004년 8월 30일

공격에 노출될지 예상할 수 없게 된다. 셋째, 참여자들 사이에 또는 참여자들과 제어 Server 사이에 교환되는 정보에 대한 무결성이 보장되어야 한다. 무결성이 보장되지 않는 경우는 의도적으로 통신 내용이 변조될 수 있을 뿐만 아니라 정상적으로 영상회의를 개최할 수 없도록 하는 서비스 거부 공격도 가능해진다[10, 12, 14].

본 논문에서는 위에 열거한 보안 취약점에 대해 인증 및 기밀성을 제공할 수 있는 방안으로서, H.323 영상회의 시스템에서의 사용자 인증 및 미디어의 암호화/복호화를 구현한다. 영상회의에 대한 암호화는 DES, Triple-DES, AES[2] 등의 블록 암호 알고리즘을 구현하여 보호하였고, 미디어 암호화를 위하여 사용된 비밀키는 공개키 기반 및 Diffie-Hellman[16]을 이용한 TLS을 통해 안전하게 분배한다. 사용자 인증과 미디어 암호화를 위하여 TLS를 적용한 점, 보안성을 향상시키기 위하여 국내 공인인증 규격을 만족하는 공개키 기반 인증서를 적용하고, 블록 암호화 알고리즘의 특성을 분석하여 영상회의에 미치는 영향을 분석하였다.

본 논문의 구성은 2장에서 본 논문의 근간이 되는 영상회의 기술과 보안 기술에 대한 내용을 살펴본다. 3장에서는 본 논문에서 제안하는 영상회의 모델과 각각의 모델에 적용할 보안 프로토콜에 대하여 기술한다. 4장에서는 구현한 결과와 각각의 블록 알고리즘에 대한 성능분석 결과를 기술하고, 5장에서 결론을 맺는다.

## 2. 관련 연구

### 2.1 H.323 영상회의 표준

H.323[3]은 인터넷과 같은 TCP/IP 패킷 네트워크에서 오디오, 비디오, 데이터의 송수신을 지원하는 멀티미디어통신 표준이다. H.323의 장점은 PSTN과 같은 기존 네트워크를 통해 주고 받는 패킷의 형태를 변경하지 않고 멀티미디어 서비스를 사용할 수 있도록 해주고, LAN과 GSTN, N-ISDN, B-ISDN 등 다른 네트워크와의 상호운용성에 대한 표준을 제공해 준다. H.323은 패킷 네트워크에서 실시간 점대점 및 다지점 멀티미디어 통신을 제공하기 위한 구성 요소, 프로토콜 및 절차를 정의한 것으로, 구현을 위해서는 단말, 게이트웨이, 게이트키퍼, MCU(Multipoint Control Unit)의 네 가지 구성요소가 필요하다. 단말은 실시간 양방향 통신을 지원하는 종단 장치이다. 모든 단말은 오디오, 비디오와 데이터 서비스를 지원한다. H.323 영상회의 시스템 단말은 채널의 사용과 협상에 대한 능력을 제공하는 H.245 호 시그널링 및 설정을 위한 Q.931, 게이트키퍼와의 통신 프로토콜인 RAS (Registration/Admission/Status), 오디오와 비디오 패킷의 순서화를 담당하는 RTP/RTCP 등을 반드시 지원하여야 한다[6-8]. 또한 선택적으로 비디오 코덱, T.120 데이터 회의 프로토콜, MCU 능력, 게이트웨이 등을 지원할 수 있다. 게이트웨이는 H.245와 Q.931[7] 프로토콜을 사용하여 H.323 단말이나 LAN 상의 다른 게이트웨이와 WAN 상의 다른 ITU 단말간에 실시간 양방향 통신을 제공하는 종단 장치이다. 즉, PSTN, ISDN 등의 네트워크에 연결된 단말과 링크를 설정하고자 할 때 필요한 것으로, 다른 네트워크와 연결하지 않을 경우에는 불필요하다. 게이트웨이는 H.323 종단장치와 다른 형태의 단말 장치간의 변환기능을 수행하며 오디오와 비디오 코덱간의 변환을 수행한다. 또한 LAN과 SCN(Switched Circuit Network) 간에 호를 설정하고 해제하는 역할을 담당한다. H.323오디오 코덱은 5.3~64kbit/s 범위의 오디오 코덱을 규정하고 있다. 기본적으로 PCM 방식인 G.711을 사용하도록 규정하고 있으나, G.711은 전화네트워크에서 사용하도록 설계된 코덱으로 대역폭이 작은 인터넷에서의 통신에는 이보다 좋은 음질을 제공하는 G.723.1이나 GSM6.10을 제공한다. 비디오 코덱은 H.261/QCIF를 지원한다. H.261은 64kbps 속도로 352×288 픽셀을 초당 30프레임 이하로 전송한다[4].

### 2.2 영상회의 사용자 인증과 암호화

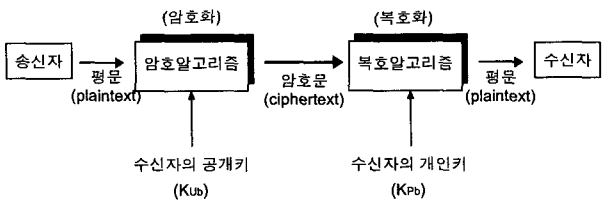
#### 2.2.1 공개키 암호 알고리즘

공개키 암호 알고리즘(Public-Key Crypto Algorithm)은 암호화하거나 복호화하는데 쓰이는 키가 두개가 존재하는 알고리즘이다. 즉, 어느 하나의 키로 암호화한 것은 다른 하나의 키로만 복호화할 수 있다. 이러한 성질로 공개키 암호 알고리즘은 비대칭 암호 알고리즘(Asymmetric Crypto Algorithm)이라고도 한다. 두 개의 키는 수학적 함수를 기반으로 서로 연관이 있는 키 쌍으로 하나의 키는 누구든지 사용할 수 있게 공개하고 다른 하나는 외부에 공개되지 않도록 보관한다. 이때 공개하는 키를 공개키(public key)라고 하며 자신만이 볼 수 있도록 보관하는 키를 개인키(private key)라고 한다[1]. 공개키 암호를 이용해서 송신자와 수신자가 암호 통신을 하기 위해서는 (그림 1)과 같은 과정을 거친다. 먼저 송신자는 수신자 B의 공개키($K_{Ub}$)로 메시지를 암호화하여 암호문을 수신자에게 전송한다.

$$C = EK_{Ub}(M)$$

그러면 수신자 B는 암호문을 자신의 개인키($K_{Pb}$)로 복호화하여 원래의 메시지를 얻는다.

$$M = DK_{Pb}(C)$$




(그림 1) 공개키 암호 시스템

공개키 암호 시스템은 비밀키 암호 시스템에서 제공할 수 없는 디지털 서명 기능을 제공해준다. 디지털 서명은 송신자 A가 평문을 자신의 개인키($K_{Pa}$)로 암호화(서명)한 암호(서명)문을 전송한다.

$$S = EK_{pa}(M)$$

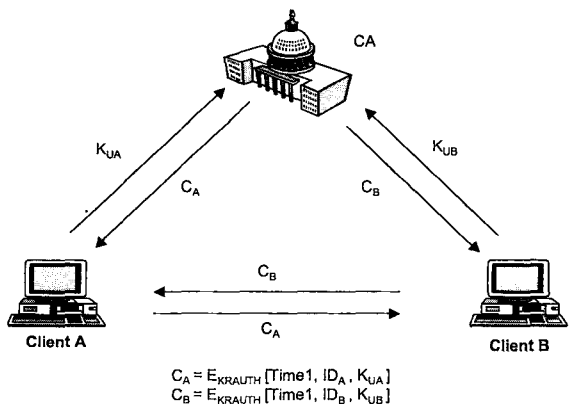
수신자는 전송받은 암호문을 송신자 A의 공개키($K_{Ua}$)로 복호화함으로써 이루어진다.

$$M = EK_{Ua}(S)$$

이때 개인키를 알고 있는 사람은 오직 송신자 A밖에 없기 때문에 A의 공개키로 확인되는 서명을 한 사람이 A라는 것을 확인할 수 있다. 이러한 과정은 디지털 데이터로 작성된 문서에 작성자나 송신자의 도장을 찍는 것과 동일한 효과를 얻을 수 있다[15].

2.2.2 공개키 기반 인증

영상회의를 하기 위해서는 사용자 인증을 받아야 한다. 사용자 인증은 회원가입을 통해 이루어진다. 회원가입은 사설 PKI 기반[15]의 인증서를 통해 영상회의 서버에 로그인하게 된다. 로그인 하기 위한 아이디와 패스워드는 암호화하여 로그인 과정에서 허가받지 않은 제3자가 중간에 로그인 정보를 가로채기 하더라도 비밀키가 없으면 로그인 정보를 알아내기 어렵도록 한다. 회원에 등록하고 아이디와 암호기반의 로그인이나 인증서기반의 로그인 과정을 통하여 사용자 인증을 받으면 영상회의에 참여할 수 있게 된다. 영상회의 참여자는 영상회의 서버에 접속하여 자신의 인증서 Cert를 전송한다. 영상회의 서버는 인증서 발급을 위해 인증서버에 인증서 Cert를 인증경로를 통하여 CA서버에게 검증하고 올바른 인증서이면 영상회의 서버에 인증서를 전송하여 인증을 확인하게 되고 영상회의에 참여할 수 있도록 한다.




(그림 2) PKI 기반 인증 흐름도

(그림 2)에서 Client A와 Client B는 CA의 사용자 이고 Client A와 Client B는 사전에 CA에게 자신의 공개키를 등록($K_{UA}$, $K_{UB}$)하여 CA로부터 각각 $C_A$, $C_B$를 수신받아 자신의 PC에 보관하였다가 P2P로 통신하고자 할 때 각각의 인증서를 암호화 처리된 메시지와 함께 보낸다. 암호화 처리된 메시지는 서로의 공개키를 CA로부터 받아 암호화 처리 과정에서 사용한다. CA가 Client A와 Client B에게 인증서를 보낼때 Timestamp와 난수를 포함하여 송신하는데 이는 추후 Client A와 Client B가 서로 인증서내의 공개키를 확인하는 과정에서 인증서의 유효성을 판단하는 기준이 되도록 하였다. Client A와 Client B에게 보낸 $C_A$는 Client B가 이미 가지고 있는 CA의 공개키로 복호화하여 Client A의 공개키를 다음과 같이 확인한다.

$$B = D_{KUAUTH}[C_A] = D_{KUAUTH}[E_{KRAUTH}[Time1, ID_A, K_{UA}]$$
$$= [Time1, ID_A, K_{UA}]$$

2.3 키 분배 프로토콜

공개키 기반 암호화 알고리즘은 비밀키 암호화 알고리즘에 비해 암/복호화시간이 상당히 오래걸리기 때문에 데이타를 공개키로서 암/복호화 해서 전송하는 것은 매우 힘들다. 따라서 통신의 암호화는 비밀키를 이용하여야 하나 비밀키는 통신하기 이전에 동일한 키가 미리 분배되어 있어야한다는 문제가 발생한다. 이러한 조건을 만족시키기 위하여 비밀키 알고리즘으로 실제 데이타를 암/복호화를 하지만 이를 위한 비밀키는 공개키 알고리즘으로 서로 교환하는 방법을 사용하게 된다. 본 논문에서는 P2P의 화상회의(1 : 1)일 경우에는 Diffie-Hellman[12, 16]을 이용한 키 분배 프로토콜을 사용하며 다수간 화상회의 (1 : N)일 경우 공개키 기반의 키 분배 방식을 사용하였다. 키 분배 프로토콜(key agreement scheme)은 Diffie-Hellman 알고리즘 등을 이용하여 서로 상대방에게 필요한 정보를 교환하여 Shared secret를 생성하는 방법이다. 크게 Shared secret를 서로 공유하는 과정인 agreement와 공유된 secret를 이용하여 필요한 Master secret나 KEK(Key encryption Key)를 유도하는 과정인 key derivation 과정으로 나누어진다.

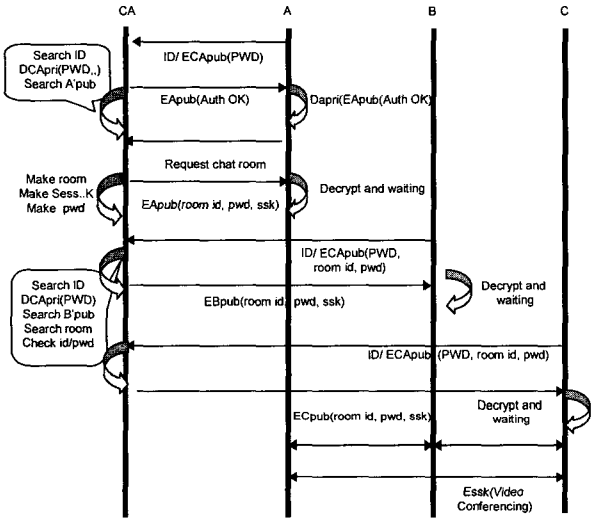
공개키 기반의 키 분배 방식은 사용자가 ID/PWD로 로그인 할 때 로컬 컴퓨터에 존재하는 개인키로 패스워드를 암호화하여 전송하며, 영상회의 서버는 암호화된 값을 서버의 개인키로 해독하여 사용자를 위한 세션키를 만들고 해당 사용자의 공개키 값으로 암호화 하여 전송하게 된다. (그림 3)은 1 : N 다자간 영상회의에 대한 인증절차를 보여주는 것으로 A는 회의실 개설자이고 B와 C는 회의실 참여자이다.

- **용어 정의**
  - Apub : 사용자 A의 공개키, Bpub : 사용자 B의 공개키, Cpub : 사용자 C의 공개키
  - Apri : 사용자 A의 비밀키, Bpri : 사용자 B의 비밀키, Cpri : 사용자 C의 비밀키

- ECApub : 사용자 A의 공개키를 암호화, DApri : 사용자 A의 비밀키를 복호화
- EBpub : 사용자 A의 공개키를 암호화, DBpri : 사용자 B의 비밀키를 복호화
- ECpub : 사용자 C의 공개키를 암호화, DCpri : 사용자 C의 비밀키를 복호화

회의실 개설자 A는 회의실을 개설하기 위해 CA로부터 인증을 받는다. 이때 A는 ECApub(pwd)를 사용하여 자신의 패스워드를 CA의 공개키로 암호화하여 CA로부터 EApub (Auth OK) 형태로 인증을 받게 된다.

이때 CA가 A에 대해 인증한다는 것을 의미하는 OK 메시지를 A의 공개키로 암호화 해서 CA가 A에게 보낸 메시지를 DApri(EApub(Auth OK)) 형태로 A의 개인키로 복호화하여 자신이 A임을 증명하도록 한다.



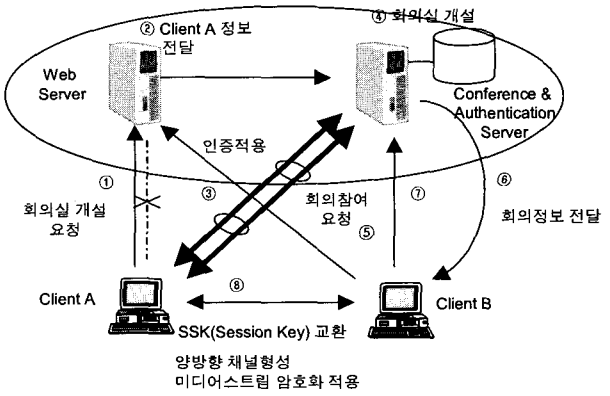

(그림 3) 1 : N 다자간 영상회의시 인증 절차

B와 C도 영상회의에 참여하기 위해 A와 같은 인증절차를 거치는데 이때 CA는 B와 C의 영상회의 참여자에게 공개키를 이용해서 room id, pwd, session key를 EBpub(room id, pwd, ssk)와 ECpub(room id, pwd, ssk)의 형태로 암호화해서 정보를 보낸다. 인증절차가 끝나면 A와 B, A와 C, B와 C는 서로 P2P 형태로 영상회의 데이터의 헤더정보를 암호화하여 상대방에게 전송함으로서 보안성있는 영상회의가 가능하게 된다.

## 3. 보안성있는 영상회의 시스템의 설계 및 구현

### 3.1 인증을 적용한 P2P 기반 영상회의

본 논문에서 영상회의 기본 모델에 사용자 인증과 P2P로 데이터암호화를 처리하여 실시간으로 영상회의를 수행하는 모델을 제안한다. P2P 영상회의 모델은 회의실을 개설하거나 회의 제어를 위한 제어정보에 대하여 공개키 기반 TLS[11, 13]를 통해 암호화함으로서 보안성을 강화하였다. P2P 영상회의 모델은 회의를 준비하는 과정에서는 Server의 도움을 받지만 회의가 시작된 후에 회의 참여자 간에 교환되는 모든 정보들이 참여자들 간에 직접 전달되는 모델이다. P2P 기반 영상회의는 (그림 4)와 같은 시나리오로 이루어진다.




(그림 4) P2P 기반 영상회의 모델

Client A와 Client B는 영상회의 인증절차를 거쳐 사전에 인증을 받은 후 회의실에 들어갈 수 있게 된다.

① 회의대기 상태 있는 Client A는 웹Server에 회의실 개설을 요청한다. 이때 Client A는 사전에 약속된 회의실 번호를 전달한다.

② 웹Server는 영상회의 Server 프로세스를 생성하고 해당 프로세스에 Client 1에 대한 정보를 전달하고, Client A에게 영상회의 Server 프로세스에 대한 정보를 전달한다.

③ Client A는 웹Server와의 연결을 종료하고 영상회의 Server 프로세스에게 연결을 요청하여 회의실 개설을 요청한다. 이때 Client A는 영상회의가 시작될 경우 다른 Client와 통신할 수 있는 정보를 영상회의 Server 프로세스에게 전달한다. 이 단계에서는 제어정보에 대해 TLS를 적용하여 암호화를 수행한다.

④ 영상회의 Server는 웹Server로부터 받은 회의실 번호와 Client A로부터 받은 회의실 번호가 같은 경우 회의실을 개설한다.

⑤ Client B는 웹Server에 회의 시작을 요청한다. 이때 사전에 약속된 회의실 번호를 전달한다.

⑥ 웹Server는 요청한 회의실 번호에 해당하는 회의실이 개설되었는지를 확인하고 개설된 경우에 영상회의 Server 프로세스에게는 Client B의 정보를, Client B에게는 해당 회의실을 관리하는 영상회의 Server 프로세스의 정보를 전달한다.

⑦ Client B는 영상회의 Server 프로세스에게 Client A의 정

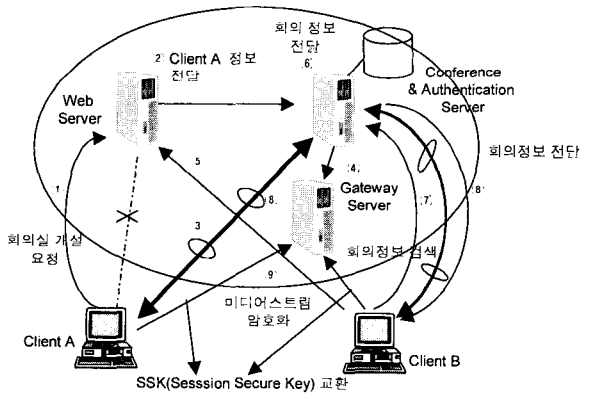
보를 조회하고 응답 받는다.

⑧ Client B는 Client A에게 양방향 채널을 요청하여 영상회의를 시작한다. 이때 영상회의에 필요한 스트림 데이터의 헤더부분을 암호화하여 실시간으로 전송한다.

P2P 기반 모델은 회의 도중에 발생하는 모든 데이터를 참여자들 간에 직접 전달되므로 네트워크 효율을 증가시킬 수 있을 뿐만 아니라 별도의 Server를 필요로 하지 않는다. 그러나, 방화벽을 설치하여 보안을 강화하고 있는 조직에서는 별도의 Server를 필요로 하는 경우가 있는데 다음 절에서 논하기로 한다.

### 3.2 인증을 적용한 Server 기반 영상회의

Server 기반 회의 모델은 회의를 준비하는 과정뿐만 아니라 회의 도중에도 Server의 도움을 받아서 회의 참여자들 간에 정보를 교환하는 모델이다. Server 기반 회의 모델의 동작 절차는 (그림 5)와 같다. Server 기반 모델은 회의 도중에 발생하는 모든 데이터가 Server를 경유하여 전달되므로 비효율적이다. 그러나, Client 환경에 방화벽이 설치되어 있어서 접근이 자유롭지 않은 환경에서 불가피한 경우 사용자의 선택에 의하여 Server기반 회의를 진행할 수 있도록 한다.




(그림 5) Server 기반 영상회의 모델

Client A와 Client B는 영상회의 인증절차를 거쳐 사전에 인증을 받은 후 영상회의실에 들어갈 수 있다.

① Client A은 웹Server에 회의실 개설을 요청한다. 이때 Client는 사전에 약속된 회의실 번호와 방화벽 사용 유무를 전달한다.

② 웹Server는 영상회의 Server 프로세스를 생성하고 해당 프로세스에 Client1에 대한 정보를 전달하고, Client 1에게 영상회의 Server 프로세스에 대한 정보를 전달한다.

③ Client A은 웹Server와의 연결을 종료하고 영상회의 Server 프로세스에게 연결을 요청하여 회의실 개설을 요청한다. 이때 새로운 참여자가 회의에 참여하기 위해 영상회의 서버에 접속하기 위해서는 인증절차를 거친 후 영상회의에 참여할 수 있다. 이 단계에서는 제어정보에 대해 TLS를 적용하여 암호화를 수행한다.

④ 영상회의 Server는 웹Server로부터 받은 회의실 번호와 Client로부터 받은 회의실 번호가 같은 경우 회의실을 개설하고 참여자들의 영상 정보를 릴레이 할 게이트웨이 프로세스를 생성한다.

⑤ Client B는 웹Server에 회의 시작을 요청한다. 이때 사전에 약속된 회의실 번호를 전달한다.

⑥ 웹Server는 요청한 회의실 번호에 해당하는 회의실이 개설되었는지를 확인하고 개설된 경우에 영상회의 Server 프로세스에게는 Client B의 정보를, Client B에게는 해당 회의실을 관리하는 영상회의 프로세스의 정보를 전달한다.

⑦ Client B는 영상회의 Server 프로세스에게 Client A의 정보를 조회한다.

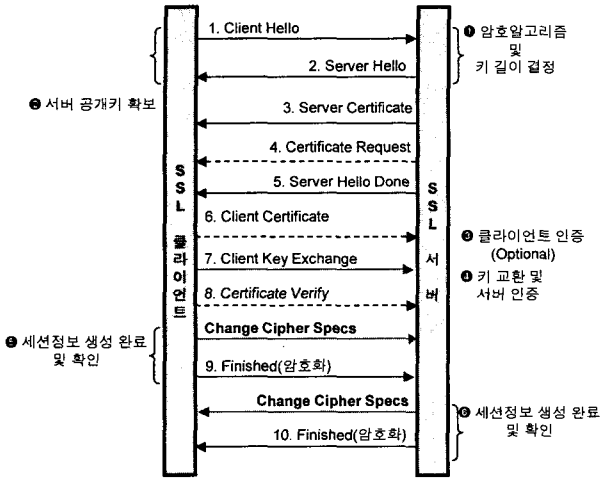
⑧ 영상회의 Server 프로세스는 ClientA, B에게 게이트웨이 프로세스의 정보를 전달한다.

⑨ Client A는 게이트웨이 프로세스에 연결을 요청하여 회의를 시작한다. Client A와 Client B가 게이트웨이를 통하여 연결되면 게이트웨이 프로세스는 영상 정보를 릴레이 하고 미디어 데이터에 대한 암호화를 수행한다.

### 3.3 보안 프로토콜 적용

본 논문에서 제안한 영상회의는 웹Server, 영상회의 Server, 게이트웨이 Server와 회의 참여자들로 구성된다. 각 구성 요소들 간에 발생할 수 있는 보안 취약점들을 요약하면, 참여자들의 신분 확인, 회의를 준비하기까지 과정에서 교환되는 제어정보에 대한 무결성 및 기밀성, 회의가 진행되는 동안에 참여자들 간에 교환되는 미디어 정보의 기밀성에 대한 보안 대책이 필요하다. 따라서 이러한 보안 취약점은 웹 서버에 공개키 기반 서버인 사설 CA를 두어 인증서를 통한 사용자 인증을 확인함으로서 해결한다. 인증서를 적용한 트랜스포트 보안 프로토콜은 2장에서 언급한 바와 같이 참여자 뿐만 아니라 회의에 사용되는 하드웨어 자원들에 대한 인증도 가능하여 보안성이 강화된 사용자 신분확인 서비스를 제공할 수 있다. 또한, 트랜스포트 계층 보안 프로토콜은 다른 구성 요소들 간의 연결에도 투명하게 적용할 수 있는 장점을 제공한다. 트랜스포트 계층 보안 프로토콜의 적용은 (그림 6)에서 나타낸 바와 같이 Client와 Server간에 인증하는 절차로 이루어진다. TLS(Transport Layer Security)의 Full Handshake 과정은 Client가 Server에게 Client Hello 메시지를 전송함으로써 시작된다. 이 때 Client가 사용할 수 있는 관용 알고리즘의 목록, 공개키 알고리즘의 목록, 압축 방법 목록들을 전송한다. Client Hello 메시지를 수신한 Server는 Client가 전송한 매개 변수들의 목록에서 세션에 적용할 것을 결정

하며, 이에 대한 응답으로 Server Hello 메시지를 전송한다.




(그림 6) Client와 Server의 인증절차[17]

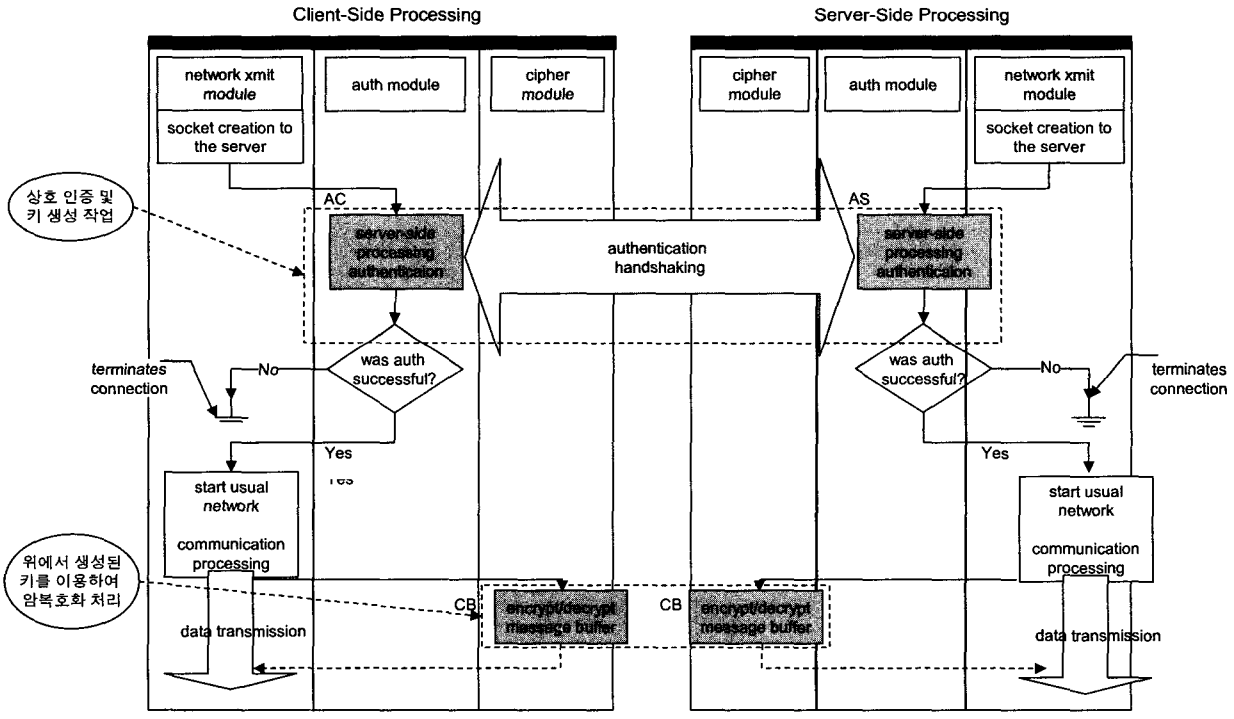
또한, Server 자신의 인증서를 전송하고 세션에 적용할 매개 변수들을 전자 서명한 값을 Client에게 전송한다. 이어서 Client인증을 위하여 Client 인증서를 요청한다. Client는 Server로부터 받은 전자 서명된 매개 변수에 대한 서명을 검증하여 1차적으로 Server를 인증할 수 있다. 서명 검증이 성공적으로 완료되면 Client는 Server가 인증서를 요청한 경우 인증서를 Server에게 전송한다. 또한, 그 동안 주고 받은 메시지들을 전자서명하여 Server에게 전송한다. Server는 전자서명된 메시지들을 수신하여 전자 서명을 검증하고 성공적으로 서명을 검증하면 Client 인증에 성공한 것이다. 이 과정을 통하여 서로를 인증하고 필요한 암호 매개 변수들을 생성한 Client와 Server는 Finished 메시지를 보내서 Handshake 과정을 종료하면 사용자 데이터를 교환할 준비를 마친 것이다. 회의 참여자들 사이에서 교환되는 메시지에 대한 무결성과 기밀성은 레코드 프로토콜에 의하여 수행된다. 교환되는 메시지에 MAC 코드를 생성하여 교환함으로써 무결성을 제공하고, 핸드쉐이크 동안에 공유된 키에 의한 암호화를 통하여 무결성이 보장된다. 미디어스트림에 대한 암호화 알고리즘 및 키 길이의 선택은 핸드쉐이크 하는 동안에 협상된다. 따라서 RC2, DES, Triple-DES, SEED[9, 12]와 같은 알고리즘을 자유롭게 선택할 수 있다.

## 4. 영상회의 시스템의 암호화 구현 및 성능 분석

### 4.1 영상회의 시스템의 암호화 구현

본 논문에서 영상회의의 인증과 암호화 구현을 위해 (그림 7)와 같이 Client에서 인증하는 AC(Authentication for Client) 모듈과 서버에서 인증하는 AS(Authentication for Server) 모듈을 사용하였다. 영상회의시 주고 받는 미디어 데이터의 암호화와 복호화를 위해 메시지버퍼(CB(Cipher message Buffer))를 사용하였다.

본 논문에서 사용한 영상압축과 음성압축 코덱으로는 PCM 방식인 G723.1과 GSM6.10을 사용하였고, 네트워크 평균 대역폭으로는 음성은 1.4kb, 영상은 4kb~2kb 기타 1kb로 전송 대역폭을 설정한 후 대역폭에 따라 영상프레임의



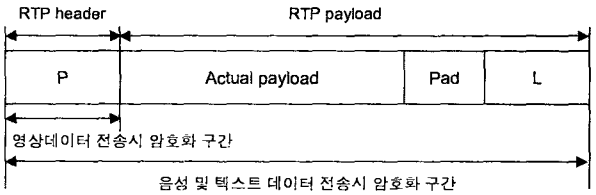

(그림 7) 영상회의 암호화 구현 절차

대역폭을 조절하면서 데이터를 송신하도록 하였다. 네트워크의 환경에 따라 전송되는 대역폭의 변화가 있을 경우 프로토콜을 변경하여 사용한다. 영상프레임은 일반적으로 32bit로 전송된다. 대역폭의 계산은 네트워크 상황에 따라 대역폭의 평균값을 채택하였으며 평균치에서 벗어나는 부분은 최저 값으로 계산하였다.

### 4.2 보안 적용 영상회의 패킷

• Control Server Packet

(그림 8)에서 보는 바와 같이 회의실의 개설 및 입장, 참여, 연결된 사용자 정보, 채팅 등을 위한 서버와의 연결을 위한 Packet, 접속한 회의실 참여자의 리스트 정보를 갖고 회의 진행의 제어권을 변경할 수 있다.




(그림 8) Control Server Packet 구조

암호화하기 위한 평문은 항상 블록 길이와 같아야 한다. 영상회의에서의 비디오 데이터는 항상 가변적이므로 Pad를 사용하여 블록의 길이를 맞추어야 하고, 일반적인 오디오 데이터는 항상 고정된 Octet 길이를 가지므로 별도의 처리가 필요 없다. 본 논문에서는 H.235 프로토콜에서 권장하듯이 부족한 블록의 길이만큼 0x00의 값을 채워 넣어서 블록의 길이를 맞추는 Zero 패딩방법을 적용하였다.

• Gateway control process Data Packet 구조

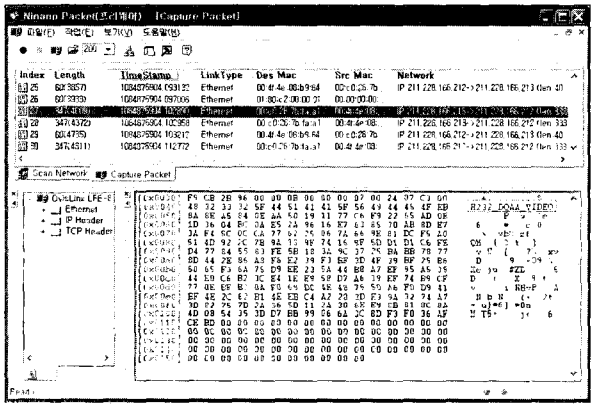
(그림 9)는 P2P또는 Gateway Control process Data Packet 구조로 영상회의 참여자가 음성, 영상, 화이트보드, 첨부파일 등을 송신하기 위한 Packet 구조로 송신측의 ID와 수신측의 ID, 송신데이터 형식인 영상, 음성, 화이트보드 Data와 특정한 회의실 참여자에게 송신할 수 있도록 구성되어 있다. 파일전송 시 데이터를 보내는 도중에 계속 보낼 경우 처리와 파일의 이름과 크기, 데이터의 끝을 명시한 정보를 포함하고 있고 데이터전송의 승낙과 취소에 대한 처리를 하도록 한다.

| Command | Flag | Source id | Destination id | Data Type | Data length | Data |
|---|---|---|---|---|---|---|

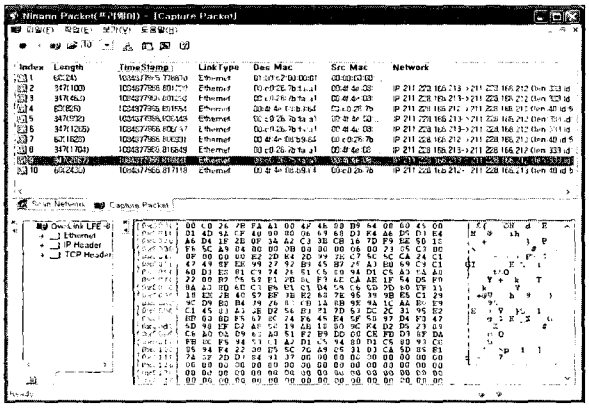
(그림 9) P2P 또는 Gateway Control process Data Packet 구조

#### 4.2.1 미디어 스트림의 암호/복호화 구현결과

미디어 스트림의 암호화는 호 설정 동작에 의한 공통키의 생성, 비밀키의 분배, 그리고 오디오, 비디오 스트림의 암호화로 이루어진다. 암호화를 적용한 영상회의 시스템은 속도가 일반적으로 느린 점을 감안하여 스트림암호화를 적용하더라도 미디어 지연속도를 최대한 빠르게 하도록 데이터에 대한 암호화 방법은 Message Buffer를 사용하였다. 특히 영상데이타의 경우 데이터 량이 매우 크고 헤더 부분이 없이는 해독이 불가능 하기 때문에, 텍스트 및 음성 데이터와는 달리 영상 데이터의 헤더 부분만을 AES등 대칭키로 암호화 하여 전송하였다. (그림 10)과 (그림 11)은 암호화 되지 않았을 때의 데이터를 스니핑 하고 암호화 한 영상회의를 진행했을때, 그 데이터를 비교한 것이다. 특히 (그림 10)의 경우에서는 데이터의 헤더 부분에 "H232_DQAA_VIDEO"라는 프로토콜 정보 및 데이터에 관련한 정보들이 노출되게 되는데 암호화를 적용했을 경우에는 (그림 11)에서처럼 헤더 정보를 전혀 볼 수 없게 되며, 데이터의 내용을 확인할 수 없도록 암호화하게 된다.



(그림 10) 영상 데이터 스니핑한 결과



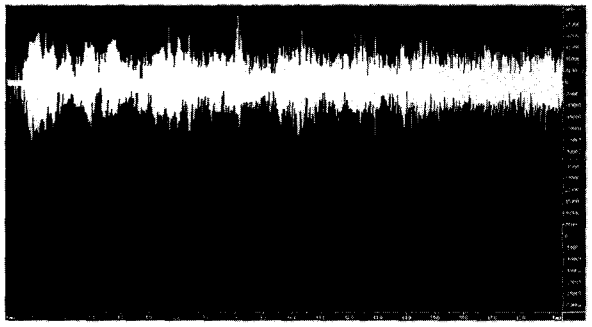
(그림 11) 암호화된 영상 스니핑 결과

#### 4.2.2 음성 스트림의 암호화 결과

암호화 통신을 한 영상회의 비디오 및 오디오 데이터는 암호화 되어있기 때문에 정확한 키를 가지고 있지 못하면 보거나 들을 수가 없다. 특히 영상인 경우는 화면이 노이즈로 가득차 보이지 않는 현상을 띄게 되며, 보다 중요한 오디오 데이터의 경우에도 암호/복호화가 수행되어 각각의 터미

널에서만 정상적인 음성을 들을 수 있다. (그림 12)와 (그림 13)은 이러한 잘못된 비밀키를 사용하여 복호화 하는 경우, 비 정상적인 오디오 데이타를 갖게 되는 것을 실험을 통해 시연하였다.

(그림 12) 정상적인 키를 사용한 음성파형



(그림 13) 복호화가 안된 음성 파형

(그림 12)은 정상적인 키를 사용하여 음성으로 통신한 것을 기록하여 음성 파형 변환기로 변환한 것으로서 정확한 음성과 내용을 확인할 수 있었으나 (그림 13)은 비정상적인 키로 강제 복호화한 내용을 음성 파형 변환기로 변환한 것으로서 음성을 구분할 수 없고, 비정상적인 잡음으로 인해 음원이 망가진 형태의 파형을 볼 수 있다.

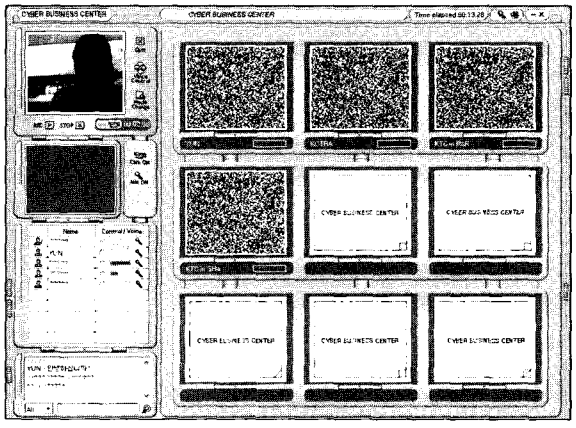
〈표 1〉 음성 복호화 파일의 데이터 파형분석

| | 정상복호화 | 비정상복호화 |
|---|---|---|
| Min Sample Value : | -20043 | -25867 |
| Max Sample Value : | 17351 | 25275 |
| Peak Amplitude : | -4.27dB | -2.06dB |
| Possibly Clipped : | 0 | 0 |
| DC Offset : | 0 | 0 |
| Minimum RMS Power : | -38.88dB | -37.1dB |
| Maximum RMS Power : | -10.1dB | -8.35dB |
| Average RMS Power : | -20.58dB | -16.05dB |
| Total RMS Power : | -18.87dB | -14.64dB |

4.2.3 화상 스트림의 암호화 결과

(그림 14)은 정상적인 사용자들이 영상회의를 진행하고 있는 모습이다. 각 사용자들 사이의 데이터는 암호화 통신을 하고 있으며, 영상이 매우 뚜렷함을 볼 수 있다. 반면 (그림 15)은 암호화 통신을 sniffing 하여 회의실 번호 및 ID등을 해킹을 통하여 획득하여 영상회의에 참여한 모습을 캡쳐했다. 그러나 예상과는 달리 비디오 및 오디오 데이터는 암호화 되어있기 때문에 정확한 키를 가지고 있지 않기 때문에 보거나 들을 수가 없다. 특히 영상인 경우는 화면이 노이즈로 가득차서 상대방의 화상이 나타나지 않는 현상을 보였으며, 기존 사용자들은 허가받지 않은 사용자의 모습을 알 수 있게 되어 누가 불법적으로 접근하고 있는지 확인 할 수 있다. 물론 공격자가 데이터를 암호화 한다면 기존 사용자도 알 수 없지만 암호화 키를 공유하지 않고 있기 때문에 이러한 방법은 불가능하다고 할 수 있다.

(그림 14) 정상적인 화상회의 모습



(그림 15) 불법적인 접근을 통한 화상회의 참여 모습

4.3 성능평가

본 논문에서 제안한 영상회의 시스템에 암호화 알고리즘을 적용한 경우 오디오, 비디오 데이터를 암호/복호화 하는 경우에 대해 각각의 알고리즘별 미디어 전송지연시간을 측정한 결과는 <표 2>와 같다.

<표 2>에서 보는바와 같이 미디어 전송에 따른 지연시간

에 대한 성능 측정은 5MByte 정도 분량의 영상회의 데이터를 암호화를 적용하지 않았을 경우(Not Encrypted)와 각각의 대칭키로 암호화 하였을 경우 걸리는 시간을 측정하였다. 구동되는 서버는 일반 x86 계열의 CPU 2Ghz 4개를 가진 컴퓨터에 메모리는 512M로 하였으며, 통신 대상자는 일반적으로 네트워크 속도가 128KB/sec 정도가 나오는 16곳에서 기본사양을 가진 PC로 동시 화상회의를 실시하였다. 음성 및 화상에 대한 미디어 데이터를 5Mbyte 정도 사용하였을 때 나타난 결과표이다.

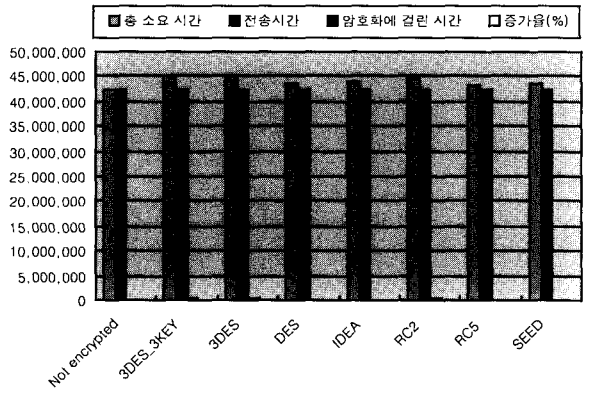
〈표 2〉 5Mbyte 미디어 전송시 소요시간

(단위 : micro second)

| Algorithm | 총소요시간 | 전송시간 | 암호화시간 | 증가율(%) |
|---|---|---|---|---|
| Not encrypted | 42,452,264 | 42,452,264 | 0 | 0 |
| 3DES_3KEY | 45,207,904.70 | 42,450,358.70 | 275,754.60 | 0.649563943 |
| 3DES | 45,222,272.40 | 42,452,704.40 | 276,956.80 | 0.65239583 |
| DES | 43,554,251.30 | 42,450,883.30 | 110,336.80 | 0.259907929 |
| IDEA | 43,839,485.50 | 42,454,157.50 | 138,532.80 | 0.326326059 |
| RC2 | 44,951,342.40 | 42,460,974.40 | 249,036.80 | 0.586627842 |
| RC5 | 43,244,046.50 | 42,455,795.40 | 78,825.11 | 0.185679402 |
| SEED | 43,484,614.70 | 42,451,300.70 | 103,331.40 | 0.2434061 |

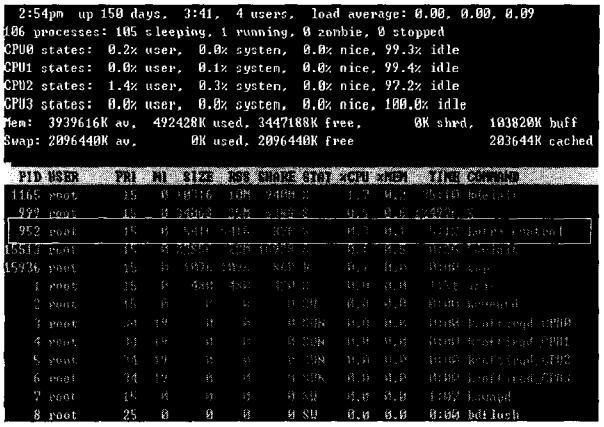
* 총소요시간(micro sec) = 네트워크 전송시간 + 암호화 시간
* 증가율(%) = (암호화시간 / 암호화 하지 않았을 때의 총 소요시간 ) * 100

<표 2>에서 나타내는 바와 같이 RC5 알고리즘과 DES알고리즘을 사용했을 때가 다른 알고리즘을 사용할 때보다 암호화 하는데 가장 적은 시간이 걸려, 미디어 데이터를 빠른 속도로 전송 할 수 있었음을 알 수 있다.




(그림 16) 5Mbyte 미디어 전송시 소요시간

그러나 (그림 16)에서 보면 전체적인 시간으로 나타낸 암호화에 걸린 시간은 극히 적고 암호화한 데이터를 전송해서 처리하는 시간과 암호화 하지 않은 데이터를 보내어 처리한 결과가 거의 차이가 나지 않기 때문에 사용자들이 암호화에 따른 지연시간을 느끼지는 못 할 정도로 매우 빠르게 수행됨을 알 수 있다.




(그림 17) 서버기반의 화상회의시 CPU 성능측정

본 논문에서 제안/구현한 Pear-to-Pear기반의 화상회의 시스템은 메인 서버에 영향을 거기 주지 않게 된다. 따라서 (그림 17)는 사용자단에 침입차단시스템이 설치되어 있다고 가정하고 서버 기반의 화상회의 시스템을 기동하였을 때, 동시 16명이 화상회의 시스템을 이용하고 있을때 서버의 성능 상태를 측정하였다. kotra_control 이라고 하는 데몬은 화상회의 서버 데몬으로서 암호/복호화를 처리하는 과정에서 사용되는 메모리로 약 0.1%의 사용 증가를 가져 왔으며, 약 0.3%의 CPU사용 증가율을 나타내었다. 따라서 본 논문이 제안/구현한 영상회의 서버는 1,500명 이상의 동시 접속을 처리할 수 있고, 암호/복호화의 과정에서 컴퓨터의 리소스를 매우 적게 사용함을 알 수 있다.

## 5. 결 론

본 논문에서는 트랜스포트 보안 프로토콜을 적용한 영상회의 시스템을 설계하여 구현하였다. 트랜스포트 보안 프로토콜은 국내 공인인증 규격을 만족하는 공개키 기반 인증서를 적용하였다. 트랜스포트 보안 프로토콜을 적용하여 영상회의 시스템의 제어 정보를 보호함으로써 사용자 인증, 제어 정보에 대한 기밀성 및 무결성을 제공할 수 있었다. 본 논문에서 DES, Triple-DES, AES 알고리즘을 구현하여 미디어 스트림의 암호화에 적용함으로써, 각각의 알고리즘이 영상회의 시스템에 미치는 영향을 분석하였다. 분석 결과 보안성을 확보하는 암호/복호화 과정을 거치는 동안 암호화를 적용하는 경우와 비교하여 미디어 스트림 패킷의 전달 지연속도에 영향을 미치지 않음을 알 수 있으며, 메모리의 사용량이 크게 증가하지 않음을 알 수 있다. 따라서, 인증 및 암호/복호화 기능의 추가에도 불구하고 영상회의의 성능이 저하되는 않는 결과를 보여준다. 또한, 트랜스포트 계층의 보안 프로토콜과 공개키 기반의 CA를 구축하여 사용함으로써 미디어 스트림 암호화 과정에서 사용되는 비밀키를 분배하는 문제도 해결할 수 있었다.

## 참 고 문 헌


[1] E. Rescorla, Diffie-Hellman Key Agreement Method, IETF RFC 2631, 1999.

[2] Federal Information Processing Standards Publication, Announcing the Advanced Encryption Standard(AES), 2001.

[3] ITU-T Recommendation H.323, Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-Guaranteed Quality Service(ver4), 2000

[4] Jacobson, V. and McCanne, S., "Visual Audio Tool," Lawrence Berkery Laboratory.

[5] ITU-T Recommendation H.225.0, Media Stream Packetization and Synchronization Non-Guaranteed Quality of Service LANs(ver4), 2000.

[6] L. Berc, W. Fenner, R. Frederick, S. McCanne, "RTP Payload Format for JPEG-compressed Video," RFC 2035, October, 1996.

[7] ITU-T Recommendation H.245, Control Protocol for Multimedia Communication(ver8), 2001.

[8] ITU-T Recommendation H.235 Security Encryption for H-series Multimedia terminals(ver3), 2001.

[9] R. Rivest, A Description of the RC2(r) Encryption Algorithm, IETF RFC, 2268, 1998.

[10] William stallings, Cryptography and Network security, Prentice Hall, 1998.

[11] S. A. Thomas, SSL&TLS Essentials : securing the web Wiley, 2000.

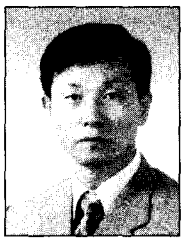
[12] 한국전자통신연구원, 암호학의 기초, 경문사, 1999

[13] T. Dierks, C. Allen, "The TLS Protocol Version 1.0," IETF RFC 2246, January, 1999.

[14] M. Baugher, D. McGrew, Cisco Systems, Inc. M. Naslund, E. Carrara, K. Norrman, Ericsson Research, "The Secure Real-time Transport Protocol(SRTP)," IETF RFC 3711, March, 2004.

[15] Russ Housley and Tim Polk, Planning for PKI, John Wiley & Sons, 2002.

[16] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory, Vol.1T-11, No.6, November, 1976.


### 정 용 득

e-mail : jungyd@kotra.or.kr

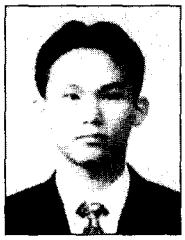
1988년 목포대학교 전산통계학과 학사

1990년 숭실대학교 전자계산학과 석사

2001년 숭실대학교 컴퓨터학부 박사과정 수료

1997년~현재 대한무역투자진흥공사 차장

관심분야 : 암호학, 멀티미디어정보통신, PKI


### 이 상 훈

e-mail : iam@leesanghun.pe.kr

2001년 숭실대학교 컴퓨터학과 학사

2003년 숭실대학교 컴퓨터학과 석사

2003년~현재 숭실대학교 컴퓨터학부 박사과정

관심분야 : 바이러스, 암호학, 침입차단 시스템, PKI



### 전 문 석

e-mail : mjun@comp.ssu.ac.kr

1980년 숭실대학교 전자계산학과 학사

1986년 University of Maryland 전산과 석사

1989년 University of Maryland 전산과 박사

1989년 Morgan State University 전산수학과 조교수

1989년~1991년 New Mexico State University 부설 Physical Science Lab. 책임연구원

1991년~현재 숭실대학교 정보과학대학 부교수

관심분야 : 암호학, 침입차단 시스템, PKI