韓國컴퓨터情報學會 論文誌
第15卷 第12號, 2010. 12.

2010-15-12-3-4

화상상담 인증 : 안전한 키 관리 프로토콜 설계

정 용 득*

Video Conferencing Authentication : A Key Management Protocol Design for safety

Jung Young Deug*

요 약

다자간 화상상담에서 회의 참여자의 인증을 위해 참여자의 ID와 패스워드를 대칭키로 암호화하여 전송하는 방식은 비밀키의 수가 많아지게 되어 암호화와 복호화를 위한 키의 관리가 어렵다는 것과, 제3자가 대칭키를 스니핑할 수 있어서 화상상담의 보안성이 떨어지는 문제점이 있다. 본 논문에서는 화상상담에서 보안성을 높이기 위해, 첫째, 다수의 회의 참여자를 PKI 기반의 X.509 인증서로 인증하고, 둘째, 영상통신에서 참여자의 개인키를 교환하여 세션공유키로 만들고 세션공유키의 조합을 통해 키를 만들어 참여자가 바뀔 때마다 키를 갱신하였다. 셋째, 화상회의시 전송되는 미디어 데이터의 RTP 페이로드를 암호화하여 전송함으로써 보안성을 높였다.

Abstract

There is an authentication method for participants with an encrypted ID and password as a symmetric-key in multilateral video conferencing. It is hard to manage when the security-keys makes many while the transportation processing for the encryption and decryption get complicated when the video conferencing involves a number of participants and the third party as an attackers to gain unauthorized symmetric-key to access video conference which makes a problem less secrecy. This study suggests three ways to enhance security in video conference: first, we present PKI-based X.509 certificate for authenticating the participants of multilateral conferencing and we suggest to encode and decode the video conference media data using a secrecy key created by each of the conference participants; second, a more secured multilateral video conferencing can be expected in a group communication by using the participants secrecy key in creating and distributing group keys, where the group key will be renewed whenever there is change in the group member; and finally, we suggest to encode the RTP payload of the media data before transmission.

▸ Keyword : 화상상담, H.323. RTP, PKI

• 제1저자 : 정용득
• 투고일 : 2010. 09. 27, 심사일 : 2010. 10. 07, 게재확정일 : 2010. 10. 11.
* 한세대학교 정보통신학부

Ⅰ. 서 론

인터넷과 같이 신뢰할 수 없는 네트워크 환경에서의 화상상담은 악의를 가진 제3자에 의해 화상상담이 방해 받을 수 있다. 인터넷을 통해 전송되는 멀티미디어 데이터의 안전한 통신을 보장하기 위해서는 암호학적인 기법을 이용하여 자체의 프로토콜로 보호할 필요가 있다. 안전한 화상상담을 보장하기 위해서는 첫째, 참여자(member)를 인증하는 방법으로 공개키 기반 구조(Public Key Infrastructure : PKI)를 사용하는 것이다. 공개키 기반구조는 신뢰할 만한 인증기관이 발행한 공개키 인증서(Public Key Certificate : PKC)와 전자서명(Digital Signature)을 통해 사용자를 인증할 수 있어서 화상상담 참여자의 신원을 보장할 수 있다[3]. 둘째, 화상상담시 전송되는 미디어 데이터의 무결성과 기밀성을 보장하기 위한 방법으로, 회의실 그룹 내에서 키를 소유한 화상상담 참여자들만이 안전한 대화가 가능하도록 그룹의 각 참여자가 랜덤하게 생성한 숫자를 조합하여 키를 만들어 키의 소유자에 한하여 참여를 제한하는 방법이다. 셋째, 화상상담시 세션정보를 암호화하여 보냄으로써 안전한 화상상담이 가능하도록 하는 것이다.

본 논문에서는 보안성 있는 다자간 화상상담을 위해 기존의 화상상담 보안 표준을 참조하여 화상상담 참여자의 인증과 키를 이용한 참여자의 관리를 통해 화상상담 데이터를 안전하게 전달하는 프로토콜을 제안한다.

본 논문의 구성은 5장으로 구성되어 있으며, 각 장의 주요 내용은 다음과 같다. 2장에서는 화상상담 참여자가 제3의 신뢰기관인 인증기관을 어떻게 이용하는지 공개키 기반구조에 대한 내용을 살펴보고 화상상담을 위한 키 관리에 대해 기술한다. 3장에서는 본 논문에서 제안하는 인증서 기반의 공개키 기반구조를 적용한 보안성 있는 다자간 화상상담 프로토콜을 기술하고, 제안한 프로토콜을 이용하여 화상상담 시스템 내부적으로 수행하는 보안 화상상담 트랜잭션에 대해 기술한다. 4장에서는 본 논문에서 제안한 프로토콜을 적용한 키 관리시스템을 구현하여 실험을 통해 키의 생성과 수행시간을 분석한다. 화상상담시 전송되는 미디어 데이터의 암호화와 복호화에 대한 성능을 분석하고, 5장에서 결론과 향후 연구과제에 대하여 기술한다.

Ⅱ. 화상상담시스템의 인증과 키관리

2.1 화상상담 시스템

최근 인터넷의 기술과 속도가 향상됨에 따라 인터넷의 TCP/IP 프로토콜을 기반으로 한 시스템이 주류를 이루고 있다[6]. 국내에서는 ETRI에서 ITU-T H.323 표준[1][2]의 MPEG4[3] 코덱을 이용한 시스템 등 다수의 시스템이 있으며, IETF 표준의 SIP(Session Initiation Protocol)를 기반으로 한 시스템으로는 국내 여러 대학과 회사 등에서 개발한 시스템이 있다[6].

국외에서는 Claremont 대학에서 개발한 의료용 진단과 치료를 위한 어플리케이션 시스템을 SIP를 기반으로 인터넷의 IP로 음성과 멀티미디어를 전달할 수 있도록 하였으며, MD5 Digest Hashing 메커니즘으로 인증기능을 제공하고, 클라이언트 버전인 CGUsip Client1.1은 데이터의 보안기능이 없으며, 데이터의 암호화는 통신상의 기밀성을 보장하고 메시지가 전송되는 동안 수정되지 않도록 하였다. 인증에 기반한 사용자 에이전트 CGUsipClientv1.1는 사용자 요청에 대한 처리가 필요한 정보인 사용자 이름과 패스워드를 등록서버에 전달하는 기능을 수행한다[10,11].

2.2 화상상담 시스템의 보안

화상상담시 전송되는 영상정보는 디지털화 된 패킷형태로 전달하며 패킷의 전달시 보안상 위험에 노출되어 있다. 디지털로 전송되는 영상과 음성정보는 내부나 외부 사용자로부터 스니핑(sniffing)이나 패킷의 캡처로 음성의 도청이나 영상정보의 복제를 통한 위장이나 미디어데이터 자체를 위·변조할 수 있기 때문에 보안이 필요하다[12]. 영상정보의 보안을 위해서는 영상정보 자체에 원래의 소유자가 아니면 식별하기 어려운 워터마킹(watermarking)을 삽입하거나, 영상신호를 채널로 부호화하여 스크램블 함으로써 채널의 암호를 모르면 왜곡된 형태의 이미지로 보일 수 있도록 하여 안전한 화상상담이 가능하도록 하는 방법이 있다[4,13]. 1:1 화상상담에서 보안을 적용할 경우 서버와 클라이언트에 인증 프로토콜을 설치하여 IPSec(Internet Protocol Security)이나 SSL(Secure Socket Layer), TLS (Transport Layer Security)와 같이 채널자체를 암호화하는 방법이 있다[8,9]. VoIP를 기반으로 한 SIP 표준의 화상상담 시스템에서 보안을 적용할 경우, 영상이나 음성정보는 공개키를 이용하여 암호화하고 개인

비밀키를 모르는 제3자가 중간에 네트워크를 침해하더라도 개인 비밀키를 모르면 내용을 알아보기 어렵게 하는 방법이 있다. 이밖에 웹서버나 화상상담서버, 미디어서버에 임의의 사용자 접근을 차단하기 위해 방화벽을 설치하거나 RSA(Rivest Shamir, and Adelman) 공개키 기반의 인증을 통해 사용자를 통제하는 방법이 있다[7].

2.3 키 관리

2.3.1 영상통신의 보안적 요소

화상상담 멤버간에 안전한 통신을 위한 보안적 요소로 다음과 같은 요구사항을 만족하여야 한다[14].

① 키 보안 - 화상상담과 관계없는 제3자는 키를 사용할 수 없어야 한다.

② 후방향 보안(backward secrecy) - 회의에 참여했던 참여자가 이전에 사용했던 키에 대한 부분집합에 관한 정보를 알 수 없어야 한다.

③ 전방향 보안(forward secrecy) - 회의에 참여하고자 하는 참여자가 앞으로 사용할 현재 키의 부분 집합에 관한 정보를 알 수 없어야 한다.

④ 키의 독립성(key independency) - 현재 키의 부분집합에 관한 정보를 알 수 없어야 한다.

2.3.2 키의 분배와 관리

영상통신에서 멤버간에 생성한 키를 안전하게 배포하기 위해서는 세션공유키는 키의 안전한 전달을 위해 중간노드와 단말까지 전달하는 경로의 길이를 최대한 짧게 할 필요가 있다[5][7]. 세션공유키는 키가 전달된 후에 즉시 폐기할 필요가 있으며 또 다른 전달경로를 거치게 하고 타임스탬프와 함께 보내며 같은 세션공유키는 반복하여 전달하지 않고 세션을 다시 설정하여 이전에 전달됐던 세션의 생명주기는 반복하지 않도록 한다[14].

III. 화상상담 인증 및 키 관리기법

3장에서는 2장에서 언급한 PKI 기반의 사용자 인증과 회의 참여자간의 키의 관리, 미디어데이터에 대한 암호화를 위한 제안내용을 기술하고자 한다. 본 논문에서 사용한 수식의 표기는 표.1과 같다.

표 1. 제안된 프로토콜의 표기
Table 1. protocol sign of proposed this paper

표 기	설 명
Certi	사용자 인증서(User Certificate)
Tokeni	토큰으로 id, Nonce, 일련번호(sequence number), 시간 값(time stamp)을 포함한다.
Sigi	사용자 전자서명(Signature)
Ssk	비밀 세션키(Secure Session Key)
K0	키(Group_Key)
H(Ssk)	세션키, 제어메시지(control message) 전송을 위한 일방향 해쉬 함수
Room_id	회의실 id
a, b, c	랜덤하게 생성된 값
g	생성자(generator)
p	자연수
pub	사용자의 공개키
pri	사용자의 개인키
ECApub(x)	CA의 공개키로 x를 암호화 한다.
DApri(x)	사용자 A의 개인키로 x를 복호화 한다.

3.1 키 트리에서 키 생성

본 논문에서 제안하는 키 트리를 이용한 키 관리 기법은 그림 1과 같이 키 트리를 2진트리로 구성하고 그룹에서 8개의 멤버에 대한 키들 간의 관계를 표현하고 있다.

회의 참여자간의 키의 생성은 Diffie-Hellman을 이용한 키 합의 프로토콜을 확장한 수식을 사용한다[7,14].

Diffie-Hellman 키 교환 알고리즘은 상대방에게 필요한 정보를 교환하여 공유 비밀키(shared secret)를 생성하며, 참여자간에 랜덤하게 생성한 값을 서로 공유하는 과정인 합의를 통해 공유된 비밀키를 생성하여 분배한다.

키의 생성과 관리를 위해 멤버노드는 단말노드로 지정하고, 원노드는 중간노드로 구성하며, 루트는 키로 지정한다. 멤버간에 생성된 키의 안전한 전송을 위해 멤버간에 고유한 비밀키의 교환을 통해 생성한 키는 키를 관리하는 중간노드를 지정한다.

그림 1에서 원에 있는 공유키는 두개의 멤버에 대해 개인이 랜덤하게 생성한 고유한 숫자를 교환하는 알고리즘에 의해 얻어지는 키로 구성되는데 멤버의 비밀키는 a_j, 중간노드는 공유키로 $K\{li, ri\}$ 쌍으로 왼쪽노드인 l과 오른쪽 노드인 r이 조합하여 공유키를 만들고 루트 키는 K_0로 그룹키 이다. 각 멤버는 공유키에 접근이 가능하고 이 공유키는 트리의 경로상에 있는 루트 노드에서부터 아래의 멤버들에게 전달된다.

반대로 멤버노드인 단말노드인 멤버 M1과 M2는 공유키 K1,2는 물론 세션공유키 GK_3을 알고 있으며, 부모노드인 $K_{1,4}$을 공유하여 키 K_0를 알 수 있게 된다. 그림 1과 같이 공유키를 생성하는 프로세스로부터 시작하여 모든 멤버들은 생성자 g와 큰 소수 p에 대한 값에 합의하여 공유키를 계산한다. 각 멤버 M_i는 a_i에 각각 해당되는 랜덤한 수를 선택한다. 만일 8명의 멤버가 트리에서 같은 키의 자 노드 M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8이 있을 때 각각 고유의 랜덤 수에 해당하는 비밀키 *a1, a2, a3, a4, a5, a6, a7, a8* 를 만들어 랜덤숫자를 멱승하여 다음과 같이 세션공유키와 키를 만든다.

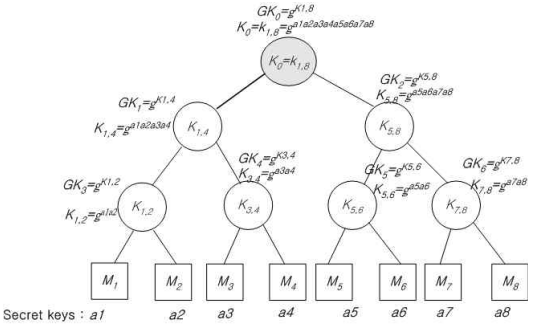

그림 1. 키 생성을 위한 2진트리 구조
Fig 1. Key creation based on binary tree

① M_1은 M_2에게 값 g^{a1}을 보내고, M_2는 M_1에게 값 g^{a2}를 서로 교환한다. g^{a1}과 g^{a2}는 중간노드인 공유키인 $K_{1,2}$ 에게 보내 조합하여 $K_{1,2} = g^{a1a2}$ 값을 구한다. $K_{1,2}$ 값을 생성자 g가 공유키 값을 한번 더 멱승하여 세션공유키를 만들어 GK_3으로 매핑하여 $GK_3 = g^{k1,2}$ 를 계산할 수 있으며, 세션 공유키는 GK_3는 키의 유출을 막기 위해 상위노드로 전송할 때만 사용하고 폐기한다.

② M_3는 M_4에게 값 ga3을 보내고, M_4는 M_3에게 값 ga4를 서로 교환한다. M_3과 M_4는 $K_{3,4}$에게 값 ga3와 ga4를 서로 교환하여 조합하여 $K_{3,4} = g^{a3a4}$ 값을 구한다. $K_{3,4}$는 세션공유키인 GK_4로 매핑하여 $GK_4 = g^{k3,4}$ 로 계산한다.

③ M_5는 M_6에게 값 g^{a5}을 보내고, M_6는 M_5에게 값 g^{a6}을 교환한다. M_5와 M6은 K5,6에게 값 ga5와 g^{a6}을 보내 조합하여 $K_{5,6} = g^{a5a6}$ 값을 구한다. $K_{5,6}$은 세션 공유키인 GK_5로 매핑하여 $GK_5 = g^{k5,6}$로 계산한다.

④ M_7은 M8에게 값 g^{a7}을 보내고, M_8는 M_7에게 값 g^{a8}을 교환한다. M_7과 M_8은 $K_{7,8}$에게 값 g^{a7}과 g^{a8}을 보내 조합하여 $K_{7,8} = g^{a7a8}$ 값을 구한다. $K_{7,8}$은 세션공유키인 GK_6로 매핑하여 $GK_6 = g^{k7,8}$로 계산한다.

⑤ 중간노드 $K_{1,2}$와 $K_{3,4}$는 각각의 값 g^{a1a2}와 g^{a3a4}을 상위노드인 $K_{1,4}$ 에게 보내 $K_{1,4} = g^{a1a2a3a4}$ 값을 구한다. $K_{1,4}$는 세션공유키인 GK1로 매핑하여 $GK_1 = g^{k1,4}$을 계산한다.

⑥ 중간노드 $K_{5,6}$과 $K_{7,8}$은 각각의 값 g^{a5a6}과 g^{a7a8}을 상위노드인 $K_{5,8}$에게 보내 $K_{5,8} = g^{a5a6a7a8}$결과를 구한다. $K_{5,8}$은 세션공유키인 GK_2로 매핑하여 $GK_2 = g^{k5,8}$ 로 계산한다.

⑦ 중간노드 $K_{1,4}$와 $K_{5,8}$은 각각의 값 $g^{a1a2a3a4}$과 $g^{a5a6a7a8}$을 상위노드인 $K_{1,8}$ 에게 보내 $K_{1,8} = g^{a1a2a3a4a5a6a7a8}$ 값을 구하여 $K_{1,8}$값을 그룹키인 GK_0로 매핑하여 $GK_0 = g^{k1,8}$을 계산한다. 그룹키인 GK_0는 그룹조정자에게 전달한다. 이 그룹키의 값은 그룹조정자 GC내에서 중간노드의 공유키와 개인비밀키, 멤버들 각각 고유한 식별번호를 보관하고 있다. $GK_0 = g^{k1,8} = K_0 = K_{1,8} = g^{k1,4}(g^{k5,8}) = g^{k1,2}(g^{k3,4})(g^{k5,6}(g^{k7,8})) = g^{a1a2a3a4}(g^{a5a6a7a8})$의 결과를 얻게 된다.

3.2 제안된 보안 화상상담 시스템 프로토콜

본 논문에서 제안한 화상상담 시스템에서 사용하는 모듈의 기능은 다음과 같다.

○ Control Daemon : 회의요청 메시지에 대해 사용하지 않는 회의실을 할당하기 위해 프로세스를 생성하는 기능을 한다.

○ Gateway Daemon : Control Deamon이 생성한 프로세스로부터 요청받은 회의실 관리 프로세스의 처리를 위해 데이터 교환을 위한 채널 설정과 회의실의 고유한 Room ID를 관리한다.

○ Gatekeeper Process : 요청 및 제어 세션 프로세스에 관한 에러가 발생할 경우 복구를 위한 처리와 프로세스 정보의 라우팅 기능을 수행한다.

○ MCU(Multilateral Control Unit) Daemon : 다수가 참여하는 화상상담에서 논리채널의 세션 제어정보와 멀티캐스트, 유니캐스트의 선택, 비디오 및 음성 코덱의 선택 등을 제어하고 관리하는 역할을 한다.

3.2.1 화상상담 신청

회의 주관자 MC(Master of Conference)가 화상상담을 위해 MCU에게 회의를 신청하는 경우의 트랜잭션은 그림 1과 같다. 본 논문에서는 화상상담 주관자나 참여자가 인증서를 획득하는 과정은 IKE나 SSL의 핸드쉐이크(handshake) 과정을 통해 안전하게 인증서를 획득한 것으로 한다.

3.2.2 화상상담 참여 신청 및 키의 생성

회의 주관자 MC가 다자간 회의를 위해 MCU로부터 회의실 번호를 할당받아 대기하고 있는 상태에서 참여자 B가 회의참여를 신청하는 경우의 트랜잭션은 그림 1과 같다.

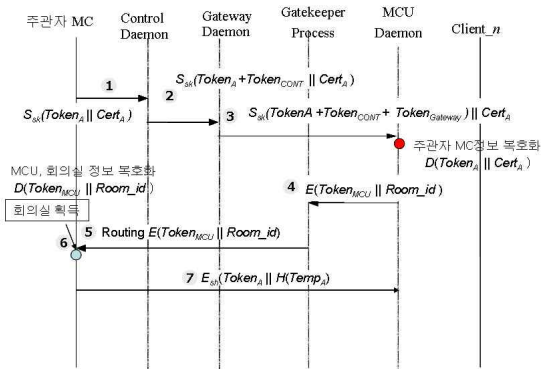

그림 1. MC가 회의를 신청할 때 트랜잭션
Fig 1. When MC request to transaction

① Client_B -> Control Daemon : $S_{sk}(Token_B \,||\, Cert_B)$

회의참여자 Client_B는 회의 참여를 신청하기 위해 자신의 인증서 $Cert_B$와 $Token_B$를 암호화해서 Control Daemon에게 보낸다.

② Control Daemon -> MCU Daemon :

$S_{sk}(Token_B + Token_{CONT} \,||\, Cert_B)$

Control Daemon은 회의 참여를 요청받고 회의실을 할당하기 위해 Client_B의 인증서 $Cert_B$와 $Token_{CONT}$, $Token_B$를 포함한 세션키를 암호화해서 MCU Daemon에게 보낸다.

③ MCU Daemon 은 세션 공유키와 그룹키 $K_0 = g^a \bmod p$ $(g^b \bmod p) \equiv g^{ab} \bmod p$ 를 만들고 회의실번호 Room_ID를 생성한다.

④ MCU Daemon -> Gatekeeper Process :

$E[H(S_{sk}(Token_{MCU} \,||\, K_0, Room\_id)]$

MCU Daemon은 $Room\_id$ 와 그룹키K_0, $Token_{MCU}$를 포함한 세션공유키를 일방향 해쉬로 처리하고 암호화해서 Gatekeeper Process에게 보낸다.

⑤ Gatekeeper Process -> MC :

$E[H(S_{sk}[(Token_{MCU} \,||\, K_0, Room\_id))]$

Gatekeeper Process는 회의실 주관자인 MC에게 $Token_{MCU}$와 그룹키K_0, $Room\_id$, $Token_{MCU}$를 포함한 세션공유키를 일방향 해쉬로 처리하고 암호화해서 Routing한다.

⑥ MC -> MCU : ACK $E_{sh}(Token_A \,||\, H(Temp_A)$

MC와 Client_B는 MCU에게 $Token_A$와 $Token_B$를 중간에 제3자가 개입하지 않았다는 것을 증명하기 위해 세션공유키 $E_{sh}(Token_A \,||\, H(Temp_A)$를 암호화하여 MCU에게 보내 안전한 화상상담을 진행한다.

⑦ Call Establishment : 제어정보를 암호화 하여 전송하는 절차인 Q.931, H.245의 호설정 절차가 끝난다.

Ⅳ. 제안된 키 관리시스템 분석 평가

본 논문에서는 제안한 키 관리기법에 의한 시스템을 구현하였다. 키 관리시스템은 인증서를 이용하여 화상상담에 참여하는 참여자의 인증서를 받아서 화상상담 참여자의 파라메타 값을 추출하여 3장에서 제안한 확장된 Diffie-Hellman 키 합의 프로토콜을 적용하였다. 이 키는 화상상담 참여자간에 암호화를 수행하기 위한 비밀키로 참여자간 키의 생성은 그룹 조정자가 담당하도록 하였으며, 키의 분배는 회의 참여자에게 IKE를 통해 안전하게 전달되도록 한다.

4.1 인증 및 키 관리 시스템

키의 생성은 그림 4와 같이 화상상담 참여자의 화면에서 자신의 파라메터 값을 생성하여 제어정보와 암호화하여 서버에게 보내면, 그림 5와 같이 서버는 참여자의 정보를 복호화하여 키를 만들게 되고 이 키를 안전한 세션 공유키를 이용하여 화상상담 참여자들에게 전달하게 된다.

이후에 화상상담 참여자가 그룹에서 탈퇴하게 될 때, 제어정보를 서버에 자신의 파라메터 값과 같이 보내게 되고 이 파라메터를 받은 서버는 키를 새로 갱신하여 다시 화상상담 참여자에게 세션공유키를 이용하여 배포하게 된다. 화상상담 참여자는 기밀성을 보장하기 위해 식별번호와 시간 값을 동시에 보내게 된다. 보안성을 높이기 위해 키의 크기는 최소 1024bit나 2048bit가 되도록 그룹에서의 파라메터 값 g와 p의 값을 128bit이상이 되도록 하였다.

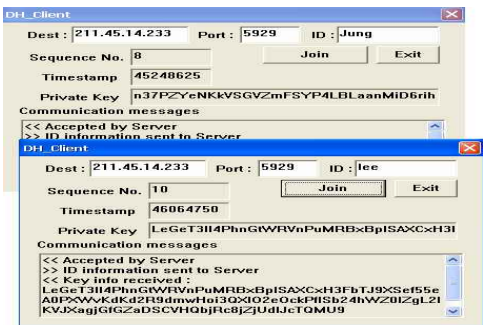

그림 4. 화상상담 참여자의 모니터 화면
Fig 4. Video conference client monitor

그림 5. 화상상담 서버의 모니터 화면
Fig 5. Video conference server monitor

본 논문에서 사용한 영상압축 코덱은 JPEG, MPEG4를 음성압축 코덱으로는 PCM 방식인 G723.1과 GSM을 사용하였고, 네트워크 평균 대역폭으로는 음성은 1.4kb, 영상은 4kb~2kb 기타 1kb로 전송 대역폭을 설정한 후 대역폭에 따라 영상 프레임의 대역폭을 조절하면서 데이터를 송신하도록 하였다.

그림 6은 그룹 멤버의 크기에 따른 키의 생성 수행시간을 그래프로 나타낸 것으로 멤버의 수가 많을수록 키를 만드는데 걸리는 시간이 많이 드는 것을 알 수 있다.

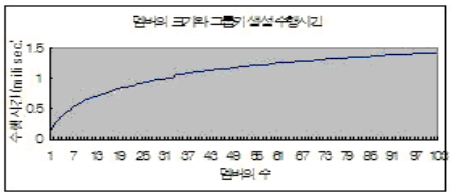

그림 6. 멤버의 크기와 키 생성 수행시간
Fig. 6. member size & key creation time

4.2 미디어 스트림의 암호/복호화

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. 그림 7의 경우에서는 RTSP(Real Time Stream Protocol) 프로토콜에 대해 헤더 부분을 제외한 페이로드 전체를 암호화함으로서 헤더정보만을 암호화하게 되면 제3자가 헤더를 복호화하여 데이터를 볼 수 있게 된다. RTP(Real Time Protocol) 프로토콜에 대해 헤더 부분을 제외한 24Byte 길이의 음성페이로드 전체를 32Byte 암호화 모듈을 이용하고 나머지 바이트는 패딩으로 처리한 결과는 그림8과 같다. 비밀키를 이용하여 암호화하고 나머지를 패딩으로 처리함으로서 헤더정보만을 암호화하게 되면 제3자가 헤더를 복호화하여 데이터를 볼 수 있게 된다. 하지만 헤더정보는 공개하고 페이로드 전체를 암호화하게 되면 제 3자가 헤더 정보로 페이로드를 복원할 수 없기 때문에 원래의 영상이나 음성을 복원 할 수 없게 된다.

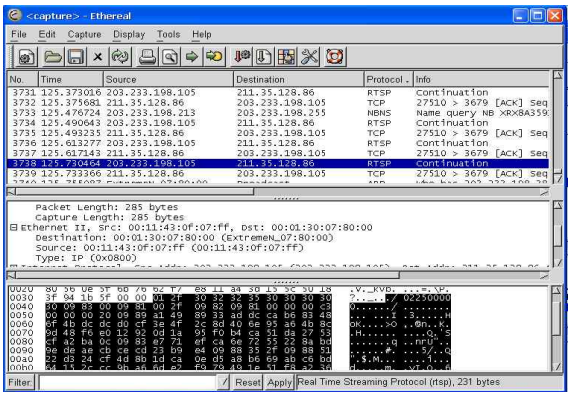

그림 7. 미디어스트림 암호화결과
Fig 7. data captured by media stream encryption

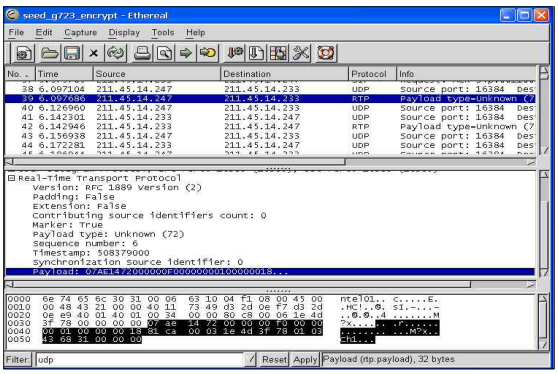

그림 8. 음성 암호화 결과
Fig 8. data captured by voice encryption

영상데이터의 암호화는 속도의 지연을 최소화하기 위해 MJPEG 코덱이나 정지영상인 JPEG 코덱을 사용함으로서 서비스가 가능하도록 하고, JPEG 코덱의 특성상 가변길이의 페이로드를 암호화하는데 드는 시간을 최소화 할 수 있게 된다.

4.3 영상 데이터 스트림의 암호화

그림 9는 본 논문에서 실험한 화상상담시스템의 구성도이며,

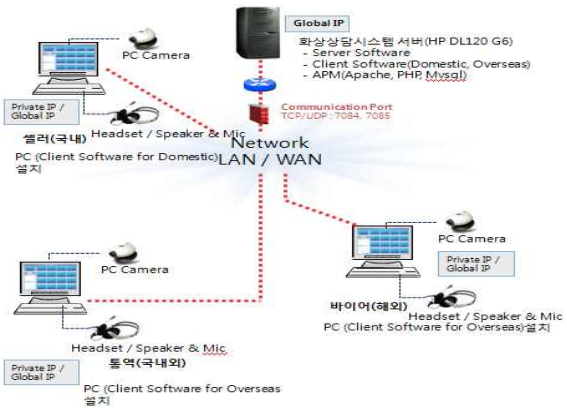

그림 9 화상상담시스템 구성도
Fig. 9. Video conference system configuration

그림 10은 화상상담에 정상적으로 로그인한 그림으로 각 사용자들 사이의 데이터는 암호화 통신을 통해, 영상과 음성이 전달된다. 그림 11은 암호화 통신을 스니핑하여 회의실 번호 및 ID를 해킹하여 획득함으로서 화상상담에 참여한 모습을 캡쳐한 모습을 실험하였다. 실험결과 비디오 및 오디오 데이터는 암호화 되어있는 상태로 정확한 키를 가지고 있지 않기 때문에 보거나 들을 수가 없음을 확인하였다.

그림 10. 정상적인 영상회의 모습
Fig. 10. normal video conference

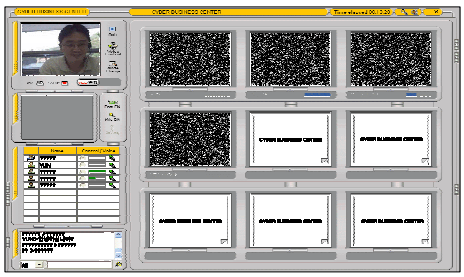

그림 11. 불법적인 접근을 통한 영상회의 참여 모습
Fig. 11. abnormal video conference

특히 영상데이터는 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 않기 때문에 이러한 방법은 불가능하다고 할 수 있다.

4.4 분석 및 비교 평가

본 논문에서 제안한 인증서를 기반으로 한 키 관리 시스템이 보안성이 높은 것으로 평가된다. 본 논문에서 제안한 시스템은 기존 화상상담 시스템과 비교 분석한 결과 첫째, 안전성 측면에서, 공개키를 이용한 인증서를 이용하고 매번 검증하기 때문에 키에 대한 노출과 사전공격에 안전하다. 둘째, 신뢰성 측면에서, 화상상담서버가 제3의 신뢰서버로서 자체 CA로 인증서를 기반으로 함으로 화상상담 참여자를 인증하고 검증함으로서 항상 신뢰할 수 있다.

표 2. 암호화에 대한 분석
Table 2. encryption analysis

비교 항목	A사	제안시스템
인증 방법	패스워드	인증서 기반
세션키의 노출 가능성	매우 높음	낮음
그룹 키의 노출 추적	불가능	가능
미디어 자체 암호화 방식	RTP payload header	RTP payload
적용 시스템	보안 영상회의	보안 영상회의

셋째, 가용성 측면에서, 미디어데이터의 암호화 지연시간을 최소화하기 위해 RTP 전송패킷의 길이를 가변적으로 하고 영상의 움직임이 발생할 때만 전송하여 미디어의 전송량을 최소화함으로서 상대적으로 가용성의 향상을 가져왔다고 할 수 있다. 넷째, 추적성 측면에서, PKI기반의 인증서를 사용함으로 키의 보관과 관리가 간단하여 키의 유출을 방지할 수 있고 키가 유출됐다고 의심되면, 키를 갱신함으로서 전방향 보안성과 후방향 보안성을 보장할 수 있다. 다섯째, 키관리 측면에서, IKE로 키를 교환하고 그룹조정자가 키를 관리하므로 키의 관리가 안전하고 간단하다.

V. 결 론

본 논문에서는 TCP/IP 기반의 네트워크를 이용하여 다수가 참여하는 화상상담에서 회의 참여자의 인증과 송수신 미디

어데이터의 암호화를 통해 보안성을 높인 프로토콜을 제안하였다.

본 논문에서는, 첫째, 다자간 화상상담에서 사용자의 접근을 확보하기 위한 방법으로 공개키 기반의 인증서를 이용하여 화상상담 참여자를 인증하는 프로토콜을 제안하였다. 둘째, 인증을 받은 화상상담 참여자가 그룹내에서 참여자간에 랜덤하게 생성된 고유한 비밀키를 조합하여 공유함으로서 공유키의 소유자끼리만 화상상담이 가능하도록 하였다. 그리고 세션 공유키의 안전한 전송을 위해 개인의 서명키와 제어정보의 전송시 생성되는 일련번호와 시간을 붙여 일방향 해쉬하고 암호화하여 전송하도록 하였다. 그 결과 제어정보를 받은 참여자가 원래의 제어정보를 전송한 참여자에게 검증을 요청함으로서 제어정보가 변조 되지 않도록 하였다. 셋째, 제어데이터와 미디어데이터의 안전한 전송을 위해 미디어데이터를 암호화하여 송신하고 수신할 때 복호화 하도록 하였다. 이때 사용하는 암호화 알고리즘으로는 미디어 전송지연의 영향을 최소화할 수 있는 대칭키 암호화 알고리즘인 DES, 3DES, RC5, SEED를 사용하였다. 음성과 영상 스트림 데이터의 전송시 많은 시간이 소요됨을 감안하여 G.723.1, GSM과 MPEG4, MJPEG 압축코덱을 선택하여 사용하여 화상상담 시스템의 가용성을 높이도록 하였다.

참고문헌

[1] ITU-T Online site *http://www.itu.int/rec/recomm-endation.asp?type=folders &lang=e&parent=T-REC -H.323*

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

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

[4] L.Lo Iacono and C.Ruland, "Confidential Multimedia Communication in IP Networks", Proceedings of 8th IEEE International Conference on Communication Systems, Singapore, 2002.

[5] M. Baugher, D.McGrew, D.Oran, R. Blom, E.Carrara, M,Naslund, and K.Norrman, "The Secure Real-time Transport Protocol", IETF RFC 3711, 2004.

[6] MHandley, H.Schulzrinne, E.Schooler, and J.Rosenberg, "SIP : Session Initiation Protocol", IETF RFC 3261, 2002.

[7] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik, "New Multiparty Authentication Services and Key Agreement Protocols". IEEE Journal on selected areas in communication, Vol. 18,No.4, April 2000.

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

[9] Radha Poovendran and John S.Baras, "An Information Theoretic Approach for Design and Analysis of Rooted Tree Based Multicast key Management Schemes", IEEE Transaction on Information Theory, Vol.47, No.7, November 2001.

[10] Richard J,Spillman, "Classical and Contemporary Cryptology", Pearson PrenticeHall, 2005.

[11] Sandra Rafaeli and David Hutchison, "A Survey of Key Management for Secure Group Commu nication" ACM Computing Surveys, Vol. 35, No.3, September 2003, pp.309-329.

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

[13] Yong-Deug Jung, Dae-Woo Park, and Moon-Seog Jun, "The Analysis of New Video Conference System for Secure Communications", GESTS International Trans-action on Computer Science and Engineering Volume 2, Number 1, March 2005.

[14] O.Rodeh, K.P.Birman, and D.Dolev, "Optimized Group Rekey for Group Communication Systems", Network and Distributed Systems Security, 2000.

저 자 소 개

정 용 득

2005. 12 : 숭실대학교 박사
1990. 8 : 숭실대학교 석사
1990.10~2010.9 현재 : KOTRA 재직중
2000.3~2001.8 : 성결대학교 겸임교수
2010.8 : 한세대학교 강의
성결대학교 강의