韓國 컴퓨터情報學會 論文誌
第10卷 第4號, 2005. 9.

2005-10-4-1-15

영상회의 시스템에서 멀티미디어 데이터 특성에 따른 보안 방법

한 군 희*

Security Method of Multimedia Data Characteristics on Video Conference System

Kun-Hee Han*

요 약

영상회의 시스템을 인터넷상에서 다양하게 사용하려는 시도가 이루어지고 있다. 이런 부분의 연구는 오디오, 비디오 압축 기법, 멀티미디어 데이터의 동기화, 다자간의 영상회의를 지원하기위한 IP multicast의 Mbone의 연구가 활발하게 이루어지고 있고, 통신의 회선속도가 고속화됨에 따라 인터넷에서 영상을 통한 다양한 멀티미디어 서비스가 이루어지고 있다. 개방형 분산 인터넷 통신망 환경에서의 영상회의는 영상회의 데이터인 영상 및 음성 보안에 대한 문제가 심각하게 대두된다. 본 논문에서는 영상회의에서 멀티미디어 데이터의 특성에 따른 보안 방법을 제시하고자 한다.

Abstract

Video conference system it is various at internet and uses the reading is become accomplished. Research of like this portion synchronization of audio, the compression technique and multimedia data, supports the video conference the research of the Mbone of the IP multicast for being active, being become accomplished the multimedia service which is various an video from internet, the line speed of communication becomes high-speed anger and to follow leads is become accomplished. The video conference from opening elder brother dispersion internet network environment the problem against the image which is an image conference data and a voice security is serious and it raises its head. To sleep it presents the security method which from the video conference it follows in quality of multimedia data from the dissertation which it sees and it does.

▸ Keyword : video conferencing, Authentication, IP multicast, private key

• 제1저자 : 한군희
• 접수일 : 2005.07.11, 심사완료일 : 2005.09.05
* 천안대학교 정보통신학부 교수

Ⅰ. 서 론

오디오, 비디오 기술의 발전으로 시공간을 초월한 영상 멀티미디어 데이터 전송이 원활해가고 있다. 이로 인한 데이터에 대한 무결성 보안에 대한 중요성이 확대되고 있다. 현재 전 세계는 하나의 거대한 시장을 형성하고 자국, 타국을 막론하고 활발한 거래 활동을 하고 있다. 막대한 비용과 시간이 필수적으로 요구되는 이러한 활동이 점차 증폭되면서, 원가절약의 측면에서 음성, 그래픽, 데이터 및 영상 등 모든 형태의 정보매체를 전송할 수 있는 영상회의(video conferencing)의 필요성 또한 지속적으로 요구되고 있는 실정이다. 예를 들어, 어떤 다국적 은행에서는 서울에 있는 고객과 싱가포르, 홍콩, 뉴욕, 런던 등의 매니저를 연결시켜 서비스를 제공할 수 있다. 만일 특정 지역의 매니저가 고객을 만나기 위해 여행을 하는 경우, 항공료나 호텔 요금 등의 여행경비뿐 아니라 시간도 소모하게 되므로, 이러한 접근 방법은 시간이나 비용을 비효율적으로 이용하는 전형적인 방법이다.

영상회의는 전 세계적인 상거래는 물론 교육, 진료, 공동작업, 원격지 감시 및 보안, 재택근무 등 무궁무진한 응용분야를 가지고 있어, 이에 필요한 소프트웨어와 하드웨어 등 관련 산업계에 미치는 파장이 매우 크다[2].

다양한 형태의 영상회의 중 컴퓨터와 개방형 네트워크를 이용한 "데스크 탑 영상회의 시스템"은 기존의 네트워크와 널리 보급되어 있는 개인용 컴퓨터를 이용하여 쉽게 이루어질 수 있는 반면, 개방형 네트워크상에서의 보안이 제공되지 못하여 이용자가 안심하고 사용할 수 없다는 한계가 있다.

본 논문에서는 개방형 네트워크상에서의 보안에 관한 취약성을 보완해주는 보안성을 제공하고, 통신 트래픽, 압축 및 복원 처리에 최소 부하를 주는 영상회의 보안 프레임워크를 제시한다. 2장에서는 영상회의에서의 보안 요구사항에 대해 설명하고, 3장에서는 보안 영상회의에 대한 전체 프레임워크와 영상회의 보안을 위한 인증 서비스를 다룬다. 4장에서는 보안 영상회의에서의 세션키 생성 프로토콜을 설명하며, 결론에서는 앞에서 제시한 프레임워크의 정당성 및 향후 해결점을 다룬다.

Ⅱ. 영상회의 보안 요구 특성

영상회의를 위한 멀티미디어 데이터의 보안을 위한 특성들이 필요하다. 영상회의의 안전성 보장을 위한 암·복호화 기능은 처리시간을 최소화하여 실시간 특성을 보장해야 한다. 암·복호화 하기 위한 모든 비밀키는 일회성을 가지며, 회의에 참가하는 사용자에게 그 세션동안 유효한 비밀키에 해당하는 세션키를 회의 개시자의 요구에 의해 시큐리티서버가 생성하며, 영상회의서버를 통해 회의자가 전달받도록 한다. 동일한 세션키를 사용하여 회의 참여자는 기밀성과 무결성을 제공받는다.

영상신호를 압축하는 복합적인 기법에서 영상회의시 송수신되는 모든 데이터는 암호화를 통하여 기밀성을 유지하여야 하지만 영상 데이터의 모든 프레임을 암·복호화 하는 것은 상당한 오버헤드를 가지므로 매 프레임 당 하나의 매크로블럭만을 암호화 하여 영상회의 시스템의 보안 요구사항을 충족시켜야 한다.

다자간의 영상회의는 하위통신프로토콜(Mbone)의 멀티캐스팅을 이용함으로써[4] 한번의 전송으로 안전한 채널을 확보하고 통신 트래픽을 최소화 하여야 한다[1]. 아래에서 영상회의 상의 최소 보안 요구사항을 제시한다.

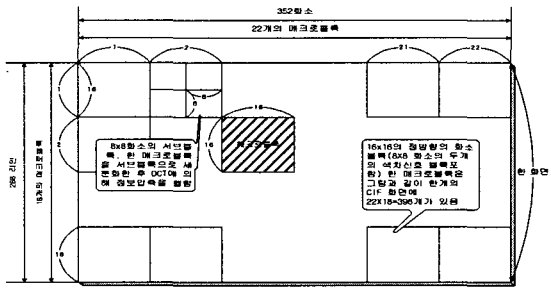

그림. 1 매크로 블록
Fig. 2 Macro Block

1. 인증(Authentication)으로 허가된 사람만이 허가된 영상회의에 참여할 수 있는 권한을 얻을 수 있어야 한다.

2. 기밀성(Confidentiality)으로 송신자가 수신자에게 전송한 멀티미디어 데이터가 도중에 다른 사람의 손에 들어간다 하더라도 내용의 노출을 막을 수 있어야 한다.
3. 무결성(Integrity)으로 송신한 멀티미디어 데이터의 내용과 수신된 메시지의 내용이 전송 도중에 불법적인 변경이 일어났는지를 알 수 있어야 한다.
4. 접근통제(Access Control)로 영상회의 자원에 대한 정당한 접근권한을 갖고 있는 사용자만이 영상회의에 참여하고, 회의 중에 불법적인 공격에 방해를 받지 않도록 접근통제가 가능하도록 해야 한다.

III. 보안을 위한 프레임워크

기밀성을 유지하기 위해 영상회의 당사자간에 하나의 공통된 세션키를 세션 확립시 안전하게 분배한다. 영상회의 개시자가 시큐리티서버에 영상회의를 개시할 목적으로 인증을 받고 나면, 키 분배 서버는 회의에 참여하는 모든 사용자에게 한 세션동안 사용할 세션키를 무작위로 생성한 후, 이것을 안전한 프로토콜 절차에 맞도록 사용자당 하나씩 토큰을 생성하여 영상회의서버에게 전달한다.

이때 정당한 회의 참여자는 영상회의서버에 접속하여 세션키를 부여 받고 회의가 진행되는 동안 이 세션키를 가지고 동영상, 음성, 공유 데이터 작업을 위한 화이트보드의 기밀성 및 무결성을 유지한다. 영상회의는 실시간으로 이루어져야 함으로 암·복호화하는 시간은 최소화하여야 한다.

공개키를 사용하는 경우 멀티캐스트(multicast) 시스템에서 모든 수신자에게 서로 다른 키를 사용하여 매 패킷마다 암·복호화가 각기 발생하고 실시간 적으로 들어오는 매 패킷을 구분하기 어려울 뿐더러 복호화하는 오버헤드 때문에 비대칭키는 다자간 실시간 시스템에서 사용이 비효율적이다[3].

따라서 RTP(Real-Time Transport Protocol)를 위한 보안은 사용자의 투명성과 처리속도 및 패킷의 오버헤드를 중요하게 고려해야 한다.[4] 사용되는 알고리즘 중 메시지 요약(MD5)과 DES는 음성 및 영상을 처리할 정도로 충분히 빠르게 수행하지만 전자서명을 위한 RSA의 처리속도가 상당히 느리다.

짧은 음성 데이터는 상당한 오버헤드를 가지게 된다. 따라서 패킷 손실율이 적은 경우 여러 패킷을 모아서 하나의 MD5로 적용하는 것이 효율적이다. 안전한 영상회의 시나리오를 구성하면 아래 (그림 2)와 같다.

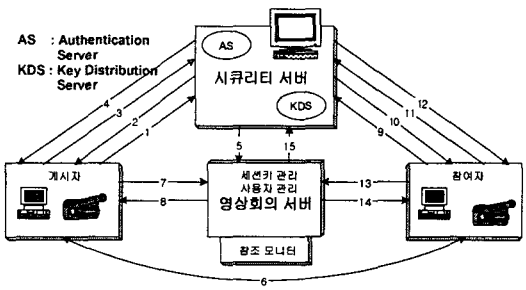

그림 2. 안전한 영상회의 시나리오
Fig. 2 Safe Video conferencing Scenario

① 개시자는 영상회의 진행을 맡고 있는 사용자를 의미하며 최우선적으로 인증을 받기 위해 자신의ID로 시큐리티서버내의 인증서버에게 인증을 요청한다.

② 인증서버는 난수를 발생하여 개시자에게 시도(challange)로 요청한다.

③ 개시자는 자신의 ID와 참여자 ID 목록을 시큐리티서버와 개시자의 대칭키로 암호화하여 시큐리티서버에 전달한다.

④ 인증절차가 정당하게 이루어지면 시큐리티서버의 비밀키(private key)로 개시자 ID와 유효기간을 서명하여 개시자에게 인증서를 전달한다.

⑤ 시큐리티서버는 개시자 ID 및 모든 참여자 ID에 대한 세션키를 위한 토큰을 생성하여 영상회의서버에게 전달한다. 인터넷 환경의 다중 도메인 경우의 다자간 회의인 경우에도 시큐리티서버 사이에 인증당국을 통한 공개키 메커니즘이 적용되어 안전한 채널이 확보가 된다.

⑥ 개시자는 영상회의 참여요구를 참여자에게 호출한다.

⑦ 개시자 클라이언트는 자신의 ID 및 시큐리티서버에서 수신한 인증서를 영상회의로 전달하여 세션키를 요청한다.

⑧ 영상회의서버는 요청한 세션키를 시큐리티서버 공개키로 암호화 하고 무결성을 위해 개시자 ID 및 세션키를 해쉬한 서명 값을 개시자에게 전달한다.

⑨ 참여자 인증을 위한 절차는 ①과 동일하다.

⑩ 참여자 인증을 위한 절차는 ②와 동일하다.

⑪ 참여자는 개시자 ID와 자신의 ID를 시큐리티서버 B와 참여자의 대칭키로 암호화하여 전달한다.

⑫ 인증절차가 정당하게 이루어지면, 시큐리티서버 B의 비밀키로 참여자 ID와 유효기간을 서명하여 참여자에게 인증서를 전달한다.

⑬ 참여자 클라이언트는 자신의ID와 ⑫에서 수신한 인증서를 영상회의서버로 세션키를 요청한다.

⑭ 영상회의서버는 요청한 세션키를 시큐리티서버의 공개키로 암호화하고 무결성을 위해 참여자 ID 및 세션키를 해쉬한 서명 값을 참여자에게 전달한다. 위 절차 후 안전한 채널을 확보한 영상회의가 시작되고, 종료된다.

⑮ 영상회의가 종료되면 확보된 모든 키를 영상회의에서 삭제되고, 영상회의 종료 사실을 시큐리티 서버에 전달한다.

인증을 위한 개시자 및 참여자 절차인 〔단계 1〕, 〔단계 2〕는 3.1절의 메커니즘에 의해 내부적으로 이루어진다. 영상회의서버는 사용자의 세션관리, 세션키 생성을 위한 토큰을 관리한다. 만약 시큐리티서버에게 인증 받지 않은 사용자나 영상 서버에 확인절차를 갖지 않은 사용자가 세션키 정보를 탈취하여 공격하더라도 세션키 정보를 해독할 수 없으므로 다자간에 안전한 채널을 가지게 된다.

3.1 인증 서비스

영상회의에서 인증은 회의를 시작하기 전에 가장 먼저 이루어져야 하는 것으로, 침입자를 자신의 영상회의 시스템 영역으로부터 일차적으로 차단할 수 있도록 해주는 것이다.

본 논문에서는 구현이 용이하고 다자간 영상회의 참여자 모두를 하나의 그룹으로 인증 할 수 있기 때문에 시도-응답(Challenge-response) 방식을 인증 메커니즘으로 사용하고 있지만 다른 어떤 방식을 쓰더라도 응용 서비스에 영향을 미치지 않도록 독립성을 유지하였다. 지능형 토큰은 하드웨어나 소프트웨어로 실현할 수 있다.

본 논문에서는 추가적인 비용을 가지지만 암호화 알고리즘의 고속 수행과 마스터키 같은 기밀정보의 안전함을 장점으로 가지는 스마트카드를 통한 하드웨어 구현 방법을 적용한다.

인증의 핵심 기술인 인증 프로토콜은 다음과 같다.

① 클라이언트는 시큐리티서버에게 사용자의 이름을 담은 인증 요구를 전달한다.

② 시큐리티서버는 난수를 발생하여 클라이언트에 시도(Challenge)로 전달한다.

③ 시큐리티서버는 사용자의 이름을 이용하여 데이터베이스에서 비밀 키를 꺼내 클라이언트의 난수를 암호화하기 시작한다.

④ 클라이언트는 DES와 비밀키를 이용하여 난수를 암호화하고, 그것을 서버에게 시도에 대한 응답으로 전달한다.

⑤ 서버는 암호화된 두 난수를 비교하여 일치하면 사용자의 정당함을 인정한다.

Ⅳ. 세션키 생성 프로토콜

본 장에서는 영상회의 보안 서비스에 세션키를 제공하기 위한 세션키 생성과 관리를 위한 방안을 제시한다.

영상회의 보안 시스템이 작동되면서 사전에 알고 있어야 하는 키는 동일한 도메인에서 키분배 서버(KDS)와 사용자 간에 대칭키를 소유하고 있어야 한다. 또한 각 시큐리티 도메인의 키분배서버들은 자신의 비밀키를 가지고 있고 이에 대응되는 공개키는 신임장 관리자에게 넘겨져 보증 되어져야 한다.

위와 같이 작동 준비가 되어져 있는 상태에서 제일 먼저 클라이언트는 키분배 서버에게 키를 요구하는 단계가 이루어진다. 이 프로토콜에서 수행되는 일들은, 첫째로, 클라이언트는 하부 메커니즘에게 서비스 받고자 하는 영상회의서버와의 안전한 통신을 위한 세션키를 요구한다. 둘째로, 하부 메커니즘은 영상회의서버와의 안전한 통신에 필요한 대칭키(클라이언트와 영상회의 서버 사이)를 생성하기 위해 기반이 되는 기본키를 키분배 서버에게 요청한다. 안전한 세션키 분배에 사용되는 프로토콜의 데이터는 아래와 같다. 인증절차 〔단계 1〕와 〔단계 4〕에서 4회의 통신 트래픽은 2회의 단계로 함축적인 방법도 가능하다.

〔단계1〕 인증절차(개시자)

① ID개시자

② R : Random Number

③ {R, ID개시자, ID참가자 list}K시큐리티서버A,개시자

④ 〔ID개시자, 유효기간〕K시큐리티서버Apri

〔단계 2〕 세션키 분배를 위한 토큰 생생 및 분배

⑤ ID개시자, {세션키}K시큐리티서버Apub, 〔H(ID개시자, 세션키)〕K시큐리티서버Apri ID참여자, {세션키}K시큐리티서버Bpub, 〔H(ID참여자, 세션키)〕K시큐리티서버Apri

⑥ 영상회의 참여요구 메시지 호출

〔단계 3〕 개시자가 영상회의 서버로부터 세션키를 얻어온다

⑦ ID개시자, 〔ID개시자, 유효기간〕K시큐리티서버Apri

⑧ ID개시자, {세션키}K시큐리티서버Apub, 〔H(ID개시자, 세션키)〕K시큐리티서버Apri

〔단계 4〕 인증절차(참여자)

⑨ ID참여자

⑩ R : Random Number

⑪ {R, ID개시자, ID참여자}K시큐리티서버B,참여자

⑫ 〔ID참여자, 유효기간〕K시큐리티서버Bpri

〔단계 5〕 참여자가 영상회의 서버로부터 세션키를 얻어온다

⑬ ID참여자, 〔ID참여자, 유효기간〕K시큐리티서버Bpri

⑭ ID참여자, {세션키}K시큐리티서버Bpub, 〔H(ID참여자, 세션키)〕K시큐리티서버Apri

⑮ 영상회의 종료 전달

단일 도메인의 경우 시큐리티서버 A는 시큐리티서버 B와 같으며, 다중 도메인의 경우 시큐리티서버 A는 시큐리티서버 B와 다른 서버가 된다. 다중 도메인일 때 인증당국(CA)을 통하여 안전한 채널이 유지된다.

V. 결론

본 논문에서 제시한 안전한 영상회의 시스템의 요구조건은 다음과 같은 보안 서비스를 만족하는 영상회의 시스템이 된다.

- **인증(Authentication)**
  스마트카드와 시도-응답(Challenge-response) 방식의 인증을 통하여 인증서비스를 제공함으로써 만족된다.
- **기밀성(Confidentiality)**
  랜덤하게 발생된 세션키로 DES 알고리즘을 이용하여 암호화함으로 만족된다.
- **무결성(Integrity)**
  MD5를 이용하여 메시지 요약문을 비교하므로써 가능하다.
- **접근통제(Access Control)**
  영상회의서버에서 영상회의 참여자가 정당한지를 참조 모니터를 통하여 접근통제를 하기 때문에, 인증을 받지 않고는 영상회의서버로부터 정보를 제공하지 못한다. 따라서 불법적인 공격자가 불법적으로 정보를 제공 받을 수 없다.

본 논문에서 제안된 영상회의 시스템은 위에서 요구되는 모든 보안 서비스를 만족함으로써 안전한 영상회의 시스템을 구축하여 개방된 인터넷 통신망 환경에서도 안전하다.

그러나 영상을 전송하는 과정에서 송신단에서 한 프레임 내의 매크로 블럭만을 암호화하는 것과 수신단에서 복호화하는 과정의 영상 에러를 어느 정도까지 허용하면서 무결성 및 기밀성을 지원할 것인가에 대한 기준이 제시된 예는 아직 없는 실정이다.

본 논문에서는 암·복호화하는 과정이 송신자측에서는 프레임당 하나의 매크로 블록을 암호화하지만, 수신자측에서는 시작점에서 비트 스트림 형태의 데이터를 매 프레임 내에 암호화된 임의의 매크로 블럭을 구분하기가 어려운 단점이 있다.

앞으로 이런 부분이 안전한 "데스크 탑형 영상회의 시스템"이 되기 위해서 연구 되어야 할 부분이다.

참고문헌

[1] David D. Clark, "Supporting Real-Time Applications in an Integrated Services Packet Network," ACM Multimedia, Nov. 1996.

[2] H. Schulzrunne, "Issues in Designing a Transport Protocol for Audio and Video Conferences and other Multiparticipant Real-Time Applications," Internet Draft, Audio-Video Transport Working Group, Oct. 1993.

[3] ITU-T Recommendation H.261

[4] Steven McCanne, Van Jacobson, "VIC: A Flexible Framework for Packet Video," ACM Multimedia, Nov. 1995.

[5] 신승수, 한군희, "CDN에서 패스워드를 이용한 키 교환 프로토콜", 한국컴퓨터정보학회 논문지,제10권 제3호, pp. 133-141, 2005. 7

[6] 장경옥, 구항욱, 오창석, "패킷 분석을 이용한 내부인 불법 질의 탐지", 한국컴퓨터정보학회 논문지, 제10권 제3호, pp. 259-265, 2005. 7

저 자 소 개

한 군 희

현재 천안대학교 정보통신학부 교수

〈관심분야〉 인터넷 보안, 영상 신호 처리