H.235 프로토콜에 의한 영상회의의 인증과 암호화 구현

심 규 복[†] · 이 건 배[††] · 성 동 수[†††]

요 약

본 논문에서는 영상회의 시스템에서의 사용자 인증 및 미디어 스트림의 암호화를 지원하기 위한 H.235 프로토콜의 구현에 대하여 기술한다. H.235 프로토콜은 ITU-T에서 권고된 H.323 영상회의의 보안 프로토콜로써 불법적인 공격자에 의한 도청 및 조작 방지를 위한 프로토콜이다. 본 논문의 구현에서는 패스워드 기반의 대칭키 암호 인증 방법을 사용하고, Diffie-Hellman 키 분배 알고리즘과 대칭키 암호 알고리즘인 RC2, DES, Triple-DES를 사용하여 미디어 스트림의 암호화를 구현한다. 또한, 추후의 확장성을 고려하여 차세대 표준 암호인 128비트 AES와 한국형 암호인 128비트 SEED를 포함시켜 구현한다. 구현된 인증 방법과 미디어 스트림의 암호화는 네트워크 상에서 개인적인 정보를 노출시키지 않으면서 터미널의 사용자를 확인하는 것이 가능하고, 영상회의의 기밀성을 유지시켜줌을 알 수 있다. 또한, 미디어 스트림의 암호/복호화를 지원해 주면서도 암호화에 따른 지연시간과 메모리가 증가하지 않음으로써 영상회의 시스템의 성능을 저하시키지 않음을 알 수 있다.

An Implementation of Authentication and Encryption of Multimedia Conference using H.235 Protocol

Gyu-Bok Sim[†] · Keon-Bae Lee[††] · Dong-Su Seong[†††]

ABSTRACT

This paper describes the implementation of H.235 protocol for authentication and media stream encryption of multimedia conference systems. H.235 protocol is recommended by ITU-T for H.323 multimedia conference security protocol to prevent from being eavesdropped and modified by an illegal attacker. The implementation in this paper has used password-based with symmetric encryption authentication. Media streams are encrypted using the Diffie-Hellman key exchange algorithm and symmetric encryption algorithms such as RC2, DES and Triple-DES. Also, 128-bit Advanced Encryption Standard and 128-bit Korean standard SEED algorithms are implemented for the future extension. The implemented authentication and media stream encryption has shown that it is possible to identify terminal users without exposing personal information on networks and to preserve security of multimedia conference. Also, encryption delay time and used memory are not increased even though supporting media stream encryption/decryption, thus the performance of multimedia conference system has not deteriorated.

키워드 : H.235 보안 프로토콜(security protocol), H.323 영상회의(multimedia conference), 인증(authentication), 암호 알고리즘(encryption algorithm), 대칭키(symmetric key)

1. 서 론

정보화 사회에 살고있는 우리는 급속하게 발전하는 컴퓨터와 통신기술에 의존하여 정보를 교류하고 있다. 인터넷을 통한 정보 교류는 물론이고, 금융 서비스, 전자 상거래, 국가의 중요 정보 교류가 다양한 형태의 컴퓨터 네트워크와 통신 수단을 이용하여 이루어지고 있으며, 앞으로도 정보교류에서 컴퓨터 및 통신 기술의 의존도는 더욱 높아질 것이다. 이러한 장점에도 불구하고, 날로 증가하는 불법적인 도청이나 해킹 등에 대한 문제점과 우려가 증가하는 것이 현실이다. 따라서, 최근 보안을 유지하기 위한 노력이 활발하게 전개되고 있으며, 안전한 정보 교류 기능을 제공하는 정보 보호 기술은 매우 중요한 과제로 대두되고 있다.

정보통신의 발달과 함께 영상회의는 중요 정보통신 응용들 가운데 하나이며, 이러한 영상회의 표준안은 크게 ITU-T(International Telecommunication Union Telecommunication Standardization Sector) 및 IETF를 중심으로 이루어지고 있다. 그 중 H.323[1]은 ITU-T에서 제안된 영상회의 표준안으로써 QoS가 보장되지 않는 인터넷망에서 운용되는 프로토콜이며, 차세대 이동 통신인 IMT2000에서도 사용될 현재 가장 각광 받는 영상회의 프로토콜 중 하나이다. H.323의 내부구성은 호 설정에 관련하는 H.225[2], 각종 제어신호를 주고받는 H.245[3], 비디오 코덱과 오디오 코덱으로 구성되어 있다. 이러한 H.323을 근간으로 하는 영상회의 시스템은 마이크로소프트사의 Netmeeting을 비롯하여 많은

† 준 회 원 : (주)디지탈미디어테크 연구원
†† 정 회 원 : 경기대학교 전자공학전공 교수
††† 종신회원 : 경기대학교 전자공학전공 교수
논문접수 : 2002년 2월 25일, 심사완료 : 2002년 4월 8일

제품들이 개발되어 이용되고 있다.

이러한 제품들의 단점중의 하나가 보안이 취약하다는 점이며, 이는 특정 분야에서 이의 사용을 꺼리는 이유 중의 하나이다. 또한, H.323은 인터넷에서 이용되는 영상회의 표준안이며, 이로 인하여 회선망을 이용하는 영상회의보다 보안이 더 더욱 취약하다. 특히, 보안이 중요시되는 국방 및 기업 등에서는 H.323의 사용을 꺼리는 이유 중의 하나일 것이다. 이러한 시점에서 ITU-T에서는 영상회의 표준안 H.323에서 사용되는 보안 프로토콜로써 H.235 프로토콜[4]을 권고하였다. 초기의 H.235 표준안은 많은 문제점들을 포함하고 있었으나, 최근에 발표된 표준안은 그 문제점들을 대부분 해결하였고, 각 연구소 및 업계에서는 이의 구현을 위하여 노력하고 있다. 이의 중요성을 인식하여, 본 논문에서는 H.235 표준안을 분석하고 구현한 뒤, 기존에 개발된 H.323 영상회의 시스템에 이를 추가한다.

H.235 프로토콜은 영상회의에서 가능성이 있는 불법적인 공격에 대한 방어를 위하여 대칭키 암호 알고리즘인 RC2[5], DES[6], Triple-DES[7]을 사용하고, 해쉬함수인 SHA(Secure Hash Algorithm), MD5(Message Digest Algorithm)와 여러 가지 메시지 필드의 사용을 권고하고 있다. 또한, 정당한 사용자임을 확인하기 위하여 다양한 인증 방법과 그에 따른 미디어 스트림의 암호화 방법을 권고하고 있다[4].

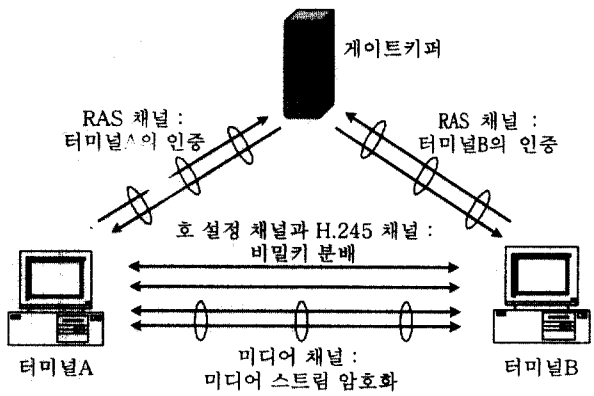
본 논문에서는 H.235 프로토콜에 기반하여 H.323 영상회의 시스템에서의 사용자 인증 및 비디오, 오디오 신호와 같은 미디어 스트림의 암호/복호화를 구현한다. 정당한 사용자의 인증을 위해 H.235 프로토콜의 패스워드 기반의 대칭키 암호(password-based with symmetric encryption) 인증 방법을 사용하고, Diffie-Hellman 키 분배 알고리즘[8], RC2, DES, Triple-DES와 같은 대칭키 암호 알고리즘을 사용한 미디어 스트림의 암호/복호화를 구현한다. 또한, 추후의 확장성을 고려하여 차세대 표준암호로 선정된 AES(Advanced Encryption Standard) 알고리즘인 128비트 Rijndael 암호 알고리즘[9]과 한국형 암호인 128비트 SEED 알고리즘[10]을 적용하여 미디어 스트림의 암호/복호화를 구현한다. 특히, 한국형 암호 알고리즘을 H.235에 처음으로 추가하여, 선택 가능한 암호화의 범위를 넓혔다는 점이 본 논문의 특징 중의 하나이다.

본 논문에서 구현된 H.235 프로토콜을 H.323 영상회의 시스템 내에서 동작시켜 본 결과, 게이트키퍼(gatekeeper)를 통하여 정확한 사용자 인증이 가능하다. 또한, 여러 가지 암호 알고리즘을 사용하여 미디어 스트림의 암호화를 수행한 결과, 보안성을 확보하는 암호/복호화 과정을 거치면서도 암호화를 적용하지 않는 경우와 비교하여 미디어 스트림 패킷의 전달 지연 속도에 영향을 미치지 않음을 알 수 있으며, 메모리의 사용량도 크게 증가하지 않음을 알 수 있다. 따라서, 인증 및 암호/복호화 기능의 추가에도 불구하고 영상회의의 성능이 저하되지 않는 결과를 보여준다.

2. H.235 프로토콜

2.1 H.235 프로토콜과 H.323 프로토콜의 상호 관계

H.323 영상회의 시스템 내에서 H.235 프로토콜이 관여하는 부분으로는 터미널과 게이트키퍼 사이에 교환되는 RAS(Registration, Admission, Status) 메시지, 터미널과 터미널 사이에 교환되는 H.225.0 메시지와 H.245 메시지, 그리고 영상회의를 위해 교환되는 오디오, 비디오 데이터들이다. H.323 영상회의 시스템과 H.235 프로토콜의 동작간의 관계는 H.323 영상회의 시스템은 RAS 채널, 호 설정 채널, H.245 채널, 미디어 채널들을 통하여 영상회의를 수행한다. 이때, H.235 프로토콜은 RAS 채널을 통해서 게이트키퍼에 의해 정당한 사용자를 인증하고, 호 설정 채널과 H.245 채널을 통해서 미디어 스트림을 암호화 할 비밀키를 분배한다. 이렇게 분배된 비밀키를 사용하여 미디어 채널을 통해 교환되는 오디오와 비디오 데이터를 암호화하게 된다. (그림 1)은 H.323 영상회의 시스템 내에서의 H.235 프로토콜의 동작을 보여준다.



(그림 1) H.323 영상회의 시스템에서 H.235 프로토콜의 동작

2.2 H.235 프로토콜의 구성

H.235 프로토콜의 전체적인 구성은 사용자 인증과 미디어 스트림의 암호화 과정으로 구성된다.

인증이란 일반적으로 메시지 인증, 사용자 인증 및 이러한 기능을 합친 디지털 서명 등으로 분류할 수 있다. 메시지 인증은 정보가 변경되지 않고 본래의 정보 그대로임을 보증하는 기능이고, 사용자 인증은 정보 시스템에서 정보의 생성, 전송, 처리, 기억, 판단 등의 행위에 관여한 사용자가 바로 정당한 사용자임을 보증하는 기능이다[11]. H.235 프로토콜에서는 모든 인증들을 지원하기 위하여 여러 가지 인증 방법을 권고하고 있다. 즉, H.235 프로토콜에서는 단방향 인증과 양방향 인증을 제공하며, 사용되는 인증 방법으로는 사전에 어떠한 과정을 거쳐 공유된 사용자의 정보를 이용하는 subscription 기반의 인증 방법과 사전 과정 없이 Diffie-Hellman 키 분배 알고리즘을 사용하는 인증 방

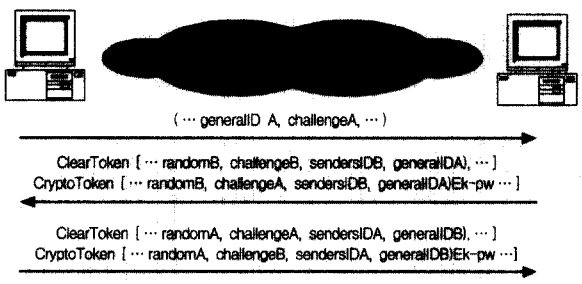
법이 권고되고 있다. 이외에도 별개의 프로토콜인 IPSec(Internet Protocol Security)[12], 또는 TLS(Transport Layer Security)[13]을 사용하는 방법도 가능하다.

Diffie-Hellman 키 분배 알고리즘을 사용하는 인증 방법은 교환되는 메시지 필드에 Diffie-Hellman 파라미터를 포함시켜 교환함으로써 각각의 터미널은 공통된 키를 생성할 수 있다. 이렇게 생성된 키는 다음에 교환되는 메시지를 암호화하는데 사용되며, 생성된 암호문은 상대방이 정당한 사용자임을 인증하는데 사용된다.

Subscription 기반의 인증 방법에는 패스워드 기반의 대칭키 암호 인증, 해쉬함수를 적용한 인증, 디지털 서명을 이용한 인증의 3가지 인증 방법이 있다. 패스워드 기반의 대칭키 암호 인증은 사전에 공유된 패스워드와 대칭키 암호 알고리즘을 사용하여 사용자를 인증하는 방법이다. 해쉬함수를 적용한 인증은 패스워드를 사용한 인증 방법과 동일하게 동작하며, 단지 다른 점은 교환되는 인증 필드가 해쉬 알고리즘에 의해 생성된다는 것이다. 디지털 서명을 사용한 인증은 교환되는 인증 필드가 디지털 서명과 인증서를 포함할 뿐 다른 인증방법과 동일하게 동작한다.

본 논문에서는 subscription 기반의 인증 방법 중 하나인 패스워드 기반의 대칭키 암호 인증 방법을 사용하여 게이트키퍼를 통하여 사용자를 인증하는 방법을 구현한다.

패스워드 기반의 대칭키 암호 인증 방법은 사전에 공유된 패스워드와 대칭키 암호 알고리즘을 사용하여 사용자를 인증하는 방법이다. (그림 2)는 패스워드 기반의 대칭키 암호 인증 방법을 보여준다. 먼저 인증될 터미널은 공유된 패스워드를 사용하여 정해진 메시지 필드를 암호화한다. 이렇게 암호화된 필드는 인증을 수행할 터미널에게 전송되고, 상대방이 정당한 사용자임을 인증하는데 사용된다[4].



(그림 2) 패스워드 기반의 대칭키 암호 인증 방법

미디어 스트림의 암호화는 각각의 터미널이 공통된 비밀키를 공유한 상태에서 대칭키 암호 알고리즘을 사용하여 수행된다. 미디어 스트림의 암호화를 위한 비밀키는 H.323 영상회의 시스템의 동작 과정에서 H.245 채널을 통해 마스터에 의해 회의 참석자에게 분배된다. 또한, 보안성을 향상하기 위해 비밀키는 일정 시간에 한번 씩 갱신되고, IPSec 또는 TLS 프로토콜을 사용하지 않는 방식에서는 비밀키가 노출되는 것을 방지하기 위해 Diffie-Hellman 키 분배 알고리즘에 의해 생성된 키를 사용하여 암호화되어진다[4]. 이렇게 분배된 비밀키는 H.323 영상회의 시스템에서 사용되는 미디어 스트림 즉, 오디오와 비디오 데이터를 권고된 RC2, DES, Triple-DES 대칭키 암호 알고리즘을 사용하여 암호/복호화함으로써 영상회의 내용의 기밀성을 유지시켜준다.

3. H.323 영상회의에서의 사용자 인증 및 암호화 구현

3.1 구현된 H.235 프로토콜의 구성

본 논문에서 구현된 H.235 프로토콜의 구성은 크게 사용자 인증과 미디어 스트림의 암호화로 구성된다. 인증 과정에서는 패스워드 기반의 대칭키 암호 인증 방법을 사용하여 게이트키퍼를 통해 단방향 인증을 수행하며, 미디어 스트림의 암호/복호화 과정에서는 H.235 프로토콜에서 권고된 RC2, DES, Triple-DES 대칭키 암호 알고리즘과 키 분배에 사용되는 Diffie-Hellman 키 분배 알고리즘을 사용한다. 또한, 암호/복호화의 보안성을 향상시키기 위해 128비트 차세대 표준 암호인 AES와 한국형 암호인 128비트 SEED 알고리즘을 적용하여 구현한다. <표 1>은 본 논문에서 구현된 H.235 프로토콜의 구성을 나타낸다.

〈표 1〉 구현된 H.235 프로토콜의 구성

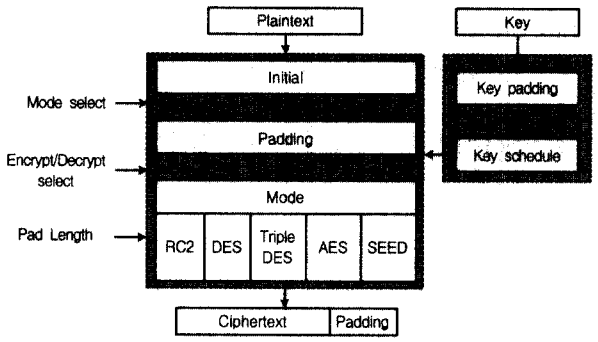
Security Service	RAS	H.225.0 Call	H.245	RTP
인 증	Password-based symmetric encryption			
기밀성	RC2, DES, Triple-DES, AES, SEED		RC2, DES Triple-DES, AES, SEED	RC2, DES, Triple-DES, AES, SEED
비밀키 발생		Diffie-Hellman		
사용되는 비밀키	Subscription based password		Diffie-Hellman에 의해 생성된 키	분배된 비밀키

3.2 암호 알고리즘의 구현

3.2.1 대칭키 암호 알고리즘의 구현

H.235 프로토콜에서 대칭키 암호 알고리즘은 패스워드 기반의 대칭키 암호 인증과 미디어 스트림의 암호화를 위해 사용된다. 미디어 스트림을 위한 대칭키 암호 알고리즘의 구현은 처리속도도 중요하지만 영상회의의 기능에 영향을 미치지 않아야 한다. 즉, 컴퓨터 시스템이 오디오 및 비디오 데이터의 처리를 수행하는데 영향을 주지 않아야 한다. H.235 프로토콜에서 기본적으로 권고한 암호 알고리즘은 64비트 암호 알고리즘인 RC2, DES, Triple-DES를 사용한다. 본 논문에서는 기밀성을 향상시키고, 추후에 추가될 확장성을 고려하여 차세대 표준 암호인 128비트 AES의 처리가 가능하게 구현하고, 한국형 암호인 128비트 SEED 암

호 알고리즘을 추가하여 구현한다. (그림 3)은 본 논문에서 구현된 각각의 대칭키 암호 알고리즘의 전체적인 블록도를 보여준다.

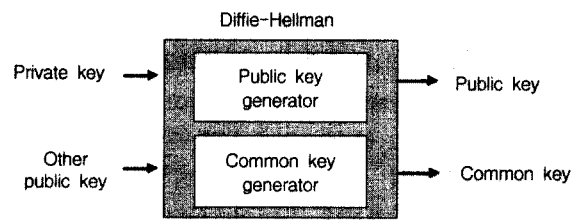


(그림 3) 구현된 대칭키 암호 알고리즘의 블록도

대칭키 암호 알고리즘은 데이터를 블록단위로 암호화하는 방식이다. 즉, 암호화하기 위한 평문은 항상 블록의 길이와 같아야 한다. 오디오 스트림은 고정된 Octet 길이를 가지므로 별도로 처리할 부분이 없지만, 암호에 사용되는 암호키와 비디오 스트림은 가변적인 길이를 가지므로 이것을 해결하기 위해서는 패딩(padding) 과정이 필요하다. 본 논문에서는 H.235 프로토콜에서 제안된 패딩 방법을 사용한다. 먼저, 키 패딩과정은 사용자가 제공하는 키가 블록의 길이와 다른 경우 적용되며, 길이가 적으면 모자라는 비트 수만큼 0x00 값을 채워 넣는 제로(zero) 패딩 방법을 사용하고 길이가 초과하면 사용자로부터 제공된 키를 블록의 길이로 자르고 그것들을 XOR하여 암호키로 사용한다. 비디오 스트림은 모자란 길이만큼 0x00을 채워 넣는 제로 패딩 방법을 사용한다[14].

3.2.2 Diffie-Hellman 키 분배 알고리즘의 구현

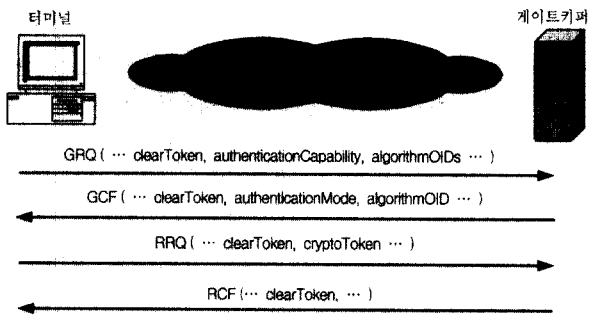
본 논문에서 구현된 Diffie-Hellman 키 분배 알고리즘에서는 사용되는 파라미터 생성에 걸리는 지연시간을 줄이기 위해 고정된 파라미터를 사용한다. (그림 4)는 구현된 Diffie-Hellman 키 분배 알고리즘의 전체 블록도를 나타낸다. Public key generator는 사용자에 의해 제공되는 개인키를 사용하여 공개키를 만드는 부분이며, common key generator는 자신의 개인키와 상대방의 공개키를 사용하여 공통된 키를 생성하는 블록이다.



(그림 4) 구현된 Diffie-Hellman 키 분배 알고리즘의 블록도

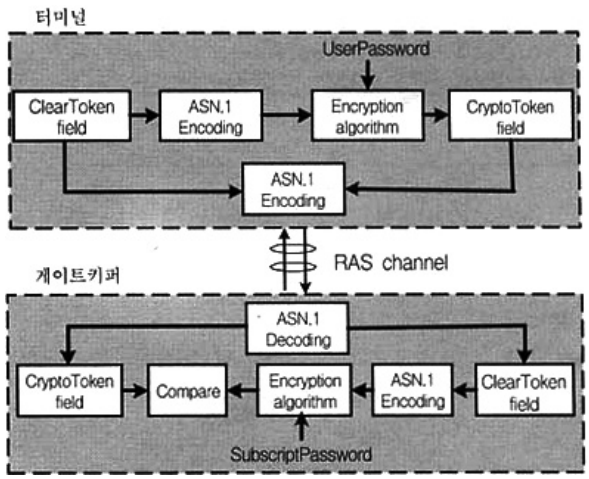
3.3 패스워드 기반의 대칭키 암호 인증의 구현

패스워드 기반의 대칭키 암호 인증은 미리 공유된 패스워드와 대칭키 암호 알고리즘을 사용하여 사용자를 인증하는 방법이다. 구현된 패스워드 기반의 대칭키 암호 인증은 게이트키퍼가 터미널을 인증하는 단방향 인증이다. 따라서, 터미널은 단지 인증에 사용될 메시지를 생성하는 부분만을 가지며, 메시지를 처리하고 인증하는 부분은 게이트키퍼에 구현된다. (그림 5)는 인증이 수행되는 과정에서 터미널과 케이트키퍼 사이에 교환되는 RAS 메시지를 보여준다.



(그림 5) RAS 메시지

H.323에서는 4개의 메시지, 즉 GRQ(GatekeeperRequest), GCF(GatekeeperConfirm), RRQ(RegistrationRequest), RCF(RegistrationConfirm)을 사용하여 터미널이 게이트키퍼에게 등록된다. H.235 프로토콜은 이 모든 메시지에 사용자의 인증을 위해 다양한 필드를 포함한다. 먼저 clearToken 필드는 일반적인 터미널의 정보를 담는 필드로써 네트워크 상에 노출되는 정보를 담는다. authenticationCapability 필드는 터미널이 지원할 수 있는 인증 방법을 표현하는 필드이고 algorithmOIDs 필드 역시 터미널이 지원할 수 있는 암호 알고리즘의 정보를 담는 필드이다. 그리고, cryptoToken 필드는 clearToken 필드와 게이트키퍼에 의해 제공된 challengeString을 포함하여 암호화된 필드로써 사용자를 인증하는데

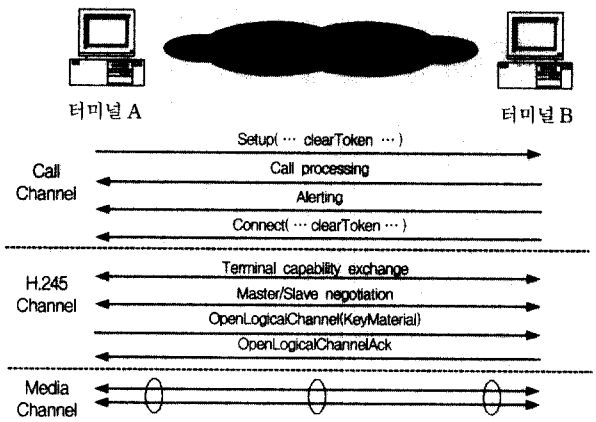


(그림 6) cryptoToken 필드의 생성 및 확인

사용되는 인증 필드이다. (그림 6)은 구현 과정에서 사용되는 cryptoToken 필드의 생성과 확인 과정을 나타낸다. 만일 인증이 성공되면 터미널은 게이트키퍼에 등록되며, 다른 등록된 터미널과 영상회의를 수행할 수 있다.

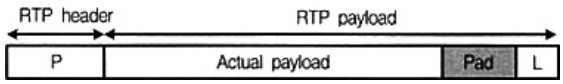
3.4 미디어 스트림의 암호화 구현

게이트키퍼에게 인증된 터미널은 호 설정 메시지와 H.245 제어 메시지 교환에 의해 다른 터미널과 영상회의를 할 수 있다. (그림 7)은 구현에 사용된 호 설정 메시지와 H.245 메시지의 교환을 보여준다.



(그림 7) 호 설정 메시지와 H.245 메시지

호 설정에서의 H.235 프로토콜의 동작은 setup과 connect 메시지의 clearToken 필드 내의 dhkey 필드를 사용하여 Diffie-Hellman 파라미터를 교환한다. 교환이 끝나게 되면 각각의 터미널은 교환된 파라미터를 사용하여 서로 공통된 키를 생성하게 된다. 호 설정이 이루어지면 H.245 채널을 통해 터미널간에는 마스터-슬레이브의 결정, 미디어 스트림에서 사용될 암호 알고리즘의 종류 결정, 오디오 및 비디오의 능력 교환 등 여러 가지 성능 교환이 이루어진다. 이때, H.235 프로토콜의 동작은 H.245 채널을 통해 미디어 스트림을 암호화하기 위한 비밀키를 분배한다. 비밀키의 분배는 H.245 채널을 통한 마스터-슬레이브 결정 후에 마스터에 의해 openLogicalChannel 메시지 또는 openLogicalChannelAck 메시지를 사용하여 다른 터미널로 분배되어 진다. 분배된 비밀키는 비디오 및 오디오 데이터를 암호화하는데 사용된다. 특히 비디오 데이터를 위하여 RTP 패킷은 패딩된 크기를 포함한다. (그림 8)은 패딩된 데이터를 네트워크상에 전송할 때의 패킷을 보여준다. 여기서, 마지막 바이트 L은 패딩 바이트를 나타낸다[4].



(그림 8) RTP 패킷

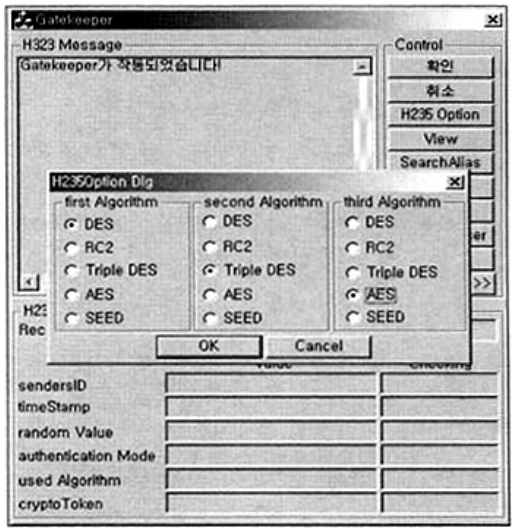
4. H.235 프로토콜의 구현 결과 및 성능평가

4.1 패스워드 기반의 대칭키 암호 인증의 구현 결과

패스워드 기반의 대칭키 암호 인증은 미리 공유된 패스워드를 이용하여 사용자를 인증하는 방법이다. (그림 9)는 패스워드 기반의 대칭키 암호 인증이 구현된 터미널을 보여준다.

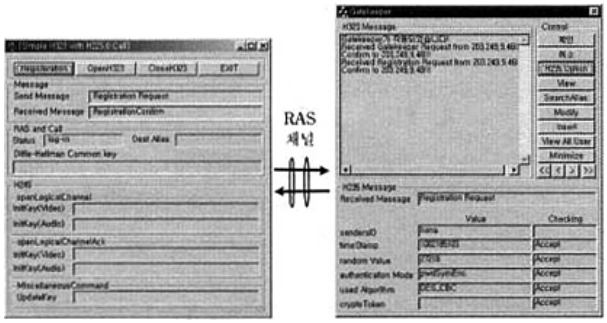
(그림 9) H.235가 구현된 터미널

패스워드 기반의 대칭키 암호 인증이 적용된 게이트키퍼는 인증에 사용될 대칭키 암호 알고리즘을 정하여 터미널을 인증하게 된다. (그림 10)은 패스워드 기반의 대칭키 암호 인증이 구현된 게이트키퍼를 보여준다.



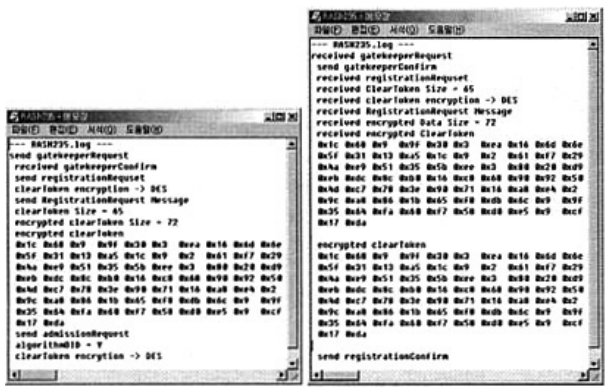
(그림 10) H235가 구현된 게이트키퍼

(그림 11)은 구현된 패스워드 기반의 대칭키 암호 인증 방법을 사용하여 게이트키퍼가 터미널을 인증하는 것을 보여준다.



(그림 11) 패스워드 기반의 대칭키 암호 인증

터미널에 의해 제공되는 정보 즉, sendersID, timeStamp, randomVal, authenticationMode, algorithmOID등을 게이트키퍼는 확인하고 인증 필드인 cryptoToken을 확인하여 사용자를 인증하게 된다. (그림 12)는 게이트키퍼와 터미널 사이에 인증을 위하여 교환된 데이터와 생성된 데이터를 보여준다. 여기서 encrypted clearToken은 인증 필드인 crypto-Token 필드를 나타낸다.

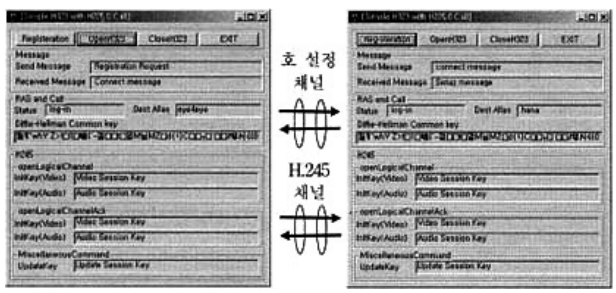


터미널 게이트키퍼

(그림 12) 패스워드 기반의 대칭키 암호 인증 결과

4.2 미디어 스트림의 암호/복호화 구현 결과

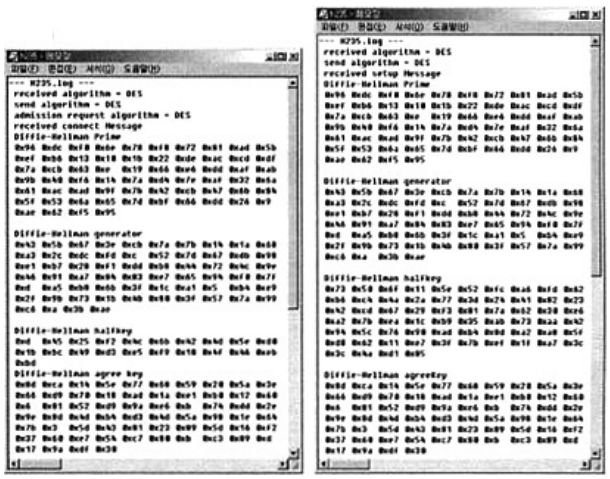
미디어 스트림의 암호화는 호 설정 동작에 의한 공통키의 생성, H.245 채널을 통한 비밀키의 분배, 그리고 오디오, 비디오 스트림의 암호화로 이루어진다. (그림 13)은 2개의 터미널 사이의 호 설정 채널 동작에 의해 생성된 공통키와 H.245 제어 채널을 통해 분배된 비밀키를 보여준다.



터미널 A 터미널 B

(그림 13) 호 설정과 H.245 제어 채널의 동작

(그림 14)는 호 설정 동작에서 교환되거나 생성된 데이터로써 prime과 generator는 공개키 또는 공통키를 생성하는데 사용되는 Diffie-Hellman 파라미터이고, halfkey는 사용자에 의해 제공된 개인키를 사용하여 생성된 공개키이다. 그리고, agree key는 서로 교환된 파라미터와 사용자의 개인키를 사용하여 생성된 공통키로써 터미널 A와 터미널 B가 서로 같음을 볼 수 있다.



터미널 A 터미널 B

(그림 14) 호 설정에 의해 생성된 Diffie-Hellman 파라미터

(그림 15)는 H.245 채널을 통해 분배되는 비밀키로써 비디오 데이터를 암호화하하는 video key와 오디오 데이터를 암호화하는 audio key, 일정 시간마다 갱신되는 update key를 보여준다.

터미널 A 터미널 B

(그림 15) H.245 채널을 통해 분배된 비밀키

(그림 16)은 분배된 비밀키와 대칭키 암호 알고리즘을 사용하여 영상회의 상에서 비디오 데이터가 정상적으로 암호/복호화 된 결과를 보여준다. 터미널 A와 터미널 B의 하측 영상이 자신의 영상이며, 자신의 영상을 비밀키와 대칭키를 사용하여 암호화된 비디오 데이터로 전송하면 비밀키를 사용하여 복호화한 영상이 상대편 화면의 상측에 표시됨을 알 수 있다. 또한, 오디오 데이터의 경우, 암호/복호화가 수행되어 각각의 터미널에서 정상적인 음성을 들을 수 있다.

이때, 불법적인 틀린 비밀키를 사용하여 복호화하는 경우, 정상적인 오디오, 비디오 데이터를 얻지 못함으로써, 잡음 소리와 비정상적인 영상만을 얻음을 알 수 있었다.

터미널 A　　터미널 B

(그림 16) 비디오 스트림의 암호/복호화

4.3 H.235 프로토콜의 적용에 따른 성능평가

H.323 영상회의 시스템에서 H.235 프로토콜을 적용하지 않는 경우와 H.235 프로토콜을 적용하고 여러 가지 암호 알고리즘을 사용하여 오디오, 비디오 데이터를 암호/복호화하는 경우에 대해 암호/복호화에 따른 지연시간과 계산에 사용되는 메모리 면에서 비교 한 결과는 각각 <표 2>, <표 3>과 같다. 이 실험은 AMD-800MHz CPU와 256MB 메모리를 갖는 PC와 LAN 상에서 측정한 결과이다.

〈표 2〉 오디오 데이터의 암호화에 따른 지연시간과 메모리 사용량

암호화 방법	지연시간 /100 패킷 (msec)	암호화 지연시간 (msec)	암호화 지연시간의 증가율 (%)	사용된 메모리 (Kbyte)	메모리의 증가율 (%)
No encryption	15990	-	-	4372	-
RC2	15996	6	0.037	4400	0.64
DES	15993	3	0.018	4380	0.18
Triple-DES	16053	63	0.39	4392	0.45
AES	16003	13	0.081	4408	0.82
SEED	15996	6	0.037	4436	1.46

〈표 3〉 비디오 데이터의 암호화에 따른 지연시간과 메모리 사용량

암호화 방법	지연시간 /100 패킷 (msec)	암호화 지연시간 (msec)	암호화 지연시간의 증가율 (%)	사용된 메모리 (Kbyte)	메모리의 증가율 (%)
No encryption	12001	-	-	7336	-
RC2	12006	5	0.041	7352	0.28
DES	12007	6	0.049	7400	0.87
Triple-DES	12081	80	0.66	7428	1.25
AES	12010	9	0.074	7504	2.29
SEED	12008	7	0.058	7580	3.32

<표 2>와 같이 100 패킷의 오디오 데이터를 전송하는 경우, 암호를 적용하지 않는 경우(No encryption)와 비교하여 암호화 과정에 의한 지연시간이 사용되는 암호 알고리즘에 따라 평균적으로 3~63msec 정도 더 소요된다. 이는 오디오 데이터에 암호화를 적용하여 기밀성을 높이는 반면, 0.018~0.39% 정도의 지연시간 증가율에 불과한 것을 알 수 있다. 또한, <표 3>과 같이 100 패킷의 비디오 데이터를 전송하는 경우, 사용되는 암호 알고리즘에 따라 평균적으로 5~80msec 정도 더 소요되며, 이는 0.041~0.66% 정도의 증가율에 불과한 것을 알 수 있다.

H.235 프로토콜에 기반한 암호/복호화를 처리하는 과정에서 사용되는 메모리의 증가는 오디오 데이터의 암호화의 경우에는 사용되는 알고리즘에 따라 0.18~1.46% 정도 증가하며, 비디오 데이터의 암호화의 경우에도 0.28~3.32% 정도 증가함을 알 수 있다. 이는 영상회의의 암호/복호화의 과정에서 컴퓨터의 리소스를 적게 사용함을 알 수 있다.

따라서, 실제적으로 영상회의 시스템에 적용한 결과, 오디오 및 비디오 데이터의 암호/복호화에 따른 지연시간과 메모리 사용량에 따른 시스템의 저하 효과는 무시할 수 있었다. 이는, H.323 영상회의 시스템에 H.235 프로토콜을 적용하는 경우와 적용하지 않는 경우를 비교하여 실제 영상회의상의 오디오와 비디오의 차이를 느끼지 못함 알 수 있었다.

5. 결 론

본 논문에서는 H.235 프로토콜에 기반하여 H.323 영상회의 시스템에서의 사용자 인증 및 미디어 스트림의 암호/복호화를 구현하였다.

인증을 위해 H.235 프로토콜의 패스워드 기반의 대칭키 암호에 인증 방법을 사용하였고, Diffie-Hellman 키 분배 알고리즘, RC2, DES, Triple-DES와 같은 대칭키 암호 알고리즘을 사용한 미디어 스트림의 암호/복호화를 구현하였다. 또한, 추후의 확장성을 고려하여 차세대 표준암호로 선정된 AES 알고리즘인 128비트 Rijndael 암호 알고리즘과 한국형 암호인 128비트 SEED 알고리즘을 적용하여 미디어 스트림의 암호/복호화를 구현하였다.

본 논문에서 구현된 H.235 프로토콜을 H.323 영상회의 시스템에서 동작시켜 본 결과, 패스워드 기반의 대칭키 암호 인증은 네트워크 상에서 사용자의 정보를 노출시키지 않으면서 대칭키 암호 알고리즘과 cryptoToken 필드만을 사용하여 사용자를 인증할 수 있었다. 또한, 여러 가지 암호 알고리즘을 사용하여 미디어 스트림의 암호/복호화를 수행한 결과, 기밀성을 증가시키는 암호화 과정을 거치면서도 암호화를 적용하지 않는 경우와 비교하여 미디어 스트림 패킷의 전달 지연 속도에 영향을 미치지 않으면서도, 메모리 사용량도 거의 증가하지 않음으로써 영상회의의 성능

이 저하되지 않는 결과를 얻을 수 있었다.

따라서, 본 논문의 결과를 살펴볼 때, 구현된 H.235는 표준안에 권고한 암호화 알고리즘들뿐만 아니라 한국형 알고리즘을 포함하고 있으며, 속도 및 메모리 사용량을 살펴볼 때, 기존의 H.323 프로그램에 거의 부담을 주지 않도록 구현되었음을 알 수 있었으며, H.235가 효율적으로 구현되었음을 알 수 있었다.

앞으로의 연구과제로는 게이트키퍼에 의해 모든 것이 제어 가능한 게이트키퍼 라우트 모델을 분석하고 구현해야 할 것이다.

참 고 문 헌

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

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

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

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

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

[6] FIPS Publication 46-3, "Data Encryption Standard (DES)," U.S. DoC/NIST, 1999.

[7] 박창섭, 암호이론과 보안, 대영사, 1999.

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

[9] Federal Information Processing Standards Publication, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001.

[10] 한국정보보호센터, 128비트 블록 암호알고리즘(SEED) 개발 및 분석 보고서, 1998.

[11] 한국전자통신연구원, 암호학의 기초, 경문사, 1999.

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

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

[14] Bruce Schneier, Applied Cryptography, Wiley, 1996.

심 규 복

e-mail : hana@dmtech.co.kr

2000년 경기대학교 전자공학과 졸업(공학사)

2002년 경기대학교 대학원 전자공학과 졸업 (공학석사)

2002년~현재 (주)디지탈미디어테크 연구원

관심분야 : 암호보안, VoIP, ASIC 설계

이 건 배

e-mail : kblee@kuic.kyonggi.ac.kr

1982년 한양대학교 전자공학과 졸업(공학사)

1984년 한양대학교 대학원 전자공학과 졸업 (공학석사)

1989년 한양대학교 대학원 전자공학과 졸업 (공학박사)

1998년~1999년 UCLA 방문연구교수

1991년~현재 경기대학교 전자공학전공 부교수

관심분야 : VoIP, 암호보안, ASIC 설계

성 동 수

e-mail : dssung@kuic.kyonggi.ac.kr

1987년 한양대학교 전자공학과 졸업(공학사)

1989년 한국과학기술원 전기및전자공학과 졸업(공학석사)

1992년 한국과학기술원 전기및전자공학과 졸업(공학박사)

1992년~1993년 한국과학기술원 정보전자연구소 연구원

2002년~2003년 University of Washington 방문연구교수

1993년~현재 경기대학교 전자공학전공 부교수

관심분야 : MoIP, 멀티미디어통신, 병렬처리