H.235에 기반한 영상회의 시스템의 인증 및 암호화 구현

심규복,° 이건배, 성동수
경기대학교 대학원 전자공학과
{mr1973, kblee, dssung}@kuic.kyonggi.ac.kr

Implementation of Authentication and Encryption of Multimedia Conference based on H.235

Gyu-Bok Sim°, Keon-Bae Lee, Dong-Su Seong
Dept. of Electronic Engineering, Graduate School, Kyonggi University

요 약

본 논문에서는 ITU-T 영상회의 프로토콜 표준안(H.323)에서 보안 프로토콜로 권고된 H.235를 기반으로 하여 사용자 인증, 비디오 및 오디오 데이터의 암호화, 암호키의 보호에 대하여 구현한다. 인증 방법으로는 패스워드 기반의 대칭키 암호 인증을 사용하고, 비디오 및 오디오 데이터의 암호화에 사용되는 암호키의 보호를 위해서는 DES와 Diffie-Hellman의 키 분배 방법을 사용한다. 또한, DES를 사용한 비디오 및 오디오 데이터의 암호화/복호화를 보여준다.

1. 서론

급속하게 발전하는 컴퓨터와 통신 기술에 의해 텍스트 위주의 정보교환에서 탈피하여 영상과 음성을 지원하는 멀티미디어라는 새로운 매체가 등장하였다. 이에 ITU-T에서는 영상회의 시스템인 H.323을 표준안으로 권고하고 있으며[1], 영상회의의 기밀성과 사용자를 확인하는 인증을 위해 H.235 보안 프로토콜을 같이 권고하고 있다.

H.235 프로토콜은 영상회의에서 가능한 공격에 대한 방어 목적으로 여러 가지 보안 기능을 제공한다. 우선 수동적 공격 즉, 공격자들의 도청 방지를 위해 대칭키 암호 알고리듬인 DES, RC2, Triple-DES의 사용을 권고하고 있으며, 능동적 공격 즉, 의도적으로 공격자가 메시지의 내용을 변조, 삽입, 삭제, 재생하는 것을 방지하기 위하여 해쉬함수인 SHA(Secure Hash Algorithm), MD5(Message Digest Algorithm)와 더불어 여러 가지 메시지 필드의 사용을 권고하고 있다.

본 논문에서는 영상회의에서 H.235 프로토콜을 기반으로 하는 사용자 인증, 비디오 및 오디오 데이터의 암호화와 이에 사용되는 암호키의 보호에 대하여 구현한다.

2. H.235 프로토콜

H.235 프로토콜에서 제공하는 서비스는 사용자를 확인하는 인증과 인증된 사용자만이 데이터를 확인할 수 있게 해주는 기밀성으로 크게 나눌 수 있으며, 부가적으로 무결성이 제공된다. 인증 방법으로는 패스워드 기반의 대칭키 암호 인증, 패스워드 기반의 해쉬 알고리듬에 의한 인증, 인증서 기반의 서명 인증 등과 같은 subscription 기반의 인증 방법과 Diffie-Hellman의 키 분배 방법이 제안되고 있다[2]. 또한, 별개의 프로토콜인 IPSec(Internet Protocol Security)이나 TLS(Transport Layer Security)를 사용하는 방법도 가능하다[2]. 데이터의 암호화에 사용되는 방법으로는 대칭형 암호 알고리듬인 DES, RC2와 Triple-DES의 사용을 제안하고 있다[2].

본 논문에서는 사용자들이 이용하기 쉽고, 일반적으로 많이 사용되고 있는 subscription 기반의 패스워드 기반의 대칭키 암호 인증 방법을 사용하고, Diffie-Hellman 키 분배 알고리듬과 대칭키 블록 암호 알고리듬인 DES를 사용하여 미디어 데이터의 암호화를 제공하는 방법을 구현한다.

2.1 패스워드 기반의 대칭키 암호 인증

H.235 프로토콜에서 제안된 subscription 기반의 인증 방법 중 하나인 패스워드 기반의 대칭키 암호 인증은 사전에 사용자의 alias 주소와 패스워드를 게이트키퍼(gatekeeper)와 공유한 후, 이를 이용하여 사용자를 인증하는 방법이다. 그림 1은 기존의 H.323 프로토콜에서 사용되는 RAS(Registration, Admission, Status) 메시지에 H.235 프로토콜 인증 메시지 필드가 포함되어 터미널과 게이트키퍼 사이에 교환되는 것을 보여 준다.

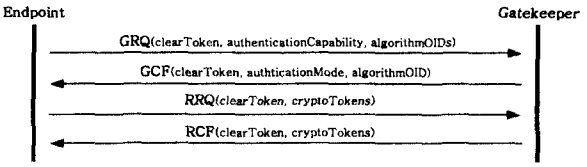

그림 1. RAS 메시지

먼저, 터미널은 GatekeeperRequest 메시지의 clearToken 필드 내에 H.235 프로토콜에서 사용될 TimeStamp, RandomVal와 사전에 공유된 자신의 alias 주소들을 포함시키며, 터미널 자신이 지원 가능한 인증 방법과 대칭키 암호 알고리듬을 authticationCapability 필드와 algorithmOIDs 필드에 각각 포함시켜 게이트키퍼에게 보낸다. 이 메시지를 받은 게이트키퍼는 터미널이 보낸 인증 방법 중 패스워드 기반의 대칭키 암호 인증 방법을 선택하고, 이를 authenticationMode 필드에

포함시킨다. 또한, 사용될 암호 알고리듬으로는 DES를 선택하여 algorithmOID 필드에 포함시키고, 랜덤하게 생성된 challengeString을 clearToken 필드에 포함시켜 터미널에게 GatekeeperConfirm 메시지를 보낸다. 이것을 받은 터미널은 선택된 인증 방법, 즉 패스워드 기반의 대칭키 암호 인증 방법에 따라서 RandomVal, TimeStamp, generalID, sendersID, ChallengeString을 포함하는 하나의 메시지 블록, 즉 clearToken 필드를 미리 공유된 패스워드를 사용하여 선택된 암호 알고리듬인 DES를 사용하여 암호화한 후 cryptoToken 필드에 포함시킨다. 이렇게 설정된 clearToken과 cryptoToken은 RegistrationRequest 메시지에 포함되어 게이트키퍼에게 보낸다. 메시지를 받은 게이트키퍼는 똑같은 방법으로 clearToken 필드에 포함되어 있는 RandomVal, TimeStamp, generalID, sendersID, ChallengeString을 하나의 메시지 블록으로 만들어 선택된 알고리듬 DES와 alias 주소에 해당하는 패스워드를 사용하여 암호화한다. 여기서, 생성된 암호문은 터미널이 보낸 cryptoToken과 비교하여 인증을 수행한다. 만일 인증이 성공하면 터미널은 게이트키퍼에게 등록이 되어 다른 터미널과 영상회의를 수행할 수 있다.

2.2 Diffie-Hellman에 의한 미디어 데이터의 암호화

게이트키퍼에게 인증된 터미널은 호 설정 메시지와 H.245 제어 메시지를 사용하여 다른 터미널과 영상회의를 할 수 있다. 그림 2는 호 설정 메시지에 포함되는 H.235 메시지 필드와 H.245 제어 메시지를 통한 세션 키의 분배를 보여준다.

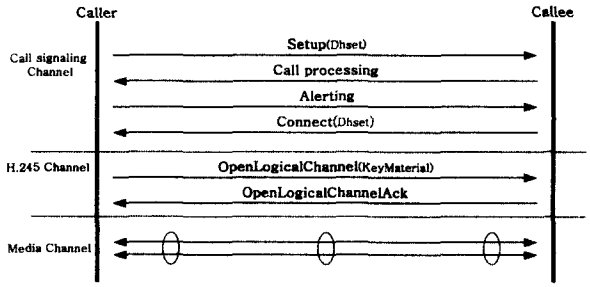

그림 2. 호 설정 및 H.245 제어 메시지

먼저 Caller에 의해 보내지는 Setup 메시지의 DHset 필드 내에는 Diffie-Hellman 키 분배 알고리듬을 사용하여 생성된 자신의 공개키와 생성에 사용된 Diffie-Hellman 파라미터가 포함된다. 이것을 받은 Callee는 Caller의 파라미터를 사용하여 자신의 공개키를 만들고, 각각의 공개키를 사용하여 공통키를 생성한다. 또한, Callee에 의해 보내지는 Connect 메시지에는 Callee의 공개키를 DHset 필드에 포함시켜 전송함으로써 Caller 또한 Callee와 같은 공통키를 생성할 수 있다. 이렇게 생성된 공통키를 사용하여 Caller나 Callee 중 마스터가 되는 터미널은 세션 키를 암호화하여 KeyMaterial 필드 내에 포함시켜 슬레이브에게 H.245 채널을 통해 분배한다. 이렇게 분배된 세션 키는 비디오 및 오디오 데이터를 암호화하는데 사용된다.

3. H.235에 기반한 사용자 인증 및 미디어 데이터의 암호화 구현

본 논문에서는 H.323 영상회의 시스템에서 패스워드 기반의 대칭키 암호 인증 방법과 Diffie-Hellman 키 분배 알고리듬을 사용한 공통키의 생성, DES를 사용한 미디어 데이터의 암호화를 구현한다.

3.1 패스워드 기반의 대칭키 암호 인증 방법의 구현

구현된 패스워드 기반의 대칭키 암호 인증 방법은 게이트키퍼가 터미널을 인증하는 단방향 인증이다. 따라서, 터미널은 단지 메시지를 생성하는 부분만을 가지고 있으며, 메시지를 처리하고 인증하는 부분은 게이트키퍼에서 구현된다.

그림 3은 사용자 인증을 위해 사용되는 cryptoToken 필드의 생성과 확인 과정을 보여준다.

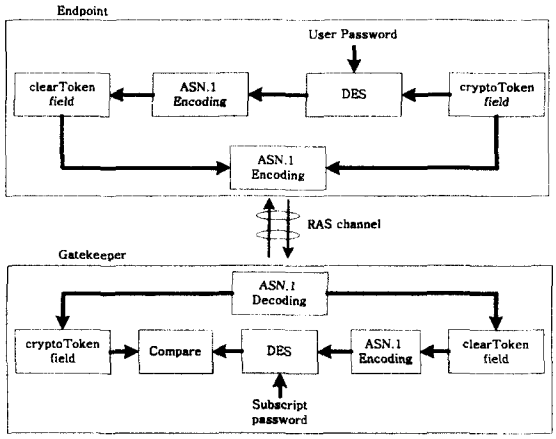

그림 3. cryptoToken의 생성 및 확인

그림 4는 게이트키퍼 상에서 구현된 패스워드 기반의 대칭키 암호 인증을 보여준다.

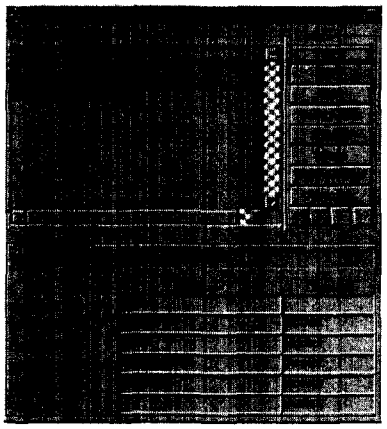

그림 4. 게이트키퍼

RegistrationRequest 메시지를 받은 게이트키퍼는 먼저 sendersID를 확인하고 TimeStamp와 RandomVal를

확인한다. 또한, 앞에서 협상된 authenticationMode가 패스워드 기반의 대칭키 암호 인증 방법인지를 확인하고, 사용할 알고리듬이 DES 인지를 확인한다. 이러한 절차가 끝나면 최종적으로 cryptoToken을 확인하며, 등록을 요청한 터미널은 다른 등록된 터미널과 연결할 수 있는 권한을 가지게 된다.

3.2 Diffie-Hellman과 DES를 사용한 미디어 데이터의 암호화 구현

등록을 마친 터미널은 AdmissionRequest 메시지를 사용하여 자신이 연결하고 싶은 터미널의 정보를 게이트키퍼로부터 받은 후, 호 설정 메시지를 사용하여 연결을 시도한다. 호 설정 과정에서 H.235 프로토콜은 Diffie-Hellman 키 분배 알고리듬을 사용하여 서로가 공유할 수 있는 공통키를 생성하게 된다. 그림 5는 터미널에 적용된 공통키 생성 방법을 보여준다.

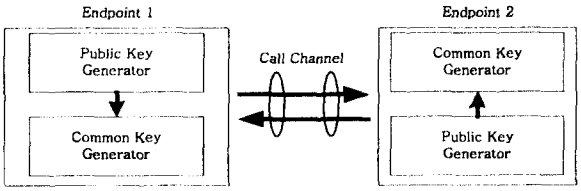

그림 5. 공통키 생성

그림 6은 H.323 터미널[4]에 Diffie-Hellman 키 분배 알고리듬을 적용하여 내부에 생성되는 터미널간의 공통키를 보여준다.

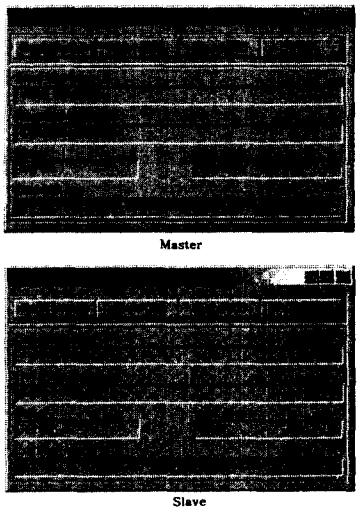

그림 6. 생성된 공통키

호 설정을 마친 터미널은 생성된 공통키를 사용하여 H.245 제어 메시지를 통해 세션 키를 암호화한 후 분배한다. 이렇게 분배된 세션 키는 비디오 및 오디오 데이터를 암호화하는데 사용된다. 본 논문에서는 미디어 데이터의 암호화/복호화에 DES를 사용하며, 대칭키 암호 알고리듬인 DES는 블록단위로 암호화하는 방식을 사용한다. 즉, 암호화하기 위한 평문은 항상 블록 길이와 같아야 한다. 영상회의에서 사용하는 오디오 데이터는 항상 고정된 Octet 길이를 가지므로 별도의 처리가 필요 없으나, 비디오 데이터는 가변적인 길이를 가지므로 별도의 처리를 하여 블록 길이에 맞추어야 한다. 본 논문에서는 H.235 프로토콜 권고 안에서 제안된 Zero 패딩(padding) 방법을 사용한다. 이 패딩 방법은 부족한 블록 길이만큼 0x00의 값을 채워 넣어 블록의 길이를 맞춰준다. 그리고, 전송할 때 RTP payload의 마지막 바이트에 패딩된 정보를 포함하여 복호화 할 때 원래의 데이터가 변형되는 것을 방지한다[2,3]. 그림 7은 Zero 패딩된 RTP 패킷을 보여준다.

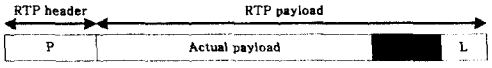

그림 7. Zero 패딩된 RTP 패킷

그림 8은 DES를 사용하여 비디오 데이터가 성공적으로 암호화/복호화가 되는 결과를 보여준다. 또한, 오디오 데이터 역시 암호화/복호화가 되어 각각의 터미널에서 정상적인 음성을 들을 수 있다.

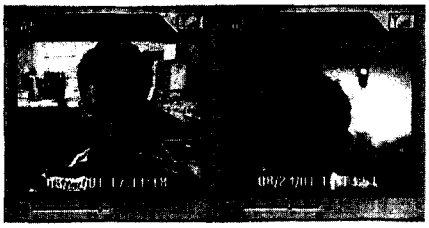

그림 8. 비디오 데이터의 암호화/복호화

4. 결론

본 논문에서는 H.323 영상회의 프로토콜을 위한 보안 프로토콜인 H.235를 기반으로 하여 사용자 인증, 비디오 및 오디오 데이터의 암호화를 구현하였다. 구현된 H.235 프로토콜은 패스워드 기반의 대칭키 암호 인증 방법을 사용하였고, Diffie-Hellman 키 분배 알고리듬과 대칭키 암호 알고리듬인 DES를 사용하여 비디오 및 오디오 데이터를 암호화하였다. 구현된 인증 방법과 암호화는 사용자의 정보를 네트워크에 노출하지 않으면서도 정확한 동작을 보여 주었으며, H.323 영상회의 프로토콜이 동작하는 데에도 영향을 미치지 않았다. 앞으로의 연구 과제는 H.235 프로토콜에서 권고된 또 다른 인증 방법과 암호화에 대해 구현해야 할 것이다.

참고문헌

[1]ITU-T Recommendation H.323, Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-Guaranteed Quality of Service.
[2]ITU-T Recommendation H.235, Security Encryption for H-series Multimedia terminals
[3]Bruce Schneier, Applied Cryptography, Wiley
[4]"H.323 영상회의 시스템", 경기대학교 대학원 정보통신연구실