

# H.235 기반 VoIP 보안 시스템 구현

학생회원 임 범 진\*, 홍 기 훈\*, 정회원 정 수 환\*, 유 현 경\*\*, 김 도 영\*\*

## Implementation of Secure VoIP System based on H.235

Bumjin Im\*, Kihun Hong\* *Student Members,*

Souhwan Jung\*, Hyun-Kyung Yoo\*\*, Do-Young Kim\*\* *Regular Members*

### 요 약

본 논문에서는 ITU-T에서 제안한 H.323 VoIP의 보안 프로토콜인 H.235에 대하여 연구하고 이를 구현한 VoIP 보안 시스템을 구축하여 VoIP 보안 프로토콜의 요구 사항 및 방향을 제시하였다. H.235 annex D에서 제안하고 있는 VoIP 단말 시스템에 대한 보안 기능을 구현하였으며 구현 결과에 대하여 분석하고 구현 시 추가로 요구되는 사항들을 언급하였다. H.235에서는 HMAC을 이용한 인증과 Diffie-Hellman을 이용한 키 교환 및 음성 데이터의 암호화를 위한 세션키 생성, 그리고 RTP 음성 데이터의 암호화를 위한 DES, 3DES, RC2 등을 지원하고 있으며 본 논문에서는 한국형 암호 알고리즘인 SEED, 그리고 차세대 암호 알고리즘인 AES를 구현하여 표준에서 지원하지 않는 방식에 대한 구현을 실시하였다.

### ABSTRACT

In this paper, H.235-based security mechanism for H.323 multimedia applications was implemented. H.235 covers authentication using HMAC, Diffie-Hellman key exchange, session key management for voice channel, and encryption functions such as DES, 3DES, RC2. Extra encryption algorithms such as SEED, and AES were also included for possible use in the future. And, we also analyzed the quality of service (QoS), the requirement of implementation, and interoperability to the result in this study. The results could be applied to secure simple IP phone terminals, gateways, or gatekeepers.

### 1. 서 론

1990년대부터 급속히 발달하고 확산된 인터넷 서비스 가운데 현재 각광을 받는 서비스로 멀티미디어 서비스가 대두되고 있다. VoIP(Voice over IP) 역시 이러한 인터넷을 통한 멀티미디어 서비스의 하나로 기존에 사용하고 있는 공중전화망(PSTN)과 같은 서비스를 인터넷망에서 제공할 수 있도록 한 것으로 편리한 기능과 국제 전화를 포함하여 저렴한 가격으로 제공되는 서비스를 장점으로 많은 서비스 업체가 현재 서비스 중이다. 최근의 VoIP 서비스는 인터넷 기술 발전과 더불어 통화 품질 보

을 위한 연구가 진행 중이며 일반전화망에서 제공되고 있는 호 전환, 호 보류 등의 부가 서비스로의 영역을 넓히고 있으며 인터넷폰 서비스 제공자(ITSP) 간 서비스도 개발하는 등의 연구 노력으로 인하여 VoIP 기술의 발전은 더욱 가속화될 전망이다.

그러나 VoIP는 IP 네트워크를 이용하는 서비스이므로 IP 네트워크가 가지고 있는 특징을 그대로 따르기 때문에 IP 네트워크의 보안 취약점을 그대로 갖고 있다. 따라서 이러한 공격에 대한 방어와 안전한 VoIP 서비스를 위해서 보안 시스템을 적용할 필요가 있으며 메시지의 인증과 무결성 보장, 그리고 음성 데이터에 대한 기밀성을 보장해야 하며 합법적

\* 숭실대학교 정보통신전자공학부 통신망 보안 연구실(souhwanj@ssu.ac.kr)

\*\* 한국전자통신연구원 네트워크기술연구소 네트워크서비스연구부 VoIP 네트워크연동팀

논문번호: 020011-0108, 접수일자: 2001년 1월 8일

※ 본 연구는 한국전자통신연구원 위탁수행과제 지원으로 수행되었습니다.

인 감청(Lawful interception)을 지원할 수 있어야 하고, 기존 VoIP 시스템과의 호환성도 유지해야 한다.

현재 ITU-T, IETF, ETSI 등의 통신 표준화 기구에서는 VoIP의 보안 표준화를 서두르고 있으며 VoIP 서비스 업체에서도 속속 보안을 적용한 VoIP 솔루션을 선보이고 있다. ITU-T에서는 H.323 시스템의 보안을 위한 H.235를 제안하여 단말, 게이트웨이 및 게이트키퍼 등에 적용할 수 있는 보안 권고안을 제안하고 있으며, IETF에서는 SIP RFC 문서를 통하여 SIP의 보안에 대한 표준을 제안하고 있고 ETSI에서는 TIPHON 보안을 위한 위협 유형, 감청 및 ITSP간 정보 교환을 위한 프로토콜을 제안하고 있다. Netspeak 사에서는 VPN 기술과 VoIP 기술을 접목한 서비스를 개발하여 서비스중이고, CcheckPoint 사에서는 H.323 기반 VoIP의 방화벽 통과 기능과 RSVP 등의 QoS를 고려한 방화벽 시스템을 개발하였으며, 일본의 NTT Docomo의 경우 모바일 환경에서의 IPv6 및 멀티미디어 서비스 구현을 위한 제어 및 보안 플랫폼 구축 등에 관한 연구가 현재 진행 중이다. 본 논문에서는 II장에서 H.235 표준을 기반으로 구현한 VoIP 보안 기술에 대하여 언급하고 III장에서는 H.235 구현 내용과 구현 결과를 기술하는데 특히, 구현된 결과물의 음질과 구현 시 고려해야 할 사항 그리고 표준의 새로운 버전에 반영되어야 할 사항들을 서술하고 있다.

## II. H.235 기반의 VoIP 보안 기술

### 1. H.235 기술 개요

H.235는 ITU-T의 VoIP 표준안인 H.323의 보안 표준안을 말한다<sup>[1][2]</sup>. ITU-T에서는 VoIP만을 위한 보안 표준안을 제안한 것으로 IPsec, TLS 등의 낮은 계층의 프로토콜에 대한 보안을 정의한 기존의 보안 프로토콜과는 달리 VoIP만을 위한 보안 프로토콜이라는 특징이 있기 때문에 VoIP에 최적화되어 있다고 할 수 있다.

H.235는 H.225.0의 RAS(Registration, Admission, and Status)에 대한 보안, 호 처리에 대한 보안 및 세션 키의 생성, H.245에서의 security capability 교환, 그리고 음성 데이터의 보안인 미디어 암호화 부분으로 구성되어 있고, 부록에서는 ASN.1 메시지 정의 및 네트워크의 기반 구성을 다룬 baseline security, 제 3자 인증을 통한 방법을 제안한 signature security profile, 그리고 무선 VoIP 보안을 위한 security for mobile H.323

system으로 이루어져 있다<sup>[3][4]</sup>.

H.235는 먼저 RAS 메시지를 통하여 게이트키퍼와의 인증 과정을 정의하고 있고, 호 설정 시 상대방과의 인증 과정을 포함하며 이 때 세션 키의 암호화 교환을 위한 Diffie-Hellman 키를 교환하고 호 설정 후 H.245 메시지에서는 capability 교환과 같은 양식으로 security capability 교환을 실시한다<sup>[7]</sup>. 음성 채널을 생성할 때, 이미 교환된 capability 중 한 가지를 선택하여 음성 데이터의 암호화 알고리즘으로 이용하고, 동시에 호 설정 시 교환되었던 Diffie-Hellman 키를 이용하여 마스터가 생성한 세션 키를 암호화하여 전송한다.

### 2. Baseline Security

H.235 Annex D인 Baseline security는 일반적인 H.323 네트워크에서의 보안 적용에 대한 내용을 다루고 있으며 H.225.0 RAS, 호 설정, H.245 capability에 대한 교환 및 미디어 암호화에 대한 보안으로 이루어져 있고 구성 가능한 네트워크의 구성도 다루고 있다<sup>[5]</sup>. Baseline security는 H.235가 수행되어야 할 가장 기본적이고 필수적인 부분을 다루고 있으며 SET(Simple Endpoint Type)에서의 보안에 대한 기본 방향을 제시하고 있다.

#### 2.1 H.225.0 호 설정 메시지 인증 및 Diffie-Hellman 키 교환



그림 1. H.225.0에서의 보안 메시지

그림 1과 같이 H.225.0에서는 호 설정과 함께 해당 메시지의 인증과 H.245 세션 키 교환을 위한 Diffie-Hellman 키 교환을 수행한다<sup>[7]</sup>. Caller 측에서 Setup 메시지의 hash 필드에 인증 메시지를 삽입하고 dhkey 필드에 Diffie-Hellman 정보를 삽입하여 전송하면 callee는 전송 받은 메시지에서 hash 필드를 이용하여 인증 여부를 확인하고 dhkey 값을 이용하여 키를 생성한 후 Connect 메시지에 자신의 인증값과 Diffie-Hellman 정보를 삽입하여 전송한다.

2.1.1 메시지 인증

H.225.0 메시지 인증 알고리즘은 패스워드 기반의 HMAC-SHA1-96을 이용한다<sup>9)</sup>. HMAC-SHA1은 160 비트의 출력이 나오는데 이 중 왼쪽 96비트를 사용하게 된다. 해쉬 함수는 일반적으로 메시지의 무결성을 보장하기 위하여 사용되지만 HMAC은 키가 삽입되기 때문에 인증의 역할도 하며 좌, 우 시프트 연산으로 이루어진 해쉬 함수 특성상 HMAC 또한 고속 처리가 가능하고 H.235에서는 텍스트 키를 SHA1을 이용하여 160bit로 확장한 후 HMAC의 키로 사용한다.

2.1.2 Diffie-Hellman 키 교환

Diffie-Hellman 키 교환(Key agreement)은 1976년에 Diffie와 Hellman에 의해 제안된 키 교환 알고리즘으로 두 사용자가 사전에 어떠한 비밀교환 없이 안전하지 않은 매체상에서 공통키를 교환하도록 하며 소수(prime number) p와 p보다 작은 정수 g(generator)를 갖으며 이 두 파라미터는 공개되며 서로 같은 p, g 값을 이용하여 key를 계산해 내는 알고리즘을 말한다. 하지만 Diffie-Hellman은 Man-in-the-middle 공격에 취약점을 갖는다. 공격자가 A와 B사이에서 Diffie-Hellman 메시지를 교환하면서 A와 B가 통신하는 것처럼 가짜하여 키를 교환하여 키를 알아낼 수 있기 때문에 Diffie-Hellman 키 교환은 반드시 인증과 함께 이루어져야 한다.

H.235에서는 음성 데이터 암호화 키 교환에 사용하기 위하여 Diffie-Hellman 키 교환을 이용한다. Diffie-Hellman을 이용하여 교환된 키로 음성 데이터의 암호화에 필요한 키를 암호화하여 전송하며 이 과정은 H.245에서 이루어진다. 이 과정은 H.225.0의 dhkey 필드를 이용하여 Diffie-Hellman 메시지를 교환한다. 이 때 Setup과 Connect 메시지는 HMAC에 의하여 인증이 이루어지기 때문에 Man-in-the-middle 공격을 방지할 수 있다. H.235에서는 Diffie-Hellman에 사용될 512bit의 p는 개발자가 선택하도록 하고 g는 2로 고정시켜 놓았으며 3DES를 위하여 1024bit는 표준안으로 정해진 p를 쓰도록 하고 있다.

2.2 Security Capability 교환 및 세션키 생성

H.245에서는 음성 데이터의 암호화에 사용될 암호화 알고리즘의 단말 지원 여부(capability)를 교환한다(그림 2.) H.235 security capability는 H.323에

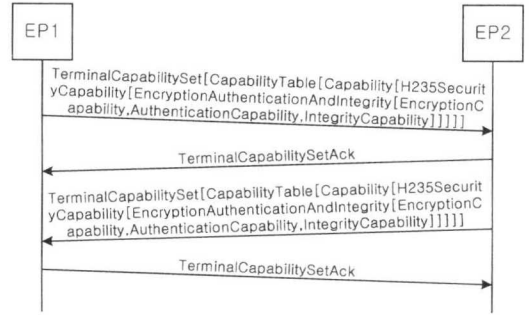


그림 2. H.245 보안 capability 교환 메시지

서 교환하는 audio, video capability 등과 같은 방법으로 전송되고 같은 방법으로 처리된다.

Capability 교환 후 H.245에서는 master slave determination 과정을 거치게 된다. 이 과정을 거치고 나면 마스터로 결정된 단말이 음성 데이터 암호화에 쓰일 키를 생성하게 된다. 이 때 생성되는 랜덤 bit 키의 크기는 DES 56bit, 3DES 168bit이다.

2.3 보안 알고리즘 설정 및 암호화 키 교환

Capability 교환을 통하여 교환된 암호화 알고리즘은 테이블 형태의 연결 리스트(linked list)로 단말에 저장되며 이 때 단말은 자신의 capability와 상대방의 capability 두 개의 테이블을 가지게 된다. 두 단말은 독립적으로 상대방의 테이블을 기준으로 자신의 테이블과 데이터를 비교하여 일치하는 데이터가 있으면 해당 capability를 이용하여 통신을 실시한다. 음성 capability가 설정되면 보안 capability를 설정하는데 이 과정 역시 테이블에 저장된 보안 capability를 비교하여 설정하게 된다. 이 과정을 통하여 설정된 capability는 OpenLogicalChannel 메시지를 통하여 전송되는데 이 메시지에 그림 3과 같이 AudioCapability와 H235Media를 함께 전송하게 된다.

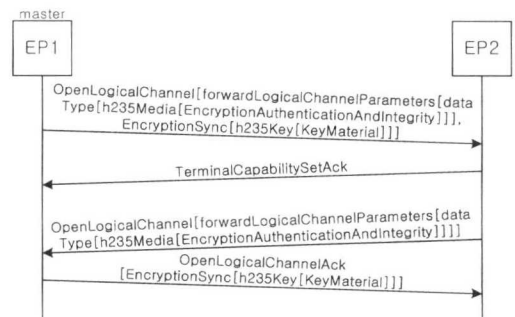


그림 3. OpenLogicalChannel 보안 메시지

이와 동시에 마스터는 생성된 키를 OpenLogical Channel의 EncryptionSync 필드를 이용하여 슬레이브에게 전송한다. 마스터는 OpenLogical ChannelAck 메시지에도 EncryptionSync 메시지를 삽입하여 OpenLogicalChannel이 전송되지 않을 경우를 대비한다. 암호화키는 Diffie-Hellman으로 공유된 키로 암호화를 하며 키를 암호화하는 암호화 알고리즘은 DES, 혹은 3DES를 사용할 수 있고 DES를 사용할 때에는 512bit Diffie-Hellman 키 교환을 이용하며 3DES를 사용할 때에는 1024bit Diffie-Hellman을 이용한다. 이 때 사용하는 알고리즘은 모두 CBC(Cipher Block Chaining)모드를 사용하며 이를 위해 IV(Initiation Vector)를 함께 전송해야 한다. IV는 Sequence 번호와 timestamp를 연결하여 생성하며 IV가 sequence 번호와 timestamp의 연결보다 클 때에는 sequence 번호와 timestamp를 계속 반복시켜 생성한다. 공유된 KeyMaterial은 음성 데이터의 암호화에 사용되게 되며 음성 데이터 암호화에 사용될 IV는 암호화키의 암호화에 사용된 IV를 사용한다.

#### 2.4 음성 데이터의 암호화

상기의 과정을 거쳐 호 설정에 대한 인증을 수행하고 음성 통신에 사용될 암호화 알고리즘이 설정되었으며 암호화에 사용될 키와 IV를 결정하였다. 이러한 정보를 이용하여 실제 음성 데이터를 암호화하게 되는데 RTP 패킷의 헤더는 제외하고 RTP 페이로드만을 암호화하게 된다. 페이로드만을 암호화하게 되면 헤더까지 암호화하지 않으므로 암호화 지연을 줄일 수 있으며 수신이 잘못되거나 시간이 지난 RTP 패킷의 헤더정보만을 해석함으로써 복호화하지 않고 바로 삭제할 수 있기 때문에 CPU 자원의 낭비를 막을 수 있는 장점을 갖고 있다.

암호화는 음성 코덱을 거쳐 인코딩된 음성 데이터 프레임을 RTP 패킷에 삽입할 때 이루어지며 이때 블록 단위의 암호화로 인한 패딩을 실시한 후 RTP 패킷에 실어서 전송한다. 수신단에서는 코덱에 의해서 디코딩되기 전에 복호화 과정을 거친다.

#### 2.5 Anti-spamming 알고리즘

Anti-spamming 알고리즘은 RTP 패킷의 replay 공격을 방지하기 위해 제안된 메커니즘이다. replay 공격법을 이용하게 되면 통신 당사자는 음성을 들을 수 없거나 잡음이 섞이게 되어 통신이 불가능하게 된다. 이를 방지하기 위한 anti-spamming 알고리

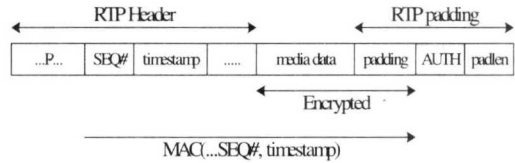


그림 4. Anti-spamming 알고리즘

즘은 그림 4와 같이 RTP 패킷의 뒷부분에 인증 코드를 삽입함으로써 이루어질 수 있으며, 이에 따른 연산 지연이 발생하지만 HMAC 등의 고속 알고리즘을 이용하기 때문에 지연이 크지 않다.

### III. H.235 구현 내용 및 구현 결과

본 논문에서는 Annex D에서 권고하고 있는 보안 사항과 SASET(Secure Audio Simple Endpoint Type)에서 권고하는 단말을 구현하여 실험하였으며 H.235에서 사용하는 보안 알고리즘을 구현, 실험하였다. 결과적으로 단말의 인증, 보안 능력(capability) 교환, 키 분배 및 음성 데이터의 암호화를 구현하였다.

#### 1. 시스템 구현환경

본 논문에서는 VoIP 보안 시스템을 구현하기 위하여 Windows 2000을 운영체제로 하는 Pentium II 시스템을 이용하여 MS Visual C++ 6.0으로 컴파일하여 구현하였으며 네트워크는 일반적인 IP 네트워크를 이용하였고, VoIP의 소스는 openh323.org의 openh323 프로젝트의 공개 소스를 이용하였는데 openh323은 리눅스와 윈도우 운영체제를 지원하는 프로그램이다<sup>[10]</sup>. OpenH323 프로젝트는 ITU-T의 H.323 프로토콜을 기반으로 구현하였고 음성전화, 화상회의 등을 구현하는 프로젝트로 ohphone은 음성 통신을 IP 네트워크에 적용하도록 구성한 프로그램이다. 본 프로그램은 TCP 1720번 포트로 대기하며 연결 요청이 들어오면 UDP와 RTP를 이용하여 양방향(Full Duplex)으로 통신하는 구조이며 GSM, G.711, G.729 등의 음성 코덱을 지원한다.

#### 2. 구현 내용 및 동작 시현

H.235 Annex D를 기반으로 H.323 단말에 구현된 사항은 앞에서 기술한 표준의 내용을 충실하게 따라 구현하였다. 게이트키퍼에 단말을 등록하기 위한 RAS 메시지에 사용자의 패스워드를 기반으로 메시지의 인증을 구현하였고, 호 시그널링을 위한

H.225와 H.245 메시지에 패스워드 기반의 인증과 공유키를 위한 Diffie-Hellman 알고리즘을 추가하였으며 이를 기반으로 미디어 암호화에 사용되는 키를 공유하는 프로토콜과 보안 능력 교환을 구현하였다. 본 연구에서는 음성 암호화를 위해 H.235 annex D에서 권장하고 있는 DES, 3DES 외에 한국형 암호화 알고리즘인 SEED를 구현하였으며 DES의 차기 암호화 알고리즘인 AES도 구현하였다<sup>[11][12]</sup>. 그러나 SEED와 AES 알고리즘의 경우 표준안에 정의되지 않기 때문에 알고리즘의 표기를 nonStandard로 정의하여 사용하였다. 각 알고리즘에 사용되는 랜덤 bit 키의 크기는 DES 56bit, 3DES 168bit, SEED 128bit, AES 128bit이다. 결과적으로 단말의 인증, 보안 능력(capability) 교환, 키 분배 및 음성 데이터의 암호화를 구현하였다. 구현 결과 구현된 모든 기능은 정상 동작하였으며 표준안에서 원하는 동작을 모두 수행하였다. 본 연구에서는 DES, 3DES, SEED, AES의 암호화 알고리즘과 GSM 음성 코덱을 이용하여 실험하였고, 암호화 모드는 CBC 모드를 이용하였다. 구현 결과 보안을 적용하지 않은 H.323 시스템과 비교하였을 때 투명하게 동작하였다.

보안 응용 시스템의 경우, 추가적인 보안 처리로 성능의 저하나 QoS를 떨어뜨릴 수 있으나 구현한 결과, 보안 알고리즘을 적용한 VoIP의 계산량 증가로 인한 지연 증가는 거의 발생하지 않았으며 이에 따른 문제점 또한 발생하지 않았다. 이것은 논문 [13]에서 암호 알고리즘을 적용한 VoIP 시스템의 QoS를 측정할 결과와 같으며, 아래의 표 1은 논문 [13]에서 언급하고 있는 결과에 대하여 각 패킷간 지연 시간 차이의 변화를 알아보기 위한 실험 결과이다. 이 결과에서 전송 전 패킷의 암호화 시점과 패킷 전송 시점, 패킷 수신 시점, 그리고 마지막으로 복호화 시점에서 패킷간 지연시간의 표준편차를 구해 본 것이다. 이 표에서 알 수 있듯이 DES와 SEED, AES 암호 알고리즘은 암호 알고리즘을 적용하지 않은 경우와 거의 유사한 특성을 보였고

표 1. 각 처리 시점에서 패킷간 지연 시간의 표준편차

알고리즘	NO	DES	3DES	SEED	AES
암호화	26.703	26.677	28.733	26.699	26.703
패킷전송	26.722	26.692	28.776	26.728	26.698
패킷수신	26.728	26.725	28.685	26.777	26.715
복호화	17.422	17.424	19.604	17.372	17.446

3DES의 경우 다소 지연 시간의 변화가 확인되었다. 실제로 3DES를 이용하여 암호화를 수행하였을 경우, 지연 시간과 지연 시간의 변화로 약간의 통화품질의 저하를 초래하였다.

호 설정 메시지의 크기는 대폭 증가하였지만 호 처리에 대한 지연 유발은 발생하지 않았다.

### 3. 구현 시 고려 사항

본 연구에서 특별히 고려해야 할 사항은 상호 연동성(Interoperability)과 표준의 문제점이다. 즉, 표준에는 명시되어 있지 않는 사항이나 표준의 표현이 불명확한 경우에 대한 접근을 주관적으로 하였기 때문에 발생할 수 있는 상황에 대한 고려가 필요하다. 또한 표준에 정의되어 있으나 실제 시스코와 같은 네트워크 업계에서 사용되는 방법이 다른 경우에 이러한 제품들과의 호환성을 위해 각 업계의 비표준적인 방법을 모두 구현해 주어야 하는 문제들이다.

첫째로 RAS 메시지에 대한 보안이 각 업체별로 다르게 구현되어 있어 이 것을 연동시키기 위해서는 표준의 인증 방법과 각 업체의 인증 방법을 모두 구현해야 한다. 표준의 인증 방법은 패스워드 기반의 MAC 코드를 이용한 인증 방법을 권고하고 있는데 반하여, 시스코 게이트 키퍼의 경우 표준에서 정의한 필드를 사용하지 않고 기존의 인증 시스템인 Radius(Remote Authentication Dial In User Service)와 연동시키기 위해 CHAP(Challenge Handshake Authentication Protocol) 인증 방법을 사용하여 구현되어 있다. 따라서 시스코 게이트키퍼를 사용하는 경우에는 반드시 CHAP 인증 방법을 통해 Radius 서버에서 인증을 받아와야 한다. 시스코 뿐만 아니라 각 업체별로 다른 RAS 인증 방법을 사용하고 있으므로 ITU-T에서는 업계의 요구 사항을 반영하고 통일된 인증 방법을 사용하여 H.323 프로토콜의 보안에 호환성을 갖추어야 할 것이다.

둘째로 암호화 알고리즘 설정 시 결정 방법에 따른 문제의 발생이 가능하다. H.323에서는 송수신의 음성 코덱을 다르게 사용할 수 있도록 정의되어 있다. 이것은 양 단말이 사용하는 음성 코덱이 다를 경우를 대비한 것인데, 암호화라는 점에서는 같은 방법을 사용하는 것에 대한 분석이 필요하다. H.235에서는 마스터가 암호화에 사용될 키를 슬레이브에게 전달하도록 되어 있는데 이는 두 단말이 같은 암호화 알고리즘을 사용한다는 것을 의미할 수 있고, 일반적인 보안 프로토콜의 암호화 시에도 역시

양단간 같은 알고리즘을 사용한다. 또한 미디어 암호화를 위한 알고리즘은 키를 암호화한 알고리즘과 같은 알고리즘을 사용하도록 되어 있는데, 키의 전달이 먼저 수행되고 이후에 보안 capability를 교환하게 되므로 보안 capability의 교환이 별 의미를 갖지 못한다. 따라서 본 연구에서는 키의 암호화에 사용된 알고리즘을 미디어의 암호화 알고리즘으로 선택하도록 하였다.

이러한 구현상 고려할 사항들은 표준안에는 명시되어 있지 않기 때문에 표준의 해석 방법에 따라 이러한 방법을 이용하지 않는 다른 H.235 기반 VoIP 보안 시스템과의 연동 시 문제가 발생할 수 있다. 따라서 표준에서는 이러한 점을 명확하게 제시하여야 한다.

추가로 구현된 H.235 시스템의 문제점으로는 보안 capability 교환 시 보안 알고리즘의 nonStandard 교환을 들 수 있다. 표준에서는 DES, RC2, 3DES를 지원하도록 권고하고 있지만 AES나 SEED와 같이 다른 알고리즘에 대한 OID는 정의하고 있지 않기 때문에 비표준 번호로 정의해서 사용하였다. 이는 다른 H.235 기반 VoIP 보안 시스템과 상호 운영이 불가능할 수도 있음을 보여주고 있으며 이에 대한 다음 버전의 표준화 동향 및 개발자 동향을 파악할 필요가 있다. 또한 본 논문에서 구현한 SEED, AES는 표준안에서 권고하고 있는 암호화 알고리즘이 아니므로 상호 운영 측면에서의 이용은 불가능할 것으로 보이지만 새로운 암호화 알고리즘을 적용할 수 있는 용이한 방안과 구현을 통해 알고리즘의 검증을 제시할 수 있었다. 또한, ARM7TDMI 프로세서와  $\mu$  Clinux를 운영체제로 하는 임베디드 환경에서 구현해 본 결과, 사용된 알고리즘 중에서 Diffie-Hellman은 계산에 많은 시간이 소요되는 알고리즘으로 일반 PC에서는 상관없지만 VoIP 시스템이 임베디드 환경의 계산 능력이 낮은 CPU를 사용하는 시스템에 탑재되는 경우, 초기 호 설정에 수초의 많은 지연 시간이 발생하였다. 따라서 표준 설계 시에 알고리즘의 운영 환경과 운영 성능을 고려해야 할 것이다.

#### IV. 결론

본 논문에서는 ITU-T에서 제안하는 H.323 시스템의 보안 프로토콜인 H.235를 구현하고 실험하여 문제점을 분석하는 연구를 진행하였다. H.235 보안 프로토콜 및 알고리즘을 분석하고 H.235 annex D

에서 제안하는 보안 기능들에 대한 동작 실험을 완료하였으며 동작 결과를 도출하고 문제점을 분석하였다.

표준안에서 정의하고 있는 보안 기능들에 대한 구현은 openh323.org의 공개 프로젝트에 구현할 수 있었으며 정상적인 기능 수행을 확인할 수 있었고 HMAC을 이용한 H.225.0 메시지 인증, Diffie-Hellman 키 교환 알고리즘에 의한 키 생성, 보안 capability 교환, 음성 암호화키 생성 및 교환에 대한 구현 단계까지의 자세한 사항을 분석하고 구현하였으며 구현 후 성능과 데이터 전송량에 대한 분석을 실시하였다.

구현한 결과 예상되었던 암호화 연산에 의한 지연은 거의 발견되지 않았으며 이는 CPU의 처리속도가 음성 처리에 대한 연산량보다 크기 때문으로 사료되며 H.235 보안이 구현되지 않은 시스템과의 운영도 문제없이 동작하였다.

본 논문에서 구현한 VoIP 보안 시스템은 상호연동성(Interoperability)에 대한 테스트가 이루어지지 않아 계속적인 개발 및 표준화 동향 분석이 이루어져야 할 것이다. 또한 H.235에서 선택적으로 지원할 수 있도록 정의한 media anti-spamming에 대한 연구 및 구현이 선행되어야 한다. 이와 함께 H.235의 프로토콜 측면에서의 보안 취약점 및 단점 등에 대한 연구 또한 수행되어야 할 것이다.

#### 참고 문헌

- [1] H.235 v2, "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," ITU-T, 2000
- [2] H.323 v4, "Packet-based multimedia communications systems," ITU-T, 2000
- [3] H.225.0, "Call signaling protocols and media stream packetization for packet-based multimedia communication systems," ITU-T, 2000
- [4] H.245, "Control Protocol for Multimedia Communication," ITU-T, 2000
- [5] H.235 v2 Annex.D, "Baseline Security Profile," ITU-T, 2000
- [6] H.235 v2 Annex.E, "Signature Security Profile," ITU-T, 2000
- [7] PKCS #3, "Diffie-Hellman Key-Agreement Standard version 1.4," RSA lab., 1993
- [8] H.323 Annex.J, "Security for H.323

Annex.F(SASET),” ITU-T, 2000

[9] RFC 2104, “HMAC: Keyed-Hashing for Message Authentication”, IETF, 1997

[10] http://www.openh323.org “OpenH323 Project”

[11] TTAS.KO-12.0004 , “128비트 블록암호알고리즘 표준(SEED),” 한국정보통신기술협회, 1999

[12] Joan Daemen, Vincent Rijmen, “AES Proposal: Rijndael,” NIST, 1999

[13] 홍기훈, 임범진, 정수환, “암호화 연산에 따른 VoIP QoS 측정 및 분석,” 한국정보보호학회 종합학술발표회 논문집 Vol.11, No.1, pp. 223-227, Nov. 2001.

1998년~현재 : 숭실대학교 정보통신전자공학부 조교수

<주관심 분야> VoIP security, Security Protocol, 사용자 인증, Cryptography

유 현 경(Hyun-Kyung Yoo)

정회원



1997년 2월 : 한밭대학교

정보통신공학과 졸업

2000년 2월 : 충남대학교

정보통신공학과 석사

2000년 4월~현재 :

한국전자통신연구원

VoIP 기술팀 연구원

<주관심 분야> VoIP, VoIP security, VoIP codec

임 범 진(BumJin Im)

학생회원



2000년 2월 : 숭실대학교

정보통신공학과 학사

2002년 2월 : 숭실대학교

정보통신공학과 석사

2000년 3월~현재 :

삼성종합기술원

<주관심 분야>통신망보안, VoIP 보안

김 도 영(Do-Young Kim)

정회원



1985년 2월 : 성균관대학교

전자공학과 졸업

1987년 2월 : 성균관대학교

전자공학과 석사

1987년 2월~현재 :

한국전자통신연구원

네트워크연구소 VoIP

기술 팀장

2000년 12월~현재 : VoIP 포럼 H.323 기술분과위원장

<주관심 분야> VoIP, 고속 실시간 QoS 데이터처리, 멀티미디어 게이트웨이, 신호게이트웨이

홍 기 훈(Kihun Hong)

학생회원



2000년 2월 : 숭실대학교

정보통신공학과 학사

2002년 2월 : 숭실대학교

정보통신공학과 석사

2002년 3월~현재 : 숭실대학교

정보통신공학과 박사과정

<주관심 분야>멀티미디어보안, 네트워크보안, 멀티캐스트 보안

정 수 환(Souhwan Jung)

정회원



1985년 2월 : 서울대학교

전자공학과 졸업

1987년 2월 : 서울대학교

전자공학과 석사

1988년~1991년 : 한국통신

전임연구원

1996년 : 미 워싱턴

주립대(시애틀) 박사

1996년~1997년 : Stellar One SW Engineer