# VoIP 보안 시스템의 QoS 측정 및 분석

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

# Impact of Cryptographic operations on the QoS of VoIP system

**Ki-Hun Hong*** *student member*,
**Sou-Hwan Jung*, Hyun-Kyung Yoo**, Do-Young Kim**** *regular members*

요 약

본 논문에서는 VoIP의 보안을 위하여 적용된 암호화와 보안 적용 방식이 실시간 통신에 미치는 영향을 알아보기 위해 암호화에 주로 사용되는 DES, 3DES, SEED, AES 등의 암호 알고리즘을 VoIP에 적용한 후 지터나 RTT, 패킷 손실률 등의 여러 가지 QoS 요소를 측정하여 보았다. 또한 각 알고리즘별 암·복호화 전과 후의 패킷 처리 시간 간격을 측정하여 암호화로 인한 시간 간격의 변화를 알아보았고, 음성으로 재생되기 직전의 처리 시간 간격을 측정하여 각 패킷이 어느 정도 주기적으로 공급되는지 여부와 실제 음질을 비교하여 보았다. 또한 대표적인 실시간 멀티미디어 보안 프로토콜인 H.235와 SRTP에서의 RTP 보안 적용 방식을 비교하여 키 교환 및 보안성과 공격 방어 측면 그리고 RTP 보안 적용의 효율성 등을 분석하였다.

Key Words : VoIP; Security; QoS.

ABSTRACT

The encryption of packets increases delay and delay jitter that may degrade the quality of service (QoS) in real-time communications. So, we analyzed the delay jitter, delay, and interval delay between consecutive packets which were encrypted by the DES, 3DES, SEED and AES algorithms in this study. The interval delay and jitter of three algorithms such as the DES, SEED, AES were similar to the results of no encryption. But in the case of 3DES, the encryption of packets increases the variance of interval delay and jitter in comparison with other algorithms. we also analyzed properties of security and an efficiency of RTP security between SRTP and H.235.

## I. 서 론

인터넷 멀티미디어 기술과 네트워크 고속화 기술의 발전에 힘입어 VoIP(Voice over IP), 화상 통신, VoD(Video on Demand) 서비스, 동영상 강의나 동영상 쇼핑 등 많은 미디어 응용 서비스가 현재 제공되고 있는 가운데 가장 많은 관심의 대상이 VoIP 서비스이다. VoIP는 기존의 공중전화망(PSTN) 기반의 전화 서비스를 대체할 인터넷 기반의 서비스이며 특히 외국과 같이 상당한 원거리의 사용자에게는 전화비용의 부담을 줄여 줌으로써 사용이 급격히 증가하고 있고 많은 VoIP 관련 기업들의 연구가 진행되고 있어 음질의 향상을 보이고 있다. 그러나 인터넷은 공개된 네트워크로 사용자의 인증 없이 누구나 접속하여 사용할 수 있는데 VoIP는 인터넷을 이용한 응용 서비스이므로 음성 패킷의 안전성을 보장하지 못하며 도청자가 통화 내용을 도청하거나 패킷을 변조하여 악용할 소지가 충분하다. 반면에 네트워크 기술은 일반화되고 있으며 여러 가지 해킹 도구들도 인터넷을 통해 유포되고 있어 이제 전문적인 지식을 가지지 못한 학생이나 일반인들도 해킹을 쉽게 할 수 있는 실정이다. 이러한 해킹을 막기 위한 방법으로 기존의 보안 프로토콜

* 숭실대학교 정보통신전자공학부 통신망 보안 연구실 (souhwanj@ssu.ac.kr),
** 한국전자통신연구원 네트워크기술연구소 네트워크서비스연구부 VoIP 네트워크연동팀
논문번호: 020103 - 0308, 접수번호: 2003년 3월 8일
※본 연구는 한국전자통신연구원 위탁수행과제 지원으로 수행되었습니다.

을 이용한 방법들이 제시되고 있다. 인터넷 보안의 필요성에 따라 SSL(Secure Socket Layer), SET (Secure Electronic Transactions), PGP(Pretty Good Privacy)등의 여러 가지 기존 보안기술들이 응용되어 사용되고 있다. 그러나 이 기술들은 서비스 별로 요구에 따라 각 응용계층에 맞추어 설계된 보안 프로토콜이기 때문에 실시간 통신에 최적화되어 있지 못하다. SSL은 트랜스포트 계층의 보안 프로토콜로서 암호화 소켓 채널을 통해 전송하는 방식으로 현재 가장 널리 사용되고 있으나 주로 웹브라우저용으로 사용되고 있다. SET은 단순한 암호화 기법이 아닌 전반적인 전자상거래의 지불구조를 정의하고 여기에 인증체계와 암호화 기술을 더하여 만들어진 종합적인 보안시스템이므로 인터넷폰 등의 실시간 보안 통화 시스템에 사용되어질 수 없다. 그리고 PGP 역시 전자메일을 위한 특정 분야를 지원하는 프로토콜이므로 적용에 어려움이 있다[1].

현재 VoIP을 위한 보안 프로토콜로는 ITU-T에서 H.323의 보안을 지원하기 위해 만든 H.235가 대표적이고 IETF에서는 SIP(Session Initiation Protocol)를 위한 보안 관련 문서들도 발표되고 있으나 SIP에서는 RTP 보호에 대한 부분을 아직 고려하고 있지 않다. 그러나 IETF의 Audio/Video Transport 워킹그룹에서 RTP를 보호하기 위해 SRTP(The Secure Real-time Transport Protocol)가 인터넷 드래프트로 제안되어 있는 상태이다. 실시간 통신 시스템에서 보안의 적용은 보안 프로토콜을 위한 시그널링과 음성 패킷의 암호화로 나눌 수 있는데 VoIP 보안 서비스의 질은 보안 적용 후 음질에 미치는 영향이 가장 주요한 요소가 될 것이다. 이러한 음질의 저하를 지터와 지연 시간 또는 암·복호화 전과 후의 패킷간 지연 시간 변화율 등의 QoS 요소를 측정하여 음질에 미치는 영향을 알아보았다. 또한 패킷에 보안을 적용 후 VoIP 서비스를 방해하기 위한 공격들에 대하여 어떤 인증 방법이 VoIP 서비스를 유지할 수 있는 지와 보호 범위, 암호화 적용 방법에 따른 계산 지연 시간 그리고 보안 적용으로 인하여 전송 시 에러의 전파 정도 등 음질에 악영향을 미칠 수 있는 요소들을 H.235와 SRTP 기반으로 분석하였다.

이 논문에서는 우선 II 장에서 VoIP 보안 프로토콜의 종류와 구성을 살펴보고 III 장에서는 보안 VoIP 시스템의 QoS 요소 측정 및 실험을 통해 보안 적용이 서비스의 질에 미치는 영향을 알아보았다. IV 장에서는 H.235와 SRTP를 패킷 인증과 보호 범위, 암호화 모드에 따른 계산 지연 시간, 그리고 에러 전파 측면에서 분석하였다. 마지막으로, V 장에서는 결론으로 실시간 보안 시스템이 갖추어야 할 보안 적용 방향에 대하여 기술하였다.

## II. VoIP 보안 기술

### 1. H.235

H.235는 ITU-T에서 제안한 H.323을 위한 보안 프로토콜로서 VoIP에서 보안 시그널링을 통해 음성 패킷을 암호화하여 도청을 방지하기 위한 기밀성과 패킷의 무결성 제공을 목적으로 한다. H.323 단말은 게이트키퍼와의 RAS 절차에서 패스워드를 이용한 사용자의 인증과 메시지의 무결성을 제공하며 H.225 에서는 메시지의 인증과 무결성 및 세션키의 암호화를 위한 Diffie-Hellman 키 생성 등의 세 가지 보안 기능을 갖는다. H.245에서는 음성 데이터의 암호화에 사용될 암호화 알고리즘의 단말 보안 지원 여부(Security capability)를 교환하며 음성의 암호화에 사용될 키를 생성하여 Diffie-Hellman 키로 암호화하여 전송하고 공유된 키를 사용하여 음성 패킷을 암호화하여 전달하며 수신측은 암호화된 패킷을 복호화하여 음성을 재생함으로써 공개된 네트워크인 인터넷에서 도청을 방지할 수 있다. 또한 DoS(Denial-of-Service)공격을 막기 위해 Media Anti-spamming 기능을 사용하여 패킷의 정당성 여부를 빠르게 판단함으로써 공격으로 인한 시스템의 과부하를 막는다[2].

### 2. SIP 보안

IETF에서 작업중인 SIP에서는 보안을 위한 새로운 메커니즘을 정의하지 않고 주로 기존에 사용하고 있는 보안 메커니즘을 사용한 보안 모델을 제시하고 있으며 HTTP나 SMTP 같은 프로토콜에서 사용되는 방법을 적용하고 있다. SIP 보안에서 중요한 요구 사항으로는 여러 가지 다양한 환경과 응용 프로그램에 적용할 수 있는 보안 메커니즘과 최소의 복잡성을 필요로 하고 있어 새로운 기반 구조나 알고리즘의 확장은 지양하고 있다. RFC 2543에서는 기존의 HTTP에서 사용하고 있는 basic과 digest 인증 방법을 SIP에서 제시하였고 PGP 암호화 방법을 사용하여 end-to-end 메시지 암호화 방법을 제시하였다. 그러나 PGP 암호화 방법은 키 교환 방법 확장성 등의 문제점으로 인해 2543bis version 3에서

는 이를 제거하게 되었다. 따라서 2002년 1월에 발표된 2543bis version 6에서는 end-to-end 메시지 암호화를 위한 방법으로 S/MIME을 새롭게 제시하였고 현재는 RFC 3261이 표준이며 세션 시그널링만을 정의하고 있으므로 RTP를 보호하지 않는다[3].

### 3. SRTP

SRTP는 IETF에서 오디오 및 비디오 전송 부문을 연구하는 avt(Audio/Video Transport) 워킹 그룹에서 RTP 데이터 보호를 위해 제안한 인터넷 드래프트 상태의 프로토콜이다. SRTP 드래프트는 SRTP와 SRTCP를 정의하여 RTP와 RTCP를 모두 보호하며 암호화와 인증을 지원한다. RTP 데이터 보호인 만큼 키 교환 메커니즘은 정의하지 않으며 키가 다른 방법에 의해 교환되었다는 가정 하에서 교환된 마스터 키와 마스터 salt키를 이용하여 세션의 암호화와 인증에 사용되는 세션 암호화 키, 세션 인증 키, 세션 salt 키 등을 생성하며 패킷 인덱스와 키 추출 비율을 사용하여 패킷의 일정 비율마다 키를 다르게 생성하여 사용할 수 있도록 하였다. 암호화 알고리즘은 현재 AES(Advanced Encryption Standard)를 지원하며 운영 모드는 카운터 모드와 f8 모드를 지원한다[4].

## Ⅲ. VoIP 보안 시스템의 QoS 요소 측정 및 분석

### 1. 개요

VoIP에 RTP 패킷 암호화를 적용하여 실제 사람의 귀를 통해 인식되는 통화 품질이 시스템에 따라 다소 저하되는 것을 감지할 수 있었다. 이는 암·복호화 과정이 추가되어 음성 패킷의 처리에 추가적인 시간이 소요되기 때문이며 실시간 통신에서 적합한 암호 알고리즘을 찾고, 각 암호 알고리즘에 대한 QoS 요소를 측정하고 분석하여 암호화가 음질에 미치는 영향을 파악하기 위한 목적으로 실험을 하였다. 이 실험에서는 음질에 가장 많은 영향을 줄 수 있는 지터와 RTT(Round-Trip Time)를 측정하고 패킷 손실률과 순서가 바뀐 패킷의 수, 지터 버퍼 크기의 시간 내에 도착하지 못한 패킷의 수 그리고 패킷을 처리하는 시점의 변화 등을 측정하였다. 지터는 도착하는 각 패킷의 시간차에 대한 변화율을 의미하는 것으로 이 것은 지터 버퍼의 크기를 벗어날 경우, 음성을 재생할 시간 안에 도착하지 못하므로 음질이 끊어지는 현상을 초래한다. RTT는 상대방과의 패킷 전달 시간을 측정하기 위한 요소로서 실시간 통화에서 지연 시간이 길게 되면 상호간의 통화가 불가능하게 된다. 패킷 손실률은 패킷 자체가 인터넷을 통해 라우팅 되는 중간에 여러 가지 원인으로 인하여 목적지에 도착하기 전에 사라져서 음성을 재생하지 못하게 된다. 인터넷은 데이터그램 방식이므로 라우팅되는 중간에 네트워크의 사정에 따라 라우팅되는 경로가 달라질 수 있다. 이러한 경우 패킷은 전달되는 순서가 바뀌어 도착하게 되는데 실시간으로 음성을 재생하는 인터넷폰의 경우 이러한 패킷을 순서에 맞추어 이전 패킷이 도착할 때까지 재생을 중단 할 수 없으므로 패킷의 손실로 볼 수 있다. 패킷이 처리되는 각 시점의 변화는 암·복호화 이전 혹은 이후에 각 패킷이 처리되는 시간 간격을 측정하여 음성이 재생되기 직전에 원활히 음성 프레임이 공급되는지 등을 파악할 수 있다. 이 실험에서는 위와 같은 요소들을 암호화 알고리즘을 변화시키며 측정하고 분석하여 각각의 알고리즘들이 음질에 미치는 영향에 대하여 살펴보았다.

### 2. 측정 시스템 및 환경

실험은 4가지의 암호 알고리즘을 각각 RTP에 적용하여 알고리즘에 따른 QoS 파라미터의 차이를 알아보았다. 이 실험에 사용되는 암호 알고리즘은 DES(Data Encryption Standard), 3DES, SEED, AES(Advanced Encryption Standard)등이며 시그널링은 암호화가 적용되지 않고 음성에만 암호화를 적용하였으며 운영 모드는 CBC(Cipher Block Chaining) 모드를 사용하였다.

그림 1에서 볼 수 있듯이 VoIP 모듈에 4개의 암호 알고리즘을 추가하여 보안을 적용하지 않은 트래픽을 포함한 총 5가지의 트래픽에 대한 QoS 파

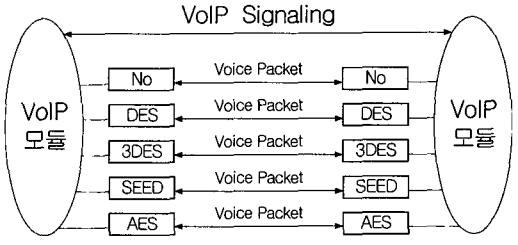


그림 1. QoS 실험을 위한 구성

라미터를 측정하였다. 실험 환경은 IP Phone과 같은 적은 자원을 가진 시스템을 고려하여 펜티엄

233㎒ 64MB 메모리의 시스템을 사용하였고, VoIP 시스템은 OpenH.323 프로젝트를 사용하였으며 네트워크 혼잡에 의한 실험의 오차를 줄이기 위해 두 대의 컴퓨터는 크로스 케이블을 이용하여 직접 연결하였다[7]. 실험은 각각의 암호 알고리즘에 대하여 총 3회를 실시하였으며 이 값들을 모두 측정치 계산에 사용하였다.

## 3. QoS 요소의 측정 및 분석

### 1) 지터의 측정과 분석

지터는 앞에서 언급한 바와 같이 도착하는 패킷 간의 지연 시간 변화율을 의미한다. 우선 지터를 구하기 위해서는 interval 지연 시간을 계산하여야 하는데 다음의 식(1)로 표현할 수 있다. R(n)은 수신 시스템에서 n번째 패킷을 수신한 시간을 의미하며, S(n)은 송신 시스템에서 n번째 패킷을 전송한 시간을 의미한다. 즉, D(n)은 n번째 패킷과 n-1번째 패킷의 시간 간격이 송수신을 통해 증감하는 시간을 의미한다.

$$D(n)=(R(n)-R(n-1))-(S(n)-S(n-1)) \quad (1)$$

위의 식(1)에서 구한 지연 시간을 이용하여 아래의 식(2)와 같이 지터를 표현할 수 있다[8].

$$J(n)=\frac{15}{16}J(n-1)+\frac{D(n)}{16} \quad (2)$$

지터를 측정하기 위해 사용된 인터넷폰의 지터 버퍼는 50msec으로 설정하여 지터를 측정하였다. 이 지터 버퍼는 가변적인 도착 시간의 간격을 완충하는 역할을 하기 위해서 설정하는 버퍼로 설정된 버퍼의 크기 이하로 패킷이 일찍 도착하면 음성의 재생이 가능하지만 그 이상이면 정상적인 음성의 재생이 불가능하다. 그러나 지터버퍼는 VoIP 통신

표 1. 50msec내에 도착하는 패킷의 백분율

| 지터 버퍼 / 알고리즘 | 50 msec |
|---|---|
| No encryp. | 98.50 % |
| DES | 98 % |
| 3DES | 94.06 % |
| SEED | 98 % |
| AES | 95.59 % |

에서 지연시간을 추가시키므로 과대한 지터 버퍼는 정상적인 통화에 악 영향을 줄 수 있다.

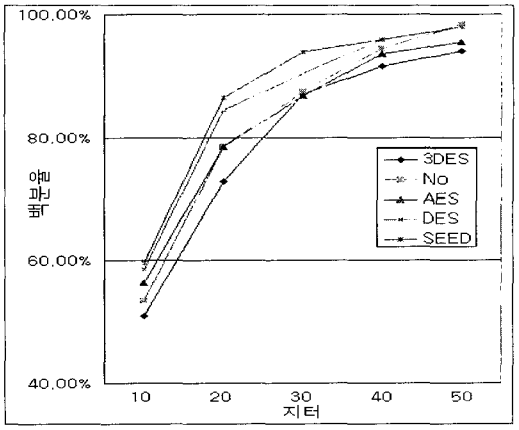


그림 2. 지터에 따른 패킷의 누적 백분율

표 1에서 볼 수 있듯이 50msec 이내에 도착한 패킷의 백분율을 보면 유사한 값을 나타내지만 암호화를 적용하지 않은 경우와 DES 그리고 SEED를 적용한 경우, 98 % 이상의 많은 패킷이 지터 버퍼의 범위 안에 도착하였다. 그림 2는 10msec 에서 50msec 까지의 지터에 따른 패킷수를 누적 백분율로 표시하여 그린 그림이다. 10msec 이하와 50msec 이상은 커다란 차이를 보이지 않아 제외하였다. 이 그래프에서 SEED를 적용할 경우 작은 지터값을 갖는 것을 알 수 있고, 50msec 누적 분포를 보면 암호를 적용하지 않은 경우가 98.5%로 가장 좋은 결과를 나타내었다. 그러나 3DES를 적용한 경우, 50msec까지 전반적으로 가장 적은 패킷의 분포를 보이고 있는데 DES 암호화를 세 번 수행하는 3DES의 특성으로 인하여 가장 암호화 시간이 길기 때문으로 분석된다.

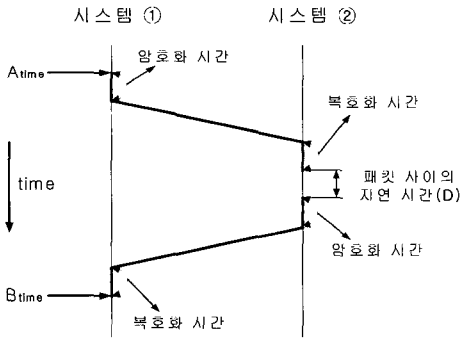


그림 3. RTT 측정 모델

### 2) RTT의 측정과 분석

RTT은 네트워크 상에서 상대방에게 요청한 응답

이 전송되는 시간과 응답이 수신되는 시간의 합을 의미하는데 이것은 요청 패킷이 시스템을 출발하여 도착한 시간과 요청을 수신한 시스템에서 응답한 패킷이 도착한 시간을 의미하므로 VoIP 응용프로그램에서 암호화하는 시간이 제외된 것이다. 따라서 암호화와 복호화가 포함된 RTT을 측정하기 위해서 실제 전송되는 음성 패킷을 이용하여 그림 3과 같은 측정 모델을 사용하였다. 그림 3은 RTT를 측정하기 위한 모델로서 일반적인 RTT 측정 모델에 암호 알고리즘의 연산 시간을 포함한 것이며 아래의 식(3)과 같이 암호화가 포함된 RTT를 구할 수 있다.

$$RTT = B_{time} - A_{time} - D \qquad (3)$$

RTT는 시스템 ①에서 암호화가 수행되기 직전 즉, $A_{time}$ 의 타임스탬프를 저장하고 시스템 ②에게 요청 패킷이 전달되어 복호화한 후에 다시 시스템 ①에 응답이 도착하여 복호화되는 시점 B의 타임스탬프를 저장하여 B에서 A를 감산함으로써 계산된다. 그러나 응답을 보내온 시스템 ②에서 요청 패킷을 받은 후 응답 패킷이 생성되어 보내기 직전까지의 시간 D는 RTT에 포함되지 않아야 하므로 역시 감산하였다.

표 2는 실험을 기반으로 한 RTT의 평균값으로서 암호화를 적용하지 않은 경우가 가장 낮고 DES 알고리즘이 적용된 경우 가장 큰 것을 볼 수 있다. 그러나 RTT는 요청과 응답에 의해 주기적으로 측정하였고 RTP의 페이로드가 132 bytes로 그리 크지 않기 때문에 암호화에 그렇게 많은 시간이 소요되지 않음을 예상 할 수 있다. 실제로 실험을 통해 132 bytes의 데이터를 암호화하는 시간을 측정하여 보았다. 그러나 암호화 수행 시간만을 측정하기에는 윈도우즈 2000 운영체제의 시간 정밀도는 세밀하지

표 3. RTT 평균.

| 알고리즘 | RTT 평균 |
|---|---|
| No encryp. | 0.18286 sec |
| DES | 0.21200 sec |
| 3DES | 0.20189 sec |
| SEED | 0.19768 sec |
| AES | 0.20739 sec |

못하였다. 추가로 패킷 손실률과 순서가 바뀐 패킷(Out of order)의 수 그리고 지터 버퍼 크기의 시간

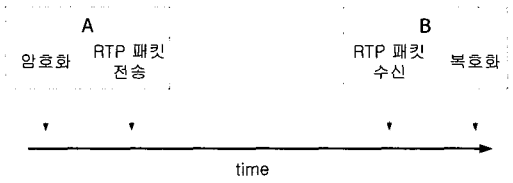


그림 4. Interval 지연 시간 측정

내에 도착하지 못한 패킷의 수 등을 측정하였으나 거의 발생하지 않았다.

3) 패킷 Interval 지연 시간의 측정과 분석

각각의 패킷이 전송되거나 수신되는 시간의 변화를 측정하기 위하여 패킷을 암호화한 시점과 패킷을 전송하기 직전, 패킷을 수신한 시점 그리고 패킷의 음성 부분을 복호화하여 재생하기 직전의 시간을 측정하여 각 패킷간의 시간차를 계산해 보았다. 그림 4는 시스템 A에서 B로 RTP 패킷이 전송되는 과정 중에서 앞에서 언급한 4가지 시점을 나타내고 있다. PC의 성능에 따라 다른 값을 측정하기 위해 A 시스템은 펜티엄 233㎒ 64 MB이며 B 시스템은 펜티엄 733㎒ 128 MB를 사용하였다.

패킷간의 시간차의 측정은 패킷의 전송 혹은 수신 시점을 측정하고 그 다음 패킷에서 측정된 시간을 이용하여 차를 계산하였다. 이러한 차분값은 각 지점에서 패킷의 처리 시간이 규칙적으로 처리되는지의 여부를 알아보는 것으로 실시간 통신인 VoIP 시스템에서 적절한 시간 내에 각 시점에 패킷이 도착하는지 파악하여 음성의 재생이 잘 수행되는지 여부를 알아볼 수 있다.

$$diff = currentPacketTime - lastPacketTime \qquad (4)$$

측정한 diff 값은 변화가 거의 없이 일정하게 유지되어야 실시간 음성의 재생에 안정적으로 음성 프

표 2. A에서 B로 가는 패킷에서 diff의 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 |

레임을 제공해 줄 수 있다. 따라서 diff 값의 변화 정도를 알아보기 위해 diff 값의 표준 편차를 구하

표 4. B에서 A로 가는 패킷에서 diff의 표준편차

| 알고리즘 | NO | DES | 3DES | SEED | AES |
|---|---|---|---|---|---|
| 암호화 | 0.258 | 0.236 | 0.291 | 0.308 | 0.233 |
| 패킷전송 | 0.259 | 0.240 | 0.297 | 0.316 | 0.241 |
| 패킷수신 | 4.283 | 4.206 | 11.367 | 4.113 | 3.966 |
| 복호화 | 29.323 | 29.313 | 31.694 | 29.350 | 29.313 |

여 변화 정도를 알아보았다. 다음의 표 3은 그림 4의 상황에서 시스템 A에서 시스템 B로 가는 트래픽에 대한 diff 값의 표준 편차를 보여주고 있다. 표 3에서 볼 수 있듯이 3DES을 제외한 다른 암호 알고리즘이나 암호화를 하지 않은 경우에는 거의 유사한 값이 나오는 것을 볼 수 있으며 3DES의 경우 상대적으로 큰 값이 나오는 것을 볼 수 있다.

표 4는 앞에서 본 표 3과 반대로 시스템 B에서 시스템 A로 가는 트래픽에 대하여 측정한 값이다. 표 4에서 보여주는 시스템 B에서 A로 가는 패킷의 측정값은 전송 시 SEED의 경우가 많은 변화가 일어나고 있는 것을 볼 수 있으나 복호화 직후의 시점에서는 3DES가 가장 큰 표준편차 값을 보여주고 있다. 4 곳의 시점 중에서 가장 관심을 가지고 보아야 할 곳은 복호화 직후의 시점으로 실제적인 음성의 재생은 음성 프레임의 복호화 후에 코덱 처리 부분으로 넘어가 사운드 장치로 보내지므로 이 시점에서의 변화율이 음성 재생에 가장 커다란 영향을 미치게 된다. 따라서 A에서 B로 혹은 B에서 A로 가는 패킷에 대한 측정치 중에서 복호화 직후에 측정된 diff 값의 변화 정도를 보면 3DES가 가장 크게 변화하는 것을 알 수 있다. 이 것은 실제로 암호화하는 속도를 보아도 알 수 있는데 3DES는 보안의 강도를 높이기 위해 DES의 암호화 과정을 3번 반복하여 수행하기 때문에 DES에 비해 3배의 시간과 연산이 필요하다. 따라서 알고리즘별 암호화 연산 시간을 측정하기 위하여 대량의 데이터를 이용하여 암호화를 수행하고 이를 시간으로 나누어 표 5의 암호화 속도를 얻을 수 있었다. 표 5는 펜티엄 733㎒ 128 MB의 환경에서 암호화 속도를 측정한 값이다.

표 5에서 볼 수 있듯이 3DES의 암호화 속도가 31.966Mbps로 가장 느린 것을 알 수 있고 DES나 SEED는 유사한 수치이며 AES가 가장 빠른 것을 알 수 있다. 그러나 암호화 시간은 매우 적은 시간으로 DES 이상의 속도를 가지는 알고리즘은 암호

표 5. 알고리즘별 암호화 속도

| 알고리즘 | 암호화 속도 |
|---|---|
| DES | 95.612Mbps |
| 3DES | 31.966Mbps |
| SEED | 85.997Mbps |
| AES | 168.111Mbps |

화하지 않은 패킷의 시간과 비교하여 볼 때, VoIP 패킷의 처리에 거의 영향을 주지 않는 것을 알 수 있었다. 그러나 3DES 알고리즘은 상대적으로 느린 속도를 보이며 이 것은 패킷의 처리에 추가적인 과부하를 제공함으로써 음성 재생 시간을 불규칙적으로 변화시켜 음질을 저하시키는 것을 실험을 통해 알 수 있었다.

4) 3DES 알고리즘 적용

패킷의 크기 자체가 크지 않으므로 그리 커다란 지연 시간이 발생하지 않지만 암·복호화 시간에 의해 주기적이어야 하는 패킷의 처리 시간에 불규칙적인 요소가 포함되어 있다. 실험 결과 3DES가 암호화 속도의 저하로 실시간 통신에 다소의 악영향을 주는 것을 알 수 있었는데 H.235나 IPsec등의 프로토콜에서 3DES를 기본 암호화 알고리즘으로 채택하고 있다. 더욱 문제되는 것은 IP 단말기나 게이트웨이의 경우, PC에 비해 상당히 적은 속도의 프로세서를 사용하기 때문이다. 따라서 실시간 통신에 3DES을 적용하여 사용할 수 있는 PC의 성능을 파악하여 보았다. 이 실험을 위해 733㎒의 PC와 각각 133, 233, 350㎒ 의 CPU와 64MB 메모리를 가지는 PC에서 3DES가 적용된 VoIP로 실험을 하여 실제 사람이 귀로 인식하는 것과 diff 실험값을 측정하여 보았다. 표 6에서의 수치는 주로 음질에 실질적인 영향을 미치는 수신시와 수신 후 복호화시 diff의 표준편차인데 133㎒ PC의 경우 거의 말을 구분할 수 없었고, 패킷이 대부분 도착하나 복호화 후에 음성을 재생하는 시점에서 시간 간격의 불규칙성이 증가하여 측정한 3000개의 패킷 중에서 복호화시에 거의 50%에 가까운 1406개의 패킷이 재생되지 못하고 버퍼에서 버려졌다. 반면에 233㎒은 수신시의 diff 표준편차는 컸지만 지터 버퍼의 영향으로 복호화시 이후에는 133㎒에 비해 상대적으로 적은 수치를 보여주며 대부분의 패킷이 정상적으로 처리되어 암호화가 적용된 패킷도 정상적으로 처리

표 6. 수신시와 복호화시 diff의 표준편차

| CPU | 수신시 | 복호화시 |
|---|---|---|
| 133㎒ | 5.51 | 146.92 |
| 233㎒ | 11.36 | 31.69 |
| 350㎒ | 0.48 | 9.24 |

되어 안정적인 음질을 나타냈다. 350㎒ PC는 더욱 안정적인 수치와 음질을 보여주고 있으며 따라서 최소한 233㎒ 이상의 PC에서 보안을 적용한 VoIP의 사용을 권장한다.

지금까지 보안 VoIP 시스템에서 통화 음질에 초점을 맞추어 RTP 패킷의 암호화 성능을 실험 및 분석하여 보았다. 그러나 이러한 문제는 시스템의 성능을 높이거나 암호화 전용 칩을 사용하여 지연 시간을 크게 줄일 수 있다. 따라서 IV장에서는 보안 프로토콜이나 키 교환 문제 그리고 패킷 인증 문제를 통한 QoS와 보안성 분석을 하여 보았다.

## Ⅳ. RTP 보안 적용 방식 분석

### 1. H.235와 SRTP

실시간 기반의 멀티미디어 통신에 사용되는 RTP 패킷을 보호하기 위해 표준화되고 있는 프로토콜은 크게 H.235와 SRTP로 나눌 수 있다. 물론 RTP 패킷을 보호하는 목적은 같지만 적용하는 암호 알고리즘과 적용 방식에 따라 공격 가능성이나 에러 전파로 인한 RTP 페이로드의 손실 범위 혹은 처리 시간 등이 다르게 나타날 수 있다. 따라서 H.235와 SRTP 프로토콜의 키 관리 측면과 사용자 인증 방법에 따른 보안성을 분석하여 보고, 암호 알고리즘의 적용 방법에 따른 RTP 데이터의 확장 여부와 에러 전파 문제, 그리고 암호화 계산 지연 시간을 줄이기 위한 pre-computation의 가능 여부 등을 분석하여 볼 것이다.

### 2. H.235와 SRTP의 보안 적용 방식 분석

1) 키 관리 및 보안성

H.235는 Diffie-Hellman을 이용하여 양단 간에 공유키를 생성하며, 음성을 보호할 세션키를 랜덤하게 생성한 후 공유키로 암호화한 다음 전달한다. 이 세션키는 암호화에만 사용되고 인증에는 사용하지 않으며 인증을 위한 키는 패스워드를 기반으로 생성하여 사용한다. 따라서 인증키는 사용자 자신의 인증 기능을 가지게 된다. 반면에 SRTP는 자체적인 키 교환 메커니즘을 가지고 있지 않으며 다른 키 관리 프로토콜에 의해 공유된 마스터키와 salt 키를 기반으로 세션키와 인증키를 생성하여 사용한다. 인증키는 공유된 마스터키를 기반으로 생성되므로 마스터키가 사용자의 고유 특성을 반영하지 못하는 경우, 사용자를 인증하지 못하고 단지, 무결성만을 보장하게 된다.

무결성 측면에서 두 프로토콜을 비교하여 보면 RTP 패킷에서 헤더 부분은 두 프로토콜 모두 인증을 수행하지만, RTP 페이로드의 경우는 SRTP만이 인증을 수행한다. 따라서 H.235는 페이로드 부분에 대하여 무결성을 보장하지 못하며 페이로드가 변조되면 이를 감지하기 어렵다. 특히, RTP 페이로드는 대부분 멀티미디어 데이터이므로 암복호화되어도 데이터의 의미를 파악할 수 없으므로 정상적으로 처리된다. H.235에서 RTP 스트림에 대한 무결성과 replay 공격 방어는 차후 연구 과제로 명시하고 있다. 또한 암호화로 인한 보호의 범위는 두 프로토콜이 같으며 무결성의 범위는 H.235의 경우 헤더 중 타임스탬프까지만 무결성을 보장한다. RTP는 RTCP와 같이 사용되는데 SRTP에서는 RTCP를 RTP와 다른 스트림으로 구분하여 RTCP만을 위한 세션키들을 따로 생성하고, RTCP 필드 자체도 다르기 때문에 보호 부분과 IV 생성도 다르게 정의하고 있다. 반면에 H.235에서의 RTCP를 전혀 고려하고 있지 않고 이를 차후 연구 과제로 미루고 있어 현재로는 RTCP를 보호하지 않고 있다.

SRTP는 암호화와 인증 시에 Key_derivation_rate을 두어 일정한 패킷의 수마다 세션키들을 다시 생성하여 사용하므로 공격자가 모을 수 있는 암호문이 제한될 수 있어 키 재교환 주기까지 같은 키를 사용하는 H.235에 비해 상대적으로 보안성이 좀더 강화된다고 볼 수 있다.

2) 공격 방어 측면

가능한 공격을 기반으로 각 프로토콜의 보안성을 분석하면, 우선 DoS(Denial of Service) 공격의 경우, H.235는 DoS 공격을 방어하기 위해 media anti-spamming 기능을 이용하여 패킷을 송신 전에 RTP 헤더 필드 중 64bits(SEQ와 타임스탬프)를 이용하여 MAC 코드를 생성하고 RTP 패킷에 첨부한다. 따라서 수신자는 수신된 패킷의 첨부된 인증 코드와 계산값을 비교하므로 DoS 공격을 방어할 수

무결성만을 확인하므로 복호화되기 전에 패킷의 정당성을 빠르게 확인할 수 없다. 또한 신분 가장 공격의 경우, H.235는 패스워드 기반의 인증키를 사용하여 메시지를 인증하기 때문에 사용자를 인증할 수 있지만, SRTP는 키 관리 프로토콜에서 사용자 인증을 지원하지 않으면 SRTP 자체만으로는 사용자와의 연관성이 없으므로 사용자를 인증하기 어렵다.

SRTP는 RTP 패킷의 인증 범위가 헤더와 페이로드를 포함하므로 페이로드를 변조하는 경우, 이를 인증 과정에서 감지하여 패킷을 버릴 수 있다. 그러나 H.235의 경우, H.323 시그널링에만 인증을 제공하고 RTP 패킷의 인증 과정을 정의하지 않았으며, media anti-spamming 기능을 사용한다 하더라도 헤더의 64bits 만을 인증하기 때문에 암호화된 페이로드를 변조하면 인증 과정에서 이를 감지할 수 없다. 따라서 이렇게 변조된 데이터는 코덱을 거쳐 소리로 출력되게 될 것이다. 물론 암복호화를 거치기 때문에 공격자가 의미 있는 소리를 넣을 수는 없지만 음성 통신을 방해하는 잡음을 넣을 수 있는 여지는 있다.

Replay 공격 측면에서 살펴보면, H.235는 단순히 암호화와 media anti-spamming 기능만으로 RTP 패킷의 replay 공격을 막지 못한다. Media anti-spamming은 RTP 헤더의 SEQ와 타임스탬프를 이용하여 인증 코드를 붙이기 때문에 이전에 수신한 반복된 패킷이 수신되어도 인증에 성공한다. 이는 H.235가 슬라이딩 윈도우와 같은 패킷 수신 확인 메커니즘을 사용하지 않기 때문이며 거의 모든 패킷에 동일한 키를 사용하기 때문이다. 반면에 SRTP에서는 패킷 인덱스와 Key_derivation_rate에 따라 세션 인증키 생성이 되어 인증키가 바뀌게 되므로 주기를 벗어난 반복된 패킷은 인증에 실패하게 된다. 그러나 이 Key_derivation_rate의 주기가 매우 길 경우, 그 주기 동안에 같은 인증키가 사용되는 위험성이 있다. 하지만 인증 코드 생성 시에 SEQ와 타임스탬프가 포함되므로 Replay 공격을 막을 수 있으며 슬라이딩 윈도우 메커니즘을 사용하므로 이미 시간이 많이 지난 패킷을 걸러낼 수 있다.

3) 보안 효율성

SRTP는 마스터키와 cryptographic context가 교환된 이후, RTP가 전송되기 전에 각 패킷 인덱스를 기반으로 각 패킷마다의 키 스트림을 미리 생성해 놓을 수 있다. 따라서 실제 실시간 데이터가 생성되면 바로 키 스트림과 Exclusive_or 연산만을 수행하여 암호화할 수 있으므로 실시간 데이터 처리에서 지연 시간을 줄일 수 있다. 반면에 H.235에서는 실시간 데이터가 발생하면 이를 암호 함수에 입력으로 넣어 연산이 끝나고 나온 결과값을 전송하므로 암호화 계산의 지연시간이 실시간 데이터의 실시간성을 훼손할 수 있다.

에러 전파 측면에서 보면 SRTP는 키 스트림과 RTP 페이로드를 Exclusive_or 연산하므로 전송 중간에 에러가 발생하면 에러난 부분(bits)이 한정되어 다른 부분에 영향을 미치지 않는다. 그러나 H.235는 CBC 모드를 기반으로 하기 때문에 에러가 발생하면 에러가 발생한 블록과 그 다음 블록이 영향을 받게 된다. 따라서 사용된 암호 알고리즘 블록 크기의 2배에 해당하는 데이터가 영향을 받는데 DES의 경우 16바이트의 데이터가 손실되게 된다. 그러나 RTP에서 전달되는 데이터는 대부분 실시간 데이터로 작은 크기를 가진다. 코덱과 패킷에 포함되는 프레임의 수에 따라 영향이 달라질 수 있지만 일반적으로 음질을 향상하기 위해 패킷당 하나 혹은 두 개의 프레임을 전송한다. 대표적인 G.723.1 코덱을 기준으로 설명하면 한 프레임이 20 혹은 24 바이트의 크기를 가지며 30msec의 지속 시간을 가진다. DES 암호 알고리즘을 적용한 이러한 패킷에 에러가 발생하면 암호 알고리즘의 확산 특성과 CBC 모드의 chaining 특성에 의해 한 프레임의 대부분인 (2/3) 16바이트에 에러가 발생하고 30msec의 시간

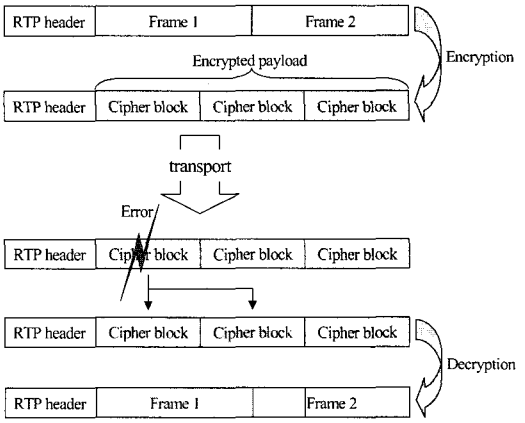


그림 8. 에러 전파

동안 음성이 들리지 않게 된다. 또한 한 패킷에 두

동안 음성이 들리지 않게 된다. 또한 한 패킷에 두 개의 프레임을 전송하는 경우, 24바이트 크기의 코덱을 사용하고 DES와 같이 8바이트 블록의 암호 알고리즘을 사용하면 암호화할 데이터가 8의 배수로 프레임간 에러의 전파가 발생하지 않는다. 하지만 암호 블록과 코덱의 프레임 블록이 배수 관계에 있지 않으면 첫 프레임의 마지막과 두 번째 프레임의 처음 부분이 하나의 암호 블록에 겹치게 되어 이 블록에서 에러가 발생하면 최소 두 개의 코덱 프레임에 에러가 전파되게 된다. 그림 5는 이러한 현상을 보여 주고 있는데 프레임 1과 프레임 2가 암호 블록에 의해 나뉘어져 하나의 암호 블록에 들어가게 되면, 전송 중 프레임 1과 프레임 2의 공동 암호 블록 앞에서 한 비트의 에러가 발생하여도 이 에러는 CBC 모드의 특성에 의해 다음 암호 블록까지 전달된다. 따라서 프레임 1 전체와 프레임 2의 일부분까지 에러가 전파되므로 프레임 2도 역시 사용할 수 없게 된다. 이러한 특성은 UDP 기반의 적은 데이터가 전달되는 실시간 멀티미디어 통신에 많은 데이터 손실을 가져오게 되므로 보안 표준화 제정 시 고려되어야 한다.

데이터의 확장 측면에서 보면 SRTP는 RTP 페이로드 크기의 키 스트림과 RTP 페이로드를 Exclusive_or 연산하므로 암호화된 데이터가 증가하지 않는다. 그러나 H.235에서 PKCS 패딩 CBC 모드를 사용하면 RTP 페이로드를 암호 블록의 배수로 패딩을 시켜주어야 하기 때문에 증가하게 된다.

암호 알고리즘 및 운영 모드를 비교하여 보면 H.235 알고리즘은 DES, 3DES, RC2 등이 사용되는데 이러한 알고리즘들은 이미 오래 전에 개발된 알고리즘들이고 DES는 이미 안전성에 의심을 받고 있다. 또한 3DES의 경우, DES 암호 계산을 세 번 반복하므로 안전성은 있지만 시간이 많이 소모되어 실시간 트래픽을 전송하는 RTP 입장에서는 부담스러운 암호알고리즘이다. 반면에 SRTP는 차세대 암호 알고리즘인 AES를 사용하여 높은 안전성과 빠른 속도를 지원하여 실시간 데이터의 암호화에 적합하다.

SRTP에서는 키 관리 프로토콜에 따라 마스터키를 재 교환하며 하나의 마스터키와 마스터 salt 키를 이용하여 Key_derivation_rate에 정의된 주기에 따라 패킷 인덱스를 이용하여 다른 세션키를 생성하여 사용할 수 있다. 또한 RTP 패킷의 SEQ 한계를 넘겨 사용하기 위해 32 비트 크기의 rollover counter(RTP의 SEQ가 한계를 넘어 다시 0으로 설정될 경우 1 증가)를 두어 패킷 인덱스의 한계를 2^48까지 증가시켰다. 이 것은 실시간 통신에서 멀티미디어 데이터 송수신 중간에 키 교환이 발생하여 지연시간이 발생하는 것을 방지할 수 있다. 반면에 H.235에서는 2^32개 이상의 블록이 같은 키로 암호화되지 않도록 규정하고 있다. 따라서 구현 시에는 2^30 블록이 같은 키로 암호화되면 키 업데이트를 수행하도록 하고 있다.

표 7. SRTP와 H.235의 RTP 보안 특성 비교

| 기능 | SRTP | H.235 |
|---|---|---|
| 키 관리 | × | ○ |
| 사용자 인증 | × | ○ |
| RTP 페이로드의 무결성 | ○ | × |
| RTCP 보호 | ○ | × |
| Pre-computation | ○ | × |
| 에러 전파 | × | ○ |
| 데이터 확장 | × | ○ |

표 7은 지금 까지 분석한 SRTP와 H.235의 보안적 기능을 요약한 표로서 대조적인 특성들을 비교하고 있다. SRTP 측면에서는 키 관리를 다른 프로토콜에 의존하고 있으며 메시지에 대한 인증은 수행하지만 사용자에 대한 인증은 수행하지 않는다. RTCP는 SRTCP를 정의하여 SRTP와 같은 수준의 보안을 제공한다. 또한 암호화 계산 시 키 스트림의 pre-computation이 가능하여 실시간 데이터의 전송에 효율적이며 에러의 전파가 발생하지 않아 채널의 에러에 강하며 데이터가 암호화 처리 후에 증가하지도 않는다. 반면에 H.235에서는 pre-computation이 불가능하며 에러 전파가 많이 발생하고 데이터의 확장도 발생하여 보안 효율성 측면에서 떨어진다. 또한 RTCP를 보호하지 않으며 RTP 페이로드에 대한 무결성도 확인을 하지 않는다. 다만 키 교환 메커니즘을 정의하고 있고 사용자 기반의 패스워드를 사용하여 인증을 수행하는 것이 장점이다. 이러한 문제점들을 고려하여 다음 표준의 제정 시에 수정되어야 할 것이다.

## V. 결 론

실용적인 기술로 변화하고 있는 VoIP 서비스는 이제 음질과 보안성을 확보해야 지속적으로 사용자

를 확대할 수 있고 기존 전화를 대체할 수 있을 것으로 예상된다. 그러나 보안을 적용한 VoIP 시스템의 경우 음질은 보안의 추가 작업으로 실시간 통신에 악영향을 미쳐 음질의 저하를 가져온다. 따라서 본 논문에서는 여러 가지 암호화 알고리즘을 이용한 음성 패킷의 실시간 암호화 실험을 통해 추가적인 암호화 연산 시간이 실시간 통신에서 지연 시간과 지터를 증가시켜 음성의 질을 떨어뜨릴 수 있다는 것을 알 수 있었다. 일반적으로 빠른 속도의 DES, SEED, AES 등의 암호 알고리즘은 음질의 변화를 감지하기 어려웠지만 3DES의 경우 시스템의 성능에 따라 사람의 귀로 음질의 저하를 인식할 수 있었으며 측정한 수치를 통해서도 3DES가 패킷 처리 시간에 많은 변화를 초래한다는 것을 알 수 있었다. 특히, 음성 품질의 평가에 가장 중요한 음성 재생 직전의 처리 시간에 대한 변화율을 측정하여 보니 3DES가 다른 암호 알고리즘에 비해 상대적으로 큰 변화율을 보였다. 이 것은 하나의 호를 처리하는 사용자측 시스템에서는 큰 문제가 되지 않을 수 있지만 폰 게이트웨이와 같이 동시에 많은 호를 처리해야 하는 시스템에서는 호 처리 프로세스간 자원의 공유로 인해 암호화 연산 과부하가 발생하여 패킷처리 시간이 증가하고 패킷간의 시간차에 변화가 심해져 지터가 증가한다. 알고리즘별 실시간 음성 통신 시스템의 음질에 대한 실험을 통해 나온 결과를 토대로 현재 진행중인 VoIP 보안의 설계 작업에서 암호화에 따른 음질의 영향을 고려하여야 할 것이며 특히, 3DES 알고리즘의 경우 실시간 음성 시스템에 적용할 경우 VoIP가 운영될 시스템의 계산 능력을 측정하여 사용 가능한지를 판별한 후 적용해야 한다.

또한 실시간 멀티미디어 통신의 보안 프로토콜 특성을 비교, 분석하여 문제점을 찾고 개선점을 제시하였다. H.235의 경우, 키 교환과 기밀성 그리고 DoS 공격에 대한 방어 등 전체적인 보안 구조를 정의하고 있지만 보안 프로토콜의 효율성 측면에서 에러 전파로 인한 데이터의 추가 손실과 RTP 페이로드의 무결성을 제공하지 못하는 등의 다소 문제점이 발견되었으며 아직 RTCP 보안을 지원하지 못한다. SRTP는 순수 RTP 측면에서 접근하여 키 교환을 정의하지 않았으며 보안성과 효율성 측면에서 H.235와 비교하여 상대적으로 좋은 특성을 가지고 있다. 단지, 사용자 인증과 DoS 공격에 대한 방어책을 지원하지 않고 있다.

앞으로 실시간 보안 시스템은 많은 성장이 예상되는 화상회의나 동영상 서비스 등의 실시간 통신 보안에 응용되어 질 수 있을 것으로 예상한다. 따라서 여기에 적용되는 보안은 실시간 통신을 고려하여 보안의 효율성과 실시간성을 보장해 주어야 한다. 이러한 연구는 앞으로 진행되는 멀티미디어 기반 실시간 통신의 보안 프로토콜 설계 시에 고려될 수 있을 것으로 예상한다. 이 연구에 추가하여 앞으로 진행될 연구에서는 다자간 실시간 멀티미디어 통신을 위한 보안에서 RTP 패킷의 효율적인 인증에 관한 연구가 가능할 것이다.

## 참 고 문 헌


[1] William Stallings, "Cryptography and Net-work Security: Principles and Practice," *Prentice-Hall*, 1999.

[2] H.235 v2, "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals," *ITU-T*, 2000.

[3] Internet Draft, "SIP: Session Initiation Protocol RFC 2543 bis-07", *IETF SIP WG.*, 2002.

[4] Internet Draft, "SRTP: The Secure Real-time Transport Protocol," *IETF AVT WG.*, 2002.

[5] TTAS.KO-12.0004, "128비트 블록암호알고리즘 표준(SEED)," *한국정보통신기술협회*, 1999.

[6] Joan Daeman, Vincent Rijmen, "AES Proposal: Rijndeal," *NIST*, 1999.

[7] http://www.openh323.org/, "Open H.323 Project".

[8] William Stallings, "High-speed networks," *Prentice Hall* 1998.

[9] Bill Douskails, "IP Telephony: The Integration of Robust VoIP Service," *Prentice Hall* 2000.

[10] Davidson Peters, "Voice over IP Fundamen-tals: A systematic Approach to Understanding the Basics of Voice over IP," *Cisco Press*, 2000.

[11] Peter B. Busschbach, "Toward QoS Capable Virtual Private Networks," *Bell Labs Technical Journal*, pp. 161-175,

October-December 1998.

[12] Manuel Gunter, Torsten Braun, Ibrahim Khalil, "An Architecture for Managing QoS-enabled VPNs over the Internet," *IEEE, Proceedings of the 24th Conference on Local Computer Newworks*, pp. 122-131, October 1999.

홍 기 훈(Ki-Hun Hong) 학생회원

2000년 2월: 숭실대학교 정보통신공학과 학사
2002년 2월: 숭실대학교 정보통신공학과 석사
2002년 3월~현재: 숭실대학교 정보통신공학과 박사과정

<주관심분야> VoIP 보안, 네트워크 보안

정 수 환(Sou-Hwan 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
1997년~현재: 숭실대학교 정보통신전자공학부 조교수

<주관심분야> 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: 한국전자 통신연구원 네트워크연구소 연구원

<주관심분야> NGN, FTTH, VoIP, Security

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

<주관심분야> VoIP, 고속 실시간 QoS 데이터처리, 멀티미디어 게이트웨이, 신호게이트웨이