암호화 연산에 따른 VoIP QoS 측정 및 분석

홍기훈*, 임범진*, 정수환*

*숭실대학교, 정보통신전자공학부

Impact of Cryptographic operations on the QoS of VoIP system

Ki-hun Hong*, Bumjin Im*, Souhwan Jung*

*School of Electronic Engineering Soongsil Univ.

요 약

보안을 위한 암호화는 실시간 통신인 VoIP에 패킷의 추가적인 작업이 요구되므로 음질에 악영향을 미치게 된다. 이러한 영향을 파악하고 분석하기 위해 DES, 3DES, SEED 그리고 AES 등의 암호 알고리즘을 VoIP 시스템에 적용하여 지터나 RTT 혹은 패킷 손실율과 같은 QoS 요소를 측정함으로써 각 암호 알고리즘의 연산이 실시간 통신에 미치는 영향을 알아보았다.

I. 서론

인터넷 응용 기술과 멀티미디어 기술의 발전에 힘입어 인터넷폰, 화상 채팅, VoD 서비스, 동영상 강의나 동영상 쇼핑 등 많은 미디어 응용 서비스가 현재 제공되고 있는 가운데 가장 많은 관심의 대상이 인터넷폰이다. 인터넷폰은 기존의 전화 서비스를 대체할 것으로 예상되며 특히 외국과 같이 상당한 원거리의 사용자에게는 전화비용의 부담을 줄여 줌으로서 사용이 급격히 증가하고 있고 많은 VoIP 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 도청하여 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 현실이다. 이러한 해킹을 막기 위한 방법으로 기존의 보안 프로토콜을 이용한 방법들이 제시되고 있다. 인터넷 보안의 필요성에 따라 SSL(Secure Socket Layer), SET(Secure Electronic Transactions), PGP(Pretty Good Privacy)등의 여러 가지 기존 보안 기술들이 응용되어 사용되고 있다. 그러나 이 기술들은 서비스 별로 필요에 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 브라우저용으로 사용되고 UDP를 지원하지 못한다. 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.

현재 VoIP을 위한 보안 프로토콜로는 ITU-T에서 H.323의 보안을 지원하기 위해 만든 H.235가 대표적이며 SIP을 위한 보안 관련 문서들도 IETF에서 발표되고 있으며 범용 프로토콜인 IP Security를 응용하는 방법도 제시되고 있다. 그러나 보안의 적용은 실시간 통신 시스템인 VoIP에 보안 프로토콜을 위한 시그널링과 실제적인 음성 패킷의 암호화 등의 추가적인 작업이 필요함으로써 음질에 영향을 미친다. 이러한 음질의 저하를 지터와 지연 시간 등의 QoS 요소를 이용하여 측정하고 음질에 미치는 영향을 알아보았다.

이 논문에서는 우선 VoIP 보안 시스템의 구성과 보

안 VoIP 시스템의 QoS 요소 측정 실험 그리고 마지막으로 결론에서 구성된 시스템과 각각의 암호화 알고리즘이 QoS에 미치는 영향과 향후 연구 방향에 대하여 기술하였다.

II. VoIP 보안 프로토콜

1. IPSec 기반 VoIP 보안 시스템

인터넷폰은 사용자의 프로그램과 게이트키퍼 사이에 사용자 인증이 처리된 후 사용자의 음성은 폰 게이트웨이와 사용자의 프로그램 사이에 직접적으로 전송된다. 이러한 음성을 암호화하여 보호하기 위해서는 폰 게이트웨이와 사용자 프로그램 사이에 보안 채널을 형성하여 사용자의 음성 패킷을 보호해야 한다. 그러나 폰 게이트웨이는 세계 여러 기업에서 생산되어 사용되고 있는 제품으로 보안이 고려된 폰 게이트웨이가 아직 출시되지 않은 상황에서 보안 프로토콜을 인터넷폰에 적용하는 방안을 고려해야 한다. H.323 단말 프로그램 또한 상당히 많은 종류가 사용되고 있고 사용자들의 시스템도 역시 각기 다르기 때문에 대부분의 H.323 단말을 수용하면서 사용자의 여러 가지 운영체제도 수용할 수 있는 보안을 적용해야 한다. 그리고 VoIP 자체도 H.323과 SIP로 분리되어 발전하고 있기 때문에 보안 프로토콜이 각각의 VoIP에 의존적이어야 한다. 이 것에 비추어 IPSec은 상위 레이어인 인터넷폰 프로그램 자체를 수정하지 않고 보안을 적용 할 수 있는 좋은 예가 될 수 있다. 위의 여러 상황을 고려하여 다음의 그림에서 인터넷폰 보안의 적용 예를 볼 수 있을 것이다.

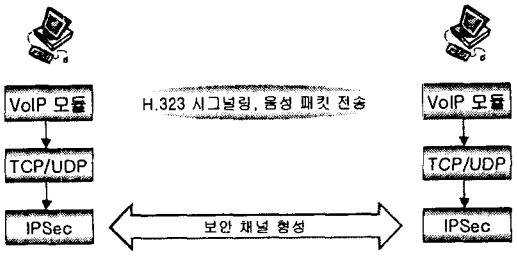

그림 1: VoIP와 IPSec 프로토콜의 결합.

그림 1에서는 VoIP 모듈이 어떠한 프로토콜이든지 상관없이 네트워크 스택을 통해 IP 레이어에 전달된 패킷을 IPSec 드라이버가 이전에 공유한 보안 설정과 키를 사용하여 암호화하여 안전하게 상대방에게 전달한다.

2. H.235 기반 VoIP 보안 시스템

H.235는 H.323을 위한 보안 프로토콜로서 인터넷폰에서 시그널링을 통해 음성 패킷을 암호화하여 도청을 방지하는 목적이다. H.323 단말은 게이트키퍼와의 RAS 절차에서 패스워드를 이용한 사용자의 인증과 메시지의 무결성을 제공하며 H.225에서는 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 재생함으로서 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.

III. 암호 알고리즘별 QoS 요소의 측정 및 분석

1. 개요

IPSec 프로토콜을 이용하여 VoIP에 보안을 적용해 보았지만 실제 사람의 귀를 통해 인식되는 통화 품질은 다소 떨어지는 것을 감지할 수 있었다. 이는 암호화와 복호화 과정이 추가되어 음성 패킷의 처리에 추가적인 시간이 소요되기 때문이다. 따라서 실시간 통신에 가장 적합한 암호 알고리즘을 찾고 각각에 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 손실율과 순서가 바뀐 패킷(Out of order)의 수 그리고 지터 버퍼 크기의 시간 내에 도착하지 못한 패킷의 수 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 요소로써 실시간 통화에서 지연 시간이 길게 되면 상호간의 통화가 불가능하게 된다. 패킷 손실율은 패킷 자체가 인터넷을 통해 라우팅 되는 중간에 여러 가지 원인

으로 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. 이 실험에서는 위와 같은 요소들을 암호화 알고리즘을 변화시키며 측정하고 분석하여 각각의 알고리즘들이 음질에 미치는 영향에 대하여 살펴보았다.

2. 측정 시스템의 구조

실험은 4가지의 암호 알고리즘을 각각 인터넷폰에 적용하여 알고리즘에 따른 QoS 파라미터의 차이를 알아보았다. 이번 실험에 사용되는 암호 알고리즘은 DES, 3DES, SEED, AES 등이며 시그널링은 암호화가 적용되지 않고 음성에만 암호화를 적용하였다.

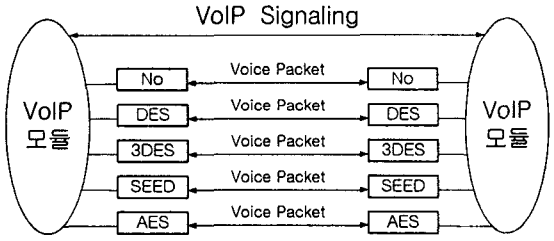

그림 2: QoS 실험을 위한 구성.

그림 2에서 볼 수 있듯이 VoIP 모듈에 4개의 암호 알고리즘을 추가하여 보안을 적용하지 않은 트래픽을 포함한 총 5가지의 트래픽에 대한 QoS 파라미터를 측정하였다.

3. QoS 요소의 측정 및 분석

1) 지터의 측정과 분석

지터는 앞에서 언급한 바와 같이 도착하는 패킷 간의 지연 시간의 변화율을 의미한다. 우선 지터를 구하기 위해서는 interval 지연 시간을 계산하여야 하는데 다음의 식(1)로 표현할 수 있다.

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

위의 식(1)에서 구한 지연 시간을 이용하여 아래의 식과 같이 지터를 표현할 수 있다.

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

지터를 측정하기 위해 사용된 인터넷폰의 지터 버퍼는 50 msec으로 설정하여 지터를 측정하였다. 이 지터 버퍼는 가변적인 도착 시간의 간격을 완충하는 역할을 하기 위해서 설정하는 버퍼로 설정된 버퍼의 크기 이하로 패킷이 늦게 도착하면 음성의 재생이 가능하지만 그 이상이면 정상적인 음성의 재생이 불가능하다. 그러나 지터버퍼는 VoIP 통신에서 지연시간을 추가시키므로 과대한 지터 버퍼는 정상적인 통화에 악 영향을 줄 수 있다.

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 %

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.

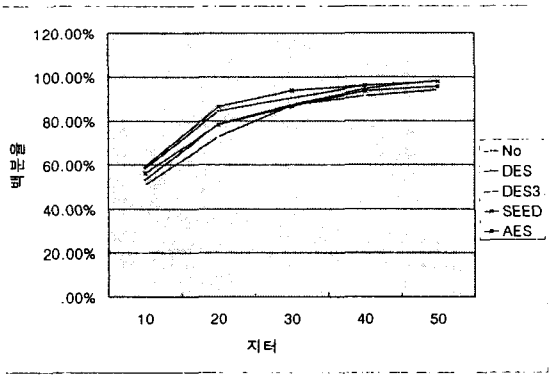

그림 3: 지터에 따른 패킷의 누적 백분율.

그림 3은 10msec 에서 50msec 까지의 지터에 따른 패킷수를 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 3DES

가 가장 암호화 시간이 길기 때문으로 분석된다.

2) RTT의 측정과 분석

RTT은 네트워크 상에서 상대방에게 요청한 응답이 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 다음과 같은 측정 모델을 사용하였다.

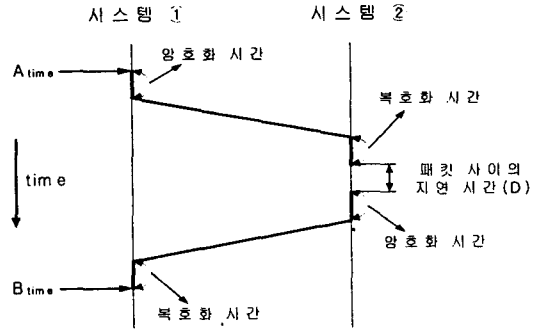

그림 4: RTT 측정 모델.

그림 4는 RTT를 측정하기 위한 모델로서 일반적인 RTT 측정 모델에 암호 알고리즘의 연산 시간을 포함한 것이며 아래의 식과 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 시간 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 시간은 RTT에 포함되지 않으므로 역시 감산하였다.

표 2: RTT 평균.

알고리즘	Avg. of RTT (단위:sec)	암호화 속도 (단위:Mbps)
No encryp.	0.182863	-
DES	0.212005	95.612
3DES	0.20189	31.966
SEED	0.197684	85.997
AES	0.207398	168.111

표 2는 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 132byte로 그리 크지 않기 때문에 암호화에 그렇게 많은 시간이 소요되지 않음을 예상 할 수 있다. 실제로 실험을 통해 132byte의 데이터를 암호화하는 시간을 측정하여 보았다. 그러나 암호화 수행 시간만을 측정하기에는 Windows 2000 운영체제의 시간 정밀도는 세밀하지 못하였다. 따라서 알고리즘별 암호화 연산 시간을 측정하기 위하여 대량의 데이터를 이용하여 암호화를 수행하고 이를 시간으로 나누어 표 2의 암호화 속도를 얻을 수 있었는데 실험 환경은 펜티엄 733 Mhz, 256Mbyte 램을 장착한 PC이다.

추가로 패킷 손실율과 순서가 바뀐 패킷(Out of order)의 수 그리고 지터 버퍼 크기의 시간 내에 도착하지 못한 패킷의 수 등을 측정하였으나 거의 발생하지 않았다.

IV. 결론

실용적인 서비스로 변화하고 있는 인터넷폰 서비스는 이제 음질과 보안성을 확보해야 지속적으로 사용자를 확대할 수 있고 기존 전화를 대체할 수 있을 것으로 예상된다. 그러나 보안을 적용한 VoIP 시스템의 경우 음질은 상대적인 보안의 추가 작업으로 실시간 통신에 악영향을 미쳐 음질의 저하를 가져온다. 따라서 이러한 보안의 처리가 실시간 통신에 미치는 영향을 알아보기 위해 실험을 해 보았다. 그러나 암호화하는 데이터의 크기가 일반적인 데이터의 전송에 비해 상대적으로 매우 작은 양이며 한 PC당 하나의 호만을 처리하므로 세밀한 데이터를 측정하기 곤란하고 운영체제의 시간 정밀도가 낮아 정확한 특성의 자료를 측정하기 곤란하였다. 따라서 암호화의 처리가 과부하 현상을 보이기는 하지만 각 암호 알고리즘별로 큰 특성을 확인하지 못했다. 더욱 정확하고 세밀한 자료를 얻기 위하여 여러 호를 동시에 처리하는 환경을 구성하여 시스템의 과부하 현상을 실험할 계획이며 패킷의 송신과 수신 시간을 측정하여 패킷간의 시간 간격차를 관찰할 계획이다.

이러한 연구에 추가로 각 알고리즘의 모드별로 실험 환경을 추가하거나 스트림 암호 알고리즘을 적용하여 실험함으로써 패킷의 전송 시간 간격이나 패킷 수신 시간 간격 등의 더욱 다양한 결과를 분석하거나 실제 게이트웨이와 같은 실험 환경을 구성하여 많은 보안 호를 발생시켜 게이트웨이에서 발생할 수 있는 문제점을 관찰하는 연구가 요

구되어 진다.

참고문헌

[1] http://www.ietf.org/html.charters/ipsec - charter.html, "IP Security Protocol Working Group".

[2] William Stallings, "Cryptography and Network Security: Principles and Practice," Prentice-Hall, 1999.

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

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

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

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

[7] Bill Douskails, "IP Telephony: The Integ- ration of Robust VoIP Service", Prentice Hall 2000.

[8] Davidson Peters, "Voice over IP Fun- damentals: A systematic Approach to Under- standing the Basics of Voice over IP," Cisco Press, 2000.

[9] Peter B. Busschbach, "Toward QoS Capable Virtual Private Networks," Bell Labs Technical Journal, pp. 161-175, October-December 1998.

[10] Daniel Muller, Gunter Schafer, Jochen Schiller, "An Efficient Authentication Protocol for High Performance Net- works," IEEE, Proceedings of the Globecom '98, V.2, pp. 886-891, November 1998.

[11] 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.