Journal of The Korea Society of Computer and Information
Vol. 18, No. 4, April 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.4.087

이종의 통신망 간에 VoIP 미디어 암호화를 위한 RTP(Real-time Transport Protocol)의 재설계 및 성능 분석

오 형 준*, 박 재 경**, 원 유 헌*

Redesign and Performance Analysis of RTP(Real-time Transport Protocol) for Encryption of VoIP Media Information between Different Communication Networks

Hyung-Jun Oh*, Jae-Kyoung Park**, Yoo-Hun Won*

요 약

본 논문에서는 단일망 및 서로 다른 통신망간의 통신 시에 VoIP 미디어 정보에 대해 암호화 작업을 수행할 수 있도록 기존의 RTP 프로토콜을 재설계하고 성능 분석을 수행한다. VoIP 미디어 정보를 암호화하기 위한 기존의 방법으로 SRTP나 ZRTP와 같은 방법들이 사용되고 있다. 그러나 기존의 기법들은 서로 다른 통신망간의 VoIP 서비스 시 양단의 단말 간에 암호화 작업을 수행하지 못하는 문제를 가지고 있다. 본 논문에서는 이를 해결하기 위해 재설계된 RTP를 제안한다. 재설계된 RTP는 암호화와 관련된 모든 정보를 RTP 내에 포함시킴으로써 게이트웨이 장비에서 SIP 및 SDP 정보에 대한 수정이 발생하여도 암호화에 영향을 받지 않도록 설계한다. 또한, RTP 내부에 암호화 여부에 대한 코드를 포함시켜 서로 다른 망간의 암호화 통신 시에 게이트웨이 장비에서 RTP 헤더에 대한 수정을 방지함으로써 무결성을 유지하도록 하여 서로 다른 사설망 간의 VoIP 서비스에서도 암호화된 미디어 정보의 교환이 수행되도록 설계한다. 그리고 재설계된 RTP와 기존의 암호화 방법인 SRTP와 ZRTP에 대한 성능 분석을 수행한다.

▸ Keywords : VoIP, RTP, SRTP, ZRTP, 암호화

•제1저자 : 오형준 •교신저자 : 오형준
•투고일 : 2013. 3. 13, 심사일 : 2013. 3. 27, 게재확정일 : 2013. 4. 4.
•이 논문은 2012학년도 홍익대학교 학술연구진흥비에 의하여 지원되었음
* 홍익대학교 컴퓨터공학과(Dept. of Computer Engineering, Hongik University)
** 한국과학기술원 사이버보안연구센타(Cyber Security Research Center, KAIST)

Abstract

In this paper, we suggest redesigned RTP protocol that is able to perform encryption of VoIP media information for single private network and between the different private networks. And we conduct a test for performance analysis. Such as SRTP or ZRTP methods have been used for VoIP media encryption. But, the existing encryption techniques have problem that can not perform end-to-end encryption between different private networks. In order to solve this problem, in this paper, we redesign RTP protocol. Redesigned RTP includes all information for encryption of VoIP media. Therefore the encryption is not affected by modification of SIP and SDP information that occurred in gateway. Also, redesigned RTP includes code for whether or not to apply encryption. By using the code, modification of RTP header from gateway prevents. As a result, redesigned RTP maintain the integrity and the RTP is able to perform encryption between the different private networks. Also, we conduct a test for performance analysis of SRTP, ZRTP and redesigned RTP.

▸ Keywords : VoIP, RTP, SRTP, ZRTP, Encryption

I. 서 론

최근 많은 관심을 받고 있는 VoIP(Voice Over Internet Protocol)[1] 서비스는 기존의 IP(Internet Protocol)망을 이용하여 음성 데이터를 전송하는 기술로 저렴한 통신비용과 다양한 부가 서비스를 제공한다는 장점과 기존의 IP 기반 네트워크 자원의 가용성과 효율성을 극대화할 수 있다는 장점 때문에 유/무선 환경에서 점점 더 광범위하게 사용되고 있다. VoIP 서비스는 기존의 인터넷망을 그대로 활용하기 때문에 인터넷망에서 발생할 수 있는 보안 취약성뿐만 아니라 공중전화망과 유/무선 인터넷망의 연동에 따른 여러 가지 보안 취약성을 갖고 있다[2]. 이러한 다양한 보안 취약성에 대한 VoIP 서비스의 주요 공격 유형들로는 도청 및 감청, DoS(Denial of Service) 공격, 스팸, 서비스 오용 공격 등을 들 수 있다. 특히, 이 중 VoIP 미디어 정보에 대한 도청은 기밀 정보의 유출을 발생시킬 수 있고 이로 인해 보안상 큰 문제를 야기 시킬 수 있다[3].

VoIP 서비스를 운용할 때 서비스 시나리오의 유형은 PC-to-PC, PC-to-Phone, Phone-to-Phone 형태로 구분할 수 있다. 이 때, VoIP 서비스에 참여하는 단말들은 단말 모두가 단일 통신망 내에 위치하여 통신을 하는 경우와 참가 단말들의 일부가 외부의 일반망 또는 외부의 사설망과 같은 외부의 통신망에 위치하여 통신을 하는 두 가지 유형으로 VoIP 서비스를 이용한다. VoIP 서비스를 이용하여 통신을 할 때 하나의 단일 통신망 내에서 통신을 하는 경우는 일반적으로 사설망을 이용한다. 이 경우, VoIP 서비스가 진행되는 동안 미디어 정보에 대해 외부자에 의한 도청 및 감청으로 인한 기밀 정보 유출이 어렵다는 장점을 갖는다. 그러나 이러한 경우에도 사설망 내부에서의 도청 및 감청으로 인한 기밀 정보의 유출이 발생할 수 있다. VoIP 서비스 시 참여자의 일부가 외부의 통신망에 위치할 경우에는 STUN(Simple Traversal of UDP through NAT), TURN(Traversal Using Relay NAT), ICE(Interactive Connectivity Establishment), SBC(Session Border Controller)[4]와 같은 게이트웨이 장비들을 이용한다. 이러한 게이트웨이 장비는 하나의 망 내에 있는 참여자와 외부망에 있는 참여자 간의 통신이 가능하도록 하는 장비이다. 게이트웨이 장비를 이용하여 VoIP 서비스를 수행할 경우 서로 다른 망에 있는 참여자간의 통신이 가능하다는 장점이 있지만 외부자에 의한 도청 및 감청으로 인한 기밀 정보의 유출이 발생할 수 있다는 보안 취약점 문제가 나타난다. 이러한 도청 및 감청 문제를 해결하기 위해서는 VoIP 서비스에서의 전송 정보에 대한 암호화가 필요하다[3]. 현재 이러한 암호화를 위해 SRTP(Secure Real-time Transport Protocol)[5]와 ZRTP(Zimmerman Real-Time Transport Protocol)[6]가 많이 사용되고 있다. 그러나 SRTP와 ZRTP는 단일 사설

망 내에서의 전송 정보에 대한 암호화는 처리할 수 있지만 서로 다른 망에 있는 참여자간의 전송 정보 암호화에 대해서는 문제를 발생시킨다. 본 논문에서는 이러한 문제점을 해결하기 위한 방법으로 VoIP 서비스 시 미디어 정보 전송을 담당하는 RTP(Real-time Transport Protocol)[7] 프로토콜을 단일 통신망 및 이종의 통신망에서 암호화를 효율적으로 수행할 수 있도록 재설계하고 이를 적용한 VoIP 서비스의 성능 분석을 수행한다.

본 논문의 구성은 2장에서 본 연구의 배경이 되는 VoIP와 VoIP 서비스 수행 시 필요한 프로토콜에 대해 알아본다. 3장에서는 서로 다른 통신망 간에서 VoIP 서비스 수행 시 기존의 방법인 SRTP와 ZRTP 방법을 이용하여 VoIP 미디어 정보를 암호화 할 때 발생하는 문제점을 살펴본 후 이를 해결하기 위한 방법으로 RTP 프로토콜을 재설계하고 이를 적용한 암호화 과정에 대해 설명한다. 그리고 이를 적용할 경우의 VoIP 서비스의 성능을 분석한다. 마지막으로 4장에서 결론을 맺는다.

II. 관련 연구

1. VoIP

VoIP 서비스는 음성 데이터 전송 시 인터넷의 IP 계층을 이용하는 기술이다. VoIP는 지능화된 호 처리와 VoIP 서비스의 생성 및 수행, 서비스 관리 기능 등을 담당하는 응용 계층(Application Layer)과 호 처리, 호 변환, 자원 관리, 매체 제어 등의 기능 등을 수행하는 신호 계층(Signaling Layer), 그리고 RTP 및 RTCP(Real-time Transport Control Protocol)[8] 프로토콜 등을 이용하여 실제 데이터 처리 및 전달 또는 변형, 품질 보장, 톤 발생 기능 등을 담당하는 매체 계층(Media Layer)의 3계층으로 나누어지며 계층별로 상대방과 같은 프로토콜을 이용하여 통신작업을 수행한다.

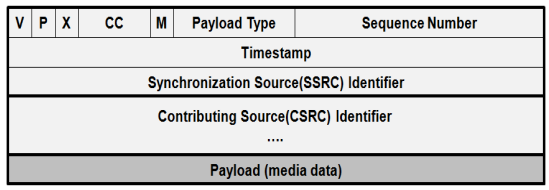
VoIP 서비스 처리 절차는 통신을 위한 세션 수립 및 해제와 관련된 호 처리와 호 처리를 통해 연결된 세션을 이용하여 음성 데이터를 주고받는 미디어 데이터 처리 단계로 이루어진다.

1.1 호 처리 프로토콜

VoIP 서비스는 호 처리 작업을 수행하기 위해서 H.323, SIP(Session Initiation Protocol)[9] 등의 프로토콜을 사용한다. H.323 프로토콜은 인터넷을 포함한 패킷 네트워크에서 실시간 음성, 영상 및 데이터 통신을 위한 프로토콜로 가장 먼저 발표된 VoIP 지원 프로토콜이다. 따라서, 초창기 VoIP 서비스에서 널리 사용되었으나 기본적으로 패킷 교환 방식의 랜 망에서의 다자간 음성, 화상, 데이터 통신을 지원하기 위해서 개발된 기술 방식이므로 광대역 네트워크와 대규모 사용자에 대한 지원에 있어서 한계성을 지닐 뿐 아니라 서비스 구현이 복잡하고 호환성을 보장하지 못한다는 단점을 가지고 있다. SIP는 이러한 단점을 보완하기 위해 제안된 프로토콜이다. SIP는 HTTP(HyperText Transfer Protocol)와 유사한 텍스트 기반의 메시지를 사용함으로써 헤더의 확장이 용이하고, 간단하게 세션을 설정하고 수정 및 종료할 수 있을 뿐만 아니라 다양한 멀티미디어 서비스를 쉽게 수용할 수 있고 개발이 쉽다는 장점을 가지고 있다. 따라서, 최근의 VoIP 시스템에서는 호 설정 프로토콜로 SIP를 주로 사용한다.

1.2 미디어 데이터 전송 프로토콜

VoIP 서비스는 호 설정 프로토콜을 이용하여 호 설정이 수행된 후 음성 또는 영상 데이터를 RTP를 이용하여 전송한다. RTP는 실시간 데이터 전송을 위한 표준 패킷형식이며, 종단간 네트워크 전송 프로토콜로써 오디오, 비디오 등의 실시간 데이터를 멀티캐스트나 유니캐스트로 전송하기에 적합한 기능을 제공한다. 그림 2는 RTP의 패킷 구조를 보여준다.



RTP 패킷은 버전 정보를 비롯하여 Payload 데이터 식별자, 시퀀스 넘버, 타임스탬프 등의 정보를 포함한다. 그러나, RTP 패킷에는 보안 관련 정보가 정의되어 있지 않기 때문에 암호화와 같은 보안 작업을 위해서는 별도의 보안 관련 프로토콜을 적용해야 한다.

2. VoIP 미디어 데이터 보안 프로토콜

VoIP 서비스는 그림 3과 같이 SIP와 같은 호 처리 프로토콜을 통해 호 설정이 이루어진 후 RTP를 통해 음성 데이터가 전송된다. 따라서, VoIP 시스템 운용 시 호 설정이 수행되는 시그널링 채널에 대한 보안과 음성 데이터와 같은 미디어 데이터의 보안이 필수적이다.

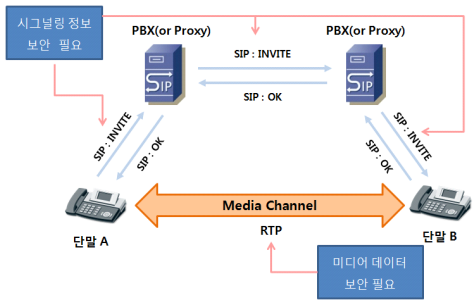


그림 3. VoIP 서비스 보안 요청 영역
Fig. 3. VoIP service security request zone

이를 위해 시그널링 보안에는 TLS, IPSec과 같은 보안 프로토콜을 적용하고, 미디어 보안을 위해서는 SRTP, ZRTP 등의 보안 프로토콜을 적용한다. 본 논문에서는 미디어 보안을 위한 연구를 진행한다.

표 1. VoIP 보안 프로토콜
Table 1. VoIP Security Protocol

구분	보안 프로토콜	
사용자 인증	HTTP Digest	
시그널링 보안	TLS	IPSec
미디어 보안	SRTP, ZRTP	
키 관리	SDES, MIKEY	IKE

2.1 SRTP(Secure Real-time Transport Protocol)

SRTP는 RTP 프로토콜의 확장으로 음성 및 영상 패킷을 전달하는 RTP 트래픽과 RTP에 대한 관리 프로토콜인 RTCP 트래픽에 대해 기밀성, 메시지 인증 및 재전송 방지 등의 보안 서비스를 제공하는 프로토콜이다. 그림 4에서 보듯이 SRTP는 VoIP의 실시간 트래픽 특성을 고려하여 보안 서비스를 적용 시 필요한 부하를 최소화하기 위해서 RTP 페이로드 부분만 암호화하는 방법을 통해 높은 성능을 보장하고 있다.

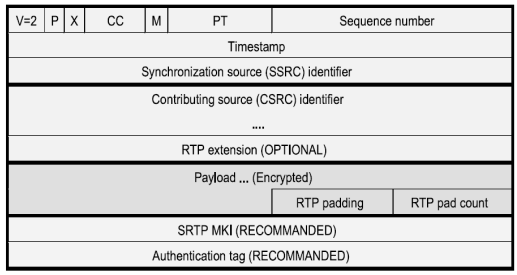
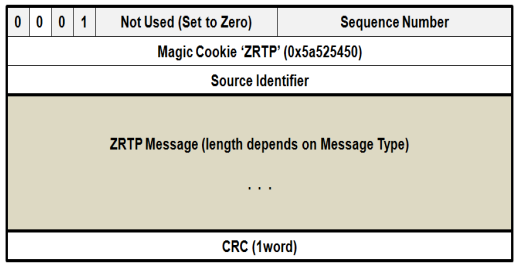


그림 4. SRTP Packet 형태
Fig. 4. SRTP Packet Format

SRTP는 AES(Advanced Encryption Standard) 등의 암호화 알고리즘을 사용하는데 SRTP 내에 키 교환 메커니즘이 정의되어 있지 않기 때문에 별도의 키 관리 프로토콜을 적용해야 한다[3].

2.2 ZRTP(Zimmerman Real-time Transport Protocol)

ZRTP는 Diffie-Hellman 키 교환 방법을 지원하기 위한 RTP 헤더의 확장으로 키 교환 과정을 수행하여 SRTP 세션을 수립한다. ZRTP는 RTP 내에 포함되기 때문에 시그널링 프로토콜의 지원을 필요로 하지 않는다는 특징을 갖는다. ZRTP는 양단간에 미디어 경로를 통해서 ZRTP 핸드셰이크를 수행함으로써 SRTP에 필요한 키를 교환한다. 키 교환 과정을 미디어 경로에서 수행하기 위해서 RTP 헤더 구조를 따르면서도 RTP 데이터와 구분이 가능하도록 그림 5와 같이 매직 쿠키 값과 같은 고유한 헤더 형태를 사용한다. 따라서 RTP 세션에서 RTP 데이터를 수신하는 도중에 ZRTP 기술을 통한 키 교환 과정의 수행이 가능하며, ZRTP 과정이 완료된 후 RTP 세션을 SRTP 세션으로 전환한다.



III. VoIP 미디어 정보 암호화를 위한 RTP 재설계

1. 기존 방법의 문제점

VoIP 서비스 시 양단간의 미디어 정보에 대한 암호화를 위해서는 SRTP를 많이 이용한다. SRTP는 별도의 키 교환 프로토콜을 필요로 하기 때문에 MIKEY, ZRTP와 같은 키 교환 방법을 같이 사용한다. 이 때, 양단의 단말기들은 단일 통신망 내에 모두 위치하거나 서로 다른 통신망에 각각 위치할 수 있다.

1.1 단일망 내에서의 VoIP 서비스

VoIP 서비스 시 양단의 단말기가 모두 단일 통신망 내에 위치하는 경우 SIP 정보는 VoIP 장비들을 이용하여 처리하고 미디어 정보들은 양단의 단말기가 직접 교환하여 처리한다. VoIP 서비스는 미디어 정보 교환 시 암호화 처리를 위해서 SRTP를 사용한다. SRTP는 키 관리를 위해 별도의 키 관리 프로토콜을 사용한다. 키 관리 프로토콜들은 MIKEY, ZRTP 등을 사용하는데 MIKEY는 키 교환을 위한 암호화 정보를 시그널링 채널에서 취급하고 ZRTP는 미디어 채널에서 처리한다. MIKEY와 같이 시그널링 채널의 지원을 받는 키 관리 프로토콜을 사용하는 SRTP는 SIP 내의 SDP(Session Description Protocol) 메시지를 이용하여 암호화를 위한 정보를 교환하여 암호화된 미디어 채널을 수립한 이후 이를 통해 미디어 정보를 교환한다. 암호화를 위해 SRTP를 적용하는 경우 SIP 정보 교환 시에 공격자에 의해 의도적으로 SDP에 포함되어 있는 암호화 정보가 훼손되거나 암호화 정보에 대해 문제가 발생할 경우에는 암호화 세션이 수립되지 않을 수 있다. SRTP를 위한 키 교환 시 ZRTP를 사용할 경우에는 암호화 정보를 시그널링 채널에서 취급하지 않고 미디어 채널을 이용하여 단말 간에 직접 교환한 후 암호화된 SRTP 세션을 수립하기 때문에 SIP 정보 교환 시 암호화 정보의 누락으로 인하여 암호화 세션이 성립되지 않는 문제를 해결하고 있다. SRTP/MIKEY와 SRTP/ZRTP는 두 방법 모두 단일 사설망 내에 위치하고 있는 양단의 단말간의 미디어 정보 암호화를 수행함에 있어서 암호화 적용이 가능하다.

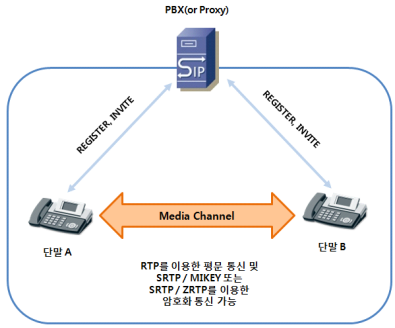


그림 6. 단일망 내에서의 VoIP 서비스
Fig. 6. VoIP Service in Single Network

1.2 서로 다른 망에서의 VoIP 서비스

VoIP 서비스의 또 다른 시나리오는 그림 7과 같이 양단의 단말기가 각각 서로 다른 통신망에 위치하고 있는 경우다. 이 경우 단일 통신망에서의 VoIP 서비스와는 달리 양단의 단말 간에 암호화 통신 시 문제점이 발생한다.

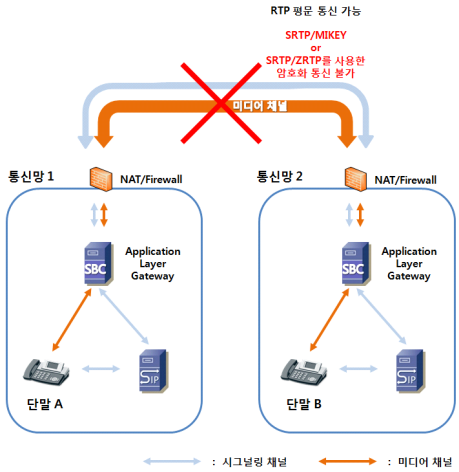


그림 7. 서로 다른 망에서의 VoIP 서비스
Fig. 7. VoIP Service between Different Networks

서로 다른 통신망에서의 VoIP 서비스 수행 시 사설 IP와 공인 IP간의 변환 작업을 필요로 하는 경우가 발생하는데 이를 처리하기 위해서 NAT(Network Address Translation)[10]를 사용한다. NAT는 OSI 7 Layer에서 Layer 3의 IP 주소와 Layer 4의 포트 번호에 대해 주소 변환을 수행한다. 통신 프로토콜을 설계할 때는 해당 프로토콜이 NAT 환경에 영향을 받지 않도록 애플리케이션 계층에서 IP 주소나 포트 번호를 직접적으로 다루지 않도록 설계하는 것이 일반적이다. 그러나, VoIP 서비스에서 호 설정 및 처리를 담당하는 SIP 프로토콜은 SIP 메시지 내부에 사설 IP 주

소를 포함하도록 설계되었음에도 불구하고 애플리케이션 계층에서 동작한다. NAT는 SIP 메시지 내의 사설 IP 주소를 공인 IP 주소로 변환하지 않기 때문에 송신자가 보낸 SIP 메시지에 대한 회신과 향후 이 송신자에 대한 세션 설정 시도 및 RTP 패킷의 라우팅에서 문제가 발생한다. VoIP는 이러한 문제들을 해결하기 위해서 SIP 메시지 내의 사설 IP 주소를 공인 IP 주소로 변경하는 게이트웨이 장비를 이용한다. 이러한 게이트웨이 장비들에는 STUN(Simple Traversal of UDP through NAT), TURN(Traversal Using Relay NAT), ICE(Interactive Connectivity Establishment), SBC(Session Border Controller) 등이 있는데 이 중 중앙 제어가 가능한 SBC를 최근 많이 사용하고 있다. SBC와 같은 게이트웨이 장비들은 VoIP 서비스 수행을 위해서 SIP 정보와 SDP 정보 그리고 RTP 패킷의 헤더 정보를 수정한다. 암호화를 하지 않은 RTP 패킷의 헤더 정보에 대한 수정은 패킷 전달 시 문제가 되지 않지만 SRTP나 ZRTP와 같이 암호화된 RTP 패킷의 헤더 정보를 수정하게 될 경우 패킷의 무결성에 문제가 발생하게 된다[11]. 이로 인해 양단의 단말 간에 인증 및 암호화 세션 수립 작업이 제대로 이루어지지 않아 VoIP 미디어 정보가 도청 및 감청 공격에 노출되어 기밀 정보의 유출이 발생하는 문제가 일어날 수 있다. 이를 해결하기 위한 부분적인 해결 방법의 하나로 양단말간의 암호화가 아닌 홉 간의 암호화를 진행하는 방법이 있지만 이는 반복적인 암/복호화의 작업으로 통신품질의 저하를 초래할 뿐만 아니라 통신 사업자가 다를 경우 인코딩 방법의 차이로 인하여 암/복호화 자체가 불가능하다. 따라서 서로 다른 통신망에서 양단의 단말 간에 암호화된 VoIP 서비스를 수행하기 위해서는 이러한 문제를 해결할 수 있는 새로운 암호화 지원 프로토콜을 필요로 한다.

2. 재설계된 RTP 제안

본 논문에서는 이종의 통신망 간의 VoIP 서비스 수행 시 양단간의 암호화 작업을 지원하기 위해 기존의 RTP를 재설계한다. 재설계된 RTP는 암호화와 관련된 모든 정보를 RTP 내에 포함시킴으로써 게이트웨이 장비에서 SIP 및 SDP 정보에 대한 수정이 발생하여도 암호화에 영향을 받지 않도록 설계한다. 또한, RTP 내부에 암호화 여부에 대한 코드를 포함시켜 양단간의 암호화 통신 시에는 게이트웨이 장비에서 RTP 헤더에 대한 수정을 방지함으로써 무결성을 유지하도록 한다. 따라서 서로 다른 사설망 간의 VoIP 서비스에서도 암호화된 미디어 정보의 교환이 수행된다.

2.1 재설계된 RTP 패킷 구조

재설계된 RTP 패킷 구조는 그림 8과 같다.

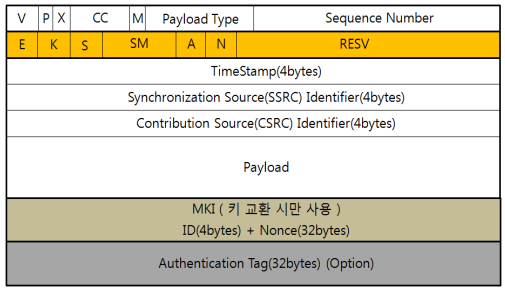


그림 8. 재설계된 RTP 패킷 구조
Fig. 8. Redesigned RTP Packet Format

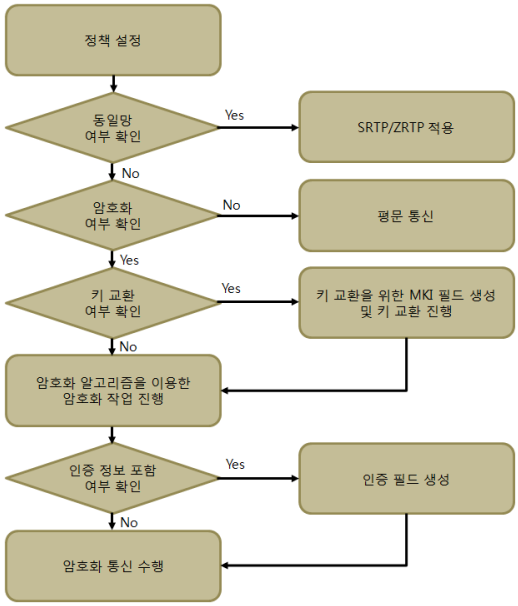
각 필드의 세부 사항을 살펴보면 V(Version) 필드에서 Sequence Number 필드까지와 TimeStamp와 SSRC, CSRC 필드는 기존의 RTP와 동일하다. E필드는 암호화 여부를 표기하는 필드로 암호화가 되어 있을 경우 게이트웨이 장치는 RTP 패킷의 헤더 정보를 수정하지 않고 중계 작업만을 진행한다. K(Key Exchange) 필드는 현재 RTP 패킷이 키 교환 작업을 진행하기 위한 패킷인지를 나타내는 것으로 K 필드가 키 교환 작업으로 설정되어 있을 경우에만 MKI 정보를 포함하도록 한다. 키 교환 시에만 MKI 정보를 포함하도록 하는 것은 키 교환 작업이 아닌 데이터 교환 작업 시에는 RTP 패킷의 사이즈를 줄여서 오버헤드를 감소하기 위한 것이다. 키 교환 작업은 ZRTP와 마찬가지로 Diffie-Hellman 키 교환 방법을 사용한다. SM(Secure Method) 필드는 암호화에 사용한 알고리즘을 표시하며, A(Authentication) 필드는 인증 정보에 대한 적용 여부 필드로 해당 필드가 설정되어 있을 경우에만 Authentication Tag 정보를 포함시키도록 한다. 인증 태그는 옵션 사항으로 A 필드가 설정되어 있지 않은 경우 생략함으로써 VoIP 서비스의 성능 감소를 방지하도록 한다. N 필드는 네트워크의 구성이 동일망인지 서로 다른 망인지를 나타낸다. 동일망의 경우에는 ZRTP와 같은 방법으로 동작하도록 한다. 각 필드의 세부사항은 표 2와 같다.

표 2. 재설계된 RTP 패킷 필드
Table 2. VoIP Security Protocol

필드명	내 용
E(Encryption)	2bit, 암호화 적용 여부
K(Key Exchange)	2bit, 키 교환 여부
S(Sender/Receiver)	2bit, Sender/Receiver 여부
SM(Secure Method)	6bit, 적용 암호화 알고리즘 표시
A(Authentication)	2bit, 인증 정보 포함 여부
N(Network)	2bit, 동일망 여부 표시
RESV(Reserved)	16bit, 확장성을 고려한 예약 필드
MKI	36bytes, 4byte의 ID와 32bytes Nonce 포함
Authentication Tag(Option)	32bytes, SHA256 알고리즘을 통해 생성된 인증 정보 제공

2.2 재설계된 RTP 처리 과정

재설계된 RTP는 정책 설정 단계와 처리 단계로 구분될 수 있다. 송신자 측에서 진행하는 정책 설정 단계에서는 암호화 적용 여부, 암호화 알고리즘, 인증 정보 포함 여부와 키 교환 여부 및 동일망 여부를 설정한다. 암호화 알고리즘은 DES, 3DES, AES를 선택할 수 있도록 하고, 동일망 여부는 SIP 레지스터 서버를 통해 확인하여 설정하도록 한다. 정책 설정이 완료되면 해당 정보를 제안 RTP의 해당 필드에 반영한다.



동일망일 경우에는 재설계된 프로토콜과 기존의 프로토콜을 모두 반영할 수 있지만 기존에 널리 사용되고 있는 SRTP/ZRTP를 따르도록 하고 서로 다른 망일 경우에는 제안 RTP를 적용하도록 한다. 키 교환 필드가 설정되어 있는 경우 MKI 필드에 ID와 Nonce 값을 포함시키고 DH 알고리즘에 따라 키 교환을 진행한다. 암호화 설정 시 페이로드를 설정 암호화 알고리즘으로 암호화하고 인증 필드 설정 시 SHA256을 이용하여 인증 태그를 생성해서 포함시킨다. 그림 9는 재설계된 RTP 처리 과정을 보여준다.

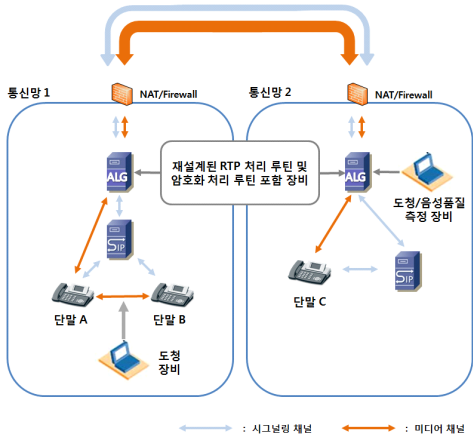
수신측에서는 설정된 내용에 따라 키 교환 작업 진행과 암호화된 데이터의 복호화 작업, 인증 작업을 진행한다.

3. 암호화 적용 여부 및 성능 평가

본 논문에서 제안한 재설계된 RTP의 암호화 적용 여부 및 통화 품질에 미치는 영향을 확인하기 위해 SRTP와 시그널링 채널의 지원을 받는 키 교환 방법인 MIKEY의 조합과 SRTP/ZRTP를 적용한 암호화 통신과 비교 분석을 진행한다.

3.1 실험 환경

실험을 위한 전체적인 구성도는 그림 10과 같다.



각 실험에 필요한 프로토콜 및 시스템을 이용하여 암호화 적용 여부 및 성능을 측정한다. VoIP 단말기의 호처리 및 미디어 처리를 위하여 OpenSIP[4]를 이용하고 NAT를 통과하기 위한 게이트웨이 장비로는 본 논문에서 제안한 RTP 처리 루틴을 포함하고 있는 암호화 장비를 사용한다. 기본적으로 이종의 통신망 간에서는 hop-by-hop의 방식으로 암호화

를 진행 시에도 데이터 인코딩 방법의 차이로 인하여 암호화 통신이 불가능하나 본 논문에서는 기존의 방법을 이용한 암호화 통신 시 동일한 인코딩 방법을 사용함을 가정하여 실험을 진행한다.

3.2 암호화 적용 여부

암호화 적용 여부를 확인하기 위하여 공개된 도청 툴인 Wireshark[12]를 이용한다. VoIP 미디어 정보에 대한 암호화 및 암호화된 정보의 송/수신이 제대로 이루어지는지 확인하기 위하여 100번의 통화를 시도하였다. 실험 결과, SRTP/MIKEY방법과 SRTP/ZRTP 방법은 단일 통신망 내에서의 통신 시에는 암호화가 가능한 반면 서로 다른 통신망일 경우에는 홉 간의 암호화만 가능함을 확인하였다. 홉 간의 암호화는 많은 암복호와 작업으로 VoIP 서비스의 성능 저하를 초래할 뿐만 아니라인코딩 방법의 통일을 요구하기 때문에 실제 서비스에서 적용하기는 어렵다. 반면 본 논문에서 제안한 방법은 양단의 단말의 위치에 상관없이 암호화가 적용될 수 있음을 확인하였다.

표 3. VoIP 미디어 정보에 대한 암호화 여부
Table 3. Encryption for VoIP Media Information

암호화 기법	암호화 적용 여부		
	단일 통신망	서로 다른 통신망	
		Hop-by-Hop	End-to-End
SRTP/ MIKEY	O	O	X
SRTP/ ZRTP	O	O	X
제안방법	O	O	O

3.3 성능 평가

VoIP 서비스의 성능 평가를 위해서 SRTP/MIKEY 방법과 SRTP/ZRTP, 그리고 본 논문에서 제안하는 방법에 대해 100번의 통화를 시도하여 미디어 전송을 위한 설정 시간과 패킷 지연 시간과 지터 값을 측정한다. 미디어 설정 시간에는 기본적인 설정 시간(α), DH 키 교환을 위한 핸드셰이크 시간(β), 키 교환을 위한 메시지 생성(δ), 검증(ε), 그리고 교환된 키를 SRTP로 전달하는 시간(λ)들이 요구된다. 표 4는 각 방법별로 요구되는 미디어 설정 시간을 보여준다.

표 4. VoIP 미디어 전송을 위한 설정 시간
Table 4. Set Time for VoIP Media Transmission

암호화 기법	설정 시간 요소
SRTP/ MIKEY	$\alpha + \delta + \varepsilon + \lambda$
SRTP/ ZRTP	$\alpha + \beta + \lambda$
제안방법	$\alpha + \beta$

SRTP/MIKEY 방식은 호 설정 시 키 교환에 필요한 정보를 처리하기 때문에 추가로 발생되는 메시지가 없다. 따라서, 기본적인 설정시간과 DH의 키 교환을 위한 메시지 생성 및 검증 시간과 교환된 키를 SRTP로 전달되는 시간이 요구된다. SRTP/ZRTP는 복잡한 핸드셰이크 과정 때문에 미디어 설정 시간이 오래 걸린다. 본 논문에서 제안한 방법 역시 SRTP/ZRTP의 키 교환 과정을 따르기 때문에 미디어 설정 시 SRTP/MIKEY 보다는 많은 시간을 필요로 한다. 그러나, 제안 방법은 교환된 키를 SRTP로 전달하여 설정할 필요가 없기 때문에 SRTP/ZRTP 보다 미디어 설정 시간을 단축할 수 있다.

또 다른 성능평가 요소로 음성품질을 측정한다. 각 보안 프로토콜이 음성품질에 주는 영향을 비교하기 위해 음성 통신의 평균 패킷 지연 시간과 패킷 지연 분포 값인 지터 값을 측정한다. 음성 품질 측정을 위해 OmniPeek[13]을 이용한다.

표 5. VoIP 음성 품질 측정 결과
Table 5. Result of VoIP Voice Quality Measurement

평균 패킷 지연 시간은 전체 통화 중 발생하는 모든 패킷에 대한 평균 지연이기 때문에 특정 시점에 대한 음성 품질을

보장하지는 않는다. 그러나, 지터의 경우는 패킷 지연 시간에 대한 분포이기 때문에 지터 값이 작다는 것은 지연의 편차가 적음을 나타내고 전체 통신 시 특정 패킷에 대해 큰 지연을 발생시키지 않음을 의미한다. 표 5는 음성 품질 측정 결과를 보여준다. 표 5에서 볼 수 있듯이 기존의 방법들에 비해 본 논문에서 제안한 방법의 경우 평균 패킷 지연 시간과 지터가 더 작음을 볼 수 있다. 이는 기존 방법들의 경우 홉 간의 전달 지연이 발생하기 때문으로 본 논문에서 제안한 프로토콜은 기존의 프로토콜과 비교하여 비도는 낮지 않으면서 성능을 개선했음을 볼 수 있다.

IV. 결 론

기존의 IP 네트워크를 활용하는 VoIP 서비스는 IP 환경에서 나타난 기존의 보안 문제를 비롯하여 다양한 보안 취약점에 노출되어 있다. 특히, 도청 및 감청으로 인한 기밀 정보의 유출은 주요 보안 이슈 중의 하나로 이를 방지하기 위한 보안 기법으로 SRTP나 ZRTP를 주로 사용한다. SRTP와 ZRTP는 통신에 참여하는 양단의 단말들이 동일 통신망 내에 위치하고 있을 경우에는 암호화 작업을 수행함에 있어서 문제점을 드러내지 않지만, 양단의 단말들이 서로 다른 통신망에 위치하고 있을 경우에는 암호화 작업을 수행하지 못한다. 양단의 단말들이 서로 다른 통신망에 있을 경우 VoIP 통신을 위한 정보 전송 시 NAT 및 방화벽을 통과할 수 있도록 게이트웨이 장비를 사용하여야 하는데 이 경우 게이트웨이 장비에서 SIP 메시지 및 RTP 헤더 정보를 수정한다. 이로 인해, 암호화된 데이터에 대해 무결성 에 대한 문제가 발생하게 되고, 인증 데이터의 훼손 및 복호화 작업이 진행되지 못하는 문제점을 나타낸다.

본 논문에서는 서로 다른 통신 망간에서의 VoIP 서비스 수행 시 VoIP 미디어 정보에 대한 암호화 과정에서 발생할 수 있는 문제점을 확인하고 이를 해결하기 위한 방법으로 RTP 패킷이 게이트웨이 장비를 통과하여도 무결성에 문제가 발생하지 않도록 재설계된 RTP 프로토콜을 제안하였다. 재설계된 RTP는 암호화 여부를 구분할 수 있도록 설계하여 기존의 SRTP/MIKEY 또는 SRTP/ZRTP와는 달리 게이트웨이 장비에서 서로 다른 통신망간에 암호화된 미디어 정보를 원활하게 교환할 수 있음을 확인하였다. 본 논문에서 제안한 방법은 음성 품질의 저하 없이 암호화 통화가 가능함을 확인하였으나 미디어 설정에 소요되는 시간이 SRTP/MIKEY에 비해 많이 요구됨을 알 수 있었다. 이는 키 교환 시 SRTP/ZRTP의 키 교환 방법을 따르기 때문인데, 차후 간략화된 키 교환 알고리즘에 대한 연구가 필요하다.

참고문헌

[1] JaeHong Min, PyungDong Jo, "VoIP Technology Trends", Weekly Trends of Tech. No.1021, http://www.itfind.or.kr

[2] JaHyun Koo, "VoIP Service Security Vulnerability Analysis", Journal of Korea Institute of Information Security & Cryptology, Vol.16, No.1, pp.60-63, 2006.

[3] Hyung-jun Oh, Yoo-hun Won, "A Design of Encryption Method for Strong Security about Tapping/Interception of VoIP Media Information between Different Private Networks", Journal of Korea Society of Computer Information, Vol.17, No.3, pp.113~120, Mar 2012.

[4] Sessiong Border Controller, http://www.opensipstack.org

[5] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K.Norrman, "The secure real-time transport protocol (SRTP)," RFC 3711, March 2004.

[6] P. Zimmermann, A. Johnston, and J. Callas, "ZRTP: Media Path Key Agreement for Secure RTP," Internet-Draft, March 2009.

[7] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A transport protocol for real-time applications," RFC 3550, July 2003.

[8] C. Huitema, "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)", RFC 3605, Oct 2003.

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP : Session Initiation Protocol", RFC 3261, June 2002.

[10] K. Egevang, P. Francis ,"Network Address Translator (NAT)", RFC 1631, May 1994

[11] Eunsung Park, Dongsu Seong, Keonbae Lee, "Refinement of RTP Processing Unit in SBC for VoIP Media Encryption between Private

Networks", Journal of Korean Institute of Information Technology, Vol.9, No.8, pp.185-191, Aug 2011.
〔12〕 Wireshark, http://www.wireshark.org
〔13〕 OmniPeek, http://www.wildpackets.com

저 자 소 개

오 형 준
2002 : 홍익대학교
컴퓨터공학과 공학사.
2004 : 홍익대학교
컴퓨터공학과 공학석사.
현 재 : 홍익대학교
컴퓨터공학과 박사과정.
관심분야: VoIP, 네트워크 보안
Email : hjoh@hongik.ac.kr

박 재 경
1994 : 동국대학교
컴퓨터공학과 공학사.
1996 : 홍익대학교
전자계산학과 이학석사.
2002 : 홍익대학교
전자계산학과 이학박사
현 재 : 학국과학기술원
사이버보안연구센타 연구위원
관심분야 : 네트워크 보안, 사이버 보안
Email : wildcur@kaist.ac.kr

원 유 헌
1972 : 성균관대학교 수학과 이학사.
1975 : 한국과학기술원
전자계산학과 이학석사.
1985 : 고려대학교
전자계산학과 이학박사.
현 재 : 홍익대학교
컴퓨터공학과 교수
관심분야 : 프로그래밍 언어론, VoIP,
네트워크 보안
Email : yhwon@hongik.ac.kr