VoIP Firewall/NAT Traversal 문제 해결을 위한 구조

최경호 강부중 노인우 임을규
한양대학교
beltre@hanyang.ac.kr, deviri@hanyang.ac.kr, inwoo13@hotmail.com, imeg@hanyang.ac.kr

The Structure of Solving VoIP Firewall/NAT Traversal Problem

Kyoung Ho Choi, Boo Joong Kang, In Woo Ro, Eul Gyu Im
Hanyang Univ.

요 약

VoIP(Voice over Internet Protocol)란 음성 데이터를 IP 데이터그램 방식으로 기존 인터넷망을 통해 전달해 주는 기술을 말한다. 기존 인터넷망을 이용하여 음성 데이터를 전달해 줌으로써 기존의 음성 전화 서비스에서 사용되던 회선비용을 크게 절감할 수 있다는 점은 VoIP의 장점 중 하나이다.

그런데 VoIP를 기존의 인터넷망에 그대로 적용하기에는 VoIP에서 사용되는 프로토콜의 특성으로 인해 어려움이 따르게 된다. 즉, 기존의 인터넷망에서 사용되고 있는 방화벽과 NAT(Network Address Translator)장비는 보안을 위해서는 필수적인 요소들 이지만, VoIP의 통신 입장에서는 음성 데이터의 원활한 통신을 방해하는 요소로 작용을 하게 된다. 이러한 문제는 VoIP 통신에 사용되는 시그널링 프로토콜인 H.323과 SIP 프로토콜의 연결 설정과 데이터 전송에 사용되는 동작 방식이 방화벽과 NAT장비의 기능에 충돌하는 점 때문에 발생하게 된다.

따라서 기존의 인터넷망을 그대로 사용하면서 VoIP의 통신이 원활하게 이루어지도록 하기 위해서는 이러한 문제의 해결이 반드시 이루어져야 한다. 본 논문에서는 기존에 Firewall/NAT Traversal 문제 해결을 위해 연구되던 기법들에 대해 살펴보고, 새로운 구조를 제시한다.

1. 서 론

VoIP(Voice over Internet Protocol) 기술은 회선교환 기술을 이용하여 음성 데이터를 전송하던 기존의 방식과 다르게 음성 데이터를 패킷 형태로 변환하여 패킷교환 방식으로 기존 인터넷망을 사용하여 전송하는 기술을 말한다. VoIP 기술의 가장 큰 장점은 기존의 인터넷망을 이용하여 음성 전화 서비스를 구현함으로써 기존에 사용되던 회선 비용을 크게 절감할 수 있다는 점을 들 수 있다. 이러한 VoIP 기술은 인터넷 전화 서비스 이외에도 웹 콜 센터, 통합 메시징 서비스 등 각종 부가 서비스와 영상회의 등 인터넷상에서의 멀티미디어 서비스에 대한 핵심 기술이라는 점에서 전 세계적으로 적극적인 기술개발과 서비스 투자가 이루어지고 있다.

그런데 이러한 VoIP 통신을 기존의 인터넷망에서 그대로 사용하기 위해서는 해결해야 할 한 가지 문제점이 발생하게 된다. 즉, VoIP 통신에 사용되는 시그널링 데이터와 음성 데이터가 기존의 인터넷망에서 널리 사용되고 있는 방화벽과 NAT(Network Address Translator) 장비를 통과할 수 있어야 한다는 것이다. 보안을 위한 목적으로 패킷을 필터링하는데 사용되는 방화벽과 공인 IP의 자원을 관리하는데 사용되는 NAT장비는 기존 인터넷망에서 중요한 역할을 하지만 VoIP 통신의 기본적인 특징과 충돌을 일으켜 VoIP의 시그널링과 음성 데이터의 원활한 통신을 방해하는 역할을 하게 된다.

VoIP 통신에 사용되는 대표적인 시그널링 프로토콜로는 ITU-T에서 개발한 H.323 프로토콜과 IETF에서 개발한 SIP 프로토콜이 있다.[1] H.323 프로토콜은 연결 설정을 위해 특정한 역할을 담당하는 H.225, H.245등의 프로토콜을 사용하고, 음성 데이터의 전송을 위해 RTP 프로토콜을 사용한다. H.323 프로토콜의 특징은 특정 세션의 연결을 위해 사용할 주소를 전 단계의 세션에서 결정한다는 점이다. 즉, 초기 연결 설정을 위해 사용되는 H.225 프로토콜이 다음 단계인 H.245 프로토콜의 연결에 사용할 주소를 설정해주게 된다. SIP 프로토콜은 연결 설정을 위해 세션에 대한 정보인 SDP가 포함된 메시지를 주고 받으며, 이 때 음성 데이터의 통신에 필요한 RTP 프로토콜이 사용할 주소를 설정해주게 된다.[2]

VoIP 통신에 사용되는 시그널링 프로토콜인 H.323과 SIP 프로토콜은 동적인 포트의 사용과 서로 통신할 주소를 패킷의 페이로드 부분에 담아 교환하는 특징을 가지고 있다. 이러한 특징은 VoIP의 음성 데이터가 방화벽과 NAT를 원활히 통과하지 못하게 되는 문제점을 발생하게 된다. 따라서 VoIP 통신이 방화벽과 NAT를 포함하고 있는 기존의 인터넷망에서 원활하게 이루어지도록 하기 위해서는 이러한 문제의 해결이 반드시 이루어져야 한다. 본 논문에서는 2장과 3장에서 VoIP 시그널링 프로토콜과 Firewall/NAT Traversal 문제에 대해 논하고, 4장에서 Firewall/NAT Traversal 문제 해결을 위한 기존의 연구들을 알아보고, 5장에서 새로운 구조를 제시한

뒤 6장에서 결론 및 향후 계획을 제시하겠다.

2. Firewall/NAT Traversal Problem

2.1. H.323 Protocol

H.323 프로토콜은 인터넷을 포함한 패킷 네트워크에서 실시간 음성, 영상 및 데이터 통신을 위해 ITU-T에 의해 개발된 프로토콜로 QoS(Quality of Service)가 보장되지 않는 packet-based network같은 기존 네트워크의 하부구조를 변경하지 않고 멀티미디어 서비스를 사용할 수 있다는 특징을 가진다.

H.323은 call signaling 부분과 음성 데이터 통신부분의 두 부분으로 나누어지며 전체적인 통신과정은 [그림 1]과 같다.

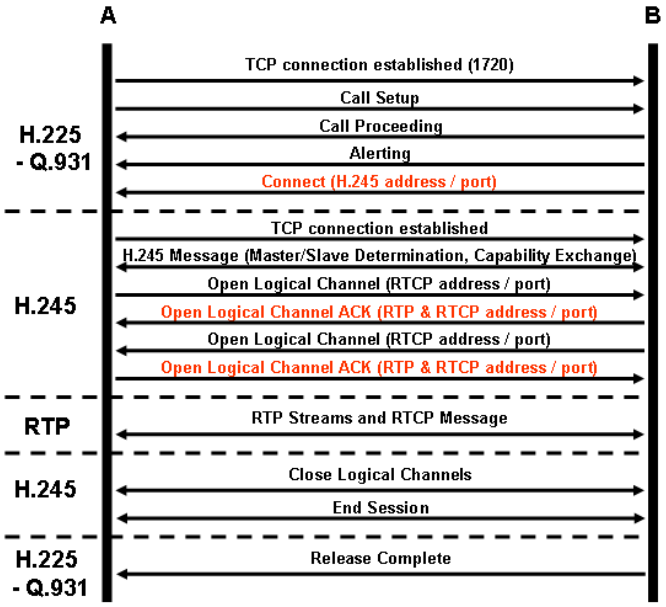

그림 1 : H.323 Call Setup Process

• H.225 - Q.931 protocol

두 H.323 단말간의 연결을 초기화 하기위해 사용하는 프로토콜로 TCP를 통해 전달되며, 고정 포트인 1720 포트를 사용한다.[2] 연결을 알리는 connect 메시지를 통해 다음 단계인 H.245 세션이 사용하게 될 IP 주소와 포트 번호를 알려주게 된다.

• H.245

Call에 대한 제어를 담당하는 프로토콜로 RTP에 의해 전달되는 모든 미디어 채널의 협상과 설정에 사용된다. 대표적인 기능에는 다음과 같은 것들이 있다.

- Capability Exchange

각 단말은 전송하게 될 미디어 형태, 코덱, 비트율 등과 같은 수신능력과 송신능력을 서로 교환한다.

- Open Logical Channel

오디오, 비디오 및 데이터 통신을 위해 사용될 논리 채널의 개폐를 제어한다. 이 때, RTP가 사용하게 될 IP 주소와 포트 번호를 결정하게 된다.

이와 같이 H.323 프로토콜은 데이터의 전송을 위해 연결을 설정하는 각 과정에서 사용할 주소를 전 단계에서 동적으로 결정하여 통신하고, 그 주소를 패킷의 페이로드 부분에 담아 보낸다는 특징을 가지고 있다. 이러한 특징으로 인해 H.323에서 사용하는 시그널링 데이터와 음성 데이터가 방화벽과 NAT장비를 원활하게 통과하지 못하게 되는 문제가 발생하게 된다.

2.2. SIP Protocol

SIP(Session Initialization Protocol)는 인터넷 기반 멀티미디어 세션을 생성하고, 수정하고 종료하는 역할을 하는 시그널링 프로토콜로 IETF에 의해 개발되었다. SIP의 역할은 메시지 교환을 원하는 주체들 간에 메시지 세션을 제어하기 위한 정보를 교환하는 것이다.

SIP는 통신을 위한 제어신호의 교환역할만 담당하며 실제 데이터의 처리는 RTP 등의 별도의 프로토콜에 담당시킨다. 즉, SIP는 RTP가 사용할 포트와 사용할 코덱 등의 정보를 담고 있는 SDP(Session Description Protocol)를 전달함으로써 세션의 정보를 교환하게 된다.

SIP는 연결 설정을 위해 고정된 TCP, UDP 5060 포트를 사용하며, 실제 데이터의 전송을 담당하는 RTP는 SIP를 통해 교환되는 SDP 메시지에 정의되어 있는 포트를 사용하게 된다. SIP의 전체적인 통신과정은 [그림 2]와 같다.

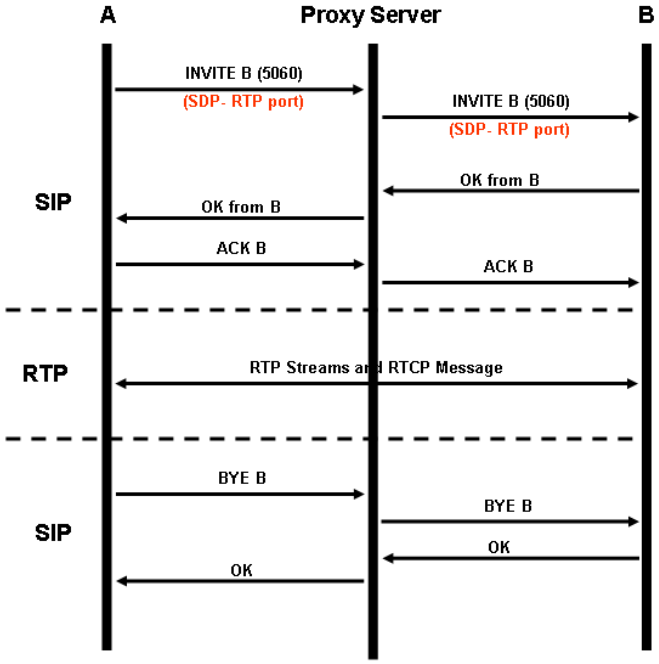

그림 2 : SIP Call Setup Process

이와 같이 SIP 프로토콜은 연결설정을 위해서는 일반적으로 고정된 포트인 5060포트를 사용하지만, 실제 데이터의 전송을 담당하는 RTP 프로토콜은 SIP의 연결설정 과정에서 전달되는 SDP 메시지 내에 정의되어 있는 포트를 사용하게 된다.[2] 이러한 구조로 인해 SIP도 H.323과 유사하게 음성 데이터가 방화벽과 NAT를 원활하게 통과하지 못하는 문제가 발생하게 된다.

2.3. VoIP Communication with Firewall

방화벽은 부적절하고 위험하다고 판단되는 패킷들을 보안 정책에 따라 차단하는 역할을 한다. 일반적으로 기본적인 규칙은 다음과 같다.

- 내부 네트워크로부터 통신이 시작된 외부 네트워크로부터 오는 패킷들은 내부 네트워크로의 진입을 허용한다.

- 외부 네트워크로부터 통신이 시작된 외부 네트워크로부터 오는 패킷들은 내부 네트워크로의 진입을 허용하지 않는다.

- 외부 네트워크로부터 통신이 시작된 외부 네트워크로부터 오는 패킷들의 경우 well-known 포트로 연결된 패킷이라면 내부 네트워크로의 진입을 허용한다.

[그림 3]은 VoIP 통신이 방화벽을 통과할 때의 문제점을 보여주고 있다.

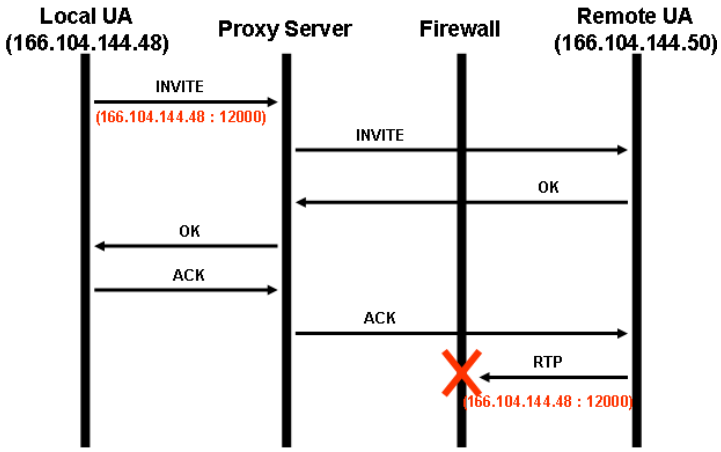

그림 3 : Firewall Traversal Problem

SIP 프로토콜은 음성 데이터의 통신에 사용되는 RTP 프로토콜이 사용할 IP 주소와 포트 번호를 연결 설정 단계에서 설정해 주게 된다. 즉, Local UA는 연결 설정을 위해 INVITE 메시지를 보낼 때 SDP 메시지 내에 RTP 통신을 위해 사용할 IP 주소와 동적으로 할당된 포트 번호를 담아 Remote UA에 알려주게 된다. 이 INVITE 메시지를 받은 Remote UA는 SDP 메시지 내에 있는 IP 주소와 포트번호로 RTP 통신을 시도하게 된다.[3] 그러나 방화벽은 동적으로 생성된 임의의 포트를 사용하는 외부 네트워크로부터 생성된 패킷은 부적절한 패킷으로 판단하여 차단하게 된다. 따라서 이 RTP 트래픽은 방화벽에 의해 차단되어 Local UA에 전달되지 못하는 문제점이 발생하게 된다.

2.4 VoIP Communication with NAT

NAT는 private network에서 임의로 사용하는 사설 IP 주소와 public network에서 사용하는 공인 IP 주소를 상호 변환시켜줌으로써 공인 IP 주소를 다수가 사용할 수 있도록 해주는 기능이다. 즉, 패킷이 private network와 public network 사이에 전송될 때 패킷의 헤더 부분에 있는 주소를 변경하여 주는 기능을 한다.

[그림 4]는 VoIP 통신이 NAT 장비를 통과할 때의 문제점을 보여주고 있다.

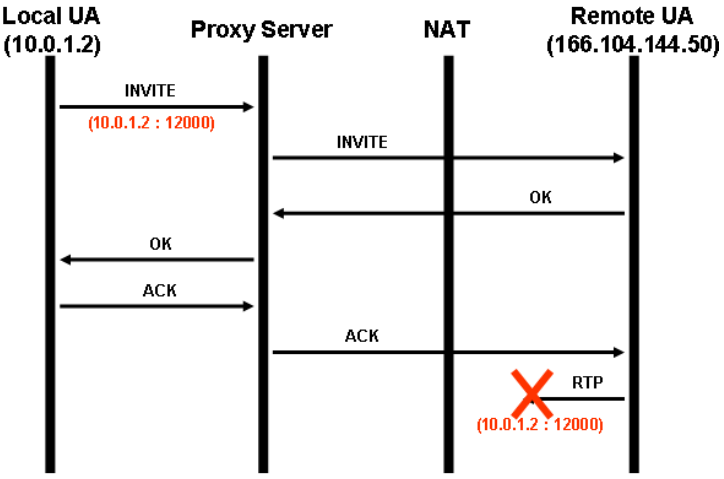

그림 4 : NAT Traversal Problem

Remote UA는 RTP 통신을 위해 연결 설정 시 SDP 메시지를 통해 전달 받은 IP 주소와 포트 번호를 사용하게 된다. Local UA는 private network내에 존재하는 단말로 SDP 메시지에 사설 IP 주소를 담아 보내게 된다. NAT 장비는 주소 변환 시 헤더 부분에 있는 주소만을 변경하고, 페이로드 부분에 있는 주소는 변경할 수 없기 때문에 Remote UA는 사설 IP 주소로 RTP 통신을 시도하게 된다. 그러나 사설 IP 주소는 public network에서는 사용할 수 없는 주소이기 때문에 Remote UA는 이 사설 IP 주소로는 Local UA와 통신을 할 수 없게 되는 문제점이 발생하게 된다.

3. 문제 정의

2절에서 살펴본바와 같이 VoIP 통신이 방화벽과 NAT 장비를 통과하여 이루어지게 하기 위해서는 몇 가지 해결해야 할 문제가 발생하게 된다. 이는 VoIP 통신에 사용되는 시그널링 프로토콜인 H.323과 SIP의 다음과 같은 기본적인 특징이 방화벽과 NAT 장비의 기능과 충돌되는 점 때문에 발생하게 된다.

- 동적인 포트의 사용
- 다음 단계의 통신에 사용할 주소를 페이로드 부분에 저장

VoIP 통신에 동적인 포트를 사용하는 특징은 방화벽의 기능과 충돌을 일으키게 된다. VoIP 통신이 동적인 포트를 사용하기 때문에 VoIP 통신에 사용되는 패킷들이 방화벽을 통과하기 위해서는 방화벽의 모든 포트가 열려 있어야 한다. 하지만 이는 보안상 심각한 문제가 발생하게 된다.

그리고 VoIP 통신에서 다음 단계의 통신에 사용할 주

소를 페이로드 부분에 저장하는 특징은 NAT 장비의 기능과 충돌을 일으키게 된다. NAT 장비는 private network와 public network 사이의 통신에서 주소를 변환시킬 때 패킷 헤더부분의 주소만 변환 시키고, 페이로드 부분은 변환을 시키지 못한다. 이는 private network내의 단말이 자신의 사설 IP를 다음 단계의 통신에 사용하기 위해 페이로드 부분에 담아 보내게 되었을 때 문제가 발생하게 된다.

따라서 VoIP 통신이 기존의 인터넷망에서 원활히 이루어지게 하기 위해서는 이러한 문제들의 해결이 필요하게 된다.

4. 관련연구

4.1. Middlebox communication (MIDCOM)[4]

이 방식은 신뢰할 수 있는 외부의 MIDCOM agent를 두어 MIDCOM agent가 방화벽 또는 NAT 장비를 직접 제어하는 방식이다. VoIP 통신에서 signaling 과 음성 데이터의 원활한 통신을 위해 MIDCOM agent는 보안 정책에 따라 시그널링과 음성 데이터가 방화벽을 통과하도록 허용한다. MIDCOM은 PDP(Policy Decision Point) 구성요소를 두어 보안 정책을 관리하게 된다.

[그림 5]는 MIDCOM의 구조를 보여주고 있다.

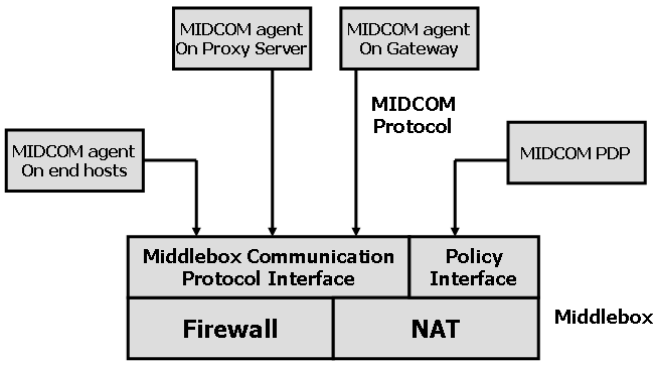

그림 5 : MIDCOM Framework

4.2. Midcom-unaware NAT/Firewall Traversal[5]

이 방식은 시그널링 데이터와 음성 데이터를 각각 분리하여 처리하는 방식이다. 즉, 시그널링 데이터의 처리는 signaling proxy server가 담당을 하고, 음성 데이터의 처리는 media proxy server가 담당을 하게 된다.

시그널링 데이터의 통신은 keep-alive 패킷을 이용해 주기적으로 시그널링 세션을 유지해 줌으로써 외부에서 내부로의 연결을 가능하게 해 준다. 그리고 음성 데이터의 통신을 위해서는 [그림 6]과 같은 방식으로 통신을 하게 된다.

Signaling proxy server는 INVITE 메시지를 받으면 media proxy server 에게 IP 주소와 포트 번호를 예약하도록 한다. 그리고 INVITE 메시지의 SDP를 수정하여 RTP 패킷을 media proxy server의 할당된 주소로 전송하도록 UA2에게 알려준다. 또한 OK 메시지의 SDP를 수정하여 RTP 패킷을 media proxy server의 할당된 주소로 전송하도록 UA1에게 알려준다.

UA1과 UA2는 각각 RTP 패킷을 media proxy server로 보내고, media proxy server는 패킷을 수신하여 각각의 소스 IP 주소와 포트번호를 연결할 대상의 외부 IP 주소와 포트 번호와 대응시킨다. 이후 전송되는 음성 데이터는 media proxy server로 전송되어 목적지 주소와 포트 번호가 변경되어 각각의 UA에게 전달된다.

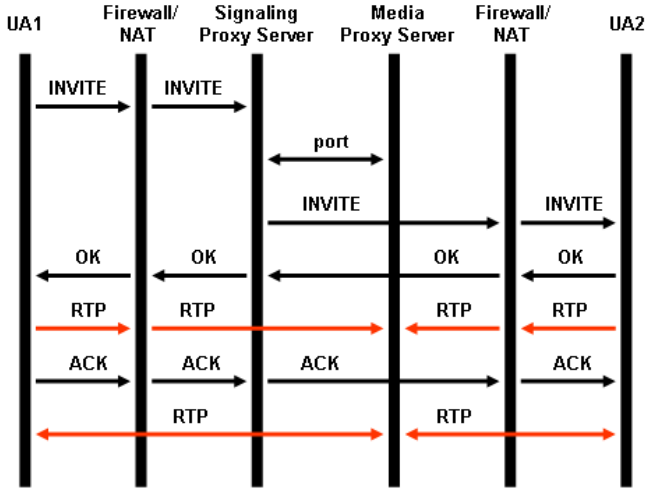

그림 6 : Midcom-unaware NAT/Firewall Traversal

4.3. Simple Traversal of UDP through NAT (STUN)[6]

이 방식은 NAT 장비가 주소 변환 시 패킷의 헤더 부분에 있는 주소만을 변경하고, 페이로드 부분에 있는 주소는 변경할 수 없기 때문에 VoIP 통신이 원활히 이루어지지 않는 문제를 해결하기 위해 제안된 방식이다.

STUN 프로토콜은 단말이 NAT 장비 뒤에 위치하는지 여부를 판단해주고, NAT장비 뒤에 위치해 있다면 어떤 종류의 NAT 장비 뒤에 위치해 있는지를 판단해 준다. 그리고 private network내에 있는 단말이 public network와의 통신에 사용할 공인 IP주소와 포트 번호를 알려주는 기능을 한다. 이렇게 하여 얻은 공인 IP주소와 포트번호를 패킷의 페이로드 부분에 담아 보내게 되면, 기존의 VoIP 통신에서 NAT 장비와의 충돌되는 점을 해결할 수 있게 된다.

그런데 STUN 프로토콜은 symmetric NAT 의 특성으로 인해 symmetric NAT 환경에서는 동작하지 않는 단점을 가지고 있다. 이러한 문제점을 보완하기 위해 TURN(Traversal Using Relay NAT) 방식이 제안되었다. 이 방식은 TURN 서버가 자신의 공인 IP 주소를 private network내에 존재하는 단말에 제공해 줌으로써 두 단말간의 통신이 TURN 서버를 경유하여 이루어지게 하는 방식이다.[7]

5. 제안하는 구조

VoIP 통신에서 Firewall/NAT Traversal 문제를 해결하기 위한 많은 연구들이 이루어져 왔으며, H.323 프로토콜의 경우에는 Firewall/NAT Traversal 문제 해결을 위해 H.460.17, H.460.18, H.460.19의 표준을 정의하고 있

다. 하지만 이는 H.323 프로토콜에 관한 Firewall/NAT Traversal 문제 해결을 위한 표준으로 SIP 프로토콜에의 적용에는 적합하지 못하다.

SIP 프로토콜을 사용하여 통신을 하는 경우 public network의 단말이 private network내의 단말로 연결을 시도하는 경우는 방화벽과 NAT 장비의 방해를 받지 않고 통신을 할 수 있다. 그러나 private network내의 단말이 public network의 단말로 연결을 시도하는 경우는 방화벽과 NAT 장비로 인해 통신이 원활하게 이루어지지 않는 문제가 발생을 하게 된다. 따라서 private network내의 단말이 public network의 단말로 연결을 시도하는 경우에 대한 문제를 해결하기 위한 구조를 제시하겠다.

VoIP 통신에서 Firewall/NAT Traversal 문제를 해결하기 위한 전체적인 구조는 [그림 7]과 같다.

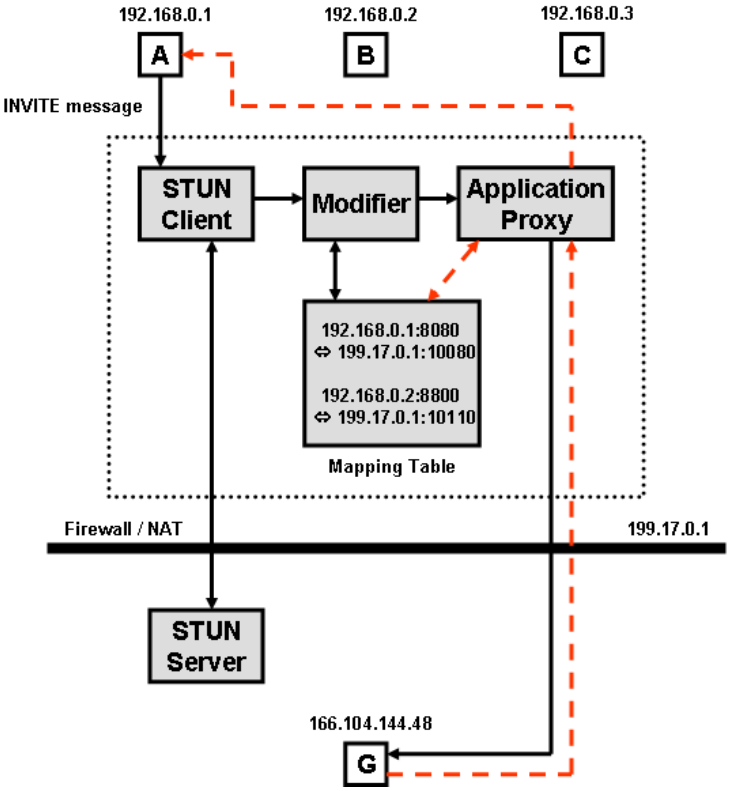

그림 7 : 제안하는 구조

각 모듈은 다음과 같은 기능을 하게 된다.

• STUN Client

STUN Server에 쿼리를 보내어 private network내에 있는 단말이 public network와 통신할 수 있는 공인 IP 주소와 포트번호를 얻는 기능을 한다.

• Modifier

INVITE 메시지 내의 SDP 메시지에 저장되어 있는 RTP 통신에 사용할 주소와 포트 번호를 STUN Client를 통해 얻은 공인 IP주소와 포트번호로 대치한다. 그리고 이전에 SDP 메시지에 저장되어 있던 주소와 STUN Client를 통해 얻은 주소를 Mapping table 에 저장한다. 이 INVITE 메시지를 받은 public network의 단말은 대치된 공인 IP주소와 포트번호 RTP 패킷을 보낼 수 있다.

• Application Proxy

STUN Client를 통해 얻은 공인 IP주소와 포트번호로 INVITE 메시지를 보내주고, RTP 패킷을 받기 위한 세션을 유지해준다. Public network의 단말은 이 세션을 통해서 private network내에 존재하는 단말로 패킷을 보낼 수 있다.

RTP 패킷을 받았을 시는 mapping table에 저장된 정보를 이용하여 RTP 패킷을 목적지 단말에 전달해 주게 된다.

6. 결론 및 향후 계획

VoIP 기술은 기존의 인터넷망을 이용하여 음성 전화 서비스를 구현함으로써 기존에 사용되던 회선 비용을 크게 절감할 수 있다는 장점을 가지고 있다. 그러나 VoIP 통신이 기존의 인터넷망에서 원활히 이루어지게 하기 위해서는 방화벽과 NAT 장비와 충돌되는 점을 해결해야만 한다.

우리는 VoIP 통신이 방화벽화 NAT 장비와 충돌되는 점을 해결하기 위한 구조를 제시하였다. NAT 장비와 충돌되는 문제 해결을 위해 INVITE 메시지 내의 SDP 메시지를 수정하는 구조를 제시하였고, 동적으로 할당된 포트를 가진 패킷이 방화벽을 통과하기 위한 방법으로 private network에서 미리 열어둔 세션을 통해 private network로 패킷을 전송하는 방법을 제시하였다.

VoIP 통신이 실시간으로 이루어져야 한다는 점을 고려해 볼 때 INVITE 메시지를 실시간으로 수정할 수 있는 알고리즘의 개발이 요구되어 진다.

참고문헌

[1] U.Black, "Internet Telephony Call Processing Protocol", Prentice Hall, 2001

[2] D.Richard Kuhn, Thomas J.Walsh, Strffen Fries, "Security Consideration for Voice over IP Systems", NIST SP800-58, 2005

[3] A.B.Johnston, "SIP Understanding the Session Initiation Protocol", Artech House, 2001

[4] P.Srisuresh, J.Kuthan, J.Rosenberg, A.Molitor, A.Rayhan, "Middlebox communication architecture and framework", RFC3303, 2002

[5] S.Sen, P.Sollee, S.March, "Midcom-unaware NAT/Firewall Traversal", Internet Draft, 2002

[6] J.Rosenberg, J.Weinberger, C.Huitema, R.Mahy, "Simple Traversal of User Datagram Protocol Through Network Address Translators", RFC3489, 2003

[7] J.Rosenberg, R.Mahy, C.Huitema, "Traversal Using Relay NAT", Internet Draft, 2005