

VoIP, MoIP 표준과 보안 이슈

IP를 이용한 음성 및 비디오, 인스턴트 메시징, Application 공유 등을 구현하는 실시간 통신플랫폼은 표준에 기초하여 설계되어야 한다. 인터넷은 일반적으로 Best effort Network로써, 회선망처럼 QoS(Quality of Service)를 보장하지 못한다. 이런 Network에서 VOIP를 위한, 표준 프로토콜, 시스템의 구성, 작동구조 및 QoS를 보장하기 위한 방법 등을 알아보고, VoIP의 보안 취약성에 대해 알아본다.

개요

VoIP란?

VoIP(Voice over Internet Protocol)는 인터넷망을 통해 음성신호를 실어 나르는 기술로, 기존 회선교환방식의 일반전화와 달리 인터넷의 근간인 인터넷프로토콜(IP) 네트워크를 통해 음성을 전송한다. 그러나, 인터넷은 일반적으로 Best effort Network로써, 회선망처럼 QoS(Quality of Service)를 보장하지 못함에도 불구하고, 인터넷의 발전에 따라 전 세계에 통일된 데이터망(Internet)이 형성되면서 음성, 비디오, 데이터를 IP 네트워크에 통합하여 전송하기 시작하였다.

일반적으로 VoIP의 시작은 오래되었으나, 최근에는 다양한 융합형태의 VoIP가 등장하고 있고, 경비절감을 위해 급성장세를 보이고 있다. 우리나라에서 시내전화 사업자가 VoIP 서비스를 하려면 인터넷 전화사업 허가를 받아 식별번호 '070'을 사용해야 한다.

VoIP 기본기술

IP Network의 실시간 통신플랫폼은 표준 신호프로토콜을 사용해야할 뿐만 아니라, 인터넷망에 대한 이해가 없으면 실현할 수 없다.

인터넷에서 QoS(Quality of Service)는 Bandwidth, Delay, Packet Loss가 일정한 허용범위 내에 있어야 한다. 그리고, RTP(Real Time Transport Protocol), RTCP(Real Time Control Protocol) 등과 적절한 Codec 기술이 적용되어야 한다. 예를 들면, Media를 전송하기 위한 대역폭으로 G.711(64kbps), G.729(8kbps) 등과 수백ms 이하의 지연시간, 시스템에서 허용(복구) 가능한 Packet Loss의 발생 등이 보장되어야 한다.

인터넷에서 회선망과 같은 QoS(Quality of Service)를 보장 받기 위해서는 Bandwidth를 충분히 확보하거나, Delay, Packet Loss 등과 적절히 타협해야 될 것이다(Public 인터넷망의 Bandwidth는 Guaranty 되지 않는다).

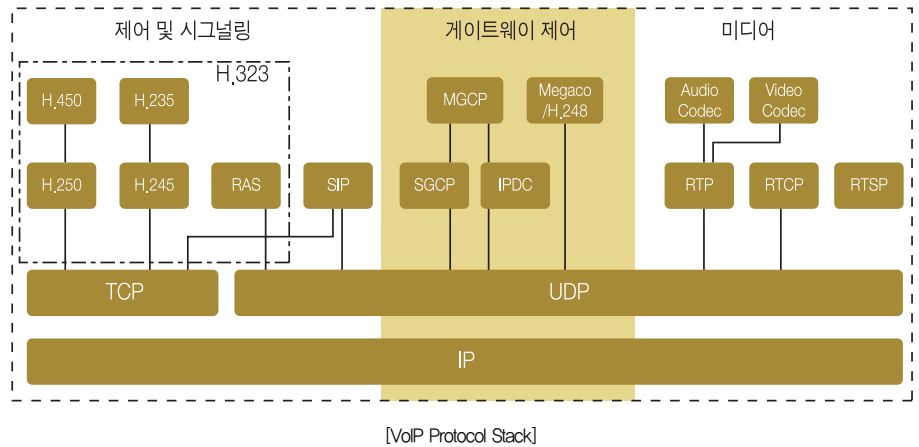
VoIP는 Call 제어에 사용되는 SIP or H.323, 음성 및 비디오 신호를 디지털 형식으로 변환하고, 신호의 효율적인 전송을 위해 압축/압축해제를 실행하는 Codec, 그리고 통신 세션을 모니터링하는 RTP 및 RTCP 등이 지원되어야 한다.

표준 프로토콜

표준의 종류

VoIP는 다음의 표준 프로토콜이 서로 조합된다.

- 제어 및 Signalling 프로토콜 : H.323, SIP 등
- 게이트웨이 제어 프로토콜 : MGCP, Megaco
- 미디어 코딩 및 전송 프로토콜 : RTP, RTCP, A/V Codec 등

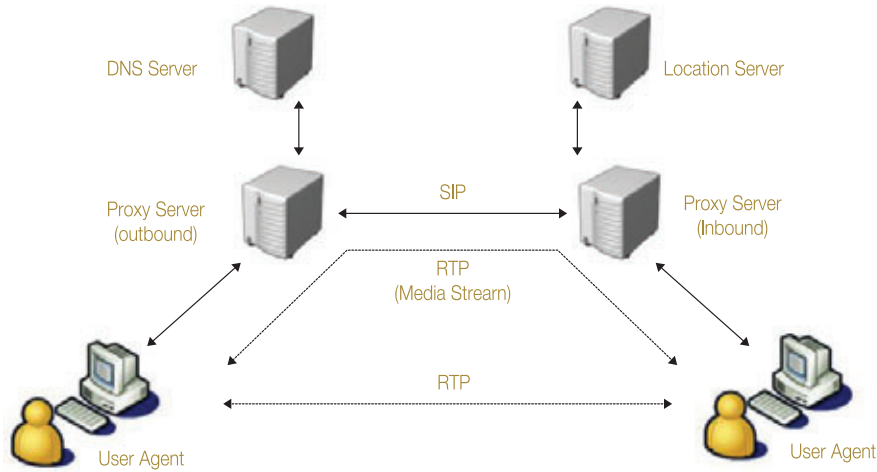


인터넷에서 전화처럼 Call(호)을 제어하기 위해서는 표준화된 제어와 신호프로토콜이 중요하다. 게이트웨이 제어 프로토콜은 IP 망과 PSTN 망을 연결하는 기간사업자의 몫이다. 대표적인 Signalling 프로토콜로 H.323, SIP가 있지만, H.323은 전화망이 우선되는 시대에 효과적이었고 아직도 많은 부분에서 사용되고 있다. 인터넷망을 근간으로 하고 미래지향적으로 생각한다면, SIP에 대한 이해도를 높이는 것이 좋다.

구분	H.323	SIP
개요	· QoS가 보장되지 않는 LAN상에서 실시간 음성, 데이터, 영상 등을 전송하는 표준	· 인터넷상에서 멀티미디어 서비스를 위한 표준
관련 장비	· H.323 단말 · H.323 게이트웨이 · 게이트키퍼	· SIP 단말 · Location 서버 · Proxy 서버
특징	· 가장 먼저 나타난 프로토콜이며, 가장 많이 사용되었지만, · 호설정 과정이 복잡하고, 새 IP망에서는 부적합 · 호환성, 확장성 부족	· 호설정이 단순 · IP7기반에 적합
표준 단체	· ITU	· IETF

SIP(Session Initiation Protocol) 구성 요소

SIP는 다수의 사람이 화상회의나 전화통화를 할 때 사용자를 제어하기 위한 프로토콜로써, 회의나 전화통화에 상대방을 쉽게 초대할 수 있도록 하기 위해 만들어졌다.

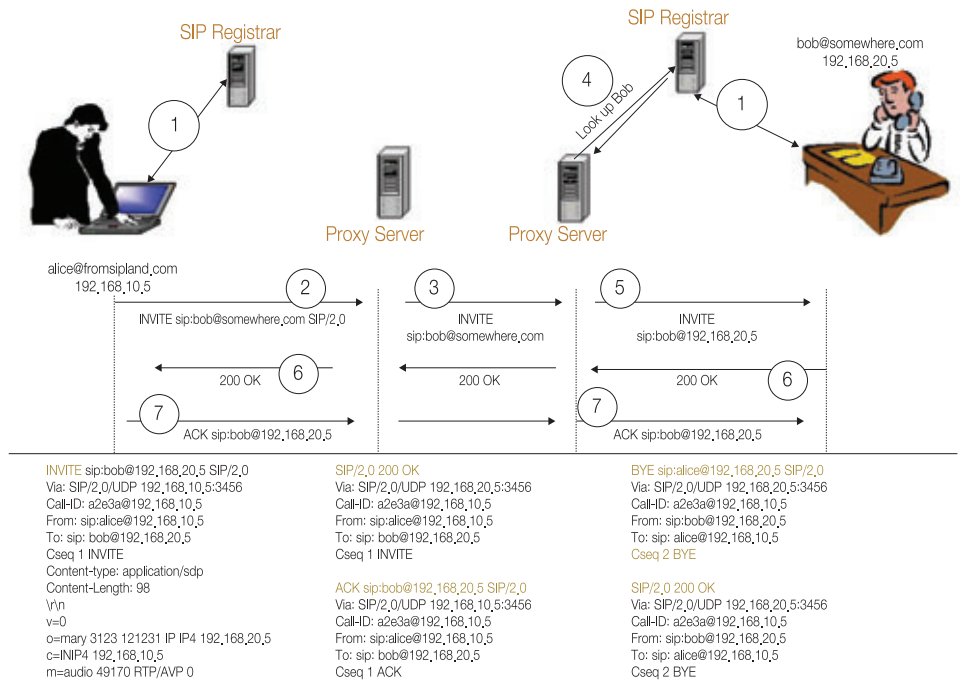


[SIP 시스템의 구성]

- User Agent(UA) : 전화를 걸고 받을 수 있고 SIP 프로토콜의 기능을 지원하는 터미널.
- Location Server : SIP 네트워크에서 주소를 확인한 후에 확인한 주소에 맞는 위치를 검색하기 위한 서버 또는 컴포넌트.
- Registrar Server : SIP 사용자 단말기가 SIP 네트워크의 일부분으로 등록을 하기 위해 필요한 서버 또는 컴포넌트.
- Proxy Server : 여러 User Agent로부터 SIP 요청을 받아 Next hop으로 전달해 주는 서버.
- Redirect Server : 다른 Client들로부터 들어오는 요청을 연결해 주고, Proxy 서버의 Processing 부하를 경감.

SIP 작동 구조

- ① 송신자(Alice)가 수신측(Bob) 초대하기 위하여 Proxy 서버에 초대 메시지를 보낸다.
- ② Proxy 서버에서 수신측(Bob) 주소를 가지고 위치를 알기 위해 Location 서버에 문의한다.
- ③ Location 서버는 수신측(Bob)의 위치를 Proxy 서버에 알려준다.
- ④ Location 서버로부터 받은 위치정보를 이용하여 수신측(Bob)에게 초대 메시지를 보낸다.
- ⑤ 수신측(Bob)은 초대 메시지를 받으면 전화벨을 울려 전화가 온 것을 알린다.
- ⑥ 200OK 메시지를 송신측(Alice)에게 보내 연결이 만들어진 것을 알린다.
- ⑦ 200OK에 대해서 송신측(Alice)은 ACK로 응답하고 통화가 시작된다.



[SIP 동작순서, 출처: Wikipedia]

SIP 메서드 기능

- INVITE : SIP 세션을 시작하기 위한 요청, 발신자로부터 수신자에게 보냄
- ACK : 수신자가 호출을 수락, ACK는 발신자로부터 수신자에게 보냄
- OPTIONS : 발신자가 수신자에게 자체 기능으로 응답할 것을 요청
- BYE : 세션을 종료하기 위한 요청, BYE는 발신자나 수신자가 보낼 수 있음, BYE를 수신하는 당사자가 BYE로 응답할 필요는 없음
- CANCEL : 일시 중지된 요청을 취소함
- REGISTER : 발신자가 현재 위치를 관리자 서버에 등록하기를 원함
- SUBSCRIBE : 발신자가 수신자의 상태 정보에 대한 업데이트를 요청
- NOTIFY : 자신의 업데이트된 상태를 가입한 당사자 자체에 전달함
- MESSAGE : 인스턴트 메시지를 보내는 데 사용

[SIP 메시지 값]

메시지 종류	값	기능
INVITE	1xx	Informational
ACK	2xx	Success
BYE	3xx	Redirection
CANCEL	4xx	Client Error
REGISTER	5xx	Server Error
OPTION	6xx	Global Error

RTP(Real Time Transport Protocol)

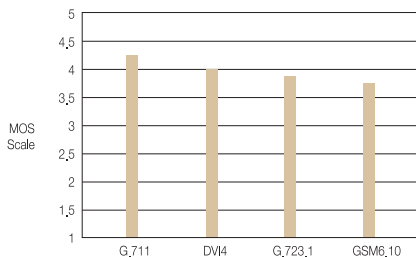
RTP에는 실시간 세션에 관한 정보가 포함되어 있으므로, 응용 프로그램은 지터, 잘못된 패킷 순서 및 삭제된 패킷을 조정할 수 있도록 되어 있다. RTP와 RTCP(Real Time Control Protocol)는 UDP와 함께 기본 전송 계층으로 사용되고, IP와 함께 기본 네트워크 계층으로 사용된다. RTP는 특정 미디어 스트림의 송신자와 수신자 간에 협상된 동적 UDP 포트를 사용한다.

- Payload Type : RTP 페이로드 유형을 정의
- Sequence Number : 시퀀스 번호는 임의 값에서 시작하여 전송된 각 RTP 패킷에 대해 1씩 증가, 실시간 응용 프로그램에서 이 값을 사용하여 패킷 손실을 확인하고 올바른 패킷 순서를 복원
- Timestamp : 타임스탬프 값은 RTP 패킷에서 첫 번째 옥텟의 샘플링 순간. 사용되는 샘플링 빈도는 데이터 유형에 따라 다르다. 예를 들어, G.711 음성 코덱을 사용할 경우 샘플링 빈도는 8kHz로 설정
- Synchronization Source ID : 무작위로 선택된 숫자로 시작되는 SSRC 값은 각 RTP 세션에 대해 RTP 스트림의 소스를 식별

관련 Codec

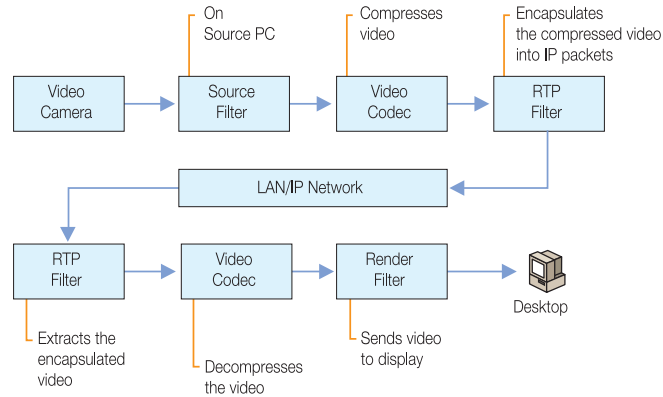
VoIP를 위한 코덱은 기술의 발전이 가장 빠른 분야라고 할 수 있다.

음성코덱은 G.711(PCM, 64kbps), G.729(CS-ACELP, 8Kbps) G.723.1(MLQ, 5.3kbps) 등이 있다. VoIP에서 가장 많이 사용하는 오디오 Codec은 G.729이며, Encoding, Decoding 지연시간을 최소화할 수 있어야 한다.



[오디오 코덱의 MOS(Mean of Square) 등급을 통한 오디오 품질]

영상회의를 위한 코덱은 H.261, H.262(MPEG-2), H.263, H.264(MPEG-4 AVC), VC-1(SMPTE 421) 등이 있다.



[비디오 압축과 풀기]

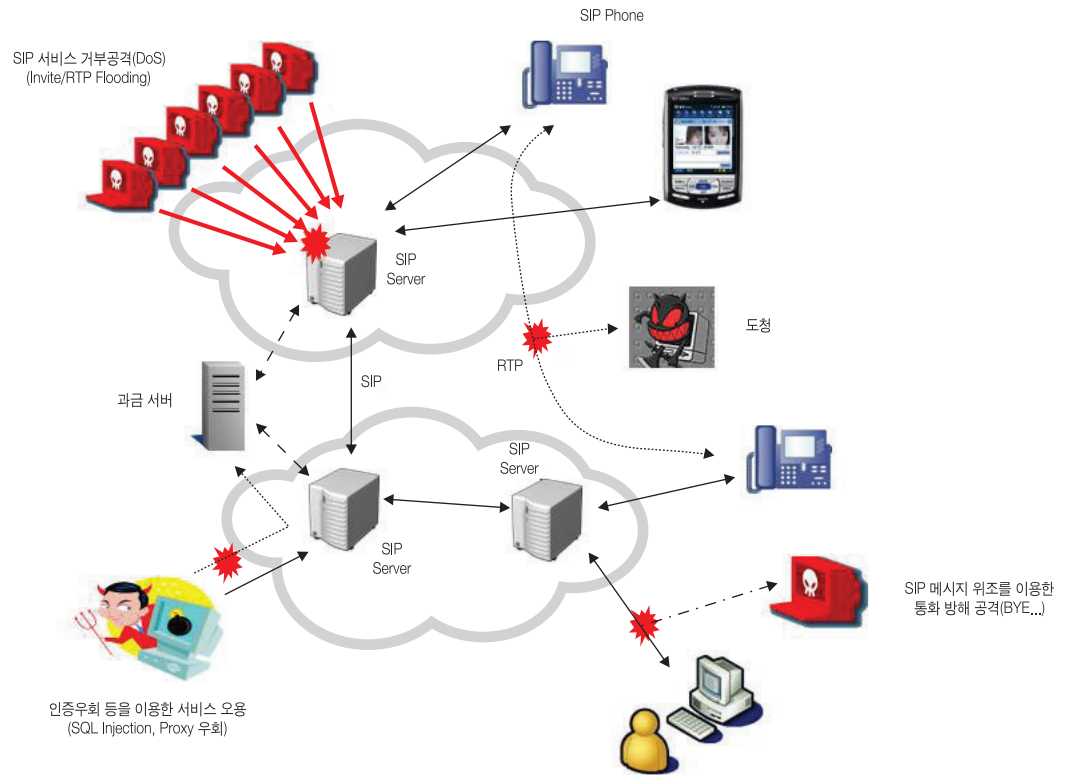
비디오 코덱은 CPU 사용량이 많기 때문에 H/W 또는 S/W 타입에 따라서, 엔코딩/디코딩 시간, 압축효율, 대역폭 등을 고려하여 최적의 코덱을 선정해야 한다.

영상전화 Codec은 H.263에서 최근에는 H.264, VC-1 고품질 코덱의 사용이 증가하는 추세이다. H.264는 화질이 우수하지만, VC-1에 비하여 동일화질에 대한 코딩 복잡도가 높아서 CPU의 사용량이 많다. 이에 비해, WMV9를 근간으로 하는 VC-1은 로열티 Free, PC 친화적인 특징이 있으나, Microsoft 의존적이다.

VoIP의 보안 취약성

VoIP는 일반적인 TCP/IP의 보안위험 요소와 도청의 위험요소 등을 안고 있다.

- 다양한 DoS(Denial of Service) 공격 등에 의해 서비스 회사 서버를 공격함으로써 유료 사용자들이 정상적인 통화서비스를 제공 받을 수 없으며, 이를 이용해 서비스 회사로부터 금전적인 이득을 취할 가능성이 있다.
- IP망 Sniffing 또는 Spoofing을 통한 도감청(Eavesdropping).
- 부정한 방법으로 서비스 사용 : VoIP 서버에 액세스할 수 있는 침입자는 저장된 음성 데이터 및 전화 서비스 자체에도 액세스할 수 있다. 사용자 계정의 전화통화 내용을 도청하거나 사용자 계정을 사용하여 전화를 무단으로 사용할 수 있다.
- 스팸 광고의 채널 : 비교적 비용이 낮으며, 자동화가 쉬워 스팸의 또 다른 채널로 사용될 가능성이 매우 크다.
- 바이러스 공격 : VoIP 서버 컴퓨터가 바이러스에 감염되면 전화 서비스를 제공할 수 없다. 또한, 해당 시스템에 연결된 다른 컴퓨터에도 영향을 줄 수 있다.



- 비표준 기술에 의한 일부 특정 취약점 및 사기에 노출.
- Registration Hijacking 등

VoIP 보안을 강화하기 위한 조치를 위해 방화벽, 정기적인 소프트웨어 업데이트, 안티바이러스 소프트웨어, 안티스파이웨어 소프트웨어 및 강력한 암호를 사용하여 컴퓨터를 지속적으로 보호해야 한다.

결론

IP를 이용한 음성 및 비디오, 인스턴트 메시징, Application 공유 등을 구현하는 실시간 통신 플랫폼은 표준에 기초하여 설계되어야 한다. 그렇지 않다면 향후 All IP망으로 발전하는데 있어서 지속적인 확장과 생존이 어려울 수 있다.

SIP 프로토콜의 표준화를 통하여 타 시스템과 호환성을 유지해야 하고, Roaming을 고려해야 한다면 게이트웨이를 통한 변환 등도 필요하다.

향후, Overlay Network에서 SIP를 이용한 융합 서비스 기술이 지속적으로 발전될 것으로 보인다. 이러한 서비스 기술은 저탄소 녹색성장에 크게 기여하게 될 것이다. 그리고 저탄소 녹색방송에도 사용될 것 기대한다.