Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review: Signalling Protocols in VoIP Technology

GARIMA SAINI [*]
IT Department
Dehradun Institute of Technology,
Dehradun India

NIDHI SETHI
IT Department
Dehradun Institute of Technology
Dehradun India

Abstract— The aim of this paper is to introduce the reader into VoIP by presenting the evolution of the technology. This paper gives a brief introduction of VoIP technology: the network structure, protocols, echo and delay, jitter, vocoder distortion and packet loss in VoIP network.

Keywords—VoIP, SIP, MGCP, RTP

I. INTRODUCTION

VoIP technology is rapidly emerging technology. This technology allows users to make free calls between computers and among devices that have access to the Internet and there is also the possibility of making international or long-distance calls at very low rates unlike normal phone lines. Video telephony is probably the first new service that will come forward that helps set VoIP apart from traditional telephone systems. Voice over IP (VoIP) applications treat voice, video, data, or facsimile as simple data, which may be packetized and transmitted in real time over IP networks. Voice band audio is digitized at the source, the data packets are transmitted over IP networks using VoIP protocols, and demodulated at the destination.

II. VOIP PROTOCOLS

There are a number of protocols that may be employed in order to provide for VoIP communication services. In this section, we will focus on those which are most common to the majority of the devices deployed and being deployed today.

1) H.323

The H.323 standard was developed for transmitting audio and video over the Internet. H.323 is superior in a number of ways: better interoperability with the PSTN, better support for video, excellent interoperability with legacy video systems, and reliable out-of-band transport of DTMF. H.323 is also widely used in room-based video conferencing.

2) SIP

Session Initiation Protocol (SIP) is designed to manage and establish multimedia sessions, such as video conferencing, voice calls, and data sharing. The SIP implementation is certainly easier to develop and troubleshoot.

SIP Agents- Session Initiation Protocol supports a variety of agents to perform different services for SIP enabled devices in a network.

User Agent- A SIP user agent (UA) is an endpoint device that supports SIP. SIP is used to establish connections and enable sessions between SIP UAs. A UA acts on behalf of a user, usually a person but can be another protocol. UA is comprised of both client (UAC) and server (AS) applications. At a minimum, a UA supports the Session Description Protocol (SDP) which defines the type and characteristics of a session to be established UAs. The UA notifies other UAs and servers of the capabilities it supports, including methods, SIP extensions, and message body types. This allows UAs to offer and then select mutually supported algorithms, codecs, ports, and other characteristics to be used when establishing a session.

Back-to-Back Agent- A back-to-back user agent (B2BUA) acts as an intermediary. It receives a SIP request and issues a new request that is a reformulated version of the original. Similarly, responses are handled in the same way. It may be used to isolate different UAs and hide information about one UA from the other. A B2BUA can also be used to provide other services but this can introduce additional latencies and potential packet loss. A common application of a B2BUA is an Application Layer Gateway that can be used for example in firewalls to enable SIP and other media packets to pass.

SIP Gateways- A SIP gateway acts as an interface between two domains – one being SIP and the other another protocol. It translates between the two protocols and similar to a presence agent isolates the interacting agents in the different domains. Unlike a UA, the gateway can support interactions of multiple agents between the separate domains. A gateway can terminate the signaling path and sometimes the media path. In the case of a SIP to PSTN interface, the SIP gateway terminates both the signals and media and converts the signals and media from the one protocol format to the other.

Servers- SIP servers accept SIP requests and respond to them. A server is an application that may act on the behalf of a SIP client or user agent (UA) or may provide information or direction to a UA. There are several types of SIP servers including proxy, redirect, and registration.

Proxy Server- A proxy server acts on behalf of a UA or even another proxy. The proxy's purpose is to facilitate a connection between UAs to establish a session for VoIP or other activity. A proxy does not originate SIP requests. It forwards requests and responses received from one UA or another proxy on to another proxy or UA. A proxy does not interpret a SIP message, only pass it on to the next link in the chain. It will access other servers, e.g. DNS or other MIB, to get routing information for the next proxy server or the endpoint UA. In so doing, the proxy will modify message header information to update source and destination as the message is propagated from the originating UA through one or more proxy servers and ultimately to the endpoint UA. A proxy may be either a stateless or stateful server. Stateless proxies process a SIP request and respond accordingly. No information is retained regarding the source, destination, or anything pertaining to the message contents. By definition, a stateless proxy cannot retransmit messages since it has no information of previous dialogs. Stateful proxies, on the other hand, monitor message transactions and use timers to initiate a message retransmit or other action indicate by the current state. Redirect Server- Unlike a proxy server, the redirect server responds to SIP requests but does not forward these requests to another server or UA. Like a proxy, the redirect server can use DNS or other MIB to get user information to provide to the requestor.

Registration Server- A registration or registrar server accepts requests from a UA to register an address of record with the server. The server records the address of record along with the device URI so that requests form another UA can be routed to the URI.

3) RTP

The Real-time Transport Protocol (RTP) was designed to provide real-time transmission of data such as audio or video over a network. RTP is augmented by a related control protocol, Real-time Control Protocol (RTCP), that can be used for quality of service monitoring, statistics collection, and minimal control of a related RTP stream. RTP is a UDP based protocol that provides services such as payload type identification, sequence numbering, and time stamping of packets. Since RTP is delivered over UDP, which is an unreliable transport mechanism, there is no guarantee that a packet will be delivered, that packets will be delivered in the order in which they were sent, or that packets will be delivered at a constant rate. The packet sequence numbers and time stamps allow for an application receiving RTP packets to reconstruct a sender's packet sequence and detect changes in network jitter and adjust accordingly.

4) SRTP

One of the areas of concern for people communicating over the Internet is the potential a person to eavesdrop on communication. To address these security concerns, RTP was improved upon with the result being called Secure RTP. Secure RTP provides for encryption, authentication, and integrity of the audio and video packets transmitted between communicating devices.

5) MGCP

A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. A decomposed multimedia gateway consists of a Call Agent, which contains the call control "intelligence", and a media gateway which contains the media functions, e.g., conversion from TDM voice to Voice over IP. MGCP (Media Gateway Control Protocol) defines a protocol which can be used to manage the elements of a decomposed media gateway. Media gateways contain endpoints on which the Call Agent can create, modify and delete connections in order to establish and control media sessions with other multimedia endpoints. Also, the Call Agent can instruct the endpoints to detect certain events and generate signals.

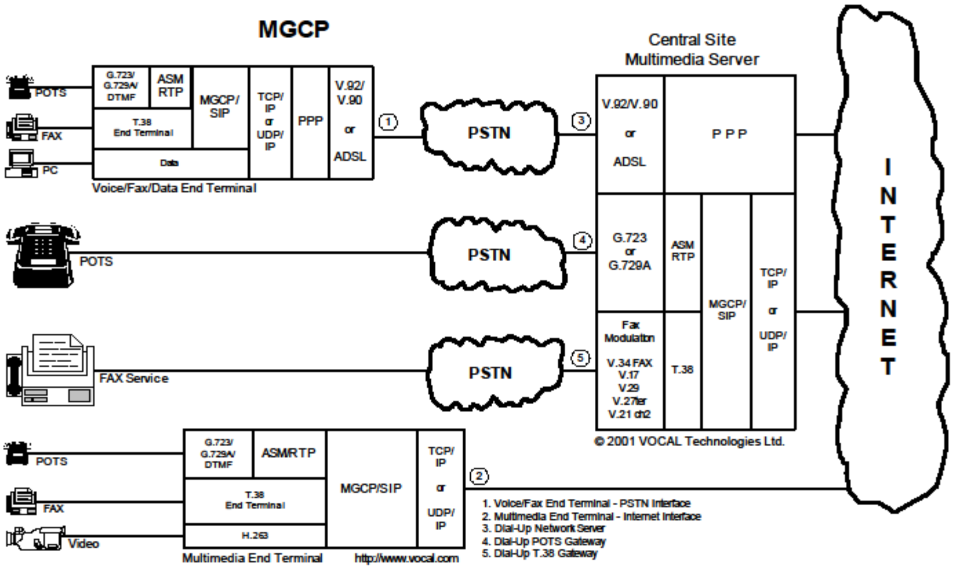

Fig. 1 MGCP Scenario

The endpoints automatically communicate changes in service state to the Call Agent. Furthermore, the Call Agent can audit endpoints as well as the connections on endpoints. MGCP assumes a call control architecture where the call control "intelligence" is outside the gateways and handled by external call control elements known as Call Agents. The MGCP assumes that these call control elements, or Call Agents, will synchronize with each other to send coherent commands and responses to the gateways under their control. If this assumption is violated, inconsistent behavior should be expected. MGCP does not define a mechanism for synchronizing Call Agents. MGCP is, in essence, a master/slave protocol, where the gateways are expected to execute commands sent by the Call Agents.

III. HOW VOIP WORKS

VoIP or Voice over Internet Protocol has been largely heralded as the telecommunications paradigm. VoIP transmits data from the traditional analog Public Switched Telephone Network (PSTN) across an IP network through the use of an Analog Telephone Adapter (ATA). The signal is broken up into frames and the information in each frame is stored in digital packets that are sent over the network. Each packet has header information that gives the receiving end information about how to reconstruct the signal. This header is essential as each packet traverses the network independently and each may encounter different transmission scenarios.

1) Echo and Delay in VoIP Networks

Echo in VoIP networks is introduced by impedance mis-matching in the PSTN being carried over into the digital network. Thus, VoIP echo paths resemble line echo paths in their sparseness, but differ due to their much longer echo tails and delay. This is due to the plurality of different processing steps that the speech needs to undergo. The continuous real time valued speech signal needs to be sampled, transmitted, and reconstructed, which adds extra delay and length to the echo path.

2) Jitter in VoIP Networks

Jitter effects are typically due to either clock slippage or network delay. Clock slippage occurs when a clock rate difference exists between the receiving and transmitting side that can cause either lost packets or duplicate samples due to buffer read errors. If the buffer is persistent and circular, and the receiver is sampling faster than the transmitter then values will be duplicated, and similarly a slower receiver will miss values. Network delay shifts the body of the impulse response along the echo path. Each packet may experience different levels of network traffic while in route, and thus may arrive out of sequence. Since the speech signal processing needs to reconstruct the signal at the other end, delay results.

3) Vocoder Distortion and Packet Loss in VoIP Networks

Conversion of a speech frame into a packet is typically done with a low bit rate vocoder for efficiency and ease of transmission. A vocoder essentially attempts to represent the speech frame by a smaller set of parameters that will excite a speech production model on the receiving end. Distortion is introduced by an inaccurate representation, pre- or post-filtering, and by parameter quantization, and thus non-linearity is introduced into the echo path which will degrade the performance of the linear echo canceller. The effect packet loss has on the performance on an echo canceller depends on how such a packet is recovered in each instance. One such method is packet concealment, in which the lost packet is somehow replaced on the receiving end. Typical replacement possibilities are silence, noise, the previous packet. Alternatively, you might want to attempt an extrapolation from the previous packet.

IV. CONCLUSIONS

This paper covered the fundamental issues concerning VoIP and its aim was to inspire readers look further in this very interesting technology. Judging from the architecture and the variety of possible applications of VoIP technology, it is easy to conclude that this technology will play a significant role in many aspects of everyday life

ACKNOWLEDGMENT

This work is completed under the guidance of Prof. Nidhi Sethi. I express my gratitude towards them for their continuous support on this research. I would also like to thank the reviewers for their suggestions to improve this paper.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, *"SIP: Session Initiation Protocol,"* RFC 3261 (proposed standard), June 2002.

[2] A. Keromytis, *Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research*. Springer, 2011.

[3] VoIPSA.org, "*VOIPSEC mailing list on VoIP security issues,"* http://voipsa.org/mailman/listinfo/voipsec voipsa.org, Jan. 2009.

[4] Errol A. Blake, 'Network *security: VoIP security on data network--a guide'*, InfoSecCD '07 Proceedings of the 4th annual conference *on Information security curriculum development,* ACM, September 2007.

[5] Ahuja, S. R. and Ensor R., (2004) *'VoIP: What is it good for?' Queue, Volume 2 Issue 6,* ACM