Voice over Internet Protocol (VoIP): A Brief Review

ANURAG K MADHESHIYA[1], KIRAN S KALE[2], SHIV K YADAV[3], JIGNESHKUMAR R. VALVI[4]
[1,2,3,4] Department of Electronics and Communication, SVNIT Surat, India

Abstract -- VoIP stands for Voice over Inter Protocol. It is a communication protocol mainly used for voice communication, data transfer and video calling. It is based on packet transmission over internet network. Paul Baran and other researchers developed the packet network in the mid twentieth century. In 1973 Dany Cohen first demonstrated packet voice in flight simulator application. Due to its digital nature it is easy to operate on this protocol.

Index Terms: MGCP, Packet, QoS, SIP

I. INTRODUCTION

Voice over Internet Protocol also known as Voice over IP and VoIP is a communication standard for transmission of voice signal, data transmission and video conferencing. Actually this technology follow packet switching. In packet switching first the input signal (voice, data, video) converted into digital form so other operation becomes simple after this we do encoding, compressing of digital data to make more secure transmission through channel. Then after this we transmit the signal over the channel. At receiver side we do reverse of it but it also require an addition block before receiver to store packets and reorder these packets because in packet switching different packets follow different path so reaches in random manner.

II. IMPLEMENTATION OF VoIP

Implementation of Voice over IP is a challenging issue. Because we should implement optimal protocol in each layer.

Protocols: There are three protocols widely used in the implementation of VoIP:

(1) H.323 Family of protocols

H.323 protocol is International Telecommunication Union (ITU) recommended protocol. It has a family of protocols that are used for different purpose like setting up calls, registering the calls, authenticating and terminating the call. Protocol belonging to H.323 family of protocol uses TCP and UDP connection for transportation. For call registering and call signaling H.225 protocol is used. For media session establishment and controlling H.245 is used. For conferencing T.120 protocol is used [3]-[4].

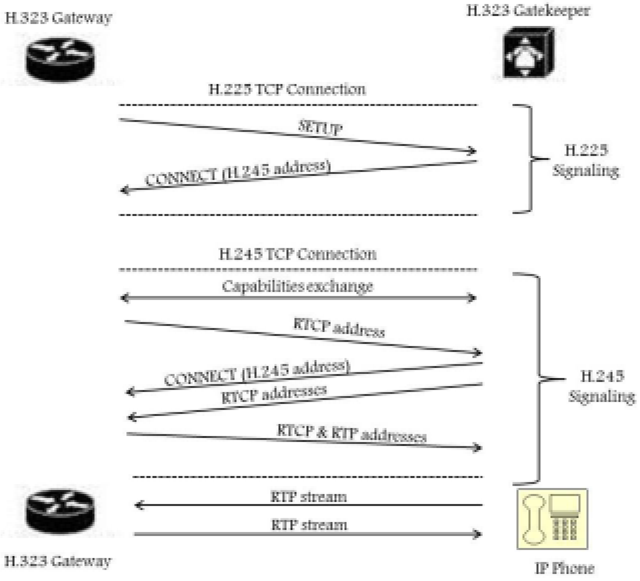

Figure 1: Call flow of H.323

(2) Session Initiation Protocol (SIP)

Session Initiation Protocol is developed by IEEE. This standard protocol is used for initiation of a user session. To modify it and to terminate interactive user session. SIP can be used to establish audio or video conferencing which IP network.

Session Initiation Protocol uses two protocols first RTP/RTCP for transporting voice data in real time. Second protocol is SDP, and it is used for coding data.

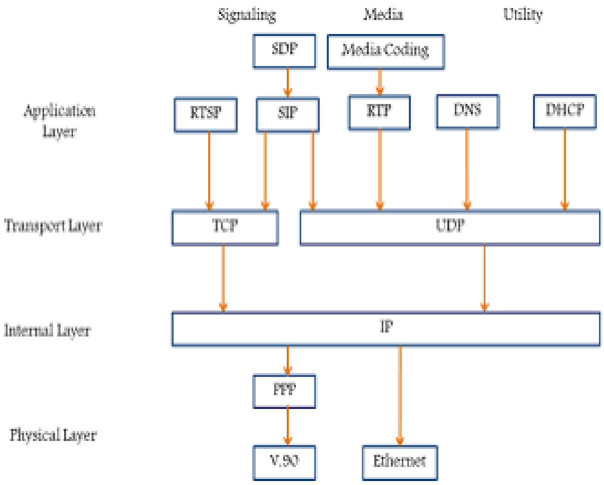

Figure 2: SIP Protocols

(3) Media Gateway Control Protocols (MGCP)

Media Gateway Control Protocol is used for interfacing between two VoIP gateways. It provides communication between different components. SIP is complementary protocol of MGCP. MGCP des not synchronize call agents. It assumes they are already synchronize. [1]

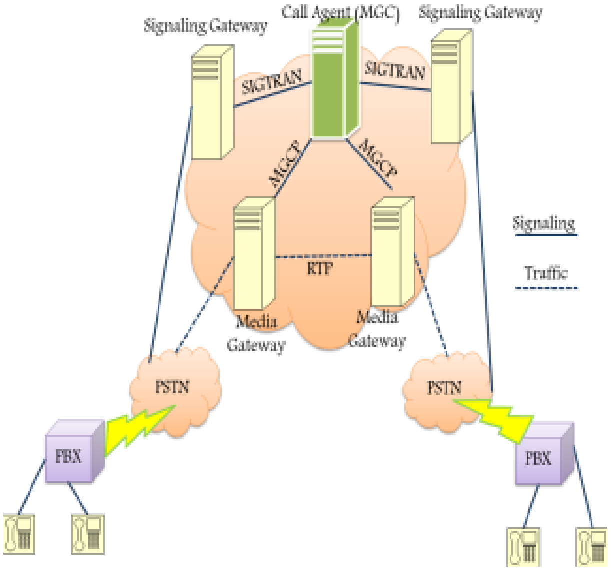

Figure 3: MGCP Architecture

Data Processing in VoIP System

VoIP works on mainly digital data. The working of VoIP system can described as, at transmitter our voice data is in the analog form we converts it into digital data using analog to digital converter after this we do encoding, compressing of digital data to make more secure transmission through channel. We use different voice codec like G.711, G.723 and G.729 or others for coding. Then after this we transmit the signal over the channel [2]. At receiver side we do reverse of it but it also require an addition block playout buffer for proper sequencing of packets. If this buffer become full than other packets are discarded. It give packet loss.

Quality of Service (QoS) in VoIP

Quality of Service is a relative term which depends mainly on cost, if you pay more you get better service. QoS can be defined for any network as ability of network to provide good services that satisfy its customers. QoS in VoIP can be depends on following factors

• Delay: Delay can be found as the total time taken from one end user to other end user. As delay increases, quality of service becomes poorer. Some system does not tolerate delay and some can tolerate comparatively more delay. We require minimum delay so less packet loss at receiver. According to ITU-Tone way latency should be less than 150ms.

• Jitter: The variation in packet's delivery time in IP network which is not constant is known as jitter. It may give rise to transmission delay. Jitter should be less than 100ms for good transmission.

• Packet Loss: Packet loss is one of the measure of quality of service. Higher the packet loss lower the quality of service. Packet loss occurs mainly due to traffic congestion. We can reduce this loss with optimum controlling of the traffic. We should give priority to voice packets

• Echo: In PSTN network echo is mainly electrical whereas in VoIP network it mainly acoustic echo. If echo is more in the communication network we cannot able to decode transmitted signal properly. Hence quality of service decreases. It occurs mainly at caller side.

•Throughput: Throughput is defined as total received bits over total transmitted bits for a given time interval. It depends on number of users using the network at same time. To increase voice throughput we have to give higher priority to voice packets.

III. VoIP SECURITY

VoIP Attacks: VoIP is a well-known and popular system. Attackers usually target well-known and popular systems and applications. So we have to take care of VoIP. There are some attacks on the VoIP.-

• Denial of Service (DoS): In this type of attack, attacker blocks the server. Now server cannot give its service. System may shutdown, or current application stops working, or system may corrupted. From this attack router functions like bandwidth, IP address reduces [3],[4]

• Network Sniffing: In this type of attack, attacker first observes the traffic pattern in network. This observation is done due to sharing of transmission medium. After observing traffic pattern attacker tries to hack data.

• Eavesdropping: In this type of attack, attacker gets the ability to monitor the signals that are exchanging between users. By this attacker gets sensitive information of the users.

• Spoofing: In this type of attack, attacker behaves like authorized person to extract the sensitive information from users through call

• Spam over Internet Telephony (SPIT): Spam over Internet Telephony is VoIP spam. For VoIP communication it is a serious issue. It is prerecorded and self-dialed call which uses VoIP. It is more severe as compared with email spam. [5]

IV. SECURITY MEASURES

Reported Problem on DoS

Due to DoS, server cannot give its service. System may shutdown, or current application stops working, or system may corrupted. Solutions to avoid a DoS attack:

• Monitoring and filtering – to maintain security if you found suspicious users, take strict action against them like cut his connection.

• Authentication – Take identification from users to authenticate there message in the network.

• Server design – Protection of CPU, memory, and network connection should be done first against any DoS attacks.

Reported Problem on Eavesdropping

An attacker listen forward calls and also has unauthorized access to network running on VoIP with the help of vendors. Solution to Eavesdropping:

- Employing flawless hardware.
- Only authorized and trustful people should be given to access network.
- Implementation of security based on MAC address in the network.
- Devices running in unauthorized mode should regularly scan the network.
- Encryption of VoIP traffic is another solution.

Reported Problem on Spoofing

This type of problem comes mainly in banking and online transfer of money. Attacker cheats with customers for finding credit card details. Solution to Spoofing:

• For sensitive data there should be extra security and authentication.

V. ISSUES OF VoIP

There are many issues with VoIP system. The major issues are given below:

• Quality of voice: Communication through VoIP is less reliable in compare to PSTN which uses circuit switching. Because circuit switching uses dedicated path for communication whereas VoIP uses packet switching which is non-dedicated path transfer. Quality of Service can be improved by giving priority to voice packets over other packets [5].

• Security: Security is one of the main issue which should be solved in any network. VoIP uses internet for transmission of voice and other data signal but it is not a secure medium. One can intercept the calls, stole your identity, Denial of Service (DoS) and so other security issues. By using tunneling protocols like Layer 2 security can be provided [5].

- Integration with Public Switched Telephone Network

Since PSTN came earlier than VoIP so everyone has PSTN. Now VoIP comes with more benefits but it cannot replace PSTN instantly because every user cannot afford it. It takes time for replacement of PSTN. We can solve this problem by using an adapter which connect VoIP to PSTN and vice versa [5],[6].

- Scalability: Any technology should be scalable so as VoIP. The main obstacle in its scalability is high growth rate in VoIP users. We have to maintain approximately same quality of service so scalability becomes complex. [3]

VI. CONCLUSION

From this paper we can conclude that Voice over Internet Protocol is mainly based on packet switching and IP technology. This paper gives brief idea of VoIP communication. The voice signal should be given preference over others for better quality of service. There are many problems like delay, packet loss, quality of service etc. which should be minimize for better outcome.

REFERENCES

[1] Karim, A. VoIP Performance Over different service Classes under Various Scheduling Techniques. Australian Journal of Basic and Applied Sciences, 2011. 5(11): p. 1416-1422.

[2] M.Perkins, K.Evans, D. Pascal, and L. Thorpe, “Characterizing the subjective performance of the ITU-T 8 kb/s speech coding algorithm

[3] ITU-T G.729,” IEEE Commun. Mag., vol. 35, pp. 74–81, Sept. 1997.

[4] Cerf, V.; Kahn, R. (May 1974). "A Protocol for Packet Network Intercommunication". IEEE Transactions on Communications. 22 (5):637648. doi:10.1109/TCOM.1974.1092259

[5] Dawood, H.A. IPv6 Security Vulnerabilities. International Journal of Information Secirity Science, 2012. 1(4): p. 100-105.

[6] “Speak Freely History". Brian C. Wiles. April 18, 1999. Retrieved 2013-03-19.