A Review Paper on Voice over Internet Protocol (VoIP)

Aastha Tiwari*
Research Scholar, M.tech. 2nd Computer Networks
[1]*Bhilai Institute of Technology, Durg, Chattisgarh, India*
tiwariaastha17@gmail.com
S. D. Mishra
[2]*Bhilai Institute of Technology, Durg, Chattisgarh, India*
sdmishra1982@gmail.com

Abstract

Voice over internet protocol (VoIP) is a communication protocol existing over a network. The IP network can acknowledge to the user to make telephone calls using the VoIP technology. This paper will define voice over internet protocol (VoIP). Some security problems may occur due to all over deployment of VoIP in Packet Switched wire and wireless network. VoIP is most important technologies in the world of communication by using SIP and H.323 signaling protocols. VoIP works over the wireless local area network (WLAN) faces many challenges due to the loose natured wireless network. In this paper we will describe issues like Quality of services (Qos) and security of VoIP Attacks.

Keywords: VoIP, SIP, H.323, QoS, security.

1. INTRODUCTION

Voice over internet protocol is most important technology and voice communication through internet. VoIP is a form of transmission that allow any person to make phone calls by using internet connection. VoIP technology also permits the user to make and receive calls to and from any landline numbers usually for a service charge. VoIP is powerful platform for the upcoming next generation application. It is almost used in all devices by using IP address VoIP mainly transmits the voice packets to the over the IP networks [1][2][3]. VoIP is signaling protocols which are used to set up and tear down calls. IP telephony is basically needs VoIP to send calls over the network. These new phone services are based on the transmission of voice over packet switched IP networks. VoIP technology introduces the actual protocol process of transmission of voice over an IP network and IP telephony. IP telephony needs VoIP to send calls over the network.

2. PROTOCOLS

There are a number of protocols that may be employees in order to provide the VoIP communication services. In this section of paper we will describe the three VoIP protocols, they are as follows :-

2.1 H.323 Familay Protocol

H.323 protocols is recommended by (ITU) International Telecommunication Union and consist of family of protocols, which are used for call setup, terminating call, registration process of calls, authentication and other function of VoIP. **Figure 1.** Shows H.323 families are transported over the TCP or UDP protocol connections H.323 family include some other protocols. H.225 is used for registration of calls, admission and call signaling. H.245 is used for the establishing connection and control the media session and T.120 is used in conferencing applications. The G.7xx series defines audio codes used by H.323 used RTP for media transport and RTCP for control of the RTP sessions Some components are used in H.323 protocol. Multimedia Terminal, DNS Server, Gateway, Gatekeeper, Multicast and multiport control unit [6][8][5].

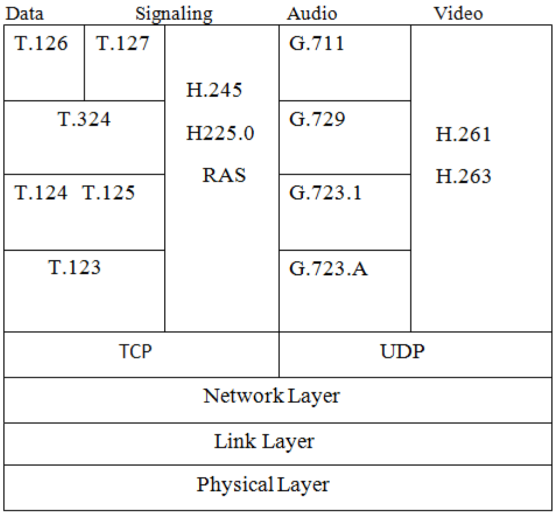

Figure 1. H.323 Protocol Family.

2.2 Session Initiation Protocol (SIP)

SIP Session initiation protocol is a protocol which is developed by IETE (Institute of Electronics and Telecom Engineering) and it is proposed for initiating a user session, modifying and terminating user session which involves video, voice, text messaging, online games and other multimedia elements. SIP can establish interactive session for audio/video conferencing and interactive gaming creating over IP network. These services providers divide the basic IP telephones services with internet and chatting services. Its protocol is based on RFC 2543, is a text based protocol; callers and callers are identified by the SIP address. When making a SIP call, a caller first needs to locate the appropriate server and send it a request. The caller can either directly reach the caller or indirectly through the redirect servers. The caller ID field in the SIP message Header uniquely identifies the call. SIP makes communication through using two protocols RTP and RTCP used to transport voice data in real time and SDP is used to negotiate participant capabilities, certification type etc as shown in figure 2.

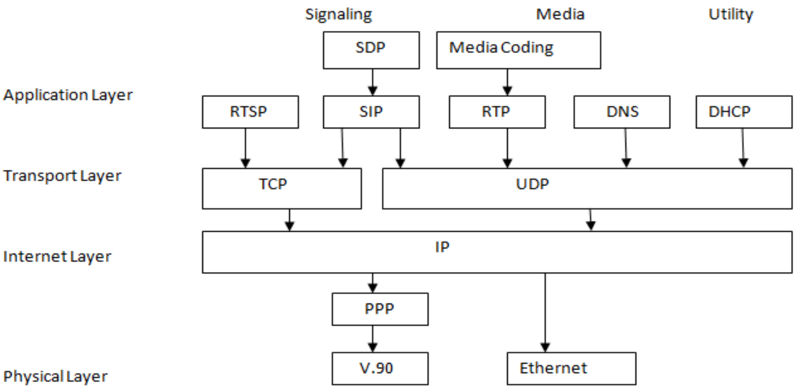

Figure 2. SIP Protocol.

SIP has become more popular than the H.323 family protocol. Some components are used in H.323 protocol.DNS Server, Proxy Server, Location Server, Redirection Server, Registration Server[5][6][8].

2.3 Media Gateway Control Protocol (MGCP)

MGCP (media gateway protocol) is used to communicate between the separate components of a decomposed VoIP gateway. It is complementary protocol of SIP and H.323. MGCP Architecture is shown in **figure 3.** It is a control protocol, which is allowing a central coordinator to monitor events in IP phones and gateway and instructs them to send media to corresponding address. The call control intelligences are located outside the gateways and are handled by external call control elements, the call agent MGCP assumes that these call control elements or call agents will synchronize with each other to send coherent command to the gateways under their control it is a master/slave protocol. MG (Media Gateway) is the Slave and MGCP act as the master/slave protocol [5][8].

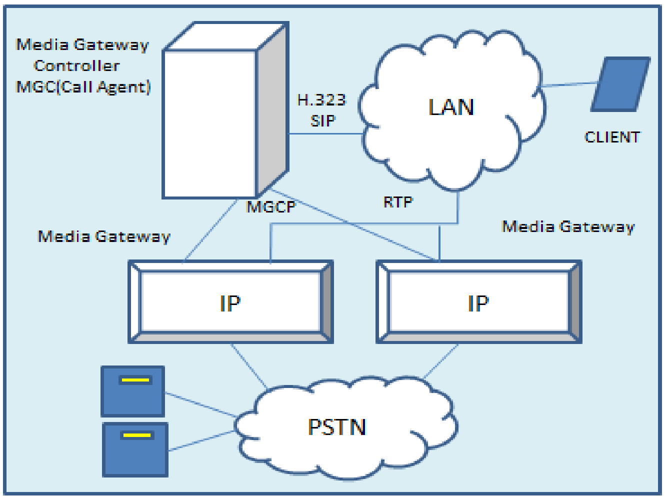

Figure 3. MGCP Architecture

3. PERFORMANCE CRITERIA

1 Delay is the total time taken to travel a voice message from source to destination [6]. Delay is mostly caused by network congestion which leads to a slow delivery of data packet [4][5].

2 Packet Loss Packet loss is one type of issue in VoIP technology many data protocol affects the use of packet loss problem [9]. Packet loss is that problem which occurs when any data are lost from the network congestion and late arrival of data to the destination end. In any case of packet loss the sender is informed to retransmit the lost packets and that may cause more delay occur in transmission which is affect the QoS and VoIP [6].

3 Jitter: IP packet does not confirm the delivery time of any packet which is defined by the variation in transmission delay [4]. This variation is called jitter and it has

produced more negative effect on voice quality of VoIP technology. The level of jitter variation acceptains is less than 100ms in a network[5].

4 Echo: Echo can be loud , Echo occur when caller at the sender side hears a reflection of his VoIP after he talks at the mouth piece of the phone cell (microphone) whereas the calls does not notice the echo[4]. Echo could be electrical echo which exists in PSTN network[9].

5 Throughput: This specification concerns about the maximum bits accept out of the total bits sent during an interval time [6]. VoIP throughput will depend on number of concurrent users [4][5].

4 ISSUES OF VoIP

1 Quality of Voice: The implementation of IP does not guarantee real time transmission of voice packet. IP was made for data packets which guarantee error free order by order delivery of the data packets [5].

2 Security :In comparing to PSTN network VoIP technology faces many security challenges and PSTN provide high level of security due to their loosely characters but sometimes some issues are similar for both like eavesdropping type of attacks and toll fraud. "*Man in the middle*" is a type of eavesdropping which listening and changing conversing is possible for attackers. Attacker is able to interrupt the conversions then play back previous conversion instead to change the conversion like "yes" to "no" or take advantage by asking username and password. In tall fraud the motivation is making free calls especially for high cost long distance calls actually fraudulent calls are billed to a victim and it is typically possible due to miss configuration [4].

3 Scalability: Since calls over IP have lower cost and work on improving the quality of voice as well as transmission is going on .there has been a high growth rate in VoIP users. The obstacle lies in its scalability VoIP technology should scalable enough for large user markets as well as private and public service [5].

4 Integration With In Public Switch Telephone Network (PSTN) :VoIP technology works as a PSTN network and they appear as a single network to the users of this service. In VoIP technology your phone number has an IP address so every time a VoIP phone engage is a call, its IP address is translated into talks at the mouth piece of the phone cell (microphone) whereas the calls does not notice the echo. Echo could be electrical echo exists in PSTN network [5].

5 Interoperability: We need to exchange the signaling mechanism of PSTN with VoIP signaling mechanism if you want to make VoIP common among internet users. Some of the useful signaling mechanism are H.323 protocol standard, SIP protocol are MGCP, These all protocols are used to transfer the data, voice, video over the same wire of network[5][4].

5. VoIP SECURITY

There are some security challenges occurred by VoIP, When any attackers attack VoIP between two users.

1. Denial Of Service (DoS): DOS (Denial of service attack) it is the most important risk, Which tries to make resources unavailable VoIP DoS attack aimed to bring a service down. VoIP runs voice over stream of IP packets, for example hackers can keep packet streaming running or they can make system busy with flooding of call requests. A DoS attack usually blocks the service of the server [7]. Solution of DoS service attack avoids are monitoring and filtering to maintain lists of suspicious users. Authentication process is done by both users before messaging [5].

2. Spoofing: Only one of the types of VoIP spoofing is caller ID spoofing. Where the attacker masquerades itself as an authorized VoIP user and place a call. The attackers can now trick the user in giving away sensitive data spoofing in the VoIP version of traditional phishing. There are several reports that banks and online payment services were victims of attacks the attacker called a credit card customer and deceived the customer into giving away any sensitive information based on their accounts by declaring that there had been fraudulent activity on their accounts[5][6].

3. Toll Fraud: Toll fraud is the activity to have unauthorized access to the VoIP service using for monetary gain. Toll fraud can be recognized by manipulating the signaling message or the configuration of VoIP components. The solution of Toll fraud is VoIP providers who can prevent toll fraud by configuring powerful firewalls that prevent attacks and by protecting the ports [5].

4. Spam Over Internet Telephony (SPIT): VoIP spam also called spam over internet telephony (SPIT) is turning out to be serious problem for VoIP network solution of SPIT attack in VoIP networks is a standard blacklisting approach, let through all the calls coming from a known IP address[7].

6. CONCLUSION

In this paper we have made a review on VoIP, which is based on over WLAN (Wireless LAN) and process of call flows and setup between the users by using VoIP protocols. As a major concern issues QoS, security, are explained in this paper. VoIP tolerates some time packet loss problem; it is very sensitive for delay factor jitter also plays an important role on voice quality improvement. Jitter buffer is defined for smooth transfer of the packet and we have also discussed the services of VoIP. This paper is also a brief study on protocols which are used to support the VoIP technology. The VoIP technology is based on two main terminology, which are PSTN (Public switch telephone network) and IP technology. It can be useful in utilize VoIP services in our daily life communication activities.

REFERENCES

[1] Angelos D. Keromytis Symantec Research Labs Europe Frame, ”A Survey of Voive Over IP Security Research”.

[2] BUR, GOODE, ”Voice Over Internet Protocol (VoIP)”, Proceedings of The IEEE, Volume 90, No.-9 (September 2002).

[3] Floriano De Rango, MouroTropea, Peppino Fazio, Sulvotore Marono, “Overview on VoIP: Subjective and Objective Measurement Methods”, International Journal, Volume 6, No. 1B, (January 2006).

[4] Haniyeh kazemitabar, Sameha, Ahmed, KashifNisaer, Abas B Said, Halabi B Hasbullah, “A Survey on Voice IP Over Wireless LANs”, World Academy of Science, Engineering and Technology 71 (2010).

[5] Urjashee Shaw, Boddy Sharma, ”A Survey Paper On Voice Over Internet Protocol(VoIP)”, International Journal of Computer Application(0975-8887) Volume 139-No.-2, (April 2016).

[6] Rahul Singh, Ritu Chauhan, ”A Review Paper: Voice Internet Protocol”, International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, (January 2014).

[7] Matthew Ruch, “VoIP Security”, (2010).

[8] Rakesh Arora, “Voice Over IP: Protocol and Standards”, (November 23, 1999), ”From http://www.cis.onio-state.edut ~jain/cis788-99/voip-protocols/index.html.

[9] Ajay kumar, “An Overview of Voice Over Internet Protocol (VoIP)”, RIVIER College online Acadmic Journal, Volume 2, (Number1, Spring 2006).

[10] B. Goode, ”Voice Over Internet Protocol(VoIP)” Browes Journels & Magazines proceedings of the IEEE, Volume 90 Issue 9, (10 December 2002).