A Survey Paper on Voice over Internet Protocol (VOIP)

Urjashee Shaw
Department of CSE & IT
School of Technology
Assam Don Bosco University
Guwahati, Assam, India

Bobby Sharma
Department of CSE & IT
School of Technology
Assam Don Bosco University
Guwahati, Assam, India

ABSTRACT
Voice over Internet protocol (VoIP), which is a communication protocol existing over a network. The IP network can makes it possible for users to make telephone calls using the VoIP technology. Use of VoIP and Internet telephony has increased significantly in the recent years. These new phone services are based on the transmission of voice over packet switched IP networks. VoIP can be realized on any data network that uses IP, like the Internet, Intranets and Local Area Networks (LAN). VoIP customers use their Internet connection to connect to the Internet as well as to make phone calls. VoIP is the real-time transfer of voice signals using the Internet Protocol (IP) over the Internet or a private network. In simpler terms, your voice is converted to digital signal by VoIP that travels over the internet. The key factors that entice enterprises to switch to VoIP are its flexibility and cost efficiency. Some security problems may arise due to the widespread deployment of VoIP. Voice over IP (VoIP) has the potential to provide interactive communication services like video and voice conferencing. VoIP helps to transfer data which are difficult to transfer over circuit-switched wired and wireless networks.

Keywords
Qos, Proxy, TCP, UDP, Spam, PSTN, DSL, Playout, LAN

1. INTRODUCTION
Voice over Internet Protocol (VoIP) is a form of transmission that allows any person to make phone calls over a broadband internet connection. VoIP access usually allows the user to call others who are also receiving calls over the internet. Interconnected VoIP connections also allow users to make and receive calls to and from conventional landline numbers, usually for a service charge. A type of adapter is used in some VoIP services which require a computer and a dedicated VoIP telephone. VoIP can also be described as a distinct solution which enables the transmission of voice signals over internet connection rather than the traditional telephone line[1].

In today's VoIP implementations, the voice analog signals are sampled and encoded using codec then encapsulated into an IP packet and carried over data cables or the internet infrastructure in the same way that data packets are carried [7].

Earlier, VoIP required a headset to be plugged into the computer, and the speaker and receiver could only speak with others who had a similar set up. They had to inform each other ahead of time, in order to signal the user at the other end of the incoming call and the time of call [8].

In November 1977, the Internet Engineering Task Force published the Specifications for the NVP (network voice protocol). In the abstract to this document, the purpose of the research was elucidated. The paper illustrated the development and the demonstration of the feasibility of secure and high-quality as well as low-bandwidth, real-time, full-duplex digital voice-to-voice communications over packet-switched data communications networks[1].

In the mid-90s, IP networks were growing, the technology had advanced and there has been an extensive use of Personal Computers. The belief that VoIP could make some significant impact on the market resulted in high expectations which resulted in the distribution of the first software package[1].

In its early stages, the VoIP technology was not fully developed and there were many loopholes. There was a big gap between the marketing structure and the technological reality.This can be concluded that technical shortages stopped any major development or changes in VoIP. However, lately VoIP has continued to make technological and viable progress. Signaling protocols are used to set up and tear down calls, carry data required to locate users and negotiate capabilities[8].

One key advantage of VoIP include making long distance calls at very cheap prices which include calls to other countries with the flexibility of using the same number in different parts of the world [2].

This paper will examine the implementation of VoIP, security risks and analyze the risks associated with VoIP, QoS while using a wireless connection.

This paper has been divided into 5 sections: (i) implementation of VoIP; (ii) security and risks involved and also analyze the risks; (iii) Configuration of VoIP; (iv) Wireless compatibility of VoIP and (v) Issues of VoIP.

2. IMPLEMENTATION OF VoIP

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

2.1.1 H.323 Family of protocols
H.323 protocol is recommended by (ITU) International Telecommunication Union and consists of family of protocols used for setting up calls, terminating calls, registering the calls, authenticating and other functions. These protocols that belong to the H.323 family are transported over TCP or UDP connections. H.323 family of protocol includes **H.225** used for registration of calls, admission, and call signaling. **H.245** is used to establish and control the media sessions and **T.120** is used for conferencing applications in which a mutual whiteboard application is used. The **G.7xx** series defines audio codec used by H.323, and the **H.26x** series defines the video codec. H.323 uses **RTP** for media transport and **RTCP** for control of the RTP sessions [1][7].

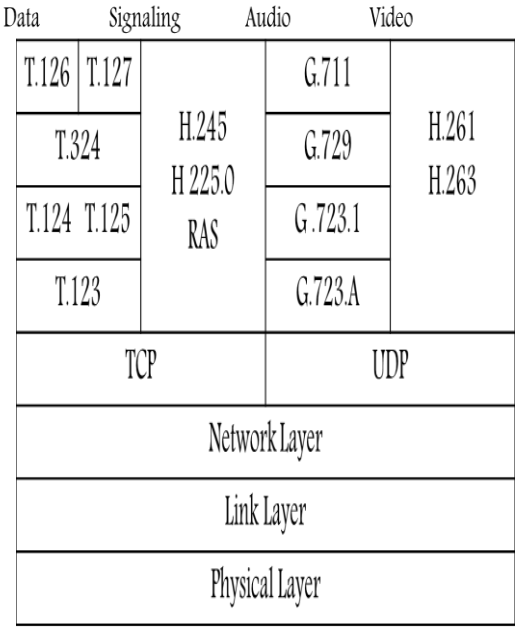

Figure 1: H.323 Family Protocol Stack [17]

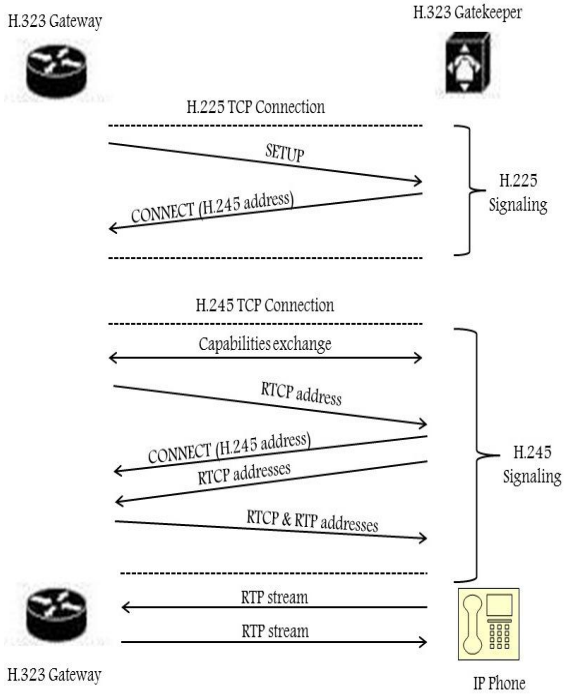

Figure 2: Call flow of H.323

2.1.2 Session Initiation Protocol (SIP)

SIP, Session Initiation Protocol is a protocol developed by IETE (Institute of Electronics and Telecommunication Engineering) and is the proposed standard for initiating a user session, modifying and terminating an interactive user session that involves video, voice, instant messaging, online games and other multimedia elements. SIP can establish interactive sessions for audio/video conferencing and interactive gaming deployed over IP networks. These enabling service providers integrate the basic IP telephone services with Web and chat services.

SIP makes communication possible through two protocols **RTP/RTCP** used to transport voice data in real time and **SDP** is used to negotiate participant capabilities, codification type, etc. SIP offers an alternative to the complex H.323 protocols. Due to its simpler nature, SIP has become more popular than the H.323 family of protocols [1][7][14].

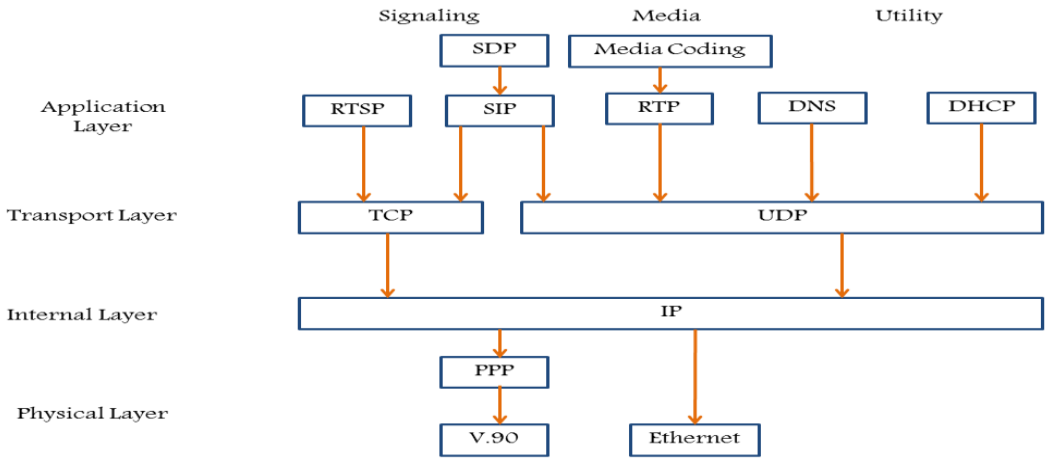

Figure 3: SIP Protocols

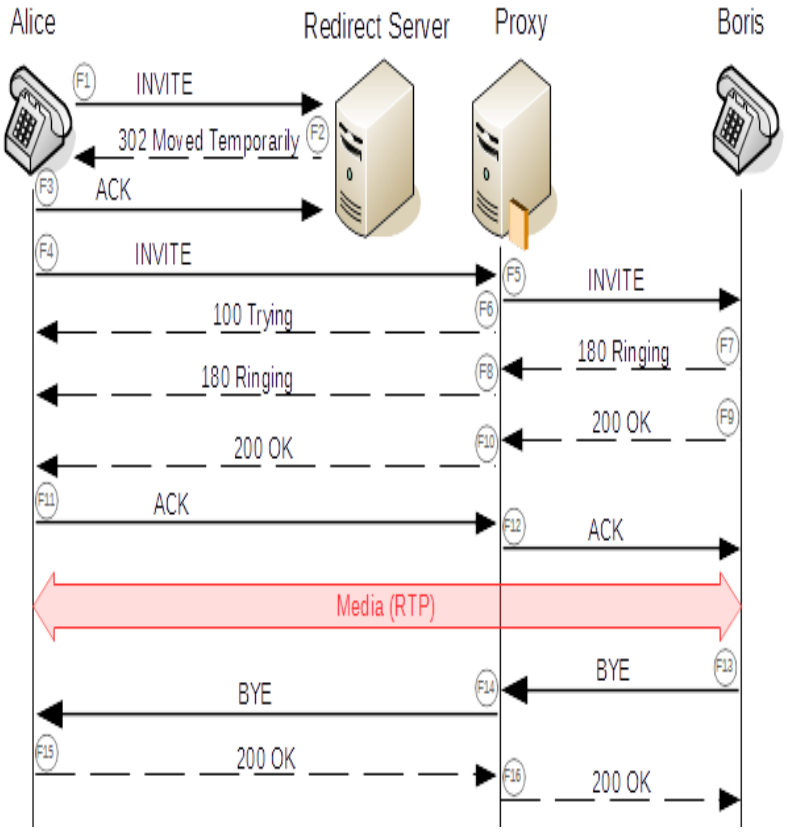

Figure 4: SIP call Flow

2.1.3 Media Gateway Control Protocols (MGCP)

MGCP, Media Gateway Control Protocol is used to communicate between the separate components of a decomposed VoIP gateway. It is a complementary protocol to SIP and H.323. Within MGCP the MGC server or more commonly known as "call agent" is mandatory as MGC manages calls and conferences, and supports the services provided. The MG (Media Gateway) endpoint is ignorant of the calls/conferences and does not maintain call states. MGs execute commands that are sent by the call agents. MGCP assumes that call agents synchronize with each other sending coherent commands to MGs under their control. MGCP does not have any mechanism for synchronizing call agents. MG is the slave and MGC acts as the master so MGCP is a master/slave protocol [1][7][11].

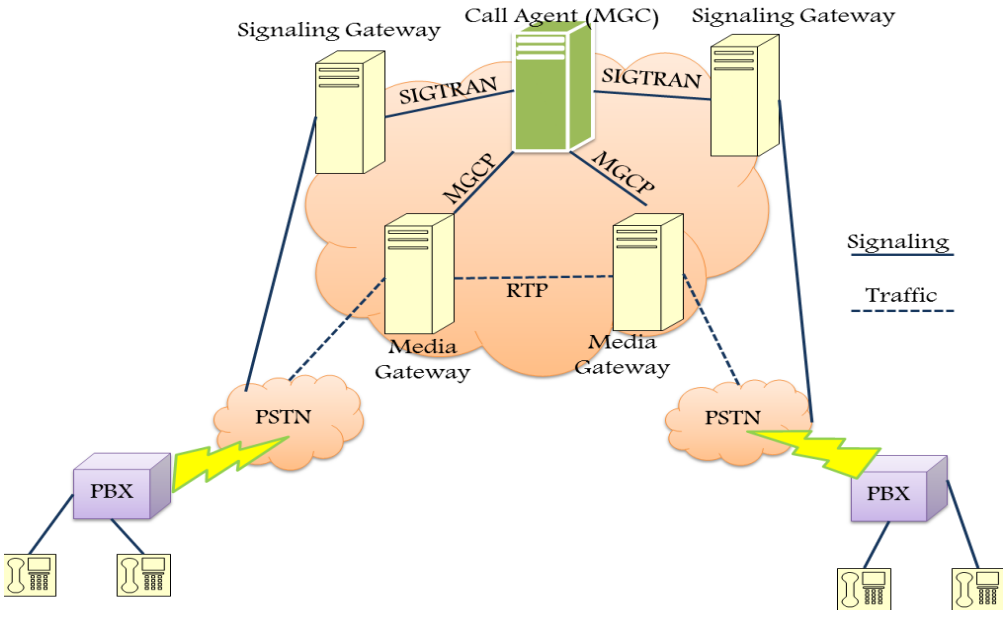

Figure 5: MGCP Architecture

2.2 Data Processing in VoIP System

At the sender side, analog voice signals are converted into digital signals, compressed and then set into a prearranged format using voice codec such as G.711, G.729, and G.723 etc. Next the encoded voice is broken down into equal size packets. Furthermore, in each packet, headers from different layers are attached to the encoded voice. The protocol headers added to voice packets are of RTP, UDP, and IP as well as Data Link Layer header [8].

The packets are then sent over the network (IP) to its destination where the decoding and de-packetizing of the received packets is carried out. During the transmission process, jitter (time variation of packet delivery) may occur. Hence, a playout buffer is used that smoothens the playout at the receiver end which may have a delay caused due to jitter. Packets are queued at the playout buffer for a stipulated time before being played. However, packets that arrive later than the playout time are discarded. VoIP uses the signaling protocols namely Session Initiation Protocol (SIP) and H.323. These signaling protocols are required to establish VoIP calls and to close the media streams between the clients [1].

2.3 Quality of Service (QoS) in VoIP

(QoS) is defined as the network's ability to provide good services that satisfy its customers. QoS in VoIP are briefly described in following sections [1][17][11].

2.3.1 Delay

Delay can be defined as the total time it takes between a speaker speaking a word from one end and the receiver hearing it in the other line of communication. Delay can be categorized into: source delay, receiver delay, and network delay. ITU-T suggests that one-way latency should not be more than 150 ms.

2.3.2 Jitter

IP network does not give guarantee of packet's delivery time, which may give rise to transmission delay. This variation is known as jitter and it has negative effects on voice quality. Jitter may lead to the loss of voice packets. In VoIP jitter measurement calculations are defined in **IETF RFC 3550 RTP** and **IETF RFC 3611 RTP.** The acceptable level of jitter variation is less than 100ms in a network

2.3.3 Packet Loss

Packets transmitted over IP network may be lost in the network or may arrive corrupted or late. Packets are discarded, if they arrive late at the jitter buffer of the receiver Packets may also be discarded in case the jitter buffer or router buffer is full. Therefore packet loss is the loss which occurs due to network congestion in the network and/or late arrival. G.729 codec a common codec used by VoIP requires a packet loss of less than 1 percent to avoid any audible error

2.3.4 Echo

In VoIP, Echo occurs when caller at the sender side hears a reflection of his voice after he talks at the mouth-piece of the phone (may be a microphone) whereas the callee does not notice the echo. Echo could be electrical echo which exists in PSTN networks or acoustic echo which is an issue in VoIP networks.

2.3.5 Throughput

This parameter concerns about the maximum bits received out of the total bits sent during an interval of time. Throughput in VoIP will depend on number of concurrent users and the codec used. Usually voice packets are given higher priority so the throughput of voice packets over data packets in a channel is higher.

3. VOIP SECURITY

3.1 VoIP Attacks/Threats

Attackers usually target some popular and well-known systems and applications. VoIP has become one of such application. VoIP like any another system or applications have its weakness, thus protocol designers need to address it before successfully installing VoIP on a universal scale. Therefore this section, presents a study of attacks on the VoIP.

3.1.1 DoS (Denial of Service)

DoS (Denial of Service) attacks which reduces the number of available IP addresses, bandwidth and other router functions. A DoS attack usually blocks the service of the server. A VoIP based DoS attack bombards a call processing application with large amounts of concurrent requests that it cannot process, causing the shutting down of the application, thereby denying service to authorized or intended users. DoS attacks can be directed toward any network element to disrupt the system's functionality. [1][6][12]

3.1.2 Network Sniffing

Network Sniffing attacks occur when an individual or attacker is observing the network traffic patterns. Typically, any system (user/attacker) on a network that is sharing a transmission medium has the ability to view other system's traffic.[1][7]

3.1.3 Eavesdropping

Eavesdropping is an endeavor towards collecting sensitive information to prepare for a cyber-attack or to gain intelligence. In VoIP, eavesdropping is a scenario where the attacker is able to monitor signal or media contents that are exchanged between users in order to examine communications to prepare for other future attacks.[7]

3.1.4 Spoofing

One of the types of VoIP spoofing is caller ID spoofing where the attacker masquerades itself as an authorized VoIP user and places a call. The caller ID that appears on the user side appears authentic even though the attacker is using unfair means. The attacker can now trick the user in giving away sensitive data. Spoofing is therefore the VoIP version of traditional Phishing. [1][12]

3.1.5 Toll Fraud

Toll fraud is the ability to have an unauthorized access to the VoIP services usually for monetary gain. For VoIP providers, this is one of the most critical attacks. Toll fraud can be recognized by manipulating the signaling messages or the configuration of VoIP components, including the billing systems. [6]

3.1.6 SPam over Internet Telephony (SPIT)

Due to its much lower communication costs, VoIP network has become more attractive as an alternative to the current PSTN as well as a target for spammers. VoIP spam is a prerecorded, self-dialedphone calls using Voice over Internet Protocol. VoIP spam also known as Spam over Internet Telephony (SPIT) is turning out to be a serious problem for VoIP networks. SPIT is more severe than your e-mail spam due of its attacking nature which requires a real-time defense mechanism. [1][12]

3.2 Security Measures

3.2.1 Reported Problem on DoS

There has been a report that certain VoIP phones are susceptible to both DoS attacks and certain VoIP routers are also vulnerable to malicious traffic. Solutions to avoid a DoS attack: [12]

- Monitoring and filtering – to maintain lists of suspicious users and deny those users from obtaining any connection/session.
- Authentication – to authenticate the identity of a user before forwarding his/her messages through the network.
- Stateless proxy – to lower the dangers of memory exhaustion (DoS) stateless proxy can be used to perform other security checks such as user authentication, third party registration, and filtering spam sources.
- Server design – to make CPU, memory, and network connection the first line of defense against any DoS attacks. [1][12]

3.2.2 Reported Problem on Eavesdropping

An Internet Security System's team discovered the flaws in VoIP system in a vendor's call manager. The vendors give an attacker the facility to listen in or forward calls, in addition to gaining unauthorized access to networks running on VoIP. [12]Solution to Eavesdropping:

- Employing flawless hardware.
- Only authorized people should be given access to wiring closets.
- Vulnerable network point should implement a port based MAC address security; for example, on a reception courtesy phone.
- A process should regularly scan the network for devices running in unauthorized mode.
- Another solution is encryption of VoIP traffic [1][12]

3.2.3 Reported Problem on Spoofing

There have been several reports that banks and on-line payment services were victims of attacks where the attacker called a credit-card customer and deceived the customers into giving away sensitive information regarding their accounts by declaring that there had been fraudulent activity on their accounts. [12]Solution to Spoofing:

- An effective authentication module combined with encryption would be an effective solution to spoofing and masquerading attacks. [1][12]

3.2.4 Reported Problem on Toll Fraud

Toll Fraud threat is often most important in the eyes of large organization. A successful theft of service from a large organization can go unnoticed for quite some time, allowing the attacker to rack up a large bill at the organizations expense. However toll fraud is also quite easy to accomplish. A simple configuration problem in the dial plan can leave lines open for test purpose and remote access can be abused by an attacker.

It is however profitable from the point of view of the attacker to commit toll fraud because once the attack is over the attacker can abuse the service quite rapidly by reselling them with no real costs involved from the attacker's side.[12]Solution to Toll Fraud:

VoIP providers can prevent toll fraud by configuring powerful firewalls that prevent attacks and by protecting the ports. VoIP providers must also actively monitor their networks, so that they know who has access to the network and at what frequency, and who is generating what kind of traffic. [1][12]

3.2.5 Reported Problem on SPIT

It is possible in a network for an attacker to impersonate as another VoIP caller. For example, an attacker could possibly inject a fake ID into an ordinary VoIP call so that the receiver mistakes the call to be genuine and coming from a known and trusted source. The receiver mistaken by the electronic ID of the caller, may place unwarranted trust in the person at the other end. In such a communication, the receiver may be hoaxed into disclosing personal information like account numbers, SSN, or answers to security questions: a mother's maiden name, for example. [12]Solution to SPIT:

- A standard blacklisting approach, let through all the calls coming from a known IP address.
- VoIP vendors also provide security measurements to block suspicious callers.
- Above all receiver should be alert not to divulge any important information to the attacker. [1][12]

4. CONFIGURATION OF VOIP

4.1 Adapters (USB)

VoIP phone adapters allow us to use any traditional telephone to place VoIP calls. They usually look like USB adapters. These USB adapters have a typical modular telephone phone port to which one can connect a regular phone line. Once attached, your phone operates as if connected to normal phone service. [1]

4.2 Software controlled VoIP applications: softphones

Softphones are phones that allow us to make VoIP phone calls directly from a computer that has an internet connection. Softphones make call with the help of a PC headset and a sound card. A softphone is just like a normal phone just with the difference that the connection is coming from your PC. VoIP providers give away softphones for free in exchange of availing their service. Software controlled VoIP application allows users to talk to other people using these services at no extra cost. [1]

4.3 Dedicated VoIP phones

A VoIP phone seems like a regular telephone (can be cordless as well). A dedicated VoIP phone connects directly to a computer network rather than a conventional telephone line. A dedicated VoIP phone may work in two ways 1) a phone and base station that connects to the internet 2) it may function on a local wireless network. Dedicated VoIP phones require a provider as well as a service plan. [1]

4.4 Dedicated routers

These routers in VoIP allow user to connect conventional phones to the internet to place VoIP calls where the router is connected to an ADSL/Cable modem and allow users to attach a traditional telephone. VoIP routers have the additional functionality of an IP router as which allows us to connect to the PC as well. VoIP providers configure these routers under a specific plan for a service fee. These routers can also perform their functions independent of any computer or any software. [1]

5. WIRELESS COMPATIBALITY OF VOIP

With a wireless router, mobile devices and smart-phones can also use the VoIP system. If you install a wireless LAN, you need appropriate security such as a firewall or encryption. [10]

Problems with wireless VoIP:

- VoIP on LAN is deployed mostly in corporate environments, i.e., in companies rather than houses. Wireless VoIP poses problems of scalability for enterprises. [15]
- As in case with all wireless network. Quality of Service (QoS) is poor in comparison to wired networks. [15]
- Set up cost and maintain cost is higher in a wireless VoIP network. [15]
- Due to a number of access points within the limited area of network security threat is higher over a wireless VoIP network. [15]

6. ISSUES OF VOIP

The popularity of VoIP will depend on some key issues. Some of these issues are a resultant of the fact that IP was designed for data packets while some issues stem from vendors that are not meeting the requirements to the standards. The key issues are discussed as follows:

Quality of voice

The design of IP does not guarantee real time transmission of voice packets as IP was designed for data packets which guarantee error free sequential delivery of data packets. Acceptability of VoIP is dependent on delay which must not exceed a given threshold value. Prioritization of Packets means giving voice packets high priority can guarantee good quality of voice. [17]

Interoperability

You need to replace the signaling mechanism of PSTN with VoIP signaling mechanism if you want to make VoIP common among internet users. Some of the acceptable signaling mechanisms are H.323 standards, SIP protocols and MGCP. Each of these protocols integrates data, voice and video over the same wire. [17]

Security

The question of security arises because the backbone of VoIP is the internet which is not a very secure medium. There can be interception of calls, DoS, identity theft. Security can be provided by using tunneling protocols like Layer 2 Tunneling the encryption mechanism used is Secure Sockets Layer (SSL), but encryption is not widely available for VoIP. [17]

Integration with Public Switched Telephone Network(PSTN)

VoIP works in union with PSTN 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 engages in a call, its IP address is translated into the phone number and handed over to PSTN network. You need the combination of both VoIP a PSTN because not everyone has switched to VoIP and there are an enormous number of users still using PSTN. [17]

Scalability

Since calls over IP have lower cost and the 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 main obstacle lies in its scalability. VoIP technology should scalable enough for large user markets as well as private and public services. [17]

7. CONCLUSION

The foundation block of VoIP is set on two technology - the telephone (PSTN network) and Internet (IP technology). Tremendous works and research on these two fields has made the existence of VoIP possible.

This paper has been a brief study on the protocols used to support VoIP technology, the threats that may occur in a VoIP communication and the security measures taken to avoid these threats. Security for a VoIP system should implement concrete security on the internal network. It should be protected from the threats of hostile networks and any threats to the internal network. The load of the VoIP system should be accommodated by the network and the servers involved. Packet loss, delay jitter and throughput all contribute to degraded voice quality. Additionally, because network congestion can occur at any time in any portion of the network.

8. REFERENCES

[1] Sanjay Kumar Sonkar, Rahul Singh, Ritu Chauhan, Ajay Pal Singh "A Review Paper: Security on Voice over Internet Protocol from Spoofing attacks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2012.

[2] Ahmad Ghafarian, Randolph Draughorne, Steven Grainger, Shelly Hargraves, Stacy High, and Crystal Jackson "Securing Voice over Internet Protocol", ISSN 1896-7094.

[3] Aladdin Sleem Olugbenga Olumuyiwa Khaled Kamel "Real time performance evaluation of voice over IP call quality under varying network conditions", International Journal of Applied Science and Technology Vol. 1 No. 6; November 2011.

[4] Barrie Dempster "VoIP Security Methodology and Results", An NGSSoftware Insight Security Research (NISR) Publication.

[5] Rahul Singh, Ritu Chauhan "A Review Paper: Voice over Internet Protocol", International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471 Vol. 3 Issue 1, January-2014.

[6] Ajay Kumar "An overview of voice over internet protocol (voip)", Rivier college online academic journal, volume 2, number 1, spring 2006.

[7] Phithakkitnukoon, Santi; Dantu, Ram and Baatarjava, Enkh-Amgalan (2008). "VoIP security – attacks and solutions", Information Security Journal: A Global Perspective.

[8] Henning Sanneck, Nguyen Tuong Long Le, Martin Haardt and Werner Mohr "Selective Packet Prioritization forWireless Voice over IP", Siemens AG, Information and Communication MobileNetworks.

[9] Prateek Gupta, Vitaly Shmatikov "Security Analysis of Voice-over-IP Protocols", The University of Texas at Austin

[10] Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said, Halabi B Hasbullah "A Survey on Voice

over IP over Wireless LANs", World Academy of Science, Engineering and Technology 71 2010.

[11] The status of Voice over Internet Protocol (VoIP) worldwide, 2006, INTERNATIONAL TELECOMMUNICATION UNION.

[12] Arlindo F. da Conceicao, Jin Liy, Dinei A. Florencioand Fabio Kon "Is IEEE 802.11 ready for VoIP?", Department of Computer Science, Institute of Mathematics and Statistics, University of Sao Paulo Communication and Collaboration Systems, Microsoft Research.

[13] ChintanVaishnav "Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation" Master of Science, Electrical EngineeringColorado State University, USA.

[14] Henning Schulzrinne "A comparison of sip and h.323 for internet telephony", Department of computer science, Columbia University New York.

[15] Kaur-Kehal, R., & Sengupta, J. (2011). "A comprehensive review on improving QoS for VoIP in wirelessmesh networks". Journal of Gobal Research in Computer Science, 2, 32-33.

[16] S.Feroz and P.S.Dowland, "Security and Risk Analysis of VoIP Networks", Network Research Group, University of Plymouth, United Kingdom.

[17] Voice over IP : Protocols and Standards. Retrieved October 17, 2005, from http://www.voip-voice-over-ip.com/internetphone/protocols.htm.