Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2018, 5(7):96-106**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

A Review of Voice over Internet Protocol

Ayodeji Ireti Fasiku

Computer Engineering Department, Ekiti State University, Ado – Ekiti, Nigeria

Abstract The prevalence of network infrastructure in enterprise and the fact that Internet Protocol (IP) is the protocol that connects, locates and identifies devices on a network has made Voice over internet protocol a powerful service platform for transferring voice calls on a network. As a result, voice over internet protocol has been a predominant technology within the past few years that organizations use to transmit voice over an IP network. However, like any other technology, it has a number of benefits and promising attributes that gives it edge over the traditional Public Switched Telephone Network (PSTN) though a number of risks are also associated with it. This paper describes the Voice over Internet Protocol technology.

Keywords Voice over internet protocol, Public Switched Telephone Network and Internet protocol

Introduction

In less than two decades, Voice over Internet Protocol (VoIP) has revolutionized the telecommunications industry and it has helped to knock down barriers in international communication, providing a genuine alternative to telephone calls made using traditional telecoms infrastructure and providing near-universal access to cheap calls for anyone with a computer and an internet connection. The advent of the Internet brought with it an abundance of innovation regarding communication. Of course, there was email in the beginning, but then people started wondering whether they could communicate in real-time. This brought about instant messaging, which put America Online (AOL) in the spotlight as the most popular provider but others wanted a more personal connection, they wanted to hear another person's voice over the Internet in real time, which brings us to VoIP.

Voice over IP (VoIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network so VoIP can be achieved on any data network that uses IP, like Internet, Intranet and Local Area Networks (LAN). It enables advanced communication services over data networks. The steps and principles involved in originating VoIP calls are similar to traditional digital telephony and involve signaling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network. However, the digital information is packetized, and transmission occurs as IP packets over a packet-switched network. VoIP systems employ session control and signaling protocols to control the signaling, set-up, and tear-down of calls. It allows phone calls to be route over a data network thus saving money and offering increased features and productivity. VoIP specifically refers to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the Public Switched Telephone Network (PSTN) [5].

History of VoIP

Voice over Internet Protocol (VoIP) transmission began in 1973 as a result of the experimental Network Voice Protocol invented for the Advanced Research Projects Agency Network (ARPANET). However, it wasn't until 1995 that the first Internet Phone Software (Vocaltec) appeared. Vocaltec brought to market the first internet phone software called the Internet Phone. The Vocaltec software compressed the voice signal, translated it into digital packets, and distributed it over the Internet. The technology solution worked well as long as both the

caller and the receiver had the same hardware and software. Although sound quality was poor and cannot be compared to that of Public Switched Telephone Network (PSTN), the effort led to the first IP phone. Early adopters were largely made up of hobbyists who quickly recognized the potential of transmitting voice data packets over the Web instead of communicating through the traditional telephone companies. Vocaltec was designed to run on a home computer, integrated with sound cards, microphones and speakers. Vocaltec achieved initial success with Internet Phone and launched a successful Initial public Offering (IPO) in 1996. This company delivered the first true VoIP software application and helped lay the groundwork to grow the VoIP industry [6].

In the 1990's, VoIP services mainly relied upon advertising sponsorship to subsidize costs and attract customers. The gradual introduction of broadband Ethernet technologies delivered greater call clarity and reduced latency. This permitted large technology companies such as Cisco Systems and Nortel to start making VoIP equipment that was capable of switching, therefore functions that had previously been handled by a computer's CPU, such as switching a voice data packet into something that could be read by the PSTN (and vice versa) could now be offloaded to another more powerful device. Since 2000, VoIP usage has expanded dramatically. There are several different technical standards for VoIP data packet transfer and switching and each is supported by at least one major manufacturer. Mass market VoIP telephony began in 2004 with the introduction of VoIP calling plans which permitted subscribers to make calls just as they would with conventional telephone company services. VoIP has gone from being a fringe development to a mainstream alternative to standard telephone service [8].

VoIP Architecture

One of the main features of the VoIP technology is that it may be deployed using a centralized or a distributed architecture. The majority of current VoIP systems are deployed using a client-server centralized architecture. A client-server VoIP system relies on the use of a set of interconnected central servers known as gatekeepers, proxy servers, or soft-switches.

A gatekeeper or call manager node is optional for a VoIP network. In an H.323 IP telephony environment, a gatekeeper works as a routing manager and central manager that manage all the end nodes in a zone. A gatekeeper is useful for handling VoIP call connections includes managing terminals, gateways and MCU's (multipoint control units). A VoIP gatekeeper also provides address translation, bandwidth control, access control. Therefore, A VoIP gatekeeper can improve security and Quality of Service (QoS). A VoIP gateway is also required to handle external calls. A VoIP gateway functions as a converter that converts VoIP calls to/from the traditional PSTN lines, it also provides connection between a traditional PBX (Private Branch Exchange) / Phone system and an IP network [7].

The central servers are responsible for users' registration as well as the establishment of VoIP sessions between registered users. Figure 1 shows an example of a VoIP system deployed using the client-server architecture. As it is illustrated in the figure, each central server handles (registers, establishes a session with a local or a distant user, etc.) a set of users. Each user must be registered on one of the central servers (registrar server) to be able to exchange data with other registered users. A user gets access to the service only over the registrar server [11].

The main issues of the client-server VoIP systems are the presence of single points of failure (central servers), scalability, availability, and security.

In order to overcome the shortcomings of the client-server model, and help the development of scalable and reliable VoIP systems, the development communities start tending towards the deployment of the VoIP service using a peer to-peer decentralized architecture. Actually, a peer-to-peer VoIP system allows service provision through the establishment of a symmetric collaboration between the system nodes (peers) communicating according to a given logic architecture (overlay). This helps the deployment of scalable, cost-effective, and more reliable systems VoIP systems. Other required VoIP hardware includes a VoIP client terminal, a VoIP device could be an IP Phone, or a multimedia PC or a VoIP-enabled workstation runs VoIP software.

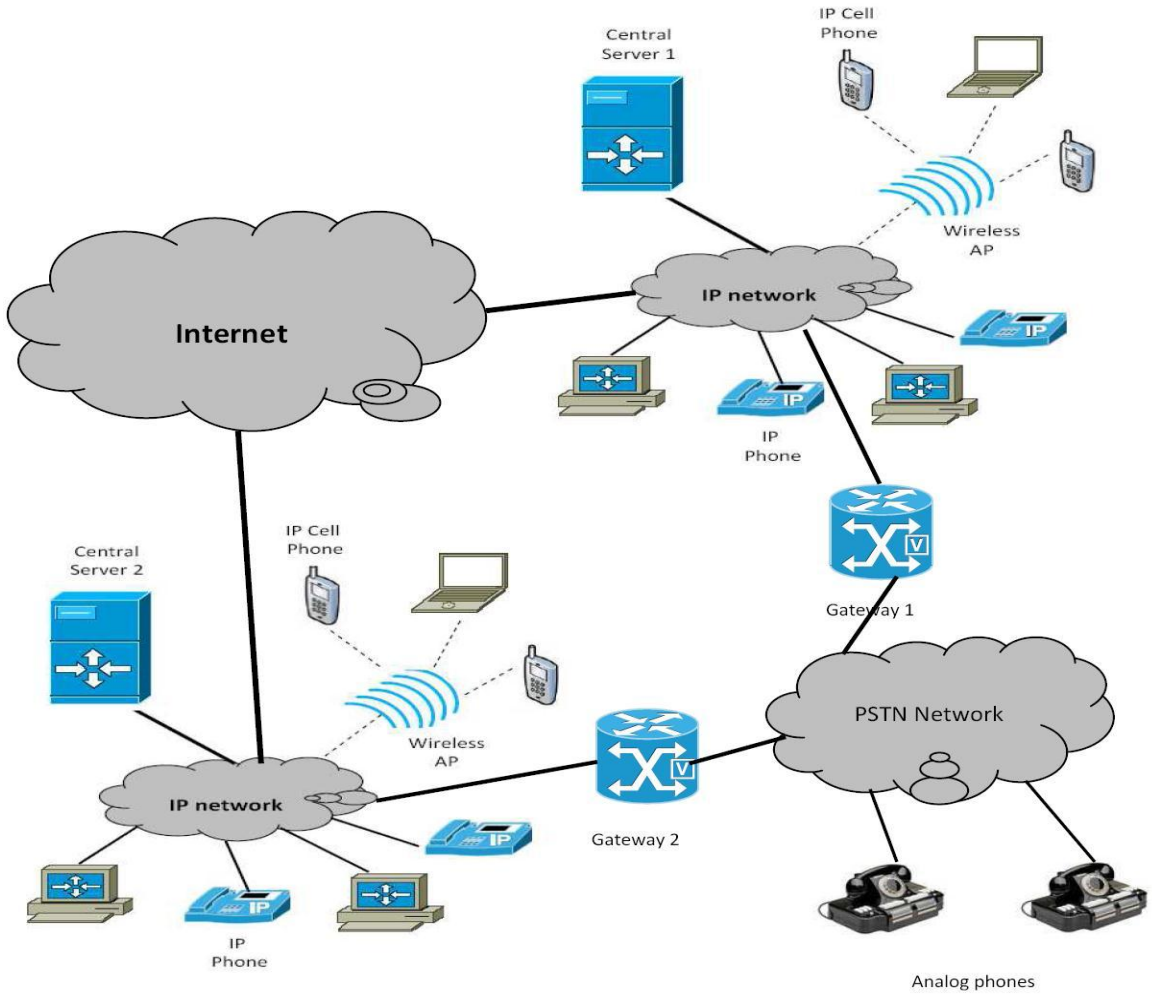

Figure 1: Client-Server VoIP Architecture: An illustrative example

VoIP Protocols

Voice over IP is implemented in various ways using protocols. There are majorly three types of protocols which are widely used in VoIP implementations. They are: H.323 protocols, the Session Initiation Protocol (SIP) and the Media Gateway Controller Protocol (MGCP) [4].

A. Establishing VoIP Connections With H.323 Protocol

H.323 is the International Telecommunication Union's (ITU) standard protocol for establishing VoIP connections in a packet-based multimedia communication system. The H.323 specifications define various signaling functions, as well as media formats related to packetized audio and video services. Generally speaking, the H.323 standards were the first to be classified and solve multimedia delivery issues over LAN technologies. As IP networking and the Internet became prevalent, many Internet standard protocols and technologies were developed based on the H.323 concepts like H.225 and H245. H.323 networks contain three primary solution components:

i. Call processing servers, which store and apply information on network topologies and endpoints, for routing calls to VoIP gateways and end user devices.
ii. Media gateways, which serve both as the H.323 termination endpoint and interface with non-H.323 networks, such as the PSTN.
iii. Gatekeepers, which function as a central unit for call admission control, bandwidth management and call signaling [9].

Although gatekeepers are not required elements in H.323, they can increase the network's overall scalability by separating call control and management functions from the gateways. Figure 2 shows the H.323 architecture.

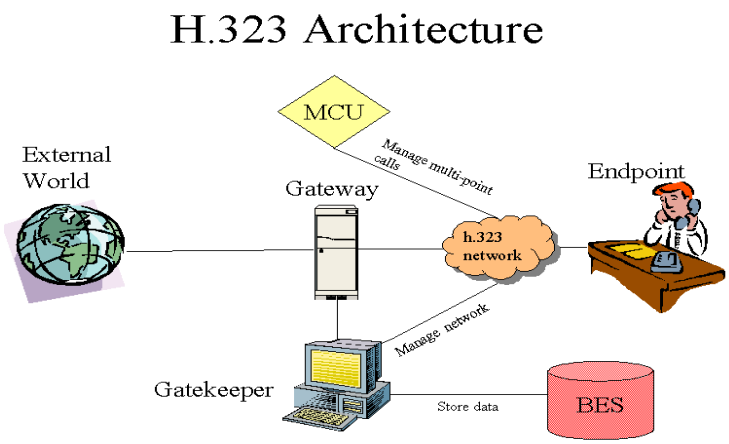

Figure 2: H.323 architecture

B. Establishing VoIP Connections with Session Initiation Protocol (SIP)

Many VoIP networks use the Internet Engineering Task Force (IETF's) signaling protocol Session Initiation Protocol (SIP), to handle the setup and tear down of multimedia sessions between endpoints. This lightweight, text-based signaling protocol is transported over either Transmission Control Protocol (TCP) or User Defined Protocol (UDP). SIP uses invitations to create Session Description Protocol (SDP) messages to carry out capability exchange and to setup call control channel use. These invitations allow participants to agree on a set of compatible media types. The powerful SIP client-server application supports user mobility with two operating modes: proxy and redirect. In proxy mode, SIP clients send requests to the proxy server. The proxy server either handles the requests or forwards them to other SIP servers. Proxy servers can insulate and hide SIP users by proxying the signaling messages. To the other users on the VoIP network, the signaling invitations look as if they are coming from the proxy SIP server.

When the SIP server is operating in redirect mode, the SIP client sends its signaling request to a SIP server, which then looks up the destination address. The SIP server returns the destination address to the originator of the call, who uses it to signal the destination SIP client. The ability to proxy and redirect requests to the end user's current location is critical to supporting a highly mobile voice user base. SIP enables users to inform the SIP server of their current location (IP address or URL) by sending a registration message to a registrar. As a result, although early VoIP deployments were based on H.323, SIP has become the protocol of choice. This SIP architecture is shown in figure 3.

SIP (as defined in RFC 2543) is the basis for the IP Multimedia Subsystem (IMS) multimedia data and control protocol framework that the IETF is developing in conjunction with the Third-Generation Partnership Project (3GPP). IMS uses SIP and other standard interfaces between applications, network layers, and back-office systems to create a flexible framework that can deliver any kind of traffic (voice, data, video, or multimedia) over any wireless or wire line access network [11].

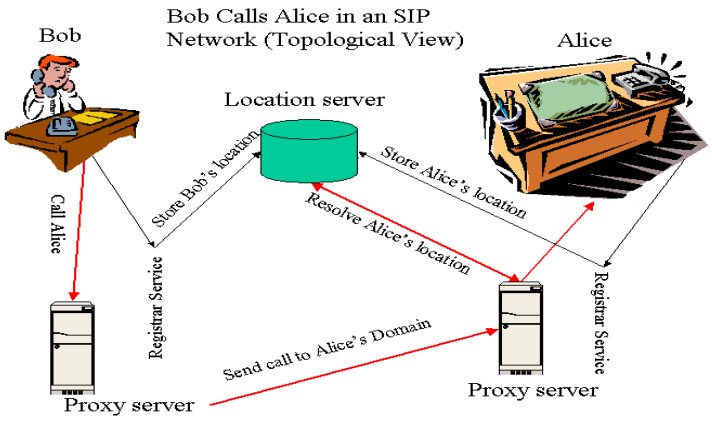

Figure 3: SIP architecture

C. Signaling Control Information between VoIP Network Elements

The ITU and IETF also define VoIP control protocols designed to exchange signaling control information between VoIP network elements. The earlier of these protocols, Media Gateway Control Protocol (MGCP), is currently supported by the IETF as an informational standard. MGCP is used to signal control information between VoIP network elements. MGCP segments the functionality of a traditional voice switch into three functional units: the media gateway, media gateway controller, and signaling gateway. This enables network - managers to manage each VoIP gateway independently as a separate entity.

MGCP is a master-slave control protocol that coordinates the actions of media gateways. The media gateway controller, also known as a call agent, manages the call-related signaling control intelligence, while the media gateway informs the media gateway controller of service events. The call agent instructs the media gateway to create and tear down connections when the calls are generated [10].

VoIP Implementation

There are four different ways of implementing a VoIP call and each of these cases require the use of Internet Protocol (IP). The four different types are:

i. PC to PC
ii. PC to Telephone
iii. Telephone to PC
iv. Telephone to Telephone

Circuit Switching and Packet Switching

In transmission of data beyond a local area, communication is typically achieved by transmitting data from source to destination through a network of intermediate switching nodes. The two technologies used in wide-area switched networks are circuit switching and packet switching. These two technologies differ in the way the nodes switch information from one link to another on the way from source to destination [1].

VoIP Equipments

Voice over IP is associated with equipment that provides the ability to dial telephone numbers and communicate with parties on the other end of a connection who have either another VoIP system or a traditional analog telephone. The following are needed to deploy and implement a VoIP network [12]:

i. **Data Network:** A data network with less congestion is needed to deploy a VoIP system since voice are packetized and transmitted over data networks. These networks are IP networks and can be internet, intranet, or any packet switched network.
ii. **Traditional Telephone Handset:** Usually these products have extra features beyond a simple handset with dial pad. Many have a small LCD screen that may provide browsing, instant messaging, or a telephone directory, and which is also used in configuring the handset to gain access to enhanced features such as conference calls or call-park (automatic callback when a dialed number is no longer busy). Some of these units may have a "base station" design that provides the same convenience as a conventional cordless phone.
iii. **Conferencing Units:** These provide the same type of service as conventional conference calling phone systems, but since communication is handled over the Internet, they may also allow users to coordinate data communication services, such as a whiteboard that displays on computer monitors at both ends.
iv. **Mobile Units:** Wireless VoIP units are becoming increasingly popular, especially since many organizations already have an installed base of 802.11 networking equipment. Wireless VoIP products may present additional challenges if certain security issues are not carefully addressed.
v. **PC Or "Softphone":** With a headset, software, and inexpensive connection service, any PC or workstation can be used as a VOIP unit, often referred to as a "softphone". If practical, softphone systems should not be used where security or privacy are a concern. Worms, viruses, and other malicious software are common on PCs connected to the internet, and very difficult to defend against. Well known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages

can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of "softphones", for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

vi. **Dedicated Router:** These devices allow any user to use its own traditional phone to place VoIP calls. They are connected to cable/DSL modems (or any high-speed internet source) and allow any user to attach an ordinary telephone. Once these routers are configured with an appropriate VoIP provider and service plan, There is no need of special software or interaction with a computer. In fact, there is only need to pick up your phone and dial a number at the dial tone. You can also bring your own adapter with you when you travel and make calls wherever broadband internet access is available.

vii. **Adapters (USB):** USB devices also allow you to use a traditional phone to place VoIP calls. They usually come in the form of USB adapters that are slightly larger than the typical thumb drive. They feature a standard modular phone jack to which you can attach an ordinary phone line. Once connected, your phone behaves as if it were connected to standard phone service.

viii. **Software-Controlled VoIP Applications:** There are many software applications ("softphones") that allow you to place VoIP phone calls directly from an ordinary computer with a headset, microphone, and sound card. Internet telephony service providers usually give away their softphones but require that you use their service. Together, these applications and services enable users to talk to other people using the same service at no cost, and to the rest of the world for a fee. Software-based VoIP applications are quite attractive to consumers because they often already have most of the components necessary to get started at little to no cost.

ix. **Dedicated VoIP Phones:** A VoIP phone looks like an ordinary corded or cordless telephone, but it connects directly to a computer network rather than a traditional phone line. A dedicated VoIP phone may consist of a phone and base station that connects to the internet or it may also operate on a local wireless network. Like the VoIP adapters mentioned above, dedicated VoIP phones also require a provider as well as a required service plan.

Benefits of VoIP

Voice over Internet Protocol (VoIP) technology refers to a series of transmission capabilities that make communication over the Internet a possibility. VoIP, colloquially known as Internet telephony, converts voice vibrations to compressed digital signals that translate to Internet Protocol (IP) packets. These IP packets are then transmitted and converted to a regular telephone signal if the user has a regular telephone. In essence, if you are using a VoIP telephone system, you are basically using the Internet to make phone calls. Internet telephony offers services and benefits unparalleled by traditional phones. The key benefits of the VoIP technology are as follows [7] :

i. **Cost savings:** The most attractive feature of VoIP is its cost-saving potential. For users, VoIP makes long-distance phone calls inexpensive. For companies, VoIP reduces cost for equipment, lines, manpower, and maintenance. For service providers, VoIP allows the use of the same communication infrastructure for the provision of different services which reduces the cost of services deployment.

ii. **Provision of new communication services:** In addition to the basic communications services (phone, fax), the VoIP technology allows users to check out friends' presence (such as online, offline, busy), send instant messages, make voice or video calls, and transfer images, and so on.

iii. **Phone portability:** VoIP provides number mobility; the phone device can use the same number virtually everywhere as long as it has proper IP connectivity. Many business people today bring their IP phones or soft-phones when traveling, and use the same numbers everywhere.

iv. **Service mobility:** Wherever the user (phone) goes, the same services will be available, such as call features, voicemail access, call logs, security features, service policy, and so on.

v. **Integration and collaboration with other applications:** VoIP allows the integration and collaboration with other applications such as email, web browser, instant messenger, social-networking applications, and so on.

Risk Factors

A new technology is always developed to correct the drawbacks and limitations of the previous one but somewhere it also has its own setbacks, like any emerging technology, there are still a few kinds in the system. However, as standards are developed it becomes more reliable and achieves greater acceptance. A number of disadvantages associated with the technology are [14]:

i. **Loss of Voice Quality:** Technologists understand that data networks are very different from voice networks. On the data network, especially on those Ethernet transports that dominate corporate computing environments, packets bounce around somewhat indeterminately. They can collide and get distorted or even lost. Error correction mechanisms in Ethernet hardware and the IP protocol itself can readily compensate for these phenomena on the data side. But such problems can adversely affect voice calls, which require a good quality, real-time flow of packets from one end of the network to the other. And, while the human brain can comprehend human speech even when there is a lot of distortion, users have become accustomed to a certain level of call quality.

ii. **Loss of Reliability:** Data networks are not yet as reliable as voice networks. We all know what it is like to have our computer freeze or to be told that the network is “down." But this rarely happens with our phones or our telephone carriers. Immediate and uninterrupted access to others over the phone is such an essential aspect of conducting business that few executives want to put voice communications at risk, regardless of how attractive the potential savings may be.

iii. **Vendor Architecture Dependence**: The pace of change in computing and communications technology today makes vendor ``lock-in" a major concern for any potential buyer. There are really two aspects of lock-in that trouble most decision makers. One is the possibility that another, superior solution for VoIP will come along shortly after a commitment has been made to a particular vendor's product. If the investment in that product is substantial, it's usually impractical to scrap it and switch to the better approach. Of even greater concern for technology managers, however, is the fact that selection of one vendor's approach to voice/data convergence may cause a lock-in that extends far beyond the VoIP solution itself, forcing a long-term commitment to that vendor's overall networking architecture. This concern is exacerbated by the lack of clear standards in the VoIP market. In the absence of such standards, technology managers have legitimate concerns about committing their companies to any proprietary architecture.

iv. **Lack of Expertise and Experience**: VoIP technology is new. Every new tool must be tested and mastered. This takes time. Haste makes waste. Without the proper expertise and careful planning the technology can work against the customer.

Applications of Voice over IP

VoIP is the ability to make telephone calls (i.e., to do everything we can do today with the PSTN) over IP-based data networks with a suitable quality of service (QoS) and a much superior cost/benefit. VoIP could be applied to almost any voice communications requirement, ranging from a simple inter-office intercom to complex multi-point teleconferencing/shared screen environments. The quality of voice reproduction to be provided could also be tailored according to the application. Customer calls may need to be of higher quality than internal corporate calls, for example. Hence, VoIP equipment must have the flexibility to cater to a wide range of configurations and environments and the ability to blend traditional telephony with VoIP [1]. Some examples of VoIP applications that are useful are:

i. **PSTN gateways**: Interconnection of the Internet to the PSTN can be accomplished using a gateway, either integrated into a PBX or provided as a separate device. A PC-based telephone, for example, would have access to the public network by calling a gateway at a point close to the destination (thereby minimizing long distance charges).

ii. **Internet-aware telephones**: Ordinary telephones (wired or wireless) can be enhanced to serve as an Internet access device as well as providing normal telephony. Directory services, could be accessed over the Internet by submitting a name and receiving a voice (or text) reply.

iii. **Inter-office trunking over the corporate intranet**: Replacement of tie trunks between company-owned PBXs using an Intranet link would provide economies of scale and help to consolidate network facilities.
iv. **Remote access from a branch (or home) office:** A small office (or a home office) could gain access to corporate voice, data, and facsimile services using the company's Intranet (emulating a remote extension for a PBX, for example). This may be useful for home-based agents working in a call center.
v. **Voice calls from a mobile PC via the Internet:** Calls to the office can be achieved using a multimedia PC that is connected via the Internet. One example would be using the Internet to call from a hotel instead of using expensive hotel telephones. This could be ideal for submitting or retrieving voice messages.
vi. **Internet call center access:** Access to call center facilities via the Internet is emerging as a valuable adjunct to electronic commerce applications. Internet call center access would enable a customer who has questions over the Internet to access customer service agents online. Another VoIP application for call centers is the interconnection of multiple call centers. Take the example of a Web-enabled call center. One of the biggest obstacles that companies face in converting Web site visitors into Web site buyers is poor online interaction. In a store, customers can ask a nearby salesperson a question that may end up determining whether or not they head for the checkout line. On a Web site, that kind of interaction is more problematic. But using VoIP, site visitors can click a button and open up a voice conversation with a real, live call center agent who can quickly address any question or problem the customer might have.

Security Threats to Voice over IP

VoIP systems rely heavily on a data network and this dictates its degree of vulnerability, which implies how much it is subjected to security weaknesses and any types of attacks associated with loss of data network. For example, in a conventional telephone system, physical access to the telephone lines or a compromise of the office private branch exchange (PBX) is required for in order to conduct activities such as wire-tapping. But for VoIP, voice is converted into IP packets that may travel through many network access points. Therefore the data is exposed to many more possible points of attack that could be used for interception by intruders. The following present the different types of attacks that can occur when making or receiving a call [3].

i. **Theft of service and abuse:** This type of attack is mostly directed towards the service provider where malicious user uses the service fraudulently with an intention of not paying for it. There are various methods the hacker can use in achieving this fraudulent task. In its simplest form of toll fraud, the attacker places call using an unused IP phone by impersonating the identity of the rightful user of the telephone. In a more complex scenario, the attacker may place a rouge IP phone in the network or an unauthorized call can be made by bridging the gateway.
ii. **IP Spoofing:** This is when an attacker poses to be someone else in order to gain access to restricted resources or steal information. This type of attack can take a variety of different forms; for instance, an attacker can change the protocols which are used as the Internet Protocol (IP). The address of authorized user is given in order to get into their accounts. Also, an attacker may send fraudulent emails and set up fake websites in order to capture user's login names, passwords and account information.
iii. **Masquerading:** This is the pretense of an entity to be another entity. It takes place when the hacker within or outside a network pretends to a remote user as the rightful recipient when in fact he is having a conversation with the hacker. This usually occurs in cases where the hacker assumes the place of someone that is not well known
iv. **Call interception:** This is the act of unlawfully monitoring voice packets or RTCP transmission. This type of attack can be linked to wiretapping in a packet switched network where hackers captures and analyze voice packet payload when it's being transmitted over the IP network. Hackers can make use of data sniffing and other well-known hacking tools to detect, alter, store and playback the captured voice packets because voice travels in packets over the data network.
v. **Call Hijacking:** This is the act of hijacking or redirecting an ongoing conversation to a different end point. The hacker could swap the original voice mail address with the hacker's IP address thereby opening a channel for the hacker. In this case, all the VoIP calls will not reach its intended destination. Similar tools used in launching call interception are used in achieving call hijack.

vi. **Denial of Service (DoS):** Some researchers claimed that DoS attack is the most harmful VoIP attack due to the fact that it has a direct impact on customers and results in loss of productivity, revenue and system downtime. This attack prevents the valid users of the network from using the features and the services of the network. The major way of launching this type of attack is by flooding the network or server with spurious traffic with the intension of overloading it. This causes serious degradation of the network with unavailability of service. IP phones and Gateways can also be subjected to flooding attack in an attempt to disrupt voice communication. Identified the ping command which uses ICMP (Internet Message Control Protocol) as one of the major means of carrying out flooding attack

vii. **Eavesdropping:** This concept in VoIP is quite different from that of the conventional eavesdropping in a data network. Eavesdropping in VoIP occurs when a voice packet is intercepted by the attacker using programs like VOMIT (Voice over Misconfigured Internet Telephony).This enables the attacker to listen to voice conversation without the knowledge of the target. The network requires a physical access to ensure interception of signaling and media stream conversation. Separate network protocol like UDP or TCP is used for signaling messages and ports from media itself. Media streams are transmitted over UDP using RTP (Real Time Protocol).

Quality of Service

Quality of Service (QoS) refers to the ability of a network to provide better service to selected network traffic over various underlying technologies, including IP-routed networks. QoS features are implemented in network routers to provide better and more predictable network service by [13]:

i. Supporting dedicated bandwidth
ii. Improving loss characteristics
iii. Avoiding and managing network congestion
iv. Shaping network traffic
v. Setting traffic priorities across the network

This has an immediate impact on VoIP. In order to achieve toll quality voice, the application necessitates high Quality of Service (QoS) support, such as reserving enough bandwidth (as determined by the codec) and proactively avoiding congested networks. To configure an IP network for real-time voice traffic, the appropriate QoS needs to be selected for both edge and backbone routers in the network. Edge routers perform packet classification, admission control, and configuration management; in contrast, backbone routers perform congestion management and congestion avoidance [2]. The following are the factors affecting quality of service:

i. **Delay:** This is the time interval between the instant that the talker speaks and the listener hears. This is the most important factor in determining the voice quality for VoIP**.** One major problem that delay can cause is Speech Overlap. In a regular conversation when a talker finishes speaking, he or she waits for the listener to speak. If response does not arrive within a suitable time, then talker begins speaking again and before he or she gets the delayed response it collides with the talker's speech.

ii. **Jitter:** This is the variation in arrival rate of voice packets at the destination. This is due to the fact that packets will reach their destinations by a number of different routes which introduce varying delays to the packets passing through. A jitter buffer smoothes the jitter problem by playing out the voice frames at a constant rate. In order for jitter buffer not to introduce unnecessary delay or packet loss, it should be adaptive, that is, it should monitor timestamps of arriving packets and adjust the buffer size accordingly. This kind of adaptive buffer size will minimize itself in low-delay environments. In environments with varying delay such as the Internet, jitter buffer adapts itself to increasing or decreasing delay variations.

iii. **Packet Loss:** This is common in both private and public IP networks. Packet loss happens when the network is congested with too much traffic or bandwidth is overrun and when the network quality is poor, that is, the network has unsteady network components or underpowered equipment. Those reasons mentioned above are valid for both voice and data packets. However, voice packets unfortunately have one more factor to be discarded; voice packets are discarded when they arrive at their destinations too late to be useful by exceeding the jitter buffer's time limit. Packet loss is not an issue for data packets which use Transmission Control Protocol (TCP). TCP provides reliability by detecting and retransmitting dropped packets. However, VoIP,

which requires real-time transmission of packets, cannot use TCP's retransmission mechanism because a late packet equals a lost packet for a VoIP application and TCP introduces unacceptable delay for voice packets.

iv. **Echo:** This is an electrical reflection of a signal through the network. Echo is generally the result of a mismatch in impedance between the 4-wire network switch connection and the two-wire local loop.

v. **Throughput:** The amount of data received at the destination is termed as throughput of that communication. It is calculated in terms of bits/sec or Kbit/sec. for any network to be more efficient, it must have more throughput value. We can say that the throughput of the network is directly proportional to performance of the network.

vi. **Load**: the amount of data a network can carry in the intervals of time is termed as load of that communication network. If X is the maximum load of the network, then there will be a network link failure if the communication tries to carry more than X. it is calculated in terms of bits/sec or Kbits/sec. For any network to be more efficient, it must have less load value. The load of the network is inversely proportional to performance of the network.

vii. **Mean Opinion Score (MOS):** is a measure of voice quality, and is a quality measure that has been used in telephony for decades as a way to assess the human users' opinion of call quality. The test is used widely in VoIP networks to ensure quality voice transmission, test for quality issues, and provides a metric by which to measure voice degradation and performance. With the increased popularity of VoIP phone services, MOS scoring is essential to ensuring client satisfaction for continued network growth.

In VoIP, voice vibrations are compressed to digital signals that translate to Internet Protocol (IP) packets with the aid of codecs or encoding techniques. When making a call over the Internet, the software (soft-phone) or hardware needs to use a codec to send/receive information in a certain format and convert it to the sounds you hear. The codec is the component in an IP phone that encodes and digitizes the voice and converts it back into an analog stream of speech during a VoIP call. The codec is the analog-to-digital-to-analog converter. Every codec has a capability to produce a specific quality of speech. QOS (quality of speech) is variant and totally subjective to the user/listener experience. MOS (Mean opinion Score) is a benchmark to determine quality of voice generated by a specific codec which is determined through an experiment where a range of user review and judge the quality of voice and grade it from 1, being worst, to 5, being best and then the result is compiled to come up with the MOS value for certain codec. There are several voice digitization standards and some proprietary techniques in use for VoIP transmission. Most vendors support one or more of the following ITU standards and avoid proprietary solutions. Some of these ITU standards are: G.711, G.729, G.723.1, G.722 [9].

Conclusion

VoIP can be applied to almost any voice communications requirement, ranging from a simple inter-office intercom to complex multi-point teleconference/shared screen environments. The quality of voice reproduction to be provided should be satisfactory. Hence, VoIP equipment must have the flexibility to cater for a wide range of configurations, environments and the ability to blend traditional telephony with VoIP.

The theories behind the VoIP technology have been reviewed explicitly and it appears that the advent of this technology will make a remarkable change in the telecommunication industries.

References

[1]. Kundaje A., Bhatia G., Dalvi M., Haridas M. and Nandi S., (2001); "Voice over IP", BEng, Veermata Jijabai Technological Institute Matunga, Mumbai, India.

[2]. Mehta P.C. and Udani S., (2001); "Overview of Voice over IP", University of Pennsylvania, USA.

[3]. Osananaiye O. A., (2012); "Implementing Security on a Voice over Internet Protocol (VoIP)", IOSR Journal of Computer Engineering (IOSRJCE), ww.iosrjournals.org, PP. 24-30, Vol. 4, No. 30.

[4]. Sonkar S. K., Singh R., Chauhan R. and Singh A. P., (2012); "Security on Voice over Internet Protocol from Spoofing attacks", International Journal of Advanced Research in Computer and Communication Engineering, www.ijarcce.com, PP. 153-160, Vol. 1, No. 3.

[5]. Amor L., (2010); "VoIP Technology: Security Issues Analysis", Taif University, Kingdom of Saudi Arabia.

[6]. Anestic P., (2014); "Voice over Internet Protocol", Journal of Computation and Modelling, PP 299-310, Vol. 4, No.1, Scienpress Ltd.
[7]. Angelos D. K., (2010); "A comprehensive Survey of Voice over IP Security Research" IEEE Communications Survey and Tutorials, Columbia University, New York, U.K.
[8]. Ajar K., (2006); "An Overview of Voice Over Internet Protocol (VoIP)", River College Online Academic Journal, www.rivier.edu/journal, PP. 1-13, Vol. 2, No. 1.
[9]. Alsahlany A. M., (2014); "Performance Analysis of VoIP Traffic over Integrating Wireless LAN and WAN Using Different Codecs", International Journal of Wireless & Mobile Networks, www. Ijwmn.com, PP. 79-89, Vol. 6, No. 3.
[10]. Kuhn D. R., Walsh T. J. and Fries S., (2005); "Security Considerations for Voice over IP Systems", Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, Montgomery county, Maryland.
[11]. Kulkarni S., Thontadhary H. J. and Devaraju J. T., (2011); "Performance Evaluation of VoIP In Mobile WIMAX;
[12]. Lydia U., (2009); "Voice over Internet Protocol(VoIP) as a communication tool in South Africa business", Department of Accounting, Stellenbosch University, Private Bag X1,Matieland 7602, South Africa.
[13]. Richard D. K., Thomas J. W. and Steffen F., (2015); "Security Consideration for Voice over IP System", Recommendation of The National Institute of Standard Technology, Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, U.S.
[14]. Selvakumar V., (2011); "Evaluating the Quality of Service in VoIP and Comparing the Various Encoding Techniques", MSc, University of Bedfordshire, Bedfordshire, United Kingdom.