Disruptive Technologies, Innovation and Global Redesign:

Emerging Implications

Ndubuisi Ekekwe
African Institution of Technology, USA & Babcock University, Nigeria

Nazrul Islam
Aberystwyth University, UK & Middlesex University, UK

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Senior Editorial Director: Heather Probst
Book Production Manager: Sean Woznicki
Development Manager: Joel Gamon
Development Editor: Hannah Abelbeck
Acquisitions Editor: Erika Gallagher
Typesetter: Adrienne Freeland
Cover Design: Nick Newcomer, Lisandro Gonzalez

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Disruptive technologies, innovation and global redesign: emerging implications / Ndubuisi Ekekwe and Nazrul Islam, editors.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4666-0134-5 (hbk.) -- ISBN 978-1-4666-0135-2 (ebook) -- ISBN 978-1-4666-0136-9 (print & perpetual access) 1. Disruptive technologies. 2. Technological innovations. I. Ekekwe, Ndubuisi, 1973- II. Islam, Nazrul, 1973-
HC79.T4D57 2012
338'.064--dc23

2011039612

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 15
VoIP vs GSM Technology:
The Way of the Future for Communication

Ikponmwosa Oghogho
Landmark University, Nigeria

Dickinson C. Odikayor
Landmark University, Nigeria

Abayomi-Alli Adebayo
Igbinedion University Okada, Nigeria

Samuel T. Wara
Igbinedion University Okada, Nigeria

ABSTRACT

This chapter presents VoIP as a disruptive technology to GSM technology as well as the issues, controversies, and problems surrounding its deployment. It gives a general introduction of the evolution of communication systems from the POTS, to GSM, and now VoIP. Several issues that surround the deployment of VoIP such as provision of PSTN equivalent services by VoIP service providers, regulation of the service, introduction of latency and other counter measures by some operators, threat posed to PSTN providers due to emergence of VoIP, the need for technical standardization of VoIP, security issues, different cost structure, and quality of service provided were also discussed in details. Solutions and recommendations were suggested to overcome the challenges outlined. VoIP is presented as the way of the future for communication. When this finally happens depends on how fast the challenges outlined in this chapter are addressed. Future and emerging research trends in the deployment of VoIP such as locating users in a secure and reliable way, monitoring VoIP networks, as well as intrusion detection and prevention on SIP were also considered, after which, conclusion was made. This chapter is both informative and interesting.

DOI: 10.4018/978-1-4666-0134-5.ch015

INTRODUCTION

A new invention, a new product and a new technology are applauded for only as long as it takes a newer and better invention, product and technology to be developed. Year in and year out, new technologies emerge to replace old ones which join the queue as history. The plain old Telephone system (*POTS*) or the landline was the main communication system used for *communication* for many years despite its attendant problems, which include: slow growth (especially in underdeveloped countries like Nigeria) very long period required to design and roll out the Networks, very high capital requirements to build Public Switching Telephone Networks (*PSTNs*) and the long time required to get meaningful returns on investment which is of great concern to investors. Due to little or no competition, *POTS* continued to dominate the *communication* industry until the development of GSM technology. The rate at which the mobile phone technology overtook the POTS was far more than what the key players in the *communication* industry would have anticipated. This marked the beginning of a new era that many players in the communication industry thought would last for a very long time (Oruame, 2010). The very fast growth of *GSM technology* has been both phenomenal and unpredictable for equipment vendors and investors alike. Unlike what was the case for landlines, GSM technology showed so fast a growth that it was certain that the influence of landline telephony would continue to decline and that the mobile phone would take over the communication industry. In Nigeria it took just months for this to happen.

Today, it is interesting to note that Internet telephony is already a *disruptive technology* to *GSM technology* and the *POTS* variants including the landline, in the same way that the mobile was a disruptive technology to the landline. The rate at which this is happening may not be as fast as how it happened between GSM technology and the POTS variants. It is no longer news that the circuit switch used in GSM technology is presently being replaced by the packet switch where there is no difference between data and voice or voice and video but everything is simply a packet of data to be decoded into its original form at the point of termination. There is no international or local traffic. Traffic is traffic. Soft switch (packet switch) is presently being deployed and voice over internet protocol (VoIP) is no longer limited to the croaking device being used with a phone jack into a Personal Computer (PC). It is now available in the same mobile phone being carried around and in the stationary phone box in the home or office desk with very high voice clarity. Due to the emergence of *VoIP* and the strides being taken to improve on the technology that supports it, so as to overcome the challenges that are presently limiting its use, it is now glaring that the reign of *GSM technology* based phones would end unceremoniously in the not distant *future*.

Although there is no classified definition of VoIP, it is a technology that allows you to carry voice traffic on a data network. The modem technology allows voice networks to carry data traffic hence what we have today is a reversal of technology that allows data networks to carry voice traffic. Voice, while still a dominant application is gradually being supplanted by data. When developing countries like Nigeria are building their national technology infrastructure today, the dominant consideration will not be to use it to carry voice traffic but to make it data ready as this is the way of the *future*. Voice will only ride on this data infrastructure just like e-mail, SMS, video etc.

VoIP despite its numerous advantages has a number of challenges which has greatly reduced its deployment and use by several potential subscribers. These problems include: security *issues*, geo-location deficiency, poor reliability (poor quality of service), deficiency of handling emergency call services, difficulty of Numbering and number portability, little or no *regulation* on tariffs, Cross-border *issues* etc. Huge invest-

ments in time, money and resources are being deployed to find solutions to these problems, so that the numerous advantages that VoIP offers can be enjoyed without the attendant disadvantages presently being experienced.

This chapter will present broad definitions and discussions of several authors on *VoIP* as a *disruptive technology* to *GSM technology* and the numerous *issues*, controversies and problems surrounding their views.

The chapter will also present the Authors perspectives on the *issues*, controversies, problems etc as they relate to *VoIP* being a *disruptive technology* to *GSM technology* and the way of the *future* for *communication*. Comparative presentation of what has been, or is currently being done will also be presented.

Solutions and recommendations in dealing with the *issues*, controversies and problems presented will be discussed.

Future and emerging trends on *VoIP* as a *disruptive technology* to the *GSM technology* will also be discussed.

Finally, a summarized discussion of the overall coverage of the chapter and the concluding remarks will be provided.

BACKGROUND

Man's existence cannot be separated from his desire to communicate with his fellow man. Right from the days of the early man he has devised means of communicating with others which include use of fires, striking of unique sounds, placement or arrangement of stones etc. The discovery of radio waves and how to transmit and receive them positioned the modern day man on a new course of how to carry out his communication business. Man has long taken advantage of the discovery that sound travels through solids (wires) which has led to the development of the Public Switched Telephone Network (PSTN). Being able to communicate using the *PSTN* was a wonder and many players in the *communication* industry quickly invested in the industry so as to reap high returns. Many governments such as the United States of America and Britain also supported researches on improving the already existing *PSTN* especially during the world wars since they needed it to be able to send and receive messages to and from their officers and soldiers who were difficult to reach with letters.

The growth of the plain old Telephone system (*POTS*) or the landline was very slow especially in underdeveloped countries like Nigeria. It also required a very long period to design and roll out the Networks as well as a very high capital requirement to build Public Switched Telephone Networks (*PSTNs*). It also had the added disadvantage of the long time frame to get meaningful returns on investment which is of great concern to investors. Due to little or no competition, *POTS* continued to dominate the *communication* industry until the development of *GSM technology*. The rate at which the mobile phone technology overtook the POTS was far more than what the key players in the communication industry would have anticipated. This marked the beginning of a *new era* that many players in the communication industry thought would last for a very long time (Oruame, 2010). Their assumption must have been based on the length of time it took before another technology (GSM) could be developed that threatened the Plain old telephone system. This assumption was however faulted as it did not take too long before VoIP was developed with its many attractive features.

VoIP is a general term referring to the digitization of an analog voice generated signal, the transmission of that signal over any IP network, and the transformation back to an analog voice signal at the receiving end. (Bhan, 2006). In VoIP, the circuit switch used in GSM technology based telephony is replaced by the packet switch where there is no difference between data and voice or voice and video but everything is simply a packet of data to be decoded into its original form at the

point of termination. (Task Force, 2006). This replacement also eliminated the need for the associated bandwidth used for signalling in *PSTNs*. This is because *VoIP* uses *protocol* separation for signalling and media whereas *PSTNs* uses channel separation for them. What makes *VoIP* really attractive to customers is the substantial low *cost* of obtaining the service when compared with the *GSM* service. All you really need is a connection to the *internet* and the installation of the necessary software to your system.

Data Transmission via the Internet

The *internet* is presently the world's largest information data base. Using your PC or other *internet* ready electronic device and making the necessary connection to the *internet*, you can send and receive almost any kind of information right from your home or office. Information or data can be routed from one computer or other electronic devices to another on the Internet using network protocols (e.g Transmission control protocol (TCP)/Internet protocol (IP)). At least one unique IP address is assigned to each computer or electronic device on the internet to identify it. Voice data, data, video and other messages sent or received are divided into small chunks known as packets. Each of these packets contains both the receiver and the senders address. Packets are sent to a computer that serves as a gateway and has some knowledge about a small part of the Internet. The gateway forwards the packet to an adjacent gateway after reading the destination address. This process is repeated until one gateway recognizes the packet as belonging to a computer within its immediate domain. That gateway then forwards the packet directly to the computer whose address is specified. Packets can arrive in a different order than the order in which they were sent. This is so because a message is divided into a number of packets and each packet can, if necessary, be sent via a different route across the *Internet* using the User Datagram Protocol (UDP) so that network nodes can process them as ordinary data packets. Packets use the Real-time Transfer Protocol (RTP). RTP has special header fields that hold data needed to reassemble the packets into a continuous voice stream on the recipient's end. On the recipient's end, the process is reversed. Data is extracted from the RTP and reassembled, and another digital-analogue converter transforms the packets back into analog sound. The duty of the IP is just to deliver them. The Transmission Control Protocol (TCP) then put them back in the right order. Figure 1 shows Voice data processing in a VoIP system.

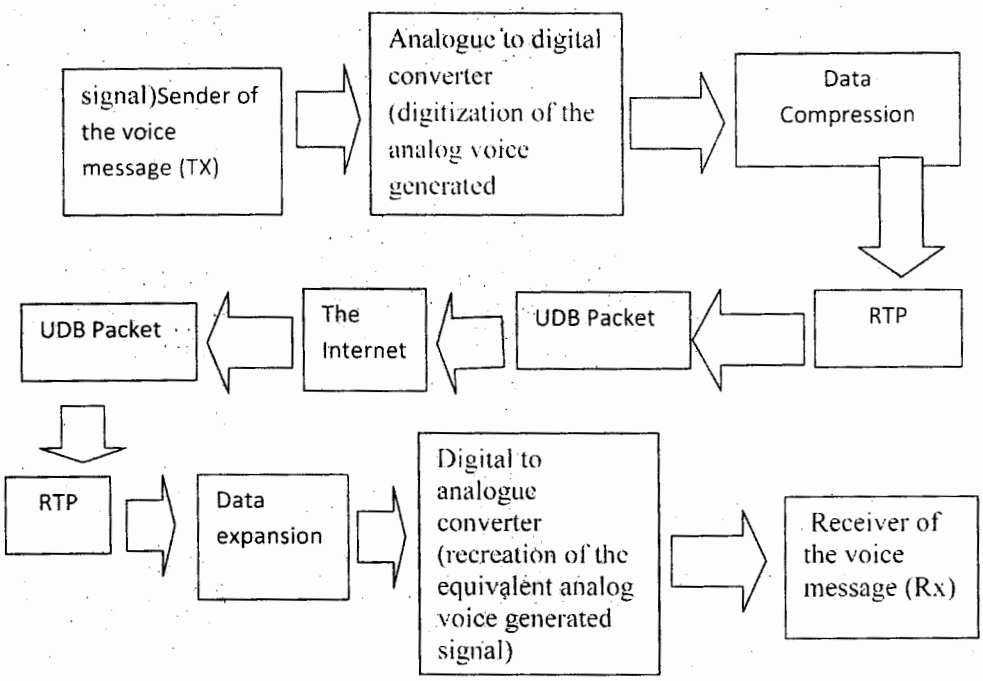
What is Vo-IP?

Voice Over Internet Protocol (*VoIP*) is the routing of voice *communications* over any kind of digital, IP-based network instead of dedicated voice transmission lines. *VoIP* is also called *Internet telephony* because it is the technology that makes it possible to have a telephone conversation over the *Internet*. *VoIP* eliminates the need for circuit switching used in *PSTNs* and the associated bandwidth used for signalling because it uses packet switching for data transmission over an IP based network. IP packets carrying voice data are sent over the network only when data needs to be sent, as is the case when a caller is talking.

VoIP traffic does not necessarily have to travel over the public Internet because it may also be deployed on private IP networks, such as a company's Intranet or a telecommunications carrier's IP network. For individual users, VoIP can be implemented through an existing broadband connection to the *internet* such as DSL or cable modems. An analog telephone adapter (ATA) is required to connect a telephone to the broadband Internet connection.

VoIP is presently being used by some companies (Vonage, AT& T CallVantage etc) to offer unlimited calling in the US, to Canada and some selected countries in Europe and Asia, all for a flat monthly charge. The caller, after subscribing

Figure 1. Voice data processing in a VoIP system



to these companies, can make and receive calls from anywhere in the world, at no extra cost using VoIP calls. Calls travel via IP and do not incur charges as they would do over the PSTNs. Also, since VoIP registered phone number travels with the telephone adapter (a virtual phone number), it is possible to place and receive calls anywhere there is access to a broadband connection to the Internet. What this means is that a telephone number registered in Nigeria can place and receive calls on that number from anywhere in the world as long as there is access to a broadband connection to the Internet.

VOIP Fast Market Growth and Investment

VoIP is seen today as one of the most promising IP applications working its way into the main stream of our everyday life. It will continue to affect the way we do business and communicate in this decade and perhaps decades after. It is a technology that started innocuously towards the end of the twentieth century, took on steam in this decade and has threatened the whole *communication* industry with its ability to change the pricing fundamentals of the industry. It has become such a *disruptive technology* that it has leveled the playing field between already established carriers who still deploy the circuit switch technology and upstarts in the telecommunications industry who presently use the packet switch technology. While not without problems, VoIP promises a more efficient and *cost* effective replacement for traditional wireline telephony while allowing for the possibility of data rich enhancements to voice *communication*.

The business environment has changed dramatically within the last decade. Globalization and market liberalization has changed the way a firm competes within this business environment and how the firm interacts both with its customers and

suppliers. Both customers and competition have become global. To reduce cost and to ensure easy access to customers, production and sourcing have shifted overseas. Technology has also become more complex and sophisticated and the use of *communication* networks is widely available at many parts of the world. More firms than ever are using technology for a variety of tasks and several options exist for technology procurement. Today the Internet makes it possible for customers to have access to a wealth of information about products, markets, and a firm's competition. It is now evident that customers have become more demanding in terms of price, features provided, product quality, delivery, level of service, and responsiveness hence many firms have begun to form alliances and partnerships to manage their supply chain so as to manage customer expectations and needs (Mathiyalakan, 2006).

Firms are looking at many strategic options and are exploring the use of Voice over Internet Protocol (*VoIP*) as a means to cut costs, to improve productivity, and the firm's strategic position. The VoIP industry is in an active growth state, with firms valued at multi-billion dollar levels and a host of technology companies struggling for positions in the growing market of VoIP applications and carriers.

Bank of America is deploying more than 180,000 Cisco VoIP phones across its branches, Boeing has announced plans to equip its 150,000 workers with VoIP, Ford has a deal with SBC to deploy 50,000 VoIP phones, Vonage has nearly 600,000 customers and new subscribers at the rate of 15,000 per week and BT, the major telecommunications player in UK has announced that it plans to convert its infrastructure to VoIP by 2009 (Mathiyalakan, 2006).

Many consumers prefer to use *VoIP* because of its low cost and improved data features. Rapid growth is being experienced today in the market for VoIP. Skype, the world's largest *VoIP* provider which was recently purchased by eBay for about $2.3 Billion, reports to have over 56 million users worldwide and a current growth rate of 150,000 plus users per day. The Yankee is the number one VoIP provider in North America. Other major VoIP providers are Vonage, Primus and AT&T CallVantage.

Residential phone service is leading this strong growth trend, with rapid adoption in the United States of America, Japan and Western Europe. In addition to growing adoption in residential markets, the business sector is beginning to accept *VoIP* as an alternative to traditional telecom solutions. More corporations are turning to VoIP as their voice technology of choice. A Network General Corporation survey of network IT personnel cited VoIP as the most important network initiative in the near *future*. However, growth in this area is being limited due to *VoIP issues* of security and reliability, but as these problems are addressed, it is expected that the business sector will willingly adopt VoIP technology (Task Force, 2006). Jupiter Research, gave a projection in the year 2004 that over 20.4 million US households will subscribe to a VoIP based broadband telephony service by 2011. This is a remarkable 17-fold increase from the 1.2 million subscribers in 2004.

For a third world country like Nigeria, cheaper *communication* within the country and outside is a strong factor in growing our economy to catch up with the rest of the world. This will give Nigeria and other developing countries a comparative advantage in global competitive trade collaborations. It is therefore very clear that VoIP gives the developing nations of the world a chance to key into the current technology that is being implemented worldwide without going through the long transition experienced in the developed world with their very developed and existing TDM infrastructure.

Issues, Controversies, and Problems on Deployment of VoIP

In deploying *VoIP* over the *Internet*, various *issues*, controversies and problems have been recognised. They include (WGIG, 2011):

1. **Provision of PSTN equivalent services by VoIP service providers:** The need for *VoIP* operators and service providers to provide *PSTN* equivalent services such as emergency dialling, ring tones, lawful intercept, numbering and number portability etc is one of the issues that must be addressed if VoIP must be accepted as the *technology* for communication in the *future*.
2. **Regulation issues:** The debate of whether *VoIP*, as a telephony service, should be subject to the same, or similar, national and international *regulation* as the *PSTN* is also a major issue being considered. Some national monopolies and/or national regulators take legal, regulatory, and/or technical steps to prohibit VoIP, primarily because of concern over potential loss of revenue coming from PSTN international calls.
3. **Introduction of latency and other counter measures by some operators:** Some operators introduce latency and other countermeasures into their *VoIP* traffic flows so as to reduce the level of service quality available to users who try to use the best effort VoIP, which generally incurs no expense above normal Internet connections charges. These operators have a corporate policy of attempting to prevent any *VoIP* service for which they cannot charge.
4. **Threat posed to PSTN providers due to emergence of VoIP:** The threat posed to traditional PSTN service providers due to emergence of VoIP because voice revenues are still the main source of income for these traditional network providers is also an issue to be considered.
5. **The need for technical standardization of VoIP:** The need for technical standardization to ensure smooth interconnection between *VoIP* network and existing *PSTN* and between *VoIP* networks of different operators.
6. **Security issues of VoIP:** Security *issues* of VoIP must be considered since it is based on Internet technology. *VoIP* is exposed to the danger of cyber-attacks such as distributed denial of services (that are not generally present in the PSTN), susceptibility to SPAM (which is similar to unwanted calls on the *PSTN* but would require different control mechanisms), data and other vital information accessibility by unwanted persons, etc.
7. **Different cost structure of VoIP:** *VoIP* could develop different ***cost*** structure depending on different business models from legacy telephone system. The charging structure and method is the major concern of operators and service providers as are the rules for settlement between operators.
8. **Quality of service provided:** As service providers offer a wide-range of services with varying bandwidth and network technology, Quality of Services (QoS) also varies among service providers. However, there is no common understanding for quality of VoIP services, no standard accepted method for ensuring QoS between operators and neither objective evaluation criteria nor reliable reporting mechanisms.

The Threat Posed on Traditional PSTN Service Providers Due to Emergence of VoIP because Voice Revenues are Still the Main Source of Income for These Traditional Network Providers

VoIP providers are obviously unwelcome competitors for traditional wireline service providers. Competitive threats usually come in two flavors, namely new licenses and Innovation. Markets

normally favour transformation that follows Schumpeter's creative destruction theory as it yields either lower prices or higher functionality. However some companies like Neotel and Cell C have made good ground in South Africa through the Government bequeathed licensed route, adopting the same circuit switched technologies of the other industry incumbents. The problem here is that large scale investment is required to leverage the license and deliver a return, which can only be achieved quickly by way of continued high prices.

The feature of *VoIP* that has attracted the most attention is its cost-saving potential. By moving away from the public switched telephone networks, long distance phone calls become very inexpensive. Instead of being processed across conventional commercial telecommunications line configurations, voice traffic travels on the Internet or over private data network lines.

VoIP is also cost effective because all of an organization's electronic traffic (phone and data) is condensed onto one physical network, bypassing the need for separate PBX tie lines. Although there is a significant initial start-up cost to such an enterprise, significant net savings can result from managing only one network and not needing to sustain a legacy telephony system in an increasingly digital/data centred world. Also, the network administrator's burden may be lessened as they can now focus on a single network. There is no longer a need for several teams to manage a data network and another to manage a voice network.

The FCC is constantly being petitioned by the telecom industry to treat *VoIP* as standard telephony, yet to this point it has largely resisted. VoIP providers face resistance from traditional telecom companies on many fronts. For example VoIP providers Vonage, theglobe.com and Voiceglo holdings have been sued in a patent infringement lawsuit by Sprint/Nextel (Task Force, 2006). These agitations are basically because VoIP providers are providing the same service at much lower costs. Hence customers are making the choice of using *VoIP* calls rather than subscribing to the Traditional call service providers. This is causing their revenue base to drop and they are trying to put pressure on FCC to issue licences to VoIP service providers also.

The threat posed by VoIP to the traditional voice telephony was demonstrated in America when a company called Vonage rolled out a National VoIP service which made the traditional carriers to look like potential dinosaurs. The big carriers initially saw VoIP as a nuisance used by small companies to make cheap international calls. They are now all scrambling to change their networks to conform to VoIP in a fundamental shift that will change the entire communication industry in America.

A similar trend occurred in Nigeria, when as a result of the deployment of *VoIP technology* in cyber cafes, the Nigerian telecommunications Company (NITEL) was forced to review its international tariff when it was faced with stiff competition from these cafes who offered VoIP calls at fractions of the murderous rates NITEL charged Nigerians. Cyber cafes were charging less than N50/min when NITEL was charging N120/min in the year 2000. The death of NITEL is not traceable to GSM companies alone, but due to a *technology* called *VoIP*. Many traditional call service providers have however upgraded their systems so that they too can offer VoIP calls. This is to enable them retain their customers and revenue base.

From the consumer's point of view, *VoIP* is that system that enables you to make calls almost free to anywhere in the world. This was first available to the masses in Nigeria only through cyber cafes. In large companies where there is broad band access, VoIP is also available as it rides on the broadband network. Companies with large branch networks also implement *VoIP* to allow them make free calls within their network. Calling card operators use VoIP to allow users make mostly international calls with any phones, while incurring an addition local charge on the phone used. Today there are Wifi handsets in the market as well as equipment vendors ready to

push *internet* telephony. Now you can use your Wifi phone to dial another Wifi phone separated by thousands of kilometers for zero fees. All you need is the existence of internet connection at both ends. The Private telephone Operators (PTOs) on their own can also implement VoIP to enable subscribers on their network to make international and trunk calls at reasonable prices, though more expensive than what obtains in the cyber cafes. So, whoever is using *VoIP*, one common factor is that the consumers make calls at substantially reduced rates. Customers can make over 70% savings due to calls using *VoIP*, hence they preferred it above *PSTN* based services which makes the traditional telephony service providers feel threatened.

It is however necessary to state clearly that the cost advantage of *VoIP* over *GSM technology* partially depends on the present nonexistence of strict *regulation* of VoIP by the government whereas traditional voice telephony service providers are being *regulated*. In Nigeria today, for example, there is presently no *regulation* on VoIP calls. Also if the GSM Technology based communication service providers are further deregulated, the cost advantage of *VoIP* over (*POTS*) and *GSM technology* may disappear.

Security Issues of VoIP

VOIP a cheap and readily deployable voice services has come with a massive price tag on security and privacy. Security administrators might be tempted to assume that because digitized voice travels in packets, they can simply connect VoIP components into their already secured networks and still have a very stable and secure voice network. This is however not true because existing firewalls cannot efficiently handle new VoIP protocols such *as the session initial protocol (SIP)* and a wide range of vendor proprietary protocols. This is because they rely on dynamic port ranges and do not support Network Address Translation (NAT) very well.

Some newer firewalls (such as Session Border Controls, or SBC's) address most of these problems, but most firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and similar security devices rely on deep packet inspection techniques. These techniques introduce delay and jitter to the VoIP packet streams, thus impacting overall Quality of Service (QoS). In VoIP, the maximum packet delay is set to 150 ms (and even higher in some cases), but the multilayer nature of security infrastructure could add significant delays and jitter that would make the VoIP services unusable (Bhan, 2006). Therefore, network administrators only implement these common security techniques to VoIP networks sporadically to avoid QoS issues, but this haphazard implementation has left *VoIP* vulnerable to traditional network threats. Some of these threats as they apply to VoIP are listed below.

Denial of Service (DoS) Attacks

Service availability attacks are viewed as the most harmful to VoIP due to its direct impact to customers, resulting in loss of revenue and profit, system downtime and loss of productivity. They are especially destructive to services such as E-911 (Emergence Response Service 911 on VoIP), where disruption could lead to catastrophic damages.

Latency turns traditional security measures into double-edged swords for VoIP (Bhan, 2006). As discussed above, traditional security measures such as encryption and firewall can protect VoIP networks, but they also introduce significant delay. Latency isn't just a QoS issue but also a security issue because it increases the system's susceptibility to denial-of-service (DoS) attacks.

Unlike data networks, where partial DoS attacks would only cause loss of bandwidth and thus slow down network traffic, delaying voice packets in a *VoIP* network for only a fraction of a second would cause them to become unintelligible at the destination and render the service

unusable. The necessary impediment is even less when latency-producing security devices are slowing down traffic.

Another problem that makes *VoIP* extremely susceptible to DoS attacks is packet loss during transmission. Given VoIP's real-time nature, data is never stored in a VoIP scenario, so any packet loss cannot be retransmitted like ordinary data networks. Fortunately, since the packets in voice networks are small (generally ten to 50 bytes), loss of a single packet would hardly affect the voice transmission. However, in most traditional IP networks, buffered transmission generally results in the loss of all packets being delivered at the same time. "Packet losses as low as one percent can make a call unintelligible, depending on the compression scheme used. A five-percent loss is catastrophic, no matter how good the codec (Bhan, 2006). Therefore, computer worms could easily target VoIP networks since the loss of bandwidth could potentially knock out the network, though it might not disrupt conventional IP networks.

The need for gateways for the interaction between VoIP networks and the traditional *PSTNs* has also created soft spots for new attacks. These attacks may be aimed at either network and can include Destination Unavailable (DUNA) or Signaling Congestion (SCON) attacks.

Eavesdropping

For the conventional telephones, eavesdropping requires that a line be tapped or a switch be penetrated. Physical access to the PSTN telephone cable also makes eavesdropping harder and more detectable. Furthermore, proprietary *protocols* and specialized software make the process very difficult. This is not the same for VoIP and IP networks. The convergent nature of the VoIP and IP services, with VoIP and data often transmitted through the same logical network gives attackers convenient and secure access for eavesdropping. Standardized protocols, along with readily available tools to monitor and control network packets, make this process almost trivial. Many good quality open source packages are available for such monitoring, including both SIP and *H.323* plug-ins for packet sniffers such as Ethereal analyzer. Voice Over Misconfigured Internet Telephones (VOMIT) a publicly available utility can convert standard tcpdump format files into .wav files that any computer can play. Other utilities like Tcpdump, available for both Linux and Windows, make *VoIP* eavesdropping accessible to anyone with a PC and internet. The software distributions (generally available for download via the provider's website) for VoIP services also increase the potential for eavesdropping. A technical hacker can modify the software update and host it for download via a rogue server (Bhan, 2006). Using familiar transmission control protocol (TCP) attacks such as Address Resolution Protocol (ARP) cachepoisoning techniques (changing the MAC address associated with a particular IP address) to substitute a rogue server for the correct one, the attacker can cause users to download the hacked software. Another attack that is easier is to set up a rogue server with modified configuration files containing the IP addresses of call managers. The calls of the victims are then routed through the attacker's call manager, thus providing eavesdropping and traffic analysis opportunities to the hacker.

The increasing use of VoIP services in the Critical Infrastructures (CI) sector has also made eavesdropping a critical issue. Confidentiality of conversations is required for many CI services. *VoIP* can open the doors for eavesdropping or sniffing on both media and signalling traffic. Current VoIP deployments provide very few protections from eavesdropping and sniffing, especially against inside intruders (Bhan, 2006).

Spoofing

Identity management is extremely complicated in the VoIP scenario because it is not necessary to have a physical device attached to a VoIP num-

ber. This issue is further complicated by the use of Universal Reference Identification (URI) by some providers for user identification. The way to distribute the identification information that is linked together to different parties is another challenge for deploying VoIP. The lack of standards makes VoIP extremely susceptible to spoofing attacks. For example, the attackers can spoof the IP addresses as well as caller identification to deceive the callee in a *VoIP* session.

Another known spoofing vulnerability in *VoIP* is the ability to spoof the caller's identification information that gets displayed to the callee. Using a SIP10 enabled VoIP hardware such as the Cisco ATA 186 Analog Telephone Adaptor, the attacker only needs to call up a regular phone line, place the caller on hold and flash over to a dial tone using the three-way call feature, and then call a second party for this to work. The caller's ID information that tends to show up is the first called party's telephone number with either their name listed or "unknown name" showing on a conventional caller ID-enabled telephone (Bhan, 2006). This attack is extremely dangerous, especially in corporations and the CI sector where it could be used to break into voice mail accounts or for Private Branch eXchange (PBX) exploitations with the aim of gathering proprietary information. It also allows the attacker to use social engineering to commit telephone and toll frauds.

Theft of Service

In the Edwin Pena and Robert Moore *VoIP* fraud, the accused criminals secretly routed more than ten million calls through unsuspecting companies while selling telephony service cheap to customers, blatantly exposing the immaturity of *VoIP* security. By using dummy servers to conduct millions of scans for vulnerabilities on computer networks, Pena orchestrated a "brute force" attack to identify the prefixes needed to gain access to *VoIP* network. The attack could have also been used to conduct toll frauds by setting up a calling company in a developing country with calling rates as high as $5 a minute, then placing calls to it using hacked *VoIP* networks or user accounts. The unsuspecting users and companies would be left with the bill while the attacker enjoyed pure profits.

Security vulnerabilities of the user's software could also be targets for attacks by hackers. Sniffing user accounts and passwords would again give attackers means of abusing *VoIP* networks for profitable frauds such as identity theft, long distance, or toll frauds. The clear trend, though, shows that hacking the VoIP segment can be quite profitable, and companies should expect more attacks. Besides causing financial damages to the unsuspecting parties, theft of service also severely impacts the availability of a system and the *QoS* of *VoIP* services.

Spam over Internet Telephony (SPIT)

Analogous to the email spam problem in data networks, security analysts have envisioned a major attack of voice and video messages in *VoIP* networks. Even though mass advertising attacks have been launched by advertising agencies on the regular *PSTN* network, the complexity and costs of doing so are prohibitive for mass harassment. However, *SPIT* becomes a major issue without traditional telephony lines. The access to millions of *internet* phones and traditional *PSTN* phones via the internet at extremely low costs is a resource just waiting to be abused by attackers once penetration of VoIP services have gained significant momentum. SPIT poses a potentially critical threat to *VoIP* services as millions of unwanted voice messages (e.g. advertisements) could overwhelm customers. Although this attack seems extremely similar to email spamming attacks, and there are advanced solutions such as blacklists and quarantines developed to combat email spam, applying those technologies to *VoIP* networks would be extremely hard given its real-time nature and difficulty in deciphering the content of the message.

SPIT attacks that target the *PSTNs* from the VoIP networks would almost be impossible to block.

There are also concerns of session hijacking in VoIP, whereby an attacker would be able to capture a video conference channel and transmit advertisements instead. Similar attacks would also be possible on voice conversations which could be hijacked for impersonation or broadcasting mass messages.

Quality of Service (QoS) Provided

For several countries, the provision of information on *quality of service* information is at the discretion of individual *VoIP* providers (Czech Republic, Ireland, Switzerland, Estonia, Denmark, Spain and Norway) (European Regulators Group, 2006). However, a number of other countries (Hungary, Slovenia, Bulgaria, Sweden, Cyprus, Germany, Italy, Austria, Malta and Lithuania) do require that all or particular VoIP service providers provide *QoS* information (ERG, 2006).

Where information is required, the quality of service parameters vary widely. They include transmission delays, packet losses, supply times, fault rates, fault repair times, billing complaints, complaint resolution times, the guaranteed level of quality and the date when the service shall be commenced. Hungary and Cyprus have developed specific QoS parameters for VoIP services (ERG, 2006).

In Spain and Ireland, VoIP providers must inform their customers about the manner in which a VoIP service may differ from traditional telephone services and any other restriction while the UK has consulted on this type of requirement (Okabe, 2006). In many countries this information is made available in the subscriber agreement for the provision of the service. However, some countries do require specific modes and regularity of publication.

In theory, VoIP can provide reduced bandwidth use and quality superior to its predecessor, the conventional PSTN. That is, the use of high bandwidth media common to data communications, combined with the high quality of digitized voice, make *VoIP* a flexible alternative for speech transmission. In practice, however, the situation is more complicated. Routing all of an organization's traffic over a single network causes congestion and sending this traffic over the *Internet* can cause a significant delay in the delivery of speech. Also, bandwidth usage is related to digitization of voice by codecs, circuits or software processes that code and decode data for transmission. That is, producing greater bandwidth savings may slow down encoding and transmission processes. Speed and voice quality improvements are being made as VoIP networks and phones are deployed in greater numbers, and many organizations that have recently switched to a VoIP scheme have noticed no significant degradation in speed or quality (Kuhn, 2005).

Solutions and Recommendations

Today's enterprise administrators face a multitude of VoIP management challenges. These challenges begin when first preparing for VoIP implementation, continue throughout VoIP deployment, and persist as VoIP traffic traverses across complex, heterogeneous network links. Some *solutions* and recommendations needed to combat these problems are outlined in this section.

1. VoIP should be regulated under the existing regulatory regime.

VoIP should be regulated under the existing regulatory regime. The regulators should however adopt a technologically neutral approach to *VoIP regulation* and they should take a light handed regulatory approach, to the extent that this is possible. This will be weighed against the need to protect consumers as well as the interests of licensees. Thus rules created for *PSTN* may not be applied to some VoIP providers or services.

2. VoIP providers should be categorized into two broad categories.

VoIP providers should be categorized into two broad categories, namely:

a. **Facilities based providers** who under the current system would be individual licensees entitled to own, maintain and operate a telecommunications network *VoIP* providers, who own, operate or maintain a traditional *PSTN* should be required to meet the same standards in the provision of *VoIP* as are imposed on them as *PSTN* providers. These operators may be subject to requirements of universal service, and must provide access to emergency numbers and directory enquiry services. In terms of numbering VoIP providers within the PSTN category will be facilitated under a numbering plan similar to that provided to PSTN operators. This category of VoIP service providers should be regulated in the same manner as the traditional PSTN voice service. They should not be made to obtain new licences for the VoIP services which they provide (Chen, 2002).

b. **Service based providers** who lease network elements from locally licensed network operators/individual licensees, to resell services. These service based/ class licence *VoIP* providers should be regulated via means of a new, VoIP/IP Telephony class licence (Christiana, 1999). This is necessary so as to protect the interests of consumers, promote fair competition in the market, compensate traditional *PSTN* or network operators fairly for the use of their network, and to ensure that all persons or entities providing telecommunications services to the public are properly licensed. Service based VoIP providers should be treated as customers of incumbent PSTN operators required to negotiate commercial agreements to provide services. However, agreements between services based VoIP providers should be subject to regulatory review and approval by the regulatory body.

3. Peer to peer social networks should not be regulated.

The Government should forebear from regulating peer to peer social networks and internet telephony services (i.e. these services should be unregulated.) No rules should be developed to regulate IP to IP calls in the short to medium term (Bill, 1999).

4. Geographical numbers should be provided without discrimination.

VoIP providers should be provided with geographical numbers without discrimination. The allocation of these numbers should be facilitated by the regulator as opposed to incumbent network operators. It is also recommended that no obligations on number portability be imposed at this time on either category of *VoIP* provider since the technology is still being developed.

5. VoIP service providers should provide access to emergency services to customers.

VoIP service providers should provide access to emergency services to customers. This provision of access to emergency services should however be discretionary for service type VoIP providers in the short term. Hence both categories of *VoIP* provider should be required to provide clear information to customers about the limitations of VoIP services that they provide in the event of, certain occurrences (e.g the failure of the broadband connection or power outages).

6. No new or extra quality of service standards should be imposed over and above existing standards already required of individual licensees and resellers in existing legislation in force.

In keeping with the policy of technological neutrality VoIP operators in the same category as PSTN operators should adhere to the standards required of PSTN operators. However, as *VoIP* is a developing *technology* and a VoIP telephony market may take time to develop, the regulatory body should continue to observe developments and to make appropriate recommendations where necessary. Efforts should be made by the Government, VoIP Service providers, research Institutes, etc to develop the technology on which VoIP is based so that QoS can be improved.

7. Facilities based/individual licensees should be required to provide directory enquiry services for subscribers of other licensees.

In keeping with the objectives of taking a light handed regulatory approach, and bearing in mind the need to preserve the principle of technological neutrality, existing directory requirements should be applied to facilities based operators or individual licensees only. This is reasonable because the provision of *VoIP* services by a traditional *PSTN* operator represents only a new technology to provide a service essentially similar to traditional voice service, individual licensees should not distinguish between VoIP customers and other customers on the existing PSTN in this area.

8. VoIP providers should work closely with law enforcement agencies where requested.

VoIP providers should be fixed with a general obligation to work closely with law enforcement agencies where requested. This is in the interest of national security and/or public safety, to allow law enforcement to intercept communications.

9. Same security ICT laws should apply to VoIP.

The adoption of any specific rules on security of VoIP services at this time is not necessary as there are already ICT security laws that deal with it. Service providers who offer publicly available communication services over the internet should inform subscribers of the measures that can be taken to protect the security of their communications.

10. Existing rules on privacy protection applicable to all existing licensees should be extended to VoIP providers.

General requirements on providers to supply their service in a manner that protects the privacy of persons as well as an obligation to obtain the express acknowledgement from the customer that he understands the service limitations with respect to privacy, should apply in the case of such providers.

11. There should be massive investment to develop VoIP technology.

All stake holders (Governments, research institutes, private and public companies etc) in the *communications* Industry should invest in research aimed at providing scientific and pragmatic *solutions* to *VoIP* challenges so that the technology can be improved considerable to the extent that the challenges presently being faced by those who want to deploy the technology will be overcome.

FUTURE RESEARCH DIRECTIONS

The rise of *VoIP technology* presents a number of security and management challenges. VoIP is still in its infancy, hence there are no standard solutions for addressing these challenges. These challenges demand new conceptual and pragmatic solutions from researchers in government, academic, and private organizations.

The 1st IEEE workshop on VoIP Management and Security of 2006 was one of the most important workshops on *VoIP technologies*. Private companies and major university research centres were brought together with the objective of creating the first collaborative research vision on the management of VoIP and the security of related infrastructures. The result of the workshop was an exploratory forum with researchers from all over the world proposing new *solutions* and alternatives to improve VoIP security. Some of the major developments and the most innovative proposals of this workshop along with the technological problems that inspired those proposals are (Bhan, 2006) given below.

Locating Users in a Secure and Reliable Way: Proposed by Lei Kong, Vijay Arvind Balasubramaniyan and Mustaque Ahamad

They proposed a new lightweight scheme for securely and reliably locating *SIP* users. These researchers are part of the Georgia Tech College of Computing and claim that one of the most important problems facing *VoIP* is locating the communicating parties via the *internet* in a secure and reliable way.

Many companies are exploring a variety of security mechanisms and different algorithms that include the use of SIP. The authors claim that these algorithms are weak and expensive to deploy, and they proposed a new, alternate scheme to protect the integrity of *SIP* contact addresses. They also point out that this would achieve a high availability of *SIP* services through replication. For this to happen, it is necessary to have an end user public key distributed through the scheme that can also be used for end-to-end user authentication and for session key exchange (Bhan, 2006).

The authors also proposed that *SIP* phones should stop bothering the registrar services and sign their own contact address bindings on behalf of their users. This way, the integrity of the caller and the callee can be verified through the simple use of public keys, and this would also reduce the workload on the registrars. It is important to clarify that the authors are not proposing the use of end-user certificates but instead a change in the *SIP* architecture itself to distribute user public keys (Bhan, 2006).

The authors made an important assumption that could be a weakness in their proposal, which is that all involved SIP servers have certificates issued by a well known public authority. Moreover, they also assume that the caller and the callee trust each other enough to correctly establish the contact's identity and address bindings for their own domains, which does not have to be the case all the time. After all, not all the numbers dialled from telephones are "secure" numbers or are directed to "secure" entities.

Nevertheless, the authors reported that they can protect SIP contact addresses through user signatures, which clearly avoids relying on public key infrastructures through the chaining of trust among SIP entities across the domains. The use of a distributed public key scheme like the one they propose could be of great help for the industry's efforts on security, and while their preliminary experimental results look promising, the idea requires more research on the scalability and performance of a VoIP system using their proposal.

Monitoring VoIP Networks: Proposed by Toshiya Okabe, Tsutomu Kitamura, and Takayuki Shizuno who are Researchers for the System Platforms Research Laboratories of the NEC Corporation in Japan

They proposed a technique that aims to maintain communication confidentiality in VOIP networks.

One important component of securing *VoIP* is considering the emergence of impersonating traffic, P2P traffic, and SPAM over Internet Telephony (SPIT), all of which adversely use the network resources to hurt consumers. Carrier networks should provide a better service by identifying and separating the traffic without peeking into the contents of the data packets.

To accomplish this goal, the authors have studied techniques to identify illegal traffic from limited information. This limited information could include headers or transmission patterns in the packets. The authors proposed a traffic identification technique for a real-time application that uses statistical information such as the frequency of packet arrival. This technique is useful in preventing impersonation attacks by identifying the traffic generated by not only *VoIP* packets but also video applications that are more complex (Bhan, 2006).

They focused on preventing illegal use of network resources by finding out the real time communication flow represented by VoIP. There are already several conventional techniques for flow identification.

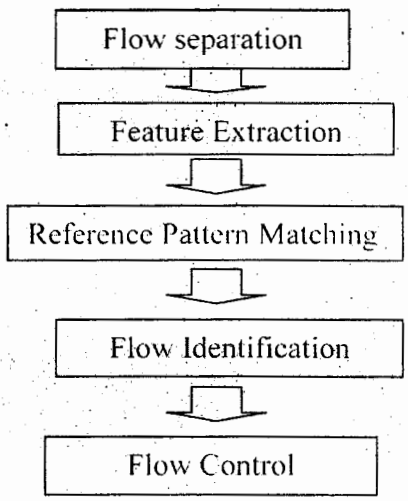
The first one is the host behaviour approach which uses a technique that seeks to infer an application that generates traffic by establishing a relationship between a host and others, and it focuses on that relationship. The problem here is that it is rather difficult to maintain a high detection accuracy if two or more applications are running on one host. This technique also requires a lot of computational power, which is not suitable for large networks (Walsh, 2005).

The second one is the traffic behaviour approach which uses the behaviour of the network traffic to locate an application generating that traffic. These techniques have a variety of weaknesses that have stopped their implementation on current networks.

After evaluating the weaknesses of each approach, the authors propose the use of a flow identification technique that is based on flow-level behaviour as shown in Figure 2. The authors propose a multi-step process. First, the received traffic is divided into flows or different streams of data. As the division is being made, a time stamp is given to each packet. The packet size is also measured and recorded. Next, the feature of the flow is extracted. Usually, this feature is statistical information that is obtained from each flow without checking the payload of each packet, which gives users the confidence that their VoIP Company is not "listening" to what they are saying. After that, the data obtained is verified against established reference patterns of illegal "eavesdropping." Next, there is verification process with the reference pattern that is cyclical. This verification process seeks to avoid false negatives. Finally, a flow control is performed on the traffic with the parameters established by the company.

One of the most interesting features of this project is that the authors were able to launch a prototype to monitor the flow of known VoIP programs, such as Skype, *SIP* softphone, and Microsoft Netmeeting. Moreover, they also tested their application with P2P programs like Kazaa. Their results were very promising, and the authors believed that this technique can also be used to grasp network trends and predict the degradation of the *communication* quality in *VoIP* traffic (Bhan, 2006).

Figure 2. Proposed flow identification process (Satya, 2006)



Intrusion Detection and Prevention on SIP: Proposed by a Team of Researchers from the University of Pisa in Italy and the Ecole d'Ingénieurs et de Gestion du Canton de Vaud in Switzerland

Their proposal is referred to as the first intrusion detection system for VoIP by many stake holders in the Industry. For this team of researchers, and for most of the scientists in the workshop, *VoIP* deployment is expected to grow, but with them, intrusion problems similar to those found in data networks will start appearing as well. The authors proposed to analyze the VoIP requirements for intrusion detection and prevention systems and offered a prototype implementation.

They showed the working prototype of the *SIP* intrusion detection and prevention system implemented using the popular Snort software. This scheme is not different than the one used in many regular corporate networks for intrusion detection. The authors believe that using Snort is an essential part of their technique. These network-based techniques should be implemented in devices able to observe the traffic to be analyzed. Therefore, the entry point of a *SIP* network is best suited to implement their system, which would nothing else than a SIP-aware firewall (Veeraraghavan, 2001). In addition to filtering, their prototype was able to distinguish legitimate from illegitimate requests. They accomplish this feature by checking the *SIP* syntax of the message against the *SIP* rules in search for discrepancies, by checking the *SIP* mandatory fields for correct size and headers and by verifying the SIP state table. This is extremely important to prevent SPIT because this check performs a rate limitation on the number of transactions a particular user can initiate in a time period.

These techniques, combined with a regular network intrusion detection system for SIP, are quite revolutionary, and the authors were able to test their ideas successfully using a brute force generator that tried to sabotage their VoIP network. The implementation of Snort in *VoIP* could be an important step against future threats.

However, as the authors are quick to point out as well, there will be great challenges with trying to implement this system on a network that could have millions of people trying to place a call at a given moment (Bhan, 2006).

Improvements on these methods and new methods of tackling VoIP issues are presently being developed.

CONCLUSION

This chapter presented *VoIP* as a *disruptive technology* to *GSM technology*. This chapter also discussed what happened to the *POTS* when the *GSM technology* was developed. Several *issues*, controversies and problems bothering on deployment of VoIP were also discussed. Recommendations on how the issues raised can be solved were made after which *future* and emerging research trends relating to *VoIP* deployment were considered.

One thing that stands out in all of these discussions is that *VoIP* is the way of the *future* for *communication*. It may not have taken over the *communication* industry completely due to the challenges outlined above. It will certainly become the accepted *technology* for *communication* in the near future as solutions will be found that will make its deployment very attractive and secure when compared with the traditional PSTN system.

REFERENCES

Bhan, S., Clark, J., Cuneo, J., & Mejia-Ramirez, J. (2006). *Information and security issues in voice over Internet protocol*. CS 4235, Fall 2006 report.

Bill, D. (1999). *IP telephony: The integration of robust VoIP services*. Prentice Hall.

Boothby, C. (2005). Liability issues in a VOIP environment. *Business Communications Review, February*, 43-45.

Chen, D., Garg, S., Kappes, M., & Trivedi, K. (2002). *Supporting VBR VoIP traffic in IEEE 802.11 WLAN in PCF mode*. (Tech. Rep. AT&R-2002-026). Basking Ridge, NJ: Avaya Laboratories.

Christian, H., Jane, C., Petros, M., & Darek, S. (1999). An architecture for residential Internet telephony service. *IEEE Network, 13*(3), 56–63. doi:10.1109/65.767139

ERG. (2006). VoIP and consumer issues. [European Regulators Group.]. *ERG Report, 6*, 39.

Kuhn, R. D., Walsh, T. J., & Fries, S. (2005). *Security considerations for voice over IP systems*. National Institute of Standards and Technology (NIST) Special publication 800-58

Mathiyalakan, S. (2006). VoIP adoption: Issues & concerns. *Communications of the IIMA, 6*(2), 19–24.

Okabe, T., Kitamura, T., & Shizuno, T. (2006). *Statistical traffic identification method based on flow-level behavior for fair VoIP service. IEEE Xplore*. Atlanta, GA: Georgia Tech Lib.

Oruame, S. (2010). *VoIP and the end of GSM service*. IT Edge News.

Task Force. (2006). *Emerging technology issues: VoIP and Wi-Fi, 511 deployment*. 511 Deployment Coalition, 1-16. [Technologies and Service Task Force.]. *Future*, 511.

Veeraraghavan, M., Cocker, N., & Moors, T. (2001). Support of voice services in IEEE 802.11 wireless LANs. *Proceedings of INFOCOM'01*, (Vol. 1, pp. 488–497).

Walsh, T. J., & Kuhn, D. R. (2005). Challenges in securing voice over IP. *IEEE Security & Privacy Magazine, 3*(3), 44–49. doi:10.1109/MSP.2005.62

WGIG. (2011). *Draft WGIG issue paper on VoIP*. World Group on Internet Governance. Retrieved from http://www.wgig.org/docs/WP-VoIP.pdf

KEY TERMS AND DEFINITIONS

Communication: The activity of conveying meaningful information which requires a sender, a message, and an intended recipient, even though the receiver may not be present or aware of the sender's intent to communicate at the time of communication.

Disruptive Technology: A new technological innovation, product or service that eventually overturns the existing dominant technology or product in the market.

Global System for Mobile Communications (GSM): The most popular standard for mobile phones in the world.

H.323: An International Telecommunications Union (ITU) umbrella specification which defines a series of protocols for visual-audio communication sessions on any packet network.

Internet: The concentration of the world's public IP-based packet-switched network.

Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the Internet.

Issues: Important problems or topics for debate or discussion.

POTS: Meaning plain old telephone system which was used for communication before the development of GSM technology.

Public Switched Telephone Network (PSTN): Is the aggregate of the world's public circuit-switched telephone networks.

Quality of Service (QoS): Refers to the probability of the telecommunication network meeting a specified traffic contract, or in many cases is used informally to refer to the probability of a packet succeeding in passing between two points in the network within its desired latency period.

Regulation: A rule or a directive made and enforced by an authority which if not complied with attracts a sanction.

Session Initiation Protocol (SIP): A protocol and the proposed standard for handling interactive multimedia user sessions through different media, including VoIP.

Solution: The correct answer to a problem.

Voice over Internet Protocol (VoIP): The routing of voice communications over any kind of digital, IP-based network instead of dedicated voice transmission lines.