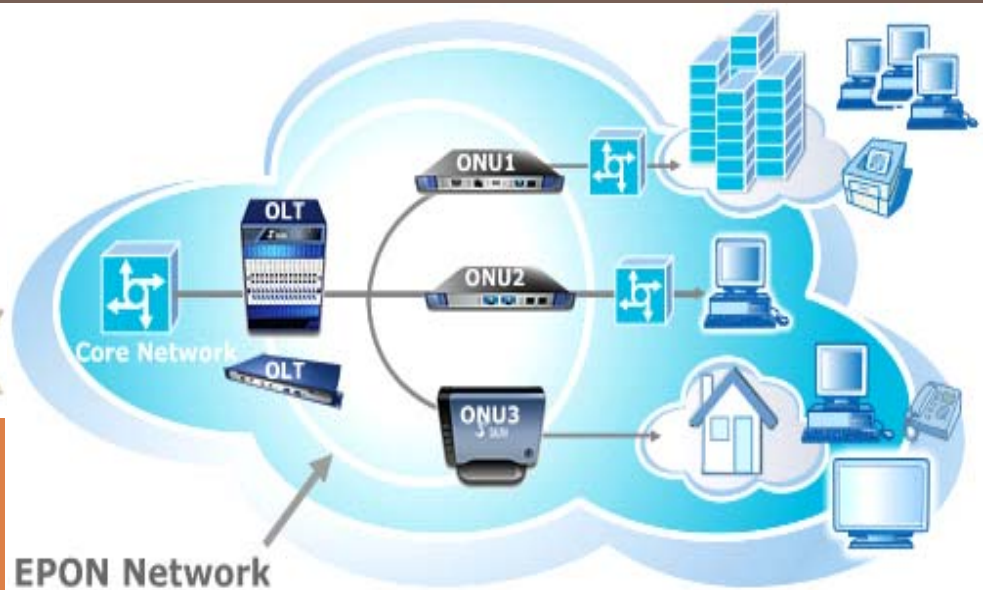


PROCEEDINGS OF THE NATIONAL SEMINAR ON EMERGING TRENDS IN COMMUNICATIONS TECHNOLOGIES(NSETCT-2009) 24 JULY 2009

DRONACHARYA COLLEGE OF
ENGINEERING, KHENTAWAS, FARRUKH NAGAR, GURGAON-
123506



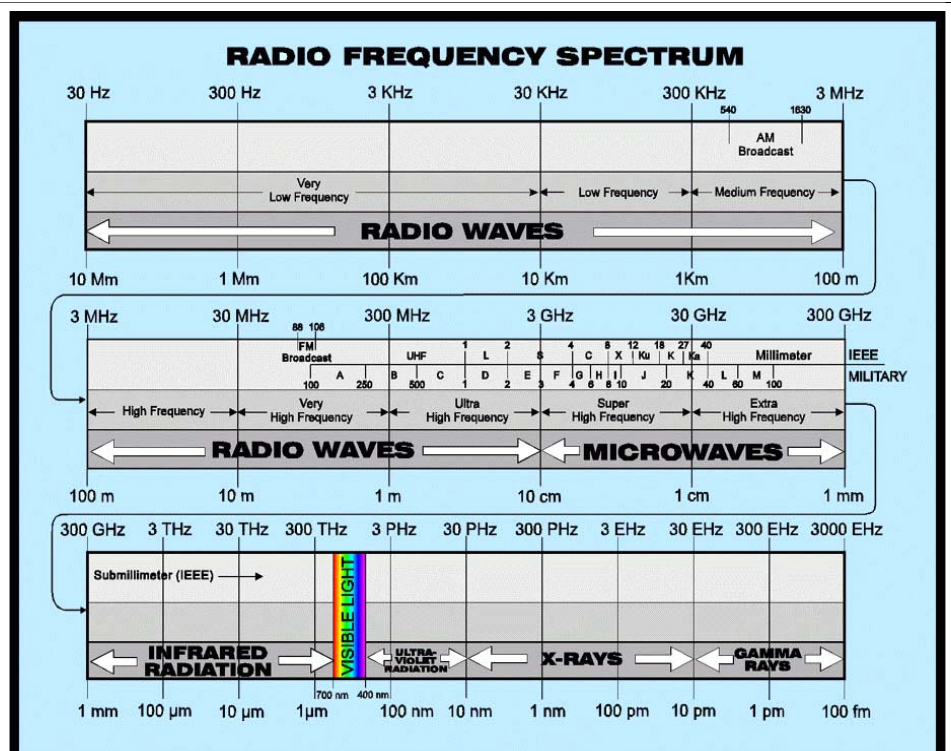
Chief Patron
Dr. Satish Yadav
Chairman, DCE, Gurgaon

Patron
Prof. (Dr) B.M.K. Prasad

Convener
Prof. Onkar Singh

Co-Convener
Prof. H.S. Dua

Coordinator
Prof. Y. P. Chopara



CONTENTS

Messages	i - iii
Forward	iv-v
Section I: Key Note Address	3
<i>Prof H.S. Dua</i>	
Section – II :Technical Papers	
1. Passive optical access network technologies: a review of Present techniques and future evolution <i>Prof Kishori Sharan Mathur</i>	8
2. An Insight Into Bluetooth Technology <i>Prof Y.P. Chopra</i>	25
3. Mobile IP and Challenges <i>Prof. (Mrs.) A.N.Mahajan</i>	32
4. Nanoelectronics in Quantum Computers <i>Naresh Kumari and Sakshi Pahuja</i>	37
5. Network Security <i>Mrs.Dimple Saproo</i>	43
6. Nanoelectronics <i>Swati jha</i>	48
7. Evolution Of 4G Technology <i>Jyoti Dargan and Vinita Sahu</i>	54
8. Network Security using Firewalls <i>Meha sharma and Pooja Yadav</i>	63
9. Internet Protocol Television (IPTV) <i>Amninder Kaur and Shampy Ajrawat</i>	70
10. Wavelet Based Compression of Radiological Images for Telemedicine Applications <i>Taslima Ahmed (Sr.Lecturer), Tazeem Ahmad Khan (Asstt. Prof.)</i>	76
11. Quality of Service in Networks <i>Kavita Choudhary</i>	82

SECTION I
KEY NOTE ADDRESS

DEPARTMENT
OF
ELECTRONICS AND COMMUNICATION ENGG.

**KEY NOTE ADDRESS AT THE NATIONAL SEMINAR
ON
EMERGING TRENDS IN COMMUNICATION TECHNOLOGIES
AT
DRONACHARYA COLLEGE OF ENGINEERING, GURGAON
BY
PROFESSOR H. S. DUA**

hodece@dronacharya.info

Respected Chief Guest, Ladies and Gentlemen, at the outset, let me place on record my sincere appreciation to the management and Hon'able Principal for allowing the Department of Electronics and Communication Engineering to organize a National Seminar on the subject of 'Emerging Trends in Communication Technologies.

During my address, I will be highlighting some of the latest developments related to various communication technologies like Wireless Communication, Satellite Communication, Software Defined Radio, Optical Fiber Communication and Next Generation Networks (NGN).

GENERAL

The Communication Technology has taken a big leap forward and received the national recognition as the key driver for development and growth. The telecom growth in India is the fastest in the world. Tele density is about 25% and it is increasing at a very fast rate.

With the introduction of 3G technology higher data transfer speeds are available and down loading of voice, sound, photo and video will be much faster. By 2012 every fifth handset in India will be 3 G enabled.

WIRELESS BROADBAND

Deployment of copper and cable would not be able to serve more than 15 % of the Indian population. There is a rapidly growing demand for wireless technologies due to non – availability of quality copper and fiber cable. Generally, developed countries have broad band infrastructure based on fiber; whereas developing countries on the other hand tend to rely more on wireless solutions, like Wi -max and Wi -Fi etc. Wi max technology can reach up to a range of more than 100 km and deliver data rate up to 75 Mbps against 54 Mbps and a range of just about 100 m given by Wi – Fi sets.

SATELLITE COMMUNICATION

Dr. Vikram Sarabhai, the founder father of Indian space program had envisioned that space technology is a powerful tool which can play a vital role in development of the country. Currently nearly 100 earth stations and more than 60,000 VSAT's are operating in the Govt and Private sectors. More than one crore households in India are now receiving the DTH satellite TV and radio transmission.

SPECIAL APPLICATION OF SATELLITE COMMUNICATION

Indian Space Research Organization (ISRO) is launching a new Radar Imaging Satellite (RISAT) which will help in assessing the agriculture produce during monsoon season.

TELE- MEDICINE

This facility using satellite communication connects the hospitals and community health centers located at remote locations with super specialty hospitals for providing expert consultation.

TELE-JUSTICE

Court hearings for dangerous prisoners can be conducted without moving the prisoners from jail using Satellite Communication and audio – video conferencing.

Multimedia, IP-TV, mobile TV is emerging as new application areas in the field of Satellite Communication.

SOFTWARE DEFINED RADIOS (SDR)

The Communication Industry is now looking for ways to create radios that can handle multiple freq. bands, understand multiple transmission protocols and be easily upgrade.

SDR provides a single radio Transreceiver capable of functioning like a cordless telephone, cell phone wireless e – mail system, wireless fax and wireless web browser.

In fact, SDR is a step in the direction of having Integrated & Programmable Communications, which is the future of communication technology. SDR'S are implemented with multiple processors e.g., separate one for internet working, intranet working, security and modem processing. All the signal processing is implemented in software. This strategy leads to device flexibility and system upgradeability. Once reconfigurable equipment is deployed in the field, system tuning, function changes etc can be accommodated purely in software.

OPTICAL COMMUNICATION

The optical communication is facing the “capacity crisis “as there is a requirement to send more and more data along the optical fiber cables.

RESOLUTION OF CAPACITY CRISIS

One way is to lay more and more fibers. The second is to increase the bit rate using TDM on existing fibers. Present demand is about 40 Gbps, which is not possible with TDM. Alternative is DWDM – Dense Wave length Division Multiplexing. The DWDM systems are bit rate and format independent and hence can be integrated with existing equipment of the network. Thus DWDM systems can carry up to 80 wavelengths at a total of 400 Gbps to transmit 90,000 volumes of an encyclopedia in one second.

NEXT GENERATION NETWORKS (NGN)

NGN refers to a converged network capable of carrying voice, data video, VOIP, Broadband, multimedia etc over the same network. It is expected that NGN would phase out the existing class of networks at a point of time in the future, as NGN aims to deploy one network platform to support all types of traffic.

NGN envisages use of a Multi- protocol label switching mechanism that enables data networks to efficiently prioritize information based on the type of information contained within the packet.

CONCLUSION

The Communication technology is advancing at a galloping rate. The information carrying capacity of future systems will enable video, data, audio and multimedia to be handled simultaneously. In last about half an hour, I have tried to highlight recent advances in some of the Emerging Communication Technologies. Different speakers will be giving you more information on specific areas on the various communication related topics.

Thank you

SECTION II
TECHNICAL PAPERS

PASSIVE OPTICAL ACCESS NETWORK TECHNOLOGIES: A REVIEW OF PRESENT TECHNIQUES AND FUTURE EVOLUTION

Kishori Sharan Mathur

Professor, Department of Electronics and Communications Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email:kishorimathur@hotmail.com

Dr C Ram Singla

Advisor (R&D) & Professor of Electronics and Communications Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email:crslibra.1010@gmail.com

ABSTRACT

The paper reports that for first mile connectivity, Passive Optical Access Network Techniques are superior than SDH based STM Ringes, Cable Modems, DS1, T3, T1 etc. Techniques. A typical EPON technique with various network architectures is described and advantages of All Optical Access Network Arcticture are highlighted. Future PON WDM techniques are discussed. Finally Holey fibers which have important utilities in PON networks due to extremely bent tolerant and low loss charteristics are discussed.

Keywords: PON, EPON, OLT, ONU, ODN, WDM PON, Holey Fibers

1. INTRODUCTION

1.1 In recent years with the emergence of fiber optical communications the telecommunications backbone has experienced substantial growth. But the 'last mile' still remain the bottleneck between high capacity local area network (LANs) and the backbone networks. The most widely deployed 'broadband' solution was digital subscriber lines (DSL) and cable modem (CM) networks. In metropolitan areas where there is high concentration of users, the access network often includes high capacity synchronous transport modules (STM) rings, optical T3 lines and copper base T1's. The cost of operating these services is high due to the requirement of active electronic components at the outside plant such as regenerators, amplifiers, switches, lasers etc. In such a case, a new technology was required which is inexpensive, efficient, maintenance free, simple, scalable and capable of delivering bundled voice, data and video services. Passive optical access networks (PONS) which represent the convergence of low cost electronic equipment and low cost fiber infrastructure, appears to be the best choice for the next generation access networks.

1.2 The fundamental benefit of PON technology is it is flexibility, reliability and simplicity. It eliminates active network components, such as amplifiers, switches or regenerators, with PON architecture, all active components are placed at the end i.e. at central office (CO) and at user premises. At outside plant i.e. in the field is only the optical fiber and passive optical splitters are placed. It requires minimum maintenance and eliminate expensive controlled environment (i.e. Air conditioning etc). There is no electronic active equipment installed in outside plant. Also there as is no requirement of elaborate power supply network. Secondly, PON technology employs bi-directional communications over a single fiber. This reduces the amount of fiber needed by more than half. The single strand of fiber can feed as many as sixty four or thirty two service drops and at multiple user locations. Presently PON technology can deliver up to 2.4 Gbps of bandwidth, enabling it to deliver voice, data & video services for Fiber to the business/Fiber to the home (FTTB/FTTH) applications. EPON is a point to multi point technology. Figure 1 shows a PON point to multi point network architecture.

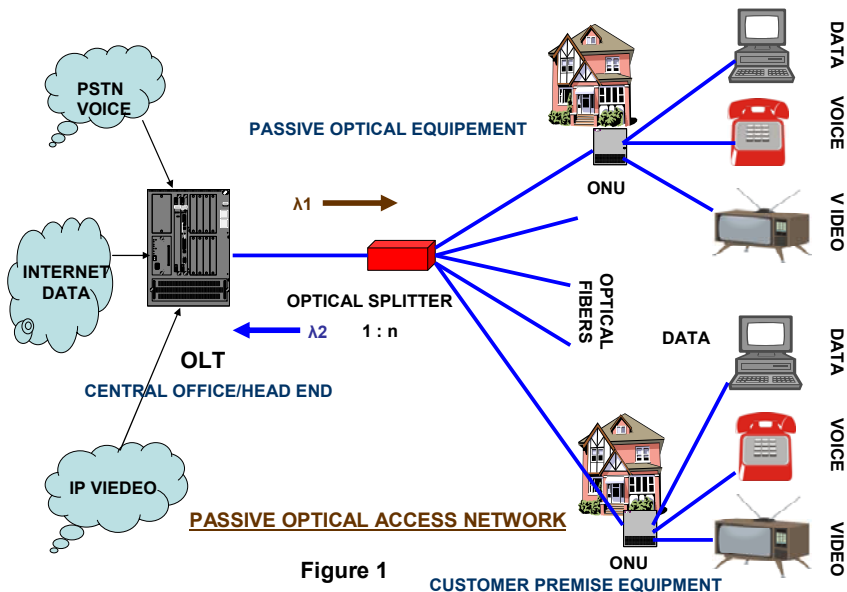


Figure 1

CUSTOMER PREMISE EQUIPMENT

2. EXISTING PON TECHNOLOGIES

As on today following existing Broadband FTTx solutions are available.

- (i) ITU – T BPON (Broadband PON)
- (ii) ITU – T GPON (Gigabit PON)
- (iii) IEEE EPON (Ethernet)

Broadband PON (BPON), are Asynchronous Transfer Mode PON (APON) enhanced by an optical overlay channel for video services. It is widely deployed and mature technology supported by Alcatel 7340 FTTU. BPONs are typically deployed with 622 M bits / sec in the down stream and 155 M bits up stream, giving each user a down stream capacity of 20 to 30 M bits /Sec. Layer 2 protocol in BPON is based on ATM technology.

Gigabit PON (GPON) standards includes a variety of line rates up to 2.488 Gigabits/Sec, symmetric and asymmetric. Net bandwidth of GPON is higher than EPON. Layer 2 protocol in GPON is based on either Ethernet or ATM technology.

Ethernet PON (EPON) supports symmetric 1Gbps/sec bit streams. EPON is compatible with existing Ethernet networks. Layer 2 protocol in E PON is based on Ethernet technology.

At the physical layer, current PON standards include WDM to separate the up stream (1310 nm) and down stream (1490 nm) and to provide an additional overlay channel (1555 e.g. for video). Table gives an overall view of PON standards.

PON Standards - Overview

	BPON	EPON	GPON
Standard	ITU G.983	IEEE802.3ah	ITU G.984
Data Packet Cell Size	53bytes	1518 bytes	53 to 1518 bytes
Maximum Wavelength	622 downstream; 155 upstream	Symmetric 1.2Gbps	Configurable 2.4Gbps downstream 1.2 Gbps Upstream
Traffic Modes	ATM	Ethernet	ATM Ethernet or TDM
Voice	ATM	VoIP or TDM	TDM
Video	1550nm overlay	1550 nm overlay	Either over RF or IP
ODN Classes Supported	A, B and C	A and B	A, B and C
Max PON Splits	32	16/32	64

3. PON ARCHITECTURE

To understand PON architecture let us describe EPON access technology. The rapid decline in the cost of fiber optics and Ethernet equipment resulted in the spread of Ethernet technology from local area network (LAN) to the metropolitan area network (MAN) and the wide area network (WAN) as uncontested standard. The convergence of these two factors is leading a fundamental paradigm shift in the communication industry, a shift that is ultimately leading to wide spread adoption of a new optical IP Ethernet architecture that combines the best of fiber optics and Ethernet technologies. This architecture is now the dominant means of delivering bundled data, video and voice services over a single platform. Optical 'first mile' i.e. the 'last mile' connectivity (which is now renamed as 'first mile' by the networking community to symbolize its priority and importance) connects the service provider central office to the business and residential subscriber. This 'first mile' connectivity can be on a point to point Ethernet link or it could be a curb switched Ethernet or based on Ethernet PON (EPON) connectivity.

3.1 The passive elements of an EPON are located in the optical distribution network (also known as the out side plant) and include single mode fiber optic cable, passive optical splitters/couplers, connectors and splices. Active network elements (NEs), such as the OLT and multiple ONUs are located at the end points of the PON. Optical signals traveling across the PON are either split onto multiple fibers or combined onto a single fiber by optical splitter/couplers, depending on whether the light is traveling up or down the PON. The PON is typically deployed in a single fiber, point to multipoint, tree-and-branch configuration (Fig. 01) for residential applications. There are various topologies for PON configuration which will be discussed subsequently in this paper.

4. ACTIVE NETWORK ELEMENTS

It consists of CO chassis and ONUs that are located at both ends of the PON. The CO chassis is located at the service providers CO, headed or POP and houses OLTs, network interface modules (NIM), and the switch card module (SCM). The PON connects an OLT card to 32/ 64 ONUs each located at a home or at small office/home office (SOHO) site. The ONU provides customer interface for data, video and voice services as well as network interfaces for transmitting traffic back to the OLT.

5. MANAGING DOWNSTREAM/UPSTREAM TRAFFIC IN AN EPON

In EPON, the process of transmitting data downstream from the OLT to multiple ONUs is fundamentally different from transmitting data up stream from multiple ONUs to the OLT. The different techniques used to accomplish downstream and up stream transmission in an EPON are illustrated in Fig 2 and 3.

In Fig 2, data is broadcast downstream from OLT to multiple ONUs in variable length packets of up to 1,518 bytes, according to the IEEE 802.3 protocol. At the splitter, the traffic is divided into three signals carrying all of the ONUs specific packets. When data reaches the ONU, it accepts the packets that are intended for it and discards the packets that are intended for other ONUs based on media access Control (MAC) address.

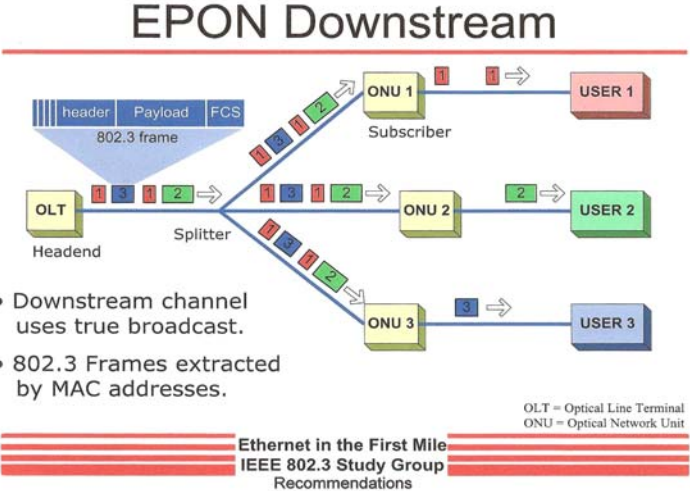


Figure 2

In Fig 3, shows how up stream traffic is managed utilizing TDM technology, in which transmission slots are dedicated to the ONUs. The time slots are synchronized so that upstream packets from ONUs do not interfere with each other once the data is coupled onto the common fiber. For example, ONU-1 transmits packet 1 in the first time slot, ONU-2 transmits packet 2 in a second non overlapping time slot and ONU-3 transmits packet 3 in a third non overlapping time slot.

EPON Upstream

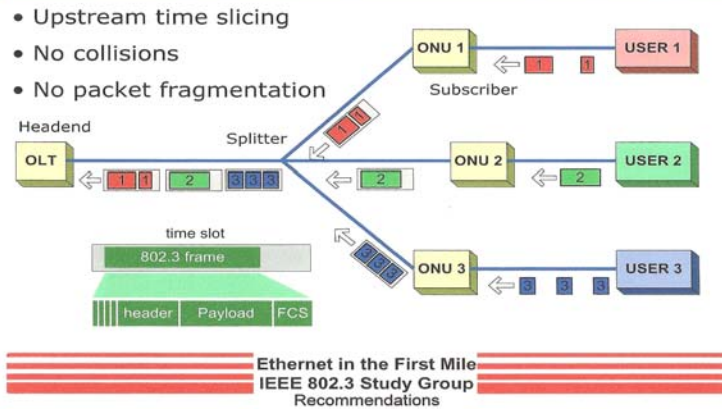


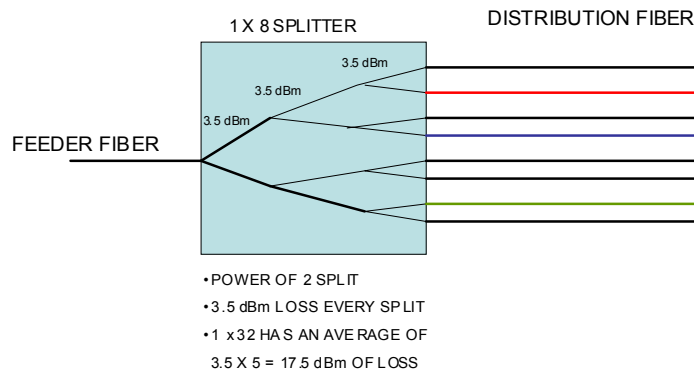
Figure 3

EPONs are employed using two wavelengths design i.e. separate wavelengths for downstream and upstream traffic. In a typical architecture, 1510 nm wavelength carries data, video and voice downstream while a 1310 nm wavelength is used to carry video-on-demand (VOD)/channel change requests, as well as data and voice, upstream. Typically using a 1.25 Gbps bi-directional (PON), the optical loss with this architecture gives the PON a reach of 20 Km over 32 splits.

6. PASSIVE SPLITTERS

Passive splitters are the essential elements that take a passive point to multipoint PON possible figure 4 shows how it works. Optical splitters are implemented using cascading 1:2 power splits where input optical power is distributed two ways and results in a signal loss of 3.5 db. As each branch is further split, more distribution is achieved and additional loss occurs given by the power of two. For example, a 1:32 splitter will have 5(i.e., 2^5) splits and results in 5×3.5 db which equates to a power loss of 17.5 db. Standard PONs is specified for 20 kilometers between the OLT and ONU and typically allow

minimum
of 1:16
splits and
maximum
of 1:64
splits.



As
splitters
involve
high
power
loss,
network

FIG. 4 OPTICAL SPLITTERS

design must carefully balance the need for higher split ratio, longer loop distance and the cost of higher power ODN (Optical Distribution Network which consist of fiber cable, optical splitters, splice points, connectors, jumpers and various enclosures that house these elements). ODNs are specified by attenuation ranges they offer e.g. class A for 5 to 20 db, class B for 10 to 25 db and class C is for 15 to 30 db. The higher the attenuation allowed, the longer the potential distance and higher the split ratio that can be supported.

7. ODN TOPOLOGIES

7.1 Centralized Splitter Topology

In a centralized architecture, the splitters are all located in the primary flexibility point. The primary flexibility point is the ODN element where the feeder plant and distribution plant are cross connected. As shown in the figure 8, the distribution fiber cable includes a separate fiber for each drop. As the distribution fiber passes by a group of houses (e.g. a group of four homes), a drop box is used to allow access to the fibers serving the homes in that group. The rest of the fibers remain unbroken and continue down the distribution fiber cable run.

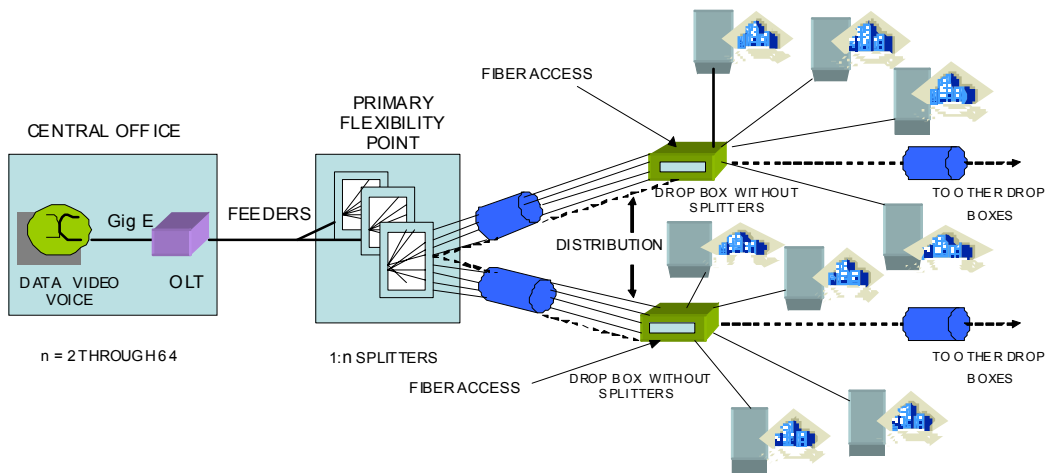


FIG. 5 CENTRALIZED SPLITTER TOPOLOGY

The centralized splitter scheme can be viewed as more future proof because it uses direct fiber links from the primary flexibility point to the customers and enables technologies, such as: WDM-PON (wavelength division multiplexing PON).

7.2 Distributed Splitter Topology

Instead of locating all the splitters at a primary point, it is possible to have a splitter in multiple points in a cascading fashion. Figure 6 shows how the splitter fiber can be split 1:16 ways using splitters located in the primary flexibility point. Each one of the branch fibers in the distribution cable can be further split 1:4 ways in the drop box. Only one fiber is needed to serve a group of homes, instead of dedicated fibers for each home as in the centralized model. The single fiber is split and cross connected to a drop cable for each home at the drop box.

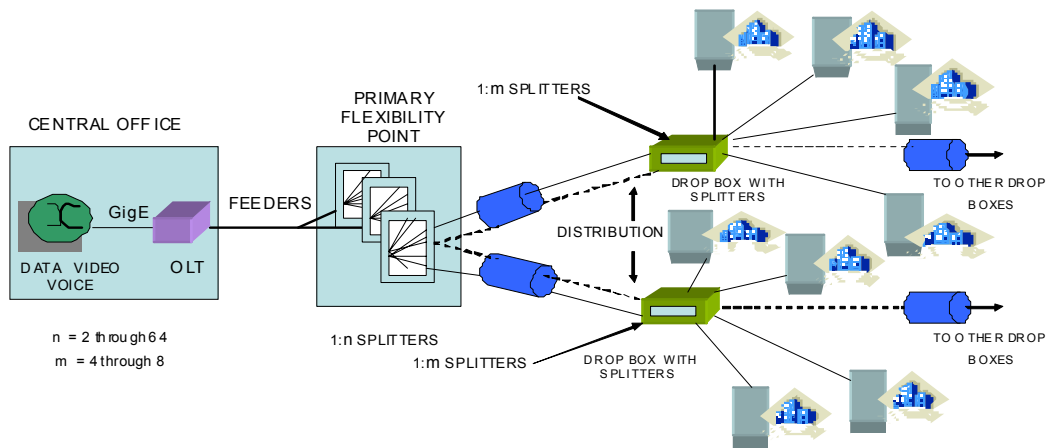


FIG. 6 DISTRIBUTED SPLITTER TOPOLOGY

In some deployment situations (particularly with RF overlay) where high transmit launch is required because of loop length; a distributed model offers some advantages by reducing the effect of stimulated brillouin scattering (SBS). In this case, the first stage splitters can be located in the CO and can immediately reduce the power level, thus avoiding any possible SBS effect. SBS can be also addressed by using SBS suppression technique at the transmitters that can increases the SBS threshold and allow higher launch power. Also, it is possible to select suitable optical fiber which allows significant higher launch power. In either centralized or distributed cases, however, using a higher split ratio of 1:64 provides significant saving in the out side plant as well as in the CO electronics and passive connectivity.

In the 'first mile' point to multipoint (PtMP) network, there are several topologies suitable for the access network, including tree, tree and branch, ring or bus topology (See Fig 7) using 1:2 optical tap couplers and 1:N optical splitters, PONs can be flexibly deployed in any of these topologies.

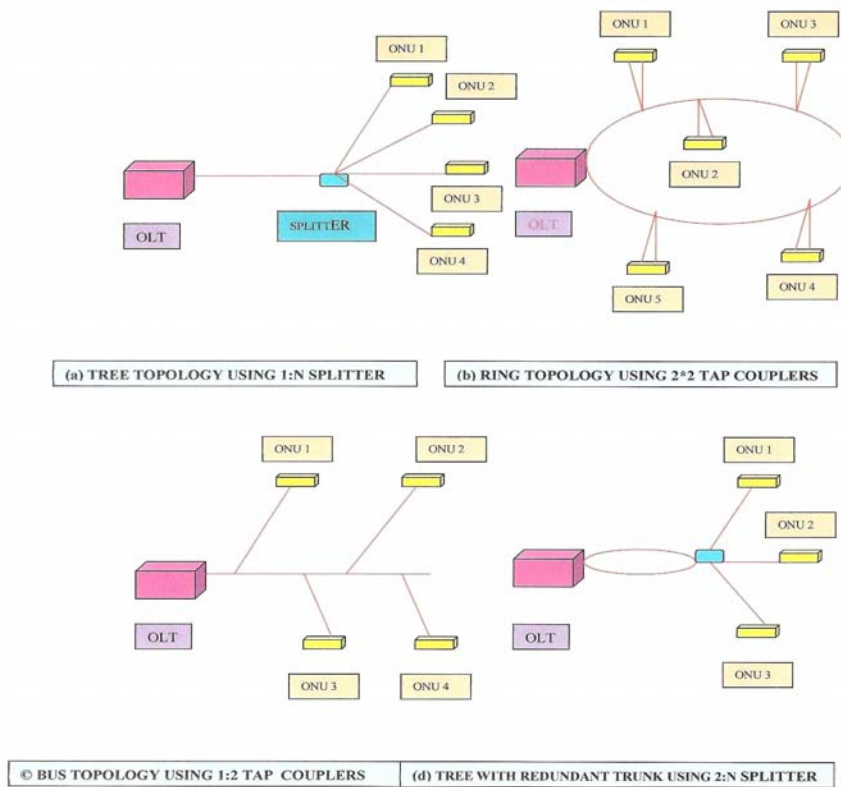


Figure 7

8. REMOTE OLT FOR LONGER LOOPS

While most loops around the world are much shorter than 20 Kilometers distance, there are still situations where the distance required is significantly longer. In these situations, the best option is to locate the OLT in remote cabinet as shown in Fig 8. The OLT hardware must be able to operate normally over the extended temperature range of -40°C to $+65^{\circ}\text{C}$ required for out door deployment. The distance between the remote cabinet and the CO is limited by the transport mechanism chosen and the type of optical interfaces used in the OLT.

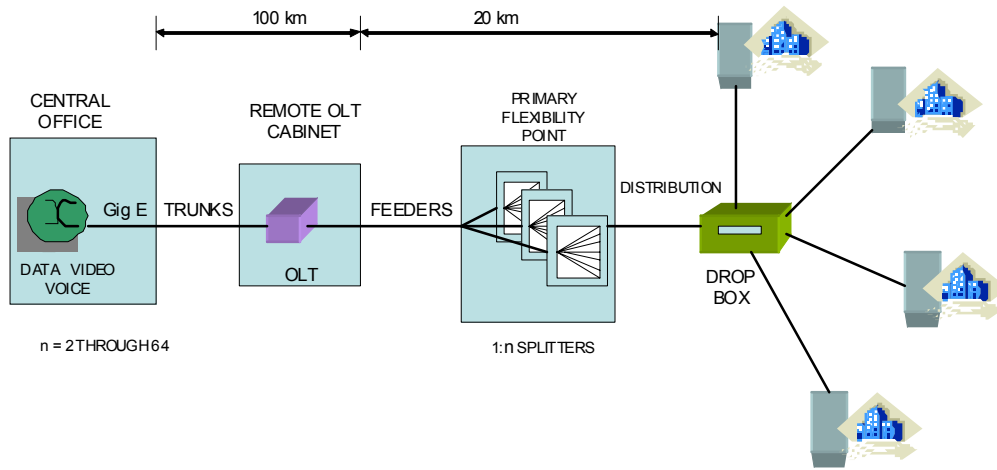


FIG. 8 OLT IN OUTSIDE PLANT CABINET

9. NET WORK AVAILABILITY: REDUNDANCY AND PROTECTION SWITCHING

Different protection architecture has been specified in the BPON standards by ITU-T, based on principles similar to those for high-speed core networks.

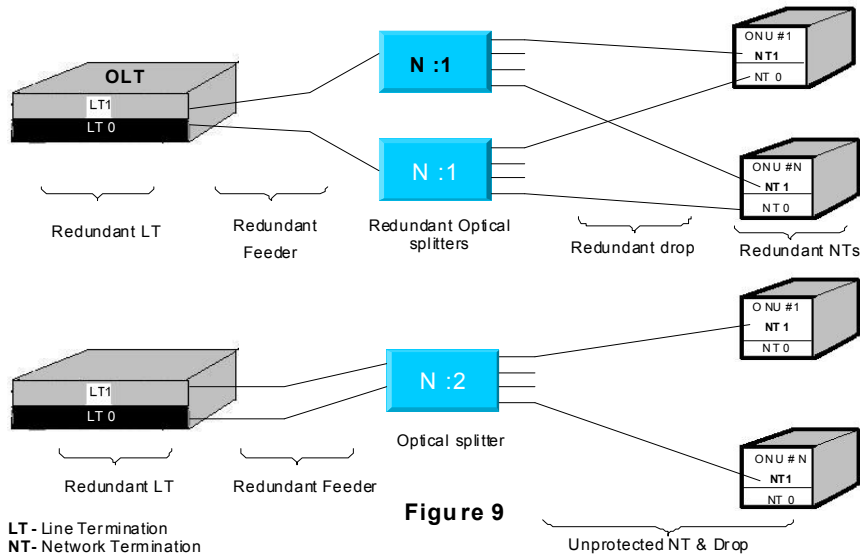


Figure 9
 Redundant PON Configuration: Full Redundancy (Type 'C' top)
 OLT & Root Redundancy (Type 'B' bottom)

The most secure way to protect the network especially for mission critical applications is by duplicating each optical transceiver, each splitter and each fiber section (Type C in Figure 9). For ordinary user, a reduced redundancy that protects the feeder section of the PON, but not the final drop section, would be sufficient (Type B in Figure 9).

9.1 The advantages of using PONs in subscriber access network are numerous and are as follows:

- (a) PONs allows for long reach between CO and customer premises, operating at distances over 20 Km.
- (b) PONs minimizes fiber deployment in both the CO and the local loop.
- (c) PONs provides higher bandwidth due to deeper fiber penetration, offering gigabit-per-second (Gbps) solutions.
- (d) Operating in the downstream as a broadcast network. PONs allow for video broadcasting either as IP video or analog video.
- (e) PONs eliminate the necessity of installing active electronic equipments e.g. L2 & L3 switches, Add-drop multiplexers (ADMs), Digital Cross Connects (DCCs), Routers etc. thus avoiding the gruesome task of maintaining these equipments and providing power to them i.e. there will be no requirement of DG Sets, UPS and battery banks. Instead of active devices PONs will employ OLT at CO and ONUs at user locations and outside plant will use only the optical fiber and small passive optical splitters/couplers that are simpler, easier to maintain and longer lived than active components.
- (f) Being optically transparent end to end PONs allow upgrades to higher bit rates or additional wavelength.
- (g) As far as ATM technology is concerned the cost of ATM switches and network cards are roughly eight times more expensive than Ethernet switches and network cards.
- (h) EPON's network electronic element such as OLT and ONU can have a life cycle of at least seven years or more, the PON that connects the electronics can last more than 30 years. Once the fiber network is properly installed, it can be used to deliver virtually unlimited amounts of bandwidth by upgrading or changing the electronics.

9.2 In a typical example optical line terminal (OLT) provide a direct optical interface to the Ethernet/IP network core and have built in L2/L3 switching and routing functionalities. Typically one OLT can support upto 8 PON links, each delivering 1 Gbps of shared bandwidth between upto 64 subscribers, serving a maximum of 512 subscribers from a single compact chassis. Typical power consumption of an OLT is about 100 watts. On the other end ONU which is installed at customer premises provides typically for 10/100 M-Base-T Ethernet points with advanced L2 functionality for data & IP TV video service delivery. The ONU can be configured and managed remotely by OLT housed at CO; ONU provides an uplink to the central office through its GEAPON port and downstream link to individual user through four Ethernet ports. It's a future proof solution enabling FTTx delivering voice, high bit rate data and video over a signal fiber. The typical power consumption is only 12 watt and typical operating temperature is from 0° to 40° C, humidity is from 5% to 90%. Optical loss budget is 29 dB and maximum reach is upto 20 Kms.

10. WDM-PON

One of the future PON access technology is WDM PON which offers the flexibility and high capacity point to point network, delivering very high bandwidth than the present TDM based PON deployments. It's scalable from 100 Mbps to 1Gbps and beyond and in the future can be amplified to long reach PONs. Figure 10 shows a future WDM PON deployment.

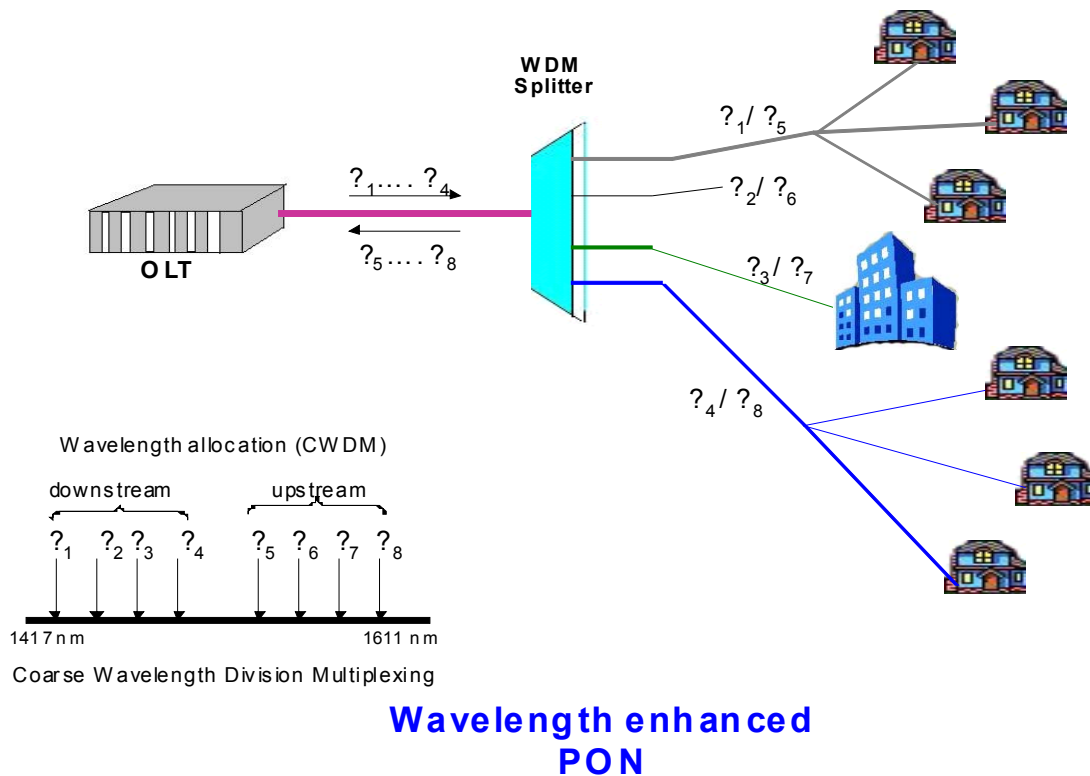


FIGURE 10

In WDM PON, a single wavelength redirected to an end user from central office (CO) to passive wavelength router located at outside plant (OSP). These wavelengths are in point to point fashion and are independent of each other. The wavelength router can route up to 32 lambdas' with future growth expected to 128 wavelengths. For long reach WDM PON access networks erbium doped fiber amplifiers can be used as pre amplifiers at splitter locations but the only constrains is that it operates in "C" band only hence its difficult to achieve DWDM PON. The answer to this is employment of "Quantum dot" amplifier technology which covers the entire fiber spectrum. One of the proposed WDM PON techniques is as follows:

10.1 Using Injection Seeded Optical transmitters

This approach involves remote seeding of the optical transmitter by another light source. In this technique, in addition to the usual downstream data signal, the ONTs receive an additional unmodulated optical seed signal at the wavelength designated for upstream transmission. These seed signals can be generated by an unmodulated broadband light source (BLS) by slicing its broad band spectrum with an AWG. The BLS can be an unmodulated low power Erbium doped fiber amplifier (EDFA) which is generating Amplitudes spontaneous emissions (ASE) as shown in Figure 11.

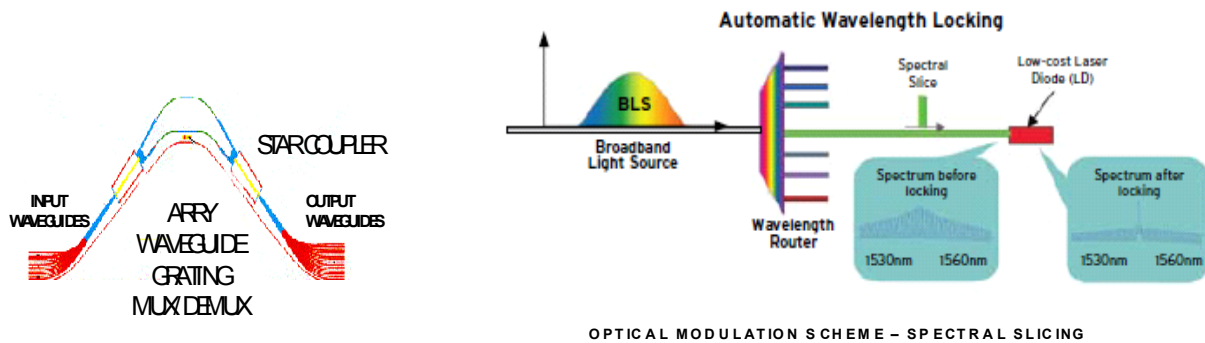


Figure 11

The ONTs receive this seed light, modulated their data onto it, amplify it and reflect it upstream towards the OLT. After injection locking signal, the FP lasers multimode spectrum is transformed into a quasi-single mode signal similar to DFB laser like signal which suitable for data transmission upstream and reduces mode partition noise and dispersion. Other than this there are several other techniques under considerations as follows:

- (a) Employment of Wavelength tuneable lasers as Distributed Bragg reflector (DBR) lasers offering wide range of tuning.
- (b) Wavelength – settable lasers having an array of 32 DFB lasers for selection of effective tuning range for 32 splits.
- (c) Slotted Fabry Perot (SFP) laser. These low cost lasers can be used both for tuneable single mode laser and injection locked laser.

11. ADVANCES IN OPTICAL FIBERS TRANSMISSION AND DEVELOPMENT OF INSTALLATION TECHNIQUES IN PON BASED OPTICAL NETWORKS

In future, metro and access networks will have peta bits per second transmission levels. To achieve such ultra high-speed rates research is focusing on development of Holey fiber technologies which can penetrate into ordinary household in the same way as metal cord which can be freely bent, folded, and tied and gives very low transmission loss..Figure 12 shows three types' holey fibers:

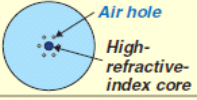
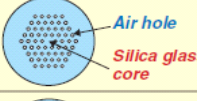


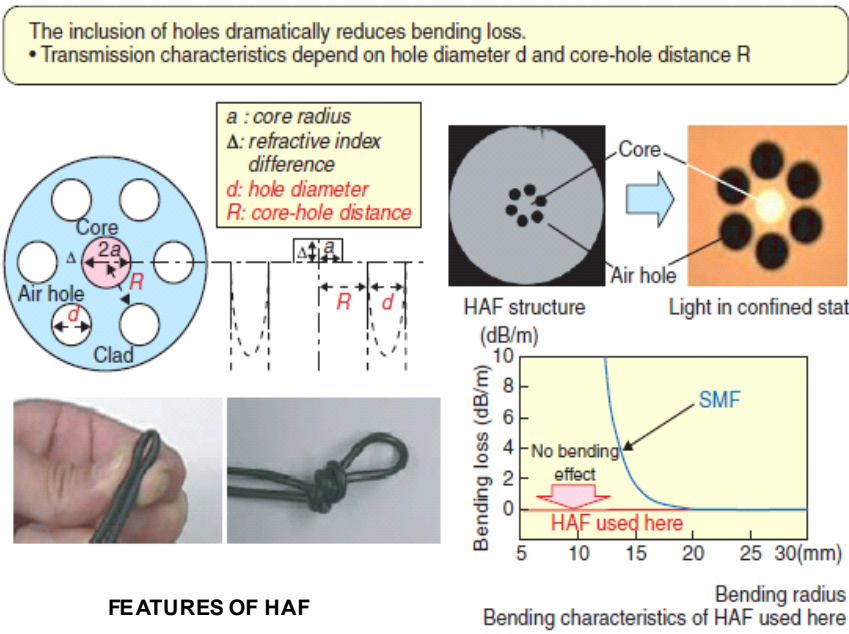
	Cross section and waveguiding principle	
Hole-assisted fiber (HAF)		Core: high-refractive-index glass Clad: hole-added glass Waveguiding principle: total reflection
Photonic crystal fiber (PCF)		Core: silica glass Clad: glass with holes added Waveguiding principle: total reflection
Photonic band-gap fiber (PBGF)		Core: hollow Clad: hole-added glass Waveguiding principle: Bragg reflection
Existing optical fiber (SMF)		Core: high-refractive-index glass Clad: glass Waveguiding principle: total reflection

FIGURE 12

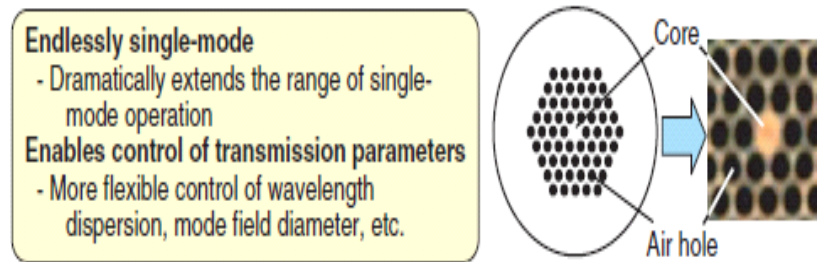
(a) Hole Assisted Fibers (HAF):

Such fibers have six holes arranged around high refractive index core. This type of structure results in a strong light confining effect and improves the bending loss characteristics dramatically. HAFs has almost no loss even for bending radius under 5 mm. Hence, HAF optical fibers cords can continue to operate even when it is bent, folded or bundled. Also, HAFs have same mechanical strength as of standard single mode fiber (SMF).



(b) Photonic Crystal Fibers (PCF)

These fibers convey light through a silica glass core surrounded by several dozen holes. In these fibers there is no high refractive index section; instead, light is confined at the centre of several dozen holes. Refer Figure 14. With PCF it is possible to alter the dispersion characteristics by modifying the size and arrangements of air holes to achieve flexible level of dispersion control. Another important feature of PCF is manufacture of such fiber with a single material resulting in the hope of achieving the theoretical minimum loss for silica glass.



PCF STRUCTURE

FIGURE 14

©Photonic Band Gap Fiber (PBGF):

It has hollow core surrounded by dozens of holes in the cladding and utilizes the principle of diffraction to propagate via air or through a solid. These fibers have limitless design possibilities of photonic band gap structure with the inherent low material dispersion of air which can result in creation of highly controllable dispersion profiles. Hence, these fibers have advantage of ultra low attenuation (Theoretical attenuation predicted is less than 0.001 db/km), low non linearity and limitless dispersion flexibility required in transmission fibers.

CONCLUSION

With the evolution of DWDM PON technologies it is possible to tap unlimited bandwidth of the optical fiber which is as high as 200 Tera Hz and have theoretical channel capacity of the order of 1000 Tera bits/sec considering Shannon's channel capacity formula. In future it will be possible to extend same unlimited bandwidth to the end users through All Optical Passive Optical Networks.

References

- [1] FARMER James O "Jim", Optical considerations in FTTH Networks, April 2007
- [2] Wagner Rich, Broad Band Access Network Options, Corning Inc., 22 April 2003.
- [3] Garvey Patrick, an Overview of ITU-T G657: Characteristics of bend insensitive, single mode optical fiber for access networks, April 2007.
- [4] Ethernet Passive Optical Networks, Web Profourum Tutorials, I E C.Org.
- [5] Meis David, How Invisible Should Your FTTH Network Be? Light wave.
- [6] Roycraft B, Mondal S K, Lambkin P, Engelestaedter P, Corbett B, Peters F H, Smyth F, Berry L, Peters, Phelen R, Donegan J F, Ellis A. D. ,White Paper.
- [7] Ethernet Passive Optical Network (EPON) A Tutorial, Metro Ethernet Forum, 2005.
- [8] "Nortel" Position Paper, Ethernet over WDM PON Technology Overview.
- [9] Karmer Glen, Mukherjee Biswanath, Mrislos Ariel., White Paper.
- [10] Shimizu Masatoshi, Optical Access Network Technology (Optical Media Technology) Towards Expansion of FTTH, Tsukuba Forum 25 Oct 2007.

AN INSIGHT INTO BLUETOOTH TECHNOLOGY

Professor Y P CHOPRA

Department of Electronics and Communication Engineering
Dronacharya College of Engineering, Gurgaon
Email : yashpal_chopra@yahoo.co.in

ABSTRACT

This paper intends to describe the basics of Bluetooth technology with its applications and benefits. Bluetooth technology is a low cost, low power and short range wireless radio communication technology for ad-hoc wireless communication of voice & data anywhere in the world. It has made a phenomenon growth during the last 10 years. It is an open specification, works in ISM band of 2.4 – 2.483 GHz. It is unlicensed. Today most of the electronic devices like PCs, mouse, keyboard, projector, phones, notebooks and palmtop computers are Bluetooth enabled. This technology is based on frequency hopping spread spectrum & Gaussian Frequency Shift Keying modulation is used. To avoid interference Adaptive frequency hopping is used. Protocols have been laid for initiating the communication between the devices. Maximum of 8 devices can be in an ad-hoc communication net called Piconet. One device acts as a master & other slave. Master & slave can reverse the roles. The Bluetooth chip just costs under \$3. During 2007-2008 more than 4 billion Bluetooth enabled products were marketed. Phones make maximum market. Security concerns have been taken care of by adoption of encryption techniques. The future of Bluetooth lies in enhancing the security of data transfer speed & avoidance of interference.

Keywords: Frequency Hopping Spread Spectrum, Adaptive Frequency Hopping, Piconet, Scatternet, Security

1. INTRODUCTION

Bluetooth is a wireless communication of low cost, low power, and short range radio technology. It offers a uniform structure for a wide range of devices to conduct and communicate with each other while maintaining high level of security. Its fundamental strength is the ability to simultaneously handle both data and voice transmission.

2. ORIGIN OF THE NAME

Bluetooth technology was originally developed by Ericsson, the Swedish phone manufacturer as a method to allow electronic devices such as mobile phone or a computer to use short radio waves to connect to each other without the use of cables or wires. Bluetooth was named after a late 10th century king Harald Bluetooth, king of Denmark and Norway (to 985 A.D.). He is known for his unification of previously warring tribes from Denmark (Including Scania present day Sweden) and Norway. Bluetooth likewise was intended to unify different technologies, such as computers and mobile phones [7].

3. BLUETOOTH LOGO

Bluetooth logo shown in fig. 1 merges the Nordic runes analogous to the modern latin H and B: *hagall and Bbjarkan from the younger runes forming a bind rune [1].

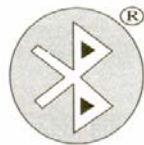


Figure 1: Bluetooth Logo

4. DEVICES OPERABLE

WITH BLUETOOTH

Fig. 2 shows the different types of devices that can be linked by wireless personal area network communication [2].



Figure 2: Devices in Bluetooth operation

This example shows that the computer can be located near the devices such as a keyboard, mouse, monitor, speakers, microphones and presentation projector. As these devices are brought within a few meters of each other, they automatically discover the availability and capabilities of other devices. If these devices have been set up to permit communication with other devices, the user will be able to use these devices as if they were directly connected to each other. As the devices are removed from the area or turned off, the option to use these devices will be disabled from the user.

5. RADIO SPECTRUM

Bluetooth devices operate in the 2.4GHz ISM (Industrial, Scientific and Medical) band. It is an unlicensed free band in most of the countries. Bandwidth is sufficient to define 79 1-MHz physical channels. Gaussian FSK modulation is used with a binary one represented by a positive frequency deviation and a binary zero represented by a negative frequency deviation from the center frequency, the minimum deviation is 115 KHz [5].

6. POWER OF TRANSMISSION

Bluetooth is power class dependent. The three power classes which cover effective ranges are shown in the table-1 below:

TABLE: 1 Bluetooth Power Transmission Classes

Class	Maximum permitted power mW/dBm	Range Approx.
Class-I	100mW(20 dBm)	~ 100 meters
Class-II	2.5 mW(4dBm)	~10 meters
Class-III	1mW(0 dBm)	~ 1 meters

It has been seen that in most cases the effective range of class 2 devices is extended if they connect to class 1 transmitter, compared to pure class network. This is accomplished by higher sensitivity and transmitter power of the class 1 device [7].

7. SPECIFICATIONS & FEATURES

Bluetooth specifications were developed in 1994 by Saap Haartsen (joined six months later by Swen Mattsen) who were working for Ericsson mobile platforms in Sweden. The specification was based on frequency hopping spread spectrum technology. The specifications were formalized by the Bluetooth Special Interest Group(SIG) formed on May20, 1998, Sony Ericsson, IBM, Intel, Toshiba and Nokia and later joined by many other companies. Various versions were developed and used. The current versions in used and those under development are given below.

7.1. Bluetooth 1.1:

- Ratified as IEEE standard 802.15-2002
- Added support for non-encrypted channel
- Received Signal Strengths Indicator(RSSI)

- Transmission speeds of 721Kbps.

7.2. Bluetooth 1.2:

This version is backwards compatible with 1.1 and major enhancements include:

- Faster connection and discovery.
- Use of Adaptive Frequency –Hopping Spread Spectrum (AFH) which improved resistance to RF interference by avoiding the use of crowded frequencies in the hopping sequence.
- Extended synchronous connections (E-SCO) which improved voice quality of links by allowing retransmissions of complete packets.

7.3. Bluetooth 2.0:

This version was adopted on 10 Nov 2004 and had following features:

- backward compatible with 1.1
- Induction of enhanced data rate of 3.0Mbps
- Three times faster transmission speed up to 10 times in certain cases(up to 2.1 Mbps)
- Lower power consumption through a reduced duty cycle.
- Simplification of multi-Unit scenario due to more available bandwidth.

7.4. Bluetooth 2.1:

This code named Lisbon was adopted by Bluetooth SIG on Aug1, 2007. It includes following features:

- fully backward compatible with 1.1
- Extended enquiry response:- provides more information during the enquiry procedure to allow better filtering of devices before connection. This information includes the name of the device, a list of services the device supports as well as other information
- Sniff subrating:- It reduces the power consumption when devices are with sniff's low power mode, especially on links with asymmetric data flows. Human interface devices (HID) are expected to benefit the most. With mouse and keyboard devices increasing the battery life by a factor of 3 to 10
- Secure simple securing

7.5. BLUETOOTH 3.0:

This version is code named Seattle. In addition to having features of 2.1 version it is planned to adopt Ultra Wide Band Radio technology. This will enhance data transfer rates of up to 480 Mbps while building on the very low power idle modes of Bluetooth.

8. TECHNOLOGIES

The key technologies used for transmission of data/text are Frequency Hopping Spread spectrum and Adaptive Frequency hopping.

8.1. FREQUENCY HOPPING:

Frequency Hopping spread spectrum is a process where a message or voice communications is sent on a radio channel that regularly changes frequency (hops) according to a predetermined code. The receiver of the message or voice information also receives on the same frequency using the same frequency hopping sequence. This technique provides firstly resistance to interference and multipath effects and secondly a form of multiple accesses among co-located devices in different piconets.

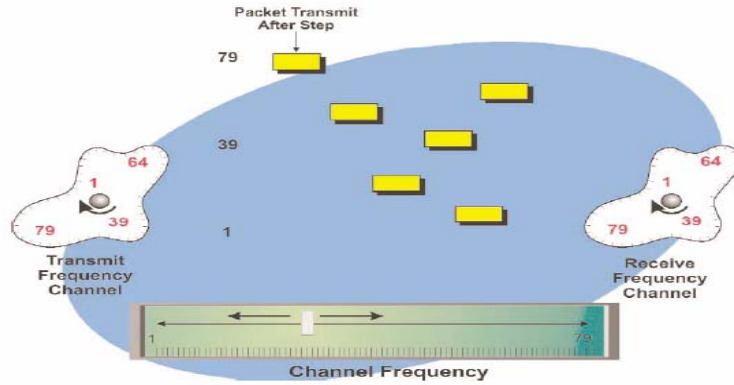


Fig. 3 above shows a simplified diagram of how Bluetooth system uses frequency hopping to transfer information(data) from a transmitter to a receiver using 79 communication channel each of 1 MHz bandwidth [2]. The hop rate is 1600 Kbps per second so that each physical channel is occupied for duration of 0.625ms. Each 0.625ms time period is referred to as slot and these are numbered sequentially. TDD discipline is used.

8.2. ADAPTIVE FREQUENCY HOPPING:

Bluetooth specification 1.2 introduced adaptive frequency(AFH) that can reduce the effects of interference between Bluetooth and other types of devices. The AFH adapts the access channel sharing method so that the transmission does not occur on channels that have significant interference.

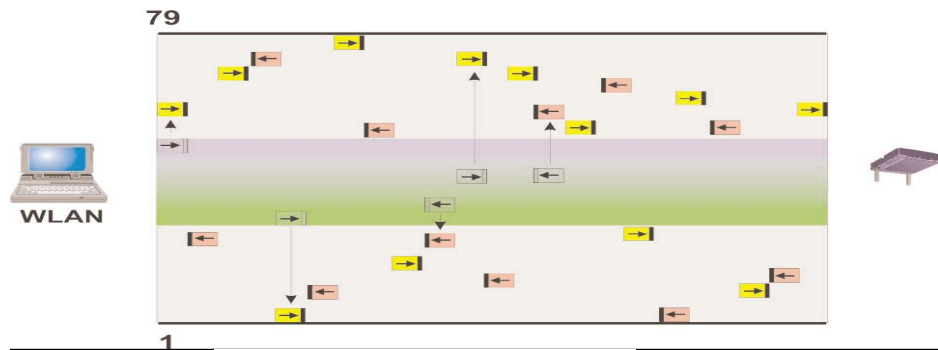


Figure 4: Adaptive Frequency Hopping

By using interference avoidance, devices that operate within the same frequency band and with in the same physical area can detect the presence of each other and adjust their communication system to reduce the amount of overlap caused by each other.

Fig 4 shows how blue tooth device changes its hopping pattern to avoid interface to and from other device that operate within its frequency band. This example share that after detecting the presence of a continuous signal being transmitted by the video camera in the 2.46 GHz band , the blue tooth device automatically changes its frequency hopping pattern to avoid transmitting on the frequency band that is used by video camera signal transmission.

This results in more packets being successfully sent by the Bluetooth device and reduced interface from the Bluetooth device to the transmitted video signal.

9. COMMUNICATION & CONNECTION

The basic unit of networking in Bluetooth is a piconet an adhoc network consisting of a master and from one to seven active slave devices(Fig5) .

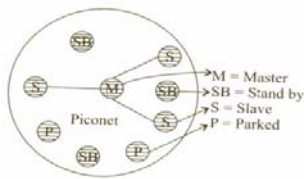


Fig.5 Piconet

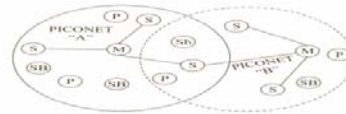


Fig.6 Scatternet

The master makes the determination of the channel (FH sequence) and phase (timing effect ie when to transmit) that shall be used by all device on this piconet. One master can interconnect with upto seven active slave devices because a three bit MAC address is used. Upto 255 further slave devices can be inactive and parked, which the master device can bring into active status at any time (stalling - 2002). At any given time data can be transferred between the master and one slave. The master rapidly switches from slave to slave in a round- robin fashion. Either device may switch the master slave role at any time.

Bluetooth specification allows connecting 2-or more piconets together to form a scatternet(Fig.6) with some device acting as a bridge by simultaneously playing the master role and the slave role in one piconet (Sanjeev kumar-2008). These devices have yet to come, though they were supposed to appear in 2007.

10. SETTING UP CONNECTION

Any Bluetooth device will transmit the following sets of information on demand.-device name, device class, list of devices and technical information for example device features manufacturer, Bluetooth specifications and clock offsets.

Any device can perform an enquiry to find other device to which to connect, and any device can be configured to respond to such inquires. However if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information about it if requested. Use of device services may require pairing on acceptance by its owner, but the connection itself can be started by any device and held until it goes out of range.

Every device has a unique 48-bit address. These addresses are generally not shown in inquires. Instead friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for device in lists of paired devices.

11. SECURITY CONCERNS OF BLUETOOTH

A security protocol prevents an eaves dropper from gaining access to confidential information exchange between two Bluetooth devices. For maintaining security at the link layer 4, different entities as under are used.

- a) 48 bit device (BD-ADDR) ie a unique address for each Bluetooth device.
- b) a 128 bit random number(RAND)
- c) A private device key of 128 bits for authentication.
- d) A private device key of 8 to 128 bit for encryption.
- e) Link level encryption and authentication.
- f) Personal identification number(pin for device access)
- g) These keys are not transmitted over wireless. other parameters are transmitted over wireless which in combination with certain information known to the device can generate the keys.

Number of steps are carried out in a sequential manner by 2 devices which have to implement authentication and encryption.

12. BLUETOOTH APPLICATIONS

In order to use Bluetooth, a device has to be compatible with certain Bluetooth profile. These define the possible applications and uses. These are as given below (Sanjeev Kumar-2008)

- a. Wireless control of and communication between a cell phone and hand free handset or car kit.(This was one of the earliest applications to become popular)
- b. Wireless networking between PCs in a confined space where little bandwidth is required.
- c. Wireless communication with PC input & output device the most common being the mouse, keyboard and printer.
- d. Transfer of contact details, calendar appointment and reminders between devices in OBEX.
- e. Replacement of traditional and serial communications in text equipment, GP services & medical equipment
- f. Transfer of files between devices via OBEX.
- g. For controls where infrared was traditionally used.
- h. Sending of small advertising hoardings to other, discoverable, Bluetooth device.
- i. Wireless control of some console- Nintendo's wii and Sony's play station3 both use Bluetooth technology for their wireless controllers.
- j. Sending commands and software to the LEGO Mindstorms NXT instead of infrared.

13. BENEFITS OF BLUETOOTH TECHNOLOGY

Bluetooth technology has come to stay and is being adopted more & more all over the globe. It offers the following benefits:

- a. Globally available free of cost
 - b. Easy to use: It is an adhoc technology that requires no fixed infrastructure & is simple to install.
 - c. Globally accepted specification: Bluetooth Special Interest Group formed by leading communication & software companies have ensured that all manufacture follow the same specifications in their products
 - d. Secure connection: It incorporates adaptive frequency hopping techniques and built in 128 bit energy phase and pin code authentication procedure. This ensures that security is maintained between the two Bluetooth devices in communication with each other.
 - e. A Bluetooth chip that enables the device to become Bluetooth enabled costs just under \$3. 4000 companies have now become members of Bluetooth SIG.

14. FUTURE OF BLUETOOTH TECHNOLOGY

Future enhancement will ensure much higher data transmission rates, more rapid signal acquisition, and better co-existence through interference avoidance

Multiple forms of modulation will be used to achieve data rates in excess of 2 to 10 bits per hertz.

CONCLUSION

Bluetooth technology has proved very effective in replacing cables for short range applications with very low power and that too at low cost. The Bluetooth chip costs just under Rs.150. It has made tremendous progress which can be guessed from the fact that over 4 billion Bluetooth enabled devices were marketed in 2008. Security concerns have been dually taken care of. The future of Bluetooth technology lies in enhancing the data speed rate over long ranges with minimum of interferences.

References

- [1]Kumar Sanjeev (2008) - Wireless & Mobile Communication
- [2]Luhar D.R. – Introduction to Bluetooth-Sigma Publishing
- [3]Muller (2001) - Bluetooth Demystified
- [4]Prabhu CSR & Reddi AP (2004)
Bluetooth technology & its Application with Java & J2
- [5]Stalling W (2008) - Wireless Communications & Network
- [6]Verma Brijesh (2008) - Wireless Communication
- [7]Bluetooth-Wikipedia the free encyclopedia

MOBILE IP AND CHALLENGES

Prof. (Mrs.) A.N.Mahajan
ECE Department
Dronacharya College of Engineering Gurgaon 123506
Email id anmahajan@yahoo.co.in

Abstract—

The recent years have witnessed a tremendous growth in the number of mobile internet users and the need for mobility support is indispensable for seamless internet connectivity. Mobile IP is a mobility support protocol that supports roaming across multiple Access Points without having to re-establish the end to end connection. In this paper, we take the position that despite several challenges that Mobile IP faces, it would turn out to be the protocol for supporting mobility in the future. We support our claim by analyzing the factors that would influence the widespread adoption of Mobile IP and we go further to discuss the counter claims in an effort to convince the reader that the advantages of Mobile IP outweigh its disadvantages.

I. INTRODUCTION

With the increase in popularity of the Vehicular Networking research and the resistance in the internet community to developing a radically different networking stack, there is a need for supporting highly mobile clients using the existing TCP/IP protocol stack. In the current implementation of wireless networks, when a node moves from one access point to another access point, it re-establishes the connection every time with a different IP address. This increases the cost of the network and also provides an interrupted service.

The necessity for uninterrupted communication when the mobile device moves from one location to another calls for a new technology. This kind of communication can be efficiently implemented using Mobile IP. Mobile IP, is an extension to standard Internet Protocol proposed by the Internet Engineering Task Force(IETF). It maintains the same IP address even when the host node moves from one network to the other. Hence with the implementation of Mobile IP it is possible to have a continuous connectivity with the network irrespective of the location of the host node. In my opinion, Mobile IP will be successful in the future as it has several notable features like no geographical limitation, no physical connectivity required, supports security, no modifications for the current IP address. The main factors that influence the need for Mobile IP are mobility support, increased number of mobile users.

- Standardization, uses the current IP Protocol
- Inter-Operability, can be used across different service providers.
- Alternative technologies, lack of proper alternatives other than Mobile IP
- IPv4 availability, limited availability of IPv4 address necessitates the need for Mobile IP
- Improved security, while registering with the home agent Mobile IP could be extended. Mobile IP could be extended to encompass all the technologies for seamless mobility if the following issues are resolved. These are
 - Security Issues
 - Triangulation Problems
 - Reliability Issues
 - Latency Issues

This paper describes the working of Mobile IP in section II, addresses the factors that influence the need for Mobile IP in section III and the issues to be resolved for successfully implementing Mobile IP in section IV and the section V of the paper has the conclusion.

1.1. BACKGROUND

It is necessary to be familiar with few terminologies before understanding the working of Mobile IP.

Mobile Node (MN): This corresponds to the node which moves from the home network to the foreign network. This node is assigned a permanent IP address to which the packets are always sent. The packets that are sent from other nodes to the mobile node will always be destined to its home IP address.

Home Network (HN): This is the network to which the mobile node is permanently connected. This subnet corresponds to the home address of the mobile node as well as home agent.

Home Agent (HA): The Home Agent forwards the packets to the mobile node that are destined for it. When the mobile node is in foreign network then it is the responsibility of the home agent to forward the packets that are destined to the mobile node to the foreign agent

Foreign Network (FN): This is the network to which the mobile node attaches itself after moving from the home network.

Foreign Agent (FA): Foreign Agent is a router located in the foreign network to which the mobile node is attached. It is configured to receive and forward the packets that are destined to the mobile node when the mobile node has a foreign agent care of address. While using collocated care of address, this foreign agent is used as a default router or for registering with the foreign network.

Care-of-Address (COA): This is the address that the mobile node uses for communication when it is not present in its home network. This can either be foreign agent care-of-address or a collocated care-of-address.

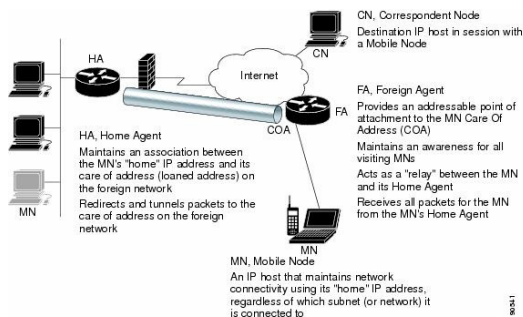
- Foreign Agent Care-of-Address (FA COA): The mobile node uses foreign agent's IP address as its care-of-address

- Collocated Care-of-Address (CO COA): The network interface of the mobile node is temporarily assigned an IP number on the foreign network.

Correspondent Node (CN): It is the node which communicates with the mobile node. This node can be located in any network and routes the packets to the home network of the mobile node.

Tunneling: The process of encapsulating an IP packet within another IP packet in order to forward the packets to some other place other than the address that is specified in the original destination field. When a mobile node is away from its home network, the packets that are sent to the home agent have to be directed to the mobile node care of address, for this purpose it is necessary to encapsulate the IP packet with new source and the destination IP address. The path that is followed by this encapsulated IP packet is called tunnel.

Fig. 1. Architecture of Mobile IP



For the Mobile IP to work effectively the three important entities that are to be altered are mobile node, home agent and foreign agent when the mobile node uses foreign agent care-of-address. If collocated care-of-address is used, then home agent is alone modified. It is preferred to have foreign agent type of care-of-address in IPv4 because of its limited address space.

As shown in the figure 1 when the mobile node moves from its Home Network, it has to get connected to a foreign network. There are two ways of finding agents when the mobile node is away from the home network. The first is by selecting an agent from among those periodically advertised, and the second is by sending out a periodic solicitation until it receives a response from a mobility agent. The mobile node thus gets its care-of-address associated with its foreign agent. After receiving the care-of-address, the mobile node has to register this address with the home agent. As the correspondent node sends packets to the mobile node, the packets are will be forwarded to the home network. On the reception of the packets, the Home Agent encapsulates these packets within another packet with the source IP address as Home Agent address and the destination IP address as Foreign Agent care-of-address and forwards it to the Foreign Agent. Using collocated are-of-address, the Foreign Agent is responsible for unmarshalling the tunnelled packets and sending it to the mobile node. Also it is responsible for sending the packets from the mobile node to correspondent node and to the home

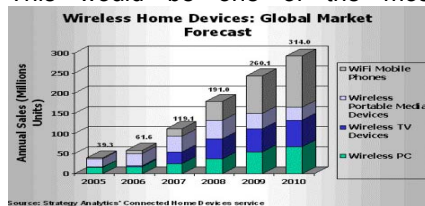
agent. On the other hand, with foreign agent care-of-address, the mobile node is directly connected to the foreign network.

1.2. THE NEED FOR MOBILE IP

Though the growth of Mobile IP was slow compared to the Wireless LAN, the need for Mobile IP is increasing rapidly.

2 Mobility Support

Figure 2 plots the forecasted number of mobile devices in the year 2010. We can see that the forecasted number of mobile devices is predicted to go up by 314% for the year 2010. This increase in turn translates to increased number of mobile devices and thus increased need for mobility support. This would be one of the most compelling reasons for the deployment of Mobile IP



3. Standardization

The way the Internet Protocol, the protocol that connects the networks of today's Internet, routes packets to their destinations according to IP addresses. All the devices like Desktops, Laptop's, PDAs, iPhones are all assigned an IP address. Mobile IP also uses the standard TCP/IP protocol suite. So any device that supports IP can also support Mobile IP. Mobile IP does not drop the network prefix of the IP address of the node, which is critical to the proper routing of packets throughout the Internet. There are several advantages of using TCP/IP stack in Mobile IP.

3.1 Failure recovery: If there is a failure in a particular sub network, then it is still possible to establish the connection with the remaining networks.

3.2 Adding Networks: It is possible to add more access points without changing the existing design.

3.3 Platform independent: The standard TCP/IP protocol is platform independent and hence this makes it possible for Mobile IP to be implemented in different devices like cellular phones, iPhones, Laptops with Macintosh, Windows, Linux etc.

3.4 Reduced Cost : There is a great reduction in cost because maintenance becomes simpler and any error handling can be performed easily. Also modifications in the existing network can be implemented without much overhead in cost

4. Inter-Operability

There are various service providers available and with different network connections. With a heterogeneous network there is need for a standard protocol to be used with all these providers for an effective communication. This scenario can be explained better with the mobile phone services. For mobile phones there are various service providers available and also there is a need for connecting the call from one service to another service. For instance a node from a PSTN network to a mobile node of an ATNT network or an ATNT mobile node to a Verizon mobile node. Mobile IP allows this kind of interoperability to provide a good communication between all the nodes that are connected to different networks across the world.

5. Alternative Technologies

In order to support mobile communication without disconnecting from the network there are only two possible solutions that are available apart from Mobile IP. These are as follows :

- 1) the node must change its IP address whenever it changes its point of attachment.
- 2) host-specific routes must be propagated throughout much of the Internet routing fabric. These alternatives are not widely accepted because in the first method it is not possible to maintain the connection in transport layer and higher layers of the protocol suite and in the second method there will be scalability problems with increase in the number of wireless devices. Therefore Mobile IP would turn out to be the quick fix at least in the next decade for providing seamless mobility support for the end-users.

6. IPv4 Availability

Just as IPv4 has become the de facto standard for networked communication, the cost of embedding substantial computing power into handheld devices has plummeted. As a result, the using a temporary IP for mobile communication uses exhaustive number of IPv4 addresses. The number of IPv4 address can be efficiently used by using Mobile IP, in which each host is assigned a permanent IP address.

7. Improved Security

Security problems are considered when registering to the home agent. All registration messages between a Mobile Node and Home Agent are required to contain the Mobile-Home Authentication Extension (MHAE). The integrity of the registration messages is protected by a preshared 128-bit key between a Mobile Node and Home Agent. The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity. Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a Mobile Node and Foreign Agent and between a Foreign Agent and Home Agent, respectively. Replay protection uses the identification field in the registration messages as a timestamp and sequence number. The Home Agent returns its time stamp to synchronize the Mobile Node for registration.

8. THE ISSUES WITH MOBILE IP

There are some limitations with the Mobile IP and hence one could argue that the Mobile IP cannot be successful. This section explains the challenges face by Mobile IP and solutions are proposed for the same.

8.1. Security Issues

The major security issues and their corresponding solutions that are concerned with the Mobile IP are presented below.

9. Denial Of Service Attacks

The Denial of Service Attacks can be caused when an attacker sends a tremendous number of packets to a host (e.g., Web server) that brings the hosts CPU to its knees. In the meantime, no useful information can be exchanged with the host while it is processing all of nuisance packets. It can also be cause when an intruder somehow interferes with the packets that are flowing between two nodes on the network or when a malicious host generates bogus registration request specifying his own IP address as the care-of address for a mobile node All packets sent by correspondent nodes would be tunneled by the nodes home agent to the malicious host. The possible prevention method for this is to require cryptographically strong authentication in all registration messages exchanged by a mobile node and its home agent. Also Mobile IP by default supports MD5 Message-Digest Algorithm that provides secret-key authentication and integrity checking. The solution is either by the use of Link-Layer Encryption where it is assumed that key management for the encryption is performed without disclosing the keys to any unauthorized party or the use of End-to-End Encryption. Session- Stealing, this type of attack involves transmitting various nuisance packets to prevent the legitimate node from recognizing that the session has been captured. The attack can be prevented from the above actions, end-to-end and link layer encryptions. Insider Attack This usually involve a disgruntle employee gaining access to sensitive data and forwarding it to a competitor. The solution for this is to enforce strict control for who can access what data, to use a strong authentication of users an computers and to encrypt all data transfer on an end-to-end basis between the ultimate source an ultimate destination machines to prevent eavesdropping. In order to prevent, the Identification field is generated is a such a way that it allows the home agent to determine the next value. In this way, the malicious host is thwarted because the Identification field in his stored Registration Request will be recognized as being out of date by the home agent. Other Attacks The malicious host can connect to the network jack and figure out the IP address to use, and finally tries to break to the other hosts on the network. He can find out the network prefix that has been assigned to the link on which the network jack is connected. Also an intruder can guess a host number to use, which combined with the network-prefix gives him an IP address to use on the current link or else proceeds trying to break into the hosts on the network guessing user-name/password pairs. To prevent such attacks all publicly accessible network jack must connect to foreign agent that demands any nodes on the link to be registered. Otherwise, remove all non-mobile nodes from the link and require all legitimate mobile nodes to use link layer encryption.

9.1. Triangulation Problem

The basic idea behind triangle routing is that a mobile node wants to send packets to another node that is on the same network. The receiver node happens to be far away from the mobile nodes home network. Then the sending node addresses all the packets to the home network. They pass through the Internet to reach the home agent and then tunnels them back across the Internet to reach the foreign agent. Triangle routing problem delays the delivery of the datagrams to mobile nodes and places an unnecessary burden on networks and routers along their paths through the Internet. This all can be improved by techniques in the route optimization, delivery of packets directly to care of address from a correspondent node without having to detour through the home network. The sending node should be told the care-of address of the mobile node. The sending node makes its own tunnel to the foreign agent, an optimization of the process that was a fore mentioned. In the case where the sender contains the required software to learn the care-of address and is able to create its own tunnel, then the route is optimized. If not, another route must obviously be taken. A home agent finds out that a packet is being sent from one of the mobile nodes that it supports. From here, the home agent is aware that the sender is not using the optimal route. It then sends a binding update message back to the source as well as forwarding the packet back to the foreign agent. The source then uses this information, if proficient, to construct an entry in the binding cache. This binding cache is a book of mappings from mobile node addresses and care-of addresses. The next time this source has a packet to send to that mobile node, it will find the section in the cache and will tunnel the packet directly to the foreign agent.

9.2 Reliability Issues

The design of Mobile IP is founded on the premise that connections based on TCP should survive cell changes. However, opinion is not unanimous on the need for this feature. Many people believe that computer communications to laptop computers are sufficiently bursty that there is no need to increase the reliability of the connections supporting the communications. The analogy is made to fetching Web pages by selecting the appropriate URLs. If a transfer fails, people are used to trying again. This is tantamount to making the user responsible for the retransmission protocol and depends for its acceptability on a widespread perception that computers and the Internet cannot be trusted to do things right the first time. Naturally, such assumptions are strongly distasteful to many Internet protocol engineers. Nevertheless, the fact that products exhibiting this model are currently economically viable cannot be denied. Hopefully in the near future better engineering will counter this perception and increase the demand for Internet reliability.

10. CONCLUSION

Mobile IP which has a slow growth compared to the Wireless LAN seems to be a failure technology but Mobile IP has great potential. The increased user convenience and the reduced need for application awareness of mobility can be a major driving force for its adoption. It has been shown in this paper that even with the limitations that are present in the implementation of Mobile IP, there will be a higher need for Mobile IP in the future. Security needs are getting active attention and will benefit from the deployment efforts underway. There are works that are going on in this field to overcome the limitations that are currently present in Mobile IP. This paper has also discussed few of the challenges that are faced by the Mobile IP and solutions have been proposed for a successful deployment of Mobile IP in the future.

REFERENCES

- 1 Applicability statement for ip mobility support.
<http://www.rfc-editor.org/rfc/rfc2005.txt>.
- 2 Introduction to mobile ip [ip tunneling] - Cisco Systems.
- 3 Mobile communication – John Schiller

Nanoelectronics In Quantum Computers

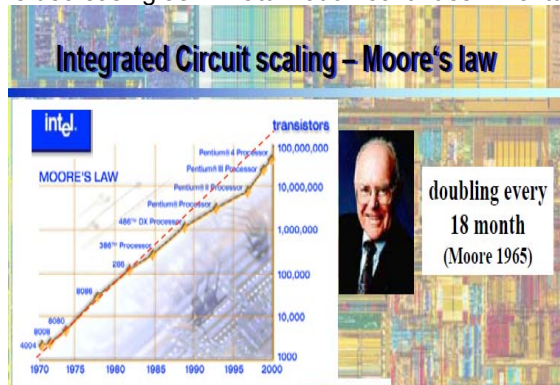
Abstract

Over the past forty years scientists have investigated and tried to understand unusual quantum phenomena, but is it possible that a new kind of computer can be designed based entirely on quantum principles. Nanoelectronics makes base for quantum computer. The extraordinary power of the quantum computer is a result of a phenomenon called quantum parallelism, a mechanism that enables multiple calculations to be performed simultaneously, which is the basic principle of Quantum computer.

Keywords Quantum properties,nanoelectronics,bottom-up,top-down approach.

Introduction

In the late 1960s, Gordon Moore, the co-founder of Intel Corporation, made a memorable observation that has since become known as Moore's Law. He noted that the number of transistors chip roughly doubled every 18 months. This trend has remained true for the past four decades. Following on from this law came the prediction that by the year 2015 the feature sizes of devices will become less than 0.1 μm . Another consequence of Moore's Law is that as transistors get smaller they contain fewer and fewer electrons. Figure 8.1b shows how the number of electrons used to store one 'bit' of information is decreasing as miniaturization continues. Eventually we will reach a limit of one electron per 'bit'.



Nanoelectronics is the emerging field of building electronic devices at the atomic level to harness these small-scale 'quantum' properties of nature.

This is about the development of nanoelectronics and the tools required to observe and manipulate atoms and applications.

There are essentially two different approaches to creating very small devices.

1. Firstly there is the increasingly precise 'top-down' approach of finely machining and finishing the materials, which can be compared to a sculptor carving a statue out of marble.
2. The second approach is called the 'bottom-up' approach, where individual atoms and molecules are placed or are self-assembled precisely where they are needed. This is a close approximation to understanding how nature works. For many years chemists have been using the 'bottom-up' approach to synthesis molecules to produce millions of different molecular structures. Nanotechnology researches have been developing a set of techniques known as molecular self-assembly and produced nanoelectronic components, such as molecular switches made a few molecules, and molecular wires and molecular transistor.

What will nanoelectronics do for us?

During the past 50 years due invention has changed many aspects of modern life, and all modern appliances such as radios, washing machines, computers, mobile phones, television and calculators utilize transistors built at the micron scale.

We are in the midst of the Information Age, where information is all and the ability to rapidly process and interpret huge amounts of data is paramount. It is clear that nanoelectronics will assist in processing and transferring huge amounts of data. It is also certain that the computer and hence nanoelectronics will be essential in the developing Genetic Age or other forthcoming ages.

Nanotechnology offers the possibility of building a new generation of electronic devices in which electrons are confined quantum mechanically to provide superior device performance. The high electron mobility transistor (HEMT) and the quantum well laser are just two examples where quantum mechanical confinement has led to better performance in terms of efficiency, speed, noise reduction and enhanced reliability. These devices are considered the first generation of quantum semiconductor devices that operate with quantum electronic states. They are used in the widespread commercial exploitation of communication and computational systems. We are now approaching. Over the past two decades discrete nanoelectronic devices have been proposed and successfully demonstrated in research laboratories, such as resonant tunneling diodes (RTD), single electron transistors (SETs) and a broad class of devices comprised of quantum dots and molecules

One of the ultimate quantum electronic systems is a computer that operates purely on quantum principle using individual atoms or molecules. Even a small so-called '**quantum computer**' has been predicted to be so powerful that it can perform certain calculations that all the computers on the universe.

Quantum electronic devices

Single electron transistors:

If we fabricate a small region or dot in a semiconductor that is no greater than 10-1000 nm in diameter, small dimensions of the dot means that the energy level spacings are correspondingly large. The electrons occupy discrete quantum levels similar to atomic orbital in atoms, and have a discrete excitation spectrum. In a similar way as the ionization energy, there is a corresponding energy to add or remove an electron from the dot called the 'charging energy – E_c '.

SETs have been fabricated using scanning tunneling microscopy and atomic force microscopy at sub-10 nm dimensions and this has produced single electron effects at room temperature force microscopy image of this devices showing the source and drain made from oxidized titanium (light regions) surrounding a metallic titanium island (dark) of dimensions 30 nm², here the gate is underneath the island rather than at the side . The island is so small that it can only hold a few free electrons. By applying a voltage to the underlying gate the potential barrier to an electron hopping onto the island decreases so that one electron at a time can flow through the island. If the gate voltage is further increased so that the potential on the island is lowered by E_c , then this second electron can now tunnel onto the island.

Thus, gradually increasing the voltage, V_g , causes a series of periodic oscillations in the source-drain current (or conductance G (e^2/h)), with each peak corresponding to the equilibrium number of electrons on the island increasing by one. These oscillations are a characteristics signature of single-electron Coulomb blockade effects. SETs are extremely sensitive to small changes in their local electrostatic environment.

Carbon nanotube transistor:

Nanotubes offer many exciting applications, from microscopic wires to diodes and transistors. Tolerant to extreme temperatures can pass current almost without any resistance. They are also smaller than any wires in today's electronics. Valuable property is that, like semiconductors, they can be made either insulating or a type of nanotube that is a semiconductor about one nanometer in diameter is laid across two electrodes a source and drain – on a silicon surface. Applying a voltage to the silicon substrate induces carriers onto the nanotube to turn the transistor on. Nanotubes, as the name suggests, are as narrow as the double stranded DNA molecule that carries our genetic information. So

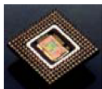
arranging nanotubes into electronic circuitry could allow miniaturization by a factor of about 100 over the current limit.

Quantum Information and Quantum Computers

mainstream electronics

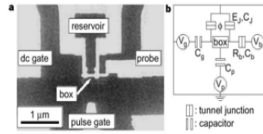


top-down
silicon



radically new concepts ...

Quantum Computer



Solid-state qubits under control ?

QUANTUM COMPUTING:
DREAM OR NIGHTMARE?

„The weirdest computer of all“ (The Economist)



Over the past 40 years scientists have investigated and tried to understand unusual quantum phenomena, but is it possible that a new kind of computer can be designed based entirely on quantum principles. The notion of a quantum computer has existed since 1982, when the famous physicist Richard Feynman outlined how such a device might operate. The extraordinary power of the quantum computer is a result of a phenomenon called quantum parallelism, a mechanism that enables multiple calculations to be performed simultaneously. This is in stark contrast to a classical computer which can only perform operations one at a time, albeit very quickly. The field of quantum computation has remained a largely academic one until the 1990s, when it was shown that for certain key problems quantum computers could, in principle, out-perform their classical counterparts. Since then research groups around the world have been racing to pioneer a practical system. However, trying to construct a quantum computer, at the atomic scale, is far from easy, since it requires the ability to manipulate and control single atoms.

How Is A Quantum Computer Different To A Classical Computer ?

Whilst it may appear that computers can understand us, in reality they understand nothing at all. All computers can do is recognize two distinct physical states produced by either electricity, magnetic polarity or reflected light. Essentially they can understand when a switch is on or off. Indeed the ‘brain’ of the computer – the central processing unit – consists of several million tiny electronic switches called transistors. A computer therefore appears to understand information only because it contains so many transistors and operates at such phenomenal speeds, assembling its individual switches into patterns that are meaningful to us. Information is therefore represented by groups of on/ off switches to give us data. If we consider the writing on this page, the data is just the individual letters, which taken out of context mean nothing. A computer takes this meaningless data and groups it together into useful information, such as spreadsheets, graphs and reports.

In the computer world everything is a number. Letters are represented by a string of numbers. In a classical computer everything is represented by the state of the computer’s electrical switches and hence there are only two possible states, on and off, giving us the binary number system. The smallest possible unit of data is stored as a ‘bit’ – either a 0 or a 1. A group of eight bits is called a byte, an important unit since there are enough different 8-bit combinations to represent all the characters on a keyboard, including all the letters, numbers, punctuation marks and so on. The way in which the numbers are arranged to represent the letters of the alphabet is called a text code, and very early on programmers realized they needed a standard code that everyone could agree on. This standard code allows any programmer to use the same combinations of numbers to represent individual pieces of data. The three most popular codes are EBCDIC, ASCII and Unicode.

The processing that takes place within the computer therefore involves either comparing numbers or carrying out mathematical calculations. The computer’s flexibility comes from being able to establish

order sequences of different operations and changing those sequences. The computer can perform two types of operations: arithmetic and logical. Arithmetic operations include addition, multiplication and division. Logical operations include comparison, such as determining whether one number is greater than or less than another number. Data is input into the computer, a program is written to perform operations on these numbers and then the result is read out.

In a quantum computer the rules are changed. Not only can a quantum bit (referred to as the 'qubit') exist in the classical 0 and 1 states, but it can also be in a 'superposition' state, where it is both 0 and 1 at the same time. If every qubit in a quantum computer is in a superposition state then the computer can be thought of as being in every possible state that those qubits can represent.

Another way of understanding the difference between a quantum and classical computer is if we consider a register of three classical bits. Using 0s and 1s in binary code it is possible to represent any number between 0 and 7 at any one time (see Table) below.

Three classical bits registering numbers between 0 and 7

Bit1	Bit2	Bit3	represented no.
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

Now consider a register of three qubits. If every qubit in a quantum computer is either in a 0 or 1 state then the three-qubit in a quantum computer is either in a 0 or 1 state then the three-qubit register stores any one of the 8 distinct possibilities and is identical to the classical computer. However if one of the qubits is in a superposition of both 0 and 1, then the register can store two distinct possibilities at the same time. If each qubit is in a superposition state this quantum register can be storing all of the number from 0 to 7 simultaneously (see Table below).

Three quantum bits (qubits) registering numbers between 0 and 7

Qubit1	Qubit2	Qubit3	represented no.
0	0	[0] [1]	0,1 simultaneously
0	1	[0] [1]	2,3 simultaneously
1	0	[0] [1]	4,5 simultaneously
1	1	[0] [1]	6,7 simultaneously
0	[0] [1]	[0] [1]	0,1,2,3 simultaneously
1	[0] [1]	[0] [1]	4,5,6,7 simultaneously
[0] [1]	[0] [1]	[0] [1]	0-7 simultaneously

The beauty of quantum mechanics is that these superposition states can be created and uncoupled afterwards. A processor that can use registers of qubits will in effect be able to perform calculations

using all possible values of the input registers simultaneously. This phenomenon is called quantum parallelism, and is the motivating force behind the research being carried out in quantum computing.

How Does A Quantum Computer Work?

Information comes in discrete chunks similar to the discreteness of energy levels in an atom. As discussed, in a classical computer this information is digital and is passed on as a series of bits. A quantum computer must match this discrete character of digital information to the strange discrete character of quantum mechanics. To do this a quantum system such as an atom can be used since this has discrete energy levels that could hold bits of information similar to transistors – in one energy state it can be 0 and in another energy state it can be 1. For a cluster of atoms to work as a computer it must also be possible to load information onto the system, process that information by means of simple logical manipulations and to read out the answer. Another way of saying this is that quantum systems must be able to read, write and do arithmetic.

Writing To An Idealized Atomic-Quantum Computer

One way is to excite atoms using laser light. We can consider the ground state of hydrogen atom as having energy, E_0 . If we want to write a 0 into this atom we do nothing. However if we want to write a 1 we can excite it from the ground state to an excited state, E_1 , using a pulse of laser light with an energy of $E_1 - E_0$. As an electron absorbs a photon it will gradually move from the ground state to the excited state. If the atom is already in the excited state the same pulse will tell it to emit a photon and go to the ground state. Therefore the pulse of light tells the atom to flip its qubit and is a method of information storage.

In a classic computer this would lead to errors since it can only exist in 0 or 1 state and we wouldn't be sure which state it would end up in. In the quantum world the atom is in a superposition state of both the 0 and 1 state with equal amplitudes; that is, the qubit is only flipped halfway.

Read From An Idealized Atomic-Quantum Computer

This is very similar to the writing process. For this we need a third energy level, E_2 , which is well separated from E_0 and E_1 . We now apply an energy pulse, $E_2 - E_1$ that is different to $E_1 - E_0$, and analyse the photon emitted. If the electron is originally in the state E_1 it will absorb this photon and be excited to the energy level E_2 – a higher, less stable state. As a result it will rapidly decay, emitting a photon of energy $E_2 - E_1$. If the electron is in the ground state nothing will happen since it is not the right energy to excite it to E_2 .

Quantum Computation

Classical computers are comprised of electronic circuits that contain many different components such as resistors, capacitors and transistors. Calculation are performed by repeating tasks, such as flipping a bit from one state to another, over and over at great speed. Flipping bit is equivalent to the logical operation called NOT where true 1 becomes false and false 0 becomes true 1.

How does this work in quantum computer? All we need is the ability to flip qubit and to be able to control a suitable non-linear interaction between them. Simple two bit quantum logic operations have already been performed with particle spins. The spin of a particle is an ideal qubit because it can take only one of two values – it can either be spinning in one direction with respect to magnetic field (1), or in the opposite direction (0). In a hydrogen atom both the proton and electron have a spin, so a single hydrogen atom in a magnetic field is thus a two – Qubit system. It is possible to flip the individual spin by using short bursts of high frequency radiations. The interaction between the electron and proton also makes it possible to perform non-linear operations, such as flip the proton spin only if the electron spin is 1.

The Power Of Quantum Computation

With only one qubit a quantum computer can already do things no classical computer can do. Take a single atom in a superposition state of 0 and 1. If we make it fluoresce to try and discover what state it is in, half the time it emit a photon (showing that it in the one state) and rest of the time no photon is emitted and the qubit is in 0 state. This mean that the bit is a random bit- we have produced a random number generator, something a classical computer cannot create. The real power, however, of quantum computation occurs with a many qubit system.

Power Of Classical Computer

Consider the problem of having a random phone number written on a piece of paper, but we don't know who the number belongs to. If we check the phone directory, a classical computer can help speed up the problem. The computer checks each number in the directory sequence, starting with the A's and working through to the Z's until it finds the number. The power of the computer is that it checks each number very quickly. If we wanted to increase the speed of finding the answer we could add another computer, getting no. to check from A-L and the other to check from M-Z. Adding one more computer means we have three computers, one checking from A-I, one from J-R and the last from S-Z. So adding another computer simply increases the power of the computation by one. Thus, in a classical system the power of this look-up system increases linearly with the number of computers used.

Power Of A Quantum Computer

Unlike a classical computer, each time we add a qubit to a quantum computer the power doubles. Consider a quantum bit or qubit as a coin. Unlike a classical coin, which can either land as head or tails when thrown, the entangled state of the qubit means that it can be both heads (H) and tails (T) at the same time (@). In the classical situation when we add a second coin there are HH, TT, HT and TH solutions, however when we add a second qubit there are another four solutions, H@, @H, @@, T@ and @T. It is this increase of computer power that drives the push for a practical quantum computer. It has been predicted that a 40-qubit computer could recreate in a little more than 100 steps, a calculation that would take a classical computer with a trillion bits several years to finish.

Conclusion

In a quantum computer the rules are changed from classical computing. Not only can a quantum bit exist in the classical 0 and 1 states but it can also be in a superposition state where it is both 0 and 1 at the same time. If every qubit in a quantum computer is in a superposition state then the computer can be thought of as being in a every possible state that those qubits can represent.

References

- [1]Melosh, N.; Boukai, Akram; Diana, Frederic; Gerardot, Brian; Badolato, Antonio; Petroff, Pierre & Heath, James R. (2003). "Ultrahigh density nanowire lattices and circuits".
- [2]Das, S.; Gates, A.J.; Abdu, H.A.; Rose, G.S.; Picconatto, C.A. & Ellenbogen, J.C. (2007). "Designs for Ultra-Tiny, Special-Purpose Nanoelectronic Circuits". IEEE Trans. On Circuits and Systems
- [3]Goicoechea, J.; Zamarreño, C.R.; Matiasa, I.R. & Arregui, F.J. (2007). "Minimizing the photobleaching of self-assembled multilayers for sensor applications".
- [4]Petty, M.C.; Bryce, M.R. & Bloor, D. (1995). An Introduction to Molecular Electronics.
- [5]Aviram, A.; Ratner, M. A. (1974). "Molecular Rectifier". Chemical Physics Letters
- [6]Aviram, A. (1988). "Molecules for memory, logic, and amplification". Journal of the American Chemical Society
- [7]Jensen, K.; Jensen, K.; Weldon, J.; Garcia, H. & Zettl A. (2007). "Nanotube Radio".

NETWORK SECURITY

Mrs.Dimple Saproo

Assistant Professor, Department of Electronics & Communication Engineering

Dronacharya College of Engineering, Gurgoan

Email d_saproo@indiatimes

ABSTRACT:

Network security is a very important and sensitive issue in today's scenario as in run to make the society paper free every organization is moving towards the centralised computer network systems. In such situations hiding important information from unauthorised agencies becomes very important to prevent various types of cyber and heinous crimes and in order to make the human life much safer. In this paper various types of insecure methods of data managements are shown and at the same time methods to secure the information are discussed with efficient examples.

Keywords: security, principles, vulnerabilities, environment threats, attacks

1. INTRODUCTION:

The term security means many things home security system, child physical security, national security, home security, computer security. The purpose of the computer security is to prevent the weakness from being exploited. Its objective is to protect the resources of your computer system

2. NEED OF SECURITY:

- \$10 M transferred out of one banking system.
- Loss of intellectual property -\$2M in one case, the entire company in another.
- Extensive compromise of operational system -15,000 hours recovery operation in one case.
- Alteration of medical diagnostic test result.
- Extortion –demanding payment to avoid operational problem.

3. TERMINOLOGY:

Vulnerabilities: It is the weakness in the security system.

Threats: Is the set of system that has the potential to cause loss or harm.

4. SECURITY APPROACHES:

- **Security models:** An organisation can take several approaches to implement its security model.
 - a) No security
 - b) Security through obscurity
 - c) Host security
 - d) Network security
- **Security management Practices:**
 - a) Affordable
 - b) Functionality
 - c) Culture issue
 - d) Legality

5. PRINCIPLES OF SECURITY:

- **Confidentiality:** It provides for the secrecy of information. The confidentiality only allows authorized user to have access to information. The confidentiality service must work with the accountability service to correctly identify individuals. The confidential service protects against

the access attacks. it must take into account that information may reside in physical form in paper files, in electronic form in electronic files, and in transit.

- **Integrity:** It provides the correctness of information. integrity allows the user to have the confidence that the information has not been modified by an unauthorised individual. It protects against the modification attack.
- **Availability:** It provides for information to be useful. Availability allows user to access computer system, the information on the system, and the application that performs operations on the information. It also provides for the communication systems to transmit information between locations or computer system.
- **Accountability:** It does not protect against attacks by itself. It must be used in conjugation with other services to make them more effective.

Security Environment

- **Threats:**
When vulnerabilities are exploited they become threats.

Table 1: Goal vs. Threats

Goal	Threats
Data confidentiality	Exposure of data
Data integrity	Tampering with data
System availability	Denial of service

- **Intruder:**
 - People who are nosing around places where they have no business.
 - Common categories: casual snooping by non-technical users.
 - Snooping by insiders.
 - Determined attempt to make money.
 - Commercial or military espionage.

Attack from inside the system

- Unauthorised access
- Login spoofing
- Trojan horses
- Logic bombs
- Trap doors
- Buffer overflow

Authentication:

It proves the user is the one whom the user claims to be strength and reliability of authentication depends on the mechanism used

Authentication mechanisms:

Something the user knows i.e. Password, pin no, mother's middle name

Password:

It is the simplest form of authentication, it is to be known only to the user and system as shown in fig 1

What is more secure?!



Authentication is based on knowing the
<name, password> pair

Fig1: Pass word Authentication

Attacks on password:

- Social engineering
- Search the system list of password
- Try the pass word likely for the user (guessing)
- Try many probable pass words
- Try all possible passwords

Pass word selection criteria:

Counter attack five password attacks. Password should be changed regularly. The same set of password should not be repeated regularly. Something the user has .i.e. token, key , magnetic card as shown in fig2

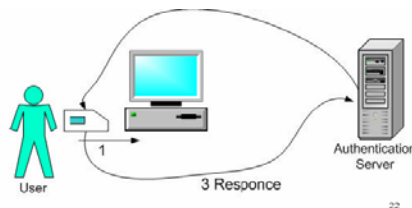


Fig 2: Authencation Server

Things the user is based on biometrics i.e. finger print, DNA, facial, voice, retina based upon measurement of some unique physical characteristics of an individual as shown in fig3. It provides much better form of authentication and it is socially accepted

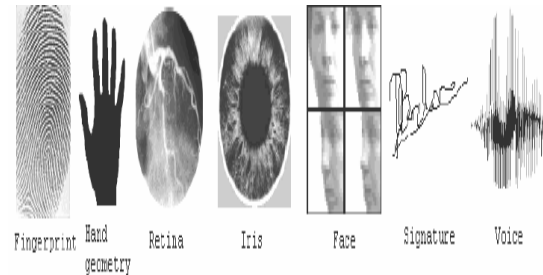


Fig 3: Biometrics

Trojan horse: The name is given based on the Greek legend. It is a malicious program that offers the required functionality. It provides the hidden work as well. The torzon horse I LOVE YOU can cause a DOS attack through the consumption of resources

Logical bomb: Class of malicious code that determines or goes off when specific condition occurs

Trap door: It is also called back door. It is an undocumented entry to the system. It is inserted during code development

6. ATTACKS FROM OUTSIDE THE SYSTEM:

It is related mainly to network security

External threats is code transmitted to target machine

Threats: DOS, virus, worms, mobile code

Viruses: It is a program that can pass on malicious code to other non malicious programs by modifying them, that can produce itself

It attacks itself to the program either destroy it or coexist with it

A good virus:

- Rapid wider infection
- Harder to detect and rid of
- Ability to re –infect home programming
- Easy to create
- Machine and OS dependent

Damages caused by virus

- Black mail
- Denial of service as long as virus runs
- Permanently damaged hardware
- Intra-corporate dirty tricks

How virus spreads

- When you run or install programs includes viruses with itself
- e-mail attachments which executes automatically

- Executable zip files
- Micros

Types of virus

- Companion viruses
- Memory resident viruses
- Boot sector viruses
- Micro virus
- Detecting virus
- Based on the signature
- Integrity checkers
- Execution pattern
- Transmission pattern

Worms:

- Is a program that spreads copies of itself through a network
- It also copies itself as standalone programs
- Worm spread through a network
- Example :Nimdi

7. SOLUTION:

- Cryptography
- Hash function
- Digital signature
- VPN
- Firewalls
- Protecting servers
- Trusted system

8. DESIGN PRINCIPLES FOR SECURITY

- System design should be public
- Default should be no access
- Check for current authority
- Give each process least possible privileges
- Protection mechanism should be
- Scheme should be psychologically acceptable

CONCLUSION:

- Security is a dynamic process which has a role to play
- Third world countries should not be a playground for hackers
- Awareness is the best way of protection

REFERENCES

- [1] http://www.cert.org/reports/dsit_workshop.pdf
- [2] <http://www.denialinfo.com/>
- [3] <http://www.cisco.com/public/cons/isp/documents/IOSEssentiPDF.zip>
- [4] <http://www.cert.org/>
- [5] <http://www.first.org/>
- [6] <http://www.cisco.com/warp/public/707/21.html>
- [7] http://www.cisco.com/warp/public/707/sec_incident_response.shtml
- [8] Cisco Security Advisories
- [9] <http://www.cisco.com/warp/public/707/advisory.html>
- [10] Characterizing and Tracing Packet Floods Using Cisco Routers

- [11] <http://www.cisco.com/warp/public/707/22.html>
- [12] Strategies to Protect Against Distributed Denial of Service
- [13] <http://www.cisco.com/warp/public/707/newsflash.html>

NANOELECTRONICS

Swati Jha

Assistant Professor, Department of Electronics and Communication,
Dronacharya College of Engineering, Gurgaon-123506, India
Email: swati.jha21@yahoo.co.in

Abstract: Nanoelectronics, as the name suggests, refers to the use of nanotechnology on electronic equipments/components, especially transistors. Nanoelectronics often refer to transistor devices that are so small that inter-atomic interactions and quantum mechanical properties can't be ignored. As a result, present transistors (for example: recent Intel Core i7 processors) do not fall under this category, even though these devices are manufactured under 65nm or 45nm technology. Single electron transistors, which involve transistor operation based on a single electron and Nanoelectromechanical systems (NEMS) are some of the very known examples using the fundamentals of nanoelectronics

Keywords: *Nanotechnology, Molecular electronics, Nanoionics, Nanophotonics, Nanocircuits, Nanosensors, Bio-nano generators, Quantum Computers.*

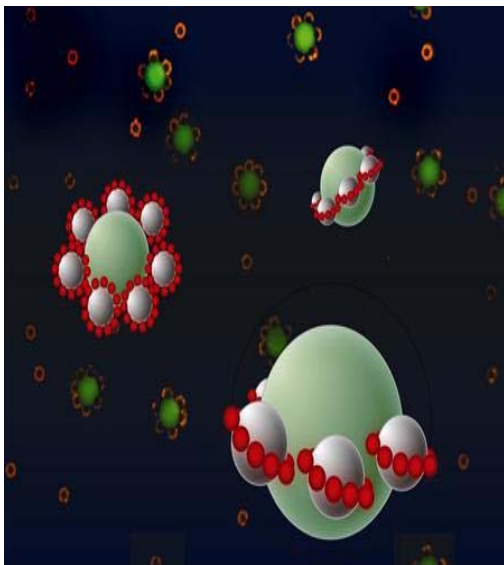
1. Introduction

We all are aware about the Keyword "Nanotechnology" which is a technology dealing with all those materials which are not more than 100nm in size. But at the same time it's equally true that anything less than 100nm always doesn't come under this category. The particles/components must possess some unique properties to be called a nanomaterial. Nanoelectronics are sometimes considered as disruptive technology because the presently manufactured electronic components are significantly different from their traditional counterparts.

1.1 Basic constituents of Nanoelectronics:

a) Nanofabrication: Nanofabrication refers to fabrication methodologies employed for nanoelectronic materials. With the advancements in these technologies scientists have been able to construct ultradense parallel arrays of nanowires, as an alternative to synthesize nanowires individually [1][2].

b) Nanomaterials electronics: Besides being small and allowing more transistors to be packed into a single chip, the uniform and symmetrical structure of nanotubes allows a higher electron mobility (faster electron movement in the material), a higher dielectric constant (faster frequency), and a symmetrical electron/hole characteristic [3].



c) Molecular electronics: Molecular electronics [4], a very new technology, which is still in its infancy, brings hope for truly atomic scale electronic systems in the future. One of the promising applications of molecular electronics was proposed by the IBM researcher Ari Aviram and the theoretical chemist Mark Ratner in their 1974 papers "Molecules for Memory, Logic and Amplification", in which they had described a Unimolecular rectifier.[5] Later, in 1988, Aviram described in detail a theoretical single-molecule field-effect transistor[6]. Further concepts were proposed by Forrest Carter of the Naval Research Laboratory, who, proposed single-molecule logic gates. This is one of the many possible ways in which a molecular level diode/transistor might be synthesized by organic chemistry. Spintronics, which harness the spin of the electron as well as its charge, is compatible with the emerging field of

molecular electronics.

d) Nanoionics: This subfield of nanoelectronics studies the transport of ions rather than electrons in nanoscale systems.

e) Nanophotonics: It studies the behaviour of light on the nanoscale, and has the goal of developing devices that take an advantage of this behaviour.

Fig. 1 Axial quadrupole nanostructures

2. The First Molecular Electronic device

In 1974, John McGinness and his coworkers described the putative "First experimental demonstration of an operating voltage-controlled switch"[7]. This device used DOPA melanin, an oxidized mixed polymer of polyacetylene, polypyrrole, and polyaniline. The "ON" state of this switch exhibited almost metallic conductivity. With the development of the Scanning Tunneling Microscope (STM) and later the Atomic Force Microscope (AFM) have facilitated manipulation of single-molecule electronics.

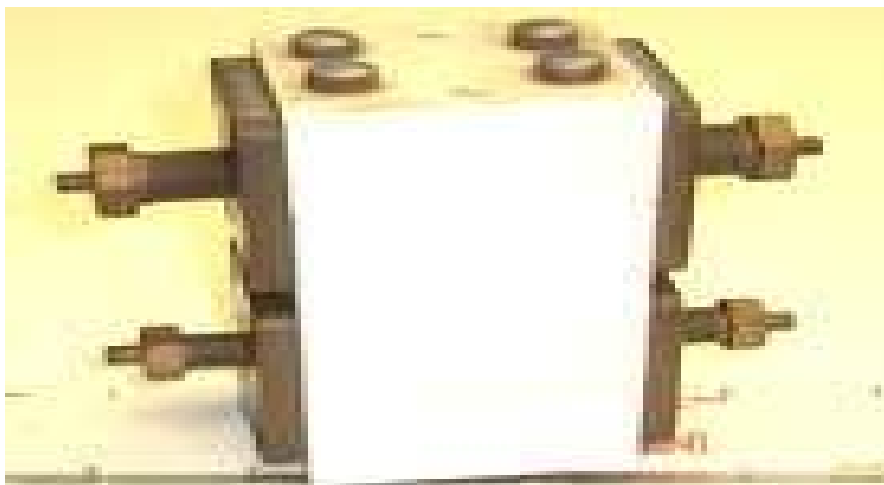


Fig. 2 Voltage-controlled switch, a molecular electronic device from 1974.

3. Nanowires

These are Semiconductor one-dimensional structures with novel electrical and optical properties that can be used as building blocks in nanoscale devices such as field-effect transistors, sensors and light-emitting diodes. Hybrid devices combine the flexibility of organic materials such as polymers with the useful electronic and optical properties of semiconductor materials. At present, however, these structures lack mechanical strength and this limits their use in practical applications.

4. Nanocircuits

Nanocircuits are electrical circuits on the scale of nanometers. We all are aware that one nanometer is equal to 10^{-9} meters or a row of 10 hydrogen atoms. With circuits becoming smaller, there is an ability to fit more on a computer chip. This allows more complex functions using less power and at a faster speed. Nanocircuits are organized into three different parts: transistors, interconnections, and architecture, all dealt with on the nano scale. A variety of proposals have been made to implement nanocircuitry in different forms including Single-Electron Transistors, Quantum dot cellular automata, and Nanoscale Crossbar Latches. However, new researches target on the incorporation of nanomaterials to improve the design of MOSFETs, which currently

pre-wired so as to eliminate the difficult task of trying to connect transistors together with nanowires.

iii) The last part of nanocircuit organization is **architecture**. This has been explained as the overall way the transistors are interconnected, so that the circuit can plug into a computer or other system and operates independently of the lower-level details. With nanocircuits being so small, they are destined for errors and defects. Scientists have devised a way to get around this. Their architecture combines circuits that have redundant logic gates and interconnections with the ability to reconfigure structures at several levels on a chip. The redundancy lets the circuit identify problems and reconfigure itself so the circuit can avoid more problems. It also allows for errors within the logic gate and still have it work properly without giving a wrong result.

Scientists in India have recently developed the world's smallest transistor which will be used for nanocircuits. The transistor is made entirely from carbon nanotubes. Nanotubes are rolled up sheets of carbon atoms and are more than a thousand times thinner than human hair. Instead of taking the traditional top-down approach, the bottom-up approach is adopted because of the sheer size of these nanocircuits. Unlike conventional circuit design, which proceeds from blueprint to photographic pattern on to the chip, nanocircuit design will begin with the chip—a haphazard jumble of components and wires, (not all of which will even work) and gradually sculpt it into a useful device[11]. Scientists and engineers have created all of the essential components of nanocircuits such as transistors, logic gates and diodes. They have all been constructed from organic molecules, carbon nanotubes and nanowire semiconductors. The only thing left to do is find a way to eliminate the errors that come with such a small device and nanocircuits will become a way of all electronics.

5. Nanoelectronic Devices

5.1 Radios

Nanoradios have been developed structured around carbon nanotubes[12].

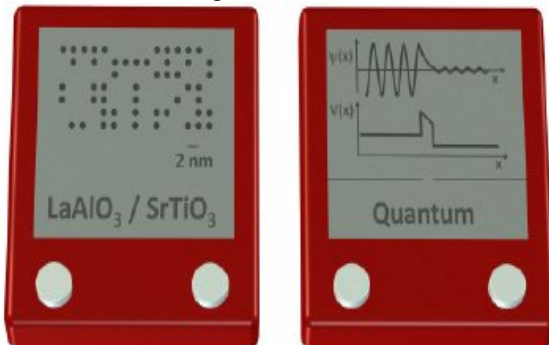
5.2 Computers

Nanoelectronics hold the promise of making computer processors more powerful than are possible with conventional semiconductor fabrication techniques. A number of approaches are currently being researched, including new forms of nanolithography, as well as the use of nanomaterials such as nanowires or small molecules in place of traditional CMOS components.

5.3 Transistors

A team in US has made tiny transistors, the building block of computer processors, a fraction of the size of those used on advanced silicon chips. They created its nanotech transistors using two ceramic crystal materials known as lanthanum aluminate and strontium titanate.

When sandwiched together, these natural insulators conduct electricity as a positive charge is passed across them. Using the tip of an atomic force microscope, they applied voltage to etch a tiny conducting wire between the two materials, which can later be erased by reversing the charge.



5.4 Thin Film

Another team from the University of Massachusetts Amherst and the University of California Berkeley has made a film material capable of storing data from 250 DVDs onto a surface, the size of a coin. They have tried to use polymers to create

sheets of semiconductor films but the material often lost its structure when spread over large surfaces. To overcome this, the team lead by Thomas Russell of the University of Massachusetts heated sapphire crystals to create pattern of ridges on the surface.

Fig 4 The Transistor and its characteristics

6. Future Applications of Nanoelectronic Devices

6.1 Energy production

Research is ongoing to use nanowires and other nanostructured materials with the hope to create cheaper and more efficient solar cells than are possible with conventional planar silicon solar cells.[13] It is believed that the invention of more efficient solar energy would have a great effect on satisfying global energy needs.

There is also research into energy production for devices that would operate in vivo, called bio-nano generators. A bio-nano generator is a nanoscale electrochemical device, like a fuel cell or galvanic cell, but drawing power from blood glucose in a living body, much the same as our body generates energy from food. To achieve the effect, an enzyme is used that is capable of stripping glucose of its electrons, freeing them for use in electrical devices. The average person's body could, theoretically, generate 100 watts of electricity (about 2000 food calories per day) using a bio-nano generator [14]. The electricity generated by such a device could power devices embedded in the body (such as pacemakers), or sugar-fed nanorobots. Much of the research done on bio-nano generators is still experimental, with Panasonic's Nanotechnology Research Laboratory among those at the forefront.

6.2 Medical diagnostics

There is great interest in constructing nanoelectronic devices [15][16][17] that could detect the concentrations of biomolecules in real time for use as medical diagnostics[18], thus falling into the category of nanomedicine[19]. A parallel line of research seeks to create nanoelectronic devices which could interact with single cells for use in basic biological research. These devices are called nanosensors. Such miniaturization on nanoelectronics towards in vivo proteomic sensing should enable new approaches for health monitoring, surveillance, and defense technology. Nanosensors are any biological, chemical, or sugery sensory points used to convey information about nanoparticles to the macroscopic world. Their use mainly include various medicinal purposes and as gateways to building other nanoproducts.

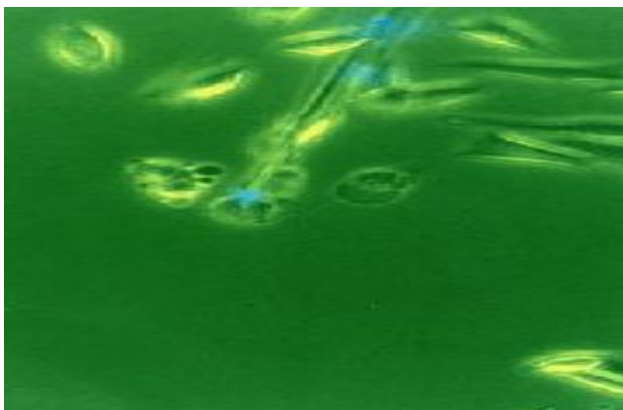


Fig. 5 A nanosensor probe carrying a laser beam (blue) penetrates a living cell to detect the presence of a product indicating that the cell has been exposed to a cancer-causing substance.

By measuring changes in volume, concentration, displacement and velocity, gravitational, electrical, and magnetic forces, pressure, or temperature of cells in a body, nanosensors are able to distinguish between and recognize certain cells, most notably those of cancer, at the

molecular level in order to deliver medicine or monitor development to specific places in the body. In addition, they may be able to detect macroscopic variations from outside the body and communicate these changes to other nanoproducts working within the body.

Another example of nanosensors involves using the fluorescence properties of cadmium selenide quantum dots as sensors to uncover tumors within the body. By injecting a body with these quantum dots, a doctor could see where a tumor or cancer cell was by finding the injected quantum dots, an easy process because of their fluorescence. Developed nanosensor quantum dots would be specifically constructed to find only the particular cell for which the body was at risk. A flipside to the cadmium selenide dots, however, is that they are highly toxic to the body. As a result, researchers discovered zinc sulfide quantum dots which are not quite as fluorescent as cadmium selenide, but the same can be augmented when combined with other metals like

manganese and various lanthanide elements. In addition, these newer quantum dots become more fluorescent when they bond to their target cells.

One of the first working examples of a synthetic nanosensor was built by researchers at the Georgia Institute of Technology in 1999. It involved attaching a single particle onto the end of a carbon nanotube and measuring the vibrational frequency of the nanotube both with and without the particle. The discrepancy between the two frequencies allowed the researchers to measure the mass of the attached particle.

7 Conclusion

It has become very clear that the trend in downscaling transistors will end in 10 to 15 years (Top-down approach) since the transport equations that govern the operation of conventional transistors and interconnects are no longer valid in devices with nanometer dimensions. To continue the evaluation of ultra-fast and ultra-dense microelectronics, we must search for revolutionary devices and IC architectures based on new operation principles (Bottom-up approach). Ideally, these new devices should not only be ultra small and fast, but also have high functionality and be capable of performing tasks such as parallel computing to make Quantum Computers.

References

- [1] Melosh, N., Boukai, Akram, Diana, Frederic, Gerardot, Brian, Badolato, Antonio, Petroff, Pierre & Heath, James R. (2003). "Ultrahigh density nanowire lattices and circuits".
- [2] Das, S., Gates, A.J., Abdu, H.A., Rose, G.S., Picconatto, C.A. & Ellenbogen, J.C. (2007). "Designs for Ultra-Tiny, Special-Purpose Nanoelectronic Circuits".
- [3] Goicoechea, J., Zamarreño, C.R., Matiasa, I.R. & Arregui, F.J. (2007). "Minimizing the photobleaching of self-assembled multilayers for sensor applications".
- [4] Petty, M.C.; Bryce, M.R. & Bloor, D. (1995). *An Introduction to Molecular Electronics*. London: Edward Arnold.
- [5] Aviram, A.; Ratner, M. A. (1974). "Molecular Rectifier".
- [6] Aviram, A. (1988). "Molecules for memory, logic, and amplification". *Journal of the American Chemical Society* 110 (17): 5687–5692.
- [7] Tour, James M.; et al. (1998). "Recent advances in molecular scale electronics". *Annals of the New York Academy of Sciences* 852: 197–204.
- [8] Colinge, J., Multiple-gate SOI MOSFETs, *Solid-State Electronics* 48, 2004
- [9] Stokes, Jon. "Understanding Moore's Law", *Ars Technica*, 2003-02-20.
- [10] Patch, Kimberly. "Design handles of nanocircuits", *TRN*, 2003-03-26.
- [11] Eds. *Scientific American*, 94.
- [12] Jensen, K.; Jensen, K.; Weldon, J.; Garcia, H. & Zettl A. (2007). "Nanotube Radio". *Nano Lett.* 7 (11): 3508–3511.
- [13] Tian, Bozhi; Zheng, Xiaolin; Kempa, Thomas J.; Fang, Ying; Yu, Nanfang; Yu, Guihua; Huang, Jinlin & Lieber, Charles M. (2007). "Coaxial silicon nanowires as solar cells and nanoelectronic power sources". *Nature* 449: 885–889.
- [14] "Power from blood could lead to 'human batteries'". *Sydney Morning Herald*. August 4, 2003.
- [15] LaVan, D.A.; McGuire, Terry & Langer, Robert (2003). "Small-scale systems for in vivo drug delivery". *Nat Biotechnol.* 21 (10): 1184–1191.
- [16] Grace, D. (2008). "Special Feature: Emerging Technologies". *Medical Product Manufacturing News*. 12: 22–23.
- [17] Saito, S. (1997). "Carbon Nanotubes for Next-Generation Electronics Devices". *Science* 278: 77–78.
- [18] Cavalcanti, A.; Shirinzadeh, B.; Zhang, M. & Kretly, L.C. (2008). "Nanorobot Hardware Architecture for Medical Defense". *Sensors* 8 (5): 2932–2958.
- [19] Couvreur, P. & Vauthier, C. (2006). "Nanotechnology: intelligent design to treat complex disease". *Pharm. Res.* 23 (7): 1417–1450.

EVOLUTION OF 4G TECHNOLOGY

Jyoti Dargan

Department of Electronics & Communication Engineering,
Dronacharya College of Engineering, Gurgaon-123506, India
Email: Jyoti_dargan@hotmail.com

Vinita Sahu

Department of Electronics & Communication Engineering,
Dronacharya College of Engineering, Gurgaon-123506, India
Email: vinitasahu@yahoo.co.in

ABSTRACT:

At present 2G Technology (GSM) is widely used worldwide. The problem with the 2G technology is that the data rates are limited. This makes it inefficient for data transfer application like video conferencing, music or video downloads. To increase the speed various new technologies have come into picture. The first is 2.5G (GPRS) technology that allows the data transfer at a better rate than GSM and recently 3G (WCDMA / UMTS) technology has come into picture. The Maximum theoretical data transfer with this 3G technology is 2Mbps. practically it could be a maximum of 384kbps or even less. Then the Wi-Max technology came into picture. It can deliver upto 70Mbps over a 50 Km radius. The 4G technology which is at infancy is supposed to allow data transfer upto 100Mbps outdoor and 1Gbps indoor. This technology will be able to support interactive services like video conferencing (with more than two sites simultaneously), wireless internet etc.

Keywords: 4G Technology, Evolution of 4G Technology, Orthogonality, OFDM Technique, OFDM Transmitter, OFDM Receiver.

1. TECHNICAL ASPECTS OF 1G TO 3G:

The first generation (1G) began in the early 80's with commercial deployment of Advanced Mobile Phone Service (AMPS) cellular networks. Early AMPS networks used Frequency Division Multiplexing Access (FDMA) to carry analog voice over channels in the 800 MHz frequency band.

The second generation (2G) emerged in the 90's when mobile operators deployed two competing digital voice standards. In North America, some operators adopted IS-95, which used Code Division Multiple Access (CDMA) to multiplex up to 64 calls per channel in the 800 MHz band. Across the world, many operators adopted the Global System for Mobile communication (GSM) standard, which used Time Division Multiple Access (TDMA) to multiplex up to 8 calls per channel in the 900 and 1800 MHz bands.

The International Telecommunications Union (ITU) defined the third generation (3G) of mobile telephony standards – IMT-2000 – to facilitate growth, increase bandwidth, and support more diverse applications. For example, GSM could deliver not only voice, but also circuit-switched data at speeds up to 14.4 Kbps. But to support mobile multimedia applications, 3G had to deliver packet-switched data with better spectral efficiency, at far greater speeds.

However, to get from 2G to 3G, mobile operators had make "evolutionary" upgrades to existing networks while simultaneously planning their "revolutionary" new mobile broadband networks. This led to the establishment of two distinct 3G families: 3GPP and 3GPP2.

The 3rd Generation Partnership Project (3GPP) was formed in 1998 to foster deployment of 3G networks that descended from GSM. 3GPP technologies evolved as follows.

- General Packet Radio Service (GPRS) offered speeds up to 114 Kbps.
- Enhanced Data Rates for Global Evolution (EDGE) reached up to 384 Kbps.

- UMTS Wideband CDMA (WCDMA) offered downlink speeds up to 1.92 Mbps.
- High Speed Downlink Packet Access (HSDPA) boosted the downlink to 14Mbps.
- LTE Evolved UMTS Terrestrial Radio Access (E-UTRA) is aiming for 100 Mbps.

GPRS deployments began in 2000, followed by EDGE in 2003. While these technologies are defined by IMT-2000, they are sometimes called "2.5G" because they did not offer multi-megabit data rates. EDGE has now been superseded by HSDPA (and its uplink partner HSUPA). According to the 3GPP, there were 166 HSDPA networks in 75 countries at the end of 2007. The next step for GSM operators: LTE E-UTRA, based on specifications completed in late 2008.

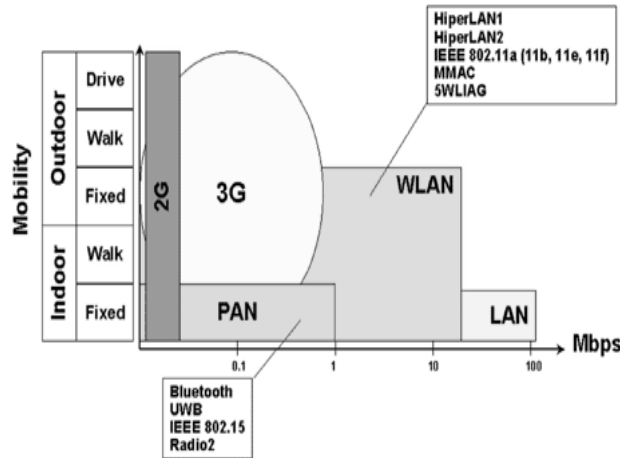


Figure 1: practical domains of technologies

"The problem with 3G is that it's still a voice-oriented service," said Paul Sergeant, marketing director for Motorola's Moto Wi4 unit. "What's leftover goes to data."

The problems with the previous technologies are with the speed, stability and general clunkiness of "the internet on wireless". While limited applications such as e-mail have worked well, broader internet surfing has been less than stellar.

But both solutions have drawbacks: Wi-Fi access is limited to specific hot spots and, even then, prone to interference and scalability limits. And broadband-access products by Verizon Wireless and Sprint/Nextel -- while offering wider geographic coverage -- are expensive at about \$60 per month.

Mobile broadband, as opposed to fixed wireless technology, has so far involved cramming packet-based data services into networks originally intended for circuit-switched voice calls.

2. EVOLUTION OF 4G TECHNOLOGY:

4G is not a new system design from scratch but 4G is a concept of

"Integration and Convergence"

The 4G technology includes the best features of 2G, 3G, Wi-Fi, Wi-PAN (Bluetooth), and Wi-Max technologies with additive features. Packing so much intelligence in smaller and smaller physical space, esp. User Equipment (UE) 4G can be defined as:

“IP + WPAN + WLAN + WMAN + WWAN + any other stragglers = 4G”

The entire network would be packet-switched (IP Based). All switches would be digital. Higher bandwidths of 100MHz, and data could be transferred at much higher rates the cost of data transfer would be comparatively very less and global mobility would be possible. The security features will be much better. The smart antennas will be used and improved access technologies like OFDM and MC-CDMA (Multi Carrier) will be used.

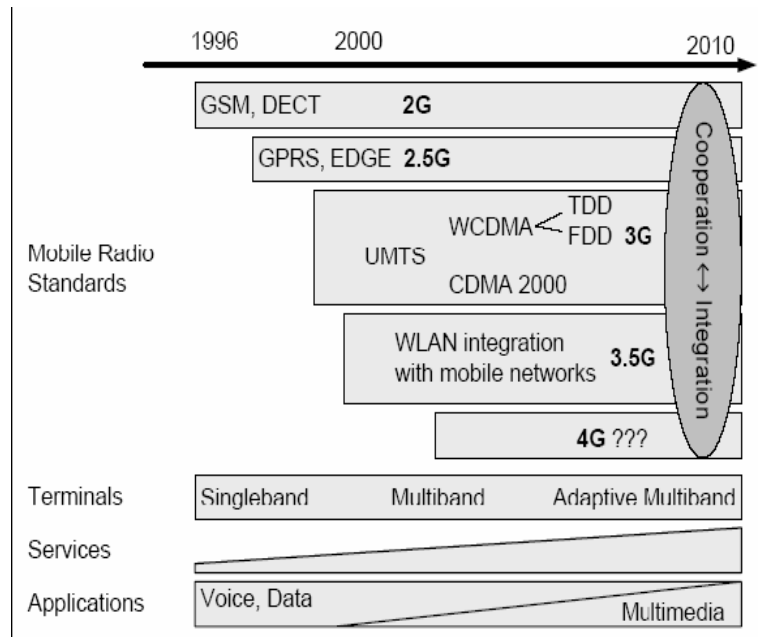


Figure 2: integration of different generations

New 4G technologies, however, aim to create fully packet-switched networks optimized for data -- whether the digital bits represent voice, data or multimedia content.

The 4G operate in two bands: 2.3GHz-2.5 GHz, and 4.9GHz-6GHz, both licensed and unlicensed.

3. ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM):

OFDM is a frequency division multiplexing scheme utilised as a digital multicarrier modulation method. A large number of closely-spaced orthogonal *sub-carriers* are used to carry data. The data is divided into several parallel data streams or channels, one for each sub-carrier. Each sub-carrier is modulated with a conventional modulation scheme (such as quadrature amplitude modulation or phase shift keying) at a low symbol rate, maintaining total data rates similar to conventional *single-carrier* modulation schemes in the same bandwidth.

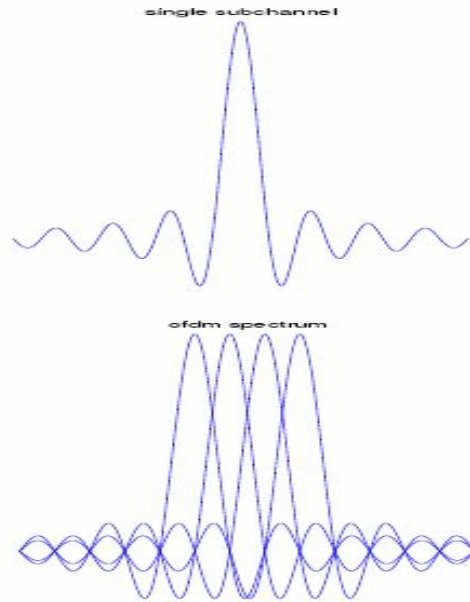


Figure 3: OFDM wave

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions — for example, attenuation of high frequencies in a long copper wire, narrowband interference and frequency-selective fading due to multipath — without complex equalization filters. Channel equalization is simplified because OFDM may be viewed as using many slowly-modulated narrowband signals rather than one rapidly-modulated wideband signal. The low symbol rate makes the use of a guard interval between symbols affordable, making it possible to handle time-spreading and eliminate inter symbol interference (ISI). This mechanism also facilitates the design of single-frequency networks, where several adjacent transmitters send the same signal simultaneously at the same frequency, as the signals from multiple distant transmitters may be combined constructively, rather than interfering as would typically occur in a traditional single-carrier system.

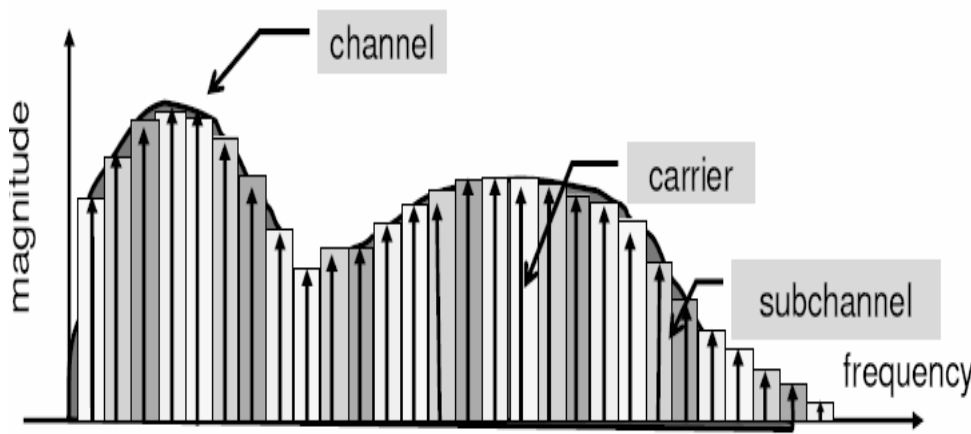


Figure 4: OFDM spectrum

4. ORTHOGONALITY:

In OFDM, the sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other, meaning that cross-talk between the sub-channels is eliminated and inter-carrier guard bands are not required. This greatly simplifies the design of both the transmitter and the receiver; unlike conventional FDM, a separate filter for each sub-channel is not required.

The orthogonality requires that the sub-carrier spacing is given by:

$$\Delta f = k/(T_U) \text{ Hertz,}$$

where T_U seconds is the useful symbol duration (the receiver side window size), and k is a positive integer, typically equal to 1. Therefore, with N sub-carriers, the total passband bandwidth will be

$$B \approx N \cdot \Delta f \text{ (Hz).}$$

5. IMPLEMENTATION USING THE FFT ALGORITHM:

The orthogonality allows for efficient modulator and demodulator implementation using the FFT algorithm on the receiver side, and inverse FFT on the sender side.

6. GUARD INTERVAL FOR ELIMINATION OF INTER-SYMBOL INTERFERENCE:

One key principle of OFDM is that since low symbol rate modulation schemes (*i.e.* where the symbols are relatively long compared to the channel time characteristics) suffer less from inter symbol interference caused by multipath propagation, it is advantageous to transmit a number of low-rate streams in parallel instead of a single high-rate stream. Since the duration of each symbol is long, it is feasible to insert a guard interval between the OFDM symbols, thus eliminating the inter symbol interference.

The guard interval also eliminates the need for a pulse-shaping filter, and it reduces the sensitivity to time synchronization problems.

7. CHANNEL CODING AND INTERLEAVING:

OFDM is invariably used in conjunction with channel coding ([forward error correction](#)), and almost always uses frequency and/or time interleaving.

Frequency (subcarrier) interleaving increases resistance to frequency-selective channel conditions such as fading. For example, when a part of the channel bandwidth is faded, frequency interleaving ensures that the bit errors that would result from those subcarriers in the faded part of the bandwidth are spread out in the bit-stream rather than being concentrated. Similarly, time interleaving ensures that bits that are originally close together in the bit-stream are transmitted far apart in time, thus mitigating against severe fading as would happen when travelling at high speed.

However, time interleaving is of little benefit in slowly fading channels, and frequency interleaving offers little to no benefit for narrowband channels that suffer from flat-fading

The reason why interleaving is used on OFDM is to attempt to spread the errors out in the bit-stream that is presented to the error correction decoder, because when such decoders are presented with a high concentration of errors the decoder is unable to correct all the bit errors, and a burst of uncorrected errors occurs.

A common type of error correction coding used with OFDM-based systems is [convolutional-coding](#), which is often concatenated with Reed-Solomon coding. Convolutional coding is used as the inner code and Reed-Solomon coding is used for the outer code — usually with additional interleaving (on top of the time and frequency interleaving mentioned above) in between the two layers of coding. The reason why this combination of error correction coding is used is that the Viterbi decoder used for convolutional decoding produces short errors bursts when there is a high concentration of errors, and Reed-Solomon codes are inherently well-suited to correcting bursts of errors.

Popularly used error correction coding types include turbo codes and LDPC codes. These codes only perform close to the Shannon limit for the Additive White Gaussian Noise ([AWGN](#)) channel, however, and some systems that have adopted these codes have concatenated them with either Reed-Solomon (for example on the [MediaFLO](#) system) or [BCH codes](#) (on the [DVB-S2](#) system) to improve performance further over the wireless channel.

8. OFDMA:

In Orthogonal Frequency Division Multiple Access (OFDMA), [frequency-division multiple access](#) is achieved by assigning different OFDM sub-channels to different users. OFDMA supports differentiated quality-of-service by assigning different number of sub-carriers to different users in a similar fashion as in CDMA, and thus complex packet scheduling or media access control schemes can be avoided.

8.1 OFDM TRANSMITTER:

An OFDM carrier signal is the sum of a number of orthogonal sub-carriers, with [baseband](#) data on each sub-carrier being independently modulated commonly using some type of [quadrature amplitude modulation](#) (QAM) or [phase-shift keying](#) (PSK). This composite baseband signal is typically used to modulate a main [RF](#) carrier.

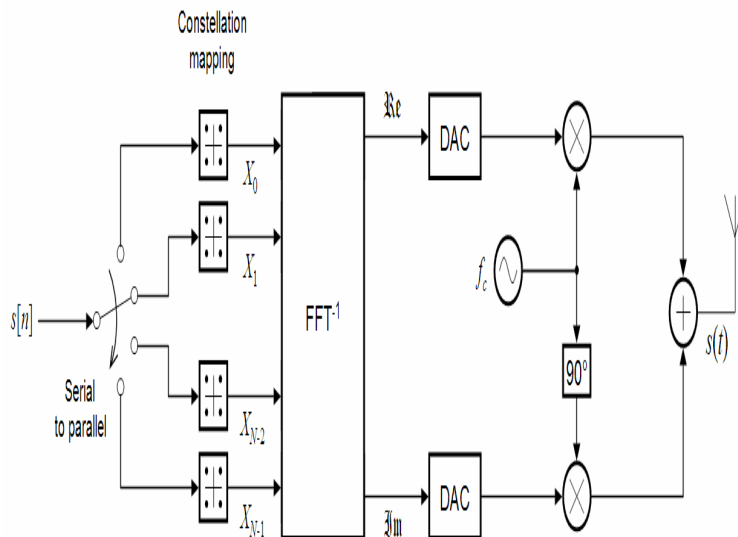


Figure 5: OFDM transmitter

$s[n]$ is a serial stream of binary digits. By inverse multiplexing, these are first demultiplexed into N parallel streams, and each one mapped to a (possibly complex) symbol stream using some modulation constellation (QAM, [PSK](#), etc.).

An inverse FFT is computed on each set of symbols, giving a set of complex time-domain samples. These samples are then [quadrature](#)-mixed to passband in the standard way. The real and imaginary components are first converted to the analogue domain using digital-to-analogue converters (DACs); the analogue signals are then used to modulate cosine and sine waves at the [carrier](#) frequency, f_c , respectively. These signals are then summed to give the transmission signal, $s(t)$.

8.2 OFDM RECEIVER:

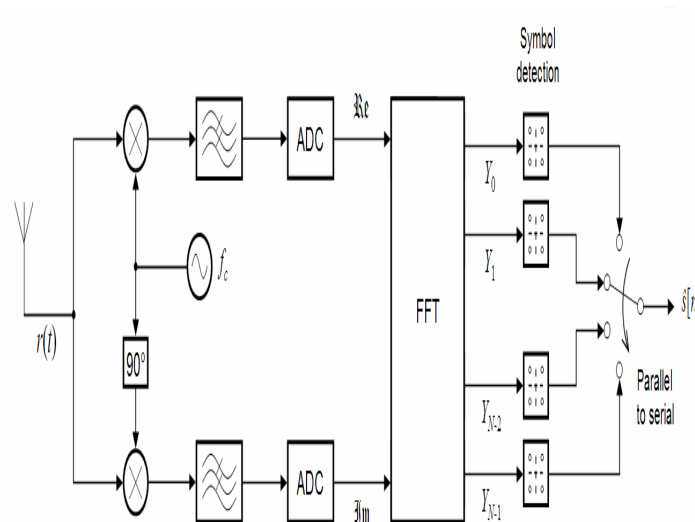


Figure 6: OFDM receiver

The receiver picks up the signal $r(t)$, which is then quadrature-mixed down to baseband using cosine and sine waves at the carrier frequency. This also creates signals centered on $2f_c$, so low-pass filters are used to reject these. The baseband signals are then sampled and digitized using analogue-to-digital converters (ADCs), and a forward FFT is used to convert back to the frequency domain.

This returns N parallel streams, each of which is converted to a binary stream using an appropriate [symbol detector](#). These streams are then re-combined into a serial stream, which is an estimate of the original binary stream at the transmitter.

9. SPACE DIVERSITY:

In OFDM based wide area broadcasting, receivers can benefit from receiving signals from several spatially-dispersed transmitters simultaneously, since transmitters will only destructively interfere with each other on a limited number of sub-carriers, whereas in general they will actually reinforce coverage over a wide area. This is very beneficial in many countries, as it permits the operation of national [single-frequency networks](#) (SFNs), where many transmitters send the same signal simultaneously over the same channel frequency. SFNs utilise the available spectrum more

effectively than conventional multi-frequency broadcast networks (MFN), where program content is replicated on different carrier frequencies. SFNs also result in a [diversity gain](#) in receivers situated midway between the transmitters. The coverage area is increased and the outage probability decreased in comparison to an MFN, due to increased received signal strength averaged over all sub-carriers.

Although the guard interval only contains redundant data, which means that it reduces the capacity, some OFDM-based systems, such as some of the broadcasting systems, deliberately use a long guard interval in order to allow the transmitters to be spaced farther apart in an [SFN](#), and longer guard intervals allow larger SFN cell-sizes. A rule of thumb for the maximum distance between transmitters in an SFN is equal to the distance a signal travels during the guard interval — for instance, a guard interval of 200 microseconds would allow transmitters to be spaced 60 km apart

10. CHALLENGES:

The major challenges in implementation of 4G technology are:

- The integration across different topologies.

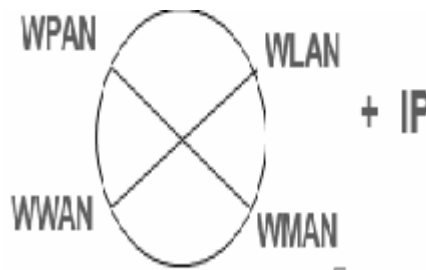


Figure 7: multi disciplinary cooperation

- Efficient signal processing and optimization algorithms are required.
- Efficient implementation of MC-CDMA, OFDM, QPSK, M-QAM and FFT Techniques are required.
- Improved protocols for traffic characteristics management to reduce burstiness and improve directionality.
- Requirement for improved hardware frequency synthesis techniques.
- Challenge of maintaining Shannon's Fundamental Law of data communication
- Appropriate addition of guard band to data is required.
- Challenge to reduce Inter Symbol Interference (ISI).
- Requirement of smart antennas.
- Requirement of sensitive transceiver design with low noise figure, high gain, wider bandwidth, high sensitivity, spurious rejection, low power consumption, frequency reuse.
- Requirement of efficient error correction coding.

11. DEVELOPEMENTS:

The Japanese company 'NTT DoCoMo' has been testing a 4G communication system prototype with 4x4 MIMO called VSF-OFCDM at 100 Mbit/s while moving, and 1 Gbit/s while stationary. In February 2007, NTT DoCoMo completed a trial in which they reached a maximum packet transmission rate of approximately 5 Gbit/s in the downlink with 12x12 MIMO using a 100MHz frequency bandwidth while moving at 10 km/h, and is planning on releasing the first commercial network in 2010.

'Digiweb', an Irish fixed and wireless broadband company, has announced that they have received a mobile communications license from the 'Irish Telecoms regulator-ComReg'. This service will be issued the mobile code 088 in Ireland and will be used for the provision of 4G Mobile communications. 'Digiweb' launched a mobile broadband network using FLASH-OFDM technology at 872 MHz.

'Pervasive networks' are an amorphous and at present entirely hypothetical concept where the user can be simultaneously connected to several wireless access technologies and can seamlessly move between them (See vertical handoff, IEEE 802.21). These access technologies can be Wi-Fi, UMTS, EDGE, or any other future access technology. Included in this concept is also smart-radio (also known as cognitive radio technology) to efficiently manage spectrum use and transmission power as well as the use of mesh routing protocols to create a pervasive network.

'Verizon Wireless' announced on September 20, 2007 that it plans a joint effort with the 'Vodafone' Group to transition its networks to the 4G standard LTE. On December 9, 2008, 'Verizon Wireless' announced that they intend to build and begin to roll out a 'LTE network' by the end of 2009.

'Telus' and 'Bell Canada', the major Canadian 'cdmaOne' and 'EV-DO carriers', have announced that they will be cooperating towards building a fourth generation (4G) 'LTE wireless broadband network' in Canada. As a transitional measure, they are implementing 3G UMTS to go live by early 2010.

'Sprint' announced it will be offering a 3G/4G connection plan for \$79.99, but it is only currently available in Baltimore

12. FUTURE ASPECTS:

Researchers are working on highly advanced feature like speaking without using vocal chords, communicating using our senses and knowing which direction the call is coming from, how far the other party is, etc. Most of these features are not available with 4G but may come in 5G technology.

CONCLUSION:

4G is being developed to accommodate the [QoS](#) and rate requirements set by forthcoming applications like wireless broadband access, [Multimedia Messaging Service](#) (MMS), [video chat](#), [mobile TV](#), [HDTV](#) content, [Digital Video Broadcasting](#) (DVB), minimal services like voice and data, and other services that utilize bandwidth.

The 4G working group has defined the following as objectives of the 4G wireless communication standard:

- A [spectrally efficient](#) system.
- High network capacity.

- A nominal data rate of 100 Mbit/s while the client physically moves at high speeds relative to the station, and 1 Gbit/s while client and station are in relatively fixed positions as defined by the [ITU-R](#).
- Smooth [handoff](#) across heterogeneous networks.
- Seamless connectivity and global [roaming](#) across multiple networks.
- High quality of service for next generation multimedia support.
- Interoperability with existing wireless standards.
- An all IP, packet switched network.

In summary, the 4G system should dynamically share and utilize network resources to meet the minimal requirements of all the 4G enabled users.

REFERENCES:

- [1] "4G - Beyond 2.5G and 3G Wireless Networks". MobileInfo.cm. <http://www.mobileinfo.com/3G/4GVision&Technologies.htm>. Retrieved on 2007-03-26.
- [2] "Mobility Management Challenges and Issues in 4G Heterogeneous Networks". *ACM Proceedings of the first international conference on Integrated internet ad hoc and sensor networks*. May 30 - 31, 2006. <http://delivery.acm.org/10.1145/1150000/1142698/a14-hussain.pdf?key1=1142698&key2=8898704611&coll=GUIDE&dl=&CFID=15151515&CFTOKEN=6184618>. Retrieved on 2007-03-26.
- [3] Werner Mohr (2002). "Mobile Communications Beyond 3G in the Global Context" (PDF). *Siemens mobile*. http://www.cu.ipv6tf.org/pdf/werner_mohr.pdf. Retrieved on 2007-03-26.
- [4] G. Fettweis, E. Zimmermann, H. Bonneville, W. Schott, K. Gosse, M. de Courville (2004). "High Throughput WLAN/WPAN" (PDF). WWRF. http://www.wireless-world-research.org/fileadmin/sites/default/files/about_the_forum/WG/WG5/Briefings/WG5-br2-High_Throughput_WLAN_WPAN-V2004.pdf.
- [5] [^] Nomor Research: White Paper on LTE Advance
- [6] [^] Morr, Derek (2009-06-09). "Verizon mandates IPv6 support for next-gen cell phones". <http://www.personal.psu.edu/dvm105/blogs/ipv6/2009/06/verizon-mandates-ipv6-support.html>. Retrieved on 2009-06-10.
- [7] [^] "DoCoMo Achieves 5 Gbit/s Data Speed". *NTT DoCoMo Press*. 2007-02-09. <http://www.nttdocomo.com/pr/2007/001319.html>.
- [8] Press Release: Digiweb Mobile Takes 088
- [9] TELUS (2008-10-10). "Next Generation Network Evolution". TELUS. <http://www.telusmobility.com/network/>.
- [10] Suk Yu Hui; Kai Hau Yeung (December 2003). "Challenges in the migration to 4G mobile systems". *Communications Magazine, IEEE* (City Univ. of Hong Kong, China) **41**: 54. doi: 10.1109/MCOM.2003.1252799. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1252799&isnumber=28028.
- [11] "4G Mobile". *Alcatel-Lucent*. 2005-06-13. <http://www.alcatel.com/publications/abstract.jhtml?repositoryItem=tcm%3A172-262211635>.
- [12] Robertson, P. Kaiser, S. "The effects of Doppler spreads in OFDM(A) mobile radio systems", Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS.
- [13] Coleri, S. Ergen, M. Puri, A. Bahai, A., Channel estimation techniques based on pilot arrangement in OFDM systems. *IEEE Transactions on Broadcasting*, Sep 2002. "
- [14] Hoeher, P. Kaiser, S. Robertson, P. "Two-dimensional pilot-symbol-aided channel estimation by Wienerfiltering". *IEEE International Conference on Acoustics, Speech, and Signal Processing*, ICASSP-97, 1997.
- [15] Noah Schmitz (March 2005). "The Path To 4G Will Take Many Turns". *Wireless Systems Design*. <http://www.wsdmag.com/Articles/ArticleID/10001/10001.html>. Retrieved on 2007-03-26.
- [16] "WINNER - Towards Ubiquitous Wireless Access". WINNER. 2007. http://www.comnets.rwth-aachen.de/typo3conf/ext/cn_download/pi1/passdownload.php?downloaddata=860%7C1
- [17] Nomor Research: White Paper on LTE Advance the new 4G standard
- [18] Brian Woerner (June 20-22, 2001). "Research Directions for Fourth Generation Wireless" (PDF). *Proceedings of the 10th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '01)*. (118kb)
- [19] 3GPP specification: Requirements for further advancements for E-UTRA (LTE-Advanced)
- [20] Numerous useful links and resources for OFDM - WCSP Group - University of South Florida (USF)
- [21] WiMAX Forum, WiMAX, the framework standard for 4G mobile personal broadband
- [22] Flarion Technologies, the inventor of FLASH-OFDM
- [23] QUALCOMM, parent company of Flarion Technologies

- [24] Stott, 1997 [1] Technical presentation by J H Stott of the BBC's R&D division, delivered at the 20 International Television Symposium in 1997; this URL accessed [24 January 2006](#).
- [25] Page on Orthogonal Frequency Division Multiplexing at http://www.iss.rwth_aachen.de/Projekte/Theo/OFDM/node6.html accessed on [24 September 2007](#).
- [26] Siemens demos 360 Mbit/s wireless
- [27] 1994 US Patent 5,282,222 for wireless data transmission - The patent "tree" rooted on this patent has upwards of 20000 nodes and leaves references.
- [28] An Introduction to Orthogonal Frequency Division Multiplex Technology
- [29] Short Introduction to OFDM - Tutorial written by Prof. Debbah, head of the Alcatel-Lucent Chair on flexible radio.

NETWORK SECURITY USING FIREWALLS

Meha Sharma

Assistant Professor, Department of Electronics and Communications Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email:meha_sh@yahoo.co.in

Pooja Yadav

Assistant Professor, Department of Electronics and Communications Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email:poojayadav_55@yahoo.co.in

ABSTRACT:

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. It is a software or hardware that is normally placed between a protected network and a not protected network and acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in. A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A firewall's function within a network is similar to physical firewalls with fire doors in building construction. In the former case, it is used to prevent network intrusion to the private network. In the latter case, it is intended to contain and delay structural fire from spreading to adjacent structures. Without proper configuration, a firewall can often become worthless. Standard security practices dictate a "default-deny" firewall rule set in which the only network connections which are allowed are the ones that have been explicitly allowed. Unfortunately, such a configuration requires detailed understanding of the network applications and endpoints required for the organization's day-to-day operation. Many businesses lack such understanding, and therefore implement a "default-allow" rule set, in which all traffic is allowed unless it has been specifically blocked. Firewalls can be implemented in either hardware or software or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet especially intranets. All messages entering or leaving the intranet pass through the firewall which examines each message and blocks those that do not meet the specified security criteria.

1. FIREWALL TECHNIQUES:

There are several types of firewall techniques:

1. [Packet filter](#): It looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users but it is difficult to configure. In addition, it is susceptible to IP spoofing.
2. [Application gateway](#): It applies security mechanisms to specific applications such as FTP and Telnet servers. This is very effective but can impose performance degradation.
3. [Circuit-level gateway](#): It applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made packets can flow between the hosts without further checking.
4. [Proxy server](#): It intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

2. HISTORY:

The term "firewall" originally meant a wall to confine a fire or potential fire within a building. Later uses refer to similar structures such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment. Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity. The predecessors to firewalls for network security were the routers used in the late 1980s to separate networks from one another. The view of the Internet as a relatively small community of compatible users who valued openness for sharing and collaboration was ended by a number of major internet security breaches which occurred in the late 1980s.

2.1 First Generation - Packet Filters

The first paper published on firewall technology was in 1988 when engineers from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls. This fairly basic system was the first generation of what would become a highly evolved and technical internet security feature. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin were continuing their research in packet filtering and developed a working model for their own company based upon their original first generation architecture. Packet filters act by inspecting the packets which represent the basic unit of data transfer between computers on the Internet. If a packet matches the packet filter's set of rules the packet filter will drop (silently discard) the packet, or reject it (discard it and send error responses to the source). This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (it stores no information on connection state). Instead it filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol) and for TCP and UDP traffic, the port number. TCP and UDP protocols comprise most communication over the Internet and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a "stateless" packet filter can distinguish between and thus control those types of traffic (such as web browsing, remote printing, email transmission, file transfer) unless the machines on each side of the packet filter are both using the same non-standard ports.

2.2 Second Generation-Stateful Filters

From 1989-1990 three colleagues from AT&T Bell Laboratories, Dave Presetto, Janardan Sharma, and Kshitij Nigam developed the second generation of firewalls calling them circuit level firewalls. Second (2nd) generation firewalls in addition regard placement of each individual packet within the packet series. This technology is generally referred to as a stateful packet inspection as it maintains records of all connections passing through the firewall and is able to determine whether a packet is either the start of a new connection, a part of an existing connection or is an invalid packet. Though there is still a set of static rules in such a firewall the state of a connection can in itself be one of the criteria which trigger specific rules. This type of firewall can help prevent attacks which exploit existing connections or certain Denial-of-service attacks.

2.3 Third Generation-Application Layer

Publications by Gene Spafford of Purdue University, Bill Cheswick at AT&T Laboratories and Marcus Ranum described a third generation firewall known as an application layer firewall also known as a proxy-based firewall. The product was released by DEC who named it the DEC SEAL product. DEC's first major sale was on June 13, 1991 to a chemical company based on the East Coast of the USA. TIS under a broader DARPA contract developed the Firewall Toolkit (FWTK) and made it freely available under license on October 1, 1993. The purposes for releasing the freely available not for commercial use FWTK were: to demonstrate via the software documentation and raise the bar of firewall software being used. The key benefit of application layer filtering is that it can understand certain applications and protocols (such as File Transfer Protocol, DNS or web browsing) and it can detect whether an unwanted protocol is being sneaked through on a non-standard port or whether a protocol is being abused in any harmful way.

3. TYPES OF FIREWALLS

There are several classifications of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

3.1 Network Layer and Packet Filters

Network layer firewalls also called packet filters operate at a relatively low level of the TCP/IP protocol stack not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules or default rules may apply. Network layer firewalls generally fall into two sub-categories, [stateful](#) and [stateless](#). Stateful firewalls maintain context about active sessions and use that state information to speed packet processing. Any existing network connection can be described by several properties including source and destination IP address, UDP or TCP ports and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer or completion connection). If a packet does not match an existing connection it will be evaluated according to the rule set for new connections. If a packet matches an existing connection based on comparison with the firewall's state table it will be allowed to pass without further processing. Stateless firewalls require less memory and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However they cannot make more complex decisions based on what stage communications between hosts have reached.

3.2 Application Layer

Application layer firewalls work on the application level of the TCP/IP stack (i.e. all browser traffic or all telnet or ftp traffic) and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender). In principle application firewalls can prevent all unwanted outside traffic from reaching protected machines. On inspecting all packets for improper content firewalls can restrict or prevent outright the spread of networked [computer worms](#) and [trojans](#). In practice however this becomes so complex and so difficult to attempt (given the variety of applications and the diversity of content each may allow in its packet traffic) that comprehensive firewall design does not generally attempt this approach.

3.3 Proxies

A proxy device (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests for example) in the manner of an application whilst blocking other packets. Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

4. UNIFIED THREAT MANAGEMENT:

A product category called unified threat management (UTM) has emerged. These devices promise integration, convenience and protection from pretty much every threat out there and are especially valuable to small and medium-sized businesses. An effective UTM solution delivers a network security platform comprised of robust and fully-integrated security and networking functions such as network firewalling, intrusion detection and prevention (IDS/IPS) and gateway anti-virus (AV) along with other features such as security management and policy management by a group or user. It is designed to protect against next generation application layer threats and offers a centralized management through a single console all without impairing the performance of the network.

4.1 Advantages of UTM

Convenience and ease of installation are the key advantages of threat management security appliances. There is much less human intervention required to install and configure these appliances. The advantages of UTM are listed below:

- **Reduced complexity:** The integrated all-in-one approach not only simplifies product selection but product integration and ongoing support as well.
- **Ease of deployment:** Since there is much less human intervention required customers themselves or vendors can easily install and maintain these products.
- **Integration capabilities:** These appliances can easily be deployed at remote sites without the help of any security professional on site. In this scenario a plug-and-play appliance can be installed and managed remotely. This kind of management is synergistic with large centralized software-based firewalls.
- **The black box approach:** Users have a tendency to play with things and the black box approach limits the damage users can do. This reduces trouble calls and improves security.
- **Troubleshooting ease:** When a box fails it is easier to swap out than troubleshoot. This process gets the node back online quicker and a non-technical person can also do it. This feature is especially important for remote offices without dedicated technical staff onsite

5. HARDWARE VS SOFTWARE FIREWALLS

Firewalls can be either hardware or software. The ideal firewall configuration will consist of both. In addition to limiting access to computer and network a firewall is also useful for allowing remote access to a private network through secure authentication certificates. Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers and should be considered an important part of system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers but for larger networks business networking firewall solutions are available. A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

For individual home users, the most popular firewall choice is a software firewall. Software firewalls are installed on the computer (like any software) and can be customized allowing some control over its function and protection features. A software firewall will protect the computer from outside attempts to control or gain access and depending on choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on the system. Additionally software firewalls may also incorporate privacy controls, web filtering and more. The downside to software firewalls is that they will only protect the computer they are installed on not a network so each computer will need to have a software firewall installed on it.

The differences between a software and hardware firewall are vast and the best protection for the computer and network is to use both as each offers different but much needed security features and benefits. Updating the firewall and operating system is essential to maintain optimal protection as is testing the firewall to ensure it is connected and working correctly.

6. PERSONAL FIREWALL:

A personal firewall is an application which controls network traffic to and from a computer permitting or denying communications based on a security policy. A personal firewall differs from

a conventional firewall in terms of scale. Personal firewalls are typically designed for use by end-users. As a result a personal firewall will usually protect only the computer on which it is installed. Many personal firewalls are able to control network traffic by prompting the user each time a connection is attempted and adapting security policy accordingly. Personal firewalls may also provide some level of intrusion detection allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

7. BASTION HOST

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application for example a proxy server and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose which is either on the outside of the firewall or in the Demilitarized Zone and usually involves access from untrusted networks or computers.

Common characteristics of bastion host are:

- The bastion host hardware platform executes a secure version of its operating system making it a trusted system.
- Only the services that the network administrator considers essential are installed on the bastion host.
- Each proxy is configured to support only a subset of the standard applications command set.
- A proxy generally performs no disk access other than to read its initial configuration file.

Examples

These are several examples of bastion host systems/services:

- Web server
- DNS server(Domain Name System)
- Email
- FTP server (File Transfer Protocol)
- Proxy server

8. FIREWALL CONFIGURATIONS

There are three common firewall configurations:

8.1 Dual-Homed Host Architecture

A dual-homed host architecture is built around the dual-homed host computer, a computer which has at least two network interfaces. Such a host could act as a router between the networks these interfaces are attached to. It is capable of routing IP packets from one network to another. However to implement a dual-homed host type of firewalls architecture this routing function is to be disabled. Thus IP packets from one network (e.g., the Internet) are not directly routed to the other network (e.g., the internal, protected network). Systems inside the firewall can communicate with the dual-homed host and systems outside the firewall (on the Internet) can communicate with the dual-homed host but these systems can't communicate directly with each other. IP traffic between them is completely blocked. The network architecture for a dual-homed host firewall is pretty simple. The dual homed host sits between and is connected to, the Internet and the internal network. Dual-homed hosts can provide a very high level of control. If packets are not allowed to go between external and internal networks at all any packet on the internal network that has an external source is evidence of some kind of security problem. In some cases a dual-homed host will allow to reject connections that claim to be for a particular service but that don't actually contain the right kind of data. (A packet filtering system on the other hand has difficulty with this level of control.) However it takes considerable work to consistently take advantage of the potential advantages of dual-homed hosts. A dual-homed host can only provide services by proxying them or by having users log into the dual-homed host directly.

8.2 Screened host architecture

The bastion host sits on the internal network. The packet filtering on the screening router is set up in such a way that the bastion host is the only system on the internal network that hosts on the Internet can open connections to (for example to deliver incoming email). Even then only certain types of connections are allowed. Any external system trying to access internal systems or services will have to connect to this host. The bastion host thus needs to maintain a high level of host security. The packet filtering also permits the bastion host to open allowable connections (what is "allowable" will be determined by site's particular security policy) to the outside world. The packet filtering configuration in the screening router may do one of the following:

- Allow other internal hosts to open connections to hosts on the Internet for certain services
- Disallow all connections from internal hosts (forcing those hosts to use proxy services via the bastion host).

This architecture allows packets to move from the Internet to the internal networks it may seem more risky than a dual-homed host architecture which is designed so that no external packet can reach the internal network. In practice however, the dual-homed host architecture is also prone to failures that let packets actually cross from the external network to the internal network. (Because this type of failure is completely unexpected they are unlikely to be protected against attacks of this kind.) Furthermore it's easier to defend a router which provides a very limited set of services than it is to defend a host. For most purposes the screened host architecture provides both better security and better usability than the dual-homed host architecture.

Compared to other architectures, there are some disadvantages to the screened host architecture. The major one is that if an attacker manages to break in to the bastion host, there is nothing left in the way of network security between the bastion host and the rest of the internal hosts. The router also presents a single point of failure if the router is compromised the entire network is available to an attacker.

8.2 Screened Subnet Architecture

The screened subnet architecture adds an extra layer of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the Internet. Bastion hosts are the most vulnerable machines on the network. In spite of best efforts to protect them they are the machines most likely to be attacked, because they're the machines that can be attacked. If as in screened host architecture the internal network is wide open to attack from bastion host then the bastion host is a very tempting target. There are no other defenses between it and other internal machines (besides whatever host security they may have which is usually very little). By isolating the bastion host on a perimeter network, the impact of a break-in on the bastion host can be reduced. It gives an intruder some access, but not all. With the simplest type of screened subnet architecture there are two screening routers each connected to the perimeter net. One sits between the perimeter net and the internal network and the other sits between the perimeter net and the external network (usually the Internet). To break into the internal network with this type of architecture an attacker would have to get past both routers. Even if the attacker somehow broke in to the bastion host, he'd still have to get past the interior router. There is no single vulnerable point that will compromise the internal network. Some sites go so far as to create a layered series of perimeter nets between the outside world and their interior network. Less trusted and more vulnerable services are placed on the outer perimeter nets farthest from the interior network. The idea is that an attacker who breaks into a machine on an outer perimeter net will have a harder time successfully attacking internal machines because of the additional layers of security between the outer perimeter and the internal network. This is only true if there is actually some meaning to the different layers. However if the filtering systems between each layer allow the same things between all layers the additional layers don't provide any additional security.

9. FUTURE ASPECTS

Firewalls will have to be able to communicate with network security control systems reporting conditions and events allowing the control system to reconfigure sensors and response systems. A firewall could signal an intrusion detection system to adjust its sensitivity as the firewall is about to allow an authenticated connection from outside the security perimeter. A central monitoring station could watch all this, make changes, react to alarms and other notifications and make sure that all antivirus software and other content screening devices were functioning properly. The Intrusion Detection System (IDS) and firewall reconfiguration of network routers based on perceived threat is a reality today. Also firewall resident IDS and help-desk software enables another vendor's system to expand from a prevention mechanism into detecting and responding. The evolution continues and firewalls are changing rapidly to address the next 100 (Internet) years.

CONCLUSION

Firewalls play an important part in a multilevel multilayer security strategy. Internet security firewalls will not go away because the problem firewalls address-access control and arbitration of connections in light of a network security policy will not go away. As use of the Internet and internetworked computers continues to grow the use of Internet firewalls will grow. They will no longer be the only security mechanism but will cooperate with others on the network. Firewalls will morph as they have from what we recognize today just as walls of brick and mortar were eventually replaced by barbed wire, motion sensors, video cameras, brick and mortar. But Internet firewalls will continue to be a required part of the methods and mechanisms.

REFERENCES:

- [1]. Audin, G. "Next-Gen Firewalls :What to Expect." Business communications Review, June 2004.
- [2]. Bellovin, S. and Cheswick, W. "Networks Firewalls". IEEE Communications magazine, September 1994.
- [3]. Champman, D., and Zwicky, E. Building Internet Firewalls. Sebastopol, CA; O' Reilly, 2000.
- [4]. Cheswick, W., and Bellovin, S. Firewalls and Internet Security : Repelling the wily Hacker. Reading, MA :Addison – Wesley, 2003.
- [5]. Felten, E. "Understanding Trusted computing: Will Its Benefits outweigh Its Drawbacks?" IEEE Security and Privacy, May/June 2003.
- [6]. Gasser, M. Building a secure computer System. New York: Van Nostrand Reinhold, 1998.
- [7]. Gollmann, D. Computer Security. New York: Wiley, 1999.

INTERNET PROTOCOL TELEVISION (IPTV)

Amninder Kaur

Asst. Professor ,Department of Electronics and Communication Engineering
Dronacharya college of engineering,
Gurgaon-123506, India
Email: amninder_kaur@rediffmail.com

Shampy Ajrawat

Asst. Professor ,Department of Electronics and Communication Engineering
Dronacharya college of engineering,
Gurgaon-123506, India
Email: shampy19sweet@gmail.co.in

ABSTRACT:

IPTV is in the early stages of fundamentally changing the way programming and advertising is delivered to consumers. While much of the initial focus of IPTV deployments is aimed at quality delivery of streaming video, consumers will be won or lost based on which IPTV service best fits their lives. IPTV service delivery requires both quality video and event-based, personalized data management unique to each viewer. For IPTV to meet its full potential, service deployments need a data management and middleware layer that can scale to support millions of consumers concurrently interacting with thousands of information sources in real time. This paper will investigate the technology that is fueling this new Internet protocol television (IPTV) infrastructure. The first portion will be looking at the video encoding method and the second portion will focus on the video-over-IP network design that is being used for IPTV

Keywords: Multimedia Computer, IP Set Top Boxes (IP STB), IP Televisions

1. INTRODUCTION:

IPTV is basically a fusion of voice, video, and data service. It is not a new idea or, rather, development, but it is a result of high bandwidth and high speed Internet access. In earlier days, the speed of the Internet did not suit the concept and, as a result, it affected the voice and video services. In recent times, the speed of Internet and bandwidth has increased considerably, making IPTV prevail and become reasonably successful. Also, first generation Set Top Boxes were prohibitively expensive. Technology costs now permit a viable business model.

Internet Protocol Television (IPTV) is a service for the delivery of broadcast TV, movies on demand and other interactive multimedia services over a secure, end-to-end operator managed broadband IP data network with desired QOS to the public with a broadband Internet connection. IPTV system may also include Internet services such as Web access and VOIP where it may be called Triple Play and is typically supplied by a broadband operator using the same infrastructure. IPTV is not the Internet Video that simply allows users to watch videos, like movie previews and web-cams, over the Internet in a best effort fashion. IPTV technology offers revenue-generating opportunities for the telecom and cable service providers. For traditional telephone service providers, Triple Play is delivered using a combination of optical fiber and digital subscriber line (DSL) technologies to its residential base. Cable television operators use a similar architecture called hybrid fiber coaxial (HFC) to provide subscriber homes with broadband, but use the available coaxial cable rather than a twisted pair for the last mile transmission standard. Subscriber homes can be in a residential environment, multi-dwelling units, or even in business offices.

2. MAJOR FUNCTIONAL COMPONENTS OF THE IPTV ARCHITECTURE:

- **Content Sources** - It receives video content from producers, and other sources, encodes the content and, for VoD, stores content in an acquisition database.
- **Service Nodes** - It receives video streams in various formats, then reformats and encapsulates them for transmission with appropriate Quality of Service (QoS). Service Nodes also communicate with the Customer Premises Equipment (CPE) for service management.
- **Wide Area Distribution Networks** - This is the core and access network that provides the distribution of IPTV data streams from the Service Nodes to the Customer Premises. The Networks include the backbone network and access equipments. For telecom operators, the Digital Subscriber Line Access Multiplexers (DSLAMs) is often used as the access equipment, while for cable operator's hybrid fiber coaxial (HFC) is used.
- **Customer Access Links** - These are the existing loop plant and the phone lines to homes using the higher-speed DSL technologies such as ADSL2+ and VDSL. For cable subscribers, DOCSIS is used. Service providers may also use a combination of Fiber-to-the Curb (FTTC) and DSL technologies or implement direct Fiber-to-the-Home (FTTH) access depending on the richness of their IPTV service offerings.

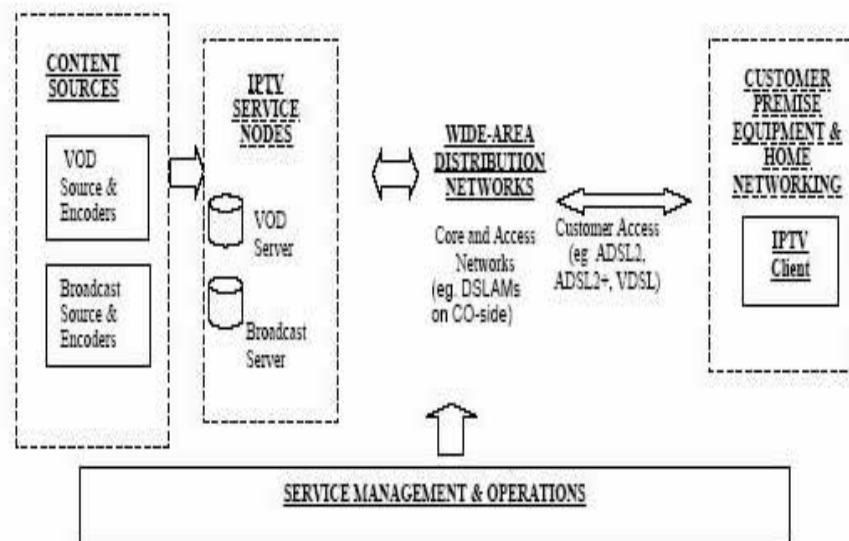


Fig1: IPTV Architecture

- **Customer Premises Equipment (CPE)** - The CPE device provides the broadband network termination (B-NT) functionality at a minimum, and may include other integrated functions such as routing gateway, set-top box and home networking capabilities.
- **IPTV Client** - The IPTV Client is a device, such as a set-top box, that terminates the IPTV traffic at the customer premises. It performs the functional processing such as setting up the connection and QoS with the Service Node, decoding the video streams,

channel change functionality, user display control, and connections to standard-definition TV or HDTV monitors.

3. IPTV SYSTEM

This diagram shows the IPTV system gathers content from a variety of sources including network feeds, stored media, communication links and live studio sources. The head-end converts the media sources into a form that can be managed and distributed. The asset management system stores, moves and sends out (playout) the media at scheduled times. The distribution system simultaneously transfers multiple channels to users who are connected to the IPTV system. Users view IPTV programming on analog televisions that converted by adapter box (IP set top box), on multimedia computers or on IP televisions (data only televisions).

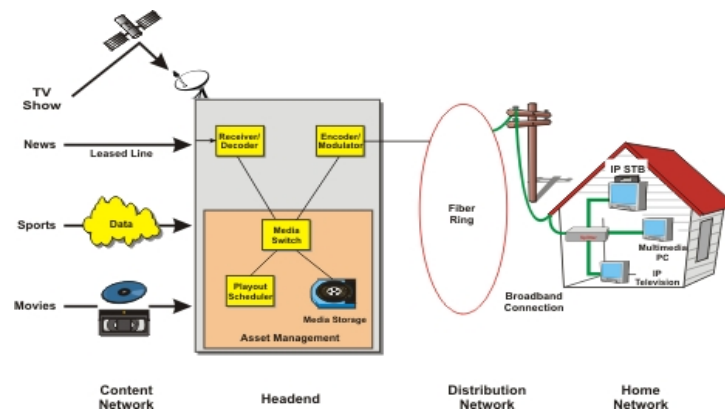


Fig.2: Diagram of IPTV System

3.1 IP STB:

This figure shows a functional block diagram of an IP STB. This diagram shows that an IP STB typically receives IP packets that are encapsulated in Ethernet packets. The IP STB extracts the IP packets to obtain the transport stream (TS). The channel decoder detects and corrects errors and provides the transport stream to the descrambler assembly. The descrambler assembly receives key information from either a smart card or from an external conditional access system (e.g. via a return channel). Using the key(s), the STB can decode the transport stream and the program selector can extract the specific program stream that the user has selected.

The IP STB then demultiplexes the transport stream to obtain the program information. The program table allows the IP STB to know which streams are for video, audio and other media for that program. The program stream is then divided into its elementary streams (voice, audio and control) which is supplied to a compositor that create the video signal that the television can display.

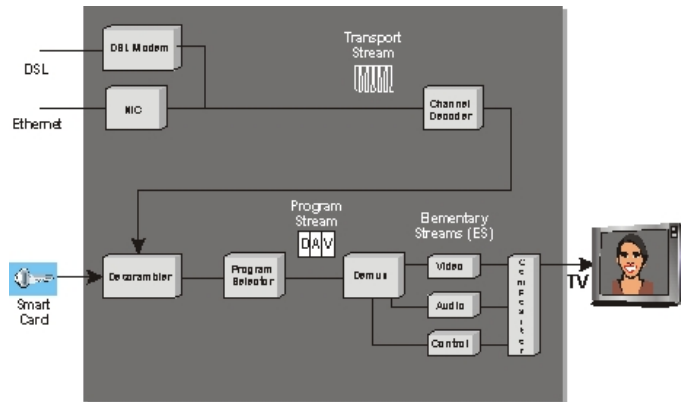


Fig. 3: Diagram of IP STB

3.2 IP VIDEO SYSTEMS:

This figure shows how video can be sent via an IP transmission system. This diagram shows that an IP video system digitizes and reformats the original video, codes and/or compresses the data, adds IP address information to each packet, transfers the packets through a packet data network, recombines the packets and extracts the digitized video, decodes the data and converts the digital video back into its original video form.

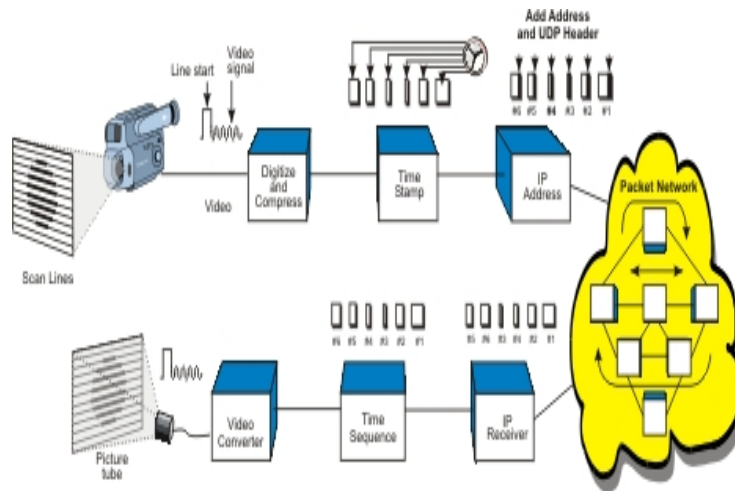


Fig. 4: Diagram of IP Video System

4. IPTV NETWORK AND SERVICE QUALITY METRICS:

4.1 Video on demand – VOD:

Video on demand (VOD), enable you to watch video which you want to watch. Video-on-Demand is an ideal application for broadband IP networks. It provides entertainment-on-demand by taking advantage of the network's two-way communication capability. IP-based VOD systems are commonly distributed to make efficient use of broadband IP infrastructures such as DSL. In these

environments it is important to reassure content owners that their content is protected, both while in transit over the backbone and while sitting on remote VOD server installations

4.2 Interactivity and T-commerce:

Interactive television allows viewer to interact with television content i.e. there is two way connection with Content provider and viewer. Generally It is known as iTV. T-commerce enables you to buy products from TV. T-commerce comprises TV shopping, direct response TV, Travel shopping and Interactive TV applications

4.3 Follow Me TV:

IPTV enables user to have same experience anywhere as they have in home while watching TV. IPTV allows users to store their personal preferences at Service Provider end so that they can use anywhere. They can also share their personal preferences with others.

4.4 Collaborative/Shared Viewing:

IPTV enables you to share viewing between digital home equipments. IPTV allows you to do Home Networking i.e. you can connect your any device like DVD player, STB, VCR, Digital Cams, PC or any other devices with your TV using IP to share or store content between them.

5. IPTV STANDARDS:

IPTV solutions are based on a combination of standard and proprietary technologies. There is no existing standard which cover all IPTV needs but there are multiple standards which could fulfill certain requirement of IPTV. MPEG : MPEG standards can be used for Content Encoding, Streaming and delivering. MPEG-21. DSL-Forum : For remote management protocol TR-069 and for Qos TR-098 can be used. CEA (Consumer Electronic Association) and DLNA (Digital Living Networks Alliance): defines some standards for home equipments. And DVB standards are used for delivering the contents.

There are other standardization bodies which are doing efforts for IPTV like, The IPTV Interoperability Forum/ Alliance for Telecommunications Industry Solutions (IIF/ATIS). ITU-T IPTV Focus Group formed Apr 13th, 2006 to coordinate the IPTV global standardization efforts. Strong push from Korea with Telecommunications Technology Association (TTA), China with Communication Standards Association (CCSA), and Japan with Association of Radio Industries and Businesses (ARIB)

6. FUTURE IPTV:

IPTV with NGN is a future of IPTV. A Next-Generation Network (NGN) can be describe as a telecommunications packet-based network that handles heavy traffic (such as voice, data, and multimedia). NGN architecture enables content providers to deliver their heavy media content across the network. It allows them to move beyond IPTV/Multimedia to develop and deliver a various integrated media services to Multimedia Home Networks it also provide unparalleled linkages among the network, middleware and video/IPTV services.

CONCLUSION:

IPTV enables broadband service providers provide the “triple play” to users, open opportunity to takeover TV market and earn money. On the other hand viewer will get advanced and on demand entertainment. An IPTV offers you a advanced multi channel high definition TV (HDTV) as well as on demand entertainment.

IPTV technology promises to give better and more contents available, Because of two way connection between viewer and service provider will know the views personal preferences and entertain them accordingly. IPTV Middleware providers' gives focus on making more content available to viewers, easy to use and portable solutions.

REFERENCES:

- [1] K. Kerpez, G. Lapiotis, J. B. Lyles, R. Vaidyanathan, "Network Management, Surveillance, and Testing for IPTV Service Assurance," IEC Report on IPTV, To Be Published.
- [2] Dino Stavrou, "Delivering the Promise of IPTV," IEC Report on IPTV, To Be Published.
- [3] ITU-R BT.1359-1, "Relative Timing of Sound and Vision for Broadcasting," 1998.
- [4] Video Quality Experts Group (VQEG), www.its.bldrdoc.gov/vqeg.
- [5] ITU-T Recommendation J.144, rev. 1, "Objective perceptual video quality measurement techniques for digital cable television in the presence of a full reference," (March 2004).
- [6] Pinson and Wolf, "A New Standardized Method for Objectively Measuring Video Quality," IEEE Transactions on Broadcasting, pp. 312-322, September 2004.
- [7] ANSI T1.801.03-2003, "Digital Transport of One-Way Video Signals - Parameters for Objective Performance Assessment."
- [8] Pattara-Atikom, S. Banerjee, and P. Krishnamurthy, "Predicting the Quality of Video Transmission over Best Effort Network Service," Proceedings of the 12th International IEEE Conference on Computer Communications and Networks, ICCCN 2003. pp. 445-449.
- [9] A. R. Reibman, V. A. Vaishampayan, and Y. Sermadevi, "Quality Monitoring of Video over a Packet Network," IEEE Transactions on Multimedia, Vol. 6, pp. 327-334, April 2004.
- [10] S. Tao, J. Apostolopoulos, and R. Guerin, "Real-Time Monitoring of Video Quality in IP Networks," ACM NOSSDAV '05, pp. 129-134, June 13-14, 2005.

WAVELET BASED COMPRESSION OF RADIOLOGICAL IMAGES FOR TELEMEDICINE APPLICATIONS

Taslima Ahmed (Sr.Lecturer), Tazeem Ahmad Khan (Asstt. Prof.)

IIMT College of Engineering Gr. Noida, UPTU, INDIA
ahmed.taslima@gmail.com, khan_taz@yahoo.com

ABSTRACT

Recently, the wavelet transform has emerged as a cutting edge technology within the field of image compression research. Embedded zero tree wavelet coder (EZW) is the first algorithm to show the full power of wavelet based image compression. In this paper we have evaluated and compared the performance of Haar and Daubechies wavelets for radiological image compression using EZW. The comparison is made between the Haar and Daubechies 2, 4 and 6 wavelets for some modalities of medical images (such as X-Ray, CT-scan and MRI). All the images are 8 bit gray scale images and size 128x128 pixels. The compression process is done at different threshold values. The qualitative and quantitative results of these simulations are presented. Our results show that different wavelet filters performed differently for different medical images, but the difference between each other was not great in case of CTscan and MRI images while it is in case of Xray image. So, the choice of best wavelet filter in medical image compression is mostly depends on the image content.

KEYWORD: DWT, EZW , JPEG

1. Introduction

Many evolving multimedia applications require transmission of high quality images or video over networks with limited bandwidth. One obvious way to solve this problem is to increase the bandwidth available to all users but it will definitely increase the technological and economic difficulties. Another way is to reduce the volume of the data that must be transmitted. In addition, advanced medical imaging requires storage of large quantities of digitized clinical data which must be compressed before transmission and storage. However, the compression will reduce the image fidelity, especially when the images are compressed at lower bit rates. The reconstructed images suffer from blocking artifacts and the quality of the image is severely degraded under high compression ratio as shown by JPEG standard [1]. In recent years, research activities in image coding have often focused on the discrete wavelet transform (DWT). The first journal paper describing a wavelet application in medical imaging -- noise reduction in MRI by soft – thresholding in the wavelet domain – also appeared in 1992 [2]. An article on lossless compression of grayscale medical images is found in [3]. An article on efficient image compression of medical images using the wavelet transform and fuzzy c-means clustering on region of interest is found in [4]. A large palette of wavelet applications in medical imaging is provided in [5]. The concept of EZW coder was given by Shapiro through its groundbreaking paper in 1993 [6]. EZW coder is the first algorithm to show the full power of wavelet based image compression. Performance evaluation of Haar wavelet on image compression is given in [7]. Good compression results are obtained using haar and daubechies wavelet filters by other researchers also [1].

2. Wavelet Transform

Wavelets are mathematical functions that cut data into different frequency components, and then study each component with a resolution method to its scale. Wavelet transform (WT) represents an image as a sum of wavelet functions (wavelets) with different locations and scales. A wavelet is a (ideally) compact function, i.e., outside a certain interval it vanishes. Implementations are based on the fast wavelet transform, where a given wavelet (mother wavelet) is shifted and dilated so as to provide a base in the function space. In other words, a one- dimensional function is transformed into a two dimensional space, where it is approximated by coefficients that depend on time

(determined by the translation parameter) and on scale, (determined by the dilation parameter). Any decomposition of an image into wavelets involves a pair of waveforms: one to represent the high frequencies corresponding to the detailed parts of an image (wavelet function Ψ) and one for the low frequencies or smooth parts of an image (scaling function Φ). The two waveforms are translated and scaled on the time axis to produce a set of wavelet functions at different locations and on different scales. Each wavelet contains the same number of cycles, such that, as the frequency reduces, the wavelet gets longer. The result of wavelet transform is a set of wavelet coefficients, which measure the contribution of the wavelets at these locations and scales.

3. Embedded zero tree wavelet (EZW) encoding

The concept of EZW was introduced by Shapiro. The zero-tree structure combined with bit plane coding is an efficient compression scheme for the discrete wavelet transformation. The *embedded zero-tree wavelet* (EZW) coding scheme has proven its efficiency, quality and computation simplicity. Also the EZW algorithm generates an embedded bit stream in which information is sent to the decoder in the order of its importance; importance is judged by how much the information reduces the distortion of the reconstructed image. This embedded technique has two important advantages. First, the bit rate control allows one to stop the coding process at any point. Second, the image can be reconstructed from a point where the encoded bit stream has been disrupted, even with reduced quality.

4. Implementation

In this work, BMP format radiological images are used for compression and implementation is done using MATLAB. Figure 1 shows the block diagram of our approach.

5. Results

Three different radiological images: X-ray, CT-scan, MRI was taken and scanned using HP scanner with 200 dpi. The scanned images were converted to appropriate dimensions through Adobe photoshop 7.0 tools. All these images are on gray scale with depth 8 bits per pixel and size 128x128 pixels. The width and height of each image is 1.63cmx1.63cm with 8 bits/sample, thereby yielding 16384 samples in total. The gray scale image had a minimum level of 0 and a maximum of 255. The algorithm is tested for the BMP format images. The filter used was Haar and Daubechies 2, 4, 6 (denoted as db2, db4, db6). In this work we compress each medical image from different modalities by using wavelets mentioned above. All these radiological images are of 8-bit gray scale images. Table-1 shows the performance evaluation of EZW coder applied to the wavelet coefficients of different radiological images of 128x128. Six level decomposed images are used. Reconstructed images at different PSNR values are achieved by assigning the different threshold values in the quantization process. Table-1 shows the values of compression ratio, bits per pixel and PSNR for different wavelets at different threshold values. All these results are taken for three radiological images (CT-Scan, X-ray and MRI). Figures 2 to 4 shows the Original images and reconstructed images at different PSNR values.

6. Discussion on results

The results of EZW coder implementation on MATLAB are shown in Figures 5 to 7. The original X-ray image is illustrated in Fig. 2(a) and the reconstructed images obtained using EZW coder at different threshold values 4, 32 and 64 are in Figures 2(b), 2(c) and 2(d) respectively. It may be observed that as the threshold value is decreased, more and more lower bits are transferred due to the addition of more number of detail coefficients of image at the decoder side. This results in the decrease in compression ratio and the value of PSNR therefore increases. Fig. 3(a) shows the original CT-Scan image and the reconstructed images at threshold values 2, 32 and 128 are shown in figure 3(b), 3(c) and

3(d). Fig. 4(a) shows the original MRI image and the reconstructed images at threshold values 2, 32 and 64 are shown in figure 4(b), 4(c) and 4(d).

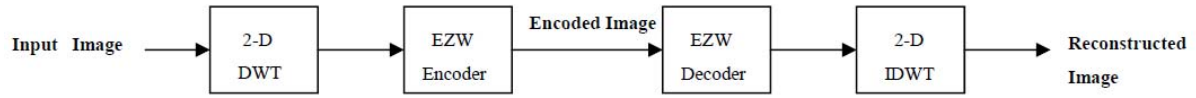


Figure 1- Block diagram

TABLE 1
Performance evaluation of EZW at 6 levels of decomposition for 128x128 radiological
Images (gray scale)

IMAGE	THRESHOLD	Haar wavelet			db-2 wavelet			db-4 wavelet			db-6 wavelet		
		C.R	bpp	PSNR(dB)	C.R	bpp	PSNR(dB)	C.R	bpp	PSNR(dB)	C.R	bpp	PSNR(dB)
CT-Scan	1	2.318	3.451	45.68	2.418	3.308	47.18	2.158	3.707	44.99	1.774	4.51	47.91
X-Ray		2.128	3.76	54.33	2.392	3.344	48.44	2.1	3.81	50.08	1.661	4.816	49.04
MRI		1.283	6.235	44.62	1.258	6.36	46.10	1.131	7.075	43.62	1.123	7.121	45.16
CT-Scan	2	3.148	2.541	44.87	3.338	2.396	45.95	2.982	2.682	44.17	2.38	3.361	46.44
X-Ray		3.198	2.5	52.52	3.704	2.16	46.52	3.095	2.584	47.53	2.38	3.361	46.92
MRI		1.67	4.79	43.84	1.676	6.36	46.10	1.516	5.277	42.80	1.295	6.177	44.00
CT-Scan	4	4.606	1.736	42.49	4.936	1.62	43.04	4.475	1.787	42.00	3.407	2.348	43.18
X-Ray		5.307	1.507	48.90	6.05	1.322	43.26	4.766	1.678	43.81	3.334	2.4	43.57
MRI		2.82	2.826	40.76	2.989	2.676	40.97	2.721	2.94	40.06	2.232	3.584	40.64
CT-Scan	8	7.571	1.056	38.56	8.350	0.958	39.95	7.291	1.097	38.49	5.162	1.549	38.92
X-Ray		10.126	0.79	44.62	10.233	0.781	39.34	7.416	1.078	39.75	4.88	1.64	39.75
MRI		5.70	1.403	36.01	6.36	1.257	36.06	5.56	1.438	35.75	4.47	1.789	35.99
CT-Scan	16	14.60	0.548	34.14	16.77	0.477	34.54	13.22	0.605	34.54	8.827	0.906	34.62
X-Ray		21.417	0.373	40.41	18.724	0.427	35.5	12.545	0.637	35.92	7.798	1.028	35.88
MRI		13.023	0.614	31.73	32.83	0.244	28.56	26.172	0.305	28.56	8.511	0.94	31.83
CT-Scan	32	34.565	0.231	29.84	38.64	0.207	30.38	24.862	0.322	30.57	15.784	0.506	30.46
X-Ray		48.76	0.164	36.64	40.156	0.202	31.86	21.416	0.373	32.20	12.73	0.628	32.10
MRI		34.06	0.234	28.04	32.83	0.244	28.56	26.172	0.305	28.56	17.228	0.464	28.47
CT-Scan	64	85.33	0.093	26.08	90.519	0.088	26.87	49.35	0.162	27.19	31.089	0.257	27.05
X-Ray		113.77	0.07	33.45	80.709	0.1	28.34	39.67	0.201	28.73	27.9	0.286	28.63
MRI		106.38	0.075	25.04	103.04	0.077	25.52	73.142	0.109	25.52	41.27	0.194	25.42
CT-Scan	128	315.07	0.025	23.17	248.24	0.032	24.09	127	0.063	24.25	73.801	0.108	23.99
X-Ray		303.4	0.026	30.64	153.12	0.052	25.54	63.50	0.126	25.56	38.73	0.206	25.79
MRI		341.33	0.023	22.51	334.36	0.024	22.82	192.75	0.041	23.00	124.12	0.064	22.77

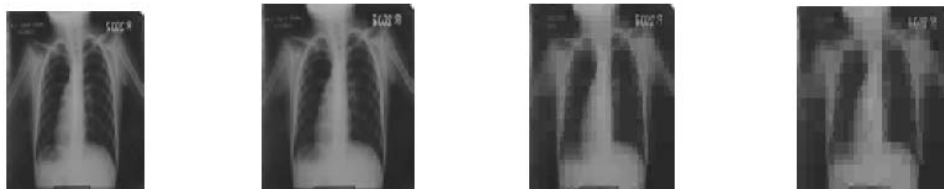


Figure 2- (a) Original X-ray image (b) Reconstructed X-ray image PSNR=48.90 (c) Reconstructed X-ray image PSNR=36.63 (d) Reconstructed X-ray image PSNR=33.44

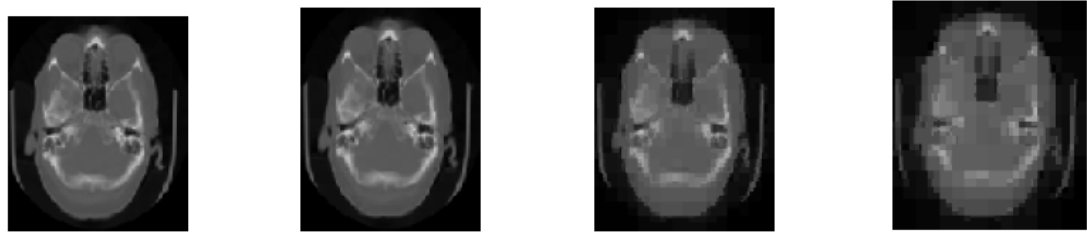


Figure 3- (a) Original CT-Scan image (b) Reconstructed CT-Scan image PSNR = 44.87 (c) Reconstructed CT-Scan image PSNR=29.83 (d) Reconstructed CT-Scan image PSNR=23.17

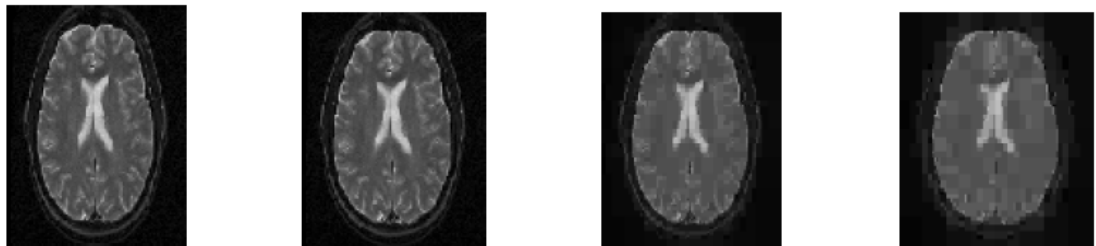


Figure 4- (a) Original MRI image (b) Reconstructed MRI image PSNR = 44.74 (c) Reconstructed MRI image PSNR=28.56 (d) Reconstructed MRI image PSNR=25.52

Figure 5 shows the curve between the bits per pixel and PSNR values for different wavelets (Haar, db2, db4, db6) applied to CT-scan image. The compression process is done at different threshold values (1 to 128). From the results that obtained, it is observed that the db2 is the best suited wavelet for CT-scan image at all bit rates from 0.032 to 3.308 as it gives the highest and consistent PSNR values for this image content. It is seen from the curve that the different wavelet filter performed differently for different radiological images but the difference is not great in case of CT-scan image. Figure 6 shows the curve between the Bits per pixel and PSNR values for different wavelets (Haar, db2, db4, db6) applied to MRI image. The compression process is done at different threshold values (1 to 128). From the results that we obtained, it is observed that the haar is the best suited wavelet for X-ray image and 'db6' gives the worst performance at all bit rates from 0.026 to 3.76 as it gives the highest and consistent PSNR values. The difference between curves is considerable in case of X-ray image for this image content. There will be approximate 9 db decrease in value of PSNR at the same compression ratio if we use 'db6'. Figure 7 shows the curve between the Bits per pixel and PSNR values for different wavelets (Haar, db2, db4, db6) applied to MRI image. The compression process is done at different threshold values (1 to 128). From the results that we obtained, we observe that the 'db2' is the best suited wavelet for MRI image.

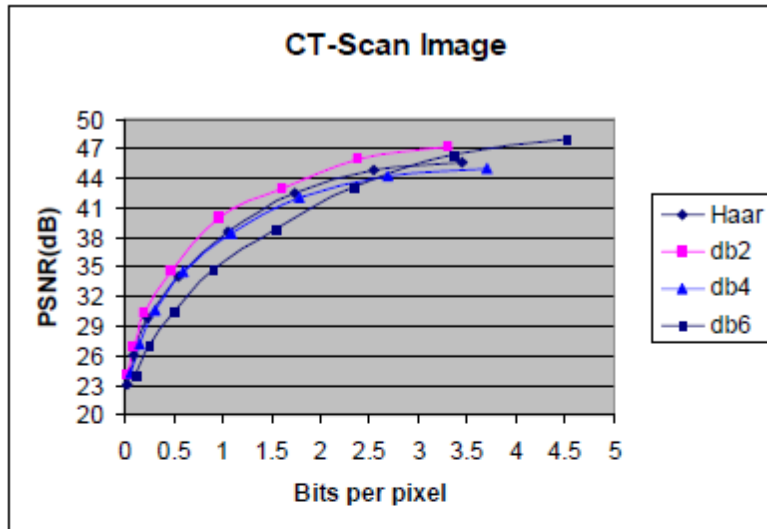


Figure 5 - PSNR vs. Bpp for CT-scan image

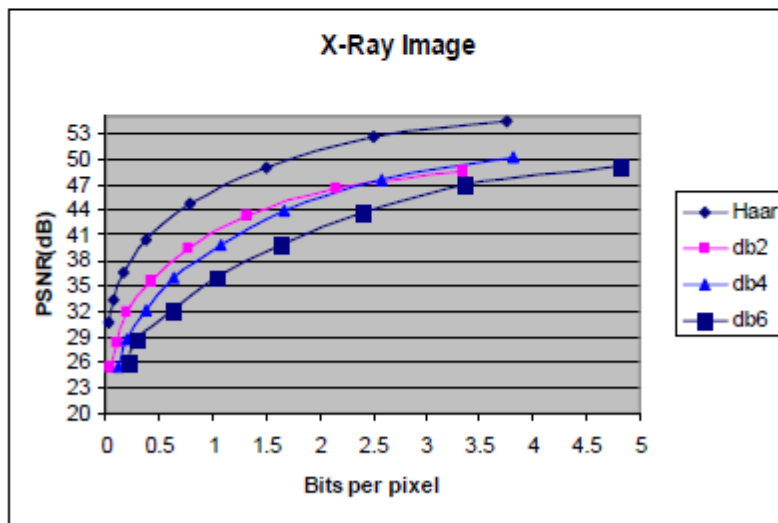


Figure 6 - PSNR vs. Bpp for X-ray image

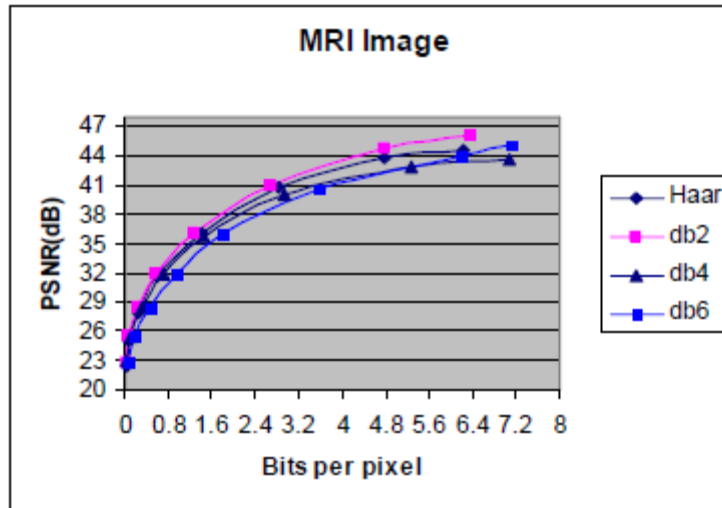


Figure 7 - PSNR vs. Bpp for MRI image

7. CONCLUSION

From the results presented in this paper, it can be concluded that different wavelet filters performed differently for different radiological images but the difference is not great in case of CT-scan and MRI images while it is so in case of X-ray image. So, the choice of best wavelet in radiological image compression is mostly depend on the image content. It is also observed from the results that 'haar' is the best suited wavelet for compression of X-ray image we have taken as it gives the highest PSNR values at all bit rate. For CT-scan and MRI image 'db2' is the best suited wavelet.

References

- [1] Sonja Grgic, Mislav Grgic, " Performance Analysis of Image Compression using Wavelet",IEEE Transactions on Industrial Electronics, vol.48, no. 3, pp. 682-695, June 2001.
- [2] J.B Weaver, X.Yansun, .M.Healy Jr, and L.D. Cromwell, "Filtering noise from images with wavelet transforms,"Magn. Reson. Med., vol.21,pp.288-95,1991
- [3] David A.Clunie, "Lossless Compression of Grayscale Medical Images- Effectiveness of Traditional and state of the Art Approaches" Quintiles Intelligent Imaging, 521 Plymouth road, Suite 115, Plymouth Meeting PA 19462
- [4] D.A Karras, S.A Karkanis and D.E. Maroulis, "Efficient Image Compression of Medical Images Using the wavelet Transform and Fuzzy c-means clustering on Regions of Interest" Univ. of Piraeus, dept. of Business Administration, rodu 2, Ano Iliupolis. Athens 16342,Greece
- [5] A.Aldroubi and M.Unser, Wavelets in Medicine and biology. Boca raton, FL: CRC, 1996.
- [6] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients", IEEE Trans. On Signal Processing, 41 (December 1993) 3445-3462
- [7] Rohini Nagapadma, G.J. Ramya, H.N Nagalakshmi and Narsimh Kaulgud, "Performance Evaluation of Haar Wavelet on Image Compression"Proceedings of the International Conference on Cognition and Recognition
- [8] Amit Garg, " Telemedicine for a modern hospital", M.Tech. Proj. Report (3rd sem) , Deptt of Electronics Engg, AMU, 2005

Quality of Service In Networks

Kavita Choudhary
KIIT College of Engineering, Gurgaon
kavitapunia@gmail.com

ABSTRACT

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

A network or protocol that supports QoS may agree on a traffic contract with the application software and reserve capacity in the network nodes, for example during a session establishment phase. In the field of telephony, quality of service was defined in the ITU standard X.902 as "A set of quality requirements on the collective behavior of one or more objects". When looking at packet-switched networks, Quality of Service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, Grade of Service, etc. Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver:

Dropped packets

The routers might fail to deliver (drop) some packets if they arrive when their buffers are already full. Some, none, or all of the packets might be dropped, depending on the state of the network, and it is impossible to determine what will happen in advance. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

Delay

It might take a long time for a packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. In some cases, excessive delay can render an application such as VoIP or online gaming unusable.

Jitter

Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.

Out-of-order delivery

When a collection of related packets is routed through the Internet, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a

different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of isochronicity.

Error

Sometimes packets are misdirected, or combined together, or corrupted, while on route. The receiver has to detect this and, just as if the packet was dropped, ask the sender to repeat itself.

QoS Protocols

- ReSerVation Protocol (RSVP): Provides the signaling to enable network resource reservation (otherwise known as Integrated Services). Although typically used on a per-flow basis, RSVP is also used to reserve resources for aggregates.
- Differentiated Services (DiffServ): Provides a coarse and simple way to categorize and prioritize network traffic (flow) aggregates.
- Multi Protocol Labeling Switching (MPLS): Provides bandwidth management for aggregates via network routing control according to labels in (encapsulating) packet headers.
- Subnet Bandwidth Management (SBM): Enables categorization and prioritization at Layer 2 (the data-link layer in the OSI model) on shared and switched IEEE 802 networks.

Qos Parameters

QUALITY OF SERVICE PARAMETERS

Service Level	Application	Priority Mapping
1	<ul style="list-style-type: none"> • Non-critical data • Similar to Internet today • No minimum information rate guaranteed 	<ul style="list-style-type: none"> • Best-effort delivery • Unmanaged performance
2	<ul style="list-style-type: none"> • Mission-critical data • VPN outsourcing, e-commerce • Similar to ATM VBR 	<ul style="list-style-type: none"> • Low loss rate • Controlled delay and delay variation
3	<ul style="list-style-type: none"> • Real time applications • Video streaming, voice, videoconferencing 	<ul style="list-style-type: none"> • Low loss rate • Low delay and delay variation

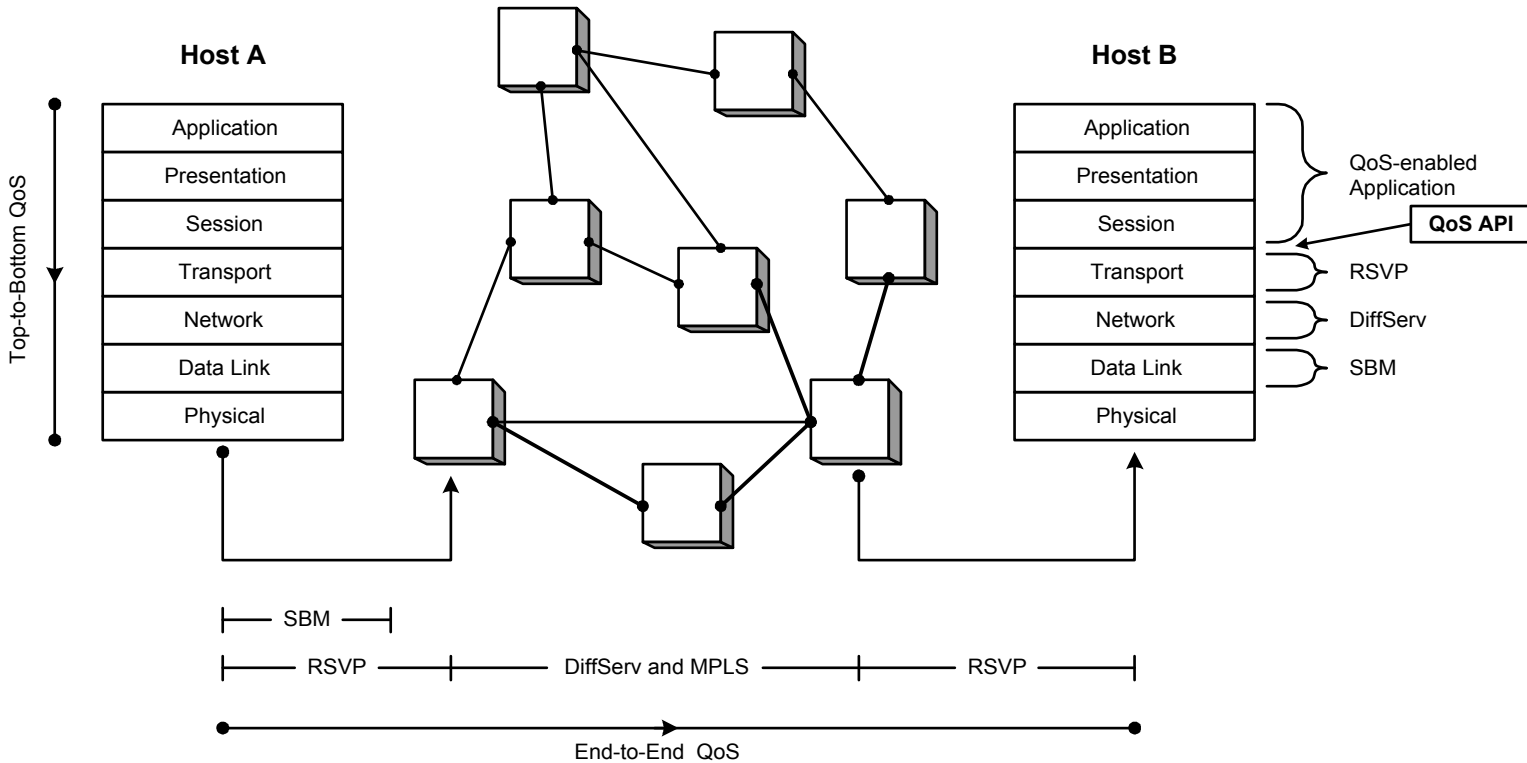


Fig.1: QoS Architecture

Pending Problems

- It is still not clear where to locate QoS functionality.
- It is not clear what QoS support should a protocol provide.
- There is not a clear QoS architecture.
- There is not a clear agreement on services.
- However, many aspects are under consideration.

Conclusion

- IP has provided a “best-effort” service in which network resources are shared equitably. Adding quality of service support (QoS) to the Internet raises significant concerns, since it enables differentiated services that represent a significant departure from the fundamental and simple design principles that made the Internet a success. There is a significant need for IP QoS and protocols have evolved to address this need.
- The standards are not fully developed yet, and there are still some important considerations such as multicast support that require further attention, but deployment is already underway on many IP networks.

Downloads/Seminars/Proceedings_ETCT.html

References



1. eventsandseminars_Archive.html QoS management in mobile IP networks using a terminal assistant in INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT Int. J. Network Mgmt 2009; 19: 1–24.
2. http://www.nortelnetworks.com/solutions/collateral/qos_wp.pdf
3. http://www.qosforum.com/white-papers/qosprot_v3.pdf
4. http://www.qosforum.com/white-papers/Need_for_QoS-v4.pdf