ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 08, pp.36996-37001, August, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

EXPLORATION OF COMPUTER NETWORKS

***Sujata Chowgule and Asha Rani Borah**

Department of Computer Science, New Horizon College of Engineering, Bangalore, India

ARTICLE INFO

Article History:
Received 28th May, 2016
Received in revised form
20th June, 2016
Accepted 06th July, 2016
Published online 31st August, 2016

Key words:

Computer Networks,
Big Data,
Data Mining.

ABSTRACT

Data Analysis has been the source of learning for every field from psychology, biology, astronomy to very recent social networking and online shopping. The customer who has always been the center for any business is even more important to businesses all over the world. The actions, reactions and responses of the customer today can be captured very easily. This is possible due to the widespread use of the computer like devices (PC, laptop, mobile, tablet etc) and networking. Current businesses have seen a steep increase in growth through the use of data mining, analysis and customer behavior predictability. In this paper we present the existing system of computer networks and explore them to understand the significance of each entity, their behavior, scope and limitations. The in-depth learning of computer networks brings the realization as to how frugally the network data has been comprehended. The data about the activities of the users of the computer networks has been studied and used to gain insights of behavior. The data related to the devices themselves remains unexplored to benefit both the user and the provider.

Citation: Sujata Chowgule and Asha Rani Borah, 2016. "Exploration of computer networks", *International Journal of Current Research*, 8, (08), 36996-37001.

INTRODUCTION

Computers today have ceased to exist as standalone entities. The mention of a computer possessed by an individual comes with the assumption that they are definitely connected to the world through the World Wide Web. An Internet connection is or has become a basic facility that is present in every home. The Internet and the connectivity that it provides are playing a very important role in the life of every individual. The world statistics puts the number of Internet Users to 40% of the world population. It was less than 1% in 1995. The number of users has increased tenfold from 1999 to 2013. The number of connections is 3,362,435,789 and counting. The Computers and the Internet are held together by the Network. The world-wide network of computers can be accessed via a computer, mobile telephone, digital TV, games machine, PDA, etc. This Network service can be provided through either a fixed (wired) or mobile network: analogue dial-up modem via standard telephone line, DSL (Digital Subscriber Line), Integrated Services Digital Network (ISDN). This project is sponsored by Mr. Pankaj Kumar Roy, Director, AVIN Networks Private Limited, Bangalore 560102. AVIN Networks is a software developer and supplier providing standards-based and customized Broadcast OSS and Telecom NGOSS solutions. or ADSL, High speed leased lines, Cable modem, Fiber Optic Cables, Satellite broadband network, Power-line, Mobile broadband network, WiMAX, Fixed CDMA via a handset or USB modem, card, or Integrated SIM card in a computer. Hence networking and plumbing are analogous to each other. It places lines of connectivity between the end points that desire to communicate. Today every area of computing be it, Distributed Computing or Distributed Databases is all network based.

****Corresponding author: Sujata Chowgule,***
Department of Computer Science, New Horizon College of Engineering, Bangalore, India.

Computer Networks

Basics of Networking

The basic structure of a computer network [2] consists of one or more end-points that are connected to each other using wires and/or cables. These connected end-points are facilitated to send data (electronic information) to and fro thus enabling communication. The devices used for computing can be workstations, mainframes, PCs, or scientific computers; these devices can be connected to other peripheral devices, such as printers, modems, and CD-ROM towers. *Fig. 1* shows a basic computer network. The end-points may be a Personal Computer, a Wireless Access Point, a Network Printer, a Fax machine, a Server etc. There is no limitation of the number of such end-points, no restriction of the location of the devices and neither a compulsion on the capabilities of the device so as to participate in the network. The connections are possible through the use of various connecting media and devices

(consisting of hardware and software components) such as cables, wires, switches, bridges, routers, gateways etc accommodating traffic between unlike systems.

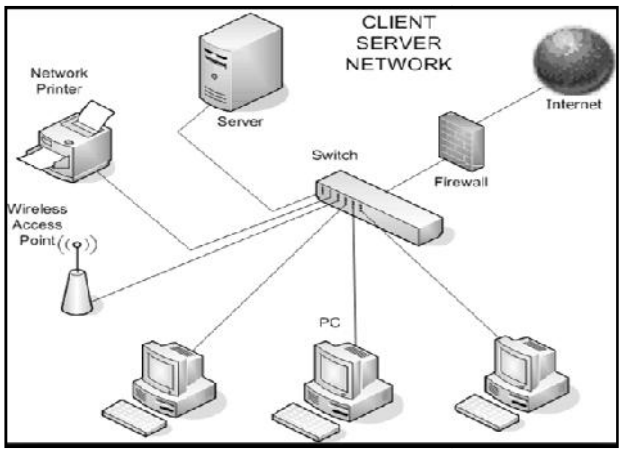

Fig. 1. Network connected of end-point systems

The introduction of standard policies and protocols helped in the networking dissimilar products while reducing the cost. Standardization organizations, government or industry-sponsored, are responsible for a variety of activities such as developing, revising, amending, coordinating and producing technical standards to address the needs of the industry. Standardization regulates the functioning of the industries and providing compatibility among different vendors. The OSI model is the standard for network architecture and is the most commonly used for networking. OSI is based on layered architectures; i.e., different layers in the software and hardware are committed to different network functions. The lower layers exchange information between directly connected nodes and communicate as electronic signals E.g. voltage. The middle layers generally deal in detecting and correcting transmission errors and providing end-to-end connectivity. The upper layers are devoted to higher level functions as translating data for use in end-user applications, encryption and presentation. The Firewall is the protection in a private network from the public network ensuring security of data within the private network. It continuously monitors and controls the information flow. The traffic in a network is governed predefined security rules. Technically the Firewall is a various programs running at the network gateway for the protection of the resources belonging to the private network from the malicious intensions of outsiders or even at times within the private network.

Benefits of Networks

Networks facilitate businesses to reduce their expense and improve competence by sharing data and common equipment, such as printers, among connected computers. Earlier printers were shared in other ways, like carrying information on disks or pen drives from one PC to another, or using manual or electronic data switches, networks provide the capacity to contain more users with less frustration and no manual intervention. The networks thus allow the power of mainframes or minicomputers to be used in harmony with personal computers. The larger machines like the mainframe servers can process large and complex jobs, such as maintaining records that are millions of lines needed by a national company, while individual PCs used by individuals handle smaller jobs such as word processing. Many software programs also offer license agreements for networks, thus making it more cost effective instead of purchasing separate copies for each machine. The costs of implementing a network depend on issues of desired performance, level of compatibility, and whether addition of special components is required. Coordination of all data and applications through a single network can be achieved in various ways. A centralized system when used in administration simplifies many aspects of networking. Computer security among individual hard drives is a laborious task. Using appropriate software, effective implementation can be achieved in a network. Techniques such as password authentication for public users may be used to check access. Generally, security measures are more vulnerable at machines with single user operating systems than those with network security precautions.

Network Devices

The types of machines that can be connected to a network include PCs, intelligent workstations, clients, host computers, dumb terminals, and file and other types of servers. File servers are used to control network activity such as printing, data sharing, and controlling security. When considering the selection of a file server the important factors to be measured are its speed, processor performance, memory, hard drive capacity, and most importantly, its compatibility with network software.

Network Computers

Impelled by the progress in Internet technology only a minimum of required corporate applications could be maintained on the PC and the other applications could credibly be retrieved from a central computer, the server. Advances in software and data portability, such as HTML documents on the Web and the platform-independent Java language, permit the Network Computer users to simply download necessary programs and files from a central repository, instead of storing them locally on each computer. These Network Computers are nothing but the end point systems in the large network of systems. Topology refers to the physical layout of the network, architecture refers to the broad design of the rules computers must follow in order to communicate. The specific rules to be followed are called protocols; thus architectures are collections of protocols and may also include more standards (specifications) for both hardware and software. Architectures may be either centralized or decentralized. The former design class is used when many users need the same information resulting in lower maintenance to update and maintain the network. However, distributed processing via decentralized networks is the upcoming standard. It allows work to be disseminated among participating systems. In the process exploiting capabilities of powerful systems connected in the network.

The topology which is the physical layout of the network is important to configuration management (Douglas E. Comer, 2013). The three commonly used arrangements are the bus,

ring, and star as shown in *Fig. 2*. The bus configuration is characterized by each node being connected to a common cable. The node detects messages addressed to it. This configuration is reliable, using the least amount of cabling and is often used in offices. However, this is not the case in fiber-optic systems. The ring layout nodes retransmit packets of information along adjacent nodes. This configuration has the possibility of greater transmission distances and useful in fiber-optic systems. The components necessary can be more expensive compared to the previously discussed layout. IBM's Token Ring configuration is a popular implementation of the ring layout.

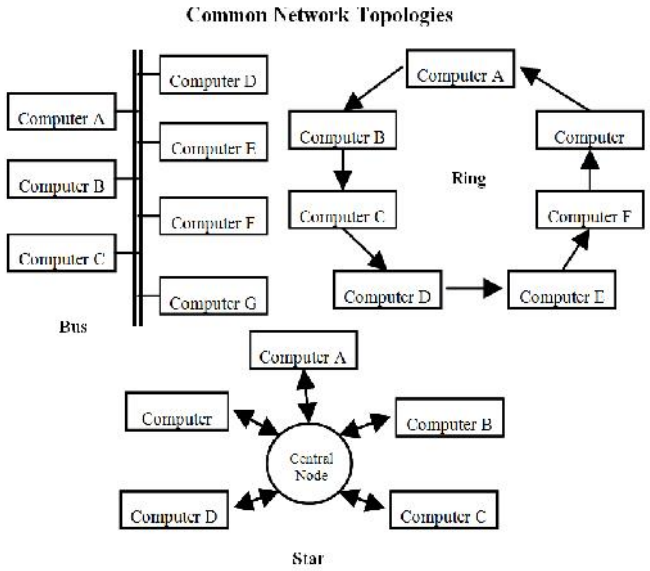

Fig. 2. Common Network Topologies

The star arrangement is one where all traffic is routed through one single central node. It facilitates simplified monitoring and security. Also, unlike the other layouts, the failure of one node does not cause the entire network to fail, unless it is the central node. The central node is however a bottleneck. This drawback is corrected by employing the clustered star layout, in which a number of star networks are linked together.

Servers

Computers that run software so as to facilitate a number of different kinds of network activities are called Servers. They are inherently software packages providing various functionalities. A Server could thus be just another computer that has advanced hardware capabilities and housing or running the specific software packages. A single physical computer system could host any number of server-related processes. The three most commonly used types of server functions are file servers, network servers, and printer servers.

File servers could be run in either a dedicated or a non-dedicated mode. In large network applications, a disk subsystem increases the file server performance. Network servers are used in various network activities, such as e-mail processing, while printer servers administer traffic on networked printers.

Storage Area Networks

Storage area networks (SANs), are high-speed networks consisting of storage devices that work in combination with servers and other network devices. Network storage space is particularly critical for system backups. The development of this relatively recent set of network technologies has been as effective a solution to the inefficiencies of maintaining a host of separate disk subsystems. Almost all companies of any size perform regular system backups, the cumbersome process of backing up as well as restoring data can be slow and a liability for companies that support 24/7 availability. SANs are hence used to reduce such liability and improve the overall efficiency of the system.

More Network Devices

Connecting components such as bridges, routers, and gateways are used to divide networks into sub-networks both physically and logically. Also these may be used to extend the cabling range and/or to connect dissimilar networks or to subdivide networks into segments, which is useful for isolating faults. Repeaters are used to extend the physical distance that network data can travel. Repeaters cannot provide isolation between the components they join. Accordingly the functional layer of operation is dictates the classification of connecting devices. Bridges operate at OSI layer two i.e. Data Link Layer. They isolate segments from a network backbone. They are used to connect two networks with matching lower layers and to convert one lower level technology into another. They can be configured to pass on only fitting messages. Routers operate at layer three i.e. Network Layer. Like bridges they can be used to separate network segments from a backbone, but unlike bridges, they can connect segments with different lower-layer protocols. "Routers" are a hybrid between bridges and routes that operate at layers two or three. Gateways operate at layer four i.e. Transport layer or higher. For a PC to access a minicomputer or mainframe a gateway is necessary. They have a more intricate design and are expensive than the other connecting devices. They have the capability to convert data between dissimilar networks. The *Fig. 3* below shows the scope of the functioning of the connecting devices in the OSI Reference Model.

Connectivity Media

Media to connect network components is analogous to our nervous system. A number of cables exist in the market; like any other hardware equipment, their price is dictated by their performance. At the most simple and cheap, two PCs can be connected by using a null modem cable. While at the upper end of the spectrum, wireless and satellite connections are used by large corporations and the military. The initial cable to be widely used is coaxial cable. It is shielded and resistant to electrical noise and has established its usefulness in many a factory. Twisted-pair cable, also called UTP (unshielded twisted pair), replaced coaxial cable in most applications. It is a cost effective solution but affected by noise, similar to telephone wires.

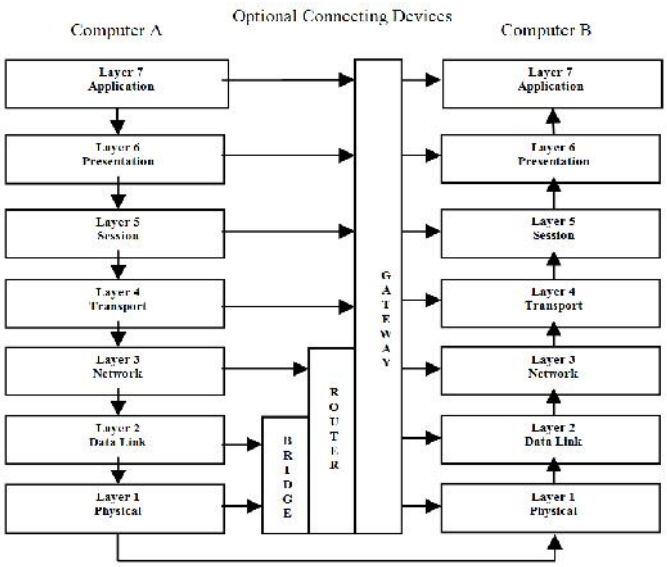

Fig. 3. Scope of connecting devices

Fiber optics is the most expensive and the fastest of all cables. Fiber-optic technology has proven to achieve speeds of several hundred gigabits per second (GBPS) or faster, most commercial applications use between 2.5 and 10 GBPS. Experts have hypothesized that using multiplexing technology the fiber-optic capacity can be pushed to trillion bits per second (TBPS). Also the fiber-optic cable is immune to electrical interference. Hence it is the technology frequently used for high-volume backbones connecting network segments. Wireless systems used for connecting workstations with the file server, microwave dishes connecting computers over long distances and satellite transmission used to transmit price changes among stores in national retail chains are other technologies used for connecting systems. Microwave dishes are limited to line-of-sight transmissions and can be affected by environment conditions. Depending upon frequency, microwave equipment has a transmission limit of 30 miles. Network equipment vendors must manufacture connectors to interface computing devices with the connecting media. While mainframes usually have connectors built in, PCs require the addition of a network interface card (NIC).

Network Software

The connected network of computers, routers, switches, bridges, cables and wires and any other physical hardware is a system that is as good dead without the software running through its veins. The hardware is as important without which the software is then meaningless. Networking Software is specific to performing activities related to monitoring, controlling and maintaining the network. The architecture class of networking used may be centralized or decentralized i.e. distributed but the general structure for the applicability of the networking software is as shown in the *Fig. 4* There is a manager of the network called the NMS – Network Manager System and the rest of the network end points called the Managed Objects. The Network software runs through all these systems with one of the nodes configured as the NMS. The software for the manager and agent are residing in the corresponding entity nodes. There are many agent nodes that are managed by the manager node called as the NMS or Network Management Station. Each of these agent nodes can be managed due to the software installed in the node. The network could have more than one manager nodes depending on the size of the network, the required functionality or geographic distribution of the network. The agent nodes in the network is any component ranging from a PC to a server, a hub or a router or any other component in the network with the installed software or to say in other terms, one for which the MIB information exists. Such a node is hence called a “managed object” or simply MO.

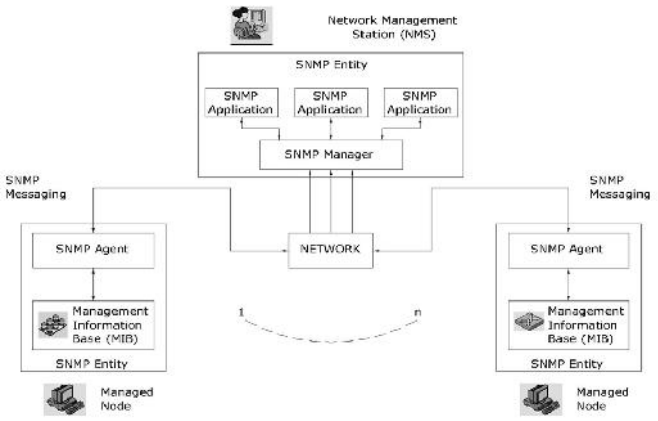

Fig. 4. Fundamental structure of the NMS

Network software is needed to perform network functions. In a LAN, each computer on the network has the network software installed, and the network servers run the network operating system. Two of the most common LAN networking packages is Microsoft's Windows NT and Novell's NetWare. Network software functions include file transfer, real-time messaging, auto-format of e-mail, creating directories and unique addresses for each node. The network software packages contain utilities such as problem detection, performance analysis, configuration assistance, usage and accounting management (billing) and network security. Below is a list of the top Network tools for monitoring devices, services, ports or protocols and analyzing traffic on your network.

Microsoft Network Monitor features include support for over 300 public and Microsoft proprietary protocols, simultaneous capture sessions, a Wireless Monitor Mode and sniffing of promiscuous mode traffic, amongst others.

Nagios provides features such as alerting, event handling and reporting and helps to ensure that critical systems, applications and services are always up and running.

OpenNMS is an enterprise grade network management application that offers automated discovery, event and notification management, performance measurement, and service assurance features.

Advanced IP Scanner - allows connecting to common services such as HTTP, FTP and shared folders if they are enabled on the remote machine. Also facilitates to wake up and shut down remote computers.

Capsa Free allows monitoring network traffic, troubleshoot network issues and analyze packets. Supports for over 300 network protocols (including the ability to create and customize protocols), MSN and Yahoo Messenger filters, email monitor and auto-save, and customizable reports and dashboards.

Network Provider

Network Service Provider (NSP) is the business entity that has the necessary resources to provide the required connectivity to individual users, institutions, firms or businesses. They are responsible for making provisions for the infrastructure i.e. providing backbone service to an Internet Service Provider (ISP) thus together providing access to Internet. The NSP and ISP may or may not be owned by the same business house. Network service providers may consist of telecommunications companies, data carriers, wireless communications providers, Internet service providers, and cable television operators offering high-speed Internet access.

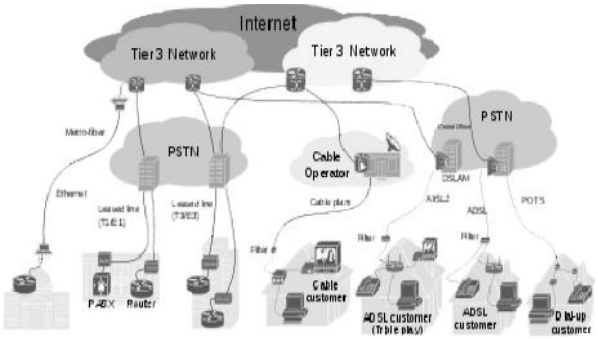

Fig. 5. Comprehensive Network showing all entities

Many different types of computer networks exist. Some networks are defined by their geographic layout, for example local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). LANs are the most common and generally the fastest. Networks may be public - Internet; semi-public - subscription networks (including subscription-based Internet service providers and other content-based networks); or private - internal corporate LANs, WANs, intranets, and extranets. Generally networks are privately owned. They may be open, linked or closed i.e. self-contained not allowing connectivity with outside resources. Most corporate networks lie in between often allowing access to the outside which is tightly restricted. The relatively few public ones, like the Internet, have a very large user base. The NSP (together representing the NSP and ISP) supports the various types of networks directly or indirectly. The NSP has the entire infrastructure with the hardware and the software required for networking in its radar. The private corporate networks although self-contained would be crippled and limited to communicate within the organization without the NSP. Hence NSPs are responsible for realizing the globally connected world view.

Network Administration

Network Administration is the often a complicated job. The network manager must ensure that all the hardware and software work together. An important aspect of the job is fault management, or the detection, isolation, and resolution of problems in the network. Performance management guarantees that data exchange proceeds at an acceptable rate, a factor influenced by workload and the configuration of the network. Network Administrator is also responsible for account management, user activity monitoring, and security management (user authentication and authorization). Network administration requires immense awareness of the agile network. This knowledge is hard to maintain when network managers are always busy with routine service problems and internal concerns. Hence many larger companies have chosen to outsource some or all of these duties to specialized firms.
Network administrator job demands extensive technical knowledge and the ability to learn the intricacies of new networking and server software packages quickly. Smaller organizations generally outsource this function. Network administrators are responsible for various tasks like monitoring, testing, updates and security installs, E-mail and Internet filters and evaluating the network among others.
The data gathered by the NMS is currently used to monitor the network functioning in real-time. It allows the administrators to view the current situation of the network at specific points under his/ her administration and make necessary decisions to relieve congestions or take remedial actions to fault reports. The system is comprehensive to handle and notify the administrator of errors or undesirable situations in the network. The administrator is in a position to only respond to the information arising from monitoring of the network. It is an automatic system with its own set of limitations.

Network data analysis

The area of networking presents a huge scope for improvement as to how the provisioning of services can be more accurate and real-time while being profitable to both the user and provider. This area has seen very limited attention. The newer areas of machine learning and big data analysis have opened the industry to exploration of the data archived in storage systems. There is greater demand for the data and the knowledge to be gained from its analysis. The application of big data analysis and machine learning algorithms has seen a steep growth in industries that are directly connected to end users such as social networking, online shopping, etc. The data gathered from the managed objects by the NMS can be a source of rich information to network administrators and NSP's in general. The NMS is continuously being informed about the functioning of the various nodes that are connected to the system. This may range from the fault status of the node, the usage of bandwidth at a link or by a customer, the volume of traffic being handled currently, etc. This data is very important to the NSP and helps to gather an insight into its operations and performance.

Current Network Limitations

The analysis of the network big data can empower the NSP by gathering knowledge about its network and customers so as to provide proactive services. The network big data analysis can empower the NSP by congregation of knowledge related to network and customers thus enabling provision of proactive services. The network big data has been unexplored till date

and can do wonders to how the customer will be treated in future. The entire process would be automatic and the intelligent systems would be providing rich valuable data about the network and its customers handy for use by network administrators to benefit the NSP business owners as well as the customer himself.

The limitation can be summarized as follows:

Limited Data Storage: The network data with abundance of information needs to be archived and analyzed.

Limited Data Visibility: Network data from NMS currently presents the administrator with the information of the on-goings of the network at the present moment alone. There is very limited or no access to the past data about the network.

No scope for Predictions: The opportunities that open may range from load sharing by sharing of bandwidth during peak seasons, indentifying faulty regions and their classification based on historical performance, real-time traffic diversion decisions for priced customer etc.

Big data analysis benefits

Big Data archived for the purpose of analysis would lay down the initial foundation that would help in gathering useful knowledge. The data may be subjected to various algorithms so as to learn its behavior. The algorithms that may be used are Gaussian distribution, Logarithmic, and Linear, Sinusoidal etc. The data that will be analyzed would range from faults occurring at the managed nodes, bandwidth usage by individual nodes and customers, traffic patterns for particular path or concerned with a select customer, etc. The analysis would be beneficial to the Network Service Provider in the following ways.

Identification of Faulty nodes, paths and geographies:

The data gathered over time would be analyzed for frequency of faults at a particular node, during selected period and for location of the faulty nodes. The learning thus gained would be analyzed to observe patterns if any.

Identification of congested paths and geographies: The traffic conditions for paths and geographies would provide with information on the congestion patterns for the entire year and the previous and so on.

Identification of bandwidth consumption by geographies and consumer

Usage of bandwidth by location and consumer would help the Network Service Provider know which geographies are consuming how much during the said period. Similarly the usage of bandwidth by the customers over historical time may also be learned. The learning and observation would provide insightful information that will help in understanding the historical behavior of the network, customers and on a microscopic basis the selected node, path and selected area. The comparison say during same month every year for all previous years would provide information if the behaviors are repetitive and what factors influence such behavior. For example consider Goa during the month of December would see increased inflow of tourists due to festivities. Another example could be that the analysis yields results that one particular region is say 35% faulty most part of the year. Knowing this the Network Administrator can easily divert the traffic of valuable customers from anther path instead.

Conclusion

In future when we have a good experience with the network at our home/office, may not be a chance incident. Instead it could be the precise calculation of software as this residing at the providers' server making considerate adjustments. Thus valuable clientele are served with the most favorable experience in spite of existing anomalies. Such anomalies are being consciously and selectively avoided. The data from the network nodes is an unexplored area and can provide inquisitive minds a lot of scope for thought and learning.

Acknowledgment

At the outset, I would like to express my sincere thanks to Dr. Manjunatha, Principal, New Horizon College of Engineering, Bangalore, for providing me an opportunity to continue my studies. My special gratitude to Dr. Prashanth C.S.R, HOD of CSE Dept, New Horizon College of Engineering and Technology, for his guidance, support and providing a knowledgeable environment. My sincere thanks go to my guide, Ms. Asha Rani Borah, Professor, Dept. of CSE, Sr. Asst. Prof, Dept. of CSE for their guidance, cooperation, constant encouragement and whole hearted support. Also, I would like to thank all the faculty members of Department of Computer Science and Engineering, New Horizon College of Engineering. Finally, I would sincerely like to express my honest gratitude towards Sir Pankaj Kumar Roy, Director, AVIN Networks Private Limited and his team for their guidance and support which has made my post graduation experiences a true success.

REFERENCES

Douglas E. Comer, 2013. Internetworking with TCP/IP Volume One, 6th Edition, PHI – 2014.

Richard Burke, J. 2004. Network Management: Concepts and Practice, A Hands-On Approach.

http://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

Larry Peterson and Bruce S Davis. 11 Mar 2011. Computer Networks: A Systems Approach, 4th Edition. http://it.mesce.ac.in/downloads/computernetwork/Computer_Networks_Peterson__A_Systems_Approach__Fourth_Edition.pdf

http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

****