IMPLEMENTATION OF POLICY BASED ROUTING IN OSPF USING IPV4/IPV6 OVER NG-SDH NETWORK FOR DTS.

SUPRIYA MASKARE, POOJA PATIL, SAYALI PATIL
BE Students, Department of Electronics Engineering, All India Shree Shivaji Memorial Society's Institute of Information Technology (Pune)

DR.D.K.SHEDGE, DR.M.P.SARDEY
Professor, Department of Electronics Engineering, All India Shree Shivaji Memorial Society's Institute of Information Technology (Pune)

Abstract- Traditional routing is destination-based, meaning packets are routed based on destination IP address. However, it is difficult to change the routing of specific traffic in a destination-based routing system. With Policy Based Routing (PBR), you can define routing based on criteria other than destination network—PBR lets you route traffic based on source address, source port, destination address, destination port, protocol, or a combination of these. Implementation of Policy based routing in OSPF allows sets of networks to be grouped together in an area. The topology of an area is hidden from the other Autonomous System (AS) thus reducing the routing traffic. OSPF was the first widely deployed routing protocol that could converge a network in the low seconds, and guarantee loop free paths.

Keywords- SDH, Policy Based Routing (PBR), WSN, Autonomous System (AS).

1. INTRODUCTION

1.1 INTRODUCTION OF THE PROJECT

In Computer Networking, policy-based routing (PBR) is a technique used to make routing decision based on policies set by network administrator. PBR gives you a flexible means of routing packets by allowing you to configure a defined policy for traffic flows, lessening reliance on routes derived from routing protocols & gives you more control over routing by extending and complementing the existing mechanism provided by routing protocols. It allows you to specify a path for certain traffic, such as priority traffic over a high-cost link [1]. Implementation of policy based routing in OSPF is based on shortest path first Algorithm. It is Designed by Dijkshtra & it is open to all i.e. any company can use this protocol in router. OSPF is a link state routing protocol. i.e each router can send link information to other router. Information can be IP address, Subnet Mask, Port number. OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection [2]. OSPF propagates link-state advertisements (LSA) rather than routing table updates. Because only LSAs are exchanged instead of the entire routing tables, OSPF networks converge more quickly than RIP networks. OSPF uses a link-state algorithm to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-state database, which is a list of each of the router usable interfaces and reachable neighbors [3]. Link State protocol type of routing protocol requires each router to maintain at least a partial map of the network using the Dijkshtra algorithm, a well-known algorithm for computing single-source shortest path in a graph. Each router calculates the shortest path to each network and enters this information into the route table. Neighbor discovery is the first step in getting a link state environment up and running. In keeping with the friendly neighbor terminology, a HELLO packet is used for this step. After the adjacencies are established, the routers may begin sending out LSAs. When a network link changes state, a notification, called a link state advertisement is flooded throughout the network [4]. All routers store a copy of all LSAs and it is seen in a database. The completed topological database, also called the link state database, describes a graph of the internetwork. OSPF uses three types of ID's:

1.Area ID: A Router within an area must maintain a topological database for the area to which it belongs.

2.Router ID: It is used to provide a unique identity to OSPF router.

3. Process ID: The process ID is the ID of the OSPF to which the interface belongs. Two OSPF neighboring routers can have different process IDs. OSPF uses link Authentication i.e. router can have password. To reset Password, we use MD-5 protocol. In Modern telecommunication systems, the increasing demand for new services, like video and data, calls for more complicated transmission methods, higher communication speeds, and more complex network topologies. These requests, in turn, impose high design accuracy and perfect synchronization techniques of data signals [5]. The term 'Synchronization' is nowadays broadly used in telecom to encompass the methods that enable oscillators at different locations to be set to the same frequency within specified limits. With the introduction of Pulse Code Modulation (PCM) for telephony in the late 1960s which allows a single line to be used by multiple signals; using a digital time-domain multiplexing where the analog telephone signal is sampled, quantized and transmitted, network communications were being changed into digital technology and the demand for a bigger bit rate also increased. Plesiochronous Digital Hierarchy (PDH) was introduced by ITU-T G.702 [1] to cope with the increasing demand for higher bit rates; it uses a basic multiplex of 2Mbps with other stages of 8, 34 and 140Mbps. Due to the fact that PDH wasn't quite synchronous, multiplexers uses a little overhead on their high speed trunks to help cater for the differences in the data rates of streams in ports with low speed. Due to the varying developments adopted by different networks, interconnecting gateways between networks was

expensive and difficult; also PDH was not flexible which made monitoring and management more difficult to realize. Synchronous Digital Hierarchy (SDH) was developed to fix some of the limitations experienced in PDH. As more people began to use SDH, management capabilities increased because of the comprehensive monitoring and the high capability management throughout the network [4].

1.2 SYNCHRONOUS DIGITAL HIERARCHY (SDH)

Unlike PDH, SDH is based on repeated hierarchy of fixed length frames that are designed to carry isochronous traffic channels. It eliminates mountains of multiplexers by allowing single stage multiplexing and de-multiplexing thereby reducing hardware complexities [1]. Some of the recommendations for the development of SDH were to define a structured multiplexing hierarchy, to define a proper protection and management mechanism, to define (optical components) physical layer requirements and to define multiplexing of different sources over SDH. The basic concept for data rates in SDH is four times the data rate for twice the cost and the table below shows the most common rate for SONET/SDH [3].

A. SDH Network elements

The different network elements in SDH include:

1) Synchronous multiplexer: The synchronous multiplexer performs both the live line transmitting functions and multiplexing, it replaces Plesiochronous multiplexers and line transmitting equipments. There are two types of synchronous multiplexers;

- Terminal Multiplexers (TM): These multiplexers accept a number of tributary signals and multiplex them into appropriate aggregate signals.
- Add and Drop Multiplexers (ADM): ADM allows it to be possible to “ADD” channels or “DROP” channels from “THROUGH CHANNELS”. It is SDH building block for local access to synchronous network [4].

2) Synchronous Digital Cross Connect: The cross connect equipment acts as a switch that can pick out one or more lower order channels without the need for a transmission channel.

3) Regenerators: This is a device that regenerates the signals. The major use of regenerators is for long distance data transfer of more than 50km, termination is performed and the optical signal is regenerated [4].

B. SDH Frame Structure

The SDH frame structure is based on synchronous byte wise multiplexing of several building blocks. Such synchronous multiplexing elements are structured fixed size sets of bytes, which are byte-interleaved or mapped one-into-the-other to eventually form STM-N frames. The STM-1 frame is the basic transmission format for SDH. The frame lasts for 125µs, equivalent to 0.125 kHz [2].

C. SDH Virtual Container Structure

Virtual containers (VCs) are the basic building block, which maps a payload that can be any PDH signal as well as other lower-order synchronous multiplexing elements

[5]. VCs are individually and independently accessible within SDH frames through pointer information directly associated with them by multiplexing. These overhead bytes are added whenever the layer is introduced and removed when the layer is terminated [1].

D. Structure of SDH Overheads

The SDH Overheads support: monitoring, messaging, labeling, and switching control. In each layer, specific bytes are allocated per frame, or per multi-frame; Overheads allow for monitoring of both ends from one end, for sector management (transit traffic), and central management via Data Communications Channel (DCC).

E. SDH Layers

The SDH layer consists of four sub-layers, which are path, regenerator section, photonic layer and multiplex section. The SDH framing structure defines overheads operating at these layers to estimate error rate, communicate alarm condition and provide maintenance support[6].

F. SDH Network Topology

1) Point-Point Link: Based on PDH systems which provide point – point connections, SDH will replace these systems with STM-4 line systems [4]. In this system, regenerators may be used to avoid transmission issues, no routing or de-multiplexing is done along the path [3].

2) Ring Topology: This is the most used topology, in this topology, two or four fibers can be used and an ADM at each node [3]. The ring network is a route back to itself that facilitates the development of protocols that can detect if there is a failure in the fibre and re-establish connection back quickly.

3) Star Topology: The traffic here passes through a central hub where the hub is a Synchronous Digital Cross Connect [4].

4) Linear Bus Topology: The Linear bus topology has great flexibility and is used when there is a need for protection [4].

G. Advantages of SDH

Comparing SDH to PDH, the transmission rates of SDH can go up to 10Gbps, it is easier to extract and insert low bit rate channels to high bit streams. SDH systems include auto backup and restore/repair mechanisms in case of failure, and a failure in a link or a network element does not amount to the failure of the entire network. Other

1.3 POLICY BASED ROUTING

This document is not restricted to any specific hardware or software versions. The information shown in this document is based on the software and hardware versions below.

- Cisco IOS® Software Release 12.3(3)
- Cisco 2500 series routers

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

1.4 Aim and Objectives

Aim-

1. Implementation of policy based routing in open shortest path first (OSPF) using ipv4 over NG-SDH network.
2. To allow routers to exchange information over networks.
3. To maintain reliability and Security while transferring packet.

Objectives

1. To develop basic network element and need of SDH network
2. To design & understand basic concept of routing in OSPF using ipv4
3. To develop and configure Router in OSPF.
4. To study advantages of SDH over PDH network.
5. To develop security while packet transferring.

2. LITERATURE REVIEW

Amer Nizar Abu Ali et al. This makes the characteristics of IPv6 over IPv4 tunnels very vital to the performance of the global IPv6 Internet. IPv6 over IPv4 tunnels are widely used to form the global IPv6 Internet. This paper demonstrates the two tunnels and show when to immigrate from IPv4 to IPV6.Then the risks of immigration are discussed [1]. The migration from IPv4 to IPv6 must be implemented node by node by using auto configuration procedures to eliminate the need to configure IPv6 hosts manually. This way, users can immediately benefit from the many advantages of IPv6 while maintaining the possibility of communicating with IPv4 users or peripherals. Consequently, there is no reason to delay updating to IPv6.In this paper we are going to investigate the IPV6 and the IPV4 and when to decide to immigrate to IPV6 [2].

Annish Brislin M R et al. In Existing System Network plays a vital role that helps to share information and resources and implement centralized management system. To enable the network features, all organizations and ISPs have designed and implemented IPv4 network to share their voice/data/video applications. IP is internet protocol and works on third layer of OSI model and forward packets from one node to another. IPv4 enables encapsulation and add more information that helps for efficient transmission of data [3]. IPv4 address is32 bit address and have maximum of 2^32 combination address. The goal of this paper is to investigate the behavior of routing convergence. It begins with an explanation of IP addressing. Next, the report discusses the two routing protocols: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) into great detail. The report then examines the structure of a routing table and the route selection process. In order to be practical in the investigation of the routing convergence, we perform an experiment that involved seven Cisco routers. It is assumed that an end customer requires redundancy for its Wide Area Network (WAN) connection [4].

Alex Hinds et al. IPv4 includes no quality of service mechanisms: IPv6 adds support for Quality of Service (QoS) mechanisms through the use of flow control bits; these will enable routers to priorities packets based upon QoS considerations and economies storage by aggregating routing tables. We will critically review two popular interior routing protocols for IPv6; Open Shortest Path First version 3 (OSPFv3) and Enhanced Interior Gateway Routing Protocol version 6 (EIGRPv6) and compare the changes these protocols have undergone to support IPv6[5]. Traditional IPv4 routing protocols must be replaced with new IPv6 compatible protocols to ensure systems continue to operate effectively; however, these protocols have undergone significant changes in order to support IPv6. Understanding these changes is important when selecting a routing protocol for a system, in order to facilitate this, a study and comparison of two popular routing protocols; OSPF and EIGRP has been undertaken. The major changes between the IPv4 and IPv6 editions have been identified and discussed and the two protocols have been compared against a number of criteria [6].

Suleiman Y. Yerima et al. describe the implementation of admission control schemes as an essential building block of our QoS management framework. Measurement-based admission control is implemented within the framework Java-based prototype that has been developed on a Linux based experimental test bed. This is driven and enabled by the network monitoring and resource control elements within the subsystems of the framework, thus allowing for closed-loop, adaptive and scalable QoS control along the transport plane infrastructure. Furthermore, an experimental analysis of the measurement-based schemes is presented whilst comparing with parameter-based admission control [7]. Such technical challenges of heterogeneous QoS management in converged networks could be surmounted by deployment of Policy-Based Network Management (PBNM) techniques. PBNM allows for configuration and control of the network as a whole thus eliminating the need to configure and individually manage each network entity. This paper presents the implementation and analysis of various measurement-based admission control schemes developed within a Java-based prototype of our policy-based framework. The evaluation is made with real traffic flows on a Linux-based experimental test bed where the current prototype is deployed. Our results show that unlike with classic MBAC or PBAC only schemes, a hybrid approach that combines both methods can simultaneously result in improved admission control and network utilization efficiency [8].

S. Y. Yerima et al. CNQF is aimed at providing homogenous, unified and adaptive measurement-based QoS control and resource management over heterogeneous access technologies. By leveraging PBNM paradigm, the CNQF architecture provides the means for application transparency across existing and emerging access technologies, thus permitting applications to be transport-layer agnostic when deployed. CNQF is designed to provide unified, scalable QoS control and resource management through the use of a policy-based network management paradigm. It achieves this via distributed functional entities that are deployed to co-ordinate the resources of the transport network through centralized policy-driven decisions supported by measurement-based control architecture. We present the CNQF architecture, implementation of the prototype and validation of various inbuilt QoS control mechanisms using real traffic flows on a Linux-based experimental test bed [9].

Dr. Khaldoun Batiha et al. This paper outlines suggested modifications on the IPv6 protocol addressing type and size in comparison with current IPv6 protocol and shows how badly we really need these modifications to improve the overall internet performance as much as possible. It not only takes a deep look at the addressing type and size that IPv6 presents, but it also gives a good idea of what really the IPv6 modification based on significant needs for these modifications. Also, this paper presents an attempt to implement the suggested modifications to improve overall performance in the internet [10]. It also discusses the predicted exhaustion dates of unallocated IP addresses for size range between 32-bit and 128-bit in the internet. IPv6 protocol is the next candidate protocol after IPv4 protocol that used for a long time. For this protocol the addressing types and address size are discussed to list some modifications that could improve its performance through the internet. At the same time, we prove that multicast addressing type is the most important addressing type since it can mimic any other addressing type. Finally, a short study is developed in order to reduce the current IPv6 address size to have less overhead in the basic header packet; this reduction omits about 40% of the overall basic IPv6 basic packet overhead [11].

Mohammad Azmi Al-Madi et al. A development for the IPv6 was performed by the Internet Engineering Task Force (IETF). This organization increased the success to the IPv6 than was in the IPv4; besides, the Quality of Service (QoS) was integrated and developed by the IETF organization. This paper, we propose an enhanced technique model for policy routing management in the TV broadcasting which is called the PBR and QoS Control Routing for Multi-Channel Adaptive Streaming (PQMAS) technique. Our technique combines three basic concepts which are; QoS, Policy-Based Routing (PBR) and the Controlling Network Traffic (CNT). These combinations are a complement to the Multi-Channel Adaptive Streaming (MCAS) framework, besides, new rules in the PBR were proposed. The main aim of this paper is to study and understand the broadcasting network that can be managed by a routing policy. Such an example of an important protocol that plays an essential role through the broadcast is the Internet Protocol Television (IPTV) [12].

S. Deepa et al. Internet Protocols and the implementation of Routing Protocols such as Internet Protocol Security (IPsec), Policy Based Routing (PBR) are used to provide enhanced security in the network layer. This paper work is being currently implemented in RGMTTC (Rajiv Gandhi Memorial Telecom Training Center) of BSNL (Bharat Sanchar Nigam Limited) to provide a secured service to its customers by delivering the IP packets, through IPv6 network in an efficient manner by using Routing protocols and security schemes. The PBR overwrites the normal routing procedures and these packets choose the path as directed by the network admin. The network can be made more efficient by providing security scheme to secure the packets from the hackers. This process will minimize the network collision and by implementing security schemes in IPv6 network, the IP packets are delivered securely and also take the path as desired by network administrator [13].

Dipti Chauhan et al. In the current scenario as the exponential growth of internet has led to the shortage of IPv4 addresses. IPv4 is the most dominant addressing protocol used on the Internet and most private networks today. With the advent of wide variety of devices and upcoming technologies, the limited addresses of IPv4 are not able to cope with the current internet. IPv6 was mainly developed to resolve the addressing issues as well the security concerns which are lacked by IPv4. One of the major challenges in the internet is to deploy IPv6. In the transition to IPv6, both IPv6 and IPv4 will co-exist until IPv6 eventually replaces IPv4. In this paper an attempt is being made to enlighten the importance of IPv6 in current scenario and the key reasons to deploy the IPV6, and also discusses the standards and techniques which are required for smooth interoperation between the two protocols. IPv6 is acknowledged to provide more address space, better address design, and greater security. IPv4 offers 32-bit address space and IPv6 offers 128-bit address space [14].

Ranjit Sadakale et al. This paper is presenting improved AODV protocol, in order to consider different parameters like node mobility, sent packet rate, delay and throughput. Results are implemented using Network Simulator-2. Vehicular Ad-hoc Network (VANET) is considered as a sensor network with special characteristics and some advance features. For VANET nodes treated with high mobility and fast topology change. These nodes can sense its neighboring area to provide various services like traffic monitoring, speed of vehicle and some environmental parameters monitoring. One of the advances reactive routing protocol is Ad Hoc on-demand Distance Vector (AODV) is most commonly used routing protocol in topology based routing. VANETs considered as distributed, self-organizing network to provide communication for moving vehicles. Many researchers trying to develop Vehicular Ad-hoc network because of its flexibility and free network communications [15].

Henry Chukwuemeka Paul et al. The Network Layer is responsible for the delivery of individual packets from the source host to the destination host. Reddy et al (2012) discussed about the Internet Protocol (IP) as the Network Layer of the TCP/IP protocol suite. An explained study is performed on the addressing architecture. However, these techniques prove to be most efficient in the study which has been performed. This paper targets at a comparative study on the throughputs in bits/ seconds, packet throughputs, delay in networks, response time in seconds of both IPv4 and IPv6. evaluating, compare and report result based on the performance of two protocol stacks (IPv4 and IPv6) in terms of various parameters that is analyzed when the data is being transmitted from one client to another or to a server over a wired network on IPv4 in comparison with the IPv6, thus proposing a system that supports the co-existence of both IPv4 and IPv6. The issue of the

new-generation numbering system of the Internet Protocol version 6 (IPv6) is addressed as exhaustion of address space of the numbering system of Internet Protocol version 4 (IPv4) becomes a problem [16].

Dr. Sandeep Tayal et al. IPv4 is the main form of Internet set of rules to be generally operates, and be a large piece of today's Internet activity. There are a little more than 4 billion IPv4 addresses. While that is a great deal of IP locations, it is insufficient to keep going forever. IPv6 is the 6th correction to the Internet Protocol and the successor to IPv4. IPv4 areas are starting at now depleted in Internet Assigned Numbers Authority (IANA) and have drained in Regional Internet Registries (RIRs) while more clients are constantly including into the Internet. IPv6, as the main accessible cutting edge Internet convention, is still not industrially fruitful acknowledged in light of the fact that a plan that could explain the relocation of IPv4 assets to IPv6 organize, and in addition common correspondence between the two contrary conventions, has not been completely created and conveyed. Interpretation arrangement gives an appropriate way to deal with address this issue. In this survey paper, we checked on research papers exhibited by the specialists in the vicinity of 2007 and 2015 identified with IPv4 and IPv6 asset movement and convention move conspires and watched issues related system security, tending to and blunder identification in the execution of IPv6[17].

Palukuru Venkata Praneeth Reddy et al.
It is designed giving main importance to scalability, which means we will never run out of IP addresses. Each and every individual on the planet can have billions of individual IP addresses. IPv6 also offers features such as security and automatic configuration. All these put together form a new and improved internet. The old network cannot be put aside for new. Both should coexist for an extended transitional period. Further, IPv6 is still untested. So; this new architecture must be validated before deploying in a large scale. IPv6 is not the entire solution to all internet problems. Internet Protocol Version 6 (IPv6) holds the future of ip addressing. It has many advantages compared to IPv4. The basic framework of IPv6 protocol was interchanged by the Internet Engineering Task Force. Present paper provides an introduction to IPv6 by giving the results that can be obtained by deploying the technology. It also explains some of the technical features and advantages of IPv6[14].

Manal M. Alhassoun et al. The objectives of this survey paper are to highlight the issues related to the IPv6 deployment and to look into the IPv4 to IPv6 transition mechanisms. Furthermore, provide insight on the global effort around the world to contribute in IPv6 deployment. In addition, identify the potential solutions or suggestions that could improve the IPv6 deployment rate. In order to achieve the said objectives, we survey number of papers on IPv6 deployment from different countries and continents. The use of the Internet is growing over the time. Many days to day activities are depending on the Internet and lot of services is provided through the Internet too such as: social networking websites, search engines, video calls and many more. In order to reach these services; people use devices connected to the Internet such as computers, mobile phones, Personal Digital Assistants (PDA). In addition to solving the address the limitations, IPv6 has many improved features [12].

Babu Ram Dawadi et al. This forced the world required to migrate into IPv6 as a new addressing paradigm. Currently, the term 'migration' refers to different research dimensions in the world of science and engineering. The Information and Communication Technology (ICT) service providers are in the rush of not only the migration to IPv6 but also towards the migration into cloud computing and software defined networking, where "migration in togetherness" is coined to enter into the new era of IT based businesses and services. IPv4 and IPv6 are not interoperable. Hence moving into IPv6 operable network is a gradual process. The concerned organizations throughout the world are in different stages of network migration to IPv6. Service Providers and organizations of the developing countries are lacking behind the migration due to the lack of awareness, training, and cost of transition. This paper proposed the network transition steps after highlighting the migration strategies for Service Providers (SP) with different transition technologies. The Internet user growth has rapidly increased throughout the world for almost a decade, and 32-bits IPv4 address space limitations have become severe. IPv4 address space is allocated by IANA, the central registry for RIRs and from RIRs to NIRs or LIRs according to the hierarchical structure of the registry, and then assigned to end users [13].

3. PROPOSED METHODOLOGY

3.1 System Architecture Diagram

SDH frame

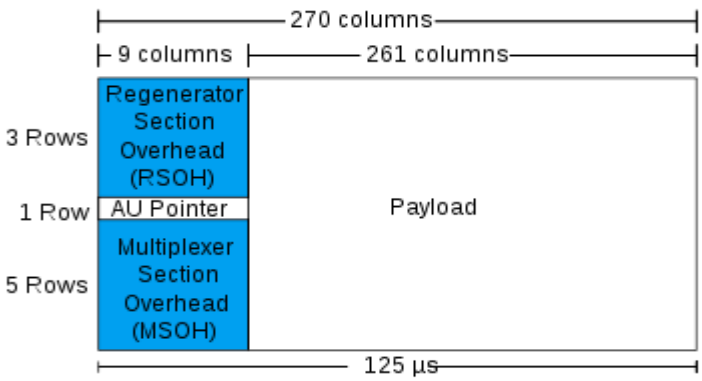


Fig 01 Proposed Methodology

An STM-1 frame. The first nine columns contain the overhead and the pointers. For the sake of simplicity, the frame is shown as a rectangular structure of 270 columns and nine rows but the protocol does not transmit the bytes in this order.

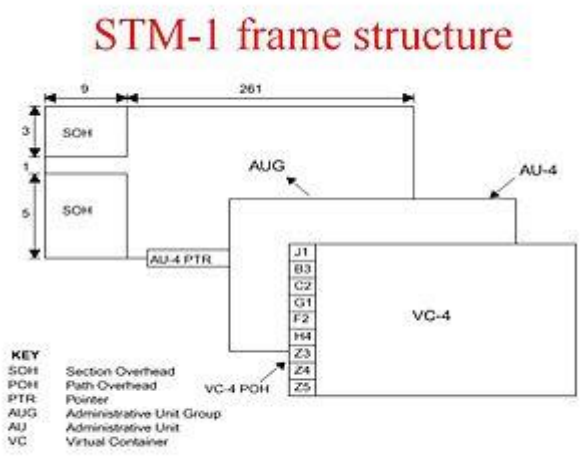


Fig 02 STM-1 Frame Structure

For the sake of simplicity, the frame is shown as a rectangular structure of 270 columns and nine rows. The first three rows and nine columns contain regenerator section overhead (RSOH) and the last five rows and nine columns contain multiplex section overhead (MSOH). The fourth row from the top contains pointers. The Synchronous Transport Module, level 1 (STM-1) frame is the basic transmission format for SDH—the first level of the synchronous digital hierarchy. The STM-1 frame is transmitted in exactly 125 µs, therefore, there are 8,000 frames per second on a 155.52 Mbit/s OC-3 fiber-optic circuit.[nb 1] The STM-1 frame consists of overhead and pointers plus information payload. The first nine columns of each frame make up the section overhead and administrative unit pointers, and the last 261 columns make up the information payload. The pointers (H1, H2, H3 bytes) identify administrative units (AU) within the information payload. Thus, an OC-3 circuit can carry 150.336 Mbit/s of payload, after accounting for the overhead.[nb 2] Carried within the information payload, which has its own frame structure of nine rows and 261 columns, are administrative units identified by pointers. Also within the administrative unit are one or more virtual containers (VCs). VCs contain path overhead and VC payload. The first column is for path overhead; it is followed by the payload container, which can itself carry other containers. Administrative units can have any phase alignment within the STM frame, and this alignment is indicated by the pointer in row four.

The section overhead (SOH) of a STM-1 signal is divided into two parts: the regenerator section overhead (RSOH) and the multiplex section overhead (MSOH). The overheads contain information from the transmission system itself, which is used for a wide range of management functions, such as monitoring transmission quality, detecting failures, managing alarms, data communication channels, service channels, etc. The STM frame is continuous and is transmitted in a serial fashion: byte-by-byte, row-by-row. The STS-1 payload is designed to carry a full PDH DS3 frame. When the DS3 enters a SONET network, path overhead is added, and that SONET network element (NE) is said to be a path generator and terminator. The SONET NE is line terminating if it processes the line overhead. Note that wherever the line or path is terminated, the section is terminated also. SONET regenerators terminate the section, but not the paths or line. An STS-1 payload can also be subdivided into seven virtual tributary groups (VTGs). Each VTG can then be subdivided into four VT1.5 signals, each of which can carry a PDH DS1 signal. A VTG may instead be subdivided into three VT2 signals, each of which can carry a PDH E1 signal. The SDH equivalent of a VTG is a TUG-2; VT1.5 is equivalent to VC-11, and VT2 is equivalent to VC-12. Three STS-1 signals may be multiplexed by time-division multiplexing to form the next level of the SONET hierarchy, the OC-3 (STS-3), running at 155.52 Mbit/s. The signal is multiplexed by interleaving the bytes of the three STS-1 frames to form the STS-3 frame, containing 2,430 bytes and transmitted in 125 µs. Higher-speed circuits are formed by successively aggregating multiples of slower circuits, their speed always being immediately apparent from their designation. For example, four STS-3 or AU4 signals can be aggregated to form a 622.08 Mbit/s signal designated OC-12 or STM-4. The highest rate commonly deployed is the OC-768 or STM-256 circuit, which operates at rate of just under 38.5 Gbit/s.[12] Where fiber exhaustion is a concern, multiple SONET signals can be transported over multiple wavelengths on a single fiber pair by means of wavelength-division multiplexing, including dense wavelength-division multiplexing (DWDM) and coarse wavelength-division multiplexing (CWDM). DWDM circuits are the basis for all modern submarine communications cable systems and other long-haul circuits.

3.2 Working of the System

1. **Synchronous optical networking** (**SONET**) and **synchronous digital hierarchy** (**SDH**) are standardized protocols that transfer multiple digital bit streams synchronously over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs). At low transmission rates data can also be transferred via an electrical interface. The method was developed to replace the plesiochronous digital hierarchy (PDH) system for transporting large amounts of telephone calls and data traffic over the same fiber without the problems of synchronization.

2. SONET and SDH, which are essentially the same, were originally designed to transport circuit mode communications (e.g., DS1, DS3) from a variety of different sources, but they were primarily designed to support real-time, uncompressed, circuit-switched voice encoded in PCM format.[1] The primary difficulty in doing this prior to SONET/SDH was that the synchronization sources of these various circuits were different. This meant that each circuit was actually operating at a slightly different rate and with different phase. SONET/SDH allowed for the simultaneous transport of many different circuits of differing origin within a single framing protocol. SONET/SDH is not a communications protocol in itself, but a transport protocol.
3. Due to SONET/SDH's essential protocol neutrality and transport-oriented features, SONET/SDH was the obvious choice for transporting the fixed length Asynchronous Transfer Mode (ATM) frames also known as cells. It quickly evolved mapping structures and concatenated payload containers to transport ATM connections.
4. In other words, for ATM (and eventually other protocols such as Ethernet), the internal complex structure previously used to transport circuit-oriented connections was removed and replaced with a large and concatenated frame (such as STS-3c) into which ATM cells, IP packets, or Ethernet frames are placed Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph, which may represent, for example, road networks. The algorithm exists in many variants; Dijkstra's original variant found the shortest path between two nodes, but a more common variant fixes a single node as the "source" node and finds shortest paths from the source to all other nodes in the graph, producing a shortest path tree.
5. For a given source node in the graph, the algorithm finds the shortest path between that node and every other. It can also be used for finding the shortest paths from a single node to a single destination node by stopping the algorithm once the shortest path to the destination node has been determined . For example, if the nodes of the graph represent cities and edge path costs represent driving distances between pairs of cities connected by a direct road, Dijkstra's algorithm can be used to find the shortest route between one city and all other cities . As a result, the shortest path algorithm is widely used in network routing protocols, most notably IS-IS and Open Shortest Path First (OSPF). It is also employed as a subroutine in other algorithms such as Johnson's. Dijkstra's original algorithm does not use a min-priority queue and runs in time O(|V|^2) (where |V| is the number of nodes. This is asymptotically the fastest known single-source shortest-path algorithm for arbitrary directed graphs with unbounded non-negative weights. In some fields, artificial intelligence in particular, Dijkstra's algorithm or a variant of it is known as uniform-cost search and formulated as an instance of the more general idea of best-first search.

4. SYNCHRONOUS DIGITAL HIERARCHY(SDH)

It is a standard protocol that transfer multiple digital bit stream synchronously over optical fiber cable. It provides faster and less expensive network interconnection than traditional Plesiochronous digital hierarchy (PDH). It was developed to eliminate synchronous issues

SDH STANDARDS:

The new standard appears first as SONET, drafted by bellcore in the united state, and then went through revisions before it emerges in a new form compatible table with the international SDH. Both SDH and SONET emerge between 1988 and 1992.

SONET is an ANSI standard,it can carry as payloads the north american PDH Hierarchy of bit rates: 1.5/6/45 Mbps,plus 2Mbps (known in the united states as E1).SDH imbraces most of SONET & is an international standard,but it is often regarded as a european standard because it suppliers - with 1 or 2 exceptions-carry only the ETSI-defined European PDH bit rates of 2/34/140Mbps(8Mbps is omitted from SDH). both ETSI & ANSI have defined,detail SDH / SONET feature options for use within their geographical spheres of influence.

The original SDH standard defined the transport of 1.5/2/6/34/45/140 Mbps within a transmission rate of 155.52 M bps. & is being developed to carry other types of traffics such as asynchronous transfer mode(ATM) and internet protocol (IP), within rates that are integer multiples of 155.52Mbps. The basic unit of transmission in SONET is at 51.84 Mbps, but in order to carry 140Mbps, SDH is based on Three times this (I.e.155.52Mbps[155Mbps]). Through an approriate choice of options, a subset of SDH is compatible with subnet of SONET;Therefore,traffic interworking is possible. Interworking for alarms and performance management is generally not possible between SDH and SONET systems. It is only possible in a few cases for some feature between vendors of SDH & slighty more between vendors of SONET.

Although SONET & SDH were conceived originally for optical fiber transmission,SDH radio system exists at rates compatible with both SONET &SDH.

4.1 SDH SYSTEM

4.2 ETHERNET

Ethernet is the traditional technology for connecting wired local area networks (LANs), enabling devices to communicate with each other via a protocol -- a set of rules or common network language. As a data-link layer protocol in the TCP/IP stack, Ethernet describes how network devices can format and transmit data packets so other devices on the same local or campus area network segment can recognize, receive and process them. An Ethernet cable is the physical, encased wiring over which the data travels. Any device accessing a geographically localized network using a cable i.e., with a wired rather than wireless connection likely uses Ethernet -- whether in a home, school or office setting. From businesses to gamers, diverse end users depend on the benefits of Ethernet connectivity, including reliability and security.

Ethernet working:

The Institute of Electrical and Electronics Engineers Inc. (IEEE) specifies in the family of standards called IEEE 802.3 that the Ethernet protocol touches both Layer 1 -- the physical layer -- and Layer 2 -- the data link layer -- on the OSI network protocol model. Ethernet defines two units of transmission: packet and frame. The frame includes not just the payload of data being transmitted, but also:

1. The physical media access control (MAC) addresses of both the sender and receiver;
2. VLAN tagging and quality of service information; and
3. Error correction information to detect transmission problems.

Each frame is wrapped in a packet that contains several bytes of information to establish the connection and mark where the frame starts. Engineers at Xerox first developed Ethernet in the 1970s. Ethernet initially ran over coaxial cables, while a typical Ethernet LAN today uses special grades of twisted pair cables or fiber optic cabling.

5. ALGORITHM USED

1. ECC (Elliptic Curve Cryptography) Algorithm

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

Assume that those who are going through this article will have a basic understanding of cryptography (terms like encryption and decryption).

The equation of an elliptic curve is given as,

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number'd' within the range of 'n'.

Using the following equation, we can generate the public key

Q = d * P

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.

'Q' is the public key and'd' is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be C1 and C2.

C1 = k*P
C2 = M + k*Q
C1 and C2 will be sending.

Decryption

We have to get back the message 'm' that was send to us,

M = C2 – d * C1
M is the original message that we have send.

Proof
How do we get back the message?

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P)
(C2 = M + k * Q and C1 = k * P) = M + k * d * P – d * k *P

(Canceling out k * d * P) = M (Original Message)

2. Elliptic Curve Digital Signature Algorithm

Source, with domain parameters D = (q, FR, a, b, G, n, h), public key Q and private key d, does the following steps to sign the message m

Step 1: Selects a Random number k ∈ [1, n – 1]

Step 2: Computes Point kG = (x, y) and r = x mod n, if r = 0 then go to Step 1

Step 3: Compute t = k–1 mod n
Step 4: Compute e = SHA-1(m), where SHA-1 denotes the 160-bit hash function

Step 5: Compute s = k– 1 (e + da*r) mod n, if s = 0 go to Step 1

Step 6: The signature of message m is the pair (r, s)
Step 7: Source sends Destination the message m and her signature (r, s)

To verify Alice's signature, Bob does the following (Note that Bob knows the domain parameters D and Alice's public key Q)

Step 1: Verify r and s are integers in the range [1, n – 1]
Step 2: Compute e = SHA-1(m)
Step 3: Compute w = s–1 mod n
Step 4: Compute u1 = e.w and u2 = r.w
Step 5: Compute Point X = (x1, y1) = u1G + u2Q

Step 6: If X = O, then reject the signature
Else compute v = x1 mod n
Step 7: Accept source signature if v = r

An illustration of the above steps is represented below

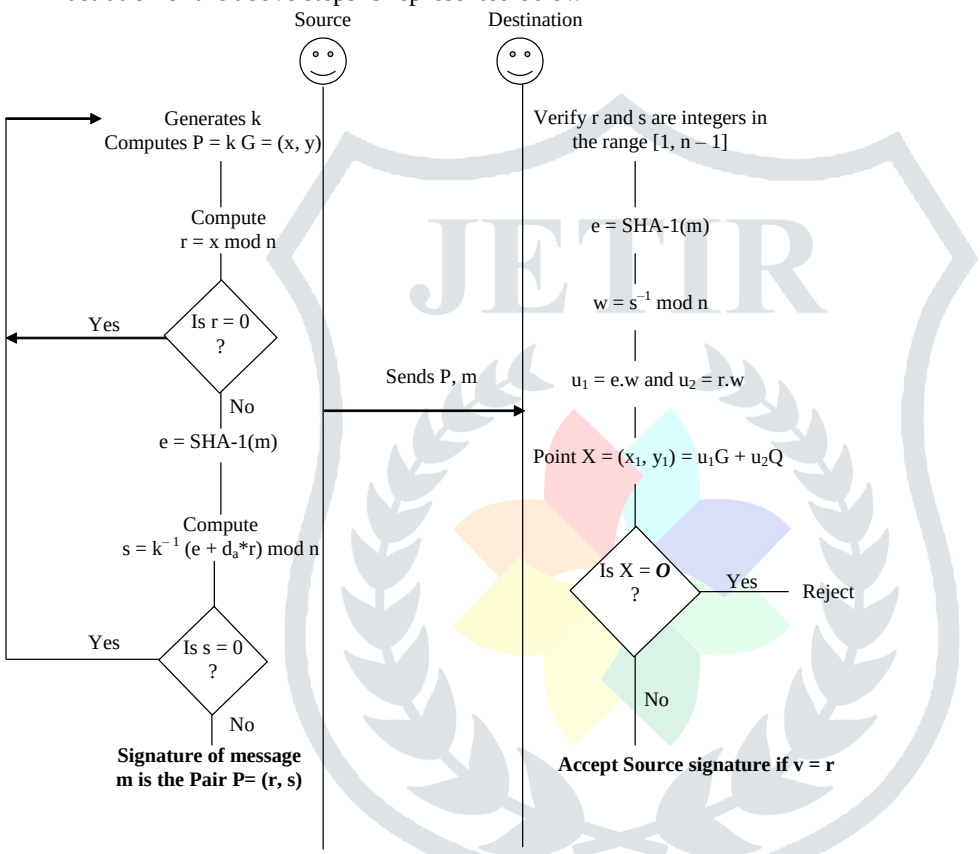


Figure 5: Illustration of Elliptic Curve Digital Signature Algorithm

Proof for verification
If the message is indeed signed by source, then s = k–1 (e + d*r) mod n.

That is, k = s–1 (e + d.r) mod n = s–1 e + s–1 d.r = w.e + w.d.r = (u1 + u2.d) mod n …… [1]
Now consider u1G + u2Q = u1G + u2dG = (u1 + u2.d) G = kG from [1]
In step 5 of the verification process, we have v = x1 mod n, where,
Point X = (x1, y1) = u1G + u2Q. Thus we see that v = r since r = x mod n and x is the x coordinate of the point kG and we have already seen that u1G + u2Q = kG

3. Secure routing Protocol ARAN:

ARAN or authenticated routing protocol detects and protects against malicious actions by third party and peers in ad hoc network. Two distinct stages of ARAN consist of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. ARAN makes the use of cryptographic certificate to accomplish its task.

a) Route Initiation Step

Stage 1 each node, before attempting to connect to the ad hoc network, must contact the certification authority and request a certificate for its address and public key.

Stage 2 The second operational stage of the protocol ensures that the intended destination was indeed reached. Each node must maintain a routing table with entries that correspond to the source-destination pairs that are currently active. The route discovery of the ARAN protocol begins with a node broadcasting a route discovery packet (RDP) to its neighbors.

b) Route maintenance

When no traffic has occurred on an existing route for that route' s lifetime, the route is simply de-activated in the route table. Data received on an inactive route causes nodes to generate an Error (ERR) message. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR messages must be signed.

4. Dijkstra's shortest path algorithm

Given a graph and a source vertex in the graph, find shortest paths from source to all vertices in the given graph. Dijkstra's algorithm is very similar to Prim's algorithm for minimum spanning tree. Like Prim's MST, we generate a SPT (shortest path tree) with given source as root. We maintain two sets, one set contains vertices included in shortest path tree, other set includes vertices not yet included in shortest path tree. At every step of the algorithm, we find a vertex which is in the other set (set of not yet included) and has a minimum distance from the source. Below are the detailed steps used in Dijkstra's algorithm to find the shortest path from a single source vertex to all other vertices in the given graph.

Algorithm
1) Create a set sptSet (shortest path tree set) that keeps track of vertices included in shortest path tree, i.e., whose minimum distance from source is calculated and finalized. Initially, this set is empty.

2) Assign a distance value to all vertices in the input graph. Initialize all distance values as INFINITE. Assign distance value as 0 for the source vertex so that it is picked first.

6. RESULT AND DISCUSSION

- **Routing Protocol:-**

A **routing protocol** specifies how **routers** communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. **Routing** algorithms determine the specific choice of route. Each **router** has a priori knowledge only of networks attached to it directly.
Routing is the process of selecting best paths in a **network**. In the past, the term **routing** also meant forwarding **network** traffic among **networks**. However, that latter function is better described as forwarding.
Routing Algorithm: -
Algorithm shortest Distance (*Network*, *source*):

```
Create Node set Q

For each Node v in Network:            // Initialization
        dist[v] ← INFINITY      // Unknown distance from source to v
   prev[v] ← UNDEFINED   // Previous node in optimal path from source
   add v to Q         // All nodes initially in Q (unvisited nodes)

dist[source] ← 0                  // Distance from source to source

While Q is not empty:
   u ← Node in Q with min dist[u] //Source node will be selected first
  remove u from Q

  For each neighbor v of u:          // where v is still in Q.
     alt ← dist[u] + length (u, v)
     if alt < dist[v]:        // A shorter path to v has been found
       dist[v] ← alt
        prev[v] ← u
return dist [], prev []
```

Invariant hypothesis: For each visited node u, dist[u] is the shortest distance from source to u; and for each unvisited v, dist[v] is the shortest distance via visited nodes only from source to v (if such a path exists, otherwise infinity; note we do not assume dist[v] is the actual shortest distance for un-visited nodes). The base case is when there is just one visited node,

namely the initial node source, and the hypothesis is trivial. Assume the hypothesis for *n-1* visited nodes. Now we choose an edge uv where v has the least dist[v] of any unvisited node and the edge uv is such that dist[v] = dist[u] + length[u,v]. dist[v] must be the shortest distance from source to v because if there were a shorter path, and if w was the first unvisited node on that path then by hypothesis dist[w] > dist[v] creating a contradiction. Similarly if there was a shorter path to v without using unvisited nodes then dist[v] would have been less than dist[u] + length [u,v].

- **Performance metrics used**

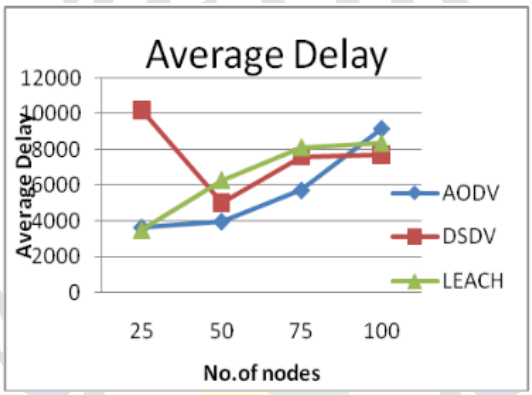
In this section performance metrics are use d to evaluate performance of routing protocols and data dissemination protocols scheme when no in networking processing is performed and no caching is used.

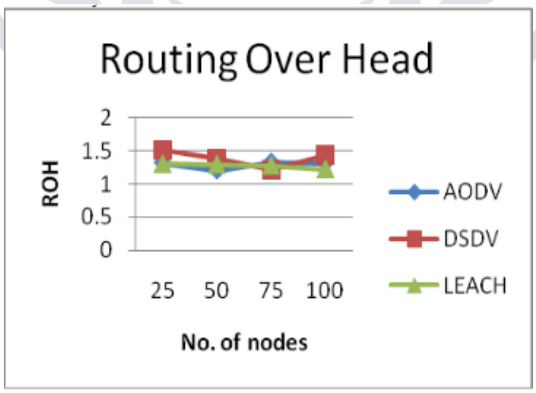
1. Packet Delivery Ratio
2. Routing Over Head (ROH)
3. Throughput (Kbps)
4. Average End to End Delay (ms)

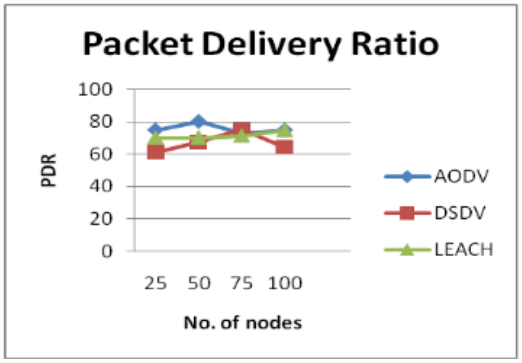
- **Simulation Parameter:**

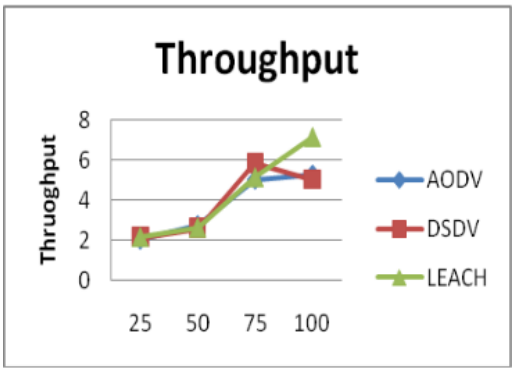
Parameter	Value
Simulation Time	500ms
Terrain Area	600*500
Time Arrival	32ms
Protocol	TCP/IP
No of Node	25,45,100

- **Comparison Graph:**

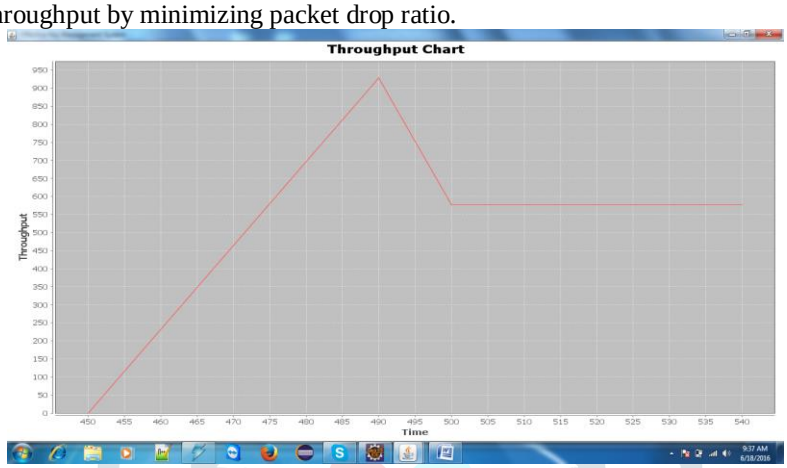








In proposed system SDH Routing technique help to improve the security and energy efficiency of wireless network. Proposed algorithm computes for maximizing throughput by reducing overhead of sensor node with shortest path algorithm. It computes throughput by minimizing packet drop ratio.



CONCLUSION

Thus we can conclude that OSPF is the open IP protocols that are proven and reliable in large scale networks. OSPF Performs better in terms of cost of transmission and is suitable for larger networks. It also provides maximum throughput and lowest queuing delay. OSPF Allows router to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service & provide loop-free topology. It can on most routers, since it is based on an open standard.

REFERENCES

[1] Amer Nizar Abu Ali "Comparison study between IPV4 & IPV6" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012 ISSN (Online): 1694-0814 www.IJCSI.org

[2] Annish Brislin M R "Analysis of IPv6 Network by enabling RIP and OSPF" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Website: www.ijareeie.com Vol. 6, Issue 4, April 2017

[3] Alex Hinds "Evaluation of OSPF and EIGRP Routing Protocols for IPv6" International Journal of Future Computer and Communication, Vol. 2, No. 4, August 2013

[4] Suleiman Y. Yerima "Implementation and Evaluation of Measurement-Based Admission Control Schemes within a Converged Networks Qos Management Framework" International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.4, July 2011

[5] S. Y. Yerima "Design and Implementation of a Measurement-Based Policy-Driven Resource Management Framework for Converged Networks" ICTACT Journal on Communication Technology: Special Issue on Next Generation Wireless Networks and Applications, June 2011, Volume – 2, Issue – 2

[6] Dr. Khaldoun Batiha "Improving Ipv6 Addressing Types and Size" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.4, July 2013

[7] Mohammad Azmi Al-Madi "A Proposed Model for Policy-Based Routing Rules in the IPv6 Offering QoS for IPTV Broadcasting" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008

[8] S. Deepa "Implementing Policy Based Routing Technique and Providing Security in IPv6 Network" International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 4 Issue: 4 502 - 506

[9] Dipti Chauhan "A Survey on Next Generation Internet Protocol: IPv6" International Journal of Electronics and Electrical Engineering Vol. 2, No. 2, June, 2014

[10] Ranjit Sadakale "An Efficient AODV Routing Protocol for Vehicular Ad hoc Network" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-4, February 2019

[11] Henry Chukwuemeka Paul "A Study on Ipv4 and Ipv6: The Importance of Their Co Existence" International Journal of Information System and Engineering Vol. 4 (No.2), November, 2016 ISSN: 2289-7615
[12] Dr. Sandeep Tayal "A Review paper on Implementation Issues in IPv6 Network Technology" International Journal of Electronics Engineering Research. ISSN 0975-6450 Volume 9, Number 4 (2017) pp. 491-498 © Research India Publications http://www.ripublication.com
[13] Palukuru Venkata Praneeth Reddy "Importance and Benefits of IPV6 over IPV4: A Study" International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2250-3153
[14] Manal M. Alhassoun "A Survey of IPv6 Deployment" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, 2016
[15] Babu Ram Dawadi "Service Provider IPv4 to IPv6 Network Migration Strategies" Vol. 6, No. 10, October 2015 ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences ©2009-2015 CIS Journal. All rights reserved.
[16] Yukio Kobayashi "SDH-based 10 Gbit/s Optical Transmission System" NTT Optical Network Systems Laboratories 1-2356 Take, Yokosuka, Kanagawa, 238-03 Japan 0-7803-1820-X/94 $4.00 *0* 1994 IEEE.
[17] S. Aisawa "40Gbit/s multi-lane distribution interface converter and its application to cost-effective optical transceiver for 40G SONET/SDH signals" Proc. of SPIE-OSA-IEEE/Vol. 8309 830925-1