PERFORMANCE COMPARISON OF ROUTING ALGORITHMS USED IN PACKET SWITCHING COMPUTER NETWORKS

NAWFAL QASIM YASEEN

AUGUST 2015

PERFORMANCE COMPARISON OF ROUTING ALGORITHMS USED IN PACKET SWITCHING COMPUTER NETWORKS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES OF
ÇANKAYA UNIVERSITY

BY
NAWFAL QASIM YASEEN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
COMPUTER ENGINEERING

AUGUST 2015

Title of the Thesis: **Performance Comparison of Routing Algorithms Used in Packet Switching Computer Networks.**

Submitted by **Nawfal Qasim YASEEN**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Müslim BOZYİĞİT
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Barbaros PREVEZE
Supervisor

Examination Date: 25.08.2015

Examining Committee Members:

Assist. Prof. Dr. Barbaros PREVEZE	(Çankaya Univ.)	
Assist. Prof. Dr. Emre SERMUTLU	(Çankaya Univ.)	
Assoc. Prof. Dr. Fahd JARAD	(UTAA)	

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Nawfal Qasim YASEEN

Signature :

Date : 25.08.2015

ABSTRACT

PERFORMANCE COMPARISON OF ROUTING ALGORITHMS USED IN PACKET SWITCHING COMPUTER NETWORKS

YASEEN, Nawfal Qasim
M.Sc., Department of Computer Engineering
Supervisor: Assist Prof. Dr. Barbaros PREVEZE
August 2015, 64 pages

This thesis investigates and compares some of the routing algorithms based on multi-protocol label switching (MPLS) architecture to provide better Traffic Engineering (TE) for the networks. The main issue here is focusing on the dependency on the rapidly growing internet service on Traffic Engineering. The MPLS is a modern technique which provides the real time communications of the multimedia data on the network service in such a way that it enhances and increases the speed of the routers. Furthermore, the MPLS architecture allows defining explicit routers in the network and ensures the Traffic Engineering Management. MPLS is developed and researched as one of the most important protocols among the protocols of today which have been built depending on the algorithms designed to get shortest path in the network for packet transmission. Another essential point are the internet service providers (ISP) which are needed to improve routing algorithm used on MPLS routers . Thus, the algorithm should be clarified and developed to suit the router devices. The advanced routing algorithms also use the advantage of MPLS network. There are many advanced routing algorithms that have been researched and used with MPLS protocol. The most important types support finding solutions according to the demand of label switching path (LSP) by use of traffic based routing, to decrease the blocking probability in the future. Therefore, in this thesis a well-known MPLS protocol network is studied using Matlab implementation. Then, it is applied with some routing algorithms. Finally, the simulation results are investigated and analyzed from different point of views. At the end of the work, some investigated routing algorithms are suggested for different kind of network conditions. These simulation results also demonstrate the advantages of integrated routing algorithms used in packet switching computer networks.

Keywords: MPLS, Routing Algorithms, Throughput.

ÖZ

PAKET ANAHTARLAMALI BİLGİSAYAR AĞLARINDA KULLANILAN ROTALAMA ALGORİTMALARININ PERFORMANS KARŞILAŞTRIRMASI

YASEEN, Nawfal Qasim
Yüksek Lisans, Bilgisayar Mühendisliği Bölümü
Danışman: Yrd. Doç. Dr. Barbaros PREVEZE
Ağustos 2015, 64 sayfa

Bu tez ağ üzerindeki trafik mühendisliğinin daha iyi sağlanabilmesi için kullanılan Çok Protokollü Etiket Anahtarlama (MPLS) mimarisi tabanlı rotalama algoritmalarının incelenmesini ve karşılaştırılmasını içermektedir. Ağlar üzerinde yapılan bu çalışmada sürekli olarak büyüyen internet servislerinin Trafik Mühendislği üzerine etkilerine odaklanılmaktadır. MPLS, ağ üzerinde kullanılan yönlendiricilerin hızını arttıracak ve gerçek zamanlı çoklu ortam verilerinin aktarılacak şekilde ağ servislerini sağlayan modern bir teknik kullanır. Ayrıca, MPLS mimarisi ağ üzerinde bulunan farklı yönlendiricileri tanımlar ve trafik yönetiminin sağlanmasını garanti altına alır. MPLS'in günümüzde en kısa yoldan gönderim yapılacak yulu seçen birçok protokol içinden en iyier inden birisidir. Bir diğer önemli nokta ise, İnternet Servis Sağlayıcılarının (ISP) MPLS yönlendiricileri üzerinde çalıştırılan rotalama algoritmalarını geliştirme gereksinimlerinin olmasıdır. Bu algoritma sade ve yönlendiricilerde uygulanabilecek nitelikte olmalıdır. Gelişmiş rotalama algoritmaları, MPLS ağının rotalama algoritmalarını geliştirme avantajlarını da kullanırlar. MPLS üzerinde araştırılmaya devam edilen ve kuuanılan birçok gelişmiş rotalama algoritması bulunmaktadır. Bunlardan en önemlileri ise, trafik durumuna göre karar vererek bloke olma olasılığını azaltan rotalama teknikleri ile her türlü etiket anahtarlamalı yol (LSP) isteği için çözüm sunan trafik tabanlı algoritmalardır. Bu nedenle bu tezde, bilgisayar ağlarında iyi bilinen bir protokol MATLAB ile benzetim yoluyla çalışılmış ve daha sonra bazı farklı rotalama teknikleri bu protokol üzerinde uygulanmıştır. Son olarak, simulasyon sonuçları incelenmiş ve farklı bakış açılarından analiz edilmiştir. Çalışmanın sonunda, farklı ağ koşulları için; incelenen rotalama algoritmalarından bazıları önerilmiştir. Bu benzetim sonuçları, paket anahtarlamalı bilgisayar ağlarında entegre edilerek kullanılan rotalama algortimalarının avantajlarını göstererek ortaya koymaktadır.

Anahtar Kelimeler: MPLS, Rotalama Algoritmaları, Etkin Çıktı Oranı.

ACKNOWLEDGEMENTS

All profound praise, glory and thanks to Allah Almighty, the most Compassionate and the most Merciful (Subhanahu Wa Taalaa) Who has given me courage and patience and inspired me to carry out this work. Allah's peace and blessings be upon His last Prophet Muhammad.

I would like to thank my supervisor, Assist. Prof. Dr. Barbaros PREVEZE for his continuous support, encouragement and advice in the course of writing my thesis. Many thanks are due to all the academic teaching staff at the department of computer engineering for their efforts and guidance throughout the study period. I dedicate this thesis to my father whose support makes my way of success. I extend my acknowledgement and deep love to my mother for her support, kindness and her prayers which paved my way towards success in life. To my dearest and lovely brother and sisters, my brother in law, for continuous supporting along the period of my study. I also wish to express my sincere gratitude to my dear wife for her continuous support and help in both good and hard times. Besides I would like to devote this effort for my precious stone, my son Muhammad. Finally, my thanks go to the friends who stood with me throughout the study period, and to everyone who helped in a way or another in bringing out this piece of work.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

ARIS	Aggregate Route-Based IP Switching
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CAR	Committed Access Rate
CEF	Cisco Express Forwarding
CR-LDP	Constraint Routed- Label Distribution Protocol
CSR	Cell Switching Router
DS	Differentiated Service
EGP	Exterior Gateway Protocol
FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base
FR	Frame Relay
FRR	Fast Re-Route
FRTS	Frame Relay Traffic Shaping
GMPLS	Generalized MPLS
HDLC	High-Level Data Link Control
IETF	Internet Engineering Task Force
IGP	Internal Gateway Protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Server Provide
LDP	Label Distribution Protocol
LER	Label Edge Router
LMP	Ling Management Protocol
LSP	Label Switching Path
LSR	Label Switching Router

MPLS	Multi-Protocol Label Switching
MPLS-TE	Multi-Protocol Label Switching-Traffic Engineering
MPOA	Multi-Protocol Over ATM
NNHop	Next Next Hop
OPVN	Optical Virtual Private Network
OSI	Open System Interconnection
OSPF	Open Shortest Protocol First
PHB	Per Hop Behavior
PLR	Point of Local Repair
PPP	Point-to-Point Protocol
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RIP	Routing Information Protocol
RRR	Routing with Resource Reservation
RSVP	Resource Reservation Setup Protocol
RSVP-TE	Resource Reservation Setup Protocol-Traffic Engineering
SIN	Ship's-In-the Night
TE	Traffic Engineering
VC	Virtual Circuit
VCI	Virtual Circuit Identifier
VOIP	Voice Over IP
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WRED	Weighted Random Early Detection

CHAPTER 1

INTRODUCTION

1.1 Introduction

In order to build an internet network and other networks, the scientists and companies around the world have been finding and working on many techniques during the last 20 years especially those ones which are relating network protocols. The development of these network protocols led to the making of the networks more comprehensive. This happened especially after the industrial field developed that followed the suggestions and the designing of new protocols which started experiencing due to these networks [1].

In the past, the main idea of the network was achieving a communication between the source and destination nodes through giving an IP to each of them, this connection was supposed to receive and send a packet of data from a source to a destination and then vice versa, without delivering any insurance to the destination, also that might take time in millisecond. As mentioned and discussed above this created more than one problem; especially relating to the reliability and time delay.

Therefore intelligence of algorithm that uses to find the best path between source and destination is of extreme importance, as the idea of giving an IP to each node is meant to make this easier. Yet another idea is to make the IP change dynamically, this idea helps in overcoming many problems that are caused by the catastrophes or wars and unexpected errors which confuse the systems, especially huge systems [2]. Therefore the network should realize the requirements of modern life and

Applications like the ones which need real time processing, high speed, high security such as banking and shopping through internet [3].

The effective services like IP Telephone need predicting and finding the shortest path between two nodes. Thus, the next generations of systems insist on supporting the real time applications, video and voice applications. As the using of Virtual Private Network (VPN) network motivates the providers of IP technique to search about additional mechanisms to control the motion effectively inside IP protocols. İn order to satisfy all requirements, the internet service providers should provide a high performance service and high performance in finding the best path. Here is another method that is used for finding the best path, this method depends on using Asynchronous Transfer Mode (ATM) over IP by using virtual circuits (VC's) or multi-protocol over ATM (MPOA), but this method is complicated and costly therefore the scantiest offer is to find a method simpler than MPOA. All previously discussed methods may do by MPLS because MPLS is combination between the properties of Simplified transmitter switches in link layer and with control and flexible routing in network layer [4]. As mentioned above, the MPLS is a technology that leads to the future of IP networks by including the Internet which provides a new scheme for sending data effectively that affects the traffic Engineering [5]. Moreover, it is originally used as a tool to send packages in networks, i.e., IP packets effectively across ATM networks, through managing the networks by connecting certain classes of packets with virtual ATM circuit. This technique effectively integrates the connection oriented technology by packet switching [6].

Now here one has discussed the main challenges faced by networks in general:

- Scalability: the networks should not be limited virtually in size, the information should grow very fast and also needs proportion in network which is growing every day, and could and should be carried on router at the least.
- Evolvability: one of the great challenges is to achieve modification and development without effecting network distribution.

- Integration: the combination between many applications is an example of system integration. The subject of integration at all layers is very important to design an interactive network [7].

1.2 Importance of the Research

The importance of this thesis is be clear in the beginning in order to build new and modern networks which provide the best world criteria and also are in touch with advanced routing algorithms and modern technology.

1.3 Thesis Goals

In this thesis, we look at the different routing algorithms techniques that can be used for route packets and reroute traffic faster in case of a failure in a network. Focus is especially made on three routing algorithms which are used in MPLS which is applied in MATLAB. The aim of this thesis is to look at the different routing algorithms and to see the result that makes the traffic flows in an MPLS domain resilient for real time services. The same traffic can be rerouted in the network as fast as possible.

1.4 Advantages of the Research

One of the main advantages of this thesis is that it focuses on the issue of conventional routing protocols, which is, they do not take capacity constraints and traffic characteristics into account when routing decisions are made. The outcome is that, that some segments of a network can become congested while other segments along alternative routes get underutilized.

The other advantage is this, that MPLS networks consider the natural development of networks in order to secure necessary requirements to support the huge improvement in the ever growing internet services while, at the same time, enabling the network managers to control the traffic with higher levels and preventing congestion.

MPLS technologies provide transmission capability by adding tags to distinguish packet. During transmission, if package is sent by road congestion, the packet chooses the shortest created backup path and prefers the way where traffic is minimal. Basically, the idea is to have only the first router do an IP lookup, then all future routes in the network can do exact matching "switching" based on a label. This would reduce load on the core routers, where there is high-performance. Hence, the main reason of finding the MPLS are the necessity for increasing internet speed, as well as implementing traffic engineering (TE) and improving network resiliency with MPLS fast reroute.

Multi-Protocol Label Switching-Traffic Engineering (MPLS-TE) advantages can be summarized as the followings:

- With MPLS, traffic engineering features emerge in the layer 3, which enhance IP traffic, directed by enforced constraints according to the network chart and its capacity.
- Routing of IP traffic across network depends on the traffic resources requirements and available resources in a network.
- Using constrained routing where the traffic flow path is the shortest path that corresponds to the resources requirements or constraints of bandwidth requirements and traffic flow priority.
- The ability to share unequal carrying cost on the paths.
- It calculates link bandwidth and traffic flow size when specified routers are used across the network [5].

1.5 Problem of the Research

In packet switching computer network, if a failure occurs, then each router in the network has to be informed about the failure and the routing tables in each router has to be recomputed using a shortest path first algorithm. When routing tables have been recomputed and converted, all paths that have used a failed link or node are rerouted through other links. The recovery mechanisms rely on the capabilities of the routing protocols. Routing protocols make the network able to survive one or multiple links or node failures, but they do not guarantee to have the same percentage in the development of the system by using fast reroute mechanism. The most important issue which is focused in our work is how can one increase the throughput and decrease the loss rate in packet switched computer networks. Here it should be kept in mind; the recovery strongly depends on the dimension of the network and on the used routing protocol.

1.6 Thesis Organization

This thesis is divided into eight chapters. Chapter two gives an introduction of the MPLS architecture, the basic functionality of MPLS and some of the functionalities in MPLS that can be used for traffic engineering. Chapter three gives a short introduction to traffic engineering which is today's one of the main reasons of MPLS use. Chapter four includes an overview of the common failures in MPLS networks, explanation of failure detection mechanisms and some recovery techniques for MPLS networks. This is done because it is important to know how recovery is performed with MPLS, this gives an insight into some of the strengths of MPLS recovery and a comparison for protection types in MPLS. Chapter five includes background and literature review information. Chapter six will give an overview of available simulator environments that can be used for MPLS simulations. Chapter seven provides simulation results that demonstrate the effectiveness of the routing algorithms in MPLS. The simulations done for this thesis are explained and the results from those simulations are analyzed. Chapter eight presents conclusion that are drawn from the qualitative analysis of the architecture and quantitative simulation results. This is followed by a brief description of the opportunities for further research in the future.

CHAPTER 2

MPLS ARCHITECTURE

2.1 Overview

In the beginning, the internet applications and requirements were simple and based on simple program with interfaces to support networks that was further based on T1/E1 and T2/E2 techniques. But this simplicity did not agree with the new application because it needs to increase its speed as well as the bandwidth. So, for that many devices it was necessary to make support of switching into link layer and network layer. At the time of layer 2, devices solve the bottleneck problem via sub networks; the devices of switching in layer 3 cause the bottleneck problem to decrease by using high-speed switching devices.

Most of the routing protocols today are built on depending on the algorithms which are designed to get the shortest possible path in the network to send a packet [7]. But it neglects other parameters like delay, bottleneck, irritation that reduce the network performance.

2.2 Traditional Routing and Packet's Switching

In the environment of traditional routing, the packet is sent (hop-by-hop) via internal gateway protocol's (IGP's) like routing information protocol (RIP), Open Shortest Protocol First (OSPE), and exterior gateway protocol (EGP's) like Border Gateway Protocol (BGP). This is done by referring to the addresses of layer 3 in front of the target in the table in order to enter the next hop. This operation is repeated at each hop by hop until the packet reaches the destination node. Figure 1 shows how the packets route to router F; the router C will refer to router F, after that router C determines the best route according the specifications determined by the IGP. IGP protocols have the ability to develop, but the main problem is that they do not have the abilities to route as an autonomous system, network management, traffic engineering, or as Scalable IP Services. Moreover, as observed in Figure 1, in the traditional routing environments, the router should make the decision to forward the packets that should send to router F according to metric system that Specified by the IGP. In the case of OSPF, the metric system should depend on many criteria whilst the packet bandwidth still uses the main criteria. As shown in Figure 1, the packets from routers A or /and B, that should reach to router F, have the same path, therefore the bandwidth of router D is greater than others like DS-3S, and the path of router E is connected through T-1s lines. Thus router D is going to be a unique router that is used until an error occurs in the network [2].

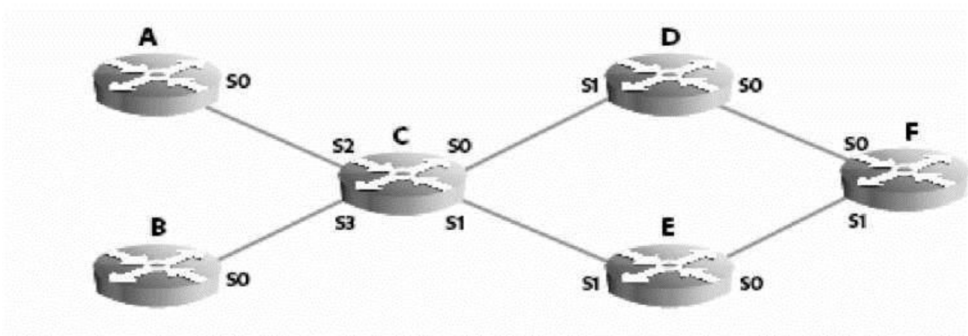


Figure 1 Example of Traditional Routing [2]

The traditional packet replacement could be summarized as follows:

- Searching about IP address of routing in table, It may include many of the appropriate harmonics.
- Selecting the destination network that compatible to the mask of sub network.
- Find the header of MAC address for the next hop, and copy it to the head of the packet [8].

2.3 New Scheme for Sending

The internet network service is a technique which became increasingly popular over the last century. Today, many applications like Voice Over IP (VOIP) or watching TV videos on internet have also become popular. This happened after the WWW used the IP as the top most communications system in terms of popularity. The providers of internet developed according to the internet expansion. At the same time the economic conditions have the main role in choosing networks of the next generation.

The increasing number of users and clients, who use the network cause an increase in the number of routing tables, the routers must process the received data in routing tables. Therefore achieving optimality is the goal of the internet service providers at all times. As the IP protocol was not designed to be effective. Hence, we need to find best solutions to process the packets of data [9].

The service providers, that use the ATM techniques, do not have the ability to develop themselves to a new technique. Many of internet providers include the ATM in their networks, and new applications which are capable of supporting both ATM and IP but they do not provide techniques promised by the companies, despite their promises. Many researches have been done on MPLS in the last past year, and techniques have been applied of MPLS in internet services and providers.

The MPLS produces a new sending structure which affects the traffic engineering and applies VPN as shown in Figure 2 [5].

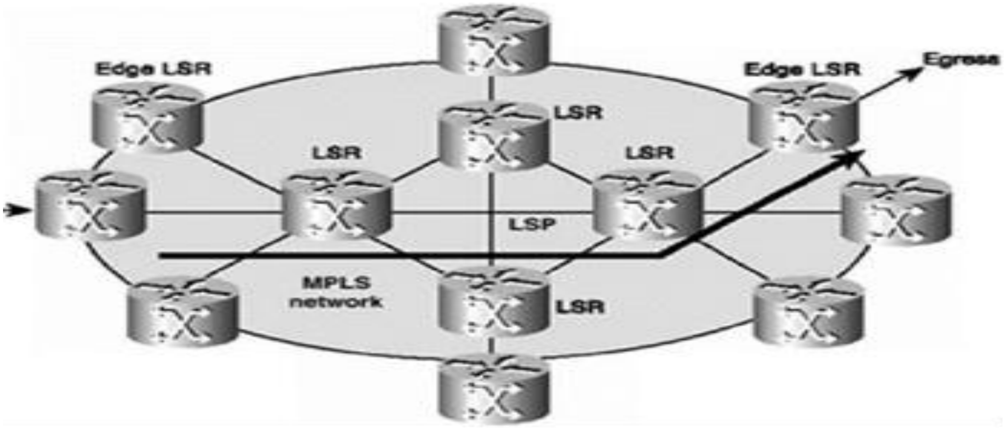


Figure 2 Topological of MPLS [5]

In a few years, the MPLS has developed to be the main tool for the internet providers in order to increase the income. There are rapid growing services that use or support the MPLS [10]. The success of MPLS belongs to the reality of the network which has the ability of carrying all traffic that starts form the IP until reaching the VOIP, and layer 2. The MPLS is considered a tool to be unique for unification the IP networks, Voice, Frame Relay, and ATM in a unique environment that provides better services in comparison to its minimal cost [11].

2.4 The Benefits of MPLS

The exchanging methods are based on label for routers and ATM allows taking the sending decisions according to the contain labeling instead of finding a complex routes based on IP address to the target.

One of the main reasons of MPLS is its necessity for increasing internet speed. The IP packets replacement is slower than the replacement of labeled packets because of searching for the label in the head of packets. The router send IP packet through searching for the destination IP address and finds the match address in the routing table. This depends on the application which is designed by the company which designs that software. The structure of IP addresses which consist of four digits, therefore the searching for IP address is complex and consumes time [11].

2.4.1 Virtual Private Network (VPN)

By using the MPLS, the services providers can create VPN networks at layer 3 through their network for multiple clients, by using general environment and without using decoding applications and end destination. As a result for the MPLS the LSP makes an effective channel through IP network as shown in Figure 3. It also isolates the traffic in a channel from other channels when exchanging the Label Switching Router (LSR). Therefore a lot of virtual private networks can do work on MPLS structure [12].

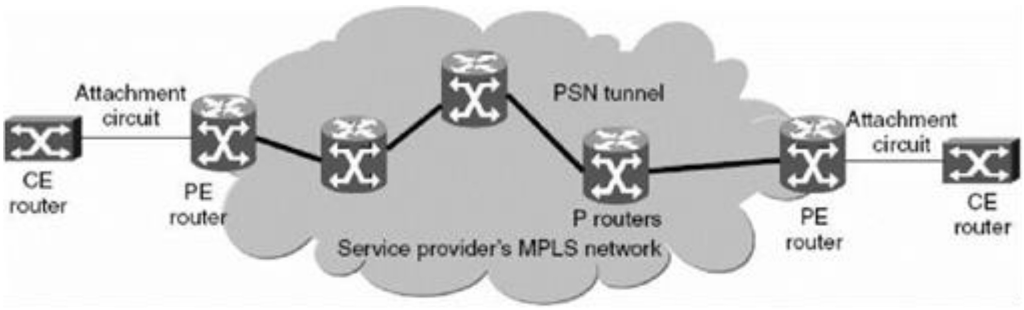


Figure 3 MPLS-VPN Structure [12]

2.4.2 Traffic Engineering (TE)

This TE provides the ability to find a single path or multi specific paths to transfer data at a network and also has the ability to prepare the performance properties for traffic class, enhancing performance property by using bandwidth service for used paths. At each network there is a node suffering from congestion, while another node is still not being used, this is due to the routing protocol which chooses the shortest path regard less of the parameters of other networks, like use of node and the requirements of traffic using Traffic Engineering, the network operators can redistribute packets to balance the data on channels and give equal service to all customers. The MPLS provides a huge network with affectivity, and this is the best way to apply the traffic engineering. The traffic engineering guides the MPLS data flow through organizing the recourses and distributes it to the actual bandwidth. This operation prevents the unexpected congestion, and has the ability to recover from link or node failure [13].

2.4.3 Quality of Service (QoS)

By using the service MPLS, the service provider ensures many class of quality of services, for the users of VPN. MPLS, the QoS is a basic item of MPLS. The MPLS does not need to include QoS in IP network because of these properties included in the MPLS. The MPLS could be used to apply the quality for ATM services which provide a service of voice and video with high reliability. Besides to transfer data, Such a service is demanded today by many applications. MPLS supports benefits of following QoS.

- Classify and make mark to each packet: allow packet classification by dividing the traffic into many priority levels or services levels.
- Preventing the congestion: prevent congestions using random discovery algorithm which is called Weighted Random Early Detection (WRED) to insure port management.
- Congestion management: it is necessary to use stack technique when congestion happens to ensure that important application that has the priority traffic than the other applications with low priority. There are many stacking methods for example: priority stacking, normal stacking etc.
- Traffic enhancement: the traffic monitoring leads to the traffic enhancing the network. Imagining the traffic to be easier in the range of using ports, while the monitoring make it's specific. For example; Frame Relay Traffic Shaping (FRTS), and Committed Access Rate (CAR).
- Pointing: Resource Reservation Setup Protocol (RSVP) It is the main machine to control traffic in the network. The RSVP can demand recourses from the network which achieve certain traffic through any network [14].

2.4.4 General Use of Standardized Network Structure

In MPLS, the main idea is labeling packets that enter in accordance to addresses or some other criteria and are replaced all traffic through general structure; this is a great benefit of MPLS technique. One of reason that makes IP protocol control the networking world is that, many techniques pass through it. Not only the data passes through IP but it passes through phone also. By using the MPLS with IP, we can expand the abilities as many as we want. The adding of labeling to the packet support with carrying other protocols like IPv4, Point-to-Point Protocol (PPP), high level data link control (HDLC), Ethernet, IPv6, and the technique of layer 2, the MPLS merging the performance and The advantages of switching of layer 2 (data link layer), with the ability to expand route to the layer 3 (Network layer) , this allows the providers services to face the challenges of growing the use of network with ensuring the chance of services discriminating among services without effecting the current network structure.

The structure of MPLS is flexible and could employee any technique for any other network. Also, supportive MPLS is available for all layer 3 protocol. The MPLS introduces IP service over ATM in a good manner. MPLS supports the creation of different guides between the source and the destination in an internet network which is based on routers. By merging the MPLS in The structure of their networks, this leads to the decrease of the cost of many servers that increase the income and the productivity and produce different services and win the competition in comparison to the servicers which did not use the MPLS [5].

Apart from all the previously mentioned issues, the customer's services providers have faced huge problem of presenting multiple services over a public network structure without collision among themselves whereas MPLS has solved this problem [15].

We can abstract the main differences between MPLS network and the classical IP network form supporting the quality of services , traffic engineering, and the capability to expand, integrating with voice and video as shown below in Table 1 [7].

	MPLS Network	classical IP Network
Scalability	Creates small number of adjacencies for optimal protocol routing performance	Creates large number of router adjacencies which adversely effects routing protocol performance
Traffic Engineering	Label switched paths (LSP's) can be manually created through the network to ensure QoS guarantees and provision new services	Best effort delivery only
Quality of Service	Maps specific IP flows to ATM classes of service	NO differential IP QoS support
Voice and data integration	Standard voice quality achievable with traffic engineering and QoS support	Voice over IP treated as best effort delivery

Table 1 The Features of the MPLS Network Versus Traditional IP Network [7]

2.5 The Revolution of MPLS

The first goal of switching which is based on the label is the proximity of speed switching of layer 2 to the speed of layer 3. The first rationalization for techniques like MPLS, is considered the main benefit of using switching of the layer 3 that uses the technique which is based on using Application Specific Integrated Circuit (ASIC) , that could do searching about routes in a compatible velocities for most port types, this led to create a group work which is called Internet Engineering Task Force (IETF) in 1997. The MPLS developed from previous techniques including copies of tag replacement like Cisco's Tag Switching, IBM's Aggregate Route-Based IP Switching (ARIS) Toshiba's Cell-Switched Router (CSR), Ipsilon's IP Switching, and Lucent's IP Navigator. The Cisco worked to develop the MPLS criteria that merged most of the benefit of Cisco, the MPLS introduced in switching BPX and MGX in client line in addition to the router which was based on MPLS [5]. The main property of MPLS network could be used to create different tunnels for many types of motion through network core [5].

2.6 MPLS and Internet Infrastructure

The MPLS effects on the mechanism of sending IP packets and decides the path which packets should pass through the internet, and this has resulted in the basic structure of the internet.

The MPLS makes IPV6 simple to spread because of the routing algorithms that are used by MPLS for IPV4 and could be applied on IPV6 with the uses of routing protocols which support the addresses of IPV6. The MPLS directly benefit internet, the greatest benefit is related to the traffic engineering for server provider, this leads to higher degree in the using of sources that increase the efficiency [5].

2.7 The Application of MPLS

The first version of Tag switching in CISCO IOS allows traffic engineering, which at first is called Routing with Resource Reservation (RRR). The first application of engineering traffic in CISCO IOS was constant. This means, the network operator should Prepare all hops that follow a certain flow of traffic in the network. The next application makes the traffic engineering dynamical through using expansion for the routing protocol; in this case the operator does not need to Prepare channels for traffic engineering hop-by-hop in constant form. The routing protocol for node status holds additional information to be able to create channels in a more dynamic method. These channels reduce the size of the work that the operator should do. This makes traffic engineering in MPLS more popular. Until the foundation of MPLS VPN the MPLS was not so popular, but when CISCO introduced a version CISCO IOS 12.0(5)T and the CISCO IOS version that supports MPLS VPN, it became popular , [11]. Another application for MPLS that is considered very important, is Fast Re-Route (FRR). This technique support a mechanism which makes special spare channels and fast reroute for traffic from paths (TE) which is protected by spare channels at the time of connection failure. These channels are found by Resource Reservation Setup Protocol-Traffic Engineering (RSVP-TE). One of the most important applications in the MPLS is general MPLS (GMPLS). The goal is to integrate the controlling in the routing layer with the optical sending layer, and thus facilitate the application of traffic engineering across the network [16]. GMPLS sends the packet in high speed that closes to the speed of optical speed, also ensuring central management, Load balancing, the GMPLS is considered the main reason the finding of Optical Virtual Private network (OPVN) [17]. The GMPLS has the ability to inform the neighbor node if an error has happen in the network [18].

2.8 Understanding MPLS

MPLS is considered the normative copy of the technique Cisco System Tag Switching which combines flexibility and expansion ability in routing of the layer 3 with traffic engineering characteristic. Also, MPLS is built on understanding tag replacing that specialization in short tags with limited length for packets or cells which inform switching nodes how to send data. To understand even better, one can compare MPLS with post office which is one of the famous examples to describe MPLS, when the post office receives part of posts. That post is processed at the sorting department, the letters are checked and tagged by mark, and this mark identifies the path of message until it reaches the determined destination. The mark refers to the path from another company. If each classification establishment reread message address, the delivery of message will not be delivered in the right time. The same thing is done with the MPLS, if each router reread the address information of IP packet, this is considered as a waste of time, the MPLS saves routing sources through making the decision of routing for just one time and make the other routers routing decisions depending on tags only [19].

The Table (2) shows the comparison between IP and MPLS techniques from the analyzing tags, routing decision, cost, and supporting multi broadcasting [20].

	MPLS	IP
Entire IP header analysis	Performed only once at the ingress of the packet's path in the network	Performed at each hop of the packet's path in the network
Routing decisions	Based on the number of parameters including the destination address in the IP header like QoS, data types(voice), and so on	Based on the destination address in the IP header
Support for unicast and multicast data	Requires only one forwarding algorithm	Requires special multicast and routing forwarding algorithms

Table 2 Comparison Between MPLS and IP Techniques [20]

It can be noted from the Table (2) that MPLS combines the two techniques, the first is IP technique which includes simple and open standard and the second is ATM technique which moves towards the quality of service and control movement [21]. The keys of understanding the MPLS starts from defining all these components of MPLS as shown in Figure 4.

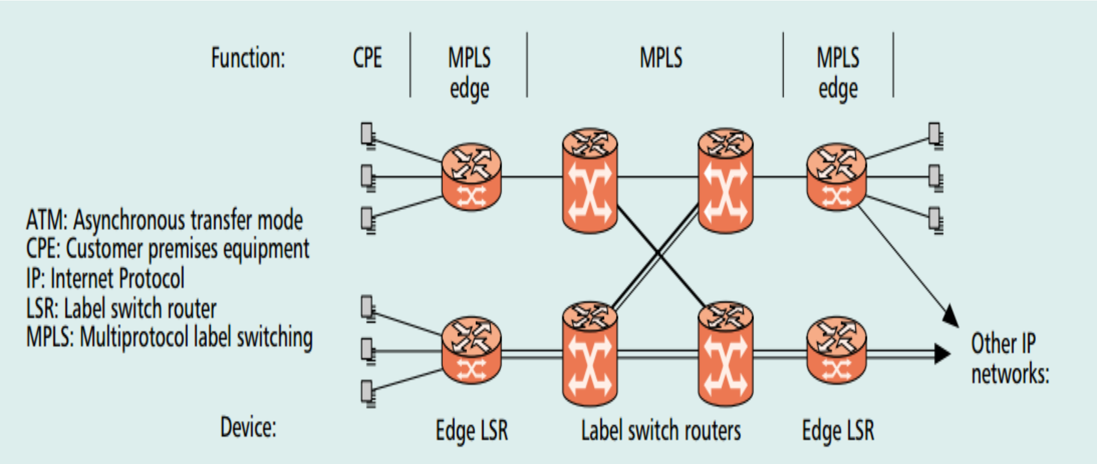


Figure 4 MPLS Components [22]

2.9 MPLS with OSI Standard

The Open System Interconnection (OSI) consisted of seven layers, the first layer is of physical layer and the last layer is the application layer. The physical one is related with cables and a mechanical and electrical property, the layer 2 is related with the connected data like for example the connection of two machines, but not for more than. Layer 3 or network layer formats packets from end to end. The most famous protocol of layer 3 is IP protocol.

As MPLS is not needed in layer 2 or 3therefore it does not need to be compatible with OSI protocol type [11]. In conclusion, it may be easier to introduce MPLS as 2.5 protocols as shown in Figure 5 [23] and [24].

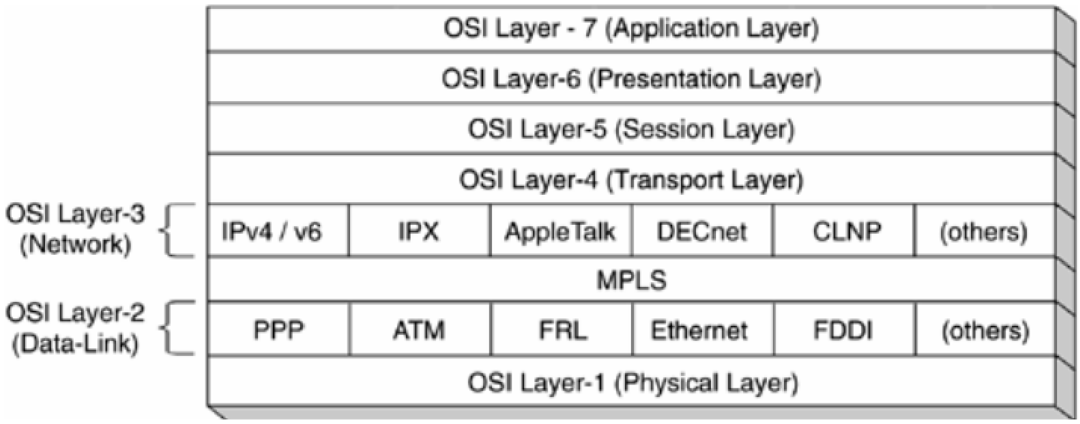


Figure 5 MPLS Layer [11]

2.10 The Label

The label is defined as Multiprotocol Label Switching Architecture in IETF with fixed length and locally defines the use of Forward Equivalence Class (FEC), the tag which is placed on the packet that displays the FEC that belong to the packet [25]. Which represents the abstract for header packet of IP, although it is contained inside each required information which is send to the packet from the source to the destination.

2.10.1 Understanding labels

To understand the mechanism of MPLS one can start from the following:.

- The efficiency of hardware component of MPLS is to read the tags and use the basis to send packets.
- A tag is specified to each packet to identify the priority of destination, VPN membership, the properties of service efficiency and routing the traffic engineering that needs to use the packet.
- Local meaning of the label, this means that the tags must be unique. Only on the base of each port [2].

  The Figure 6 shows format and insert position of MPLS label.

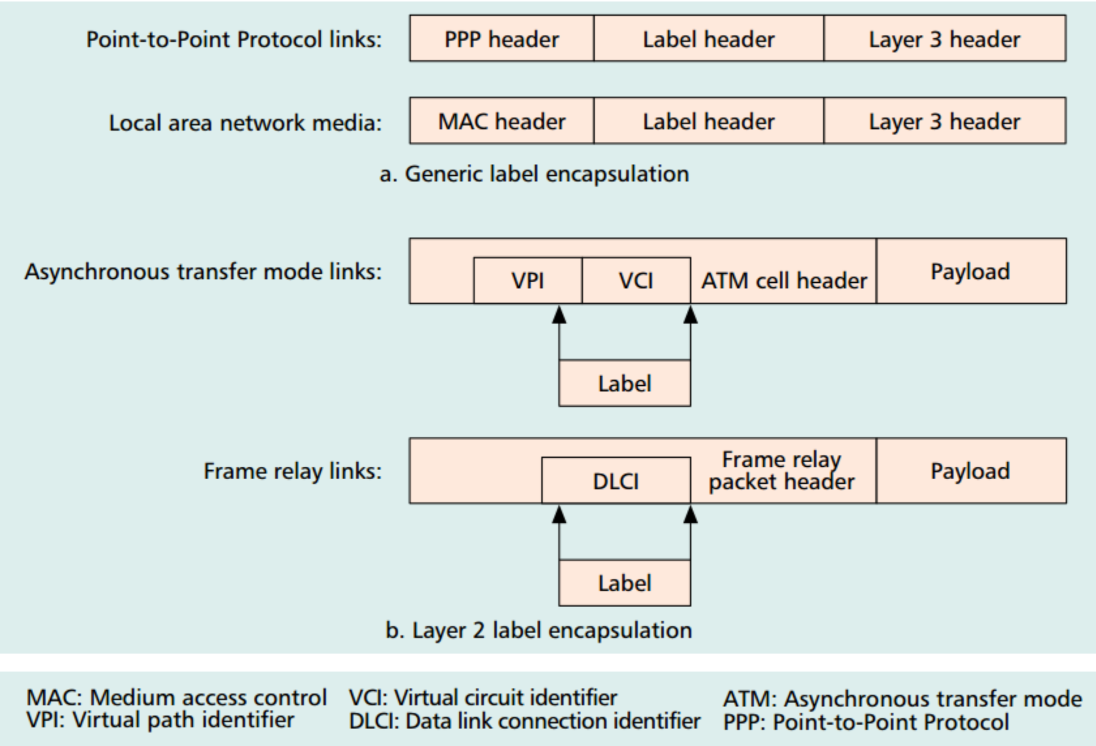


Figure 6 Carrying a Label on a Packet [22]

2.10.2 Label structure

MPLS label as shown in Figure 7, that represents a field of 32 bit and consist of the following elements:

- Label value: it is local significance that consists of 20 bits.
- Bit experimentalism (EXP): that reserves three bits which can be connected between information; Differential Services (DS), Per Hop Behavior (PHB).
- The bit in the stack: if it is equal to 1 that means enter the element with priority in the stack, and 0 which means entry for all other elements without priority.
- Time To Leave (TTL): eight bits that use to decode the value of leaving time or hop number [26].

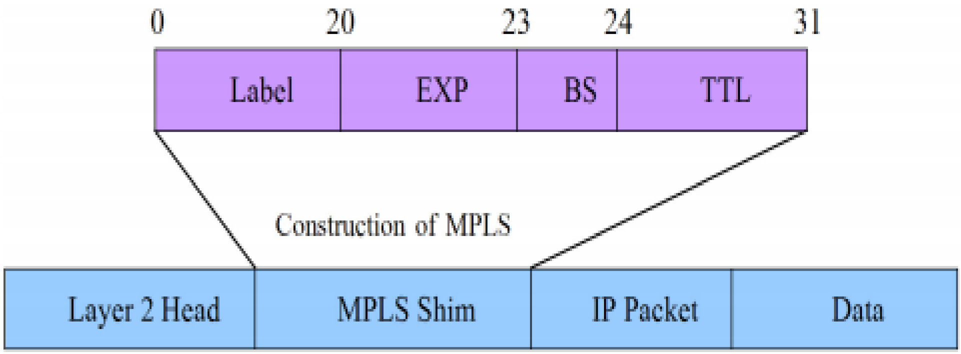


Figure 7 MPLS Layer with Label Components [26]

2.11 MPLS Terminology

Below several terminologies are given of MPLS:

2.11.1 The MPLS Domain

The MPLS domain can be divided into MPLS core and MPLS edge. The core consists of nodes neighboring only to MPLS capable nodes, while the edge consists of nodes neighboring both MPLS and incapable nodes.

2.11.2 Label Switching Router (LSR)

The routers of switching label are considered for the main machine that replaces packets according to the table [23]. The main task of the router is to send packets in a very high speed. Usually the router considers the kernel for label switching that includes classical IP protocol in order to know the capability to reach to network layer [14]. Some nodes of MPLS work as ATM switches and as MPLS nodes at the same time. The MPLS nodes that are based on ATM have a very important property that is called ship-in-the-night (SIN). This property allows both protocols ATM and MPLS to work separately at the same port; this is very beneficial in the processing of packets of the IP traffic that are not labeled [27].

2.11.3 Label Edge Router (LER)

The label edge router is a device that switches the network layer that is found at the edge of MPLS [23]. The main task of LER's is to apply the labels or marks on packets that are going in the MPLS network and removing labels from the packets to leave MPLS network [14]. The LER also checks packets from other classical environment and perform classification on the security and efficiency of service. The LER utilizes the protocols of classical router to determine information of capability to reach network like OSPF and Intermediate System to Intermediate System (IS-IS). After that applies the suitable label for the packet and send the packet to the other hop.

2.11.4 Label Switching Path (LSP)

This is one of the most important concepts for the actual use of MPLS. An LSP is required for any MPLS forwarding to occur. It also can be fixed or made dynamic by setting of dynamic LSP which is prepared by using routing information, but fixed or static LSP is configured by the company related with it [23]. The packet is forwarded solely based on the information in the MPLS header and the interface that the packet arrives on, which is used as an index in table lookups that specifies the packet treatment. There are three basic types of operations that can be applied to a packet.

- Push the label stack.
- Swap the top label with a new label.
- Pop the label stack [28].

2.11.5 Forwarding Equivalence Class (FEC)

This name is given to the group of similar traded packets destined to the same route is FEC. The FEC is considered as any group of packets that are sending the same way through a network. The FEC includes all packets which are address compatible with destination address in IP network, or a group of packets which have same address source and destination. The FEC built from the information taken from IGP, like OSPF or IS-IS [29].

2.11.6 Label Stack

Label stack is by putting multi label inside the packet, which a MPLS can support by the pyramidal routing. That is group of labels linked with packet in stack label. When the packet passes the network the switching happens for the top label only.
Stacking label is a very effective property of MPLS which enables the LSR's for inserting additional label at the beginning of each labeled packet, and creates closed channel that has the ability to share many LSP’s. At the end of the channel the LSR removes label of stack. Moreover; when the ATM has a single level of stacking where the MPLS support infinite stacking, the service provider could use label stacking to merge hundreds and thousands of LSP's inside a few network channels between existing nodes. A few channels mean few routing tables, which lead to making the duty of service provider easier [30].

2.11.7 Label Distribution

This is when the router switches labels of a following packet and sends it to a selected path. The router must have a method in learning the value of the label which is expected. The MPLS protocol is not determined by one protocol to distribute labels among LSRs. In fact it allows a clear way to use distributed label in different scenarios as shown below:

- Label Distribution Protocol (LDP).
- Constrain Routed –Label Distribution Protocol (CR-LDP).
- Resource Reservation Setup Protocol (RSVP).
- Border Gateway Protocol (BGP).
- Open Shortest Protocol First (OSPF) [20].

In fact the used protocol needs to depend on requirements that are offered by a Special network. The LDP is designed for this use but the LDP cannot comply with all requirements of QoS. In order to support the QoS application, the LDP should be able to select and reserve network resources along the path of switching label in a correct way, so as to support one should use existing protocol reserved resources and expand it to distribute label, or take a protocol which can distribute the label and expand it. An example is the RSVP protocol, another example is of reserved sources is LDP and BGP. There are protocols to create tunnel for traffic to allow better traffic, these protocols are CR-LDP and RSVP-TE. Also, the OSPF protocol processes traffic engineering to become OSPF-TE [17].

2.12 Tunneling MPLS

The tunneling key properties in MPLS, especially when using VPN is when the operation of switching labels for LSP between LSRs, that supports the LSP, therefore the medium LSRs that LSP passes through does not need to check the contents of data packets that are coming to the LSRs. For this reason we could represent that LSPs form tunnels through each part of the MPLS network. Each tunnel contains obscure information between the tunnel entrance and the LSRs' exit, this means that the entered data includes the IP tag that could encrypt without any bad effect to that ability to send data . Tunneling MPLS is as shown in Figure 8.

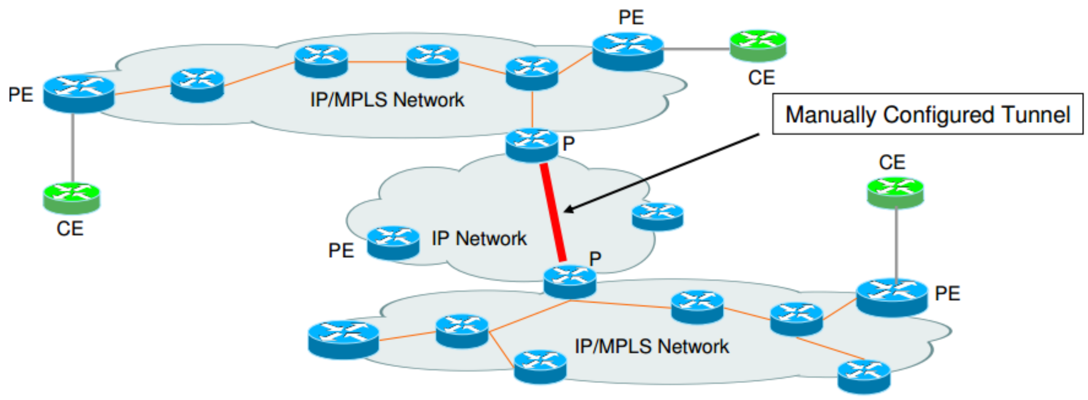


Figure 8 Example of Tunneling MPLS [31]

2.13 The Mechanism of MPLS

The MPLS network consists of a group of nodes called LSRs that able to switch and route packets according to the label attached to each packet, the labels identifies flow of packets between the start and end points, or in case of multi broadcast between sources each coming from FEC, so the MPLS is a technical route connection accompanying each FEC that describe the traffic of requirements QoS for that flow. The LSRs do not need to check or process the IP tag, instead of that each packet is send simply according to the value of label, for this reason the operation of sending is simpler from that one used in IP router [26]. In a traditional routing, each router should process each packet to achieve next hop that should be taken until it reaches the final destination, this operation repeats hop by hop that causes delay through each router along the path of IP [15], [32]. This effects the real time applications . In other words, in MPLS network only the LER processes each packet a fully. While LSR through the network that sends the packets according to the label along label path, in this way it prevents the MPLS from searching about IP address along the path [33]. This operation reduces the delay that is caused by the classical router network. The main difference is between routing the IP and MPLS.

Now one can discuss the working of MPLS with more detail. The next steps show how the packets are send through MPLS network as shown in Figure 9.

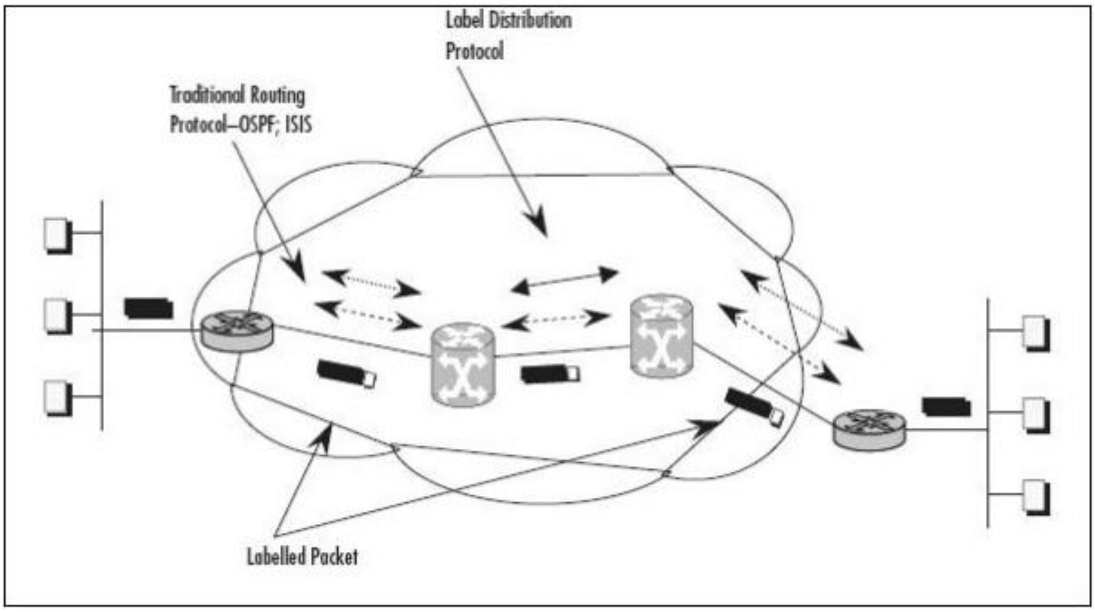


Figure 9 Transmission Packets of MPLS [33]

- After creating routing tables, the LDP links dynamically to all routing IP in router table.
- At the time of entering of unlabeled IP packets to LER, the router asks for routing IP table and sends data base information, the router choose which interface should the packet send, and which label should be determined for each packet. The decision of which interface should the packet send does not depend on a subsequent of destination, but there is FEC which could represent subsequent but it could represent the packet style as well as send the packet out through a way suitable interface towards the router of next hop.
- When the LSR meets the Labeled packet, it reads the label value of the next packet, by using the value of next label as a guide; the switch checks Forwarding Information Base (FIB) of sending Label to determine the outer label. The value of next label switches with the value of outer label and replaces the packet using suitable port towards next hop.

- The packets send through MPLS network in this way hop by hop until it reaches the router of outer label, the LER searches the next label in FIB and determines that there is no outer label, at this time the LER removes the label and sends packets as traditional IP packets [34].

CHAPTER 3

MPLS BASED TRAFFIC ENGINEERING ARCHITECTURE

3.1 Overview

This chapter is described as the basics of the properties of MPLS that can be used for traffic engineering. The main property of MPLS is that makes it useful for traffic engineering is its possibility to compute a path from source to destination that is subject to a set of constraints, and forward traffic along this path. Forwarding traffic along such a path is not possible even with the best effort of IP routing, since the IP forwarding decision is made independently at each hop, and is based solely on the packet's IP destination address. MPLS can easily achieve this forwarding traffic along an arbitrary path. The explicit routing capabilities of MPLS allow the creator of the LSP to do the path computation, establish MPLS forwarding state along the path, and map packets into that LSP. Once a packet is mapped onto an LSP, forwarding decisions are based on the label, and none of the intermediate hops can make any independent forwarding decisions based on the packet's IP destination. This property of MPLS can be used to achieve performance objectives such as optimization of network resources and placement of traffic on particular links [28].

The view that internet will convert to multiple service like gathering audio, video and data connections. Traffic of internet is advancing in shape of geometric progression according to the ever growing traffic. Huge internet service provides response to challenges that result from internet growth and development, for that three integrated initiatives are applied:

- Expandable internet structure.
- Expand of possibility.
- Traffic engineering.

Traffic engineering is a familiar subject in connection industry. Traffic engineering uses the network. Moreover, today most of the network is based on Packet. So that, they use connective communication for the sake of repetition and easiness. If there is a mistake, it leads to the use of IP routing devices making new paths in the network. It is limited by many elements, one of them is the parameters of the link connection, which has to be treated for the effects on traffic movement. MPLS secures to solve the case and is needed more to balance the movement in the network by building LSP and to allow for the users to practice the traffic inside this path [16].

3.2 Understanding Traffic Engineering

Before understanding modality of MPLS use for traffic engineering; we have to explain traffic engineering, there are two types of engineering which are network engineering and traffic engineering:

- Network Engineering: it is operating of the network to fit the traffic. We do this by predicting about the traffic flow modality across the network. After that, we ask for circuits and suitable network devices like routers, exchangers. Traffic engineering is carried out rather relatively long time like weeks, months, years due to the adjustment of the new circuit or devices which requires long time.
- Traffic Engineering: it is operating of traffic to fit the network. Traffic engineering is a process of network paths selection so as to balance the traffic approaches throughout various rooting operations. It could be said that it is the controlling process by traffic flow across physical network to gain the ideal using conditions for sources. When it is applied correctly, the traffic engineering helps the carrier to use all sources efficiently [35].

When routing throughout uses old IGP algorithms that may create circuits which lead to non-balanced in usage, gradually making some circuits become crowded while the others still remain empty. IGP parameters make it able to secure routing of requested traffic as it becomes difficult to manage when networks are huge and having a lot of additional routing [9].

Traffic engineering with MPLS attempts to take the best among traffic engineering techniques with routing contact such as ones located in ATM, Permanent Virtual Circuit (PVC) and merges it with IP routing.

3.3 Traffic Engineering before MPLS

How traffic engineering was before MPLS ?

Let us take a look at two different techniques used for achieving IP and ATM traffic engineering. IP traffic engineering is the most common but very poor one. The essential method to control the path that is taken by IP across network is cost alteration on specific link. IP traffic engineering is still valid and a lot of huge networks are using it successfully, but IP traffic engineering still is suffering from some problems that cannot be solved. In contrast, ATM enables us to use PVC's across network from traffic source to destination. This means that we have more clear control on the traffic flow on the network. Some of huge internet service providers around the world have used ATM to lead the traffic around their networks. This is achieved by throughout building of Mesh network from ATM PVC's among set of routers. One of related problems with this method is that Mesh network completely leads to this $O(N^2)$ which is the main problem. This is disproportionate and cause to create more significant problems in some huge networks.

IP routers is done by routing building on the intended destination when sending traffic , then this helps in indicating that routers used shortest path algorithm, in order to calculate the shortest distance between it and destination. This distance can be the number of hops to specific protocols such as RIP or the total calculation, the total links calculation that adds on a path from network device to the destination. It does not matter if there are any other additional paths in the network. In case of existing traffic prepared for sending, always traffic flows across shortest path or lesser cost of link between any nodes; according to OSPF algorithm even the traffic path can be kept, even if the path is crowded and injected, the traffic is sent across the shortest path. This causes loss of some of the data packets [16].

3.4 $O(N^2)$ Problem

$O(N^2)$ is a method to express specific expansions mechanisms, in this case, the number of nodes (N) increased that influence the node failing mostly increased by square node number $O(N^2)$, so when router fails, the effect on the network is increased by $O(N^3)$ through increase in N. To understand it better one needs to comprehend where the $O(N^2)$ and $O(N^3)$ come from. In case of $O(N^2)$ when link fail in Mesh network structure, that means it comes from the dual nodes at the end of that link which tells the entire neighbor nodes about failing of link and in turn, each of these nodes tell their neighbors.

For $O(N^3)$ when node fails, all of the neighbor nodes, will tell the related nodes that a node failed. Thus, the nodes which receive this information will forward or send it to its neighbor.

3.5 Fish Problem

In order see this problem more realistically, it can be understood from a classical example of traffic engineering in Figure 8. In this Figure there are paths which go from R_2 to R_6.

$R_2 \rightarrow R_5 \rightarrow R_6$

$R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_6$

Due to the fact that all the links have the same cost (15), with natural transmission, according to the destination, the entire packets come from R_1 and R_6 from the same outlet of R_2 towards R_5 because of the cost of upper path, as it is lesser than lower path. This leads us to various problems. This is shown in Figure 10.

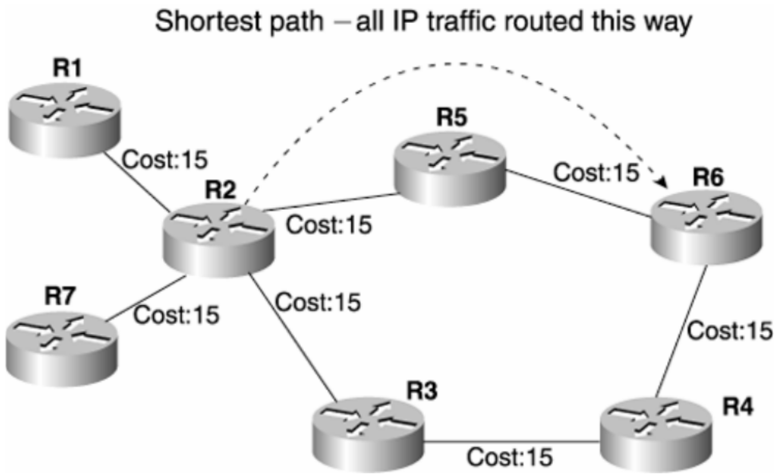


Figure 10 Fish Problem [14]

This problem seems very difficult with transmission according to the destination. If you make a cost of the longest path (R_2-R_3-R_4-R_6) lower than the cost of the shortest path, the entire traffic goes down across the shortest path. Therefore that problem does not get solved but is transferred. In Figure 10, one is able to change links cost, where the shortest and longest path has the same cost that eases the problem. This solution is fitted with tiny network only, like he networks that exist in the Figure 10, we are going to get poor or bad bandwidth.

Figure 11 shows the routers R_3, R_4, R_5 where ATM switches or exchanges the network which makes the problem easy to solve with ATM network. There are only two built of PVC's from $R_2$to R_6 and those have equal cost. This problem is solved due to R_2 which has two paths to R_6 and probably uses these two paths to carry different and rational data. The accuracy of the load sharing mechanism can be changed but generally Cisco Express Forwarding (CEF) with balanced load which is built on every source that uses both paths equally. Building with two equal cost paths across network is more flexible and feasible solution as it is better than alteration links cost in ATM network due to the fact that there is no other device connected with network which might be influenced by changing parameters. This is essential in making ATM engineering traffic more effective than IP traffic engineering and that is highlighted in Figure 11.

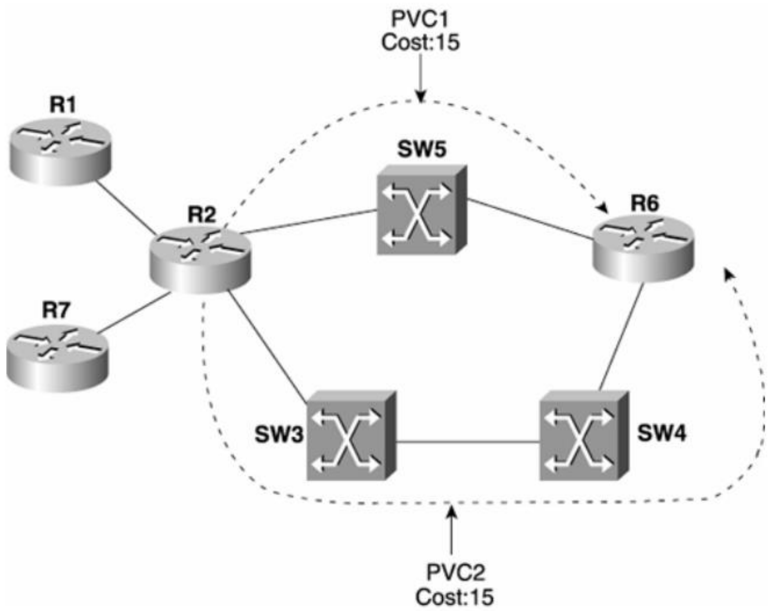


Figure 11 Fish Problem in ATM [14]

3.6 Traffic Engineering with MPLS (MPLS-TE)

MPLS-TE emerges between traffic engineering of ATM properties and flexibility performance of IP class service. MPLS-TE allows us to build label switching paths across network which send traffic down a simulation to (ATM VC's), MPLS-TE LSP that allows to the end traffic engineering header tunnel controlling path which is taken through traffic to a specific destination. This method is more flexible than traffic sending depending on address destination only. In contrast, with ATM VC's, the nature of MPLS-TE is to avoid the problem following $O(N^2)$ and $O(N^3)$ that happens in ATM and other layers models. Instead of neighbors formation across TE Traffic Engineering Paths, MPLS uses a mechanism called auto route to build routing table which utilizes MPLS-TE LSP's without building full network of routing neighbors. In similarity to ATM, MPLS-TE by reserved bandwidth on network when building LSP's, MPLS reserved enough networks in process of finding paths across network in contrast to ATM that cannot achieve reservation in sending level but instead reservation is accomplished in controlling level only. MPLS-TE enables operator to build TE tunnel/LSP along the path to achieve bandwidth requirements not necessary for the short one. In addition, MPLS-TE applies traffic on the new path. Thus, links are used with only available bandwidth.

3.7 Solving of Fish Problem through Using MPLS-TE

MPLTS-TE LSP's can be placed on a random path similar to MPLS-TE in devices like in fish problem shown in Figure 12.

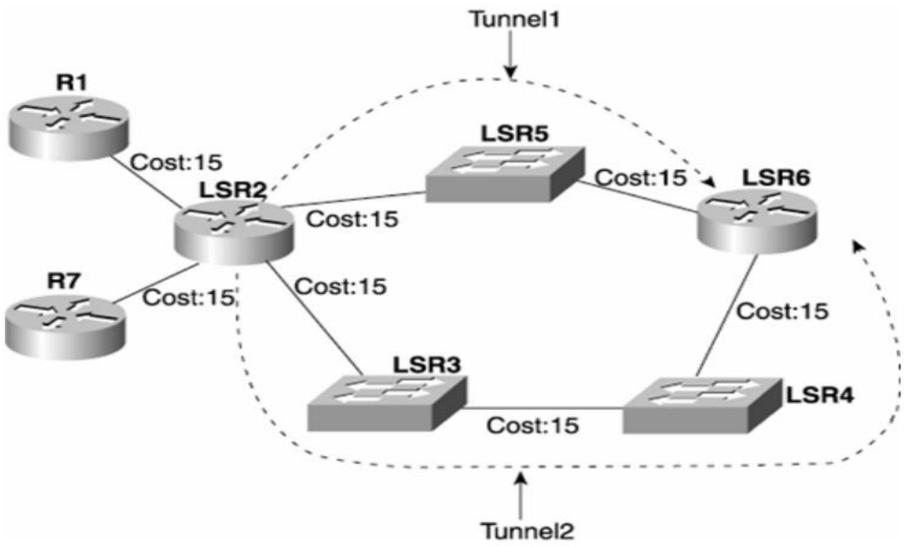


Figure 12 Solving of Fish Problem with LSR's [14]

The three essential differences between ATM and MPLS-TE are given as follows:

- MPLS-TE send packets while ATM uses cells, it can merge between MPLS-TE and integration of MPLS/ATM but this matter is not applied yet.
- ATM requires full network of neighbor's routers while MPLS TE does not.
- In ATM internal network chart is invisible to the existing routers on the network edge. In MPLS, IP routing protocols announce topology chart as MPLS-TE is built on network [34].

3.8 Using of MPLS in Practical Applications

There are three essential applications for MPLS-TE in our life:

- Improvement of network use.
- Processing of unexpected traffic jam and congestion.
- Processing of link or node failure.

Sometimes, the enhancement of network uses named strategic method to propagate MPLS, in other words it is called the achievement of overall association network. The other correct method to propagate MPLS is processing of unexpected congestion which is known by technical method. This method includes sending traffic by IGP and builds TE-LSP's only after congestion discovering. This allows in keeping the whole or the entire network. The third reason of using of MPLS-TE is, rapid recovery of link or node falling. MPLS-TE has a component called fast reroute recover which allows to enforce decreasing of packet loses or waste in case of link or node failing on the network, we can use MPLS-TE in order to FRR only and to prevent MPLS-TE driving traffic on the various paths which are not selected by IGP. Routing with Resource Reservation (RRR) create a specific path or more, with securing bandwidth for each link in the network, keeping into consideration the policy constraints that are related with links and physical sending resources and network topologic chart. This helps in sending chart build on routed packets according to the available resources and traffic classification policy. The pointing protocol that is used in RRR is RSVP. RSVP creates LSP tunnels across MPLS network automatically. RSVP chooses the engineered physical path according to the tunnel resources requirements and available bandwidth in the network. Tunnel can decrease or increase resource reservations automatically based on the variable conditions of network. MPLS paths can determine throughout the hop consequence, which path to use. MPLS flow messages across path and tag sending information regarding every LSR necessary along the way. The network operator can limit policy for any packets that uses specific path. In other words, network operator can classify packets or applications that use traffic engineered routing [14].

CHAPTER 4

PROTECTION AND RECOVERY

4.1 Overview

This chapter describes how the recovery can be performed in a network. Common network failures are discussed in this chapter in addition to ways to detect failures, also some current solutions for how network recovery and protection can be performed and presented by MPLS. If a failure occurs in a network, a network recovery is achieved by moving traffic from the failed part of the network to another section of the network. It is important to perform the network recovery operation as fast as possible in order to prevent many packets from getting dropped at the failure point. If this is achieved quickly, the failure can go unnoticeable (resilient). One of the largest motivations for MPLS recovery is the ability to ensure recovery from a link or node failure with minimal disruption to the data traffic. Recovery techniques can be used in both Circuit Switched and Packet switched networks. When a link or node in a network fails, traffic that is using the failed component must change the used path to reach the destination. The path that the traffic is using before the failure is called the primary path or the working path and the new path is called the backup path.

Often recovery techniques consist of four steps. First, the network must be able to detect the failure. Second, nodes that detect the failure must notify certain nodes in the network of the failure. The nodes that are notified of the failure depend on which recovery technique is used. Third is, a backup path must be computed. The Fourth, instead of sending traffic on the primary path a node called Path Switching Node must send traffic on the backup path instead. This step is called switchover and it completes the Repair of the network

After a failure, we consider a unicast communication as illustrated in Figure 13.

Figure 13 MPLS with no Protection [28]

When a link fails on the path between the sender and the receiver, users experience service disruption until these four steps are not completed. The length of the service disruption is the time between the last bits sent before the failure occurred or is received or identified, and the instance when the first bit of data that uses the backup path arrives at the receiver. The total time of service disruption can be calculated according to the following formula:

Service Disruption = Time to detect failure + Time to notify + Time to compute backup + Time to switchover [28].

In a normal IP network, the best path is where the calculation happens (on-demand) when a failure is detected. It can take several seconds to recalculate the best paths and to push those changes to the router hardware. Moreover, a transient routing loop may also occur, as every router in the networks learns about the topology change. With MPLS Fast Reroute, the best next path calculation happens before the failure actually occurs. The backup paths are pre-programmed into the router forwarding information base, FIB awaiting activation, which can happen in milliseconds following failure detection, because the entire path is set within the LSP, routing loops cannot occur during convergence, even if the path is briefly made sub optimal.

4.2 Types of Errors in Networks

Different types of errors in networks happen when any of the resources within a network might fail. The traditional error in a network is a link failure caused by a link getting cut or unplugged by a mistake. The human factor can very often be the cause of failure. Failures may also arise due to the aging process of equipment or its components or other hardware or software failures in router equipment.

4.3 Failure Detection

If a failure occurs in a network, there must be a method to detect the failure has occurred so that the recovery operation can start. Failure detection depends on the type of failure and may happen because of the failing node, at a node adjacent to the failure or at a configured point of repair in the network. Failure detection can involve multiple layer mechanisms and in this section an overview of failure detection techniques is presented [36].

4.3.1 Link Management Protocols (LMP)

LMP are used by a node in a network to monitor individual connections. The end device in a network sends status enquiry message to the network node at every polling interval. The node responds with a status message that verifies the link integrity. If the node does not respond, the downstream node can communicate upstream until the fault is isolated, and then report this to a local management component [37].

4.3.2 IGP hellos

IGP use setup routing tables which run “hello message” exchanges to check if a link is active. If a node does not receive a pre-set number of hello messages from its adjacent neighbors, then a failure is detected.

4.3.3 IGP Topology Updates

An IGP protocol sends periodically topology updated messages, if the topology has changed or a failure has occurred then this can be detected.

4.3.4 Signaling Hellos and Keep Alive

Many signaling protocols include "hello message" processing where adjacent nodes, poll each other periodically to check if a link between them is active. Signaling protocols can also use “keep alive” messages, as example RSVP uses this method to keep a path reserved in a network (soft state). Such soft state mechanisms are implemented by the use of timers and these timers are often set with high tolerance to limit the signaling traffic.

4.3.5 Hardware Manager

Some devices have software and hardware that monitor the state of the controller cards, line cards and the software running on them. If a failure occurs in the device, then it can become aware that it is not working correctly.

4.3.6 Loss of Light (LOL)

On optical links a, failure like in the case of cutting fiber happens is detected at the downstream node of the fault through loss of light. The upstream node is unaware of the failure on the link; it can inform the failure through a link management protocol.

4.3.7 Loss of Electric Connectivity

Failure of an electrical link (for example Ethernet cables) is detected by the line card and reported to the device driver. The failure is detected when the line card detects that there is no electrical connectivity on the link. Failure on an electrical link is detected at both the upstream and downstream ends of a link because electrical links are bidirectional.

4.3.8 Signaling Error Notification:

If a signaling protocol fails to set-up a path, upstream nodes notifies by an error message sent by the node that has failed to set up the path. This failure message can include crank back information whereby set-up failure information of a path set-up is returned to allow new set-up attempts to be made, avoiding the blocked resources [38].

4.4 Link Protection/ Next-Hop Backup

As it clear from the name, it is a link protection that includes protection in case of link failure. In these days, links become more authentic but statistics still reveal or show that most of unmanaged errors in network occur due to links errors. So the protection of links errors is necessary in any network. Link protection is done through FRR which is an advanced and modern technique. Node should prepare in order to protect links, so a spare channel is made to specialize around the node that requires a protection to the next hop. This is explained in Figure 14.

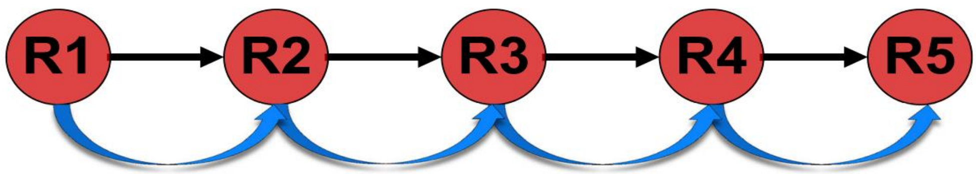


Figure 14 MPLS Link Protection [28]

4.5 Node Protection/Next-Next-Hop Backup

In node protection, usually, spare channel is prepared to the next node hop and failure is discovered based on lose of carrier or alarms of Synchronous Optical Network (SONET). In node protection, the described mechanism is similar to link protection except that the spare channel which always is prepared for the node that is after the next hop. When fail is discovered by message leaving for example Hello, Then Point of Local Repair (PLR) point of local repair node reroute traffic to inside spare channel, then to the next hop Next Next Hop (NNHOP). MPLS packets which appear at end of NNHOP may not have the correct tags, in order to merge point to carry the traffic beyond to that or further. In purpose to avoid traffic rejection at the end of spare channel, spare channel head exchanges the main channel tag with expected tag from merge point and assume spare channel tag, this confirms that MPLS travelling packets from spare channel carry the correct tags, thus the exchange is done to the correct destinations. This is shown by an example in Figure 15.

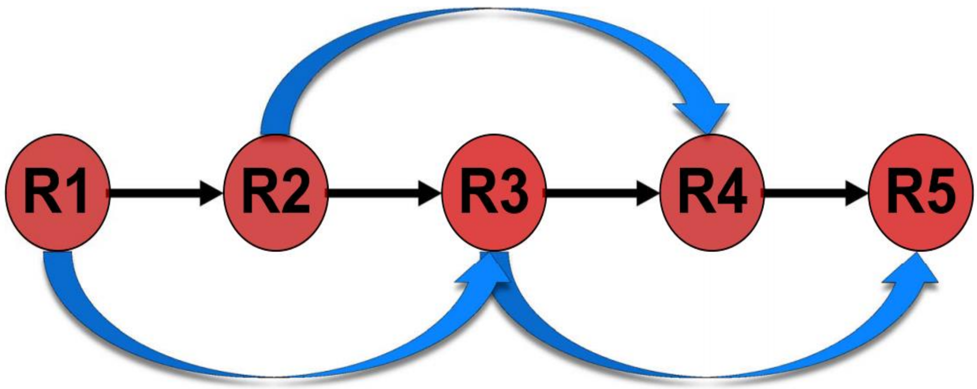


Figure 15 MPLS Node Protection [28]

4.6 Path Protection

The last pattern of protection patterns is called path protection which is the ability to protect (end-to-end) path, more throughout specializing or limiting spare channel done previously. This is called End-to-End protection, so if any failures happen along the path like node failure, link failure, the end of header reroutes the traffic inside spare path as shown in Figure 16.

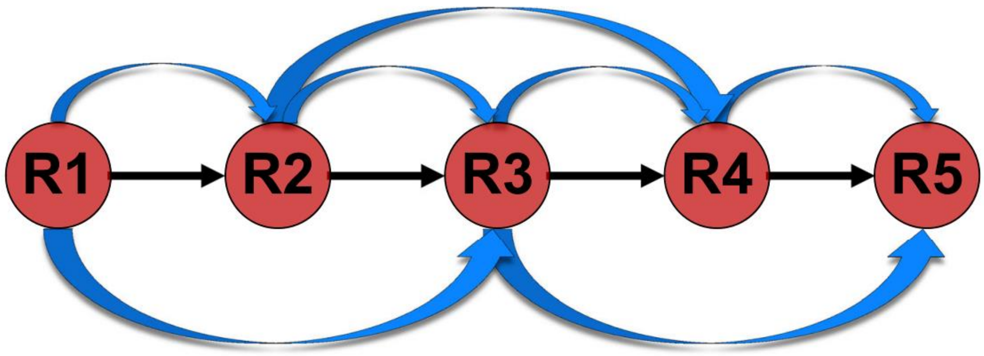


Figure 16 MPLS Link and Node Protection [28]

In the same Figure 16, the notification about this failure should reached to the end of head TE channel to redirect the traffic. The advantage of path protection is, LSP spare channel protect main LSP from the all error types (link and node errors) along the path except the errors that might happen at the entrance of LER and at the exit of LER or the related errors that may influence on the main and spare path at the same time [39].

CHAPTER 5

BACKGROUND AND LITERATURE REVIEW

5.1 Background

According to the investigations of real time and multimedia features of the network services, the necessity for a foundation of a new protocol is quite obvious like the combination between protocols on broadband networks such as FR, ATM and IP protocol. This protocol does not reduce the speed of broadband network and also does not change the existing entire architecture of IP network. MPLS protocol is researched and developed by encapsulation a small tag to IP package on MPLS domain. MPLS is carried out by encapsulating a tiny header to the package of IP on MPLS domain; therefore there no big alteration is clear in the operations of MPLS. Each header has a label which can be utilized for switching method to decrease the time delay package on every router and keep the proper broadband network velocity. The MPLS use label for switching technique [5], [40] and [41].

5.2 Literature Review

This part is focused on the presentation of scientific references that specify the basic features of routing algorithm models and routing algorithms on MPLS. There are many studies in this field; the following is a summary of each study in terms of its goals, importance and the conclusions.

[42], This presents a study of organized algorithms of advanced research routing which takes MPLS network benefits to range routing algorithms, traffic engineering and load balancing. There are several advance routing algorithms on MPLS which has been investigated before too. Advanced routing algorithm is classified into two kinds. QoS based on routing algorithm which supports constriction routing and QoS services Traffic based routing which is the other kind which supports discovering solution or clarification adequate for several LSP demands and decreases blocking in future. Advanced routing algorithms are very hard for applying on router because each router has a specific memory, CPU velocity and roles of operating system. Therefore, advanced routing algorithms are just applied on server with centralized model. Some modern projects regarding the algorithms work and research with advanced routing.

With the shortest path algorithms there is one main drawback which becomes evident when an arc is good for using with many source destination pairs; some source-destination pairs choose this arc for their path and can induce the collision on this arc.

Traffic based routing algorithm not only optimize network resource for present time, but also for future demands. Traffic based routing algorithm predicts the links that can be blocked if we route many traffics through them and will reduce routing traffic going through these links.

Shortest path algorithms consist of two types: first one is based on the information of current network, it computes and chooses the links that minimize the ability of blocking network for future demands. Second one is based on statistical information measured by server or router that gives approximate information about the demands in future. We named this statistical information "profile". After having profiles we solve linear programming to find optimal solution satisfying all profiles, i.e., to find optimal solution for the future.

Following, are some traffic-based routing algorithms that support basic concept and suggest general ideals for traffic-based routing algorithms. Like: Minimum Interference Routing Algorithm (MIRA) [43], dynamic on line routing algorithm (DORA) [44] and depending on the information of profile like: profile based routing (PBR) [45].

In [43], the researcher finds an approximate solution to solve the NP problem that can be described by Minimum Interference Routing Algorithm. (MIRA) algorithm from the residual bandwidth information of all arcs, we can compute the max flow of all ingress-egress pairs. With each ingress egress pair, we find min-cut sets; the arcs that belong to these sets are called critical links. Critical links limit the max flow of the ingress egress traffic pairs that go through them. So, MIRA algorithm goal is to maximize to avoid the routing through critical links.

A study of Dynamic Online Routing Algorithm (DORA) is presented in [44], DORA is different from MIRA because MIRA is based on max flow, while DORA depends on the number of paths going through a link (consider all ingress-egress pairs). The symbol (n) represents the number of paths (of all ingress-egress pairs) which are going through an arc, and the value of n is proportional to the number of collisions; the larger the value of n, the larger ability to collide on this arc in the future, therefore the DORA choose n to represent the weight of each arc and run the shortest path algorithm to find the shortest path that has the minimum weight value. Furthermore, by combining n with another optimal constrained metric (example m), DORA algorithm can build weight value by the formulation: $w = an' + (l - a) m'$.

In [45], the researcher uses a server or router to measure the traffic going through the network, by using the traffic flow profiles which exited previously. Each profile includes Bi, which denotes all bandwidth requirement of aggregated LSP setup that alternate the requests between source (si) and destination (di) that belongs to a class and is mapped according to class ID. In order to achieve high ration of satisfying all requests in the future, we have to do the following;

- Solve simultaneous equations to find the traffic caused by each ingress-egress pair distributed on each link.
- Determine its class and use the results of first step for each class to initialize network topology, then use shortest path algorithm to find optimal solution

The main objective is not for all profiles to be successfully achieved, but for all PBR to maximize the number of satisfied LSP demands so the goal of PBR algorithm minimizes the traffic routing.

In [46], the explicit routing algorithms for Internet traffic engineering are introduced. Explicit routing is accepted as a better solution, with the ability to improve network utilization more efficiently than the current destination based routing, and the multi-protocol label switching MPLS standard that made the explicit routes implementable. Internet Server Provide (ISP) now has fine granularity control over the traffic distribution across their backbones by overlaying explicit routes carefully over the physical network. The main traffic engineering problem is setting up explicit routes to meet bandwidth demands between the edge nodes of the network, and at the same time optimizing the network performance.

In [47], the researchers focused on Dual and suggested novel substitute improvements named algorithms of Alternative enhancement for Enhanced Associativity Based Routing (AEABR) and Associativity Tick Averaged ABR (ATAABR), and suggested comparison with Associativity Based Routing (ABR) enlarged Enhanced Associativity Based Routing (EABR) algorithm. It is proven by them, that carrying out is supplied through AEABR with taking care to EABR or ABR rather than the other individual hop relay, choosing algorithms like, minmax path, minimum distance path, nearest node to the source, path according to power threshold and path according to path wastage. The analysis has investigated wastage of bandwidth and message overhead for each algorithm. It has been noticed from the results that the links on the paths assembled throughout AEABR can still be connected for a long time more than EABR. It is explained that ATAABR developed EABR connection at lower levels and needs less algorithm adjustment and calculation time since AEABR is developed by Route reconstructions (RRC) number over connection outage time. Moreover, it also has been referred that ATAABR and AEABR enhance the stability of connection EABR throughout preserving connection outage time at its lowest level since ATAABR needs less adjustment on algorithm and requires shorter calculation time. There has been a transaction between the decrease message overheads and decrease route reconstructions number or reduce outage times.

In [48], this work, aim is to improve a genetic algorithm to solve problem of network routing protocol. The algorithm should discover the shortest path between source and destination nodes. Literally, the problem of routing solves the problem of utilizing methods of search graph to discover the shortest path. The improved genetic algorithm is compared with Dijkstra's algorithm to solve problem of routing. The results confirm the possibility of the suggested genetic algorithm. The performance gained is very close or similar to Dijkstra's algorithm. Genetic algorithms (GAs) are globally searched and optimization techniques modeled from natural selection, genetic and evolution. The GA simulates this process through coding and special operators. A genetic algorithm maintains a population of candidate solutions, where each candidate solution is usually coded as a binary string called a chromosome. A set of chromosomes forms a population, which is evaluated and ranked by fitness evaluation function. The fitness evaluation functions play a critical role in Gas because it provides information about the quality of each candidate. The initial population is usually generated randomly. The evolution from one generation to the next one involves mainly three steps: fitness evaluation, selection and reproduction.

This [49] study investigates the fastest packet transportation in light-loaded wireless networks. It is shown that the end-to-end packet delay depends largely on the locations of the relay nodes that make the packet go forward and there also exists a shortest-delay path theoretically. The researcher proposes a routing algorithm to locate a fast relay path in actual networks to achieve the near-shortest packet delay. In order to identify the fastest path algorithm, we have to first determine the desired locations of the relay nodes from a mathematical model. Then we have to design a routing algorithm to discover this fastest path. The investigation demonstrates the new routing algorithm can successfully transport a packet in the near-shortest time, especially when node density is high.

In [50], the aim of the study is to provide a wider combination of genetic algorithm and ant colony algorithm. The Ant colony algorithm is considered as a modern method of heuristic biological designing that has capability of parallel processing and global searching, but the operation of merging velocity is slow because of the weak pheromone on the advanced path. Genetic algorithm has been included to algorithm Ant colony in every suggested algorithm. The genetic algorithm benefit quite quickly by blending or merging and algorithm's merging velocity of Ant colony is well accelerated. Genetic algorithm alteration mechanism develops Ant colony algorithm which then has the ability to keep away from being tricked in a local optimal. The imitation reflects the new algorithm is active in answering arrangement or distribution lattice planning problem. Genetic algorithm is an adaptive guiding search algorithm which is based on Developmental thoughts of environmental choice and genetic. The primer notion of genetic algorithm is to model to imitate processes in environmental system required for estimation, specifically those one that follow the principles that are established firstly by Charles Darwin for endurance of fittest. So it represents an intelligent exploitation of an accidental quest with a clear search for space to answer the problem. Genetic algorithm is a random search technique which depends on the manners of estimation. A combinational algorithm is drawn from the qualities of genetic algorithm and algorithm of ant colony. On the norms of ant colony algorithm movement is that genetic algorithm is added to ant colony algorithms every generation in the combinational algorithm. Ant colony algorithm solutions complete at each generation which is taken as a primary population of genetic algorithm, and the universal ideal solution for ant colony algorithm similarly is linked to the primary population of genetic algorithm. Therefore a set of fresh solutions are formed throughout several repeated estimation of genetic algorithm. Ant colony universal ideal solution is selected from the ideal solution of genetic algorithm and the universal solution of ant colony algorithm. The pheromone has been modernized. In the genetic algorithm alteration mechanism, ant colony algorithm can be evaded by being trapped in a local ideal.

In [51], the researcher proposed a new distributed algorithm for the dynamic computation of the shortest paths in a computer network. According to this algorithm, each node maintains the lengths of the shortest path at each network destination and feasibility vector. Update messages from a node are sent only to its neighbors; each such message contains one or more entries, and each entry specifies the length of the selected path to a network destination, and also whether the node requires inter nodal coordination. The new algorithm extends the Jaffe-Moss routing algorithm by allowing nodes to choose a new successor to destinations with no need for inter nodal coordination if the new successors are considered to be, at most at the same distance as the current successors. The proposed algorithm can be extended to support distributed source routing (in which the source node specifies the complete path to the destination) by requiring that both update messages and both distance and routing tables include the penultimate hop in the shortest paths to the destinations.

[52] The aim of this study is to propose a newly modified version of MENTOR (Mesh Network Topological Optimization and Routing) called Enhanced MENTOR, or E-MENTOR, which is able to assign traffic with the Equal Cost Multi-Path (ECMP) routing. MENTOR is an efficient heuristic design algorithm network that assigns traffic flow while selecting links which are to be installed. MENTOR is suitable for designing networks categorized as virtual circuit packet switching such as FR, ATM and MPLS networks. However, MENTOR cannot be directly applied to datagram packet switching networks such as the ones which are completely IP router network. This is because the traffic flows which are determined by the original MENTOR are not always the shortest path routing based on IP link weight assignment. To solve this problem, Cahn proposed a modified version of MENTOR called MENTOR-II in which appropriate link weights are assigned to the installed links such that the traffic route always stays on the path with minimum distance. However, it should be noted that the traffic flows assigned by MENTOR-II are limited to a single path routing. Still there are some disadvantages of E-MENTOR algorithm and which are:

The routing cost (Delay) is averagely higher than that of a network designed with MENTOR algorithm while the routing cost of a network designed with MENTOR-II algorithm is averagely a bit lesser than that of a network designed with just MENTOR. The reliability is averagely the same, i.e., EMENTOR algorithm is a bit less reliable than MENTOR algorithm while MENTOR-II algorithm is a bit more reliable than MENTOR algorithm.

Yet there is an advantage of E-MENTOR algorithm as well and that is: The average installation cost is lower than that of a network designed with MENTOR-I while the installation cost of a network designed with MENTOR-II algorithm is higher than that of a network designed with just the MENTOR.

CHAPTER 6

METHODOLOGY

6.1 Overview

This chapter presents the new proposed cognitive methods and the performance of these methods that produced good results; the improvements for several routing algorithms such as Ant-Colony algorithm, fastest path algorithm and shortest path algorithm are also shown in this section. Finally these routing algorithms have been compared in the MPLS network and it is observed according to the results acquired from the simulation part, by using these novel methods, real-time video and voice packet transmission is achieved. The system throughput per node is improved, and the data packet loss rate is minimized, the delay time and the packet loss rate are also very effective. (The loss rate, delay count, number of transmitted packets per second and average hop count decides the throughput). Effects of ant colony routing algorithms, fastest path and shortest path routing algorithms on throughput improvement methods are investigated. The simulation results demonstrate the advantages of integrating the recovery methods.

6.2 Analyzing and Designing the Program

This part of the chapter provides a description of the simulation that starts with exploring overall MPLS network details and representing the functions. As well as defining the functions that are related to the MPLS networks. Moreover, exploring the previous methods of MPLS is introduced in the literature part. Also, the research has defined the required parameters to implement all functions in MATLAB program in order to be ready to run the simulation. Parameters are explained and illustrated with examples of all the nodes generating packets and all the node transfer packets to random nodes. The simulation knows of the number of packets transmitted or lost and generated. Then, the designing of the MPLS in MATLAB program and applying of the three routing algorithms and getting the simulation results from the evaluated MPLS system as well as comparing of the results for throughput with those taken from exploring the methods. Another essential point at the time of confirming results (which leads to the implementing of the design of recovery mechanism of the MPLS) of what the next step, is confirming the results of recovery method and that one is which is evaluated too. Finally, comparison operation is done between taken and proposed results and the implemented novelty results for applying routing algorithms in the best of the recovery methods to improve its performance along showing of the improvement of the proposed method which is done graphically.

6.3 Flow Chart

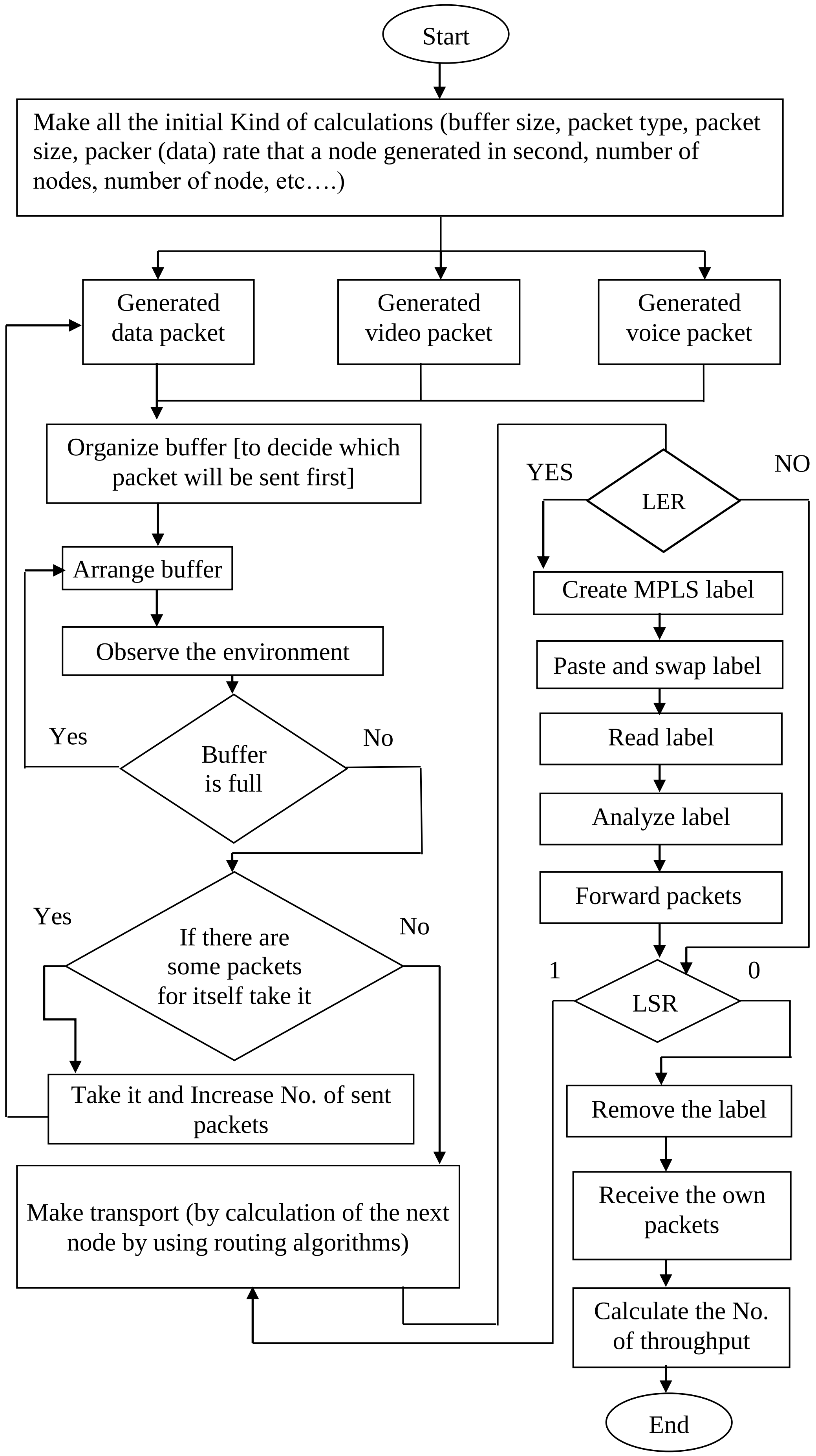


Figure 17 The Overall Algorithm Used by Each Node in the Simulation

6.4 Relational Mapping

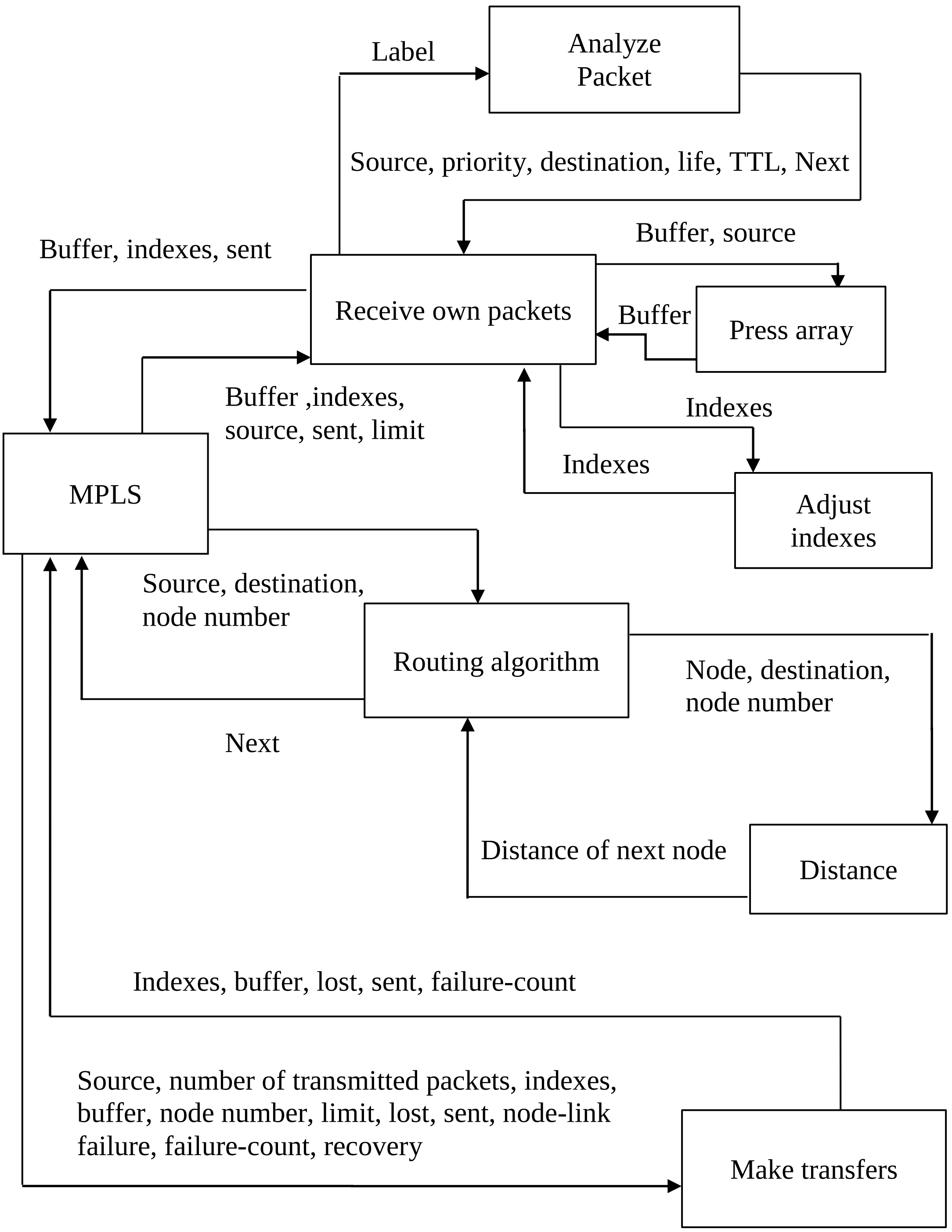


Figure 18 Diagram of Relation Between All Functions

6.5 Routing Algorithm Functions Details

This work has studied the effects of ant colony algorithm, fastest path algorithm and shortest path routing algorithms on the output enhancement of these novel methods. The supply of MPLS network has been utilized and technique of routing algorithm determination has been carried out to the system simultaneously for and in same circumstances and reasons and they are compared for their effects on system performance as well. The effects of algorithms on the output results improvement of these novel methods are also investigated. The analysis results could be demonstrates in different modeling diagrams and which show the basics of each routing algorithm used in the simulation.

6.5.1 Ant Colony Algorithm Explanation

Algorithm of ant colony had been motivated by the actual ant colony's manner. It is a fresh emulate biotic algorithm. It has been known since ten years based on the observation outcome directly from the environment. In the living or real environment ants are capable to discover the foodstuff from the shelter in closer path without any noticeable reminder. Ant colony algorithm core is used for organizing the pheromone departure by the ant and to discover the ideal path; Ants send this type of pheromone in the pathway and make the other ants observe to specific extent by the even effect of their manner. The more ants pass-through the same path is the added pheromone of going to gather by the succeeding ants who possess more prospect to choose those paths which have additional pheromone; therefore, it is taken as a confident response. Ant algorithms have been effectively utilized to explain several NP difficulties; like TSP, graph coloring, job-shop scheduling and problematic assignment. Nevertheless, it frequently bring two basic difficulties; the first one is the search simply goes into the local finest case of solving the problem; for example, the whole single finding out of a comprehensive unity explanation after the process of searching to identify grade. All of this makes a deadlock happen which cannot be accomplished in an explanation space. It is a probable outcome in the universal optimal and another one is, it requires long time for the converge at the universal optimal level. Answering result equivocates between local optimal answer and universal optimal answer [50]. The diagram of ant colony algorithm function is as shown in Figure 19.

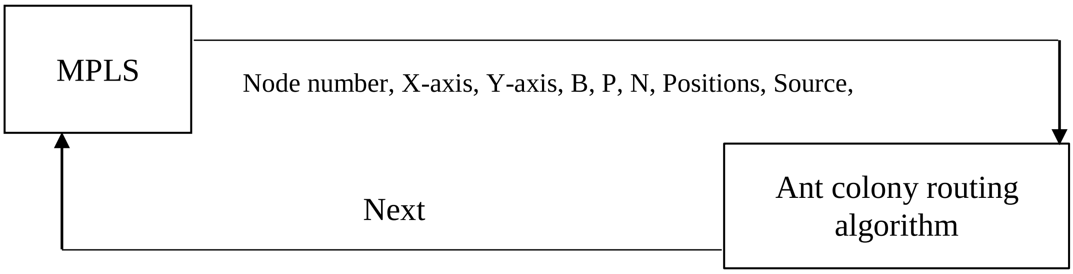


Figure 19 Diagram of Relation Between MPLS and Ant Colony Algorithm Function Details

6.5.2 Fastest Path Algorithm Explanation

In order to identify the fastest path, the first step is determining the desired locations of the relay nodes from a mathematical model. Then we have to design a routing algorithm to discover the fastest path. The investigation demonstrates that this new routing algorithm can successfully transport a packet in the near-shortest time, especially when node density is high. This is the fastest packet transmission algorithm based on the analysis of node information; the packet is transmitted at the fastest speed if the next-hop node is located at a distance of $x*$ from the forwarding node and in the direction towards the destination. In this design a routing algorithm identifies the next-hop relay nodes in order to achieve the fastest packet transmission. The fastest packet transmission algorithm runs on node u_i that forwards a packet to destination u_d. The vectors $u_i$and $u_d$denote the locations of u_i and u_d . The environmental parameters α, B, P and N are constant and previously known. symbol δ which defines the radius of the region in which the next-hop relay node can be searched **.** This new algorithm assumes the knowledge of node locations; it can view as a variant of the geographic routing algorithms. Here we specifically assume the following information which is available to every node.

- The location of the node itself.
- The location of the packet destination.
- The locations of the neighbor nodes that are defined by a neighborhood radius ρ.

The Fastest Packet Transmission Algorithm which runs on every node in the network, identify the next-hop node, a forwarding node u_i which finds out the transmission radius x∗, which at first. X∗ can accurately determine by using the following Equation

$$x * \approx \left(\frac{P}{N\,(e^{\alpha}-1)}\right)^{\frac{1}{\alpha}} \tag{6.1}$$

After that, if x∗ ≥$\|u_i u_d\|$ where $u_d$is the destination node, the packet is sent directly to u_d. In this case, u_i computes the capacity *C* of the wireless link connecting itself and the destination node u_d, and then sends the packet at the computed bit rate *C*. Here the higher rate than *C* will cause incorrect reception at u_d and lower rate than *C* will introduce transmission delay. Otherwise, if it is at x∗<$u_i u_d$, then least one needs more relay node. In this case, $u_i$at first determines the desired location of the next-hop node, then finds the node closest to the desired location, and then finally computes the link capacity to send the packet with correct rate to the identified next-hop node [49]. The diagram of fastest path algorithm function is shown in Figure 20.

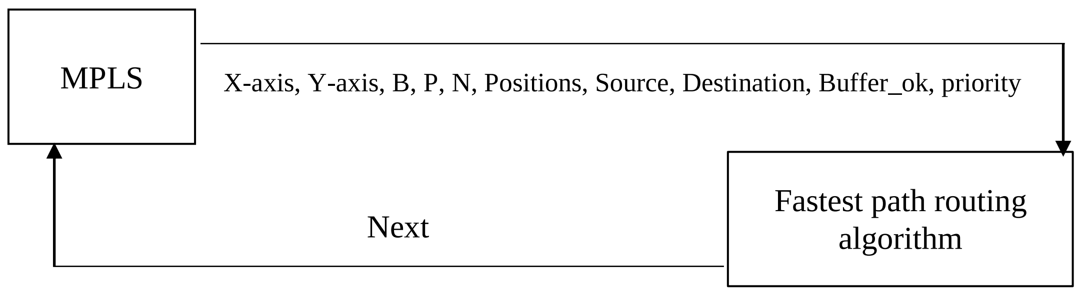


Figure 20 Diagram of Relation Between MPLS and Fastest Path Algorithm Function Details

6.5.3 Shortest Path Algorithm Explanation

IP routing is generally based on the destination address and simple metrics such as hop-count or delay [53]. The shortest-path algorithm is the most widely used routing algorithm in the current time in internet. Therefore, there are a numerous shortest path algorithms available; some of them are applicable r in wireless sensor networks. The Floyd-Warshall's Algorithm is used for computing shortest paths between different nodes in an ordinary graph but this algorithm is not exactly applicable for routing in wireless networks because of the absence of handshaking mode. Generally, shortest path routing algorithms aim to consume the minimum amount of energy. It is important that we understand its performance in the context of traffic engineering. The cost metric is determined by using the Equation below,

$$a^{k}_{ij} = \frac{1}{cij} \tag{6.2}$$

Where cij is the total capacity of the link. A simple variation to the shortest path routing is the minimum hops routing. In this case, we use the number of hops as the metric and always choose the path with the minimum hops [46]. Each node maintains the lengths of the shortest path to each network destination and also to a feasibility vector. Updated messages from a node are sent only to its neighbors; each message contains one or more entries, and each entry specifies the length of the selected path to a network destination [51]. Dijkstra's Algorithm is followed for routing through shortest path. Dijkstra's algorithm discovers the lowest cost path for a given source vertex (node) in the graph between that vertex and also between each of the vertex. It might be utilized to find out the shortest paths costs from lone vertex to distinct destination vertex, breaking out the algorithm throughout once the shortest path to vertex destination has been specified. For example, if the graph vertices distances between couples linked by direct road, this algorithm can be utilize to discover the shortest route between single city and other cities. This type of path which is the shortest path, has first been utilizing spread in protocols of network routing; most notably OSPF (Open Shortest Path First)which is a protocol of dynamic routing. It is a connect case or state routing protocol and it is a part of inner gateway protocols set. OSPF preserves chase of the whole nodes, all network topology and connections with that network [48]. The diagram of the shortest-path algorithm function is shown in Figure 21.

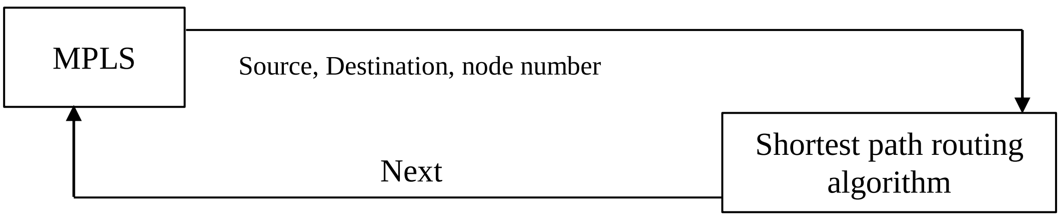


Figure 21 Diagram of Relation Between MPLS and Shortest-Path Algorithm Function Details

CHAPTER 7

EXPERIMENTAL RESULTS AND ANALYSIS

7.1 Overview of Implementation

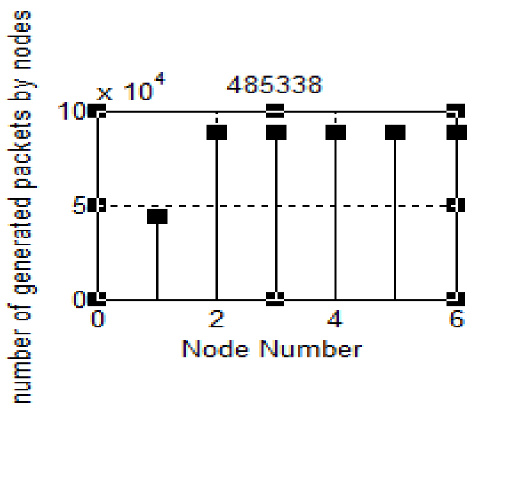
In our work, three algorithms such as Ant colony, fastest path and shortest path are used for the simulation of MPLS technique. These algorithms are suggested due to the simplicity, fast routing and effective transmitting of the packet. The simulation is done by using MATLAB codes. The main function of this simulation is to compare the performance that is achieved by applying routing algorithms in MPLS network.

7.2 Simulation Results

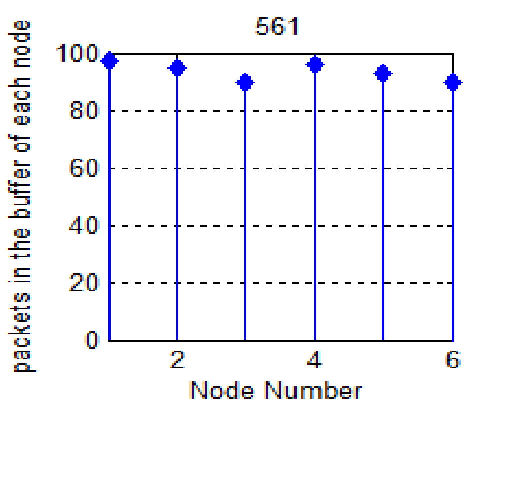
We have continuously transmitted packets using all these algorithms separately for 100000 unit of time (5 *ms*) for long implementation and 250 unit of time (5 *ms*) for short implementation. The results of the simulation for each of the routing algorithms are evaluated by the simulation program as given in Figures (22-25).

7.2.1 Ant Colony Algorithm Results

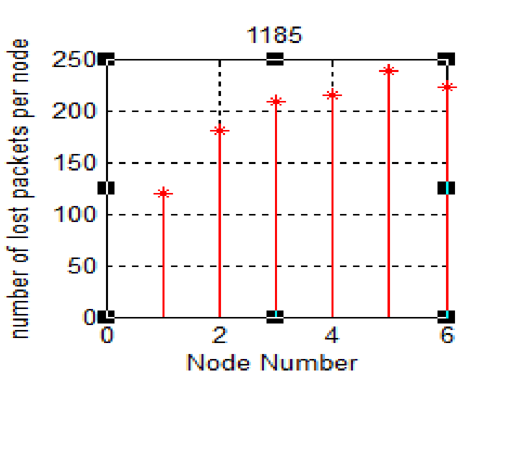
The results show of the ant colony algorithm that the number of generated packets by node is 485338 and packets in the buffer of each node are 561. Also, the nod error or link error is 1185. Moreover, the successfully transmitted packets count nearly to 483592. Additionally, the throughput of this algorithm is 2.96536e+07 for long implementation, as well as the throughput of this algorithm for short implementation is 2.93408e+07. The results of this algorithm are shown in Figure 22.



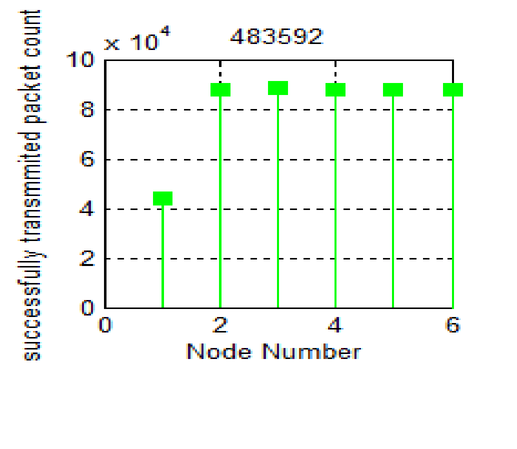
a. number of generated packets by nodes



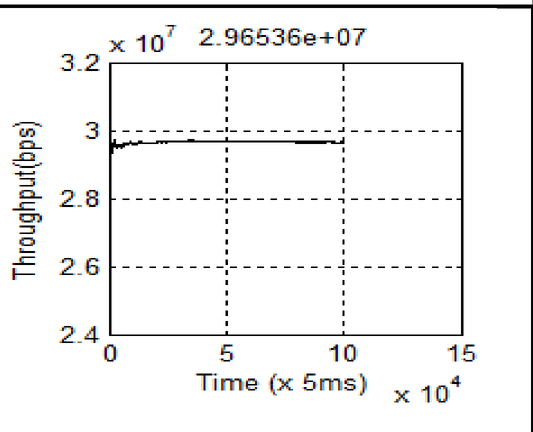
b. packets in the buffer of each node



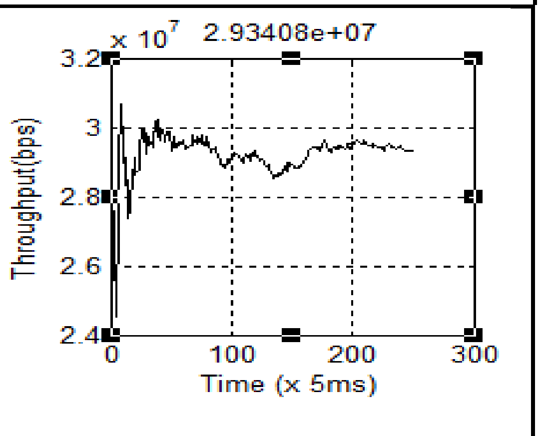
c. number of lost packets per node



d. successfully transmitted packet count



e. throughput for long implementation

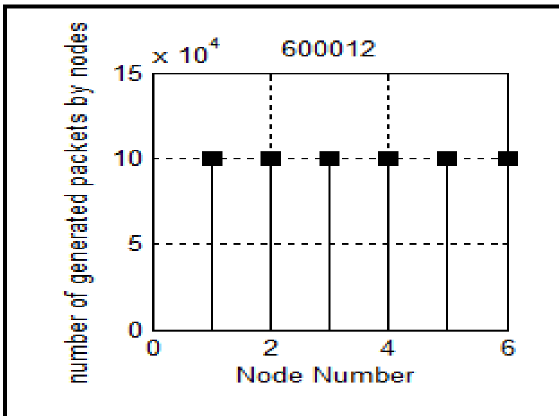


f. throughput for short implementation

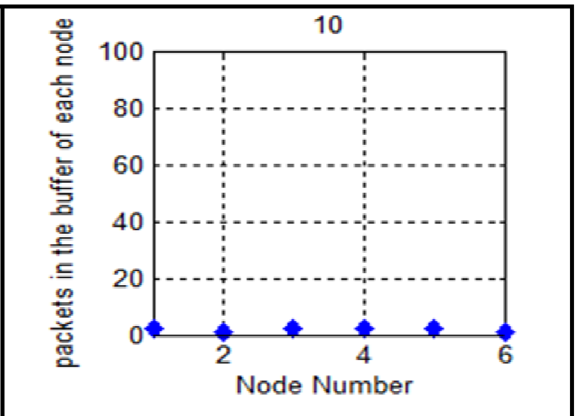
Figure 22 The Results by Use of Ant Colony algorithm

7.2.2 Fastest Path Algorithm Results

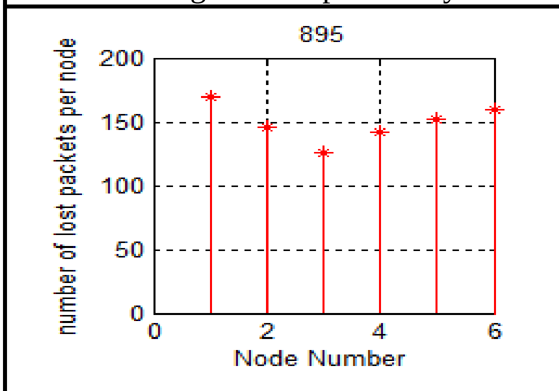
The results show that the number of generated packets by node is 600012 and the packets in the buffer of each node are 10. Also, the nod error or link error is 895. Moreover, successfully transmitted packet count nearly to 599107. Additionally, the throughput of this algorithm is 3.67369e+07 for long implementation, as well as throughput of this algorithm for short implementation is 3.66454e+07. The results of this algorithm are shown in Figure 23.



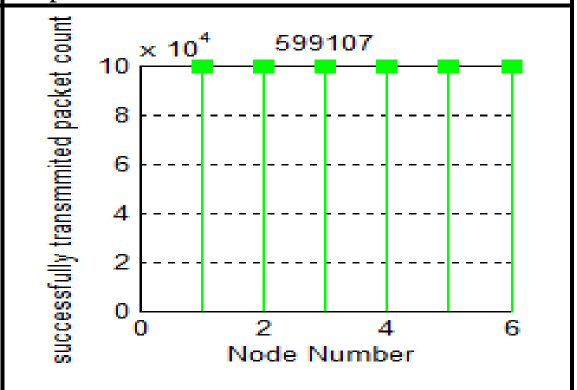
a. number of generated packets by nodes



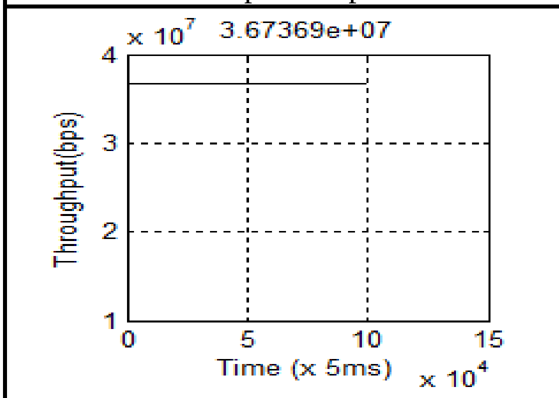
b. packets in the buffer of each node



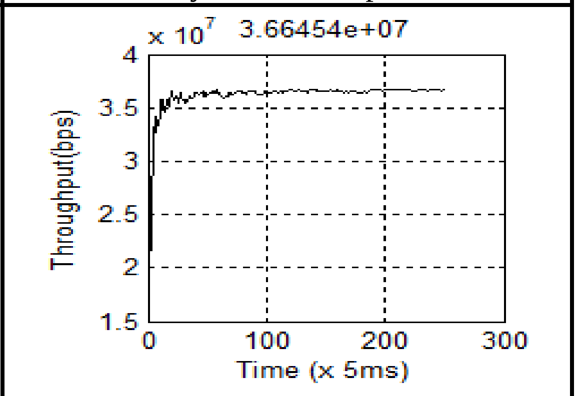
c. number of lost packets per node



d. successfully transmitted packet count



e. throughput for long implementation

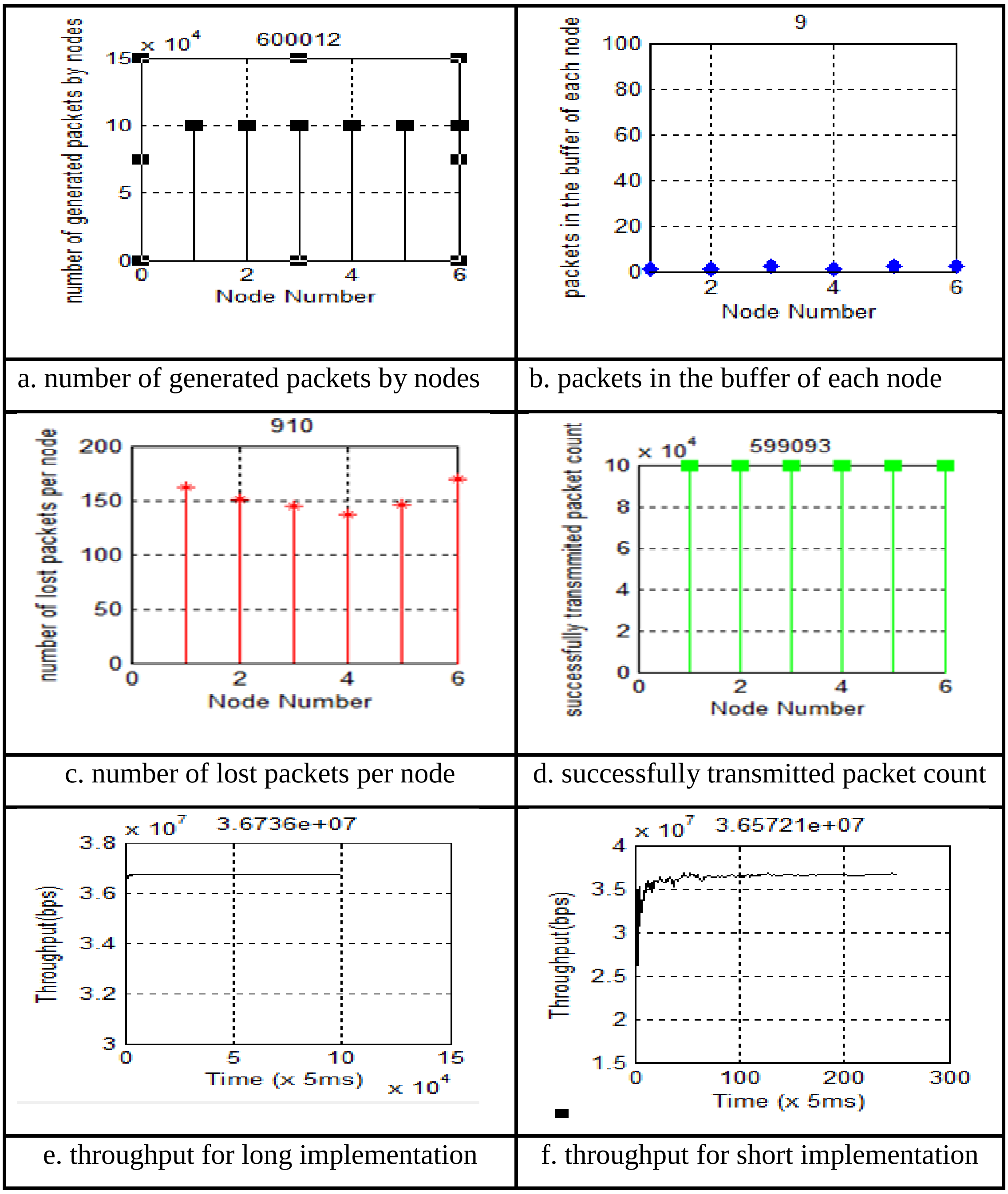


f. throughput for short implementation

Figure 23 The Results by Use of Fastest Path Algorithm

7.2.3 Shortest Path Algorithm Results

The results show that the number of generated packets by node is 600012 and packets in the buffer of each node are 9. Also, the nod error or link error is 910. Moreover, successfully transmitted packet count nearly to 599093. Additionally, the throughput of this algorithm is 3.6736e+07 for long implementation and the throughput of this algorithm for short implementation is 3.65721e+07. The results of this algorithm are shown in Figure 24.

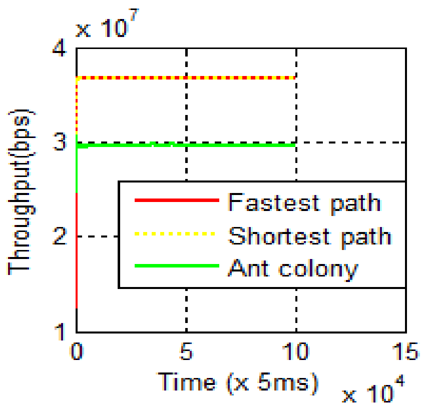


a. number of generated packets by nodes
b. packets in the buffer of each node
c. number of lost packets per node
d. successfully transmitted packet count
e. throughput for long implementation
f. throughput for short implementation

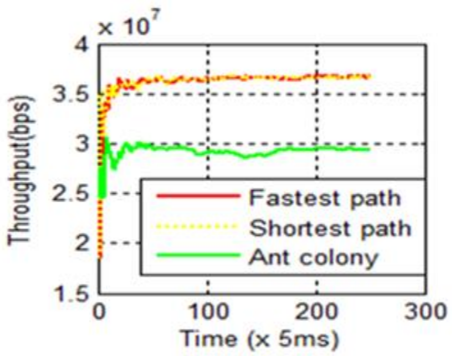
Figure 24 The Results by Use of Shortest Path Algorithm

7.2.4 Comparison of Throughput Results

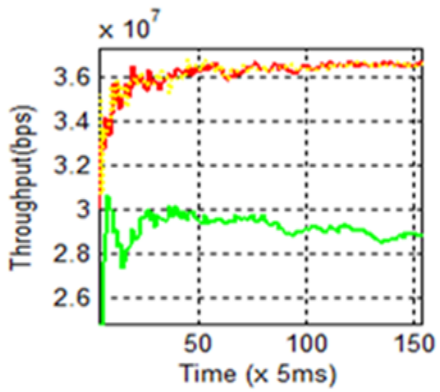
The comparison among the three algorithms is done by comparing the throughput of these algorithms. The comparison includes two run modes, the longtime mode and short time mode. The number of lost packet in the ant colony algorithm is higher than the other two algorithms also the number of transmitted packets of fastest and shortest algorithm is higher than ant colony algorithm. In other words, the ant colony algorithm has the lowest throughput while the shortest path is close to fastest algorithm and both of them are better than the former one. The comparisons of throughput results of these algorithms are shown in Figure 25 that illustrates the differences among them.



a. the throughput of three algorithms for long time implementation



b. The throughput of three algorithms for short time implementation



c. The throughput of three algorithms for short time implementation with zoomed in

Figure 25 The Differences by Use of Three Algorithms

The throughput results of these algorithms are as shown below in Table 3.

Time / Algorithms	30	2e+04	4e+04	6e+04	8e+04	10e+04
Ant colony algorithm	2.923e+07	2.964e+07	2.968e+07	2.967e+07	2.965e+07	2.965e+04
Fastest path algorithm	3.618e+07	3.674e+07	3.674e+07	3.674e+07	3.674e+07	3.674e+07
Shortest path algorithm	3.577e+07	3.673e+07	3.673e+07	3.673e+07	3.673e+07	3.673e+07

Table 3 The Comparisons of Throughput Results of Three Algorithms

The results from Table 3 shows that the fastest algorithm has better throughput and shortest path algorithm is lesser than fastest in it, but the difference between the two is very small, however, the Ant colony algorithm is the worst one among the three algorithms. The throughput is high for shortest path and fastest path algorithms which is due to the low value of number of lost packets and that also is related to the high value of the number of transmitted packets.

CHAPTER 8

CONCLUSION AND FUTURE WORK

8.1 Overview

As we have presented in the literature review and in the examples of the routing algorithms, the main aim is underlining the potential problems and feasible solutions to these problems as an answer to the research questions. This chapter presents the findings and helps in discovering throughout the thesis. There also some suggestions for the future work and further research avenues for follow-up studies. We again underline that this study proposes some methods achieved for throughput improvement of the systems either by using ant colony algorithm or fastest path routing algorithm or shortest path algorithm. This chapter concludes with the benefits of the research study in the light of answers to the research questions about properties of routing algorithms applied on MPLS network.

.

8.2 Findings

The findings emerged from this study are not limited to the research questions defined in Chapter 1. There are also some additional findings that open further research topics as well.

Findings that have been achieved through this study include the following:

- The literature review in chapter 5 shows that routing algorithms at various types can implement MPLS protocol in a simulation program. Chapter 6 provides many examples reported in the literature which shows some successful implementations of the MPLS protocol in MATLAB.
- Chapter 4 lists some potential problems which can be faced during the implementation of real networks. It is possible to solve these problems;

where the 4th chapter shows that these problems can be solved by proposed recovery methods.

- The simulation results demonstrate the advantages of integrating the recovery methods to the protocols**.**
- Because of its effect, the routing algorithm used in the simulation with the MPLS technique has great importance on the resultant throughput**.** Therefore the ant colony, fastest path and shortest path routing algorithms are developed and implemented in the MATLAB MPLS simulation
- Chapter 7 shows the Routing algorithms embedded in the MPLS system which run simultaneously, and make their own decisions under the same conditions.
- The proposed methods improve the throughput when used with the ant colony or the fastest path or shortest path routing algorithm. Since the routing algorithms generate the routes for the packets, the fastest path algorithm always achieves greater output for both long and short implementations. The fastest path routing algorithm is therefore preferable for our proposed methods.

8.3 Conclusion

In this work, the calculation of packet loss rates and throughput values are presented. It is shown that the packet loss rate and the throughput calculation results matches with the corresponding simulation results. The throughput of MPLS network is improved by the use of novel cognitive methods. It is also shown that the proposed methods achieved the throughput improvement in the systems by using either ant colony or fastest path or shortest path routing algorithms. It is finally shown that the fastest path routing algorithm provides higher throughput values than the ant colony and shortest path routing algorithms**.** The system throughput also has greater value when fastest path algorithm is used As a result it is concluded as, he fastest path routing algorithm has the best throughput and shortest path algorithm is less than it, but the difference between them is quiet small.

8.4 Suggestions for Future work

To enhance the performance of the proposed system, some future studies are recommended:

- Using all the methods and results of this study in designing or analyzing a mobile multimedia network.
- Designing another transmission methods inside the MPLS network, and making a comparison between them.
- Using more than three algorithms and making a comparison between them.
- Using another environment like Lab View or OPNET (Optimized Network Engineering Tool) etc.

REFERENCES

1. **YAN K., (2005),** *"Network Protocol"*, Javvin Technologies, USA, pp. 342-344.

2. **AHMAD S. A., DAND A. D., JAFAR M., (2006**), "*Multi-Protocol Label Switching (MPLS)"*, Journal of Studies and Scientific Research of Engineer Sciences, Syria, vol.28, no.1, pp.179-198.

3. **ARMITAGE G., *(*2000),** *"Quality of Service in IP Network"*, New Riders Publishing, USA, pp. 336-338.

4. **DRAGOS S., COLLIER M. (2002),** "*Design and Implementation of an MPLS Based Load Balancing Architecture for Web Switching"*, School of Electronic Engineering, Germany, pp.9-11.

5. **ALWAYN V., (2002),** "*Advanced MPLS Design and Implementation"*, Cisco Press, USA, pp.496-498.

6. **WELZL M., (2005),** "*Network Congestion Control -Managing Internet Traffic"*, John Wiley & Sons, England, pp. 263-266.

7. **RYAN J., (1998),** *"Multiprotocol Label Switching (MPLS)"*, the Applied Technologies Group, pp. 47-50.

8. **RETANA A., SLICE D., WHITE *R.*, *(*1999),** *"Advanced IP Network Design (CCIE) Professional Development",* Cisco Press, USA, pp.368.

9. **REGIS J., (2002),** *"Broadband Telecommunications",* McGraw−Hill, USA, pp. 573-575.

10. **MINEI I., LUCEK J., (2005),** *"MPLS Enabled Applications Emerging Developments and New Technologies",* John Wiley and Sons, England, pp.406-410.

11. **GHEIN D. L., (2007),** *"MPLS Fundamentals",* Cisco Press, USA, pp.626-627.

12. **BATES J., GALLON C., BOCCI M., WALKER S., TAYLOR T., (2006**), "*Converged Multimedia Networks"*, John Wiley and Sons, England, pp.348-350.

13. **OSBORNE E., SIMHA A., (2003),** *"Traffic Engineering with MPLS",* Cisco Press, USA, pp.608-611.

14. **FLANNAGAN E. M., DURAND B., SOMMER V. J., BUCHMANN M., FULLER M., (2001),** "*Administering Cisco QoS*, Syngress", USA, pp.535-537.

15. **PIGNATARO C., KAZEMI R., DRY B., (2002**), "*Cisco Multiservice Switching Networks"*, Cisco Press, USA, pp.480-481.

16. **MORROW M., SAYEED A., (2007),** "*MPLS and Next Generation Networks: Foundations for NGN and Enterprise Virtualization"*, Cisco Press, USA, pp.422-425.

17. **GALLAHERS R., (2003),** "*MPLS Training Guide: Building Multi-Protocol Label Switching Networks"*, USA, pp.301-304.

18. **HALABI S., (2003),** "*Metro Ethernet"*, Cisco Press, USA, pp.240-244.

19. **BONEY J., (2005),** *"Cisco IOS in a Nutshell"*, O'Reilly, USA, pp.796-798.

20. **MINOLI D., (2002),** "*Voice Over MPLS: Planning and Designing Networks"*, McGraw Hill, USA, pp.443-447.

21. **MARCHESE M., (2007),** “*QoS Over Heterogeneous Networks”*, John Wiley and Sons, England, pp.307-310.

22. **Lawrence J., (2001),** *“Designing Multiprotocol Label Switching Networks”,* Cisco Systems, USA, pp. 134-142.

23. **CASTELLI J. M., (2003),** *“Network Sales and Services Handbook”*, Cisco Press, pp.464-470.

24. **DOYLE J., (2005),** “*OSPF and IS-IS Choosing an IGP for Large-Scale Networks”*, Addison Wesley, USA, pp.480-483.

25. **ROSEN E., VISWANATHAN A., CALLON R., (2001),** “*Multiprotocol Label Switching Architecture”*, USA, pp.61-65.

26. **STALLINGS W., (2001),** “*MPLS”*, The Internet Protocol Journal, USA, vol.4, no.3, pp.2-14.

27. **MORRIS B. S., (2003),** “*Network Management Mibs and Mpls”*, Prentice Hall, USA, pp.416-420.

28. **Petersson J. M. O., (2005),** *“MPLS Based Recovery Mechanisms”,* Master Thesis, University of Oslo, Norway, pp. 28-42.

29. **REGAN J., (2002),** “*CCIP: MPLS Study Guide”*, Sybex, USA, pp.466-468.

30. **GOLENIEWSKI L., JARRET T. W. K., (2007),** “*Telecommunications Essentials, Second Edition: The Complete Global Source”*, Addison Wesley, USA, pp.928-930.

31. **Townsley M., (2005),** *“MPL Saver IP- Tunnels”,* Cisco System, USA, pp. 12-15.

32. **REDDY K., (2004),** “*Building MPLS-Based Broadband Access VPN's”***,** Cisco Press, USA, pp.408-413.

33. **HUSSAIN I., (2004),** "*Fault-Tolerant IP and MPLS Networks"*, Cisco Press, USA, pp.336-339.

34. **JAFAR M., Dndh R., Ahmed S. A., (2008),***" Multi-Protocol Label Switching*", Master Thesis, Faculty of Mechanical and Electrical Engineering, pp. 51-55.

35. **THOMAS M. T., PAVLICHEK D., DWYER H. L., CHOWBAY R., DOWNING W., SONDEREGGER J., (2002),** "*Juniper Networks® Reference Guide: JUNOS™ Routing, Configuration, and Architecture"*, Addison Wesley, USA, pp.880-884.

36. **Harrison E., Farrel A., Miller B., (2001),** *"Protection and Restoration in MPLS Networks",* pp. 1-10.

37. **Lang et al. J. P., (2001),** *"Link Management Protocol (LMP)",* pp. 10-20.

38. **Farrel et al. A., (2003),** *"Crankback Signaling Extensions for MPLS Signaling",* pp. 23-30.

39. **TAN N., (2005),** "*MPLS for Metropolitan Area Networks"*, Auerbach, USA, pp.403-407.

40. **Uyless B., (2002),** *"MPLS Label Switching Network",* Prentice Hall, pp. 12-19.

41. **Harnedy S., (2002),** *"MPLS Primer",* Prentice Hall, USA, pp. 512-516.

42. **Hung T. C., Thanh N. H., Thang N. D., Jung W. J., Kim T. I., Kim S. H., Yang W. J., (2002),** *"Advanced Routing Algorithms and Load Balancing on MPLS",* Uyless Black, South Korea, pp. 1-6

43. **Kodialam M., and Lakshman T., (2000),** *"Minimum Interference Routing with Applications to MPLS Traffic Engineering",* Proceedings of IEEE INFOCOM, pp. 884-893.

44. **Boutaba R., Szeto W., (2002**), *"DORA: Efficient Routing for MPLS Traffic Engineering"*, Journal Of Network And Engineering, Iraq, pp. 309-325.

45. **Suri S., Waldvogel M., Bauer D., Warkhede P. R., (2002),** *"Profile-Based Routing and Traffic Engineering"*, Proceedings of IEEE INFOCOM, Amsterdam, pp. 351-365.

46. **Wang Y. and Wang Z., (2002),** *"Explicit Routing Algorithms for Internet Traffic Engineering"*, Bell Laboratories, pp. 582-588.

47. **Preveze B. and Safak A., (2012),** *"Comparative Analysis of Novel Long Life Routing Methods in Mobile Networks",* Ankara, Turkey, pp. 1-6.

48. **Nagib G. and Wahied G. A., (2010),** *"Network Routing using Genetic Algorithms",* International Journal of Electrical and Computer Sciences, vol. 10, no. 2, pp. 1-5.

49. **Xu Y., Wang W., (2009),** *"Finding the Fastest Path in Wireless Networks",* North Carolina State University, USA, pp. 1-5.

50. **Dong y., Gu J., Li N., Hou X., Yan W., (2007),** *"Combination of Genetic Algorithm and Ant Colony Algorithm for Distribution Network Planning"*, Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Tianjin, China, pp. 1-4.

51. **Garcia-Luna- Aceves J. J., (2009),** *"A Distributed, Loop-Free, Shortest-Path Routing Algorithm",* Information Sciences and Technology Center, pp. 1-13.

52. **Jaroenrat K., Pathom N. T., Chimmanee S., Charnkeitkong P., (2010),** *"Algorithms for IP Networks Design with ECMP Routing Enable"*, Thailand, pp.420-425.

53. **Huitema C., (1995),** "*Routing in the Internet",* Prentice Hall, pp. 12-15.

APPENDICES A

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: YASEEN, Nawfal Qasim

Date and Place of Birth: 11 August 1982, Mosul

Marital Status: Married

Phone: 00905388419332, 009647701604406

Email: aboalnoon2012@gmail.com , zlzaaoy@yahoo.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
M.Sc.	Çankaya University, Computer Engineering	2015
B.Sc.	Technical College of Mosul, Computer Technology Engineering	2005
High School	Al-Sharqiya High School	2001

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2005- Present	Ministry of Electricity in Iraq	Specialist Employee

FOREIN LANGUAGES

English

HOBBIES

Reading, Football, Swimming, Traveling, Fitness.