

Transactions on Networks and Communications

ISSN: 2054-7420

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD	I
DISCLAIMER	II
Links Utilization in MPLS Networks Operating with Traffic Engineering Signal Protocols Ghufran Saady Abd-almuhsen Mahmoud M. Al-Quzwini Raad Sami. Fyath	1
Efficient On-Line Traffic Policing for Confidence Level based Traffic Model Lie Qian	28
Mobile Operators as Banks or Vice-Versa? and: Regulators' Interest in the Best Efficiency of Payments Louis François Pau	42
An SMS Based Push Email Server Izang Aaron.A Omotunde Ayokunle A Kuyoro Shade Abel Samuel and Mensah Yaw	54
Network Flexibility and Policy making in Software Defined Networks Abhinav Sharma Manu Sood	63
Efficient Cooperative MAC and Routing in Wireless Networks Shamna H R Lillykutty Jacob	79

EDITORIAL ADVISORY BOARD

Dr M. M. Faraz
Faculty of Science Engineering and Computing, Kingston University London
United Kingdom

Professor Simon X. Yang
Advanced Robotics & Intelligent Systems (ARIS) Laboratory, The University of Guelph
Canada

Professor Shahram Latifi
Dept. of Electrical & Computer Engineering University of Nevada, Las Vegas
United States

Professor Farouk Yalaoui
Institut Charles Dalaunay, University of Technology of Troyes
France

Professor Julia Johnson
Laurentian University, Sudbury, Ontario
Canada

Professor Hong Zhou
Naval Postgraduate School Monterey, California
United States

Professor Boris Verkhovsky
New Jersey Institute of Technology, Newark, New Jersey
United States

Professor Jai N Singh
Barry University, Miami Shores, Florida
United States

Professor Don Liu
Louisiana Tech University, Ruston
United States

Dr Steve S. H. Ling
University of Technology, Sydney
Australia

Dr Yuriy Polyakov
New Jersey Institute of Technology, Newark,
United States

Dr Lei Cao
Department of Electrical Engineering, University of Mississippi
United States

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone's views or feelings etc.

Links Utilization in MPLS Networks Operating with Traffic Engineering Signal Protocols

Ghufran Saady Abd-almuhsen¹, Mahmoud M. Al-Quzwini², and Raad Sami. Fyath³
Department of Computer Engineering, Al-Nahrain University, Baghdad, Iraq
¹ghufransaady@yahoo.com, ²quzwini72@yahoo.com, ³rsfyath@yahoo.com

ABSTRACT

Multiprotocol Label Switching (MPLS) is a technology that ensures efficient transmission with high speed and lower delays. Traffic Engineering (TE) signal protocols are usually used for active management of the MPLS networks for efficient utilization of resources. This paper presents performance investigation of MPLS TE signal protocols to get a guideline to utilize transmission links efficiently. Comparison is made between two TE signal protocols, namely Resource Reservation Protocol (RSVP) and Constraint-based Routing Label Distribution Protocol (CR-LDP). Simulation results are presented for three MPLS networks having different topologies, which are implemented in OPNET (version 14.5) environment to support different applications in the absence and presence of quality of service (QoS) algorithms. The results reveal that MPLS network with CR-LDP TE signal protocol has better performance in the term of link utilization. The RSVP reserves certain paths for transmission while the CR-LDP utilizes almost all of the available links.

Key words: MPLS Networks, Traffic Engineering Signal Protocols, Quality of Service.

1 Introduction

Multi Protocol Label Switching is raised from the Internet Engineering Task Force's (IETF) effort to standardize a number of proprietary multilayer switching solutions that were initially proposed in the mid-1990s. MPLS integrates layer 3 (routing) and layer 2 (switching) functionalities [1]. MPLS introduces connection-oriented forwarding model by replacing the routing of IP packets based on the IP header information with the short four-byte label-based switching, as shown in Figure (1).

The mechanism does not build forwarding decision based on the traditional destination IP address on sophisticated lookup routing table. This fixed-length switching concept is to some extent similar to that used in ATM and Frame Relay networks, and it is independent of the used layer 2 technologies. MPLS has been designed to provide an admirable solution to present shortcomings of IP routing in the area of Traffic Engineering (TE), Quality of Service (QoS), Virtual Private Networks (VPN) and Differentiated Services (DiffServ) [2]. In comparison of DiffServ with MPLS which is evolving as a futuristic protocol. MPLS is desirable over DiffServ since it utilizes "Multi Protocol Architecture" depending on simple label switching technique. Traffic can be simply differentiated thereby ensuring QoS based on traffic types. Applications like VPNs need MPLS to achieve high quality end-to-end service. The new and better network topologies-

Any Transport over MPLS (AToM), MPLS over Voice over Internet Protocol (VoIP) and video traffics etc. have resulted in perceivable QoS [3].

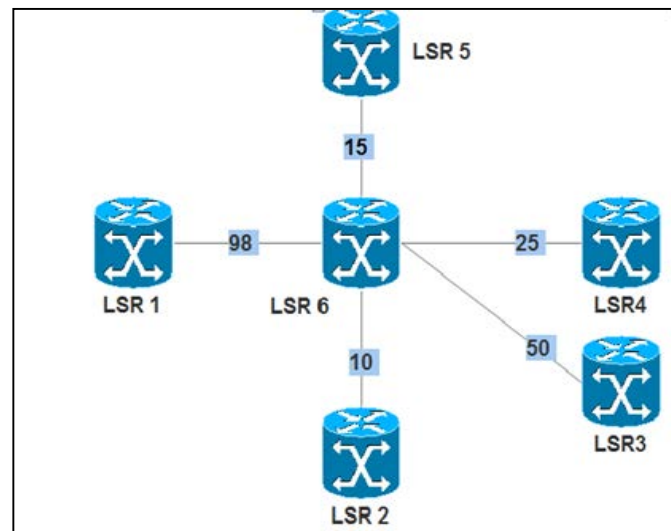


Figure (1): MPLS forwarding label between routers. LSR denotes Label Switching Router

MPLS enabled network can provide efficient TE services, flow based services, better traffic shaping, etc. In [4], routing based traffic flow shaping is introduced, where total traffic is split over multiple Label Switching Paths (LSPs) in the MPLS network. This method is powerful for solving some of the routing problems like mismatch and bottleneck problems. Network with MPLS can propose good QoS to delay critical traffic such as meetings, VoIP and video conference. Network failure such as crash of network elements, link faults or congestion are easily managed in MPLS networks [5].

MPLS can be considered a technology to forward the packets in IP intangible networks. The Entire MPLS network can be split into two parts namely MPLS edge and MPLS core [6]. MPLS edge is the border of the MPLS network consisting of egress and ingress routers. MPLS core bound intermediate Label Switching Routers (LSRs), through which Label Switched Paths (LSPs) are established [7].

A traffic engineering matter in the Internet consists of setting up paths between the edge routers in a network to meet traffic needs while attaining low congestion and improving the utilization of network resources. Practically, the usual key purpose of traffic engineering is to eliminate the utilization of the most heavily used links in the network, or the maximum of link utilization. As the maximum link utilization qualitatively reveals that congestion sets in when link utilization rises higher, and hence it is necessary to eliminate the link utilization throughout the network such that no bottleneck link occurs. It is known that this problem of reducing the maximum link utilization can be achieved by the multi-commodity network flow formula of powerful routing, which leads to dividing traffic over multiple paths between source and destination pairs [8]. This paper addresses link utilization in MPLS-based networks incorporating TE signal protocols and Qos algorithms.

2 Related Work

In 2010, Shyry and Ramachandran [9] discussed the effect of MPLS on network performance with the aid of the Nash equilibrium algorithm. The results show that optimized performance can be obtained by

reducing the latency and raising the link utilization. But rising link utilization leads to a gradually increase of the congestion in the network. To overcome this specific problem, a formulation called dual programming formulation was performed which has group of constraints that have to be satisfied along with Open Shortest Path First (OSPF) protocol so as to eliminate the maximum link utilization.

In 2011, Pelsser and Bonaventure [10] discussed the Service Provider's (SP's) requirements for the utilization of MPLS LSPs across Autonomous System (AS) boundaries. A minimum set of extensions was introduced to Resource Reservation Protocol-Traffic Engineering (RSVP-TE) that allows setting inter-AS LSPs in accordance with the Service Provider requirements. The results show how LSP protection techniques can be extended to provide links or node failure protection for the border routers and inter-AS.

In 2012, Bongale [5] compared link utilization among networks running Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and MPLS. The results showed that networks configured with OSPF and RIP routing technicalities are not capable of managing the incoming traffic efficiently. When the network traffic increases, shortest path from source node to destination node is heavily congested and lead to loss of transmitted data, while MPLS is capable of handling incoming traffic effectively by portioning the traffic over unutilized links. This will ensure packets, that entering into MPLS core, to reach the destination with minimum queuing delay. The results also indicate that MPLS-TE is most appropriate for enormous traffic volume. OPNET simulator was used to get the results and performance was compared considering data consisting of voice traffic and web browsing only.

In 2012, Aziz et al. [11] presented a QoS performance study of real-time applications such as video conferencing and voice in terms of Packet Delay Variation (PDV) over DiffServ in the absence and presence of MPLS-TE in IPv4/IPv6 networks using OPNET simulator. The interaction of Assured Forwarding (AF) traffic aggregation, Expedited Forwarding (EF), link congestion, in addition to the effect of performance metric like PDV were also studied. The performance of DiffServ and MPLS-TE combination in IPv4/IPv6 network was elucidated and analyzed. The results show that IPv6 encounter more PDV than their IPv4 counterparts.

In 2013, Bhandure et al. [12] studied MPLS and Non-MPLS networks and presented an overview of the MPLS technology and related IETF standards. The results show that MPLS is faster and has better performance than traditional IP routing. Performance was compared by observing parameters such as number of transmitting received packets, Jitter (delay variation) and end-to-end delay. GNS 3.0 simulator was used to simulate the networks. The simulations were setup using a traditional IP network without TE (composed of OSPF and BGP) and MPLS network (composed of OSPF and BGP).

In 2013, Ibrahim [13] discussed the performance of MPLS-TE signal protocols, namely the Resource Reservation Protocol (RSVP) and Constraint based Routed-Label Distribution Protocol (CR-LDP), with different applications including voice, video and data. Performs evaluation of the two protocols shows that CR-LDP outperforms the RSVP in terms of response time and the average transmitted and received packets in all applications. The link utilization capability of these protocols was also addressed with different transmission loads.

In 2014, Sulaiman and Alhafidh [14] discussed the performance analysis of multimedia traffic over MPLS communication networks with TE. The performance metric of MPLS-TE and IP model networks was compared. The compared parameters were end-to-end delay, delay variation, packet send and receive,

File Transfer Protocol (FTP) responsetime. The results show that MPLS-TE performance is better than traditional IP network model.

Most of the previous works focus on traffic performance comparison between both MPLS and Non-MPLS networks by using simulation tools. This paper focuses mainly on the performance of MPLS networks when TE is taking into account with some signaling protocols (CR-LDP and RSVP) and QoS algorithms. Emphasize is being placed on the key role played by link utilization.

3 Background

This section introduces brief description of MPLS network and TE signal protocols.

3.1 MPLS Network

In MPLS, packets are sent to their destinations by labeling them and forwarding them. Short, fixed-length labels are added to the IP packets when they enter the network. Consequently, instead of using the IP header information, the labels are used to forward the packets to their destinations. To do this, a new protocol is developed for classifying the labels. Extensions to existing protocols are also used to ease this [15].

MPLS can be considered a technology to forward the packets in IP intangible networks. The Entire MPLS network can be split into two parts namely MPLS edge and MPLS core [16]. MPLS edge is the border of the MPLS network consisting of egress and ingress routers shown in Figure (2). MPLS core bound intermediate Label Switching Routers (LSRs), through which Label Switched Paths (LSPs) are established [16].

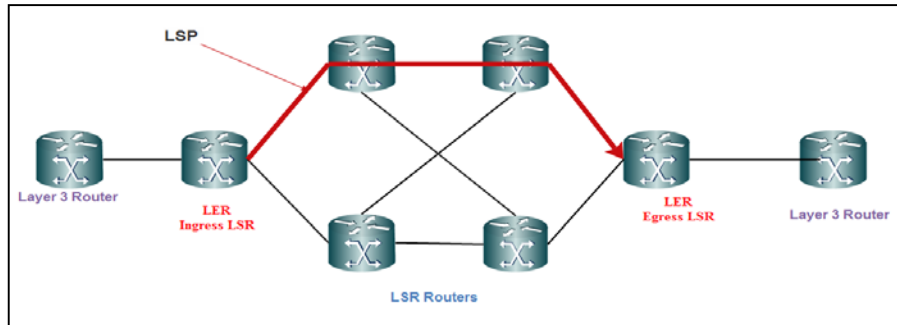


Figure (2): MPLS domain network

General terms correlating with MPLS network and their explanation are specified in the following

- Label Description: A short, fixed length packet identifier.
- Label Edge Router (LER): A device that operates at the edge of the access network and MPLS network.
- Label Switching Router : A router which is located in the MPLS domain and forwards the packets based on label switching.
- Forward Equivalence Class (FEC) : A description of a group of packets sharing the same transport requirements.
- Label Switched Path (LSP) : A route established between two Label Edge Router (LER) which work as a path for forwarding labeled packets over LSPs.

The two planes, namely control plane and data plane, highlight the operation of MPLS are shown in Figure (3) [17].

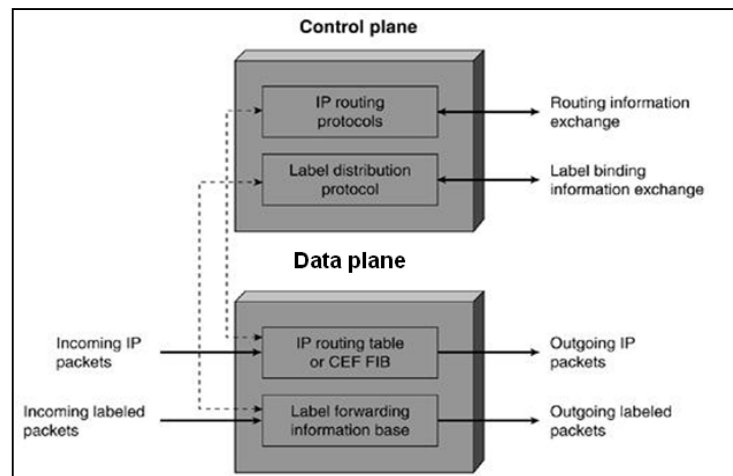


Figure (3): MPLS planes [17]

3.2 Traffic Engineering Signal Protocols

With the standardization of MPLS by IETF, traffic engineering obtained its popularity due to the supported features of the MPLS for Traffic Engineering more than the traditional IP networks. The main structure blocks of the MPLS Traffic Engineering Model are Path Management, Network State Information Dissemination, Traffic Assignment and Network Management [16]. Due to the online and offline usability of the MPLS network and the capability to list at any point of time, Traffic Engineering has gained its popularity [18]. The packets in MPLS network are forwarded using the level swapping. This forwarding of packets gives more control for expeditiously forwarding packets [17]. Figure (4) shows the relation between Interior Gateway Protocol (IGP), MPLS and constraint-based routing for the path selection in a network. The path selection procedure depends on the availability of the protocols. In absence of MPLS, the path selection is done by IGP and in the presence of the MPLS the path selection or the signaling protocols of the MPLS are implemented [19].

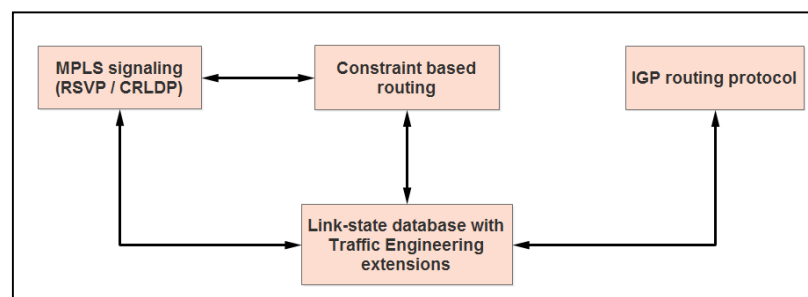


Figure (4): Interaction of the various components of an MPLS-based Traffic Engineering solution [19].

Traditionally IP packets were forwarded looking into its destination address at every router in the path. The packets were forwarded based on the shortest path metric, which is the cost calculated using the time it takes to reach the next hop. When the traffic in the network increases, the link with shortest path becomes heavily congested while the links with higher paths are underutilized resulting in the uneven loads in the links available, on the cost of traffic resources. The development of MPLS addresses these

problems with the use of constraint based routing (CBR). The dynamic use of the measuring tools and the accountability of all the possible multiple paths and its characteristics (bandwidth, policy and topology) by CBR makes it easier for implementation of Traffic Engineering efficiently [17].

Signaling protocols are used to set up the paths for the packets to follow, these paths are usually known as Label Switched Path. There are many protocols which can be used for paths selection, but here only the signaling protocols that support Traffic Engineering are explained [18]. In this paper, two types of signal protocols are used, Constraint-Based Label Distribution Protocol (CR-LDP) and Resource Reservation Protocol (RSVP).

3.3 Constraint-Based Label Distribution Protocol

Label Distribution Protocol (LDP) is designed by a working group at IETF from the ground up for the particular reason for distributing MPLS labels, consequently setting up LSPs in the MPLS domain. LDP works closely with IGP routing protocols and is usually called "hop-by-hop" forwarding. LDP does not support TE because it always chooses the same physical path that traditional IP routing would select. The reason behind setting up an LSP that follows the same path as traditional IP instead of just using traditional IP routing was primarily to accelerate the forwarding in routers. In traditional IP routing the next hop for each packet is found by a longest match prefix lookup on the IP header in the routing table. These lookup could in some cases, where the routing tables were large, be time consuming and it was surmised that data forwarding with label switching instead of IP lookups would speed up data forwarding. However, the forward speed of IP packets is not a matter anymore. Because of the development in routing technology, LDP is not frequently used for label distribution nowadays. There is an extension to the original LDP protocol that presents the new functionality of the LDP protocol called CR-LDP [20].

CR-LDP is an extent of LDP to support constraint based routed LSPs. The term constraint implies that in a network and for each group of node there exists a group of constraint that must be satisfied for the link or links between two nodes to be selected for an LSP. LSRs that use CR-LDP to interchange label and FEC mapping information are called LDP peers, they interchange this information by forming a LDP session [21].

3.4 Resource Reservation Protocol

An alternate signaling protocol to LDP and CR-LDP is the resource reservation protocol traffic engineering (RSVP-TE). RSVP-TE is an extension of the resource reservation protocol which was designed to support the integrated services (intserv) architecture. The intserv architecture was improved by IETF in the mid 1990s with a view to introducing QoS in the IP network.

The following two service classes were defined in intserv [17], [22]

- i. **Guaranteed service:** This service provides firm bounds on the end-to-end queuing delay with no packet loss for all conforming packets.
- ii. **Controlled-load service:** This service provides the user with a QoS that closely approximates the QoS of the best effort service that the user would receive from an unloaded network. Specifically, a user might assume the following:

- A very high percentage of transmitting packets will be successfully transported by the network to the receiver. The percentage of packets not successfully transported must widely approximate the basic packet error rate of the transmission links
- The end-to-end delay experienced by a very high percentage of the transported packets will not greatly achieve the minimum end-to-end delay experienced by any successfully transported packet.

RSVP is soft state protocol, which means that when a path has been setup by RSVP it has to be regularly updated to keep the resources reserved. The requests for reservation are made from the receiver end of the path, so RSVP is a receiver-oriented protocol. When RSVP is used for LSP setup the ingress router starts by sending a PATH message on the path where an LSP will be set up. Each transportation router on that path has to examine if it has the possibility to set up the requested LSP. If the requested LSP is discarded, an error message is returned upstream until it reaches the ingress router. Furthermore the path message is sent to the next transportation router in the path until it arrives the egress router [23].

4 Simulated Network Topologies and Setup Parameters

This section presents a full description of network setup and topologies that used in the simulation. An investigation of MPLS Traffic Engineering signal protocols capabilities to utilize the transmission link in the absence and presence of QoS is also presented. Different applications including voice, video, File Transfer Protocol (FTP), Telnet, print, Electronic mail (E-mail), database and Hyper Text Transfer Protocol (HTTP) are used for the performance evaluation. The parameters that are considered throughout the study are Throughput (the average number of bits successfully transmitted or received by the transmitter or the receiver channel per unit time, in bits per sec) and Link utilization (the percentage of the throughput to the data rate of the link used in the transmission).

The simulation environment used in this work is based on Optimum Network Engineering Tool (OPNET) 14.5 simulator. OPNET is a real-time simulator suitable mainly for the design and analysis of network models. The VoIP traffic is sent between the workstation (voice 1) and workstation (voice 2). The same terminology is followed with video traffic, which is sent between the workstation (video 1) and workstation (video 2). For other applications, (HTTP, FTP, Database, E-mail, Print and Telnet), the traffic is sent between workstations and servers.

4.1 Network Topologies

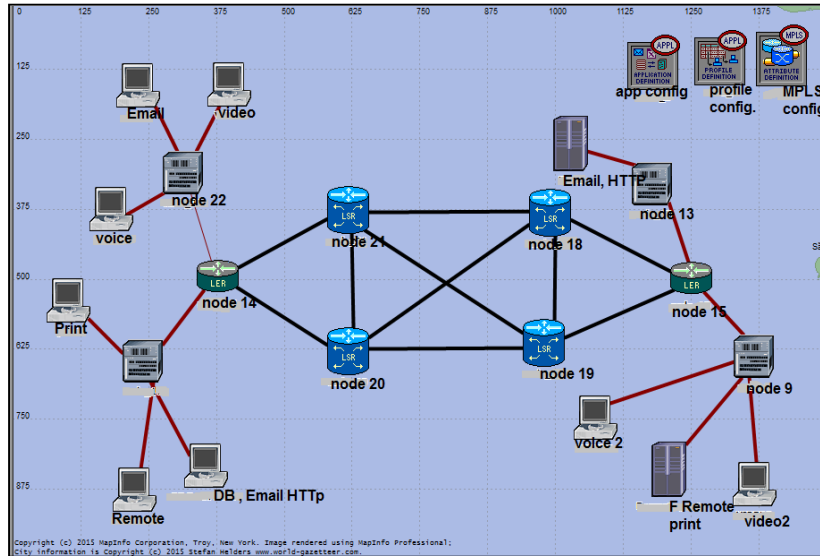
The following parameters are considered in the simulation

- (i) DS1 links (data rate 1.544 Mbps) are used in the core network.
- (ii) Network applications are divided into low, medium and high loads.

Figures (5a)-(5c) show the topologies of the three simulated MPLS networks using the two TE signal protocols (RSVP and CR-LDP). The first network has six routers, two LER routers and four LSR routers as shown in Figure (5a). In the second network, the number of routers increases. The network uses eight LSR routers and two LER routers, as shown in Figure (5b). The third network has same number of routers as the second network but with increasing number of links (38 links) as shown in Figure (5c).

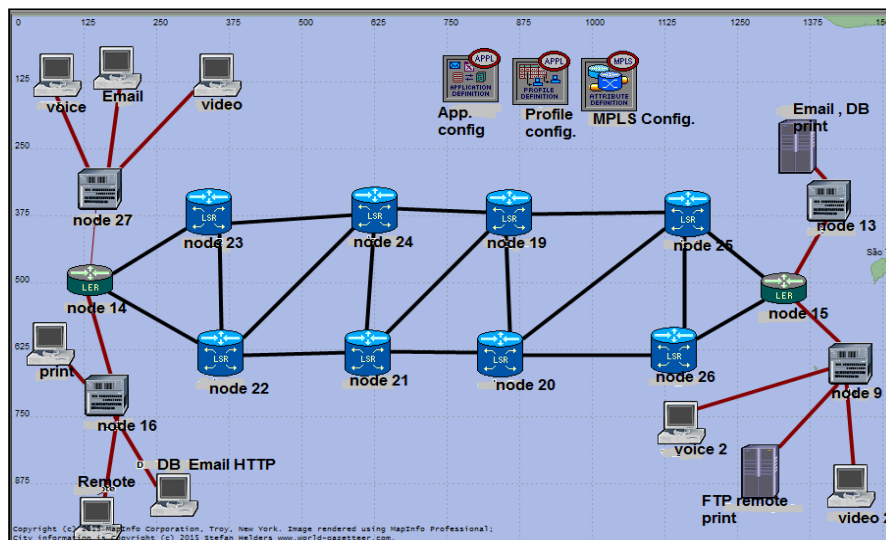
Table (1): Numbers of elements used in the simulated three networks.

Networks	Number of Elements		
	LSR Router	LER Router	Link
First	4	2	20
Second	8	2	28
Third	8	2	38

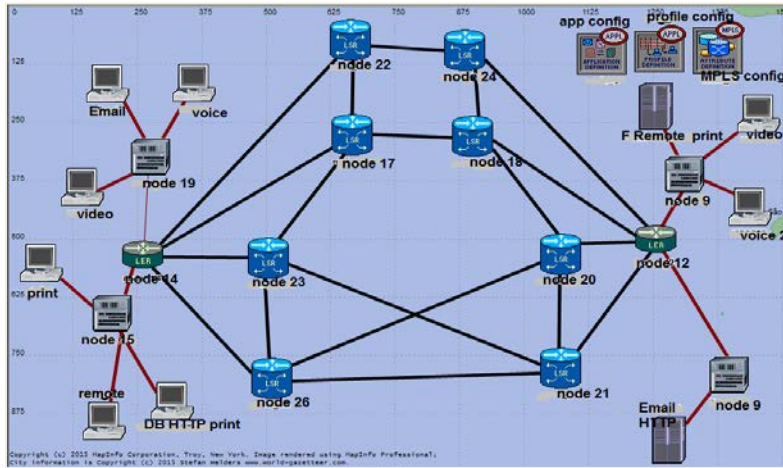


(a)

Figure (5): MPLS network topologies used in the simulation.
 (a) First network (b) Second network (c) Third network.



(b)



(c)
Figure (5): continued.

4.2 Parameters used in the Simulation

Table (2) shows the parameters of the applications to be used during the simulations. Voice work stations use G.711 codec with data rate of 64 kbps. There are many factors that indicate the quality of voice which include choice of codec, packet loss, and delay. For VoIP applications, it is required that end-to-end packet delay shouldn't exceed 150ms in order that the quality of the established VoIP call is acceptable [25]. The voice delay in G.711 can be divided into two contributing components, which are explained as follows

- (i) The delay provided by the G.711 codec for encoding and packetization is 1 and 24ms, respectively. Therefore, the delay at the transmitter according to these two delays with compression is approximated to a fixed delay of 25 ms.
- (ii) At the receiver, the delay comes from decompression, buffering, playback, and depacketization delay. The total delay due to these factors mentioned above is approximated to a fixed delay of 45 ms.

Table (2): Applications parameters

VoIP Applications	
Encoder Scheme	G.711 (PCM)
Type of Service	Interactive Voice
Video Applications	
Frame rate	10 frames/sec
Frame Size	128*120 pixels
Type of Service	Streaming Multimedia
FTP Applications	
File Size	5000 byte
Type of Service	best effort
HTTP Applications	
HTTP Specification	HTTP 1.1
Page Properties	1000 byte
Type of Service	best effort
Print Applications (color file)	
File size	3000-90000 byte
Type of Service	Best effort

Telnet Applications	
Terminal Traffic (normally distributed)	Mean =144, variance=60 byte
Type of Service	Best effort
E-Mail Applications	
E-Mail Size	2000 byte
Type of Service	best effort
Database Applications	
Transaction Size	512 byte
Type of Service	Best effort

The maximum acceptable network delay can be determined from the above transmitter and receiver delays to be 80 ms nearly (150-25-45) ms, where the 150 ms represents the maximum acceptable end-to-end delay, so that the quality of the established VoIP call is acceptable [26]. Video workstations transfer 10 frames per second (sec); each frame be formed of 128x120 pixels. FTP work stations used files of size 5000 bytes [27]. HTTP work stations use pages of size 1000 bytes, HTTP 1.1 is employed in this study, HTTP 1.1 is a revision of the original HTTP (HTTP 1.0). In HTTP 1.0 a separate connection to the same server is made for every resource request. HTTP 1.1 can reuse a connection multiple times to download images, page inter-arrival times are exponentially distributed with mean 60 sec [28]. Emails are sent with inter-arrival times exponentially distributed with mean 360 sec. For database application, the transactions arrive with inter-arrival times exponentially distributed with mean 12 sec. Telnet application initiates commands from terminal to telnet host, these commands consist of a normally distributed amount of bytes with mean 144 and variance 60. Best-effort service means that the user obtains unspecified variable bit rate and delivery time, depending on the current traffic load of the network [26].

5 Link Utilization in the Absence of QoS

In this section, the link utilization of the three MPLS networks operating with CR-LDP and RSVP under different load conditions (low, medium and high) are studied and compared. No QoS algorithms are applied here. The term uplink refers to the paths carrying data from the work stations side to the server's side and the term downlink refers to the paths carrying data from the server's side to the work stations side.

The first MPLS Network used in the simulation is shown in Figure (5a) and examined here under low-load condition. Figures (6a) and (6b) show the link utilization for the uplink paths and down link paths of the MPLS network with CR-LDP TE signal protocol, respectively. Figures (6c) and (6d) present the uplink and downlink utilization of the MPLS network with RSVP TE signal protocol, respectively.

Tables (3)-(5) list the average link utilization of all paths when the two TE signal protocols are used in the three networks, respectively. Results are given for the three load conditions (low, medium, and high). The numbers given in the tables are the time averages of the results obtained in the simulation (such that given in Figure (6)).

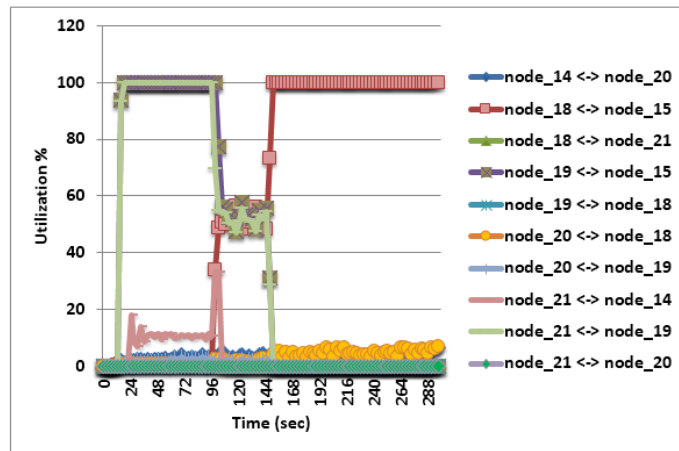


Figure (6a): Link utilization of the uplink paths of network 1 with CR-LDP TE signal protocol (low load)

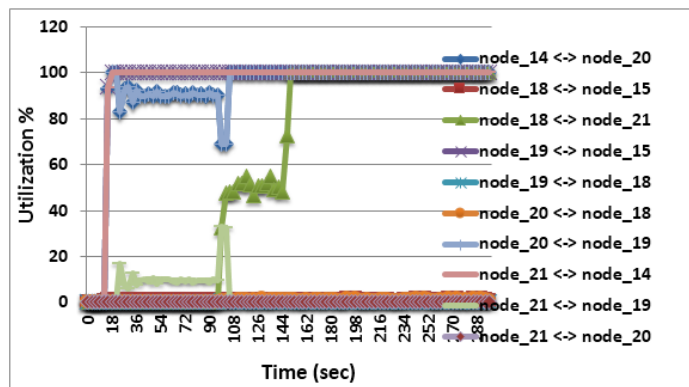


Figure (6b): Link utilization of the downlink paths of Network 1 with CR-LDP TE signal protocol (low load).

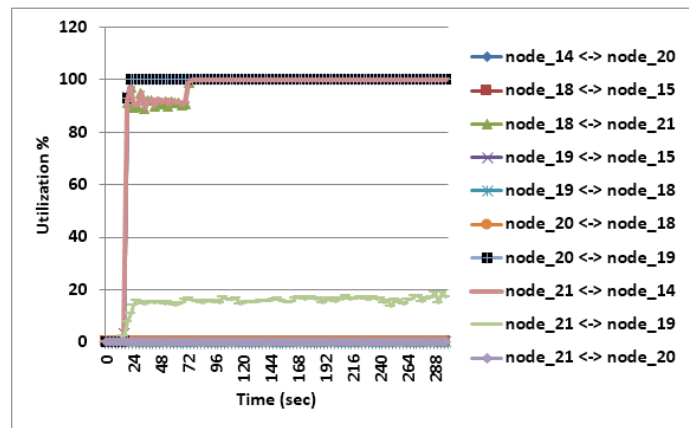


Figure (6c): Link utilization of the uplink paths of Network 1 with RSVP TE signal protocol (low load).

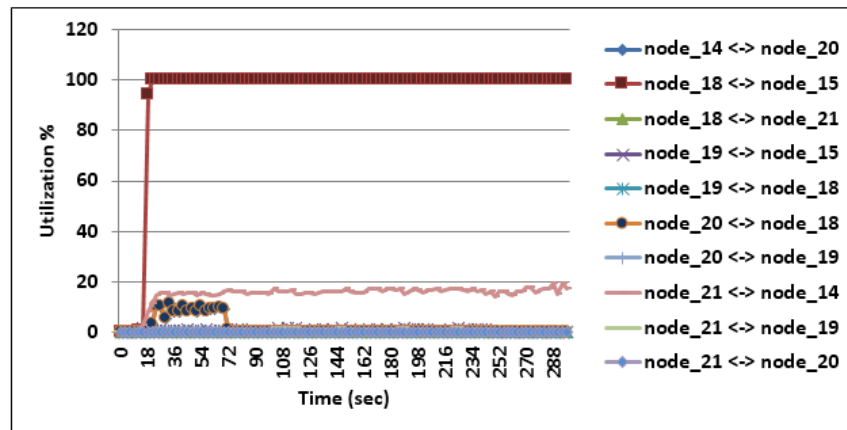


Figure (6d): Link utilization of the downlink paths of Network 1 with RSVP TE signal protocol (low load).

Table (3): Average link utilization of Network 1 operating with CR-LDP and RSVP TE signal protocols in the absence of QoS.

Link	Utilization %					
	Low load		Medium load		High load	
	CR-LDP	RSVP	CR-LDP	RSVP	CR-LDP	RSVP
14→20	3.20	92.03	18.80	11.42	18.80	11.42
20→14	89.35	2.05	35.32	59.68	35.32	59.68
18→15	46.06	0.00	92.03	8	92.03	8
15→18	1.07	92.04	3.90	93.37	3.90	93.37
18→21	0.43	90.06	2.39	33.26	2.39	33.26
21→18	45.55	0.00	91.86	6.49	91.86	6.49
19→15	49.29	92.07	4.28	87.19	4.28	87.19
15→19	93.34	0.00	92.02	1.86	92.02	1.86
19→18	0.00	0.00	0	0	0	0
18→19	0.00	92.22	0	0	0	0
20→18	2.18	0.00	14.90	0	14.90	0
18→20	0.00	1.99	1.52	59.69	1.52	59.69
20→19	1.10	92.02	3.91	11.01	3.91	11.01
19→20	89.34	0.00	34.80	93.32	34.80	93.32
21→14	4.46	90.17	59.61	33.79	59.61	33.79
14→21	93.34	0.00	59.61	1.36	59.61	1.36
21→19	48.30	0.00	0.40	87.01	0.40	87.01
19→21	4.06	92.04	57.23	0	57.23	0
21→20	0.00	0.00	0	0	0	0
20→21	0.00	0.00	0	0	0	0

Table (4): Average link utilization of Network 2 in the absence of QoS.

Link	Utilization %					
	Low load		Medium load		High load	
	CR-LDP	RSVP	CR-LDP	RSVP	CR-LDP	RSVP
14→23	37.58	11.68	37.58	11.68	0.62	92.64
23→14	6.58	71.86	6.58	71.86	88.66	0.00
20→19	0.00	0.00	0.00	0.00	0.00	0.00
19→20	0.00	0.00	0.00	0.00	0.00	0.00
20→25	0.43	0.00	0.43	0.00	0.00	0.00
25→20	6.58	17.95	6.58	17.95	3.46	0.00
20→26	56.43	83.51	56.43	83.51	80.87	0.00
26→20	12.51	0.00	12.51	0.00	0.33	92.62
21→19	0.00	0.00	0.00	0.00	0.00	0.00
19→21	0.00	0.00	0.00	0.00	0.00	0.20
21→20	56.85	83.52	56.85	83.52	80.87	0.18
20→21	87.30	18.07	87.30	18.07	3.77	92.62
21→24	0.00	0.00	0.00	0.00	0.00	0.00
24→21	0.00	0.00	0.00	0.00	0.00	0.00
22→14	87.30	19.88	87.30	19.88	3.86	92.64
14→22	58.02	84.82	58.02	84.82	92.05	16.04
22→21	56.86	83.52	56.86	83.52	80.92	0.18
21→22	58.02	18.10	58.02	18.10	3.86	92.62
22→24	1.17	1.31	1.17	1.31	11.14	15.86
24→22	0.00	1.80	0.00	1.80	0.00	0.24
23→22	0.00	0.00	0.00	0.00	0.00	0.00
22→23	0.00	0.00	0.00	0.00	0.00	0.00
23→24	37.58	11.69	37.58	11.69	0.62	92.64
24→23	6.58	72.29	6.58	72.29	89.08	0.00
24→19	38.74	12.98	38.74	12.98	11.75	92.77
19→24	6.58	74.07	6.58	74.07	89.08	0.24
25→15	39.17	12.98	39.17	12.98	11.79	92.77
15→25	92.43	92.04	92.43	92.04	92.62	0.44
25→19	6.59	74.1	6.59	74.1	89.19	0.00
19→25	38.74	12.98	38.74	12.98	11.88	92.77
26→15	56.42	83.09	56.42	83.09	80.44	0.00
15→26	12.51	0.00	12.51	0.00	0.00	92.63
26→25	0.00	0.00	0.00	0.00	0.00	0.00
25→26	0.00	0.00	0.00	0.00	0.00	0.00

Table (5): Average link utilization of Network 3 in the absence of QoS.

LINK	Utilization %					
	Low load		Medium load		High load	
	RSVP	CR-LDP	RSVP	CR-LDP	RSVP	CR-LDP
12→18	0.00	6.95	14.28	8.16	21.80	92.29
18→12	93.07	92.18	5.68	43.68	0.00	4.16
12→20	93.07	0.00	93.07	0.00	0.00	13.34
20→12	0.00	7.15	2.30	1.00	2.20	2.82
12→21	0.00	0.00	0.00	1.00	93.06	1.18
21→12	2.22	0.88	1.03	3.41	1.74	91.86
12→24	0.00	92.50	5.68	43.95	0.00	4.14
24→12	0.00	6.95	14.28	8.17	21.80	91.98
14→17	93.08	0.00	0.17	59.60	93.37	22.22
17→14	0.00	0.88	0.00	0.00	0.00	6.74
14→22	1.20	0.50	93.09	1.09	4.44	5.52
22→14	12.26	63.90	93.06	92.18	0.00	25.22
14→23	0.00	12.87	12.37	44.05	0.00	4.16
23→14	93.06	29.59	14.28	8.28	21.80	92.29
14→26	93.07	92.50	5.68	0.00	0.00	0.00
26→14	0.00	7.03	0.00	0.00	0.00	0.00
17→18	0.00	0.00	93.09	60.14	93.37	25.25
18→17	0.00	0.00	0.00	92.58	0.00	18.40
18→20	1.20	6.13	0.00	0.00	0.00	0.00
20→18	12.26	92.51	0.00	0.00	0.00	0.00
21→20	0.00	0.00	0.00	0.00	0.00	6.79
20→21	0.00	0.00	93.09	60.16	93.36	22.58
21→23	12.26	64.11	0.00	1.00	0.00	1.19
23→21	1.20	0.50	1.03	3.37	1.74	92.29
22→17	0.00	0.00	0.00	0.00	1.74	0.00
17→22	2.22	1.00	0.00	0.00	0.00	0.00
22→24	0.00	0.00	1.02	3.43	0.00	92.29
24→22	0.00	0.00	0.00	1.00	93.06	1.20
23→17	2.22	1.00	0.00	0.00	0.00	0.00
17→23	0.00	0.00	0.00	0.00	0.00	0.00
23→26	0.00	0.00	0.00	0.00	0.00	0.00
26→23	0.00	0.00	0.00	0.00	0.00	0.00
24→18	0.00	0.00	0.00	0.00	2.20	0.00
18→24	0.00	0.00	0.00	0.00	0.00	0.00
26→20	0.00	7.38	2.30	1.00	0.00	2.84
20→26	93.07	0.00	93.07	0.00	0.00	13.62
26→21	0.00	5.78	10.08	0.00	0.00	2.83
21→26	0.00	29.76	0.00	92.56	0.00	11.92

Investigating the results in Tables (3)-(5) show the following findings

- (i) The MPLS network with CR-LDP TE signal protocol has better performance in term of link utilization. The RSVP reserves certain paths for transmission, while the CR-LDP utilizes most

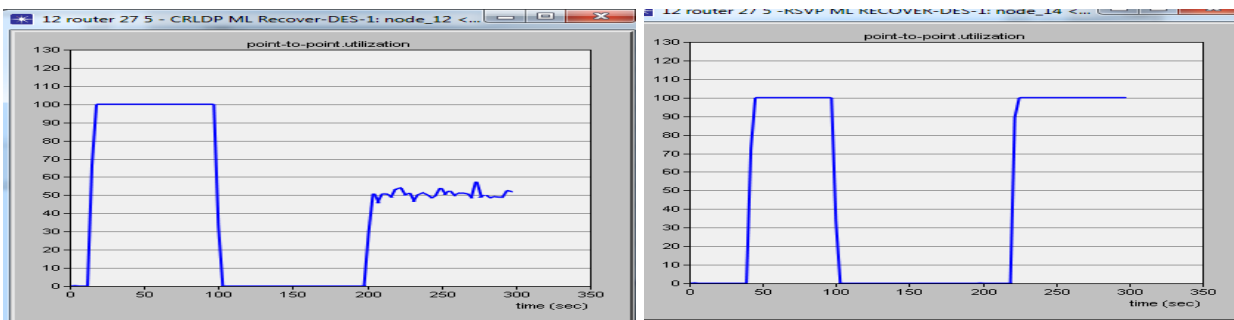
of the available links. Table (6) shows the total number of links utilized by the two protocols for the three networks.

Table (6): Total number of links utilized by the MPLS networks with two TE signals protocols

Network	TE signal protocol	Total number of utilized links		
		Low load case	Medium load case	High load case
Network 1	CR-LDP	15	15	16
	RSVP	10	11	14
Network 2	CR-LDP	25	23	22
	RSVP	17	21	18
Network 3	CR-LDP	22	24	28
	RSVP	14	15	20

- (iii) The CR-LDP TE signal protocol manages almost equally to recognize the size of the load transmitted in both directions. Therefore, equal utilization of the links in both directions is observed.
- (iv) The CR-LDP capabilities for utilizing transmission links is affected by network topology. The difference also can be noticed in the number of utilized links as given in Table (6).
- (v) When Network 3 operates under high load condition, the RSVP TE signal protocol reservation of certain links leads to congestions in some paths (path 14→22, path (22→14)). However, it uses these two paths at nearly full rate (93%) in the uplink which reveals the inability of this protocol to manage the utilization between uplink traffic and downlink traffic on the same path.

The investigation is carried further to address the ability of MPLS networks operating with CR-LDP and RSVP TE signal protocols to detect and recover fault links. The results are given for Network 3 only since other networks have similar behavior. Figure (7a) shows CR-LDP TE signal protocol capabilities to detect transmission links failure and the speed of recovery. Figure (7b) presents RSVP TE signal protocol capabilities to fault links detection and speed to recover it. Fail link time is considered at 100 sec and recover time is set to 200 sec. The results show that both CR-LDP and RSVP detect the fail links at the same time. For fault link recovery, the results show that the CR-LDP protocol is faster than RSVP protocol in terms of recovered links. Unlike the RSVP protocol, the CR-LDP protocol starts using the link immediately after the link being reconnected.



(5a)

(5b)

Figure (7): Utilization of (node12→ node18) link. CR-LDP TE protocol (a) RSVP TE protocol

6 Links Utilization of QoS-Supported MPLS Networks

This section presents performance investigation of MPLS Traffic Engineering signal protocol capabilities to utilize the transmission link under Quality of Service (QoS) conditions. The used QoS algorithms are First-In First-Out (FIFO), Priority Queuing (PQ), Weighted Fair Queuing (WFQ) and Custom Queuing (CQ). The results are represented for the three networks addressed in Section 5 with the same parameters and applications. The average link utilization of the first network under different QoS algorithms is listed in Tables (7)-(9) for low-, medium-, and high-load conditions, respectively. Results related to the second and third networks are given in the Appendix.

Tables (10a)-(10c) list total number of links utilized by the two protocols in the three networks when applying QoS for the three load conditions, respectively. These tables show that the four queuing algorithms have similar effect (in term of utilized links) on MPLS networks operating with CR-LDP TE signal protocol. This is not true when the RSVP TE signal protocol is used.

7 Conclusions

The performance of the MPLS CR-LDP and RSVP Traffic Engineering signal protocols has been evaluated and compared in the term of link utilization with and without applying QoS. Different networks scenarios and different applications, including video conferencing, voice, E-Mail, FTP, HTTP, DB, print and telnet traffic have been.. The main conclusions drawn from this study are

- (i) MPLS network with CR-LDP TE signal protocol has better performance in the term of link utilization. The RSVP reserves certain paths for transmission while the CR-LDP utilizes almost all of the available links.
- (ii) The CR-LDP protocol is even better in terms of link management between uplink traffic and downlink traffic on the same path.
- (iii) The CR-LDP TE signal protocol is faster than RSVP protocol in terms of discovery of recovered links, it starts using the link immediately after the link being reconnected.
- (iv) There is inefficient link utilization with the RSVP protocol in which the reservation of specific links for transmission produces transmission failure and packets drop at high loads.
- (v) The MPLS TE signal protocol capability of link utilization is almost independent of network topology or number of utilized links.
- (vi) Applying QoS improves the performance of RSVP TE signal protocol while the number of utilized links increases. For CR-LDP the same number of links is used before and after applying QoS.

Table (7): Average link utilization of Network 1 operating with QoS under low load condition.

Link	Utilization %							
	CR-LDP				RSVP			
	FIFO	PQ	WFQ	CQ	FIFO	PQ	WFQ	CQ
14→20	70.70	70.36	70.98	70.97	14.90	15.23	15.05	15.12
20 →14	1.72	27.00	31.00	30.79	0.86	0.80	1.06	1.04
18→15	47.98	54.23	45.98	46.01	69.42	69.42	56.71	56.74
15→18	75.37	70.96	70.35	70.33	0.87	0.87	1.28	1.29

18→21	49.18	45.12	49.20	49.27	0.33	0.34	0.74	0.75
21→18	0.85	9.79	1.21	1.31	69.36	69.36	54.44	54.42
19→15	25.72	26.88	27.92	27.97	12.52	12.63	12.65	12.63
15→19	15.014	1.57	14.19	13.98	69.73	69.98	69.96	69.95
19→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18→19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→18	46.88	48.92	44.97	44.90	2.39	2.61	2.41	2.50
18→20	0.00	26.17	21.28	21.18	0.55	0.54	0.55	0.55
20→19	24.08	21.58	26.37	26.42	12.52	12.63	12.65	12.63
19→20	1.72	1.02	9.94	9.82	0.33	0.27	0.52	0.50
21→14	54.13	45.53	53.53	53.51	69.69	69.94	69.95	69.95
14→21	2.64	15.02	2.92	3.02	69.63	69.37	54.45	54.43
21→19	1.80	5.51	1.76	1.76	0.00	0.00	0.00	0.00
19→21	13.31	0.60	4.53	4.44	69.41	69.72	69.44	69.45
21→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→21	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table (8): Average link utilization of Network 1 operating with QoS under medium load condition.

Link	Utilization %							
	CR-LDP				RSVP			
	FIFO	PQ	WFQ	CQ	FIFO	PQ	WFQ	CQ
14→20	70.70	70.97	71.02	70.36	17.13	17.38	66.34	66.32
20→14	30.95	17.39	22.84	22.90	69.92	70.00	66.95	66.95
18→15	23.28	23.95	28.06	31.66	69.52	69.53	67.35	67.39
15→18	70.39	12.33	71.02	70.98	12.30	12.33	12.26	12.26
18→21	49.23	50.00	49.63	49.23	0.00	0.00	12.07	12.07
21→18	2.06	69.32	2.07	10.59	69.31	69.32	1.05	1.16
19→15	52.62	51.74	48.98	55.34	12.13	12.15	0.00	0.00
15→19	14.11	69.46	1.99	1.72	69.43	69.46	68.76	68.71
19→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18→19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→18	21.37	21.90	26.19	21.27	5.06	5.32	66.34	66.32
18→20	21.30	12.33	21.75	22.09	12.30	12.33	0.20	0.20
20→19	49.58	49.41	45.19	49.22	12.07	12.07	0.00	0.00
19→20	9.86	68.44	1.28	1.00	68.93	68.44	66.77	66.77
21→14	53.55	50.61	50.17	49.79	0.50	1.02	14.06	14.02
14→21	6.25	69.40	6.02	18.28	69.37	69.40	1.14	1.25
21→19	4.24	3.71	40.00	7.97	0.00	0.00	0.00	0.00
19→21	4.52	1.02	0.74	0.75	0.50	1.02	2.00	1.95
21→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→21	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table (9): Average link utilization of Network 1 operating with QoS under high load condition.

Link	Utilization %							
	CR-LDP				RSVP			
	FIFO	PQ	WFQ	CQ	FIFO	PQ	WFQ	CQ
14→20	70.45	70.45	70.50	71.05	70.02	28.98	27.20	27.48
20→14	61.84	61.0	62.46	61.20	69.63	69.98	18.03	17.59
18→15	60.82	61.30	62.38	70.39	1.03	69.53	17.29	17.68
15→18	70.39	70.39	70.43	70.39	0.98	69.41	65.92	65.60
18→21	21.26	21.47	21.63	7.07	0.98	1.07	65.91	65.59
21→18	15.96	16.56	15.86	7.07	0.00	68.41	0.00	0.00
19→15	36.83	34.77	36.19	36.74	69.90	21.86	69.56	69.46
15→19	30.24	28.81	29.54	29.41	70.40	19.87	20.40	19.85
19→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18→19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→18	48.51	48.72	48.20	44.42	1.03	8.11	17.29	17.68
18→20	49.27	49.07	48.96	49.31	0.00	68.35	0.00	0.00
20→19	22.08	21.88	22.47	26.99	69.00	20.88	9.92	9.81
19→20	14.39	17.89	14.19	18.32	69.63	6.99	18.03	17.59
21→14	37.18	32.50	37.07	32.39	1.75	13.95	67.73	67.43
14→21	30.63	29.36	29.52	16.96	2.23	69.39	65.87	65.51
21→19	15.00	13.13	13.99	9.98	2.23	0.98	65.87	65.51
19→21	16.19	11.27	15.69	11.42	0.77	12.89	2.38	2.27
21→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→21	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table (10a): Total number of links utilized by the two protocols when applying QoS (low load condition).

Network	TE signal protocol	Total number of utilized links			
		FIFO	PQ	WFQ	CQ
Network 1	CR-LDP	15	16	16	16
	RSVP	15	15	15	15
Network 2	CR-LDP	18	18	18	18
	RSVP	15	16	16	16
Network 3	CR-LDP	20	19	20	19
	RSVP	25	23	23	239

Table (10b): Total number of link utilized by the two protocols when applying QoS (medium load condition).

Network	TE signal protocol	Total number of utilized links			
		FIFO	PQ	WFQ	CQ
Network 1	CR-LDP	16	16	16	16
	RSVP	14	14	13	13
Network 2	CR-LDP	15	15	15	15
	RSVP	20	21	20	20
Network 3	CR-LDP	25	25	25	25
	RSVP	22	23	24	22

Table (10c): Total number of link utilized by the two protocol when applying QoS (high load condition).

Network	TE signal protocol	Total number of utilized links			
		FIFO	PQ	WFQ	CQ
Network 1	CR-LDP	16	16	16	16
	RSVP	15	15	14	15
Network 2	CR-LDP	18	18	18	18
	RSVP	20	17	1	19
Network 3	CR-LDP	22	22	22	22
	RSVP	21	18	20	20

REFERENCES

- [1] A. Hussain, S. Nazeer, T. Abdullah, B. Yaseen and A. Salam "Network Resilience in Multiprotocol Label Switching" Journal of Asian Scientific Research, Vol.2, No.4, PP. 221-227, April 2012.
- [2] B. Forouzan, "Data Communications and Networking", McGraw-Hill Higher Education, 4th Ed., PP. 101-110, 2006.
- [3] Dr. R. Naoum and M. Maswady, "Performance Evaluation for VoIP over IP and MPLS", World of Computer Science and Information Technology Journal, Vol. 2, No. 3, PP. 110-114, May 2012.
- [4] T.J. Shi, G. Mohan, "An Efficient Traffic Engineering Approach Based on Flow Distribution and Splitting in MPLS Networks", Computer Communications, Vol. 29, No. 9, PP. 1284-1291, May 2006.
- [5] A. Bongale, "Analysis of Link Utilization in MPLS Enabled Network using OPNET IT Guru", International Journal of Computer Applications, Vol. 41, No.14, PP. 35-40, March 2012.
- [6] H. Perros, "An Introduction to ATM Network", 1st Ed., Cary, USA, 2001.
- [7] R. Peterkin "A Reconfigurable Hardware Architecture for VPN MPLS based Services", MSc. Thesis, School of Information Technology and Engineering, University of Ottawa, April 2006.
- [8] Y. Lee, Y. Seok, Y. Choi and C. Kim "A Constrained Multipath Traffic Engineering Scheme for MPLS Networks", Electronic Telecommunication Research Institute, 2002.
- [9] S. Shyry and V. Ramachandran, "Finagling Congestion in Selfish Overlay Routing Belittling Link Utilization" , Proc. IEEE, PP. 308-311, November 2010.
- [10] C. Pelsser , O. Bonaventure "Extending RSVP-TE to support Inter-AS LSPs", Proc. CiteSerr, Vol 41, No.5, PP. 122-128, May 2011.
- [11] T. Aziz, N. Islam khan and A. Popescu , "Effect of Packet Delay Variation on Video/Voice over DIFFSERV-MPLS in IPV4/IPV6 Networks", International Journal of Distributed and Parallel Systems, Vol.3, No.1, pp.27-47, January 2012.

- [12] M. Bhandure, G. Deshmukh and Prof. V. J n, “ Comparative Analysis of Mpls and Non -Mpls Network”, International Journal of Engineering Research and Applications, Vol. 3, No. 4, PP. 71-76, August 2013.
- [13] S. Ibrahim, ” Performance Evaluation of Traffic Engineering Signal Protocols in MPLS Network “, M.Sc. Thesis, Al-Nahrain University, April 2013.
- [14] A. Sulaiman and O. Alhafidh” Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering“, International Journal of Computer Networks and Communications Securitik Vol. 2, No. 3, PP. 93 -101, March 2014.
- [15] S. Ibrahim and M. AL-Quzwini, “Performance Evaluation of MPLS TE Signal Protocols with Different Audio Codecs for Voice Application”, International Journal of Computer Applications, Vol. 57, No.1, pp. 56-60, November 2012.
- [16] H. Perros, “An Introduction to ATM Network”, 1st Ed., Cary, USA, 2001.
- [17] R. Peterkin “A Reconfigurable Hardware Architecture for VPN MPLS based Services”, MSc. Thesis, School of Information Technology and Engineering, University of Ottawa, April 2006.
- [18] T. Latif and K. Malkajiri, “Adoption of Voice over Internet Protocol,” Lulea University of Technology, 2007.
- [19] O. Dokun and A. Gift “PDH (Plesiochronous Digital Hierarchy) /SDH-SONET (Synchronous Digital Hierarchy / Synchronous Optical Networking)”, International Journal of Mathematics and Engineering Research, Vol 3, No 1, January 2015.
- [20] A. Kumar and S. G. Thorenoor, “Analysis of IP Network for Different Quality of Service.” In International Symposium on Computing, Communication, and Control (ISCCC), Proc .of CSIT Vol. 1. IACSIT Press, Singapore. 2011.
- [21] P. Ivaniš and D. Drajić “The Simulation Model of Optical Transport System and Its Applications to Efficient Error Control Techniques Design”, Electronic, Vol. 13, No. 2, December 2009.
- [22] K. Januu and R. Deekona,“ OPNET Simulation of Voice Over MPLS With Considering Traffic Engineering”, M.Sc. Thesis, School of Engineering, Blekinge Institute of Technology, Sweden, June 2010.
- [23] J. Evans and C. Filsfils, ”Deploying IP and MPLS QoS for Multiservice Networks”, 1st Ed., Elsevier Inc, San Francisco, USA, 2007.
- [24] V. Alwayn, “Advanced MPLS design and Implementation, Cisco Systems”, Cisco press 201, West 103rd Street Indianapolis, 2001.

- [25] K. Salah and A. Alkhoraidly "An OPNET-Based Simulation Approach for Deploying VoIP", International Journal of Network Management Int. J. Network, DOI: 10.1002, PP. 159–183, 27 January, 2006.

- [26] H. Asif and G. Kaosa, "Performance Comparison of IP, MPLS and ATM Based Network Cores using OPNET", IEEE Computer Society, August, 2006.

- [27] A. Hadi, "Modeling Computer Laboratories in University that Contains Eight Colleges by Using OPNET Software", Journal of Kerbala University, Vol. 7, No.1, PP.108-123, 2009.

- [28] S. Kuribayashi," Proposed Optimal LSP Selection Method in MPLS Networks", International Journal of Computer Networks & Communications Vol.3, No.1, PP. 241-250, January 2011

Appendix: Effect of QoS on the Performance of Networks 2 and 3

Table (A1): Average link utilization of Network 2 operating with QoS (low load).

Link	Utilization %							
	CR-LDP				RSVP			
	FIFO	PQ	WFQ	CQ	FIFO	PQ	WFQ	CQ
14→23	69.78	70.21	70.10	70.21	69.89	70.1	66.09	65.98
23→14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
19→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
25→20	0.22	0.40	1.05	0.31	0.00	0.00	0.00	0.00
20→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→20	69.73	70.37	70.00	70.15	13.04	12.72	14.07	14.03
21→19	0.70	0.83	0.78	0.71	0.00	0.00	0.00	0.00
19→21	0.15	0.23	0.91	0.21	69.48	69.49	64.55	64.55
21→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→21	69.76	70.40	70.05	70.18	0.00	12.72	14.07	14.07
21→24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→21	0.00	0.00	0.00	0.00	2.89	0.00	0.00	0.00
22→14	69.56	69.89	69.76	69.89	70.08	70.16	70.06	70.06
14→22	1.77	2.03	1.91	2.12	70.08	2.29	2.58	2.55
22→21	0.70	0.85	0.79	0.72	0.00	0.00	0.00	0.00
21→22	69.78	70.42	70.09	70.20	70.08	70.16	70.06	70.06
22→24	1.10	1.17	1.15	1.43	2.90	2.29	2.59	2.55
24→22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
22→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→24	69.77	70.20	70.09	70.20	69.89	70.15	66.08	65.98
24→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→19	69.78	70.21	70.10	70.20	69.91	70.18	67.92	67.87
19→24	0.00	0.00	0.00	0.00	69.49	69.50	64.55	0.00
25→15	69.53	69.85	69.74	69.86	69.90	70.18	67.92	67.87
15→25	0.37	0.63	1.94	0.53	69.90	69.50	67.92	64.55
25→19	0.19	0.27	0.95	0.25	69.49	69.50	64.55	64.55
19→25	69.78	70.41	70.10	70.20	13.04	12.72	14.07	14.03
26→15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
15→26	69.73	70.37	70.00	70.15	0.00	0.00	0.00	0.00
26→25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
25→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table (A2): Average link utilization of Network 2 operating with QoS (medium load).

Link	Utilization %							
	FIFO CR-LDP	PQ CR-LDP	WFQ CR-LDP	CQ CR-LDP	FIFO RSVP	PQ RSVP	WFQ RSVP	CQ RSVP
14→23	69.90	70.16	70.21	70.17	1.66	1.47	14.10	14.05
23→14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
19→20	46.14	0.00	0.00	0.00	0.00	69.50	0.00	0.00
20→25	0.00	0.00	0.00	0.00	0.00	57.53	0.00	0.00
25→20	43.22	43.99	44.20	43.40	7.00	14.16	1.30	1.28
20→26	0.00	0.00	0.00	0.00	0.24	0.12	1.10	1.04
26→20	0.27	0.22	1.11	0.31	2.10	0.00	70.08	70.15
21→19	0.00	0.00	0.00	0.00	63.03	0.38	3.05	2.92
19→21	23.88	26.39	26.21	26.70	9.10	70.18	0.00	0.00
21→20	0.00	0.00	0.00	0.00	0.24	57.64	1.10	1.03
20→21	46.40	44.19	45.30	43.70	0.00	0.00	70.12	70.19
21→24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→21	0.00	0.00	0.00	0.00	70.10	70.21	0.00	0.00
22→14	69.57	69.77	69.77	69.79	70.07	70.17	70.12	70.11
14→22	0.00	0.00	0.11	0.00	70.07	70.18	56.88	56.68
22→21	0.00	0.00	0.00	0.00	63.28	58.02	4.14	3.95
21→22	69.80	70.07	70.10	69.84	0.00	0.00	70.12	70.19
22→24	0.00	0.00	0.00	0.50	6.82	12.19	52.74	53.67
24→22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
22→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→24	69.90	70.16	70.20	70.16	1.66	1.47	14.10	14.05
24→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→19	69.90	70.16	70.20	70.16	8.47	13.65	66.068	66.26
19→24	0.00	0.00	0.00	0.50	70.03	69.50	0.00	0.00
25→15	69.64	69.81	69.84	69.82	70.13	70.26	68.92	68.78
15→25	69.78	70.07	70.08	70.22	70.14	14.03	1.30	1.28
25→19	23.90	26.43	26.23	26.86	63.03	0.00	0.00	0.00
19→25	69.90	70.17	70.21	70.31	2.10	14.03	68.92	68.88
26→15	0.00	0.00	0.00	0.00	0.24	0.12	1.10	1.04
15→26	0.27	0.21	1.08	0.30	0.00	0.00	70.09	70.15
26→25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
25→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table (A3): Average link utilization of Network 2 operating with QoS (high load)

Link	Utilization %							
	CR-LDP				RSVP			
	FIFO	PQ	WFQ	CQ	FIFO	PQ	WFQ	CQ
14→23	60.07	10.12	8.32	69.49	28.33	15.51	35.20	35.71
23→14	0.00	0.00	0.00	0.00	14.28	0.38	69.82	69.66
20→19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.13
19→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.69
20→25	0.00	0.00	0.00	0.12	69.48	0.00	0.00	0.00
25→20	49.30	49.38	44.20	10.20	0.40	0.00	0.40	0.40
20→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→20	0.22	0.59	1.11	69.25	69.93	69.80	17.66	16.02
21→19	21.47	21.55	21.68	6.47	0.00	0.00	53.99	53.87
19→21	21.25	21.64	26.21	4.54	0.00	0.00	0.00	0.00
21→20	0.00	0.00	0.20	0.19	69.48	0.00	0.00	0.00
20→21	49.50	49.91	45.30	70.47	69.97	69.51	18.05	53.87
21→24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→21	0.00	0.00	0.00	0.00	0.00	69.80	0.00	16.41
22→14	70.05	70.34	70.33	70.36	69.48	70.41	18.05	16.42
14→22	69.93	70.20	0.11	18.20	69.63	12.14	54.00	0.00
22→21	21.50	21.68	21.88	6.65	69.48	0.00	54.00	53.87
21→22	70.31	70.28	70.10	6.65	69.97	0.00	18.05	0.00
22→24	48.70	48.88	48.71	11.83	0.00	69.51	0.00	0.00
24→22	0.00	0.00	0.00	0.00	0.00	0.38	0.00	0.00
23→22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
22→23	0.00	0.00	0.00	0.00	0.00	12.51	0.00	0.00
23→24	6.11	10.17	8.37	69.49	28.33	15.51	35.20	35.71
24→23	0.00	0.00	0.00	0.00	14.29	12.60	69.82	69.82
24→19	53.75	57.14	57.04	70.66	28.33	70.81	35.20	35.71
19→24	0.00	0.00	0.00	0.00	14.29	70.81	69.82	69.82
25→15	70.06	70.16	70.23	70.15	0.00	70.81	70.44	70.26
15→25	70.28	70.20	70.08	14.61	14.29	69.80	70.22	70.22
25→19	21.26	21.65	21.62	4.68	14.23	12.51	69.83	69.22
19→25	70.26	70.36	70.21	70.37	28.33	0.00	70.45	70.22
26→15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
15→26	0.21	0.55	1.09	69.25	69.48	0.00	17.65	16.02
26→25	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.0
25→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table (A4): Average link utilization of Network 3 operating with QoS (low load)

LINK	Utilization %							
	RSVP				CRLDP			
	FIFO	PRI	WFQ	CUST	FIFO	PRI	WFQ	CUST
12→18	70.52	71.15	55.22	44.40	12.78	12.73	13.44	0.64
18→12	0.52	0.54	0.53	0.55	0.63	12.79	0.63	0.63
12→20	0.54	0.54	0.53	12.70	0.19	0.20	0.23	12.40
20→12	0.60	0.69	0.63	0.62	48.12	48.01	47.85	43.48
12→21	0.11	0.17	12.30	0.15	70.25	70.19	70.22	70.18
21→12	0.57	12.72	0.57	0.57	12.17	0.00	12.17	0.00
12→24	0.52	0.54	0.53	0.54	0.63	12.79	0.63	0.63
24→12	70.52	71.15	55.21	44.39	12.76	12.73	13.44	0.64
14→17	70.89	70.54	66.83	66.76	0.00	0.00	0.00	0.00
17→14	12.06	0.00	0.00	0.00	0.00	0.00	0.47	0.13
14→22	0.60	0.69	0.63	0.62	70.29	70.22	70.29	70.84
22→14	1.04	1.04	1.04	13.21	0.21	0.20	0.55	12.43
14→23	0.52	0.54	0.53	0.54	0.65	13.04	0.65	0.65
23→14	70.52	71.15	55.22	44.39	13.02	12.98	13.70	0.65
14→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→18	70.88	70.53	66.82	66.75	22.30	22.21	22.45	27.37
18→17	12.56	0.50	0.52	0.51	0.00	0.00	0.79	0.15
18→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
21→20	12.06	0.00	0.00	0.00	0.00	0.00	0.48	0.13
20→21	70.88	70.54	66.83	66.75	0.00	0.00	0.00	0.00
21→23	0.11	0.17	12.30	0.15	70.12	70.06	70.08	70.06
23→21	0.57	12.72	0.57	0.57	12.17	0.00	12.17	0.00
22→17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→22	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
22→24	0.57	12.72	0.57	0.57	12.42	0.00	12.42	0.00
24→22	0.11	0.16	12.30	0.15	70.18	70.18	70.22	70.18
23→17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18→24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→20	0.60	0.69	0.63	0.62	48.05	48.08	47.93	43.66
20→26	0.54	0.54	0.53	12.70	0.21	0.22	0.25	12.66
26→21	0.00	0.00	0.00	0.00	22.37	22.28	22.53	27.45
21→26	0.51	0.50	0.52	0.51	0.00	0.00	0.00	0.00

Table (A5): Average link utilization of Network 3 operating with QoS (medium load).

LINK	Utilization %							
	RSVP				CR-LDP			
	FIFO	PQ	WFQ	CQ	FIFO	PQ	WFQ	CQ
12→18	1.09	0.19	1.18	13.31	1.11	1.15	1.106	13.23
18→12	14.1	1.97	1.82	1.82	1.08	13.16	1.02	13.17
12→20	0.00	0.00	12.17	0.00	1.00	1.00	1.00	1.03
20→12	0.11	0.12	0.00	0.00	2.56	2.56	2.34	2.74
12→21	13.17	0.48	1.02	1.02	12.22	12.32	12.30	0.17
21→12	3.83	4.07	4.20	3.83	70.31	70.06	70.46	70.06
12→24	14.09	1.97	1.82	1.82	1.08	13.16	1.02	13.17
24→12	1.09	0.19	1.18	13.31	1.11	1.15	1.11	13.23
14→17	70.55	70.51	55.37	66.79	0.00	0.00	0.00	0.00
17→14	68.89	57.73	43.67	43.65	22.12	22.09	21.97	22.25
14→22	1.13	13.37	13.22	1.12	7.05	7.22	6.94	7.40
22→14	1.69	13.43	14.09	1.77	49.13	49.12	49.32	49.00
14→23	14.09	1.97	1.82	1.82	1.10	13.42	1.04	13.43
23→14	1.09	0.19	1.18	13.31	1.12	1.17	1.12	13.49
14→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→18	70.57	71.13	68.00	67.78	4.58	4.75	4.70	4.76
18→17	70.57	71.17	45.57	45.41	70.27	70.24	70.29	70.23
18→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
21→20	68.89	57.74	43.67	43.65	22.19	22.16	22.05	22.31
20→21	70.54	4.07	55.36	66.79	0.11	0.11	0.11	0.11
21→23	13.17	0.48	1.02	1.02	12.22	12.32	12.30	0.17
23→21	3.83	0.00	4.21	3.83	70.56	70.19	70.81	70.18
22→17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→22	0.00	0.48	0.00	0.00	0.00	0.00	0.00	0.00
22→24	3.83	4.06	4.21	3.83	70.57	70.18	70.80	70.18
24→22	13.17	0.00	1.02	1.02	12.47	12.57	12.55	0.18
23→17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18→24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→20	0.11	0.12	0.00	0.00	2.69	2.58	2.37	2.76
20→26	0.00	0.00	12.17	0.00	1.00	1.00	1.02	1.04
26→21	1.02	13.26	13.13	1.03	4.52	4.69	4.62	4.70
21→26	1.69	13.43	1.93	1.77	48.22	48.22	48.40	48.06

Table (A6): Average link utilization of Network 3 operating with QoS (high load).

LINK	Utilization %							
	RSVP				CR-LDP			
	FIFO	PRI	WFQ	CUST	FIFO	PRI	WFQ	CUST
12→18	12.05	0.00	0.00	0.00	0.32	0.62	2.31	12.43
18→12	13.38	27.23	19.02	31.33	0.00	0.00	0.00	0.00
12→20	0.00	0.00	0.00	12.17	0.00	0.00	0.00	0.00
20→12	6.92	7.71	10.77	10.13	2.90	13.10	5.55	3.62
12→21	2.41	2.15	2.33	2.40	0.46	1.36	2.44	.68
21→12	0.00	0.00	0.00	0.00	70.10	70.11	70.16	70.50
12→24	13.38	27.23	19.03	31.34	12.10	0.00	0	0
24→12	12.05	0.00	0.00	0.00	0.32	0.61	2.31	12.43
14→17	70.84	70.51	54.63	54.64	10.00	10.00	22.01	10.05
17→14	1.50	13.68	42.43	42.40	24.84	23.03	22.32	23.19
14→22	9.33	1.00	25.24	12.33	7.40	25.90	14.01	11.89
22→14	69.25	57.69	20.76	24.32	46.18	48.28	49.01	47.50
14→23	13.38	27.23	19.02	31.33	0.00	0.00	0.00	0.00
23→14	12.05	0.00	0.00	0.00	0.33	0.62	2.33	12.68
14→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→18	70.84	70.54	68.1	56.67	14.51	22.66	30.56	18.31
18→17	70.75	71.37	63.19	54.56	70.80	71.08	71.11	70.45
18→20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
20→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
21→20	1.5	13.68	42.43	42.41	24.97	23.65	22.50	23.26
20→21	70.84	70.51	54.63	54.63	10.04	9.96	22.27	10.08
21→23	2.41	2.15	2.33	2.40	0.46	1.36	2.44	0.68
23→21	0.00	0.00	0.00	0.00	70.23	70.26	70.33	70.34
17→22	0.00	0.00	0.00	0.00	00.00	0.00	0.00	0.00
22→24	0.00	0.00	0.00	0.00	70.23	70.38	70.33	70.85
24→22	2.41	2.15	2.33	2.40	0.47	1.36	2.46	0.69
23→17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
17→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
23→26	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→23	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
24→18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18→24	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
26→20	6.92	7.71	10.77	10.13	2.92	13.38	5.57	3.65
20→26	0.00	0.00	0.00	12.16	0.25	0.25	0.25	0.25
26→21	2.43	2.30	14.48	2.21	4.52	12.82	8.58	8.29
21→26	69.26	57.70	20.76	12.16	46.1	48.24	48.99	47.34

Efficient On-Line Traffic Policing for Confidence Level based Traffic Model

Lie Qian

*Dept. of Chemistry, Computer & Physics Science, Southeastern Oklahoma State University, Durant, OK,
USA*

lqian@se.edu

ABSTRACT

On-line traffic, such as conversational call, live video, serves a large group of applications in the internet now days. An important feature of on-line traffic is that they are not pre-recorded and no exact information about each session's traffic is known before the traffic happens. S-BIND (Confidence-level-based Statistical Bounding Interval-length Dependent) traffic model was proposed to characterize such traffic for QoS admission (GammaH-BIND) and policing purpose. A state-dependent token bucket based statistical regulator was proposed to police the traffic using S-BIND parameters. However, the proposed regulator can output traffic within the expected S-BIND parameters if the input traffic is random or is just trying to transmit large amount of traffic without exploiting the regulator's token bucket design. In this paper, the author shows that if the source of the traffic understands the bucket's behavior, it can tune the traffic and cause significant violations in the regulator's output traffic. A new design of state-dependent token bucket for the regulator is proposed in this paper to remove such potential problem and an optimization algorithm is given to improve the regulator's efficiency by removing redundant token buckets in the regulator.

Keywords: Traffic Model, QoS, Policing

1 Introduction

On-line traffic, such as conversational call, live video, serves a large group of applications in the internet now days. Most of such on-line traffic are delay sensitive and have Quality of Service (QoS) requirements. QoS refers to the capability of a network to provide better service to selected network traffic or flows [1]. QoS requirements can be described by parameters such as delay, packet loss rate, jitter, and etc.

To fulfil QoS requirements, network cannot allow unlimited amount of traffic enter the network without admission control. Admission control algorithms are used to decide if a new incoming traffic flow will affect the QoS of the existing traffic in the network while it trying to receive its expected QoS. Proposed admission control algorithms can be classified into two categories: measurement-based and traffic descriptor-based admission control [1]. Measurement-based admission control algorithms [3-6] measure the traffic condition in the network and estimate the QoS in the network with the new arriving traffic flows. The admission decisions are made based on such estimation. Such measuring requires significant changes in the network's architecture. Traffic descriptor-based admission controls [7-12] allow the

network to make admission control decisions based on existing and new coming traffic's characterizations (parameters), which are used to calculate the QoS in the network that can be received by the existing and the new arriving traffic flows. This kind of admission control relieves network from constant traffic measuring in the network, which could be a significant burden to the network, and requires less modification in the network architecture. Furthermore, with the introduction of DiffServ QoS architecture [13], where the per-flow information can be maintained in a centralized QoS controller (bandwidth broker) [14, 15], traffic descriptor-based admission control process can be decoupled from routers to solve scalability problems in routers.

The effectiveness of the traffic descriptor-based admission control depends heavily on the accuracy of the traffic models that are used to characterize the existing and incoming new traffic. Among the proposed traffic models [1, 16-24], Confidence-level-based Statistical Bounding Interval-length Dependent (S-BIND) [1] model doesn't require pre-existing traffic traces to get the parameters and thus could be applied to On-Line traffic. GammaH-BIND admission control algorithm was proposed in [1] to perform admission control based on S-BIND traffic model parameters. After being admitted, network traffic described by S-BIND parameters need to be regulated at the entrance of the network to ensure that the traffic going through the network does follow its declared S-BIND parameters. In [2], the authors propose a state-dependent token bucket based statistical regulator to police the S-BIND network traffic. The regulator is composed of a series of state-dependent token buckets. Each token bucket is established based on the parameters of on linear section on the S-BIND's constraint function. However, the regulator proposed in [2] could output traffic violating the S-BIND's parameters under certain circumstances when the source understands the regulator's design and tunes its traffic to get the worst case from the token buckets in the regulator. Also setting up a token bucket for each linear section could be redundant when some buckets could be stricter than the others and make them unnecessary in the regulator.

This paper analyses the real constraint function for the state-dependent token buckets proposed in [2] and their worst cases which could generate output traffic violating the S-BIND parameters. Based on the analysis, a new design of the state-dependent token buckets is first proposed to output the traffic within S-BIND limit even in the worst case. Secondly an optimization algorithm will be proposed to remove the redundant token buckets in the regulator to improve the regulator's efficiency. The empirical analysis presented in this paper show that the new token buckets always output traffic within the S-BIND parameter's limit and the optimization algorithm could detect redundant token buckets in the regulator.

The remainder of this paper is organized as follows. The related works in traffic models and traffic regulating are discussed in Section 2. Section 3 presents the worst case analysis of the token buckets, the new token bucket design and the optimization algorithm. The empirical analysis results are demonstrated in Section 5. The conclusions are given in Section 6.

2 Related works

In this section, a brief review of the network traffic models and policing is given. First let's define the network model used in this paper composed of a centralized traffic controller in a network domain. The traffic controller uses traffic admission processes to admit new traffic going through the domain based on the new traffic's descriptors (parameters) while ensuring all existing traffic's QoS in the domain. Ingress edge routers are the routers through which the network traffic enter the domain. After the new traffic is

admitted, regulators need to be deployed at the ingress edge routers to ensure that the traffic behave as described in the admission control process

2.1 Confidence-level-based Statistical BIND (S-BIND) traffic model

Among traffic descriptors, binding traffic models bound the traffic volume. Traffic constraint function, denoted as $b(t)$, is the essential part for binding traffic models. A network traffic flow is said to be bounded by $b(t)$ if during any interval of length of u , the amount of traffic transmitted by this flow is less or equal to $b(u)$. Other than (σ, ρ) pair [21, 22], $(X_{min}, X_{ave}, I, S_{max})$ model proposed in [7], and Bounding Interval-dependent (BIND) based models are proposed [16, 23, 24], D-BIND [16] is a traffic model specifying the maximum arrival rates for several time intervals known as multiple rate interval pairs. D-BIND works well for deterministic bounding and off-line traffic, but is not suitable for on-line traffic. For on-line traffic other than video, bounding the transmission in each interval with the worst case rate estimated from the traffic behavior properties may compromise the effectiveness of D-BIND. In [1], authors developed a new Confidence-level-based Statistical BIND (S-BIND) traffic model. The S-BIND model defines p time interval rate pairs as:

$$\{(R_k, I_k) \mid k = 1, \dots, p\} \quad (1)$$

where, $I_1 < I_2 < \dots < I_{k-1} < I_k$. I_k denotes the time interval length, and R_k is the rate, at which the flow is allowed to send in any period of I_k statistically. In S-BIND, random variable S_k is defined as:

$$S_k(a) = \text{prob}\left(\frac{A_j[t, t+I_k]}{I_k} \leq a\right), \forall t \geq 0 \quad (2)$$

Here, $A_j[t_1, t_2]$ denotes the amount of arrivals in traffic flow j within time interval $[t_1, t_2]$. S_k reflects the distribution of flow's transmission rate over time interval I_k and has density function $s_k(a)$. For each time interval I_k , R_k is defined in S-BIND by using random variable S_k 's density function $s_k(a)$ as following:

$$\int_0^{R_k} s_k(t) dt = \varepsilon \quad (3)$$

When $\varepsilon=1$, R_k will be the same as in D-BIND. The smaller ε we set, the smaller R_k we will get, and the higher network utilization can be expected in admission control because more traffic will be admitted. For different kinds of on-line traffic such as conversation, videoconference, high motion video, low motion video, game data and etc., S-BIND parameters can be pre-defined with different confidence levels through experiments or statistical data analysis.

Along with GammaH-BIND admission algorithm developed in [1], S-BIND can achieve maximum valid network utilization for both low bursty and high bursty traffic.

2.2 Token Bucket Based Statistical Regulator

After a network traffic flow being admitted by the domain's controller based on the flow's descriptors, the traffic flow needs to be monitored during its life time to ensure that it doesn't violate its claimed traffic descriptor by sending too much data into the domain. Regulators at the ingress router are responsible for this kind of monitoring. The traffic flow violating its claimed descriptor could be disconnected or its excessive data packets could be dropped at the ingress routers.

Most known policing mechanisms, such as Leaky Bucket, Token Bucket, the Triggered Jumping Window [25], Dual Leaky Bucket [26], BLLB [27], FBLLB [28] cannot handle statistical traffic models, such as S-BIND, where the traffic rates are allowed to exceed the parameters statistically. The authors in [2] developed a Token Bucket Based Statistical Regulator. Multiple state-dependent token buckets with dynamic token generation rates are cascaded together to regulate S-BIND traffic. One bucket is deployed for each linear segment in the constraint function $b(t)$ derived form S-BIND traffic model. Each bucket handles packets statistically. A state diagram is given in **Figure 1** to show the bucket’s behavior.

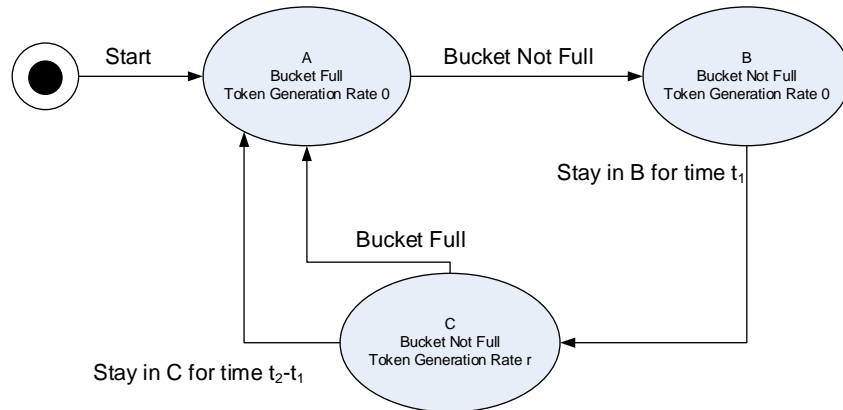


Figure 1: Token Bucket’s Behavior

For each linear segment in the constraint function $b(t)$, it has two end points, one at (t_1, b_1) , and one at (t_2, b_2) , where $t_1 < t_2$, $b_1 \leq b_2$. A state-dependent token bucket corresponding to this segment has bucket depth b_1 , and the token generation rates $r = (b_2 - b_1) / (t_2 - t_1)$. In the example shown in **Figure 2**, the segment for Bucket1 has parameters: $t_1 = a$, $t_2 = b$, $b_1 = c$, $b_2 = d$. The segment for Bucket2 has parameters: $t_1 = b$, $t_2 = f$, $b_1 = d$, $b_2 = e$.

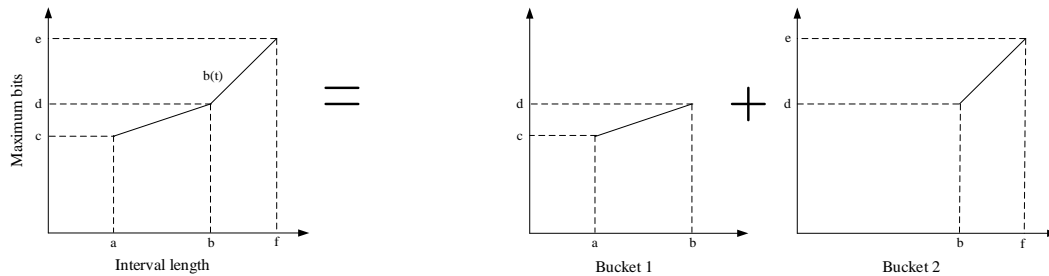


Figure 2: Cascade of Token Buckets for Non-Concave Constraint Function

Different from traditional deterministic token buckets which drop incoming packets when there is not enough token left in the bucket, regulator proposed in [2] is allowed to forward packets even when the token is not enough statistically based on the confidence level specified in S-BIND traffic model. When a packet p with size s needs to be transmitted while the token left in bucket is $t < s$, the transmission probability of the packet is calculated as (4).

$$P_{transmit} = \begin{cases} (1 - \varepsilon) - \frac{t_{neg}}{t_{neg} + t_{pos}} & \text{if } \frac{t_{neg}}{t_{neg} + t_{pos}} < (1 - \varepsilon) \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

In (4), the transmitting probability mainly depends on the variables t_{neg} and t_{pos} , while ε is a confidence level parameter from S-BIND traffic model, which should be a constant for the life time of the bucket. t_{neg} is counted as the time when the token bucket has negative amount of token and t_{pos} is calculated as the total time minus t_{neg} .

3 Efficient Token Bucket Based Statistical Regulator Design

In this section, the author first derives the complete constrain function for each token bucket in the statistical regulator proposed in [2], then proposes a new bucket design and an optimization algorithm to remove the redundant token buckets to reduce the ingress routers' policing burden.

3.1 Constrain Function for Each Token Bucket

The regulator proposed in [2] is composed of a series of token buckets, one for each linear section on the constrain function derived from S-BIND traffic model. Let's say we have a token bucket B following the linear section between points (t_s, b_s) and (t_e, b_e) on the constrain function diagram as shown in Figure 3. All traffic of this flow need pass bucket B to be admitted into the domain (of course, also need pass all other token buckets in the same regulator). Here a question we are facing is what the output traffic will like under different time intervals.

Formally, let $A_j[t_1, t_2]$ denote the total number of bits sent by flow j between time t_1 and t_2 . Flow j is bounded by constraint function $b(t)$ if $A_j[t, t+u] \leq b(u)$, for all $t, u > 0$. Based on the token bucket's behavior state diagram in Figure 2, let's discuss the maximum volume of traffic could be forwarded in bucket B within any time interval $t_1 \leq \Delta t$, where $\Delta t = t_e - t_s$. We consider the following 3 scenarios:

Scenario 1: t_1 starts in state A. Immediately before t_1 starts, the token bucket shifts its state from C to A and have a full bucket of token (bucket size is b_s). Therefore during t_1 , b_s amount of traffic could be forwarded at least and the token bucket shift to state B immediately after t_1 starts. However, state B requires the token bucket stay in state B for time length t_s with no new token generated. Let's say, in the worst case, t_1 is greater than t_s and before the end of t_1 the state shifts to C, in which tokens are generated at the rate of $r = \Delta b / \Delta t$, where $\Delta b = b_e - b_s$. Because t_1 is less than Δt , which is the time the bucket need to stay in state C to achieve maximum token generated, the bucket will remain in state C at the end of t_1 . Therefore, at the end of t_1 , in the worst case, the token bucket is still in state C and the total amount of traffic delivered during t_1 is $b_s + \Delta b = b_e$.

Scenario 2: t_1 starts in state B. In order to get the worst scenario, we assume that t_1 starts at the very end of state B (so that more token could be generated very soon after switching to state C) and the token volume left in the bucket is $b_s - \varepsilon$, where ε is a very small non zero value (could be the size of the smallest packet in the network). After t_1 starts, in the worst case, the token bucket immediately switches to state C and generates token in the rate of $r = \Delta b / \Delta t$ for Δt time, i.e. generate Δb traffic and at the end of t_1 the token bucket becomes full and switches to state A. The consumed token volume during this period is $b_s - \varepsilon + \Delta b + b_s = b_e + b_s - \varepsilon$ which has upper bound of $b_e + b_s$.

Scenario 3: If t_1 starts during state C, the token generated before the token bucket is full is less than Δb and the bucket could become full when the state switch to A. The token generated is $\Delta b + b_s = b_e$.

Among the 3 scenarios above, it is obvious that scenario 2 is the worst case in which the token generated is bounded by

$$b(t_1) = \begin{cases} b_s + \frac{\Delta b}{\Delta t} t_1 & \text{if } t_1 < \Delta t \\ b_e + b_s & \text{if } t_1 = \Delta t \end{cases} \quad (5)$$

In scenario 2, after t_1 ends in the worst case, the bucket will stay in state B with no token generated (i.e. no traffic can be forwarded) for at least t_s amount of time, which gives us the bound for time interval $\Delta t + t_s = t_e$ as second part in (6) below.

$$b(t) = \begin{cases} b_s + \frac{\Delta b}{\Delta t} t & \text{if } t < \Delta t \\ b_e + b_s & \text{if } t \geq \Delta t \text{ and } t \leq t_e \end{cases} \quad (6)$$

Therefore for $t \leq t_e$, we can have the constraint function for a linear segment B depicted in the Figure 3 below.

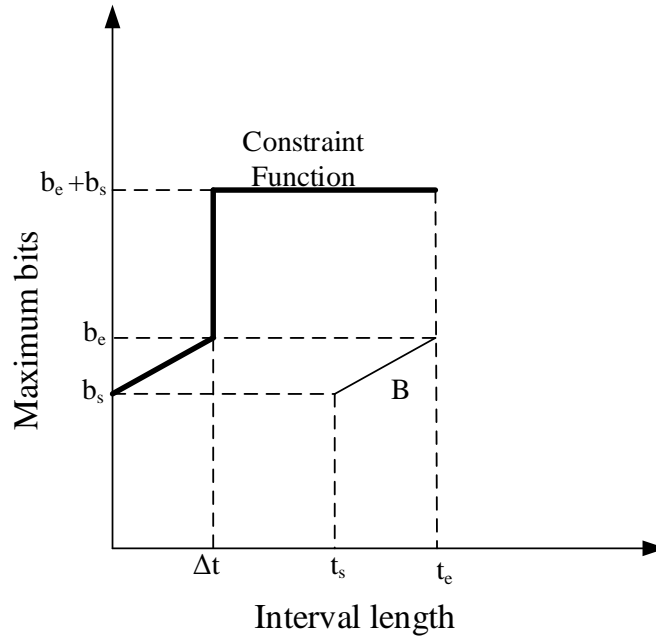


Figure 3: Constraint Function for One Token Bucket in $[2] t \leq t_e$

For the time interval t that is greater than t_e , its first t_e amount of time will send in the worst case $b_e + b_s$ amount of traffic as shown in Figure 3. After that, the bucket will come back to the beginning of scenario 2 and get ready to shift to state C. At this moment, the tokens in the bucket has been counted in $b(t_e) = b_e + b_s$ already. Therefore only the newly generated tokens in state C will be counted and added to the constraint function. The token generated (i.e. traffic allowed to be forwarded) in the period of the second period of t_e is only $\Delta b + b_s = b_e$, in which Δb is the amount of tokens generated in state C with rate $r = \Delta b / \Delta t$ and b_s is the amount of tokens generated when the bucket switches to state A. Put all rounds together, we can get the general constraint function for the linear section between (t_s, b_s) and (t_e, b_e) as below in (7) and depicted in Figure 4.

$$b(t) = \begin{cases} b_s + \left\lfloor \frac{t}{t_e} \right\rfloor b_e + \frac{\Delta b}{\Delta t} t & \text{if } t \% t_e < \Delta t \\ b_s + \left(\left\lfloor \frac{t}{t_e} \right\rfloor + 1 \right) b_e & \text{if } t \% t_e \geq \Delta t \end{cases} \quad (7)$$

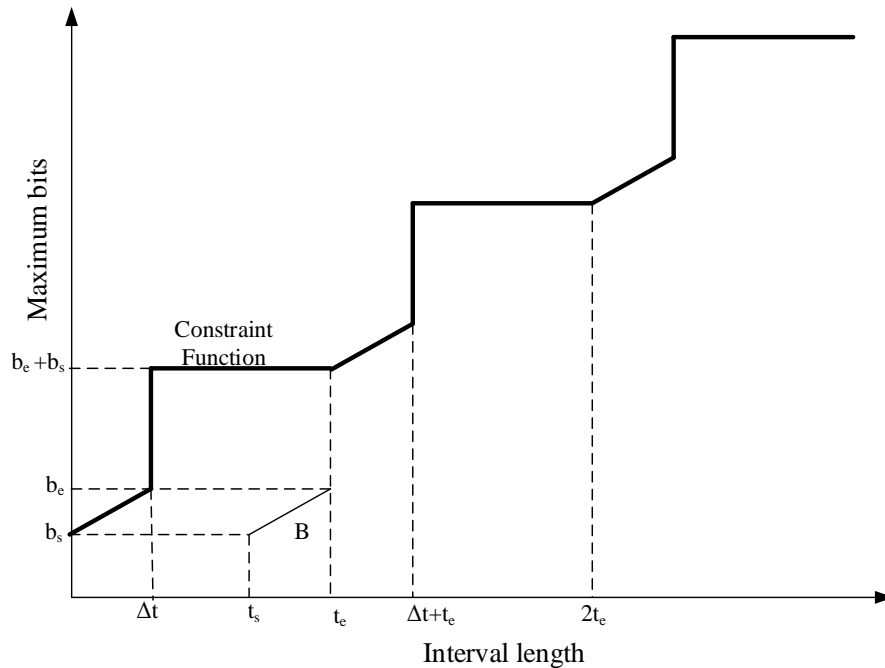


Figure 4: Constraint Function for One Token Bucket in [2]

3.2 Token Bucket Based Statistical Regulator Optimization Algorithm

In this subsection, a new state dependent token bucket is proposed to have tighter constraint function compared to [2], which is analyzed in subsection 3.1. This newly designed token bucket's token generation behavior could be summarized in Figure 5, where Δt is the difference between t_e and t_s of the corresponding linear segment between (t_s, b_s) and (t_e, b_e) in the S-BIND model. The token bucket for this linear segment has bucket size of b_s . The initial state of the token bucket is state A1 with full bucket of tokens and 0 token generation rate. The first difference here compared to the design in [2] is that after state B, the bucket will go back to state A then to B for one more round before it goes to state C. Therefore, 2 more states are added to separate different visits to states A and B. Now state A is divided into states A1 and A2; B is divided into B1 and B2. The second difference is that the bucket switches to state B1 or B2 from A1 or A2 respectively only after the bucket is empty. By doing this, the starting of state B1 or B2 are postponed compared to [2] which can reduce the traffic crowded at the transition time between B2 and C under the worst case as described in scenario 2 in subsection 3.1. The third change is in the transition from state C to A1. If the transition is triggered by the volume of tokens in the bucket in C reaching b_s , no token needs to be added. If the transition is triggered by the expiration of Δt , the volume of tokens need to be added during the transition, noted as b_{jump} , following the formula (8).

$$b_{jump} = \begin{cases} b_s - \Delta b & \text{if } \Delta t < t_s \\ b_s - t_s r & \text{if } \Delta t \geq t_s \end{cases} \quad (8)$$

where Δb is the difference between b_s and b_e , $r = \Delta b / \Delta t$. With this new design, we can see that after the transition from C to A1, the bucket is not necessarily full. The reduction in the b_{jump} from b_s in [2] helps to give a tighter constraint function.

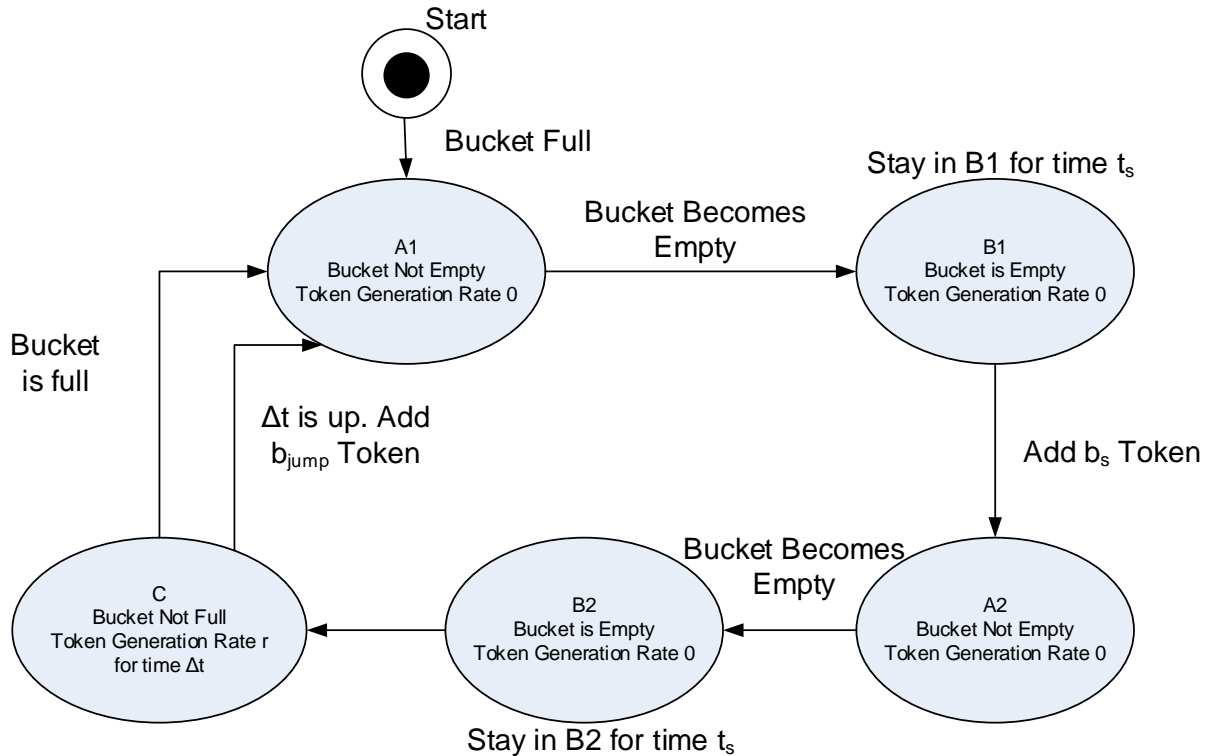


Figure 5: New Token Bucket's Behavior

Based on the new design, the maximum amount of consumed token cannot exceed b_s for any time interval less or equal to t_s . Let's discuss the constraint function for the time interval t less or equal to t_s under following 3 scenarios.

Scenario 1: We have a full bucket of token (b_s in total) in state A2 and time interval t starts. Under this scenario, because the bucket will generate no token for consumption for t_s amount of time after the bucket is empty, the time interval t cannot reach state C for any new token to be generated. The amount of traffic that can be forwarded is limited by the volume of token available in state A2, which is bounded by the bucket size b_s .

Scenario 2: We have an empty bucket at the beginning of state C and the time interval t starts. If Δt is greater than t_s , time interval t will end before the switching to A1 happen and the generated tokens are limited within Δb . If Δt is less than t_s , second case of b_{jump} in (8) could happen and the overall generated tokens are $\Delta b + b_{jump} = \Delta b + b_s - t_s r < b_s$. That's because $t_s r > \Delta t r = \Delta b$. Therefore the volume of token could be generated within the time interval t is still limited by the greater one between b_s and Δb .

Scenario 3: This scenario is trivial, if the time interval t starts in state A1, the bucket has to wait at least t_s amount of time in B1 for the next token to be added.

Now let's discuss the tokens generated in the next Δt amount of time after the end of the first period of t_s just discussed.

Following scenario 1, the next Δt amount of time in state C, Δb tokens could be generated in the worst case under rate r , which bounds the tokens in time interval $t_e = t_s + \Delta t$ within $b_s + \Delta b = b_e$. At the end of t_e , b_{jump} could happen in the worst case and the scenario go back to the beginning of scenario 1. Before that the total tokens generated in the period of t_e is $b_e + b_{jump}$.

Following scenario 2, the next Δt amount of time is spent in state C and A1. In the worst case the whole period of t_e could span the state C and A1 altogether (include the first t_s amount of time discussed in scenario 2). State C generates $\Delta b + b_{jump}$. At the end of A1, b_s is added. In total, $\Delta b + b_{jump} + b_s = b_e + b_{jump}$. After that, the scenario go back to the beginning of scenario 3.

Based on the discussion above, we can depict the constraint function for linear segment B as below in Figure 6. Compare to Figure 4, this newly designed regulator's constraint function is significantly tighter.

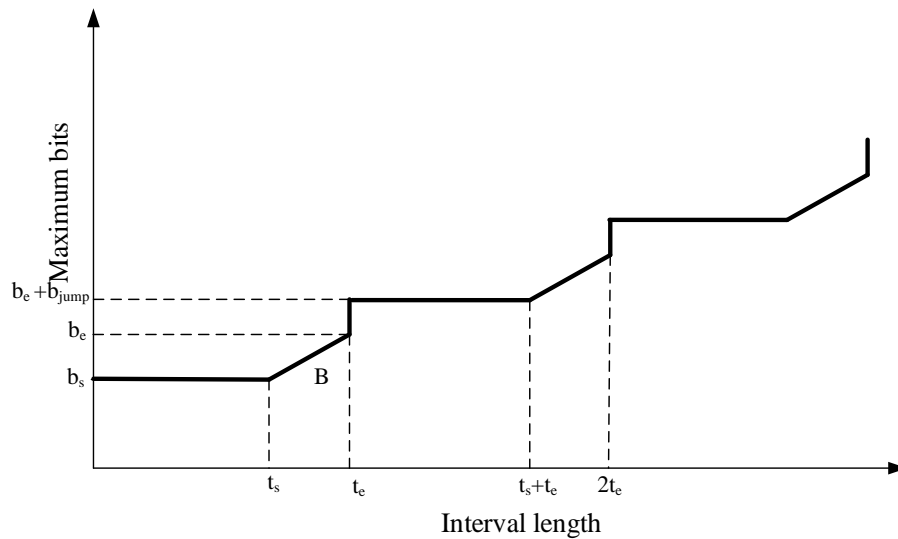


Figure 6: New Token Bucket Constraint Function

Based on the constraint function depicted in Figure 6, we can get the general constraint function for the linear section between (t_s, b_s) and (t_e, b_e) as below.

$$b(t) = \begin{cases} b_s + \left\lfloor \frac{t}{t_e} \right\rfloor (\Delta b + b_{jump}) & \text{if } t \% t_e < t_s \\ b_s + \left\lfloor \frac{t}{t_e} \right\rfloor (\Delta b + b_{jump}) + (t \% t_e - t_s)r & \text{if } t \% t_e \geq t_s \end{cases} \quad (9)$$

3.3 Remove Redundant Buckets

After having the complete constraint function (9) for a given token bucket in this new design, we can take a look at the token buckets needed in the regulator. Based on the original design in [2], one token bucket is setup for each linear segment on the constraint function of the S-BIND descriptor. In reality, because of convex segments in $b(t)$, it is possible that a bucket, say B, has its constraint function below another bucket C's constraint function at all time. In another word, bucket B's output is always smaller than the amount of traffic allowed by bucket C at any time interval. In this case, there is no need for bucket C and we can reduce the traffic policing burden in the regulator by removing C's bucket to be more efficient in resource consuming.

Here is a new method used to decide when a token bucket is redundant. For a token bucket B' for segment from point (t'_1, b'_1) to (t'_2, b'_2) , if there exists one bucket B for the segment between (t_1, b_1) and (t_2, b_2) , we can remove B' in our regulator if and only if:

- B' 's linear rate is higher than B , i.e. $\frac{b'_2 - b'_1}{t'_2 - t'_1} > \frac{b_2 - b_1}{t_2 - t_1}$ AND
- B' 's segment is somewhere after B 's in the overall $b(t)$ derived from multiple rate interval pairs, i.e. $t'_1 > t_2$ AND
- B' 's constraint function $b_{B'}(t)$ is above B 's function anywhere between t'_1 and t'_2 , i.e. $\forall t, \text{ where } t'_1 \leq t \leq t'_2, b'_1 + (t - t'_1) \frac{b'_2 - b'_1}{t'_2 - t'_1} \geq b_B(t)$ is true, where $b_B(t)$ follows (9).

For example in Figure 7, after we have a bucket for B , segment C doesn't require an extra bucket in policing because it is totally above $b_B(t)$. However, if we have a segment D instead of C , then we still need a bucket for D to properly regulate the traffic. By using the method above, after admitting one flow, the network domain can calculate and setup only the necessary buckets to regulate the incoming traffic efficiently.

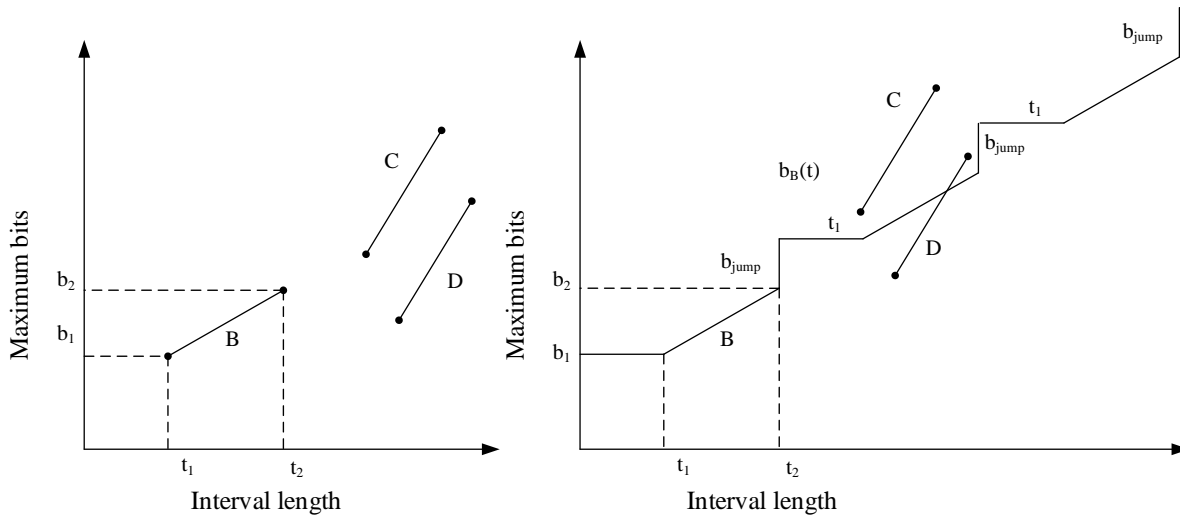


Figure 7: Redundant Token Bucket in Regulator

4 Empirical Analysis

In this section, simulation results are presented for empirical analysis. In [2], the input malicious traffic is modeled as ON-OFF Markov process. The traffic volume is large (when the malicious traffic keep staying in ON state for most of the time), but the pattern of the traffic cannot get the worst out from the buckets in the regulator. In this paper, simulation is built based on a specially designed traffic pattern, which could put the buckets into their worst case scenario and we can see that the output traffic from the regulator in [2] violates the S-BIND traffic descriptor.

4.1 Violating Input Traffic Pattern

The S-BIND traffic descriptors used to set up the regulator are derived from ON-OFF Markov process modeling low-bursty traffic ($1/\alpha=1.587s$, $1/\beta=1.004s$, $R=64Kbps$), which simulates speech audio based on ITU-T specification. S-BIND intervals are 500ms, 750ms, 1000ms, 2500ms, 4000ms, and 5000ms. Confidence levels are 90%, 80%, 70% and 60%. The descriptors are listed in the table below, which are used to setup the regulator's token buckets in simulations.

Table 1: S-BIND Parameters Used to Setup Regulator

	500ms	750ms	1000ms	2500ms	4000ms	5000ms
90%	32Kb	48 Kb	64 Kb	132.86 Kb	186.88 Kb	223.49 Kb
80%	32 Kb	45.63 Kb	54.66 Kb	107.78 Kb	154.62 Kb	187.14 Kb
70%	24.96 Kb	33.22 Kb	41.80 Kb	87.62 Kb	133.31 Kb	163.90 Kb
60%	14.14 Kb	22.14 Kb	28.54 Kb	72.32 Kb	110.85 Kb	139.65 Kb

Among all these linear segments, due to the length of the paper, the results of the sections between 500ms and 750ms, 1000ms and 2500ms at 70% confidence level are presented in this paper for analysis. The buckets established for these two sections has the following parameters ($b_s=24.96\text{Kb}$, $b_e=33.22\text{Kb}$, $t_s=500\text{ms}$, $t_e=750\text{ms}$), ($b_s=41.8\text{Kb}$, $b_e=87.62\text{Kb}$, $t_s=1000\text{ms}$, $t_e=2500\text{ms}$).

To get the worst case out from the buckets, 2 kinds of input traffic are setup as following. The first kind of input traffic (Traffic Pattern I) is designed to get the worst case of the buckets designed in [2]. In Traffic Pattern I, the source will send a very small amount of traffic at very beginning (state A for old buckets and state A1, A2 for newly designed buckets), then the source will wait for t_s amount of time without sending anything. After that, the source will send large amount of traffic trying to exhaust any token in the bucket for Δt amount of time. Then the source will again send a very small amount of traffic to restart the loop. The second kind of input traffic (Traffic Pattern II) is designed to get the worst case of the newly designed buckets in this paper. Because the 0 token generation rate in the new buckets will last for t_s amount of time when the bucket is empty, the small amount of traffic in Traffic Pattern I will have no effect in the state transition under our newly designed bucket. Therefore, Traffic Pattern II tries to send unlimited amount of traffic all the time and tries to exhaust the tokens in the buckets all the time.

4.2 Experiment Comparison

Traffic Pattern I is tested on both old and our newly designed buckets. Traffic Pattern II is tested on our newly designed bucket. Results are presented in Table 2.

Table 2: Results Comparing New Buckets with Old Buckets in [2]

	Bucket (500ms-750ms)		Bucket (1000ms-2500ms)	
	500ms	750ms	1000ms	2500ms
Bucket Interval (t_s , t_e)	500ms	750ms	1000ms	2500ms
Bucket Volume (b_s , b_e)	24.96Kb	33.22Kb	41.80Kb	87.62Kb
70% Traffic I->Old Bucket*	33.1Kb	33.1Kb	49.5Kb	87.5Kb
70% Traffic I->New Bucket**	24.9Kb	24.9Kb	26.5Kb	57Kb
70% Traffic II->New Bucket***	24.9Kb	29Kb	40.3Kb	77.1Kb

We can see in Table 2 the old buckets cannot handle Traffic Pattern I correctly, the output traffic's S-BIND parameters (row with *) violate the expected bucket's b_s value. On the other hand, the newly designed buckets' outputs are all bounded by the expected parameters (rows with ** and ***).

The newly proposed bucket optimization algorithm described in Section 3.3 is tested on the S-BIND parameters in Table 1. The result shows that at 70% confidence level, the bucket between 4000ms and 5000ms can totally be removed from the regulator, because its constraint function is completely above the constraint function of the bucket between 1000ms and 2500ms as we derived in section 3.3. Therefore

the bucket between 400ms and 5000ms will block no traffic at all if it takes input from the bucket between 1000ms and 2500ms. By removing one bucket from the 5 buckets in the regulator, about 20% computation cost can be saved from the regulator.

5 Conclusion

In this paper, a new token bucket design is proposed for traffic using S-BIND traffic descriptor. In the new design, the bucket can regulate the traffic within the S-BIND parameter even when the source tunes the input traffic to hit the worst case of the regulator. Other than the bucket design, a new bucket optimization algorithm is proposed to reduce the number of buckets needed in a regulator by checking the constraint functions of all the buckets to remove the redundancy.

REFERENCE

- [1] Lie Qian, Anard Krishnamurthy, Yuke Wang, Yiyang Tang, P. Dauchy, and Albert Conte, A New Traffic Model and Statistical Admission Control Algorithm for Providing QoS Guarantees to On-Line Traffic. Proceedings of IEEE Global Telecommunications Conference, 2004, GLOBECOM, vol. 3, pp. 1401-1405.
- [2] Lie Qian, Yuke Wang, and Hong Shen, Token Bucket Based Statistical Regulator for S-BIND Modeled On-Line Traffic. Proceedings of IEEE International Conference on Communications, 2005, ICC, vol. 1, pp. 125-129.
- [3] J. Qiu and E. W. Knightly, Measurement-based admission control with aggregate traffic envelopes, IEEE/ACM Transactions on Networking, vol. 9, no. 2, pp. 199-210, April 2001.
- [4] B. Statovci-Halimi, Adaptive admission control for supporting class-based QoS, 2010 6th EURO-NF Conference on Next Generation Internet (NGI), pp. 1-8, 2010.
- [5] L. Breslau, E. W. Knightly, S. Shenker, I. Stoica, and H. Zhang, Endpoint admission control: architectural issues and performance, Proc. Of ACM SIGCOMM'00, pp. 57-69, September 2000.
- [6] V. Elek, G. Karlsson, and R. Ronngren, Admission control based on end-to-end measurements, Proc. Of IEEE INFOCOM, March 2000.
- [7] D. Ferrari and D. C. Verma, A scheme for real-time channel establishment in wide-area networks, IEEE Journal on Selected Areas in Communications, vol. 8, Issue 3, pp. 368-379, April 1990.
- [8] E. W. Knightly, H-BIND: a new approach to providing statistical performance guarantees to VBR traffic, Proc. Of IEEE INFOCOM '96, pp. 1091--1099, March 1996.
- [9] E. W. Knightly and N. B. Shroff, Admission control for statistical QoS: theory and practice, IEEE Network, vol. 13, Issue 2, pp. 20--29, 1999.

- [10] George Kesidis, Jean Walrand and Cheng-Shang Chang, Effective bandwidths for multiclass Markov fluids and other ATM sources, IEEE/ACM Transactions on Networking, vol. 1, pp. 424-428, 1993.
- [11] H. A. Harhira, and S. Pierre, A Mathematical Model for the Admission Control Problem in MPLS Networks with End-to-End delay guarantees, Proc. Of 16th International Conference on Computer Communications and Networks, pp. 1193-1197, 2007.
- [12] S. Alwakeel, and A. Prasertijo, Probability admission control in class-based Video-on-Demand system, 2011 International Conference on Multimedia Computing and Systems (ICMCS), pp. 1-6, 2011.
- [13] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An architecture for differential services, IETF, RFC 2475, December 1998.
- [14] Z.-L. Zhang, Z. Duan, L. Gao, and Y. Hou, Decoupling QoS control from core routers: a novel bandwidth broker architecture for scalable support of guaranteed services, ACM SIGCOMM Computer Communication Review, vol. 30, Issue 4, 2000.
- [15] A. Terzis, L. Wang, J. Ogawa, and L. Zhang, A two tier resource management model for the Internet, Proc. Of GLOBECOM '99, vol. 3 , pp. 1779 -1791, 1999.
- [16] E. W. Knightly and H. Zhang, D-BIND: an accurate traffic model for providing QoS guarantees to VBR traffic, IEEE ACM Transactions on Networking, vol. 5, Issue 2, pp. 219-231, April 1997.
- [17] H. P. Stern, S. A. Mahmoud, and K. K. Wong, A comprehensive model for voice activity in conversational speech-development and application to performance analysis of new-generation wireless communications system, Wireless Networks, vol. 2, no. 4, pp. 359-367, December 1996.
- [18] F. Beritelli, A. Lombardo, S. Palazzo, and G. Schembra, Performance analysis of an ATM multiplexer loaded with VBR traffic generated by multimode speech coders, IEEE Journal on Selected Areas in Communications, vol. 17, no. 1, pp. 63-81, January 1999.
- [19] P. R. Jelenkovic, A. A. Lazar, and N. Semret, The effect of multiple time scales and subexponentiality in MPEG video streams on queueing behavior, IEEE Journal on Selected Areas in Communications, vol. 15, no. 6, pp. 1052-1071, August 1997.
- [20] A. Lombardo, G. Morabito, and G. Schembra, An accurate and treatable markov model of MPEG-video traffic, IEEE INFOCOM, pp. 217-224, March 1998.
- [21] R. Cruz, A calculus for network delay, part I: Network elements in isolation, IEEE Transactions on Information Theory, vol. 37, Issue 1, pp. 114-121, January 1991.

- [22] S. Chong and S. Li, Probabilistic burstiness-curve-based connection control for real-time multimedia services in ATM networks, *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 6, pp. 1072-1086, August 1997.
- [23] J. Kurose, On computing per-session performance bounds in high-speed multi-hop computer networks, *ACM Sigmetrics'92*, vol. 20, Issue 1, 1992.
- [24] H. Zhang and E. Knightly, Providing end-to-end statistical performance guarantees with interval dependent stochastic models, *ACM Sigmetrics'94*, vol. 22, Issue 1, 1994.
- [25] E. P. Rathgeb, Modeling and performance comparison of policing mechanisms for ATM networks, *IEEE Journal on Selected Areas in Communications*, vol. 9, Issue 3, pp. 325-334, April 1991.
- [26] J. Turner, New directions in communications (or which way to the information age), *IEEE Communication Magazine*, vol. 24, Issue 10, pp. 8-15, October 1986.
- [27] M. Salamah and H. Lababidi, BLLB: a novel traffic policing mechanism for ATM networks, 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 411-415, August 2000.
- [28] M. Salamah and H. Lababidi, FBLLB: a fuzzy-based traffic policing mechanism for ATM networks, *ACS/IEEE International Conference on Computer Systems and Applications*, pp. 31-35, June 2001.

Mobile Operators as Banks or Vice-Versa? and: Regulators' Interest in the Best Efficiency of Payments

Louis François Pau

Erasmus University Rotterdam, Netherlands

lpau@nypost.dk

ABSTRACT

This paper addresses the strategic challenges of deposit banks, and payment clearinghouses, posed by the growing role of mobile operators as collectors and payment agents for flows of cash for themselves and between third parties. Through analysis and data from selected operators, it is shown that mobile operators as money flow handlers achieve levels of efficiency, profitability, and risk control comparable to deposit banks. Furthermore, the payment infrastructures deployed by both are found to be quite similar, and are analyzed in relation to financial profitability, strategic challenges and opportunities. This paves the way to either mobile operators taking a bigger role, or for banks to tie up such operators to them even more tightly, or for alliances/mergers to take place, all these options being subject to regulatory evolution which is analyzed as well. The consequences of the payment efficiency and architectures are mapped out in operational and regulatory terms.

Keywords: e-Business, Mobile payments, Mobile operators, Deposit banks, Payment clearinghouses, Banking regulations, Telecommunications regulations

1 Introduction and goals of the paper

The issue of industry convergence, a few say, “has had the attention of both banks and operators for years”. Financing issues apart, isn't the actual fact rather that this possible convergence at operational level has been largely ignored, as operators thought that banks were better at payment services, while banks thought operators were better at communication services [1]? The recent attention given since 2006 to mobile banking support by mobile and smartphone terminals makers, leads to the derived strategic question whether these players should sell to operators and end users, or to banks and end users as well (like smart card producers do already).

Furthermore, as a convenient explanation, parties implicitly favourable to banks have pushed through the view that mobile networks should be content and transaction neutral, with intelligence and any charging to happen in the province of the end nodes (clearing houses, customers, and banks). While this argument holds for backbone IP or Automatic-teller-machine (ATM) operators, the evolution of service demand/diversity offered by 2.5G/3G/4G mobile services and terminals goes in the opposite direction for these mobile networks.

Haven't the above perceptions been reversed by very efficient real time payments, transaction clearing systems and content-on-demand management systems at mobile operators, but also by some banks analyzing now better and more strategically their information and communication assets from a competitive point of view? Isn't it time to revisit some roles and regulations to benefit from these payment efficiencies? Isn't it time for mobile terminal and smartphone makers to position some of their models for early adoption by banks?

The mobile operators become parties to financial transactions, but this is only visible where the different regulators so allow! But, while the communications regulators might apply rather simple benchmarks to operators' financial flows, banking regulators would not even do so for payment functions because of the treasury/ cash-flow and money market implications.

These are the issues which this paper, backed by operator data analysis on one hand, and analysis of the payment infrastructures on the other hand, are analysing. The emphasis, rarely studied, is on payment efficiencies.

The reader should acknowledge that there is here no emphasis on specific Mobile banking (M-Banking) technologies (security, terminals, application software), nor on related market forces from the user demand point of view.

2 Mobile Banking as a Change Agent in Banks

For those bankers who have experienced and understood to the fullest the implications of mobile communication in their business, productivity gains in a bank or payment clearinghouse are no longer measured by the substitution of labor force by a tool!

With M-banking, every agent, that is: customer, enterprise and bank personnel alike, becomes a user as well as an information/knowledge source to the service suppliers and to other customers [2]. This is, simply put, because so many banking information, knowledge and transaction capabilities are brought into the hands of any such agent anytime and anywhere. Thus cooperation and control/audit modes, as well as some other roles, must be redefined between bank customers, banks and third parties. The major difference with the Internet alone as a change agent is the ubiquity and user access brought by mobile applications, which together cement networking and diffuse changes.

Mobile banking is also a source of value-addition to customers via personalization of features, both in a "push" mode, and in a "pull/definition" role as customers can request or configure themselves some service features; as observed already in Scandinavia, users define M-banking alerts and refuse some service offerings "pushed" down on them by some banks. Some banks have therefore chosen to add wireless systems as a strategic sale and support channel (e.g. Nordea, BNP Paribas, Bankinter, Kenyan operators, etc...).

This leads to a basic choice by top bank management: should they promote platforms supporting mobile marketing and consulting, and enhanced mobile services, OR should they allow for and play a role in mobile access to simple e- and M-banking/payment services. The third option, often stated, but not representing a pure business strategy, is to do so called "both"; investments and competence build up alone make this very difficult.

That first challenge, leads to a larger one discussed in the next section.

3 Mobile Operators as Banks or Vice-versa?

This Section raises some issues to be analysed, first on the basis of cash flow analysis, next on technology analysis in Sections 6, and Sections 2.3, 3., 4., respectively.

3.1 Mobile operators as banks

With an average 35-65 % (culture and also country dependent) of all mobile generic services being prepaid to the operator over periods of several months to their own offices or via payment agents (not only banks), aren't mobile operators short-term deposit banks holding at any time double digit Billions USD ? Going beyond collection of receivables from their own customers, to which extent should operators carry out simple payment processing functions traditionally carried out by banks between their customers and between their customers and third parties? For example, for some mobile operators whose ownership includes public utility companies, such third parties could be water, power and cable TV bills.

Furthermore, with mobile operator's capability to handle efficiently and in real-time max. Euro 100-type payments (tickets, parking...), and their ability to handle bundled service definitions, aren't operators micropayment agents [3]? In addition, in terms of cross-subsidization, are these micropayment services paid by the generic or value-added transport / communication services?

3.2 Banks as Mobile virtual network operators (MVNO's)

When banks "influence" or take over mobile operators via loan or ownership structures, why shouldn't they become mobile virtual operators to capture the operator's client base and their cash transactions covering mobile communication services, besides other payments enabled via the same transmission and transactions infrastructure?

A third party (bank subsidiary, transactions payment cooperative, etc...) can act as an aggregator, reducing the payment processing and network traffic generated by small-payment users. But adding this party reduces revenue and fee sharing between the bank and owner of the transmission infrastructure. In a way, mobile roaming operators (GRX and IPGRX operators) can be looked upon as being actually payment clearing systems, even if historically the banking shareholders of e.g. the MACH consortium failed to see this.

3.3 Payment/transactions infrastructures

Very important is the observation that actually there is not much difference at functional IT and technology levels, between the customer care and transactions platforms of mobile operators (see Figure 1), and those of banks (see Figure 2) [4] ! To a large extent, only record data structures differ. This fact is the result of the evolutions of both layered communications systems architecture, and of banking software systems architecture respectively, in that mobile networks have evolved much faster than fixed networks. The security levels offered by mobile networks inside the infrastructure are also on par with those in banking software, not the least because of added security communications hardware and controlling give. This means that:

- For a mobile operator to operate also as a payment clearinghouse, is a relatively minor issue, provided the fulfillment systems comply with interbanking data formats, which they even do more and more;

- For a bank to operate as a mobile virtual operator using a third party's access networks, is also a relatively minor issue if subscriber data are tagged with bank customer file data, which they even are more and more.

4 The slow revolution of credit card/new SIM/ Mobile phone/e-Identity combinations

It is important not to ignore present day's simple solutions which created M-Banking services for today's wireless networks, as they provide a pressure to come to grips with the issues raised in the previous two sections. Let us mention as examples, some facts:

- the current use of advanced SIM toolkits (STK) technology (Axalto, Oberthur, ATOS, Brokat, ActivCard, etc...) supporting payments, and the SIP Consortium standardizing these features;
- some mobile operators (e.g. Telenor, Orange, TeliaSonera, Vodafone) have enabled the SIM card as a Visa payment card in selected markets, and such combinations have been branded as "mobile wallets"; this has not prevented some mobile wallet operations to fold, e.g. Telefonica O2 [5];
- some operators have enabled a payment credit card as a prepayment card for mobiles (e.g. Wind Italy);
- some payment clearing houses allow mobile prepaid service reloads from mobile terminals with debit to bank accounts (e.g. Banksys and its new mother company);
- some mobile phones and smartphones have card readers;
- the Electronic Mobile Payment Services (EMPS) tested by Nordea, VISA Intl, Nokia, and others; it requires the addition of a chip inside terminals which would carry debit, credit, e-Identity, loyalty cards and access codes;
- the ability to transmit payment instructions to point-of-sales (POS) terminals from mobile terminals with Bluetooth or WiFi, without using mobile networks.

All these examples, and many more [6], develop a demand for revisiting relative roles and regulations for banks and mobile operators alike. The difficulty that, in some of the above technical alternatives, stores and point-of-sales will have to be reengineered and installed, is largely reduced by the other wireless technical alternatives which bypass such nodes altogether provided the mobile terminals can support them.

5 Some Technology Usage Lessons

Some banks, as well as mobile operators, running M-banking capabilities and services, have learned a few key things, which drive the factors discussed in Sections 1 and 2.

"New technologies" («technology push»), such as wireless in banking, do not mean only "totally new services"; most existing services are migrated to multiple access channels, and enhanced with added functionality when feasible if they mean added value.

Essential limiting factors in M-banking are the «ease-of-use» first (screen size/colour, data entry, security features...), and technology only second (capabilities of terminals, authentication techniques...). This observation is justified by a set of contributing factors:

- the social identification of the mobile terminal with its user;
- the ability to select specific payment transaction types for "real-time anywhere" downloads;

- the definitely superior capabilities of mobile terminals in terms of personalization and geo-location, bringing the banking branch to the customer;
- the strong «attractiveness» of mobile terminals as personal banking terminals, and their price/performance/user acceptance which is not necessarily second to automatic-teller (ATM) machines.
- Last, the personalization of mobile content and competitive service offerings (the theme: “MyBank is not YourBank”), is ultimately about the only way both knowledge and operational flexibility can be provided in a differentiated way by the same banking back office. The study [7] has pointed out that mobile operators, that acquire prepaid customers more selectively, and offer them well-crafted incentive programs, could significantly improve the returns from this segment. However, regarding global M-payment standards (ETSI, OMA, Mobile Payment Forum, Mobile Payment services association, M-Commerce Forum, J-Consortium, etc..), the reality is that, despite claims by some vendors, IT integrators and even operators, we are far from a common standard, so a proprietary “surprise” design may still take over ! This means that, alongside open public standards, market based standards controlled by a few parties, may still represent an often incompatible alternative-

Today, if e.g. a UK content provider wants its for-pay offerings to be directly accessible to just the entire UK national mobile subscriber base, he will have to engage individually 5 operators, all with different billing systems! A significant number of retailers will only take the plunge into M-Commerce if there is one effective M-payment solution supported by multiple vendors. As an evolution, far from ideal though, it is necessary to:

- specify which protocols operators need to use in order to support *different* payment methods (similar to the PC Internet space with distinct SSL/PKI/Certificates);
- prioritize amongst the plethora of wireless standards families for M-banking deployment (e.g. drop GSM/GPRS and deploy from HSPDA, LTE onwards);
- integrate the proprietary initiatives of some operators, who cannot wait first for the convergence to happen (e.g. Vodafone: M-Pay service, a pre-pay card for higher value transactions, etc.);
- allow and deploy temporarily cross platform solutions with reverse SMS billing (e.g. UK www.Bango.net); reverse SMS billing includes the capability to make sender (or receiver) validate a monetary transaction they initiate or authorize;
- not to be taken on by some providers who believe that they have “the” solution.

6 M-business models implications on payment transactions handled by mobile operators (Personal payments)

For the individual consumer, or agent of a product / service other than generic mobile services, the main payment models for individuals are combinations of the following six payment models:

- 1) Deducted from bill: Advertiser pays;
- 2) Deducted from bill: Retailer pays a percentage (comparable to credit cards);
- 3) Added to bill: Monthly fee added to mobile service bill for access to M-payment services;
- 4) Added to bill: Fee based, similar to SMS charge, per request or transaction;
- 5) Added to or deducted from bill: Revenue from/to individual from community referrals;

6) Added to bill; actual cost of product of service bought by mobile channel.

However, in addition, the transmission of the relevant transaction related information warrants transmission costs determined from tariffs. Communication service airtime is so expensive that banks find it, sometimes and some places, difficult to charge M-banking fees of type 4) above. Some suppliers and banks wait till operator's tariffs and prices for data transfers (GPRS, EDGE, 3G, and HSPDA) have gone down, and/or that WiFi offers better security features.

In many cases the equation is simple: between credit card or banking fees on one hand, and the total of transmission costs plus the sum of 1) to 5) on the other hand, which is the cheapest channel for the purchase of that product or service? Obviously higher fees have been charged in the past in the context of "flash or emotional purchases"; but with the present-day wireless terminals penetration in the population, their use is not reduced to such purchases any more. Even then, total transaction fees (transport, applications, transactions handling) will have to be competitive with e.g. broadband Internet transaction handling fees.

So, just by stating the relevance of this comparison, which has been done [8], a key question is why consumers and enterprises, should end up paying inflated (or double) fees on each transaction because mobile operators and payment clearing houses/banks each take their "cut" instead of fulfilling both roles and achieving better economies of scale.

Some operators (e.g. of i-Mode services, or of some mobile gaming services e.g. in Korea), learning from the huge financial success of the old X25 based Minitel services of France Telecom, not only aim at economies of scale, but also at fulfilling transactions for a fee on behalf of third parties such as content owners and banks. At the risk of simplifying, not only do these operators lock margins by service retention at communication level, but they earn additional significant margins by reducing the billing infrastructure investments of third parties, thus taking a percentage of the sum of 1) to 4) and/or billing operator fees (see Figure 3). The observed ratios of total operational margins to operating expenses plus depreciation, from such a model are observed to be above 80 %. The argument in this sub-section, is not about analyzing the "success" of these services from the demand and user points of view, but in terms of benefits to operators adopting new payment models -

7 Cases from financial analysis of mobile operators cash flow statements

7.1 Objectives and limitations

A sample of publicly listed communications operators with public wireless services was chosen, with diverse mobile penetration, economic development, countries and currencies, as well as "incumbent" roles vs. «pure wireless» plays. The time period covered was for the 1998 to 2014 accounting period, although not all data were available for all periods. For incumbents having fixed and other operations as well, mobile operations were taken equal to the ratio of mobile revenues to total revenues. Had to be excluded in a first analysis such operators as Vodafone who do not publish the accounts and data of all the national operators in which they own minority or majority positions.

The sample included: NTT DoCoMo, Singapore Telecom, Orange, Belgacom, Telenor, Nextel Sprint, TDS, Telkom Indonesia, and Estonian Telecom. It represents in total more than 144 valid complete annual data sets from the official annual filings with the national securities and exchange commissions. Because of the

amount of such data they cannot be reproduced inside this article, but are available to the research community from the annual reports.

7.2 Accounting Methodology

The emphasis in the analysis was on *Net operating cash flow (NOCF)* and its components, and on *Free cash flow*, together with subscriber, subscription type, employee, CAPEX (capital expenditure for infrastructure and services), and national discount rate data (from the National banks). In other words, in order to analyze intrinsic money flows from operations were ignored cash from investing and financing.

It is reminded that the Net operating cash flow (NOCF) can be looked upon in two ways, either as (EBIT: Earnings before interest and tax):

$$\text{NOCF} = \text{EBIT} + \text{Depreciation} - \text{Tax expenses} - \text{Increase in working capital (WCR)}$$

Where the first three terms are the Cash Margin component and the last is the Investment component, or as:

$$\text{NOCF} = \text{Net sales} - \text{Cost of goods sold} - \text{Selling \& G\&A expenses} - \text{Tax expenses} - \text{WCR}$$

It is reminded that the Free cash flow is:

$$\text{Free Cash flow} = \text{Profit after taxes before interest payment} + \text{Depreciation} - \text{WCR} - \text{New investments.}$$

It is also reminded that the Working capital requirements can, from a purely operational point of view, be estimated as including all capital equipment (CAPEX) and staff needed to run the mobile operator infrastructure and back end services.

From a financing perspective, an aggressive strategy occurs when the Cash Margin component is less than Short term debt, and a conservative one is when the reverse happens.

The working assumption is that a mobile operator running a conservative financing strategy and a positive NOCF, should be able for its operations only (ignoring investing activities and financing activities) to operate on zero short term debt and to get interest income from the NOCF (at, as an approximation, the prevailing national discount rate). It is then possible to determine the "*NOCF margin*" as being this interest income from the NOCF, in proportion to total revenues. As NOCF is not made operator segment specific in operator accounts, it was sometimes not possible to determine that "*NOCF margin*" from mobile operations only; it is most likely that this value is higher than for the combined communication services of a mixed service operator. The "*NOCF margin*" approximates the margin all short-term lending/borrowing bank operations would generate in a short-term deposit bank.

As it turns out that the share of postpaid mobile revenues to prepaid mobile revenues across operators and periods, runs at 53 %, this situation is comparable to a short term deposit/lending bank where the short-term loan portfolio aggregates to 106 % of the short term money deposits. This means that in average the operators have cash operations where the leverage is low and could still be extended.

7.3 Quantitative Results and interpretation

The data analysis produces in average over the operators and the years 1998-2014, the following indicator values:

- Mobile revenue share: 33, 6 %

- Share postpaid/prepaid in mobile revenues: 55, 13 %
- Free cash flow margin: 1, 94 %
- Net Operating Cash Flow margin: 2,136 %
- Capital expenditures/ NOCF: 84 %
- Annual revenue /employee/year: 341015 Euros
- Free cash flow from operations/employee/year: 110574 Euros
- Cellular subscribers / Mobile operations employee: 1176
- Mobile ARPU (/year): 440 Euros

The main interim conclusion to be drawn is that, in as far as the following indicators are concerned:

- Leverage of short term debt/ short term deposits,
- Net operating cash flow margin,
- Free cash flow margin,
- Free cash flow from operations/employee,
- Number of customers / Employee,

The average operator in the sample achieved similar financial results from operations than the average short term operations in a bank with limited investment operations, say a postal bank or savings and loans institutions.

7.4 Other analyses

In another large research project on Mobile payments and Electronic payment intermediaries in the Netherlands, carried out in collaboration with the European Payment Certification Institute (EPCI) [8], it has been shown that, on the basis of the cost and revenue structure for mobile payments in Scandinavia and the Netherlands, mobile operators have a significant financial upside from mobile payments (directly and indirectly through their shareholdings in payment intermediaries). Their margins are also higher than those of electronic payment platforms, largely because of the multiple uses of the same billing platforms, first for mobile traffic, then for authentication, and last as fee collection platforms for payment transactions.

In consideration of the phenomenal adoption of M-banking in some emerging countries, such as Kenya, Indonesia, Bangladesh, it should be pointed out that the operators in those countries, when they operate the M-Banking operations under adapted regulations, often achieve even better indicator values than the above [9].

8 The Alternate Scenarios

If the opportunities highlighted in Sections 1, 2 are real, existing regulations may prove a hindrance and the regulatory framework may have to evolve.

8.1 For the regulators (banking and communications regulators jointly):

The regulators have to encourage efficient and secure payments fueling commerce and other services. The non-exclusive alternatives are:

- Banks get individually restricted communications service provider licenses, and lease mobile communications infrastructure;

- Bank groups get restricted communications service provider licenses, and lease mobile communications infrastructure;
- Mobile operators (genuine or virtual) get additional deposit bank licenses on demand;
- Mobile operators (genuine or virtual) gets automatically deposit bank licenses as part of their communications license; this option is of great appeal to developing countries where the banking infrastructure, coverage and trust are far lower than those of mobile operators [10];
- Mobile payment services are authorized to be opened up for licensing by third parties for their own customers (oil companies, physical transport networks, health system...).

In any case, communications and banking regulations would have to share mandatory prescriptions in terms of cash and short term debt, which would often be a change from the present situation.

8.2 For a Bank:

The alternatives are to be chosen amongst the following alternatives:

1. Existing bank card system operator(s) own and manage servers, with proprietary applications, to handle multiple channels such as mobile; a leased line/IP access transmission solutions to the GGSN node of a mobile operator is sufficient; there is the option for a bank of owning an e-mail/SMS/MMS/IMS Service centre;
2. Banks outsource some channels (such as mobile) to IT service companies if this is accepted by operators and not too expensive, and obey IT industry standards;
3. Banks internationally create, or cooperate with, existing third party service suppliers to several mobile operators (e.g. roaming/ authentication suppliers) to enhance their services towards transactions. The bank then would align them with communications industry standards

It should be noted also that the issue spills over to payment terminals standardization; Captin, a project aiming in a first phase to standardise payment terminal and protocols, was very much aware that M-payments will face identical problems of interoperability, unless players address the issues 1)-3) above from the start and create a sufficient volume of users / subscribers using one interoperable standard.

8.3 For a mobile operator:

The non-exclusive alternatives are to:

- 1) Delegate, for a % of the transaction fees (volume based), fulfilment, collection and risk management, to banks, banking payment cooperatives, or specialized mobile payment operators; this is the by default most frequent currently found option;
- 2) Own, alone or jointly, payment clearinghouse, bank(s) or consumer credit companies to perform the services listed under 1); this is also quite common today, although different bank/credit card consortia offer competing vehicles;
- 3) Apply for a deposit banking license in their own name, manage risks and reinsurance, and handle collection on behalf of third parties (content owners, administrations and public services); this model has deployed very rapidly in mostly emerging markets, with countries such as Kenya, Indonesia taking the lead;
- 4) Split between 1) for large transactions, and 3) for small transactions and reloads (for mobile services as well content); examples include collaborations by bank ISIS in USA, and bank La Caixa

in Spain, with several operators, and in another segment T-Mobile USA's targeting of the unbanked sector.

In all cases the mobile operators must:

- develop in ITU, ETSI, 3GPP, IETF, OMG, and OMA, open public standards supporting payment technologies and their end-to-end security and tracing; this extends to the UK Payments Council harmonizing the data structures linking bank account numbers with mobile phone numbers [11];
- develop media campaigns to «prove» the equal/ higher security of mobile services, compared to many bank card solutions;
- not use proprietary technologies, non- interoperable networks and terminals. This is doomed to fail in terms of deployment, adaptations and costs!

Furthermore, the stance taken by the communications and/or banking regulators, might imply that operators would have to maintain cash positions they are not used to in many cases (due to their usual high debt leverage).

8.4 For a manufacturer of mobile terminals and smartphones:

The main implications are whether to consider banks and cash payment operators (like parking lots, pharmacies, etc.) as sales channels supplementing mobile operators and direct/indirect sales to end users. Some banks maintain expensive services and distribution of token cards to be used in connection with Internet banking or secure payment applications. By enabling at design stage embedded banking systems compliance and key generation, the mobile terminals and smartphone makers could offer the banks better devices, services, CRM, and continuous communications charges flows to banks.

9 CONCLUSION

Many of the central issues raised in this paper illustrate the often difficult recognition by some parties of the co-existence of two basic models in M-Business:

- The centralized model in M-Business: where trade, transaction rules and some generic business processes, are embedded right inside the core of enterprise and public communication networks, managed by these two parties, with a flow of service fees;
- The decentralized model in M-Business, with personalized terminals and services, offering full mobility and capability offerings, managed by user-driven exploration matching algorithms, and billing along the value chain; in this model too users are also information and know-how producers

Obviously, the banks come from the centralized model for their mass operations, but aim for the second model as value creators. The mobile operators too have the same profile, while coping with difficulties from the decentralized model they helped propagate. Thus indeed, mobile operators and some banks should be allowed to “converge” as mobility based IT slowly penetrates the conventional IT backbones of banks, and as the efficiency of transactions handling by mobile operators can give advantages to the banks adopting them while influencing the value added communication services they provide.

A way to look at this evolution is to use Michael Porter's “five forces model” [11] which also explains the convergence analyzed above in terms of competitive forces, without linking it as in this paper to technology evolution.

REFERENCES

- [1] Lewis A. 2003. Cashing in on communication. *European Communications*, 56-58, www.eurocomms.co.uk
- [2] Anonymous. 2003. Exploring a new gold mine for banks. *Asian Banker Journal*. **24**(3): 17
- [3] Tewari H., O'Mahony D. 2003. Real time payments for Mobile IP. *IEEE Communications Magazine*, 41(3): 126-136
- [4] Pau L-F. 2004. Network-based business process management: embedding business logic in communications networks. In *Smart business networks*", Vervest P.H.M., Heck E., Price K., Pau, L-F (eds). Springer: Berlin, Germany; 139-163
- [5] Sahota D. 2014. O2 wallet folds, *Mobile Communications International*, January, 08-09
- [6] Herzberg A. 2003. Payments and banking with mobile personal devices. *Communications of the ACM*, 46 (5): 53-58
- [7] Mc Kinsey. 2004. Prepaid services. *McKinsey Quarterly*, 5 April, http://www.mckinseyquarterly.com/Telecommunications/Equipment_Services/Profiting_from_prepaid_phone_customers_1420 [25 October 2011]
- [8] Warris F.S., Maqsoom F.M., Pau, L-F. 2006. Mobile Payments in the Netherlands: Adoption Bottlenecks and Opportunities, or... Throw out Your Wallets. Research report, ERIM, Rotterdam school of management, Rotterdam, Netherlands. <http://repub.eur.nl> <http://repub.eur.nl/res/pub/7593/>; and Report by EPCI, Brussels. 95 p.
- [9] Mbiti I., Weil D.N. 2011. Mobile banking: the impact of M-Pesa in Kenya. Working paper 17129, National Bureau of economic research, Cambridge, MA.
- [10] Centeno C. 2003. Adoption of e-services: I-banking in the candidate countries. Report no 77, IPTS, Sevilla, 14-23
- [11] PYMENTS.COM. 2014. A look at how payments got to where it is today. <http://www.pymnts.com/featured-stories56/2014/a-look-at-how-e-payments-got-to-where-it-is-today/>

Banking systems / Communications systems

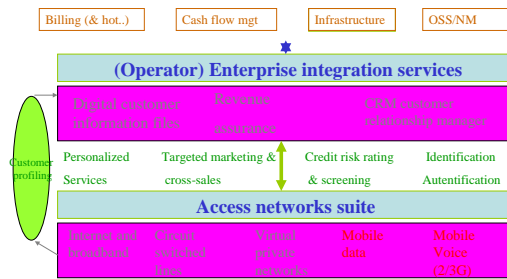


Figure 1: Mobile communications systems customer management and billing architecture

Banking systems / Communications systems

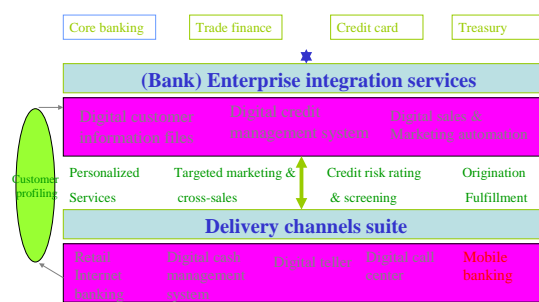


Figure 2: Payment/banking systems customer management and settlement architecture

Content provider bill collection system (e.g. Minitel/iMode) (very many content channels)

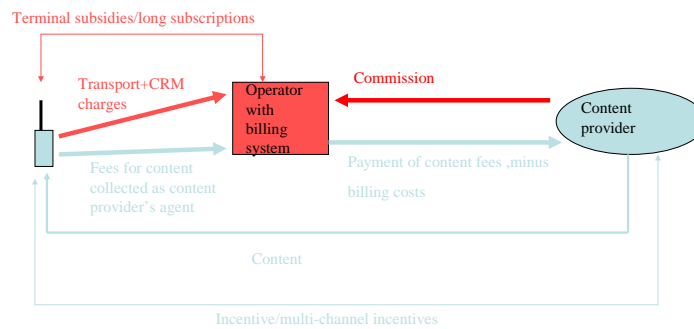


Figure 3: Collection of content owners' receivables and of own revenues by a mobile operator (e.g. i-Mode, Minitel)

An SMS Based Push Email Server

¹Izang Aaron.A, ²Omotunde Ayokunle A, ³Kuyoro Shade, ⁴Abel Samuel and ⁵Mensah Yaw
*School of Computing And Engineering Sciences, Department of Computer Science and Information
Technology, Babcock University, Ilishan Remo, Ogun State, Nigeria*
¹aaronizang89@gmail.com; ²ayo_omotunde@yahoo.com; ³afolashadeng@gmail.com;
⁴abelsammie@yahoo.co.uk; ⁵mensahyaw1983@yahoo.com

ABSTRACT

The communication industry is ever evolving with new media of communicating between people and these various media have made it impossible to determine the best means of communication. This work in its entirety aims at reducing the stress and vigour that sometimes accompany some of the different means of communication.

The email has proven to be one of the most used means of online communication. However, a major drawback of email communication is that for a mailbox to be accessed, it requires an active and working internet connection which is often times expensive and cannot be afforded continuously by an average individual.

This work was created to eliminate such factor when it comes to using the email as a means of communication by assisting the e-mail account owner to forward his newly received mail by SMS to the user's mobile phone with or without internet access on the mobile device.

Keywords- Communication, Email, SMS, Server, GSM

1 Introduction

Communication is highly essential; there are various means of communication, but there are some means of communication that cannot be overlooked in the quest for adequate communicating facilities which are: E-mail and SMS. These two means of communication have over time proven themselves to be the one of the most unavoidable, indispensable means of communication to mankind. Irrespective of the distance between the users, the information is delivered swiftly and securely.

The introduction of high-end systems has paved way for the use of Emails and SMS for data transfer, data storage and other uses that are key to the advancement of any environment. The SMS is a means of sending binary data over the air. [1].

Although it is a widely used communication mechanism for cell phone users, SMS is far more than just a technology for teenage chat. [1]

Different emails are in use nowadays, from Yahoo Mail to Gmail to Live and so on. How then do we integrate these 2 means to create a higher and more effective means of communication? This is where

these research proffer a solution that will bridge the gap between the email owner and the ability for them to access their mails.

SMS BASED PUSH EMAIL SERVER involves the transfer of mails from the mail delivery agent to the mail user agent via SMS. [2]

With the development of networks and communication technology, especially wireless communication technology, Push email is a trend on the convergence if internet and wireless communication fails. Email is a basic service of internet all the time, since it is an important way for people's communication, over thirty percent of service on the internet is the email service. [8].

The focus of this work is to design and implement an "SMS based push e-mail server", a means by which new email is forwarded to mobile devices as SMS.

2 Review of Related Works

Amanda, C.K in her report "Advantages and benefits of Emails for Business" made known how well e-mails have contributed to the success of businesses by stating that Email has revolutionized business communications. Entrepreneurs are no longer at the mercy of the speed of the post office and do not have to roll the dice on whether someone is in the office to receive a phone call. Businesses can save money, open up effective marketing options, keep communication lines open within a company and collaborate on projects all through the use of email. Up and coming generations of workers are more comfortable using email than traditional letters or memos. Companies can explore methods of using email to reach important goals and make business more efficient.

The Electronic mail (also known as email or e-mail) was invented by Ray Tomlinson in 1972 and is one of the most commonly used services on the Internet, allowing people to send messages to one or more recipients. [3].

The following are some closely related works:

2.1 How does SMS Work?

The SMC (Short message centre) is the entity that does the job of store and forward of messages to and from the mobile station.

The SME (Short Message Entity) which can be located in the fixed network or a mobile station receives and sends short messages.

The SMS GWMS (Short gateway MSC) is a gateway MSC that can also receive short messages. The gateway MSC is a mobile network's point of contact with other networks. On receiving the short message from the short message centre, GMSC uses the SS7 network to interrogate the current position of the mobile station from the Home Location register (HLR).

HLR is the main database in a mobile network. It holds information of the subscription profile of the mobile and also about the routing information for the subscriber.

The MSC (Mobile Switching centre) is the entity in a GSM network which does the job of switching connections between mobile stations or between mobile stations and the fixed network.

The VLR (Visitor Location Register) corresponds to each MSC and contains temporary information about the mobile, information like mobile identification and the cell (or a group of cells) where the mobile is currently situated .The BSS represents the Base Station system.

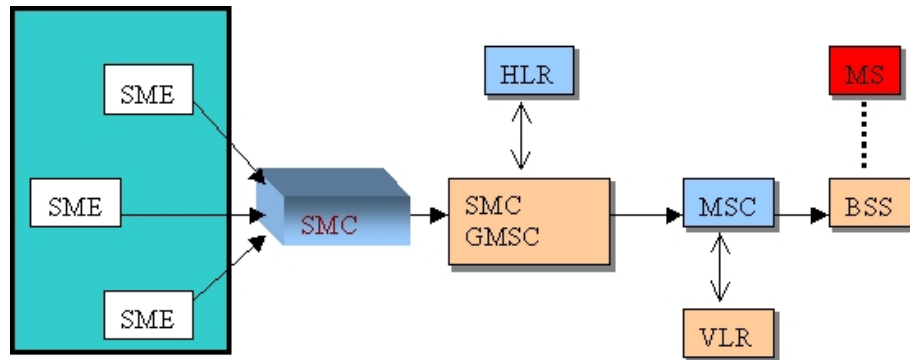


Figure 1: Organization of network elements in a GSM network that supports SMS. [4]

2.2 SMS based Facebook Notification/Registration

The SMS Based Facebook notification is software designed by Facebook to enable users receive their profile notifications via SMS.

Facebook also enables users to reply post, post updates on their timeline. This is a very effective means of communication as it enables users who are offline to be able to stay in touch with their colleagues. It also helps aids any person/people that have to reach a lot of people at the same time by update their timeline based on whatever the user has typed in his SMS. It focuses on transmission of data by the use of GSM (Global System for Mobile Communications) through asynchronous serial communication.

The objective of this work was to design a system whereby a user can send notices from cell phones and these notices sent are displayed on the user's timeline and to provide access to posting of messages. This software is only for Facebook users and is only concerned with sending of notices by authorized people. [9]

2.3 Blackberry Push E-Mail Server

Push was popularized by RIM (Research in Motion) via their implementation of a central NOC (Network Operating Centre) service for notifying devices when a new email has arrived on any of the end users email accounts. The NOC handles all the email capabilities, alleviating the processing power and constant network connectivity required for a device to continuously stay on top of its email accounts. This takes the burden off the device, and in return the device saves battery life. "Do you have a BlackBerry?" is synonymous with "do you have push email?" RIM delivered instant email to mobile devices which surpassed constantly-connected desktops in speed and efficiency in a wireless world. Perception is that RIM invented push email however this isn't the case. NTP owns the wireless email patent which many mobile handset / platform.

3 System Analysis and Design

3.1 Model

The model that was used is the waterfall model. This model has been a basis for a majority of structural system analysis methods since the 1970s. The waterfall model is also called the linear sequential life cycle

model. This model consists of different phases carried out one after the other. It is often said or believed that the model was first put forth by Winston Royce in 1970 in one of his articles; whereas he did not even use the word “waterfall.” In fact Royce later presented this model to depict a failure or a flaw in a non-working model [7]. In waterfall model each phase must be completed fully before the next phase can begin. The model is usually best small projects and projects that the requirements are certain.

The research methodology included the following steps:

- Study of the key concepts and understanding the goals of an SMS based push e-mail server.
- Reviewing related works where applicable, both successful and where such applications have failed.
- Analysis of requirements that includes user, system, functional and non-functional requirements
- Design and implementing an SMS based push e-mail server as well as testing the functionality of the system and hardware compatibility.

3.2 Application Analysis and Design

The proposed system has the following requirement as stated below

- The System shall allow users register with their e-mail address and password.
- The System shall allow users log in with their username.
- A module for checking the number of registered users.
- A module for checking the number of users with de-activated or expired accounts.
- A module for checking the number of users from a country (If the application goes international).
- A module for checking the number of visitors (people who don't register) to the site.

3.2.1 Hardware Specification

The hardware specifications for the usage of these system is subdivided into online and offline registration.

ONLINE REGISTRATION

For online registration and improved user experience while viewing the website,

A mobile device with screen sizes above 240x320 is recommended.

- Laptops, Desktops and Tablets whose date of manufacture are not older than 2010.

OFFLINE

For optimum experience while viewing e-mails on mobile, Devices with screen resolutions above 240x320 are recommended.

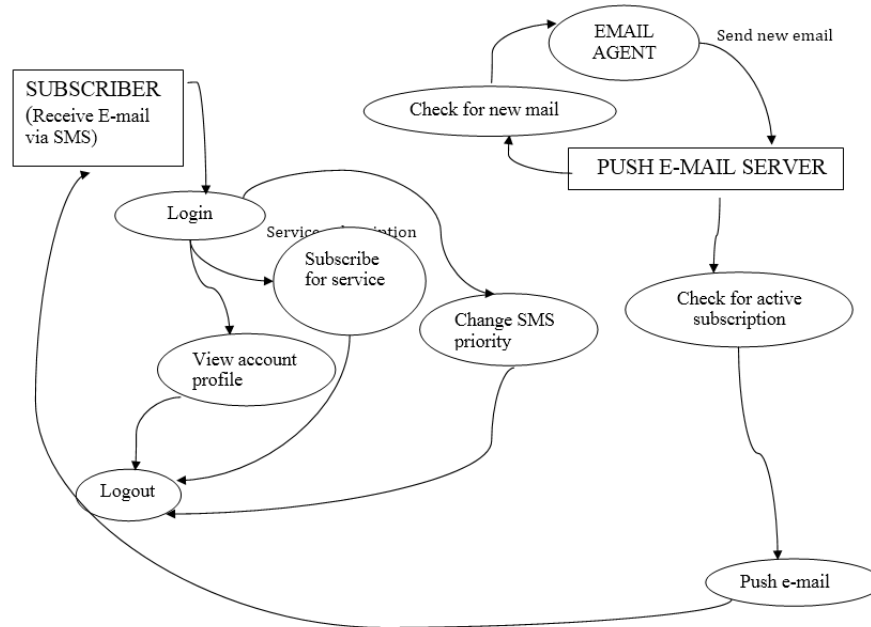


Figure 2: Data flow diagram showing the subscriber privileges

3.2.2 Explanation of the DFD

From the DFD it can be noted that, the origin of the working of the application is from the push server itself. The cron which has been set to search for new mail automatically powers up every 250 seconds and checks the mail agent (Gmail, yahoo) for new email. If cron does not detect new mail it goes back to sleep, if it does then it pulls the mail and pushes it to the actively subscribed user's mobile number as SMS. Details linked to the subscriber in the diagram indicate the services the subscriber may choose to perform without admin privileges.

3.3 System Requirements

The requirement that helps the proposed system to life after requirement gathering and implementation are divided into hardware requirements and software requirements.

3.3.1 Hardware Requirement

The hardware required to ensure the proper running of the package developed are as follows:

- An internet ready computer system.
- A Pentium or AMD processor with clock speed of 512Mhz
- A RAM size of at least 128 MB
- A hard disk capacity of at least 10 GB
- An SVGA color monitor

3.3.2 Software Requirement

These are software applications required for the proper running of the system:

- Windows 98/2000/XP/VISTA/7 operating system.

- Web Browser such Internet Explorer, Mozilla Firefox, Opera, Flock etc.
- Apache Server Version 2.0 or higher.
- MySQL database Version 5.0.51b or higher.

4 Implementation of the Application

4.1 Graphical User Interface of the Software

4.1.1 User Login/Sign Up/Administration Module

Step 1. After launching the system, the user is first taken to the system homepage upon which there is a sign up module and login module. (See Figure 3)

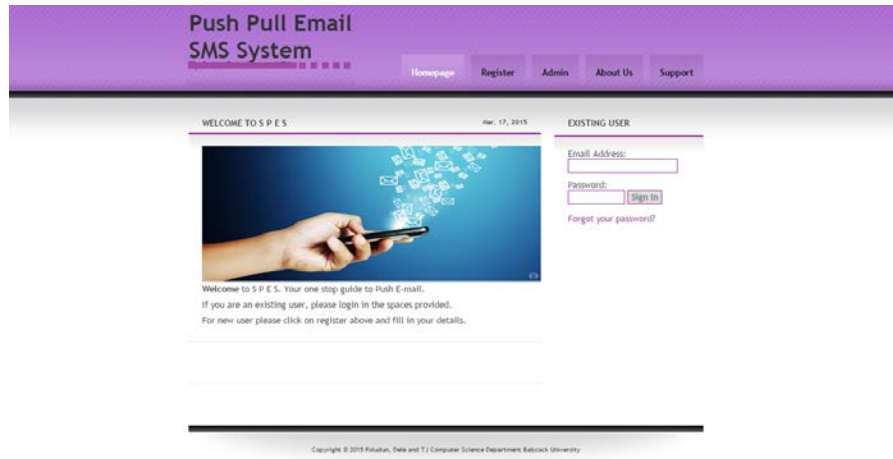


Figure 3: sign up module and login module

Step 2. The login page appears for the registered user to enter his or her username and password. Click the "Login" button. (See Figure 4)



Figure 4: Login Page

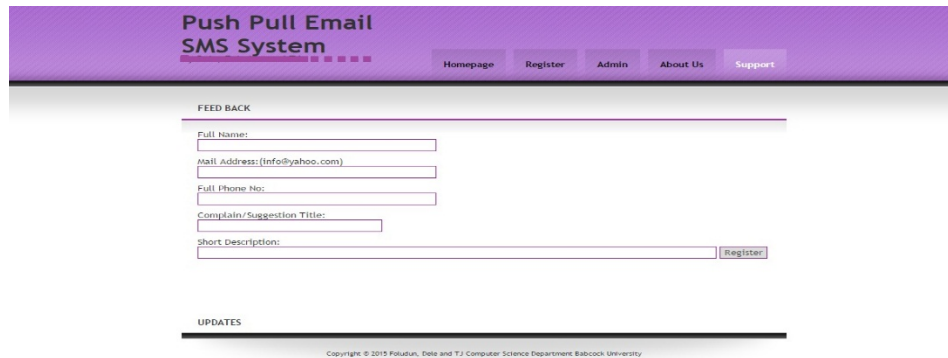
Step 3: The system test the validity of the login credentials, if invalid, the system remains on the login page with error notification. Otherwise, the system proceeds to the user account. On the user account page, the user can edit details previously submitted to the Admin. Details that can be edited include:

1. E-mail account associated with profile.
2. Mobile number associated with profile.

3. Deactivate account.
4. Subscribe to newsletter
5. Payment mode.

4.1.2 Sign Up Module

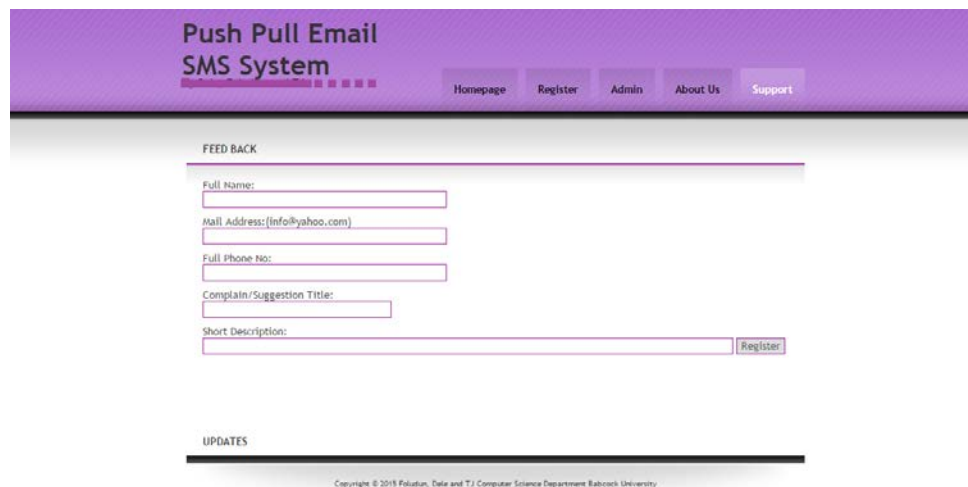
Step 1. The user visits the website and either logs in as an existing user or sign up as new users. During the Sign Up process the user is then prompted to enter his details and performs all earlier stated under the login module.



The screenshot shows the 'Push Pull Email SMS System' website. The header is purple with the system name and navigation links: 'Homepage', 'Register', 'Admin', 'About Us', and 'Support'. Below the header is a 'FEED BACK' section with a form containing the following fields: 'Full Name:', 'Mail Address:(info@yahoo.com)', 'Full Phone No:', 'Complain/Suggestion Title:', and 'Short Description:'. A 'Register' button is located at the bottom right of the form. Below the form is an 'UPDATES' section. At the very bottom, there is a small copyright notice: 'Copyright © 2015 Faluban, Dale and T.J Computer Science Department Babcock University'.

Figure 5: Sign up module

Step 2. Users have the opportunity using the post mail interface to forward complain or request to the admin and receives an auto reply acknowledging the complaint. (See Figure 6)



This screenshot is identical to Figure 5, showing the 'Push Pull Email SMS System' website with the 'FEED BACK' form. The form fields are: 'Full Name:', 'Mail Address:(info@yahoo.com)', 'Full Phone No:', 'Complain/Suggestion Title:', and 'Short Description:'. A 'Register' button is at the bottom right. Below the form is an 'UPDATES' section. At the bottom, the copyright notice reads: 'Copyright © 2015 Faluban, Dale and T.J Computer Science Department Babcock University'.

Figure 6: Feedback Mechanism

4.1.3 ADMINISTRATOR MODULE

The administrative end enables admin users to monitor the back-end application i.e. the PULL module to ensure that all aspects of the module work correctly. The administrator shall also be able to de-activate user accounts that are found to be faulty or who have breached any of the terms of usage. It provides interfaces to discharge administrative duties within the system.



Figure 7: Admin login



Figure 8: Admin panel

4.2 Summary of how our Application Work

The croon wakes up every 250 seconds to check for new email, if it does not detect any new mail it goes back to sleep and waits another 250 hours, if it detects new mail it pulls the mail using predefined IMAP protocols and assigns the header and body of the mail to their corresponding definitions in the croon. These definitions are then called in form of a sentence by the software and sent to the user by SMS. This is done by routing the SMS through an active bulk SMS gateway.

5 Conclusion and Recommendation

Basically, Web based push e-mail server is a product which takes a lot of thought, process, time and energy to develop. To develop a product that end-users would deem irrelevant would mean a failed project has been developed. The majority of design models incorporate the end-user in the beginning of the design process when analysing the need and at the end during the testing and evaluation of the product.

The aim of this work has is to enhance communication, hence it can be used by any individual organization. The importance of network reception over data connection is that there can exist a network reception capable of receiving SMS's without the existence of a data connection. However there cannot be a data connection without network reception. Thus, because the application will solely be based on just the use of the mobile phone network reception, its use is very highly encouraged.

REFERENCES

- [1] Brown, J., Shipman, B. and Vetter, R (2007) MS: THE SHORT MESSAGE SERVICE. HOW THINGS WORK, 5.
- [2] Kenneth, W. & Umbach, P. (1997). What is "Push Technology"? 18.

- [3] Lifehacker (2014, october 6). Retrieved from Life Hacker: [lifehacker.com/271974/push email-to your-phone as-a-text-message-with-flipmail](http://lifehacker.com/271974/push-email-to-your-phone-as-a-text-message-with-flipmail)
- [4] Gupta, P. (2006). Short Message Service What,How and Where.
- [5] Oludare Olaleye, Ayodele Olaniyan, Olalekan Eboda, Adeleke Awolere (2003). SMS-Based Event Notification System. Journal of Information Engineering and Applications.
- [6] Pressman, R. S. (2014). Software Engineering: A Practitioners approach McGraw Hill Professional, Fifth edition.
- [7] Royce, W. W. (1970). Managing the development of large software systems in technical papers of western show and convention.
- [8] Zheng, H. (2009). The utilization of push email in china.
- [9] Oludare Olaleye1, A. O. (2003). SMS-Based Event Notification System. Journal of Information Engineering and Applications, 8.

Network Flexibility and Policy making in Software Defined Networks

Abhinav Sharma and Manu Sood

Department of Computer Science, Himachal Pradesh University, Shimla
aasvi2006@gmail.com, soodm_67@yahoo.com

ABSTRACT

Today's computer networks are complex which is very challenging to manage as well as these traditional networks struggle to scale to the requirements of some of today's environment. SDN gives solution to all these requirements with new dynamic networking features that enhance server value and user services. SDN supplements traditional networking by offering much flexibility and software centric control creating a more policy based process for adding intelligence into today's networks. Traditionally tweaking a policy/network configuration, network administrators typically rely on a combination of manual intervention and ad-hoc scripts. In this paper we have made an attempt to show how SDN is more robust and provides users flexibility to program the network according to their needs and requirements. We have used KINETIC – a domain specific language and SDN controller to write our priority based switching application.

Keywords: Network Flexibility, Green Networking, Policies, SDN, Northbound APIs

1 Introduction

SDN is a way to manage networks that separates control plane from the forwarding plane. SDN offers a centralized view of the network giving a SDN controller the ability to act as the brain of the network. The SDN controller relays information to switch and routers via southbound APIs and to the applications with Northbound APIs [2] [6].

SDN is an additive technology that enables network administrators to solve problems that are difficult to solve with traditional methods. The goal of SDN is to solve inefficiencies in existing networks by making them more automated, dynamic and easier to adjust to changing condition. SDN separates the control plane (which decides how to handle the traffic) from the data plane (which forwards traffic according to decisions that the control plane makes). Moreover, an SDN consolidates the control plane, so that a single software control program controls multiple data-plane elements [2] [6]. Evolution of SDN dates back to 1980s when AT&T developed a Network Control Point for telephone networks, which gave operators freedom to independent evolution of infrastructure, data and services. In 1990s came the concept of Active networks, where switch perform custom computations on packets. Active networks approach was quite similar to what we are seeing for SDN today but still this technology at that time didn't took off as at that time hardware support was not cheap and there was not the concept of data-centers [1] [5]. After this the major supporting technology for SDN comes in the form of Network Virtualization. The basis of

SDN is virtualization, which in its most simplistic form allows software to run separately from the underlying hardware. We can apply the idea of virtualization to the network as well, separating the function of traffic control from the network hardware, resulting in SDN.

2 A Southbound Interface for SDN: OpenFlow

OpenFlow is a communication interface defined between the controls and forwarding layers of SDN architecture, which allows direct access to and manipulation of the forwarding plane of network devices such as switches and routers, both physical and virtual.

OpenFlow-based SDN technologies enable networks to address the high-bandwidth, dynamic nature of today's applications, adapts the network to ever-changing needs, and significantly reduces operations and management complexity [13].

OpenFlow uses the concept of flows to identify network traffic based on pre-defined match rules that can be statically or dynamically programmed by the SDN control software. Using OpenFlow, we can define how traffic should flow through network devices based on parameters such as usage patterns, application and cloud resources.

By removing the control-processing load from the switches, OpenFlow lets the switches focus on moving traffic as fast as possible. Moreover, by virtualizing network management, OpenFlow enables network operators to implement the features they want in software they control thereby promoting rapid service introduction through customization [13]. OpenFlow lets administrators prioritize different types of traffic and develop policies for how the network handles congestion and equipment problems.

OpenFlow Switches maintain a flow table containing flow entries consisting of a match condition, a list of forwarding actions, expiration settings and flow statistics as shown in fig below:

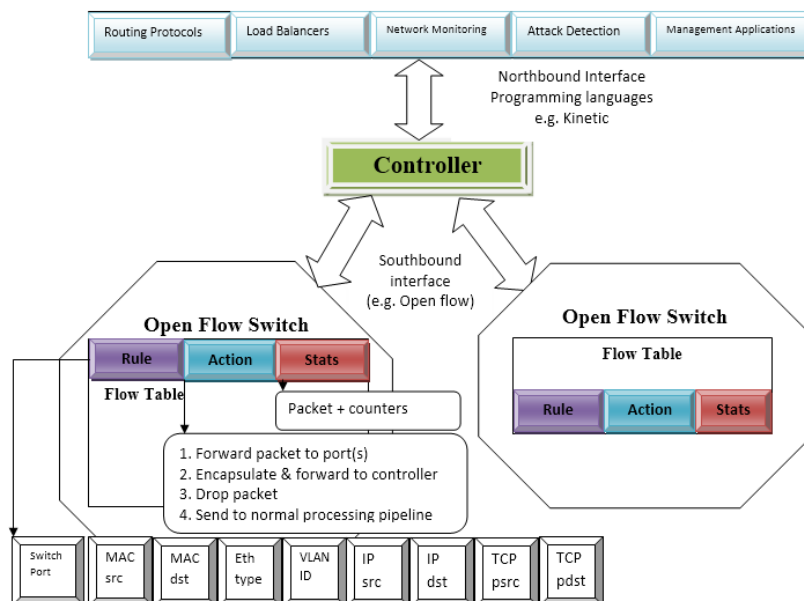


Figure 1 Open Flow-Environment: Flow-based Switching [13] [14] [15]

3 Towards Network Flexibility

3.1 Growth of Internet:

As per the estimates of internet world stats about 42.4% of the world's population uses the Internet [29]. According to ITU, almost half of the world's population will be online by the end of 2015.

There will be almost five billion things connected by the end of 2015 and three for every person on the planet – by the end of 2020. This implies Internet traffic is going to grow exponentially.

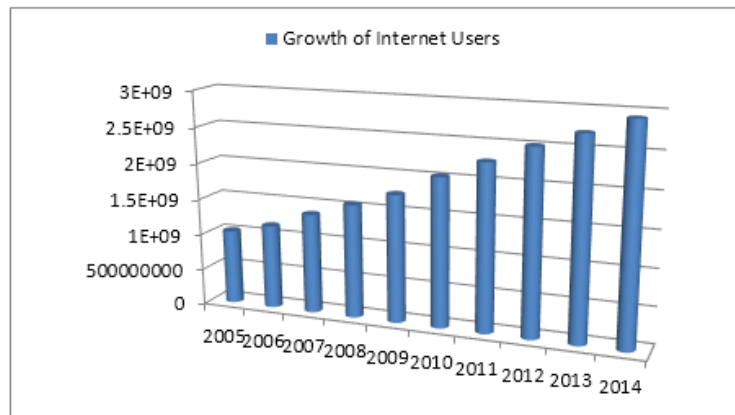


Figure 2: Growth of Internet Users [29]

The chart above shows how growth of internet users has increased in recent years. Here “Internet User” is an individual who can access the Internet, via computer or mobile device, within the home where the individual lives.

Thus network continue to increase and becoming more complex, yet configuring it remains primitive and error prone. Network operators need a dynamic and programmable approach to effectively and efficiently manage their networks to fulfil customer's requirements and assure the end-to-end service qualities.

3.2 Green Networking:

Second factor which is now becoming a major concern globally is energy consumption. Green Networking is the practice of selecting an energy-efficient networking technologies and products, and minimizing resource use whenever possible. Internet consumes between 107 and 307 GW and network devices consume around 7% of the total power consumed by Information and Communication Technology (ICT) [30] [31].

As shown in Figure 2, as the internet user base is growing exponentially, so there will be an increase in power consumption too.

In order to efficiently reduce the power consumption, there is a need of activity-adaptive internet architecture [32].

One other method to reduce energy consumption which in turn reduces operating costs of the network is to adopt technology which provides centralized management and monitoring of network and powered devices. We can make routers and switches more energy aware using network policies like link rate adaption during periods of low traffic and sleeping during no traffic. Software Defined Networking, with

one of its main feature having centralized controller makes it easy to implement such policies (activity-adaptive) thereby decreasing energy consumption too.

Table 1: Breakdown of power consumed by a router [32] [33]

	Percentage of Total Power	
	Single Chassis	Multi-chassis
Supply loss and blowers	35%	33%
Forwarding Engine	33.5%	32%
Switch fabric	10%	14.5%
Control Plane	11%	10.5%
I/O (O/E/O)	7%	6.5%
Buffers	3.5%	3.5%
Total	100%	100%

SDN has enabled an increase in link utilization to almost 100% [12] which is hardly possible in traditional networks. Moreover as from the table (i) above 11% of total power consumption in traditional switches is because of control plane but SDN by decoupling the control plane from switches is making a direct reduction of 11% in total power consumption by switches/routers.

4 Network Policies in SDN environment

In [9] the authors state that one of the major drivers for SDN is simplification. In traditional networking, to express high level network policies network operators need to configure each individual network device separately using low-level and vendor specific commands. Moreover vertical integration of control and data planes in traditional network makes it hard to deploy new networking features like routing algorithm very difficult, since it would require modification of control plane of each individual device. Thus, new networking features are commonly introduced via expensive, specialized and hard to configure equipment such as load balancers or firewalls [2]. Today's network management policies are usually decided upon by the network operator and then configured once in each network element by an administrator. The larger the network, the greater the required configuration effort becomes. Hence a one set policy is seldom modified.

In contrast to traditional networking, SDN provides a better way in form of Northbound APIs to implement or develop new networking features. One of the main aspects of SDN is centralization of controller, which with global knowledge of the network simplifies the development of network functions, services and applications. Using a centralized controller and feeding rules in this centralized controller network device can be instructed to act like a router, repeater, switch, and firewall or perform other roles as per the need of networking environment [4].

Meter, match and act are the three steps SDN undertakes to execute tasks in a policy-driven network [23]. SDN enables the metering of traffic conditions, application and user behaviour to match those conditions against a set of pre-defined criteria and then to act on the match according to a policy. Part of a policy framework is to pre-set conditions that are metered against.

With the Northbound-API of the SDN controller, the application itself can inform the network about its properties and state. This way the network controller can direct traffic flows to complement rather than disrupt each other [24] [25].

4.1 Northbound APIs

The northbound API presents a network abstraction interface to the application and management systems at the top of the SDN stack [28]. The northbound and southbound interface allows a particular network component to communicate with higher-or lower-level network component, respectively.

Northbound APIs enable basic network functions like path computation, loop avoidance, routing, security, dynamic load management, bandwidth calendaring etc.

In traditional networks, all network applications must come directly from the equipment vendors, which make it hard to change the network features as per ones need. Using Northbound APIs provided by SDN architecture network administrators can quickly modify or customize their network. One of the main advantages of Northbound APIs is that it doesn't require one to dig into different data plane devices because it's abstracted and normalized by the controller through the northbound API. Northbound API puts applications in control of the network thereby eliminating the need of tweaking an adjusting infrastructure repeatedly to get an application or service running correctly.

4.2 Programming Languages for SDN

4.2.1 Frenetic Project:

Frenetic uses SQL like query language to control the information using a collection of high-level operators for classifying, filtering, transforming and aggregating the stream of packets traversing the network [34]. It makes use of primitive predicates and set-theoretic operators. Frenetic allows parallel and sequential composition of network policies. Frenetic run time system installs rules on switches using a reactive micro-flow based strategy.

Frenetic is embedded in Python. Frenetic provides a functional reactive combinatory library for describing high-level packet forwarding policies. It supports a see-every packet abstraction which guarantees that every packet is available for analysis.

4.2.2 Pyretic:

Pyretic is member of the Frenetic family of SDN programming languages. Pyretic helps programmers to focus on how to specify a network policy at a high level of abstraction, rather than how to implement it using low-level OpenFlow mechanisms [21]. Using pyretic networking policies are specified for the entire network once rather than implementing that policy in individual switches.

Some features of Pyretic [21]:

1. Pyretic hides low level details by allowing programmers to express network policy as a function that takes a packet as input and return a set of new packets.
2. Pyretic allows programmer to write policies which matches packets based on Boolean predicates rather than bit patterns.
3. One of the main drawback before Pyretic was that how controller is going to do multiple tasks without interfering with other modules e.g. routing and server load balancing. To solve this Pyretic provides two composition operator viz. Sequential Composition (\gg) and Parallel Composition ($+$).

4.2.3 Nettle:

Nettle is based on the principle of functional reactive programming (FRP) which expresses languages as an electric circuit. In nettle, event based system is implemented declaratively where message streams is taken as a whole [36].

Nettle program work in terms of low-level OpenFlow concepts such as switch-level rules, priorities and timeouts. It allow composition of two independent modules but they are hard to implement and thus susceptible to network race conditions [35].

Nettle actually substitutes for the network controller i.e. Nettle is for general purpose programming of a network controller.

4.2.4 Procera:

Procera is a controller architecture and high level network control language that allows operators to express network policies without resorting to general purpose programming of a network controller. In Procera, policy layer acts as a policy engine, which provides guidance and directives to the network controller and this layers sits on top of the network controller. Procera applies the principles of functional reactive programming (FRP). Procera is an embedded domain-specific language (EDSL) in Haskell [37].

4.2.5 Hierarchical Flow Tables:

HFT allows high-level, network-wide policies that do not require knowledge of network topology [38]. Network policies in HFT are organized as trees of policy nodes which contain set of policy atoms. A policy atom is a (match, action) pair. HFT supports conflict resolution operators which are user-defined to resolve conflicting decisions. HFT translates policy trees to Network Flow Tables and uses Network Information Base to configure distributed network of switches. HFT also enables Participatory networking, in which end-users and their application propose changes to the network configuration [38]. HFT doesn't allow writing dynamic policies e.g. when topology changes or automatic reconfiguration. HFT have been used in PANE system.

4.2.6 Corybantic:

Corybantic makes use of the concept of modularity, wherein different independent modules manage different aspects of the network. Corybantic represents the physical topology of the network as a graph of resources including switches and links and modules are expressed in terms of virtual subset topologies of the underlying network topology [39]. Modules are written in Python.

Corybantic uses two search approaches to avoid problem of local optima, one is inspired by search heuristics used in genetic algorithm while second approach is about carefully defining a convex objective function for different modules. Corybantic used a multi-phase iterative approach to constantly adapt to new customer demands.

4.2.7 NetEgg:

Emphasis in NetEgg tools have been given to network operators who are actually not real programmers and thus they find it hard to program various network policies in Domain Specific Languages. NetEgg tool allows network operators to specify network policies using example behaviours [40]. In NetEgg, network operators specify policies using scenarios and it generates a policy table, multiple state tables and a

controller program. NetEgg approach is based on synthesizing an implementation automatically from examples.

4.2.8 Merlin:

Merlin provides a collection of high-level programming constructs for classifying packets, controlling forwarding paths, specifying packet-processing functions and provisioning bandwidth in terms of maximum limits and maximum guarantees [41]. Merlin allows dynamic modifications of policies using small run time components known as negotiation. Merlin uses regular expressions to specify the set of allowed forwarding paths through the network.

4.2.9 Kinetic:

Kinetic is a domain specific language (DSL) and SDN controller that enables writing network control program that capture responses to changing network conditions in a concise, intuitive and verifiable language [22].

Kinetic represents network policies in terms of a Finite State Machine (FSM). Different states correspond to distinct networking behaviour.

Kinetic uses Computation Tree Logic (CTL) and has the ability to automatically verify policies with the NuSMV model checker. Both of these empower network administrators to verify the dynamic behaviour of the controller before the control program are ever run.

Kinetic is build on top of Pyretic, an SDN programming language embedded in Python.

5 Policy Implementation with Kinetic

We have written a policy based application for the above topology in SDN, where networking path followed by packets will be defined based on priority level. Through this example we have made an attempt to show how SDN is making network flexible and how easily one can write network policies as per one's requirement.

When;

- Priority=1, path will be: h1->s1->s2->s3->s4->h2
- Priority=2, path will be: h1->s3->s4->h2
- Priority=3, path will be: h1->s4->h2

5.1 Topology Used

We have used two host, four switches and 1 controller topology for our kinetic application as shown in figure 3.

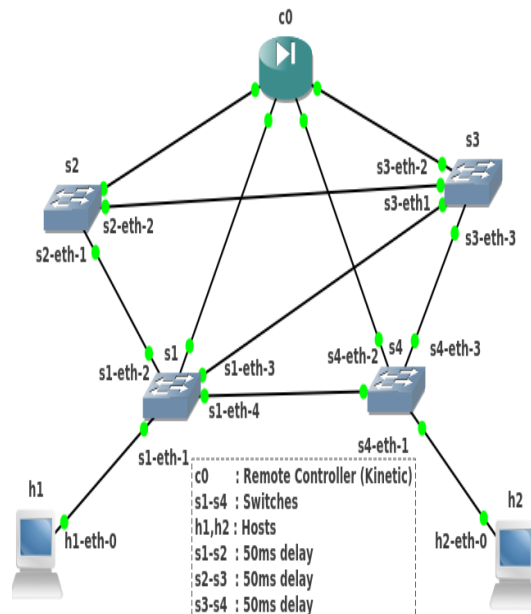


Figure 3: Topology for Kinetic Example

5.2 Ovs-ofctl-

Ovs-ofctl is the utility that comes with OpenSwitch and enables visibility and control over a single switch's flow table. It is especially useful for debugging by viewing flow states and flow counters. e.g.

dump-flows will output the following:

```
PC:~$ sudo ovs-ofctl dump-flows s1
```

```
NXST_FLOW reply (xid=0x4):
```

i.e. it return an empty flow table. This is because we have not yet started any controller for our topology.

So, if we will run ping command in mininet:

```
mininet> pingall
```

```
*** Ping: testing ping reachability
```

```
h1 -> X
```

```
h2 -> X
```

```
*** Results: 100% dropped (0/2 received)
```

Using ovs-ofctl we can also add-flows manually for switches e.g.

```
PC:~$ sudo ovs-ofctl add-flow s1 in_port=1,actions=output:4
```

```
PC:~$ sudo ovs-ofctl add-flow s1 in_port=4,actions=output:1
```

```
PC:~$ sudo ovs-ofctl add-flow s4 in_port=2,actions=output:1
```

```
PC:~$ sudo ovs-ofctl add-flow s4 in_port=1,actions=output:2
```

```
PC:~$ sudo ovs-ofctl dump-flows s1
```

```
NXST_FLOW reply (xid=0x4):
```

```
cookie=0x0, duration=49.184s, table=0, n_packets=0, n_bytes=0, idle_age=49, in_port=1
actions=output:4
```

```
cookie=0x0, duration=37.332s, table=0, n_packets=30, n_bytes=6271, idle_age=0, in_port=4
actions=output:1
```

```
PC:~$ sudo ovs-ofctl dump-flows s4
```

```
NXST_FLOW reply (xid=0x4):
```

```
cookie=0x0, duration=12.618s, table=0, n_packets=0, n_bytes=0, idle_age=12, in_port=1
actions=output:2
```

```
cookie=0x0, duration=21.419s, table=0, n_packets=3, n_bytes=557, idle_age=4, in_port=2
actions=output:1
```

In the above we have manually added flows in switches s1 and s4 using ovs-ofctl as:

```
h1(inport=eth-0)->(inport=1)s1(outport=4)->(inport=2)s4(outport=1)->(inport=eth-0)h2
```

Now after adding flows when we will run ping command in mininet :

```
mininet> h1 ping -c 2 h2
```

```
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
```

```
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.540 ms
```

```
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.070 ms
```

```
--- 10.0.0.2 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 999ms
```

```
rtt min/avg/max/mdev = 0.070/0.305/0.540/0.235 ms
```

```
mininet>
```

Now when we will start our priority application from the terminal, the controller will be up as show in fig below and we can ping host h1,h2.

```

***** NUSRV OUTPUT END *****
.
Deploy? (yes/no): yes
You entered: yes
POX 0.2.0 (carp) / Copyright 2011-2013 James McCauley, et al.
Connected to pyretic frontend.
INFO:core:POX 0.2.0 (carp) is up.
INFO:openflow_of_01:[00-00-00-00-00-04 1] connected
INFO:openflow_of_01:[00-00-00-00-00-03 2] connected
INFO:openflow_of_01:[00-00-00-00-00-02 3] connected
INFO:openflow_of_01:[00-00-00-00-00-01 4] connected
==== Count Bytes====
{}
==== Count Bytes====
{}
==== Count Bytes====
{}
==== Count Bytes====
{}
==== Count Bytes====
{}

```

Figure 4: Kinetic Controller running priority based switching application

By default policy_1 is running:

```
mininet> h1 ping -c 1 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=264 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 264.285/264.285/264.285/0.000 ms
mininet>
```

Now to change data flow to higher priority level i.e. priority_3, we can use json_sender method to tell controller externally that now data has to go on high priority path.

So we will send following event:

```
$python json_sender.py -n level -l 3 -flow="{srcip=10.0.0.1,destip=10.0.0.2}" -a 127.0.0.1 -p 50001
```

```
mininet> h1 ping -c 1 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=27.2 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 27.218/27.218/27.218/0.000 ms
mininet>
```

Similarly output for policy_2:

```
mininet> h1 ping -c 1 h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=171 ms

--- 10.0.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 171.329/171.329/171.329/0.000 ms
mininet>
```

We have defined inter-switch functions as follows:

```
def interswitchs2():
    return if_(match(inport=2),fwd(1),fwd(2))
def interswitchs3():
    match_switch =intersection([match(inport=2),match
(inport=3)])
    return if_(match_switch,fwd(1),fwd(3))
```

Here:

Syntax	Summary
fwd(a)	modify (port=a)
identity	returns original packet
match(f=v)	that a field f matches an abstract value v e.g. match(inport=2) i.e. packets comes at inport 2 of the switch

FSM description for our application is:

```
self.fsm_def = FSMDef(
    level=FSMVar(type=Type(int,set(levels)),
        init=1,
        trans=level),
    policy=FSMVar(type=Type(Policy,set([level_rate_policy(i+1)
        for i in levels ])),
        init=level_rate_policy(2),
        trans=policy))
```

NuMSV FSM model for priority application is as shown below:

```
MODULE main
VAR
    policy : {policy_1,policy_2,policy_3};
    level : {1,2,3};
ASSIGN
    init(policy) := policy_1;
    init(level) := 1;
    next(policy) :=
    case
        (level=1) : policy_1;
        (level=2) : policy_2;
        (level=3) : policy_3;
        TRUE : policy_1;
    esac;
    next(level) :=
    case
        TRUE : {1,2,3};
        TRUE : level;
    esac;
--
--
```

Finite state diagram for priority based switching is as shown below:

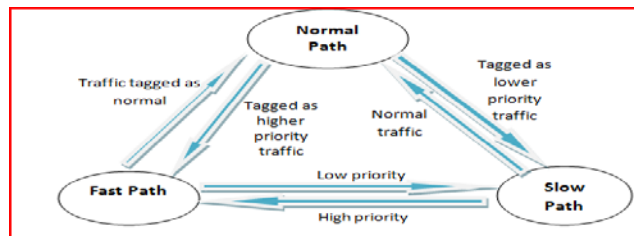


Figure 5 below shows how ping behavior varies as the priority levels for the host changes.

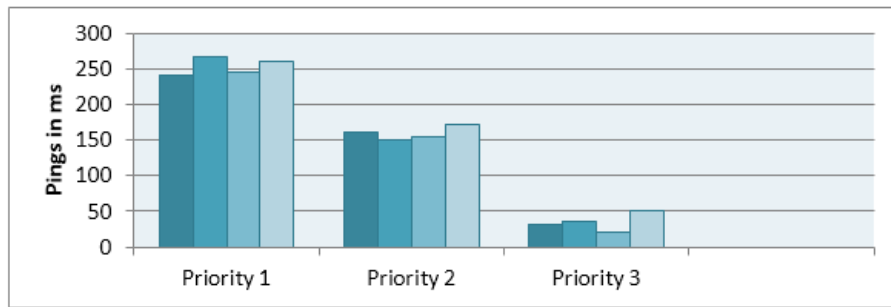


Figure 5: Ping behavior according to priority

6 SDN and Its Application Areas

6.1 SDN and Data Centers

The roots of SDN are in data centers. In general, SDN birth was mainly because of the needs of data centers. SDN has attracted many data centers operators towards it and Google has deployed SDN approach into one of its backbone WAN. The SDN deployed network has been in operation at Google and has offered benefits including higher resources utilization, faster failure handling and faster up gradation. Google has identified a number of benefits that are associated with its G-scale WAN backbone including that Google can run the network at utilization levels up to 95% [12][10].

6.2 SDN and Campus Networking

With new advent of Northbound APIs for SDN Controller like Kinetic, SDN has opened a new path to campus networking. After data centers, campus networking is the field where we require dynamic policy and network behaviour features. While with traditional network achieving a flexible network is a cumbersome process, SDN has made it an easy work. With a little line of codes, a network administrator can easily control the behaviour of network.

PROCERA a network control framework that helps operators express event-driven policies that react to various types of events [4]. In campus network, PRCOERA supports four control domains viz. Time (like peak traffic hours or session start), data usage (limiting data rate), Status (varying network speed, delay etc based on user priorities or groups) and flow (i.e. depending on to where data is going)

6.3 SDN, White-Fi and Rural Connectivity

6.3.1 SDN from India's Perspective

McKinsey Research into the internet economy has shown that internet contributes 3.4 % to GDP [44]. Further internet accounts for 21% of GDP growth over the last five years among developed countries. Moreover there was 10% increase in productivity for small and medium businesses from Internet Usage. According to 2011 Census of India, 833.5 million live in rural areas which is more than two-third of the total population and there are 111.76 million internet/ broadband subscribers[42][43]. Moreover rural internet subscribers stand at 12.89 per 100 populations. The data from the report shows that India still lacks in rural connectivity and McKinsey report [44] has revealed that how important internet is becoming for economic growth of nations. Rural areas are often ignored by network companies because the profit margins are small and it is difficult to update the required hardware [17]. Step-aside infrastructure cost, the other hindrances' in rural connectivity are network configuration, maintenance and poor road

connectivity which makes it harder for ISPs to make rural internet a profitable business by implementing specific network policies for rural areas.

With the flexibility of SDN, internet can become more widespread than it already is. The main issues with rural areas include sparse population, small profit margins and resource constraints. However recent innovations like concept of White-Fi and SDN might help to alleviate these issues. SDN can reduce Capital expenditure (CapEx) as well as Operating expenditure (OpEx) by automating network functions, technology-agnostic connections, network aware applications and software-based functionality [4][8][17][45].

The separation of network construction and network configuration allows companies to decrease start-up costs in rural environments thus making rural networking a profitable business.

White-Fi technology:

1. White-Fi technology uses the unused spectrum in frequencies utilized for broadcasting of television signals and uses it for the internet. These unused spaces are called white spaces [26][27].
2. The 200-300 MHz spectrum in the white space can reach up to 10 km as compared to current Wi-Fi technology that allows a range of only about 100 meters.
3. It can be run on solar power and thus overcome a key hindrance that currently impedes ISPs namely the high cost of installation equipment.

Thus with the advent of White-Fi technology and flexibility of SDN, rural connectivity can become more profitable and more companies will be willing to give access to more and more rural areas.

7 Conclusion

With the exponential growth of Internet user base and need for green networking, network flexibility has become an important aspect of networking field. SDN has successfully managed to pave the way towards a next generation networking, which is flexible and provides network operators to implement various kinds of network policies in a simple programming fashion without digging into specific low-level details of network devices. SDN has appeared to be a success not only in data center networking or cloud networking but also in other fields like campus networking or rural networking etc. SDN is more cost-effective, more performance oriented as well as flexible. SDN gives network administrators freedom to implement policy driven mechanisms in campus or data centers as well as allows companies to decrease start-up costs in rural areas thereby making rural networking a profitable business. Moreover with the usage of White Fi technology as communication medium and SDN as network architecture, Rural Connectivity will become more economical feasible and can easily be optimized. With high level abstraction of Northbound APIs like Kinetic and Pyretic SDN has certainly change the policy making field which is rigid and vendor specific in traditional networks. This has also opened various opportunities for implementation of green networking. For example our priority based application has shown that how easily network administrator can implement network policy configurations as per requirement which is not possible in traditional networks.

REFERENCES

- [1] Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to sdn: an intellectual history of programmable networks." *ACM SIGCOMM Computer Communication Review* 44.2 (2014): 87-98.
- [2] Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." *Proceedings of the IEEE* 103.1 (2015): 14-76.
- [3] Open Networking Foundation. *SDN Architecture Overview, Version 1.0* December 12, 2013
- [4] Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *Communications Magazine, IEEE* 51.2 (2013): 114-119.
- [5] Nunes, B., et al. "A survey of software-defined networking: Past, present, and future of programmable networks." (2014): 1-18.
- [6] Jarraya, Yosr, Taous Madi, and Mourad Debbabi. "A survey and a layered taxonomy of software-defined networking." (2014): 1-1.
- [7] Agarwal, Sugam, Murali Kodialam, and T. V. Lakshman. "Traffic engineering in software defined networks." *INFOCOM, 2013 Proceedings IEEE. IEEE*, 2013.
- [8] Zinner, Thomas, et al. *A Compass Through SDN Networks*. Tech. Rep. 488, University of Würzburg, 2013.
- [9] Shenker S. *The future of networking and the past of protocols*, Open Networking Summit, Palo Alto, CA, USA: Stanford University; October 2011
- [10] Nirmalan Arumugam; *The Thinking Network-Software Defined Networks will provide the intelligence the network needs to keep up in a cloud centric world*. Available online: [www.wipro.com/documents/insights/the-thinking-network.pdf]
- [11] Gautam Khetrpal and Saurabh Kumar Sharma; *Demystifying Routing Services in Software-Defined Networking*; Available online: [http://www.aricent.com/sites/default/files/pdfs/Aricent-Demystifying-Routing-Services-SDN-Whitepaper.pdf]
- [12] Jain, Sushant, et al. "B4: Experience with a globally-deployed software defined WAN." *ACM SIGCOMM Computer Communication Review*. Vol. 43. No. 4. ACM, 2013.
- [13] Open Networking Foundation Available online: [https://www.opennetworking.org/sdn-resources/openflow]
- [14] Foundation, Open Networking. "Software-defined networking: The new norm for networks." *ONF White Paper* (2012).
- [15] HP OpenFlow Protocol Overview; *Technical Solution Guide* Version: 1 September 2013.

- [16] Specification, OpenFlow Switch. "Version 1.1. 0 Implemented (Wire Protocol 0x02)." Available online: [<http://archive.openflow.org/documents/openflow-spec-v1.1.0.pdf>]
- [17] Hasan, Shaddi, et al. Enabling Rural Connectivity with SDN. Technical Report UCB/ECS-2012-201, University of California at Berkeley, 2012.
- [18] Limoncelli, Thomas A. "Openflow: a radical new idea in networking." Queue10.6 (2012): 40.
- [19] [Vaughan-Nichols, Steven J. "OpenFlow: The next generation of the network?"Computer 44.8 (2011): 13-15.
- [20] Stallings, William. "Software-defined networks and openflow." The Internet Protocol Journal 16.1 (2013): 2-14.
- [21] Reich, Joshua, et al. "Modular sdn programming with pyretic." Technical Reprot of USENIX (2013).
- [22] Kim, Hyojoon, et al. "Kinetic: Verifiable Dynamic Network Control."
- [23] Steve Garrsion Emerging Use Cases for SDN; February 2015. Available online: [<https://www.sdxcentral.com/articles/contributed/emerging-use-cases-for-sdn-steve-garrison/2015/02/>]
- [24] Qazi, Zafar Ayyub, et al. "Application-awareness in SDN." ACM SIGCOMM Computer Communication Review. Vol. 43. No. 4. ACM, 2013.
- [25] Jarschel, Michael, et al. "Sdn-based application-aware networking on the example of youtube video streaming." Software Defined Networks (EWSDN), 2013 Second European Workshop on. IEEE, 2013.
- [26] <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11af-white-fi-tv-space.php>
- [27] Bahl, Paramvir, et al. "White space networking with wi-fi like connectivity." ACM SIGCOMM Computer Communication Review 39.4 (2009): 27-38.
- [28] <http://searchsdn.techtarget.com/guides/Northbound-API-guide-The-rise-of-the-network-applications>
- [29] Internet Live Stats <http://www.internetlivestats.com/>
- [30] Raghavan, Barath, and Justin Ma. "The energy and emergy of the internet."Proceedings of the 10th ACM Workshop on Hot Topics in Networks. ACM, 2011.
- [31] Kaup, Fabian, Sergej Melnikowitsch, and David Hausheer. "Measuring and modeling the power consumption of OpenFlow switches." Network and Service Management (CNSM), 2014 10th International Conference on. IEEE, 2014.
- [32] Imaizumi, Hideaki, and Hiroyuki Morikawa. "Directions towards future green Internet." Towards Green Ict 9 (2010): 37.

- [33] Baliga, J., et al. "Photonic switching and the energy bottleneck." *Photonics in Switching*. Vol. 2007. 2007.
- [34] Foster, Nate, et al. "Languages for software-defined networks." *Communications Magazine*, IEEE 51.2 (2013): 128-134
- [35] Foster, Nate, et al. "Frenetic: A network programming language." *ACM SIGPLAN Notices*. Vol. 46. No. 9. ACM, 2011.
- [36] Voellmy, Andreas, Ashish Agarwal, and Paul Hudak. *Nettle: Functional reactive programming for openflow networks*. No. YALEU/DCS/RR-1431. YALE UNIV NEW HAVEN CT DEPT OF COMPUTER SCIENCE, 2010.
- [37] Voellmy, Andreas, Hyojoon Kim, and Nick Feamster. "Procera: a language for high-level reactive network control." *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012.
- [38] Ferguson, Andrew D., et al. "Hierarchical policies for software defined networks." *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012.
- [39] Mogul, Jeffrey C., et al. "Corybantic: Towards the modular composition of sdn control programs." *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*. ACM, 2013.
- [40] Yuan, Yifei, Rajeev Alur, and Boon Thau Loo. "NetEgg: Programming Network Policies by Examples." *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*. ACM, 2014.
- [41] Soulé, Robert, et al. "Merlin: A language for provisioning network resources." *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. ACM, 2014.
- [42] Indian Telecom Services Performance Indicator Report for the Quarter ending March, 2015
- [43] India Census 2011: Census of India: Census Data Online censusindia.gov.in/2011-common/censusdataonline.html
- [44] Manyika, James, et al. *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*. McKinsey & Company, 2011.
- [45] Fujitsu; *Software-Defined Networking for the Utilities and Energy Sector* Available online: [<http://www.fujitsu.com/us/Images/SDN-for-Utilities.pdf>]

Efficient Cooperative MAC and Routing in Wireless Networks

¹Shamna H R and ²Lillykutty Jacob

¹Government Engineering College Barton Hill, Thiruvananthapuram, India;

²National Institute of Technology Calicut, Kozhikode, India

shamnahr@gmail.com; lilly@nitc.ac.in

ABSTRACT

Cooperative communication refers to the collaborative processing and retransmission of the overheard information at those stations surrounding the source. It exhibits various forms at different protocol layers and introduces many opportunities for cross layer design and optimization. To fully reap the benefits of cooperative communications in wireless networks, the entire protocol stack - physical, MAC, and routing protocols - should be carefully redesigned or reengineered. In this paper, we first propose a cooperative MAC protocol by enhancing IEEE 802.11 DCF with minimal modifications to maximize the benefit of cooperative diversity. Its performance is compared to that of an existing cooperative MAC and legacy 802.11 DCF protocols and shown to be superior. We also propose a cluster based cooperative routing protocol which has minimal control overhead and time consumed in establishing the cooperative paths. Through extensive simulations, the performance of the proposed protocols are evaluated and compared to other combinations of MAC and routing protocols.

Keywords: Cooperative MAC, Cooperative Routing, End-to-End Delay, Energy Efficiency, Cross-Layer Design

1 Introduction

Cooperative networking has recently received significant attention as an emerging network design strategy for future wireless networks to cost-effectively provide multimedia services. In cooperative networking, individual network nodes cooperate to achieve network goals in a coordinated way. Cooperative transmission, which is a form of distributed spatial diversity, can offer more reliable communications, increased network capacity, extended coverage area, and more efficient communication. However, the higher layer protocols of cooperative networks must be properly designed to realize the advantages [1-3].

Most cooperative transmission schemes involve two phase of transmission: a coordination phase, where nodes exchange their own source data and control messages with each other and/or the destination, and a cooperation phase, where the nodes cooperatively retransmit their messages to the destination. In Figure 1, in the coordination phase (i.e., Phase I), the source node broadcasts its data to the relay nodes and the destination node and, in the cooperation phase (i.e., Phase II), the relay nodes forward the source's data (either by themselves or by cooperating with the source) to enhance reception at the destination. The nodes may interchange their roles as source and relay at different instants in time. To

enable such cooperation among nodes, different relay technology can be employed depending on the relative node locations, channel conditions, and transceiver complexity. Decode-and-forward, amplify-and-forward, coded cooperation, and compress-and-forward are some of the basic cooperative relaying techniques.

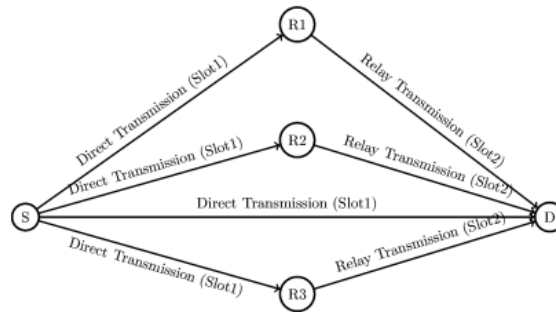


Figure 1: Cooperative Communication

The innovation of cooperative communications is not confined only to physical layer. It is available in various forms at different higher protocol layers. The cooperative MAC protocols developed in the recent years show how the benefits of cooperative diversity can be achieved by modifying the IEEE 802.11 distributed coordination function (DCF) [4-11]. Routing algorithms which are based on the cooperative communications are known as cooperative routing algorithms [12-15]. These approaches perform well in physical, MAC or Network layer separately; however, the performance can be further improved by using cross-layer methods. The cross layer approaches proposed in [16-18] consider the cross-layer optimization of physical and MAC layers.

While cooperative communication can improve network performance, it can also incur considerable overhead. This overhead includes : (i) signaling and network control overhead for cooperating entities selection and coordination; (ii) additional required resources such as bandwidth for relay transmission; (iii) energy consumption at the cooperating entities; (iv) time consumed in selecting the cooperating entities and establishing the cooperative paths; and (v) the overall added complexity to the communication and networking process [3]. Reduction of these various forms of cooperation overhead will have great impact on the cooperative network performance.

In this paper, we propose a cooperative MAC protocol for multihop networks. The proposed protocol is backward compatible with the legacy 802.11 DCF protocols. The protocol requires minimum modification to the data packet header and control packets. The simulation results show that the proposed MAC protocol achieves significant throughput improvement compared to CoopMAC (Liu et al (2007)) and IEEE 802.11 DCF protocols in single hop networks. We study the TCP performance in a multihop wireless network with the proposed cooperative MAC for channel access and show improved performance over that using legacy 802.11 DCF. We also propose a cluster based cooperative routing protocol which reduces the overhead involved in route establishment and maintenance. Extensive simulation results show that in a multihop network, the proposed cooperative MAC and cluster based routing protocols increase the end-to-end throughput and packet delivery ratio.

The rest of the paper is organized as follows. A brief description of the related works in cooperative network protocols is given in Section 2. The proposed MAC and routing protocols are presented in Section 3 and Section 4, respectively. Simulation results are discussed in Section 5. Conclusion and future work are presented in Section 6.

2 Related Work

The Cooperative MAC (CoopMAC) protocol for wireless LANs [6-8] is based on the idea of transforming a slow one-hop transmission into a faster two hop transmission, thereby decreasing the transmission time for the traffic being handled. Pei et al [16] studied how the physical layer cooperation can be integrated with the MAC sublayer for dramatic improvements in throughput and interference. The CoopMAC protocol with diversity combining is introduced in this article. When receiver combining is enabled, the relay can forward packets at a rate equal to or greater than the one that it adopts in CoopMAC where combining is not possible. Liu et al [6] verified by analysis and simulations that CoopMAC for infrastructure WLAN can achieve substantial throughput and delay performance improvements over legacy IEEE 802.11.

Korakis et al [7] extended CoopMAC into the ad hoc network environment. The implementation of CoopMAC and its performance and challenges in a real environment were reported in [8]. In [19], the authors have extended the saturation throughput analysis of CoopMAC to the non saturated network case. In [18], the authors have proposed a MAC protocol design for distributed cooperative wireless networks. They focused on beneficial node cooperation by addressing two fundamental issues of cooperative communications, namely, when to cooperate and whom to cooperate with, from a cross-layer protocol design perspective. Taking account of protocol overhead, they explored a concept of cooperation region, whereby beneficial cooperative transmissions can be identified. To increase network throughput, they proposed an optimal grouping strategy for efficient helper node selection, and devised a greedy algorithm for MAC protocol refinement.

The authors of [5] have developed rDCF protocol which enables packet relaying in the ad hoc mode of 802.11 systems by requesting each station to broadcast the rate information between stations explicitly. The rDCF exploits the physical layer multi-rate capability by enabling the sender, relay and receiver nodes coordinate to decide what rate to use and whether to use a relay node. Through simulation, the delay and throughput performance were investigated but not the energy efficiency.

Adam et al [9] have presented a Cooperative Relaying Medium Access protocol (CoRe-MAC) as an extension to CSMA/CA which addresses resource reservation, relay selection, and cooperative transmission while keeping the overhead in terms of time and energy low. They analyzed the efficiency of this protocol for packet error rate, throughput, and message delay in a multihop network. In the case of unreliable communication links, performance improvement occurs. However, for good SNR between source and destination, CoRe-MAC has similar performance as the standard CSMA/CA.

In [20], the authors have proposed a cooperative relaying without the symbol-level synchronization constraint, called Distributed Asynchronous Cooperation (DAC). With DAC, multiple relays can schedule concurrent transmissions with packet-level (hence coarse) synchronization. The receiver then extracts multiple versions of each relayed packet via a collision resolution algorithm, thus realizing the diversity gain of cooperative communication. They also designed a simple MAC protocol to exploit the benefit of DAC, and a generic approach to incorporate DAC relaying into existing routing protocols.

Cooperation may not be beneficial in certain scenarios, and hence it is crucial to develop adaptive MAC that uses cooperation only when it is needed. The authors Shan & Zhuang [17] have shown that cooperation is beneficial only when the source-destination link has a low transmission rate and/or the payload length is large enough compared to the signaling overhead for cooperation. In general, the cooperation decision at the MAC layer depends on the link quality measurements and achieved throughput. Hence, cross layer design between the PHY and MAC layers is required. MAC protocol should address the challenging issue of how to schedule the transmissions from the cooperating entities and their neighbors to avoid collisions.

The routing protocol in a cooperative network should be designed to use all cooperating entities between the source and destination nodes. A route from the source to destination becomes a sequence of cooperative links. The routing problem can be viewed as a multi-stage decision making; at each stage, the decision is to select the transmitting and receiving set of nodes [21]. The two major challenges in developing a cooperative routing protocol are the high computational complexity and the increased interference in the presence of multiple flows. Cross-layer design between the routing and MAC protocols can be beneficial to resolve the multi-flow throughput degradation issue of cooperative routing.

A novel decentralized cross-layer multi-hop cooperative protocol, namely, Routing Enabled Cooperative Medium Access Control (RECOMAC) was proposed in [22]. The protocol architecture makes use of cooperative forwarding methods, in which coded packets are forwarded via opportunistically formed cooperative sets within a region, as RECOMAC spans the physical, MAC and routing layers. Randomized space-time coding is exploited at the physical layer to realize cooperative transmissions, and cooperative forwarding is implemented for routing functionality, which is submerged into the MAC layer, while the overhead for MAC and route set up is minimized. However, it is not compatible with the conventional architecture with non-cooperative transmissions.

The problem of transmission-side diversity and routing in a static wireless network was studied by Amir et al [12]. They formulated the problem of finding the minimum energy cooperative route using dynamic programming (DP). The optimal algorithm, namely, Cooperation along the Minimum Energy Non-Cooperative Path (CAN), turned out to be computationally intractable. Hence, they proposed two suboptimal algorithms, CAN-I, and Progressive cooperation (PC-I).

Two cooperation-based routing algorithms, namely, Minimum-Power Cooperative Routing (MPCR) algorithm and Cooperation Along the Shortest Non-Cooperative Path (CASNCP) algorithm were proposed by Ibrahim in [13]. The MPCR algorithm takes into consideration the cooperative communications while constructing the minimum power route. The CASNCP algorithm is similar to CAN-I and PC-I, as it finds the shortest path route (SPR) first and then applies cooperative communications upon the SPR to reduce the transmission power.

In [14], the authors have proposed two MAC protocols (Repetition coding with maximal ratio combining MAC (MRC - MAC), Space time coding MAC(STC MAC)) and two routing protocols (Cooperative Routing Protocol (CRP), Enhanced CRP (E-CRP)). MRC-MAC is the MAC protocol to support repetition coding with MRC at the physical layer. STC-MAC is the MAC extension to support space-time coding. In the MRC-MAC and STC-MAC protocols, they assume that each hop's source, destination and two relay nodes are known to the MAC layer. CRP is based on the widely used AODV routing protocol in wireless ad-hoc networks.

The performance evaluation through simulation shows the need to incorporate adaptive decision whether to invoke cooperative relaying on each hop.

In [15], the authors have proposed and investigated a new distributed cooperative routing algorithm that realizes minimum power transmission for each composed cooperative link, given the link BER constraint at a certain target level. The key contribution of the proposed scheme is to bring the performance gain of cooperative diversity from the physical layer up to the networking layer.

The above mentioned cooperative routing protocols are all designed based on minimization of the total transmitted power. Other link costs including delay, bandwidth and link life time need to be considered. Cross layer designs to resolve the multi flow throughput degradation issue with cooperative routing also need to be addressed.

3 Cooperative MAC Protocol for Multihop Networks (M-CMAC)

We propose a cooperative MAC protocol for multihop networks. Like CoopMAC [6], in our protocol also, high data rate stations assist low data rate stations in their transmission by forwarding their traffic. A helper is selected such that two fast hop transmissions replaces one slow hop transmission. The helper with the best two hop transmission rate, which is having minimum delay for data transmission from source to helper and from helper to destination, is considered as the best helper and selected as neighbor node for that particular source-destination pair. It is assumed that the location information of the nodes are known so that the euclidean distance between every pair of nodes can be computed. Since the data rate of a link is related to the distance between the nodes, the computed distances can be easily converted to the corresponding data rates. Every node in the network maintains a cooperative table (CT) of potential helpers, which contains the MAC address of all destinations that can be reached through a single hop transmission, the direct euclidean distance to the destination, the MAC address of the helper (if a helper is present), and the total distance through the helper. If no helper is available, the helper address is same the destination address. A simple example network is shown in Figure 2, and Table 1 shows the format of CT for the network shown in Figure 2.

It is backward compatible with legacy 802.11 DCF, and has minimal modification to the data frame (MAC Protocol data unit) header and the RTS-CTS control frames. When a source node has data to send, it checks in its CT whether a helper exists for that particular destination. If a helper exists, then the source sends an RTS message to the helper, reserving the channel for a duration corresponding to single hop transmission. The format of RTS message used in our proposed protocol is shown in Figure 3.

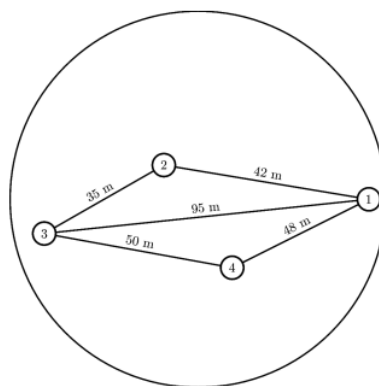


Figure 2: Helper Selection in M-CMAC Protocol

Table 1: Cooperative Table at Node 3

MAC Address of Destination	Helper Address	Direct Distance	Distance via Helper
1	2	95	77
2	2	35	-
4	4	50	-

The source saves the address of the destination node in the helper address field and the helper address is stored as the destination address. When an RTS message is received, the nodes will check the helper address field and destination address field. If the helper address field is different, then the node infers that it has to act as a helper for another node. If the helper is willing to forward the data, then it will send a CTS back to the source. The source will send the data packet to the helper if the CTS message is received. The format of MAC-PDU header is shown in Figure 4. The address of the helper is entered in the Destination address field and the original destination's MAC address is stored in the Address 3 field. Source address is saved in the Source Address field. When this packet reaches the helper, it checks the Destination address field of the MAC header and address in the field Address 3. If both are different, then the helper will copy its own address to the Source address field and the address in Address 3 field is stored in the Destination Address field. It also sends an ACK to the source to indicate the success of packet reception. Then the helper will send an RTS message to the destination and reserves the channel for single hop transmission. When this RTS message is received, the destination will send a CTS back to the helper. The helper then forwards the packet received from the source, to the destination. The destination will send an ACK to helper if the packet is received.



Figure 3 : RTS Frame Format

Unlike CoopMAC, where the channel is reserved for two hop transmissions and therefore the neighbors of source, helper and destination have to defer their transmissions until then, in our protocol, the reservation is for one hop each time. Thus there is increased number of parallel transmissions (i.e., channel reuse) in the case of our protocol.



Figure 4: MAC PDU Header Format

4 Cluster Based Cooperative Routing (CBCR) Protocol

We propose a cluster based cooperative routing protocol with the multi-hop data forwarding function realised at the link layer, where we have cooperative links (using M-CMAC described in Section 3). We use the term cluster to denote a group of nodes that can communicate with each other through a single hop transmission, and the term routing relays to denote the nodes within each cluster that forwards the packet to the next hop. A routing relay belongs to two or more clusters at the same time. The protocol involves two stages: routing relay selection phase and data forwarding phase.

4.1 Routing Relay Selection Phase

Every node in the network broadcasts periodical beacon messages to inform its presence to the neighbors. The beacon message carries the nodes's MAC address. Each node builds a relay table which includes all the neighbouring nodes it can communicate with. Each node will broadcast its neighbor list to its neighbors if any entry in the list has changed since the last broadcast. The first column of the relay table of any node X contains the MAC address of the neighboring nodes of node X. The row corresponding to each neighboring node contains the MAC addresses of all the neighbors of the neighboring node.

The routing relays are selected independently by each node, based only on its own relay table. A node is selected as relay if it connects the highest number of nodes, i.e., the longest row, or it connects nodes that are not connected by the previously selected relay nodes. Let $\{N\}$ denotes the set of all nodes that are within the single hop transmission range of Node X and $\{D\}$ denotes the set of all nodes that can be reached through the nodes in N . Let count represents the number of elements in $\{N\}$. $\{B\}$ is the set of routing relays and R_i denotes the node in the first column of row i. The algorithm to find the routing relay is explained in Algorithm 1. Before applying the algorithm, the table has to be sorted in the decreasing order of the number of neighboring nodes. ie, the details of the neighboring node that has the maximum number of neighbors is placed first. If two or more nodes have the same number of neighbors, then they are arranged in the increasing order of MAC address.

Algorithm 1 : Relay Selection Algorithm

```

1: Initialize  $\{B\} = R_1$  .
2:  $\{D\} = \{D\} - \{ \text{Neighbors of } R_1 \}$ 
3: if  $\{D\} = \emptyset$  then goto 11
4: else
5:  $i \leftarrow 2$ 
6: while ( $\{D\} = \emptyset \ \& \ i \leq \text{count} + 1$ ) do
7: if  $(\{D\} \cap \{ \text{Neighbors of } R_i \}) = \emptyset$  then
8:  $\{D\} = \{D\} - (\{D\} \cap \{ \text{Neighbors of } R_i \})$ 
9:  $\{B\} = \{B\} \cup R_i$ 
10:  $i \leftarrow i + 1$ 
11: End

```

For the multi hop network shown in Figure 5, the contents of the relay table for Node 3 is given in the Table 2. Node 8 and Node 6 are selected as the routing relays by Node 3.

4.2 Data Forwarding Phase

When a node has a packet to send, it first checks whether the destination is in the same cluster. If the destination is in the same cluster, then it checks if a helper exists for this particular destination. If a helper exists, then the packet is transmitted to the helper. If no helper is available, then the packet is transmitted directly to the destination.

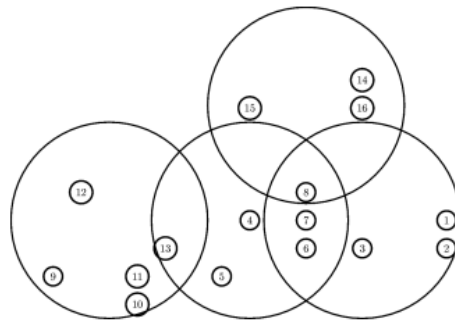


Figure 5: Cluster Selection in CBCR Protocol

If the destination belongs to a different cluster, then it searches the relay table to find if the destination can be reached through any of the routing relays. If the destination can be reached through any routing relay, the packet is forwarded to the routing relay. The packet is send to the routing relay via a helper, if a helper node exists for this routing relay. Otherwise, it is forwarded directly to the routing relay.

Table 2: Structure of Relay Table at Node 3

MAC Address of Node	Neighbor Nodes					
3	1	2	6	7	8	
1	2	3				
2	1	3				
6	3	4	5	7	8	
7	3	4	5	6	8	
8	3	4	6	7	15	16

If the destination cannot be reached through any of the routing relays, then the node multicasts the packet to all the routing relays.

5 Simulation Results

The proposed M-CMAC protocol described in Section 3 and the proposed CBCR protocol described in Section 4 have been implemented in the NS2 network simulator. Performance evaluation using these implementations are discussed in this section. A network topology of 1000 x 1000 square meter is considered. Nodes are uniformly and independently distributed at random locations. Simple path loss model is considered for wireless channel and IEEE 802.11g parameters are used for the experiments. The data rates for different transmission ranges as per IEEE 802.11g are shown in the Table 3. The simulation parameters are listed in Table 4

Table 3: Rate vs Range

Data Rate (Mbps)	6	9	12	18	24	36	48	54
Maximum Range (Meter)	100	84	77	63	51	39	34	26

Table 4: Simulation Parameters

MAC Header	240 bits
RTS	208 bits
CTS	112 bits
ACK	112 bits
Data Rate for MAC Header	6 Mbps
Slot Time	20 μ s
SIFS	10 μ s
DIFS	50 μ s
CWMin	31 slots
CWMax	1023 slots
Rety Limit	6

5.1 Performance of M-CMAC Protocol

Any node in the network can act as source node and all the nodes which are in the transmission range of a given source node are considered as destinations. Distance between the source and destination nodes are calculated and recorded as direct one hop distance in the cooperative table of the given source node. Since data rate of link is related to distance between the nodes, a helper is selected such that two fast hop transmissions replaces one slow hop transmission. The helper with the best two hop transmission rate which is having minimum delay for data transmission from source to helper and from helper to destination, is considered as best helper and selected as neighbor node for that particular source-destination pair. Figure 6 shows the relationship between the number of nodes and the overall throughput for legacy 802.11 DCF, CoopMAC and the proposed M-CMAC at a fixed payload size (1000 bytes). For 802.11 DCF network, as number of nodes increases, the throughput of network increases linearly. For CoopMAC and M-CMAC protocols, as the number of nodes increases, the availability of helpers for forwarding data packets increases and hence these protocols have better throughput compared to 802.11 DCF. This increase in throughput is due to the increase in availability of helper nodes which results in faster two hop transmission instead of single one hop transmission. The proposed M-CMAC protocol has significantly higher throughput than the CoopMAC, because of the increased channel reuse as mentioned in Section 3.

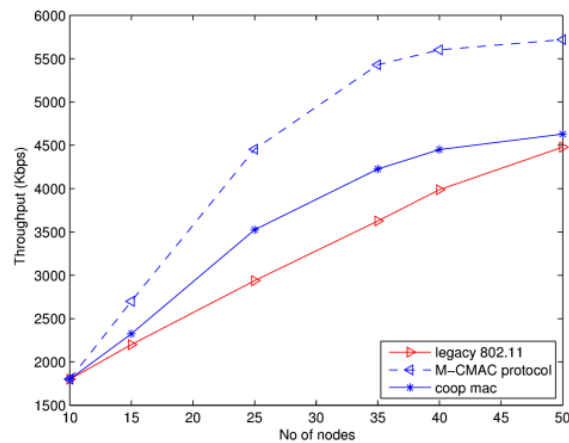


Figure 6 : Throughput vs Number of Nodes

The relationship between throughput and packet size is shown in Figure 7. When the packet size is smaller, throughput of the network is low. As the packet size increases, the throughput increases linearly and then saturates for a packet size above 1200 bytes. Again, a significant improvement with the M-CMAC protocol over the CoopMAC is obvious.

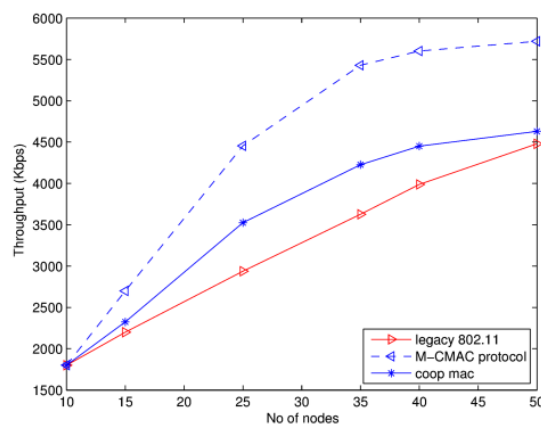


Figure 7: Throughput vs Packet Size

It is observed that the proposed protocol for adhoc networks can achieve significant throughput compared to CoopMAC and legacy 802.11 protocols. This increased throughput is due to the increased number of parallel transmissions (channel reuse) in the network. In CoopMAC, the channel is reserved for two hop transmission and therefore the neighbors of source, helper and destination have to defer their transmissions for the corresponding durations. Also in CoopMAC, the neighbors of the source node will set the NAV for a duration corresponding to the time for direct transmission between source and destination. The probability for RTS collisions are also higher for CoopMAC. In the case of our protocol, the nodes which are not in the transmission range of source and helper can transmit packets parallelly, when the source is sending packets to the helper. The nodes which are not in the transmission range of destination and helper can transmit packets parallelly, when the helper forwards the packet to the destination.

Figure 8 presents the cumulative distribution function for the packet delay in single hop adhoc network. The simulation is for a network of 40 nodes with a packet size of 1500 bytes. 16 nodes are generating packets at a rate of 1 Mbps. We can see that the delay of our protocol is significantly lower than that of legacy 802.11. This is because both M-CMAC and the CoopMAC decrease the transmission time of slow rate frames and thus more frames can be transmitted in a given period of time, a fact that decreases the queuing and service time of the frames. CoopMAC has better delay performance than the proposed protocol. This is due to the fact that contention for the medium has to be performed twice in the proposed protocol (from source to helper and helper to destination) when compared to single contention in CoopMAC.

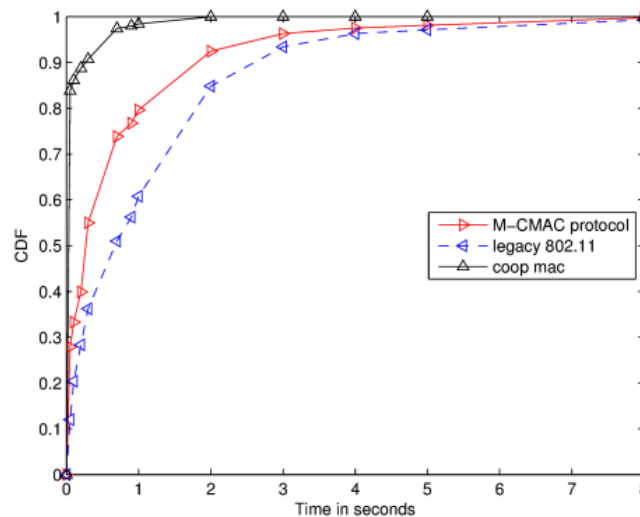


Figure 8 : CDF of Delay

The performance of UDP over the proposed MAC protocol for multihop networks is shown in Figure 9. We considered random network topology with varying number of nodes, 40 percentage active sources, 1500 bytes packets, and AODV routing protocol.

In [23], the authors study TCP performance in a multihop network using IEEE 802.11 DCF for channel access. They show that for a given network topology and flow patterns, there exists an optimal window size at which TCP achieves highest throughput via maximum spatial reuse of channel. However, TCP grows its window size beyond the optimal value, leading to throughput reduction. The relationship between TCP window size and throughput over the proposed protocol in multihop wireless networks for random network topologies were investigated (which are not shown in this paper). The relationship between packet size and throughput for 2 and 4 active TCP flows are shown in Figure 10. Our proposed M-CMAC provides significant increase in TCP throughput compared to 802.11 DCF, in all the cases.

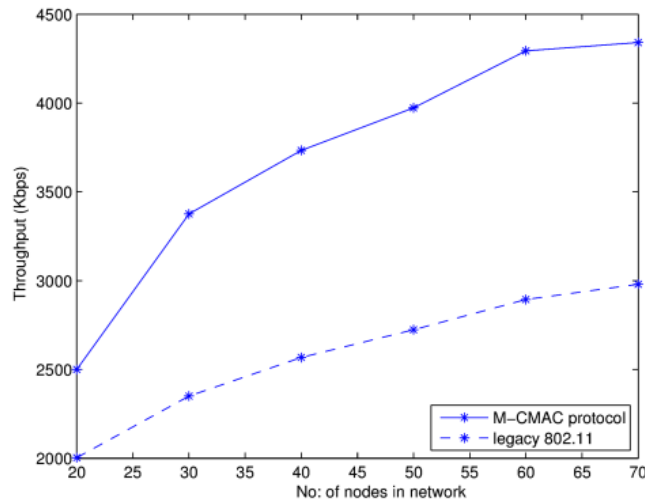


Figure 9: UDP Performance

5.2 Combined Performance of M-CMAC and CBR Protocols

The number of nodes are varied from 10 to 100 for the following results. Source nodes are assumed to generate CBR traffic of 0.5 Mbps, and 512 bytes packet size is considered. Only 20 percentage of the total nodes are generating traffic. The destination nodes are randomly chosen.

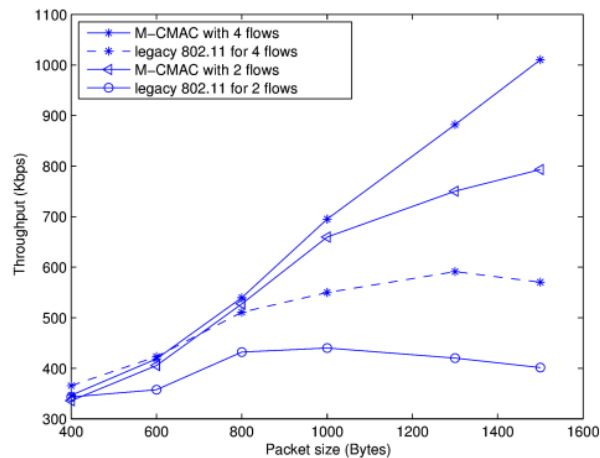


Figure 10 : TCP Performance with varying Packet size (bytes)

The performance of four combinations of MAC and routing protocols are compared : (i) AODV routing and legacy 802.11 MAC protocols; (ii) AODV routing and the proposed M-CMAC protocols; (iii) Proposed CBR and legacy 802.11 MAC protocols; (iv) Proposed CBR and the proposed M-CMAC protocols. Throughput versus number of nodes for the different combinations of the protocols are shown in Figure 11. From the figure, we can see that higher throughput can be achieved in a multi hop network by combining cluster based cooperative routing protocol and the proposed cooperative MAC protocol. The maximum throughput is obtained when the number of nodes is around 70. After that the throughput decreases.

For the remaining experiments, we considered only the proposed M-CMAC at the link layer, and compared the performance of the proposed CBCR with AODV. The average end-to-end delay for a packet is shown in Figure 12. The total delay is slightly higher for the proposed routing protocol. The proposed routing protocol achieves better packet delivery ratio compared to AODV routing protocol. This is shown in Figure 13.

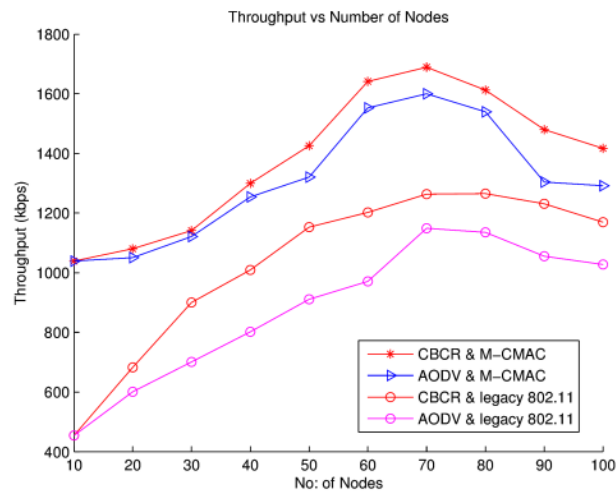


Figure 11: Throughput vs Number of Nodes

The variation of the per node energy consumption with number of nodes is illustrated in Figure 14. As the number of nodes increases, the per node energy consumption decreases. It is also observed that, compared to AODV, the energy consumption for CBCR is low and this reduction is more prominent with large number of nodes. The distribution of energy consumption in the network and its variation with number of nodes are illustrated in Figure 15 and Figure 16 for AODV and CBCR respectively. The nodes are divided into 4 bins based on energy consumption: ie $< 25\%$, $25 - 50\%$, $50 - 75\%$, $\geq 75\%$ of their initial energy. Z axis shows the number of nodes falling in each bin. It is observed that, in the case of AODV, as the number of nodes increases, majority of nodes fall under the category of $50 - 75\%$ energy consumption, and only a small number of nodes fall under the other categories. In contrast, in the case of CBCR protocol, with large number of nodes, the number of nodes consuming $50 - 75\%$ of their initial energy and those consuming $25 - 50\%$ of their initial energy approach same values. In other words, the energy consumption is more uniformly distributed in the network, thus avoiding the premature death of some nodes and enhancing the lifetime of the network.

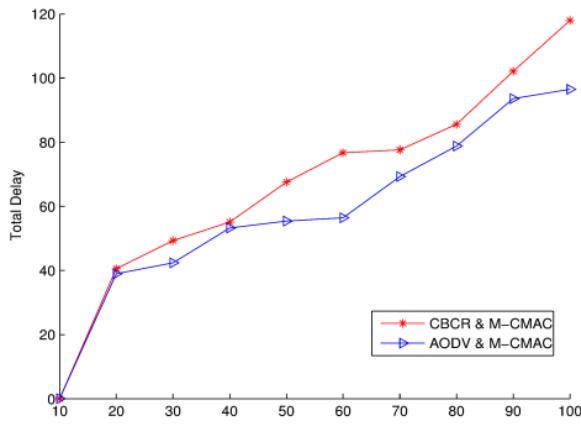


Figure 12: Average End to End Delay

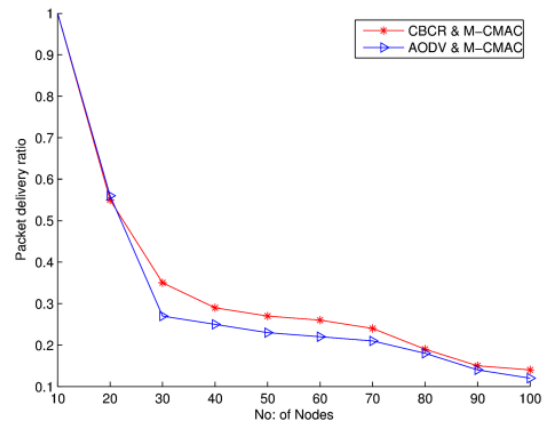


Figure 13: Packet Delivery Ratio

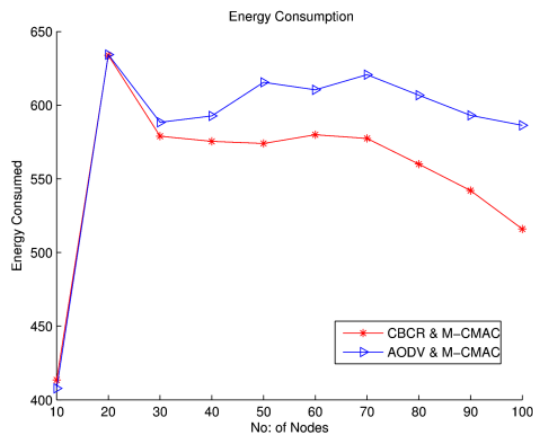


Figure 14 : Energy Consumption

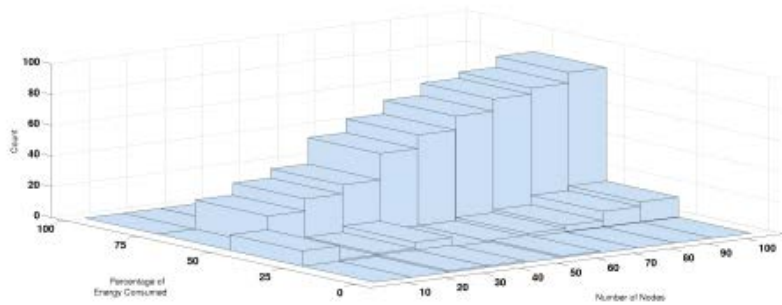


Figure 15 : Energy Distribution for AODV

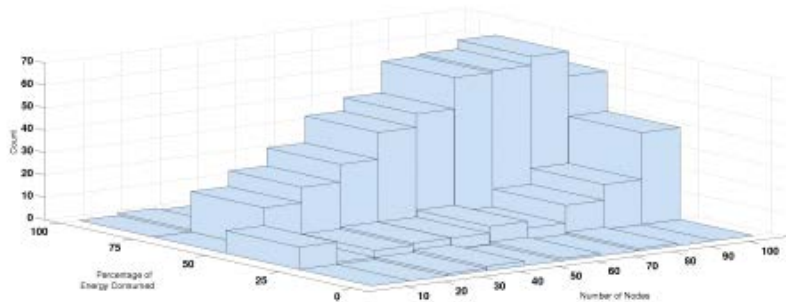


Figure 16 : Energy Distribution for CBCR

6 Conclusion

To extend the benefits of cooperative diversity at the physical layer to the higher layers of the cooperative wireless networks, we proposed an IEEE 802.11 DCF compatible cooperative MAC protocol and a minimal overhead cooperative routing protocol. Through extensive simulations, performance of the proposed protocols were evaluated in terms of throughput, delivery ratio, end-to-end delay and energy distribution. The delay performance is expected to be much better in actual network deployment, as the proposed routing protocol gets rid of the extra processing by the network layer routing protocols. This performance gain cannot be evaluated through simulation. The comparison of the proposed cooperative routing protocol with minimal energy cooperative routing protocols in the literature is the future work.

REFERENCES

- [1] Nosratinia A, Todd E Hunter, Hedayat A, Cooperative communication in wireless networks, IEEE Communications Magazine 2004, 42(10), 74 - 80.
- [2] Scaglione A, Y W Hong, 2003, Opportunistic large arrays: Cooperative transmission in multihop ad hoc networks to reach far distances, IEEE Transactions On Signal Processing, 51(8), 2082-2092.
- [3] Weihua Zhuang, Muhammed Ismail, 2012, Cooperation in wireless communication networks, IEEE Wireless Communications, 19(2), 10 -20.
- [4] Cetinkaya C, Orsun F, 2004, Cooperative medium access protocol for dense wireless networks, in The Third Annual Mediterranean Ad Hoc Networking Workshop - Med Hoc Net (Bodrum, Turkey), 197 - 207.
- [5] Zhu H and Cao G, 2006, rDCF: A Relay-enabled Medium Access Control Protocol for Wireless Ad Hoc Networks, IEEE Transactions On Mobile Computing, 5(9), 1201 - 1214.
- [6] Liu P, Tao Z and S Panwar, 2007, Co-operative mac protocol for wireless local area networks, IEEE journal on selected areas in Communications, 25, 340-354.

- [7] Korakis T, Z Tao, Y Slutskiy, S Panwar, 2007, A Cooperative MAC protocol for Ad-Hoc Wireless Networks, in Proceedings of IEEE PerCom Workshop on Pervasive Wireless Networking (PerCom Workshops '07) (White Plains, New York, USA), 532 - 536.
- [8] Thanasis Korakis, Zhifeng Tao, Shashi Raj Singh, Pei Liu, S Panwar, 2009, Implementation of a Cooperative MAC Protocol: Performance and Challenges in a Real Environment, EURASIP Journal on Wireless Communications and Networking, 2009, 1 - 19.
- [9] Adam H, Elmenreich W, Bettstetter C, Senouci S M, 2009, CoRe-MAC: A MAC-Protocol for Cooperative Relaying in Wireless Networks, in Global Telecommunications Conference 2009 (GLOBECOM 2009), 1 - 6.
- [10] Chou C T, J Yang, D Wang, 2007, Cooperative MAC Protocol with Automatic Relay Selection in Distributed Wireless Networks, in Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops 2007 (PerCom Workshops '07) (Washington, DC, USA), 526-531.
- [11] Jibukumar Mangalathu , Raja Datta, Prabir K Biswas, 2010, CoopMACA: A cooperative MAC protocol using packet aggregation, Springer Wireless Networks, 16(7), 1865-1883.
- [12] Amir E Khandani, J Abounadi, E Modiano, L Zheng, 2007, Cooperative Routing in Static Wireless Networks, IEEE Transactions on Communications, 55(11), 2185-2192.
- [13] Ibrahim A S, Zhu Han, Liu K J R, 2008, Distributed energy-efficient cooperative routing in wireless networks, IEEE Transactions on Wireless Communications, 7(10), 3930,3941.
- [14] Lin Y, Song J H and Wong V W S, 2009, Cooperative Protocols Design for Wireless Ad-Hoc Networks with Multi-hop Routing, Springer Mobile Networks and Applications, 14(2), 143 - 153.
- [15] Zhengguo Sheng, Zhiguo Ding, Leung K K, 2009, Distributed and Power Efficient Routing in Wireless Cooperative Networks, IEEE International Conference on Communications 2009 (ICC '09), 14-18.
- [16] Pei Liu, Z.Tao, Z Lin, E Erkip, S Panwar, 2006, Cooperative Wireless Communications: A Cross-Layer Approach, IEEE Wireless Communications, 13(4), 84-92.
- [17] Shan H, W Zhuang, 2009, Distributed Cooperative MAC for Multihop Wireless Networks, IEEE Communications Magazine, 47(2), 126-133.
- [18] Hanguan Shan, Ho Ting Cheng, Weihua Zhuang, 2011, Cross-Layer Cooperative MAC Protocol in Distributed Wireless Networks, IEEE Transactions on Wireless Communications, 10(8), 2603-2615.

- [19] Shamna H R, Naga Lakshmi Appari, Lillykutty Jacob, 2013, Co-operative MAC protocol: Performance modeling and analysis, IEEE Recent Advances in Intelligent Computational Systems (RAICS) 2013 , 233-238.

- [20] Zhang X, Shin K G, 2015, Cooperation without Synchronization: Practical Cooperative Relaying for Wireless Networks, IEEE Transactions on Mobile Computing, 14(5), 937-950.

- [21] Dehghan M, M Ghaderi, 2004, Energy Efficient Cooperative Routing in Wireless Networks, CPSC Technical Report 2009 : Performance Tools and Applications to Networked Systems, 209-234.

- [22] Gokturk M S, Gurbuz O, Erkip E, 2012, RECOMAC: A Cross-Layer Cooperative Network Protocol for Wireless Ad Hoc Networks, 5th International Conference on New Technologies, Mobility and Security (NTMS) 2012 , 1-7.

- [23] Zhenghua Fu, Haiyun Luo, Petros Zerfos, Lixia Zhang, and Mario Gerla, 2005, The Impact of Multihop Wireless Channel on TCP Performance, IEEE Transactions on Mobile Computing, 4(2), 209-221.