Development and Analysis of a New End-to-End QoS Mechanism for Mobile Networks

Esmat Mirzamany

School of Science and Technology

Middlesex University

A thesis submitted to Middlesex University
in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

May 2014

Abstract

The proliferation of mobile devices over the past several years has created a whole new world of the Internet. The deluge of applications for every aspect of today's life has raised the expectation of having ubiquitous connectivity, with a desired Quality of Service (QoS). However, it has violated the original Internet design which was not intended to support mobility, neither better than best-effort delivery.

The problem of end-to-end QoS provisioning has been an active area of research for many years. While designed for fixed networks, the use of QoS protocols in IP-based mobile networks, where hosts dynamically change their point of attachments, imposes new challenges to be studied and analysed. Furthermore, a massive growth in the backbone network traffic with its highly unpredictable nature can cause bottlenecks in some links while others are under-utilised, and therefore, breaching the QoS provisioning commitments. The research presented here proposes a new end-to-end QoS mechanism for mobile networks. The scheme is composed of two different approaches for QoS provisioning in access and backbone networks. Firstly, a new scheme is proposed to minimise the signalling overhead, as well as how the QoS is interrupted at the time of handover. By virtue of a developed analytical framework and simulation scenario, the performance of the scheme is investigated thoroughly, emphasising on the figures of merits that affect the efficiency of using QoS signalling protocols in access networks. Secondly, a new QoS-aware routing mechanism is proposed for backbone networks, intending to minimise the congestion on the links while complying traffic requirement. The developed optimisation framework shows that the scheme can achieve near-optimal link utilisation, even under sudden traffic spikes, while complying with traffic needs.

Acknowledgements

Never planning before to get here, till the opportunity came, I cannot express my happiness in words for one of the most worthwhile experiences in my life. While tackling the problems during a PhD, one may learn invariable lessons: self-adjustment to face the failures, the bitterness of being on the verge of hopelessness, and the beauty of getting the confidence and inclination to question all that is around, and seek out new ways of doing them. Most importantly, the lesson of learning to push yourself out of comfort zone to make progress.

Without a doubt, I would not have been able to sit and write this acknowledgement today without many people throughout my life, whose presence and true friendship in a times of need have shed the light of beauty into my life. Although not being able to name all, I will never forget any of them.

I would like to thank my supervisory team, Dr Aboubaker Lasebae and Prof Orhan Gemikonakli, who always encouraged me to think independently. Beside my advisor, I would like to offer my gratitude to all my colleagues in TG22-23, for all their supports and friendship, especially for all the fun we have had in the last three years. Ritesh, I owe you a debt of gratitude for all your help. I cannot express how much your advice, during hard times of my PhD, would help me out. Usama, I cannot thank you enough for your support to improve my writing. Pawel, thanks for all your technical arguments and vote of confidence, which always cheer me up. Thanks to you all, and the ones I missed out their names here.

My sincere thanks go to Paula Bernaschina who is always willing to go the extra mile to help students. Paula, I cannot express how grateful

I am for your help during my study at Middlesex university.

I cannot find words to express my deepest gratitude to especial friends with their cute dog. This thesis would not have been possible without the encouragement and support of them.

And foremost, I am indebted to my parents for their love, concerns and encouragement without which I would not have reached this stage.

Hannaneh

Contents

List of Figures

List of Tables

List of Abbreviations

AR	Access Router
BA	Binding Acknowledgement
BU	Binding Update
CBR	Constraint Based Routing
CN	Correspondent Node
CoA	Care-of-Address
DiffServ	Differentiated Services
ECMP	Equal Cost Multi-Path
FA	Foreign Agent
FEC	Forwarding Equivalence Class
GIST	General Internet Signalling Transport
GMAP	Gateway MAP
HA	Home Agent
HMIPv6	Hierarchical Mobile IPv6
HNP	Home Network Prefix

HoA	Home Address
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
LBA	Local BA
LBU	Local BU
LCoA	Local Care-of Address
LMA	Local Mobility Anchor
LMAP	Local MAP
LSP	Label Switched Path
MAG	Mobile Access Gateway
MAP	Mobility Anchor Point
MN	Mobile Node
MPLS	Multi-Protocol Label Switching
MRI	Message Routing Information
MRM	Message Routing Method
MRS	Message Routing State
MSpec	Mobility Specification
MT-Routing	Multi-Topology Routing
NS-2	Network Simulator-2
NSIS	Next Steps In Signalling
NSLP	NSIS Signalling Layer Protocol

NTLP	NSIS Transport Layer Protocol
O-D	Origin-Destination
OSPF	Open Shortest Path First
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PHB	Per-Hop Behaviour
PMIPv6	Proxy Mobile IPv6
QoS	Quality of Service
RCoA	Regional Care-of Address
RSVP	Resource ReSerVation Protocol
RSVP-MP	RSVP Mobility Proxy
SLA	Service Level Agreement
SMR	Session-to-Mobility Ratio
TSpec	Traffic Specification

List of Publications

- Mirzamany E., Fredrikos V., Lasebae A., Gemikonakli O., QoE-Centric Localized Mobility Management for Future Mobile Networks, GLOBCOM2014 (Under-Review)

- Mirzamany, Esmat., Lasebae, Aboubaker., Gemikonakli, Orhan. (2013) Mirzamany E., Lasebae A., Gemikonakli O., SLA based MT-Routing for Future Internet, Wireless World Research Forum Meeting 32(WWRF32),20-22 May 2014, (Accepted)

  An Efficient Traffic Engineering Based on Multi-Topology Routing for Future Internet. Computer Networks journal, Elsevier (Under Review-Second round)

- Mirzamany, Esmat., Lasebae, Aboubaker., Gemikonakli, Orhan. (2013) Comparison Between RSVP and NSIS in Mobile IP Networks. IET Networks Journal (Under Review-Second round)

- Mirzamany, Esmat., Lasebae, Aboubaker., Gemikonakli, Orhan. (2013) Efficient NSIS mobility support for mobile networks. Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on , pp.3354,3359, 8-11 September 2013

- Mirzamany, Esmat., Lasebae, Aboubaker., Gemikonakli, Orhan. (2013) An efficient resource reservation for domain based mobile IP networks: analytical approach. Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th , pp.1,6, 2-5 June 2013

- Mirzamany, Esmat., Lasebae, Aboubaker., Gemikonakli, Orhan. (2012) Using aggregated RSVP in nested HMIPv6. Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, pp.716,721, 27-31 August 2012

Chapter 1

Introduction

Of all the major inventions of the twentieth century, without a doubt, the Internet is one of the greatest inventions at all times. The widespread use of the Internet technologies has created a wave of innovations, resulting in a profound impact on human lives. Over the past few decades, the Internet's popularity has increased, so much so that life without it would be unimaginable, at least for young people if not for all.

The successful widespread adoption of the Internet has acted as a driver behind the growth of applications, from the release of the world wide web and email in 90s to a deluge of applications for different parts of today's life. With the uncontrollable increase of mobile devices and the popularity of smart phones, a second revolution of Internet has started to emerge. Even more massive than the first one, the second involves the integration of the virtual and physical worlds almost everywhere all the time. With six of the world's seven billion people have mobile phones [1], it has become the first screen of choice among many of its users, for entertainment, communication, comment, interaction, gaming and socialising. From the business point-of-view, it is a tremendous opportunity to create new revenue streams for the subscriber-saturated mobile networks. What is certain is that success cannot be achieved unless the quality of service meets the users' expectations.

The Internet owes its success to its naive operation, treating all packets with different characteristics (e.g., voice, video, data) the same. Due to the burst of real-time applications, this one-size-fit-all service design principle, although being robust enough to stand the huge expansion, cannot live up with today's demands anymore. Therefore, the need to migrate from the best-effort service model to one, in which service differentiation can be provided, seems inevitable for future Internet architectures. This challenging issue has inspired a large body of research over the last few years.

1.1 Scope of the Work

The original design of the Internet Protocol (IP), as the single common communication protocol of the Internet, does not support a better than best-effort service. Neither does it support mobility. Each of these two issues has been adequately, though separately, addressed by multiple approaches in different categories [2–7]. Mobile IP [8] is the most promising protocol proposed for supporting host mobility in IP networks. However, it is also required to provide an adequate Quality of Service (QoS) forwarding treatment to the mobile user's data flow at the intermediate nodes along a path, so that QoS-sensitive IP services can be supported over Mobile IP.

QoS provisioning has been one of the long lasting focuses in the network research community, resulting in a number of well-studied protocols, e.g., Resource ReSerVation Protocol (RSVP) [4, 6]. Nevertheless, the use of these protocols, that were originality designed in the context of a static environment (fixed hosts and networks), over Mobile IP networks has been a challenging issue. The frequent changes of mobile users' point-of-attachment in a network can cause a violation of the assured QoS, which would impose severe delays and packet losses, if not a service disconnection. Nevertheless, access network is not the only challenging part of an effort to provide an end-to-end QoS. The massive growth in backbone network traffic, and the increasingly volatile traffic patterns can cause significant scaling, provisioning and operational inefficiencies for service providers, resulting in over-utilisation of some links while others are under-utilised. There has been a great deal of research to conduct packets routing in a way that not only does a selected path fulfil a flow's requirement, but also helps to distribute traffic evenly among links.

In the work presented in this thesis, a new end-to-end QoS mechanism for mobile networks is developed, and analysed. The scheme proposes a two tier architecture. A lower tier focuses on QoS guarantees in access networks, while an upper tier is based on a QoS-aware routing in backbone networks. The mechanisms proposed for QoS provisioning in each tier are independent from each other, and therefore, can be applied separately or in combination.

The lower tier is an efficient RSVP mobility support mechanism for access networks. It stems from the intention of enhancing the efficiency of QoS-enabled mobility management, with very small change in the existing infrastructure and protocols. The proposed mechanism aims to minimise the signalling overhead, as well as the interruption in QoS at the time of handover, by localising the QoS re-establishment to the affected parts of the data path in the domain. The performance of the proposed scheme is investigated thoroughly, by means of a developed analytical framework, and a simulation scenario conducted in Network Simulator-2 (NS-2) . Various figures of merit such as a resource re-establishment latency; a network-layer signalling cost and an effect of the number of mobile nodes and their average cell residence time on it; a number of packet loss; and a number of packets treated as a best-effort are used to measure the efficiency of this scheme.

For the upper tier accountable to the QoS provisioning in backbone networks, a new QoS-aware routing of flows by means of the multi-topology routing approach is proposed. The developed mechanism is two-fold. First, new algorithms are designed to extract fully edge-disjoint logical views of a network, in a way that the delay of a longest path between each pair of nodes becomes upper bounded. Then, the longest acceptable path for each traffic type, in accordance with the negotiated Service Level Agreement (SLA), is selected. This can guarantee that the shortest paths are used by the most legitimate flows in the network, the ones that other paths cannot satisfy their delay constraints. The investigation on the performance, based on a real topology and traffic matrices, shows that the scheme can achieve efficient resource utilisation, even under unpredictable traffic spikes, while at the same time comply with traffic need.

1.2 Aim and Objectives

The aim of this work is to propose an end-to-end QoS mechanism capable of tackling challenges in access and core networks. To that end, following objectives are set out:

- Enhancing the efficiency of QoS enabled mobility management, while affecting as little as possible the existing protocols. A proposed scheme should result in reducing the resource re-establishment latency after handover, reducing the mobility-management and resource-reservation signalling overheads, reducing the number of packets treated as best-effort packets and number of dropped packets due to the handover in the network.

- Providing an acceptable level of QoS by preventing congestion in core network, taking full advantage of traffic characteristic in path selection process. A proposed scheme should lead to an even traffic distribution through all the possible paths, resulting in reducing the congestion in shortest paths.

1.3 Contributions of the Thesis

The main contributions of the research work presented in this thesis, which lead to the design of an end-to-end QoS for mobile networks, is two-fold: the work demonstrates an efficient QoS mobility support mechanism for access networks, taking into the account possible approaches for mobility management and per-flow resource reservation. Second, a new mechanism for QoS provisioning in backbone networks is proposed. To that end, the breakdown of the major contributions can be listed as follows:

- The proposal for access networks discussed in Chapter 3 is an efficient RSVP mobility support mechanism in Hierarchical Mobile IPv6 (HMIPv6) [9] networks. The architecture of the scheme, in terms of the mobility management and resource reservation, is elaborated in detail. The results obtained show that not only does the scheme reduce the signalling overhead, but also the interruption in QoS at the time of handover. An analytical framework, alongside the network level simulation scenario in NS-2, is developed to investigate the performance of the new scheme in access networks, taking into the account mobile users mobility and traffic behaviours. While being adopted in different contexts, the model is used to derive the equations used to analyse the different scenarios mentioned below.

- An efficient QoS-aware routing, based on the multi-topology routing approach, is proposed for backbone networks. New algorithms are introduced. To evaluate the degree of sub-optimality in the proposed scheme, an optimisation framework is presented that intends to minimise the cost of congestion in the network, subject to newly defined constraints in compliance with the proposed mechanism.

Apart from the main contributions, following sub-major contributions can be listed as follows:

- The applicability of the proposed scheme to other environments, with regard to the existing protocols for QoS signalling and localised mobility management protocols in access networks, is investigated. To this end, the Next Steps In Signalling (NSIS) [5, 10] protocol and Proxy Mobile IPv6 (PMIPv6) [7] are chosen as substitute for RSVP and HMIPv6, respectively.

- First-in-literature analytical-based comparison between the NSIS and RSVP operations in access networks, using the network-based localised mobility management protocol is conducted. The aim is not to advocate which one is better, but rather to study the effects of various network parameters on their performance to enlighten decision-making.

1.4 Structure of the Thesis

The structure of this thesis is designed as follows: The background study of existing solutions for providing the mobility, as well as the QoS in access and core networks are given in Chapter 2. The advantage and disadvantage of each solution are describe in detail, providing a comprehensive ground to justify the choices made in this work. Chapter 3 describes the architecture of the proposed scheme with regard to the access network, using RSVP and HMIPv6 as a QoS signalling and mobility management protocols. A developed analytical model and the NS-2 based simulation scenario are used to elaborate the performance of the scheme. The applicability of the proposed scheme to other QoS and mobility management protocols, NSIS and PMIPv6, is investigated in Chapter 4. Chapter 5 defines the first-in-literature analytical-based comparison between RSVP and NSIS in a PMIPv6-based access network. The proposed mechanism for QoS provisioning in the backbone is discussed in Chapter 6, wherein the system model, proposed heuristic algorithms and the performance analysis are described in detail. Finally, the concluding remarks and future research in Chapter 7 bring closure to this thesis.

Chapter 2

Background Study

2.1 Introduction

The Internet does not support the flow prioritisation, and neither does it include considerations for host mobility. By emerging new facets of the applicability of the Internet on users' daily lives, an end-to-end quality of service provision has become a stringent demand for ever-increasing bandwidth starved applications, and therefore, an issue of great interest within the research community. The proliferation of Internet-connected mobile users with distinct requirements, not only drives up the demands for seamless connectivity, it raises the expectations of service quality for the video-dominant mobile data traffic. Nevertheless, most of the well-known QoS protocols were designed when the mobile IP was in its infancy, and hence, mobility was not initially a concern in their design. As a result, the usage of these protocols over IP-based mobile networks, in which users frequently change their point of attachment to the fixed network, usually causes limitations in terms of operation and performance.

This chapter gives the comprehensive knowledge in this field. It starts with an overview of the major quality of service protocols standardised by IETF in Section 2.2. Section 2.3 overviews the main concept of Mobile IP. Interoperability issues between resource reservation and mobility management protocols and some of the proposed solutions are elaborated in Section 2.4. Finally, discussing major candidates for the provision of QoS support in core networks brings closure to this chapter.

2.2 Quality of Service Protocols

In recent years, multimedia services have become the most significant applications among users in the Internet. A new generation of multimedia services is considered as a solution to create new revenue streams for the subscriber-saturated networks. What is certain is that the success cannot be achieved unless the quality of service meets the users' expectation. This section describes the most important QoS mechanisms used in IP-based networks.

2.2.1 Integrated Services

The development of the Integrated Services (IntServ) architecture model [2] was motivated by the poor performance of real-time applications across the Internet, mainly caused by the variable queuing delays and congestion losses. The Internet, as originally conceived, offers only a best-effort data delivery. Therefore, a new service model of the Internet, capable of providing some control over end-to-end packet delays, was a prerequisite for new generations of Internet applications.
Another motivation for developing IntServ model, apart from guaranteeing real-time QoS, was a rising demand for controlling the allocation of bandwidth among different classes of traffic. Network operators were requesting a system model capable of dividing traffic into a few administrative classes and assigning to each a minimum percentage of the available bandwidth under overload conditions. To this end, IntServ was introduced by the Internet Engineering Task Force (IETF) as a new Internet service model. Being capable of explicitly managing network resources, IntServ can provide an end-to-end QoS to certain flows. In addition to the best-effort, IntServ supports two types of services: Controlled-load service and Guaranteed service.
The controlled-load service [11] is closely equivalent to the best-effort delivery in a lightly loaded network. Applications using this model can assume that the packet loss rate is almost equal to the basic packet error rate of the transmission medium, meaning that a very high percentage of transmitted packets will be

delivered successfully. The service also guarantees that a very high percentage of the delivered packets will experience a delay which does not greatly exceed the minimum delay experienced by any successfully delivered packet. However, the specific target value cannot be requested for delay, and neither for the loss rate in the controlled-load service.

To ensure that these conditions are met, users provide the en-route network elements with an estimation of the data traffic they will generate, indicated in the flow's Traffic Specification (TSpec), asking adequate bandwidth and packet processing resources for the lifetime of the flow. The process is done by means of a *reservation set-up protocol*, used to create and maintain a flow state in the endpoints and routers along the path to the destination. Each network element accepting a request must ensure that the requested resources are available for a flow with given TSpec without impacting earlier guarantees. This must be accomplished through active *admission control* [11].

Given the admission being granted, all the incoming packets belonging to the given flow must be mapped into the same class and receive the same treatment. This mapping is performed by the *classifier*. A class may correspond to a broad category of flows (in the case of aggregation in backbone routers) or only a single flow and is chosen based on processing the parameters in the IP packet header, called Multi-Field (MF) classification. After being classified in different queues/class, the packet *scheduler* manages the forwarding of different packets. The scheduler decides whether and which packet to transmit next, ensuring that they receive the service that has been requested [11].

Should the defined traffic properties fall outside of the ones described by the TSpec parameters, the flow may experience large numbers of delayed or dropped packets. The controlled-load service is intended to support a broad class of applications which have been developed for use in today's Internet, but are highly sensitive to overloaded conditions.

The guaranteed service [12], on the other hand, is intended to emulate, over a packet-switch network, a dedicated rate circuit. Not only does this service provide applications with a bandwidth guarantee, it can control the maximum end-to-end queuing delay. It also guarantees that packets will not be deleted due to the buffer overload, provided the flow's traffic stays within its specified traffic parameters.

The guaranteed service, however, does not control the minimal or average delay. Not being justified for all applications due to the cost aspect, such guarantees are required for applications with hard real-time requirements such as remote process control, tele-medicine, etc [13].
The IntServ provides different controlled levels of packet delivery services for applications. However, supporting this capability requires two conditions. First, both applications and all individual network elements along the path must support mechanisms to control the QoS delivered to those packets. Second, there should be a mechanism to convey QoS management information between the application and en-route network elements [14]. While the former is provided by QoS control services such as controlled-load and guaranteed services, the latter is frequently implemented by a resource reservation set-up protocol such as RSVP.

2.2.2 Resource ReSerVation Protocol

RSVP is a reservation set-up protocol for IntServ-based IP networks. It is a soft state, receiver-oriented signalling protocol, that can reserve resources for unicast and multicast applications. RSVP is used by both endpoints and routers. Endpoints utilise RSVP to request a specific QoS level for their flows. Subsequently, routers use RSVP to inform all network elements along a flow's path(s) to deliver and maintain the required QoS throughout the transmission. RSVP is not a routing protocol, however, it strongly depends on present and future routing protocols to determine where it should carry the reservation request. The information conveyed by RSVP can be categorised as follows [15]:

- **Sender-generated information:** This information describes the characteristics of the data traffic the application expects to generate (the Sender TSpec), and the format of data packets the sender originates i.e., the sender IP address and optionally the UDP/TCP sender port (the Sender Template). These parameters flow downstream towards the receiver without being modified by the intermediate nodes.

- **Intermediate-node-generated information:** This information is generated or modified by the intermediate nodes along the path between the sender and receiver. It describes the properties of data path, including the availability of specific QoS control services and parameters required by them to operate correctly. The information is carried in an RSVP ADSPEC object towards the receiver, wherein it can be used to make a reservation decision.

- **Receiver-generated information:** This information specifies the receiver's desired QoS (the FlowSpec) and a set of data packets to receive the requested QoS (the FilterSpec). The former, the FlowSpec, includes the receiver's desired integrated service type (guaranteed or controlled-load), the traffic characteristics of the data flow for which the resources should be reserved (the Receiver TSpec), and if the guaranteed service was selected, other information required to invoke this service (the RSpec). The latter, the FilterSpec, together with a session specification, defines a set of data packets to receive the requested QoS. The receiver generated information follows exactly the reverse path the data packets will use, upstream to the sender.

The two fundamental RSVP message types are *Path* and *Resv*. The *Path* message is sent by the sender downstream towards the receiver, following the same route as the data packets. The message contains the Sender Template, Sender TSpec and ADSPEC objects in addition to the previous (RSVP-aware) hop address. It creates a path state in each RSVP aware router along its way without assigning actual resources. The states keep information about the flow and IP address of the previous hop used to route the signalling messages in the reverse direction. RSVP defines a session to be a data flow with a specific destination and transport-layer protocol, identified by the destination IP address, transport protocol ID (TCP or UDP) and destination port number (optional). Session identification (session ID) is used to refer to the state stored for it.
When the receiver receives the *Path* message, it sends the reservation request (the *Resv*) message upstream towards the sender, following exactly the reverse of the path paved by the received *Path* message. The *Resv* message contains the FlowSpec and FilterSpec objects, used to create and maintain the reservation states in each RSVP-aware router along its way. These states are in charge of

actual resource reservation. Assuming admission control succeeds, The FlowSpec is used to parametrise a resource class in the router's packet scheduler, while the FilterSpec is utilised to set parameters in the packet classifier to map the appropriate packets into this class.
The *Path* messages have the same source and destination IP addresses as their associated data packets, assuring that they can be routed correctly through non-RSVP capable domains. In contrast to the *Path*, the *Resv* messages are sent hop-by-hop from the receiver to the sender. Each RSVP-aware router changes the destination address of the *Resv* messages to a unicast address of the previous hop stored in the path state (Figure 2.1). The IP source address is the address of the router sending the message. The RSVP states along the path are refreshed by sending the periodic *Path* and *Resv* messages to maintain the end-to-end reservation. By default the RSVP messages are carried by raw IP datagrams with no reliability enhancement, however, UDP encapsulation can also be used for hosts that do not support the raw network I/O capability. During its life-

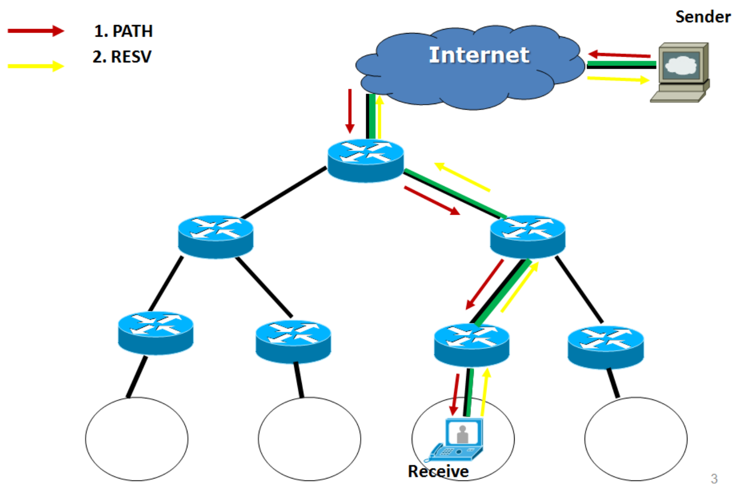


Figure 2.1: RSVP operation in wired network

time, RSVP has received substantial research community attention being one of the most persistent and altered protocols. In turn it has not escaped criticisms for its complexity, and potentially bad scalability, especially in the Internet core. In RSVP, the amount of state information is directly proportional to the number of flows, implying a massive processing and storage overhead on the core routers.

Nevertheless, instead of being abandoned, over the years several extensions to alleviate the crises have been proposed. The most recent up-to-date survey of the RSVP extensions can be found in [16].

2.2.3 Differentiated Services

The Differentiated Services (DiffServ) [17] effort in IETF has developed a simple model to differentiate the qualities of packet delivery. The intent of the DiffServ model is the provision of scalable service discrimination in the Internet with no need to have per-flow state and signalling in every router. The model achieves scalability and flexibility by separating the architecture into two major components: Forwarding path and Management plane [3].

The forwarding path behaviours, also called Per-Hop Behaviours (PHB), include the differential treatment an individual packet receives at each router's output interface queue along its path, implemented by queue management disciplines, e.g., Weighted Round-Robin (WRR). Within the backbone of the network, each router selects a particular forwarding behaviour for packets based on the value of the DiffServ Code Point (DSCP) set in the IP packet header, without having to know which flows or what types of applications the packets belong to. The process of setting the DSCP in a packet based on defined rules, or Marking, is performed at network edges, the sender or first-hop router, and administrative boundaries.

The management plane, on the other hand, involves the configuration of network elements with respect to which packets get special treatment and what kinds of rules are to be applied for allocating adequate resource to each treatment in each router. A logical entity such as bandwidth brokers is in charge of resource management in an administrative domain.

In order to enforce requirements associated with the delivery of the special treatment, the forwarding path may require some control elements, used to enforce that traffic conforms to predefined profiles. These elements include the policer and shaper. While the policer drops the out-of-profile traffic, the shaper delays packets within a traffic stream making traffic conform to its profile. However, similar to the marking, these operations need only be implemented at network boundaries or hosts while preserving the simplicity of the core network. Within the core network, routers perform a simple Behaviour Aggregate (BA) classification wherein a collection of packets with the same DSCP, crossing a link in a particular direction, are aggregated and receive the same treatment. In the DiffServ model, packets can receive one of these forwarding behaviours:

- **Default PHB:** The default PHB [3] provides the common, best-effort forwarding behaviour available in existing networks. Packets belong to this aggregate when either no other agreements are in place, or when the DSCP value is not mapped to any of the available PHBs.

- **Assured Forwarding PHB:** The Assured Forwarding (AF) PHB [18, 19] provides four different forwarding assurances/classes in ascending order of priority where each one is allocated a certain amount of buffer space and interface bandwidth. Within each AF class the IP packets are marked with one of three levels of drop precedence. The assigned drop precedence reflects the relative importance of the packet within its class in case of congestion, wherein packets with a higher drop precedence will be discarded in favour of ones with a lower value. AF is a rough equivalent of the controlled-Load services defined in the IntServ architecture.

- **Expedited Forwarding PHB:** Almost similar to the guaranteed service in the IntServ, the Expedited Forwarding (EF) PHB [20] intends to provide a low loss, low delay, and low jitter service in DiffServ domains. Such a service, when implemented, provides a premium service such as a point-to-point connection or virtual leased line. However, for optimal efficiency, it should be reserved for only the most critical applications, clearly because in case of congestion it is impossible to treat all or most traffic as high priority.

The Internet is composed of several domains managed by administrative authorities based on different policies. That means the forwarding services provided by a sender domain based on the contracted SLA may not be compatible with the ones provided by other domains. This is due to the fact that the packet handling in DiffServ architecture is left to each administrative domain. Consequently, the DSCP chosen for packets by the sender may change on their way towards the receiver. Therefore, a packet marked with a high priority may be regarded as a low priority or even best-effort, resulting in a violation of service quality. Although it is strong on simplicity, DiffServ is weak on guarantees. Finally, it does not offer any receiver control.

2.2.4 Next Steps in Signalling

In an effort to support the QoS signalling and other various signalling applications, IETF introduced the NSIS suite as a generic framework. Intended for more purposes than just resource reservation, NSIS decouples the signalling application from signalling transport. The new two-layer structure solves the lack of flexibility faced by some signalling protocols like RSVP. The signalling application layer, called NSIS Signalling Layer Protocol (NSLP), supports various signalling applications, i.e., QoS NSLP [21] or NAT/Firewall NSLP [22], that need to install and/or manipulate states for a data flow along its path in the network. The signalling transport layer, also called NSIS Transport Layer Protocol (NTLP) [5], provides the common functionality of node discovery, message routing and message transport for all the NSLP signalling applications.

QoS-NSIS Signalling Layer Protocol

The QoS NSLP, henceforth referred to as NSLP in this section, provides some forwarding resources for a flow by establishing and maintaining resource reservation states along the path. Although conceptually similar to RSVP, NSLP attempts to overcome the RSVP shortcomings by supporting additional features such as sender- and receiver-oriented reservations, location-independent session identifier (session-id) for mobility support, bi-directional reservation, and the ability to use existing transport and security protocols.

Similar to RSVP, reservation states are referred by session-id. However, unlike RSVP in which session-id is defined by a particular destination and transport protocol, NSLP uses a cryptographically random number as a session-id. This makes the session and associated states independent of the flow identity and any changes that may occur. Note that, while an RSVP session is defined as a flow with a particular destination and transport protocol, NSLP defines a session as an application layer concept for an exchange of packets between two endpoints, in which some network state is to be allocated or monitored. A certain flow(s) associated with a session is identified by the flow-id, also called Message Routing Information (MRI). MRI includes flow source and destination IP addresses, the direction of the signalling (upstream or downstream), and the Message Routing Method (MRM) which by default is the path-coupled signalling.

NSLP performs different signalling functions for sender-oriented and receiver-oriented reservations, however, in both scenarios signalling should be initiated by the sender in the downstream direction. This gives rise to NSIS problems in mobile networks discussed in Section 2.4. The reservation requirements are defined as the general parameters in the QoS Specification (QSPEC) object, interpreted by the Resource Management Function (RMF) for a desired QoS model, i.e., IntServ/DiffServ/others, in all NSLP-aware nodes along the path. The request can be accepted or rejected depending on the policy control and admission control decisions. In the sender-oriented reservation, the sender initiates a *Reserve* message towards the receiver. Upon receiving the message, the receiver sends a *Response* message to confirm the reservation establishment, following exactly the reverse of the path paved by the *Reserve* message. The *Response* message usually provides the information about the previous NSLP message (if the previous NSLP message contains the Request Identification Information (RII) object). The message cannot install any state, however, it may modify the existing states if it carries the information about an error.

For the receiver initiated reservation, the sender first sends a *Query* message towards the receiver. The message is used to request information about the data path characteristics without making a reservation. Using this information, the receiver sends the *Reserve* message to the sender that follows exactly the reverse of the path the *Query* message used. If the confirmation is requested, the *Response* should be sent by the flow sender.

Apart from the *Reserve*, *Response* and *Query*, there is another NSLP message called *Notify*, used to exchange information, typically related to error conditions, between NSLP-aware nodes. In contrast to the *Response*, the *Notify* messages are sent asynchronously, rather than in response to other messages and need not refer to any particular state or previously received message. As a soft state protocol, NSLP uses the *Reserve* message to refresh the reservation states in the downstream or upstream for the sender-oriented or receiver-oriented reservation, respectively. A refresh right along the path can be forced by requesting a *Response* from the far end. Without this, a refresh *Reserve* would not trigger *Reserve* messages to be sent further along the path, as each hop has its own refresh timer.

NSIS Transport Layer Protocol

The NTLP is a common transport layer for all the NSLP signalling applications, i.e., QoS NSLP, Firewall/NAT NSLP. The core part of the NTLP is the General Internet Signalling Transport (GIST) protocol [23], the rest comprise of the existing security and transport protocols.

While being completely independent from NSLPs, the only information visible to the GIST about them is their id (NSLP-id). GIST provides the common functionality of node discovery, message routing, and message transport for multiple signalling applications. In contrast to RSVP, in which the message routing (determining the identity of the GIST peer) and message delivery are performed in one step, the GIST performs them sequentially. It first defines a three-way handshake that probes the network to set up the necessary routing states between adjacent peers. Once the routing decision has been made, the node has to select a mechanism for transport of the message to the peer, Connection-Mode (C-Mode) or Datagram-Mode (D-Mode). The former sends the GISP messages between nodes using point-to-point messaging association (MA). The MA can use any stream- or message-oriented transport protocol with TCP as its initial choice; if security protection is required, it may use a network or transport-layer security association. In the latter, the D-Mode, the GIST messages are sent without using any transport layer state or security protection. UDP is used as the initial choice of this mode.

The GIST node discovery/message routing is triggered by receiving an NSLP signalling message, requesting the establishment of a new signalling state along a path between the sender and receiver. The request may result from a local application request or processing an incoming NSLP message. The discovery phase is performed hop-by-hop through the three-way handshake between GIST peers, performed in the D-Mode. The first message is the *Query*, destined to the

receiver of the flow. When the correct peer, a fist node supporting the requested NSLP, receives the *Query*, it sends a *Response* message to the querying node. Then, it creates the Message Routing State (MRS) to keep the identity of its upstream node for that particular session explicitly. The MRS is configured and kept separately for each flow in the GIST layer used to manage the processing of the outgoing messages. It is conceptually organised as a table in which each row corresponds to the unique combination of the MRI, session-id and NSLP-id.
When the querying node receives the *Response*, it uses the information conveyed to create its own MRS for the downstream node. At this stage the querying node can send the NSLP signalling message as a payload in the *Data* message. If the responder node asks for the confirmation, the *Confirm* is sent before the *Data* message. Upon receipt of the NSLP message to the responder node, the same process is performed between a next GIST peer along the path till the NSLP signalling message reaches the destination of the flow.
If the C-Mode operation is preferred, the MA should be established between the GIST peers during the handshake process. Similar to the D-Mode, first the *Query* and *Response* messages are sent as the UDP traffic. They contain extra information about the available combinations of the security and transport protocols carried in the Stack-Proposal object, and the overall information of the MA carried in the Stack-Config-Data object. By default, in C-Mode, the GIST handshake process is followed by the TCP three-way handshake. During the MA establishment, the responder node *should* request for the *Confirm*, which is sent as a first message within the recently established MA. In contrast to the D-Mode, the responder node creates its MRS after receiving the *Confirm* message.
Unlike the MRS, the MA is not per flow and can be used by the multiple flows between a GIST peer. Therefore, if there is an MA that can meet the requirements (the same routing state and desired properties), the *Response* and *Confirm* can be sent through it. Note that even if the MA exists, the three-way handshake should be performed between GIST peers for each flow. The process is essential to define the upstream and downstream nodes and inform them about their security and transport requirements.
GIST is a soft state protocol wherein MRS and MA states are refreshed periodically. The MA states can stay alive, with no need of sending refresh messages,

as long as at least one flow is using them. After that, if either the local policy or the GIST peer wants the MA retained, a refresh message (MA-Hello) should be sent periodically. To keep the MRS states alive, the querying node, the one that initiates the handshake process, should send a periodic *Query* message.

2.2.5 Other QoS Signalling Protocols

The section introduces briefly two proprietary QoS signalling protocols for IP networks, YESSIR and Boomerang. A survey of different signalling protocols and other architecture can be found in [24, 25].

YESSIR

To overcome the complexity and scalability issues in RSVP, YEt another Sender Session Internet Reservations (YESSIR) [26] was developed as a new resource reservation protocol. While preserving many unique features introduced by RSVP, such as soft states, advertising the network service availability and resource sharing among multiple senders, YESSIR intends to simplify the process of establishing reserved flows, and therefore, the proposed mechanism generates reservation requests by senders to reduce the processing overhead. As an in-band signalling protocol, YESSIR messages are piggybacked in the Real-Time Transport Control Protocol (RTCP) messages, a control protocol for Real Time Protocol (RTP) [27]. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio and video, over multicast or unicast network services. However, neither does it address resource reservation nor does it guarantee QoS for real-time services. RTCP works as a control protocol to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality.
YESSIR assumes that a large fraction of the applications that require guaranteed QoS are continuous media applications and that a substantial fraction of these either use or will use RTP to deliver their data. This assumption, although it offers significantly lower signalling and run-time complexity than RSVP, requires support in applications since YESSIR is an integral part of RTCP. Clearly, the most obvious disadvantage of YESSIR is that it can only be used with RTP sessions.

Boomerang

In an effort to reduce complexity, Boomerang [28] was introduced as another soft-state lightweight resource reservation protocol for IP networks. It intends to be quick and simple, yet powerful. A Boomerang signalling message is only generated by an initiating node, i.e., the sender, receiver or any Boomerang-aware node en-route, containing the desired QoS specification. The message follows standard routing protocols and allocates resources hop-by-hop in every Boomerang-aware node along the path. Upon reaching the destination (other end-point of the data flow), the message is echoed back to the initiating node. By using this method, keeping complexity and intelligence to only one end of communication while the other end only needs to be able to bounce the message back, Boomerang can provide a simple implementation. In addition, a bi-directional resource reservation can be made independently of the path by each of the end-points enabling sender- or receiver-oriented reservations.
Boomerang seems to be a very lightweight protocol with the apparent low processing overhead and bandwidth consumption. A comparison made between Boomerang and RSVP in [29] showed that the Boomerang signalling message processing overhead, defined as the time interval that a signalling message spends inside the router, is considerably lower than that of the RSVP daemon implementation. However, this superiority is mainly due to the limited functionalities provided by the protocol as compared to the ones supported in RSVP. For example, no support for multicast or policy-based interaction is provided.
Similar to those of any host-network-host protocol, Boomerang requires an implementation at (at least) one end of communication and in routers. Boomerang-unaware routers should be able to forward Boomerang messages transparently. In the initial implementation, Boomerang messages are transported in ICMP Echo/Reply messages, i.e., into the Ping message. Although encapsulating the signalling information in the ICMP messages makes the protocol implementation simple, firewalls often drop ICMP packets making the protocol implementation impractical.

2.3 Mobility Management

Internet Protocol assumes that a node's IP address uniquely identifies its physical attachment to the Internet; hence, in order to receive packets destined to the node, it should be attached to the network indicated by its IP address. Although working well under such assumption, IP cannot meet the needs of the burgeoning population of mobile users who wish to change their point of attachment from one network to another without losing their ability to communicate. To that end, Mobile IP protocol was developed as a scalable mechanism for accommodating node mobility within the Internet [8]. While being the standard network-layer solution, Mobile IP is not the only proposed solution for the node mobility support. An overview of existing protocols for mobility management in IP networks is given in [30, 31].
This section introduces the main concept of Mobile IP, including its basic operation under IPv4 and IPv6 networks, and different mobility management approaches used to design local mobility management for Mobile IP.

2.3.1 Mobile IP

Mobile IP protocol, introduced by IETF, is the standard network-layer, mobility-enabling protocol for the Internet. It enables a Mobile Node (MN) to change its serving network without need of changing its permanent IP address. This is accomplished by providing an MN with two IP addresses: Home Address (HoA) and Care-of Address (CoA). The former is a long-term IP address obtained by an MN on its home network, administrated in the same way as a permanent IP address is provided to a stationary node. The MN is always identified by its HoA, regardless of its current point of attachment to the Internet. The latter, the CoA, is a temporary IP address obtained by the MN whenever it moves to a foreign network. The CoA reflects the MN's current location in the Internet. The MN operating away from home needs to register its new CoA with its home agent, informing it about its current location. All the packets destined to the MN are then intercepted and tunnelled by the HA to the MN's new CoA. By using this mechanism, the MN can continue its ongoing communication with Correspondent Nodes (CN) after moving to a new IP subnet, while keeping its

movement transparent to the higher-layer protocols and CNs.
The main components of Mobile IP and its operation depend on the version of the Internet address protocol used in the network, IPv4 or IPv6.

2.3.1.1 Mobile IPv4

The Mobile IP protocol was initially designed to offer seamless mobility to IPv4 nodes, and hence, mainly referred to as Mobile IPv4 [32]. Its two main entities are: Home Agent and Foreign Agent. The Home Agent (HA) is an Mobile-IP-aware router on an MN's home network. It maintains the information about the MN's current location to re-direct the packets there while it is away from home. The latter, Foreign Agent (FA), is a Mobile-IP-aware router on an MN's visited network that provides routing services to the MN while registered. The FA de-tunnels the packets, that were tunnelled by the MN's HA, and delivers them to the MN. The termination point of a tunnel can be the MN instead of the FA. In this case, when the MN registers in a foreign network, instead of using the address of the FA as its new CoA, the MN should externally obtain a local address, called co-located CoA. Of the two modes, using the foreign agent CoA is preferred because it meets the community goals of better utilisation of the limited IPv4 address space. The basic operation of Mobile IP can be outlined into the following steps:

- **Movement Detection:** In Mobile IP both mobility agents, the HA and FA, advertise their presence via Agent Advertisement messages. The message is used by the MN to detect the movement and determine if it has entered a new subnet (layer-3 handover). A solicitation can be sent by a newly arrived MN to discover any prospective agent. This can reduce the handover delay influenced by the movement detection.

- **Registration:** Upon entering a new subnet, the MN needs to register with the FA and obtain a new CoA, either a foreign agent CoA or a co-located CoA. The former is the IP address of the FA obtained from the Agent Advertisement messages, while the latter is acquired by the MN through some external mechanism such as Dynamic Host Configuration Protocol (DHCP).

- **Location/Binding Update:** After obtaining the IP address, the MN registers its new CoA with the HA, informing it about its current point of attachment. The process is done through exchange of registration request and registration reply messages. The HA associates the MN's HoA with the CoA and lifetime together in a routing record known as a *binding*. While being away from home, the HA intercepts all the packets destined to the MN and tunnels them to its latest CoA.

By default packets originated by the MN carry its HoA as their source IP address. Assume that routing is independent of source address, they are delivered to CN(s) using standard IP routing mechanisms, with no need of passing through the HA. This leads to asymmetrical delays for upstream and downstream directions, known as the Triangle Routing problem. The name came from the three distinct routing paths that the round trip communications should travel, routes CN-HA-MN for the packets sent to the MN and a route MN-CN for the packets originated from the MN. An extension to Mobile IPv4 known as Route Optimization [33] was proposed to eliminate the routing anomalies caused by the Mobile IP specification. According to this extension, the CN is provided by the information about the MN's current point of attachment and kept updated whenever it changes. Being informed about the MN's CoA, the CN can tunnel packets directly to it.
Due to the security concerns, some routers do not allow forwarding of packets with a topologically incompatible source address format. This raises concerns for MNs sending packets in a visited network, using HoA as a source address. In environments where this is a problem, the reverse tunnelling [34] can be used between an MN and its HA, with the CoA and home agent address as the source and destination addresses. Upon reaching the HA, the packets are de-tunnelled and sent to their final destination, the CN. Although solving the problem, the reverse tunnelling sends the packets through a path significantly longer than the optimal one.

2.3.1.2 Mobile IPv6

In an effort to support mobility for the emerging next generation Internet (IPv6), Mobile IPv6 [35] was introduced by the IETF. Mobile IPv6 specifies a protocol which allows nodes to remain reachable while moving around IPv6 networks. The

design of this protocol has exploited both the lessons taken from the Mobile IPv4 development and the new features introduced in IPv6. Having the same concept at the core, Mobile IPv6 offers some major improvements as compared to Mobile IPv4. The use of new features introduced in IPv6, such as neighbour discovery and address auto-configuration, enables MNs to operate without any special support required from local routers in a visited network, and therefore, eliminates the necessity of having FA entity. While away from its home, an MN acquires its CoA using either a stateful or stateless auto-configuration mechanism. A stateful mechanism requires the presence of a IPv6 DHCP server located in the boundaries of the visited network, however, the tight control over address assignments can be assured. In contrast, in the stateless auto-configuration [36] the MN configures its CoA using a combination of its Ethernet hardware address, also known as MAC address, and information advertised by a local router. To ensure the uniqueness of the configured addresses on a subnet domain, MNs run a Duplicate Address Detection (DAD) algorithm on a newly configured address before assigning it to an interface. The DAD algorithm is performed on all addresses, independently of whether they are obtained via stateless auto-configuration or DHCPv6 [36].
After the IP address acquisition phase, the MN sends a Binding Update (BU) to its HA informing it about its new point of attachment. Upon receiving the message, HA responds to the MN by sending a Binding Acknowledgement (BA) message. If a CN does not support Mobile IPv6, bi-directional tunnels are established between the MN and HA. Packets from the CN are routed to the HA wherein tunnelled to the MN. Packets to the CN are tunnelled from the MN to the HA (reverse tunnelling), and then after being de-tunnelled, routed normally from the home network to their destination, the CN.
Unlike Mobile IPv4 wherein the route optimization was defined as an extension, in Mobile IPv6 route optimization support is a fundamental part of the protocol, allowing a direct communication between the MN and CN(s). However, it requires the MN to register its newly-obtained CoA with the Mobile IPv6-aware CN(s). When sending a packet to any IPv6 destination, the CN checks if any binding exists for the packet's destination address (i.e., MN's home address). If there is, the associated CoA is copied to the destination address field of the packet's header. A new type of IPv6 routing header, called Type-2 Routing header, is also

added to the packet to carry the MN's home address. Once the packet arrives at the CoA, the MN retrieves its home address from the routing header, and this is used as the final destination address for the packet. Routing the packet directly to the MN's CoA has some distinct advantages. Not only does it use the shortest path for communication, it eliminates the need of packet tunnelling, reducing the amount of resulting overhead compared to Mobile IPv4.
For packets destined to the CN, the MN copies its CoA to the source address field in the packet's header, sending them directly to the CN's IP address. The information about the MN's home address is carried in a new IPv6 extension header, called Home Address option. When the CN receives the packet, it replaces the original value of the source address field with the MN's HA, carried in the home address option. This enables the upper layers (e.g., the transport layer) to process the packet without the knowledge that it came originally from a CoA or that a Home Address option was used.

2.3.2 Localised IP Mobility Management

Mobile IPv6 empowers users to move freely within the Internet while still keeping their on-going connection(s), however, this comes at the cost of transferring signalling messages to the HA/CN after each layer-3 handover (henceforth referred to as handover in this document). The process of exchanging the BU and the BA can cause significant delays or disruptions on active connections if the HA/CN is far away. Some packets will be lost. Together with link layer and IP layer connection set-up delays, there may be effects to upper-layer protocols. Moreover, the signalling exchanges can increase the signalling overhead on the network especially on a wireless link, and finally it can jeopardize the location privacy of the MN. To alleviate such performance problems, a number of Localised Mobility Management protocols have been proposed, intending to maintain the IP connectivity and reachability of an MN when it moves, while confining the mobility management signalling to an access/local domain. Although using different approaches, i.e., host-based or network-based to be described later in this section, all the proposed solutions utilise a new entity defined as a local home agent, a home agent closer to the MN. The MN's movement over the local domain, local mobility, requires only signalling exchanges with the MN's local home agent. This is in contrast with the Global Mobility Management protocols such as Mobile IP which invalidates an MN's global unicast IP address after each handover, causing a global, end-to-end routing of signalling messages between the MN and CN/HA. Note that local domain is a generic term for a collection of fixed and mobile network components, allowing access to the Internet, all belonging to a single operational domain. Depending on the access technology, geographically the area can be large.

2.3.2.1 Host-Based Mobility

The host-based mobility management protocols require a mobile user involvement at the IP layer. The user needs to take care of the signalling required to manage its mobility, and be aware of the local/micro and global/macro mobility management solutions, thus acting accordingly. One of the most successful solutions for the host-based mobility management is HMIPv6 protocol. As a simple extension to Mobile IP, its intent is to improve the performance by handling MNs' mobility within a local region locally. The protocol utilises a new entity called the Mobility Anchor Point (MAP). The MAP is a router located in a visiting domain, usually at the gateway, acting as a local home agent. Its domain's boundaries are defined by the means of router advertisement messages advertising the MAP information to MNs.

Upon entering a new MAP domain, the MN configures two addresses: Local Care-of Address (LCoA) and Regional Care-of Address (RCoA). The former is the on-link CoA configured on an MN's interface, based on the prefix advertised by its default router. This address defines the current location of the MN within the MAP domain. It changes when the MN moves from one subnet to another both belonging to the same MAP domain (local/micro mobility). The latter, the RCoA, is formed in a stateless manner by combining the MN's interface identifier with the MAP's subnet prefix obtained from the MAP option in router advertisement messages. The RCoA changes when the MN moves from one subnet to another each belonging to a different MAP domain (global/macro mobility).

After IP-layer configuration, the MN needs to register with its local home agent, the serving MAP, by sending it a local BU. The message contains the MN's

RCoA (similar to a home address) and LCoA. The MAP will then return a BA to the MN. If the registration is successful, the bi-directional tunnel is established between the MAP and MN. After receiving the BA from the MAP, the MN should register its new RCoA with its HA/CN by sending a BU to each, as in Mobile IPv6. The message will bind the MN's original home address to the newly-configured RCoA. The confirmation of registration, the BA, will be sent to the MN. Following the successful registration, packets sent by the HA or CN to the MN will have the MN's RCoA in their destination address. The MAP, as a local HA, intercepts the packets and tunnels them to the MN's LCoA. Similarly, all packets sent by the MN are tunnelled to the MAP, having the MN's LCoA and MAP's IP address as a source and destination address in their outer header. The inner header contains the MN's RCoA as a source address and the HA/CN IP address as the destination address.

Based on this architecture, the MN's location inside the MAP domain remains transparent to all the nodes it communicates with but the MAP. Moreover, instead of exchanging a pair of BU/BA with the HA and CNs after each handover, the MN just needs to register with the MAP, as long as its movement is confined to within the MAP domain (intra-domain handover). This results in a smaller signalling overhead in comparison with Mobile IP.

2.3.2.2 Network-Based Mobility

Host-based mobility protocols require changes in MNs' software stack that may not be compatible with all global mobility protocols. Although the existing localised mobility management solutions all depend on Mobile IP or derivatives, future MNs may select other global mobility management protocols, such as Host Identity Protocol (HIP) [37]. Moreover, considering the resource constraint characteristic of mobile devices and users reluctance to host stack software modification [38], having a mechanism that relocates mobility procedures from MNs to network components has become an issue of great interest in recent years.

To that end, Network-based Localised Mobility Management (NETLMM) approach [38] was introduced to enable IP mobility for an MN without its participation, and therefore, it requires no software changes on the host. PMIPv6 is

the protocol standardised by IETF to provide this approach.
The core functional entities in PMIP are: the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). Acting as a local home agent in the PMIP domain, the LMA (usually located at the gateway) manages the MN's mobility inside domain under its control. It maintains a collection of routes for individual MNs and manages their binding states. The latter is the PMIP-enabled access router responsible for tracking the movements of the MN and initiating the required IP-layer mobility signalling on its behalf.
An MN entering a PMIP domain will be first identified by a serving MAG which the MN attached to its access link. The identification is performed by means of an MN identifier. Every MN roaming within the PMIP domain should have a unique identifier, such as a Media Access Control (MAC) address. The MN identifier has an associated policy profile, accessible by network entities i.e., MAG and LMA, that identifies the MN's serving LMA IP address (mandatory field), permitted address configuration modes, roaming policy, and MN's home network prefix. After a successful authorisation, the MAG sends a Proxy Binding Update (PBU) message to the LMA, informing it of the current location of the MN. The message contains the MN identifier for identifying the MN. On receiving the message, the LMA sets up its end-point of bi-directional tunnel to the MAG, binds the MN's home address prefix to the MAG's address, and replies back by sending a Proxy Binding Acknowledgement (PBA) message including the MN's home network prefix. On receiving the acknowledgement, the MAG configures its end-point of the bi-directional tunnel to the LMA. Having the knowledge of the MN's home network prefix allows the MAG to emulate the MN's home link. It puts this prefix in the router advertisement message and sends it to the MN. The MN, on receiving the same home network prefix, starts to configure its IP address without detecting any change with respect to the layer-3 attachment of its interface. As far as the MN is concerned, it is still in its home network. The LMA as a topological anchor point for the MN's home network prefix, intercepts all the packets destined to the MN's home address and sends them to its serving MAG through the pre-defined bi-directional tunnel. Packets sent by the MN will be received by the serving MAG and tunnelled to the LMA. The LMA, on receiving the packets, removes the outer header and routes them to the destination,the CN.

2.4 QoS Guarantees in Access Networks

During the last few years, mobile users have witnessed the rapid evolution in next generation mobile networks and services offered. A new generation of multimedia value-added services have intended to persuade potential customers to spend more, creating new service values. The competition between providers is so intense that a small improvement in service quality can go a long way. Although Mobile IP is the de facto standard chosen for IP mobility management, in its basic form it inherits the IP incapability to provide QoS guarantees, and therefore, depending on external mechanisms. Nevertheless, when compared with fixed networks, provision of QoS in mobile networks is more complex than that. This section gives insight into the problems of QoS-guarantee signalling protocols in mobile networks, and then describes some prominent solutions proposed to overcome these challenges.

2.4.1 RSVP in Access Networks

RSVP can provide guaranteed QoS on best-effort basis IP infrastructure, however, the lack of mobility considerations in its initial design has played a significant role in its inefficiency in mobile networks. RSVP and Mobile IP are both well-established protocols with satisfactory performances when deployed separately. However, if their functionality is combined, the incompatibility issues between them give raises to some serious challenges in terms of QoS deterioration and inefficient use of resources.

Tunnelling

Although being the essential part of Mobile IP, tunnelling causes significant problems for RSVP operations in mobile networks. It changes the protocol ID of the RSVP messages (i.e., *Path* and *Resv* messages) from 46 to 4, making them invisible to RSVP-aware routers along the tunnel path. Conceivably, there will not be any reservation state on the routers to meet the flow's requirements. To overcome the problem, authors in [39, 40] proposed a simple solution called RSVP Tunnels. In this method, tunnel entry and exit points in Mobile IP are considered as two end hosts, and for each RSVP session an individual RSVP Tunnel is established between tunnel end-points, if one does not exist. All end-to-end RSVP *Path* and *Resv* messages are encapsulated and passed through the RSVP tunnel, treated as a regular data packet. After reaching the tunnel exit point, packets are de-encapsulated and sent as regular end-to-end RSVP messages towards the destinations. The tunnels can be established in advance even if there are no end-to-end RSVP sessions between two tunnel end points. RSVP Tunnels have proven to be simple yet efficient. However, some refinements can be applied to end-to-end signalling management at tunnel entry points, resulting in a decrease in a number of end-to-end signalling messages passing through the tunnels.

IP-layer Handover

In RSVP, states are identified by a session-id, defined as a data flow with a particular destination address and transport layer protocol. When an MN changes its point of attachment in a network, it needs to acquire a new IP address. The change of IP address implies the change of session identity; consequently, the filters will not be able to identify the flow that had a reservation. A new end-to-end reservation should be established on a new path based on the new identity of the session, and since the old reservations will be of no use to any flow, they need to be released immediately, improving the network resource utilization. The new reservation may not be established immediately after handover, causing the QoS degradation or interruption for real time services. Therefore, the faster the resources are established along a new path, the fewer packets will be dropped or treated as a best-effort, and hence, is of great interest.

Receiver End

RSVP specification in [41] defines that only the *Path* message, RSVP message initiated by a sender, can create a new reservation state on routers along a path. The *Resv* message, the one initiated by a receiver, cannot. Conceivably when the MN as a receiver of the flow performs handover, it cannot simply invoke a resource reservation along the new path. On the other hand, RSVP in essence, does not support any internal mechanism to detect the MN's handover. Some external mechanisms should be used to inform the CN or other nodes in charge (RSVP proxy [42]) about the necessity of sending a *Path* message on the new path based on the flow's new identity. Upon receiving the message, the MN can send a *Resv* message, making the necessary resource reservation.

2.4.2 NSIS in Access Networks

Thoroughly analysing the RSVP problems in a mobile environment, the mobility support was considered in the initial stages of the QoS NSLP design. However, it was incompetent, and as a result, NSIS is experiencing the same incompatibility issues as RSVP when its functionality is combined with mobility management protocols.

Tunnelling

Similar to RSVP, without additional supports, NSIS signalling cannot be effective within IP tunnel segments of a signalling path. Traversing through the tunnel, NSIS signalling messages are transparent on the tunnelling path due to the packet encapsulation. Without having proper states to meet the flow's requirements, the tunnel segments become the weakest QoS links, and therefore, result in a violation of the end-to-end QoS support. Drawing similar concepts from RSVP Tunnels [40], authors in [43] suggested having an individual NSIS session established between the tunnel end-points, either preconfigured or dynamically created. All end-to-end QoS sessions traversing through are mapped to the NSIS tunnel session, receiving appropriate QoS treatments.

IP-layer Handover

In an effort to have mobility support, NSIS identifies a session by a globally unique session-id. That makes the session and associated states independent of the MN's location. In contrast, a flow associated with the session is identified by the MRI which is dependent on the IP addresses, and therefore, any changes to the MN's point of attachment will not affect the session but the flow associated with it. Consequently, the resource assigned to the session may not be used as it may refer to a non-existing flow. When the MRI changes due to handovers, an end-to-end signalling propagation seems inevitable. New information for proper data flow identification must be provided all the way between the data sender and receiver, e.g., in order to update filters, QoS profiles, or other flow-related session data [44]. Therefore, the NSLP signalling should be triggered after each handover along the new path while the old reservations need to be released immediately.

Being the Receiver

In NSIS, new resource reservation signalling can only be initiated in the downstream direction, from a sender to receiver of the flow. Being the sender, the MN can easily trigger the NSLP signalling messages on a new path, the *Reserve* or *Query* for the sender- or receiver-oriented reservation, respectively. However, having the MN as the receiver of the flow rises a concern. In order to reserve the resources on the new path, the next GIST peer discovery should be performed hop-by-hop on the upstream direction. However, the GIST upstream signalling is not possible except for some specific situations i.e., when the upstream peer is a default router of the single-homed network or is just one hop away which can be reached by tracking back the interface used to deliver the flow [23]. Therefore, the NSLP is very much dependent on the external driver, i.e., the network layer mobility management such as Mobile IP, to inform the CN about the MN's location and necessity of sending the NSLP messages on the downstream direction based on its new IP address.

2.4.3 Related Work

Tackling the interworking issues between the QoS signalling protocols and mobility management protocols has stimulated growing interest in the research community, resulting in the development of many proposals in recent years. Since the core of this work, in provision of QoS in access networks, is based on RSVP, this section focuses on introducing some of the prominent RSVP extensions to support mobility. However, being almost the same in the main concept of reservation signalling and the nature of the problems which arose in mobile networks, as shown earlier in this section, the similar approaches can be/have been applied to NSIS. A survey of other RSVP extensions to support mobility can be found in [16, 45].

MRSVP

MRSVP [46] is one of the first RSVP extensions for mobile networks. Intending to achieve seamless resource reservation after handover, MRSVP proposes two types of reservation: passive/advance reservation and active reservation. The MN makes passive reservations in multiple locations that might be visited during its connection lifetime, and once it enters their domain, their passive status will be changed to an active one. MRSVP assumes that this set of future locations, called Mobility Specification (MSpec), can be obtained in advance, from either the network or the MN as part of its mobility profile. The protocol introduces a new entity, called Proxy Agent, that makes the reservation along the paths, from the locations in the sender's MSpec to the ones in the receiver's MSpec. The agent located in the MN's visiting cell is called Local Proxy Agent, while the ones in other locations, specified in the MSpec, are called Remote Proxy Agent. All active and passive reservations between the MN and CN are established via the local and remote proxy agents, respectively. To increase the network utilization, the passive reservations can be used by best-effort or lower-priority traffic. However, upon changing their status to active, they need to be released immediately by the flows using them. This may cause the connection interruption and an increase in the call dropping rate.

MRSVP can guarantee a seamless QoS for the MN during handovers. However, reserving network resources as a passive reservation for MNs that *might* use them in the future causes significant wastage of resources in the network. Although they can be used by the lower-priority traffic, flows with the same QoS priority or higher cannot use them, and therefore resulting in an increase of the call blocking probability for new arrival users. Moreover, having a high number of active and passive reservation states for each MN and a necessity of sending periodic refresh messages causes a significant signalling load on the network and the processing overhead on proxy agents. Finally, the assumption of having knowledge of the MN's future locations is an important research question which has not been addressed in the paper.

The notion of using advance resource reservations has been used in other work to provide a seamless handover. Hierarchical Mobile RSVP (HMRSVP) [47] in-

tegrates RSVP with HMIP protocol. However, it makes advanced reservations only in potential inter-domain movements that cause the longer handover delay (in a boundary cell of the MN's neighbouring MAP domains). Although being more efficient than MRSVP, due to the inaccuracy of the target cell, the passive reservations made in all neighbour cells can have significant effect on resource wastage and increasing the call drop rate, as well as a number of signalling exchanges. Moreover, the scheme does not provide any solution for resource reservation problem inside the domain, raised by the intra-domain handover.
A new RSVP extension based on IP multicast was proposed in [48] in which future locations of the MN become the leaves of the multicast tree. The mobility of the host is modelled as a transition in multicast group membership, dynamically modifying every time the MN is roaming to a neighbouring cell.

Optimised ARR Scheme

A Reservation Optimised Advance Resource Reservation (ARR) Scheme [49] is another RSVP extension for mobility support. Similar to MRSVP, the protocol provides two types of reservations: an active reservation for current location and passive ones for neighbouring cells. However, to mitigate the wastage of resources caused by passive reservations, the proposed scheme includes two admission control mechanisms: a passive reservation limited mechanism and Session-to-Mobility Ratio (SMR)-based replacement mechanism.
The former intends to limit the number of passive reservations by making them inferior to the active ones. To that end, the available channels (network resources) are divided into two groups: dedicated channels and standard channels. While the active reservation requests can always use either of these channels, the passive reservations can only use the standard ones. Due to the limited amount of resources assigned to the passive reservation requests, the SMR-based replacement mechanism is defined to accept the most eligible passive reservation requests. Since the essential objective of an advance resource reservation scheme is to improve the MN's performance after handover, a request from a MN, which is most likely to perform a handover during a session and use its passive reservation, will serve first. Therefore, the less the MN's residence time in its previous cell, the

higher its chance is to perform a handover. Both admission control mechanisms are performed by a new entity located in each cell, called Enhanced Agent (EA). To guarantee that the channels are allocated correctly, the EAs monitor network resources and provide necessary information to their neighbouring EAs.
The optimised ARR scheme can achieve better utilization of resources as compared to the conventional advance resource reservation solutions such as MRSVP. However, the necessity of having the EA in each subnet and its duties increase the complexity of the mechanism. Also, similar to MRSVP, how to predict the MN position and define its mobility profile were not addressed specifically in this work.

Mobility-Aware RSVP

As expressed earlier, the major issue of using RSVP in mobile networks is MN's handovers, interrupting the acceptable level of QoS required by the flow and jeopardising its application-level performance. The interruption period consists of the time needed for the MN's location update, plus the time taken for re-establishing the resource reservation along a new path. Intending to shorten this time, Mobility-Aware RSVP [50–52] couples the existing solutions for the mobility management (i.e., HMIPv6) with RSVP, performing them as a single functional block. Based on this method, the mobility-based signalling messages, BU and BA, are carried by RSVP messages, through two newly defined RSVP objects. Mobility-aware RSVP takes advantage of RSVP capability in adding new object types for future compatibility. Base on the RSVP specification [6] any object that its class number is assigned to 11xxxxxx (where x can be 0 or 1) is considered as an unknown object class, and therefore, if the RSVP routers along the path cannot recognise it, they just forward it without further examination or modification. Exploiting this feature of RSVP, the flow end-points, MN and CN, can send mobility information (BU and BA) through RSVP objects while keeping them transparent to the routers along the path. As a result, no changes are required to be made to the legacy RSVP-enabled routers.
Mobility-Aware RSVP outperforms the other methods using conventional RSVP in mobile environments, however, both resource reservation and mobility management protocols need to be changed in order to be tightly coupled with each

other. Moreover, If the RSVP messages carrying the BU and BA get lost in the network, the handover latency increases significantly as the default time-out in RSVP protocol is 30 seconds.

RSVP-MP

Utilising the proxy concept in the localised mobility management protocols such as HMIP, RSVP Mobility Proxy (RSVP-MP) [53–55] introduces a new functional entity located at the edge of the local domain, it is e.g., an RSVP enhanced MAP, that intertwines the RSVP functionality with the localised mobility management one. The enhanced MAP divides an end-to-end RSVP reservation between the MN and CN to two parts: outside its domain and inside it. While in the former, the RSVP messages use the MN's RCoA, in the latter the reservation messages are dependent on the MN's LCoA. Upon receiving any RSVP messages, destined to the MN's RCoA, from its external interfaces, the enhanced MAP swaps the RCoA in the packet header and its content with the associated LCoA, and then forwards it to the next node inside the domain. Consequently, when the enhanced MAP receives any RSVP messages through its internal interface (MN's originated packets), it changes the LCoA in the packet with the associated RCoA and sends them to the CN.

In the case of handover, when the MN as a receiver of the flow enters a new subnet, it sends a BU to the MAP, informing it of its newly acquired LCoA. Upon receiving the message, the MAP checks if there is any reservation state for the MN's associated RCoA. If such an entry exists, a new resource reservation has to be established along the new path. To that end, the MAP sends a *Path* message to the MN's LCoA, using the CN's IP as a source address. When the MN receives the *Path*, it issues a *Resv* message destined to the CN. Along the way to the outside, the message is intercepted by the MAP, wherein any LCoA in its header and content is swapped with the RCoA, and then forwarded to the CN. At the same time, and for the uplink direction, the MN triggers the reservation on a new path by sending a *Path* message to the CN, using its new LCoA as a source address. When the MAP receives the message, it first changes the LCoA to the RCoA, and then forwards it to its external interface. Meanwhile, acting as a proxy on behalf of the CN, the MAP responds to the MN by sending a *Resv* message. By using this method, the new reservation will be established along the new path inside the domain, while the reservation for the outside part remains unchanged. Figure 2.2 shows the operation of RSVP-MP in mobile network [54].

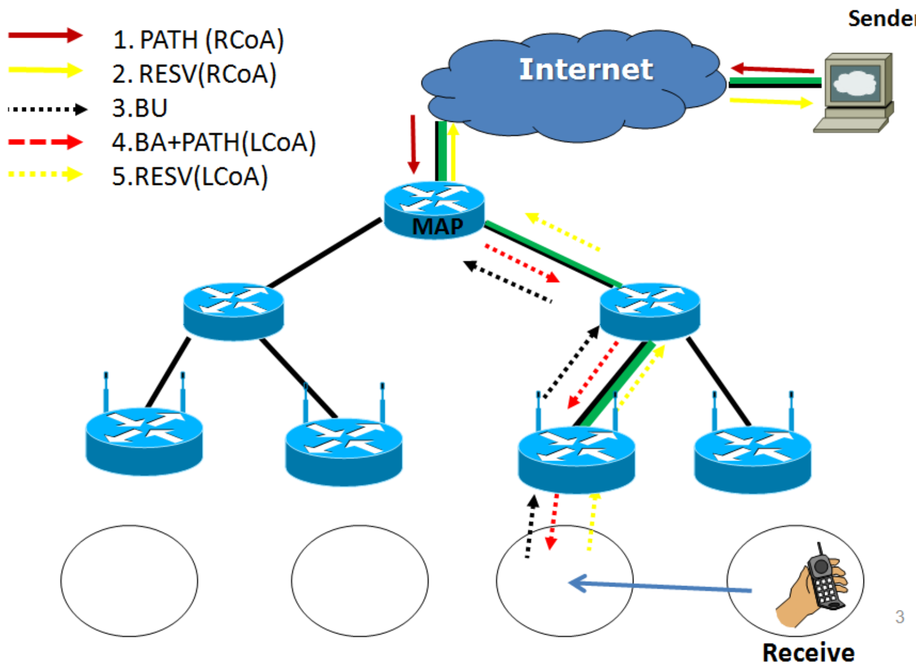


Figure 2.2: RSVP-MP operation in HMIP network

RSVP-MP avoids any type of hard-coupling between the resource reservation and mobility management protocols, reducing the complexity of the system and the changes required in the protocols stacks. Moreover, by restricting the RSVP signalling changes to the local domain, RSVP-MP can reduce the end-to-end resource re-establishment latency, between CN and MN. Nevertheless, still any change in the MN's LCoA requires a new RSVP signalling exchange between the MN and the MAP, even though the new and old paths have very much in common. Moreover, the process of swapping between the LCoA and RCoA in the packets' headers and contents causes an extra processing overhead in the MAP.

2.5 QoS in Backbone Networks

The vision of providing an end-to-end QoS was founded on the underlying assumption that a homogeneous Internet environment, equipped with QoS-enabled routers and end hosts, would be the common case. However, today's Internet architecture is in contrast to this assumption. Moreover, on the one hand, the scalability issue which arose from the state maintenance for every data flow in intermediate routers along the end-to-end path, creates a problem for the wide implementation of a fine-grained QoS, i.e., IntServ. On the other hand, the heterogeneous nature of the Internet, as a concatenation of technologically and administratively different domains, can jeopardize the coarse-grained traffic prioritization (i.e., DiffServ) based on the statically contracted SLA. Therefore, other solutions, such as Multi-Protocol Label Switching (MPLS), traffic engineering and constraint-based routing [56], have been proposed to provide QoS in backbone networks.

2.5.1 Multi-Protocol Label Switching Networks

In a connectionless network layer protocol, as a packet travels through the path, each router makes an independent forwarding decision to choose a next hop, including analysing the packet's header and running a routing algorithm. However, information contained in the packet headers is considerably more than that which is needed just to select the next router. Using this information, the process of selecting the next hop can be defined as the composition of two functions. The first one categorises the entire set of possible packets into a set of Forwarding Equivalence Classes (FEC) [57]. The second function maps each FEC to a next hop. From the forwarding decision point of view, all packets which belong to the same FEC and travel from a particular node, are identical, and therefore, follow the same path.

In a router running the conventional IP forwarding, two packets are in the same FEC if their destination IP addresses can be matched to the same longest-prefix in the router's routing table. The matching process is repeated in each node along the path wherein the packets are re-examined and assigned to an FEC. On the contrary, in Multi-Protocol Label Switching (MPLS) [57] the process of assigning a packet to a particular FEC is performed only once, as the packet enters the network. The information about the assigned FEC, encoded as a short fixed-length value known as a *label*, is sent along with the packet to the next hop. Without any further analysis of the packet's network layer header, the subsequent routers use the label as an index into a table which specifies the next hop, and a new label. The new label substitutes the old one and the packet is forwarded through the path followed by packets in the same FEC, called Label Switched Path (LSP). Forwarding packets based on labels instead of network layer destination addresses gives MPLS some outstanding features as compared to the conventional IP forwarding process. Some of them are listed below:

- Performing an FEC assignment at the entry of the network gives the ingress router the possibility of using, in determining the assignment, any available information about the packet apart from the ones obtained from its network layer header. For example, although being impossible in the conventional forwarding, the ingress router can assign different FECs for the packets arriving on different ports.

- A packet that enters the network at a particular router can be labelled differently than the same packet entering the network at a different router, and consequently, forwarding decisions that depend on the entry point to the network can be easily made.

- In some circumstances, it is desirable to route a packet through an explicitly pre-defined route, rather than the one chosen by the normal dynamic routing algorithm as the packet travels through the network. This may be done as a matter of policy, or to support traffic engineering.

According to the MPLS specification [57], not only can routers analyse a packet's network layer header to choose the next hop, but also to determine a packet's precedence or class of service, and therefore, making it possible to apply different discard thresholds or scheduling disciplines to different packets. MPLS allows (but does not require) the precedence or class of service to be fully or partially inferred from the label. In this case, one may say that the label represents the combination of an FEC and a class of service, making it possible to support differentiated services. MPLS is not a QoS technology in itself. Rather, it provides a flexible solution for support of DiffServ over MPLS networks [58]. This solution enables the MPLS network administrators to select how DiffServ BAs are mapped onto LSPs so that they can best match the DiffServ, traffic engineering [59] and protection objectives [60] within their networks.

2.5.2 Traffic Engineering

The main goal of all QoS schemes, such as IntServ and DiffServ, is to provide different levels of performance degradation during network congestion. In lightly-loaded network conditions, the IntServ, DiffServ and best-effort services differ lightly. Stimulated by this insight, traffic engineering has emerged as an efficient solution to avoid network congestion in the first place. Congestion can be caused either by the lack of enough network resources or by uneven traffic distribution among possible paths. The former occurs when all the links are overloaded, and has no solution but to upgrade the network physical infrastructure. The latter is caused by selecting the shortest path between two end-points of communication, used by dynamic routing protocols such as Intermediate System to Intermediate System (IS-IS) [61] and Open Shortest Path First (OSPF) [62]. Although the simplicity of selecting the shortest path guarantees the scalability of IP routing in a large scale network, it does not make efficient use of available resources in the network. The shortest paths between nodes may become congested while there might be unused resources on the longer paths, and as a result traffic can be unevenly distributed across the network.

To alleviate the problem, the Equal Cost Multi-Path (ECMP) feature in OSPF and IS-IS became an issue of great interest. ECMP discovers all potential paths, with identical costs, to a destination and splits traffic evenly onto the next hop routers on these paths. Although, ECMP results in a better load balance compared to a single-path routing, practically, ECMP solely supports even traffic splitting, which is not enough to approximate the optimal results obtained by using the arbitrary traffic splitting, such as in MPLS.

Traffic engineering intends to find appropriate routing and traffic allocation schemes, in order to balance the load distribution and optimise the overall network performance. Constraint-based routing is an important tool for making the traffic engineering process automatic [56]. A survey of different mechanisms used for Internet traffic engineering can be found in [63].

2.5.3 Constraint-Based Routing

Constraint Based Routing (CBR) represents a class of routing algorithms that compute routes to a flow's destination, subject to a set of requirements or constraints. One can say that CBR evolves from QoS Routing [64], but with a broader sense. Based on some knowledge of resource availability in the network, as well as the QoS requirements of the flows, QoS Routing returns the route that is most likely to be able to meet the given requirements. CBR extends the QoS-based routing concept by considering not only the topology of the network, but also the requirement of the flow, the resource availability of the links, and possibly other policies specified by the network administrators. In order to do that, routers need to distribute new link state information, including topology information and resource availability information, and to compute routes based on such information. While determining a route, CBR selects the one that can meet the criteria defined, and also can maximise the utilization of the current network facilities, thus maximise its revenue (or minimise its cost). As a result, a longer yet lightly-loaded path might be preferred to the shortest yet heavily-loaded path, hence resulting in the even distribution of network traffic. The constraints in CBR may be imposed by administrative policies (administrative-oriented), or by QoS requirements of the flow (service-oriented) [65]. The former is referred to as policy constraints and the associated routing is referred to as policy-based routing. While in the latter, the constraints imposed by QoS requirements, such as bandwidth, delay, or loss, are referred to as QoS constraints, and the associated routing is referred to as QoS-based routing [64, 66].

Policy-Based Routing

With the Internet continually growing, more stringent administrative constraints need to be considered when routing users' traffic. Policy routing ensures adequate resources/services provisioning from unauthorised users attempting to receive services that are not included in their SLAs. Policy routing, in its essence, is a matter of allocating resources in terms of business decisions. Instead of routing by the destination address, it allows network administrators to allow or deny paths, based on some pre-defined policies, such as packet size, end hosts' identity and an application or protocol used. The constraints can be provided either manually during network configuration or by extending the link state advertisement exchanged between nodes. By being more restrictive, the policy-based constraints are applied before the QoS-based constraints, especially when crossing autonomous system boundaries.

QoS-Based Routing

QoS-based routing is defined as a routing mechanism under which paths for flows are determined based on some knowledge of resource availability in the network, as well as the QoS requirement of the flows [64]. The objective of the QoS-based routing, a part from finding a path that can accommodate the requested QoS, is directing network traffic in a way that can maximise the network resource usage efficiency, e.g., improving the total network throughput, and degrade network performance gracefully during periods of heavy load.
Two major issues of QoS-based routing are: distribution of link state information and route computation complexity. One approach to dissemination of resource availability information between the nodes in the network, such as link available bandwidth, is to extend the link state advertisements of the routing protocols such as IS-IS and OSPF. However, due to the frequent change in link residual bandwidth, the trade-off should be made between the accuracy of the information and the overhead the frequent flooding of the link state advertisements introduces. The latter, the route computation algorithms and their degree of complexity, depends on the metrics chosen. Common route metrics are hop-count, bandwidth, reliability and delay, which can be categorised into three types: additive, concave, and multiplicative. Let $m(i_1, i_2)$ be a metric for link (i_1,i_2). For any path $P = (i_1, i_2, \ldots, i_n)$, metric M is:

- additive, if $M(P) = m(i_1, i_2)+m(i_2, i_3)+\cdots+m(i_{n-1}, i_n)$ (e.g., delay, jitter, cost, hop-count)

- multiplicative, if $M(P) = m(i_1, i_2) * m(i_2, i_3) * \cdots * m(i_{n-1}, i_n)$ (e.g., reliability, in which $0 \leq \mathrm{m}(i_i, i_j) \leq 1$)
- concave, if $M(P) = \min m(i_1, i_2), m(i_2, i_3), \ldots, m(i_{n-1}, i_n)$ (e.g., bandwidth meaning that the bandwidth of the path as a whole is determined by the link with the minimum available bandwidth)

Since concave metrics set the upper limit of all the links along a path, such as bandwidth, all the links that do not comply with the concave constraints can be simply pruned. Also, multiplicative metrics can be converted into additive ones by using the logarithmic function. Note that logarithm of the product is equal to the sum of the logarithms of the factors.

$$M(P) = \prod_{j=1}^{n-1} m(i_j, i_{j+1}) \tag{2.1}$$

$$M'(P) = \log\left(\prod_{j=1}^{n-1} m(i_j, i_{j+1})\right) = \sum_{j=1}^{n-1} \log m(i_j, i_{j+1}) = \sum_{j=1}^{n-1} m'(i_j, i_{j+1}) \tag{2.2}$$
$$\text{where} \quad M'(P) = \log M(P)$$

Therefore, the route computation is basically to find a best possible route that optimises additive metrics, however, it has been proven that problems involving two or more additive constraints are NP-complete [67]. Hence, tackling them requires heuristics.

2.6 Summary

This chapter gave the concise overview of different approaches used in an end-to-end QoS provisioning and mobility support. The former can be categorised in two parts: access and core networks. For the access part, RSVP was considered as a suitable candidate for providing a guaranteed QoS support per flow, establishing flow-depended states in the routers along the path. However, its problems in

mobile networks need to be overcome. Furthermore, it was shown that although mobility support was supposed to be considered in NSIS initial design, it inherited RSVP problems in mobile environment, while at the same time it proposes more complex signalling exchange between NSIS-aware nodes. With regard to the core network, due to the RSVP scalability issues, other solutions such as a constrained-based traffic engineering was considered as a handy tool in preventing congestion in the first place, and therefore, avoiding any packet loss or severe delay.
For the latter, the mobility protocol, the localised mobility management protocols have been selected as an efficient method of restricting the signalling exchange inside the domain. Two different approaches, host-based and network-based, were explained. While both follow the same concept in localising the signalling inside the domain by using a local mobility anchor point, the host-based needs the mobile user involvement in mobility detection and signalling exhcnage, while in the network-based approach these responsibilities are delegated to the mobility-aware access routers.

Chapter 3

An Efficient RSVP-Based QoS in Access Networks

3.1 Introduction

With the spread of mobile devices and the popularity of mobile multimedia applications, next generation wireless networks are expected to increase not only the quantity but the quality of the services for mobile users, and therefore, providing the appropriate level of QoS has become one of the major challenges for service providers in recent years. To that end, an extra control intelligence needs to be added to nodes along a data path, as just having simple routing and forwarding capabilities cannot fulfil customers' expectations any more. The nodes involved in forwarding the data packets need to be informed of the minimum requirements of a flow, dedicate resources, and maintain the reservation alive during the connection lifetime. Due to the frequent changes in uses' point of attachments in mobile networks, solutions for fixed networks, such as RSVP, cannot be considered as a good candidate. Both RSVP and Mobile IP can accomplish their goals separately, however, a combination of them does not work well in mobile networks. Whenever an MN moves to a new subnet, due to the changes in its address, the previous reservation is no longer valid, and a new reservation needs to be established along a new path. The process causes a significant signalling overhead and noticeable service interruption. During this time, QoS-based flows are treated as a best-effort, and therefore, prone to packet losses or severe delays in congested access networks. To mitigate these problems, an efficient RSVP mobility support for mobile networks is introduced in this chapter, intending to expedite an end-to-end resource re-establishment latency while reducing the total signalling overhead. The investigations, by means of an analytical model and a simulation, are conducted to analyse the behaviour of the proposed scheme in an access network with the localised mobility management support. The analytical framework introduced focuses on deriving total network-layer signalling costs, including the processing and propagation costs, and resource re-establishment latency. The effect of the number of mobile nodes and their average cell residence time on it, are also examined. On the other hand, the network-layer simulation scenario conducted in NS-2 investigates the behaviour of the proposed scheme in terms of the packet-loss, the number of packets treated as a best-effort, and the resource re-establishment latency.

It is of interest to note that, although, the proposed architecture is based on the RSVP signalling protocol in the HMIPv6 network, the solution can be applied to other flow-based signalling protocols in domain-based mobile networks, as discussed in the next chapter.

The remainder of this chapter is organised as follows: In Section 3.2 the architecture of the proposed scheme is studied in detail. Section 3.3 introduces the analytical framework, followed by the cost and resource re-establishment latency analysis. The simulation model was introduced in Section 3.4. Section 3.5 discusses the numerical results obtained by means of the analytical model and simulation. Finally, Section 3.6 brings closure to this chapter.

3.2 System Architecture

This section describes, in detail, the operation of the proposed scheme using RSVP, and HMIPv6 as a host-based localised mobility management protocol. The scheme architecture comprises of two parts: the mobility management and resource reservation. The former describes the approach used to support the node mobility and its location update process, while the latter defines the approach used for the resource reservation at time of handover. The aim is to have minimum changes to the current specifications of both protocols, and just in the mobility entities, while having no change in access routers and end-points.

3.2.1 Mobility Management Scheme

The proposed scheme extends the one-layer MAP architecture in HMIPv6 to two, named as Gateway MAP (GMAP) and Local MAP (LMAP). The GMAP is an enhanced version of MAP, located at the gateway of a regional network, while the LMAPs are mobility-aware entities located between the GMAP and MNs, dividing the regional network to M sub-regional domains, where M is a number of LMAPs.

Assume that each cell/subnet in the GMAP domain associates with at least one LMAP who has a knowledge of visiting MNs' home agent and CN(s) IP addresses. Under above assumptions, when an MN enters a new cell, it triggers the registration process by sending a Local BU (LBU) to a serving LMAP. The address of the LMAP can be obtained from the MAP option of a router advertisement. The sent message contains the MN's newly configured LCoA and RCoA. The LCoA is configured based on the prefix advertised by its default router, while the RCoA is based on the LMAP address's network prefix.

When the LMAP receives the message, it checks its binding cache table of any record about the MN's RCoA. If there is, it acknowledges the successful registration update by sending a Local BA (LBA) to the MN. In such a handover, called inner-LMAP handover, the MN's current location is only updated in the serving LMAP, making all MN's movements transparent to the GMAP. Figure 3.1 shows the signalling sequence of the proposed scheme during the inner-LMAP handover. If there are no records of the MN's previous location, the LMAP first assigns a unique ID to the MN. Then, it creates a binding cache entry, and configures a new RCoA$'$ based on the GMAP's subnet prefix. After that, it sends a registration request towards the GMAP. Upon successful completion of the registration, the GMAP sends a BA, keeping the LMAP address as a next destination for any packets destined to the MN. When the LMAP receives the message, it puts the RCoA$'$ in a new mobility option and forwards it to the MN. The address is used by the MN as a source address in any packets originated. Such a han-

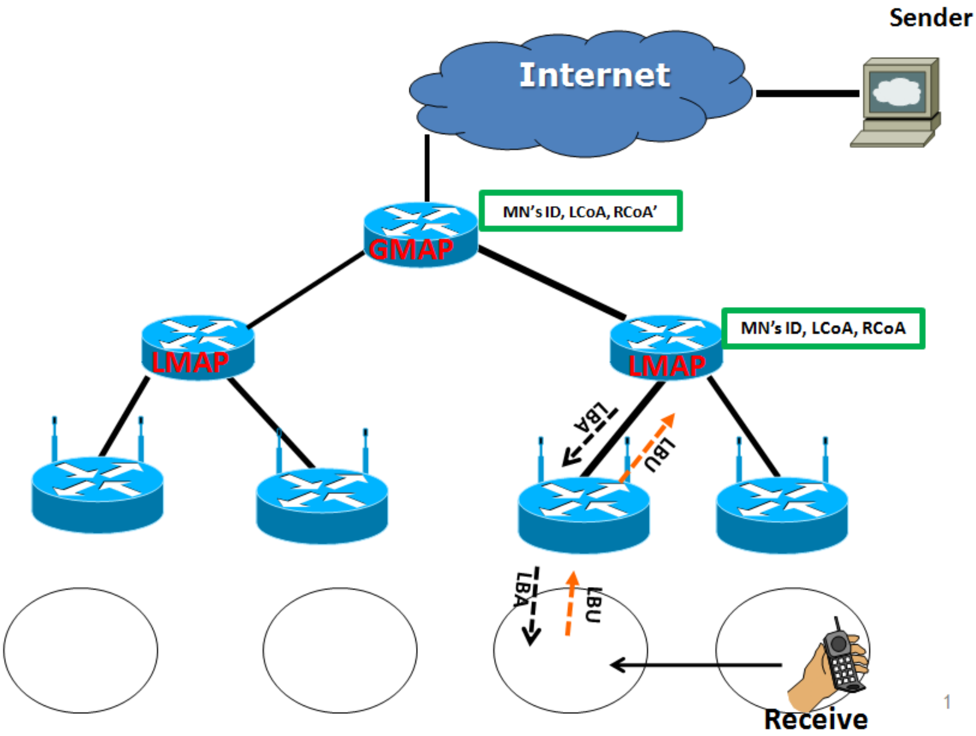


Figure 3.1: Proposed scheme signalling in inner-LMAP Handovers

dover, in which the MN's old and new LMAPs belong to a same GMAP, is called inter-LMAP handover. Figure 3.2 shows the signalling sequence of the proposed scheme during this type of handovers.

The signalling process inside the domain will be the same if the old and new LMAPs belong to different GMAPs (inter-GMAP handover). However, a new LMAP should send a BU to the MN's HA and CN(s), on behalf of the MN, informing them about its new network.

3.2.2 Resource Reservation Scheme

Tunnelling is the essential part of the Mobile IP and its extensions. However, wrapping RSVP messages makes them indistinguishable on RSVP-aware routers along a tunnel path. For each end-to-end reservation, a separate RSVP session called *RSVP tunnel* needs to be established between the tunnel end-points, i.e., the MAP and MNs.

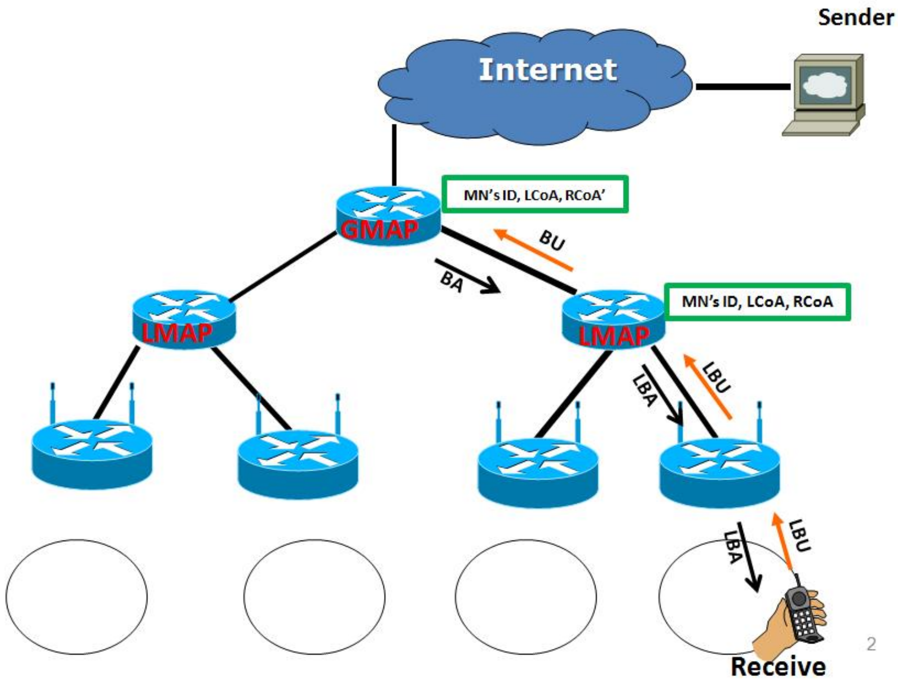


Figure 3.2: Proposed scheme signalling in inter-LMAP Handovers

Exploiting the multi-layer architecture of the proposed scheme, an end-to-end reservation inside the GMAP domain can be divided into two parts: the first part between the LMAP and MN, and the second between the GMAP and LMAP. While the former needs to be updated whenever the MN changes its point of attachment, the latter depends on the MN's current sub-domain, remaining unchanged as long as the MN stays inside it. Since the second part is the same for all MNs belonging to a same LMAP domain, instead of having an individual RSVP tunnel for each session, only one RSVP session can be used between the LMAP and GMAP as the tunnel end-points. This can reduce the processing cost on RSVP-aware routers along the tunnel, and the amount of signalling messages passed through.

According to the process explained in the mobility management scheme, a reservation message, sent by the CN to MN, contains the MN's RCoA′ as the destination IP address. When the GMAP receives this message, it acts as an endpoint of the connection, replying back to the CN on behalf of the MN. At the same time, it maps the reservation request to the pre-configured RSVP tunnel between itself and the MN's serving LMAP. However, instead of exchanging RSVP messages through the tunnel, it just sends a new defined RSVP object, called Session_Trigger (Figure 3.3), to the LMAP asking it to reserve the resources for the MN. The object contains the CN's IP address, the traffic specification, and the MN's ID. Upon receipt of this information, the LMAP works as a proxy and initiates a new RSVP session destined to the MN's current location.

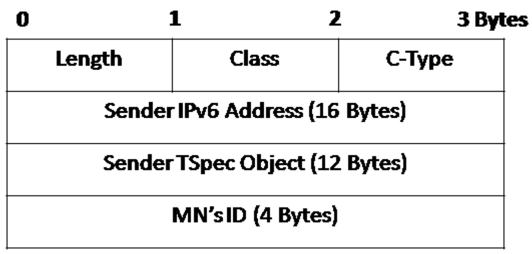


Figure 3.3: Trigger_Session Object format

When the LMAP receives this object, it tries to find the MN's LCoA base on the MN's ID, and establishes an end-to-end RSVP session between itself and the MN. When the MN receives a *Path* message originated by the LMAP, it replies back by a *Resv* message. Figure 3.4 depicts the operation of proposed scheme when the MN operates as the receiver of the flow.

In order to remove the reservation, the Delete_Session object is defined with the same structure as the Trigger_Session object, but different class type. The object can be used by either of the RSVP tunnel end points to inform the other end about the necessity of removing the resources assigned for an individual flow. Contrary to the conventional RSVP tunnel wherein all the end-to-end RSVP messages, including the set-up and refresh, are encapsulated and sent through the tunnel, in the proposed scheme only the new defined objects are exchanged between two end-points, resulting in a significant reduction of signalling overhead between tunnel end-points.

For the sake of simplicity, the static threshold-based mechanism is used to pre-allocate resources for each tunnel C_{T}, in which the maximum amount of resources authorised by administration polices is assigned, $C_{\mathrm{T}} = \psi_{max}$. However, one can use the dynamic threshold-based mechanism. In this method the constant value is assigned to the tunnel, and afterwards, based on the monitoring and predicting

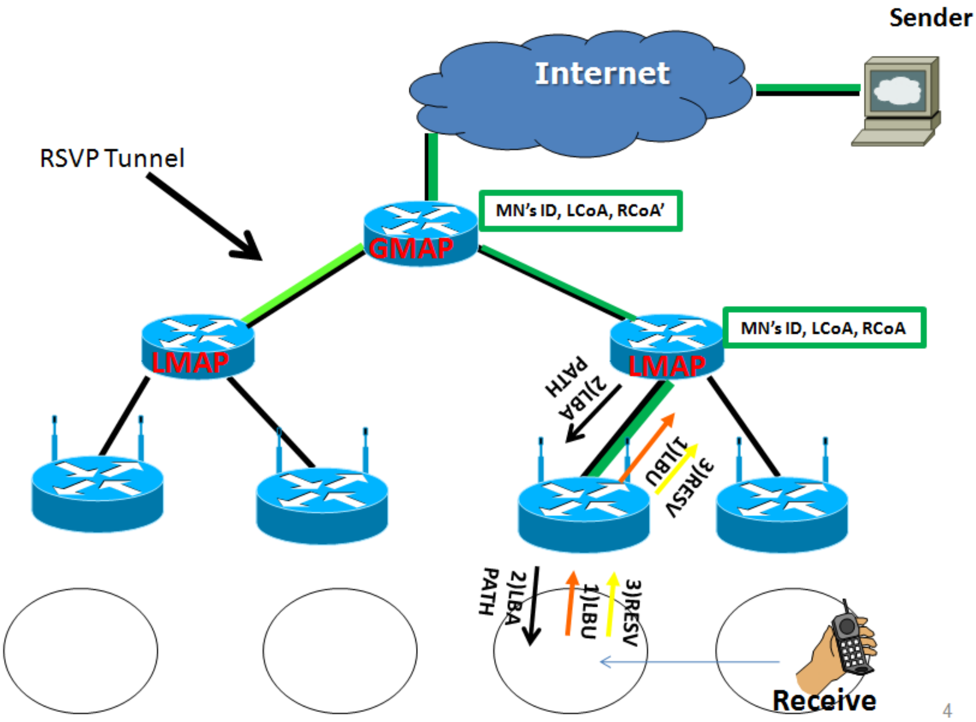


Figure 3.4: Operation of the proposed Scheme (MN as a receiver)

of the future demand the extra chunk of resources B can be added, or released.

$$\psi_{min} \leq C_{\mathrm{T}} = \psi_{min} {}^{+}_{-} B \times i \leq \psi_{max}, \quad \text{where} \quad i = 0, 1, ... \tag{3.1}$$

In order to increase the efficiency of the resources assigned to the RSVP tunnels, they can be used by the best-effort traffic, if there were no demand for them.
When the MN is the sender of the flow, the main concept is the same as the previous part. The MN starts the resource reservation process by sending a *Path* message to the CN. Upon receiving the message, the LMAP acts as an RSVP proxy and sends a *Resv* message to the MN, on behalf of the CN. At the same time, it maps the session to the RSVP tunnel between itself and the GMAP by sending the Trigger_Session object. The object includes the MN's ID, CN's IP address and Sender_TSpec of the received *Path*. When the GMAP receives this object, it initiates an end-to-end RSVP session between itself and the CN.

3.3 Analytical Model

An analytical framework for evaluating the performance of the proposed scheme is developed in this section. The framework focuses on the MN's handover scenario inside the regional domain, taking into the account its traffic behaviour and mobility behaviour. The former describes the approach used for modelling the arrival of the user session, while the latter defines the way the MN moves within the network. The expected outputs of the proposed analytical model are:

1. Probability of performing different types of handover, including the inner-LMAP, inter-LMAP and inter-GMAP handovers

2. MN's average residence time inside the regional domain, and sub-domains

Both outputs are used to derive the total cost function and resource re-establishment latency, discussed later in this section. To highlight the improvements achieved by the proposed scheme, RSVP-MP introduced in Section 2.4.3 has been chosen as a baseline protocol. The reasons for selecting RSVP-MP are: It does not waste the network resources by having the passive reservations, neither it needs the tight coupling between the mobility management and resource reservation protocols, which makes it appealing to be adopted and implemented in mobile networks.

3.3.1 User Traffic and Mobility Models

The traffic model comprises of a session and a packet, which the terms session and call can be used interchangeably. The incoming calls to the MN are the Poisson process, consequently, the Exponential distribution is considered for the inter-call time (inter-arrival time). It is possible that a new call arrives when the previous call is still in progress, and therefore, the call might be blocked. As a result, an inter-service time will differ from the inter-arrival time, and cannot follow the Exponential distribution. The phenomenon is called the *busy line* effect [68]. Assume that a call duration is smaller than the inter-arrival time, the busy line effect can be assumed insignificant. Given this assumption, the inter-service time can follow the Exponential distribution. Although other distribution models, such as Gamma and Pareto, have been proposed in the literature to model the MN's traffic behaviour, the performance evaluations in [68] show that the exponential model can be appropriate for cost analysis, making an acceptable trade-off between complexity and accuracy.

The mobility model was developed under the assumptions introduced in [69], which has been receiving considerable attentions in the literature. The model is based on the hexagonal cellular network architecture with K rings (0 to K-1), wherein each cell corresponds to one subnet domain. The innermost cell is the centre cell (ring 0). All cells around the centre cell form the ring 1. Consequently, all cells around the ring k form the ring $k + 1$. The distance of each cell from the centre cell is equal to the number of rings between them. Each MN stays in a cell for a time period then selects, with equal probability of 1/6, any of the neighbouring cells for its next position. Figure 3.5 shows the architecture of the model, with an example of the MN's movement between points A and B.

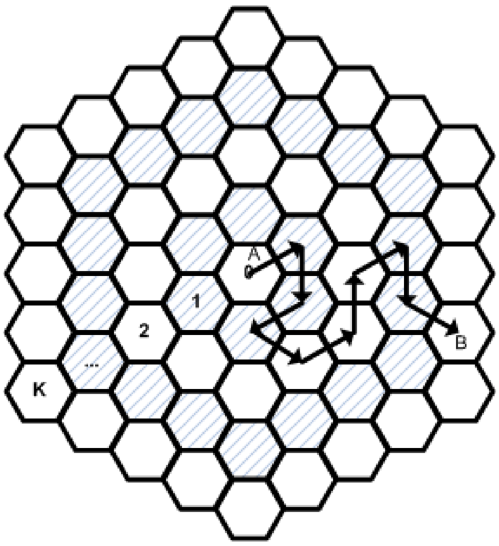


Figure 3.5: Hexagon cellular architecture

The mobility of the MN is therefore based on a two-dimensional random walk model. Between all the mobility models, the fluid-flow model and the random walk model are the two main types of mobility model that have been applied in location-management studies. The fluid-flow model can derive the average rate of boundary crossings, per unit time, out of a given area. It usually describes the mobility in terms of the mean number of users crossing the boundary of a given area, and it is difficult to apply the model to the per-user-based location-area strategies [70]. In the random walk model, on the other hand, a user randomly chooses a destination point in the given area, moves with constant speed v (uniformly distributed between $[v_{min}, v_{max}]$) on a straight line to this point, and then pauses for certain time before it again chooses a new destination [71]. Users in cells have identical movement pattern within and across boundaries. Such cells can be assigned to a single state in the Markov chain model. By using the concept of ring in a domain, the complex two-dimensional random walk can be reduced to a simple one-dimensional one with fewer states (Figure 3.6).

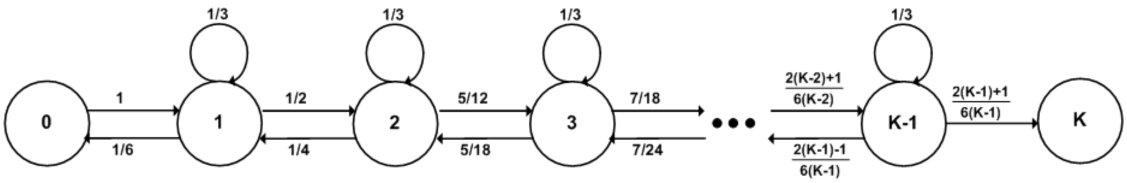


Figure 3.6: State diagram for the 1-D random walk model

Under above assumptions, the probability that the MN moves to the ring $i+1$ or $i-1$, p_i^+ and p_i^-, can be given as follows:

$$p_i^+ = \frac{2i+1}{6i} \quad \text{and} \quad p_i^- = \frac{2i-1}{6i} \tag{3.2}$$

Given K as the number of rings in the domain, the $K \times K$ transition matrix, P_K, becomes:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & . & 0 & 0 & 0 \\ 1/6 & 1/3 & 1/2 & 0 & 0 & . & 0 & 0 & 0 \\ 0 & 1/4 & 1/3 & 5/12 & 0 & . & 0 & 0 & 0 \\ 0 & 0 & 5/18 & 1/3 & 7/18 & . & 0 & 0 & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & . & \frac{2(K-1)-1}{6(K-1)} & 1/3 & \frac{2(K-1)+1}{6(K-1)} \\ 0 & 0 & 0 & 0 & 0 & . & 0 & 0 & 1 \end{pmatrix} \tag{3.3}$$

An element $p_{i,j,K}$ in P_K and P_K^n is defined as the probability that the MN locating at a ring-i cell moves to a ring-j cell in *one* and n cell boundary crossing, respectively. Let $\beta(k,n)$ be the probability that after n movements the distance between the current and initial position of the MN, defined in terms of number of rings, is k. Given the initial position is the centre cell, $\beta(k,n)$ can be defined as:

$$\beta(k,n) = P_{0,k}^{n} \quad where \quad P_{0,k}^{n} = P_{0,k} \times P_{0,k}^{n-1} \tag{3.4}$$

Assume that the domain consists of K rings, ring 0 to ring K-1, and the MN is initially located in the centre cell [72]. The probability of performing the inter-domain handover, *q(K)*, is equal to the probability that the MN be in the K^{th} ring (ring number K-1) *and* decides to go to a cell located at $(K+1)^{th}$ ring. Therefore:

$$q(K) = \pi_{\mathrm{K}} \times p_{\mathrm{K}}^{+} \tag{3.5}$$

where π_{K} is the probability that the MN being located in the K^{th} ring and is:

$$\pi_{\mathrm{K}} = \Sigma_{n=0}^{\infty}\alpha(n)\beta(K,n) \tag{3.6}$$

$\alpha(n)$ is the probability that the MN performs n handovers between two calls. Let the cell residence time follow the general distribution with the probability density function $f_m(t)$, Laplace transform $f_m^*(s)$ and with a mean of $\frac{1}{\lambda_m}$. Given that the call arrival to the MN follows the Poisson process with the rate λ_c, $\alpha(n)$ is [73]:

$$\alpha(n) = \begin{cases} 1 - \frac{1-f_m^*(\lambda_c)}{\phi} & n = 0 \\ \frac{1}{\phi}\left[1 - f_m^*(\lambda_c)\right]^2 \left[f_m^*(\lambda_c)\right]^{n-1} & n > 0 \end{cases} \tag{3.7}$$

where $\phi = \frac{\lambda_c}{\lambda_m}$ is the MN's Session-to-Mobility Ratio (SMR). Although most of the studies consider the Exponential distribution for the MN residence time, here, the Gamma distribution has been chosen. The Gamma distribution is a general type of distribution which can mimic the attributes of other distributions like the Exponential and Erlang distributions. Moreover, it has the simple Laplace transform that makes $\alpha(n)$ calculation easier. Equation 3.8 shows the Laplace transform of the Gamma distribution with a variance V and a mean $\frac{1}{\lambda_m}$:

$$f_m^*(s) = \left(\frac{\lambda_m \gamma}{s + \lambda_m \gamma}\right)^{\gamma} \qquad \text{where} \quad \gamma = \frac{1}{V\lambda_m^2} \tag{3.8}$$

After calculating the probability of performing handover, the next step is to calculate the MN's average residence time inside the domain. Assume that N(K) is the total number of cells in a domain with K rings and is equal to:

$$N(K) = \sum_{k=1}^{K-1} 6 \times k + 1 = 3K(K-1) + 1 \tag{3.9}$$

The MN's residence time in the domain, Y, can be expressed as:

$$Y = X_1 + X_2 + \cdots + X_m \tag{3.10}$$

where m is the number of cells visited by the MN, and X_i is the MN residence time in each cell with Laplace transform $f_m^*(s)$. The Laplace transform of Y can be obtained as follows:

$$\begin{aligned} f_Y^*(s) &= E[e^{-sY}] \\ &= E[E[e^{-sY}]|M] \\ &= E[E[e^{-s(X_1+\cdots+X_m)}]|M] \\ &= E[E[e^{-s(X_1)}]\ldots E[e^{-s(X_m)}]] \\ &= E[f_m^*(s)^M] \\ &= \mathcal{G}_M(f_m^*(s)) \quad \text{(by the definition } E[z^M] = \mathcal{G}_M(z)\text{)} \end{aligned} \tag{3.11}$$

The Generating function $\mathcal{G}_M(z)$ of the uniform distribution is given by:

$$\mathcal{G}_M(z) = \frac{z}{N(K)} \times \frac{1 - z^{N(K)}}{1 - z} \tag{3.12}$$

Using 3.12, the Laplace transform of Y can be written as:

$$f_Y^*(s) = \mathcal{G}_M(f_m^*(s)) = \frac{\left(\frac{\lambda_m\gamma}{s+\lambda_m\gamma}\right)^{\gamma}}{N(K)} \times \frac{1-\left(\frac{\lambda_m\gamma}{s+\lambda_m\gamma}\right)^{\gamma N(K)}}{1-\left(\frac{\lambda_m\gamma}{s+\lambda_m\gamma}\right)^{\gamma}} \tag{3.13}$$

Finally, the mean value of the MN's residence time in the domain ,$\overline{\tau}_{ha}$, can be expressed as follows [74]:

$$\overline{\tau}_{ha} = -\frac{df_Y^*}{ds}|_{s=0} = \frac{N(K)+1}{2\lambda_m} \tag{3.14}$$

3.3.2 Total Signalling Cost

The signalling overhead and resource reservation latency can be considered as useful metrics to define QoS in IP-based wireless networks [75]. This section provides detailed analysis of these metrics, in order to evaluate the performance of the proposed scheme as compared to the baseline protocol, RSVP-MP. In all scenarios, the MN is considered as a receiver of the flow, since this is the most challenging part of the RSVP operation in mobile environments.

The signalling cost is defined as the total cost needed to transmit and process extra signalling messages required during the handover process. As discussed in [76], the cost parameter has no unit but can be defined to be proportional to the delay required to send or process a signalling message. Other measurements for the cost parameters are possible. For example, the network administration can assign specific cost values to each operation based on the available bandwidth of a link, computation resources at a node, and the expenses required to operate a particular mobility agent.

The total signalling cost (C_{Total}) comprises of a location update signalling cost, packet delivery signalling cost and resource reservation signalling cost represented by C_{LU}, C_{PD} and C_{RR}, respectively.

$$C_{Total} = C_{\text{LU}} + C_{\text{PD}} + C_{\text{RR}} \tag{3.15}$$

Table 3.1: Notation of RSVP-based QoS in access networks

λ_m	MN's cell crossing rate
λ_c	MN's session arrival rate
K	number of rings in the MAP/GMAP domain
K'	number of rings in the LMAP domain
q	probability of performing the inter-MAP/GMAP handover
$(1-q)$	probability of performing the inner-MAP/GMAP handover
$q'/(1-q')$	probability of performing the inter/inner-LMAP handover
$\overline{\tau}_{ha}$	MN's average residence time in the MAP/GMAP domain
$\overline{\tau}_{m'}$	MN's average residence time in the LMAP domain
t_m	MN's average residence time in each cell
T_{rf}	binding update lifetime in the MAP/GMAP/LMAP/HA/CN
η	RSVP message processing cost at each node
T_{rrf}	RSVP message lifetime
D_{x-y}	Hop-based distance between X and Y
TC_{x-y}	transmission cost between nodes x and y ($\delta D_{x-y} + \zeta\delta$)
δ	unit transmission cost in wired link
ζ	weighting factor for the unit transmission cost in wireless link
PC_x	processing cost of mobility control packet at node X
$B_{w/wl}$	bandwidth of wired/wireless link (in bits per second)
$L_{w/wl}$	wired/wireless link propagation delay
q_f	probability of an unsuccessful message delivery on wireless link
b	size of the message in bits
T_w	time needed to determine that the message is lost

3.3.2.1 Location Update Cost

The hierarchical architecture of the mobility management scheme in RSVP-MP lets an MN have two kinds of handover: the local handover and the global. The former occurs whenever the MN moves between two cells both belonging to the same MAP (inner-MAP handover), while in the latter the cells belong to different MAPs (inter-MAP handover). The MAP registration process is the same for both scenarios, however, extra signalling messages need to be exchanged between the MN and its HA and CN during the inter-MAP handover. Apart from registration, the periodic BU and BA are exchanged between the peers in order to extend the binding lifetime. This cost is represented by C_{BR}. Given that C_g and C_l are the signalling cost of the global and local handovers, the location update cost of

RSVP-MP can be given as:

$$C_{\mathrm{LU}} = \lambda_m(qC_g + (1 - q)C_l) + C_{\mathrm{BR}} \tag{3.16}$$

Since the link layer, authentication and address configuration delays are the same in all scenarios, they are omitted in the analysis. C_g, C_l and C_{BR} can be derived as follows:

$$\begin{aligned}
C_l &= 2TC_{mn-map} + PC_{map} \\
C_g &= C_l + 2TC_{mn-ha} + PC_{ha} + 2TC_{mn-cn} + PC_{cn} \\
C_{\mathrm{BR}} &= 2\lfloor\frac{t_m}{T_{rf}}\rfloor TC_{mn-map} + 2\lfloor\frac{\overline{\tau}_{ha}}{T_{rf}}\rfloor(TC_{mn-ha} + TC_{mn-cn})
\end{aligned} \tag{3.17}$$

According to the proposed mobility management scheme, the MN can perform three kinds of handover: an inner-LMAP handover, inter-LMAP handover and inter-GMAP handover. The inner-LMAP handover occurs when the MN moves between two cells both belonging to the same LMAP in which the MN's new location needs to be updated. However, if the new cell belongs to a different LMAP, extra messages are sent to the GMAP by the new LMAP informing it about the MN's new sub-domain address. The process is called the inter-LMAP handover. It is possible that the new and old LMAPs belong to different GMAPs resulting in the MN's inter-GMAP handover. In this case, the registration process inside the GMAP is the same as the inter-LMAP, however, additional registration requests are sent by the serving LMAP to the MN's HA and CN. Considering all these kinds of handover, the location update cost in the proposed scheme can be expressed as follows:

$$C_{\mathrm{LU}} = \lambda_m\left[qC_{interGM} + (1 - q)\Big(q'C_{interLM} + (1 - q')C_{innerLM}\Big)\right] + C_{\mathrm{BR}} \tag{3.18}$$

where $C_{interGM}$, $C_{interLM}$ and $C_{innerLM}$ are the cost of the inter-GMAP, inter-LMAP and inner-LMAP handovers:

$$\begin{aligned}
C_{innerLM} &= 2TC_{mn-lmap} + PC_{lmap} \\
C_{interLM} &= C_{innerLM} + 2TC_{lmap-gmap} + PC_{lmap} + PC_{gmap} \\
C_{interGM} &= C_{interLM} + 2TC_{lmap-ha} + PC_{ha} + 2TC_{lmap-cn} + PCcn \\
C_{\text{BR}} &= 2\lfloor\frac{t_m}{T_{rf}}\rfloor TC_{mn-lmap} + 2\lfloor\frac{\overline{\tau}_{m'}}{T_{rf}}\rfloor TC_{lmap-gmap} + 2\lfloor\frac{\overline{\tau}_{ha}}{T_{rf}}\rfloor(TC_{lmap-ha} + TC_{lm-cn})
\end{aligned} \tag{3.19}$$

3.3.2.2 Resource Reservation Cost

In the RSVP-MP operation, MAP acts as an RSVP proxy dividing an end-to-end reservation between the MN and CN into two parts. The first part is between the MAP and CN based on the MN's RCoA, while the second is between the MAP and MN depending on the MN's LCoA. Consequently, any changes in the MN's LCoA or RCoA, as a result of the inner-MAP or inter-MAP handover, makes the previous reservation invalid. To fulfil the QoS requirement after handover, a new reservation should be placed along a new path immediately. Moreover, due to the soft-sate nature of RSVP, periodic messages, i.e., *Path* and *Resv*, need to be exchanged between the peers with the cost of R_{RF}. Therefore, the resource reservation cost in RSVP-MP becomes:

$$C_{\text{RR}} = \lambda_m\Big(qR_g + (1-q)R_l\Big) + R_{\text{RF}} \tag{3.20}$$

where R_l and R_g are the cost of reservation re-establishment due to the inner-MAP and inter-MAP handovers, respectively. Assume that nodes are RSVP aware, the RSVP signalling cost, including the transmission cost and processing cost in all the nodes along the path, can be given as follows:

$$\begin{aligned}
R_l &= 2TC_{map-mn} + 2D_{map-mn} \times \eta \\
R_g &= R_l + 2TC_{map-cn} + 2D_{map-cn} \times \eta \\
R_{\text{RF}} &= 2\lfloor\frac{\overline{\tau}_{ha}}{T_{rrf}}\rfloor TC_{map-cn} + 2\lfloor\frac{t_m}{T_{rrf}}\rfloor TC_{map-mn}
\end{aligned} \tag{3.21}$$

In the proposed scheme, an end-to-end RSVP session between the CN and MN is divided into three parts. The first part is between the CN and GMAP, based on the MN's GMAP domain address. The next is between the GMAP and LMAP, based on the MN's LMAP address. The last part is between the LMAP and MN depending on the MN's current point of attachment in the LMAP domain. Given R_{RF} as the RSVP refresh overhead, the resource reservation cost of the proposed scheme becomes:

$$C_{\text{RR}} = \lambda_m \Bigg(qR_{interGM} + (1-q)\Big[q'R_{interLM} + (1-q')R_{innerLM}\Big]\Bigg) + R_{\text{RF}} \quad (3.22)$$

where $R_{interGM}$, $R_{interLM}$, and $R_{innerLM}$ are the cost of reservation establishment due to the inter-GMAP, inter-LMAP, and inner-LMAP handovers, respectively. Note that the resource reservation cost comprises of the transmission and processing costs of the RSVP *Path* and *Resv* messages in all the nodes between two end-points of the reservation session. This is the same for all the reservation costs introduced in this section but $R_{interLM}$. The reason is that when the MN's changes its LMAP domain, its resource reservation request is mapped to the RSVP tunnel, established in advance between the GMAP and LMAP. Therefore, the reservation cost is diminished to the transmission of the one RSVP message, sent by the GMAP to inform a new LMAP about the MN's reservation requirement. The costs can be expressed as follows:

$$\begin{aligned}
R_{innerLM} &= 2TC_{lmap-mn} + 2\eta D_{lmap-mn} \\
R_{interLM} &= R_{innerLM} + TC_{lmap-gmap} + \eta D_{lmap-gmap} \\
R_{interGM} &= R_{interLM} + 2TC_{gmap-cn} + 2\eta D_{gmap-cn} \\
R_{\text{RF}} &= 2\lfloor\frac{\overline{\tau}_{ha}}{T_{rrf}}\rfloor TC_{gmap-cn} + 2\lfloor\frac{\overline{\tau}_{m'}}{T_{rrf'}}\rfloor \frac{TC_{lmap-gmap}}{N' \times w} + 2\lfloor\frac{t_m}{T_{rrf}}\rfloor TC_{lmap-mn}
\end{aligned} \quad (3.23)$$

where N' is the number of access routers in a LMAP domain, each serving w mobile nodes.

3.3.2.3 Packet Delivery Cost

Assume that Route Optimization is enabled, the first packet in a session goes to the HA, while the rest are directed to the MAP who intercepts and tunnels them to the MN's LCoA. The packet delivery cost of RSVP-MP can be given as:

$$C_{PD} = C_{ha} + C_{map} + C_T \tag{3.24}$$

where C_T is the packet transmission cost between the CN and MN. C_{ha} and C_{map} are the packet processing cost at the HA and MAP, respectively. Given that Θ_{ha} is a constant value for a packet processing cost at the HA, C_{ha} can be expressed as:

$$C_{ha} = \lambda_c \times \Theta_{ha} \tag{3.25}$$

The packet processing cost at the MAP consists of two parts: a cost of searching the binding table to find the MN's LCoA, as well as a cost of routing the encapsulated packet to the MN. The former is proportional to the size of the mapping table. The size of binding-table is proportional to the number of MNs located in the MAP domain. Using the Binary search, the average routing cost becomes proportional to the logarithm of the number of access routers in the MAP domain. Assuming that there are N access routers in the MAP domain, each serving w MNs, C_{map} becomes:

$$C_{map} = \lambda_c E(S)(\alpha N \times w + \beta \log(N)) \tag{3.26}$$

where α and β are weighting factors and E(S) is the average number of packets in each session. The packet transmission cost, C_T, can be found as follows:

$$C_{\mathrm{T}} = \lambda_c(E(S) - 1)TC_{cn-mn} + \lambda_c(TC_{cn-ha} + TC_{ha-mn}) \tag{3.27}$$

In the proposed scheme, C_{ha} and C_{T} are the same as the ones calculated for RSVP-MP in Equations 3.25 and 3.27. However, the packet processing cost inside the GMAP domain is higher than the one in RSVP-MP. This is due to having an extra processing cost, including the table look-up and routing costs, in the LMAP for each packet. Assume that the GMAP has N access routers, and the LMAP has N′, C_{gm} can be expressed as:

$$C_{gm} = \lambda_c E(s)[(\alpha N w + \beta \log(N)) + (\alpha N' w + \beta \log(N'))] \tag{3.28}$$

3.3.3 Resource Re-establishment Latency

The resource reservation latency t_{RL} is defined as a total time taken to perform a handover, as well as re-establish an end-to-end resource reservation along a new path in the MAP/GMAP domain. The handover latency comprises of the delays imposed by the layer 2 handover t_{L2}, new IP address configuration t_{AC}, and binding update process. In RSVP-MP, when the MAP receives a BU, it sends a BA, and afterwards a new RSVP *Path* message towards the MN. The reservation on the new route is completed when the MAP receives the *Resv* message initiated by the MN. Therefore, the reservation latency in RSVP-MP can be given as follows:

$$t_{\text{RL}} = t_{\text{L2}} + t_{\text{AC}} + [\text{M}(\text{BU}) + \text{MAX}(\text{M}(\text{BA}), \text{M}(\text{PATH})) + \text{M}(\text{RESV})]_{mn-map} \tag{3.29}$$

where $\text{M}(\text{X})$ is the time taken to send a message X between two nodes, including the transmission time and propagation time, and is equal to [77]:

$$\begin{aligned}
&\text{M} = \frac{b}{\text{B}_{w/wl}} + \text{L}_{w/wl} \\
&\text{M}_{wired} = \text{D}_{x-y} \times \text{M} \\
&\text{M}_{wireless} = \text{M} + (\text{T}_w + \text{M}) \times \frac{q_f}{1 - q_f}
\end{aligned} \tag{3.30}$$

Consequently, the message transmission time between a node X and node Y can be written as time taken in the wired part, as well as the wireless part of the route. While the former is proportional to the distance between nodes X and Y, based on the hop distance unit (denoted by the D_{X-Y}), the latter depends on the probability of the wireless link failure (q_f). Due to the unpredicted nature of the wireless link, the time of sending the message on the wireless link composes of the one successful transmission denoted by M, and $(T_w + M) \times \frac{q_f}{1-q_f}$ times unsuccessful packet transmissions [77]. For the proposed scheme, based on the probability of performing different types of handover, the resource re-establishment latency can be given as follows:

$$t_{\text{RL}} = t_{\text{L2}} + t_{\text{AC}} + q' t_{interLM} + (1 - q') t_{innerLM} \tag{3.31}$$

where $t_{innerLM}$ and $t_{interLM}$ are the reservation latency during the inner-LMAP and inter-LMAP handover, respectively. For the inner-LMAP handover, $t_{innerLM}$ can be obtained as in Equation 3.29 except that here the distance is limited between the MN and serving LMAP.
During the inter-LMAP handover, when the LMAP receives the LBU, it first sends the registration request to the GMAP. Upon receiving the message, the GMAP binds the reservation to the pre-configured RSVP tunnel. Then, by sending the Session_Trigger object piggy-backed in the RSVP message, it asks LMAP to place the reservation for the MN. $t_{interLM}$ and $t_{innerLM}$ can be given as:

$$\begin{aligned} t_{innerLM} &= [M(LBU) + max(M(LBA), M(Path)) + M(Resv)]_{mn-lmap} \\ t_{interLM} &= t_{innerLM} + [M(BU) + max(M(BA), M(Path))]_{lmap-gmap} \end{aligned} \tag{3.32}$$

Finally, for inter-GMAP handover the resource reservation latency can be expressed as the delay of an inter-LMAP handover plus the time taken to re-establish the resource reservation between the new GMAP and the CN, assuming there is no aggregated reservation between two end-points (serving GMAP and CN). The delay $t_{interGM}$ can be derived as follows:

$$t_{interGM} = t_{interLM} + [M(BU) + max(M(BA), m(Path)) + m(Resv)]_{gmap-CN} \tag{3.33}$$

3.4 Simulation Model

This section describes the network-level simulation scenario, and the metrics used to evaluate the performance of the proposed scheme as compared to the baseline protocol, RSVP-MP. The simulation scenario is set up on NS-2.33 patched with the RSVP and HMIPv6 extensions [78, 79], as well as the implementation of the proposed scheme and baseline protocol. Route Optimization is also implemented to avoid triangular routing problem. The queuing mechanism is based on the Weighted Fair Queuing (WFQ) discipline [80]. The upper bound on the number of hops through which the packet can pass varies within the certain range defined by the Time To Live (TTL) field in IP header [81]. Finally, the proposed model assumes a well behaved MN movement pattern, in which the MN moves linearly from one access router to another at a constant speed of 1 meter/s [82]. The simulation topology and its parameters are depicted in Figure 3.7, and Table 3.2. Link characteristics, namely the bandwidth (Megabits/s) and delay (milliseconds), are shown beside each link. The topology used here shows a typical Mobile IP and its extensions deployment configuration, which have been used extensively by various research in recent years [50, 82–84].

Table 3.2: Values of parameters used in the simulation

Parameter	**Value**
One hop wired link delay	2 ms
Bandwidth and Delay between GMAP-HA	10 Mbps, 18 ms
Bandwidth and Delay between GMAP-LMAP	1 Mbps, 10 ms
Bandwidth and Delay between LMAP-AR	1 Mbps, 2 ms
MN speed	1 meter/s
Frequency channel	2.437 GHz
Mobility Type	Random Walk
Propagation Model	Free Space

The simulation scenario is made up of three MNs, three CNs, a HA, a GMAP, four LMAPs and towel Access Routers (ARs). It is of interest to note that the GMAP and LMAPs are considered as a MAP and regular routing nodes in the

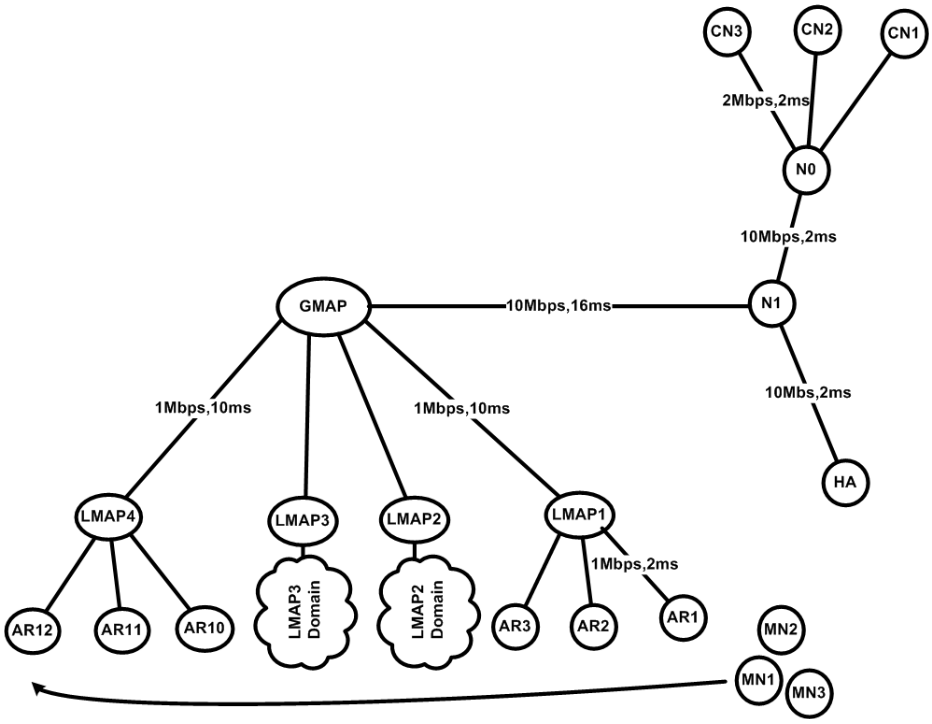


Figure 3.7: Simulation topology

RSVP-MP scenario, respectively. The topology used here reflects the set-up of an open space local environment where the MN is located, and connected to its home network via anonymous networks. It is also important to point out that the location of LMAPs are intentionally selected to be close to the MNs. This lets us to analysis the performance of the proposed scheme in the worse case scenario, wherein the LMAP domain is small. This lead to more numbers of handover to be between LMAP domains. The link between the GMAP and a dummy node N1 models the Internet backbone connection, and simulates the distance home network in the scenario (macro mobility). Below the GMAP is considered as a regional network (micro mobility). The GMAP is connected to four LMAP nodes with 10 ms, 1 Mbps links. These links make bottlenecks for flows. Each LMAP is connected to three ARs, responsible for serving MNs entering their domain. All ARs are using 802.11b in their MAC layer, and their effective coverage area is set to 40 meters in radius. The distance between each two ARs is set to 70 meters with the free space environment in between. The assumption is made to reduce the complexity of the result analysis. The MN reserves the resources in the network at the beginning of the simulation, before receiving traffic from the CN1. The NS-2 traffic source attached to the CN1 generates the constant bit rate UDP stream with a packet size of 500 bytes, and a rate of 450 Kbps which is the maximum average sending rate of Skype Video [85].

The background traffic in the network is emulated by having two best-effort traffic streams between CNs (CN2 and CN3) and two other MNs (MN2 and MN3). All three MNs are moving with the same speed toward the same direction. Each of these flows consist of the constant bit rate UDP traffic with a packet size of 500 bytes, and the rates of 150Kbps and 400Kbps used to simulate the middle and highly-loaded networks, respectively. Considering the MN1 and the background traffic, it can be noticed that the links inside the regional network are approximately 75% and 125% loaded representing the middle-loaded and highly-loaded networks. All three MNs belong to the same HA and move at the same average speed. The layer-2 handover latency and address configuration latency are set to 20 ms and 100 ms, respectively. Simulation is run for 800 seconds. During this time all three MNs perform twelve handovers inside the GMAP domain.

3.5 Performance Investigations

This section evaluates the performance of the proposed scheme by means of the analytical framework and simulation scenario, introduced earlier in Section 3.3 and 3.4 of this chapter. In mobile access networks, QoS may be defined by signalling overhead, resource re-establishment latency, packet loss, and number of packets treated as a best-effort [86–88]. Analysis of these metrics is very useful to evaluate the performance of the proposed scheme in mobile networks.

3.5.1 Analytical Metrics and Results

This section presents the numerical results of the comparison between the proposed scheme and RSVP-MP, with regard to quantitative aspects such as a signalling overhead and resource re-establishment latency. Most of the parameters

used here are the ones used in the previous work [75, 86, 89] and are as follows: $\eta = 4, \alpha = 0.2, \beta = 0.8, \theta_{ha} = 20, K = 5, K' = 3, D_{lmap-mn} = 2, D_{lmap-gmap} = 5, D_{mn-gmap} = 7, D_{mn-cn/ha} = 16, D_{cn-ha} = 6$ and $\zeta = 5$. Similar to the simulation scenario, the LMAP location is considered to be very close to the MN ($D_{lmap-mn} = 2$), making it possible to analysis the performance of the scheme in the worse case situation (having high number of inter-LMAP handover). The topology is consist of 61 cells (ARs), four LMAPs and one GMAPs.
The session arrival rate λ_c is set to 0.1, with the Exponential distribution. The number of packets per session E(S) is set to 10. The binding lifetime is 20 minutes. The RSVP tunnel refresh interval is considered to be three times more than the default value. The average cell residence time is 3 seconds. The BU processing cost in different nodes are defined as follows: $PC_{lmap} = 10$, $PC_{map/gmap} = 12$, $PC_{ha} = 24$ and $PC_{cn} = 4$. For demonstration purpose, γ is set to 1, resulting in the Exponential distribution for the MN's cell residence time with a mean and variance of $\frac{1}{\lambda_m}$ and $\frac{1}{\lambda_m^2}$ [90].

Total Cost Comparison

The total signalling cost induced by the mobility management, resource reservation and packet delivery, based on Equation 3.15, is depicted in Figure 3.8. The RSVP refresh overhead between the GMAP/MAP and CN is the same for both protocols and does not have an effect on the signalling load inside the domain, therefore, it is not considered in the results. As shown in the figure, for the small number of MNs the signalling cost of both protocols are close. However, as the number of MNs rises the noticeable difference grows, indicating the superiority of the proposed scheme by having up to 17% less signalling cost as compared to RSVP-MP. The less overhead comes from localising the MN's mobility and reservation managements inside the LMAP domain resulting in a significant reduce in the distance travelled by messages. Moreover, having a pre-configured RSVP tunnel shared between all MNs inside a LMAP domain can reduce the number of RSVP messages required to establish end-to-end reservations inside the GMAP domain.
Although the proposed scheme can achieve total cost reduction, by having less

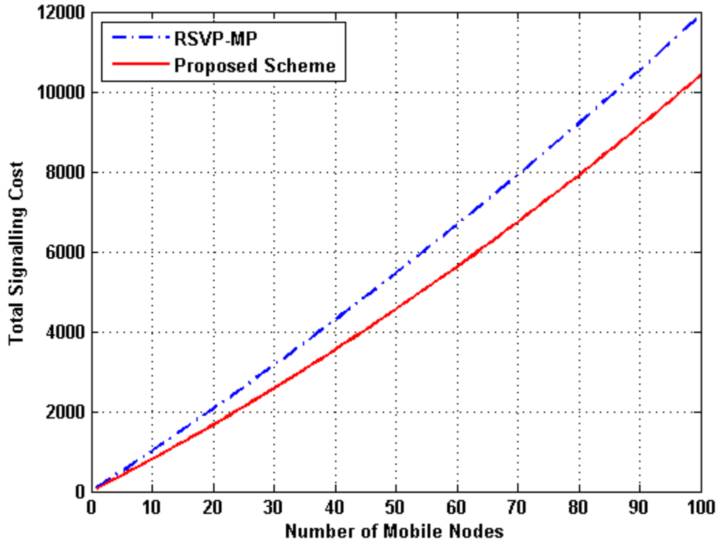


Figure 3.8: Total signalling cost as a function of number of MNs

mobility management and resource reservation signalling costs as compared to the ones in the baseline, it has a higher cost per packet delivery. Figure 3.9 shows the packet delivery cost as a function of average packet arrival rate (packet per second) for one MN. The results are obtained from Equation 5.11. As expected, the packet delivery cost increases linearly as the number of arrival packets in unit time increases. The proposed scheme higher cost, as shown in the figure, comes from having an additional mobility agent along the path, due to the two tier architecture of the propose scheme. After being processed by the GMAP, the packets are then tunnelled to the LMAP where the same process but in a smaller scale, finding the current location of the MN in the binding table (table lookup cost) and routing of the packet towards a serving access router (routing cost), should be conducted. This results in an increase in the packet delivery of the new scheme by an average of 8%. To mitigate this impact, it is possible to minimise the lookup latency in the binding table using efficient search algorithms.

Impact of SMR on Signalling Cost

The impact of the SMR on the location update and resource reservation signalling costs inside the MAP/GMAP domain, is shown in Figure 3.10. The small value

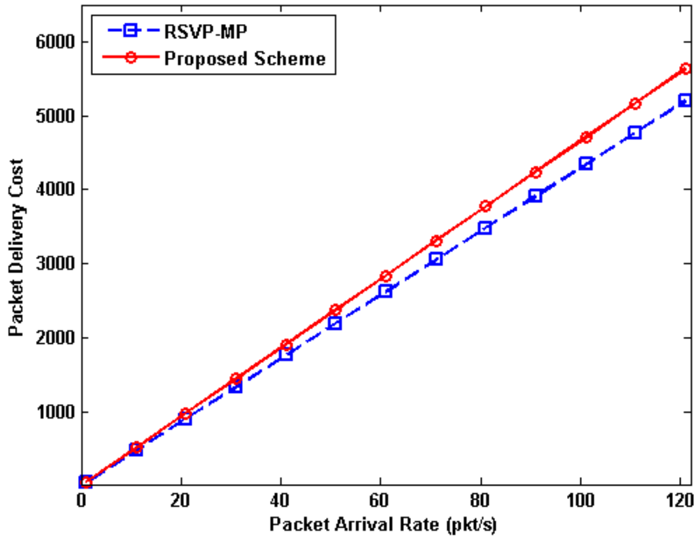
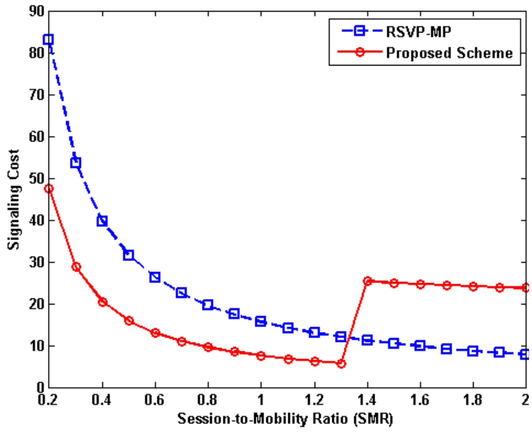
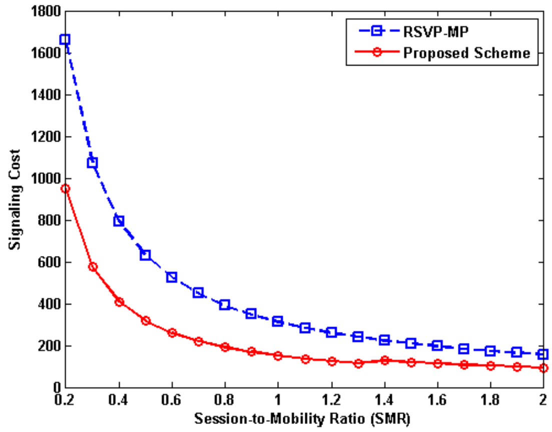


Figure 3.9: Packet delivery cost as a function of packet arrival rate

of the SMR indicates that the MN's mobility rate is higher than its session arrival rate. Consequently, the MN changes its point of attachment more frequently, resulting in the high signalling cost caused by the mobility update and resource reestablishment after each handover. On the other hand, the large value of the SMR implies the low mobility rate, leading to an increase in the MN's cell residence time. Therefore, less handover is performed, and less signalling messages are exchanged. As can be seen from Figure 3.10(a), the proposed scheme signalling cost is considerably lower than the one in RSVP-MP. However, the cost rises abruptly when the SMR value passes the point 1.4, making the proposed scheme signalling cost significantly higher. The reason is that as the SMR goes up, due to the low mobility rate, the MN's cell residence time and intuitively the MN's LMAP residence time increase. At SMR=1.4, the MN's residence time in the LMAP domain increases so much so that an extra cost is imposed by the RSVP tunnel refreshing process, resulting in a sharp rise in the signalling cost. However, the impact can be mitigated by having more number of MNs located in the LMAP domain.
Figure 3.10(b) shows the impact of the SMR on the signalling cost for the large number of MNs, 20. As shown in the figure, there is a steady reduction on the proposed scheme signalling cost over all values of the SMR. Similar to Figure



(a) One MN



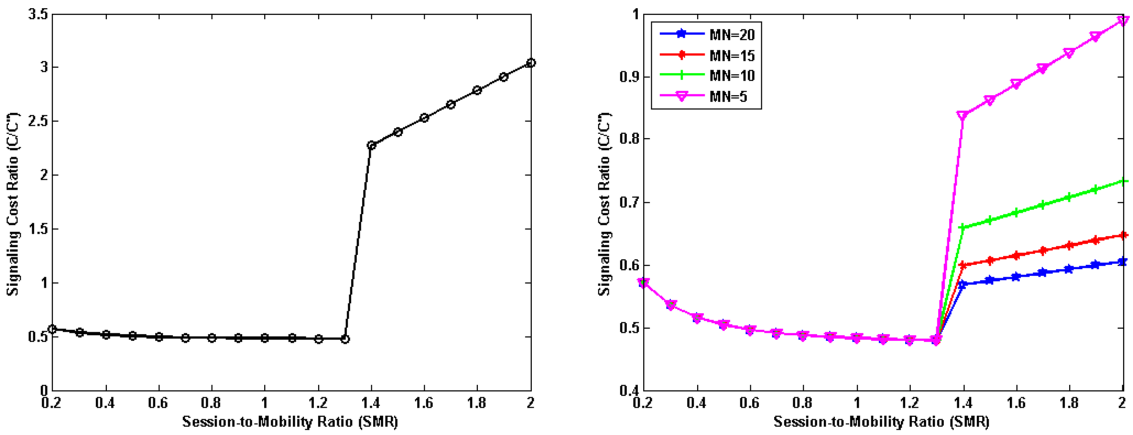
(b) 20 MNs

Figure 3.10: Signalling cost as a function of SMR

3.10(a) when the MNs' residence time in the LMAP increases (SMR $\geq$ 1.4), an extra RSVP tunnel refresh overhead is added to the cost. Nevertheless, being independent of the number of MNs alleviates its burden on the total cost, making its impact insignificant as compared to the large amount of overhead reduction accomplished.

The impact of an increase in the number of MNs can be seen more clearly in Figure 3.11 wherein the ratio of the proposed scheme signalling cost C to the RSVP-MP signalling cost C'', is presented. The RSVP tunnel refresh cost imposes significant overhead on the new scheme. However, having as less as five MNs who are in the same LMAP domain sharing an RSVP tunnel can alleviate the impact of this cost, keeping the ratio below one. As shown in Figure 3.11(b), the amount of improvement is proportional to the number of MNs in the LMAP domain. The higher the number of MNs, the better the gain of the proposed scheme.

The breakdown of the new scheme total signalling cost, including location update and resource re-establishment costs, as a function of SMR on a larger scale, is shown in Figure 3.12(a) and (b). While the former depicts the cost of each, the latter presents the ratio of each cost to its correspondent in the baseline protocol. The number of MNs is assumed to be 20. As seen in Figure 3.12(a) there is a rapid increase at SMR=4 in the new scheme mobility management cost, making



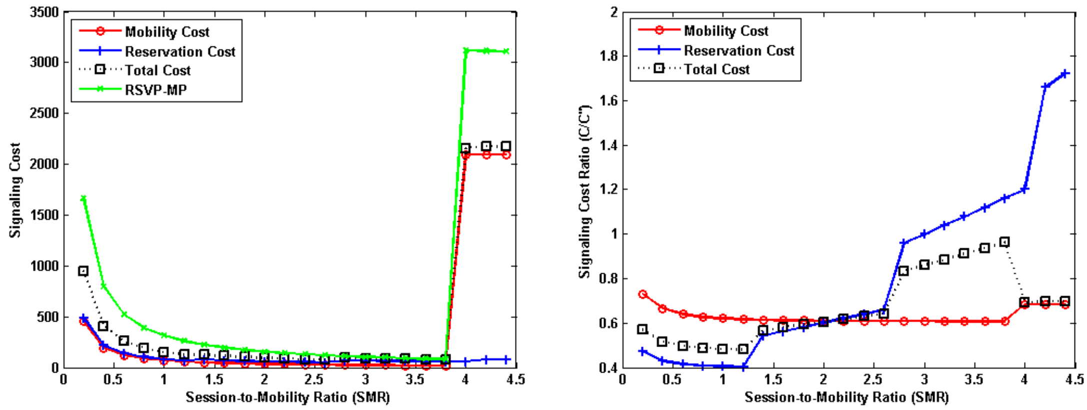
(a) 1 MN

(b) More than one MN

Figure 3.11: Signalling cost ratio as a function of SMR

a direct impact on the total cost. This is caused by an extra signalling messages sent to refresh the binding cash in the MN's home agent and CNs, which causes a significant increase in the total cost of both protocols.

The more detailed behaviour of each cost can be seen in Figure 3.12(b). While the cost ratio of location update decreases almost smoothly (except for an increase caused by the refresh signalling messages), the cost ratio of resource reservation suffers from periodic changes, imposed by the RSVP tunnel refresh cost. Although the cost can be mitigated by selecting a longer refresh period time, the global binding refresh signalling cost imposed at SMR=4 is much higher than the local RSVP-tunnel refresh signalling cost, and therefore, making it a dominant factor in the total signalling cost ratio. On the other hand, although both protocols suffer from an extra cost of sending the global binding refresh messages, the effect is less significant for the proposed scheme. The reason the new scheme has a lower refresh cost is that, unlike RSVP-MP, the origin of the refresh massages is the serving LMAP, and not the MN. This causes significant reduction in the transmission cost, guaranteeing the superiority of the new scheme in spite of larger reservation signalling cost.

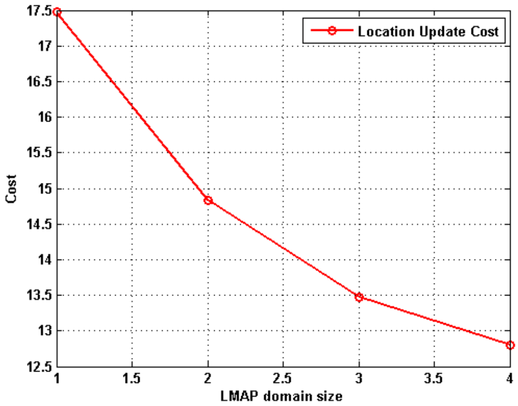


(a) Individual Cost (b) Cost Ratio

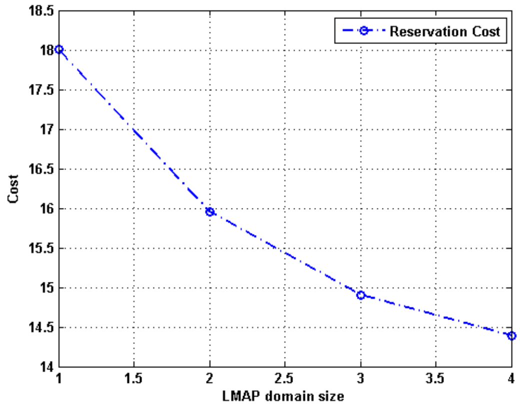
Figure 3.12: Signalling cost breakdown as a function of SMR

Impact of LMAP Size on Total Cost

The impact of the LMAP domain size, defined by the number of rings in a domain, on the total cost and its components are depicted in Figure 3.13(a)–(d). The number of MNs is set to one. As shown by the figure, increasing the number of rings results in a decrease of the location update and resource reservation costs, but an increase in the packet delivery cost. The reason they decrease is that according to Equation 3.9, the domain size is proportional to the number of rings it has. By increasing the number of rings, an MN located in a bigger LMAP domain is less likely to perform the inter-LMAP handover. Consequently, the more number of handovers can be managed locally by the serving LMAP, with no need of sending the mobility management and reservation signalling messages up to the GMAP. This results in a decrease of the location update and reservation overheads. However, this is not the case for the packet delivery cost. In general, as explained in Section 3.3.2.3, the number of cells/access routers is proportional to the number of rings in a domain. When the domain size grows, the number of access routers in the LMAP domain increases. Consequently, the size of routing tables increases, resulting in a higher routing cost for each packet.

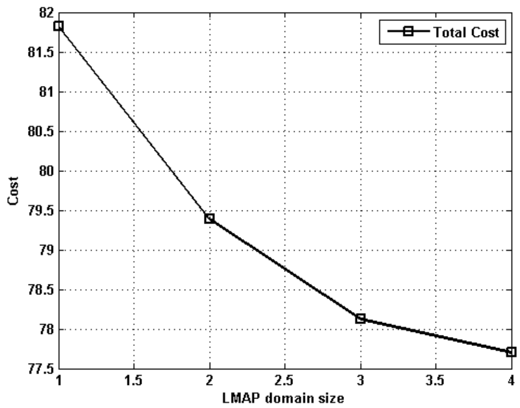


(a) Location Update Cost



(b) Resource Reservation Cost

(c) Packet Delivery Cost



(d) Total Cost

Figure 3.13: Impact of LMAP size on the costs

Impact of q' on Signalling Cost

Under the design assumptions, increasing the domain size leads to the more localised signalling management in the LMAP domain, resulting in a noticeable reduction of signalling overhead. Nevertheless, there might be exceptional situations in which the probability of performing inter-LMAP handover q' becomes higher than the inner-LMAP one, $1 - q'$. Since any increase in q' has a direct impact on the signalling overhead, it is of interest to study the effect of its change on the total signalling cost. To that end, Figure 3.14 shows the comparison of the RSVP-MP total cost and the new scheme with different values for q', as a function of cell residence time. Number of MNs is set to 20.

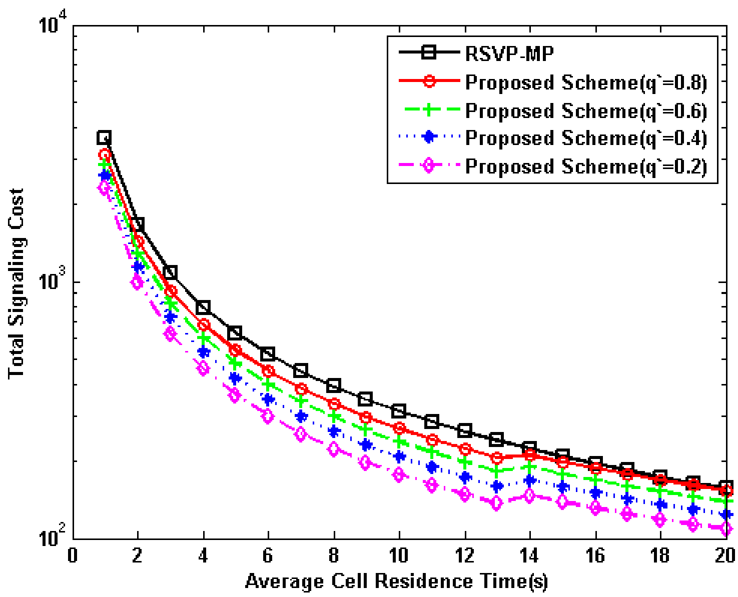


Figure 3.14: Impact of q' on signalling cost as a function of cell residence time

As shown in the figure, the higher the probability of performing inter-LMAP handover, the lower the amount of reduction of the new scheme signalling overhead. However, it is interesting to see that even when the high number of handovers is assumed to be the inter-LMAP ones, the new scheme still outperforms the baseline protocol. The inter-LMAP handover in the proposed scheme is the same as the inner-MAP handover in RSVP-MP, but with an extra cost in LMAP for each handover. When q' is very high (e.g, $q' = 0.8$), the cost of location update in the new scheme exceeds the one in RSVP-MP. On the other hand, while in RSVP-MP an end-to-end RSVP signalling propagation after each handover seems inevitable, having a preconfigured RSVP tunnel in some part of an end-to-end path results in a noticeable reduction in the reservation signalling cost of the new scheme. Interestingly, not only does this reduction cancel out the negative effect of the extra location update overhead, but it causes an average of 10% improvement in the total cost.

Resource Re-establishment Latency

One of the important metrics to assess the performance of the new scheme is the resource re-establishment latency, occurring after each handover. In order to compute this time, defined as the time the MN starts its handover till a new end-to-end RSVP session is established between the MN and MAP/GMAP, the following parameters are defined: The wired and wireless link bandwidth are set to 1Mbps and 2Mbps. The wireless link failure probability q_f is 0.2. The wired link propagation delay L_w is set to 2 milliseconds (ms). The L2 handover delay and the address configuration delay are set to 20ms and 100ms, respectively [82]. The mobility and RSVP control message size are 96 bytes and 140 bytes. The values assigned are in compliance with the ones used in the simulation scenario, making it possible to have a fair comparison of the result obtained here, and the one obtained by means of simulation, discussed in the next section.

Figure 3.15 shows the impact of the wireless link propagation delay on the resource re-establishment latency, for the different values of q'. As expected, the latency of both protocols increase linearly as the the wireless link delay increases. Exploiting the pre-configured RSVP sessions and localised signalling management, the reservation on a new path can be placed by an average of 14% faster in the proposed scheme, when $q' = 0.3$, as compared to RSVP-MP. However, as the more inter-LMAP handover occurs, the gain obtained by the new scheme falls off, reaching up to an average of 8% for $q' = 0.8$. The reason the gain drops is that each inter-LMP handover imposes an extra delay, caused by the time taken to map a new request to an RSVP-tunnel between the GMAP and a new serving LMAP.

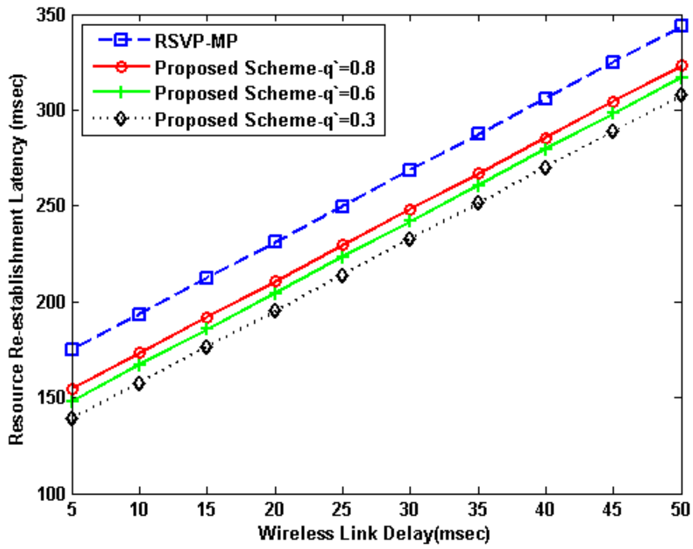


Figure 3.15: RSVp-based resource re-establishment latency as a function of wireless link delay

Assume that almost one-third of all MN's handovers are the inter-LMAP handover, i.e., $q' = 0.3$, for the small values of wireless link propagation delay (less than 10ms) the proposed scheme reduces the resource re-establishment latency by up to 21%. This result will be validated by means of simulation in the next section.

3.5.2 Simulation Metrics and Results

The comparison between the performance of the proposed scheme and RSVP-MP, by means of the network-level simulation scenario, is conducted in this section. The metrics assessed include: the average resource reservation latency, the average number of dropped packets per handover, and the average number of best-effort packets per handover. The evaluation is based on the simulation of a scenario depicted in Figure 3.7, and assumptions made in Section 3.4. The simulation was run for 100 times and the average values are used in the graphs.

Resource Reservation Latency

Figure 3.16 shows the average resource reservation latency in the proposed scheme and RSVP-MP, as a function of traffic load in the network.

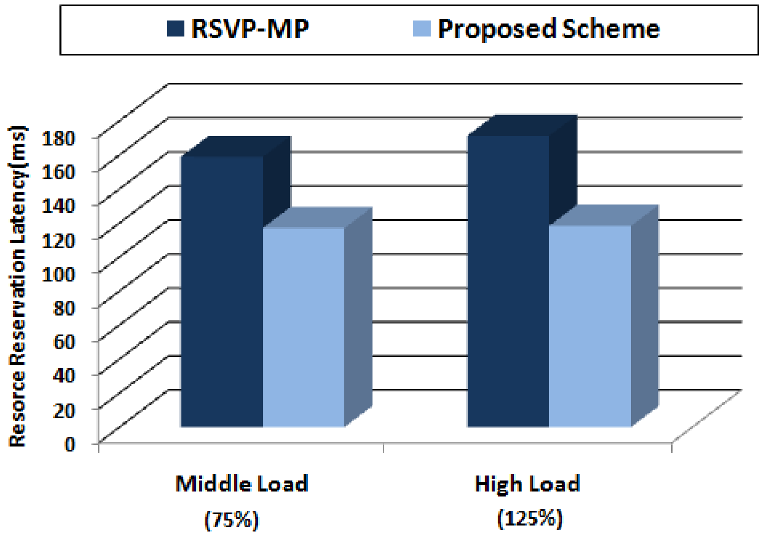


Figure 3.16: Average resource reservation latency after handover(simulation-based)

The results obtained show that the proposed scheme reduces the resource reservation latency by an average of 26% and 31%, in the middle-loaded and highly-loaded networks, as compared to the ones in RSVP-MP. The significant reduction in the reservation set-up time in the proposed scheme comes from having the pre-configured RSVP tunnel between the GMAP and LMAP. Therefore, an end-to-end reservation re-establishment after each handover is just confined to the last part of the network, between the MN and a new serving LMAP. Contrary to the proposed scheme, in RSVP-MP the RSVP signalling messages should travel between the MN and MAP after each handover, even if there is a common part between old and new paths.

Considering the fact that one-third of the handovers are the inter-LMAP one, it is of interest to note that the 26% reduction in the middle-loaded network is very close to the 21% obtained by means of analytical modelling, for the small values of wireless link propagation delay (See Section 3.5.1).

Number of Best-Effort Packets

At the time of handover, if the intermediate nodes on a new path have not been informed about a flow's requirements, the packets cannot receive better than best-effort delivery. This results in an interruption of the acceptable level of QoS required by the flow, and jeopardising its application-level performance. Such QoS interruption must be minimised. A good metric for this performance is the number of packets that may potentially get served with the default QoS at the time of handover [87]. To avoid any kind of violation in QoS, the number of such packets should be kept minimised.

Figure 3.17 shows an average number of best-effort packets, defined as the ones transmitted by the GMAP/MAP after being informed about the MN's new location till an end-to-end reservation is placed along a new path. As shown in the

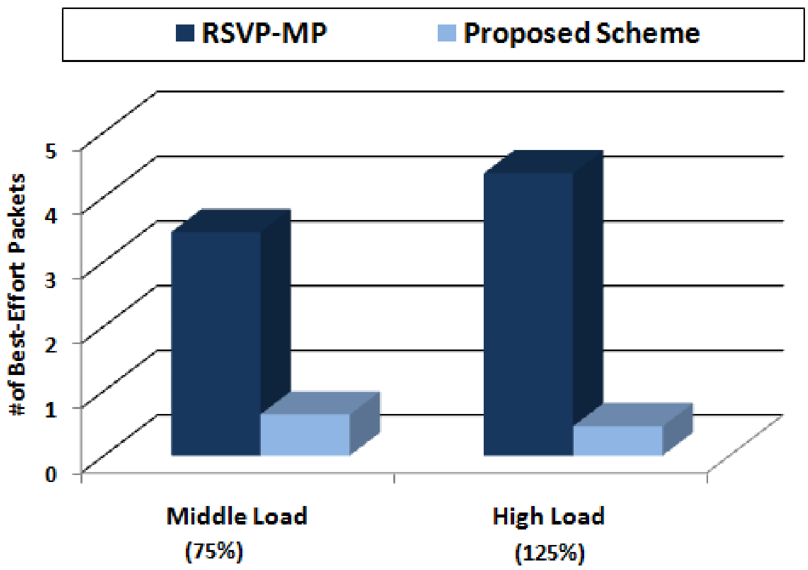


Figure 3.17: Average number of best-effort packet sent after handover

figure, the proposed scheme can achieve an average of 81% and 89% reduction in the number of packets treated as a best-effort, in the middle-loaded and highly-loaded networks, as compared to the ones in RSVP-MP. This is due to the fact

that when the LMAP receives a LBU from the MN, it sends a new *Path* message, straightforward after sending the LBA, towards the MN. Upon receiving the *Path*, a *Resv* message is sent by the MN destined to the LMAP. The end-to-end reservation in the regional network is completed when the LMAP receives the *Resv* message. However, in RSVP-MP this is a duty of the MAP to trigger the reservation signalling by sending the *Path* message.
Considering the longer distance between the MAP and MN, as compared to the distance between the LMAP and MN in the new scheme, completing the end-to-end reservation takes longer time in RSVP-MP, and therefore, results in a significant increase in the number of best-effort packets.

Number of Dropped Packets

The average number of dropped packets during a handover is defined as the number of packets dropped from the time that the MN loses its connectivity with an old access router till the time the resource reservation is established along a new path. Therefore, the total number of dropped packets includes the packets dropped during the handover in addition to the ones dropped by the nodes along the path, due to congestion. Figure 3.18 shows the average number of dropped packets during a handover in both scenarios. The result shows that the proposed scheme can reduce the number of dropped packets by an average of 12% and 43% as compared to RSVP-MP in the middle-loaded and highly-loaded network, respectively. The better achievement comes from the fact that in the proposed scheme most of the MN's handovers are the inner-LMAP type where the MN only needs to register its new LCoA with a serving LMAP. Since the LMAPs are considerably closer to the MN as compared to the MAP in RSVP-MP, the handover delay is reduced in the proposed scheme, resulting in a less number of dropped packets.
The results obtained from Figure 3.18 also shows that the difference between the number of dropped packets of the proposed scheme and RSVP-MP increases as the load in the network increases, implying that the proposed scheme is less load-sensitive than RSVP-MP.

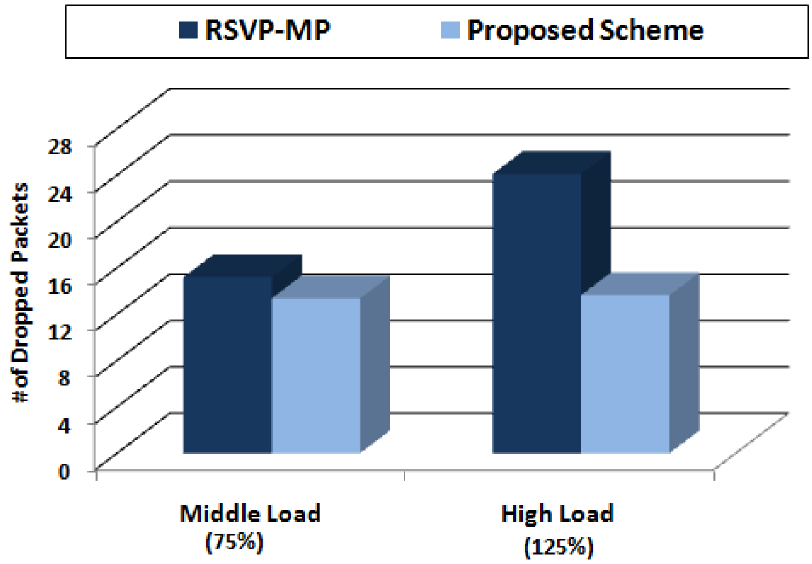


Figure 3.18: Average number of dropped packet during handover

3.6 Summary

In an effort to support an efficient QoS-enabled mobility with the minimum changes in existing protocols, the chapter proposed a new scheme to tackle RSVP problems in mobile networks, the resource re-establishment latency and signalling overhead. The comprehensive analytical framework was developed to analyse the performance of the proposed scheme as compared to RSVP-MP. Through a developed analytical framework, the performance of the new scheme is investigated thoroughly, with the focus on the various figures of merit such as resource re-establishment latency, network-layer signalling cost and effect of the number of mobile nodes and their average cell residence time on it, are used to measure the efficiency of the new scheme. Numerical results obtained showed an average of 17% and 14% improvements of the signalling cost and resource re-establishment latency in the proposed scheme over the baseline protocol.
A part from the analytical framework, the network-level simulation scenario was implemented in NS-2, used to evaluate the performance of the new scheme with regard to the resource re-establishment latency. The obtained results indicated that the proposed scheme can reduce the resource re-establishment latency by

an average of 26% and 31% as compared to RSVP-MP in the middle-loaded and highly-loaded networks, respectively. The value obtained for the middle-loaded network was very close to the 21% reduction achieved through the analytical model. Although the main purpose of the simulation was to validate the analytical result, it was used to evaluate other QoS performance metrics, such as the number of packets treated as a best-effort and number of dropped packets. Exploiting the fast reservation set-up in the proposed scheme causes an average of 81% and 89% reductions in the number of packets treated as a best-effort in the middle and highly-loaded networks. With regard to the number of dropped packets during handover, the proposed scheme can have an average of 12% and 43% reductions as compared to RSVP-MP in the middle and highly-loaded network, respectively. The results obtained by means of analytical model and network-level simulation clearly indicate the superiority of the proposed scheme to the RSVP-MP operation in mobile networks, improving the efficiency of the RSVP operation by reducing the signalling overhead, resource re-establishment latency, number of dropped packets, and number of packets treated as a best-effort.

Chapter 4

An Efficient NSIS-Based QoS in Access Networks

4.1 Introduction

MMoving towards new generations of mobile networks, multimedia services have become the most significant applications among users. A new generation of these services is considered as a solution to create new revenue streams for the subscriber-saturated mobile networks. What is certain is that success cannot be achieved unless the quality of service meets the users' expectations.

In an effort to support resource reservation signalling, IETF introduced the NSIS suite as a generic framework. NSIS can support both the sender- and receiver-oriented reservation models. However, in both scenarios only a flow sender can trigger the NSLP signalling in a downstream direction. Figure 4.1 shows the signalling exchange of each mode.

If an MN, as the sender of the flow, moves to a new cell, it can easily initiate signalling messages downstream towards a CN. However, having the MN as the receiver raises a concern. The reason it does is that the receiver cannot trigger the NSLP messages in the upstream direction. The use of an external mechanism seems inevitable to inform the CN about the MN's handover, and the necessity of having new signalling states along a new path. While the NSIS suffers from the long state set-up latency and signalling overhead, the lack of an internal

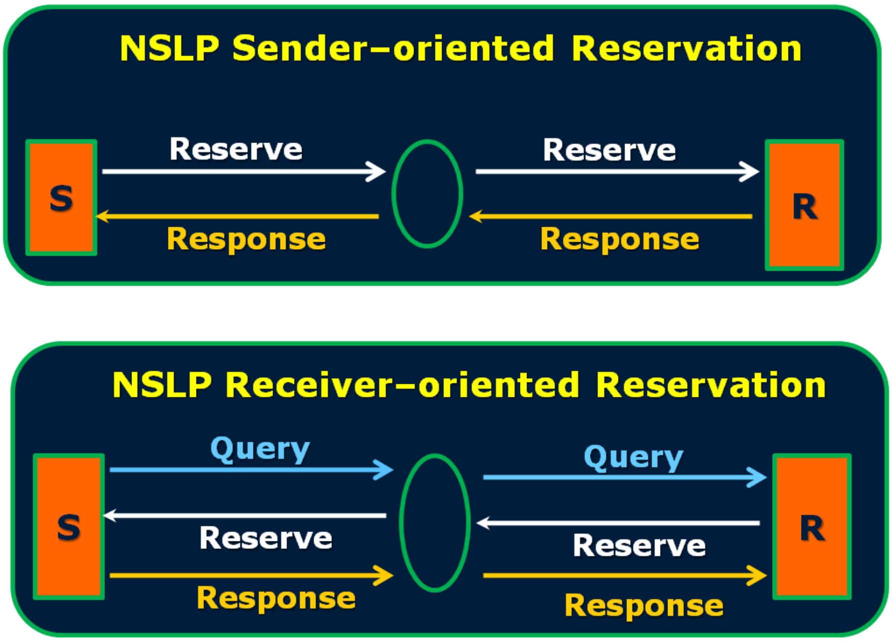


Figure 4.1: NSIS Signalling Exchange

mechanism to detect the MN's handover causes an extra burden on its operation in mobile networks.

In this chapter, the applicability of using the proposed scheme described in Chapter 3, to tackle the NSIS problems in mobile environments is discussed and, evaluated. The results obtained, by means of analytical model, show that the scheme can improve the efficiency of NSIS not only by reducing the amount of signalling overhead caused after each handover, but by expediting the resource re-establishment on a new path. Since the NSIS protocol is not supported in NS-2, the simulation experience is not conducted in this chapter.

The remainder of this chapter is organised as follows: In Section 4.2 the architecture of the proposed scheme is studied in detail. Section 4.3 elaborates the signalling cost and resource re-establishment latency. Section 4.4 discusses the numerical results obtained by means of the analytical model. Finally, Section 4.5 brings closure to this chapter.

4.2 System Model

This section describes the architecture and operation of the proposed scheme from two different aspects: the mobility management and resource reservation.

Mobility Management

The mobility protocol selected is based on the network-based localised mobility management, PMIPv6. The proposed scheme can be used in any localised-mobility management protocols. While the applicability of it in HMIPv6 environment was analysed in Chapter 3, in this chapter the proposed scheme effect in PMIPv6 environment is investigated. As explained in detail in Section 2.3.2, the main advantage of PMIP to HMIP (host-based localised mobility management protocol) is that an MN does not participate in IP mobility procedures. That is, network operators can provide mobility support without requiring additional software and complex security configuration in the mobile users. Therefore, the deployment of network-based mobility solutions is greatly facilitated.
PMIP architecture consists of LMA, usually located at the gateway of the network, and the MAGs. Using the the proposed scheme in a PMIPv6 environment, the one layer LMA architecture is extended to two: G-LMA and L-LMA. The G-LMA is located at the gateway of the regional network while the L-LMAs are located between the G-LMA and MNs, dividing the regional network to M sub-regional domains (M is the number of L-LMAs). Each MAG in the G-LMA domain associates with at least one L-LMA.
When the MN attaches to an access link, the MAG detects its movement, it then acquires the MN's identity, and determines whether the MN is authorised to use the service. For the authorised MN, the MAG sends a PBU to a serving L-LMA. When the L-LMA receives the message, it checks its binding cache table of any records about the MN's old MAG. If there is a record, it accepts the PBU and sends a PBA, including the MN's Home Network Prefix (HNP), to the MAG. The scenario is called inner L-LMA handover in which the MN's current location is only updated in the L-LMA, making all MN's movements inside the L-LMA domain transparent to the G-LMA.
However, if there are no records of the MN's previous location, the L-LMA creates

a binding cache entry for the MN and sends the registration request to the G-LMA, asking for MN's HNP. The G-LMA accepts the registration by sending a PBA and keeps the L-LMA address for next destination for any packets destined to the MN. When the L-LMA receives the PBA including the MN's HNP, it forwards it to the MAG. Upon receipt of the PBA, the router advertisement is sent by the MAG to the MN advertising the MN's HNP. At this stage, a bi-directional tunnel is established between the G-LMA and L-LMA , as well as the L-LMA and the MAG in order to convey messages to/from the MN.

Resource Reservation

Based on the proposed mobility architecture, the route between the G-LMA and MN is divided into two parts: from G-LMA to L-LMA and from L-LMA to MN. The former is the common part for all MNs located in the same L-LMA domain. Therefore, instead of having an individual NSIS session for each MN, a pre-configured NSIS session is established between the G-LMA and each L-LMA as a tunnel entry and exit points. When the G-LMA receives the reservation request for the MN, it maps the request to the NSIS tunnel between itself and the MN's serving L-LMA. Then, it passes an NSLP Query message containing the flow information to the L-LMA, asking it to reserve the resources in its domain for this MN. When the L-LMA receives this information, it works as a proxy and initiates a new NSIS session destined to the MN's current location.
To avoid an extra overhead, the mechanism used to pre-allocate resources for each tunnel C_{T} is based on the static threshold-based method in which the maximum amount of resources authorised by administration polices is assigned, $C_{\text{T}} = \psi_{max}$. However, one can use the dynamic threshold-based method where the constant value is assigned to the tunnel and then based on the monitoring and predicting of the future demand the extra chunk of resources B can be added or released from the tunnel. Therefore,
$\psi_{min} \leq C_{\text{T}} = \psi_{min} {}^{+}_{-} Bi \leq \psi_{max}, i = 0, 1, ...$
The resources assigned to these NSIS tunnels can be used by the best-effort traffic if there is no demand for them, and therefore, preventing the wastage of the resource in the NSIS tunnels.

4.3 Total Cost Function

The analytical model used to derive the equations is the one introduced in Section 3.3. It is assumed that in the PMIPv6, the LMA domain consists of K rings (ring 0 to ring K-1), and the MN is initially located in the centre cell.
The performance metrics used to analysis of the proposed scheme include the resource re-establishment latency, and signalling cost induced by the mobility management and resource reservation. Note that in all scenarios, the MN acts as a receiver of the flow since this is the most challenging part of the NSIS operation in mobile networks. Also, it is assumed that there are pre-configured NSIS sessions between the G-LMA and L-LMAs. Therefore, their set-up cost is not taken into account in the analysis, but their maintenance cost is. The total signalling cost includes a location update signalling cost (C_{LU}), a resource reservation signalling cost (C_{RR}), and the packet delivery signalling cost (C_{PD}), respectively:

$$C_{\mathrm{Total}} = C_{\mathrm{LU}} + C_{\mathrm{RR}} + C_{\mathrm{PD}} \tag{4.1}$$

The notations used in all the equations introduced in this section can be found in Table 4.1.

Location Update Cost

In PMIPv6 mobile users can perform two kinds of handover: the inner and inter-domain handovers, described in detail in [7, 91]. The LMA registration process is the same in both types of handover. However, in order to keep the current connection(s) alive after the inter-domain handover, the LMA sends a PBU to the CN(s) and MN's Home LMA informing them about the MN's new regional network. Their addresses can be obtained from the router solicitation sent by the MN, upon entering a new cell, and are passed on by the MAG to the LMA[91]. Apart from registration, the periodic PBU and PBA are exchanged between the peers in order to extend the binding lifetime in the LMA, HA and CN(s). This cost is represented by C_{BR}. Given that C_g and C_l are the signalling cost of the inter-LMA/global and inner-LMA/local binding updates, the location update

Table 4.1: Notation of NSIS-based QoS in access networks

λ_m	the MN's cell crossing rate
λ_c	the MN's session arrival rate
K	number of rings in the LMA/G-LMA domain
K'	number of rings in the L-LMA domain
q	probability of performing the inter LMA/G-LMA handover
$(1-q)$	probability of performing the inner LMA/G-LMA handover
$q'/(1-q')$	probability of performing the inter/inner L-LMA handover
t_m	the MN's average residence time in each cell/MAG domain
$\overline{\tau}_{m'}$	the MN's average residence time in the L-LMA domain
$\overline{\tau}_{ha}$	the MN's average residence time in the LMA/G-LMA domain
T_{rf}	the binding update lifetime in the LMA/G-LMA/L-LMA/HA/CN
η	NSIS message processing cost at each node
T_{rrf}	NSIS message lifetime
TC_{x-y}	transmission cost between nodes x and y$(\delta D_{x-y} + \zeta\delta)$
δ	unit transmission cost in wired link
ζ	weighting factor for the unit transmission cost in wireless link
PC_x	processing cost of control packet at node X
$B_{w/wl}$	bandwidth of wired/wireless link (in bits per second)
$L_{w/wl}$	wired/wireless link propagation delay
q_f	probability of an unsuccessful message delivery on wireless link
T_w	time needed to determine that the message is lost
b	size of the message in bits

cost can be written as follows:

$$C_{\text{LU}} = \lambda_m(qC_{\text{g}} + (1-q)C_{\text{l}}) + C_{\text{BR}} \tag{4.2}$$

where q and *(1-q)* are the probability of performing the inter-LMA and inner-LMA handovers obtained from Equation (3.5). Since the link layer, authentication and address configuration delays are the same in all scenarios; thus, they are omitted in the analysis.The detailed cost of C_g, C_l, and C_{BR} can be expressed as follows:

$$
\begin{aligned}
&C_{\mathrm{l}} = 2\mathrm{TC}_{\mathrm{mag-lma}} + \mathrm{PC}_{\mathrm{mag}} + \mathrm{PC}_{\mathrm{lma}} \\
&C_{\mathrm{g}} = \mathrm{C}_{\mathrm{l}} + 2\mathrm{TC}_{\mathrm{lma-ha}} + \mathrm{PC}_{\mathrm{ha}} + 2\mathrm{TC}_{\mathrm{lma-cn}} + \mathrm{PC}_{\mathrm{cn}} \\
&C_{\mathrm{BR}} = 2(\lfloor \frac{\mathrm{t_m}}{\mathrm{T_{rf}}} \rfloor \mathrm{TC}_{\mathrm{mag-lma}} + \lfloor \frac{\overline{\tau}_{\mathrm{ha}}}{\mathrm{T_{rf}}} \rfloor (\mathrm{TC}_{\mathrm{lma-ha}} + \mathrm{TC}_{\mathrm{lma-cn}}))
\end{aligned}
\tag{4.3}
$$

where $\overline{\tau}_{ha}$ is the MN average residence time in the LMA domain, which can be obtained from Equation 3.14.

In the proposed scheme, the MN can perform three kinds of handover: the inner L-LMA handover, inter L-LMA handover and inter G-LMA handover. In the inner L-LMA handover, the MN moves between two MAGs both belonging to the same L-LMA. The inter L-LMA handover occurs whenever the MN moves from one MAG subnet to another, each belonging to a different L-LMA. In this case, a new serving L-LMA informs G-LMA about the MN's new local domain address. In the inter G-LMA handover,, the MN enters a MAG subnet belonging to a different G-LMA. Here the new G-LMA sends the registration request to the MN's HA/CN. Therefore, the total cost in the proposed scheme can be derived as follows:

$$
C_{LU} = \lambda_m \big(qC_{glma} + (1-q)[q'C_{llma} + (1-q')C_{mag}] \big) + C_{BR} \tag{4.4}
$$

where C_{mag}, C_{llma} and C_{glma} represent the cost of inner L-LMA, inter L-LMA and inter G-LMA handovers, respectively, and are equal to:

$$
\begin{aligned}
&C_{\mathrm{mag}} = 2\mathrm{TC}_{\mathrm{mag-llma}} + \mathrm{PC}_{\mathrm{mag}} + \mathrm{PC}_{\mathrm{llma}} \\
&C_{\mathrm{llma}} = \mathrm{C}_{\mathrm{mag}} + 2\mathrm{TC}_{\mathrm{llma-glma}} + \mathrm{PC}_{\mathrm{llma}} + \mathrm{PC}_{\mathrm{glma}} \\
&C_{\mathrm{glma}} = \mathrm{C}_{\mathrm{llma}} + 2\mathrm{TC}_{\mathrm{glma-ha}} + \mathrm{PC}_{\mathrm{ha}} + 2\mathrm{TC}_{\mathrm{glma-cn}} + \mathrm{PC}_{\mathrm{cn}} \\
&C_{\mathrm{BR}} = 2(\lfloor \frac{t_m}{T_{rf}} \rfloor TC_{\mathrm{mag-llma}} + \lfloor \frac{\overline{\tau}_{m'}}{T_{rf}} \rfloor TC_{\mathrm{llma-glma}} + \lfloor \frac{\overline{\tau}_{ha}}{T_{rf}} \rfloor (TC_{\mathrm{glma-ha}} + TC_{\mathrm{glma-cn}}))
\end{aligned}
\tag{4.5}
$$

Reservation Signalling Cost

In the basic operation of NSIS in PMIPv6 networks, the LMA can act as a proxy dividing an NSIS end-to-end reservation into two parts: the outer part and the inner part. The former is between the LMA and CN, re-established with the cost of R_{g} when the MN performs the inter LMA handover. The latter is between the LMA and MN, wherein MAG acts as an NSIS proxy. This part needs to be re-established, with the cost of R_{l}, when the MN changes its point of attachment inside the LMA domain (inner LMA handover). With these insights, the resource reservation cost can be expressed as follows:

$$C_{\mathrm{RR}} = \lambda_m(qR_{\mathrm{g}} + (1 - q)R_{\mathrm{l}}) + C_{\mathrm{RF}} \tag{4.6}$$

Both R_{l} and R_{g} include the NSLP signalling cost, and the GIST three-way handshake signalling cost in the D-mode represented by C^{nslp} and C^{gist}, respectively. The costs can be written as:

$$\begin{aligned} \mathrm{R_l} &= [\mathrm{C^{nslp}} + \mathrm{C^{gist}}]_{\mathrm{lma-mn}} \\ \mathrm{R_g} &= \mathrm{R_l} + [\mathrm{C^{nslp}} + \mathrm{C^{gist}}]_{\mathrm{lma-cn}} \end{aligned} \tag{4.7}$$

The GIST cost in the D-mode includes the transmission and processing costs of the GIST *Query/Response/Confirm* messages, exchanged between the GIST peers along the path.
Since both NSLP and GIST are the soft state, the refresh messages, the *Reserve* and *Response* for NSLP and the *Query* message for GIST, should be sent periodically, though independently, between the peers. Therefore, the refresh signalling cost C_{RF} in Equation 4.6 is made up of the NSLP and GIST refresh costs, performed with the cost of RF^{nslp} and RF^{gist}. Thus:

$$\begin{aligned} C_{\mathrm{RF}} &= \lfloor \frac{\mathrm{t_m}}{\mathrm{T_{rrf}}} \rfloor [\mathrm{RF^{nslp}} + \mathrm{RF^{gist}}]_{\mathrm{lma-mn}} \\ \mathrm{RF^{nslp}} &= [\mathrm{TC^{Reserve}} + \mathrm{TC^{Response}}]_{\mathrm{x-y}} \\ \mathrm{RF^{gist}} &= [\mathrm{TC^{Query}}]_{\mathrm{x-y}} \end{aligned} \tag{4.8}$$

In the proposed scheme an end-to-end reservation between the CN and MN is divided into three parts. The first part is between the G-LMA and CN, with the cost of R_{glma}. The second part is between the G-LMA and the serving L-LMA, with the cost of R_{llma}. Finally, the last part is between the L-LMA and MN re-established, with the cost of R_{mag}. Exploiting the pre-configured NSIS tunnel between two end points, the second cost (R_{llma}) just comprises of binding an individual reservation to the NSIS tunnel, and informing the L-LMA about the necessity of reserving the resources for the MN in its domain. Therefore, the reservation cost in the new scheme can be written as follows:

$$C_{\mathrm{RR}} = \lambda_{\mathrm{m}}\left[q\mathrm{R}_{\mathrm{glma}} + (1-q)(q'\mathrm{R}_{\mathrm{llma}} + (1-q')\mathrm{R}_{\mathrm{mag}})\right] + \mathrm{C}_{\mathrm{RF}} \tag{4.9}$$

The detailed costs can be expressed as:

$$\begin{aligned}
&\mathrm{R}_{\mathrm{mag}} = [\mathrm{C}^{\mathrm{nslp}} + \mathrm{C}^{\mathrm{gist}}]_{\mathrm{llma-mn}}\\
&\mathrm{R}_{\mathrm{llma}} = \mathrm{R}_{\mathrm{mag}} + [\mathrm{TC}^{\mathrm{Query}} + \eta^{\mathrm{Query}}]_{\mathrm{glma-llma}}\\
&\mathrm{R}_{\mathrm{glma}} = \mathrm{R}_{\mathrm{llma}} + [\mathrm{C}^{\mathrm{nslp}} + \mathrm{C}^{\mathrm{gist}}]_{\mathrm{glma-cn}}\\
&C_{\mathrm{RF}} = \lfloor\frac{\mathrm{t_m}}{\mathrm{T_{rrf}}}\rfloor[\mathrm{RF}^{\mathrm{nslp}} + \mathrm{RF}^{\mathrm{gist}}]_{\mathrm{llma-mn}} + \lfloor\frac{\overline{\tau}_{\mathrm{m'}}}{\mathrm{T_{rrf}}}\rfloor[\mathrm{RF}^{\mathrm{nslp}} + \mathrm{RF}^{\mathrm{gist}}]_{\mathrm{llma-glma}}
\end{aligned} \tag{4.10}$$

The $\mathrm{C}^{\mathrm{nslp}}$ and $\mathrm{C}^{\mathrm{gist}}$ costs used in Equation 4.7 and Equation 4.10 can be written as follows:

$$\begin{aligned}
&\mathrm{C}^{\mathrm{nslp}}_{\mathrm{sender}} = [\mathrm{TC}^{\mathrm{Reserve}} + \mathrm{TC}^{\mathrm{Response}} + (\eta^{\mathrm{Reserve}} + \eta^{\mathrm{Response}})]_{\mathrm{x-y}}\\
&\mathrm{C}^{\mathrm{nslp}}_{\mathrm{receiver}} = [\mathrm{TC}^{\mathrm{Query}} + \mathrm{TC}^{\mathrm{Reserve}} + \mathrm{TC}^{\mathrm{Response}} + (\eta^{\mathrm{Query}} + \eta^{\mathrm{Reserve}} + \eta^{\mathrm{Response}})]_{\mathrm{x-y}}\\
&\mathrm{C}^{\mathrm{gist}} = [\mathrm{TC}^{\mathrm{Query}} + \mathrm{TC}^{\mathrm{Response}} + \mathrm{TC}^{\mathrm{confirm}} + (\eta^{\mathrm{Query}} + \eta^{\mathrm{Response}} + \eta^{\mathrm{Confirm}})]_{\mathrm{x-y}}
\end{aligned} \tag{4.11}$$

Note that according to the type of reservation, the receiver-oriented or the sender-oriented, the cost of NSLP varies.

Packet Delivery Cost

The packet delivery cost is the same as the one derived in Section 3.3.2.3, wherein the MAP, GMAP and LMAP are replaced by LMA, G-LMA and L-LMA,respectively.

Resource Re-establishment Latency

The resource re-establishment latency t_{RL} is defined as a time needed to perform a handover *and* re-establish an end-to-end resource reservation along a new path in the LMA/G-LMA domain. The handover latency comprises of the delays caused by the layer-2 handover and binding update. In the basic operation of NSIS, the receipt of a PBU can be interpreted as the necessity of re-establishing the resource reservation on a new path. Therefore, when the LMA receives this message, it sends a PBA along with a new NSLP message, *Reserve*[*Query*] in the sender[receiver]-oriented reservation, towards the MN. Upon receiving the message, the MN sends a *Response[Reserve]* to the LMA. Therefore, the resource reservation latency for the sender-oriented (t^{S}_{RL}), and receiver-oriented reservation (t^{R}_{RL}) can be written as follows:

$$\begin{aligned}
&t^{S}_{RL} = t_{L2} + \big[\mathrm{M(PBU)+Max(M(PBA),M(RESERVE))+M(RESPONSE)}\big]_{mn-lma} \\
&t^{R}_{RL} = t_{L2} + \big[\mathrm{M(PBU) + Max(M(PBA),M(QUERY))} \\
&+\mathrm{M(RESERVE)+M(RESPONSE)}\big]_{mn-lma}
\end{aligned} \tag{4.12}$$

where $\mathrm{M(X)}$ is the time to send a message X between two nodes, including the transmission time and the propagation time, and is equal to [77] :

$$\begin{aligned}
&\mathrm{M} = \frac{b}{\mathrm{B}_{w/wl}} + \mathrm{L}_{w/wl} \\
&where \\
&\mathrm{M}_{wired} = \mathrm{D}_{x-y} \times \mathrm{M} \\
&\mathrm{M}_{wireless} = \mathrm{M} + (\mathrm{T}_w + \mathrm{M}) \times \frac{q_f}{1-q_f}
\end{aligned} \tag{4.13}$$

The average resource re-establishment latency in the proposed scheme, for the sender- and receiver-oriented reservation, can be calculated as follows:

$$t^{S/R}_{RL} = q' t^{S/R}_{RL_{llma}} + (1-q') t^{S/R}_{RL_{mag}} \tag{4.14}$$

where $t^{\text{S/R}}_{\text{RL}mag}$ and $t^{\text{S/R}}_{\text{RL}llma}$ are the average reservation latency during the inner L-LMA and inter L-LMA handover, respectively. For the inner L-LMA handover, $t^{\text{S/R}}_{\text{RL}mag}$ can be obtained from Equation 4.12, except that here the distance is limited between the MN and serving L-LMA, resulting in a shorter distance for the signalling messages. During the inter L-LMA handover, when the L-LMA receives the PBU, it first sends the registration request to the G-LMA. When the G-LMA receives the message, it binds the reservation to the pre-configured NSIS tunnel. Then by sending the necessary information included in the NSLP *Query* message, it asks L-LMA to initiate the reservation for this MN. The equation for the resource reservation latency during the inter L-LMAP handover $t_{\text{RL}llma}$, for the sender- or receiver-oriented reservation models, can be written as follows:

$$t^{\text{S/R}}_{\text{RL}llma} = t^{\text{S/R}}_{\text{RL}mag} + [\text{M}(\text{PBU}) + \text{MAX}(\text{M}(\text{PBA}),\text{M}(\text{QUERY})]_{\text{glma}-\text{llma}} \tag{4.15}$$

4.4 Performance Investigations

This section presents the numeric comparisons of the signalling cost and resource reservation latency between the proposed scheme and the baseline protocol. The parameters used here are the ones used in [75, 92, 93]. The binding lifetime is 20 minutes. The NSIS refresh interval for the individual and pre-configured tunnel are set to 45 and 135 seconds, respectively. The average cell residence time is 30 seconds. The session arrival rate λ_c is set to 0.1, with the Exponential distribution. The PBU processing cost in different nodes are $\text{PC}_{mag} = 12$, $\text{PC}_{llma} = 18$, $\text{PC}_{lma/glma/ha} = 24$, and $\text{PC}_{cn} = 4$. The other variables are set to: $\delta = 1$, $\zeta = 10$, $\eta_{nslp} = 4$, $\eta_{gist} = 1$, $\text{K} = 5$, $\text{K}' = 3$, $\text{D}_{mag-llma} = 4$, $\text{D}_{mag-lma} = 10$, $\text{D}_{ha-cn} = 6$, $\text{D}_{lma-ha} = 25$ and $\text{D}_{lma-cn} = 8$. For demonstration purposes, γ is set to 1, resulting in the Exponential distribution for the MN's cell residence time with the mean and variance equal to $\frac{1}{\lambda_m}$ and $\frac{1}{\lambda_m^2}$, respectively [90]. Since the resource reservation refresh signalling cost between the LMA/GLMA and CN does not have any effect on the signalling load inside the LMA domain; then, it is not considered in the rest of the analytical analysis.

Figure 4.2 shows the total signalling cost, including the location update, resource reservation signalling costs and a packet delivery cost, as a function of the number of MNs in the PMIP domain. As it can be seen from the figure, in both protocols, the costs of receiver-oriented mode (RO) are higher than the sender-oriented (SO). This is due to the necessity of sending extra NSLP signalling messages between the end-points in this mode. Moreover, the results obtained show that for a small number of MNs the costs of the proposed scheme, in both sender- and receiver-oriented modes, exceed the ones in the baseline protocol.

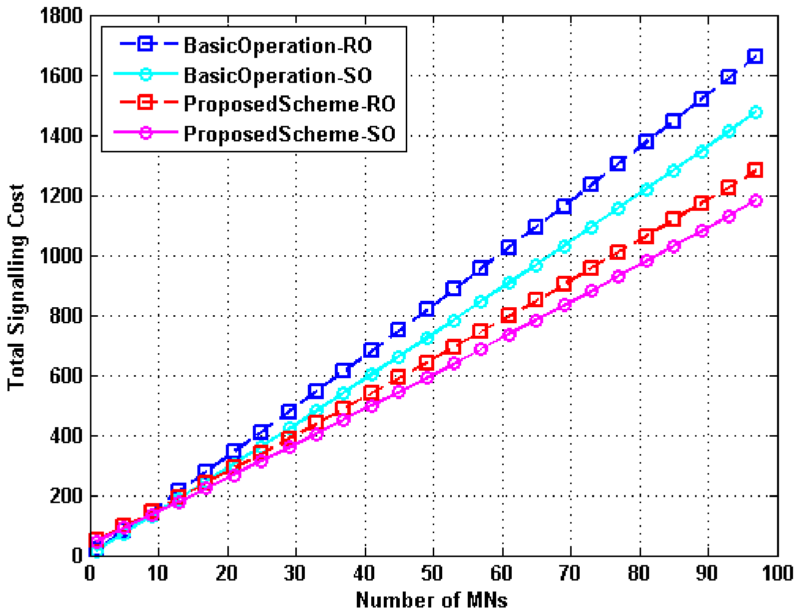
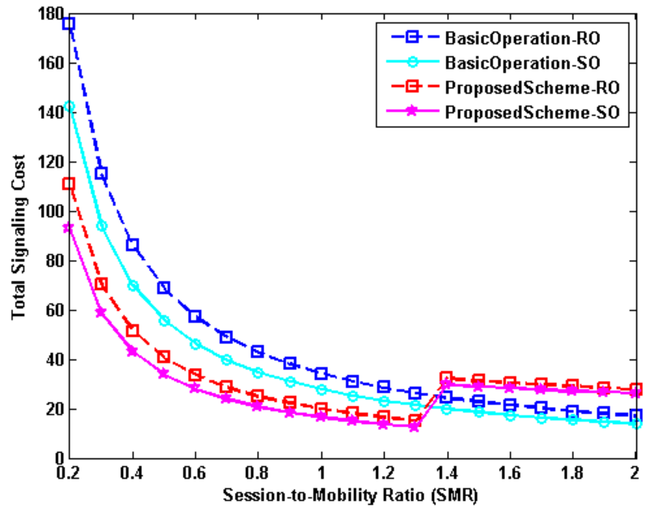


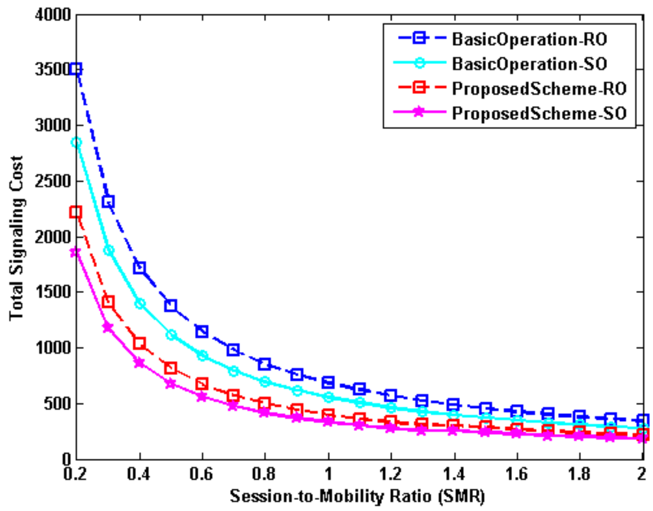
Figure 4.2: Impact of number of MNs on the NSIS-based signalling cost

The higher cost of the proposed scheme comes from the extra signalling cost imposed by refreshing the pre-configured NSIS tunnel. However, as the number of MNs increases, the total costs of the proposed scheme for both the sender- and receiver-oriented decreases. This comes from the fact that the cost of refreshing the NSIS tunnel is independent of the number of MNs in the L-LMA domain. Therefore, by increasing the number of MNs, its burden on the total cost is alleviated. The results show that using the new scheme, the total signalling cost can be reduced by an average of 5% and 10.5%, for the sender-oriented and the receiver-oriented reservation, respectively.

Figure 4.3(a) and Figure 4.3(b) show the impact of SMR on the signalling cost



(a) One MN



(b) 20 MNs

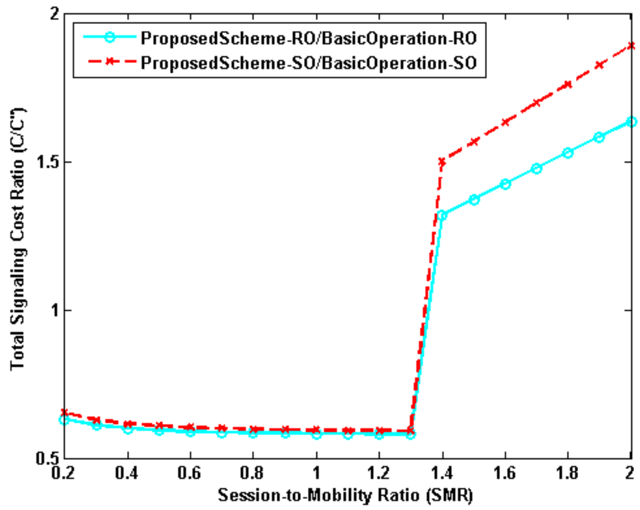
Figure 4.3: Impact of SMR on the NSIS-based signalling cost

for the 1 and 20 MNs. The SMR indicates the MN's session arrival rate to its mobility rate. The small value of the SMR means the MN's mobility rate is higher than the session arrival. Therefore, the MN changes its point of attachment more frequently, resulting in the high signalling cost induced by the mobility update and resource re-establishment after each handover. On the other hand, the large value of the SMR indicates the low mobility rate which results in an increase in the MN's residence time in each cell. Therefore, less handover is performed and less signalling is initiated.

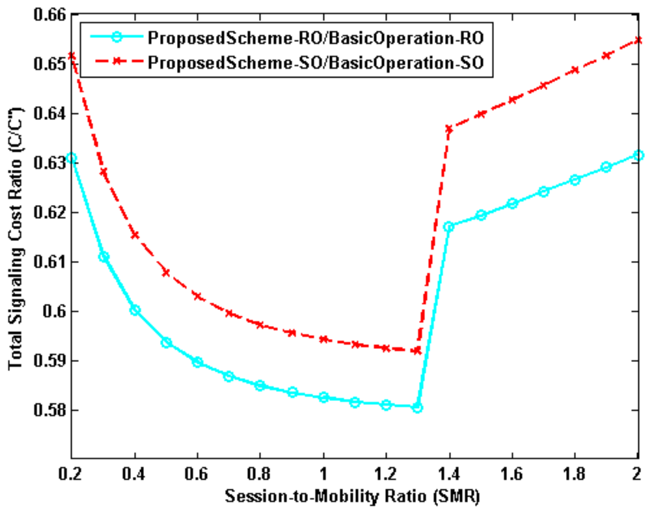
In Figure 4.3(a), the proposed scheme signalling costs for both the sender- and receiver-oriented reservation models are significantly lower than the ones in the baseline. However, when the SMR increases (SMR $\geq$1.4) the costs increase sharply. The reason is as the SMR increases the MN's cell residence time also increases. Intuitively, the MN's residence time in the L-LMA domain increases. When the SMR=1.4, the MN's residence time in the L-LMA domain reaches a point that the extra cost caused by the NSIS tunnel refreshing process is added to the total cost, resulting in a sharp increase in the total cost.

Figure 4.3(b) shows the impact of the SMR on the total signalling cost for the large number of MNs (the number of MNs is set to 20). The results obtained show that for all values of SMR, the proposed scheme shows less signalling cost as compared to the baseline. Unlike Figure 4.3(a), there is no sudden increase in the proposed scheme signalling cost for larger values of SMR. This is due to the fact that when the MNs' residence time in the L-LMA increases (large value of SMR), the extra NSIS tunnel refresh signalling overhead is added to the total cost. However, this cost is independent of the number of MNs, and therefore, having a large number of MNs makes its effect insignificant on the total cost.

The comparison of the total signalling cost between the proposed scheme and baseline can be seen more clearly in Figure 4.4(a) and Figure 4.4(b), wherein the results show the ratio of the proposed scheme signalling cost to the baseline, C and C' respectively. In both figures as the SMR increases the ratio of the proposed scheme signalling cost to the baseline decreases, which indicates more signalling cost reduction in the proposed scheme. The reason is as the SMR increases, the probability of performing the inter L-LMA handover decreases. Therefore, most of the mobility and reservation signalling costs are handled by the L-LMA, which



(a) One MN



(b) 20 MNs

Figure 4.4: The ratio of the NSIS-based signalling costs($\frac{C}{C'}$)

is located closer to the MN as compared to the LMA in the baseline protocol. However, this will not last long. The extra signalling cost due to the NSIS tunnel refreshment causes a significant overhead on the proposed scheme signalling cost resulting in a sudden slop on the ratio, when the number of MNs is 1 (Figure 4.4(a)). Nevertheless, when the number of MNs increases, the effect becomes less severe keeping the ratio still significantly low (Figure 4.4(b)).

Finally, Figure 4.5 shows the reservation re-establishment latency as a function of the wireless link propagation delay. It is defined as the time when the MN starts its handover till a new NSIS-based reservation is established, hop by hop, along the new path inside the LMA/G-LMA domain. The parameters used are set as follows: $L_w = 1ms$, $B_w = 100Mbps$, $B_{wl} = 11Mbps$, $q_f = 0.5$ and $T_{L2} = 50ms$.

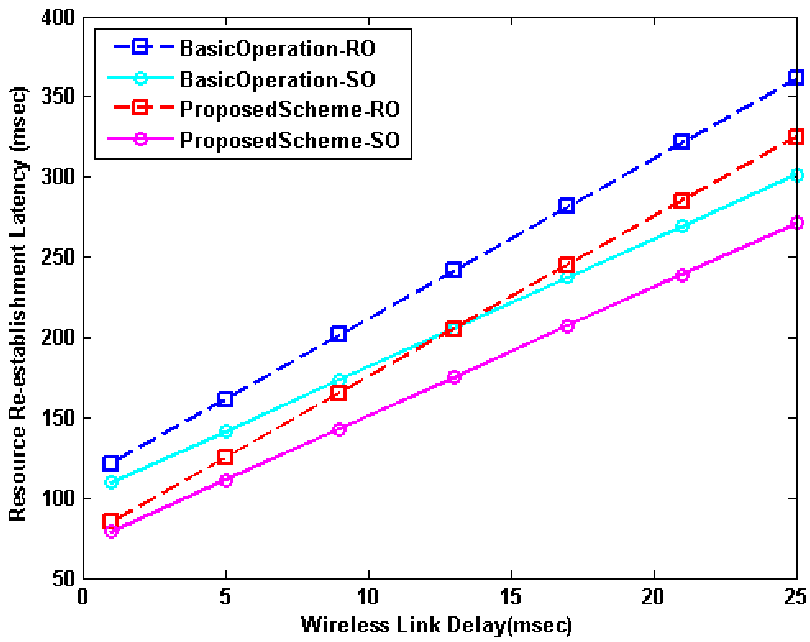


Figure 4.5: NSIS-based resource re-establishment latency as a function of wireless link delay

As it can be seen, the latency increases linearly as the wireless link propagation delay increases. Moreover, as expected, the delay of receiver-oriented reservation (the dashed-line with red and navy squares) is higher than the one in the sender-oriented (represented with solid lines in blue and purple with circle marks). However, comparing the dashed-line results with each other and the solid-lines with each other, the results obtained show that exploiting the pre-configured NSIS tunnel, the proposed scheme can reduce the resource re-establishment latency by an average of 15%, as compared to the baseline protocol.

4.5 Summary

In this chapter, the proposed scheme and analytical framework given in Section 3.3, has been adopted to tackle the NSIS problems in the PMIPv6 environment, its long resource re-establishment latency and high signalling cost. The scheme consisted of the multi-layer LMA, G-LMA and L-LMAs, and the pre-configured NSIS session between them.

Having the multi-layer mobility agent architecture can localise the MN's resource reservation and mobility management inside the domain, resulting in a decrease in the amount of the signalling cost. Results showed that under above assumptions, the new scheme has achieved an average of 5% and 10.5%, for the sender-oriented and the receiver-oriented reservation, in total signalling cost. Moreover, exploited the pre-configured NSIS sessions between the G-LMA and L-LMAs, has caused a noticeable decrease of 15% in the reservation latency.

Chapter 5

A Comparison of RSVP and NSIS in Access Networks

5.1 Introduction

IIn an effort to support resource reservation signalling and other various signalling applications, IETF introduced NSIS [5] suite as a generic framework. Conceptually similar to RSVP, NSLP attempts to overcome the RSVP shortcomings by supporting additional features such as sender- and receiver-oriented reservations, location-independent session identifier (session-id) for mobility support, bi-directional reservation, and ability to use existing transport and security protocols. Nevertheless, the gains come with the cost of significant overhead in the network. Mobility is one of the major issues in RSVP, which is also left almost untouched in NSIS. There are some proposals to address the problem [44, 94, 95], however, the lack of internal mechanism has led NSIS to the same path passed by RSVP years ago. Scalability was another issue that surrounds RSVP. Nevertheless, the results obtained from the testbed implementation in [93, 96], without considering the mobility, show that NSIS cannot address the scalability issue in RSVP, but worsens it.

In this chapter the comparison of the RSVP and NSIS operations in access networks is made. To the best of the author's knowledge, this is the first analytical comparison between these two signalling protocols in the literature. The aim is not to advocate which one is better, but rather to study the effects of various network parameters on their performance to enlighten decision-making.

5.2 Analytical Model

The analytical model used here is based on the one introduced in Section 3.3. The mobility management protocol chosen is the network-based localised mobility management protocol, PMIPv6. The protocol exempts the MN from participating in any mobility-related signalling. Similar to the one in previous chapter, it is assumed that the LMA domain consists of K rings (ring 0 to ring K-1), and the MN is initially located in the centre cell.

5.2.1 Total Cost Function

In this section, the total signalling cost and resource re-establishment latency of both protocols, RSVP and NSIS, are studied in detail. In all scenarios, the MN is considered as a receiver of the flow, since this is the most challenging part of the RSVP and NSIS operations in mobile environments. Also, it is assumed that, there is no pre-configured RSVP/NSIS sessions between LMA and MAGs.
The total signalling cost C_{Total} comprises of a location update signalling cost, a resource reservation signalling cost and packet delivery cost, C_{LU}, C_{RR}, and C_{PD} respectively.

$$C_{Total} = C_{LU} + C_{RR} + C_{PD} \tag{5.2}$$

5.2.1.1 Location Update Cost

In PMIPv6, the MN can perform two kinds of handover: the inner-domain and inter-domain handovers, described in detail in [7] and [91]. The former is performed whenever the MN enters a cell/MAG belong to the same LMA domain, while in the latter, a new cell belongs to a different LMA. The registration process to the LMA is the same for both types of handover. However, in order to keep the current connection(s) alive, after entering a new domain during the inter-domain handover, the LMA sends a PBU to the MN's Home LMA and CN(s) [91]. Their addresses are included in the router solicitation, sent by the MN upon entering a new cell, and are passed on by the MAG to the LMA. Apart from registration, the PBU and PBA should be exchanged between the peers periodically in order to extend the binding lifetime. This cost is represented by C_{BR}. Given that C_g and C_l are the signalling costs in the inter-domain/global and inner-domain/local handovers, the location update cost can be expressed as follows:

$$C_{LU} = \lambda_m \Big(qC_g + (1 - q)C_l \Big) + C_{BR} \tag{5.3}$$

where q and *(1-q)* are the probability of performing the inter-domain and inner-domain handovers obtained from Equation (3.5). Other notations are the same as the ones introduced in Table 3.1, but in the PMIP context. The cost of sending binding refresh messages C_{BR}, C_g and C_l can be derived as follows:

$$\begin{aligned} C_l &= 2TC_{mag-lma} + PC_{mag} + PC_{lma} \\ C_g &= 2TC_{lma-ha} + PC_{ha} + N_{cn}(2TC_{lma-cn} + PC_{cn}) + C_l \\ C_{BR} &= 2\lfloor \frac{t_m}{T_{rf}} \rfloor TC_{mag-lma} + 2\lfloor \frac{\overline{\tau}_{ha}}{T_{rf}} \rfloor (TC_{lma-ha} + N_{cn}TC_{lma-cn}) \end{aligned} \tag{5.4}$$

5.2.1.2 RSVP Signalling Cost

In the PMIPv6 network, the LMA can act as an RSVP proxy [42], dividing an end-to-end reservation session between the MN and CN into two parts: the outer part and the inner part. The former is between the CN and serving LMA, re-established when the MN enters a new LMA domain. In the latter, the resources are reserved between the LMA and MN, needed to re-establish when the MN enters a new cell. The cost of the outer part and inner part reservation are represented by the R_g and R_l, respectively. Thus:

$$C_{RR} = \lambda_m \Big(qR_g + (1 - q)R_l \Big) + R_{RF} \tag{5.5}$$

where R_{RF} is the cost of the RSVP refresh messages. Assume that all the nodes in the network to be RSVP aware, the RSVP signalling cost consists of the transmission cost and processing cost in all the nodes through the path. Therefore:

$$\begin{aligned}
R_l &= 2TC_{mn-lma} + 2D_{mn-lma} \times \eta \\
R_g &= 2TC_{lma-cn} + 2D_{lma-cn} \times \eta + R_l \\
R_{RF} &= 2\lfloor \frac{t_m}{T_{rrf}} \rfloor TC_{mn-lma} + 2\lfloor \frac{\overline{\tau}_{ha}}{T_{rrf}} \rfloor TC_{lma-cn}
\end{aligned} \tag{5.6}$$

5.2.1.3 NSIS Signalling Cost

Similar to the RSVP operation in the PMIP network, the NSIS end-to-end reservation can be divided into two parts: the outer part between the CN and LMA, and the inner part between the LMA and MN. Therefore, the total cost can be represented as follows:

$$C_{RR} = \lambda_m \Big(qR_g + (1-q)R_l \Big) + R_{RF} \tag{5.7}$$

The cost of each part consists of the NSLP signalling cost, and GIST three-way handshake signalling cost represented by $C^N_{l/g}$ and $C^G_{l/g}$, respectively. Since both NSLP and GIST can operate in two different modes, the sender- or receiver-oriented reservation in NSLP and the D-mode or C-mode in GIST, four different scenarios can be considered. To this end, the signalling cost of each part has been further categorised into two sub-groups. $C^{NS}_{l/g}$ and $C^{NR}_{l/g}$ represent the cost of sender- and receiver-oriented reservations, while $C^{GD}_{l/g}$ and $C^{GC}_{l/g}$ denote the GIST operations in the D-mode and C-mode. Therefore, the total signalling cost of the sender-oriented reservation in D-mode becomes:

$$\begin{aligned}
&C^{SD}_{RR} = \lambda_m \Big(qR^{SD}_g + (1-q)R^{SD}_l \Big) + R_{RF} \\
&\text{where} \\
&R^{SD}_l = [C^{NS} + C^{GD}]_{mn-lma} + [R^N_{RF} + R^G_{RF}]_{mn-lma} \\
&R^{SD}_g = R^{SD}_l + [C^{NS} + C^{GD}]_{lma-cn/ha} + [R^N_{RF} + R^G_{RF}]_{lma-cn/ha} \\
&C^{NS} = TC^{Reserve} + TC^{Response} + D(\eta^{Reserve} + \eta^{Response}) \\
&C^{GD} = TC^{Query(D)} + TC^{Response(D)} + TC^{confirm(D)} + D(\eta^{Query} + \eta^{Response} + \eta^{Confirm})
\end{aligned} \tag{5.8}$$

The total signalling cost of the receiver-oriented reservation in C-mode becomes:

$$
\begin{aligned}
C_{RR}^{RC} =& \lambda_m \Big(q R_g^{RC} + (1-q) R_l^{RC} \Big) + R_{RF} \\
R_l^{RC} =& [C_l^{NR} + C_l^{GC}]_{mn-lma} + [R_{RF}^{N} + R_{RF}^{G}]_{mn-lma} \\
R_g^{RC} =& R_l^{RC} + [C_g^{NR} + C_g^{GC}]_{lma-cn/ha} + [R_{RF}^{N} + R_{RF}^{G}]_{lma-cn/ha} \\
& \text{where} \\
C^{NR} =& TC^{Query} + TC^{Reserve} + TC^{Response} + D(\eta^{Query} + \eta^{Reserve} + \eta^{Response}) \\
C^{GC} =& TC^{Query(C)} + TC^{Response(C)} + TC^{confirm(C)} + D(\eta^{Query} + \eta^{Response} + \eta^{Confirm}) + \\
& TCPSyn/SynAck/Ack
\end{aligned}
\tag{5.9}
$$

The refresh signalling cost of the NSLP and GIST can be given as follows:

$$
\begin{aligned}
RF_N &= 2\Big[\lfloor \frac{\overline{\tau}_{ha}}{T_{rrf}} \rfloor TC_{lma-cn} + \lfloor \frac{t_m}{T_{rrf}} \rfloor TC_{mn-lma} \Big]^{Reserve/Response} \\
RF_G &= \Big[\lfloor \frac{\overline{\tau}_{ha}}{T_{rrf}} \rfloor TC_{lma-cn} + \lfloor \frac{t_m}{T_{rrf}} \rfloor TC_{mn-lma} \Big]^{Query}
\end{aligned}
\tag{5.10}
$$

The total cost of other scenarios, the sender-oriented in the C-mode and the receiver-oriented in the D-mode, can be obtained from the costs introduced in Equation 5.8, and Equation 5.9. The NSLP cost, for the sender-oriented reservation, comprises of the transmission and processing costs of the *Reserve* and *Response* messages. Given that the receiver-oriented reservation was preferred, the cost includes the transmission and processing costs of the *Query*, *Reserve*, and *Response* messages along the data path. Node that the cost includes the overhead of the *GIST-Data* message used to convey the NSLP messages as a payload.
The cost of the GIST layer depends on the type of the operation required by the flow, the D-mode or C-mode, respectively. The GIST cost in the D-mode includes the transmission and processing costs of the *Query(D)*, *Response(D)*, and *Confirm(D)* messages between the GIST peers along the path. Assume that there is no matching MA between peers in the C-mode operation, the GIST messages (*Query(C)*, *Response(C)*, and *Confirm(C)*) should carry extra objects,

i.e., Stack-Proposal and cookies, in order to establish the MA between peers. Therefore, their sizes are different from the ones in the D-mode. Moreover, the TCP three-way handshake should be performed before sending the *GIST-Confirm* message.
Both NSLP and GIST use the soft sate mechanism to manage their states. Therefore, the refresh messages, NSLP *Reserve/Response* and *GIST-Query*, should be sent periodically between the peers. The RF_N and RF_G represent their costs in this calculation. Note that their refreshing process are independent from each other. Based on [96], the refresh signalling messages in the NSLP includes both *Reserve* and *Response*. The GIST refresh mechanism consists of the MRS and MA updates, however similar to the assumption in [93], the MA refreshing overhead is not considered in this analysis.

5.2.1.4 Packet Delivery Cost

Assume that Route Optimization is enabled, the first packet in a session goes to the HA, while the rest are directed to the LMA who intercepts and tunnels them to the serving MAG. The packet delivery cost can be given as:

$$C_{PD} = C_{ha} + C_{LMA} + C_T \tag{5.11}$$

where C_T is the packet transmission cost between the CN and MN. C_{ha} and C_{LMA} are the packet processing cost at the HA and LMA, respectively. All the costs are the same as the one used in Section 3.3.2.3, Equation 3.27, Equation 3.26 and Equation 3.25.

5.2.1.5 Resource Re-establishment Latency

The resource reservation latency t_{RL} is defined as a total time taken to perform a handover, as well as re-establish an end-to-end resource reservation along a new path in the LMA domain. The time comprises of the delays imposed by the L2 handover, and binding update process represented by t_{L2} and t_{BU}, respectively. In the RSVP-based scenario, when the LMA receives a PBU, it sends a PBA, followed by a new RSVP *Path* message, towards the MN. Upon receiving the *Path* message, the MN sends a *Resv* message destined to the LMA. The reservation on the new route is completed when the *Resv* message reaches the LMA. Therefore, total resource re-establishment latency can be given as follows:

$$t_{RL} = t_{L2} + \Big[\mathrm{M(PBU)} + \mathrm{MAX}\big(\mathrm{M(PBA)}, \mathrm{M(PATH)}\big) + \mathrm{M(RESV)}\Big]_{mn/mag-lma} \tag{5.12}$$

where M is the time taken to send a message between two nodes, including the transmission time and the propagation time [77]. Therefore:

$$\begin{aligned} M &= \frac{b}{B_{w/wl}} + L_{w/wl} \\ M_{wired} &= D_{X-Y} \times M \\ M_{wireless} &= M + (T_w + M) \times \frac{q_f}{1-q_f} \end{aligned} \tag{5.13}$$

In NSIS, when the LMA receives a PBU, it sends a PBA followed by a new NSLP message (*Reserve* or *Query* message in the sender- or receiver-oriented reservation) towards the MN. Upon receiving the *Reserve*[*Query*] message, the MN sends a *Response*[*Reserve*] message to the LMA. In the sender initiated model, the reservation on the new route is completed when the *Response* message reaches the LMA. However, in the receiver initiated scenario, the reservation on the new route is completed when the *Response* message reaches the MN. Therefore:

$$\begin{aligned} t^S_{RL} &= t_{L2} + \Big[M(PBU) + Max(M(PBA), M(Reserve)) + M(Response)\Big]_{mn/mag-lma} \\ t^R_{RL} &= t_{L2} + \\ &\Big[M(PBU) + Max(M(PBA), M(Query)) + M(Reserve) + M(Response)\Big]_{mn/mag-lma} \end{aligned} \tag{5.14}$$

5.3 Performance Investigations

This section presents the numerical results of the NSIS operation in terms of the total signalling cost, bandwidth consumption, and resource reservation latency as compared to the ones in RSVP. Most parameters used in this analysis are based on the typical values found in [75, 81, 93, 96]. The domain has one LMA/GLAM consists of 61 cells. The session arrival rate, λ_c, is set to 0.1, with the Exponential distribution. The binding lifetime is 20 minutes. The RSVP and NSIS refresh interval are set to 45 seconds. The average cell residence time is 30 seconds. The control message processing cost in different nodes are defined as follows: $PC_{mag} = 12$, $PC_{lma/ha} = 24$, and $PC_{cn} = 4$. The other variables are set to: $\delta = 1$, $\zeta = 10$, $\eta_{nslp/rsvp} = 4$, $\eta_{gist} = 1$, $\eta_{tcphandshake} = 1$, $K = 5$, $D_{mag-lma} = 10$, $D_{lma-ha} = 25$, $D_{lma-cn} = 8$, $D_{ha-cn} = 8$, and $N_{cn} = 1$. For demonstration purposes γ is set to 1, resulting in the Exponential distribution for the MN's cell residence time with the mean and variance equal to $\frac{1}{\lambda_m}$ and $\frac{1}{\lambda_m^2}$, respectively [90]. Since the reservation refresh signalling cost between the LMA and CN does not have any effect on the signalling load inside the LMA domain, therefore, it is not considered in the final calculations.

Total signalling cost, including the mobility, resource reservation and packet delivery costs, as a function of the number of MNs in the PMIP domain, is depicted in Figure 5.1. The results indicate that RSVP has the smallest signalling cost, while the NSIS with the C-Mode operation in the GIST layer, and the receiver initiated reservation in the NSLP layer has the biggest one. As the comparison shows the NSIS's rich functionality, enhanced modularity, message-transfer reliability and security support are accompanied by the certain cost, increasing the total signalling cost by an average of 48% and 64% in the NSIS sender- and receiver-oriented operation conducted in C-mode, as compared to RSVP. Even without reliable transport and security support, i.e., NSIS operation in the D-mode, the overheads are noticeably higher that the one in RSVP, by an average of 24% and 41% increase in the sender- and receiver-oriented reservations. This mainly comes from decoupling the node discovery from the signalling message delivery in the GIST layer, resulting in a high number of message exchanges during the three-way handshaking process.

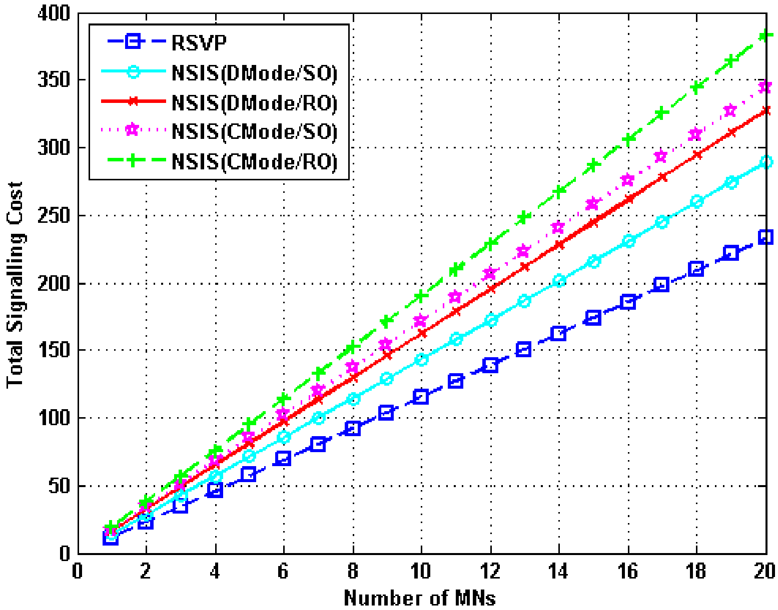
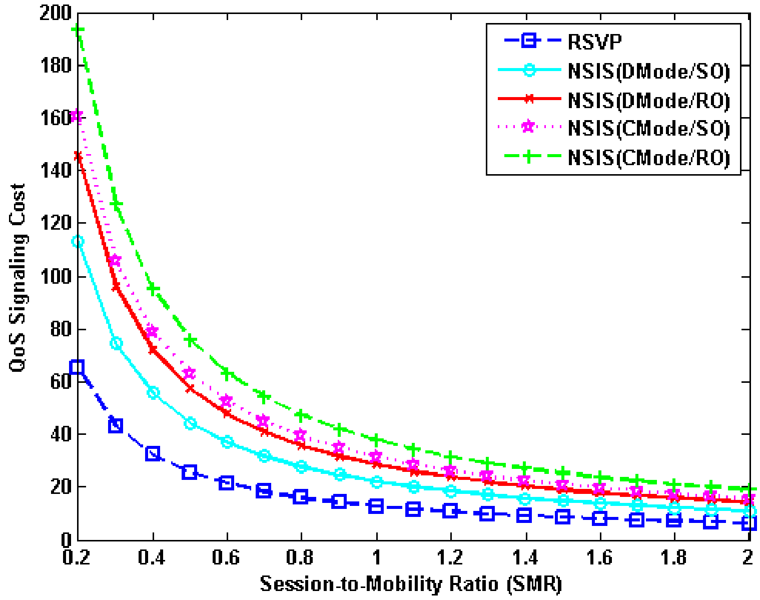
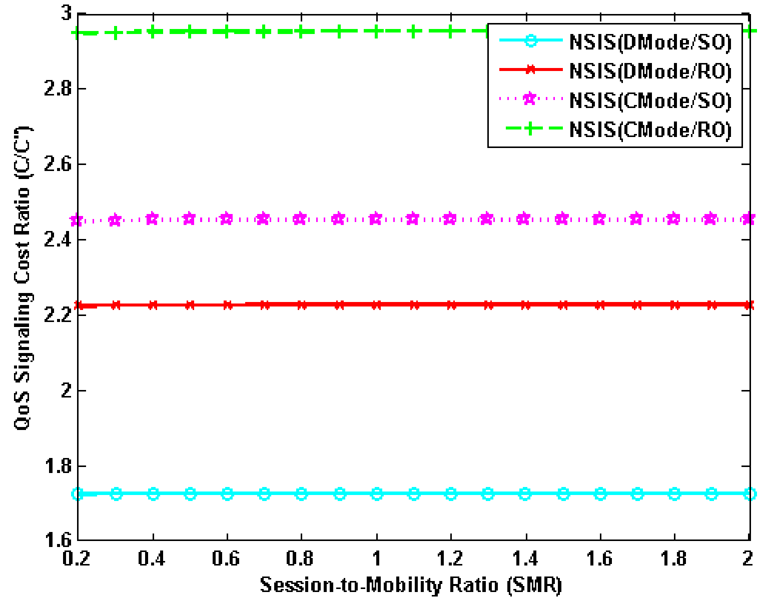


Figure 5.1: Cost comparison of RSVP and NSIS

The impact of the SMR on the resource reservation signalling cost is depicted in Figure 5.2(a). Small value of the SMR denotes that the MN's mobility rate is higher than the session arrival rate, and therefore, resulting in more frequent handovers. Having the high number of handovers increases the resource reservation signalling cost. The reason is that in order to fulfil the QoS requirement, the resources should be reserved on a new path immediately. When the SMR value is large, the MN performs less handover, intuitively, imposing less resource reservation signalling cost. As the figure shows, RSVP has the least resource reservation signalling cost among other scenarios, for all the value of SMR. The clear comparison between the RSVP and NSIS signalling cost can be shown in Figure 5.2(b), in which results indicate the ratio of the NSIS signalling cost to the RSVP signalling cost, C and C′ respectively. It is interesting to see that the simplest form of NSIS operation, the sender-oriented with neither reliability nor security support, has 80 percentage more signalling overhead as compared to RSVP. Having the NSIS operation with its full functionalities, including the receiver-oriented with TCP in its transport layer and support of using the ex-



(a) Individual Cost



(b) Cost Ratio

Figure 5.2: Impact of SMR on the RSVP and NSIS signalling cost

isting security protocols, imposes almost 3 times more overhead as compared to RSVP. Having the sequential process of discovering the next capable node and transporting the NSLP signalling message, as well as the necessity of performing both of them after each handover cause the significant increase in the NSIS signalling overhead.

Figure 5.3 shows the total amount of bandwidth consumption by the signalling messages as a function of the session lifetime. The number of active sessions is set to be one. Also, it is assumed that the MN's average cell residence time is greater than its session lifetime. Under this assumption, the impact of having an extra signalling overhead, due to the MN's handover, will be excluded.

The total bandwidth consumed comprises of the bandwidth used to set-up the reservation, as well as the one used to keep it alive during the session lifetime. Assuming that the session lasts for n seconds, the total bandwidth consumption in RSVP can be derived as follows:

$$BW = (MPath + MResv) + \left(\frac{n}{T_{rf}} \times (MPath + MResv)\right) \tag{5.15}$$

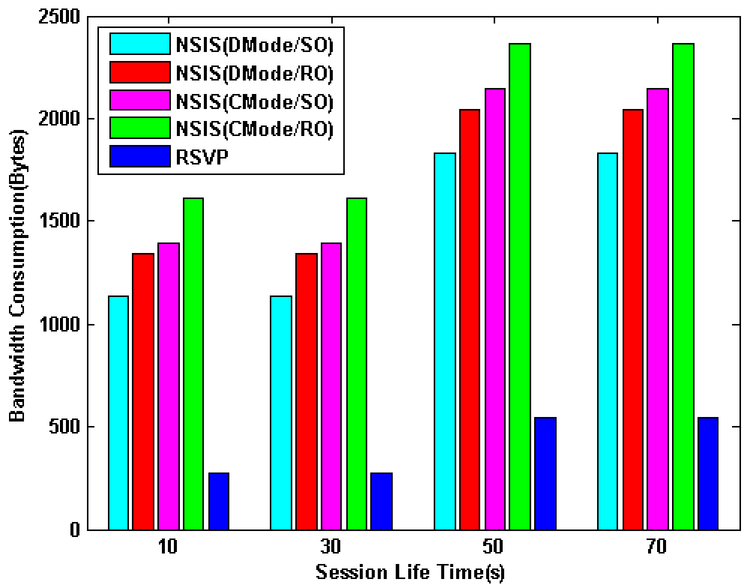


Figure 5.3: Bandwidth consumption by signalling messages

where MPath and MResv are the size of the *Path* and *Resv* messages in bytes, and T_{rf} is the refresh interval in seconds.
The amount of bandwidth taken by the NSIS signalling messages depends on two factors: the GIST layer operation mode (C-Mode or D-Mode), and the NSLP reservation type (sender- or receiver-oriented reservation). The total bandwidth consumed can be expressed as follows:

$$BW = (MGist + MNslp) + \left(\frac{n}{T_{rf}} \times (MNslpR + MGistR)\right) \tag{5.16}$$

where *MGist* represents the total size of GIST messages sent in each GIST operation mode. *MNslp* denotes the total size of NSLP messages exchanged, based on the NSLP reservation type chosen. Total size of the refresh messages, used in NSLP and GIST, are represented by MNslpR and MGistR. Table 5.1 shows the size of the messages used in each protocol, including the transport layer and IP layer overheads. Note that RSVP uses raw IP, therefore the transport layer overhead would be zero for its massages.

Table 5.1: Signalling Message Size in IPv6

Message Type	Message Size(Bytes)
NSLP Query/Reserve/Response	44/112/44
GIST(D)Query/Response/Confirm/Data	212/240/200/164
GIST(C)Query/Response/Confirm/Data	244/244/208/176
TCP Syn/SynAck /Ack	64/64/60
RSVP Papth/Resv	124/148
PMIP PBU/PBA	76/76

As shown in Figure 5.3, RSVP consumes the lowest amount of bandwidth among all the scenarios. The higher amount of the bandwidth consumption in the NSIS comes from the higher number of messages sent, and their larger sizes as compared to the ones in RSVP. By increasing the session lifetime, the costs remain constant for the all scenarios until the time that the refresh messages should be sent in order to keep the reservation alive (t = 45s). Sending the refresh messages adds extra signalling overhead in both RSVP and NSIS. The results show that the NSIS set-up operation consumes between 4 to 6 times more bandwidth compared to RSVP. This can give rise to concern to the NSIS operation and the functionality

chosen, in the heavy load access networks especially in the wireless part.
Finally, Figure 5.4 shows the reservation re-establishment latency as a function of the wireless link propagation delay. This time is defined as the time when the MN starts its handover till a new reservation is established hop by hop between the MN and LMA inside the PMIP domain. The parameters used to calculate the resource reservation latency are as follows: $L_w = 1ms$, $B_w = 100Mbps$, $B_{wl} = 11Mbps$, $q_f = 0.5$ and $T_{L2} = 50ms$.

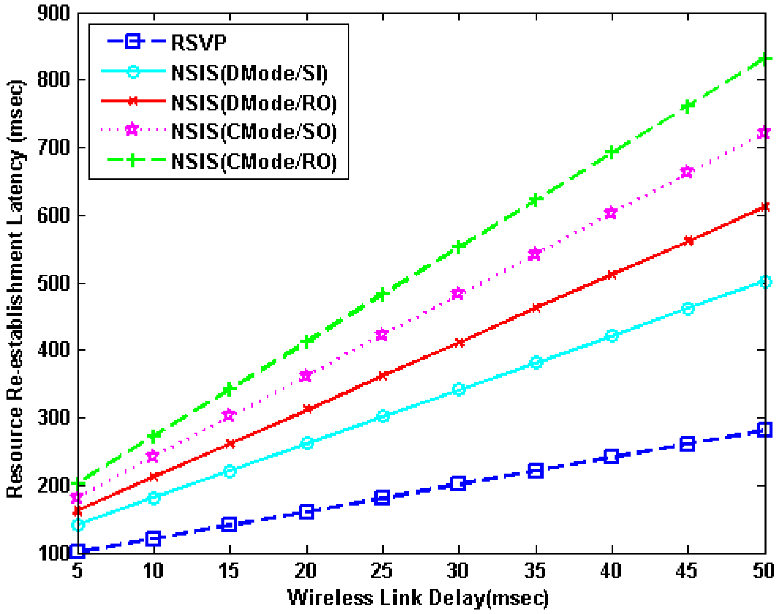


Figure 5.4: Comparison of RSVP resource re-establishment latency and NSIS as a function of wireless link delay

Since all the packets between the LMA and MAGs are tunnelled, the Crossover Node Discovery (CND) mechanism cannot be used by default, and all the signalling messages should traverse between the MN and LMA as the two end points of the session. The reason is that CRN discovery for an end-to-end path is initiated by the MN by sending a Reserve (sender-oriented case) or Query (receiver-oriented case) message. Since in PMIP the MN uses its home address as the source address after handover, a CRN is found by normal route change process,i.e., the same session-id and Flow ID, but a different identifiers of the next signalling peer defined by Source Identification Information (SII) handle.

Assuming the MN as a receiver of the flow and the LMA as a sender (on behalf of the CN), both RSVP and NSIS suffer from the lack of the internal mechanism to trigger the required signalling messages on the new path after handover (issuing the Path message in RSVP and the NSLP Query/Reserve in NSIS). Therefore, both are dependent on the external mechanism, i.e., receiving the PBU message in the PMIP protocol. The problem adds an extra delay on the reservation latency in both protocols. However, the results obtained show that RSVP has the lowest resource re-establishment latency, in the cost of having limited functionality, making it more appropriate candidate for real time applications in mobile networks. After that the NSIS sender- and receiver-oriented operations in D-mode by an average of 67% and 102%, and the NSIS sender- and receiver-oriented in C-mode by an average of 135% and 169% longer resource reservation latency, as compared to the one in RSVP, are ranked from second to the fifth.

5.4 Summary

In this chapter, a comparison between the RSVP and NSIS operations in a PMIP-based access network has been presented. Thoroughly analysing the RSVP operation, NSIS was introduced by IETF to overcome the RSVP shortcomings by supporting additional features such as sender- and receiver-oriented reservations, location-independent session-id for mobility support, bi-directional reservation, and reusing existing transport and security protocols. However, it inherits the RSVP problem in a mobile environment, while its extra functionalities come with noticeable costs. By adopting the analytical framework introduced in Section 3.3, the performance of each protocol, RSVP and NSIS, in terms of the network signalling cost, bandwidth consumption and resource re-establishment latency were investigated. The results obtained highlighted the noticeable costs of using NSIS features as compared to the plain operation of RSVP. Going through these outcomes, one can get clear insights about the pros and cons of using NSIS in access networks.

Chapter 6

An Efficient QoS-Based Routing in Backbone Networks

6.1 Introduction

As the growing multimedia applications such as IPTV and VoIP have become ubiquitous, the need to migrate from the best-effort service model to one, in which service differentiation can be provided, seems inevitable for future Internet architectures. The Internet owes its success to its naive operation, routing all requests along the shortest paths based on the predefined link weights. However, that sort of simplicity comes at the cost of optimality. It fails to effectively utilise network resources for today's traffic demand, mostly characterised by highly variable traffic behaviour over time.

In this chapter, a new multi-topology routing based traffic engineering approach is proposed. The scheme can support two major practical issues, the service level agreement requirements and link failure resiliency. First, based on a proposed algorithm, fully edge-disjoint logical views of a network are extracted, in a way that the delay of the longest path is upper bounded. Then, the proposed scheme selects the longest acceptable path for each traffic type. This can guarantee that the shortest paths are always available, and can be used by the most legitimate flows in the network, the ones that other paths cannot satisfy their delay constraints. Having edge-disjoint logical topologies, it would be possible to shift the traffic to the next to the best alternative rout in case of a link failure, and therefore, providing an efficient failure resiliency. Since the defined problem, finding the multiple disjointed logical topology, is NP-hard, heuristic algorithms to handle the problem are proposed. Thorough investigations on the performance of the proposed scheme, based on a real topology and traffic matrices, show that the scheme can achieve an efficient resource utilisation, even under sudden increases in traffic demands, while at the same time can comply with flows' service level agreements.

The rest of this chapter is organised as follows: In the next section, the related literature is reviewed. The system model and the problem definition are introduced in Section 6.3. Section 6.4 investigates the hardness of the problem. The proposed algorithms to build disjoint routing topologies, and select the best one based on the flow's requirements are discussed in Section 6.5. The numerical results are discussed in Section 6.6, followed by the remarking conclusions in Section 6.7.

6.2 Background Overview

Achieving optimal link utilisation, or more accurately the near-optimal link utilisation due to the NP-hard nature of the problem [97, 98], requires link weights adjustment, based on a network-wide view of the traffic and topology, within a domain. Such adjusted-weights would result in a balanced load distribution across all links, and total cost minimisation. The procedure, that takes the traffic matrix as an input and returns an optimal set of link weights for a given topology as an output, is called traffic engineering.

Of all of the available traffic engineering techniques, many of them rely on the offline methods, where long-term average traffic demands over multiple days or potentially months are used as an input. Though simple to implement, their output might cause a suboptimal or even an inadequate load distribution, caused by the highly unpredictable variation of traffic demand. Consequently, the next step would be using online traffic engineering, that can react to the real-time traffic demand [99, 100]. Making link weights sensitive to the current load of network, however, requires the flooding of new link weights throughout the network,

causing route instability and transient forwarding loops [101, 102].
To account for the effect of the on-the-fly link weight changes, the Multi-Topology routing (MT-Routing) [103, 104] has been used excessively in recent years [105–107], especially in the context of TE [101, 102, 108–113]. MT-Routing provides routers with multiple *logical* views of the network's physical topology, each one with an independent set of link weights. A separate routing table is maintained for each topology, allowing routers to leverage the high flexibility in better path selections.
The basic properties of the existing algorithms for building logical topologies are as follows: for each link in the network there exists at least one topology where the link is excluded. At the same time, it is tried to reduce the chance of the link being selected by all the remaining logical topologies. Consequently, the result would be multiple logical topologies with overlapped parts. Since each logical topology has a separate routing table and updating process, any decrement in its number and size can have a significant signalling and routing overhead reduction, and therefore, is of prime importance in this work.
Although having multiple logical topologies offers a high level of flexibility in path selection for different traffic types, they still share the same physical topology. Therefore, while concerning about overall resource utilisation is still indispensable, carriers have to guarantee that a topology chosen to carry a given flow satisfies its SLA requirements. Having multiple logical topologies, with the sets of link weights that minimise the overall cost of the network yet breach the SLA carrier commits to its customers, makes the solution impractical in an operational network.
Based on this insight, the approach of this work differs from the existing proposals in that, the proposed scheme focuses on an edge-disjoint logical-topologies construction and the SLA based traffic assignment. However, contrary to the current routing protocols, that send packets along a best possible route, the proposed approach always selects the last possible one, the route with the longest possible delay that does not breach the SLA. To this end, heuristic algorithms to decompose a given physical topology to multiple edge-disjoint logical ones are introduced, wherein each traffic class is assigned to one of them. The traffic demand between each Origin-Destination (O-D) pair is a combination of different

traffic classes, each with its own SLA requirement defined here as the average end-to-end delay across all O-D node pairs [114]. Therefore, the proposed approach assigns the high-priority traffic with a very tight requirements, e.g., voice, to a logical topology containing the shortest path between the pair. Unlike the high-priority traffic, which has a stringent delay requirement, low-priority traffic (e.g., data) can survive gradual degradation as the network performance reduces. Therefore, they can be mapped to a topology containing the longest path between the pair. In order to ensure a minimum acceptable service level for low-priority traffic, the proposed algorithm bounds the worst-case performance, guaranteeing that a longest path delay cannot be more than the maximum acceptable delay. If the number of disjoint topologies was more than two, other traffic types can be defined and assigned to one of the remaining topologies. The proposed algorithm can be deployed in each router independently. Moreover, having fully edge-disjoint logical topologies can enhance failure resiliency, making it more robust to changes in the network status.

6.3 System Model and Problem Definition

A network is represented by a weighted directed graph $G = (V, E, c, d)$, where V is the set of nodes and E is the set of links. The delay and capacity of a link (i, j) from node i to node j are represented by $d(i, j)$ and $c(i, j)$, respectively. Let p be a path between an origin s and a destination t, the delay of path p, as an additive metric, can be expressed as follows:

$$d(p) = \sum_{(i,j)\in p} d(i, j) \tag{6.1}$$

The traffic matrices reflect the volume of traffic $R = \{r_{st} \mid s, t \in V\}$, where r_{st} is the traffic demand between a given O-D pair $s \to t$. For each pair node, a link-based routing X is defined by a set of variables $X = \{x_{ab}(i, j) \mid a, b, i, j \in V\}$, where $x_{ab}(i, j)$ is a fraction of traffic demand between a pair $a \to b$, that goes through the link (i, j). The flow conservation and non-negativity constraints on the variable x_{ab}, can be defined by the following equations:

$$\begin{cases} \forall i,j \neq a,b: & \sum_{j:(i,j)\in E} x_{ab}(i,j) - \sum_{j:(j,i)\in E} x_{ab}(j,i) = 0 \\ \forall a,b \in V: & \sum_{j:(a,j)\in E} x_{ab}(a,j) - \sum_{j:(j,a)\in E} x_{ab}(j,a) = 1 \\ \forall a,b \in V: & \sum_{j:(b,j)\in E} x_{ab}(b,j) - \sum_{j:(j,b)\in E} x_{ab}(j,b) = -1 \\ \forall (i,j) \in E: & 0 \leq x_{ab}(i,j) \leq 1 \\ \end{cases} \tag{6.2}$$

Traffic engineering usually considers a link-cost function $\Phi(f_{i,j}, c(i,j))$ that is an increasing function of the load $f_{i,j}$ on each link (i,j). While $\Phi(f_{i,j}, c(i,j))$ can represent any increasing and convex objective function, in this work the objective is to keep the load on a link within its capacity which consequently reduces the cost $\Phi(f_{i,j}, c(i,j))$. More precisely, the defined cost function $\Phi(.)$ adds up the cost of all the links, where the cost of a link is obtained from the relationship between the link capacity $c(i,j)$, and its current load $f_{i,j}$. Based on the experimental study, the cost function is defined as follows [97]:

$$\Phi(f_{i,j}, c(i,j)) = \begin{cases} f_{i,j} & \frac{f_{i,j}}{c(i,j)} < \frac{1}{3} \\ 3f_{i,j} - \frac{2}{3}c(i,j) & \frac{1}{3} \leq \frac{f_{i,j}}{c(i,j)} < \frac{2}{3} \\ 10f_{i,j} - \frac{16}{3}c(i,j) & \frac{2}{3} \leq \frac{f_{i,j}}{c(i,j)} < \frac{9}{10} \\ 70f_{i,j} - \frac{178}{3}c(i,j) & \frac{9}{10} \leq \frac{f_{i,j}}{c(i,j)} < 1 \\ 500f_{i,j} - \frac{1486}{3}c(i,j) & 1 \leq \frac{f_{i,j}}{c(i,j)} < \frac{11}{10} \\ 5000f_{i,j} - \frac{16318}{3}c(i,j) & \frac{11}{10} \leq \frac{f_{i,j}}{c(i,j)} \end{cases} \tag{6.3}$$

Equation 6.3 is the function of link utilisation, defined as a load over a link to its maximum capacity. The higher tha value, the bigger the outcome as a cost. The logical concept behind this function is that, it is cheap to send a flow through a link with a small utilisation (defined as $\frac{f_{i,j}}{c(i,j)}$). As the utilisation approaches the link capacity, it becomes more expensive to use this link. Under above assumption, the ultimate objective is to minimise $\sum_{(i,j)} \Phi(f_{i,j}, c(i,j))$, subject to the defined constraints.

Assume there are K disjoint logical topologies each one containing a path p^k between the O-D pair indexed by (s,t). Each $p^k : k = 1, 2, ..., K$ is associated with a delay $d^k(p)$, obtained from Equation 6.1. A traffic demand r_{st} with the delay constraint D^τ, defined in its SLA requirement, can be routed through the network if there is a path in any of defined topologies whose delay is less than or equal to the delay constraint of the given flow.

$$\forall r^\tau_{st} \in R, \exists k = 1, ..., K : d(p^k) \leq D^\tau \tag{6.4}$$

where τ is one of the traffic classes defined in the SLA.
With this insight, the problem can be formulated as a linear optimisation problem with following objective and constraints, defined as below:

$$\text{Minimise} \quad \sum_{k=1}^{K} \sum_{(i,j)\in p^k} \Phi(f^k_{i,j}, c(i,j)) \tag{6.5}$$

s.t:

$$(1)\forall i \in V : \sum_{j:(i,j)\in E} \sum_{k} x^k_{st}(i,j) - \sum_{j:(j,i)\in E} \sum_{k} x^k_{st}(j,i) = \begin{cases} -1 & i = t \\ 0 & i \neq s,t \\ 1 & i = s \end{cases}$$

$$(2)\forall s,t \in V : \sum_{k\in K} x^k_{st} = 1$$

$$(3)\forall (i,j) \in E, r \in R, and \quad s,t \in V : \sum_{st} x^k_{st}(i,j) r_{st} = f^k_{i,j}$$

$$(4)\forall (i,j) \in E : 0 \leq x^k_{st}(i,j) \leq 1$$

$$(5)\forall (i,j) \in E : 0 \leq f_{i,j} \leq C_{i,j}$$

$$(6)\forall s,t \in V, r \in R, k \in K : \text{ maximise } \sum_{k\in K} O(r^\tau_{st}, k)$$

$$\text{where} \quad O(r^\tau_{st}, k) = \sum_{(i,j)\in p^k} \frac{d(i,j)}{D^\tau} \leq \Gamma$$

$d(i,j)$ comprises of both propagation and transfer delays. The flow conservation is defined in constraint(1). Constraint(2) guarantees that the sum of all traffic's fractions routed along different topologies (e.g., assigned for real-time and non real-time traffic) is equal to one. Constraint(3) shows that the load of a link

(i,j), belonged to the topology k, is equal to the sum of all the fractional traffic (between all the O-D pairs) routed through this link. Assume that the link delay and the SLA-based delay constraint D^τ are non-negative, Γ is bound to fall in the $(0, 1]$ interval. The last constraint in Equation 6.5 guarantees that the shortest paths are used by the most legitimate flows, the ones that other paths cannot satisfy their delay constraints.
Since Equation 6.5 does not comply with the standard linear programming formulation, the last constraint can be tested by solving the following *slave* linear optimisation problem:

$$\begin{aligned}
&\text{Maximise} \quad \sum_{k \in K} \sum_{(i,j) \in p^k} \frac{d(i,j)}{D^\tau} \\
&\text{s.t:} \\
&\forall k \in K : \sum_{(i,j) \in p^k} d(i,j) \leq D^\tau \\
&\forall (i,j) \in E : d(i,j) > 0, D^\tau > 0
\end{aligned} \tag{6.6}$$

Although the best-effort traffic is not included in the SLA, in order to ensure that it can still get the acceptable service, the proposed algorithms, discussed later in Section 6.5, guarantee that the longest path delay will be lower than the acceptable upper bound delay.

6.4 Hardness of the Proposed Algorithm

This section shows that finding the edge-disjoint logical topologies is an NP-hard problem. First, the definition of the problem is provided. Then, the proof of the NP-hardness of the definition is given.

Definition 1. *Let $G = (V, E, c, d)$ be a weighted directed graph with a node set V and a link set E, where each link $e_i : i = 1, 2, .., \|E\|$ has a capacity of $c(e_i)$ and a delay of $d(e_i)$. Let the delay of the longest path be bounded to D. Without loss of generality, assume that the maximum number of logical topologies is two. The problem of finding two fully edge-disjoint paths with the maximum delay of D is NP-hard.*

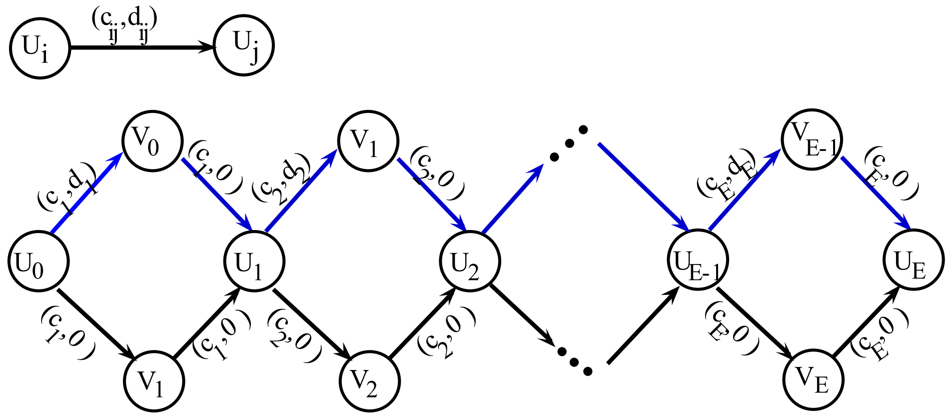


Figure 6.1: Transformation from Partition problem to the proposed scheme

Proof. Using a transformation from Partition problem, it can be shown that Definition 1 is NP-hard.

$$Partition \leq_p Definition1$$

Given a partition problem on a set E with element values $s(.)$, with the help of Figure 6.1 an instance of Definition 1 on the same set is constructed. For every $e_i \in E$, delay of each link $d(e_i)$ and the maximum delay of the paths D can be defined as $d(e_i) = s(i)$ and $D = \frac{\sum_{i \in S} s(i)}{2}$, respectively. The goal is to partition the set E into two disjoint subsets I and $E - I$ such that, the sum of the sizes of the elements in subset I is equal to the sum of the sizes of the elements in the subset $E - I$. This can be expressed as follows:

$$\sum_{s(i) \in I} s(i) = \sum_{s(i) \in E-I} s(i) = \frac{\sum_{i \in S} s(i)}{2} \tag{6.7}$$

That is by definition the Partition problem and has been proven to be NP-hard [115]. Substituting $s(i)$ by $d(e_i)$ and $\frac{\sum_{i \in S} s(i)}{2}$ by D, Equation 6.7 can be rewritten as follows:

$$\sum_{d(i) \in I} d(i) = \sum_{d(i) \in V-I} d(i) = D \tag{6.8}$$

This can give us two disjoint paths with the maximum delay of D. If there is no solution to the Partition problem defined in Equation 6.7, then there is no solution to find two disjoint paths defined in Equation 6.8. Moreover, since the transformation function is a polynomial-time function (see Figure 6.1), therefore, Definition 1 $\in$ NP-hard. $\square$

6.5 Proposed Heuristic Algorithms

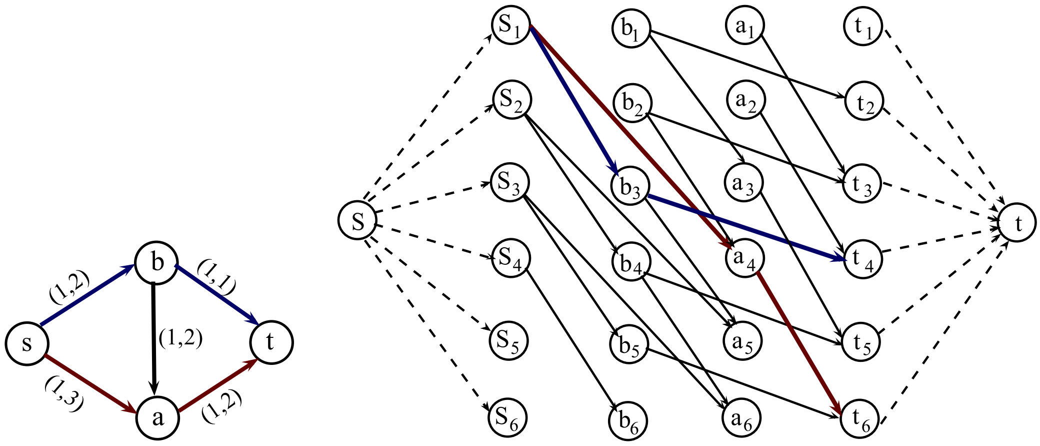
This section describes the proposed algorithms for defining the edge-disjoint routing topologies, and assigning flows to a best possible one which can fulfil their SLA needs.

6.5.1 Edge-Disjoint Routing Topologies (EDRT)

Due to NP-hard nature of the problem, a heuristic algorithm to find a set of disjoint logical topologies, while their maximum delay is less than D, is proposed in this section. The algorithm is based on a graph transformation technique used by [116]. Let an instance of the network be given by the graph $G = (V, E, c, d)$ with the maximum delay constraint $D > 0$ and O-D pair (s, t), while s is a current node and t can be any given node in the network. Both D and the delay of links are assumed to be integers. The algorithm aims to construct a *layered graph* $G^D = (V^D, E^D)$ from G in the following way:

- Make D copies $u_1, u_2, ..., u_D$ of each node $u \in V$. Node u_k in the G^D represents node u of the original network at time k.
- Include link (i_k, j_l) of capacity $c(i, j)$ in G^D whenever link $(i, j) \in E$ and $l - k = d(i, j)$. The link (i_k, j_l) in G^D represents the potential movement of a commodity from node i to node j in time $d(i, j)$.
- Reduce the multiple-source, multiple-sink problem in G^D to the single-source, single-sink problem by introducing a super-source S and super-sink t with the set of links, each with the bandwidth ∞.

It is easy to see that any path between origin s_1 and destination t in G^D has a corresponding path $p \in G$ such that $d(p) < D$. The constructed layered graph



(a) Graph G where each link is represented by (c, d)

(b) Graph G^D with D=6

Figure 6.2: Constructing a layered graph G^D from a graph G

G^D contains all the disjoint paths, with the delay less then D, between S and any given node in the network. By selecting any given node u as a destination, the set of $u_1, u_2, ..., u_D$ can be reduced to a super-sink with a set of links, each with infinite bandwidth capacity. Therefore, by moving from s_1 to the super-sink, all possible disjoint paths can be discovered. An example of the graph G and its transformation to the graph G^D with $D = 6$ is shown in Figure 6.2.

After constructing G^D, Algorithm 1 is used to find all existing disjoint logical topologies for a given network. For each link coming out of s_1, the shortest paths between s_1 and a given destination t are calculated, and the corresponding links are added to the $G_{[K]}$ (lines 6-7). The process continues until all of the other nodes are selected as a destination and their disjoint paths are discovered (loop in line 5). After adding the corresponding links to the $G_{[K]}$, these links would be deleted from the main graph G^D (line 9), guaranteeing that they will not be used in other topologies. The same process will be repeated for all of the outgoing links from s_1.

At the end if any link is left out, it will be included in the topology of which its parent link belongs, as long as the maximum delay constraint of the path is not violated. Adding these links can increase the number of possible routes in some part of each topology, resulting in a better link utilisation.

Algorithm 1 Finding K Disjoint Logical Topologies $G_{[K]}$

```
Construct G^D from G using the proposed graph transformation technique
K = 0
while outdegree(s_1) ≠ 0 do
    K = K + 1
    while all the nodes have been selected as a destination t do
        find the shortest path p_K between O-D pair (s_1, t)
        Put ∀(u, v) ∈ p_k in G_[K]
    end while
    Remove ∀(u, v) ∈ p_K from G^D
    outdegree(s_1) = outdegree(s_1) − 1
end while
return G_[k], k = 1, ..., K as the set of disjoint logical topologies
```

Not only does having fully disjoint topologies reduce the size of a routing table associated with each topology, but it increases the failure resiliency in the network.

6.5.2 Finding The Best Logical Topology

After finding all the edge-disjoint topologies in the network, all possible candidates need to be chosen for a given flow, in a way that each one complies with the flow's requirement. Algorithm 2 describes how the best set of logical topologies would be chosen by taking into the account the flow's traffic class τ and its SLA based delay constraint D^{τ}. Based on the proposed algorithm, for each logical topology, if a delay of the path between two end points in less than the flow's delay constraint, the topology is added as one possible solution. If there is more than one candidate, the path with the longest delay is selected.
Although this policy may violate routing efficiency, it is important to emphasis that the cost introduced as an objective in the optimisation is related to the congestion in the network, which is the convex function of link utilisation (Equation 6.3). In other words, the aim is to reduce the congestion in the network by shifting the traffic from highly-loaded links to the lightly utilised ones. This can help to reduce the total cost in the network.

Algorithm 2 Finding Best Topology for Flow $(r^{\tau}_{s_1t}, D^{\tau})$

for each $G_{[k]}$ **do**
  if $\frac{d(p_k)}{D^{\tau}} \leq 1$ **then**
    Add $G_{[k]}$ to the set of feasible solutions χ_r
    $\chi_r = \chi_r + 1$
  end if
end for
switch χ_r **do**
  case $\|\chi_r\| = 0$
    No feasible path is found to comply with SLA
  case $\|\chi_r\| = 1$
    Send the flow $(r^{\tau}_{s_1t}, D^{\tau})$ through the only possible topology
  case $\|\chi_r\| > 1$
    Select a topology with the highest $\frac{d(p_k)}{D^{\tau}}$ value
end switch

6.6 Performance Investigations

This section presents the numerical results obtained to measure the effectiveness of the proposed scheme. All the experiments are performed on a 2.0GHz PC with 2GB of memory. A real topology and traffic matrices are taken from Internet2 network, formerly known as Abilene [117].
The Internet2 router-level topology, shown in Figure 6.3, contains 9 advanced layer-3 nodes and 26 links, all of which have 10Gbps capacity. The delay of each link is set to an average of one week of observation obtained from OWAMP-Internet2 Network IPv4 Latency [118]. For traffic input 6 months of traffic demands driven from Abilene Observatory, publicly available at [119], is used.

Algorithms

The algorithms evaluated in this work are as follows:

- **Default-Metric**: In this algorithm, used by the Interior Gateway Protocols (IGP) e.g., OSPF, default weights are assigned to the links in operational networks. In this work the default IGP metrics assigned to the Internet2 topology are taken from [117].

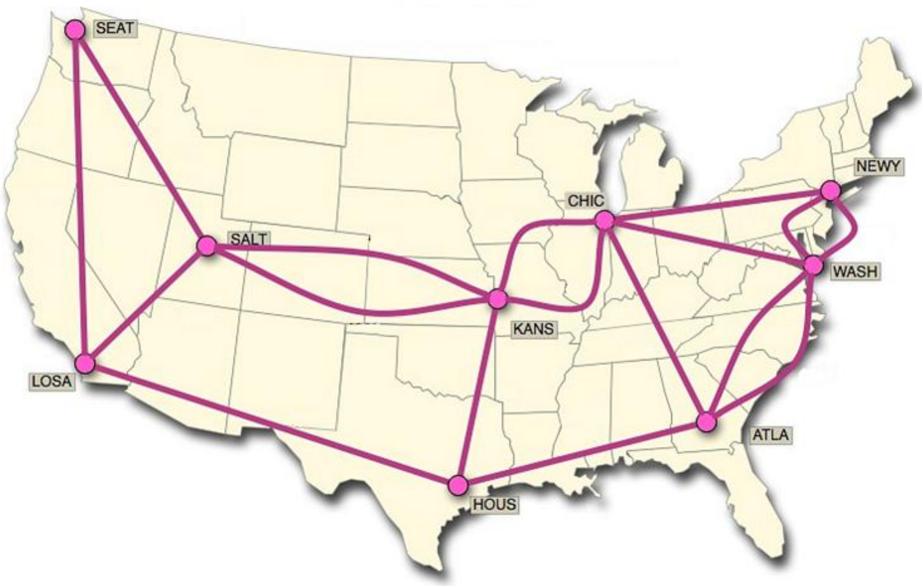


Figure 6.3: Internet2 connections [117]

- **InvCap**: This algorithm, commonly used by Cisco routers, sets the weights proportional to the inverse of the link capacity and runs OSPF [120].

- **MDelay**: In this algorithm, traffic demands are distributed in a given network based on the proposed scheme. Since the Internet2 network topology can guarantee the existence of two disjoint paths for each node pair, a traffic demand between each pair is divided into two classes with different SLA requirements: data and multimedia. The number X next to MDelay (MDelay-X%) in the upcoming figures shows the multimedia share of the total traffic between each node pair.

- **Optimal**: In this algorithm, Optimal traffic routing for a given topology and traffic demands are calculated, and used as a baseline for the comparisons.

All the algorithms have been implemented by using the IBM ILOG CPLEX [121] as the optimisation solver.

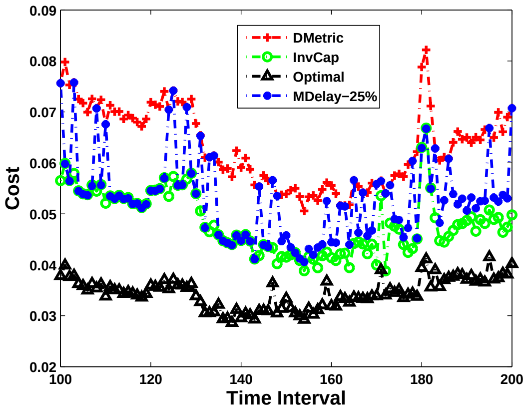
Performance Metrics:

The following two performance metrics are used to make comparisons between the algorithms: (i) the cost defined as an objective in our optimisation equation. The cost is proportional to the maximum of traffic to capacity of a link, and therefore, the small value of cost indicates the lower link utilisation. (ii) cost ratio defined as the ratio of the cost of using each algorithm to the cost of the optimal routing for given traffic matrices and network topology. For both metrics, lower values indicate more efficient resource utilisation, and hence are preferred.

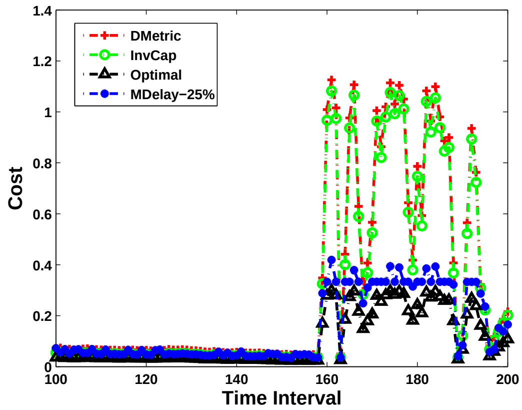
Evaluation Results:

This part compares the cost of the different algorithms versus the time interval in the Internet2 topology. Each time interval spans five minutes traffic matrix, starting from 8 AM (interval 100) in the morning to 5 PM (interval 200) in the afternoon. Based on this scale on hour period is represented by 12 intervals, each expanding for 5 minutes. Figure 6.4 shows the cost of using each method during the 4 different days of the Abilene traces. The days are extended from the one with the relatively steady traffic without having sudden and unexpected traffic spikes (April 9, Figure 6.4(a)) to the ones with the sudden increases in traffic demands during different times of the day (April 10, 12 and 14, Figure 6.4(b),(c) and (d)).

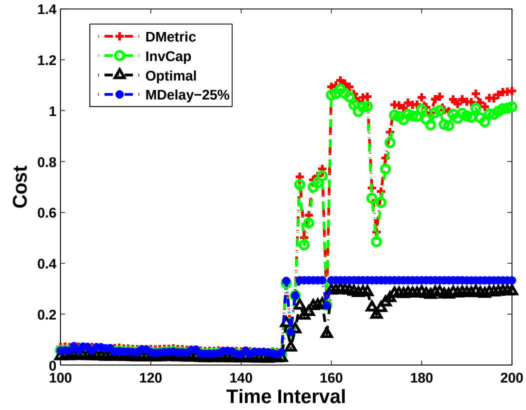
As shown in Figure 6.4(a), on April 9 the network has steady-state traffic demands with a very low network utilisation. Note that unlike Figure6.4(a) where the maximum cost is extended upto the 0.09, the other figures have a maximum cost of more than one. The reason of selecting lower unit in Figure6.4(a) is to highlight the drawback of the proposed scheme more clearly. The average optimal cost is less than 5% and there is no bottleneck link in the network at a given level of traffic. Conceivably, DMetric has the highest cost followed by the MDelay and InvCap. For the proposed scheme (MDelay), it is assumed that 25% of the total traffic between each node pair is for multimedia traffic and the rest is data. The result shows that when the network utilisation is very low, the cost of the proposed scheme is close to the InvCap and its worst-case cost does not exceed the one obtained by the DMetric. The result obtained is expectable. When the



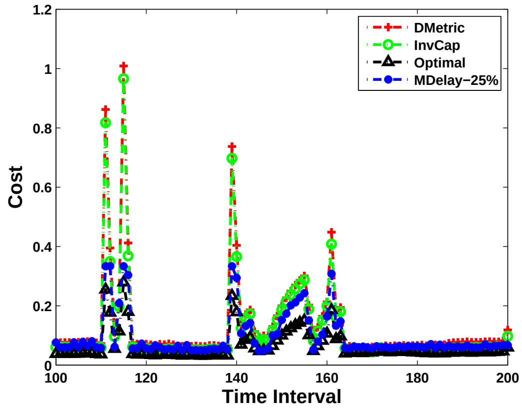
(a) Friday, April 9



(b) Saturday, April 10



(c) Monday, April 12



(d) Wednesday, April 14

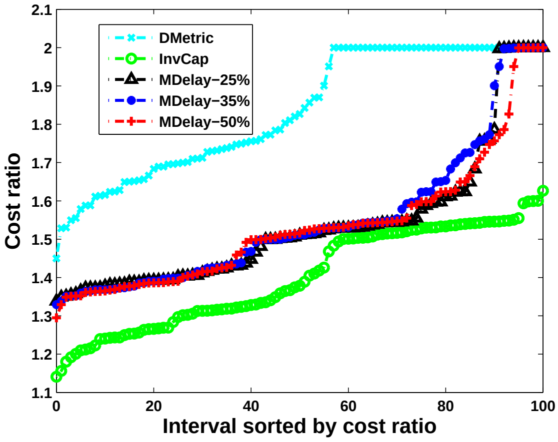
Figure 6.4: Time interval plots of cost, Abilene traces

network is highly over-provision for a given traffic demand, forcing some parts of traffic to follow the longest path would increase the cost in the network.

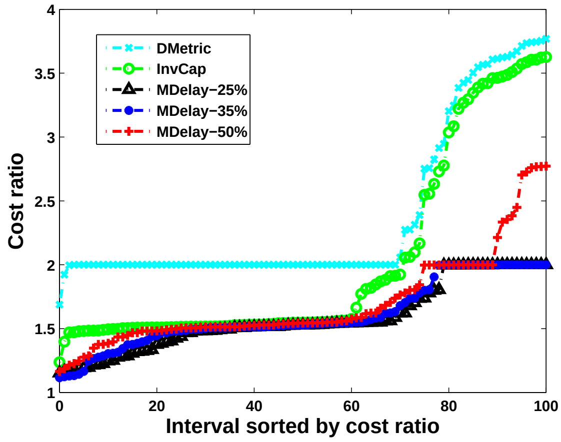
Next the performance of algorithms when the network experiences sudden and unexpected traffic spikes several times in a day, as is the case for the rest of the days in Figure 6.4, is evaluated. To make it more clear, few intervals in the day are focused. As shown in Figure 6.4(b), the network suffers sudden peak in the traffic at interval 161, increasing the optimal cost to almost 30%. Both DMetric and InvCap drive the traffic intensity of the bottleneck link to be 100% more than the optimal value, resulting in a three-fold increase in their costs (according to the cost function defined in Equation (6.3)). However, it is interesting to observe that the proposed scheme (MDelay) can achieve close to optimal performance.

Next, the cost ratio of the algorithms with respect to the optimal cost as a baseline is evaluated. Moreover, it is of interest to analyse the effect of increasing the multimedia share of the total traffic on the proposed scheme performance. Therefore, the cost ratio of the MDelay with the multimedia share of the total traffic to be equal to 25, 35 and 50 percent of the demand between each node pair is studied. Figure 6.5 depicts the results of all 4 days. The time intervals are sorted in the ascending order of the cost ratio. It is worth noting that for DMetric and InvCap the worse cost ratios (the ones with the higher values) belong to the intervals when the network experiences the sudden traffic spikes (e.g. interval 161 on April 10) or high link utilisation (e.g. interval 180 on April 12). However, in the proposed scheme the majority of worse performance ratios happen during the times when the network is highly in the over-provision state and predictable. Results also show that the proposed scheme performs well under increasing the multimedia share of the total traffic (Figure 6.5, MDelay-25%, MDelay-35% and MDelay-50%).

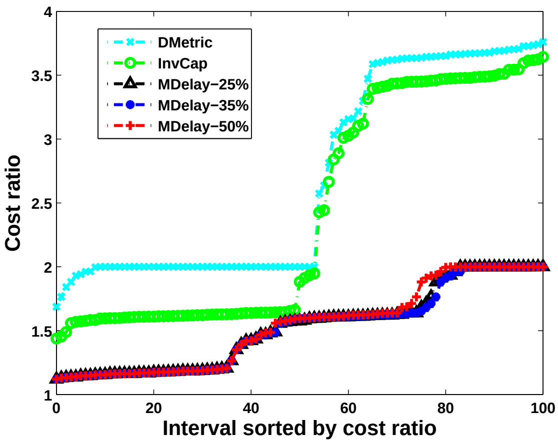
The results indicate that except for the time when the network is highly underutilised (e.g. on April 9), the proposed scheme outperforms other algorithms while at the same time tries to comply with the delay requirements of each flow. This makes the scheme more competent for future Internet with the multimedia real-time traffic being deemed to be dominant. Forcing flows to chose the longest acceptable paths and keeping the shortest path for the most eligible traffic can alleviate the effect of heterogeneous and bursty nature of multimedia traffic.



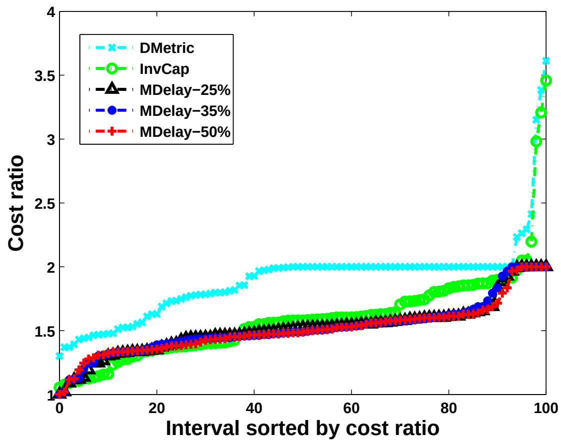
(a) Friday, April 9



(b) Saturday, April 10



(c) Monday, April 12



(d) Wednesday, April 14

Figure 6.5: Time interval plots of cost ratio, Abilene traces

The summary of the cost ratio is given in Figure 6.6. The figure compares the algorithms, including the proposed scheme with different percentages of multimedia traffic, from April 9 until April 14. The time intervals are sorted in ascending order of the cost ratio. The result indicates that even by increasing the share of multimedia traffic, the proposed scheme can perform well.
Going through all outcomes of experiments, the following conclusions can be made: (i) the proposed scheme is good at optimising the unexpectable traffic spikes or heavy traffic demands between pairs, (ii) it can achieve an acceptable performance under a highly over-provisioning network due to low traffic demands, (iii) it takes into account the QoS based requirements of the flow.

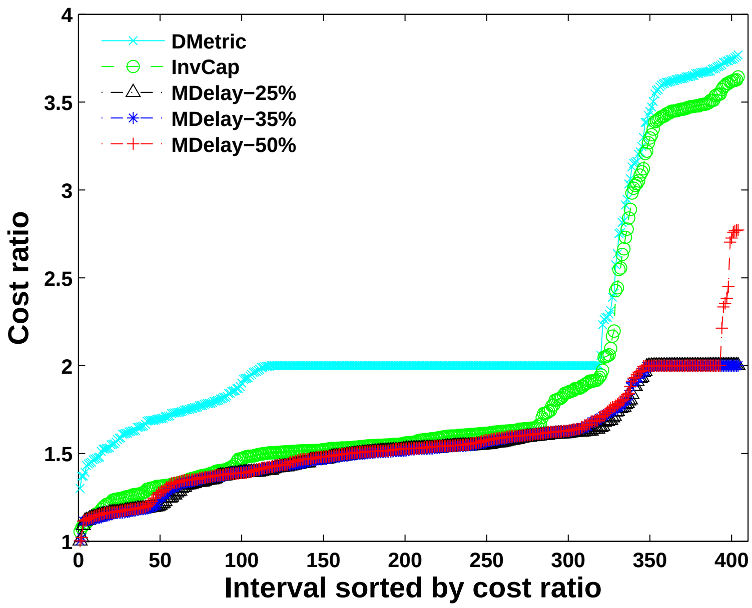


Figure 6.6: Cost ratio of Abilene between April 9-14

6.7 Summary

In this chapter, a new traffic engineering approach based on multi-topology routing was proposed. The proposed scheme provided the efficient load distribution in an IP network. Exploiting the multi-topology routing protocols, the scheme forces the traffic to go through the *longest acceptable* path, sparing the shortest paths for the most legitimate traffic, the one with the tight SLA requirements. The simulation results, based on the Internet2 routing-level topology and traffic matrices, showed that the proposed scheme can be a competent approach for future networks, with the multimedia traffic being dominant and in severe needs of the QoS based routing approaches.

Chapter 7

Conclusions and Future Work

7.1 Concluding Remarks

This thesis has proposed a new mechanism that provided an end-to-end QoS provisioning in mobile networks. The proposal was of two tiers in which the lower tier concentrated on the QoS guarantees in access networks, while the other focused on the QoS-aware routing in backbone networks. The main objectives of this design have been to not only tackle the inefficiency of QoS signalling protocols, i.e., RSVP and NSIS, in mobile environments, but provide an efficient QoS-aware routing of flows, with the objective of minimising network congestion, in backbone networks. The mechanisms proposed are independent from each other, and therefore, can be applied separately or in combination. The breakdown of the major contributions can be listed as follows:

- An efficient RSVP mobility support mechanism in Hierarchical Mobile IPv6 (HMIPv6) networks was proposed. The architecture of the scheme, in terms of the mobility management and resource reservation, are elaborated in detail. The results obtained showed that not only does the scheme reduce the signalling overhead, but also the interruption in QoS at the time of handover.

- An efficient QoS-aware routing, based on the multi-topology routing approach, was proposed. New algorithms are introduced. To evaluate the degree of sub-optimality in the proposed scheme, an optimisation framework is presented that intends to minimise the cost of congestion in the network, subject to newly defined constraints in compliance with the proposed mechanism.

Of the two, the first proposed technique, which is applicable to access networks, intended to improve the efficiency of QoS-enabled mobility management, with a light change in the existing infrastructure and protocols. It aimed to minimise the signalling overhead, as well as the interruption in QoS at the time of handover, by localising the QoS re-establishment to the affected parts of the path in the domain. To that end, the proposed architecture was comprised of the multi-layer mobility agent in the host-based localised mobility management environment, i.e., HMIPv6-based network, and the pre-configured RSVP tunnel established between them. The former localised the mobility management and resource re-establishment processes to the hierarchically distributed sub-domains, resulting in a decrease of the signalling cost. The latter alleviated the long resource re-establishment latency at the time of handover. The performance of the proposed scheme was thoroughly investigated by means of the developed analytical framework, and the network-level simulation scenario conducted in NS-2. Various figures of merit including the resource re-establishment latency; the network-layer signalling cost and the effect of the number of mobile nodes and their average cell residence time on it; the number of packet loss; and the number of packets treated as a best-effort, were used to verify the efficiency of the proposed scheme. With regards to the core networks related to the second contribution, a new QoS-aware routing, based on the multi-topology routing approach, was introduced. The proposed approach aimed to minimise the cost, in terms of the load on each link, with respect to how to select longest possible routes that comply with the flows' requirements. To that end, heuristic algorithms were presented to extract fully edge-disjoint logical views of a network in which the delay of the longest path is lower than the acceptable upper bound delay. After extracting the topologies, traffic is routed through the longest path that is in compliance with the negotiated SLA. Applying this strategy, the proposed scheme can ensure that the shortest paths in the network are always used by the flows with the tightest requirements. To investigate the performance of the new scheme, the optimisation framework was presented, aiming to minimise the congestion cost of the network subject to

defined constraints. Using a real topology and traffic matrices, the degree of suboptimality was verified. The results obtained showed that the efficient resource utilisation, even under unpredictable traffic spikes, can be ensured, while at the same time the traffic need can be fulfilled by the selected path.
In addition to the main contributions discussed above, this research work provided the following complementary contributions: The applicability of the proposed scheme to the existing QoS and mobility management protocols in a similar context, in particular NSIS and the network-based localised mobility management protocol, was investigated. To that end, the proposed architecture was used to increase the efficiency of the NSIS signalling protocol in the PMIPv6 environment, reducing its long resource re-establishment latency and high signalling cost. The numerical results obtained by means of the analytical model indicated that having multi-layer mobility agent in PMIPv6 with the pre-configured NSIS sessions between them can mitigate the costs imposed by the NSIS rich functionalities.
In order to justify the decision of selecting RSVP as the first choice of this work for QoS signalling in access networks, in spite of presence of the NSIS, the proposed analytical framework was adopted to make a clear comparison of NSIS and RSVP operations in mobile networks. Several metrics, such as the network signalling cost, the amount of bandwidth consumed by signalling messages and the resource re-establishment latency, were thoroughly investigated. The results achieved highlighted the significant costs of using the NSIS appealing features as compared to RSVP. Having these insights, one can get clear insights about the pros and cons of using NSIS in access networks.

7.2 Future Work

In this section, I would like to open the following interesting issues, that among many others, can be continued as future work.

- **New QoS Signalling for Access Networks**
  QoS provisioning in access networks has been a challenging issue in recent years. The vast majority of research has concentrated on extending the existing QoS signalling protocols for QoS provisioning in mobile environments.

However, the lack of an internal mechanism for mobility support in these protocols, which were originally designed in the context of a static environment, always causes sub-optimal performance in mobile networks. To fulfil the stringent demand for high quality for the ever-increasing bandwidth starved applications, there is a great need to have new QoS signalling which considers mobile environment characteristics, at its initial design stage. The lessons taken from the RSVP and NSIS shortcomings in mobile networks can shed light on understanding this path.

- **Traffic Optimisation in Mobile IP networks**
  Using traffic optimisation for QoS provisioning in backbone networks, due to its amount of traffic volume, has become a very intense research field in recent years. However, the deluge of bandwidth-starving applications for mobile users, peaking during the daily commute with 70% usage [122], as well as the upcoming changes in users' traffic types, has opened up a whole new area of challenges not only for backbone networks, but also for access networks. It has been estimated that these changes will lead to the 13-fold increase in global mobile data traffic between 2012 and 2017. While mobile video traffic exceeded 50% of traffic for the first time in 2012, it is expected to increase 16-fold by 2017 [123]. If not foreseen appropriately, the changes in amounts and patterns of traffic can lead to a significant inefficiency of traffic routing in access networks. It is believed that the use of QoS-aware traffic optimisation, in the context of the mobility in IP networks, is a new area with a great scope of innovation. Therefore, applying the optimisation ideas introduced in this thesis to mobile networks, wherein there are areas of congestion created due to the presence of the mobility anchor points, can yield interesting insights.

References

[1] Daily Mail:http://www.dailymail.co.uk/news/article-2297508/Six-world-s-seven-billion-people-mobile-phones–4-5billion-toilet-says-UN-report.html. October 2013. 1

[2] R. Braden, D. Clark, and S. Shenker. Integrated Services in the Internet Architecture: an Overview. RFC 1633 (Informational), June 1994. 2, 8

[3] K. Nichols, S. Blake, F. Baker, and D. Black. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474 (Proposed Standard), December 1998. Updated by RFCs 3168, 3260. 13, 14

[4] L. Zhang, S. Deering, D. Estrin, S. Shenker, and D. Zappala. RSVP: a new Resource ReSerVation Protocol. *Network, IEEE*, 7(5):8 –18, September. 1993. 2

[5] R. Hancock, G. Karagiannis, J. Loughney, and S. Van den Bosch. Next Steps in Signaling (NSIS): Framework. RFC 4080 (Informational), June 2005. 5, 15, 100

[6] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification. RFC 2205, September 1997. 2, 35

[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. RFC 5213 (Proposed Standard), August 2008. 2, 5, 87, 101

[8] C. Perkins. IP Mobility Support. RFC 2002 (Proposed Standard), October 1996. Obsoleted by RFC 3220, updated by RFC 2290. 2, 21

[9] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. RFC 5380 (Proposed Standard), October 2008. 4

[10] X. Fu, H. Schulzrinne, A. Bader, D. Hogrefe, C. Kappler, H. Karagiannis, G.and Tschofenig, and S. Bosch. NSIS: A New Extensible IP Signaling Protocol Suite. *IEEE Communications Magazine*, 43(10):133–141, October 2005. 5

[11] J. Wroclawski. Specification of the Controlled-Load Network Element Service. RFC 2211 (Proposed Standard), September 1997. 8, 9

[12] S. Shenker, C. Partridge, and R. Guerin. Specification of Guaranteed Quality of Service. RFC 2212 (Proposed Standard), September 1997. 9

[13] R.Guérin and V.Peris. Quality-of-service in packet networks: basic mechanisms and directions. *Computer Networks*, 31(3):169–189, October 1999. 10

[14] J. Wroclawski. The Use of RSVP with IETF Integrated Services. RFC 2210 (Proposed Standard), September 1997. 10

[15] P. White. RSVP and integrated services in the Internet: a tutorial. *Comm. Mag.*, 35(5):100–106, May 1997. 10

[16] F. Pana and F. Put. A Survey on the Evolution of RSVP. *Communications Surveys Tutorials, IEEE*, PP(99):1–29, June 2013. 13, 32

[17] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. An Architecture for Differentiated Services. RFC 2475 (Informational), December 1998. Updated by RFC 3260. 13

[18] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski. Assured Forwarding PHB Group. RFC 2597 (Proposed Standard), June 1999. Updated by RFC 3260. 14

[19] D. Grossman. New Terminology and Clarifications for Diffserv. RFC 3260 (Informational), April 2002. 14

[20] B. Davie, A. Charny, J.C.R. Bennet, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis. An Expedited Forwarding PHB (Per-Hop Behavior). RFC 3246 (Proposed Standard), March 2002. 14

[21] J. Manner, G. Karagiannis, and A. McDonald. NSIS Signaling Layer Protocol (NSLP) for Quality-of-Service Signaling. RFC 5974 (Experimental), October 2010. 15

[22] M. Stiemerling, H. Tschofenig, C. Aoun, and E. Davies. NAT/Firewall NSIS Signaling Layer Protocol (NSLP). RFC 5973 (Experimental), October 2010. 15

[23] H. Schulzrinne and R. Hancock. GIST: General Internet Signalling Transport. RFC 5971, October 2010. 17, 32

[24] J. Manner and X. Fu. Analysis of Existing Quality-of-Service Signaling Protocols. RFC 4094 (Informational), May 2005. 19

[25] D. Reid and M. J. Katchabaw. Internet QoS: Past, Present, and Future. *Technical Report, Department of Computer Science, The University of Western Ontario, London, Canada*, June 2004. 19

[26] P. Pan and H. Schulzrinne. YESSIR: a simple reservation mechanism for the Internet. *SIGCOMM Comput. Commun.*, 29(2):89–101, April 1999. 19

[27] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. RFC 3550 (Standard), July 2003. Updated by RFCs 5506, 5761, 6051, 6222. 19

[28] G. Fehér, K. Németh, M. Maliosz, I. Cselényi, J. Bergkvist, D. Ahlard, and T. Engborg. Boomerang – A Simple Protocol for Resource Reservation in IP Networks. In *Proceedings of the IEEE Workshop on QoS Support for Real-time Internet Applications,*, Vancouver, Canada, June 1999. 20

[29] G. Fehér, K. Németh, M. Maliosz, and Cselényi. Performance evaluation framework for IP resource reservation signalling. *Perform. Eval.*, 48(1-4):131–156, May 2002. 20

[30] I.F. Akyildiz, J. Xie, and S. Mohanty. A survey of mobility management in next-generation all-IP-based wireless systems. *Wireless Communications, IEEE*, 11(4):16 – 28, August 2004. 21

[31] Z. Zhu, R. Wakikawa, and L. Zhang. A Survey of Mobility Support in the Internet. RFC 6301 (Informational), July 2011. 21

[32] C. Perkins. IP Mobility Support for IPv4, Revised. RFC 5944 (Proposed Standard), November 2010. 22

[33] C. E. Perkins and D. B. Johnson. Route Optimization for Mobile IP. *Cluster Computing, Special Issue on Mobile Computi*, (1):161–176, 1998. 23

[34] G. Montenegro. Reverse Tunneling for Mobile IP, revised. RFC 3024 (Proposed Standard), January 2001. 23

[35] C. Perkins, D. Johnson, and J. Arkko. Mobility Support in IPv6. RFC 6275 (Proposed Standard), July 2011. 23

[36] S. Thomson, T. Narten, and T. Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862 (Draft Standard), September 2007. 24

[37] R. Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture. RFC 4423 (Informational), May 2006. 27

[38] J. Kempf. Goals for Network-Based Localized Mobility Management (NETLMM). RFC 4831 (Informational), April 2007. 27

[39] A. Terzis, M. Srivastava, and L. Zhang. A simple QoS signaling protocol for mobile hosts in the integrated services Internet. In *INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1011 –1018 vol.3, March 1999. 29

[40] A. Terzis, J. Krawczyk, J. Wroclawski, and L. Zhang. RSVP Operation Over IP Tunnels. RFC 2746, Internet Engineering Task Force, January 2000. 29, 31

[41] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. Resource ReSer-Vation Protocol (RSVP) – Version 1 Functional Specification. RFC 2205, IETF, September 1997. 30

[42] F. Le Faucheur, J. Manner, D. Wing, and A. Guillou. Resource Reservation Protocol (RSVP) Proxy Approaches. RFC 5945, Internet Engineering Task Force, 2010. 31, 102

[43] C. Shen, H. Schulzrinne, S. Lee, and J. Bang. NSIS Operation over IP Tunnels. RFC 5979 (Experimental), March 2011. 31

[44] T. Sanda, X. Fu, S. Jeong, J. Manner, and H. Tschofenig. NSIS Protocol Operation in Mobile Environments. RFC 5980 (Informational), March 2011. 32, 100

[45] A-E M. Taha, H.S. Hassanein, and H.T. Mouftah. Extensions for Internet QoS paradigms to mobile IP: a survey. *Communications Magazine, IEEE*, 43(5):132–139, 2005. 32

[46] A.K. Talukdar, B. R. Badrinath, and A. Acharya. MRSVP: a resource reservation protocol for an integrated services network with mobile hosts. *Wirel. Netw.*, 7:5–19, January 2001. 33

[47] C. Tseng, G.L. Lee, and R. Liu. HMRSVP: a hierarchical mobile RSVP protocol. In *Distributed Computing Systems Workshop, 2001 International Conference on*, pages 467 –472, April 2001. 33

[48] W. Chen and L. Huang. RSVP Mobility Support: A Signaling Protocol for Integrated Services Internet with Mobile Hosts. In *INFOCOM*, pages 1283–1292, 2000. 34

[49] H. Wang, D.I. Laurenson, and J Hillston. A Reservation Optimised Advance Resource Reservation Scheme for Deploying RSVP in Mobile Environments. *Wirel. Pers. Commun.*, 54:251–275, July 2010. 34

[50] A. Belhoul, Y. Ahmet Şekercioğlu, and N. Mani. Mobility-Aware RSVP: A framework for improving the performance of multimedia services over wireless IP-based mobile networks. *Comput. Commun.*, 32:569–582, March 2009. 35, 65

[51] A. Belhoul, Y.A. Sekercioglu, and N. Mani. WLC40-3: A Mechanism for Enhancing VoIP Performance over Wireless Networks using Embedded Mobility-Specific Information in RSVP Objects. In *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, pages 1–5, 2006.

[52] A. Belhoul, Y.A. Sekercioglu, and N. Mani. Interaction of RSVP and Mobile IPv6 Protocols: An Evaluation of Performance on Wireless Networks. In *Communications, 2006. ICC '06. IEEE International Conference on*, volume 3, pages 973–978, 2006. 35

[53] S. Paskalis, A. Kaloxylos, E. Zervas, and L. Merakos. An efficient RSVP-mobile IP interworking scheme. *Mob. Netw. Appl.*, 8(3):197–207, June 2003. 36

[54] S. Paskalis, A. Kaloxylos, E. Zervas, and L. Merakos. Evaluating the RSVP mobility proxy concept. In *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, volume 1, pages 270 – 274 vol.1, 2002. 37

[55] S. Paskalis, A. Kaloxylos, and E. Zervas. An Efficient QoS Scheme for Mobile Hosts. In *Proceedings of the 26th Annual IEEE Conference on Local Computer Networks*, LCN '01, pages 630–, Washington, DC, USA, 2001. IEEE Computer Society. 36

[56] X.P. Xiao and L.M. Ni. Internet QoS: a big picture. *Network, IEEE*, 13(2):8 –18, March 1999. 38, 41

[57] E. Rosen, A. Viswanathan, and R. Callon. Multiprotocol Label Switching Architecture. RFC 3031 (Proposed Standard), January 2001. Updated by RFC 6178. 38, 39

[58] F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen. Multi-Protocol Label Switching (MPLS) Support of Differentiated Services. RFC 3270 (Proposed Standard), May 2002. Updated by RFC 5462. 40

[59] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus. Requirements for Traffic Engineering Over MPLS. RFC 2702 (Informational), September 1999. 40

[60] V. Sharma and F. Hellstrand. Framework for Multi-Protocol Label Switching (MPLS)-based Recovery. RFC 3469 (Informational), February 2003. Updated by RFC 5462. 40

[61] D. Oran. OSI IS-IS Intra-domain Routing Protocol. RFC 1142 (Informational), February 1990. 40

[62] J. Moy. OSPF Version 2. RFC 2328 (Standard), April 1998. Updated by RFCs 5709, 6549. 40

[63] N. Wang, K. Ho, G. Pavlou, and M. Howarth. An overview of routing optimization for Internet traffic engineering. *Communications Surveys Tutorials, IEEE*, 10(1):36 –56, quarter 2008. 41

[64] E. Crawley, R. Nair, B. Rajagopalan, and H. Sandick. A Framework for QoS-based Routing in the Internet. RFC 2386 (Informational), August 1998. 41, 42

[65] O. Younis and S. Fahmy. Constraint-based routing in the internet: Basic principles and recent research. *Communications Surveys Tutorials, IEEE*, 5(1):2–13, 2003. 41

[66] G. Apostolopoulos, S. Kama, D. Williams, R. Guerin, A. Orda, and T. Przygienda. QoS Routing Mechanisms and OSPF Extensions. RFC 2676 (Experimental), August 1999. 41

[67] Z. Wang and J. Crowcroft. Quality-of-service routing for supporting multimedia applications. *Selected Areas in Communications, IEEE Journal on*, 14(7):1228–1234, 1996. 43

[68] Y. Fang. Movement-based mobility management and trade off analysis for wireless mobile networks. *Computers, IEEE Transactions on*, 52(6):791 – 803, June 2003. 52, 53

[69] I. Akyildiz, J. Ho, and Y. Lin. Movement-based location update and selective paging for PCS networks. *Networking, IEEE/ACM Transactions on*, 4(4):629 –638, August 1996. 53

[70] K.H. Chiang and N. Shenoy. A 2-D random-walk mobility model for location-management studies in wireless networks. *Vehicular Technology, IEEE Transactions on*, 53(2):413–424, 2004. 54

[71] C. Bettstetter. Mobility modeling in wireless networks: categorization, smooth movement, and border effects. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(3):55–66, July 2001. 54

[72] H. Saleet, O. Basir, R. Langar, and R. Boutaba. Region-Based Location-Service-Management Protocol for VANETs. *Vehicular Technology, IEEE Transactions on*, 59(2):917–931, 2010. 55

[73] Y.B. Lin. Reducing location update cost in a PCS network. *Networking, IEEE/ACM Transactions on*, 5(1):25 –33, Februry 1997. 55

[74] I.F. Akyildiz and W. Wang. A dynamic location management scheme for next-generation multitier PCS systems. *Wireless Communications,IEEE Transactions on*, 1:178–189, 2002. 57

[75] C. Makaya and S. Pierre. An Analytical Framework for Performance Evaluation of IPv6-Based mobility Management Protocols. *Wireless Communications, IEEE Transactions on*, 7(3):972 –983, March 2008. 57, 68, 93, 107

[76] J. Xie and U. Narayanan. Performance Analysis of Mobility Support in IPv4/IPv6 Mixed Wireless Networks. *Vehicular Technology, IEEE Transactions on*, 59(2):962 –973, February 2010. 57

[77] J. McNair, I.F. Akyildiz, and M.D. Bender. An inter-system handoff technique for the IMT-2000 system. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, pages 208–216, 2000. 63, 92, 106

[78] S. Murphy. Updated version of RSVP/ns models of Marc Greis. 2003. 65

[79] R. Hsieh. FHMIP ns-extension for Network Simulator. 2007. 65

[80] A. Demers, S. Keshav, and S. Shenker. Analysis and simulation of a fair queueing algorithm. In *Proc. ACM Sigcomm*, pages 3–12, 1989. 65

[81] J. Xie and I.F. Akyildiz. A novel distributed dynamic location management scheme for minimizing signaling costs in Mobile IP. *Mobile Computing, IEEE Transactions on*, 1(3):163–175, 2002. 65, 107

[82] R. Hsieh, A. Seneviratne, H. Soliman, and K. El-Malki. Performance analysis on hierarchical Mobile IPv6 with fast-handoff over end-to-end TCP. In *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, volume 3, pages 2488 – 2492 vol.3, November 2002. 65, 76

[83] R. Hsieh and A. Seneviratne. A comparison of mechanisms for improving mobile IP handoff latency for end-to-end TCP. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, MobiCom '03, pages 29–41, New York, NY, USA, 2003. ACM.

[84] L. Hussien, A. Hashim, A. Hassan, F. Anwar, O. Khalifa, S.A. Hameed, and W. Al-Khateeb. Simulation evaluation of DiffServ approach integrated in MIPv6 networks. *Australian Journal of Basic and Applied Sciences*, 5:386–396, January 2011. 65

[85] L. Cicco, S. Mascolo, and V. Palmisano. Skype video responsiveness to bandwidth variations. In Carsten Griwodz and Lars C. Wolf, editors, *NOSSDAV*, pages 81–86. ACM, 2008. 67

[86] C. Makaya and S. Pierre. An Architecture for Seamless Mobility Support in IP-Based Next-Generation Wireless Networks. *Vehicular Technology, IEEE Transactions on*, 57(2):1209 –1225, March 2008. 67, 68

[87] H. Chaskar. Requirements of a Quality of Service (QoS) Solution for Mobile IP. RFC 3583 (Informational), September 2003. 79

[88] G. Fankhauser, S. Hadjiefthymiades, N. Nikaein, and L. Stacey. RSVP support for mobile IP Version 6 in wireless environments. Technical Report EURECOM, Eurecom, November 1998. 67

[89] S. Pack and Y. Choi. A Study on Performance of Hierarchical Mobile IPv6 in IP-based Cellular Networks. *IEICE Transactions*, E87-B(3):462–469, 2004. 68

[90] N. Balakrishnan and Asit P. Basu. *Exponential Distribution: Theory, Methods and Applications*. T&F STM, City, 1996. 68, 93, 107

[91] Z. Ma, K. Wang, and F. Zhang. Network-based Inter-domain handover Support for Proxy Mobile IPv6. draft-ma-netext-pmip-handover-02.txt, work in progress, 2012. 87, 101

[92] G. Lee, S. Gundavelli, and T. Chung. A Performance Analysis on Route Optimization for Proxy Mobile IPv6. In *Communications, 2009. ICC '09. IEEE International Conference on*, pages 1 –6, June 2009. 93

[93] X. Fu, H. Schulzrinne, H. Tschofenig, C. Dickmann, and D. Hogrefe. Overhead and Performance Study of the General Internet Signaling Transport (GIST) Protocol. *Networking, IEEE/ACM Transactions on*, 17(1):158 – 171, 2009. 93, 100, 105, 107

[94] S. Lee, M. Kim, K. Lee, S. Seol, and G. Lee. Seamless QoS Guarantees in Mobile Internet Using NSIS with Advance Resource Reservation. In *Advanced Information Networking and Applications,AINA*, pages 464 –471, March 2008. 100

[95] R. Bless and M. Röhricht. QoS Support for Mobile Users Using NSIS. In *Proceedings of the 8th International IFIP-TC 6 Networking Conference*, NETWORKING '09, pages 169–181, Berlin, Heidelberg, 2009. Springer-Verlag. 100

[96] M. Arumaithurai, X. Fu, B. Schloer, and H. Tschofenig. Performance Study of the NSIS QoS-NSLP Protocol. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1 –6, December 2008. 100, 105, 107

[97] B. Fortz and M. Thorup. Internet traffic engineering by optimizing OSPF weights. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 519 –528 vol.2, 2000. 115, 118

[98] B. Fortz and M. Thorup. Optimizing OSPF/IS-IS weights in a changing world. *Selected Areas in Communications, IEEE Journal on*, 20(4):756 –767, May 2002. 115

[99] H. Wang, H. Xie, L. Qiu, Y. Yang, Y. Zhang, and A. Greenberg. COPE: traffic engineering in dynamic networks. *SIGCOMM Comput. Commun. Rev.*, 36(4):99–110, August 2006. 115

[100] S. Kandula, D. Katabi, B. Davie, and A. Charny. Walking the tightrope: responsive yet stable traffic engineering. *SIGCOMM Comput. Commun. Rev.*, 35(4):253–264, August 2005. 115

[101] N. Wang, K. Ho, and G. Pavlou. AMPLE: an adaptive traffic engineering system based on virtual routing topologies. *Communications Magazine, IEEE*, 50(3):185 –191, March 2012. 116

[102] S. Sundaresan, C. Lumezanu, N. Feamster, and P. Francois. Autonomous traffic engineering with self-configuring topologies. *SIGCOMM Comput. Commun. Rev.*, 41(4), August 2010. 116

[103] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen, and P. Pillay-Esnault. Multi-Topology (MT) Routing in OSPF. RFC 4915 (Proposed Standard), June 2007. 116

[104] T. Przygienda, N. Shen, and N. Sheth. M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs). RFC 5120 (Proposed Standard), February 2008. 116

[105] L. Muscariello, D. Perino, and D. Rossi. Do next generation networks need path diversity? In *Proceedings of the 2009 IEEE international conference on Communications*, ICC'09, pages 2140–2145, Piscataway, NJ, USA, 2009. IEEE Press. 116

[106] S.W. Lee, L. Kuang-Yi, and A. Chen. Energy efficient multi-topology routing configurations for fast failure reroute in IP networks. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 2785–2790, 2012.

[107] D. Tuncer, M. Charalambides, G. Pavlou, and N. Wang. DACoRM: A coordinated, decentralized and adaptive network resource management scheme. In *Network Operations and Management Symposium (NOMS), 2012 IEEE*, pages 417–425, 2012. 116

[108] A. Kvalbein and O. Lysne. How can Multi-Topology routing be used for intradomain Traffic Engineering? In *ACM SIGCOMM Workshop on Internet Network Management 2007*. ACM sigcomm, August 2007. 116

[109] A. Jaron, A. Mihailovic, P. Faucheux, and A.H. Aghvami. QoS-aware Multi-Plane Routing for Future IP-based Access Networks. In *Global Telecommunications Conference (GLOBECOM 2012), 2012 IEEE*, pages 2856 –2860, June 2012.

[110] A. Jaron, A. Mihailovic, and A.H. Aghvami. Introducing Multi-Plane Routing for next-generation all-IP wireless access networks. In *Communications (ICC), 2012 IEEE International Conference on*, pages 2856 –2860, June 2012.

[111] X. Wang, S. Wang, and L. Li. Robust traffic engineering using multi-topology routing. In *Proceedings of the 28th IEEE conference on Global telecommunications*, GLOBECOM'09, pages 6345–6350, Piscataway, NJ, USA, 2009. IEEE Press.

[112] D. Xu, M. Chiang, and J. Rexford. Link-State Routing With Hop-by-Hop Forwarding Can Achieve Optimal Traffic Engineering. *Networking, IEEE/ACM Transactions on*, 19(6):1717 –1730, December. 2011.

[113] J. Wang, Y. Yang, L. Xiao, and K. Nahrstedt. Edge-based traffic engineering for OSPF networks. *Comput. Netw.*, 48(4):605–625, July 2005. 116

[114] A. Nucci, S. Bhattacharyya, N. Taft, and C. Diot. IGP Link Weight Assignment for Operational Tier-1 Backbones. *Networking, IEEE/ACM Transactions on*, 15(4):789 –802, August. 2007. 117

[115] R. Karp. Reducibility Among Combinatorial Problems. In Raymond E. Miller and James W. Thatcher, editors, *Complexity of Computer Computations*, The IBM Research Symposia Series, pages 85–103. Plenum Press, New York, 1972. 121

[116] K. Ahuja, T. Magnanti, and J. Orlin. *Network Flows: Theory, Algorithms, and Applications*. Prentice Hall, Englewood Cliffs, NJ, 1993. 122

[117] Internet2:http://www.internet2.edu/. 125, 126

[118] OWAMP-Internet2 Network IPv4 Latency:http://bwctl.net.internet2.edu/cgi-bin/owamp.cgi. 125

[119] Abilene topology and traffic dataset. `http://www.cs.utexas.edu/~yzhang/`. 125

[120] Cisco. Configuring OSPF. `http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/`. 126

[121] IBM ILOG CPLEX. `http://www.ibm.com/developerworks/downloads/ws/ilogcplex/`. 126

[122] Traffic and Market report:http://www.ericsson.com/. May 2012. 136

[123] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017:http://www.cisco.com. Februry 2013. 136