

On Providing Flow Transparent Mobility Support for IPv6-based Wireless Real-time Services

Qi Shen † Anthony Lo ‡ Winston Seah ‡ Chi Chung Ko †

† Department of Electrical & Computer Engineering, National University of Singapore

10 Kent Ridge Crescent, Singapore 119260

Tel: [+65] 8709264, 8745156; fax: [+65] 7751910

E-mail: qishen@ieee.org, elekoc@nus.edu.sg

‡ Centre for Wireless Communications*

20 Science Park Road, #02-34/37 TeleTech Park, Science Park II, Singapore 117674

Tel: [+65] 8709130, 8709163; fax: [+65] 7795441

E-mail: loanthony, winston@cw.cw.nus.edu.sg

Abstract

With the natural convergence of wireless communications and Internet technology, mobile real-time services such as wireless mobile Internet telephony will be ubiquitous. Since the emerging Third Generation (3G) wireless networks will adopt Internet Protocol version 6 (IPv6), simultaneous Quality of Service (QoS) and mobility support in IPv6 is becoming an imperative need. The Internet Engineering Task Force (IETF) has developed ReSerVation Protocol (RSVP) and Mobile IPv6 to provide IPv6 QoS and mobility support, respectively. However, an integrated and efficient interworking of these two mechanisms is still not present. In this paper, we identify a problem with the existing RSVP and Mobile IPv6 interworking model and consequently define a Flow Transparency concept to solve this problem. We show that a flow transparent mobility scheme is essential in a desired IPv6 QoS with mobility support model. We examine this desired model and illustrate how it overcomes the problem with the existing approach and achieves a more efficient RSVP and Mobile IPv6 integration. Solutions to accomplish the desired model based on the existing infrastructure, as well as their implementation considerations, will also be presented.

Keywords: Internet, QoS, Mobility, IPv6, RSVP, Mobile IPv6, Flow Transparency

1 Introduction

Recent years have seen an apparent trend for the convergence of wireless communications and the Internet. It is envisioned that the Third Generation (3G) network architecture will be based on Internet technology for simultaneous real and non-real time services [1]. Predominant mobile real-time services in the 3G-Internet architecture,

such as wireless mobile Internet telephony, require both Quality of Service (QoS) and mobility support. The Internet Engineering Task Force (IETF) has standardized the ReSerVation Protocol (RSVP) [2] and Mobile IP [3] to support Internet QoS and mobility, respectively. In order to support QoS and mobility simultaneously, there is a need to integrate RSVP and Mobile IP.

A number of studies on interworking of these two protocols can be found in literature. Most of them [4–7] are based on Internet Protocol version 4 (IPv4). However, due to the intrinsic shortcomings in IPv4, such as limited IP addresses, poor accommodation for QoS and mobility, Internet Protocol version 6 (IPv6), also known as Next Generation Internet Protocol (IPng), has been designed by IETF and will be adopted in the emerging 3G wireless network [8]. To provide simultaneous QoS and mobility support for wireless real-time services in IPv6 environment, Chiruvolu et al. [9] recently proposed an RSVP and Mobile IPv6 [10] integration model. Under their model, resources are initially reserved between the Correspondent Node (CN) and Mobile Node (MN) 's original location. Whenever the MN changes its location which incurs a path change, an RSVP signaling needs to be performed end-to-end between the CN and MN's new location to reserve resources for the new path.

A problem with this model is long resource reservation delays and signaling overheads incurred during handoff. Each time an RSVP renegotiation has to be performed end-to-end no matter how significant the handoff affects the path between CN and MN. Before this RSVP renegotiation completes, service degradation could occur due to lack of QoS guarantee in the newly added portion of the path between the CN and MN.

In this paper, we propose a method to automatically limit the handoff RSVP renegotiation process within the newly added portion of the path between CN and MN. Thus, handoff resource reservation delays and signaling overheads can be minimized which in turn minimizes the handoff service degradation. To achieve this, a *Flow Transparency* concept is introduced. With this concept, a

*CWC is a national R & D center funded by Singapore National Science and Technology Board.

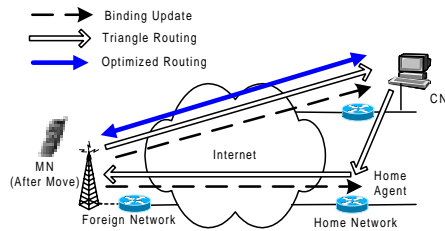


Figure 1: The Mobile IPv6 Architecture

more efficient IPv6 RSVP and Mobile IPv6 integration model which features a better exploitation of existing protocol features is proposed. Solutions to achieve this model, as well as implementation considerations are also presented. It is worth noting that, the Flow Transparency concept also applies to IPv4, but it fits more naturally in IPv6 context due to IPv6 enhanced flow handling capability.

The rest of the paper is organized as follows. Section II summarizes Mobile IPv6 and RSVP. Section III identifies the problem in the existing IPv6 QoS with mobility support model. Section IV contains our proposed IPv6 QoS with mobility support model. Section V provides our solutions to achieve this model. Finally section VI concludes the paper and presents future work.

2 Background

2.1 Mobile IPv6

The Mobile IPv6 [10] architecture is shown in Figure 1. A MN is assigned a permanent *home* address at its Home Network. When the MN moves to a Foreign Network, it obtains a *care-of* address and performs address update with its Home Agent at its Home Network by sending Binding Update. The Home Agent is responsible for maintaining an association between the MN *home* address and current *care-of* address; intercepting packets destined to MN *home* address and forwarding them to MN's current *care-of* address. In this way, MN can always be reached by its *home* address. One important feature of Mobile IPv6 is its integration of Route Optimization [11] functionality. With Route Optimization, when a MN obtains a *care-of* address, it sends Binding Update not only to its Home Agent but also to its CNs. This allows the CN to communicate directly with the MN without going through the MN's Home Agent, and thus eliminates the "triangle routing" problem in the base Mobile IPv4 protocol [3].

2.2 RSVP with IPv6 Flow Label Support

RSVP [2] is a receiver initiated, simplex resource reservation setup protocol used to request specific network QoS for applications. RSVP defines a Session to be a data flow with a *flow destination* and transport-layer protocol. The basic RSVP signaling process for a data flow involves the exchange of *Path* and *Resv* messages as illustrated in Figure 2.

Once resources have been reserved for a flow, the packet classifiers in the routers pick out packets belong to the

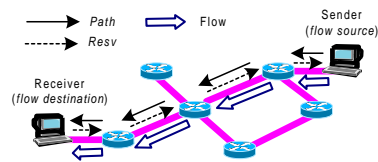


Figure 2: The IPv6 RSVP Mechanism

specific flow to receive special handling according to their QoS requirements. This classification is facilitated by the new *flow label* [12] field in IPv6 header *Flow label* support allows packets to be classified based on *flow source* and *flow label*, which is more efficient compared with that of IPv4 RSVP and avoids the layer-violation problem [2,13].

RSVP contains many features among which the following three are most related to our work. Firstly, RSVP uses a *Soft-state* mechanism which requires periodic state refresh to maintain the active reservation. Secondly, RSVP contains a *Local Repair* mechanism used to adapt to the route change. Lastly, RSVP has a *Merge* functionality which is used to reduce signaling overheads.

3 Problem in the Existing IPv6 QoS with Mobility Support Model

The existing IPv6 QoS with mobility support model [9] is shown in Figure 3. A router is responsible for multiple cells. An IP level handoff only takes place when the MN crosses two cells which belong to different subnets. The Mobile IPv6 and RSVP interworking can be illustrated with a typical wireless mobile Internet telephony application. Both telephony parties are mobile and have wireless access to the Internet. A major challenge in this model is the handoff problem. As far as handoff is concerned, we may consider one party as CN and the other party as MN without losing any generality because during a telephony session, both parties function symmetrically, i.e., both as Sender and Receiver.

The main idea of Mobile IPv6 and RSVP interworking is to use RSVP to reserve resources along the direct path between the CN and MN without going through their Home Agents since Mobile IPv6 has Route Optimization. Whenever the MN performs a handoff which incurs a path change, a new RSVP signaling process must be invoked immediately to reserve resources along the new path, instead of waiting for the next periodic RSVP state update associated with RSVP *Soft-state* mechanism. In Figure 3, when the MN performs a handoff from subnet A to subnet B, it obtains a new *care-of* address and subsequently sends a Binding Update to the CN. The CN then triggers a *Path* message (Message 1) associated with the new flow from CN to MN. Upon receiving this *Path* message, the MN replies with a *Resv* message (Message 2) immediately to reserve resources for the new flow.

In this model, the RSVP Session and the *flow destination* are identified by the MN *care-of* addresses. Therefore, both Session and flow identity changes whenever the MN obtains a new *care-of* address during handoff although the application level session is the same. For each

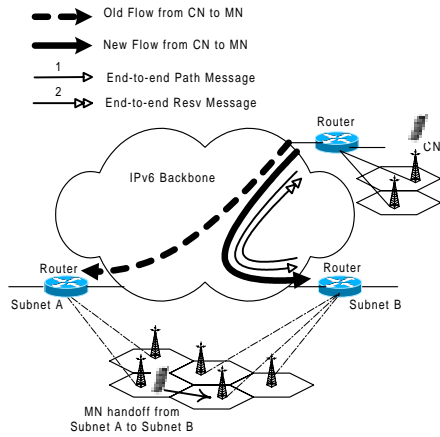


Figure 3: Existing IPv6 QoS with Mobility Support Model

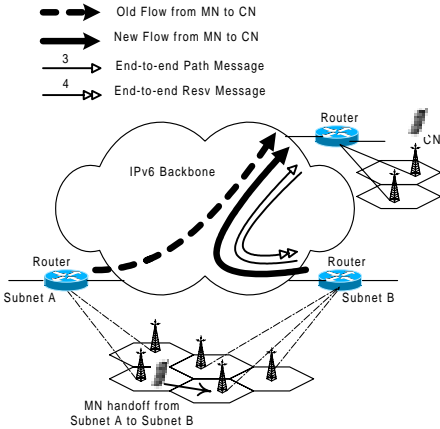


Figure 4: Extended IPv6 QoS with Mobility Support Model

handoff, the MN as receiver has to wait for a new *Path* message from the CN and only after that it can issue a new *Resv* message to the CN. All these RSVP renegotiations have to be conducted **end-to-end** even though the path change may only affect a few routers within the whole path during a single handoff. The long handoff resource reservation delays and large signaling overheads caused by this end-to-end RSVP renegotiation process could lead to notable service degradations because during this period, there might not be enough resources in the newly added portion of the flow path between CN and MN.

For interactive services such as Internet telephony, the MN acts as both Sender and Receiver. It is not difficult to extend the above model to accommodate Sender mobility as well which is shown in Figure 4. When MN is functioning as a Sender and performs a handoff from subnet A to subnet B, it obtains a new *care-of* address and consequently sends to the CN a *Path* message (Message 3) associated with the new flow from MN to CN. Upon receiving the *Path* message, the CN replies with a *Resv* message (Message 4) to reserve resources for the new flow.

Unfortunately, this process suffers exactly the same problem as when MN is a Receiver. Since change of MN *care-of* address during each handoff changes the *flow source* identity, multiple network layer flows are required to support one application data flow during node mobility. RSVP renegotiation must be performed **end-to-end**

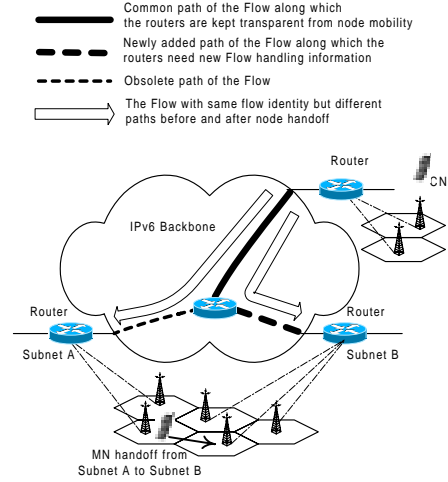


Figure 5: Flow Transparency Concept

during each handoff which causes long resource reservation delays and large signaling overheads.

4 Flow Transparency Concept and Desired Model

In the previous section, we identified the problem in the existing IPv6 QoS with mobility support model, namely, long resource reservation delays and large signaling overheads are introduced during each node handoff which could cause notable service degradation. The main cause of this problem is that RSVP and Mobile IPv6 are originally developed independently and thus lack of intrinsic collaboration; a direct combination of the two can not lead to optimized interworking. Consequently, a desired model should be able to minimize handoff resource reservation delays and signaling overheads through a more efficient integration of RSVP and Mobile IPv6.

4.1 Flow Transparency Concept

Node mobility incurs change of node address and in turn change of flow identity with MN as source or destination. This results in the same application data flow being perceived as different flows at the network layer. Since router processing needs to be based on flow, each time a flow change at the network layer makes it necessary to rebuild information in all intermediate routers along the flow path. A natural idea of solving this end-to-end renegotiation problem is, the routers which reside in the common portion of the new and old flow path should be exempted from performing handoff update; and only those routers that are in the newly added portion of the flow path need to be involved in the update process. This requires the underlying mobility support protocol to keep the node mobility completely *transparent* to the network layer flow handling mechanism. Similar to the Transport Layer Protocol Transparency concept [14] which keeps node mobility invisible to transport layer protocols, we define this transparency at the network layer as *Network Layer Flow Transparency* which is illustrated in Figure 5. The figure shows only the flow from CN to MN, Flow Transparency

for the opposite flow from MN to CN can be similarly achieved. It is important to note that with node mobility, the number and identity of routers involved in the same flow are dynamic and usually unpredictable. Only the routers that are common to both new and old path of the flow constitute the scope of Flow Transparency. This implies that an automatic flow handling adaptation mechanism for those routers in the newly added path is also required in order to exploit the Flow Transparency concept. The major advantage of Flow Transparency is that it allows the network layer flow handling mechanism to function normally regardless of node mobility which in turn brings about performance improvements for mobile QoS mechanism. The essence of providing Flow Transparency is to maintain a unique flow identity irrespective of the change of MN address.

4.2 Desired IPv6 QoS with Mobility Support Model

With the Flow Transparency concept defined, we propose a desired IPv6 QoS with mobility support model based on RSVP and a *flow transparent* Mobile IPv6. In this section we describe the basic mechanism of this model and we will provide solutions to augment Mobile IPv6 with flow transparency capability in the next section. A flow transparent Mobile IPv6 always keeps a constant *flow source* and *flow destination* for a specific application data flow so that the RSVP Session and the network layer flow identity are constant for the router flow handling mechanism (e.g., the packet classifier) regardless of node mobility. Figure 6 shows a similar architecture as in the existing model and the MN performs a handoff from Subnet A to Subnet B. Two scenarios are discussed. In the first scenario, the MN acts as a Sender, and in the second, the MN acts as a Receiver.

Scenario 1: Mobile Node As Sender

If the MN is acting as a Sender, it immediately triggers a *Path* message (Message I) to the CN - with the same source flow identity as the one before handoff. According to the *Merge* functionality of RSVP, this *Path* message will be merged at a router where there is already a *Path* state for that flow which is created during previous RSVP message exchanges. In this case, the router where merge occurs is also the nearest router common to both the old and new path (*Nearest Common Router*) for the flow from MN to CN. It sees the same *Path* message arriving with a previous hop address that differs from the one stored in the original *Path* state. This is exactly the condition RSVP needs to trigger a *Local Repair* for Sender route change, which is actually due to Sender mobility. So it will immediately send a *Resv* message (Message II) associated with that flow to reserve resources along the newly added path to the MN. It is important to note that all handoff *Path* and *Resv* message exchanges only involve routers within the newly added path and only these routers need to perform handoff update.

Scenario 2: Mobile Node As Receiver

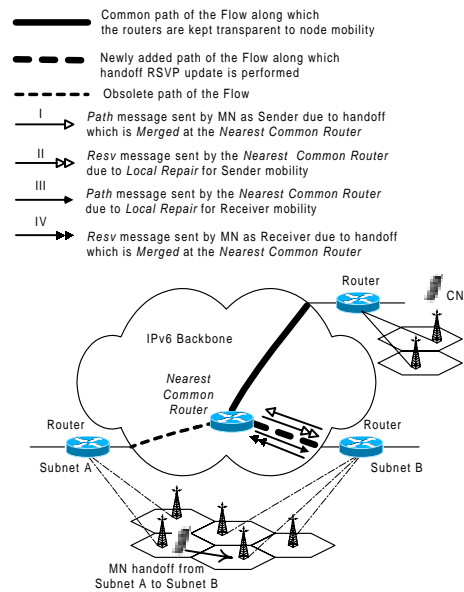


Figure 6: Desired IPv6 QoS with Mobility Support Model

The situation becomes more complicated when the MN is acting as a Receiver because RSVP functions asymmetrically for Sender and Receiver. Firstly, RSVP does not allow a Receiver to send *Resv* message before the associated *Path* message is received while it is not desirable to wait for an end-to-end *Path* message from the CN during each handoff. Secondly, although RSVP can detect Sender route change and trigger *Local Repair* for Sender automatically, it relies on extra mechanism to detect Receiver route change to trigger *Local Repair* for Receiver. The first problem is solved by letting the *Nearest Common Router* issue a *Path* message to the mobile Receiver. With the flow transparent mobility support, the information required for this *Path* message already exists in the *Nearest Common Router* during the previous RSVP message exchanges. Solving the second problem needs some minor extensions to RSVP. The Receiver should be able to inform the *Nearest Common Router* of its handoff information, which contains the *flow destination* and the MN's current address. The *flow destination* identifies the RSVP Session and is used to determine which *Path* message to send and the MN current address is used to determine where to send the *Path* message.

This handoff information may either be carried in a separate message if MN acts solely as a Receiver, or it can be piggybacked in the *Path* message sent by MN itself for Sender mobility if the MN acts as both Sender and Receiver. In both cases, the message containing this information only needs to traverse as far as the *Nearest Common Router* where there is existing RSVP state information for the flow from CN to MN. Figure 6 shows the second case, the MN mobility information is piggybacked in the *Path* message (Message I) sent by MN due to Sender mobility. Upon receiving this *Path* message, the *Nearest Common Router* will trigger a *Local Repair* mechanism for Sender mobility as described above, i.e., sending Message II. Then it also triggers *Local Re-*

pair for Receiver route change which is actually due to Receiver mobility. Specifically, it immediately sends to the MN a *Path* message (Message III) for the flow from CN to MN. Upon receiving this *Path* message, the MN replies with a *Resv* message (Message IV) to reserve resources along the newly added path. Again because of RSVP *Merge* functionality, this *Resv* message will not be forwarded farther than the *Nearest Common Router* since there is already a reservation for this flow made from that router onwards during the previous RSVP message exchanges. Hence, all the *Path* and *Resv* message exchanges due to Receiver mobility only involve routers in the newly added path and only these routers need to perform handoff update.

In conclusion, the *Flow Transparency* concept enables the above model to automatically limit handoff update only to the routers in the newly added path by exploiting two existing RSVP functionalities, *Merge* and *Local Repair*. The handoff RSVP signaling messages are nicely *Merged* at the appropriate place to minimize signaling overheads; and the *Local Repair* operation enables a fast RSVP response to handoff and results in minimized handoff resource reservation delays. As a consequence, this model obtains a natural RSVP mobility adaption through a more efficient integration of RSVP and Mobile IPv6 than the existing one which requires end-to-end RSVP renegotiation during each handoff.

5 Proposed Solutions and Implementation Considerations

5.1 Proposed Solutions

We have shown in the previous section the role of a flow transparent mobility scheme is fundamental in the desired IPv6 QoS with mobility support model. Current Mobile IPv6, although supporting Transport Layer Protocol Transparency, does not contain the notion of Network Layer *Flow Transparency*. Based on the essence of Flow Transparency, i.e., a unique flow identity should be preserved regardless of node mobility, we investigate how Mobile IPv6 can be augmented with flow transparent mobility support capability. Both scenarios, when MN acts as Sender and as Receiver, are examined below.

Scenario 1: Mobile Node as Sender

When MN is acting as a Sender, it characterizes the *flow source*. To maintain Flow Transparency, the *flow source* should be unique during node mobility. It is achieved by representing the *flow source* by the MN *home* address instead of its ever-changing *care-of* address. Specifically, MN should put its *home* address in the *sender template* field [2] of RSVP *Path* messages, and subsequent *Resv* messages sent by the Receiver will also use MN *home* address in the *filter spec* field [2]. Along with this change, the router should also be able to perform packet classification for the flow based on MN *home* address. However, current Mobile IPv6 [10] specifies a special processing about the MN *home* address for packets origi-

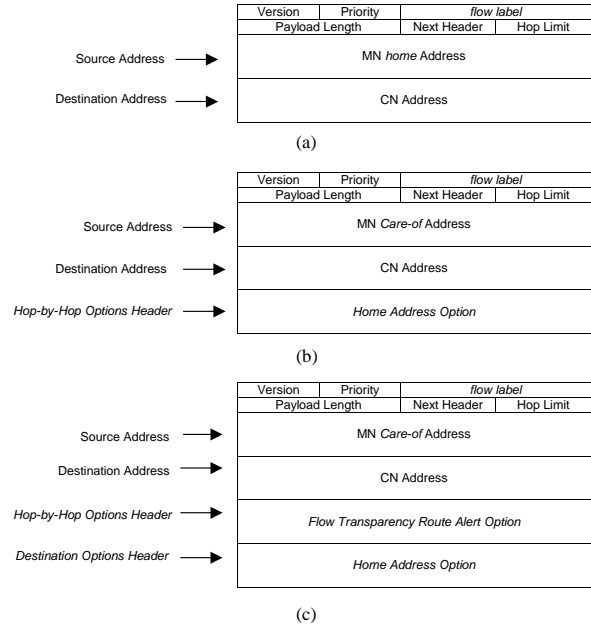


Figure 7: (a) Approach I; (b) Approach II; (c) Approach III

nated from a MN, i.e., the source address of these packets is set to MN *care-of* address and the MN *home* address is moved into a *Home Address Option* in a *Destination Options Header*. Since the *Destination Options Header* is not processed by intermediate routers during packet transmission, only changing the *flow source* to be MN *home* address causes problem for router packet classification. We propose three approaches to address this problem.

Approach I: As shown in Figure 7(a), when Flow Transparency is needed, the mobile Sender should ignore the Mobile IPv6 special processing on its *home* address and set its *home* address as packet source address directly.

Approach II: As shown in Figure 7(b), Mobile IPv6 should move the MN *Home Address Option* from *Destination Options Header* to the *Hop-by-Hop Options Header* when Flow Transparency is needed. This makes the MN *home* address visible to each intermediate routers. Routers are required to perform packet classification based on the MN *home* address.

Approach III: A new *Route Alert Option* [15] indicating the requirement for flow transparent operation can be defined. As shown in Figure 7(c), this option is carried in the *Hop-by-Hop Options Header* of IPv6 packet and the current Mobile IPv6 special processing about MN *home* address is kept intact. Upon receiving this option the router should look for the MN *home* address to perform packet classification.

Scenario 2: Mobile Node as Receiver

When MN is acting as a Receiver, it characterizes the RSVP Session and *flow destination*. To maintain Flow Transparency, this RSVP Session and *flow destination* should be unique during node mobility.

It is achieved by identifying the RSVP Session based on the MN *home* address instead of its *care-of* address. Specifically, the MN *home* address should be used in the *session object* [2] of RSVP messages. It should be noted that for packets destined to MN, Mobile IPv6 also hides the MN *home* address from all intermediate routers. IPv6 RSVP with *flow label* support, however, allows processing of packets solely based on *flow source* and *flow label* without examining the Session.

5.2 Implementation considerations

For flow transparent mobility support in the case of MN acting as Sender, Approach I is the easiest of the three approaches and also introduces no extra operation overheads. However, it may cause problems with certain security mechanisms such as “Ingress filtering [16]”. Therefore, if the current “Ingress filtering” technique is deployed, either Approach II or Approach III should be used. The main difference between Approach II and Approach III is that the former requires modification to current Mobile IPv6 while the latter does not.

Implementation of flow transparent mobility support for the case of MN as Receiver is relatively simple and requires no modification to Mobile IPv6 specification due to IPv6 *flow label* functionality.

6 Conclusions and Future Work

In this paper we have examined a fundamental requirement for accommodating real-time services in the emerging 3G-IPv6 architecture, specifically, the need for integrated QoS and mobility support in an IPv6 environment. The problem with RSVP and Mobile IPv6 interworking in the existing IPv6 QoS with mobility support model is identified, i.e., although normally a handoff only affects a few routers, an end-to-end RSVP renegotiation must be performed for each node handoff. This problem causes unnecessarily long handoff resource reservation delays and large signaling overheads which could lead to notable service degradations. In solving this problem, we have introduced a *Flow Transparency* concept which requires the mobility support scheme to provide a constant flow identity for an application data flow at the network layer regardless of node mobility. We have illustrated that a flow transparent mobility scheme is essential for a desired IPv6 QoS with mobility support model. This model exploits existing RSVP features to obtain a natural RSVP mobility adaptation and achieve minimized handoff resource reservation delays and signaling overheads, thus results in a more efficient integration of RSVP and Mobile IPv6. We have also presented solutions to accomplish the desired model based on the existing infrastructure and considered their implementation issues. The future work includes performance studies through simulation and comparisons with the existing model.

References

- [1] “3G.IP,” <http://www.3gip.org>.
- [2] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, “Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification,” *RFC 2205*, September 1997.
- [3] C. Perkins, “IP mobility support,” *RFC 2002*, October 1996.
- [4] A.K. Talukdar, B.R. Badrinath, and A. Acharya, “Integrated services packet networks with mobile hosts: architecture and performance,” *Wireless Networks*, vol. 5, no. 2, pp. 111–24, 1999.
- [5] A. Terzis, M. Srivastava, and L. Zhang, “A simple QoS signaling protocol for mobile hosts in the integrated services Internet,” *Proceedings of INFOCOM’99*, pp. 1011–18 vol.3, 1999.
- [6] I. Mahadevan and K.M. Sivalingam, “An experimental architecture for providing QoS guarantees in mobile networks using RSVP,” *Proceedings of Ninth International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC’98)*, pp. 50–4 vol.1, 1998.
- [7] A.K. Talukdar, B.R. Badrinath, and A. Acharya, “On accommodating mobile hosts in an integrated services packet network,” *Proceedings of INFOCOM ’97*, pp. 1046–53 vol.3, 1997.
- [8] B. Fernandes, “3rd Generation cellular,” *US IPv6 summit presentation*, March 2000, <http://www.ipv6forum.com>.
- [9] G. Chiruvolu, A. Agrawal, and M. Vandenhouste, “Mobility and QoS support for IPv6-based real-time wireless Internet traffic,” *1999 IEEE International Conference on Communications*, pp. 334–8 vol.1, 1999.
- [10] D. Johnson and C. Perkins, “Mobility support in IPv6,” *IETF Internet Draft*, April 2000, work in progress.
- [11] C. Perkins and D.B. Johnson, “Route optimization in Mobile IP,” *IETF Internet Draft*, February 2000, work in progress.
- [12] C. Partridge, “Using the flow label field in IPv6,” *RFC 1809*, June 1995.
- [13] S. Schmid, A. Scott, D. Hutchison, and K. Froitzheim, “QoS based real time audio streaming in IPv6 networks,” *Proceedings of the SPIE - The International Society for Optical Engineering*, vol. 3529, pp. 102–13, 1998.
- [14] P. Bhagwat, C. Perkins, and S. Tripathi, “Network layer mobility: an architecture and survey,” *IEEE Personal Communications*, vol. 3, no. 3, pp. 54–64, 1996.
- [15] C. Partridge and A. Jackson, “IPv6 router alert option,” *RFC 2711*, October 1999.
- [16] P. Ferguson and D. Senie, “Ingress filtering: defeating denial of service attacks which employ IP source address spoofing,” *RFC 2267*, January 1998.