# RIPE: Mobile IP 망에서 QoS를 지원하기 위한 RSVP-in-IP 캡슐화 방안

## (RIPE: RSVP-in-IP Encapsulation to Support QoS for Mobile IP Networks)

김 민 규 † 이 숙 헌 †† 박 명 순 †††
(Min-Kyu Kim) (Sookheon Lee) (Myong-Soon Park)

**요 약** 인터넷이 인간 삶의 모든 양상에 영향을 미치게 되면서 중요한 2가지 요구사항이 나오게 되었다. 하나는 멀티미디어 데이타 서비스 지원을 위해 높은 서비스 질(QoS)에 대한 요구이고 또 다른 하나는 유비쿼터스(Ubiquitous) 네트워크 연결을 위한 요구이다. 이러한 2가지 요구사항을 만족시킨다는 것은 인터넷이 이동하는 노메딕(Nomadic) 사용자들에게 멀티미디어 통신 지원을 가능하게 한다는 것이다. 현재 Mobile IP 메커니즘에 RSVP 적용을 통해 이동 사용자들에게 QoS 통신을 지원하는 방안으로 홈 에이전트와 외부 에이전트 사이에 RSVP를 위한 별도의 세션을 두는 방법을 명세화하는 RSVP Tunnel이 제안되었다. 그러나 이 RSVP Tunnel은 중복된 RSVP 메시지 사용으로 인해 터널에서의 대역폭 오버헤드와 메시지들 사이의 관계 문제를 야기 시킨다. 본 논문에서는 이러한 문제를 해결하기 위해 Mobile IP 망에서 효과적으로 QoS를 보장할 수 있는 새로운 캡슐화 방법인 RSVP-in-IP Encapsulation(RIPE)를 제안한다. 제안된 방법은 RSVP Tunnel 방법과 같은 어떠한 세션의 추가없이 효과적으로 Mobile IP 터널링 메커니즘에 RSVP 이동성을 보장할 뿐만 아니라 터널에서의 대역폭 오버헤드 문제와 중복 메시지들 사이의 관계 문제도 해결한다. 성능 평가는 기존 관련연구에서 제안된 RSVP Tunnel과 RIPE에 대해 평균지연, 평균데이타비율, 터널에서의 대역폭 오버헤드 등의 성능지표를 가지고 시뮬레이션을 통해 수행되었다.

**키워드** : QoS, 모바일 IP, RSVP, 캡슐화

***Abstract*** While the Internet keeps its permeation into every aspect of human life, two things stand out. One is the requirement for high quality of services to support multimedia data service. The other is the desire for ubiquitous network connection. Combining the two things makes the Internet possible in supporting multimedia communications for nomadic users on the locomotion. To support QoS communication for mobile users by applying RSVP to Mobile IP, RSVP Tunnel, which specifies building separately a RSVP session between the home agent and the foreign agent, was proposed. However, the RSVP Tunnel method breeds bandwidth overhead and association problems in tunnel because of duplicated RSVP messages use. To resolve these problems, in this paper, we propose the new encapsulation method, the RSVP-in-IP Encapsulation (RIPE) that can support QoS guaranteed service efficiently in Mobile IP networks. The proposed method supports RSVP mobility to Mobile IP tunneling mechanism efficiently without any additional session as the RSVP Tunnel scheme. Moreover it removes the critical problems of bandwidth overhead in a tunnel and association by duplicated messages. We compared the performance of our proposed scheme with RSVP Tunnel scheme in term of mean delay, mean data rate and bandwidth overhead in tunnel.

**Key words** : QoS, Mobile IP, RSVP, Encapsulation

† 학생회원 : 고려대학교 컴퓨터학과
starmin@ilab.korea.ac.kr
†† 비 회 원 : 고려대학교 컴퓨터학과
tonaido@ilab.korea.ac.kr
††† 종신회원 : 고려대학교 컴퓨터학과 교수
myongsp@ilab.korea.ac.kr
논문접수 : 2004년 5월 4일
심사완료 : 2004년 8월 2일

## 1. Introduction

There exists increasingly the number of mobile users who access the Internet over wireless networks for audio, video and other real-time multimedia service. Researches such as Integrated Services[1] or Differentiated Services[2] are cur-

rently in progress to provide environment that supports applications with quality-of-service(QoS) required by the users in wireless networks.

The Internet Integrated Services make it possible for applications to choose the control level of end-to-end delivery services for their data packets. States per packet flow in every router is required and every router also makes admission control and policy control. ReSource reservation Protocol(RSVP) [3] is a signaling protocol that can provide QoS guarantees for integrated services on the Internet.

Mobile IP[4,5] enables a mobile host to move between different IP networks and yet maintain its existing connections without the need to change its IP address to reflect its new point of attachment. This technique does not consider quality of service communication, but if only considers best effort communication. For communication that guarantees QoS for all mobile users, the RSVP protocol for the Internet Integrated Services needs to be support by the wireless network using Mobile IP.

However, RSVP cannot be used directly in a Mobile IP network environment for the following two reasons. First, end-to-end RSVP messages are invisible to the intermediate routers on an IP-in-IP tunnel[6] used in Mobile IP. Second, when the Mobile IP is handed off, new reservation should be made on a new tunnel path. To resolve such a problem, the RSVP Tunnel[7] introduces the QoS reservations over IP-in-IP tunnels where the independent session for RSVP protocol is mapped into a tunnel session between two tunnel end points. However, the use of these duplicated resource reservation signaling messages in RSVP Tunnel may demand too much bandwidth to set up a path and degrade the network performance. In this paper, we introduce an extended IP tunneling mechanism that allows RSVP to make the QoS reservations across all tunnels by using the new proposed RSVP-in-IP Encapsulation (RIPE) without establishing an additional session. The RIPE is an method for encapsulating the RSVP message within the option portion of another packet header to make the message visible for routers on a tunnel.

The rest of this paper is as follows. The background of Mobile IP tunneling, mobility issues of RSVP and RSVP Tunnel mechanism are first presented in section 2. Section 3 describes previous RSVP Tunnel problems, the proposed RSVP-in-IP Encapsulation, and RSVP-in-IP tunneling. The performance evaluation is illustrated in section 4. Finally, conclusions and future work are given in section 5.

## 2. Related works

### 2.1 Mobile IP tunneling

Mobile IP specifies enhancements that allow the transparent routing of IP packets to mobile hosts in wireless networks. Each mobile host is always identified by its home address, regardless of its current point of attachment to a network. When a mobile host moves away from its home network to a foreign network, it obtains a care-of-address, which provides information about its current location of attachment to a network. The mobile host registers with a home agent in its home network to inform the recent of its care-of-address. Data packets addressed to the mobile host are routed to its home network, where these packets are intercepted by the home agent, and then they are sent to the care-of-address toward the mobile host using a process called tunneling. The tunneling has two primary functions: encapsulation[8] of the data packet to reach the tunnel exit point, and decapsulation when the packet is delivered at that exit point. The default tunnel mode is IP-in-IP Encapsulation. Optionally, a Minimal Encapsulation [9] within IP can be used.

To encapsulate an IP packet using IP-in-IP Encapsulation[10], an outer IP header is inserted before the IP header of an existing packet. The outer IP header includes source and destination addresses identifying the entry and exit points of the tunnel. The inner IP header contains source and destination addresses discerning the original sender and receiver of the packet, respectively. The inner IP header is not changed by the encapsulator, except for decrement of the TTL, and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner IP header occurs during transmission of the encapsulated packet through the tunnel. If need be, other

protocol headers such as the IP authentication header may be inserted between the outer IP header and the inner IP header.

The IP-in-IP Encapsulation adds much overhead to its final packet because several fields in the outer IP header are duplicated from the inner IP header. To prevent this waste of space, Minimal Encapsulation has been proposed. In that scheme, instead of inserting a new header, the original IP header is modified to reflect the addressed of the entry and exit points of the tunnel, and a minimal forwarding header is inserted to keep the original source and destination addresses. Thus the care-of-address of the mobile host becomes the destination address of the IP packet and the address of the home agent becomes the source address. When the foreign agent in the tunnel exit point tries to decapsulate, it simply restores the fields in a minimal forwarding header to the IP header and removes the forwarding header.

### 2.2 Mobility issues of RSVP

The RSVP protocol was designed to enable the senders, receivers and routers to communicate with each other in order to set up the necessary router state to support the QoS services. RSVP is a novel signaling protocol in the following ways.

- It uses soft state, which means that it is tolerant of temporary loss of function without imposing fate-sharing between the end systems and the network routers. This means that QoS routing can be deployed separately.
- RSVP is quite straightforward in packet formating and operation, and it is relatively less costly to implement it in end systems and routers.

RSVP is not a routing protocol but is a signaling protocol. It is merely used to reserve resources along the existing route set up by whichever underlying routing protocol is in place. The primary messages used by RSVP are the Path message which originates from the traffic sender and the Resv message which originates from the traffic receivers. The primary roles of the Path messages are firstly, to install reverse routing state in each router along the path and secondly, to provide receivers with information about the characteristics of the sender traffic and end-to-end path so that they can make appropriate reservation requests. The primary role of the Resv message is to carry reservation requests to the routers along paths between receivers and senders. The basic operation of RSVP is as shown in the following steps.

1. When the Path messages are delivered from the senders to receivers, all RSVP capable routers on the path intercept the messages and set the Path states.
2. After the receiver receives the Path message, it should answer with a Resv message containing desired QoS parameters. The Resv messages are delivered back to the senders along the reverse links of the Path messages.
3. If the required resources on all links are available, the soft-state reservations will be established.

The RSVP solves the QoS problem with advanced resource reservation on the Internet. Now, an important trend of the researches about the RSVP support on the Internet is the expansion of accesses to mobile users[11-15]. Mobile phones, PDAs, notebook computers, and various other devices that are easy to carry around all become very popular and ubiquitous. With the help of a wireless infrastructure, it is natural that people want Internet access from these mobile devices. To provide a way for nomadic users to access the Internet seamlessly, the mobile IP explained above in Section 2.1 is proposed. However, although mobile IP can resolve that users can access the Internet wherever they go, as a next step, it needs to provide quality of service communications for the mobile users. Therefore, it is an important research topic to support RSVP mobility efficiently and effectively to provide QoS guarantees for communications over Mobile IP networks. However, two mobility issues occur when the RSVP signaling protocol is adapted to Mobile IP networks.

First, the IP-in-IP Encapsulation technique used by Mobile IP makes RSVP messages invisible to intermediate routers. If the RSVP protocol is applied to Mobile IP tunneling, RSVP message, Path and Resv, will be encapsulated in an IP-in-IP Encapsulated packet with a protocol number 4 in

the outer IP header. The RSVP protocol number 46 in the inner IP header is concealed, and the intermediate routers on the path of an IP tunnel cannot recognize RSVP signals to provide the desired QoS.

Second, RSVP cannot take cognizance of mobility because the resource reservation path cannot be dynamically adapted along with the movement of a mobile host. In other words, once a mobile host moves to a new region, its previous reserved resources are no longer available and the service quality of the mobile host may drop through due to a lack of resources reserved for the mobile host in the new region.

To resolve the mobility issues on RSVP in Mobile IP networks, some schemes have been proposed. Talukdar[16] et al. proposed Mobile Re-Source reserVation Protocol (MRSVP) to resolve the handoff impact of mobility on RSVP by making advance resource reservation. C. Tseng[17] et al. introduced a Hierarchical Mobile RSVP Protocol (HMRSVP) to integrate RSVP with Mobile IP regional registration and makes advance resource reservations only when inter-region movement may happen. The work of G. Lee[18] et al. presents Pointer Forwarding scheme to make advance resource reservations only on a forward one-step path from an mobile host along the forwarding pointer chains. In this paper, we consider RSVP Tunnel proposed by Terzis et al. to resolve the RSVP message invisibility problem.

### 2.3 RSVP Tunnel mechanism

The RSVP Tunnel is the operational method proposed to support resource reservation over IP-in-IP tunnels. The method can solve the problems of router invisibility and RSVP mobility incognizance by separately building a RSVP session between tunnel end points. This RSVP session can exist independently from the tunnel session or it can be triggered by the tunnel session. Figure 1 shows a simple RSVP Tunnel mechanism, in which the senders $S_1$ and receiver $R_1$ are connected with the RSVP session called as a end-to-end RSVP session through a tunnel session between R-entry and R-exit. The R-entry and R-exit make connection with the RSVP session called as a tunnel RSVP session providing resource reservation for the QoS guarantee[19].

Initially, a $S_1$ makes an end-to-end Path message, which is filled with the address of the sender and receiver, and the RSVP protocol number 46 in its IP header. When the end-to-end Path message is delivered to the R-entry of the tunnel entry point, the tunnel R-entry point encapsulates the message with CoA(Care-of-Address), which is the tunnel R-exit point, and sets its type field as the Mobile IP protocol number 4. As soon as sending the encapsulated end-to-end Path message, the tunnel R-entry point issues a new tunnel Path message which records the address of the tunnel R-entry and R-exit points and is set to the RSVP protocol number 46. On receiving the end-to-end Path message, each intermediate router on the path of the tunnel session directly relays the message to

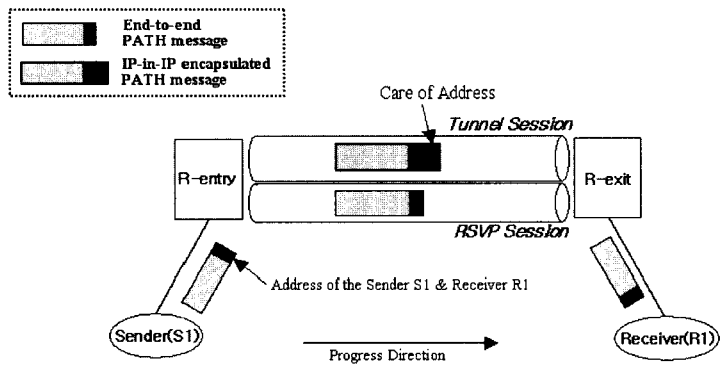


Figure 1 Mechanism of the RSVP Tunnel

the tunnel R-exit point. However, on receiving the tunnel Path message, each intermediate router performs the path finding function as described in the original RSVP protocol because of being visible in this message by the RSVP protocol number 46. When the tunnel R-exit point receives these end-to-end and tunnel Path messages, the end-to-end Path message will be decapsulated and sent to the receiver, while the tunnel Path message will be processed only by the exit point and need not be forward to the receiver. In response, after the end-to-end Path message is arrived to the receiver, it delivers an end-to-end Resv message to the sender. In the same way, when the end-to-end Resv message arrives at the tunnel R-exit point, it will be encapsulated with an IP header as described before and then be forwarded to the sender. The tunnel R-exit point soon makes a tunnel Resv message without encapsulation and sends the message to the tunnel R-entry point. Thus, after the sender and receiver negotiate with the tunnel Path and Resv message, all intermediate routers on the path of the tunnel can reserve the desired resources if sufficient resources are available.

## 3. Proposed Mechanism

In this section, we address the considerable problems of RSVP Tunnel, and to resolve the problems, propose a new encapsulation method which does not need additional packets and bandwidth in tunneling.

### 3.1 Previous RSVP Tunnel problems

Even if RSVP Tunnel can be a solution to provide QoS over IP-in-IP Tunnel, there are two critical problems to solve. One is the problem of association. The RSVP Tunnel defines and uses the association mechanism to do one-to-one mapping between tunnel session and RSVP session. To do this a new RSVP object which includes the identifier and some parameters of the tunnel session is attached to end-to-end RATH messages at R-entry and is interpreted by R-exit. However, one of the RSVP messages in the tunnel or RSVP session can be lost easily in a wireless environment. If there is a lost RSVP message in session, the session is dropped and re-built by the R-entry. It can be a considerable issue when so many mobile hosts use quality of service communications in the network. The other problem is bandwidth overhead in the tunnel. It is obvious that if a great number of mobile hosts move to other subnets, and so their flows in the tunnel are increased, the bandwidth required for the QoS in tunnel will become more than double compared to a tunnel without support of the RSVP Tunnel.

### 3.2 RIPE

We propose here a new type of encapsulation method, RIPE, to provide efficient resource reservation for mobile hosts in wireless networks applying the Mobile IP. Though the use of recursion may solve the problem of RSVP messages being invisible inside the tunnel, the method is also known to have several problems. Using only the existing IP tunnel without an additional tunnel session, having RSVP messages operate efficiently over the IP-in-IP tunnel is one of the feasible solutions for the issues. The typical case is that the RIPE eliminates problems of association between an end-to-end RSVP message and tunnel RSVP message as a mechanism of the RSVP Tunnel. Figure 2 shows a process generated as a new IP packet for an original IP packet.

To encapsulate an original IP packet in the RIPE, the contents of the encapsulation outer IP header are generated by performing a mapping from the original RSVP message to the option portion of the outer IP header. The header portion of the outer IP header records the address of the tunnel entry and exit points. The original IP header is mapped to the data portion of the encapsulation datagram recognized as the payload of the encapsulated RIPE packet by home and foreign agents. The option portion of the encapsulation outer IP header has the resource reservation information for passed routers between end-to-end hosts, and, being dealt in a portion of the header of the final encapsulated packet, can be read for any router which wants to reserve QoS resource. It is a key idea to resolve problem that tunnels make end-to-end RSVP messages invisible to the intermediate routers without using any duplicated messages as the RSVP Tunnel mechanism. The original IP header

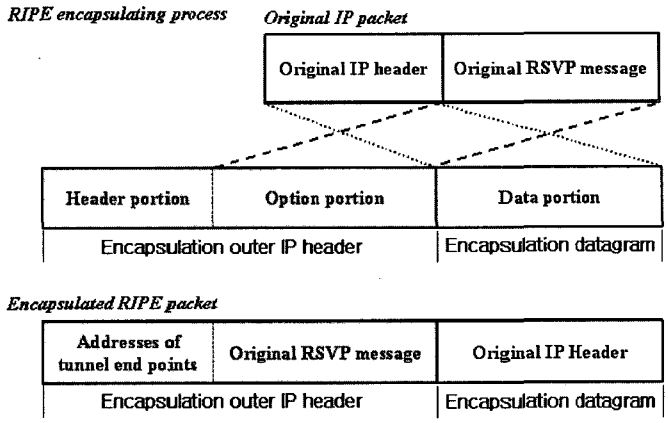


Figure 2 The RIPE packet generation process

in the datagram of RIPE packet is not changed during the tunneling except for decreasing TTL, and also does not make its option be changed up to the tunnel end point. The fields of the encapsulating Outer IP Header are set as follows:

- The Version is set to 4.
- The Type of Service(TOS) bits are copied from the original IP header.
- The Source Address and Destination Address are set to the entry-point and the exit-point of the tunnel, respectively.
- The Internet Header Length(IHL), the Total Length, and the Checksum are recomputed for the encapsulation outer IP header.
- The Identification, Flags, Fragment Offset are set as specified by [RFC 791] for any IP packet.
- The Protocol field is set to 66, which identifies the RIPE protocol, that is, option portion of the encapsulation outer IP header has the RSVP message, and the original IP header is encapsulated to the encapsulation datagram of the RIPE packet.
- The Time to Live field is decremented if the entry-point is routing the original IP packet from some interface to the tunnel interface.

### 3.3 RIPE tunneling

The RIPE packet has an IP header and its option portion, which has the RSVP message, attached in front of the IP datagram. The packet is treated as just a normal IP-in-IP Encapsulated packet at the routers on the tunnel. It is because the form of the RIPE packet is the same as that of a normal IP-in-IP Encapsulated packet. The protocol field in the encapsulation IP header allows intermediate routers to distinguish which encapsulation methods are used for the packets on the tunnel. Flows that do not need QoS reservations inside the tunnel continue to use the IP-in-IP Encapsulation. The tunneling mechanism of the Mobile IP using the RIPE is illustrated in Figure 3.

The home agent will be the tunnel entry point, while the foreign agent will be the tunnel exit point. When the mobile host moves to the network of the foreign agent, it informs the home agent of its new subnet with CoA. The home agent knows about the mobile host's CoA. Thereafter, using the RIPE, the home agent encapsulates end-to-end Path messages with tunnel QoS reservations, while normal IP packets without QoS reservations for a tunnel are IP-in-IP Encapsulated. Intermediate routers in a tunnel forward the packet based upon the encapsulation outer IP header added by the home agent. If there is need of reservation for a tunnel, intermediate routers learn about information related with routes from the option of the RIPE packet header. When the foreign agent receives a Path message from the home agent through the tunnel, and decapsulates it, the header portion of RIPE packet is replaced by the data porion of that packet. The option portion is copied to the data portion of that packet. After the decapsulation processing, the Path message transits it to the

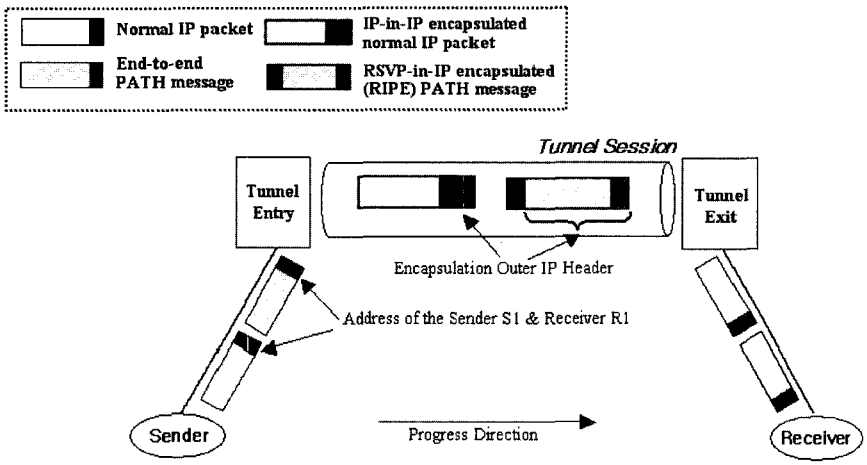


Figure 3 The RIPE tunneling mechanism

mobile host. When the foreign agent receives an end-to-end Resv message from the mobile host, it encapsulates the message within RIPE and sends it to the home agent.

## 4. Performance Evaluation

This section presents the simulation results of the performance analysis for the proposed RIPE. The performance analysis is evaluated by comparing the previous RSVP Tunnel and the proposed scheme. As our simulation tool, the NS network simulator proposed by U.C. Berkeley was used. An extension to the NS basic packet was implemented to support the tunneling mechanism being formed by two modules; the RSVP Tunnel and the RIPE. The two modules were implemented using the C++ and the Otcl languages. The simulation is performed on the side view of the mean delay, the mean throughput by the handoff rate, and the tunnel bandwidth overhead by the number of flows when there is mobile host movement.

### 4.1 Metrics and Methodology

Figure 4 presents a type of topologies used in the simulations. In this topology, we assume that the bandwidths of the link between all nodes are 5Mbps and the all transmission delays on the link from a CH to a HA are set to 10ms. The transmission delays between a HA and FAs are set to 1.5ms because they communicate with each other with tunneling fashion.

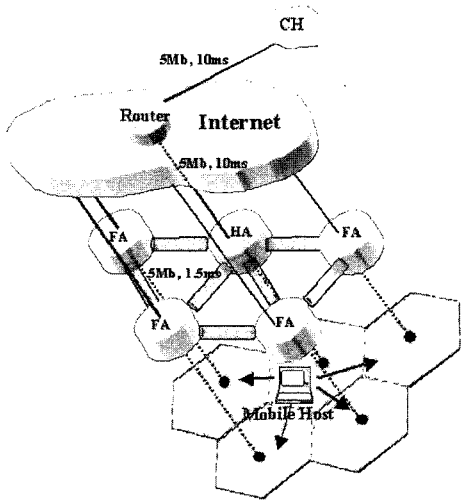


Figure 4 Simulation model

The number of mobile hosts is adjusted to from 1 to 40, and the speed of them is set to be created randomly with 10-50 Km/hour. This speed means a vehicle speed. To measure the performance comparison according to handoff probability, we assume that the mobile host moves randomly in 4 directions among sub-networks according to given handoff rate, and the CH is in a fixed position. During a time unit of the simulation, it is assumed that the CH sends data to the mobile host successfully, and the time taken in this case is calculated by sum of each transmission link delay plus encapsulation and decapsulation processing

time and RSVP path update delay time. The RSVP path update delay happens when a mobile host hands over to a foreign network. To examine the bandwidth overhead in the tunnel, we assume that the number of flows means the number of mobile hosts caused to tunneling by handoffs.

### 4.2 Simulation Results

The simulation result of the mean packet delay is shown in figure 5, where X-axis is the handoff rate and Y-axis is the mean delay. Handoff rate represents probability of that mobile host moves to other sub-networks during given one simulation time. Mean delay represents the average value of delay taken until data arrives at a mobile host from the CH. On the whole, the result shows that the mean delay of both the RSVP Tunnel based scheme and the proposed scheme are increased when the handoff rate is augmented. The reason is that the transmission delay is increased by long tunnel hop counts made as the mobile host moves away from home agent, and when the handoff happens, the packets are delayed due to the path re-establishment.

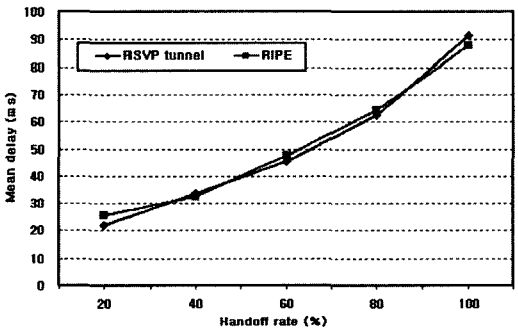


Figure 5 The mean packet delay by handoff rates

Figure 6 shows the simulation results for the mean data transmission rate of a single mobile host using the RSVP Tunnel based scheme and the proposed scheme over simulation time. During the simulation time, each scheme handoffs in different time because the movement of mobile host over the foreign network follows random motion. In this simulation, we can observe that the mobile host can maintain a stable data transmission rate at 65kbps except for the handoff time regardless of which schemes are applied. The phenomenons in figure 5, 6 show that, although RIPE does not use simple copy method as RSVP Tunnel, but uses encapsulating method by packet re-organization, it can still maintain performance as much as RSVP Tunnel.

Figure 7 shows the tunnel bandwidth overhead over the number of flows. As a whole, we can note that reserved tunnel bandwidth overhead is augmented according to an increase of the flow numbers, and until numbers are 15 flows, overheads of both schemes are almost the same. However, bandwidth overhead in the tunnel using the RSVP Tunnel based scheme is increased from 15 flows by exceeding difference comparing with the proposed scheme. The reason is that both schemes reserve more much bandwidth for QoS guarantee according as the number of flows increase, but, in case of the RSVP Tunnel, another session for messages copied from original RSVP messages is demanded in tunnel, and it makes total bandwidth overhead increase.

As a result, the proposed scheme provides similar performance between the mean delay and data rate

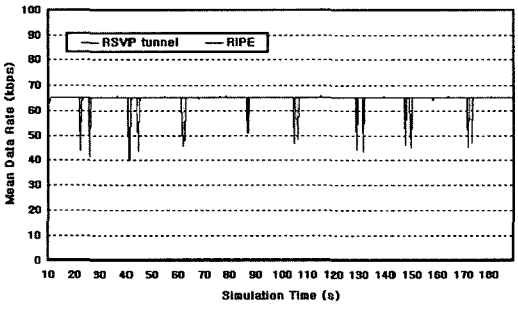


Figure 6 The mean data transmission rate

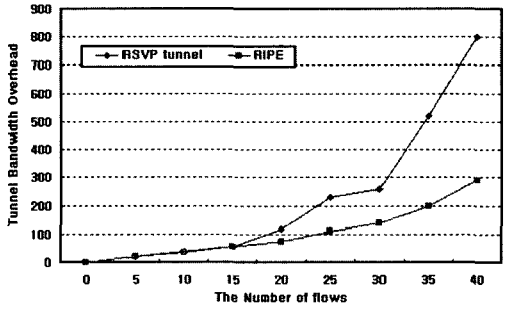


Figure 7 The bandwidth overhead in tunnel

with that of the RSVP Tunnel-based scheme. However, over the Tunnel bandwidth overhead, the proposed scheme offers about 48% lower overhead than that of the RSVP Tunnel based scheme.

## 5. Conclusions and future work

In this paper, we have presented a new scheme that can support RSVP signaling protocol for QoS to IP-in-IP tunnel used in the mobile IP. The scheme works by using the proposed RIPE for end-to-end RSVP messages over the IP-in-IP tunnel connecting the home agent with the foreign agent.

Using a simulation model, we have shown that with the introduction of the RIPE, the mean delay and data transmission rate in the tunnel between the entry and exit points is similar to those of the RSVP Tunnel, but the tunnel bandwidth overhead is greatly reduced.

For future works, we intend to work on the execution of simulations associated with the packet encapsulating at tunnel end points to evaluate the processing overhead in routers. In addition, all the Integrated Service contents cannot be supported to mobile hosts in the limited option portion of RIPE packet, to resolve this issue is, also, our future work.

## References

[1] R. Braden, D. Clark and S. Shenker, "Integrated services in the Internet architecture: An overview," RFC 1633, June 1994.

[2] S. Blake, D. Black, M. Carlson, "An Architecture for Differentiated Services," RFC 2475, December 1998.

[3] R. Braden, L. Zhang, S. Berson, S. Herzog and S. Jamin, "Resource reSerVation Protocol (RSVP) - version 1 functional specification," RFC 2205, September 1997.

[4] C. Perkins, "Mobile IP: Design Principles and Practice," Addison-Wesley/Longman Reading, MA, 1998.

[5] N. Montavont and T. Noel, "Handoff management for mobile nodes in IPv6 networks," IEEE Communications Magazine, August 2002, 38-43.

[6] W. Simpson, "IP in IP Tunneling," RFC 1853, October 1995.

[7] A. Terzis, J. Krawczyk, J. Wroclawski and L. Zhang, "RSVP operation over IP tunnels," RFC 2746, January 2000.

[8] R.A Woodburn, D.L Mills, "A Scheme for an Internet Encapsulation Protocol: Version 1," RFC 1241, July 1991.

[9] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, October 1996.

[10] S. Lepaja, R. Fleck, N.H. Nguyen, "QoS Provisioning for Mobile Internet Users," ECUMN02, August 2002, 230-236.

[11] S. Paskails, A. Kaloxylos, E. Zervas, L. F. Merakos, "An Efficient RSVP-Mobile IP Interworking Scheme," MONET, June 2003, 197-207.

[12] S-J Leu, R-S Chang, "Integrated Service Mobile Internet: RSVP over Mobile IPv4&6," Mobile Networks and Applications, 2003, 635-642.

[13] C. Q. Shen, W. Seah, A. Lo, H. Zheng and M. Greis, "An interoperation framework for using RSVP in mobile IPv6 networks," Internet Draft, July 2001.

[14] C. Shen, W. Seah, A. Lo, H. Zheng, M. Greis, "Mobility Extensions to RSVP in an RSVP-Mobile IPv6 Framework," draft-shen-nsis-rsvp-mobileipv6-00.txt, July 2002.

[15] X. Fu, "Development of QoS Signaling Protocols in the Internet," LCN'03, 2003.

[16] A. K. Talukdar, B. R. Badrinath and A. Acharya, "MRSVP: A Reservation protocol for an Integrated Services Packet Networks with Mobile hosts," Wireless Networks 7(1), 2001.

[17] C. C. Tseng, G. C. Lee and R. S. Liu, "HMRSVP: A Hierarchical Mobile RSVP Protocol," Wireless Networks 9, 2003.

[18] G. C. Lee, T. P. Wang, and C. C. Tseng, "Resource Reservation with Pointer Forwarding Schemes for the Mobile RSVP," IEEE Commun. Lett., vol. 5, no. 7, July 2001.

[19] P. Trimintzios et al., "An Architectural Framework for Providing QoS in IP Differentiated Services Networks," In the 7th IFIP/IEEE International Symposium on Integrated Network Management(IM 2001), 2001.

김 민 규

2003년 고려대학교 전산학과 학사. 2003~현재 고려대학교 컴퓨터학과 석사. 관심분야는 유비쿼터스 컴퓨팅, 모바일 IP, 웹서버 클러스터

이 숙 헌

1997년 서경대학교 컴퓨터공학과 학사 2002년 고려대학교 컴퓨터학과 석사 2002년~현재 고려대학교 컴퓨터학과 박사과정. 관심분야는 웹서버 클러스터, 유비쿼터스 컴퓨팅

박 명 순

1975년 서울대학교 전자공학과 학사 1982년 University of Utah 전기공학과 석사. 1985년 University of Iowa 전기 및 컴퓨터공학과 박사. 1975년~1980년 국방과학연구소 연구원. 1985년~1987년 Marquette University 전기 및 전산과학과 조교수. 1987년~1988년 포항공과대학교 전자전기공학과 및 전산과학과 조교수. 1988년~현재 고려대학교 컴퓨터학과 교수. 관심분야는 유비쿼터스 컴퓨팅, 웹서버 클러스터, 스토리지