MRSVP : A Reservation Protocol for an Integrated Services Packet Network with Mobile Hosts[1]

Anup K. Talukdar, B. R. Badrinath
Department of Computer Science
Rutgers University
New Brunswick, NJ 08903
{talukdar@paul,badri@cs}.rutgers.edu
Tel:732-445-2706
Fax :732-445-5530

Arup Acharya
C&C Research Labs
NEC USA
Princeton, NJ 08540
arup@ccrl.nj.nec.com
Tel:609-951-2992

Abstract

This paper describes a reservation protocol to provide real-time services to mobile users in an Integrated Services Packet Network. Mobility of hosts has significant impact on the quality of service provided to a real-time application. The currently proposed network system architecture and mechanisms to provide real-time services to fixed hosts are inadequate to accommodate the mobile hosts which can frequently change their point of attachments to the fixed network. Mobile hosts may experience wide variations of quality of service due to mobility. Therefore, a new real-time service architecture is necessary to accommodate mobile hosts which can tolerate variations in QoS and those which want mobility independent service guarantees in the same network. To obtain mobility independent service guarantees, a mobile host needs to make resource reservations at all locations it may visit during the lifetime of the connection. The currently proposed reservation protocol in the Internet, RSVP, is not adequate to make such reservations for mobile hosts. In this paper, we describe a new reservation protocol, MRSVP, for supporting Integrated Services in mobile networks.

KEYWORDS : Integrated Services, Internet Protocols, Mobility, Multimedia, Reservation Protocol, Quality of Service

Areas of interest : Multimedia Protocols, Wireless Networks and Protocols

1 Introduction

Recent progress in computing technology and wireless digital communication has made portable computers such as laptops, palmtops and personal digital assistants easily available. This has led to an intensive research in the area of *Mobile Computing* to provide mobile users access to an inter network. The research, so far, has focussed on the problem of maintaining connectivity at the network and transport layer in spite of the mobility of the mobile hosts[18, 4, 2, 14].

Also, there have been several proposals for supporting real-time applications in an Integrated Services Packet Network (ISPN). Typical applications that require real-time services include audio library, image browsing, video conferencing and video-on-demand. These multimedia applications require a bound, which may be absolute or statistical, on the delivery delay of each packet. Clark *et. al.*[7] have described an architecture for an ISPN that supports real-time traffic. Two of the main components of this architecture are the admission control scheme and the reservation protocol. Admission control scheme decides which flows should be admitted so that the QoS guarantees to all

[1]This research work was supported in part by DARPA under contract number DAAH04-95-1-0596, NSF grant numbers CCR 95-09620, IRIS 95-09816.
Corresponding Author : Anup K. Talukdar (talukdar@paul.rutgers.edu)

admitted flows can be maintained and simultaneously the network resource utilization is maximized. Jamin *et. al.* have proposed an admission control scheme for an ISPN[13]. A reservation protocol reserves resources at the routers along the data flow path. Zhang *et. al.*[27] have described a protocol, RSVP, that sets up resource reservation for real-time traffic in the internet.

As portable computers become more powerful and the accessibility of a fixed network from a mobile host becomes easier, the number of mobile users will grow and additionally the mobile users will demand the same real-time services available to fixed hosts. Applications such as *Internet Cellular Phone* [3], access to real-time data through the Web (e.g., call center application), require that the network offer quality of service to moving users. Mobility of hosts has a significant impact on the QoS parameters of a real-time application. In addition, it introduces new QoS parameters at the connection level and system level. The existing system architecture for real-time services in a network with fixed hosts is not adequate for supporting mobile hosts. Therefore a new system architecture is required to handle the effects of mobility. Talukdar *et. al.* have described a new system architecture which can accommodate mobile hosts in an ISPN[22].

In this paper we describe the reservation protocol for mobile hosts in the system architecture described by Talukdar *et. al.*[22]. The paper is organized as follows. In Section 2 we describe the effects of mobility on the real-time applications and some related works that have addressed the problem. In Section 3, we briefly describe the system architecture proposed by Talukdar *et. al.*[22]. In Section 4 we briefly describe RSVP and discuss why it is not suitable for mobile hosts and introduce MRSVP, the reservation protocol for mobile hosts. In Section 5, we give a overview of MRSVP. In Section 6, we describe the protocol. In Section 7, we conclude mentioning future works.

2 Effects of mobility

The main QoS parameters for real-time services are *packet delay*, *packet loss rate*, *delay jitter* and *throughput*. *Packet delay* is the time required by a packet to travel from the sender to the receiver. It consists of mainly two components: *propagation delay*, which is the packet propagation time and is dependent on the length of the data flow path over which the packet travels, and *congestion delay*, which is the time spent by a packet in the queue at the routers. Since the buffer size in a queue at a router is limited, packets arriving at a full queue are dropped. *Packet loss rate* is the fraction of the packets dropped per flow. *Delay jitter* is the variation of the delay between the arrivals of successive packets. The quality of a flow is also dependent on the amount of data carried by the flow per unit time, called *throughput*. To provide real-time services, a network is designed to provide sufficient guarantees on these QoS parameters.

Mobility of a host has a significant impact on these QoS parameters. When a mobile host moves from one location to another with an open connection, the data flow path changes. As a result the propagation delay of packets may change. The congestion delay at the routers along the new path may be different from that in the previous path. If the new location into which the mobile host moves, is overcrowded, the available bandwidth in the new location may not be sufficient to provide the throughput it was receiving at the previous location. In addition, the mobile user may suffer temporary disruption of service during handoff while the connection is teared down along the old path and it is established along the new path.

Therefore, the mobile users may have to adapt to these changes as they move with their connections open. In some extreme cases, some connections to the mobile users may have to be dropped if the minimum QoS requirements of all users cannot be satisfied[17, 15]. Considering these effects of mobility, a set of new service classes has been defined by Talukdar *et. al.*[22], which is briefly described in Section 3. There are, broadly, two service classes, *mobility dependent* and *mobility independent*. The users subscribing to the mobility independent service classes are not affected by the mobility of hosts, whereas those subscribing to the mobility dependent service class may experience changes in their various QoS parameters as hosts handoff from one location to another with their connections open. To provide mobility independent service guarantees, it is necessary to make resource reservation from all locations where the mobile host may visit. In this paper we propose a reservation protocol, MRSVP for mobile users in the above architecture.

Recently there has been some work addressing the problem of providing QoS to mobile hosts. Acampora and Naghshineh[1] have presented an architecture for a high-speed mobile ATM network using a new concept known as the virtual connection tree. Singh[21] has introduced two new QoS parameters, *loss profile* and *probability of seamless communication*, arising due to the mobility of the mobile host. They have described a network architecture and a suite of transport level services to satisfy these QoS parameters. Lee[15] has presented an "adaptive reserved service" framework for use in integrated services networks to support mobile connections carrying multimedia traffic. Levine *et. al.*[16] have proposed resource allocation and admission control schemes based on a new concept, called *Shadow Cluster*, to improve the QoS of mobile calls by reducing the number of dropped calls in an wireless-ATM network. However, in the solutions presented in these works a mobile host may suffer significant degradation in QoS due to mobility; the problem of providing mobility independent service guarantees and the design of the associated reservation protocol have not been addressed.

3 Architecture

In this section we give an overview of the service classes and the admission control scheme in the architecture described by Talukdar *et. al.*[22] to accommodate mobile users in an Integrated Services Packet Network. The detailed description can be found in the reference.

3.1 Service Classes

There are three service classes to which a mobile user may subscribe. These are *Mobility Independent Guaranteed*(MIG), *Mobility Independent Predictive*(MIP) and *Mobility Dependent Predictive*(MDP) services. The service guarantees provided in these service classes are as follows :

- MIG : A mobile user admitted to this service class will receive *guaranteed* service with respect to packet delay bounds as long as its moves are limited to its *mobility specification* and it is conforming to its traffic characterization. This class is appropriate for the intolerant applications which require absolute bound on packet delay.

- MIP : A mobile user admitted to this class will receive *predictive* service with respect to packet delay bound as long as its moves are limited to its *mobility specification* and it is conforming to its traffic characterization. This class is appropriate for those tolerant applications which require fairly reliable delay bounds in all locations it might visit and does not want to be affected by mobility of the hosts.

- MDP : A mobile user admitted to this service class will receive *predictive* service with high probability in all locations it may visit during the lifetime of its connection as long as it is conforming to its traffic characterization. However it may experience severe degradation of QoS and when the network is overloaded, its flow may be dropped. This class is appropriate for tolerant applications, which can tolerate the effects of delay variations and disconnection.

3.2 Service Interface

To obtain a certain QoS in an ISPN, the endpoints of a data flow is required to provide characterization of the data traffic they will generate, so that the network can reserve sufficient resources for the flow. This characterization is done with a *token bucket filter*. A token bucket filter has two parameters: its token generation rate, r, and the depth of its bucket, b, i.e. at most b tokens can accumulate in the bucket. When a packet of size p is generated, p tokens are removed from the bucket. A flow conforms to a token bucket filter (r, b) if there are enough tokens in the bucket whenever a packet is generated.

In a fixed network the required resources are reserved at the switches along the data flow path. In a mobile environment the data flow path changes as a mobile host moves from one location to another. To provide real-time services to a mobile host, it is necessary to reserve resources along all possible data paths which may be used during the lifetime of a connection. Therefore, in addition to the traffic characterization, the mobile host is also required to provide its mobility characterization to the network. In this paper we assume that, the mobility of an user is predictable so that mobility can be characterized precisely by *mobility specification* which is the set of locations the mobile host is expected to visit during the lifetime of the connection.

3.3 Admission Control

The goal of the admission control algorithm should be to admit as many mobile users as possible with the requested QoS and achieve a very high utilization of the resources. However, when a new mobile user is admitted, the system should ensure that it meets its prior commitments to previously admitted users. To admit a new flow it is necessary to perform admission control at all switches and base stations along the paths from the sender to the locations where the mobile

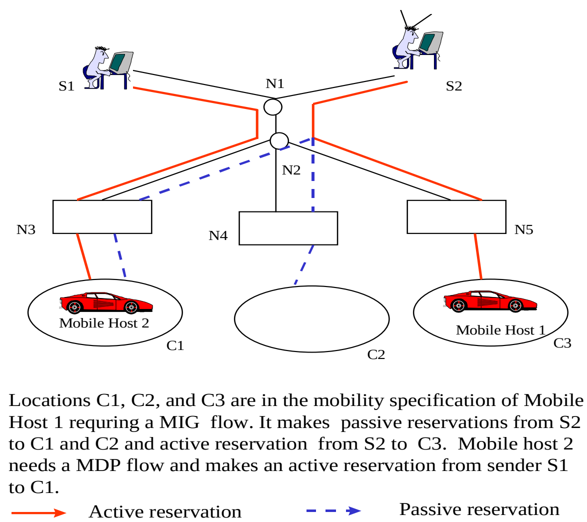


Figure 1: Reservation for Service Classes

host may visit. A flow is admitted to the network only if it passes the admission control criteria at each switch or base station where the flow requires reservation. To improve the utilization of the network bandwidth, Jamin *et. al.* have proposed a measurement-based admission control scheme for the ISPN[13]. In this scheme, instead of using the *a priori* worst case parameters, measured parameters of currently existing flows are used in the admission control criteria.

It is obvious that, the utilization of the network will be extremely low if the users of the mobility independent service classes makes bandwidth reservations along the paths from the sender to all locations where the mobile user may visit during the connection. Utilization can be improved by allowing the users of the mobility dependent service class to use the reserved but unused resources of the mobility independent service classes. Thus two types of flows have been defined. These are:

1. *Active* : A flow is active at a switch along a data path if resources are reserved for the flow at the switches along the data path and data is being transmitted to a receiver along that path. The corresponding reservation is called an *active reservation.*

2. *Passive* : A flow is passive at a switch along a data path if resources are reserved for the flow at the switches along the data path but the the data is not passing through that switch. The corresponding reservation is called a *passive reservation.*

In Figure 1, let B be the bandwidth of each link (both wired and wireless). Mobile Host 1 is connecting to a flow from sender S2. It requests MIG service and requires a bandwidth of R_1; it makes an active reservation to its current location C3 and passive reservations to the locations C2 and C3. Mobile host 2 is connecting to a flow from sender S1. It requests MDP service and requires a bandwidth of R_2; it makes an active reservation to its current location C1. At this state, consider the link (N2, N3): the bandwidth available to new flows requesting MDP service is $(B - R_2)$; for new flows requesting MIG/MIP service, the available bandwidth is $(B - R_1 - R_2)$. On link (N1,N2) the available bandwidth for a new flow is $(B - R_1 - R_2)$.

When a new flow requests admission, the admission control algorithm at a router checks that the following two conditions are not violated after admitting the new flow:

1. The overall link utilization does not exceed the link capacity

2. The delay bounds of all flows are satisfied.

A mobile user requesting a mobility independent service guarantee makes an active reservation from the sender to its current location and it makes passive reservation from the sender to all other locations in its mobility specification where it may move later. When it moves from one location to another (within its mobility specification), the active reservation to its old location is turned into a passive reservation and the passive reservation to its new location is turned into an active reservation. A mobile users requesting a mobility dependent service guarantee makes an active reservation from sender to its current location only; when it moves, it tries to make a new active reservation from the sender to its new location.

3.4 Performance

There are three main parameters that determine the performance of the system: *Network utilization*, which is the fraction of the network link bandwidth used, *flow drop rate*, which is the fraction of the admitted MDP flows that are dropped due to handoff, and *active flow count*, which is the average number of flows which are active in the network. Simulation results have shown that, when sufficient degree of multiplexing of the resources among the mobility independent and dependent flows are allowed, the utilization level of the network can be kept high without any degradation of the flow drop rate and number of active flows supported[23]. This shows that, it is viable to provide mobility independent services in a network.

4 Overview of IPv6, IETF Mobile-IP and RSVP

MRSVP is an extension of the resource reservation protocol in the internet, RSVP[27], and it closely interacts with the routing protocols. Before describing the details of MRSVP, we give brief overviews of the relevant features of IPv6, Mobile-IP and RSVP.

4.1 Overview of IPv6

In IPv6 all addresses are 128 bits long, instead of 32 bits long in IPv4. IPv6 has defined several kind of *extension headers*, which may be used to include additional information in the headers of an IPv6 packet. One of these extension headers is the *Routing header*. This Routing header is used by an IPv6 source to list one or more intermediate nodes to be visited on the way to the packet's destination. In IPv6 a new type of address called an "anycast address" is defined, which is used to send a packet to any one of a group of nodes. Each subnet has a pre-defined anycast address, called *subnet-router anycast address*, which is supported by all routers in that subnet. Packets sent to the subnet-router anycast address will be delivered to one router in the subnet. Also, there is a pre-defined multicast address for each link, called *all-routers link-local multicast address*, which is supported by all routers in that link.

4.2 Overview of Mobile-IP

The IETF Mobile-IP protocol allows a mobile node to communicate with other nodes after changing its link-layer point of attachment from one IP subnet to another without changing its IP address. A mobile node has two IP addresses assigned to its network interface. One of them is its *home address* which is permanently assigned to the mobile node. The other address is called the *care-of address*, which is associated with the mobile node when it is visiting a particular foreign subnet. The network prefix of the care-of address is same as the network prefix of the foreign subnet it is visiting. This care-of address can be the either a *foreign agent care-of address* or a *co-located care-of address*. A foreign agent care-of address is an IP address of a foreign agent in the foreign subnet. A mobile node acquires a foreign agent care-of address using Router Solicitation and Router Advertisement[18, 19, 8] messages. A co-located care-of address is a care-of address acquired by the mobile node as a local IP address. This care-of address may be dynamically acquired by the mobile node through Dynamic Host Configuration Protocol (DHCP)[10] or may be owned by the mobile node as a long-term address for its use only when visiting this foreign subnet. This association of the care-of address with the home address is called *binding*.

When a packet is sent to a mobile node's home address and the mobile node is located in its home subnet, the packet reaches the destination by normal IP routing mechanism. When away from home, a mobile node registers its care-of address with a mobility agent in its home subnet, called *home agent*. The home agent then intercepts all packets addressed to the mobile nodes home address and then tunnel each of them to the care-of address of the mobile node using IP encapsulation. On receiving an encapsulated packet, a foreign agent decapsulates it and then delivers it to the mobile node. If the care-of address is a co-located care-of address, the encapsulated packet reaches the mobile node directly and the packet is decapsulated by the mobile node.

In Mobile IPv6, every node maintains a *Binding Cache* containing the bindings of mobile nodes. A mobile node, in addition to sending its binding to its home agent, it can send the binding to its correspondent nodes communicating with it. When sending a packet to any IPv6 destination, a node checks its Binding Cache for an entry for the packet's destination address. If a cached binding is found, the packet is directly routed to the care-of address of the mobile node found in the binding using an IPv6 Routing header. Thus in Mobile IPv6, packets to a mobile node can be routed via the optimal route.

4.3 Overview of RSVP

The design of RSVP has been guided by the following goals: The ability to support heterogeneous receivers, support multicast flows and deal gracefully with changes in multicast group membership, aggregation of reservations depending on application needs, allow channel changing in a multiparty conversation, adapting to route changes, control protocol overhead and modularity. To achieve these goals, the designers have used six basic design principles. These are: receiver-initiated reservation, separating reservation from packet filtering, providing different reservation styles to dictate how to aggregate reservations, maintaining soft-state in the network, merging of control messages for protocol overhead control and transporting and maintaining opaque state to attain modularity.

There are seven types of messages in RSVP. The messages and their functions are:

1. *Path* : Sets up the path over which reservation is established.
2. *Resv* : Sets up reservation states at the routers.
3. *PathErr* : Notifies error in path set up
4. *ResvErr* : Notifies error in reservation setup and rejection of reservation request.
5. *PathTear* : Tear down path and reservation.
6. *ResvTear* : Teardown reservation.
7. *ResvConf* : Send confirmation of reservation.

Each data source periodically sends *Path* message that sets up the path state at the switches along the path from the sender to the receivers and each receiver periodically sends *Resv* message that set up reservation state at the switches along the reverse path from the receiver to the sender (Figure 2). A *Path* message carries the Sender Tspec which defines the traffic characteristics of the data flow that the sender will generate. The destination address can be a unicast address (of a host) or a multicast address. When a switch receives a *Path* message, it checks if it already has the path state for the flow; if not it creates the path state. The switch then obtains the outgoing interfaces of the path message from the routing protocol. This path message is forwarded if it is for a new flow or there is a change in routes. Otherwise the switch discards the path message and instead periodically sends its own path messages which contains the information in its path state.

On receiving a path message from a source, a receiver sends a *Resv* message. This *Resv* message contains the *flowspec* the receiver is willing to handle. The flowspec consists of a service class and two sets of numeric parameters: (1) an *Rspec* that defines the desired QoS and (2) a *Tspec* that describes the traffic characteristics of the data flow. The formats and contents of Tspec and Rspec is determined by the integrated services modules[26] and are generally opaque to RSVP. The *Resv*

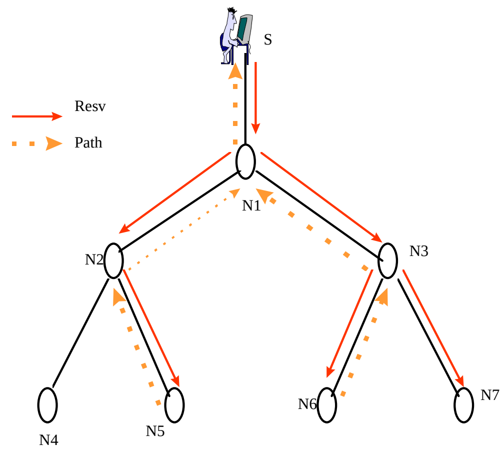


Figure 2: RSVP Messages

message traverses the reverse path of data flow from the sender to the receiver. If at any switch along this path, the reservation is rejected, the switch sends a *ResvErr* message to the receiver.

In RSVP, a flow is identified by the *destination address* of the flow, the *Protocol Id* and the *destination port number*. These informations are carried by every RSVP message in its SESSION object.

To make resource reservations for providing real-time services to mobile users additional features are required which are not currently present in RSVP. This is because of two reasons. The first reason is, to provide mobility independent service guarantees, it is necessary to make resource reservation from the sender to all locations where the mobile host is expected to visit during the lifetime of the connection: the mobile host will make an active reservation from the sender to its current location and it will make a passive reservation from the sender to each of its other locations in its mobility specification. Whenever the mobile host moves from one location to another, the active reservation from the sender to its previous location will be turned into a passive reservation and the passive reservation to its new location will be turned into an active reservation. The process of converting a passive reservation to an active reservation should be fast enough to minimize flow disruption due to handoff. The second reason is that, users subscribing to mobility dependent service guarantees make only active reservations to their current location; they do not make any passive reservations. When they move from one location to another, the process of establishing resource reservation along the path from the sender to the new location (subject to availability of resources) should be fast enough to minimize the handoff disruption; the usual periodic reservation refreshing mechanism of RSVP may not be able to adequately respond to the handoff of mobile hosts.

In the rest of this paper, we define the terms "upstream", "downstream", "previous hop" and "next hop" with respect to the direction of data flow.

5 MRSVP overview

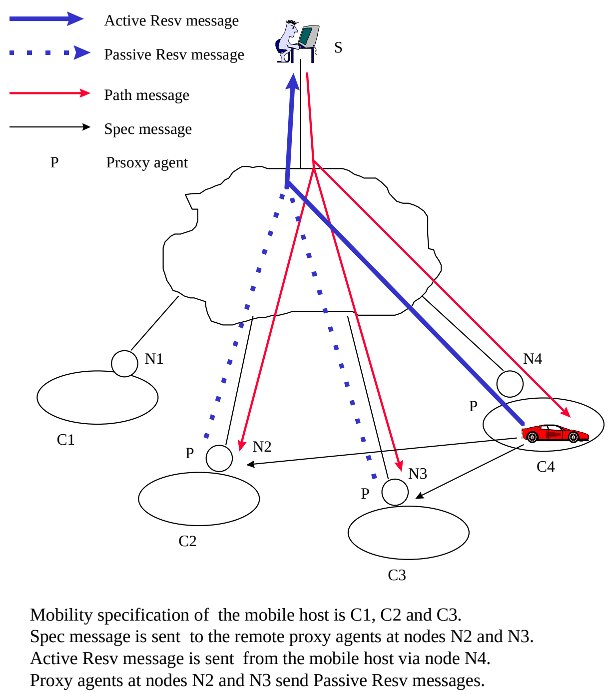


Figure 3: Overview of MRSVP

In this section, we give an overview of the MRSVP protocol. The details of the protocol and how it integrates with the Internet Protocol architecture (IPv4 or IPv6) and the routing protocols (unicast and multicast) will be described in the next section. Just as Mobile-IP protocol requires home agents and foreign agents to aid in routing, MRSVP requires *proxy agents* to make reservations along the paths from the sender to the locations in the mobility specification. The proxy agent at the current location of the mobile host is called the *local proxy agent*. The proxy agents at the other locations in the mobility specification of a given mobile host are called *remote proxy agents*. The remote proxy agents will make passive reservations on behalf of the mobile hosts. The local proxy agent of a mobile host acts as a normal router for the mobile host and an active reservation is setup from the sender to the mobile host via the local proxy agent. An important issue is how the mobile host determines who will be the proxy agents. We assume that the mobile host knows the subnets where it is likely to visit. Then it can use a *proxy discovery protocol* to determine the IP addresses of the proxy agents.

After the mobile host knows the IP addresses of its proxy agents, the most important task is to setup the paths from the sender to its current location and the proxy agents along which active and passive reservations will be setup. We consider two distinct cases:

1. The mobile host joins a multicast flow : In this case the mobile host directs the proxy agents to join the multicast group and the data flow paths are setup along the multicast routes.

2. The mobile host initiates a unicast flow : In this case the paths may be setup by unicast routing or by multicast routing.

We describe each of these cases in the following section.

After the routes of active and passive reservations are setup, the mobile host and the proxy agents will start receiving the *Path* messages. On receiving a *Path* message the mobile host will send a *Resv* message for active reservation. If a proxy agent receives *Path* messages for a multicast group, for which it is acting as a proxy agent, or for a mobile host from which it has received a request for acting as a proxy, it will make a passive reservation on the downstream link to which the mobile host will attach when it arrives in its subnet, and then send a *Resv* message to make a passive reservation (Figure 3).

In addition to the messages present in RSVP, four additional messages are required in MRSVP. These are :

1. *Join_group* : This message is sent by a mobile host to its remote proxy agents to request them to join a multicast group. It contains the multicast address of the group to join.

2. *Spec* : This message is used by a mobile host to send the flow specification to its remote proxy agents.

3. *Mspec* : This message is used by the mobile host to send its mobility specification to the appropriate node (to be described in the next section), who sets up the the routes of active and passive reservations. It contains a list of the care-of addresses of the mobile host in the foreign subnets in its mobility specification and the home address if the home subnet is also present in the mobility specification.

4. *Terminate* : This message is used by the mobile host to request its remote proxy agents to terminate reservation.

6 MRSVP Protocol Description

In this section, we provide details of MRSVP. Functionally, there are several issues in the protocol. These are discovering proxy agents, setting up routes for active and passive reservation, reservation setup, merging reservation messages, switching between active and passive reservation, soft state maintenance, tearing down of reservation, confirmation and handling of error messages. We describe each of these issues.

6.1 *Proxy Discovery Protocol* : Discovering Proxy Agents

Proxy agents set up passive reservations on behalf of a mobile host. Hence, a mobile host needs to discover these proxy agents. The *proxy agent* of a subnet supporting mobile hosts is a special MRSVP capable router in the subnet which has the following functionalities:

- All data packets to the mobile hosts in the subnet are delivered through this router.
- It can make passive resource reservation on behalf of the mobile hosts which are not currently present in the subnet.
- It can notify the results of the reservation attempt for passive reservation to the mobile host for which it was making the reservation.

We assume that a mobile host knows the subnet addresses for locations that are in its mobility specification. However, the mobile host still needs to know the addresses of the proxy agents in those subnets.

When the mobile host has a foreign agent care-of address in a foreign subnet, the foreign agent acts as the proxy agent in that subnet. As per IETF Mobile-IP, these care-of-addresses may be preallocated or they may be dynamically acquired by the mobile host when it moves into that subnet. However, the protocols for acquiring care-of address by a mobile host in a foreign subnet works only when the mobile host is present in that subnet. These protocols cannot be used by a mobile host to acquire a care-of address remotely in a foreign subnet where it is not currently present. Hence, a mobile host need to use a mechanism such as Service Location Protocol[25] to acquire care-of addresses remotely. The details of this mechanism is out of the scope of this paper.

In the following, we describe an alternative protocol for dynamically acquiring foreign agent care-of-address in a foreign subnet where the mobile host is not currently located. The protocol uses two messages, *Remote Agent Solicitation* and *Remote Agent Advertisement* . In IPv4 architecture, the protocol is as follows:

1. The mobile host sends a Remote Agent Solicitation message in which the destination address is the subnet directed broadcast address of the foreign subnet.
2. On receiving a Remote Agent Solicitation message, the foreign agent will reply with a Remote Agent Advertisement message containing the care-of address to the mobile host.

In IPv6 architecture, the protocol works as follows:

1. The mobile host sends a Remote Agent Solicitation message in which the destination address is the subnet-router anycast address of foreign subnet.

2. The router receiving this Remote Address Solicitation message, multicasts it to the all-routers link-local multicast address.

3. On receiving the Remote Agent Solicitation message, the foreign agent replies with a Remote Agent Advertisement message containing the care-of address to the mobile host.

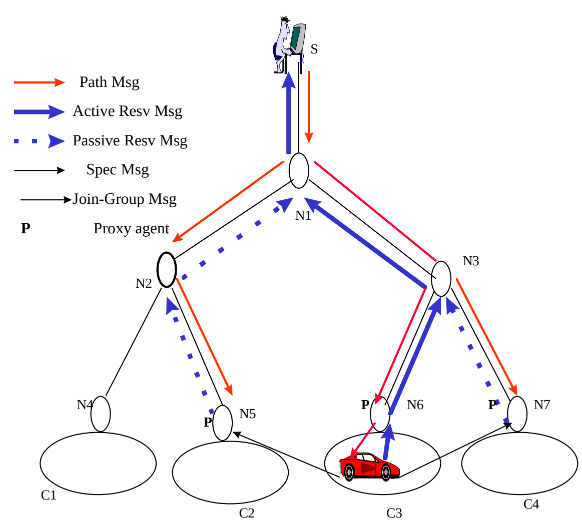
We assume that when the mobile host is in its home subnet, all packets to the mobile host are delivered via its home agent. When the mobile host is away from its home subnet, and the home subnet is also in the mobility specification, the home agent acts as the proxy agent for its home subnet.

In IETF Mobile-IP, a mobile host can also acquire a co-located care-of address by using Dynamic Host Configuration Protocol (DHCP). In this case also we can design a similar protocol to determine the co-located care-of addresses remotely. The proxy agent, in this case, is the last hop router to the mobile host in each subnet.

For simplifying the discussion, we assume that, all care-of addresses of a mobile host are foreign agent care-of addresses and the foreign agent of a subnet is also the proxy agent for a mobile host and in the home subnet, home agent is the proxy agent of the mobile host.

Having discovered the addresses of the proxy agents, the next issue is on setting up the reservation routes from the sender to the proxy agents and the mobile host. The mechanism to set up reservation routes depends on the type of the flow: multicast flow or unicast flow.

6.2 Reservation Routes : Multicast Flow



Mobility specification of mobile host is C2, C3, and C4. Mobile host joins the multicast group and informs Proxy agents at N5 and N7 to join the multicast group. Proxy agents at N5 and N7 start receiving Path messages after they join the multicast group. Proxy agents N5 and N7 send Passive Resv messages and the mobile host send Active Resv message.

Figure 4: Reservation routes for a multicast flow

To join a multicasting session, a mobile host sends two messages, a *Join_group* message containing the multicast address of the group, and a *Spec* message containing the flow specification, to each of its remote proxy agents. On receiving the *Join_group* and *Spec* messages and the remote proxy agents join the multicast group whose multicast address is specified in the *Join_group* message and record the flowspec present in the *Spec* message. The mobile host also joins the multicast group (Figure 4).

As a result, when the sender sends a *Path* message to the multicast address, it reaches the proxy agents and the mobile host. Thus the paths of active and passive reservations are setup along the multicast routes. We do not specify any particular multicast routing protocol to be used. For better network performance, a sparse-mode multicast routing protocol, like PIM-SM[11, 12] or Core-Based Tree multicast protocol[5, 6], is preferred because the set of proxy agents and the mobile host are expected to be located in close proximity.

6.3 Reservation Routes: Unicast Flow

A unicast flow is between a source and a destination. However, in our architecture of supporting integrated services to mobile hosts, a mobile host needs service guarantees in all locations in its mobility specification. Hence, even for a unicast flow, a set of proxy agents need to make passive reservations for the flow. As a result, we have two choices for setting up reservations from a set of proxy agents and the mobile host: unicast routes and multicast routes to the proxy agents.

6.3.1 Unicast Routes for Unicast Flow

In this scheme, for each flow, a specific node called the *anchor node*, is designated for setting up the routes for passive reservations. Passive reservations are setup from the anchor node to each remote proxy agent and an active reservation is setup from the anchor node to the mobile host. These active and passive reservations are merged at the anchor node and the merged reservation is setup from the sender to the anchor node. Each of these reservations are setup along the unicast routes. The exact reservation routes will depend on the choice of the anchor node. We consider two choices: the sender as the anchor node and the other, proxy agent at the home subnet as the anchor node.

- **Sender as the Anchor Node**: To setup the reservation routes, the mobile host sends an *Mspec* message to the sender containing the addresses in its mobility specification. An active reservation is setup from the sender to the current location of the mobile host and a passive reservation is setup from the sender to all other proxy agents in the *Mspec* (Figure 5).

  The advantage of this scheme is that, reservation is setup along the optimal routes. The disadvantage of this scheme is that, the sender has to implement many functionalities related to the mobile receivers.

- **Proxy agent in the home subnet as the Anchor Node**: In this scheme, the mobile host sends an *Mspec* message to its proxy agent in its home subnet (which is also its home agent).

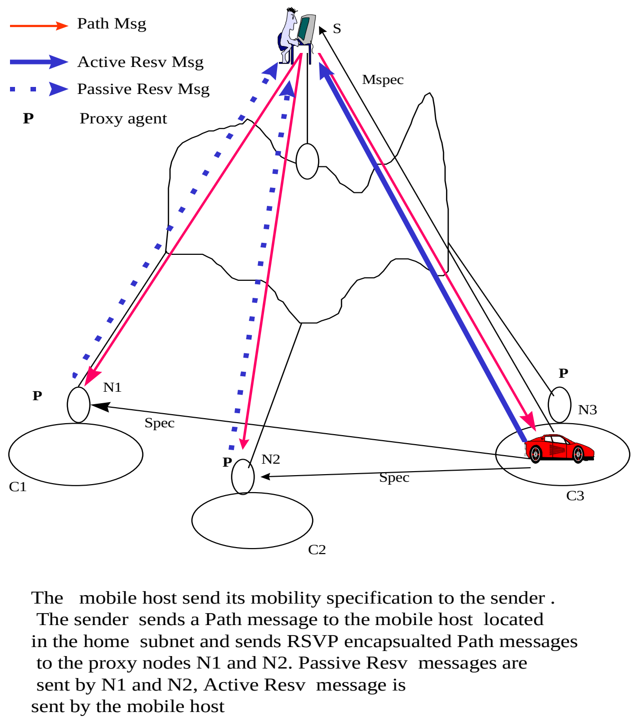


Figure 5: Reservation routes for a unicast flow (Sender as the Anchor Node)

The home agent sets up the route of active reservation from itself to the mobile host and it sets up the routes of passive reservations to all other proxy agents in the *Mspec* message. In this scheme, the mobile host should not send any binding update to the sender after the connection is setup, because otherwise, the *Path* messages and data packets of the flow will reach the mobile host via a different path over which reservation has not been established (Figure 6).

The advantage of this scheme is that the sender need not have any functionality related to mobility. The drawbacks of this scheme are: 1) the reservation is not setup along the optimal routes, 2) even though the home subnet is not in the mobility profile of the mobile host, all packets reach the mobile host via the home agent.

6.3.2 Multicast Routes for Unicast Flow

In this case, in addition to the home address and the set of care-of addresses that the mobile host has acquired by the proxy discovery protocol, the mobile host acquires a multicast address which is used as the destination address of the flow. We assume that there is a server (which may be centralized or distributed) that allocates multicast addresses to the mobile hosts. The mobile host

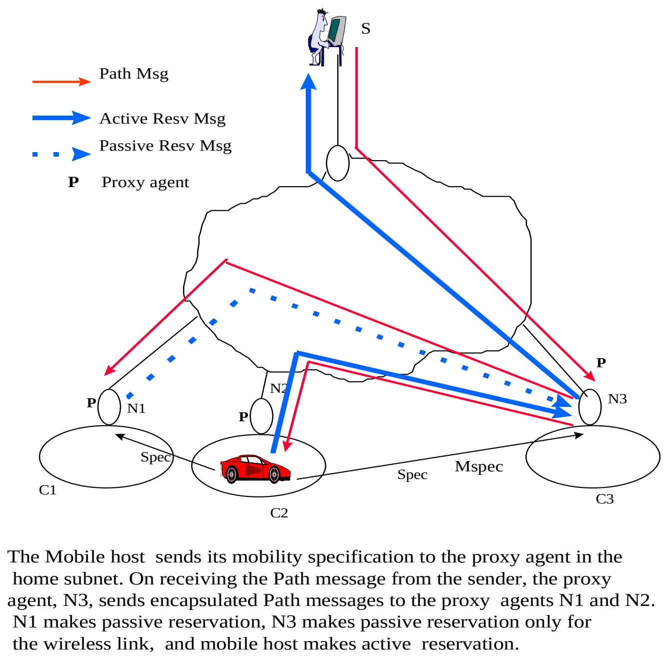


Figure 6: Reservation routes for a unicast flow (Anchor node in the home subnet)

may acquire this multicast address dynamically before each connection setup. However this may increase the connection setup time. Since in IPv6, there is an abundance of multicast addresses, we can allocate a multicast address to each mobile host permanently to reduce the connection setup time. The mobile host sends its multicast address to the sender and the scheme of route establishment for multicast flow (as described above in Subsection 6.2) is used.

The major advantage of using multicast routes for making active and passive reservations is that, reservations are setup along the routes determined by the multicast protocol used which may be optimal or near-optimal. Also, no special agent is required to setup active and passive reservations for the mobile hosts. A disadvantage of this scheme is, multicasting support is required in the network and if the multicast protocol overhead is high, the performance of the network may degrade.

6.4 Reservation Setup

To initiate the actual reservation process, the sender has to be informed of the destination address of the flow. For multicast flows, this destination address is the multicast address of the group. For a unicast flow, there are two choices as described.

If unicast routing scheme is used, the home address of the mobile host is used as the destination address of the flow. In the unicast routing scheme for unicast flows, the mobile host will send a *Mspec* message containing its care-of addresses to its anchor node. If multicast routing scheme is used, the multicast address acquired by the mobile host for the purpose of the reservation is sent to the sender.

6.4.1 *Path* Messages

In MRSVP, *Path* messages are generated and processed in the same way as RSVP, i.e they are periodically generated by the senders and intermediate routers along the path to the receivers and forwarded downstream to the destination.

If the destination address of the flow is the multicast address (this is true for multicast flows and unicast flows using multicast routes), the sender will send *Path* messages in which the IP destination address will be the multicast address. After the proxy agents join the multicast group for a mobile host, they also start receiving the *Path* messages. If the destination address is the unicast home address of the mobile host the content of the IP destination field will depend on the choice of the anchor node. If the sender is the anchor node, it will use the home address of the mobile host as the IP destination address of the *Path* messages, but it will tunnel the *Path* message to each proxy agent separately using an encapsulation scheme called, *RSVP encapsulation* (which is described below), in which the IP destination address of the outer header will be the care-of address of the mobile host. The destination address of the flow in the SESSION object of the *Path* message should be the home address of the mobile host.

If the proxy agent of the home subnet is the anchor node, the sender will use the home address in the IP destination field of the *Path* message. In this case the anchor node has to replicate and tunnel the *Path* message to each care-of address of the *Mspec* message using *RSVP encapsulation*. In the rest of this subsection we describe how the *Path* messages are tunnelled to each care-of addresses.

RSVP Encapsulation : When the anchor node receives a *Path* message for a mobile host, it will tunnel it to each care-of address of the mobility specification of the mobile host. However if the normal IP tunnelling mechanism is used, the intermediate routers will not create any *Path* state. Therefore we use a different type of encapsulation mechanism, called *RSVP encapsulation* which allows creating *Path* state at the routers in the tunnel as the encapsulated *Path* message traverses the tunnel. When the anchor node receives a *Path* message, it will encapsulate it within an outer header that contains the source and destination addresses of the tunnel. On receiving an encapsulated *Path* message, a router will access the inner RSVP flow information to setup and update *Path* state. When it reaches the end of the tunnel, the router will decapsulate it and process it as a normal *Path* message.

6.4.2 *Resv* Messages

The generation and processing of *Resv* messages in MRSVP requires additional work due to three reasons:

1. *Resv* messages may be generated for *active* and *passive* reservation.

2. Remote proxy agents may generate *Resv* messages for *passive* reservation.

3. *Active* and *passive* reservations for the same session should be merged at the routers along the common path.

In this subsection we describe how *Resv* messages are generated and processed. Merging of reservations is described in the next subsection.

On receiving a *Path message* a receiver (static or mobile host) will generate appropriate *Resv* message as in RSVP and forward it to the previous hop upstream. This *Resv* message will setup active reservation at the routers as it travels upstream.

When a proxy agent receives a *Path* message destined for a multicast or unicast address for which it has already received a *Spec* message, it will try to create reservation states for passive reservation on the downstream interface to its subnet. If it fails, it will send an UDP (User Datagram Protocol[20]) encapsulated *ResvErr* message to the mobile host. If already enough resources have been reserved, then it will send an UDP encapsulated *Resv_confirm* message to the mobile host. Otherwise it will send a *Resv* message for passive reservation upstream. Both *ResvErr* and *Resv_confirm*contains enough information so that the mobile host can decide its future course of action.

A *Resv* message received by a RSVP router may contain information for active reservation or passive reservation or both. A router maintains reservation states for both active and passive reservation for each session passing through it. When a router receives a *Resv* message it updates the reservation states for active and passive reservation appropriately depending on the content of the message (if there are no reservation states, it creates a new state). To create/update these states it uses the merging rules described in the next subsection. If this reservation becomes unsuccessful it sends a *ResvErr* message back to the sender of the *Resv* message (for passive reservation, it should be sent to the proxy agent, which then forwards it to the mobile host. This ensures that the mobile host can determine at which locations the reservations were denied). If the router already had the required reservations (both active and passive) it sends *Resv_confirm* message to the sender of the *Resv* message. Otherwise, the router immediately sends a *Resv* message upstream containing the merged state.

6.5 Merging Active and Passive Reservation

In RSVP, a router merges the flowspecs of the *Resv* messages of the same flow received from the different next hops and then sends a combined *Resv* message containing the merged flowspec to the previous hop. The merged flowspec contains the “largest” of the flowspecs requested by the next hops. The “largest” of a set of flowspecs is computed by following merging schemes which depend on the rules of comparing flowspecs[27, 26].

In MRSVP, in addition to merging flowspecs requested by the different next-hops at an interface, it must also merge the active and passive reservations for the same session. The flowspec of the merged reservation is the larger of the flowspecs of the active and passive reservations. However the data flow starts according to the flowspec of the active reservation. The result of merging an active and a passive reservation is a combined reservation containing the required flowspecs of both active and passive reservation and a combined reservation message is forwarded upstream. Thus the reservation state contains a quadruple (ARe, ATe, PRe, PTe) where ARe and PRe are the effective Rspec for active and passive reservation respectively, ATe and PTe are the effective TSpec of the active and passive reservation respectively. The steps in computing these effective values are:

1. Compute the effective flowspec of the active reservation by merging the flowspecs of active reservation from different next hops. Similarly compute the effective flowspec of the passive reservation by merging the flowspecs of passive reservation obtained from different next hops. The result is the quadruple (ARe, Resv_ATe, PRe, Resv_PTe).

2. Compute Path_Te, the sum of all Tspecs that were supplied in *Path* messages from different previous hops.

3. Compute the effective Tspecs ATe and PTe by taking the minimum of (Resv_ATe, Path_Te) and (Resv_PTe, Path_Te) respectively.

A flow is identified by the SESSION object in the RSVP messages. In an unicast flow using unicast routing the SESSION object always contains the home address of the mobile host as the destination address of the flow. In multicast flow or in a unicast flow using multicast routing the SESSION object contains the multicast address as the destination address. Thus the routers can easily identify different RSVP messages of the same flow even though the IP destination addresses of those messages may be different and reservations of the same flow at the routers along the common path (including those inside a RSVP tunnel) can be merged.

We allow heterogeneity in the flowspecs of the active and passive reservations from different locations so that a mobile host can make as much reservations as available at different locations in its mobility specification.

6.6 Switching between Active and Passive Reservation

When a mobile host with an already established connection with mobility independent service guarantee moves to a new location within its mobility specification, the active reservation from the sender to its previous location will be turned into a passive reservation and the passive reservation from the sender to its new location has to be converted to an active reservation. This can be done as part of the registration and deregistration of the mobile host at the new and old location respectively: when registering, the mobile host sends an active reservation message, whereas when deregistering the router at its old subnet it sends a passive reservation message.

6.7 Soft State

Since the underlying protocol RSVP uses soft state to manage the reservation state at routers and hosts, MRSVP also takes the same approach. Due to additional messaging required to manage passive reservation, MRSVP has two more additional overhead. These are:

- Providing the proxy agents with the flowspec : As described above, the mobile host sends *Spec* messages containing flowspecs to the proxy agents. Since the IP message delivery system is unreliable, these *Spec* messages are sent periodically to handle the occasional loss. On receiving the flowspec, the proxy agents save them. An MRSVP agent deletes itself from the set of proxy agents of a mobile host unless it receives a refresh *Spec* message from the mobile host within a certain timeout period.

- Maintaining passive reservation : A proxy agent for a mobile host sends *Resv* message periodically for passive reservation. On receiving a passive *Resv* message, a router sets up state for passive reservation. This state is deleted unless it is refreshed by new passive *Resv* message before the timeout interval. To reduce the passive reservation protocol overhead, the refresh interval for passive *Resv* messages are made at least twice that of active *Resv* messages.

- Mobility specification: For unicast flows using unicast routing scheme, the mobile host periodically sends the *Mspec* message containing the mobility specification to its anchor node.

6.8 Teardown

In RSVP reservation states are explicitly teared down under two circumstances: when a flow terminates and when the admission control rejects a reservation. In MRSVP, in addition to tearing down the active reservation it is also necessary to teardown the passive reservation. Passive and active reservations can be teared down independently. To terminate a flow, a mobile host will send a *Terminate* messages to its proxy agents. On receiving them, a proxy agent will delete the reservation state for passive reservation on its downstream link (unless some other hosts had made that reservation) and send a *ResvTear* message to teardown the passive reservation upstream. When the state times out, a router will generate the corresponding *ResvTear* message. *PathTear* messages are handled in the same way as in RSVP.

6.9 Confirmation

In RSVP, a receiver can include request for confirmation for its reservation request in the *Resv* message and specify its address where the confirmation should be sent. If the reservation request from the receiver is equal to or smaller than the reservation in place at a node, its *Resv* message is not forwarded further and if a confirmation is requested, a *ResvConf* message is sent back to the receiver.

In MRSVP, the mobile host can send a request for confirmation for its passive reservation request to its proxy agents in the *Spec* message. Then the proxy agent includes the request for confirmation in the *Resv* messages for passive reservation and specify the care-of address of the mobile host in its subnet as the destination where the *ResvConf* should be sent. When it intercepts a *ResvConf* message for passive reservation for a mobile host, it will send it to the mobile host using UDP encapsulation.

6.10 Error Messages

When a proxy agent receives a *ResvErr* message, it will forward it to the mobile host using UDP encapsulation.

7 Conclusion and Future work

In this paper we have described a resource reservation protocol , MRSVP, for mobile hosts in an Integrated Services Packet Network. The main feature of this protocol is the concept of *active* and *passive* reservations which is used to provide mobility independent service guarantees. MRSVP is an extension of the reservation protocol RSVP. Thus MRSVP contains all the functionalities and messages of RSVP. The additional features due to mobility are handled by:

1. Introducing new messages: *Join_group*, *Spec*, *Mspec* and *Terminate*. These messages are handled by the mobility agents of the network only. Other nodes of the network need not be aware of these messages.

2. Augmenting Integrated Services modules at the switches : The functionality of active and passive reservations can be implemented as part of the integrated services module. The information of active and passive reservations are carried by the RSVP messages, but they are opaque to RSVP.

3. RSVP encapsulation: When a mobile host is not in its home subnet, Mobile-IP uses tunnels to deliver packets to the mobile host. In MRSVP, messages are tunnelled using RSVP encapsulation which allows resource reservation inside a tunnel.

We are currently investigating into the issues related to scalability and security in MRSVP. The detailed specification of MRSVP[24] will be submitted as an Internet Request For Comments. We are also implementing this protocol and determining its performance overhead.

References

[1] Acampora, A. S. and Naghshineh, M., An Architecture and methodology for Mobile-executed Handoff in Cellular ATM Networks., IEEE JSAC, Vol 12, No. 8, October 1994.

[2] Bakre, A. and Badrinath, B. R., Handoff and system support for indirect TCP/IP, In Proc. of the 2nd Usenix symposium on mobile and location independent computing, pp. 11-24, April 1995.

[3] Badrinath, B. R. and Talukdar, A. K., IPv6 + Mobile-IP + MRSVP = Internet Cellular Phone?, In Proceedings of the Fifth IFIP International Workshop on Quality of Service, Columbia University, New York, USA, May 21-23, 1997, pp. 49-52.

[4] Balakrishnan, Hari, et. al., A comparison of mechanisms for improving TCP performance over wireless links, In Proc. of the ACM SIGCOMM, Stanford, CA., August 1996.

[5] Ballardie, A. J., Francis, P. F. and Crowcroft, J., Core Based Trees, In Proceedings of the ACM SIGCOMM, San Francisco, 1993.

[6] Ballardie, A., Core Based Trees (CBT) Multicast Routing: Protocol Specification, Internet Draft, Work in Progress, March 1997.

[7] Clark, D.D., Shenker, S. and Zhang, L., Supporting Real-Time Applications In An Integrated Services Packet Network : Architecture and Mechanism., Proc. SIGCOMM '92, 1992.

[8] Deering, S. E., Editor, ICMP Router Discovery Messages, RFC 1256, September 1991.

[9] Deering, S. E. and Hinden, R. M., Internet Protocol version 6 (IPv6) specification. Internet Request For Comments RFC 1883, December 1995.

[10] Droms, R., Dynamic Host Configuration Protocol, RFC 1541, October 1993.

[11] Estrin, D. *et. al.*, Protocol Independent Multicast-Sparse Mode (PIM-SM): Motivation and Architecture, Internet Draft, Work in Progress, October 1996.

[12] Estrin, D. *et. al.*, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, Proposed Experimental RFC, September 1996. Work in Progress, October 1996.

[13] Jamin, S., Danzig, P.B., Shenker, S and Zhang, L., A Measurement-based Admission Control Algorithm for Integrated Services Packet Networks., Proc. SIGCOMM '95, 1995.

[14] Keeton, K., Mah, B., Seshan, S., Katz, R. and Ferrari, D., Providing Connection-Oriented Network Services to Mobile Hosts, In Proc. of the 1st Usenix symposium on mobile and location independent computing, August 1995

[15] Lee, K., Adaptive Network Support for Mobile Multimedia, In Proc. of the 1st Annual International Conference on Mobile Computing and Networking, pp. 62-74, November 1995.

[16] Levine, D. A., Akyldiz, I. F. and Naghshineh, M., The Shadow Cluster Concept for Resource Allocation and Call Admission in ATM-Based Wireless Networks, In Proc. of the 1st Annual International Conference on Mobile Computing and Networking, pp. 62-74, November 1995.

[17] Lu, S. and Bharghavan, V., Adaptive Resource Management Algorithms for Indoor Mobile Computing Environments, Proc. SIGCOMM'96, August 1996.

[18] Perkins, C., Editor. IP mobility support. Internet-Draft, draft-ietf-mobileip-protocol-17.txt, May 1996. Work in progress.

[19] Perkins, C. and Johnson, D. B., Mobility Support in IPv6, In Proc. of the 2nd Annual International Conference of Mobile Computing and Networking, November 1996.

[20] Postel, J., User Datagram Protocol, STD 6, RFC 768, August 1980.

[21] Singh, S., Quality of Service Measures in Mobile Computing, Journal of Computer Communications, Vol. 19(1996).

[22] Talukdar, A. K., Badrinath, B. R. and Acharya, A., On Accommodating Mobile Hosts in an Integrated Services Packet Network, In the Proceedings of the IEEE INFOCOM'97, April 1997.

[23] Talukdar, A. K., Badrinath, B. R. and Acharya, A., Integrated Services Packet Networks with Mobile Hosts: Architecture and Performance, Submitted for Journal Publication, July 1997.

[24] Talukdar, A. K., An Architecture for Integrated Services in Mobile Networks, Ph.D. theses in preparation, Department of Computer Science, Rutgers University, USA.

[25] Veizades, J., Guttman, E., Perkins, C. and Kaplan, S., Service Location protocol, RFC 2165, June 1997.

[26] Wroclawski, J., The Use of RSVP with Integrated Services, Internet Draft, Work in Progress, October 1996.

[27] Zhang, L., Deering, S., Estrin, D., Shenker, S. and Zappala, D., RSVP: A New Resource ReSerVation Protocol. IEEE Network Sept. 1993.