Application-Layer Multicast for Mobile Users in Diverse Networks

Jasmine Chennikara*, Wai Chen*, Ashutosh Dutta*, Onur Altintas**

*Telcordia Technologies Inc., 445 South Street, Morristown, NJ 07960
** Toyota InfoTechnology Center, 4009 Miranda Avenue, Palo Alto, CA 94304

Abstract

As multicast services become prevalent, it is important to find viable solutions for multicasting to mobile nodes. This problem is complicated by the necessity to support multicast services over existing backbone and access networks which may have varying network and/or link layer multicasting capabilities. While most work on supporting multicast services focuses on the IP layer solution, we propose an application-layer approach to providing multicast services to mobile users traversing networks with diverse multicast capabilities. We propose placing multicast proxies in the backbone and access networks to provide several multicast-related functions at the application layer including creating virtual application-layer multicast trees for dynamically tunneling through non-multicast-capable networks. In this paper, we describe our proposed application-layer multicast architecture and its advantages to third-party service providers for multicasting to mobile users in diverse networks.

I. INTRODUCTION

Multicasting services are increasing in popularity as service providers take advantage of multicasting solutions to efficiently distribute content to a large number of users. For example, multicasting can be used to provide streaming content such as news or video to many subscribers. Additionally, multicast services could be used to provide location-based information such as traffic reports and advertisements tailored for users in a specific geographical area. While these applications gain performance when the underlying network supporting them have multicasting capabilities, the networks are not consistent in this capability across the entire infrastructure reaching the user. This is especially true when IP multicasting is not ubiquitous to all networks. The quality of multicast services also becomes problematic when service providers consider the wireless network environment and the maintenance of multicast sessions to users moving through various access network types.

Multicast services are supported currently by the deployment of techniques such as IP multicasting in the network to efficiently handle these applications. IP-layer multicast solutions for wired networks have been thoroughly investigated for non-mobile users. Joining and advertisement of multicast groups is handled through standard protocols such as IGMP (Internet Group Management Protocol) [1][2]. Multicast packets are generally routed along a single shared tree or multiple source-based spanning trees for efficient distribution. Optimized paths are established and maintained by multicast routing protocols such as PIM [3][4]. While general multicast techniques do not handle large numbers of distinct multicast groups which may be needed to designate location-specific multicast services, Explicit Multicast and SSM solutions have been proposed to address this problem. Explicit Multicast (Xcast) [5] packets include addresses of all nodes in the multicast group and is useful if the membership in each group is small. In source specific multicast (SSM) [6] each multicast group is not only defined by a multicast address but also by a sending, or source, IP address. Thus, SSM allows content providers to support services without requiring a unique IP multicast address. These techniques can be used to support localized services whereby a single address is used to specify a location-based service but a different source may be used in each location.

Although multicast-related work has been done in wired networks, wireless networks introduce other considerations. It is desirable from the user's point of view to maintain multicast services from any point of attachment to the network. For example, users in cars moving through different access networks will desire the capability to continuously receive multicast streams and location-specific information.

Research relevant to support multicasting for mobile nodes, has been done specifically for Mobile IP [7]. The bi-directional tunneling solution for Mobile IP puts the burden of forwarding the multicast packets to mobile users on the Home Agent (HA). However, when an HA has a number of users in the same multicast group visiting the same foreign network, tunneling multiple multicast packets to the foreign network is inefficient. To avoid the duplication of multicast packets, remote subscription has been proposed whereby a user desiring to join a multicast group will do so in each visited network through the Foreign agent (FA). However, this requires that after every handoff the user must rejoin a multicast group. In addition, the multicast trees used to route multicast packets will be updated after every handoff to track multicast group membership. To limit tree updates and duplication of multicast packets, proxies or agent-based solutions have also been proposed [8][9][10].

Current multicast solutions rely on knowledge and control of the network routers to perform multicast routing. However, the deployment of multicast has not been completed and is not ubiquitous to all wireline and wireless networks. Tunneling techniques have been proposed to route IP multicast packets to stationary users across non-multicast-enabled networks. Automatic Multicast Tunneling (AMT) [11] uses an encapsulation interface which takes multicast IP packets and encapsulates them in unicast packets to traverse over unicast-only networks. Similarly, UDP Multicast Tunneling Protocol (UMTP) [12] encapsulates UDP multicast packets and tunnels them through non-multicast capable networks.

Service providers require the ability to efficiently multicast to mobile users through various networks. From the service

provider's point of view, this requires some understanding of the multicasting capabilities in the various access networks over which service is provided. In most cases, the service provider will have limited knowledge and control over the backbone and/or the access networks. In addition, the service provider must be able to track the location of the mobile users in order to update and maintain location-based services. For example, in each new local area, the multicast group membership may change in order to reflect a different filter for the appropriate location–specific information.

Our proposed solution provides an infrastructure to evolve with the multicast capabilities of the network based on application-layer multicast and tunneling techniques. Although there has been some work to support multicast using an application-layer approach [12], our architecture supports user mobility through access networks with varying multicast capabilities. We introduce additional elements in the backbone and access networks to identify and tailor multicast services to users based on the location and access network information.

In Section II we detail our considerations in designing the application-layer multicast approach. In Section III we describe an application-layer multicast architecture to support third-party multicast services. We discuss multicasting using our architecture in Section IV and mobility support in Section V. In Section VI we provide our conclusions and future direction.

II. DESIGN CONSDERATIONS

The objective of the application-layer multicast architecture is to provide a solution which allows a service provider to efficiently multicast information from a media server acting as the information source and located in the backbone network to the user roaming across different access networks.

We design the application-layer solution with the following considerations in mind.

- **User mobility during multicast**: As a user moves between networks of different capabilities our solution should be able to maintain multicast sessions and if needed update geographical information for location-specific needs. As part of this, we should be able to handle handoff between dissimilar multicast-capable access networks. Maintaining the multicast session may require updating the multicast group membership as well as updates on the multicast capabilities of the new access network. The solution should take advantage of known information about the access and backbone networks to properly configure user devices and other application-layer elements to use multicast techniques. We also consider the minimum information required from the network provider to understand the multicasting available in the network.
- **Multicasting for location-specific services**: The multicast solution should be able derive location information based on advertised information about the access network or user's local area. The architecture should have the flexibility to handle various location-based filtering mechanisms. In addition, the point where the location information will be used to update the tailoring of services to the user should be near the mobile user to work efficiently. This is especially true if users are highly mobile and constant location updates will be outdated quickly if forwarded to remote network elements.
- **Multicast address management**: We also consider how to handle addressing when there may be many multicast groups. This is true if we have many location-based services and plan to use a different multicast address for each local area. If indeed unique multicast addresses are required, we then need to consider the interaction between the address manager and the set-up of local multicast proxies for specific services.

To support these goals and provide a flexible architecture to use the underlying network capabilities, we propose an application-layer solution. This would allow third-party service providers to support multicast services across access and backbone networks with incompatible multicast capabilities. The multicast architecture should overlay on the existing backbone and access network but take advantage of underlying multicast capabilities when possible. In addition, the architecture chosen should require limited control and knowledge of the underlying capabilities of the access and backbone networks.

III. ARCHITECTURE OVERVIEW

We propose an application-layer multicast architecture to support the multicast services from third-party service providers to mobile users. We accomplish our goals by establishing servers as multicast proxies in the backbone network and the edges of the access networks. The proxies will relay information from the media server to the users across diverse networks. The proxies along with the user devices will form virtual networks which will be under the full control of the service provider. The virtual network consists of three types of entities, the backbone proxies, the local proxies and the user devices as shown in Figure 1. We describe the functions of each for supporting multicast in the following sections.

A. Backbone Proxy

In the backbone network, the backbone proxies form the virtual network using tunnels (e.g., UMTP) between neighboring backbone proxies. In addition, these proxies can connect to the media servers and act as gateways to the mobile users. The virtual network of proxies can be pre-configured since these nodes are fully controlled by the service provider. The topology and tunneling among the backbone proxies are relatively fixed but can be updated periodically as proxies are removed or added into the

network. In addition, the backbone proxies should have knowledge about whether its part of the network is multicast-enabled or not. This is basic information about the surrounding network that a network provider should be able to supply.

As part of its function, the backbone proxy will intercept multicast packets from the media server. The multicast packets may be forwarded along the multicast route as determined by the multicast IP address and routing tables.

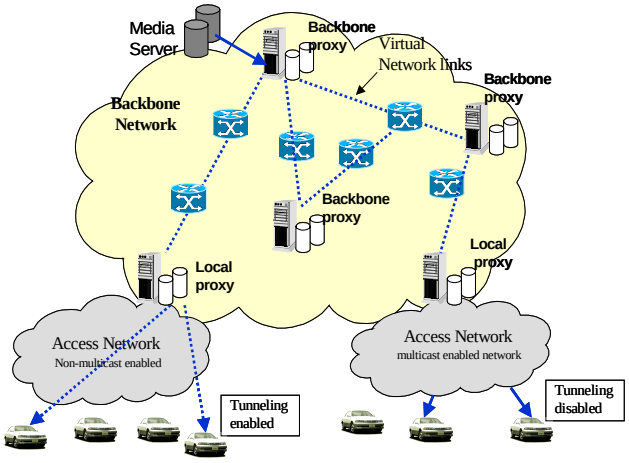

Figure 1: Multicast architecture with virtual network of proxies

The multicast packets can also be tunneled across non-multicast capable networks to the next-hop backbone proxy in order to reach the mobile user. The next-hop proxy is determined from the virtual network routing information. For different multicast groups, the virtual network can be used to form different virtual multicast trees, which will efficiently route tunneled multicast packets through the backbone network.

B. Local Proxy

Servers will also be located at the edge of the access network to act as local multicast proxies within the access network. The local area that the local multicast proxy manages may consist of one or more access networks depending on the geographical coverage of the access networks. The local proxies will join the virtual network of backbone proxies. They will advertise their multicast services to users in the local area and identify the proper multicast groups to join, if desired. Service requests from the user are intercepted by the local proxies which will also act as a gateway for the user to reach servers in the backbone networks. In addition, the proxy will determine the multicast capabilities of the access networks and tunnel through the access network to the user if no multicast is available at the lower network layers.

Local proxies may also support other functions. The local proxies can be used to provide seamless handoff of mobile users traversing access networks while in a multicast session. For non-location specific application, this is accomplished by allowing users to maintain the same multicast address even though a user's IP address may change. The local proxy may also filter information received from the media server and tailor it for the specific location-based multicast service. Thus for location-based information, handoff between the current local proxies and the target local proxies may be supported using soft handoff techniques which will allow users to maintain location services while local proxies update location-based information.

C. User Device

The user device, typically located within a moving vehicle, will have the capability of joining specific multicast groups through the local proxy using IGMP or RTCP[14]. It will receive IP multicast packets or tunneled multicast packets from the local proxies while in the local area of the proxies. The user devices may have a number of tunneling techniques it is capable of utilizing to handle multicast packets received in a non-multicast-capable access network. Thus, the user devices will have the capability of switching the tunneling on and off as required as they traverse various access network types. The tunneling is triggered by the capability of the access network as advertised by the local proxy.

IV. MULTICASTING

The proposed multicast architecture has the capability to use IP multicast when available. However, general multicast requires that unique multicast IP addresses must be used to identify a multicast group. This requires negotiation with a global multicast address allocation server to determine unique multicast addresses for each multicast service. This is even more difficult if unique multicast addresses are needed for each local area for the purposes of location-based services.

In order to manage multiple groups for multicast services, we propose using the Source Specific Multicast [6] scheme which identifies a multicast group by both the source IP address and the IP multicast address. The source address would be provided by the media server supporting the service. A backbone proxy can be selected to assign multicast addresses for multicast services in local areas. Both TTL scoped and administratively scoped multicast address management may be considered in order to minimize the multicast address management overhead required for assigning unique multicast addresses to each multicast group in each local area.

For different applications, the multicast group membership may implemented in such as way that membership changes for each coverage area. For example, video multicast may be identified by the same server and multicast address in a number of adjacent local areas since this information may not be filtered to be location-specific. On the other hand, for location-specific applications, it is more likely that there will be many distinct multicast groups, i.e., one for each local area. For local information, such as traffic conditions and advertisements, a common multicast address may be used in

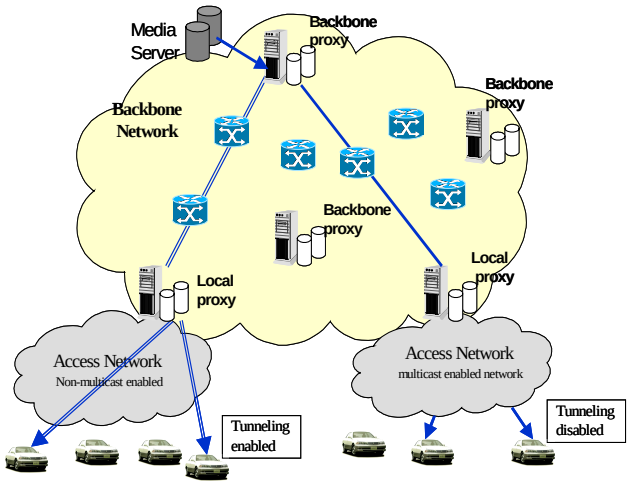

Figure 2: Multicasting through multicast-capable and non-multicast-enabled networks

every coverage area, but the server address may be different to provide the correct local information for the coverage area.

Consider the scenario shown in Figure 2. The users in both access networks desire certain services from the media server. They contact their local proxies who will forward their request to the backbone proxy. Part of the local proxy's request may be to join the multicast group or create a virtual route to the local proxy. For example, for the path on the left side of the backbone and access network, we assume that the backbone network has no multicast capability so packets are tunneled across the virtual links to the local proxy. The virtual links chosen in the backbone should be used to setup a multicast tree for efficient distribution to local proxies whose users require the same service. The virtual route to the various local proxies can be quickly determined from the topology tables already pre-configured in the backbone proxies. In addition, since the access network is not multicast capable, the local proxies tunnel the packets to the mobile users. The user device will then decapsulate the packets and process the multicast packets that are enclosed.

On the right side of the network, the multicast capabilities are enabled in the backbone and in the access network. As a result, the multicast packets can be sent without interference by either the local or backbone proxies since the underlying IP multicasting will handle the multicast routing. The message flow for a user joining a multicast group through the local proxy is shown in Figure 3. The user would join the multicast group, either locally or globally defined, as advertised by the local proxy based on the information supplied by the service provider. The local proxy may or may not be part of the multicast group. However, the local proxy advertises all services it can potentially support and only joins multicast groups based on the subscription to the specific services by users in its local area. If the local proxy is not already part of the multicast group being requested by the user, it will forward JOINs to backbone proxies. Based on the type of service, the user will join the appropriate multicast group. The backbone proxies will then forward packets to the local proxies using tunneling or native IP multicasting. In turn, the local proxies will send packets using native IP multicasting, or tunneling if the access network does not support multicast. The tunneling will be triggered in the user device to properly decapsulate tunneled multicast packets.

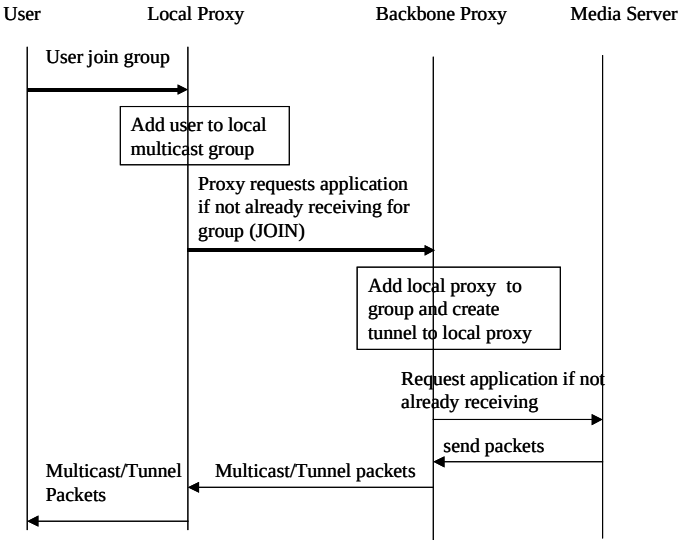

Figure 3: Message flow for multicast JOINs

V. MOBILITY

Mobile users will be traversing various access networks while maintaining multicast sessions. Since the mobility updates, i.e. IP address changes, are controlled by the network carrier, service providers need to be able to quickly react to handoffs in order to update multicast group membership or multicast location-based streams. Using the multicast architecture, we can handoff between networks with similar capabilities, e.g. between two multicast–enabled networks, as well as between networks with dissimilar multicast capabilities, e.g. between multicast and non-multicast enabled access networks. For example, a user may be in a multicast session via a tunneling setup (e.g., UMTP) in a non-multicast-enabled network. When the user then travels toward another network which is multicast-enabled, the proxies in the backbone and the access networks can negotiate among themselves to handle soft handoff of the user into the new access network while maintaining the multicast service. That is, the local proxies can join the multicast group proactively for a mobile user about to enter its local area.

We use Figure 2 again to describe a possible scenario with the source local proxy sitting in a multicast-enabled access network and the target local proxy sitting on the edge of a non-multicast-enabled access network. We can assume the backbone network is multicast capable for simplicity. We also assume there are other users in the same multicast group

in the initial access network or local area but not in the target local area. Since initially the user is in a multicast-enabled access network, the local proxy is part of the IP multicast tree and is not tunneling packets to the user.

When the user begins to move into a new access network it can begin listening for possible services and tunneling options. Based on the service requested by the user, the local proxy will join the multicast group, if it is not part of it already, and then advertise the tunneling technique to the user as shown in Figure 4.

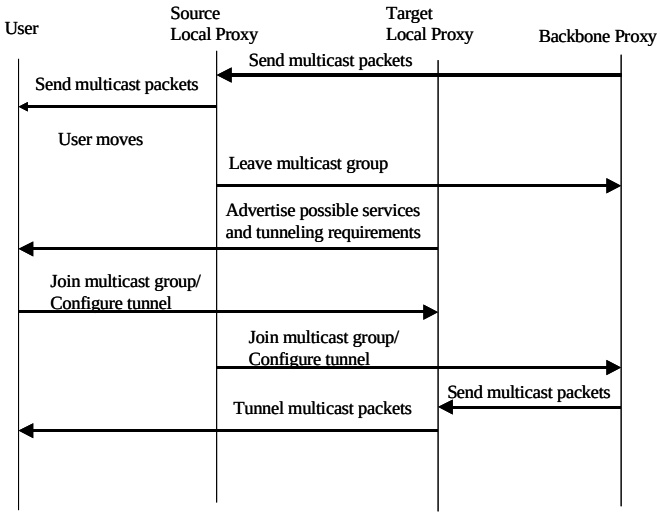

Figure 4: Message Flow for Multicast Handoff

If a user is to be provided location-specific information, the user's geographical location is required to be known by either the media server who is streaming information to the user and/or by the local proxy who is filtering the information to the user. The multicast group may be updated in each area to reflect the new location, either through the multicast address, or source address, if using SSM. There are several ways to determine the user's location. One possible method is to use GPS at the user device. This information will then be communicated to the media server or local proxies which will filter the local news and traffic information accordingly. Another method based on IP address is possible if IP address assignment is location-specific. Then the network provider can supply local proxies with a database of the IP address pools for different locations or access networks.

VI. CONCLUSIONS

While networks slowly migrate to full multicast deployment, there will be backbone and access networks which are not multicast-enabled. We propose an application-layer multicast solution that can take advantage of multicast capabilities at lower network layers while still supporting multicast across non-multicast-enabled networks. In addition, the proposed architecture also supports multicast service continuity to mobile users.

We have utilize virtual networks and multicasting proxies to handle multicasting to mobile users over diverse networks. We create a virtual network of proxies which allows us to take advantage of various levels of multicasting capability in the physical network. By moving multicast to the application layer, we avoid dependency on IP multicast and use tunneling to route multicast packets across networks without IP multicast. In addition, local proxies are used to advertise access network multicast capabilities and dynamically trigger tunnel creation to user devices in access networks which are not multicast-enabled. The local proxies can also act as filters for localized information and support location-based services to mobile users. This provides an interim solution to mobile multicast users while access and backbone networks slowly evolve to full IP multicast-capable networks.

In future work, we plan to continue investigating mobility and proxy-controlled handoff between multicast and non-multicast-capable networks. In addition, we plan to study the use of local multicast proxies to also perform unicast session handoff seamlessly and work with SIP-based mobility.

VII. ACKNOWLEDGEMENT

Authors would like to acknowledge other members of the project Yibei Ling, Yoshihisa Suwa, Harshad Tanna and Sunil Madhani for useful discussions during the project meetings. Ashutosh Dutta would like to acknowledge Henning Schulzrinne of Columbia University for many helpful discussion with respect to content distribution and multicast in general.

VIII. REFERENCES

[1] S. Deering, "Host Extension for IP Multicasting," *IETF RFC 1112*, August 1989.

[2] B. Quinn, "IP Multicast Applications: Challenges and Solutions," *IETF draft-ietf-mboned-mcast-apps-02.txt*, March 2001.

[3] Deering, D. Estrin, D. Farinacci, V. Jacobson, "Protocol Independent Multicast (PIM), Dense Mode Protocol specification," work in progress, March 1994.

[4] Deering, D. Estrin, D. Farinacci, V. Jacobson, L. Ching-gung, and W. Liming, "Protocol Independent Multicast (PIM), Sparse Mode Protocol specification," work in progress, March 1994.

[5] R. Boivie et al. , "Explicit Multicast Basic Specifications, " *IETF draft-ooms-xcast-basic-spec-01.txt*, March 2001.

[6] S. Bhattacharyya et al., "An Overview of Source-Specific Multicast (SSM) Deployment," *IETF draft-ietf-ssm-overview-00.txt*, May 2001.

[7] G. Xylomenos and G. Polyzos, "IP Multicasting for Wireless Mobile Hosts", *IEEE MILCOM*, 1996.

[8] C.L. Tan and S. Pink, "Mobicast: a Multicast Scheme for Wireless Networks", *Mobile Networks and Applications*, 1999.

[9] T.G. Harrison, C.L. Williamson, W.L Mackrell, and R.B. Bunt, "Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts," *Proc. 3rd Inter. Conference on Mobile Computing and Networking (Mobicom 97)*, September 1997.

[10] C.R. Lin and K-M. Wang, "Mobile Multicast Support in IP Networks," *IEICE Trans. Comm.*, Vol. E-84-B, No.2, February 2001.

[11] D. Thaler et al., "IPv4 automatic Multicast without Explicit Tunnels (AMT)," *IETF draft-ietf-mboned-auto-multicast-00.txt*, February 2001.

[12] R. Finlayson, “The UDP Multicast Tunneling Protocol, “ *IETF draft-finalyson-umtp-06.txt*, March 2001.

[13] A. Dutta, H. Schulzrinne, “A Streaming Architecture for Next Generation Internet”, *ICC 2001*.

[14] A. Dutta, Wai Chen, H. Schulzrinne, O. Altintas, “Mobility Support for MarconiNet”, *IEEE Broadband Wireless Summit*, May 2001.