Revista Tecnológica ESPOL, Vol. 18, N. 1, 31-36, (Octubre, 2005), ISSN : 0257-1749

Sobre el Potencial del Multicast en Capa de Aplicación

Cristina Abad Robalino
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
cabad@fiec.espol.edu.ec

Resumen

El multicast en capa IP no ha sido globalmente adoptado debido a una combinación de dificultades técnicas y no técnicas. El multicast en capa de aplicación, también llamado multicast de sistema final o multicast en redes superpuestas, es una alternativa atractiva al multicast IP por razones de administración y costo. Además, con multicast en capa de aplicación (MCA) se pueden establecer sesiones bajo demanda que son escalables a nivel de Internet, y con características de rendimiento adecuadas para distintas aplicaciones. Este artículo describe el MCA, sus usos, ventajas y desventajas, y señala los temas que aún deben ser investigados para facilitar su uso.

Palabras clave: *Multicast, capa de aplicación, sistema final, redes superpuestas, compañero-a-compañero, peer-to-peer, P2P.*

Abstract

IP multicast has not been widely deployed yet, due to a combination of technical and non-technical issues. Application-level multicast–also called end system multicast or overlay multicast–is an alternative to IP multicast usually preferred due to a combination of ease of management and low implementation cost. Furthermore, in application-level multicast (ALM) you can establish on-demand sessions that are largely scalable. This paper describes ALM, its uses, advantages and disadvantages, and identifies further research issues that should be considered.

1. Introducción

Comunicación multicast es un servicio de envío de mensajes de uno-a-muchos en una red de computadoras, con escalabilidad sub-lineal. Este tipo de funcionalidad es requerida (o deseada) para aplicaciones como streaming de archivos multimedia, simulaciones distribuidas, video-conferencias, juegos multi-usuario, distribución de contenidos, etc.

El multicast en capa IP [9] funciona a nivel de la capa de red[1], lo cual lo hace muy eficiente ya que la replicación de mensajes se realiza en los ruteadores. El problema es que aún no ha sido adoptado a nivel de Internet [3]. A los proveedores de servicios de Internet (ISPs) no les interesa habilitar la funcionalidad de multicast en los ruteadores debido a una combinación de "preocupación sobre aspectos de facturación compleja, administración y seguridades" [24]. Además, resulta caro actualizar la infraestructura de la red, y muchas organizaciones a nivel mundial todavía utilizan ruteadores que no soportan multicast IP. Problemas adicionales surgen cuando se desea que las comunicaciones multicast sean confiables[2]. El multicast en capa IP, tal y como fue definido originalmente [9], es un servicio de "mejor esfuerzo". Existen propuestas para lograr multicast confiable [13, 20], pero la falta de estándares y preocupaciones sobre el congestionamiento de la red son un problema. Finalmente, el multicast IP requiere administración para establecer y mantener los grupos, lo cual representa un problema en ambientes altamente dinámicos.

[1] En este artículo, la palabra capa se refiere a una de las siete capas del modelo referencial OSI.

[2] En redes de computadoras, transmisión confiable significa que los mensajes enviados deben llegar a todos los miembros que están funcionando correctamente, y que los mensajes enviados deben llegar a los miembros sin haber sido modificados en el camino.

Recibido: Junio, 2005
Aceptado: Agosto, 2005

El multicast en capa de aplicación (MCA) surgió [7] como una alternativa que no presenta muchos de los problemas del multicast IP. Si bien existen varios protocolos o esquemas de MCA [7, 25, 14, 4, 29, 16, 26, 17, 19, 6, 12], esta área todavía sigue en investigación. Este artículo presenta una visión general del multicast en capa de aplicación e identifica los aspectos que aún deben ser considerados para mejorar y/o complementar las soluciones existentes.

2. Generalidades

Existen programas que necesitan enviar un mismo mensaje a todo un grupo de computadoras. A esta funcionalidad se la llama comunicación de grupos o multicast. Una alternativa sencilla es hacer que el origen envíe una copia del mensaje a cada miembro del grupo. El problema es que esta solución "ingenua" es muy ineficiente y no es escalable a grupos grandes. En cambio, en el multicast IP, la red (es decir, los ruteadores) es la encargada de enviar los mensajes a cada miembro del grupo. El multicast IP es eficiente ya que los ruteadores conocen la topología física de la red y se aseguran de que este envío sea eficiente. El problema es que esta funcionalidad consume recursos de los ruteadores, por lo que sus administradores no tienen un incentivo para habilitarla. Por esta razón surgió como alternativa el multicast en capa de aplicación. Este multicast funciona con el esquema de redes superpuestas. Una red superpuesta es una red lógica formada por enlaces lógicos entre computadoras, independientes de la topología de la red física. Esto implica un costo mínimo ya que no requiere de ninguna funcionalidad a más de un software especial instalado en los computadores participantes. Por esta razón, el MCA ha tenido una gran acogida y ha sido utilizado exitosamente en una gran variedad de sistemas distribuidos.

La Figura 2 muestra las diferencias de estas tres soluciones para la comunicación de grupos.

3. Alternativas de diseño

Para entender la diferencia entre los diferentes protocolos de MCAs existentes, es necesario analizar diferentes aspectos de redes superpuestas que afectan el rendimiento de ellas.

3.1. Organización

En cuanto a su organización, las redes superpuestas se clasifican en estructuradas y no estructuradas. Las redes no estructuradas forman un grafo en el cual la relación entre los nodos no sigue ningún patrón predefinido. Por otra parte, las redes estructuradas siguen algún patrón para su construcción. Este puede ser alguna organización jerárquica, o más frecuentemente, un mapeo entre el ID de un nodo y su ubicación. A este último tipo de red superpuesta se la conoce como tabla hash distribuida (DHT).

En una red superpuesta no estructurada existen dos mecanismos multicast que se pueden utilizar: un protocolo epidémico o una estructura de distribución.

Los protocolos epidémicos se denominan así porque propagan mensajes a una manera infecciosa o también llamada "chismosa". En un protocolo epidémico, el origen envía el mensaje a todos sus vecinos en la red superpuesta. Sus vecinos lo re-envían a todos sus vecinos y así sucesivamente. De esta manera los mensajes se propagan a todos los miembros del grupo. Como la red superpuesta contiene enlaces redundantes, es posible que un nodo reciba un mensaje duplicado. En dicho caso, el nodo simplemente lo descarta en lugar de re-enviarlo. Estos protocolos proporcionan garantías de confiabilidad probabilísticas muy buenas, pero a un costo de una sobrecarga excesiva en el envío de mensajes, ya que los nodos reciben múltiples copias de cada mensaje. A la técnica de enviar o "chismear" mensajes utilizada por los protocolos epidémicos también se la llama "inundación".

El enfoque de la estructura de distribución consiste en establecer una estructura (generalmente un árbol) sobre la red superpuesta, que incluya enlaces únicos a cada nodo. Para enviar un mensaje a todos los miembros de la red, el origen lo envía a sus vecinos en la estructura (no a sus vecinos en la red superpuesta), y cada nodo lo re-envía de esta misma manera. Al final, todos recibirán el mensaje una sola vez. El principal problema de este enfoque es que si un nodo falla en el re-envío, todos los nodos que dependían de este nodo (y sus subsecuentes hijos) no recibirán el mensaje. Además, la eficiencia del multicast depende de qué tan bien se construye el árbol de envíos. Esto quiere decir que los enlaces lógicos deben ir algo acordes a la topología física real, de tal manera que se eviten el uso excesivo de canales de comunicación unicast ineficientes (por ejemplo, conexiones vía modem).

Para el caso de las redes estructuradas, el mecanismo de envío de mensajes multicast depende de la estructura de la red superpuesta. Toda red superpuesta estructurada utilizada en comunicaciones multicast tiene un mecanismo que asegura que todos los nodos reciban los mensajes, siempre y cuando ningún miembro falle durante el proceso. Hay redes que adicionalmente tienen mecanismos para asegurar la recepción de los mensajes aún en la presencia de fallas. El mayor problema de este enfoque es que la estructura de la red generalmente no

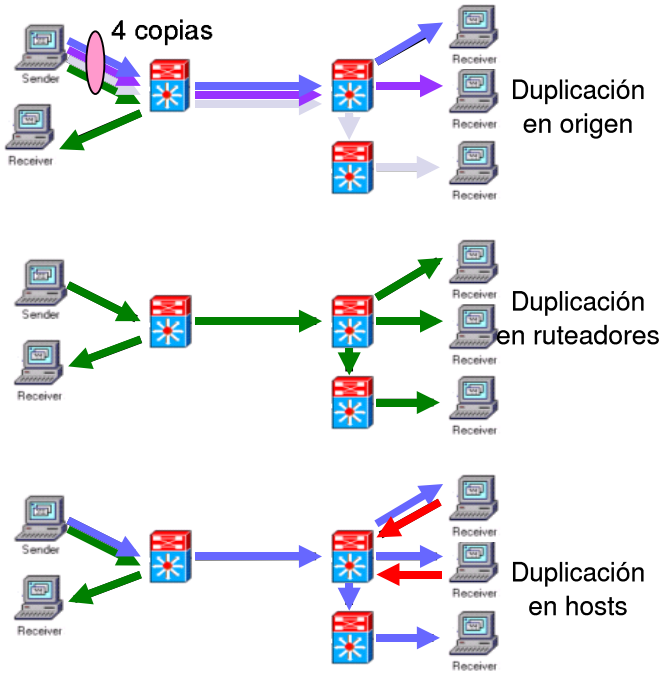

Figura 1: Ejemplo de multicast ingenuo, multicast IP y multicast en capa de aplicación, respectivamente

tiene relación alguna con la topología física de la misma. En estos casos, el resultado es muy ineficiente para comunicaciones multicast.

3.2. Administración

La administración de las redes superpuestas puede ser centralizada o distribuida. Es centralizada cuando se depende de uno o varios nodos especiales que son los encargados de organizar la red. En cambio, en el enfoque distribuido se habla de una arquitectura compañero-a-compañero (peer-to-peer) perfecta, en la que todos los nodos están al mismo nivel y se comunican entre sí para organizarse. El enfoque centralizado tiende a generar redes superpuestas más eficientes, pero al costo de una baja tolerancia a fallos, ya que si el nodo administrador falla, la red no puede seguir funcionando. En cambio, en el enfoque distribuido, existe una sobrecarga por los mensajes de control que intercambian los miembros del grupo, pero a través de este mecanismo logra tener una gran tolerancia a fallos.

3.3. Medida de cercanía

Muchos protocolos de redes superpuestas utilizan alguna medida de cercanía al momento de añadir enlaces a la red, de tal manera que la red resultante se apegue lo mejor posible a la topología física de la misma y sea lo más eficiente posible en el envío de mensajes. El problema es que estas medidas de cercanía, a nivel de capa de aplicación, no son muy exactas y pueden ser costosas de obtener. Ejemplos de medidas de cercanía utilizadas son latencia, pérdida de mensajes, tasa de transferencia extremo-a-extremo, tiempo de descarga, número de saltos en la ruta, entre otras.

La latencia de ida-y-vuelta (o RTT por sus siglas en inglés) es la demora entre el envío de un mensaje a otro nodo y la respuesta que se recibe del mismo. Por esta razón, la latencia mide tanto la cercanía de los nodos, como la capacidad de los canales entre ellos (por ejemplo, dos nodos conectados vía un par de canales de modem parecen estar muy lejos, aún cuando pueden estar ambos conectados al mismo proveedor de servicios de Internet).

La tasa de transferencia extremo-a-extremo se obtiene dividiendo el tamaño de un mensaje enviado al otro nodo, para el tiempo en que se demoró el destino en recibir el mensaje. Al igual que la latencia, mide tanto la cercanía de los nodos, como la capacidad de los canales entre ellos. La diferencia está en que tiene en consideración el hecho de que la ruta entre dos nodos puede ser muy buena para transmitir paquetes pequeños, pero debido a congestión y otras razones, puede ser mala para transmitir paquetes grandes.

Las otras medidas mencionadas son menos utilizadas ya que miden parámetros menos importantes al momento de organizar la red superpuesta.

3.4. Garantías de entrega

Garantizar que todos los miembros reciban un mensaje que ha sido enviado al grupo es bastante costoso en términos de mensajes de control y mensajes de datos enviados. Por esta razón, ciertos protocolos deciden no proporcionar este tipo de garantías. En cuanto a sus garantías los protocolos de MCA pueden ser *a-lo-mucho-una-vez* (AMU) o *cero-o-más-veces* (CMV). Entrega de *exactamente-una-vez* es imposible obtener en multicast en capa de aplicación.

4. Comparación de protocolos existentes

El Cuadro 4 compara diferentes protocolos MCA existentes en base sus características. Para una descripción detallada de los protocolos listados en el cuadro, ver [2].

5. Desafíos

Esta sección describe varios desafíos que se presentan a los desarrolladores de esquemas de multicast en capa de aplicación para obtener un servicio que sea útil a la gran gama de aplicaciones que necesitan de algún mecanismo de comunicación de grupos.

5.1. Escalabilidad

Para muchas aplicaciones, una solución multicast para pequeños y medianos grupos es suficiente. Pero para otras se necesita una solución escalable a grandes grupos. Ejemplos de este tipo de aplicaciones son las de noticias en tiempo real y las de carteleras de acciones de la bolsa. Algunos de los esquemas comparados dicen ser escalables a grandes grupos, pero es necesario un estudio más detallado con simulaciones adicionales así como pruebas reales a gran escala que permitan entender mejor las características de escalabilidad de dichas soluciones.

Un esquema de multicast puede no ser escalable debido a varias razones, incluyendo la cantidad de estado almacenado en cada nodo y la sobrecarga debido al número de mensajes de control enviados. Las sondas utilizadas por varios protocolos con la finalidad de mejorar la calidad de la red superpuesta pueden resultar abrumadoras (en cuanto a tráfico) a medida que el tamaño de la red aumenta. Nakao y otros [22] propusieron la creación de un servicio compartido para redes superpuestas que pueda ser utilizado para obtener información específica como demora de latencia y ancho de banda de diferentes rutas, y que pueda ser utilizado para construir redes superpuestas eficientes. Esta idea pretende incrementar la eficiencia y aumentar la escalabilidad ya que estas medidas pueden ser compartidas por diferentes redes superpuestas, que de otra manera deberían obtenerlas independientemente. El uso de este servicio reduciría el número de sondas enviadas, incrementando la escalabilidad.

5.2. Tolerancia a fallos

En un sistema distribuido los hosts tienen muchas responsabilidades pero a la vez son susceptibles a daños súbitos. Cualquier protocolo de multicast en capa de aplicación debe ser tolerante a fallos. A más de poder recuperarse de fallos, esta recuperación idealmente debe ser distribuida, rápida y no debe requerir el intercambio de un gran número de mensajes. En caso de fallos, las comunicaciones entre los hosts que no han fallado deben poder continuar. Además, el grupo debe poder recuperarse de particiones y rápidamente converger a una red superpuesta eficiente.

5.3. Rendimiento

En lo que respecta a rendimiento del procesamiento (throughput) y demora (latencia), la sobrecarga del protocolo multicast no debe degradar el rendimiento de las aplicaciones. Se deben utilizar medidas de "cercanía" tales como demora, ancho de banda del cuello de botella, etc. para mejorar la calidad de las redes superpuestas, sobre todo si el grupo es grande.

5.4. Calidad del servicio

Algunas aplicaciones como multimedia en tiempo real necesitan garantías de entrega de sus paquetes (en términos de la latencia de dichos paquetes). Ciertas aplicaciones tienen requerimientos flexibles, mientras otras tienen requerimientos estrictos. Ciertos protocolos recientes han sido diseñados con la finalidad de que proporcionen ciertas garantías de calidad de servicio para streaming multimedia [8], pero aún queda por ver la eficacia de estos protocolos antes de que podamos distribuir multimedia en tiempo real a nivel de una red en capa de aplicación.

5.5. Seguridades

La seguridad informática puede ser definida en términos de confidencialidad, integridad y disponibilidad. En el contexto del MCA, la *confidencialidad* se refiere a que solamente los miembros del grupo deben poder leer los mensajes enviados al grupo. La *integridad* se refiere a que los hosts deben poder verificar el origen de un mensaje, y confirmar que los mensajes no

Cuadro 1: Características de varios protocolos de multicast en capa de aplicación

	Ruteo	Construcción de árbol multicast	Tipo de árbol	Administración red superpuesta	Tamaño grupo	Medida de cercanía	Garantías de entrega
Narada	Árbol	Malla primero	Por cada origen	Distribuida	Pequeño	Latencia	AMU
ALMI	Árbol	Malla primero	Compartido	Centralizada	Mediano	Latencia	AMU
Yoid	Árbol	Árbol primero	Compartido	Distribuida	Mediano	Pérdida de datos	CMV
NICE	Árbol	Implícito	Por cada origen	Distribuida	Grande	Latencia	AMU
Bayeux	Árbol	Implícito/Malla primera	Por cada origen	Distribuida	Grande	ninguna	AMU
CAN	Inundación inteligente	N/A	N/A	Distribuida	Grande	Latencia	CMV
Scribe	Árbol	Similar a RPF	Compartido para un origen	Distribuida	Grande	Latencia	AMU
SplitStream	Árboles Múltiples	Cualquiera	Por cada origen	Distribuida	Grande	Latencia	AMU
Bullet	Malla	Cualquiera	Por cada origen	Distribuida	Grande	Ancho de banda extremo-a-extremo	CMV
Lpbcast	Inundación aleatoria	N/A	N/A	Distribuida	Grande	ninguna	CMV
BTP	Árbol	Árbol primero	Árbol Compartido	Distribuida	Mediano	Latencia	AMU
Overcast	Árbol	Árbol primero	Compartido	Distribuida	No comparable	Tiempo de descarga de 10KB & distancia de *traceroute*	AMU
HostCast	Árbol	Árbol primero	Por cada origen	Distribuida	Mediano	Ancho de banda disponible & latencia en ruta al origen	AMU

hayan sido alterados en el camino. Además, los protocolos MCA confían que los hosts sigan el protocolo tal y como fue diseñado. Si un host no sigue el protocolo a su conveniencia o retrasa los mensajes, este puede fácilmente afectar la *disponibilidad* del servicio.

En el ámbito de las seguridades en redes superpuestas, los trabajos investigativos se han concentrado en proporcionar anonimidad [27, 15], estudiar la disponibilidad [17, 5, 11] y la autenticación [18]. Recientemente, el caso específico de seguridades para MCA ha tomado algo de importancia. Mathy y otros [21] analizaron el efecto pernicioso de compañeros que mienten durante las sondas para obtener medidas de cercanía. Nicolosi y otros [23] estudiaron el envío de confirmaciones (ACKs) seguras. La distribución de llaves secretas con la finalidad de obtener confidencialidad en MCA también ha sido estudiada recientemente [1, 28]. A pesar de esto, aún existen aspectos de seguridades no estudiados. Dondeti y otros [10] identificaron los siguientes aspectos a considerar para obtener un servicio de multicast seguro y escalable: control de membresías del grupo, confiabilidad, disponibilidad, escalabilidad, confidencialidad, políticas y esquemas seguros de distribución de llaves secretas.

6. Usos

El Cuadro 6 muestra varios tipos de aplicaciones y sus necesidades con respecto a un servicio de multicast. Como puede observarse, diferentes aplicaciones tienen requerimientos diferentes. Por esta razón, no puede existir una solución genérica de MCA. En su lugar, deben existir diferentes soluciones cada una con sus características propias, de las cuales una aplicación pueda escoger para que se acople mejor a sus necesidades. Cabe recalcar que ninguno de los esquemas existentes da soporte a comunicaciones seguras.

Otro tipo de aplicaciones que no se mencionan en el cuadro pero que también utilizan alguna variante de MCA son las aplicaciones compañero-a-compañero (peer-to-peer) como por ejemplo las redes P2P para compartir archivos. En esas redes, un cliente desea obtener un archivo y envía una búsqueda a la red, la cual es divulgada utilizando algún esquema de MCA. Los detalles de implementación dependen de la red.

7. Conclusiones

Este artículo describió a los protocolos de multicast en capa de aplicación, su estado actual, sus características y sus usos. El tener un mejor entendimiento de estos esquemas es crucial para tomar decisiones bien informadas con respecto a qué protocolo utilizar dependiendo de las características de cada aplicación. Además, se incluyó una sección sobre los desafíos al diseñar un protocolo de multicast en capa de aplicación, a la vez que se identificó ciertas áreas que deberían profundizarse en trabajos investigativos futuros.

Referencias

[1] C. Abad, I. Gupta, and W. Yurcik. Adding confidentiality to application layer multicast by leveraging the multicast overlay. In *Proc. of IEEE Intl. Conf. on Distributed Computing Sys. (ICDCS 2005) Workshops*, June 2005.

[2] C. Abad, W. Yurcik, and R. H. Campbell. A survey and comparison of end-system overlay multicast solutions suitable for network centric warfare. In *Proc. of SPIE*, volume 5441, pages 215–226, Orlando, FL, July 2004.

[3] M. Ammar. Why Johnny can't multicast: Lessons about the evolution of the Internet, 2003. Presented in: The 13th Intl. Workshop on Network and Operating Sys. Support for Digital Audio and Video (NOSSDAV 2003). Slides available at: <`http://www.cc.gatech.edu/fac/Mostafa.Ammar/nossdav-key.ppt`>.

[4] S. Banerjee, B. Bhattacharjee, and C. Kommareddy. Scalable application layer multicast. In *Proc. of ACM SIGCOMM*, pages 205–217, Pittsburgh, PA, Aug. 2002.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. Wallach. Secure routing for structured peer-to-peer overlay networks. In *Proc. of Usenix Symp. on Operating Sys. Design and Impl. (OSDI)*, pages 299–314, Boston, MA, Dec. 2002.

Cuadro 2: Aplicaciones y sus características

Aplicación	Fuente	Tráfico	Tamaño grupo	Variabilidad de membresías
Pizarrón compartido	Múltiples	Pequeño	Pequeño	Baja
Juegos multi-usuario	Múltiples	Mediano	Mediano-Grande	Mediana-Alta
Cartelera de noticias/acciones de la bolsa de valores	Única	Pequeño	Grande	Alta
Simulaciones distribuidas	Múltiples/Única	Grande	Mediano	Mediana-Alta
Multimedia en tiempo real a pequeña escala	Única	Grande	Pequeño	Baja-Mediana
Multimedia en tiempo real escala corporativa o de campus	Única	Grande	Mediano	Mediana
Multimedia en tiempo real a nivel de Internet	Única	Grande	Grande	Alta
Distribución de archivos grandes (ej.: ISOs de Linus)	Única	Grande	Grande	Alta
Video conferencias	Múltiples	Grande	Pequeño	Baja

[6] M. Castro, P. Druschel, A.-M. Kermarrec, A. Nandi, A. Rowstron, and A. Singh. Splitstream: High-bandwidth multicast in cooperative environments. In *Proc. of the 20th ACM Symp. on Operating Sys. Principles (SOSP)*, Oct. 2003.

[7] Y.-H. Chu, S. G. Rao, S. Seshan, and H. Zhang. A case for end system multicast. *IEEE J-SAC*, 20(8):1456–1471, Oct. 2002.

[8] Y. Cui, B. Li, and K. Nahrstedt. oStream: Asynchronous streaming multicast in application-layer overlay networks. *IEEE J-SAC*, 22(1), Jan. 2004.

[9] S. E. Deering and D. R. Cheriton. Multicast routing in datagram internetworks and extended LANs. *ACM Trans. on Computer Sys.*, 8(2):85–110, May 1990.

[10] L. R. Dondeti, S. Mukherjee, and A. Samal. Survey and comparison of secure group communication protocols. Technical Report, University of Nebraska-Lincoln, 1999.

[11] J. R. Douceur. The Sybil attack. In *Proc. of Intl. Workshop on Peer-to-Peer Sys. (IPTPS)*, pages 251–260, Cambridge, MA, Mar. 2002. Springer-Verlag, LNCS 2429.

[12] P. Eugster, S. Handurukande, R. Guerraoui, A.-M. Kermarrec, and P. Kouznetsov. Lightweight probabilistic broadcast. In *Proc. of the Intl. Conf. on Dependable Sys. and Networks (DSN 2001)*, July 2001.

[13] S. Floyd, V. Jacobson, S. McCanne, and L. Zhang. A reliable multicast framework for light-weight sessions and application level framing. *IEEE/ACM Trans. on Networking*, 5(6):784–803, Dec. 1997.

[14] P. Francis, Y. Pryadkin, P. Radoslavov, R. Govindan, and B. Lindell. YOID: Your Own Internet Distribution. Work in Progress.

[15] M. J. Freedman and R. Morris. Tarzan: A peer-to-peer anonymizing network layer. In *Proc. of ACM Conf. on Comp. and Comm. Seccurity (CCS)*, pages 193–206, Washington, DC, Nov. 2002.

[16] D. A. Helder and S. Jamin. End-host multicast communication using switch-tree protocols. In *Proc. of the Workshop on Global and Peer-to-Peer Computing on Large Scale Distributed Sys. (GP2PC)*, May 2002.

[17] J. Jannotti, D. K. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole, Jr. Overcast: Reliable multicasting with an overlay network. In *Proc. of the 4th Usenix Symp. on Operating Sys. Design and Impl. (OSDI)*, Oct. 2000.

[18] W. Josephson, E. Sirer, and F. Schneider. Peer-to-peer authentication with a distributed single sign-on service. In *Proc. of Intl. Workshop on Peer-to-Peer Sys. (IPTPS)*, pages 250–258, San Diego, CA, Feb. 2004. Springer-Verlag, LNCS 3279.

[19] D. Kostic, A. Rodriguez, J. Albrecht, and A. Vahdat. Bullet: High bandwidth data dissemination using an overlay mesh. In *Proc. of the 20th ACM Symp. on Operating Sys. Principles (SOSP)*, Oct. 2003.

[20] J. C.-H. Lin and S. Paul. RMTP: A reliable multicast transport protocol. In *Proc. of the 15th Joint Conf. of the IEEE Computer and Communications Soc. (INFOCOM)*, Mar. 1996.

[21] L. Mathy, N. Blundell, V. Roca, and A. El-Sayed. Impact of simple cheating in application-level multicast. In *Proc. of IEEE INFOCOM*, volume 2, pages 1318–1328, Hong Kong, Mar. 2004.

[22] A. Nakao, L. Peterson, and A. Bavier. A routing underlay for overlay networks. In *Proc. of ACM SIGCOMM*, Aug. 2003.

[23] A. Nicolosi and D. Mazières. Secure acknowledgment of multicast messages in open peer-to-peer networks. In *Proc. of Intl. Workshop on Peer-to-Peer Sys. (IPTPS)*, pages 233–248, San Diego, CA, Feb. 2004. Springer-Verlag, LNCS 3279.

[24] D. Palter. Multicast fan-out saves bandwidth. *Network World*, Sept. 2002. 09/30/02.

[25] D. Pendarakis, S. Shi, D. Verma, and M. Waldvogel. ALMI: An application level multicast infrastructure. In *Proc. of Usenix Symp. on Internet Technologies and Sys. (USITS)*, pages 49–60, San Francisco, CA, Mar. 2001.

[26] S. Ratnasamy, M. Handley, R. Karp, and S. Shenker. Application-level multicast using content-addressable networks. In *Proc. of 3rd Intl. Workshop on Networked Group Communication (NGC)*, Nov. 2001.

[27] M. Waldman and D. Mazi. Tangler: A censorship-resistant publishing system based on document entanglements. In *Proc. of the 8th ACM Conf. on Computer and Communications Security (CCS)*, Nov. 2001.

[28] X. Zhang, S. Lam, and H. Liu. Efficient group rekeying using application-layer multicast. In *Proc. of the IEEE Intl. Conf. on Distributed Computing Sys. (ICDCS 2005)*, June 2005.

[29] S. Q. Zhuang, B. Y. Zhao, A. D. Joseph, R. Katz, and J. Kubiatowicz. Bayeux: An architecture for scalable and fault-tolerant wide-area data dissemination. In *Proc. of the 11th Intl. Workshop on Network and Operating Sys. Support for Digital Audio and Video (NOSSDAV)*, June 2001.