Lightweight Protection Against Inflated Subscription in Multicast Congestion Control

Sergey Gorinsky, Sugat Jain, Harrick Vin, and Yongguang Zhang

Technical Report TR2002-58
Department of Computer Sciences
The University of Texas at Austin
Taylor Hall 2.124, Austin, TX 78712, USA
{*gorinsky, sugat, vin, ygz*}*@cs.utexas.edu*

November 7, 2002

Abstract

Group membership regulation is a useful mechanism for multicast congestion control: RLM, RLC, FLID-DL, and WEBRC form a promising line of multi-group protocols where receivers provide no feedback to the sender but control congestion via group subscription. Unfortunately, the group subscription mechanism also offers receivers an opportunity to elicit self-beneficial bandwidth allocations. In particular, a misbehaving receiver can ignore guidelines for group subscription and choose an unfairly high subscription level in a multi-group multicast session; this poses a serious threat to fairness of bandwidth allocation. In this paper, we present a lightweight solution for the problem of inflated subscription. Our design guards access to multicast groups with dynamic keys and consists of two independent components: DELTA (Distribution of ELigibility To Access) – a novel method for in-band distribution of group keys to receivers that are eligible to access the groups according to the congestion control protocol, and SIGMA (Secure Internet Group Management Architecture) – a generic architecture for key-based group access at edge routers. DELTA and SIGMA are the first to solve the problem of inflated subscription in multi-group protocols for multicast congestion control.

1 Introduction

Traditionally, congestion control protocols *trust* receivers and assume that each receiver always follows its protocol to share the network bandwidth fairly with competing traffic. Unfortunately, with the growth and commercialization of the Internet, the assumption of trusted receivers is no longer tenable. Whereas information sources and network providers have an interest in fair treatment of their receivers, individual receivers have an interest in maximizing their own share of the network bandwidth. Hence, receivers may misbehave to obtain an unfair share of the network bandwidth at the expense of competing traffic. Furthermore, the widespread deployment of open-source operating systems as well as the increasing popularity of peer-to-peer applications and application-level overlay network services create ample opportunities for receiver misbehavior. Consequently, the design of congestion control protocols that are *robust* in the presence of receiver misbehavior is an important research area. In this paper, we address the problem of designing such robust protocols for multicast congestion control.

Multicast [6] is a network service for efficient dissemination of data to a group of receivers. A receiver subscribes to a multicast group by submitting the group address to the local edge router via IGMP [7], and