

Robustness of Multicast Congestion Control to Inflated Subscription

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

Laboratory for Advanced Systems Research
Department of Computer Sciences, University of Texas at Austin
{gorinsky, sugat, vin, ygz}@cs.utexas.edu

Categories and Subject Descriptors

C.2 [Computer-Communication Networks]: Network Architecture and Design

General Terms

Security, Performance, Design

Keywords

Congestion Control, Multicast, Fair Bandwidth Allocation, Misbehaving Receivers, Robustness

1. INTRODUCTION

The Internet has grown from a small testbed shared by a close-knit community of researchers to a global commercial network with a huge number of users. The change in the scale requires revisiting original assumptions in the Internet design and checking whether they match the reality of today. One such assumption is *trust*. Conventional protocols for network bandwidth allocation assume that all communicating parties follow guidelines for fair bandwidth sharing. However, a selfish receiver has incentives to acquire data at an unfairly high rate. Furthermore, open-source operating systems create ample opportunities for receiver misbehavior. For example, Savage et al show that a misbehaving TCP receiver can increase its reliable throughput substantially at the expense of competing traffic [6]. Thus, network research faces a new important challenge of robust bandwidth allocation in the presence of distrusted receivers [2].

Multicast is a service for scalable dissemination of data to a group of receivers: a receiver subscribes to the group by submitting the group address to the local edge router, and the network forwards the data to subscribed receivers. Scalable protocols for multicast congestion control require additional mechanisms, e.g., for feedback aggregation or suppression. To address heterogeneity of receivers, multicast protocols compose a session from multiple groups and provide each receiver with guidelines for choosing a fair subscription level in the session [5]. Resolving the multicast-specific challenges of scalability and heterogeneity opens new opportunities for congestion control misbehavior of receivers.

In this work, we focus on an attack of inflated subscription where a receiver ignores subscription guidelines to acquire

an unfairly high bandwidth. Figure 1(a) presents an NS-2 experiment where FLID-DL [1] receivers F1 and F2 from different sessions share a 1.5 Mbps bottleneck link with four TCP receivers T1, T2, T3, and T4. After 100 seconds, receiver F1 starts misbehaving and inflates its subscription. To resolve subsequent congestion, the well-behaving sessions reduce promptly their bandwidth consumption. Since that time on, F1 enjoys a low loss rate and unfairly high throughput of 1 Mbps. In the next section, we design mechanisms that protect multicast protocols against the threat of inflated subscription.

2. DELTA AND SIGMA

Multicast protocols are vulnerable to inflated subscription because a receiver is able to join any group. Restricted access is then an intuitive solution. Whereas group access control has been researched extensively [4], existing schemes rely on the identity of a receiver to control access. The identity, however, does not prove that the receiver follows subscription guidelines. Thus, robustness to inflated subscription requires an alternative design where the right to access a group is a function of the congestion status:

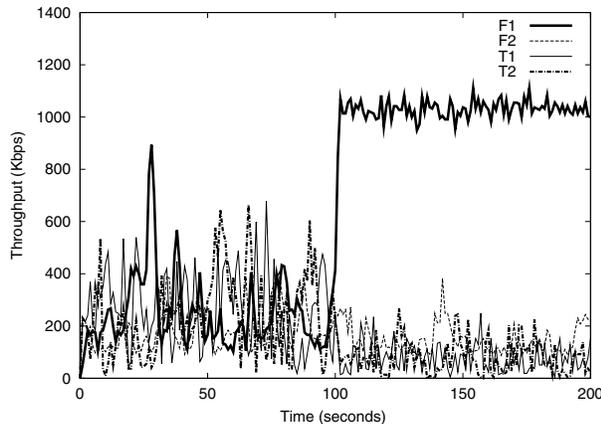
PRINCIPLE 1. Eligibility to access a multicast group should depend on adherence to the congestion control protocol.

Since network conditions change, a receiver that is currently eligible to access a group can become congested and ineligible for the group membership a moment later. Hence,

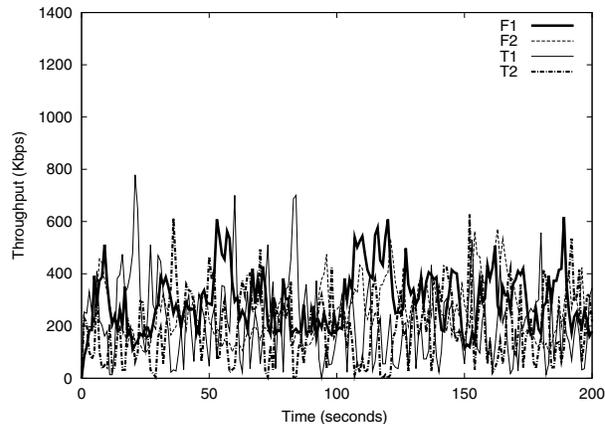
PRINCIPLE 2. Group access control should be dynamic.

Congestion-dependent group access also faces the following challenges:

- **Protocol-specific eligibility.** Different multicast protocols instantiate differently the notions of the congested state (e.g., single packet loss vs. loss rate threshold), subscription level (e.g., layered multicast vs. replicated multicast), and subscription rules. Thus, the right to access a group should be protocol-specific.
- **Generic network support.** Network modifications should be minimal and independent from details of congestion control protocols.
- **Preservation of protocol properties.** Robustness to inflated subscription should preserve efficiency, responsiveness, and other properties of protected congestion control protocols.



(a) Vulnerability of FLID-DL



(b) Robustness of FLID-DS

Figure 1: Protection against inflated subscription.

To meet these requirements, our design employs two components: protocol-specific DELTA (Distribution of ELigibility To Access) and generic SIGMA (Secure Internet Group Management Architecture).

DELTA offers in-band distribution of keys from the sender to eligible receivers. To enable dynamic access enforcement, we introduce a *time slot* as an atomic duration when the right to access a group does not change. A key represents this right. Once per time slot, the sender updates each group key and encodes it into multicast packets so that only eligible receivers can reconstruct the updated key.

Multicast congestion control protocols instantiate DELTA by choosing a protocol-specific encoding of keys into packets. We illustrate this in the context of a replicated multicast protocol where each group delivers the same content at a different rate. The protocol defines congestion as a single packet loss and states two subscription rules: (1) a congested receiver must switch from its current group to a slower group, and (2) when authorized, an uncongested receiver can switch from its current group to a faster group. To enforce these guidelines, the sender adds a nonce to each packet and defines the updated key for a group as XOR over the nonces transmitted to the group during the time slot. Then, only an uncongested receiver can reconstruct the updated key and maintain subscription to its current group. The sender enables switching of a congested receiver to a slower group by including the updated key for this group in each packet of the current group. Finally, when the protocol authorizes switching of an uncongested receiver to a faster group, a packet of the current group carries a bit indicating that the reconstructed key can be used to join the faster group.

In [3], we present a more complex algorithm that protects layered multicast protocols. There, we also explore different definitions of congestion and discuss DELTA instantiations for protocols based on explicit congestion notification, loss rate thresholds, and equation-based group subscription.

SIGMA is a generic architecture for key-based group access. Its distribution of group keys from the sender to edge routers relies on special multicast packets that carry address-key pairs of the groups. Edge routers intercept these packets without forwarding them to receivers and use the obtained

keys to enforce appropriate group access. SIGMA requires network support only from edge routers and is independent from details of protected congestion control protocols.

Figure 1(b) demonstrates that FLID-DS, our adaptation of FLID-DL using DELTA and SIGMA, is immune to inflated subscription. In [3], we show that FLID-DS preserves efficiency and responsiveness of FLID-DL without imposing a significant communication overhead.

3. CONCLUSION

We designed DELTA and SIGMA, a congestion-dependent group access scheme that protects multicast protocols against inflated subscription of misbehaving receivers. The integration of group access and congestion control indicates a need for an integrative alternative to the traditional layered network architecture.

4. REFERENCES

- [1] J. Byers, M. Frumin, G. Horn, M. Luby, M. Mitzenmacher, A. Roetter, and W. Shaver. FLID-DL: Congestion Control for Layered Multicast. In *Proceedings NGC 2000*, November 2000.
- [2] S. Gorinsky, S. Jain, and H. Vin. Multicast Congestion Control with Distrusted Receivers. In *Proceedings NGC 2002*, October 2002.
- [3] S. Gorinsky, S. Jain, H. Vin, and Y. Zhang. Robustness to Inflated Subscription in Multicast Congestion Control. Technical Report TR2003-09, Department of Computer Sciences, UT Austin, April 2003. <http://www.cs.utexas.edu/users/gorinsky/TR03-09.ps>.
- [4] P. Judge and M. Ammar. GOTHIC: A Group Access Control Architecture for Secure Multicast and Anycast. In *Proceedings IEEE INFOCOM 2002*, June 2002.
- [5] M. Luby, V.K. Goyal, S. Skaria, and G.B. Horn. Wave and Equation Based Rate Control Using Multicast Round Trip Time. In *Proceedings ACM SIGCOMM 2002*, August 2002.
- [6] S. Savage, N. Cardwell, D. Wetherall, and T. Anderson. TCP Congestion Control with a Misbehaving Receiver. *ACM Computer Communications Review*, 29(5):71–78, October 1999.