Available online at www.sciencedirect.com
ScienceDirect

Electronic Notes in Theoretical Computer Science 179 (2007) 111–121

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Towards the Construction of Attack Resistant and Efficient Overlay Streaming Topologies

Thorsten Strufe[1] Jens Wildhagen[2] Günter Schäfer[3]

Department of Telematics and Computer Networks
Technische Universität Ilmenau
Ilmenau, Germany

Abstract

Even though overlay streaming is an inherently fault tolerant and stable system architecture, careful neighbor selection is a significant task. Inappropriate routing decisions can lead to an unstable topology with only a few very important nodes on which a large set of succeeding nodes depend. The presented algorithm selects streaming neighbors based on local information, passing knowledge to parent nodes only. Similar to SplitStream [6], it creates inner-node disjoint multicast trees. The created topologies are broad and have short paths, thus improving the resistance to node failure and intentional attacks. A malicious node can neither gain any knowledge about different regions of the topology other than its own successors nor deliberately move to a more important position in the hierarchy. The characteristics of the created topologies are revised in a static simulation study calculating the vertex connectivity and packet loss on node disconnections.

Keywords: Service Availability, Application Layer Multicast, Cooperative Streaming, Resilient Overlay Networks

1 Introduction

Content dissemination generally follows one of three main delivery techniques, client-server-unicast, network multicast or application layer multicast. The client-server system architecture is relatively easy to implement and set-up and currently the prevalent solution. However, it suffers from the draw-backs of being unscalable over the number of clients and having a single point of failure: the server or cluster of servers itself. Though network layer multicast is far more scalable due to data replication in the routers of the backbone, it suffers from low acceptance and is not largely deployed today. This fact is due to a multitude of problems including billing issues and an inherent lack of scalability over the number of multicast groups [13].

[1] Email: thorsten.strufe@tu-ilmenau.de

[2] Email: jens.wildhagen@tu-ilmenau.de

[3] Email: guenter.schaefer@tu-ilmenau.de

doi:10.1016/j.entcs.2006.08.035

Overlay streaming, or application layer multicast (ALM) [7], makes use of the resources at the edge of the network and thus introduces a different load balancing scheme. Due to its self-organization it is inherently resistant towards failure of and attack on nodes. This stability is increased for multi-source systems in contrast to single-source systems, which construct only one single streaming tree. In contrast, every node receives different parts of the content from different nodes, and the nodes are not necessarily reliant on a single preceding node only. Peer-to-peer systems have proven to be very resistant both towards failures and organized interference. The robustness of this system architecture becomes apparent when observing file sharing systems and the efforts to disable them.

In contrast to client-server set-ups cooperative overlays introduce the dynamic of participants joining, leaving and failing during the service, which can cause significant jitter and packet loss. Fortunately, multimedia streaming services can tolerate the loss of a certain fraction of packets. Only if a specific error rate is exceeded, the perceived quality of the presentation drops dramatically. Hence, a streaming system can be defined as working properly as long as all participants receive the stream in an acceptable quality. The damage in turn can be measured by the fraction of defective or missing frames at the receivers.

Overlay streaming systems basically consist of two services:

- a look-up service to locate resources like content and participants
- a streaming service for parent selection and data delivery

In this paper we are concerned with the nature of the streaming service. It has high data rates and is required to efficiently deliver the entire content with strict timing constraints to all participants of the system. The voluminous content can not be cached in large quantities nor can it easily be reproduced. An additional limitation is the fact that the content originates at a single source and is routed through the whole overlay. Every node consequently is dependent on the successful operation of all preceding forwarding nodes, which are part of the path between the source and itself. Every node failure initially leads to the loss of all packets it would have forwarded at all its child nodes and successors. As the bandwidth of participating nodes is limited, the nodes usually cannot maintain a high connectivity or simply switch source nodes. Furthermore, redundant delivery of packets immediately leads to unwanted traffic overhead. These characteristics have the effect, that failures, or even worse, intentional attacks on important nodes in the streaming overlay can have a high impact on the quality of the received service.

While fundamental work has been done to understand fault tolerance of networks [1] and it is comparably easy to create topologies which are resistant to random node failure, accomplishing attack resilience seems a significantly harder task. By implementing quick fall-back strategies and creating topologies with many leaf nodes and a small number of forwarding nodes only, high resilience towards node failure can be achieved. The load in this case is provided by a few nodes only and node failures in the large set of receiving nodes do not have any impact. An attacker however will most probably try to gain as much information about the topology as