# Zugangskontrolle für einen Videoverteildienst mit Multicast

Roland Balmer and Torsten Braun

Institute of Computer Science and Applied Mathematics (IAM), University of Berne,
Neubrückstrasse 10, CH-3012 Bern, Switzerland
balmer@iam.unibe.ch
http://www.iam.unibe.ch/~rvs/

## 1 Einleitung

Mit den weit verbreiteten und immer leistungsfähigeren Zugangsmöglichkeiten zum Internet ist dieses Medium zum Verteilen von Videodaten interessant geworden. Besonders vorteilhaft hierfür ist die Übertragung mittels Multicast, da dadurch Netzwerkressourcen geschont werden. Auf der anderen Seite fehlen bei Multicast Gruppen Zugangsbeschränkungen, die für eine kommerzielle Nutzung unerlässlich sind. Dabei ist weniger der Schutz der transportierten Daten ein Problem, da hierfür konventionelle Verschlüsselungsmethoden eingesetzt werden können. Schwieriger hingegen ist die Absicherung der Ressourcereservierungen, die für eine solche Anwendung nötig sind.

In diesem Beitrag wird eine Architektur beschrieben, die eine Zugangskontrollmechanismus für einen Multicast basierten Videoverteildienst realisiert.

## 2 Videoverteildienst

Der hier verwendete Videoverteildienst soll einen Pay-TV Service basierend auf Multicast realisieren. Folgende Aspekte standen dabei im Vordergrund. Jeder Benutzer hat für empfangenen Videodaten zu bezahlen, der Dienstbetreiber hat die Rechte der transportierten Daten zu schützen und die Daten sollen mit möglichst geringer Verzögerung und ohne Verlust transportiert werden.

Der Benutzer kauft bei einer zentralen Instanz Gutscheine, mit denen er beim Dienstanbieter Schlüssel erwirbt, die er zur Dekodierung der Videodaten benötigt [BB01].

Zur Wahrung der Rechte werden die Videobilder in einzelne Teile zerlegt, mit einem Wasserzeichen versehen und kodiert [KT00][TK00]. Jeder einzelner Teil wird dabei mehrfach in einer separaten Multicast Gruppe gesendet, wobei Kodierung und Markierung jeweils unterschiedlich sind.

Der Benutzer kann nur die Teile verwenden, für die er einen entsprechenden Schlüssel besitzt. Da die Empfänger verschiedene, eindeutige Schlüsselsätze verwenden und sich somit eine einzigartige Version des entsprechenden Bildes zusammensetzen, kann festgestellt werden, welcher Benutzer dieses Bild erhalten bzw. dekodiert hat.

Um sicherzustellen, dass die Daten möglichst verlustfrei und mit wenig Verzögerung ankommen, werden von einer zentralen Instanz im Netz Ressourcen alloziert[BGB01]. Dies wird auf Anfrage des Dienstanbieters hin vorgenommen. Der Netz-Betreiber erhält keine Informationen über einzelne Empfänger, sondern lediglich die Adresse der entsprechenden Multicast Gruppen.

## 3 Zugangskontrolle

Der Netz-Betreiber, der keine Informationen über die einzelnen Benutzer besitzt, benötigt einen Mechanismus um Dienstgüten nur auf Verbindungen zu garantieren, die zu authorisierten Empfängern führen.

In unserer Architektur verwenden wir ein Protokoll zwischen Dienstanbieter (z.B. TV Sender) und Empfängern. Dabei generiert der Sender eine Anfrage, die an alle Benutzer verschickt wird. Alle berechtigten Benutzer erzeugen eine Antwort und senden diese an den Dienstanbieter zurück. Der Netz-Betreiber kann in ausgewählten Knoten kontrollieren, ob die Antworten korrekt sind und entsprechend Ressourcen allozieren. Als Basis für dieses Protokoll wird das Resource Reservation Protocol (RSVP) [BZB+97] verwendet. Dies ist nötig um sicherzustellen, dass Antwort und Anfrage dem selben Pfad, wenn auch in umgekehrter Richtung, folgen.

Die Antwort kann auf verschiedene Weise generiert werden, Eine Möglichkeit ist, dass die Anfrage eine verschlüsselte Signatur enthält, die von authorisierten Empfängern dekodiert und zurückgesendet werden kann. Alternativ können auch die gesendeten, bereits kodierten Videodaten verwendet werden, indem ein bestimmtes Datensegment eines Bildes als Antwort verlangt wird. In beiden Fällen kann der Benutzer nur dann die richtige Antwort zurücksenden, wenn er über einen entsprechenden Schlüssel verfügt. Da die einzelnen Videosegmente in verschiedenen Multicast Gruppen übertragen werden, müssen die Empfänger die Authentifizierung für alle Gruppen vornehmen.

Um zu verhindern, dass ein Netzwerkknoten die Antworten selber überprüfen muss, ist eine zentrale Instanz vorgesehen, die vom einzelnen Router zur Überprüfung einer Antwort kontaktiert wird. Auf diese Art muss der Netz-Betreiber die Datenströme nicht selber verarbeiten. Die Authorisierung der Benutzer kann zentral beim Dienstanbieter erfolgen.

## Literatur


[BB01] Levente Buttyan and Naouel Ben Salem. A Payment Scheme for Broadcast Multimedia Streams. 6th IEEE Symposium on Computers and Communications, Hammamet, Tunisia, July 2001.

[BGB01] Roland Balmer, Manuel Günter, and Torsten Braun. Video Streaming in a DiffServ/IP Multicast Network. Workshop of Advanced Internet Charging and QoS Technology at Informatik 2001, Vienna, Austria, September 2001.

[BZB+97] Bob. Braden, Lixia Zhang, Steve Berson, Shai Herzog, and Sugih Jamin. Resource Reservation Protocol, September 1997. Internet RFC 2205.

[KT00] Dimitri Konstantas and Dimitris Thanos. Commercial Dissemination of Video over Open Networks: Issues and Approaches. Internet Objects, Centre Universitaire d'Informatique, University of Geneva, September 2000. `http://cuiwww.unige.ch/OSG/publications/OO-articles/TechnicalReports/OO%/videoCommerc.pdf`.

[TK00] Dimitris Thanos and Dimitri Konstantas. COiN-Video: A Model for the Dissemination of Copyrighted Video Streams Over Open Networks. Internet Objects, Centre Universitaire d'Informatique, University of Geneva, September 2000. `http://cuiwww.unige.ch/OSG/publications/OO-articles/TechnicalReports/OO%/COiN_Video.pdf`.