Berichte aus der Kommunikationstechnik
herausgegeben von Prof. Firoz Kaderali

Band 9

Christian Grosch

Über Sicherheit und Anonymität in Multicastumgebungen

Shaker Verlag
Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Grosch, Christian:
Über Sicherheit und Anonymität in Multicastumgebungen /
Christian Grosch. Aachen : Shaker, 2002
(Berichte aus der Kommunikationstechnik herausgegeben
von Prof. Firoz Kaderali ; Bd. 9)
Zugl.: Hagen, Univ., Diss., 2001
ISBN 3-8265-9814-8

ISBN 3-8265-9814-8
ISSN 1437-7497

Shaker Verlag GmbH • Postfach 1290 • 52013 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • eMail: info@shaker.de

Über Anonymität und Sicherheit in Multicastumgebungen

Dr.-Ing. Christian Grosch

Abstract

Die Attraktivität von Multipoint-Anwendungen steigt mit der zunehmenden Erreichbarkeit von Konferenzpartnern im Internet. Der durch die Übertragung von Medienströmen mit hohen Bitraten erzeugte steigende Bandbreitenbedarf erfordert neben dem stetigen Ausbau der zugrundeliegenden Infrastruktur die Entwicklung intelligenter Multicast-Protokolle mit guten Skalierungseigenschaften und einer effizienten Ausnutzung von Netzwerk-Ressourcen.

Die Nutzung des multicastfähigen Internet-Backbones, des MBone, für Geschäftskonferenzen, Unterhaltung, Qualifikation und netzbasierte Spiele erfordert darüber hinaus die Einbeziehung von Sicherheitsmerkmalen wie Authentikation und Vertraulichkeit. Während sich eine Reihe von Ansätzen mit der Integration dieser Merkmale in bestehende Multicastumgebungen auseinandersetzen, wird in der vorliegenden Werk der Aspekt der Anonymität im Zusammenhang mit Gruppenkommunikation erstmalig umfassend betrachtet.

Aufbauend auf bekannte Ansätze im Bereich der Punkt-zu-Punkt Verbindungen, wie das Konzept der *Mixe* [1] und des *Onion-Routings* [2] erfolgt zunächst eine Analyse der Besonderheiten und Randbedingungen der Gruppenkommunikation, bevor ein System zur Multicastanonymisierung entwickelt und dargestellt wird, das sowohl die Sender- als auch die Empfängerseite berücksichtigt. Dieser Entwicklung lagen folgende Designkriterien zugrunde:

- Kompatibilität mit existierenden Protokollen und Verfahren: Integrationsfähigkeit in bestehende Umgebungen ohne Veränderung der Protokollbasis.
- Minimierung des Protokolloverheads: Insbesondere Erhaltung der Vorteile des Multicastkonzepts bei der Distribution von Medienströmen.
- Skalierbarkeit des Systems in Abhängigkeit von der geforderten Sicherheitsstufe und der Gruppengröße einer Multicastsitzung.

Im zweiten Teil des Buches erfolgt eine Bewertung des entwickelten Systems in Bezug auf den Ressourcenverbrauch, insbesondere auf die zusätzlich implizierte Netzlast. Die Betrachtung erfolgt mit analytischen Methoden und aus den Ergebnissen werden verschiedene Optimierungsverfahren abgeleitet.

Der dritte und letzte Teil schließlich beschreibt das Konzept der prototypischen Umsetzung des Systems in der Programmiersprache Java und stellt erste Messergebnisse von Laufzeituntersuchungen dar, die aus dem praktischen Einsatz dieses Prototypen auf verschiedenen Rechnerplattformen gewonnen wurden.

[1] David Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24 (Nr. 2), 2 19981
[2] David Goldschlag, Michael Reed und Paul Syverson. Onion Routing for Anonymous and Private Interent Connections. Communications fo the ACM, Vol. 24 (Nr. 2), 2 1999.