Einfluss der Verschlüsselung auf Quality of Service in ATM-Netzen bei Betriebsarten ohne zusätzlichen Bandbreitebedarf

Vom Fachbereich Elektrotechnik und Informatik der Universität Siegen zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.) genehmigte

Dissertation

von

Dipl.-Ing. Sven Kuhn

Referent:	Prof. Dr. rer. nat. Christoph Ruland
Koreferent:	Prof. Dr.-Ing. Christof Paar
Tag der Einreichung:	30. November 2001
Tag der mündlichen Prüfung:	18. Februar 2002

UNIVERSITÄT GESAMTHOCHSCHULE SIEGEN

Schriften zur Nachrichtenübermittlungstechnik

Herausgeber: Prof. Dr. Christoph Ruland

Band 4

Sven Kuhn

Einfluss der Verschlüsselung auf Quality of Service in ATM-Netzen bei Betriebsarten ohne zusätzlichen Bandbreitebedarf

SHAKER VERLAG

Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Kuhn, Sven:
Einfluss der Verschlüsselung auf Quality of Service in ATM-Netzen bei Betriebsarten ohne zusätzlichen Bandbreitebedarf /
Sven Kuhn. Aachen : Shaker, 2002
(Schriften zur Nachrichtenübermittlungstechnik ; Bd. 4)
Zugl.: Siegen, Univ., Diss., 2002
ISBN 3-8322-0047-9

ISBN 3-8322-0047-9
ISSN 1431-6560

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

Einfluss der Verschlüsselung auf Quality of Service in ATM-Netzen bei Betriebsarten ohne zusätzlichen Bandbreitebedarf

Sven Kuhn

19. Februar 2002

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Institut für Nachrichtenübermittlung an der Universität Siegen.

Dem Institutsleiter, Herrn Prof. Dr. rer. nat. Christoph Ruland, gilt mein besonderer Dank für die Möglichkeit zur Durchführung dieser Arbeit, die eingeräumte eigenverantwortliche Arbeitsweise und seine ständige Bereitschaft zur wissenschaftlichen Diskussion.

Herrn Prof. Dr.-Ing. Christof Paar von der Ruhr-Universität Bochum danke ich für die Übernahme des Koreferates.

Meinen Kollegen Christoph Stepping, Oliver Jung, Kai Wollenweber, Christian Geuer-Pollmann, Niko Schweitzer und Matthias Schneider danke ich für die freundschaftliche und konstruktive Zusammenarbeit.

Danken möchte ich auch meinen Eltern, die mich während meines gesamten Ausbildungswegs unterstützt haben.

Schließlich bedanke ich mich bei meiner Freundin Christine Resch, die mich bei der Anfertigung dieser Arbeit stets unterstützt und motiviert hat.

Siegen im Februar 2002
Sven Kuhn

Zusammenfassung

In den letzten Jahren hat die steigende Nachfrage nach Bandbreite die Entwicklung effizienter digitaler Übertragungssysteme forciert. Neue Systeme gewährleisten nicht nur hohe Übertragungsraten sondern auch ein besseres Bandbreiten-Kosten-Verhältnis. Der Asynchrone Transfer Modus (ATM) ermöglicht außer den genannten Eigenschaften auch Netzwerkmanagement und Quality of Service. Ein zusätzlicher Vorteil von ATM besteht darin, dass die Daten verschiedener Dienste (Daten, Sprache, Video) in einem Netz übertragen werden.

ATM-Netze sind nicht sicherer als andere Netzwerke. Das ATM-Forum hat daher verschiedene Vorschriften veröffentlicht, die die Sicherheitsdienste Integrität, Vertraulichkeit, Authentikation und Zugangskontrolle definieren. Zur Gewährleistung der Vertraulichkeit werden ATM-Verschlüsselungen eingesetzt, aufgrund der hohen Datenraten kommen nur symmetrische Blockalgorithmen in Frage.

Für diese Algorithmen gibt es verschiedene Betriebsarten, die eine Veränderung der ausgehandelten Qualitätsparameter hervorrufen. Keine der in dieser Arbeit untersuchten Betriebsarten benötigt zusätzliche Bandbreite für die kryptografische Synchronisation. Um jedoch die hohen Datenraten in ATM-Netzen zu gewährleisten, wird die Möglichkeit einer Parallelisierung verlangt. Bewertet wird auch der Implementationsaufwand der einzelnen Betriebsarten.

Für den Einsatz in ATM-Verschlüsselungen ist der Erweiterte CBC-Mode als Modifikation des in der ISO 10116 beschriebenen CBC-Modes geeignet. Ebenso kommen die vom *Bundesamt für Sicherheit in der Informationstechnik* speziell für ATM entwickelten Betriebsarten, *Modifizierter CBC Mode* und *Selbstsynchronisierenden Key Counter ECB Mode* in Frage. Zusätzlich wird in dieser Arbeit der *Statistische ATM Counter Mode* als neue Betriebsart vorgestellt.

Durch den Einsatz von ATM-Sicherheitsgeräten können die ausgehandelten Qualitätsparameter abhängig von der verwendeten Betriebsart herabgesetzt werden. Für die genannten Betriebsarten wird daher die jeweilige Veränderung der Performance- und Verkehrsparameter untersucht.

Da sich diese Parameter nur auf die ATM-Schicht beziehen, werden zusätzlich die Auswirkungen der unterschiedlichen Betriebsarten auf die höhere Protokollschicht untersucht, um daraus eine genauere Aussage über die Beeinträchtigung der Anwendung abzuleiten.

Abstract

The increased requirement for bandwidth capacity over the last years has prompted the development of efficient digital transmission systems. Modern systems provide higher transmission rates with a better bandwidth/cost ratio than traditional ones. The Asynchronous Transfer Mode (ATM) is one of the technologies that does not only fulfil this demand, but also offers the possibility of enhanced network management and controllable Quality of Service (QoS). To ensure an efficient transmission, the user is able to negotiate the parameters which exactly fulfil the requirements of the application. All different types of traffic, from data, phone calls to video transmissions are handled via these types of networks, based on common international standards.

ATM itself is not more secure than other networks. Thus, it requires adequate security features to protect the transmitted information and the network management. The ATM Forum has established a framework of specifications that defines objectives for security requirements. The security requirements for ATM networks consist of data integrity, confidentiality, authentication and access control for all services and management activities. To ensure confidentiality during the transmission, encryption technology is highly important. Because of the high speed, only symmetric block algorithms are applicable. New or modified modes of operation are required as high transmission rates and the negotiated QoS-parameters have to be taken into consideration. To ensure the high data rates in ATM networks, the modes of operation must allow parallel processing.

None of the examined modes of operation requires bandwidth for synchronisation purposes. Desirable is a small delay and small effort for the implementation. Suitable for ATM are the *Modified CBC Mode* and the *Selfsynchronising Key Counter ECB Mode* proposed by the „Bundesamt für Sicherheit in der Infomationstechnik“ as well as the *Extended CBC Mode* that is based on ISO 10116. To overcome the bandwidth requirements of the ATM Counter Mode, the *Statistical ATM Counter Mode* is introduced and analysed.

If ATM security devices are inserted in the network, the negotiated performance- and traffic parameters may be degraded. The level of the modification depends on the mode of operation used and on the implementation. This thesis analyses the influences on the negotiated performance- and traffic-parameters depending on the different modes of operation.

As these parameters are only related to the ATM-layer, it is also examined how the modes of operation influence the higher transport layer and therefore the quality of the application.

Inhaltsverzeichnis