

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



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



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

Copyright Shaker Verlag 2002

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen
oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungs-
anlagen und der Übersetzung, vorbehalten.

Printed in Germany.

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 *Selsynchronising Key Counter ECB Mode* proposed by the „Bundesamt für Sicherheit in der Informationstechnik“ 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

1	Einleitung	1
2	ATM-Grundlagen	2
2.1	Referenzmodell	2
2.2	ATM-Zelle	4
2.3	Zellerkennung und -kontrolle	5
2.4	Virtuelle Verbindung	8
2.5	AAL-Schicht	9
2.6	ATM über SDH	11
3	Quality of Service	13
3.1	Einführung	13
3.2	Zellübertragungsergebnisse	14
3.3	ATM Performanceparameter	15
3.3.1	Dependability Parameters	16
3.3.1.1	Cell Error Ratio	16
3.3.1.2	Cell Loss Ratio	16
3.3.1.3	Cell Misinsertion Rate	17
3.3.1.4	Severely Errored Cell Block Ratio	17
3.3.2	Delay Parameters	18
3.3.2.1	Cell Transfer Delay	18
3.3.2.2	Cell Delay Variation	19
3.4	Verkehrsparameter	21
3.4.1	Peak Cell Rate	21
3.4.2	Cell Delay Variation Tolerance	21
3.4.3	Sustainable Cell Rate	23
3.4.4	Burst Tolerance	23
3.4.5	Minimum Cell Rate	24

3.5	Serviceklassen	25
3.6	Verkehrsvertrag	27
3.7	Conformance Definition	28
4	Signalisierung	30
4.1	UNI-Signalisierung	30
4.1.1	Verbindungsauf- und -abbau	30
4.1.2	Mehrpunktverbindungen	31
4.1.3	Informationselemente	32
4.1.4	Aushandeln der Qualitätsparameter	35
4.1.5	Aushandeln der Verkehrsparameter	36
4.2	PNNI-Signalisierung	37
4.2.1	Verbindungsauf- und -abbau	38
4.2.2	Mehrpunktverbindungen	38
4.2.3	Informationselemente	39
4.2.4	Aushandeln der Qualitätsparameter	40
4.2.5	Aushandeln der Verkehrsparameter	41
5	Übertragungsstörungen und Auswirkungen	43
5.1	Fehler im Übertragungssystem	43
5.2	Signalverzögerung	45
5.3	Überlast im Netzelement	45
5.4	Gegenseitige Beeinflussung der Verbindungen	45
5.5	Ausfall von Netzelementen	46
6	Sicherheit in ATM-Netzen	47
6.1	Security Agents	47
6.2	Sicherheitsdienste	48
6.2.1	Vertraulichkeit	48
6.2.2	Datenintegrität	48
6.2.3	Authentikation	49
6.2.4	Zugangskontrolle	49
6.3	Security Information Exchange	49
7	Verschlüsselungsbetriebsarten ohne zusätzlichen Bandbreitebedarf	50
7.1	Anforderungen an Verschlüsselungsbetriebsarten in ATM-Netzen . . .	51
7.2	Verwendete Bezeichnungen	53

7.3	Erweiterter CBC	55
7.3.1	Segmentorientierte Version	55
7.3.2	Zellorientierte Version	58
7.4	Modifizierter CBC	60
7.5	Selbstsynchronisierender Key-Counter-ECB	62
7.6	Statistischer ATM Counter Mode	64
7.6.1	Funktion	64
7.6.2	Bitmusterwahrscheinlichkeit und -abstände	68
7.6.3	Startwertwahrscheinlichkeit	69
7.7	Übersicht der Eigenschaften	72
8	Annahmen zur Untersuchung der Verschlüsselungsbetriebsarten	76
8.1	Annahmen	76
8.2	Verwendete Bezeichnungen	79
9	Auswirkungen der Betriebsarten auf die Performanceparameter	80
9.1	CER Veränderung	80
9.1.1	Erweiterter CBC (segmentorientiert)	80
9.1.2	Erweiterter CBC (zell- orientiert)	83
9.1.3	Modifizierter CBC	84
9.1.4	Selbstsynchronisierender Key Counter ECB	87
9.1.5	Statistischer ATM Counter Mode	88
9.1.5.1	AAL 1 und AAL 3/4	91
9.1.5.2	AAL 5	92
9.2	CLR Veränderungen	94
9.3	CMR Veränderungen	94
9.4	SECBR Veränderungen	95
9.5	CTD Veränderungen	96
9.5.1	Erweiterter CBC	96
9.5.1.1	Segmentversion	96
9.5.1.2	Zellversion	96
9.5.2	Modifizierter CBC	98
9.5.3	Selbstsynchronisierender Key Counter ECB	98
9.5.4	Statistischer ATM Counter Mode	99
9.6	CDV Veränderungen	99
10	Auswirkungen der Implementierung auf die Performanceparameter	101

10.1 CER Veränderungen	102
10.2 CLR Veränderungen	102
10.3 CMR Veränderungen	102
10.4 SECBR Veränderungen	102
10.5 CTD Veränderungen	103
10.6 CDV Veränderungen	103
11 Auswirkung der Betriebsarten und der Implementierung auf die Verkehrsparameter	104
11.1 Auswirkungen auf die Zellraten	104
11.2 Auswirkungen auf die Burst Tolerance	105
11.3 Auswirkungen auf die Cell Delay Variation Tolerance	105
12 Simulationen	106
12.1 Klassifizierung von Simulationen	107
12.2 Diskrete Ereignissimulation	108
12.3 Erzeugung von Zufallszahlen	109
12.4 Genauigkeit von Simulationen	111
12.5 Simulator ModeSIM	112
12.6 Simulationsergebnisse	115
12.6.1 Erweiterter CBC	116
12.6.2 Modifizierter CBC	119
12.6.3 Selbstsynchronisierender Key Counter ECB	120
12.6.4 Statistischer ATM Counter Mode	122
12.6.4.1 AAL1,3/4	122
12.6.4.2 AAL5	124
13 Auswertung der Veränderungen der Performance- und Verkehrsparameter	127
14 Auswirkung der Verschlüsselungsbetriebsarten auf höhere Schichten	132
15 Zusammenfassung	139
ANHANG	142
A Referenzimplementierung SEDAN	155
A.1 Überblick	142
A.2 SDH/ATM-Interface	144

A.2.1	Schnittstellen	145
A.2.2	Aufbau	145
A.2.3	Overheadbearbeitung	148
A.2.4	Alarmauswertung	150
A.3	Verzögerungszeiten	153
A.4	Initialisierung	153
B	Simulationsergebnisse	155
C	Abkürzungsverzeichnis	174
	Literaturverzeichnis	178