

# **Stabilität und Robustheit von programmierbaren Vermittlungssystemen**

Zur Erlangung des akademischen Grades eines  
**Doktors der Ingenieurwissenschaften**  
der Fakultät für Informatik  
Universität Fridericiana zu Karlsruhe (TH)

genehmigte

**Dissertation**

von  
Dipl.-Inform.  
**Marcus Schöller**  
aus Neundettelsau

Tag der mündlichen Prüfung: 04. 05. 2006

Erster Gutachter: Prof. Dr. Martina Zitterbart  
Zweiter Gutachter: Prof. Dr. Uwe Brinkschulte



Berichte aus der Telematik

**Marcus Schöller**

**Stabilität und Robustheit von  
programmierbaren Vermittlungssystemen**

Shaker Verlag  
Aachen 2006

**Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Karlsruhe, Univ., Diss., 2006

Copyright Shaker Verlag 2006

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

Printed in Germany.

ISBN-10: 3-8322-5715-2

ISBN-13: 978-3-8322-5715-6

ISSN 0948-700X

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: [www.shaker.de](http://www.shaker.de) • E-Mail: [info@shaker.de](mailto:info@shaker.de)

*Für  
meine Mutter Barabara und meinen Vater Herbert*



---

# Vorwort

---

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Institut für Telematik der Universität Karlsruhe (TH).

Zu allererst gilt mein Dank Frau Prof. Dr. Martina Zitterbart für die Betreuung und Förderung meiner wissenschaftlichen Arbeit und für die Möglichkeit der Promotion an ihrem Lehrstuhl. Ihre Ratschläge und Anregungen haben sehr zum Gelingen dieser Arbeit beigetragen. Darüber hinaus ermöglichte sie mir, meine Arbeiten auf nationalen und internationalen Konferenzen vorzustellen. Die dort geführten Diskussionen haben die entstandene Arbeit positiv beeinflusst und Kontakte zu anderen Forschern in meinem Forschungsbereich ermöglicht. Der Austausch mit diesen war besonders in den Anfängen meiner Arbeit eine große Hilfe.

Bei Herrn Prof. Dr. Uwe Brinkschulte möchte ich mich für die bereitwillige und freundliche Übernahme des Koreferats bedanken.

Weiterhin möchte ich den Kollegen des Karlsruher Instituts für Telematik für ihre konstruktive und fruchtbare Zusammenarbeit danken. Besonderer Dank gilt dabei den Mitarbeitern des Flexinet Projekts Frau Anke Speer, Herrn Dr. Till Harbaum, Herrn Dr. Thomas Fuhrmann und Herrn Michael Conrad für ihre fachlich wertvollen Beiträge zu der gemeinsam geleisteten Arbeit. Herrn Stefan Mink gebührt der Dank für viele Diskussionen in den Bereichen Sicherheit und Robustheit, die einen zentralen Aspekt der vorliegenden Arbeit einnehmen. Weiterer Dank gebührt Herrn Dr. Till Harbaum und Herrn Ulrich Mohr für das Korrekturlesen der Arbeit. Ihre Anregungen und Verbesserungsvorschläge haben die Ausarbeitung wesentlich verbessert.

Bedanken möchte ich mich auch bei Christina Schmidt, Thomas Gamer, Lars Völker, Johann Mihutoni, Christoph Mayer, Gerhard Bocksch, Uwe Freese, Michael Scharf, Anno von Heimburg und Jan Höft für ihre Beiträge in Form meist sehr guter Diplom- und Studienarbeiten sowie ihren Tätigkeiten als wissenschaftliche Hilfskräfte. Ohne sie wäre die Arbeit nicht in dieser Form möglich gewesen.

Ich möchte mich auch bei den technischen Mitarbeitern Detlef Meier, Gentiel Mussnug und Frank Winter für ihre Unterstützung bei technischen Angelegenheiten und dem Aufbau geeigneter Infrastrukturen für die Durchführung der Untersuchungen bedanken. Ebenfalls bedanken möchte ich mich bei den Damen des Sekretariats, vor allem bei Astrid Natzberg und Doris Weber, für ihre Unterstützung bei organisatorischen Angelegenheiten.

Schließlich möchte ich mich besonders bei meiner Frau Andrea Schöller und meinem Sohn Pascal Schöller bedanken, die mich während der gesamten Arbeiten unterstützt haben und nur allzu oft auf meine Anwesenheit verzichten mussten. Ebenso möchte ich mich auch bei meinen Eltern bedanken, die mich in vielfältiger Weise von Kindheit an gefördert haben.



---

# Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Problemstellung . . . . .	2
1.2	Ziel der Arbeit . . . . .	3
1.3	Gliederung der Arbeit . . . . .	3
<b>2</b>	<b>Grundlagen</b>	<b>5</b>
2.1	Begriffsdefinitionen . . . . .	6
2.1.1	Dienst . . . . .	6
2.1.2	Signalisierung . . . . .	7
2.1.3	Stabilität . . . . .	7
2.1.4	Robustheit . . . . .	8
2.2	Aktive und programmierbare Vermittlungssysteme . . . . .	8
2.2.1	Aktive Netze . . . . .	9
2.2.2	Programmierbare Netze . . . . .	10
2.3	Beispieldienste für programmierbare Netze . . . . .	10
2.3.1	Multimedia-Transcodierung . . . . .	11
2.3.1.1	Reduzierung der Datenrate . . . . .	11
2.3.1.2	Änderung des Datenformats . . . . .	12
2.3.2	Multicast-Reflektor . . . . .	13
2.3.3	Angriffserkennung . . . . .	14
2.4	Angriffe . . . . .	15
2.4.1	Angriffe auf die Signalisierung . . . . .	15
2.4.1.1	Denial-of-Service-Angriffe . . . . .	15
2.4.1.2	Vortäuschen einer fremden Identität . . . . .	16
2.4.1.3	Offenlegen des Sitzungsschlüssels . . . . .	17

2.4.1.4	Wiederholungsangriffe . . . . .	17
2.4.1.5	Manipulation von Nachrichten . . . . .	17
2.4.2	Angriffe auf Dienstebene . . . . .	18
2.5	Kryptographische Verfahren . . . . .	19
2.5.1	Asymmetrische Kryptographie . . . . .	19
2.5.1.1	Verschlüsselung . . . . .	20
2.5.1.2	Digitale Signatur . . . . .	20
2.5.1.3	Schlüsselaustausch . . . . .	20
2.5.2	Hashfunktionen . . . . .	20
2.5.3	Hybride Verfahren . . . . .	21
2.5.3.1	Verschlüsselung . . . . .	21
2.5.3.2	Digitale Signatur . . . . .	22
2.6	Public Key Infrastrukturen . . . . .	22
<b>3</b>	<b>Flexinet</b> . . . . .	<b>25</b>
3.1	Aufbau . . . . .	25
3.2	Dienstmodule . . . . .	27
3.2.1	C-Module . . . . .	27
3.2.2	Java-Module . . . . .	28
3.2.3	Happlet-Module . . . . .	28
3.3	Architektur . . . . .	29
3.3.1	Paketklassifikation . . . . .	30
3.3.1.1	Die Netfilter-Aktion Flexinet . . . . .	32
3.3.1.2	Die Netfilter-Tabelle Flexinet . . . . .	33
3.3.2	Die Ablaufumgebung . . . . .	34
3.4	Die Konfigurationsschnittstelle . . . . .	36
3.5	Die Dienstdatenbank . . . . .	36
3.6	Erweiterungen des programmierbaren Netzes Flexinet . . . . .	38
3.7	Zusammenfassung . . . . .	40

---

<b>4 Ressourcenverwaltung</b>	<b>41</b>
4.1 Risiken auf Dienstebene	41
4.1.1 Fehlende Ressourcenfreigaben	42
4.1.2 Ressourcenüberbelegung	42
4.2 Stand der Technik	43
4.3 Komponenten der Ressourcenverwaltung	44
4.3.1 Zugriffskontrolle zu den Ressourcen	44
4.3.1.1 Unumgänglichkeit	45
4.3.1.2 Konfiguration	45
4.3.2 Der Ressourcen-Manager	46
4.3.2.1 Konfiguration der Zugriffskontrolle	46
4.3.2.2 Auslesen der Ressourcenbelegung	46
4.3.2.3 Reservierung der Ressourcen	47
4.3.2.4 Erkennung einer drohenden Überlast	47
4.4 Ressourcenbedarf einzelner Dienste	47
4.4.1 Lebenszyklus einer Dienstinstantz	47
4.4.1.1 Erzeugung der Ablaufumgebung	48
4.4.1.2 Instantiierung der Dienstmodule	48
4.4.1.3 Verarbeitung der IP-Pakete	48
4.4.1.4 Beenden der Dienstinstantz	49
4.4.2 Ressourcenbedarf einiger Dienste	49
4.4.2.1 Multicast-Reflektor	49
4.4.2.2 Angriffserkennung	49
4.5 Realisierung in Flexinet	51
4.5.1 Ressourcen der Ablaufumgebung	51
4.5.1.1 Speicherzugriff	51
4.5.1.2 Kommunikationszugriff	53
4.5.1.3 Prozesserzeugung	53
4.5.1.4 Evaluation	53
4.5.2 Warteschlangen	54
4.5.3 Überwachung der CPU	58
4.5.4 Architektur	58
4.5.4.1 Schnittstellen	59
4.6 Zusammenfassung	60

<b>5</b>	<b>Evaluation und Verlagerung</b>	<b>61</b>
5.1	Bewertung programmierbarer Vermittlungssysteme . . . . .	61
5.2	Stand der Technik . . . . .	62
5.2.1	Bewertung von programmierbaren Vermittlungssystemen . . . . .	63
5.2.2	Verlagerung von Dienstinstanzen . . . . .	64
5.3	Charakteristiken von Diensten . . . . .	64
5.3.1	Transparenz des Dienstes . . . . .	64
5.3.2	Verteilte Dienste . . . . .	65
5.3.2.1	Dienstketten . . . . .	65
5.3.2.2	Hierarchische Dienste . . . . .	66
5.3.2.3	Overlay-Dienste . . . . .	66
5.3.2.4	Zusammenfassung . . . . .	67
5.3.3	Prioritäten von Diensten . . . . .	67
5.4	Nachbarschaften . . . . .	68
5.4.1	Ring-basierte Suche . . . . .	69
5.4.1.1	Paketlebensdauer . . . . .	70
5.4.1.2	Administrative Domänen . . . . .	71
5.4.1.3	Durchführung der Suche . . . . .	72
5.4.1.4	Bewertung der Ring-basierten Suche . . . . .	72
5.4.2	Pfad-basierte Suche . . . . .	73
5.4.2.1	Symmetrische Pfade . . . . .	73
5.4.2.2	Asymmetrische Pfade . . . . .	74
5.4.2.3	Durchführung der Suche . . . . .	75
5.4.2.4	Bewertung der Pfad-basierten Suche . . . . .	75
5.4.3	Baum-basierte Suche . . . . .	75
5.4.3.1	Suche ausgehend vom Empfänger . . . . .	76
5.4.3.2	Suche ausgehend vom Wurzelknoten . . . . .	76
5.4.3.3	Durchführung der Suche . . . . .	76
5.4.3.4	Bewertung der Baum-basierten Suche . . . . .	76
5.4.4	Hybride Verfahren . . . . .	77
5.4.4.1	Durchführung der Suche . . . . .	77
5.4.4.2	Bewertung der hybriden Verfahren . . . . .	78

---

5.4.5	Bewertung . . . . .	79
5.5	Lokale Evaluation . . . . .	79
5.5.1	Ablauf der lokalen Evaluation . . . . .	80
5.5.2	Bewertung . . . . .	80
5.6	Verteilte Evaluation . . . . .	81
5.6.1	Ausbreitung der Evaluation . . . . .	82
5.6.1.1	Bewertung . . . . .	85
5.6.2	Verantwortung über die Evaluation . . . . .	85
5.6.2.1	Bewertung . . . . .	86
5.6.3	Vorzeitiger Abbruch der Evaluation . . . . .	86
5.6.3.1	Bewertung . . . . .	86
5.6.4	Reservierung der Ressourcen . . . . .	87
5.6.4.1	Evaluation mit kurzlebigen Vorreservierungen . . . . .	87
5.6.4.2	Evaluation mit einer langlebigen Vorreservierung . . . . .	87
5.6.4.3	Evaluation mit mehreren langlebigen Vorreservierungen . . . . .	88
5.6.4.4	Evaluation ohne Vorreservierungen . . . . .	88
5.6.4.5	Bewertung . . . . .	88
5.6.5	Ablauf der verteilten Evaluation . . . . .	88
5.7	Verlagerung von Dienstinstanzen . . . . .	89
5.7.1	Verlagerung des Dienstkontextes . . . . .	90
5.7.1.1	Bewertung . . . . .	91
5.7.2	Prioritäten von Diensten . . . . .	91
5.7.2.1	Bewertung . . . . .	91
5.7.3	Abschalten wegen Überlast . . . . .	91
5.7.3.1	Bewertung . . . . .	93
5.7.4	Verlagerung wegen Routenänderung . . . . .	93
5.7.4.1	Mobilität der Endgeräte . . . . .	93
5.7.4.2	Änderung der Paketweiterleitung . . . . .	94
5.7.5	Übernahme des Dienstes . . . . .	94
5.8	Realisierung in Flexinet . . . . .	95
5.8.1	Architektur . . . . .	95
5.8.2	Dienstmodul Evaluation, Knotenfindung und Verlagerung . . . . .	96

5.8.2.1	Aufsetzen und Verlagerung einer transparenten Dienstinstanz	96
5.8.2.2	Aufsetzen einer sichtbaren oder halbtransparenten Dienstinstanz	97
5.8.2.3	Verlagerung einer sichtbaren oder halbtransparenten Dienstinstanz	98
5.8.3	Nachrichtenparameter	99
5.8.3.1	Evaluation	99
5.8.3.2	Verlagerung	100
5.8.4	Verzögerung	100
5.9	Zusammenfassung	101
<b>6</b>	<b>Signalisierung</b>	<b>103</b>
6.1	Angriffe auf Vermittlungssysteme	103
6.1.1	Angriffe auf die Paketvermittlung	104
6.1.2	Angriffe auf das Routing-Protokoll	104
6.1.3	Zusammenfassung	104
6.2	Stand der Technik	105
6.2.1	Andere Forschungsansätze	105
6.2.2	Authentifizierung und Autorisierung	107
6.2.3	Sicherung der Signalisierungsnachrichten	108
6.2.3.1	Mechanismen zur Sicherung auf den Netzwerkschichten	108
6.2.3.2	Mechanismen zur Sicherung auf Anwendungsschicht	109
6.2.4	Schutz vor Wiederholungsangriffen	110
6.2.5	Schutz vor Denial-of-Service-Angriffen	111
6.3	Anforderungen an die Signalisierung	112
6.3.1	Funktionelle Anforderungen	112
6.3.2	Nicht-funktionelle Anforderungen	113
6.4	Kryptographische Fähigkeiten der beteiligten Systeme	114
6.5	Entwurf der Signalisierung	116
6.5.1	Kommunikation mit der Dienstdatenbank	116
6.5.2	Wahl des Transportprotokolls	116
6.5.3	Der Signalisierungsdienst	117
6.5.4	Wahl der Authentifizierungsmethode	118
6.5.5	Protokollmechanismen	118
6.5.5.1	Sequenznummern	118

---

6.5.5.2	Verlust von Nachrichten . . . . .	119
6.5.6	Protokollkopf der Signalisierung . . . . .	119
6.5.7	Authentizitätssicherung der Signalisierungsnachrichten . . . . .	120
6.5.7.1	Signatur der Daten . . . . .	120
6.5.7.2	Integritätssicherung durch ein asymmetrisches Verfahren . . . . .	121
6.5.7.3	Integritätssicherung durch HMAC . . . . .	121
6.5.8	Anmeldung . . . . .	121
6.5.8.1	Benutzer in fremden Domänen . . . . .	122
6.5.8.2	Angriffsmöglichkeiten . . . . .	124
6.5.9	Dienstanforderung . . . . .	124
6.5.9.1	Erzeugen des Sitzungsschlüssels . . . . .	125
6.5.9.2	Aufbau des TLS-Tunnels . . . . .	126
6.5.9.3	Angriffsmöglichkeiten . . . . .	127
6.5.10	Kommunikation mit einer Dienstinstanz . . . . .	127
6.5.11	Szenario: Ein programmierbares Vermittlungssystem . . . . .	128
6.5.12	Domäneninterne Evaluation . . . . .	129
6.5.12.1	Verteilen der Evaluation . . . . .	129
6.5.12.2	Prüfung der Evaluation-Anfrage . . . . .	131
6.5.12.3	Lokale Evaluation durchführen . . . . .	131
6.5.12.4	Dienstinstanz aufsetzen . . . . .	132
6.5.12.5	Client benachrichtigen . . . . .	132
6.5.12.6	Aufbau des TLS-Tunnels . . . . .	132
6.5.12.7	Angriffsmöglichkeiten . . . . .	133
6.5.13	Szenario: Dienstinstantiierung innerhalb einer Domäne . . . . .	133
6.5.14	Domänenübergreifende Evaluation . . . . .	135
6.5.14.1	Austausch von Sitzungsschlüsseln für die Evaluation . . . . .	136
6.5.14.2	Austausch eines neuen Master-Secrets . . . . .	136
6.5.15	Szenario: Dienstinstantiierung in einer fremden Domäne . . . . .	137
6.5.16	Bewertung des Entwurfs . . . . .	138
6.6	Realisierung in Flexinet . . . . .	139
6.6.1	Nachrichten der Anmeldung . . . . .	139
6.6.1.1	Benutzer-Authentifizierung-Anfrage . . . . .	139
6.6.1.2	Benutzer-Authentifizierung-Antwort . . . . .	140
6.6.2	Der Signalisierungsdienst . . . . .	141
6.7	Zusammenfassung . . . . .	142

<b>7 Zusammenfassung und Ausblick</b>	<b>143</b>
7.1 Ausblick . . . . .	145
<b>A Nachrichten der Signalisierung</b>	<b>147</b>
A.1 Nachrichten der Anmeldung . . . . .	147
A.2 Nachrichten der Dienstanforderung . . . . .	149
A.3 Nachrichten der Evaluation . . . . .	151
<b>Literaturverzeichnis</b>	<b>157</b>