Schwachstellensuche - Qualitätsüberwachung im Netz durch Klassifizierung des HADES One-Way Delays

Dr. Stephan Kraft, Birgit König, Martin Gründl
WiN-Labor
Universität Erlangen-Nürnberg
Martensstr. 1, 91058 Erlangen
[stephan.kraft, birgit.koenig,martin.gruendl]@dfn.de

Abstract: HADES ist ein im WiN-Labor an der Universität Erlangen entwickeltes System zur Ermittlung qualitätsrelevanter Daten wie IP-Paketlaufzeit und Paketverluste in Computernetzwerken. Gemessene und statistisch bewertete Paketlaufzeiten lassen Rückschlüsse zu, wie die Qualität von Netzwerkverbindungen einzuordnen ist und wo kritische Netzwerksituationen auftreten bzw. auftreten können. In dieser Arbeit wird das generelle Verfahren der Datengewinnung, deren statistische Analyse und die Ergebnisse in Form eines Rankings auf Layer3-Ebene vorgestellt.

1 Einleitung

Um die Dienstgüte von Netzwerkverbindungen überwachen und bestimmen zu können, hat das WiN-Labor der Universität Erlangen im Rahmen von Projekten des DFN-Verein [DFN09] im X-WiN [XWI] und im europäischen Netzwerk GÉANT [GEA] ein Messsystem [HAD09] entwickelt, welches qualitätsrelevante Daten wie One-Way Delay (Paketlaufzeit), One-Way Delay Variation (Jitter) und Paket Loss (Paketverluste) ensprechend [PAMM98, ALM99a, ALM99b, DC02] ermittelt.
Dazu werden von einer Sendestation Gruppen von UDP-Paketen in konfigurierbaren Abständen erzeugt. Die Pakete werden mit einer Sequenznummer und einem aktuellen Zeitstempel versehen und an eine Empfangsstation, die die aktuelle Empfangszeit bestimmt, gesendet. Daraus werden One-Way Delay, Delay Variation und Paketverluste der gemessenen Verbindungen ermittelt.
Eine mathematisch-statistische Analyse [HOL08] wertet die Daten durch vergleichendes Klassifizieren aus und hilft damit, Schwachstellen im Netzwerk zu finden.

2 Hades-Messsystem

2.1 IP Performance Metrics

Die Idee des Messverfahrens basiert auf Ansätzen der IETF. In der Working Group IP Performance Metrics (IPPM) wurde dazu 1998 ein umfangreiches Rahmenwerk

verabschiedet, welches Definitionen zur Messung der Netzperformance beinhaltet [PAMM98]. Damit sollen Messverfahren und deren Auswertung standardisiert werden. Zu den wichtigsten definierten Metriken gehören One-Way Delay (OWD – Laufzeitverzögerung), IP Delay Variation (IPDV, OWDV – Jitter, Differenz der OWDs aufeinanderfolgender Pakete) und Packet Loss (Anteil der verlorenen Pakete in einem bestimmten Zeitraum), anhand derer man die Dienstgüte bestimmen kann [ALM99a, ALM99b].

2.2 Zeitsynchronisation

Die Qualität der gemessenen Metriken hängt entscheidend von der Genauigkeit des Zeitstempels ab.
Das *Network Time Protocol* (NTP) ist eine Möglichkeit zur Uhrensynchronisation in paketvermittelten Kommunikationssystemen. Einem NTP-Prozess ntpd wird in regelmäßigen Abständen durch externe Signale von GPS-Satelliten oder NTP-Servern die aktuelle Uhrzeit übermittelt. Die Zeitsynchronisation wird durch die Einstellung der Frequenz der lokalen Uhr erreicht. Die aktuelle Version erreicht im Internet eine Genauigkeit im Bereich von 10 Millisekunden [NTP1, NTP2].
Beim *Global Position System* (GPS) handelt es sich um ein satellitengestütztes System zur weltweiten Positionsbestimmung, ursprünglich für den militärischen Gebrauch konzipiert. Von jedem Punkt der Erde sind vier Satelliten erreichbar. Während einer der Satelliten die Quarzuhr des GPS-Empfängers synchronisiert, dienen die anderen drei zur Positionsbestimmung [FAA]. Man kann sich der hohen Zeitgenauigkeit bedienen und die Zeitsynchronisation von unter 250 Nanosekunden nutzen.
Da die One-Way Delay Werte im Bereich von 10 Millisekunden liegen, ist NTP über das Netz nicht genau genug. Somit ist die gewählte Alternative eine GPS-Karte, die über eine angeschlossene GPS-Antenne die Signale der Satelliten empfängt und die Systemuhr via NTP synchronisiert [HOL08]. Die Genauigkeit der NTP-Synchronizität mittels GPS liegt bei 10 Mikrosekunden.

2.3 Messverfahren

Gemessen wird auf Messstationen, die aktiv UDP-Testpakete generieren, diese ins Netz einschleusen und Pakete von anderen Messrechnern empfangen [HKK06].
Der Quellrechner versieht die Pakete vor dem Senden mit einem präzisen Zeitstempel. Die zu versendenden Pakete werden gruppiert und in kurzen zeitlichen Abständen verschickt. Startzeitpunkt, Anzahl der Pakete, Paketgröße, zeitlicher Abstand der Pakete zueinander und das Ziel sind dabei variabel einstellbare Parameter.
Der Zielrechner wiederum empfängt die Pakete und speichert die Eingangszeit. Die Daten werden vom Zielrechner abgeholt und dann in einem weiteren Verfahren zur Bestimmung der Dienstgüte genutzt.
Derzeit wird alle 30 Sekunden eine Gruppe von neun Paketen mit 42 Bytes Größe verschickt. Die einzelnen Pakete haben einen Abstand von fünf Millisekunden zueinander, um Kollisionen zu vermeiden.

2.4 Verbreitung

Ausgehend von der ersten Messstation im deutschen Forschungsnetz X-WiN, installiert im Sommer 2002, hat sich das Messsystem über das Europäische Forschungsnetz GN (GÉANT) hinaus weltweit verbreitet.
Tabelle 1 gibt einen Überblick über die Beteiligung an verschiedenen Projekten, die Anzahl der mit Messstationen versehenen Standorte und die ungefähre Anzahl von Messstrecken.

Tabelle 1: Überblick über den derzeitigen Ausbaustand der HADES Messysteme.

Projekt	*Anzahl der Standorte*	*Anzahl der Messstrecken*
X-WiN	**57**	**Ca. 3500**
GÉANT	**36**	**Ca. 1200**
MDM[1]	**23**	**Ca. 500**
LHCOPN[2]	**10**	**Ca. 40**

3 Performance-Klassifizierung

Nachdem die Performance-Messungen zuverlässig verwertbare Daten liefern, besteht eine nächste Aufgabe darin, die ermittelten Daten zu analysieren, um Aussagen über die Übertragungsqualität in Netzwerken zu bekommen.
In einer vom WiN-Labor betreuten Diplomarbeit [HOL08] wurden mehrere statistische Modelle beschrieben, die beobachtete OWD (One-Way Delay) Messdaten durch wenige Parameter charakterisieren. Dazu werden 15-Minuten Intervalle in Qualitätsklassen eingruppiert und mit einer Gewichtung aufsummiert. Mittels Klassifizierung der OWD – Muster wird ein Analysesystem entwickelt, das die aktuelle Qualität von Netzwerkverbindungen automatisch einordnen und kritische Netzwerksituationen erkennen kann.

3.1 Routing Delay und Performanceklassen

Der *routing delay* ist im Gegensatz zum *intrinsic delay* der variable Teil des OWD. Während der *intrinsic delay* die minimale Zeit beschreibt, die das Signal braucht, um die aktiven und passiven Komponenten des IP-Pfades zu durchlaufen, wird der *routing delay* durch das variable Verhalten der Komponenten auf der Strecke bestimmt. Der *routing delay* wird durch Subtraktion des *intrinsic delays* vom OWD bestimmt.

Der *routing delay* (Viertelstundenwert) lässt sich folgendermaßen klassifizieren:

[1] perfSONAR Multi-Domain Monitoring, domänüberspannendes Monitoring
[2] s. Kapitel 4

- **excellent:** Diese Klasse beschreibt den bestmöglichen Zustand einer Strecke mit einem stabilen *routing delay*.
- **fair:** Damit wird eine leichte Verschlechterung einer Strecke durch eine wachsende Varianz des *routing delay* charakterisiert. Es gibt einzelne statistische Ausreißer.
- **poor:** Man sieht eine größere Streuung der Messwerte, was auf eine leichte Überlast einer Strecke hinweisen kann.
- **bad:** Diese Klasse kennzeichnet den schlechtesten Zustand einer Strecke. Es gibt eine große Streuung der Messwerte, möglicherweise durch Überlast.

3.2 Ranking

Ein auf Grundlage der Diplomarbeit entwickeltes Analysetool bestimmt die durchschnittliche Performance beobachteter Verbindungen über einen längeren Zeitraum (ein oder mehrere Tage). Im *Ranking* werden die Verbindungen miteinander verglichen. Dazu wird die Klasse *excellent* mit dem Faktor 4 gewichtet, die Klasse *fair* mit 3, die Klasse *poor* mit 2 und die Klasse *bad* mit 1. Das Vorkommen der Viertelstundenwerte je Klasse wird gezählt und auf einen Tag aggregiert. Durch die Gewichtung der einzelnen Klassen ergibt sich ein Score, der den Rang bestimmt. Der maximal erreichbare und somit „beste“ Wert für eine Verbindung und einen Tag beträgt daher 384, während im „schlechtesten“ Fall ein Score von 96 zu Buche steht.
Der dem Ranking zugrundeliegende OWD gibt keine Auskunft über die Gründe für eine bestimmte Performance auf den Verbindungen. So ist es beispielsweise durchaus verständlich, wenn das OWD bei „langen“ Strecken oder abhängig vom zurückgelegten Weg (Anzahl der Hops) größer ist. Auch eine Überlast kann zu Phänomenen im OWD führen.

4 Ranking am Beispiel des LHCOPN

4.1 Das LHCOPN

Durch den Betrieb des Large Hadron Collider (LHC) am CERN fallen große Mengen Daten an, die an verschiedenen Einrichtungen überall auf der Welt gespeichert und verarbeitet werden sollen. Das LHCOPN (Large Hadron Collider Optical Private Network) ist das Netzwerk, welches Tier0- (Datenquelle) und Tier1- (erste Verarbeitung und Speicherung) Standorte miteinander verbindet. Daran schließen sich Tier2-Standorte an, in der Regel Universitäten und andere wissenschaftliche Einrichtungen.

4.2 Laufzeitmessungen im LHCOPN

Das WiN-Labor beteiligt sich an diesem Projekt durch eine aktive Überwachung der Performance des zugehörigen Routernetzes.

An allen Tier0/Tier1-Standorten wurden HADES-Messboxen installiert: SARA/NL (Amsterdam, **NL-T1**), DE-KIT (Karlsruhe, **DE-KIT**), PIC (Barcelona, **ES-PIC**), IN2P3 (Lyon, **FR-CCIN2P3**), CERN (Genf, **CH-CERN**), CNAF (Bologna, **IT-INFN-CNAF**), NDGF (Kopenhagen, **NDGF**), BNL (New York, **US-T1-BNL**), ASGC (Taipeh, **TW-ASGC**), TRIUMF (Vancouver, **CA-TRIUMF**), FNAL (Chicago, **US-FNAL-CMS**), RAL (Rutherford, **UK-T1-RAL**).

Eine Darstellung des gemessenen OWDs zeigt Abbildung 1.

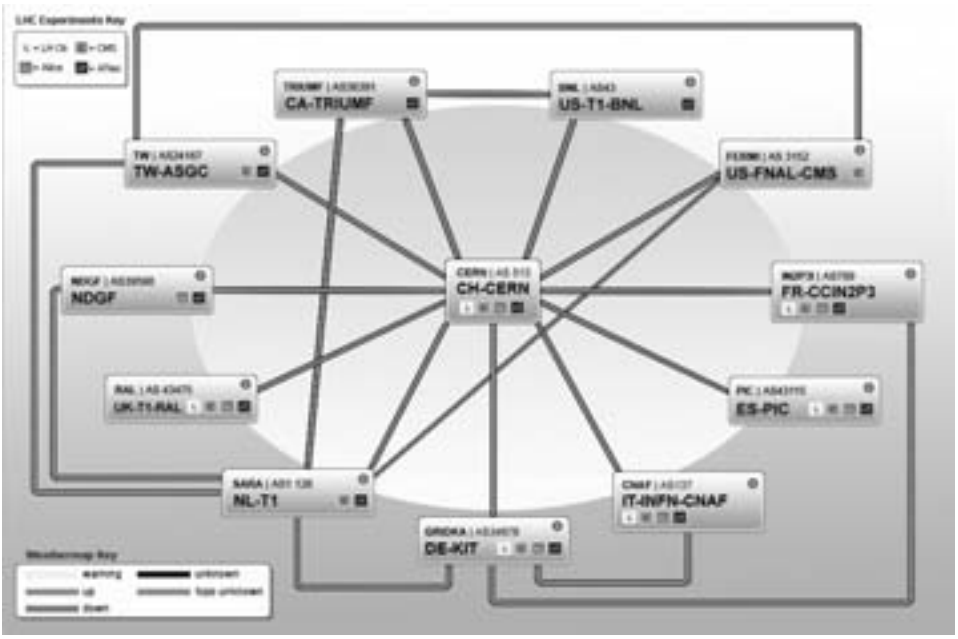

Abbildung 1: Topologie und HADES-Messungen im LHCOPN.

4.3 Ranking

Im LHCOPN werden momentan 40 Messstrecken (20 Verbindungen, jeweils Hin- und Rückrichtung) betrachtet und bewertet.
Für die folgenden Beispiele wurden über einen Zeitraum von 10 Tagen die jeweils 10 schlechtesten Verbindungen pro Tag statistisch analysiert.

Verlauf

Die Tabelle 2 zeigt exemplarisch zwei Strecken, die in der Statistik erfasst werden, aber einen unterschiedlichen Verlauf im entsprechenden Zeitraum aufweisen.

Während die Verbindung von TW-ASGC-HADES nach CH-CERN-HADES an jedem der 10 Tage mit wechselndem Rank unter den 10 schlechtesten Leitungen ist (Anzahl), an vier Tagen sogar als schlechteste Leitung (Rang 1), findet man die Verbindung von IT-INFN-CNAF-HADES nach CH-CERN-HADES nur an zwei Tagen. Das zeigt sich auch im unterschiedlichen, über die 10 Tage gemittelten Score. Je niedriger der Score, desto schlechter ist die Qualität.

Tabelle 2: Tagesranking zweier Beispielstrecken.

Messstrecke	Tag	1	2	3	4	5	6	7	8	9	10	Anzahl	Score
TW-ASGC -> CH-CERN	Rang	**4**	**3**	**1**	**7**	**7**	**1**	**1**	**1**	**1**	**1**	10	**199**
IT-INFN-CNAF -> CH-CERN	Rang	>10	>10	>10	>10	>10	**7**	>10	>10	>10	**9**	2	**257**

Gemittelte Scores

Abbildung 2 zeigt die gemittelte Summe des Scores über 10 Tage. Aufgrund der beschriebenen Gewichtung nimmt die Qualität der Verbindungen von oben nach unten ab.

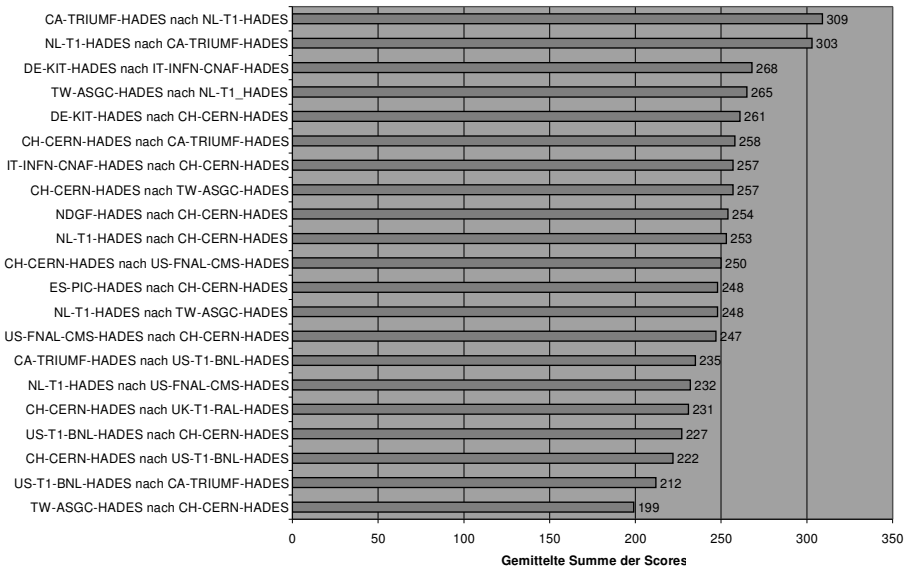

Abbildung 2: Gemittelte Summe der Scores im LHCOPN über 10 Tage.

Von den 40 im LHCOPN überwachten Verbindungen werden 21 in der Statistik aufgeführt. D.h. von den 21 Strecken ist jede mindestens einmal unter den schlechtesten 10 Strecken eines Tages gewesen. Die zwei besten der 21 Strecken liegen mit einem gemittelten Score von 309 bzw. 303 (zum Vergleich: Maximalscore = 384) deutlich über der Qualität der schlechtesten Verbindung mit einem Score von 199. In Abbildung 5 sind OWD und OWDV dieser Verbindung zu sehen.

Vorkommen im Ranking

Zählt man die Häufigkeiten des Auftretens der Verbindungen im 10-Tages Intervall, erhält man eine Häufigkeitsverteilung, die ebenso als Indiz für die Qualität der Verbindung dienen kann. Die schlechtesten Strecken treten am häufigsten auf (Abbildung 3).

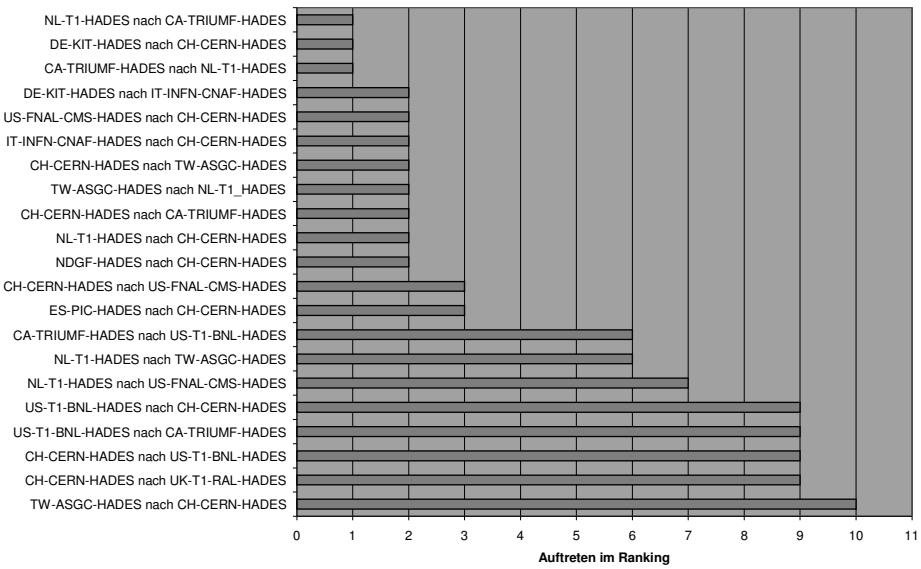

Abbildung 3: Aggregation des Auftretens im Ranking.

Die Strecke mit dem niedrigsten Score (s. Abbildung 6) ist auch hier mit dem häufigsten Auftreten im Ranking (10) am schlechtesten klassifiziert.

Aggregation nach Quelle und Senke

Eine Aggregation nach Quelle und Senke hilft bei der Suche nach Schwachstellen. Damit ist nicht nur ein Ranking der einzelnen Verbindungen möglich, sondern auch eine Bewertung der Standorte.
In Abbildung 4 wird das Auftreten eines Standortes (Senke) der letzten 10 Tage dargestellt. Zeigt sich eine relative Ausgeglichenheit beim Ranking der Standorte, liegen die Einbußen bei der Qualität der Verbindungen offensichtlich auf den Strecken selbst.

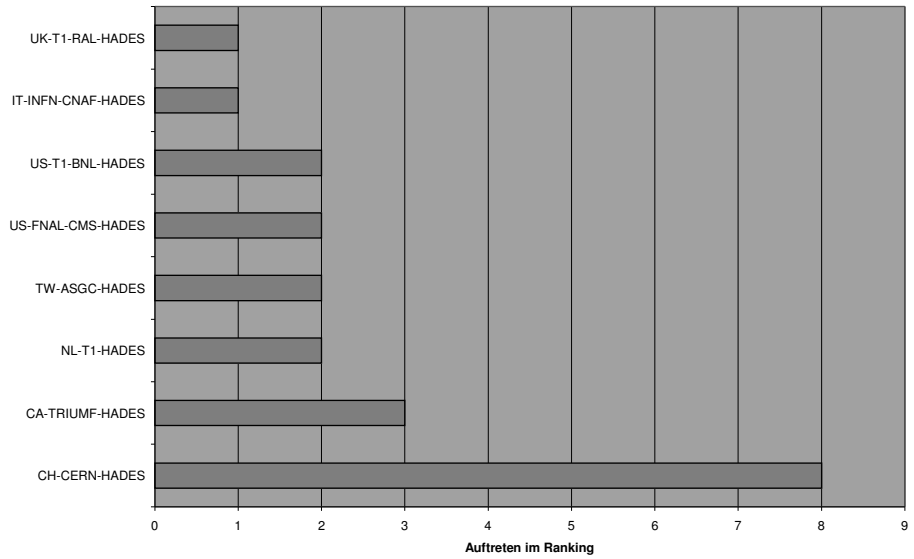

Abbildung 4: Auf Senken aggregiertes Auftreten im Ranking über 10 Tage.

In dem Fall sieht man, dass der Standort CERN wesentlich häufiger vorkommt als die anderen Standorte, was daran liegt, dass von den 40 gemessenen Verbindungen alleine 22 vom bzw. zum CERN gehen. Eine Quellen-Senken-Analyse ist sinnvoll für ein vollvermascht gemessenes Netz.

OWD und OWDV im 10-Tages-Verlauf (Abbildungen 5 und 6)

Betrachtet man den OWDV (One – Way Delay Variation, Jitter) der in Abbildung 2 an erster Stelle stehenden Verbindung (Abbildung 6) im Vergleich zur Verbindung an letzter Stelle (Abbildung 5), kann man die unterschiedliche Qualität der Verbindungen gut erkennen.
Während OWD und OWDV der Verbindung CA-TRIUMF-HADES nach NL-T1-HADES mit einem Score von 309 wenig Streuung aufweisen, ist bei gleicher Skalierung eine sehr breite Streuung auf der Verbindung TW-ASGC-HADES nach CH-CERN-HADES zu erkennen.
Ebenso kann man sehen, dass die Verbindung von CA-TRIUMF-HADES nach NL-T1-HADES wegen des ersten der ausgewählten 10 Tage im Ranking der schlechtesten 10 Verbindungen auftaucht. An diesem Tag war diese Strecke mit Rank 2 bewertet, also als zweitschlechteste Leitung. Da sie an den restlichen der 10 Tage nicht mehr unter den schlechtesten Verbindung war, ist der Score deutlich höher als bei einer über die gleiche Zeit dauerhaft schlechten Leitung.

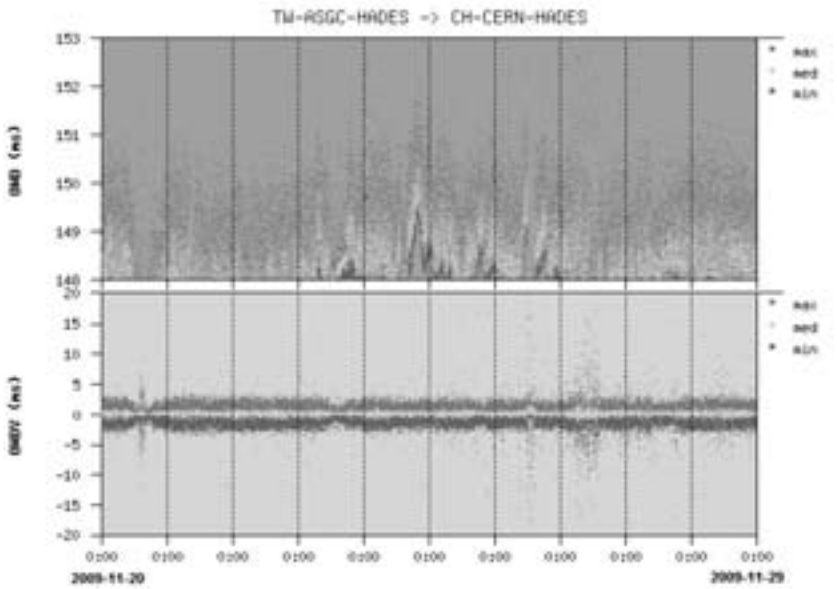

Abbildung 5: Zehn Tage Verlauf des OWD und OWDV einer Verbindung mit einem gemittelten Score von 199.

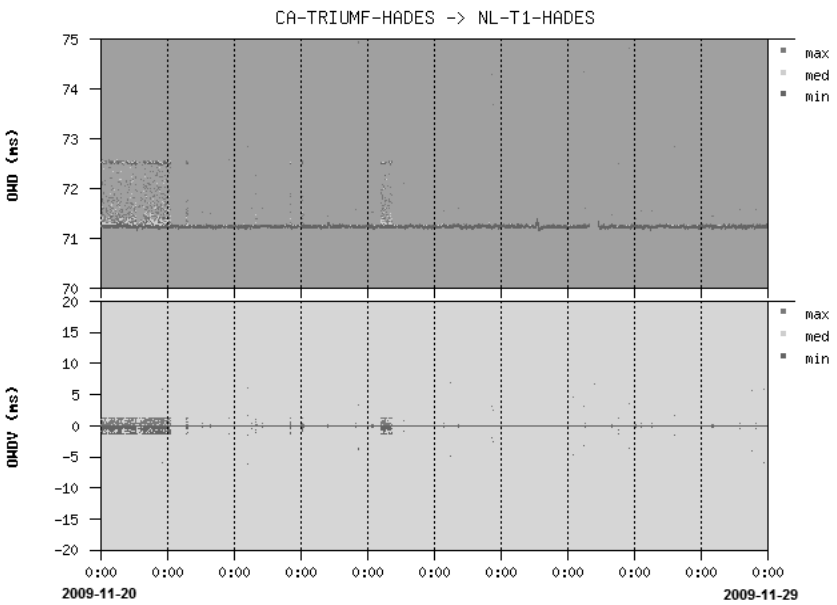

Abbildung 6: 10 Tage Verlauf des OWD und OWDV einer Verbindung mit einem gemittelten Score von 309.

5 Fazit

Die Analyse der mit dem HADES System am WiN-Labor des DFN am RegionalenRechenzentrum der Universität Erlangen-Nürnberg durchgeführten Laufzeitmessungen über einen längeren Zeitraum und damit die Bestimmung der Qualität gemessener Verbindungen ermöglicht eine Identifikation von „schlechten“ Verbindungen und liefert Informationen im Hinblick auf potentielle Schwachstellen im Netz. Das durchgeführte Ranking auf Tagesbasis und die nachfolgende Aggregation auf einen Zeitraum identifiziert sowohl Verbindungen mit kontinuierlich breiter Streuung der Messwerte, als auch Verbindungen, die temporär höhere Schwankungsbreiten aufweisen.
Für die Stellung von Verbindungen im Ranking kann es verschiedene Ursachen geben, beispielsweise die Anzahl der Hops, die Entfernung der Standorte, oder die Auslastung der Leitung (kontinuierlich, periodisch, singulär) selbst..
Die Bewertung durch das Ranking ermöglicht demnach zunächst eine Identifikation auffälliger Verbindungen, die Betrachtung der tatsächlichen Messverläufe kann dann zu geeigneten Maßnahmen zur Qualitätsverbesserung führen.

Literaturverzeichnis

[ALM99a] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Delay Metric for IPPM. http://www.rfc-editor.org/rfc/rfc2679.txt.

[ALM99b] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Packet Loss Metric for IPPM. http://www.rfc-editor.org/rfc/rfc2680.txt

[DC02] C. Demichelis and P. Chimento. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). http://www.rfc-editor.org/rfc/rfc3393.txt.

[DFN09] http://www.dfn.de/projekte/gefoerderte-projekte/.

[FAA] http://gps.faa.gov.

[GEA] The GÉANT Network. http://www.geant.net/.

[HAD09] http://www.win-labor.dfn.de/English/dienste_aktiv.html.

[HOL07] T. Holleczek: Redesign und Implementierung eines Softwarepakets zur Messung der IP Performance nach OWAMP-Standard. Studienarbeit, Universität Erlangen-Nürnberg, 2007.

[HOL08] T. Holleczek: Statistical Analysis of IP Performance Metrics in International Research and Educational Networks. Diplomarbeit, Universität Erlangen-Nürnberg, 2008.

[HKK06] P. Holleczek, R. Karch, R. Kleineisel, S. Kraft, J. Reinwand, and V. Venus. Statistical characteristics of active IP one way delay measurements. In R. Karch, editor, Proc. International Conference on Networking and Services, ICNS ’06, pages 1–1, 2006.

[NTP1] http://de.wikipedia.org/wiki/Network_Time_Protocol.

[NTP2] http://tools.ietf.org/html/rfc1305.

[PAMM98] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis. Framework for IP Performance Metrics. http://www.rfc-editor.org/rfc/rfc2330.txt.

[XWI] X-WiN – Germany’s National Research and Educational Network. http://www.dfn.de/content/xwin.