Anomalieerkennung basierend auf statistischer Modellierung von HADES Messdaten

Kai Ramsch, Birgit Kraft

DFN-Labor
Regionales Rechenzentrum Erlangen
Martensstraße 1
91058 Erlangen
{kai.ramsch, birgit.kraft}@fau.de

Zusammenfassung: Im Rahmen der Qualitätskontrolle in Weitverkehrsnetzen erfasst das am DFN-Labor entwickelte HADES Monitoringtool aktiv One-Way Delay Daten auf Messtrecken innerhalb eines Netzwerkes. Diese Daten werden visuell dargestellt und können für die Überwachung des Netzwerkes und die Analyse vergangener Ereignisse im Netz eingesetzt werden. In einem vollvermaschten Messnetz kann die Überwachung wegen der Vielzahl an Messtrecken nicht mehr manuell erfolgen. In dieser Arbeit werden daher Normalzustände für individuelle Messstrecken durch mathematische Modelle definiert und ein Algorithmus vorgestellt, der One-Way Delay Messwerte statistisch nach Anomalien durchsucht. Die Anwendung des Verfahrens auf ausgewählte Messstrecken des X-WiN demonstriert eine erfolgreiche Erkennung von Anomalien mit einer geringen Fehlerquote. Eine Analyse der Falschmeldungen ergibt, dass bei geeigneter Adaption der Datenvorverarbeitung die Anzahl der Fehler noch weiter reduziert werden kann, so dass eine automatisierte Untersuchung aller Messstrecken eines Netzes möglich wird.

1 HADES im X-WiN

Im Betrieb von Weitverkehrsnetzen spielt die Überwachung der Dienstgüte eine entscheidende Rolle. Die dem Nutzer zur Verfügung gestellte Qualität muss durch ein geeignetes Performance Monitoring sicher gestellt sein [Or12]. Das im DFN-Labor entwickelte Monitoringtool HADES[1] (Hades Active Delay Evaluation System) misst basierend auf den Ansätzen der IETF (Working Group IPPM, 1998) aktiv Metriken wie One-Way Delay (Paketlaufzeit), One-Way Delay Variation (Laufzeitschwankung) und Packet Loss (Paketverluste) [Pa98, AKZ99a, AKZ99b, DC02]. Dazu werden UDP-Paketgruppen zu je neun Paketen in konfigurierbaren Abständen von einer Sendestation in das Netz eingeschleust, mit einem Zeitstempel versehen, um dann an einer Empfangsstation deren Laufzeit zu bestimmen [Ho06]. Aktuellere Studien zeigen, dass asymmetri-

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

sche Kommunikationspfade existieren, deren Laufzeit über die OWD-Metrik korrekt gemessen werden kann [Pa08, HLC11].

Im Deutschen Forschungsnetz X-WiN[2] wird zwischen 52 Kernnetzstandorten und einigen ausgewählten universitären Einrichtungen vollvermascht gemessen. Die Zeitsynchronisation erfolgt flächendeckend über an den Standorten aufgebaute GPS[3]-Antennen, deren Zeitsignal den NTP[4]-Dienst des Linux-Betriebssystems synchronisiert. Dies liefert eine im Vergleich [VRT08] hohe Messgenauigkeit von ca. 5µs, während die One-Way Delay Werte (OWD) im X-WiN je nach Streckenlänge bis zu 14 ms betragen.

Die gewonnenen Messdaten werden gesammelt, ausgewertet und streckenbasiert dargestellt. Ein langfristiges Ziel ist deswegen das nachträgliche, aber auch zeitnahe Erkennen von Anomalien im X-WiN, um aufgetretene Ereignisse einordnen oder frühzeitig erkennen zu können. Dazu ist es nötig, die HADES Messungen dahingehend zu untersuchen, ob für jede Messstrecke ein Zustand definierbar ist, der als „normal“ zu bezeichnen wäre. Da die OWD Werte Veränderungen in der Last der beteiligten Netzkomponenten indizieren [AKZ99a], kann die Auswertung von OWD-Messdaten bei der Alarmierung im Fehlerfall, bei der technischen Fehleranalyse oder beim Qualitätsmanagement Anwendung finden.

Bei Betrachtung der gemessenen OWD Werte über einen längeren Zeitraum ist ersichtlich, dass ein definierter Normalzustand zu verschiedenen Zeiten unterschiedlich ist. Nimmt der Verkehr beispielsweise wegen topologischer Veränderungen einen anderen Weg durch das Netz, verändert sich der OWD Wert. Die Folge dieses Route Change ist ein höherer oder auch niedrigerer OWD Wert, der aber für den Zeitraum, in dem der Verkehr diesen Weg nimmt, als „normal“ angesehen werden muss (vergleiche Abb. 2 (a)).

Die mittels HADES gemessenen OWD Werte sind nicht homogen sondern unterliegen auch ohne signifikante Ereignisse gewissen systematischen Schwankungen, z.B. durch die regelmäßige GPS/NTP-Zeitsynchronisation oder technische Störungen auf den Messboxen. Auch aktive Netzkomponenten führen zu regelmäßig auftretenden, sporadischen Fehlern (Abb. 4). Obwohl die GPS-Uhren einen sehr geringen zeitlichen Versatz zwischen unterschiedlichen Messrechnern gewährleisten, kann es durch äußere Einflüsse, wie z.B. eine Erhöhung der Raumtemperatur, auch zu starken Schwankungen kommen. Diese zeichnen sich durch ein charakteristisches, zeitliches Verhalten der OWD Werte, bedingt durch das erneute Synchronisieren der Uhren, aus (Abb. 5 (a)). Diese Schwankungen sind daran zu erkennen, dass sich der zeitliche Verlauf der OWD Werte entgegengesetzter Messstrecken invertiert.

Das DFN-Labor kann im Rahmen des Qualitätsmanagements für den DFN viele Auffälligkeiten im X-WiN eindeutig ihren Ursachen zuordnen. Durch die ausreichend große Dimensionierung des Deutschen Forschungsnetzes treten betriebsbeeinflussende Überlastsituationen allerdings äußerst selten auf und lassen sich kaum zur Analyse eines

[2] https://www.dfn.de/en/
[3] http://gps.faa.gov
[4] http://www.ntp.org/

produktiven Weitverkehrsnetzes hinzuziehen. Für das Testen und Kalibrieren des in dieser Arbeit vorgestellten Anomalieerkennungsalgorithmus dienen deswegen u.a. die regelmäßig auftretenden Uhrensynchronisationsereignisse, welche sich relativ leicht in der Visualisierung erkennen lassen und gut von den systematischen Schwankungen der OWD Messdaten im Normalzustand unterscheidbar sind.

Da die Definition einer Anomalie abhängig davon ist, welcher Nutzer die Analyse der Daten zu welchem Zweck benötigt, kann es durchaus sinnvoll sein, Informationen über Uhrensynchronisationsereignisse darzustellen. Dabei kann sowohl die auslösende Komponente von Bedeutung sein, als auch die Tatsache, dass die Qualität der Messdaten und dadurch ihre Verwendbarkeit möglicherweise eingeschränkt ist.

2 Algorithmus zur statistischen Anomalieerkennung

Das Erkennen von Anomalien einer Messgröße erfordert die mathematische Beschreibung eines Normalzustandes. Im Rahmen dieser Arbeit wird der Normalzustand einer Messstrecke, d.h. einer Messung zwischen zwei HADES Messstationen mit ausgezeichneter Quelle und Senke, durch ein statistisches Modell ausgewählter One-Way Delay Werte dieser Messstrecke realisiert. Die Heterogenität der OWD Werte einer Messstrecke in produktiven Netzen verhindert eine direkte Definition des Normalzustandes aus den Daten heraus. Aus diesem Grund muss eine Datenmenge der Messstrecke ausgewählt werden, die intuitiv als normal eingestuft wird. Mit dem diese Datenmenge beschreibenden Modell können dann beliebige Daten der gleichen Messstrecke auf Normalität getestet und Anomalien erkannt werden.

2.1 Modellierung des Normalzustandes

Für die statistische Analyse wird ein Normalintervall, d.h. ein Zeitintervall in dem alle Messdaten einer Messstrecke als normal eingestuft werden, definiert. Die OWD Werte des Normalintervalls werden dann mit Hilfe des in [Ho08] vorgestellten Algorithmus durch ein Gamma-Mixture-Model repräsentiert. Dabei werden die OWD Rohdaten, formal ein Vektor Y, in zwei Vorverarbeitungsschritten erstens um Zeitsynchronisationsfehler bereinigt und zweitens um die minimale Paketlaufzeit reduziert.

Für bestimmte Anwendungsszenarien wie der Einsatz in der Performanzüberwachung eines Netzbetreibers müssen Zeitsynchronisationsereignisse aus den OWD Werten gefiltert werden. Der Algorithmus zur Erkennung von Zeitsynchronisationsfehlern [Ho08] macht sich dabei zu Nutze, dass sich der zeitliche Verlauf der OWD Werte auf entgegengesetzten Messstrecken gerade invertiert. Wenn die absoluten Differenzen der OWD Werte beider Messstrecken eine aufsteigende Sequenz genügend großer Länge (l_{min}) beinhalten, deren Summe einen Schwellwert Σ_{min} überschreitet, handelt es sich bei den OWD Werten dieser Sequenz um einen Zeitsynchronisationsfehler. Da dieser zeitliche Verlauf ebenfalls Schwankungen unterliegt, die nicht auf die Zeitsynchronisation zurück zu führen sind, müssen die absoluten Differenzen vor der Fehlererkennung geglättet werden. Diese Glättung wird durch einen Box-Filter erreicht, der jeden Messwert durch

den Mittelwert eines auf ihn zentrierten Zeitfensters von Messwerten ersetzt. Nach Anwendung dieses Filters wird allerdings auch der Zeitpunkt des Zeitsynchronisationsereignisses verschoben, da das Signal des Ereignisses zuerst den Mittelwert dominieren muss, um erkannt zu werden. Der Anfang des Zeitsynchronisationsereignisses wird deswegen um die halbe Länge des Zeitfensters vor den ersten dem Zeitsynchronisationsereignis zugeordneten Messwert vorverlegt.

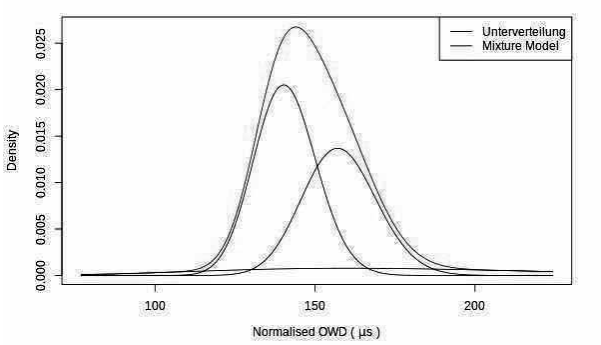

Abbildung 1: Dichtefunktion eines Gamma-Mixture-Models (Normalintervall der Messstrecke von Münster nach Oldenburg vom 24.05.11 um 12:00 Uhr bis 25.05. 11 um 8:00 Uhr mit $K = 3$).

Die OWD Werte setzen sich aus einem relativ statischen Teil, dem Intrinsic Delay, und einem variablen Teil, dem Routing Delay, zusammen. Der Intrinsic Delay wird durch die Ausbreitungsverzögerung, d.h. die minimale Zeit, die das Signal benötigt, um die aktiven und passiven Komponenten des IP-Pfades zu durchlaufen, bestimmt. Der Routing Delay ist der variable Teil der Zeitspanne, die alle beteiligten aktiven und passiven Komponenten benötigen, um das Messpaket zu verarbeiten. Es ist relativ schwierig, den Intrinsic Delay einer Messstrecke zu messen, deshalb approximiert Thomas Holleczek den Intrinsic Delay durch den kleinsten gemessenen OWD Wert innerhalb eines Zeitintervalls, in dem sich die OWD Werte nicht stark voneinander unterscheiden (Details siehe [HOL08]). Zur Berechnung des Routing Delays, also des variablen Anteils des gemessenen OWD Wertes, wird der approximierte Intrinsic Delay vom OWD Wert abgezogen.

Die aus der Vorverarbeitung resultierenden Routing Delay Werte X befinden sich nahe des Nullpunktes und ihre Verteilung kann somit gut durch Gamma-Verteilungen modelliert werden. Anschließend errechnet der Expectation-Maximisation-Algorithmus (EM-Algorithmus) das Gamma-Mixture-Model, d.h. eine gewichtete Summe von K Gamma-Verteilungen, die die Werte in X möglichst gut beschreiben (siehe Abb. 1). Formal wird die Dichtefunktion der Verteilung des Gamma-Mixture-Models durch

$$f(x) = \sum_{i=1}^{K} \pi_i \cdot \mathcal{G}_i(x) \text{ mit}$$

$$\mathcal{G}_i(x) = \mathcal{G}(x|\alpha_i, \beta_i) = \frac{\beta_i{}^{\alpha_i}}{\Gamma(\alpha_i)} x^{\alpha_i - 1} e^{-\beta_i x} \text{ und } \pi_i \in [0,1]$$

beschrieben, wobei $\mathcal{G}_i(x) = 0$ für $x \in (-\infty, 0]$ und $\Gamma(x)$ die Gamma-Funktion ist.

In anfänglichen Tests hat sich herausgestellt, dass eine Variation des Parameters K wenig an den Ergebnissen dieser Arbeit veränderte, solange $K > 2$ galt, weswegen die dargestellten Ergebnisse mit $K = 3$ erzeugt wurden.

2.2 Anomalieerkennung

Das auf das Normalintervall angepasste Gamma-Mixture-Model wird nun verwendet, um die Messdaten eines oder mehrerer Zeitintervalle zu testen. Dafür wird das zu untersuchende Zeitintervall in Testintervalle von vier Stunden Länge partitioniert. Die OWD Werte jedes Testintervalls werden dann durch zwei Arbeitsschritte vorverarbeitet und ein Chi-Quadrat Test [Ri07, S. 341] bezüglich des Gamma-Mixture-Models des Normalintervalls der Messstrecke durchgeführt.

Die Zeitsynchronisationsfehlererkennung wird analog zum ersten Vorverarbeitungsschritt bei der Auswertung des Normalintervalls durchgeführt. Für die Berücksichtigung des Intrinsic Delays der Testintervalle wurden hingegen die zwei Methoden lokaler Intrinsic Delay und globaler Intrinsic Delay implementiert. Beim lokalen Intrinsic Delay wird für jedes Testintervall ein eigenes Intrinsic Delay berechnet und von den OWD Werten abgezogen. Diese Variante ermöglicht es, die Testintervalle des zu untersuchenden Zeitintervalls trotz vorhandener Route Changes als normal zu kategorisieren, solange die vorverarbeiteten OWD Werte der Verteilung des Gamma-Mixture-Models folgen. Beim globalen Intrinsic Delay wird das Intrinsic Delay des Normalintervalls von allen OWD Werten im Testintervall abgezogen und gegebenenfalls negative Resultate verworfen. Hierbei führen Route Changes zu fehlerhafter Kategorisierung, allerdings zeigen die vorgestellten Ergebnisse, dass das Verfahren stabiler bei stark schwankenden zeitlichen Verläufen der OWD Werte ist. Unabhängig von der Vorverarbeitung der OWD Rohdaten der Testintervalle wird der Intrinsic Delay des Normalintervalls immer aus den OWD Rohdaten des Normalintervalls berechnet und abgezogen.

Bei dem anschließenden Chi-Quadrat Test werden der Wertebereich $(0, \infty)$ der Messwerte in Intervalle $(B_1, B_2, \dots, B_M)$ partitioniert (Details siehe [Ri07, S. 341]) und die Teststatistik $\mathrm{X}^2 = \sum_{i=1}^{M} \frac{(N_j^0 - N_j^e)^2}{N_j^e}$ berechnet. Hierbei ist N_j^0 die Häufigkeit derjenigen Messwerte, die in B_j liegen, und N_j^e ist die gemäß des Gamma-Mixture-Models zu erwartende Häufigkeit im Intervall B_j, d.h. $N_j^e = \int_{B_j} f(x)\, dx$. Die Teststatistik X^2 folgt einer Chi-Quadrat Verteilung mit f Freiheitsgraden, wobei f die Anzahl der Messwerte im Testinterval minus 1 ist. Wenn X^2 kleiner als das $(1-\alpha)$-Quantil der Chi-Quadrat Verteilung ist, kann man annehmen, dass die Messdaten des Testintervalls unter einem Signifikanzniveau α der Verteilung des Gamma-Mixture-Models unterliegen. Somit ergibt sich die Indikatorfunktion für die Normalität einer Messstrecke dadurch, dass das Testintervall genau dann normal ist, wenn der dazugehörige Chi-Quadrat Test erfolgreich ist. Das $(1-\alpha)$–Quantil wurde für diese Arbeit mittels $\alpha = 0.01$ gesetzt. Eine Veränderung dieses Wertes im Rahmen sinnvoller Erfahrungswerte ($\alpha \in [0.001, 0.5]$) hatte kaum Einfluss auf die Ergebnisse, könnte aber für weiterführende Studien auf anderen Messstrecken oder Zeitintervallen notwendig sein.

3 Anomalieerkennung im X-WiN

Ausgehend von den Ergebnissen der Diplomarbeit von Thomas Holleczek wurden die Parameterwerte aus [Ho08] übernommen und Berechnungen für die in Tab. 1 gelisteten Messstrecken durchgeführt.

Start Messbox	Ziel Messbox	Intrinsic Delay	Normalintervall	Testzeitraum
Koeln_DFN	Hamburg_Desy_DFN	lokal	24.05.2011:12:00- 25.05.2011:07:59	24.05.2011:00:00- 25.05.2011:23:59
Muenster_DFN	Oldenburg_DFN	global	15.09.2012:00:00- 08.10.2012:23:59	15.09.2012:00:00- 08.10.2012:23:59
Rostock_DFN	Saarbruecken_DFN	global	01.06.2011:00:00- 08.06.2011:23:59	01.06.2011:00:00- 11.06.2011:23:59

Tabelle 1: Übersicht dargestellter Messstrecken mit der verwendeten Methode zur Verarbeitung des Intrinsic Delays, sowie die Grenzen des Normalintervalls und des untersuchten Testzeitraums.

Abb. 2 (a) stellt Maxima, Mediane und Minima der OWD Werte aller Paketgruppen dar, die im Testzeitraum auf der Messstrecke vom Standort Köln zum Standort DESY Hamburg gemessen wurden. Der Messverlauf zeigt den Neustart der Messbox in Köln am 24.05.11. Am darauf folgenden Tag ist ein Route Change zu sehen, der den Intrinsic Delay als Bestandteil des OWD Wertes um mehr als eine Millisekunde erhöht. Die in Abb. 2 (b) dargestellte Indikatorfunktion stuft sowohl Testintervalle vor als auch nach dem Route Change als normal ein. Lediglich drei der Testintervalle werden als Anomalie kategorisiert. Nach dem Neustart um ca. 10:00 Uhr am 24.05.11 wurden Daten auf der Messbox komprimiert, was aufgrund der Last zu erhöhten OWD Werten führte. Das Testintervall von 8:00 Uhr bis 12:00 Uhr am 25.05.11 wird als Anomalie erkannt, da es Daten mit unterschiedlichem Intrinsic Delay beinhaltet. Im Testintervall von 0:00 Uhr

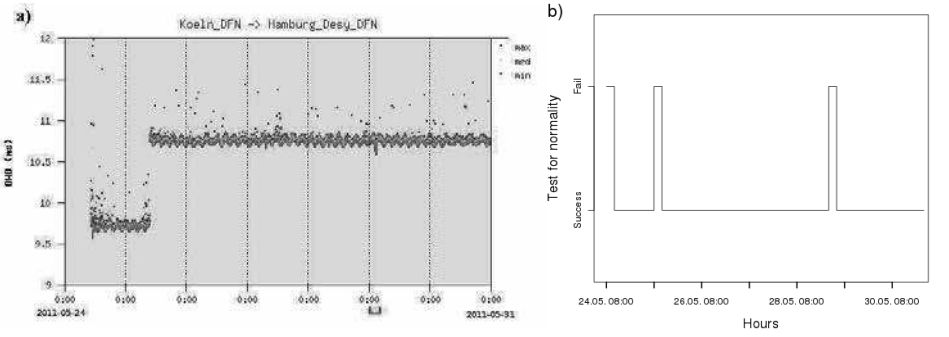

Abbildung 2: Ergebnisse für die Messstrecke von Köln nach DESY Hamburg vom 24.05.11 bis 31.05.11. **a)** Maxima, Mediane und Minima der OWD Paketgruppen. Am 24.05.11 existieren erst ab ca. 8:00 Uhr Messwerte. Am 25.05.11 um ca. 8:00 Uhr gibt es einen Route Change. Eine Schwankung nach unten am 29.05.11 reduziert den berechneten Intrinsic Delay des Testintervalls (rote Markierung). **b)** Indikatorfunktion für den getesteteten Zeitraum. Eine Skaleneinheit der Abszisse entspricht einem Testintervall. Ein Erfolg (success) bedeutet, dass das Testintervall als normal eingestuft wurde, ein Misserfolg (fail) kennzeichnet eine Anomalie, und bei einer Unterbrechung der Indikatorfunktion fehlen OWD Messwerte oder werden durch die Vorverarbeitung verworfen.

bis 4:00 Uhr am 29.05.11 führt ein Ausreißer zur Berechnung eines kleineren Intrinsic Delays, obwohl die Mehrzahl der OWD Werte dieses Testintervals in Abb. 2 (a) (rote Markierung) einen normalen zeitlichen Verlauf zeigen. Während Ausreißer nach oben relativ wenig Einfluss auf den Erfolg der Anomalieerkennung haben, führen Ausreißer nach unten dazu, dass alle OWD Werte im selben Testintervall um einen geringeren Wert als in vergleichbaren Testintervallen reduziert werden. Damit ändern sich aber die Häufigkeiten aller mit der Verteilung des Gamma-Mixture-Models verglichenen Partitionsintervalle beim Chi-Quadrat Test und dieser schlägt fehl.

Für die Anomaliedetektion in Abb. 2 (b) wurde der Intrinsic Delay lokal berechnet, damit der Route Change keine fehlerhaften Ergebnisse liefert. Diese Herangehensweise funktioniert ohne weitere Adaptionen des Verfahrens nicht bei allen Messstrecken. So kategorisiert der Algorithmus bei Verwendung eines Normalintervalls über mehrere Wochen auf der Messstrecke zwischen Münster und Oldenburg (siehe Abb. 3 (a)) alle Testintervalle als Anomalie (keine Abb.), während unter Verwendung eines globalen Intrinsic Delays lediglich vier Testintervalle in drei Ereignissen als Anomalie eingestuft werden (Abb. 3 (b)). Abb. 3 (a) zeigt am 27.09.12 eine starke Abweichung in den OWD Werten, die sich über zwei Testintervalle erstreckt. Intuitiv würde man nun erwarten, dass diese Abweichung bereits vom Vorverarbeitungsschritt des Testintervalls als Zeitsynchronisationsfehler erkannt wird. Des Weiteren würde man die Daten am 16.09.12 und 03.10.12 als normal einstufen, da sie in Abb. 3 (a) kaum von den sie umgebenden als normal eingestuften Testintervallen zu unterscheiden sind.

Grund für dieses fehlerhafte Verhalten der Anomalieerkennung ist die Skalierung der OWD Werte, d.h. die Spanne zwischen Minimum und Maximum des untersuchten Zeitintervalls. Während qualitätsbeeinflussende Ereignisse wie Route Changes (Abb. 2 (a)) und Synchronisationsprozesse (Abb. 5 (a)) Veränderungen der OWD Werte in der Größenordnung von einer Millisekunde verursachen, sind hier die Unterschiede bis auf gelegentliche Ausreißer in der Größenordnung von 0.1 ms. Dadurch überschreitet die Summe der geglätteten absoluten Differenzen zwischen Hin- und Rückrichtung der Messstrecke niemals den Schwellwert Σ_{min}, weswegen es sich, wie vom Vorverarbeitungs-

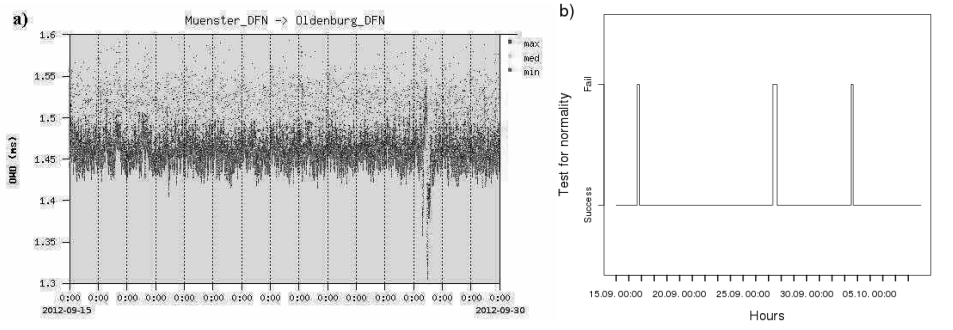

Abbildung 3: Ergebnisse für die Messstrecke von Münster nach Oldenburg. **a)** Maxima, Mediane und Minima der OWD Paketgruppen vom 15.09.12 bis 30.09.12. Am 27.09.12 ist eine Schwankung in Form eines Zeitsynchronisationsfehlers zu sehen. **b)** Indikatorfunktion für den getesteten Zeitraum vom 15.09.12 bis 09.10.12 (Beschreibung siehe Abb. 2 (b)).

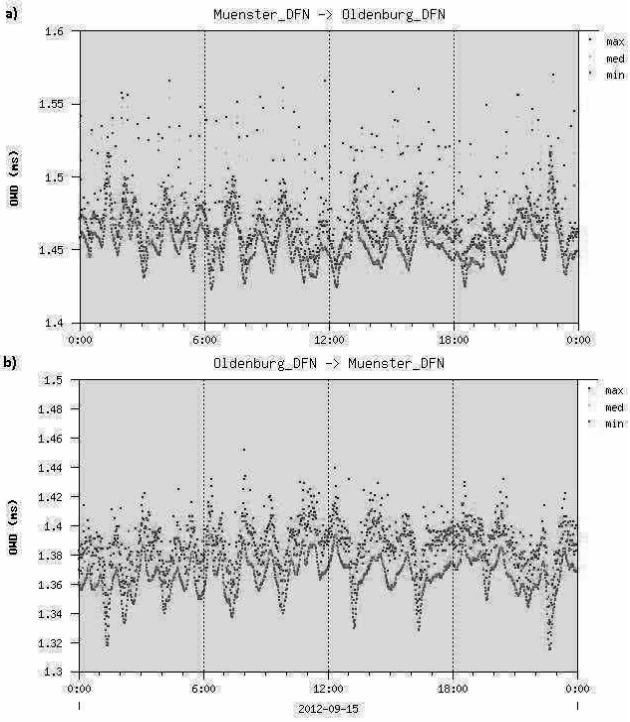

Abbildung 4: Maxima, Mediane und Minima der OWD Paketgruppen für den 15.09.12 (9 Pakete / Gruppe, 1 Gruppe / min). Messstrecke von **a)** Münster nach Oldenburg und **b)** Oldenburg nach Münster. Besonders die Minima zeigen einen jeweils gespiegelten zeitlichen Verlauf.

schritt korrekt erkannt, nicht um einen Zeitsynchronisationsfehler handelt. Die Darstellung der Messwerte eines Tages (Abb. 4 (a)) veranschaulicht, dass die Werte regelmäßigen Schwankungen unterliegen. Der Vergleich mit den Messwerten der entgegengesetzten Messstrecke (Abb. 4 (b)) ist ein starkes Indiz dafür, dass es sich bei diesen Schwankungen um die kontinuierlichen Anpassungen der NTP-Dienste der Messboxen an das Zeitsignal der GPS-Uhren handelt. Da es ansonsten kaum andere Störquellen gibt, die die Messwerte erheblich beeinflussen, passt der EM-Algorithmus das Gamma-Mixture-Model relativ genau an diese Schwankungen an. In Folge dessen werden selbst leichte Abweichungen als Anomalie erkannt, obwohl diese ‚hochpräzise' Modellierung der OWD Werte für die Anomalieerkennung keine Rolle spielen sollte.

Im dritten Datensatz auf der Messtrecke von Rostock nach Saarbrücken sind zwei Uhrensynchronisationen sichtbar (Abb. 5 (a)). Beim ersten Ereignis am 03.06.11 wurde ein Reboot der Messbox in Rostock durchgeführt. Der Ausschlag der OWD Werte entstand dadurch, dass die HADES Messungen vor dem NTP-Dienst wieder aktiv waren. Die danach folgende Schwankung ist auf das Synchronisieren der GPS-Antenne zurück zu führen. Die Vorverarbeitung reduziert in diesem Fall im ersten Testintervall erfolgreich die Messdaten und verwirft 2052 von 2133 empfangenen Messwerten. Allerdings unterliegen die verbleibenden OWD Werte dieses und des darauffolgenden Testintervalls

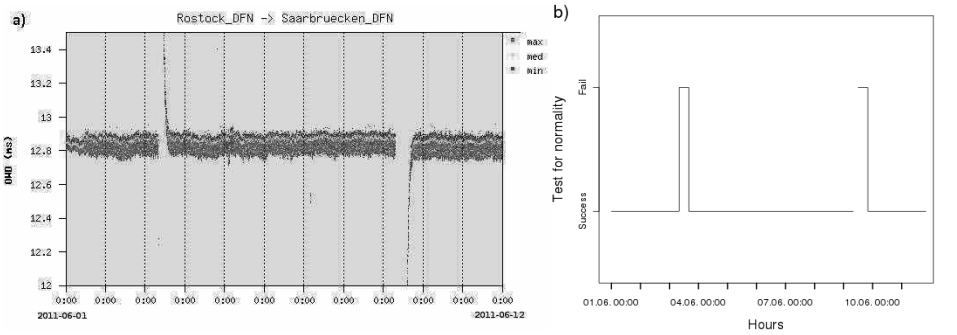

Abbildung 5: Ergebnisse für die Messstrecke von Rostock nach Saarbrücken vom 01.06.11 bis 12.06.2011. **a)** Maxima, Mediane und Minima der OWD Paketgruppen. Am 03.06.11 ist der Ausschlag eines Zeitsynchronisationsfehlers zu erkennen. Für den Ausschlag am 09.06.11 fehlen in der entgegengesetzten Messstrecke die OWD Messwerte. **b)** Indikatorfunktion für den getesteten Zeitraum (Beschreibung siehe Abb. 2 (b)).

noch nicht der Verteilung des Normalintervalls, weswegen die Indikatorfunktion in Abb. 5 (b) eine Anomalie erkennt. Das zweite Uhrensynchronisationsereignis am 09.06.11 wird von der Zeitsynchronisationsfehlererkennung nicht erkannt und von der Indikatorfunktion als Anomalie eingestuft, weil die für die Berechnung der Differenzen benötigten Messwerte der entgegengesetzten Messstrecke fehlen.

In beiden Fällen sollten die Daten dieser Testintervalle je nach Anwendung der Anomalieerkennung geeignet interpretiert werden. Für einen Netzbetreiber beispielsweise könnten diese Daten als unzuverlässig markiert werden, während ein Betreiber der Messinfrastruktur auf ein Problem des Systems hingewiesen werden könnte.

4 Diskussion

Diese Arbeit hat gezeigt, dass es mittels statistischer Methoden möglich ist, die mit dem im WiN-Labor entwickelten HADES System erhobenen Messdaten so zu analysieren, dass Ereignisse und Störungen im X-WiN automatisiert entdeckt werden könnten. Der anhand von Uhrenereignissen bewertete und kalibrierte Anomalieerkennungsalgorithmus ist in der Lage, selbst geringfügige Abweichungen vom Normalzustand einer Messstrecke zu erkennen.

In der vorgestellten Parametrisierung ist das Verfahren bei der Charakterisierung des den Normalzustand beschreibenden statistischen Modells noch nicht robust genug, wodurch in Einzelfällen manuell als normal eingestufte Datenintervalle als Anomalie kategorisiert wurden. Diese Fehleinschätzung des Algorithmus liegt an dessen automatischer Adaption an den Wertebereich der Messdaten, die systembedingte, geringfügige Schwankungen zu stark im Modell repräsentiert. Fehleinschätzungen dieser Art könnten z.B. durch Einfügen von Toleranzschwellen oder Erhöhung der Messwertegranularität verhindert werden. Dazu müssen diese Schwankungen im Rahmen einer Fehleranalyse abgeschätzt und Parameter für die Toleranzschwellen und die Messwertegranularität abgeleitet werden.

Die dargestellten Untersuchungen verdeutlichen, dass es für eine Anwendung in produktiven Netzüberwachungsszenarien wichtig ist, Ereignisse so zu klassifizieren, dass sie von Vorfällen auf der Messinfrastruktur zu unterscheiden sind. Für die Fehleranalyse und anschließende Weiterentwicklung des Verfahrens ist es deswegen von Bedeutung, Ereignisse zu finden und zu beschreiben, die eindeutig auf Netzlast oder die Störung aktiver Komponenten zurück zu führen sind bzw. diese Ereignisse in einer Laborumgebung zu erzeugen. Nach einer erfolgreichen Erkennung solcher Störungen sollte das Verfahren auf große Zeiträume und eine größere Auswahl an Leitungen angewendet werden.

Durch die statistische Analyse der HADES Messdaten wird sowohl Netzbetreibern als auch den Betreibern von Messinfrastruktur ein Tool in die Hand gegeben, mit dessen Hilfe es möglich sein wird, netzbedingte Anomalien zu erkennen und zu bewerten. In Abhängigkeit von der Zielgruppe müssen geeignete Klassen von Anomalien definiert werden, die für die betrieblichen Belange von Bedeutung sind. Wünschenswert wäre in dem Zusammenhang auch, die Zustände einer Messstrecke so genau beschreiben zu können, dass die Anomalieerkennung sehr zeitnah oder eventuell bereits im unmittelbaren Vorfeld erfolgen kann.

Danksagung: Wir möchten Patrick Gress für die Bereitstellung von Softwaremodulen für diese Arbeit danken.

Literaturverzeichnis

[AKZ99a] Almes, G.; Kalidindi, S.; Zekauskas. M.: IETF A Oneway Delay Metric for IPPM, RFC 2679, 1999.

[AKZ99b] Almes, G.; Kalidindi, S.; Zekauskas, M.: IETF A Oneway Packet Loss Metric for IPPM, RFC 2680, 1999.

[DC02] Demichelis, C.; Chimento, P.: IETF IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), RFC 3393, 2002.

[HLC11] Hong, C-Y.; Lin, C-C.; Caesar, M.: 2011. Clockscalpel: understanding root causes of internet clock synchronization inaccuracy. In Proc. 12th Int. Conf. on Passive and Active Measurement, Springer-Verlag, Berlin, Heidelberg, 2011, S. 204-213.

[Ho06] P. Holleczek et. al.: Statistical characteristics of active IP one way delay measurements. In Proc. Int. Conf. on Networking and Services, 2006, S. 1–1, 2006.

[Ho08] T. Holleczek: Statistical Analysis of IP Performance Metrics in International Research and Educational Networks. Diplomarbeit, Univ. Erlangen Nürnberg, 2008.

[Or12] Orgerie, A.-C. et. al.: Survey of Network Metrology Platforms. In IEEE/IPSJ Int. Symp. on Applications and the Internet , 2012, S. 220-225

[Pa98] Paxson, V. et. al.: IETF Framework for IP Performance Metrics, RFC 2330, 1998.

[Pa08] Pathak, A. et. al.: A Measurement Study of Internet Delay Asymmetry. In (Claypool, M.; Uhlig, S. Hrsg.): Proc. 9th Int. Conf. on Passive and Active Network Measurement, Springer-Verlag, Berlin, Heidelberg 2008, S. 182-191.

[Ri07] Rice, J.A.: Mathematical Statistics and Data Analysis. Thomson, Belmont, 3. Aufl., 2007.

[VRT08] De Vito, L.; Rapuano, S.; Tomaciello, L.: One-Way Delay Measurement: State of the Art. In IEEE Trans. on Instrumentation and Measurement 57(12), 2008, S. 2742-2750