

Forschungsprojekt  
**Ausreißererkennung in Zeitreihen  
mittels graphen-basierter Algorithmen**

im Studiengang Angewandte Informatik  
der Fakultät Informationstechnik  
Wintersemester 2020/2021

Bahar Uzun

764647

Jeremy Kielman

764097

Marcus Erz

762294

**Abgabedatum:** 18. März 2021

**Prüferin:** Prof. Dr. rer. nat. Gabriele Gühring

---

## Kurzfassung

Die Ausreißererkennung ist eine Problematik, deren Wichtigkeit in den letzten Jahren rasant zugenommen hat. Gerade die Nutzung der Datenrepräsentation, als Graphen oder Netzwerken, zur Ermittlung von Ausreißern ist rapide gestiegen. Grund hierfür sind die Vorteile, die die Abbildung von Daten in Graphen, sowie die einfachere Erkennung von Korrelationen zwischen Datenobjekten hat. Wird der Faktor Zeit hinzugezogen, so hat man die Möglichkeit, zum einen die Korrelationen besser zu erfassen und zum anderen, die strukturelle Änderung der Graphen über die Zeit zu entdecken. In einem weiteren Schritt können Zeitreihendaten als Graphen repräsentiert und deren Ausreißer effektiv identifiziert werden. [vgl. 14, S. 1]

Einerseits wird in dieser Fortsetzung des Forschungsprojekts ein dynamischer Algorithmus, NetSimile, dem einen struktur-basierten Ansatz zugrunde liegt, als Pendant zum statischen OddBall-Algorithmus, evaluiert und angewendet. Andererseits wird der dynamische MIDAS-Algorithmus, der Ausreißer in Abhängigkeit von Clusterbildungen detektiert, als Pendant für den statischen SCAN-Algorithmus näher betrachtet. Weiterhin wird der Percolation-basierte Algorithmus als weiterer kanten-basierter Ansatz zur Erkennung von Ausreißern, sowie der IsoMap-basierte Algorithmus als Teil des Forschungsprojekts angewendet um die Ergebnisse verschiedenster Ansätze miteinander zu vergleichen. [17]

Für jeden dieser Algorithmentypen werden dieselben Netzwerkdaten sowie Zeitreihendaten genutzt, damit ein stringenter Vergleich der Ergebnisse ermöglicht wird. Darüber hinaus wird für den NetSimile-Algorithmus, der ein graphen-basierter Algorithmus zur Ausreißererkennung in dynamischen Graphen ist, Optimierungsmöglichkeiten evaluiert und erste Optimierungen vorgenommen, damit dieser alle Anforderungen eines erfolgreichen Einsatzes im Gebiet der Ausreißererkennung in Zeitreihen mittels graphen-basierter Algorithmen erfüllt. Dieser ist als Teil des Forschungsergebnisses sehr gut in der Erkennung von sämtlichen Ausreißer-Arten in Zeitreihen und zudem überaus performant.

**Schlagwörter:** Anomalie-Erkennung, Ausreißererkennung, NetSimile, MIDAS, dynamische Graphen, Percolation-basierte Ausreißererkennung, IsoMap-basierte Ausreißererkennung, graphen-basierte Algorithmen, Zeitreihen, Zeitreihentransformation, graphen-basierte Datenrepräsentation, evolvierende Graphen

# Inhaltsverzeichnis

|   |     |
|---|-----|
| Abbildungsverzeichnis                           | v   |
| Tabellenverzeichnis                             | vi  |
| Listings  | vii |
| 1 Einleitung                                    | 1   |
| 1.1 Problemstellung . . . . .                   | 1   |
| 1.2 Verwandte Arbeiten . . . . .                | 2   |
| 2 Verwendete Datensätze                         | 4   |
| 2.1 Numenta-Zeitreihendaten . . . . .           | 4   |
| 2.2 Netzwerk-Datensätze . . . . .               | 4   |
| 3 Statische Algorithmen zur Ausreißererkennung  | 6   |
| 3.1 Transformation der Daten . . . . .          | 6   |
| 3.2 IsoMap-Basierter Algorithmus . . . . .      | 7   |
| 3.2.1 Grundlagen . . . . .                      | 7   |
| 3.2.2 Implementierung . . . . .                 | 8   |
| 3.2.3 Anwendung auf Zeitreihen . . . . .        | 8   |
| 3.3 Percolation-basierter Algorithmus . . . . . | 10  |
| 3.3.1 Implementierung . . . . .                 | 10  |
| 3.3.2 Anwendung auf Zeitreihen . . . . .        | 11  |
| 4 Dynamische Algorithmen zur Ausreißererkennung | 13  |
| 4.1 Transformation der Daten . . . . .          | 13  |
| 4.2 NetSimile . . . . .                         | 15  |
| 4.2.1 Grundlagen . . . . .                      | 15  |
| 4.2.2 Anwendung auf Netzwerkdaten . . . . .     | 16  |
| 4.2.3 Anwendung auf Zeitreihen . . . . .        | 19  |
| 4.3 MIDAS . . . . .                             | 23  |
| 4.3.1 Grundlagen . . . . .                      | 23  |
| 4.3.2 Anwendung auf Netzwerkdaten . . . . .     | 26  |
| 4.3.3 Anwendung auf Zeitreihen . . . . .        | 28  |
| 5 Vergleich der graphen-basierten Algorithmen   | 32  |
| 6 Fazit und Ausblick                            | 34  |
| 6.1 Fazit . . . . .                             | 34  |
| 6.2 Ausblick . . . . .                          | 34  |

|                              |    |
|------------------------------|----|
| A Gelabelter Enron-Datensatz | 35 |
| B NetSimile                  | 36 |
| C MIDAS                      | 44 |
| D Isomap                     | 47 |
| E Percolation                | 49 |
| Literaturverzeichnis         | 51 |

# Abbildungsverzeichnis

|      |   |    |
|------|---|----|
| 2.1  | Illustration einer Numenta-Zeitreihe[2] . . . . .   | 4  |
| 3.1  | Berechnung der Distanz zwischen zwei Punkten nach Anwendung des IsoMap-Algorithmus [16] . . . . . | 7  |
| 3.2  | Problem: Übergänge . . . . .  | 9  |
| 3.3  | Ablauf Percolation-basierter Algorithmus [4] . . . . .  | 10 |
| 3.4  | Vergleich Percolation-Algorithmus mit und ohne gleitendem Mittelwert . . . . .                    | 11 |
| 4.1  | Umwandlung einer Zeitreihe in einen Beispielgraphen. . . . .                                      | 13 |
| 4.2  | Datensatz für MIDAS bestehend aus Ursprungsknoten, Zielknoten und Zeitabschnitt . . . . .         | 14 |
| 4.3  | Ausreißer-Score im Enron-Datensatz mit dem NetSimile-Algorithmus . . . . .                        | 17 |
| 4.4  | Darstellung der Ausreißer in Heatmaps . . . . .   | 18 |
| 4.5  | Ausreißer-Score im Darpa-Datensatz mit dem NetSimile-Algorithmus . . . . .                        | 19 |
| 4.6  | Vollständiger Graph mit 11 Knoten . . . . .   | 19 |
| 4.7  | Ausreißer-Score der vollständigen Graphen mit gewichteten Kanten . . . . .                        | 21 |
| 4.8  | Ausreißer-Score im Enron-Datensatz mit dem MIDAS-Algorithmus . . . . .                            | 26 |
| 4.9  | Ausreißer-Score im Darpa-Datensatz mit dem MIDAS-Algorithmus . . . . .                            | 27 |
| 4.10 | MIDAS-Algorithmus angewandt auf eine Zeitreihe mit einer erhöhten Amplitude . . . . .             | 29 |
| 4.11 | Ausreißererkennung in Zeitreihen mit MIDAS-Algorithmus . . . . .                                  | 29 |
| 4.12 | Ausreißererkennung in Zeitreihen mit MIDAS-Algorithmus und Fenstergröße 110 . . . . .             | 30 |
| 4.13 | Ausreißererkennung in Zeitreihen mit MIDAS-R-Algorithmus . . . . .                                | 31 |
| A.1  | Erkannte Ausreißer des SedanSpot-Algorithmus [10] . . . . .                                       | 35 |
| B.-2 | Signaturvektoren der Zeitreihe mit vollständigen Graphen . . . . .                                | 42 |
| B.-1 | Ausreißer-Score der vollständigen Graphen . . . . .   | 43 |

# Tabellenverzeichnis

|     |  |    |
|-----|--|----|
| 3.1 | IsoMap-Performance (vgl. Kap. D) . . . . .   | 8  |
| 3.2 | Performance des Percolation-basierten Algorithmus auf Zeitreihen (vgl. Kap. E) . . . . .                     | 11 |
| 4.1 | Inhalte des Merkmalsvektors [5] . . . . .  | 15 |
| 4.2 | Inhalte des Merkmalsvektors in der modifizierten Variante . . . . .  | 20 |
| 4.3 | NetSimile-Performance auf Zeitreihen (vgl. Kap. B) . . . . .   | 21 |
| 4.4 | Parameter des NetSimile für die Anwendung auf Zeitreihen . . . . .   | 22 |
| 4.5 | Übersicht über historische Ereignisse, die den Ausreißern zuzuordnen sind . . . . .                          | 27 |
| 5.1 | Vergleich der Algorithmen . . . . .  | 32 |
| C.1 | Bewertung des MIDAS-Algorithmus bzgl. der Erkennung von verschiedenen Ausreißertypen in Zeitreihen . . . . . | 46 |

# Listings

|  |    |
|--|----|
| 4.1 Gewichtung als neues Feature . . . . . | 16 |
|--|----|

# 1 Einleitung

Im Rahmen des Forschungsprojektes wird erforscht, wie Zeitreihendaten in Graphen umgewandelt werden können und welche Algorithmen diese Graphen am besten auf Ausreißer untersuchen können. Es erfolgt eine kurze Einführung in die Problemstellung. Ebenso werden verwandte Arbeiten vorgestellt und beschrieben.

## 1.1 Problemstellung

Die Transformation von Zeitreihendaten in Graphen ermöglicht die Generierung von Korrelationen zwischen zwei Zeitelementen. Durch diese Datenrepräsentation können die Datenobjekte, die in Abhängigkeit zueinander stehen, untersucht werden. Es wird angenommen, dass in der Erforschung von graphen-basierten Algorithmen zur Ausreißererkennung, gerade in Netzwerken, Ausreißer bzw. Anomalien effizienter erkannt werden. [vgl. 14, S. 1]

In der Forschung gibt es bereits viele Algorithmen zur Ausreißererkennung, die auf statischen sowie dynamischen Graphen anwendbar sind. Die Erkennung der Ausreißer erfolgt hierbei mit verschiedenen Ansätzen. So gibt es Algorithmen, die die Struktur der Graphen näher betrachten sowie Algorithmen, die sich auf dichte-basierte Merkmale eines Graphen fokussieren. Bei der Untersuchung von dynamische Graphen haben die strukturellen Veränderungen über die Zeit ebenso wie plötzlich massiv zunehmende Aktivitäten zwischen Knoten- und Kantenpaaren eine große Bedeutung. Darüber hinaus gibt es Ansätze zur Ausreißererkennung in sequenziellen Daten. [vgl. 14, S. 3ff.]

Bisher sind in der Forschung wenige graphen-basierten Algorithmen auf traditionellen Zeitreihendaten, wie Sensordaten, die über die Zeit gesammelt werden, vorhanden. Vielmehr liegt der Fokus auf sich über die Zeit ändernden Netzwerkstrukturen.

Im Rahmen des Forschungsprojekts werden folglich die graphen-basierten Algorithmen zur Erkennung von Ausreißern in Zeitreihendaten herangezogen um erste Erkenntnisse über die Aussagefähigkeit der Ergebnisse treffen zu können. Bei einem erfolgreichen Einsatz der Algorithmen können die Anwendungsfälle auf die Bereiche Internet of Things, Autonomes Fahren sowie die Erkennung von Krankheiten wie Krebs, erweitert werden. Dies macht das Thema der Ausreißererkennung mittels graphen-basierter Algorithmen zu einem aktuellen und wichtigen Forschungsgebiet, in dem die Vorteile einer graphen-basierten Struktur auf die Zeitreihen übertragen werden.

Das Ziel der vorliegenden Arbeit setzt sich aus den folgenden Teilzielen zusammen:

1. Die Ermittlung einer Methode zur Transformation einer Zeitreihe in einen Graphen.
2. Die empirische Anwendung der graphen-basierten Algorithmen auf Zeitreihendaten und deren Analyse hinsichtlich der Erkennung von Ausreißern.

## 1.2 Verwandte Arbeiten

In diesem Abschnitt werden Ansätze zur Erkennung von Ausreißern in statischen und dynamischen Graphen vorgestellt, die im Rahmen des Forschungsprojekts zur Erreichung der Forschungsziele herangezogen werden.

Die **Ausreißererkennung in statischen Graphen** kann nach den unterschiedlichen Ausreißerkategorien unterteilt werden. So ergibt sich die nachfolgende Taxonomie.

**Struktur-basierter Ansatz:** Mithilfe der Darstellung von Knoten und Kanten in einem Ego-Netzwerk werden in [3] die zugehörigen Eigenschaften, wie die Anzahl der Knoten und Kanten, extrahiert. Im Anschluss identifiziert dieser Algorithmus diejenigen Knoten und Kanten, die sich strukturell stark von den restlichen Ego-Netzwerken unterscheiden.

**Clustering-basierter Ansatz:** In [18] werden zwei Knoten und die Überschneidung ihrer Nachbarknoten gegenübergestellt. So wird die Annahme getroffen, dass Knoten, die sehr wenige Nachbarn im Vergleich zum Rest der Knoten in Ihrer Umgebung haben, Ausreißer sind.

**IsoMap-basierter Ansatz:** Durch die Dimensionsreduktion mithilfe des IsoMap-basierten Algorithmus in [4] gehen Informationen über Ausreißer verloren. Bei dem Versuch der Rekonstruktion können diese Informationen nicht wiederhergestellt werden. Durch einen anschließenden Vergleich der extrahierten Informationen werden Ausreißer sichtbar.

**Percolation-basierter Ansatz:** In [4] wird der Percolation-basierte Algorithmus beschrieben. Bei diesem werden aus einem Graphen schrittweise die Kanten mit den höchsten Gewichten entfernt. Dadurch werden Ausreißer vom Rest des Netzwerks separiert. Die Annahme ist, dass Ausreißer-Knoten höhere Kantengewichte zu ihren Nachbarn haben.

**kanten-basierter Ansatz:** Der [8] iteriert der Algorithmus zufällig über das Netzwerk. Dabei wird festgehalten wie oft ein Knoten besucht wurde. Ausreißer-Knoten werden dabei besonders selten besucht und können somit identifiziert werden.

Die **Ausreißererkennung in dynamischen Graphen** kann hinsichtlich ihres Inputs unterteilt werden. So ergibt sich die nachfolgende Taxonomie.

**Erkennung auf Momentaufnahmen des Graphen in zeitlichen Abständen:** Der Algorithmus in [5] vergleicht verschiedene strukturelle Merkmale zweier Momentaufnahmen eines Graphen miteinander um die Ähnlichkeit zu bewerten. Der Ausreißer wird bei einer starken Veränderung des Graphen deklariert.

**Erkennung mithilfe eines Datenstroms:** Der Algorithmus in [6] vergleicht jede ankommende Kante, zum aktuellen Zeitpunkt, mit der Anzahl am bisherigen Vorkommen dieser Kante. Hierbei werden Mikrocluster entdeckt, die anomal sind.

Um die graphen-basierten Algorithmen zur Erkennung von Ausreißern in Zeitreihendaten nutzen zu können, müssen diese Daten in Graphen umgewandelt werden. Hierbei werden Distanzmaße verwendet, um die Qualität der Ausreißererkennung zu verbessern. Im Rahmen des Forschungsprojekt ist somit die **Nutzung von Distanzmaßen** essenziell.

Überblick an existierenden Distanzmaßen: Ein Vergleich der verschiedenen Distanzmaße ist in [7] zu finden. Diese werden für die Anwendung auf Wahrscheinlichkeitsdichtefunktionen evaluiert und gruppiert.

## 2 Verwendete Datensätze

In dieser Ausarbeitung wurden mehrere Datensätze verwendet, um verschiedene Algorithmen auf ihre Leistungsfähigkeit zu testen. Nachfolgend werden die hierbei verwendeten Datensätze vorgestellt.

### 2.1 Numenta-Zeitreihendaten

Der Numenta-Datensatz besteht aus einer Reihe an synthetisch erzeugten Zeitreihen, die unterschiedliche Arten von Ausreißern simulieren. Durch die Daten wird es möglich eine qualitative Aussage über die Fähigkeiten der Algorithmen zu treffen. Für die Tests auf multivariaten Zeitreihen wurden neue Zeitreihen erzeugt. Dabei wurde für die erste Dimension eine Zeitreihe der Numenta-Gruppe verwendet. Für höhere Dimensionen wurde auf eine Zeitreihe ohne Ausreißer zurückgegriffen [2].

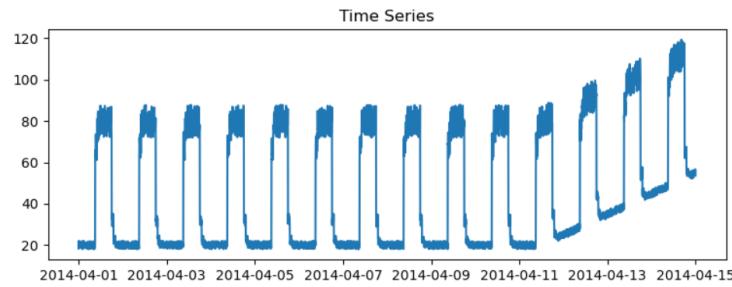


Abb. 2.1: Illustration einer Numenta-Zeitreihe[2]

### 2.2 Netzwerk-Datensätze

Zwischen den Forschungsgruppen, welche sich mit der Ausreißererkennung in Netzwerken beschäftigen, herrscht große Konkurrenz. Aus diesem Grund werden gelabelte Datensätze häufig zurückgehalten. Dadurch wollen die Forscher verhindern, dass sie ihren Wettbewerbsvorteil gegenüber anderen verlieren [1]. Aus diesem Grund ist es schwer geeignete Datensätze zu finden. Mit dem Enron- und Darpa-Datensatz konnten dennoch zwei passende Datensätze ausgemacht werden. Diese Datensätze werden im Folgenden vorgestellt.

### Enron

Der Enron Datensatz enthält die intern versendeten E-Mail Daten von rund 150 Mitarbeitern der Firma Enron. Die Daten wurden von der Federal Energy Regulatory Commission offengelegt. Enthalten sind ca. 50.000 E-Mail-Nachrichten. Für den Algorithmus wird lediglich der Zeitpunkt, an dem eine E-Mail versendet wird sowie die Sender und Empfänger festgehalten.

Für den Enron Datensatz stehen keine Labels zur Verfügung. Aus diesem Grund wurden Ausreißer, die der SedanSpot-Algorithmus gefunden hat, als Labels verwendet. [10]. Außerdem vergleichen die Autoren des SedanSpot-Algorithmus ihre Ausreißer mit der offiziellen Enron-Zeitleiste. Diese enthält ebenfalls Informationen über mögliche historische Gründe für die Ausreißer [13].

### Darpa

Der Darpa-Datensatz [11] beinhaltet 4.5 Millionen IP-zu-IP-Kommunikationen zwischen 9.400 Quell-IP's und 23.300 Ziel-IP's über einen Zeitraum von 87.700 Minuten. Jede Kommunikation ist zu einem Zeitpunkt eine gerichtete Kante von der Quell-IP zur Ziel-IP. Eine vierte Spalte des Datensatzes ist verfügbar, in der ein *label* enthalten bzw. ein Angriff gekennzeichnet ist. Der Darpa-Datensatz besteht zu über 60% aus Ausreißern.

# 3 Statische Algorithmen zur Ausreißererkennung

Die untersuchten Algorithmen können in statische und dynamische Algorithmen untergliedert werden. Für statische Algorithmen ist kennzeichnend, dass die Algorithmen im Verlauf der Zeit keine Entwicklung aufweisen. Gleiches gilt auch für die zugrundeliegenden Daten. Diese bleiben während des Algorithmus unverändert. In diesem Kapitel werden zunächst zwei statische Algorithmen zur Ausreißererkennung auf unterschiedlichen Datentypen, wie bspw. Videos, Bildern oder Netzwerken, vorgestellt. Anschließend werden die Ergebnisse verschiedener Experimente mit den Algorithmen aufbereitet. Bei den Algorithmen handelt es sich um einen auf Percolation basierenden Algorithmus (vgl. Kap. 3.3) und einen auf IsoMap basierenden Algorithmus (vgl. Kap. 3.2). In Abschnitt Kap. 3.1 wird beschrieben, wie verschiedene Datentypen in ein Netzwerk umgewandelt werden können. Dieser Schritt ist als Vorverarbeitungsschritt der Daten erforderlich.

## 3.1 Transformation der Daten

Die IsoMap- und Percolation-basierten Ansätze stellen graphen-basierte Algorithmen dar. Aus diesem Grund können sie lediglich auf Netzwerkdaten angewandt werden. Andere Datenformen müssen zunächst in einen Graphen transformiert werden, bevor die zwei Algorithmen verwendet werden können. Voraussetzung für die Transformation ist, dass eine Distanz zwischen einzelnen Datenelementen berechnet werden kann [vgl. 4, S. 2]. Der Fokus des Forschungsprojektes liegt hauptsächlich auf der Ausreißererkennung in Zeitreihen. Aus diesem Grund wird nachfolgend exemplarisch erläutert, wie Zeitreihen in Netzwerke transformiert werden können.

Für die Transformation einer Zeitreihe muss zunächst die Distanz zwischen den einzelnen Elementen bzw. Zeitpunkten der Zeitreihe berechnet werden. Hierzu wird das Distanzmaß aus Gl. 3.1 genutzt.

$$D_{ij} = \left( \sum_k |v_k^i - v_k^j|^p \right)^{1/p} \quad (3.1)$$

Für  $p = 2$  ergibt sich hierbei die euklidische Distanz. Die mit Gl. 3.1 berechneten Distanzen bilden die Kantengewichte in dem neu erstellten Netzwerk. Dabei handelt es sich um ein vollständiges Netzwerk, in dem jeder Knoten mit allen anderen Knoten über eine Kante verknüpft ist. Die Knoten des Netzwerks repräsentieren die einzelnen Elemente bzw. Zeitpunkte der Zeitreihe [vgl. 4, S. 2]. Mit dieser Vorgehensweise ist es ebenso möglich, multivariate Zeitreihen in ein Netzwerk zu transformieren.

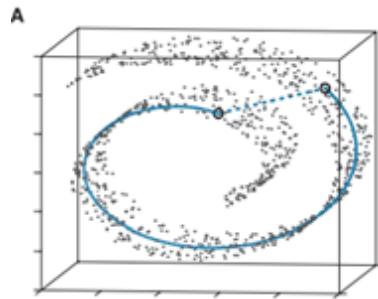
## 3.2 IsoMap-Basierter Algorithmus

Der Algorithmus verfolgt den Ansatz, Informationen über Ausreißer, durch die Reduzierung der Dimensionalität, zu eliminieren. Beim anschließenden Versuch, diese Informationen zu rekonstruieren, können durch den Vergleich mit der ursprünglichen Matrix Abweichungen bei den Ausreißerelementen festgestellt werden [vgl. 4, S. 3]. In Kap. 3.2.1 wird zunächst beschrieben, wie der IsoMap-Algorithmus eine Reduzierung der Dimensionalität durchführt. Anschließend werden in Kap. 3.2.1 die zusätzlichen Schritte erläutert, die notwendig sind um Ausreißer mithilfe des IsoMap-Algorithmus zu erkennen.

### 3.2.1 Grundlagen

#### IsoMap

Beim IsoMap handelt es sich um einen Algorithmus zur nichtlinearen Dimensionsreduktion. Zunächst werden hierbei die Nachbarn eines jeden Punktes bzw. Knotens über den Ball-Tree-Algorithmus oder den KD-Tree-Algorithmus bestimmt. Anschließend wird jeder Punkt mit den gefundenen Nachbarn verknüpft, wodurch ein neuer Körper bzw. ein neues Netzwerk entsteht. Daraufhin wird eine neue Distanzmatrix auf dem entstandenen Körper berechnet, indem die kürzeste Distanz zwischen allen Punkten auf dem Körper berechnet wird. Diese Matrix kann ebenso als geodätische Distanzmatrix  $D_G$  bezeichnet werden. Die eigentliche Dimensionsreduktion wird anschließend über die Eigenvektoren und Eigenwerte der Matrix  $D_G$  durchgeführt. Das Ergebnis der Dimensionsreduktion ist eine neue Menge an Features für jedes Element  $V^i = v_1^i \dots v_r^i$  des ursprünglichen Datensatzes. Durch das Erzeugen der Matrix  $D_G$  wird erreicht, dass nichtlineare Zusammenhänge bei der Dimensionsreduktion erhalten bleiben [vgl. 16, S. 3f.].



**Abb. 3.1:** Berechnung der Distanz zwischen zwei Punkten nach Anwendung des IsoMap-Algorithmus [16]

#### IsoMap-Algorithmus zur Erkennung von Ausreißern

Mithilfe des IsoMap-Algorithmus werden für jedes Element neue Features ( $V^i = v_1^i \dots v_r^i$ ) berechnet. In einem nächsten Schritt wird versucht, aus diesen Eigenschaften, die ursprüngliche Distanzmatrix zu rekonstruieren. Dazu wird aus den Eigenschaften  $V^i$ , unter Verwendung von Gl. 3.1, eine neue Distanzmatrix  $\hat{D}$  berechnet.

Nun können die Matrizen  $D_G$  und  $\hat{D}$  miteinander verglichen werden. Hierzu muss die Pearson-Korrelation zwischen den jeweiligen Spalten der Matrizen berechnet werden. Für Ausreißer wird angenommen, dass die Korrelation sehr niedrig ist, da Informationen über sie bei der Reduktion verloren gehen [vgl. 4, S. 3]. Die Korrelation kann also als Ausreißer-Score genutzt werden. Um zu klassifizieren, ob es sich bei einem konkreten Element um einen Ausreißer handelt, wird zunächst der Mittelwert und die Standardabweichung des Ausreißer-Scores berechnet. Falls ein Element um einen bestimmten Schwellwert vom Mittelwert abweicht, wird es als Ausreißer klassifiziert.

### 3.2.2 Implementierung

Für den IsoMap-Algorithmus stellt die Python Bibliothek 'scikit-learn' eine Implementierung zur Verfügung [15]. Diese kann in den Algorithmus integriert werden. Es muss hierbei der Zugriff auf die Matrix  $D_G$  geändert werden. Für die Implementierung der weiteren Funktionalität wird auf die Python Bibliothek 'NumPy' zurückgegriffen.

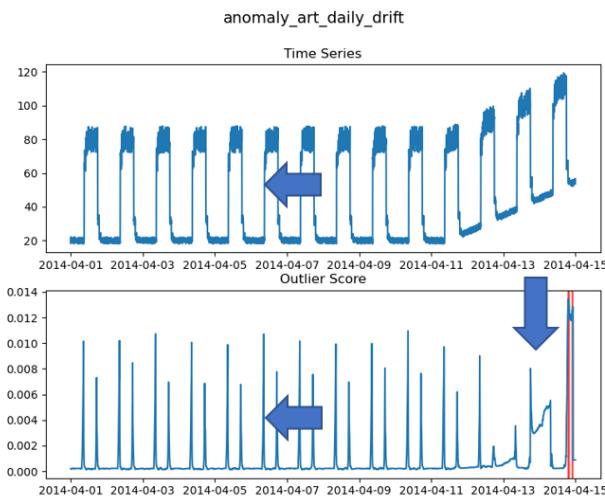
### 3.2.3 Anwendung auf Zeitreihen

| Ausreißer Typ                         | Dateiname                         | 1D |
|---------------------------------------|-----------------------------------|----|
| Einzelne Peaks                        | anomaly-art-daily-peaks           | *  |
| Zunahme an Rauschen                   | anomaly-art-daily-increase-noise  | ** |
| Signal Drift                          | anomaly-art-daily-drift           | ** |
| Kontinuierliche Zunahme der Amplitude | art-daily-amp-rise                | ** |
| Zyklus mit höherer Amplitude          | art-daily-jumpsup                 | *  |
| Zyklus mit geringerer Amplitude       | art-daily-jumpsdown               | ** |
| Zyklus-Aussetzer                      | art-daily-flatmiddle              | *  |
| Signal-Aussetzer                      | art-daily-nojump                  | -  |
| Frequenzänderung                      | anomaly-art-daily-sequence-change | -  |

Tab. 3.1: IsoMap-Performance (vgl. Kap. D)

Für die durchgeföhrten Tests wurden die Zeitreihen aus Kap. 2.1 verwendet. Um zu bewerten, wie gut der Algorithmus funktioniert, wird ein Punktesystem eingeföhrt. In diesem können maximal vier Sterne erreicht werden, die dafür stehen, dass Ausreißer sehr gut erkannt werden. Null Sterne hingegen bedeuten, dass Ausreißer überhaupt nicht erkannt wurden. Der IsoMap-Algorithmus liefert tendenziell schlechte Ergebnisse bei der Erkennung von Ausreißern in Zeitreihen. Das Hauptproblem hierbei ist, dass starke Anstiege, bei welchen es sich nicht um Ausreißer handelt, fälschlicherweise zu einem starken Anstieg des Ausreißer-Scores führen. Dies kann an den markierten Stellen in Abb. 3.2 illustriert werden. Dies kann, je nach Schwellwert, zu einer hohen Quote an *false-positive*-Klassifizierungen führen. Aus diesem Grund können tatsächliche Ausreißer häufig nicht eindeutig identifiziert werden. Eine ähnliche Problematik tritt in [17] bei der Verwendung des Random-Walk-Algorithmus auf.

Das Problem konnte hierbei gelöst werden, indem vor der Anwendung des Algorithmus, eine Glättung der Zeitreihe durchgeführt wird. Dadurch werden abrupte Übergänge in der Zeitreihe abgemildert und deshalb nicht mehr als Ausreißer erkannt [vgl. 17, S. 31-36]. Dies könnte ein möglicher Ansatz sein, um zukünftig bessere Ergebnisse erzielen zu können. Des Weiteren ist zu erkennen, dass der Algorithmus für einige Ausreißertypen nicht geeignet ist. Hierzu gehören Signal-Aussetzer und Frequenzänderungen. Bei diesen Ausreißertypen treten keinerlei unüblichen Werte auf, sondern lediglich Änderungen in der Saisonalität.



**Abb. 3.2:** Problem: Übergänge

### 3.3 Percolation-basierter Algorithmus

Bei diesem Algorithmus werden schrittweise die Kanten mit den höchsten Gewichten, aus dem mit Gl. 3.1 erzeugten Netzwerk, entfernt. Ziel dieses Prozesses ist es, Ausreißer vom restlichen Teil des Netzwerks zu trennen. Die Annahme hierbei ist, dass Ausreißer höhere Kantengewichte zu Nachbarn aufweisen und deshalb schneller separiert werden. Sobald ein Knoten komplett separiert ist, wird diesem ein Ausreißer-Score zugeordnet. Der Wert des Ausreißer-Scores wird über die zuletzt entfernte Kante des Knotens definiert. Dadurch erhalten früher separierte Knoten höhere Ausreißer-Scores als nachfolgende separierte Knoten [vgl. 4, S. 3].



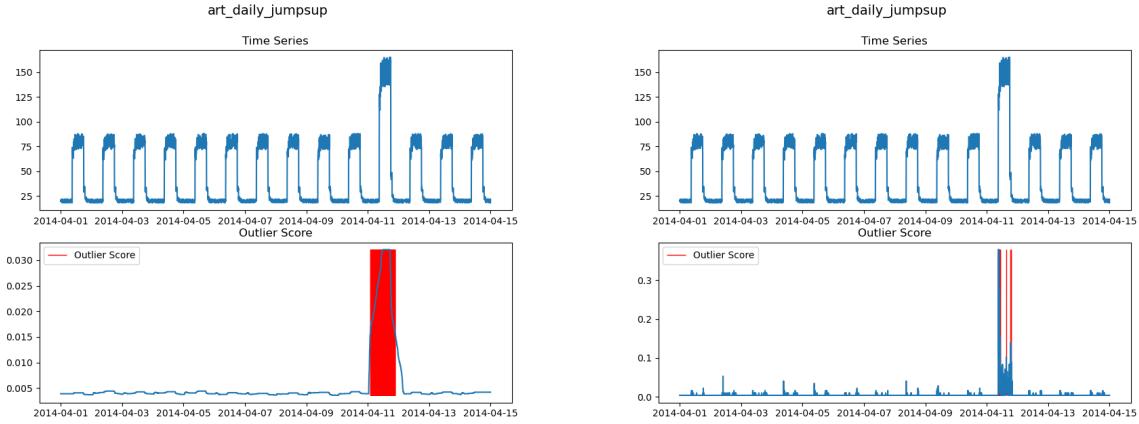
Abb. 3.3: Ablauf Percolation-basierter Algorithmus [4]

#### 3.3.1 Implementierung

Für die Implementierung des Percolation-basierten Algorithmus wurde, wie in Kap. 3.2.2, die Python-Bibliothek 'NumPy' verwendet. Während der Implementierung des Algorithmus, konnte festgestellt werden, dass die Laufzeit des Algorithmus sehr langsam ist. Aus diesem Grund wurden einige Veränderungen an dem Algorithmus vorgenommen, um die Performance zu verbessern. Dazu gehörte, dass nicht einzelne Kanten, sondern Gruppen an Kanten aus dem Netzwerk entfernt werden. Der Vorteil dieser Modifikation ist, dass seltener überprüft werden muss, ob ein Knoten weiterhin mit dem Rest des Netzwerks verbunden ist. Eine weitere Optimierung, die eingeführt wurde, ist die Verankerung eines Abbruchkriteriums. Dabei wird der Algorithmus angehalten sobald, eine bestimmte Menge an Kanten aus dem Netzwerk entfernt wurde. Da der Algorithmus nicht alle Berechnungen ausführen muss, kann damit eine Laufzeitoptimierung erreicht werden. Weiterhin konnte festgestellt werden, dass diese Veränderung keinen Einfluss auf die Qualität der Ausreißererkennung hat, da Ausreißer lediglich zu Beginn des Algorithmus gefunden werden. Ein weiteres Problem des ursprünglichen Algorithmus war, dass bei aufeinanderfolgenden Elementen der Zeitreihe teilweise starke Schwankungen im Ausreißer-Score auftraten (vgl. Abb. 3.4). Aus diesem Grund können Ausreißer, die sich über mehrere Zeitpunkte hinweg erstrecken, nicht vollständig erkannt werden. Um die Schwankungen im Ausreißer-Score abzumildern, wurde dieser geglättet. Dazu wurde die Methode des gleitenden Mittelwert auf den Ausreißer-Score angewandt.[12] In Gl. 3.2 ist eine exemplarische Formel für den gleitenden Mittelwert der Ordnung drei dargestellt.

In Abb. 3.4 ist zu sehen, wie sich der Ausreißer-Score durch das Glätten verändert.

$$m_{\text{MA}}^{(3)}(t) = \frac{1}{3} (x(t-1) + x(t) + x(t+1)) \quad (3.2)$$



**Abb. 3.4:** Vergleich Percolation-Algorithmus mit und ohne gleitendem Mittelwert

Um zu klassifizieren, ob es sich bei einem konkreten Element um einen Ausreißer handelt, wird zunächst der Mittelwert und die Standardabweichung des Ausreißer-Scores berechnet. Falls ein Element um einen bestimmten Schwellwert vom Mittelwert abweicht, wird das Element als Ausreißer klassifiziert.

### 3.3.2 Anwendung auf Zeitreihen

| Ausreißer Typ                         | Datei Name                        | 1D   |
|---------------------------------------|-----------------------------------|------|
| Einzelne Peaks                        | anomaly-art-daily-peaks           | *    |
| Zunahme an Rauschen                   | anomaly-art-daily-increase-noise  | **** |
| Signal Drift                          | anomaly-art-daily-drift           | ***  |
| Kontinuierliche Zunahme der Amplitude | art-daily-amp-rise                | ***  |
| Zyklus mit höherer Amplitude          | art-daily-jumpsup                 | **** |
| Zyklus mit geringerer Amplitude       | art-daily-jumpsdown               | **** |
| Zyklus-Aussetzer                      | art-daily-flatmiddle              | **** |
| Signal-Aussetzer                      | art-daily-nojump                  | -    |
| Frequenzänderung                      | anomaly-art-daily-sequence-change | -    |

**Tab. 3.2:** Performance des Percolation-basierten Algorithmus auf Zeitreihen (vgl. Kap. E)

Es konnte festgestellt werden, dass der Percolation-basierte Algorithmus viele Ausreißertypen sehr gut erkennt. Ob Ausreißer in einer Zeitreihe mit einzelnen Peaks gefunden werden, hängt davon ab, ob der Ausreißer-Score geglättet wird. Eine Identifizierung von einzelnen Peaks ist nur bei ungeglätteten Ausreißer-Scores möglich. Denn durch die Glättung der Zeitreihe verschwinden die Ausschläge im Ausreißer-Score. Es sollte deshalb in Abhängigkeit des Anwendungsfalles entschieden werden, ob der Ausreißer Score geglättet wird. Dabei wäre ebenfalls denkbar, dass beide Varianten zur Erkennung von Ausreißern verwendet werden. Der Percolation-basierte Algorithmus ist, genauso wie der IsoMap-basierte Algorithmus (vgl. Kap. 3.2.3), nicht dazu im Stande Ausreißer in Zeitreihen mit Signal-Aussetzern und Frequenzänderungen zu erkennen.

# 4 Dynamische Algorithmen zur Ausreißererkennung

In diesem Kapitel werden zwei Algorithmen zur dynamischen Erkennung von Ausreißern vorgestellt. Hierbei handelt es sich um den NetSimile- (vgl. Kap. 4.2) und den MIDAS- (vgl. Kap. 4.3) Algorithmus. Dynamische Algorithmen sind, im Gegensatz zu statischen Algorithmen, dazu in der Lage, Ausreißer in Echtzeitdaten zu finden. Dadurch sind diese Algorithmen in der Praxis von hoher Relevanz. Hierbei müssen Ausreißer möglichst schnell erkannt werden, um einen daraus resultierenden möglichen finanziellen Schaden zu verhindern oder zu minimieren. In Abschnitt Kap. 4.1 wird beschrieben, wie verschiedene Datentypen in ein Netzwerk umgewandelt werden können. Dadurch wird gewährleistet, dass die dynamischen Algorithmen auf unterschiedlichen Datentypen, wie z. B. Bilder, Zeitreihen oder Videos, anwendbar sind.

## 4.1 Transformation der Daten

Bevor die dynamischen Algorithmen auf die Zeitreihendaten angewendet werden können, müssen diese in Graphen transformiert werden. Diese Umwandlung erfolgt ähnlich wie bei statischen Algorithmen (vgl. Kap. 3.1). Hierbei werden jeweils schrittweise kleine Abschnitte der Daten in Graphen umgewandelt. Nachfolgend wird dies an einem Beispiel näher veranschaulicht. Ein Temperatursensor liefert jede Sekunde einen Wert. Sobald 100 Werte des Sensors eingegangen sind, erfolgt die Umwandlung dieser Daten in einen Graphen, unter Verwendung von Gl. 3.1. Dieser Vorgang wiederholt sich anschließend immer wieder. Der Wert für die Länge der Abschnitte ist hierbei frei wählbar und kann als Parameter übergeben werden. Insofern die Zeitreihe eine Saisonalität besitzt, bietet es sich an, diese für die Länge der Abschnitte zu verwenden. In einem letzten Schritt werden anschließend die Netzwerkdaten in eine Datei geschrieben. Dieser Schritt ist aufgrund der Art und Weise, wie die Algorithmen implementiert sind, notwendig. In Abb. 4.1 ist graphisch dargestellt, wie die Umwandlung der Daten in ein Netzwerk funktioniert.

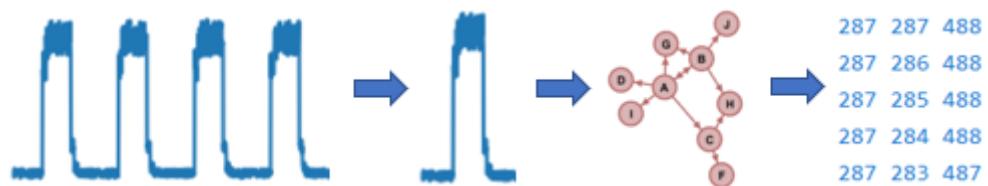


Abb. 4.1: Umwandlung einer Zeitreihe in einen Beispielgraphen.

Die verschiedenen Algorithmen erfordern unterschiedliche Übergabeformate. Aus diesem Grund werden folgend die Besonderheiten beschrieben, auf welche dabei geachtet werden muss.

NetSimile: Das Übergabeformat für den NetSimile-Algorithmus ist in [Abb. 4.1](#) ganz rechts dargestellt. Jede Zeile stellt hierbei eine Kante des Netzwerks dar. Bei der ersten Spalte handelt es sich um den Ursprungsknoten der Kante, bei der zweiten Spalte um den Zielknoten und bei der letzten Spalte um die Gewichtung.

MIDAS: Beim MIDAS Algorithmus ist es nicht möglich die Gewichtung der Kanten direkt an den Algorithmus zu übergeben, dies ist nur indirekt möglich. Dazu wird die gleiche Kante, in Abhängigkeit der Gewichtung, mehrmals an den Algorithmus übergeben. In [Abb. 4.2](#) ist ein kleiner Ausschnitt einer Datei für den MIDAS Algorithmus dargestellt.

MIDAS-R: Die Berechnungen für den MIDAS-R Algorithmus sind, im Verhältnis zum MIDAS Algorithmus, umfangreicher. Insofern für den MIDAS-R Algorithmus die gleichen Daten verwendet werden, wie für den MIDAS Algorithmus, ergibt sich für die Berechnungen eine hohe Laufzeit. Aus diesem Grund wurde eine Hauptkomponentenanalyse durchgeführt, um die Größe der Adjazenzmatrix zu verringern. Es entsteht ein kleineres Netzwerk, welches an den MIDAS-R Algorithmus übergeben werden kann.

```
248 259 7  
248 259 7  
248 259 7  
248 259 7
```

**Abb. 4.2:** Datensatz für MIDAS bestehend aus Ursprungsknoten, Zielknoten und Zeitabschnitt

## 4.2 NetSimile

### 4.2.1 Grundlagen

NetSimile ist ein skalierbarer Algorithmus zur Erkennung von Ähnlichkeiten sowie Anomalien, in Netzwerken unterschiedlicher Größen. Hierfür wird der Datensatz in gleich große Zeitintervalle unterteilt, um die daraus resultierenden Graphen auf unterschiedliche Merkmale zu untersuchen. Diese Merkmale sind strukturelle Eigenschaften der einzelnen Knoten wie bspw. die Dichte eines Knotens oder die Anzahl an Nachbarn in einem Ego-Netzwerk. Die Signatur ergibt sich aus den einzelnen Aggregationen der Knoten wie dem Median aus der Dichte der jeweiligen Knoten. So entsteht aus sieben Merkmalen und fünf Aggregationen ein Signaturvektor mit 35 verschiedenen Signaturen. So ermöglicht dieser Vektor die Beschreibung sowie den Vergleich der einzelnen Graphen. Für den Vergleich wird die Canberra-Distanz aus den Signaturvektoren zweier zeitlich nebeneinander liegenden Graphen berechnet [vgl. 5, S. 1]. Als Input für diesen Algorithmus wird eine Menge von  $k$ -anonymisierten Netzwerken mit beliebig unterschiedlichen Größen, die keine überlappenden Knoten oder Kanten besitzen, herangezogen. Das Resultat sind Werte für die strukturelle Ähnlichkeit oder den Abstand eines jeden Paares der gegebenen Netzwerke bzw. ein Merkmalsvektor für jedes Netzwerk [vgl. 5, S. 1]. NetSimile durchläuft drei Schritte, die im Folgenden beschrieben werden.

#### Extrahierung von Merkmalen

Für jeden Knoten  $i$  werden, basierend auf ihren Ego-Netzwerken, die folgenden Merkmale generiert:

|                      |   |
|----------------------|---|
| $\bar{d}_i =  N(i) $ | Die Anzahl der Nachbarn (d. h. Grad) von Knoten $i$ , wobei $N(i)$ die Nachbarn von Knoten $i$ beschreibt.  |
| $\bar{c}_i$          | Der Clustering-Koeffizient von Knoten $i$ , der als die Anzahl von Dreiecken, die mit Knoten $i$ verbunden sind, über die Anzahl von verbundenen Dreiecken, die auf Knoten $i$ zentriert sind, definiert ist. |
| $d_{N(i)}$           | Die durchschnittliche Anzahl der Nachbarn von Knoten $i$ , die zwei Schritte entfernt sind. Dieser wird berechnet als $\frac{1}{\bar{d}_i} \sum_{j \in N(i)} d_j$   |
| $c_{N(i)}$           | Der durchschnittliche Clustering-Koeffizient von $N(i)$ , der als $\frac{1}{\bar{d}_i} \sum_{j \in N(i)} c_j$ berechnet wird.   |
| $ E_{ego(i)} $       | Die Anzahl der Kanten im Ego-Netzwerk vom Knoten $i$ , wobei $ego(i)$ das Ego-Netzwerk von $i$ zurückgibt.  |
| $ E_{ego(i)}^\circ $ | Die Anzahl der von $ego(i)$ ausgehenden Kanten.   |
| $ N(ego(i)) $        | Die Anzahl von Nachbarn von $ego(i)$ .  |

**Tab. 4.1:** Inhalte des Merkmalsvektors [5]

### Aggregierung von Merkmalen

Im nächsten Schritt wird für jeden Graphen  $G_j$  eine  $K \text{ Knoten} \times \text{Merkmal}$ -Matrix  $F_{G_j}$  zusammengefasst. Diese besteht aus den Merkmalsvektoren aus Schritt 1. Da der Vergleich von  $k$ -ten  $F_{G_j}$  sehr aufwändig ist, wird für jede  $F_{G_j}$  ein Signaturvektor  $\vec{s}_{G_j}$  ausgegeben. Dieser aggregiert den Median, den Mittelwert, die Standardabweichung, die Schiefe sowie die Kurtosis der Merkmale aus der Matrix. [vgl. 5, S. 3]

### Vergleich der Signaturvektoren

Für die Ausreißererkennung werden die letzten drei Graphen anhand der Canberra-Distanz, die als Ähnlichkeitsmaß dient, herangezogen. Steigt die Canberra-Distanz zwischen zwei Graphen oberhalb des Schwellwerts, so wird dies im Algorithmus festgehalten. Falls der darauf folgende Graph ebenfalls oberhalb des Schwellwerts liegt, so wird dieser als Ausreißer definiert. Dadurch wird die Anzahl der Ausreißer reduziert, damit nur diejenigen identifiziert werden, bei denen ein Trend hin zu einem abnormalen Verhalten erkennbar ist. [vgl. 5, S. 3]

Der Algorithmus arbeitet dabei dynamisch, da die Signaturen der Graphen in einzelne Teilberechnungen aufgeteilt und zwischengespeichert werden können, ohne dass eine Neuberechnung notwendig ist. Der Schwellwert wird aus dem Median und dem Mittelwert berechnet, die ebenfalls zwischengespeichert und nach Bedarf um weitere Graphen ergänzt werden können. [vgl. 5, S. 3]

#### 4.2.2 Anwendung auf Netzwerkdaten

Beim ersten Versuch den Algorithmus auf Netzwerkdaten anzuwenden, wurde die nachfolgende Problematik festgestellt.

Der Algorithmus verwendet eine Bibliothek *igraph*, welche Kanten zwischen zwei Knoten nur einmalig hinzufügen kann. Beim Eliminieren der Duplikate wird aber ein Drittel des Datensatzes nicht berücksichtigt, wodurch wertvolle Informationen bei der Ausreißererkennung verloren gehen. Aus diesem Grund wurden die Netzwerkdaten soweit angepasst, dass Mehrfachverbindungen zwischen zwei Knoten aufsummiert und als Gewichtung dieser Kante hinzugefügt werden.

```
1 for i in range(len(e_list)):
2     g.add_edge(e_list[i][0], e_list[i][1], weight=e_list[i][2])
```

**List. 4.1:** Gewichtung als neues Feature

Dadurch kann der Datensatz zum einen vollständig analysiert werden und zum anderen kann dadurch ein weiteres Feature hinzugefügt werden, das durch die fünf verschiedenen Aggregationen den Signaturvektor um diese fünf Werte erweitert.

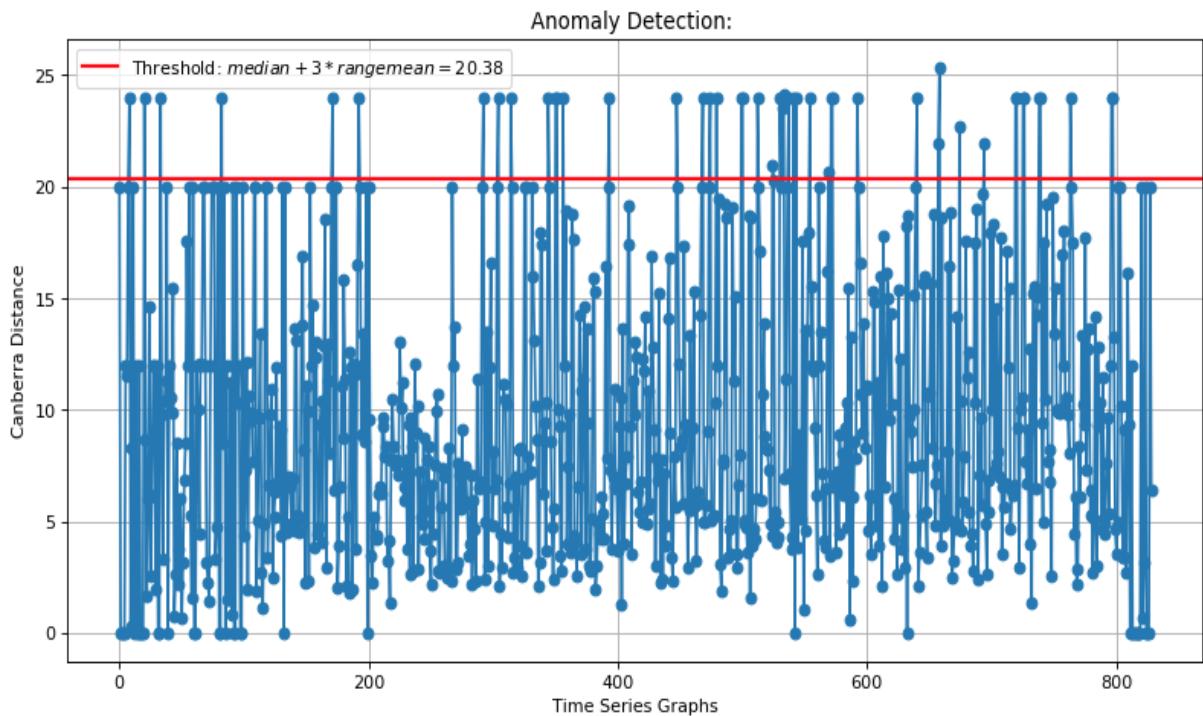
Dadurch, dass der Datensatz zuerst eingelesen und in einen Graphen transformiert wird und anschließend aus dem Graphen die jeweiligen Features extrahiert werden, verliert der Algorithmus an Performanz. Des Weiteren wird im ersten Schritt der maximale Knotenwert als Größe des Graphens übergeben.

Wird bspw. für jeden Mitarbeiter eine eigene ID übergeben und diese inkrementell erhöht, so kann es sein, dass aus einem Netzwerk mit 20 verschiedenen Knoten ein Graph entsteht, der 1000 Knoten erzeugt, weil eine ID mit dem Wert 1000 vorhanden ist. Dadurch büßt die Performanz an Geschwindigkeit ein, da Iterationen nicht über die 20 Knoten durchgeführt werden, sondern über 1000. Hierbei muss entweder der Datensatz vorab angepasst werden, indem die IDs neu vergeben werden oder der Algorithmus muss grundlegend neu aufgebaut werden. Dies wäre grundsätzlich möglich, da der Algorithmus Graphen als Ausreißer zurück gibt und keine Knoten.

Da der Fokus auf der Anwendung von Zeitreihen liegt, werden Optimierungen erst im Abschnitt Kap. 4.2.3 in Betracht gezogen.

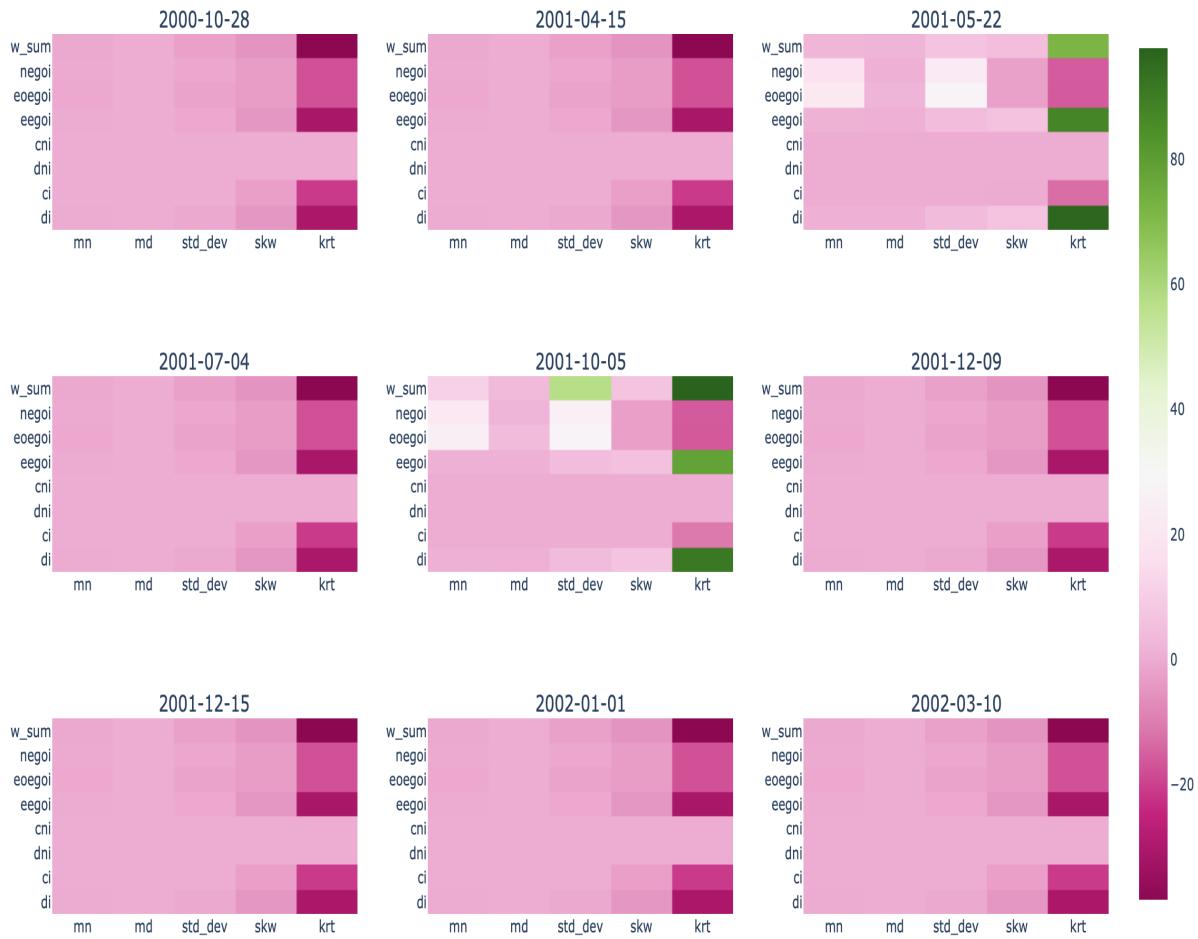
### Anwendung auf ENRON-Datensatz

Da der Enron-Datensatz ebenfalls von einem anderen Paper analysiert und veröffentlicht wurde (vgl. Kap. A), können die dort erkannten Ausreißer, zum Vergleich, in Form eines gelabelten Datensatz herangezogen werden. Betrachtet man in diesem Kontext den Ausreißer-Score, ist gut zu erkennen, dass der Ausreißer Ende 2001 als alleiniger herausstechender Ausreißer ebenso im NetSimile wiederzufinden ist. Grundlegend ist ebenso zu erkennen, dass die Ausreißer sich nur sehr wenig voneinander unterscheiden, wodurch sich eine Klassifizierung innerhalb des Ausreißer-Scores als schwierig erweist. Die Extrahierung weiterer Features könnte dieses Problem lösen, wobei dies nicht im Rahmen dieses Forschungsprojekts behandelt werden soll, da der Fokus auf Zeitreihen liegt. Der Datensatz lässt sich innerhalb von zwei Minuten analysieren, womit der NetSimile-Algorithmus performant zu sein scheint.



**Abb. 4.3:** Ausreißer-Score im Enron-Datensatz mit dem NetSimile-Algorithmus

Betrachtet man die Differenz aus dem Durchschnitt der Signaturvektoren und dem der Ausreißergraphen in einer *Heatmap*, dann ist zu erkennen, dass die Ausreißer vorwiegend von besonders großen Ego-Netzwerken und einer hohen Anzahl an E-Mails verursacht werden. Vergleicht man die Zeitleiste [13] mit den Ausreißerdaten, ist ein starker Anstieg des Email-Verkehrs im Oktober 2001 zu erkennen. Hierbei wurde von Enron ein Report, über einen Quartals-Verlust von 618 Millionen US-Dollar und eine Reduzierung des Eigenkapitals um 1.2 Milliarden, veröffentlicht. Im Dezember 2001 ist ein verhältnismäßig geringer Email-Verkehr festzustellen. Betrachtet man hierbei die Zeitleiste, so wurden in dieser Zeitspanne 4000 Mitarbeiter entlassen. [13]

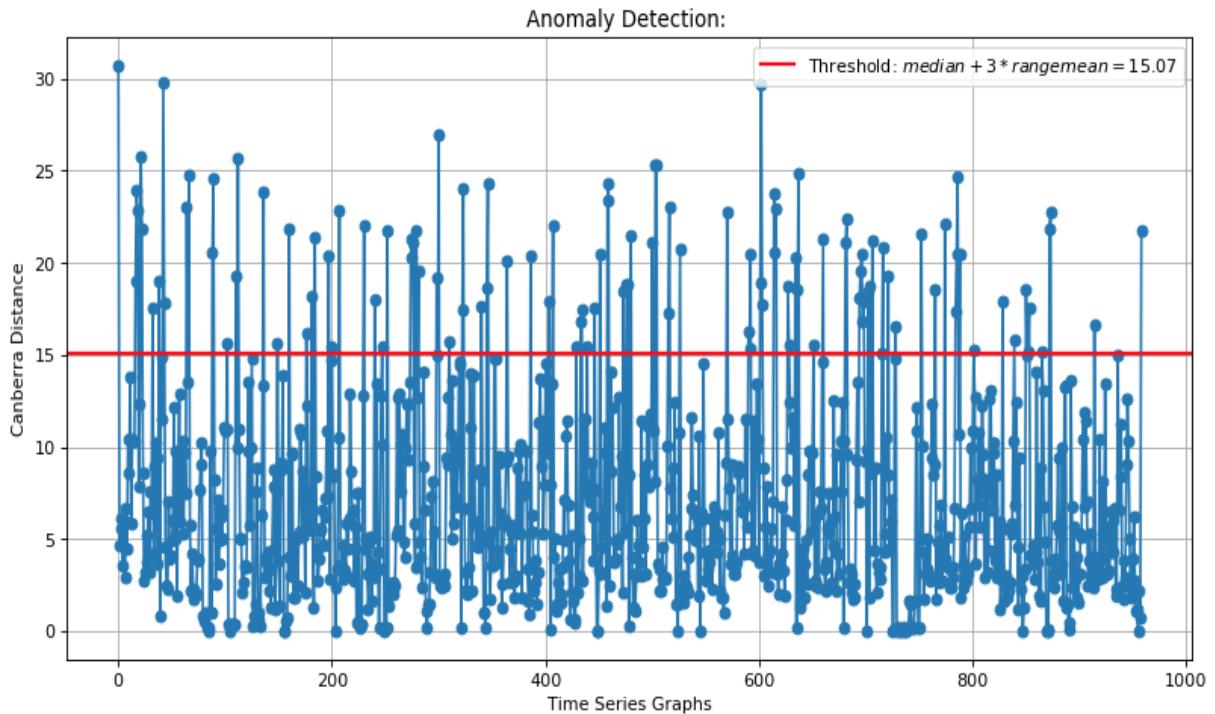


**Abb. 4.4:** Darstellung der Ausreißer in Heatmaps

### Anwendung auf Darpa-Datensatz

Beim Darpa-Datensatz können die Ausreißer besser klassifiziert werden. Die Gründe hierfür liegen an der Größe und Vielfalt des Datensatzes. Der Enron-Datensatz hat eine Größe von 1MB und ca. 50.000 Kanten. Der Darpa-Datensatz hingegen hat eine Größe von 50 MB mit 4.5 Mio Kanten. Für die Berechnung ergibt sich hierbei eine Laufzeit von drei Stunden.

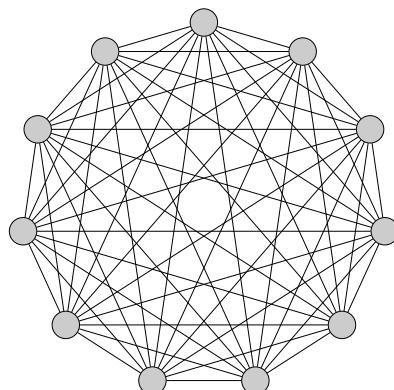
Wird für die Dateigröße der Faktor 50 und bei der Kantenanzahl der Faktor 90 gewählt, so ist bei der Berechnungszeit der Faktor 90 wiederzufinden. Bei Betrachtung der Laufzeit kann eine lineare Abhängigkeit zwischen Kantenanzahl und der benötigten Berechnungszeit festgestellt werden.



**Abb. 4.5:** Ausreißer-Score im Darpa-Datensatz mit dem NetSimile-Algorithmus

#### 4.2.3 Anwendung auf Zeitreihen

Wird der Algorithmus auf Zeitreihen angewandt, tritt folgendes Problem auf. Bei der Transformation der Daten entstehen vollständige Graphen, wodurch die strukturellen Eigenschaften sowie die daraus resultierenden Merkmale identisch werden, wie in Abb. 4.6 deutlich wird.



**Abb. 4.6:** Vollständiger Graph mit 11 Knoten

So hat bspw. das Feature  $|E_{ego(i)}^\circ|$ , in einem vollständigen Graphen, keine Aussagekraft, da jeder Knoten die gleiche Anzahl an Kanten in seinem Ego-Netzwerk aufweist. Wenn vom durchschnittlichen Signaturvektor aller Graphen die einzelnen Signaturvektoren subtrahiert werden, so resultiert dies im Wert 0 in allen Heatmaps.

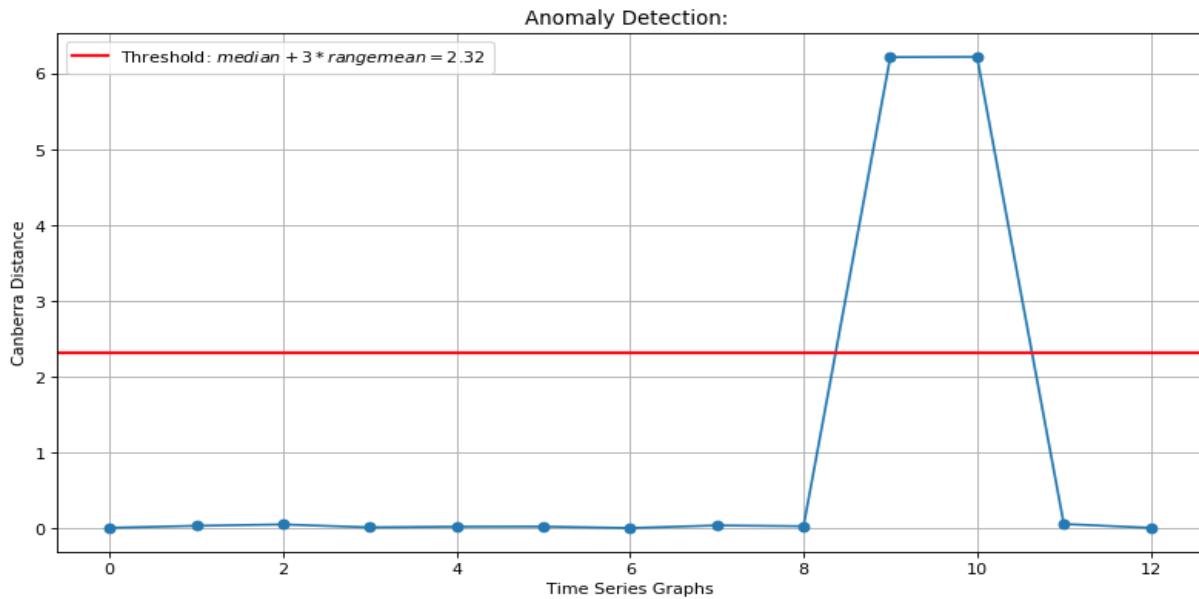
Somit müssen hierbei, für vollständige Graphen, andere Features extrahiert werden. Außerdem ist die Laufzeit in großen Datensätzen, wie z.B. dem Darpa-Datensatz, mit drei Stunden Berechnungszeit nicht performant.

Aus diesem Grund werden aus dem NetSimile lediglich die Ansätze der Merkmals-Extrahierung, die Distanzbildung zweier Signaturvektoren sowie der Schwellwert für die Ausreißeridentifizierung übernommen. Das heißt, die Netzwerke der Zeitreihe werden nicht in ein Graphenobjekt umgewandelt, sondern als Adjazenzmatrix gespeichert. Dadurch können die Features deutlich effizienter berechnet werden. Zudem werden lediglich Merkmale verwendet, die für vollständige Graphen geeignet sind. Dabei werden die nachfolgenden Merkmale neu eingeführt.

|                                   |   |
|-----------------------------------|---|
| $\sum_{i=1}^n x_i$                | Summe der Kantengewichte eines Knoten   |
| $\frac{1}{n} \sum_{i=1}^n x_i$    | Arithmetisches Mittel der Kantengewichte eines Knoten.  |
| $\sqrt[n]{\prod_{i=1}^n x_i}$     | Geometrisches Mittel der Kantengewichte eines Knoten.   |
| $\sqrt[n]{\prod_{x_i \in A} x_i}$ | Geometrisches Mittel der Kanten mit den 10% höchsten Kantengewichten. Die Menge dieser Kanten ist durch die Menge $A$ gegeben, die eine bestimmte Anzahl an Kanten $n =  A $ enthält. |
| $\sqrt[m]{\prod_{x_i \in B} x_i}$ | Geometrisches Mittel der Kanten mit den 20% höchsten Kantengewichten. Die Menge dieser Kanten ist durch die Menge $B$ gegeben, die eine bestimmte Anzahl an Kanten $m =  B $ enthält. |

**Tab. 4.2:** Inhalte des Merkmalsvektors in der modifizierten Variante

Auf diesen Merkmalen wurden anschließend die bisherigen Aggregation durchgeführt. Dadurch konnten erste Ausreißer in der Zeitreihe gefunden werden (vgl. Abb. 4.7).



**Abb. 4.7:** Ausreißer-Score der vollständigen Graphen mit gewichteten Kanten

Um zu untersuchen, wie gut der Algorithmus funktioniert, wurde er auf Zeitreihen getestet. Als Testdaten wurden ein- und zweidimensionale Zeitreihen der Numenta-Gruppe verwendet. Diese Zeitreihen enthalten verschiedene Ausreißertypen, auf denen die Erkennung der Algorithmus getestet wurde. Die Qualität der Ausreißererkennung wurde mithilfe eines Punktesystems bewertet. In diesem können maximal vier Sterne erreicht werden, die dafür stehen, dass Ausreißer sehr gut erkannt werden. Null Sterne hingegen bedeuten, dass Ausreißer überhaupt nicht erkannt wurden. Die Parameter, welche für die Tests gewählt werden mussten, werden in Tab. 4.4 beschrieben.

| Ausreißer Typ                         | Datei Name                        | 1D   | 2D  |
|---------------------------------------|-----------------------------------|------|-----|
| Einzelne Peaks                        | anomaly-art-daily-peaks           | **   | -   |
| Zunahme an Rauschen                   | anomaly-art-daily-increase-noise  | **** | *** |
| Signal Drift                          | anomaly-art-daily-drift           | **   | -   |
| Kontinuierliche Zunahme der Amplitude | art-daily-amp-rise                | **** | *** |
| Zyklus mit höherer Amplitude          | art-daily-jumpsup                 | **** | *   |
| Zyklus mit geringerer Amplitude       | art-daily-jumpsdown               | **** | -   |
| Zyklus-Aussetzer                      | art-daily-flatmiddle              | **** | *** |
| Signal-Aussetzer                      | art-daily-nojump                  | **** | *** |
| Frequenzänderung                      | anomaly-art-daily-sequence-change | **** | *** |

**Tab. 4.3:** NetSimile-Performance auf Zeitreihen (vgl. Kap. B)

**Tab. 4.3** zeigt die Ergebnisse der Tests. Es ist zu erkennen, dass die Qualität der Ausreißererkennung im eindimensionalen Fall sehr gut ist. Lediglich einzelne Peaks können durch den Algorithmus nicht als Ausreißer identifiziert werden. Außerdem wird bei *Signal Drifts* und der kontinuierlichen Zunahme der Amplitude lediglich der Anfang des Ausreißers detektiert. Aus diesem Grund wurde eine Bewertung mit drei Sternen vergeben. Im zweidimensionalen Fall ist die Qualität der Ausreißererkennung etwas durchwachsener. Auffallend ist, dass Zyklen mit höherer und niedriger Amplitude nicht als Ausreißer erkannt werden. Insbesondere ist dies auffällig, da diese Ausreißertypen üblicherweise zuverlässig erkannt werden. Außerdem ist der Algorithmus im zweidimensionalen Fall nicht mehr dazu in der Lage *Signal Drifts* zu erkennen. Andere Ausreißertypen können durch den Algorithmus weiterhin erkannt werden, jedoch oftmals nicht mit der selben Qualität.

| Parameter    | Beschreibung  |
|--------------|---|
| Periodizität | Wie in <a href="#">Kap. 4.1</a> erläutert, muss die Zeitreihe in kleinere Intervalle aufgegliedert werden. Über diesen Parameter wird die Größe der Intervalle gesteuert. Für die Tests wurde der Parameter auf 288 gesetzt, da es sich hierbei um die Saisonalität der Zeitreihen handelt. |
| Abweichung   | Legt fest, ab wann es sich bei einem Abschnitt um einen Ausreißer handelt. Der Parameter wurde für die Tests auf "3" gesetzt. Das bedeutet, wenn der Ausreißer Score um das dreifache der Standardabweichung vom Durchschnitt abweicht, wird der Abschnitt als Ausreißer gekennzeichnet.    |

**Tab. 4.4:** Parameter des NetSimile für die Anwendung auf Zeitreihen

## 4.3 MIDAS

Im Folgenden wird der MIDAS-Algorithmus vorgestellt und die Anwendung auf verschiedenen Datentypen näher erläutert.

### 4.3.1 Grundlagen

MIDAS, Eng. *Microcluster-Based Detector of Anomalies in Edge Streams*, steht für einen Algorithmus, der plötzlich auftretende Ausbrüche von Aktivitäten in einem Netzwerk bzw. Graphen erkennt. Dieses vermehrte Auftreten von Aktivitäten zeigt sich durch viele sich wiederholende Knoten- und Kantenpaare in einem sich zeitlich entwickelnden Graphen, die Mikrocluster bezeichnet werden. Mikrocluster bestehen demnach aus einem vermehrten Vorkommen eines einzigen Quell- und Zielpaares bzw. einer Kante  $(u,v)$ . Dies geschieht in Echtzeit, wobei jede Kante mit konstanter Zeit und konstantem Speicher verarbeitet wird. [vgl. 6, S. 1]

Ursprüngliche Anwendungsfälle für MIDAS sind die Erkennung von Anomalien in Computer-Netzwerken, wie SPAM oder DoS-Angriffe, sowie Anomalien in Kreditkartentransaktionen.

#### Count-Min-Sketch

Damit die relevanten Informationen für den Algorithmus mit einem konstanten Speicher verarbeitet werden, wird Count-Min-Sketch (CMS) genutzt, dass einer Streaming-Datenstruktur mithilfe der Nutzung von Hash-Funktionen entspricht. Count-Min-Sketch zählt somit die Frequenz einer Aktivität in Datenströmen. Diese Datenstruktur hat ebenfalls den Vorteil, dass man zu Beginn keine Kenntnis über die Anzahl an Quell- und Zielpaaren haben muss. [9]

MIDAS verwendet zwei Arten von CMS. Die erste Variante  $s_{uv}$  wird als die Anzahl an Kanten von  $u$  zu  $v$  bis zum aktuellen Zeitpunkt  $t$  definiert. Durch die CMS-Datenstruktur werden alle Zählungen von  $s_{uv}$  approximiert, sodass jederzeit eine angenähere Abfrage  $\hat{s}_{uv}$  erhalten werden kann. Die zweite Variante  $a_{uv}$  wird als die Anzahl an Kanten von  $u$  zu  $v$  im aktuellen Zeitpunkt  $t$  definiert. Dieser CMS ist identisch zu  $s_{uv}$ , wobei bei jedem Übergang zum nächsten Zeitpunkt die Datenstruktur zurückgesetzt wird. Dadurch resultiert aus dem CMS für den aktuellen Zeitpunkt die annähernde Abfrage  $\hat{a}_{uv}$ . [vgl. 6, S. 3]

#### Erkennung von Mikrocluster

Mithilfe der Näherungswerte  $\hat{s}_{uv}$  und  $\hat{a}_{uv}$  ist das Detektieren von Mikroclustern möglich. Hierzu wird der Mittelwert, d. h. die durchschnittliche Rate mit der Kanten erscheinen, betrachtet. Es wird hierbei angenommen, dass dieser für den aktuellen Zeitpunkt (z. B.  $t = 10$ ) äquivalent ist zu dem vor dem aktuellen Zeitpunkt ( $t < 10$ ). Dadurch wird die Annahme vermieden, dass die Daten auf einer bestimmten zugrundeliegenden Verteilung basieren oder Stationarität über die Zeit aufweisen.

Durch die genannte Annahme lassen sich vergangene Kanten in zwei Klassen einteilen. Eine für den aktuellen Zeitpunkt  $t = 10$  und eine für alle vergangenen Zeitpunkte  $t < 10$ .

Hierbei beträgt die Anzahl der Ereignisse zum Zeitpunkt  $t = 10$   $a_{uv}$  und die Anzahl der Kanten in vergangenen Zeitspunkten  $t < 10$  ist  $s_{uv} - a_{uv}$ .

Die Auswertung der Daten kann mithilfe des *chi-squared goodness-of-fit*-Test erfolgen. Hierbei wird die Summe der Klassen  $t = 10$  und  $t < 10$  für  $\frac{(\text{beobachtet} - \text{erwartet})^2}{\text{erwartet}}$  bestimmt. Bei einer Gesamtanzahl von  $s_{uv}$  Kanten ergibt sich, auf Basis eines Mittelwerts, für  $t = 10$  eine erwartete Anzahl von  $\frac{s_{uv}}{t}$  Kanten. Analog hierzu ergibt sich für  $t < 10$  eine erwartete Anzahl an  $\frac{t-1}{t}s_{uv}$  vergangenen Kanten. Daraus ergibt sich für die *chi-squared*-Statistik [vgl. 6, S. 3]:

$$\begin{aligned}
 \chi^2 &= \frac{\left( \text{beobachtet}_{(t=10)} - \text{erwartet}_{(t=10)} \right)^2}{\text{erwartet}_{(t=10)}} \\
 &\quad + \frac{\left( \text{beobachtet}_{(t<10)} - \text{erwartet}_{(t<10)} \right)^2}{\text{erwartet}_{(t<10)}} \\
 &= \frac{\left( a_{uv} - \frac{s_{uv}}{t} \right)^2}{\frac{s_{uv}}{t}} + \frac{\left( (s_{uv} - a_{uv}) - \frac{t-1}{t}s_{uv} \right)^2}{\frac{t-1}{t}s_{uv}} \\
 &= \frac{\left( a_{uv} - \frac{s_{uv}}{t} \right)^2}{\frac{s_{uv}}{t}} + \frac{\left( a_{uv} - \frac{s_{uv}}{t} \right)^2}{\frac{t-1}{t}s_{uv}} \\
 &= \left( a_{uv} - \frac{s_{uv}}{t} \right)^2 \frac{t^2}{s_{uv}(t-1)}
 \end{aligned} \tag{4.1}$$

Die Größen  $a_{uv}$  und  $s_{uv}$  können, mithilfe der CMS-Datenstruktur, approximiert werden. Daraus ergibt sich, unter Verwendung der approximierten Größen  $\hat{a}_{uv}$  und  $\hat{s}_{uv}$ , der folgende Ausreißer-Score [6, S. 4]:

$$score((u,v,t)) = \left( \hat{a}_{uv} - \frac{\hat{s}_{uv}}{t} \right)^2 \frac{t^2}{\hat{s}_{uv}(t-1)} \tag{4.2}$$

Mithilfe des in Gl. 4.2 angegebenen Ausreißer-Score lässt sich eine neue Kante  $(u,v)$  zum Zeitpunkt  $t$  bewerten. Dieser wird in einem binären Entscheidungsverfahren verwendet, um zu bestimmen, ob es sich bei einer neuen Kante um Anomalie handelt oder nicht. Die Wahrscheinlichkeit von *false-positive*-Ergebnissen soll hierbei den Schwellwert  $\epsilon$  nicht übersteigen. CMS-Datenstrukturen besitzen die Eigenschaft, dass die Approximationen  $\hat{a}_{uv}$ , für beliebige  $\epsilon$  und  $\nu$ , folgende Vorschrift mit einer Wahrscheinlichkeit von mindestens  $1 - \frac{\epsilon}{2}$  erfüllen:

$$\hat{a}_{uv} \leq a_{uv} + \nu \cdot N_t \tag{4.3}$$

$N_t$  beschreibt hierbei die Anzahl an Kanten zum Zeitpunkt  $t$ . Eine weitere Eigenschaft der CMS-Datenstrukturen ist, dass diese die tatsächliche Anzahl an Kanten nur überbewerten können:

$$s_{uv} \leq \hat{s}_{uv} \quad (4.4)$$

Der in Gl. 4.2 gegebene Score kann wie folgt angepasst werden:

$$\tilde{a}_{uv} = \hat{a}_{uv} - \nu N_t \quad (4.5)$$

Daraus lässt sich die in Gl. 4.1 gegebene Statistik anpassen:

$$\tilde{\chi}^2 = \left( \tilde{a}_{uv} - \frac{s_{uv}}{t} \right)^2 \frac{t^2}{s_{uv}(t-1)} \quad (4.6)$$

Bei Verwendung der Teststatistik in Gl. 4.6 und eines Schwellenwertes von  $\chi^2_{1-\frac{\epsilon}{2}}(1)$  ergibt sich eine Wahrscheinlichkeit für ein *false-positive*-Ergebnis von höchstens  $\epsilon$ :

$$P \left( \tilde{\chi}^2 > \chi^2_{1-\frac{\epsilon}{2}}(1) \right) < \epsilon \quad (4.7)$$

Der Term  $\chi^2_{1-\frac{\epsilon}{2}}(1)$  beschreibt hierbei das  $1 - \frac{\epsilon}{2}$ -Quantil.

### Die Erweiterung zu MIDAS-R

Bei dem MIDAS-R-Algorithmus handelt es sich um eine Erweiterung des MIDAS-Algorithmus. Das R steht hierbei für den relationalen Ansatz des MIDAS-R Algorithmus. Dabei wird versucht die räumliche oder zeitliche Verknüpfung zwischen Kanten stärker zu berücksichtigen. Es werden hierzu zwei neue Konzepte eingeführt [vgl. 6, S. 4].

**Temporal Relations:** Durch diesen Ansatz soll der Algorithmus mehr zeitliche Flexibilität erhalten. Dabei sollen Kanten aus der jüngsten Vergangenheit auch in einem neuen Zeitabschnitt berücksichtigt werden. Allerdings reduziert um eine bestimmte Gewichtung. Anstatt die CMS-Datenstruktur nach jedem Zeitabschnitt zu reseten, werden die Gewichte hierbei um einen bestimmten Prozentsatz reduziert [vgl. 6, S. 4].

**Spatial Relations:** Hierbei werden zwei neue Merkmale eingeführt, um verschiedene Ausreißertypen identifizieren zu können. Die neuen Merkmale werden hierbei in CMS-Datenstrukturen gespeichert.

Der Algorithmus speichert demzufolge diese drei Merkmale:

$\hat{s}_{uv}$  Anzahl an Kanten zwischen Knoten u und Knoten v. Dieses Feature wird auch vom MIDAS Algorithmus verwendet.

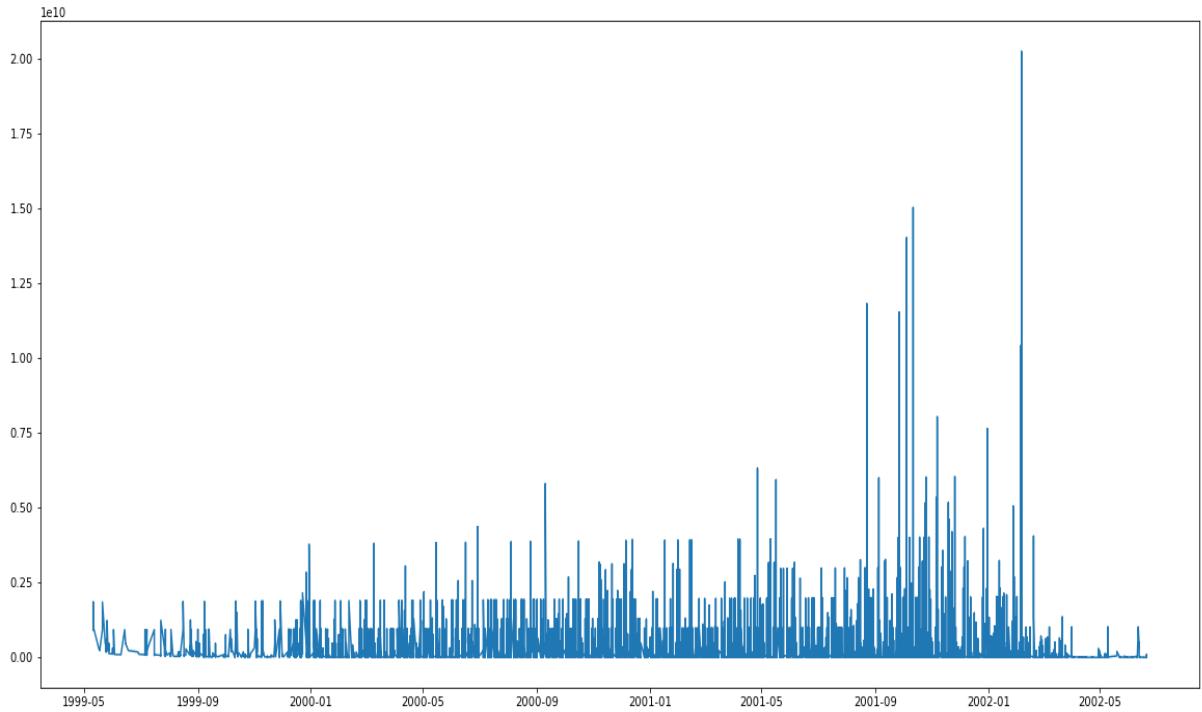
$\hat{s}_u$  Gesamtanzahl an Nachbarknoten eines Knoten u.

$\hat{a}_u$  Aktuelle Anzahl an Nachbarknoten eines Knoten u.

Aus diesen drei Features wird anschließend ein Ausreißer-Score abgeleitet. [vgl. 6, S. 5]

#### 4.3.2 Anwendung auf Netzwerkdaten

Die Anwendung des MIDAS-Algorithmus auf Netzwerkdaten erfolgte problemlos. Es werden lediglich Daten benötigt, die in jeder Zeile aus einem Eingangs-, einem Ausgangsknoten und einem Zeitstempel bestehen. In welcher Form der Zeitstempel bereitgestellt wird, ist hierbei unwichtig. Nachfolgend werden die Ergebnisse mithilfe des MIDAS-Algorithmus auf Netzwerkdaten dargestellt.



**Abb. 4.8:** Ausreißer-Score im Enron-Datensatz mit dem MIDAS-Algorithmus

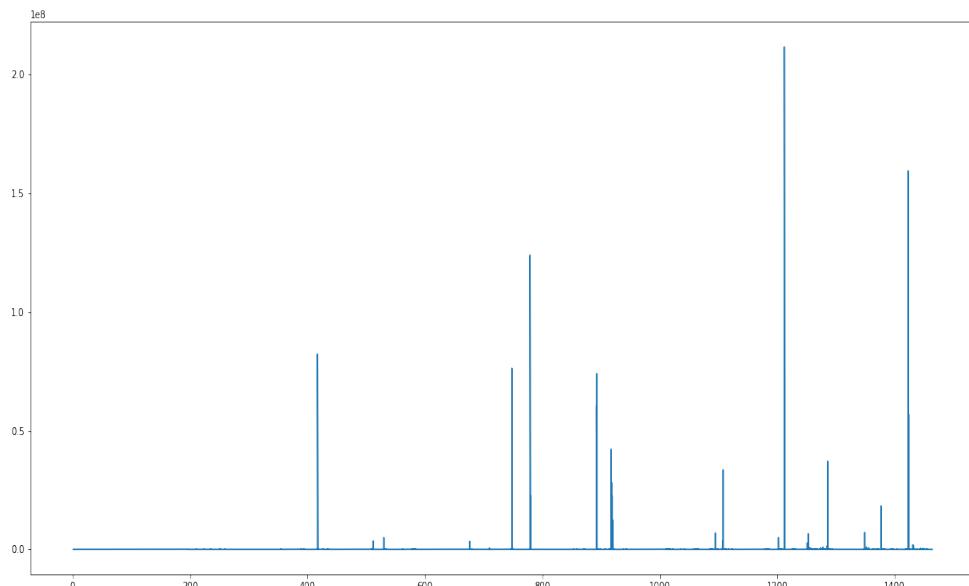
Vergleicht man die Ergebnisse aus Abb. 4.8 mit den Ergebnissen aus Kap. A, so ist zu erkennen, dass beide Algorithmen einen ähnlichen Verlauf vorweisen. Damit eine genauere Aussage getroffen werden kann, werden die MIDAS-Ergebnisse nachfolgend mit der Enron-Zeitleiste abgeglichen. So können mögliche Auswirkungen für die identifizierten Ausreißer deklariert werden. [13]

Die Tab. 4.5 bietet eine Übersicht der historischen Ereignisse, die die Ausreißer des MIDAS-Algorithmus bestätigen. Im Vergleich zu [10] werden mehr Ausreißer erkannt.

|    |  |
|----|--|
| 1. | Aktie erreicht Allzeithoch. Federal Energy Regulatory Commission ordnet Untersuchung an.   |
| 2. | <ul style="list-style-type: none"> <li>• Vierteljährliche Telefonkonferenz zur Finanzsituation und erste Symptome eines Problems.</li> <li>• „Geheimes“ Treffen – Schwarzenegger, Lay, Milken. Angebot zur Rettung der Deregulierung.</li> </ul>                         |
| 3. | <ul style="list-style-type: none"> <li>• Skilling (CEO) kündigt. Mitarbeiterin warnt Lay (Gründer) vor Pleite. Skilling verkauft seine Aktien.</li> <li>• Enron veröffentlicht 618 Mio. \$ Verlust. Interessenskonflikt wird untersucht und Akten vernichtet.</li> </ul> |
| 4. | <ul style="list-style-type: none"> <li>• Beginn der Strafverfolgung. Lay's Rücktritt</li> <li>• Interne Ermittlung verteilt die Schuld auf Führungskräfte und den Vorstand</li> </ul>  |

**Tab. 4.5:** Übersicht über historische Ereignisse, die den Ausreißern zuzuordnen sind

Ein weiterer Test erfolgte mit dem Darpa-Datensatz. [11] In Abb. 4.9 werden die Ausreißer-Scores dargestellt.



**Abb. 4.9:** Ausreißer-Score im Darpa-Datensatz mit dem MIDAS-Algorithmus

Bei der Anwendung des MIDAS auf dem Darpa-Datensatz sieht man klare einzelne Ausreißer, die entdeckt wurden. Für diesen Datensatz gibt es einen speziell für MIDAS entwickelten *ground truth*, der die *labels* für diesen Datensatz zur Verfügung stellt.

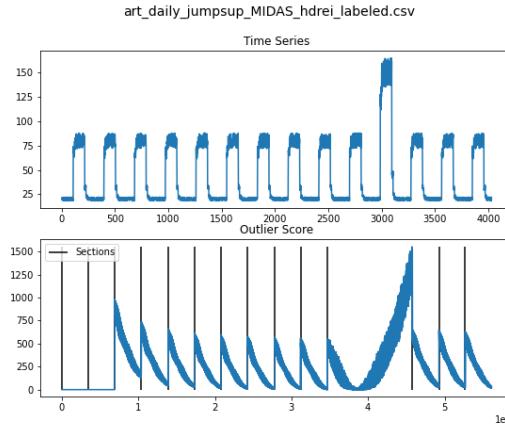
Bei der Berechnung der AUC für die ermittelten Ausreißer-Scores wird ein Wert von 0.91727 berechnet. Das bedeutet, dass der MIDAS-Algorithmus mit einer Wahrscheinlichkeit von ca. 91,73% die Ausreißer des Datensatzes richtig klassifiziert. [vgl. 6, S. 6]

Somit kann festgehalten werden, dass MIDAS hinsichtlich der Ausreißererkennung in Graphen, eine sehr hohe Genauigkeit erreicht.

#### 4.3.3 Anwendung auf Zeitreihen

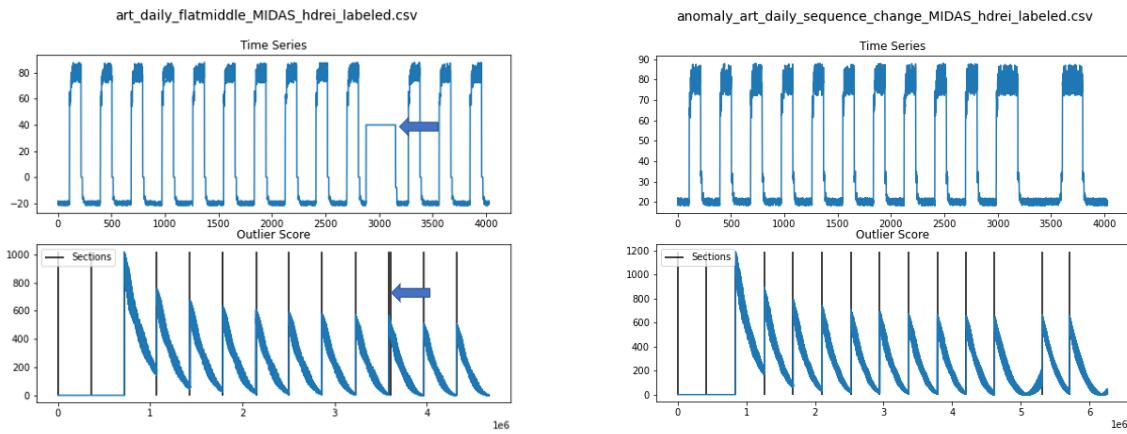
Um den MIDAS-Algorithmus auf Zeitreihen anwenden zu können, muss die Zeitreihe, wie in Kap. 4.1 beschrieben, zunächst in verschiedene Netzwerke umgewandelt werden. Bei den Tests konnte festgestellt werden, dass der MIDAS-Algorithmus nicht dazu in der Lage ist Ausreißer in Zeitreihen zu erkennen. Die vollständigen Ergebnisse der Tests können in Kap. C eingesehen werden. Hierbei ist jedoch der Verlauf des Ausreißer-Scores schwierig zu interpretieren. Es ist zu erkennen, dass der Ausreißer-Score zu Beginn eines jeden Abschnitts sehr hoch und am Ende des Abschnitts hingegen relativ niedrig ist. Grund hierfür ist, dass die Anzahl an Kanten zu Beginn eines Abschnitts, im Verhältnis zu der Anzahl an Kanten aus den vorangegangenen Abschnitten, deutlich niedriger ist. Im weiteren Verlauf werden weitere Kanten innerhalb des Abschnitts hinzugefügt. Dadurch gleicht sich die Anzahl an Kanten innerhalb der Abschnitte an und der Ausreißer-Score sinkt.

Der MIDAS-Algorithmus ist lediglich bei einer Zeitreihe dazu in der Lage den Ausreißer zu identifizieren. Hierbei handelt es sich um die Zeitreihe mit erhöhter Amplitude (vgl. Abb. 4.10). Durch den Ausschlag nach oben in der Zeitreihe entsteht ein Netzwerk mit sehr hohen Gewichten. Die hohen Gewichte führen zu einer erhöhten Anzahl an Kanten, das schlussendlich zu einem Ausschlag des Ausreißer Scores führt. Die erhöhte Anzahl an Kanten führt ebenfalls dazu, dass der Abschnitt mit dem Ausreißer in der Abbildung deutlich breiter ist als die anderen. Bei anderen Ausreißertypen sind die Differenzen zwischen den verschiedenen Elementen der Zeitreihe nicht so groß. Dadurch ergeben sich keinerlei hohe Kantengewichte und der Ausreißer kann nicht erkannt werden.



**Abb. 4.10:** MIDAS-Algorithmus angewandt auf eine Zeitreihe mit einer erhöhten Amplitude

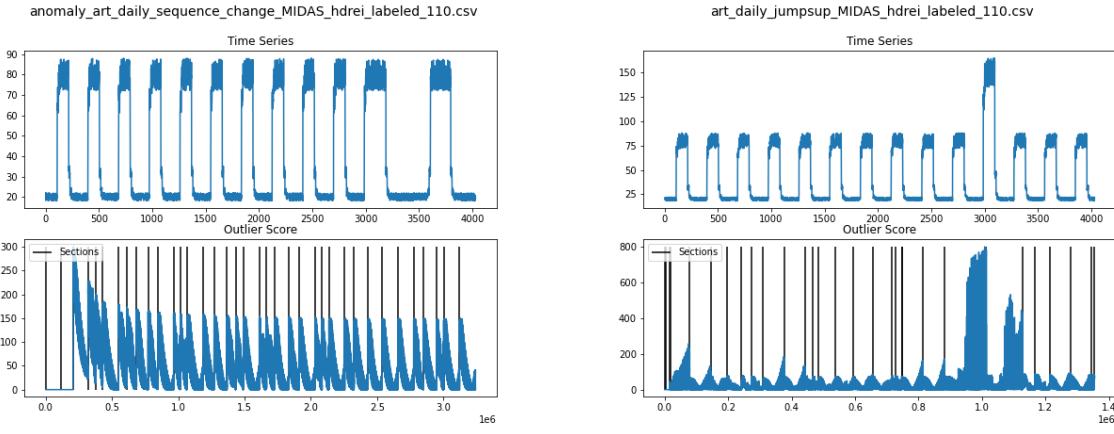
Teilweise führen die Ausreißer ebenso zu besonders wenigen Kanten (vgl. Abb. 4.11a). Bei diesem Ausreißertyp sind alle Werte auf der selben Ebene. Dadurch gehen die Kantengewichte gegen Null. Dies führt zu einem sehr kurzen Abschnitt in Abb. 4.10, der mit einem Pfeil markiert wurde. Des Weiteren ergibt sich eine leicht veränderte Anzahl an Kanten in dem Abschnitt mit Ausreißern (vgl. Abb. 4.11b). Die Abweichungen sind jedoch so gering, dass es zu keinem starken Anstieg des Ausreißer-Score kommt.



**Abb. 4.11:** Ausreißererkennung in Zeitreihen mit MIDAS-Algorithmus

Es wurden außerdem Tests durchgeführt um zu untersuchen, wie sich der Algorithmus bei veränderter Fenstergröße verhält (vgl. Abb. 4.12). Bei den Untersuchungen in Abb. 4.10 und Abb. 4.11 wurde einer Fenstergröße von 288 genutzt, die der Saisonalität der Zeitreihe entspricht. Für dieses Experiment wurde eine Fenstergröße von 110 verwendet. Es konnte festgestellt werden, dass diese Veränderung keinen zusätzlichen Nutzen erbringt.

Allerdings ist der Ausschlag nach oben im Ausreißer-Score für die Zeitreihe mit erhöhter Amplitude noch deutlicher zu erkennen. Die anderen Ausreißertypen werden weiterhin nicht erkannt.

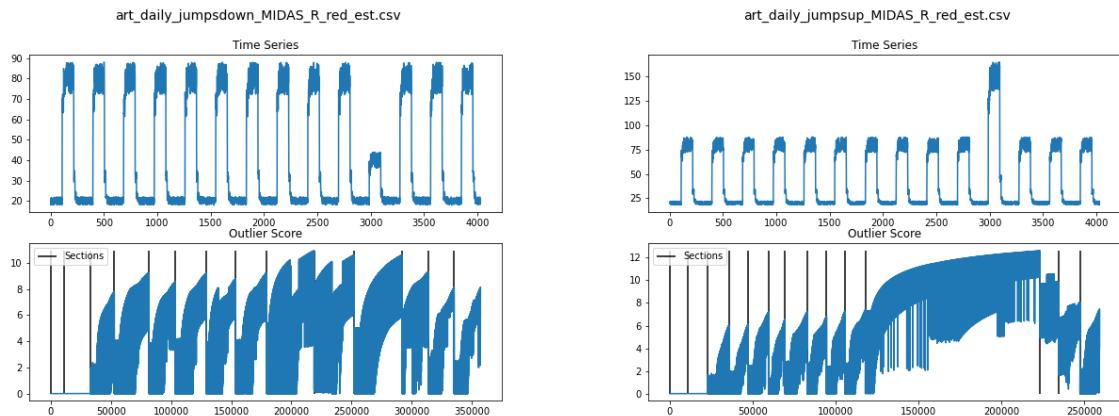


(a) Zeitreihe mit einer Frequenzänderung

(b) Zeitreihe mit erhöhter Amplitude

**Abb. 4.12:** Ausreißererkennung in Zeitreihen mit MIDAS-Algorithmus und Fenstergröße 110

In einem nächsten Schritt wurde untersucht, inwiefern der MIDAS-R-Algorithmus zu einer Verbesserung bei der Ausreißererkennung beitragen kann (vgl. Abb. 4.13). Der MIDAS-R-Algorithmus berücksichtigt, bei der Berechnung des Ausreißer-Scores, für den aktuellen Abschnitt, ebenso die Daten aus den vorherigen Abschnitten. Aus diesem Grund wurde angenommen, dass durch den Einsatz des MIDAS-R-Algorithmus die Ausschläge zu Beginn eines jeden Abschnitts ausbleiben, sodass Ausreißer deutlicher hervortreten. Es konnte festgestellt werden, dass der Ausschlag des Ausreißer-Scores, zu Beginn der Abschnitte, deutlich kleiner ist. Jedoch steigt der Ausreißer-Score zum Ende eines jeden Abschnitts wieder an. Es konnte somit keine signifikante Verbesserung bei der Erkennung von Ausreißern erreicht werden. Insbesondere, da der MIDAS-R-Algorithmus ebenso nur den Ausreißer in der Zeitreihe mit erhöhter Amplitude anzeigt. Somit wurde deutlich, dass die durch den MIDAS-R-Algorithmus eingeführten Merkmale, zu keiner Verbesserung der Ergebnisse geführt haben.



(a) Zeitreihe mit geringerer Amplitude

(b) Zeitreihe mit erhöhter Amplitude

**Abb. 4.13:** Ausreißererkennung in Zeitreihen mit MIDAS-R-Algorithmus

## 5 Vergleich der graphen-basierten Algorithmen

Die empirische Anwendung der graphen-basierten Algorithmen auf Zeitreihendaten erfolgt, sowohl mit statischen als auch mit dynamischen Algorithmen. Im Rahmen des Forschungsprojekts wurde der Fokus auf vier verschiedene Algorithmen gelegt, die das Potential zur erfolgreichen Erkennung von Ausreißern in Zeitreihen hatten. Diese werden nachfolgend verglichen und die Erkenntnisse des Forschungsprojekts aus [Kap. 3](#), sowie [Kap. 4](#) festgehalten. Durch den Vergleich soll ermittelt werden, wie erfolgreich ein Algorithmus bei der Erkennung von Ausreißern in Daten ist.

|                         | Statisch | Dynamisch | Qualität<br>Ausreißer-<br>erkennung<br>Netzwerke | Qualität<br>Ausreißer-<br>erkennung<br>Zeitreihen | Performanz |
|-------------------------|----------|-----------|--|---|------------|
| IsoMap-basiert          | +        | -         | -  | o   | +          |
| Percolation-<br>basiert | +        | -         | -  | +   | +          |
| NetSimile               | -        | +         | +  | ++  | +          |
| MIDAS                   | -        | +         | ++   | -   | o          |

**Tab. 5.1:** Vergleich der Algorithmen

In der [Tab. 5.1](#) sind die Kriterien zu entnehmen, die zum Vergleich der Algorithmen herangezogen wurden. So werden alle Algorithmen zunächst einmal in statisch und dynamisch, entsprechend der Taxonomie des Forschungsprojekts, unterteilt. (vgl. [Kap. 1.2](#)) Im nächsten Schritt werden die Ergebnisse aller Algorithmen hinsichtlich ihrer Fähigkeit gegenübergestellt, Ausreißer in Graphen und Zeitreihen qualitativ zu erkennen. Zuletzt liegt der Fokus auf ihrer Performance im Vergleich zu den anderen Algorithmen. Im Folgenden werden die Ergebnisse ausgeführt.

Der IsoMap-basierte und der Percolation-basierte Algorithmus sind statische Algorithmen, die jeweils nur auf einem Graphen angewendet werden können. (vgl. [Kap. 3](#)) Aus diesem Grund eignen sich diese nicht für die Ausreißererkennung in Netzwerken, da hierbei mehrere Graphen übergeben werden. Beide können jedoch erfolgreich auf Zeitreihen angewendet werden, wobei beim IsoMap-basierten Algorithmus die Ausreißer nur teilweise erkennbar sind, da sich die Ausreißer nur geringfügig von den anderen Werten unterscheiden. (vgl. [Tab. 3.1](#)) Der Percolation-based Algorithmus hingegen zeigt eindeutige Ausreißer, weshalb dieser Algorithmus geeignet für eine qualitative Ausreißererkennung ist. (vgl. [Tab. 3.2](#))

Bei den Ausreißertypen "Signal-Aussetzer" und "Frequenzänderung" können beide Algorithmen keine Ausreißer identifizieren. Die Performance beider Algorithmen ist gut, da sie die Berechnungen innerhalb weniger Sekunden durchführen.

Der NetSimile- und der MIDAS-Algorithmus können beide auf Netzwerkdatensätzen angewandt werden, da sie dynamisch sind. (vgl. Kap. 4) Der Unterschied hierbei liegt bei dem Ausreißer-Score. Beim NetSimile sind die erkannten Ausreißer nahezu identisch, wodurch eine Klassifizierung unzureichend ist. Beim MIDAS hingegen sind die Ausschläge weitaus größer, wodurch eine Klassifizierung erzielt wird. Bei der Anwendung auf Zeitreihen liefert der NetSimile sehr gute Ergebnisse auf den Ausreißertypen, die verwendet wurden (vgl. Kap. 4.2.3). Da sich bei der Transformation von Zeitreihen zu Graphen die Gewichtung nur geringfügig unterscheidet und der MIDAS-Algorithmus Ausreißer nur bei einer hohen Kantengewichtung erkennt, fallen die Ergebnisse hierbei schlechter aus (vgl. Kap. 4.3.3). Dementsprechend ist MIDAS für die Erkennung von Ausreißern in Zeitreihen eher ungeeignet. Bei der Performanz benötigte der NetSimile-Algorithmus ursprünglich bis zu einer Stunde, da dieser rechenintensive Bibliotheken verwendete. Durch die Verwendung anderer Bibliotheken wurde eine Optimierung erreicht. Die Visualisierung des Graphens ist hierdurch zwar nicht mehr möglich, jedoch wird die Rechenzeit auf wenige Sekunden reduziert. Der MIDAS benötigt hingegen mehrere Minuten, wodurch der NetSimile nach der Optimierung performanter geworden ist.

# 6 Fazit und Ausblick

## 6.1 Fazit

Die Erkenntnisse und Ergebnisse des Forschungsprojekts zeigen deutlich, dass graphen-basierte Algorithmen erfolgreich auf Zeitreihendaten angewandt werden können. Im Speziellen erkennen dynamische Algorithmen verschiedenste Ausreißertypen mit einer hohen Qualität. Zudem berücksichtigen diese graphen-basierten Algorithmen den Faktor Zeit, der essentiell für diesen Datentyp ist. Inbesondere der NetSimile-Algorithmus erfüllte, nach Optimierung, die Anforderungen des Forschungsprojekts. Dieser Algorithmus ist dynamisch, multidimensional, performant und die Erkennung von Ausreißern in Zeitreihen erfolgt mit einer hohen Genauigkeit. Der Schwerpunkt hierbei liegt bei der Wahl der richtigen Features. Strukturelle Merkmale sind bei vollständig verknüpften Graphen eher ungeeignet und sollten ersetzt werden durch Features wie bspw. die Gewichtung der Kanten.

## 6.2 Ausblick

Im Rahmen des Forschungsprojekts wurden drei Thematiken behandelt. Zunächst einmal wurde eine Möglichkeit ermittelt Zeitreihendaten in einen Graphen umzuwandeln. In einem weiteren Schritt wurden graphen-basierte Algorithmen auf die transformierten Zeitreihendaten angewandt. Im Anschluss wurden diese Algorithmen hinsichtlich ihrer Eignung zur Ausreißererkenntnung verglichen.

Durch die erfolgreiche Transformation von Zeitreihendaten in Graphen kann der Vorgang ebenso für andere Datenkategorien herangezogen werden, unter der Prämisse, dass Distanzen zwischen den einzelnen Elementen des Datensatzes gebildet werden können. So ist es im nächsten Schritt möglich bspw. Ausreißer in Finanzdaten oder Bilddaten zu erkennen. [vgl. 4, S. 4]

Der NetSimile-Algorithmus kann durch neue Merkmale ergänzt werden. So ist es zukünftig möglich, neben den mathematischen Merkmalen, ebenso statistische Algorithmen als Feature einzusetzen. Dadurch ergibt sich eine erweiterte und optimierte Möglichkeit um Aussagen hinsichtlich Ausreißern treffen zu können. Eine heutige Problematik des NetSimile ist zum einen die, dass er nur den Ausreißer-Graphen zurückgibt und zum anderen wird der Graph erst dann berechnet, wenn dieser alle Kanten eines Zeitintervalls beinhaltet. Hierbei können weitere Optimierungen folgen, die bspw. den Ausreißer-Graphen auf Knoten oder Kanten untersucht, die für den Ausreißer-Score am relevantesten sind. Zudem kann eine Methode ermittelt werden, die einen Graphen iterativ vergrößert, damit eventuell schon vor dem vollständigen Berechnen des Graphs bestimmt werden kann, ob es sich um einen Ausreißer handelt. Zuletzt kann der NetSimile so erweitert werden, dass er in Echtzeit Ausreißer, bspw. im IoT- oder Industrie 4.0-Umfeld, entdeckt.

## A Gelabelter Enron-Datensatz

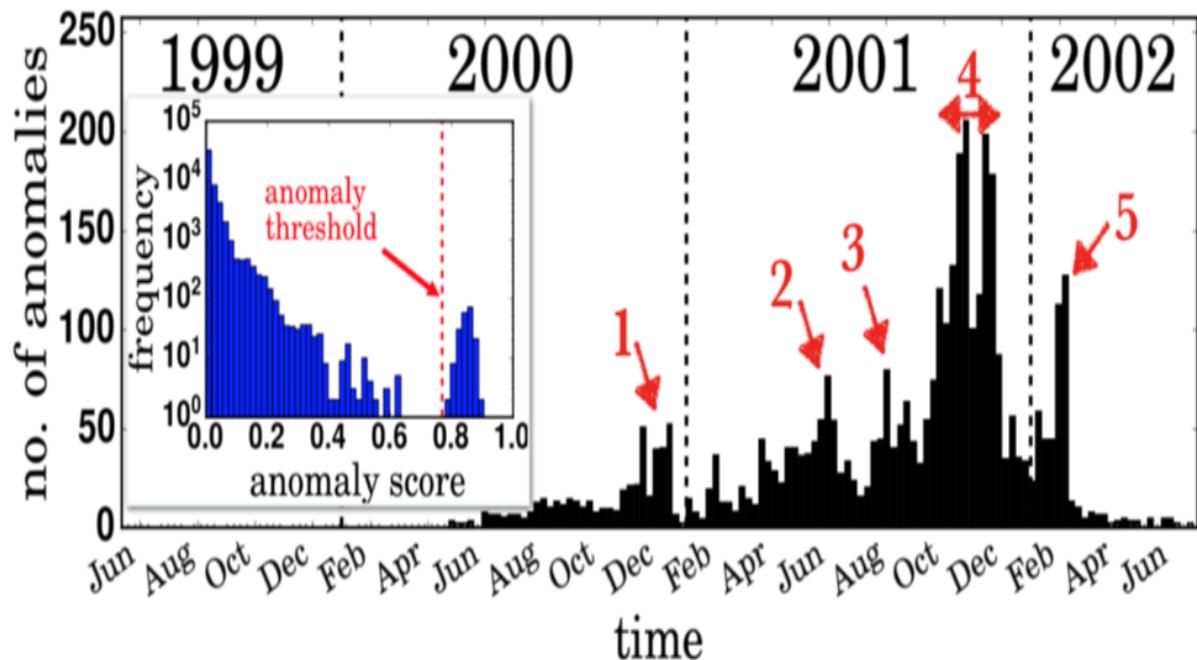
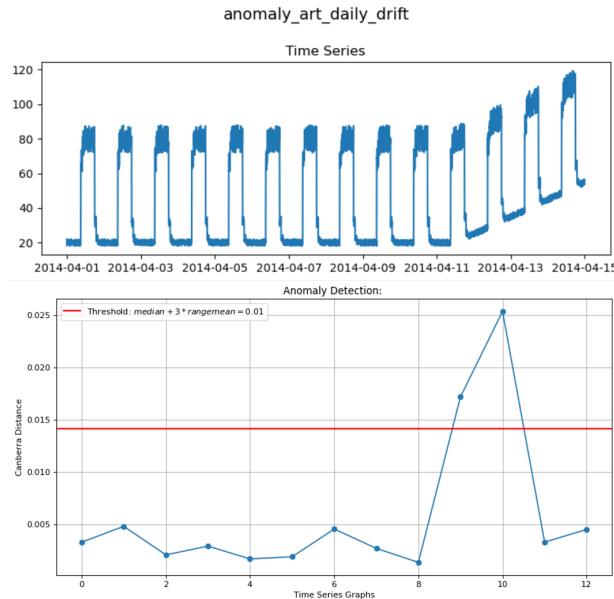


Abb. A.1: Erkannte Ausreißer des SedanSpot-Algorithmus [10]

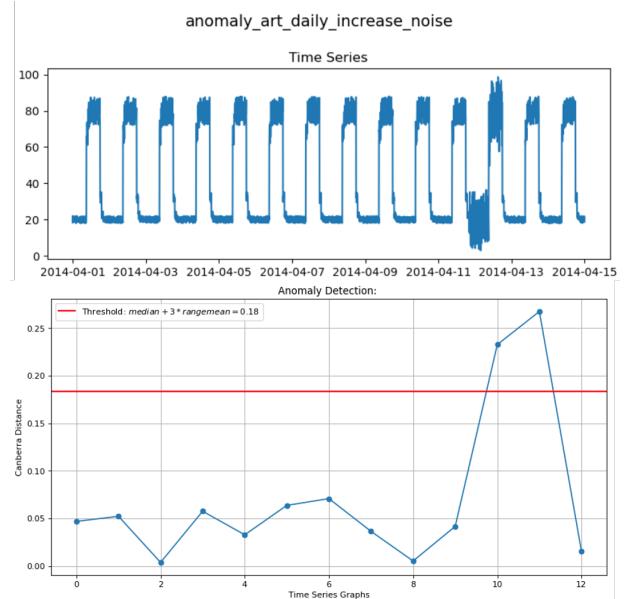


## B NetSimile

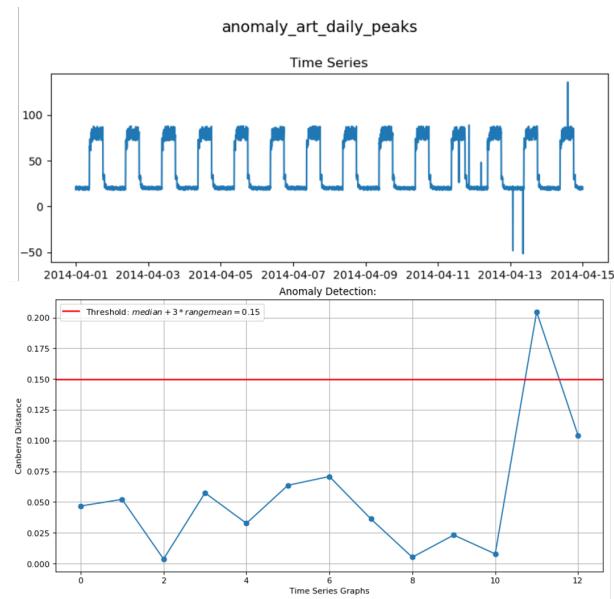
### Eindimensionales Signal



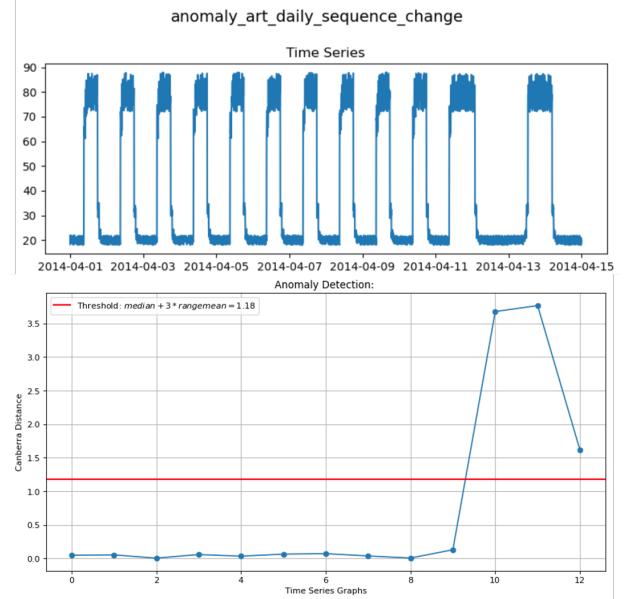
(a) Ausreißertyp Signal Drift



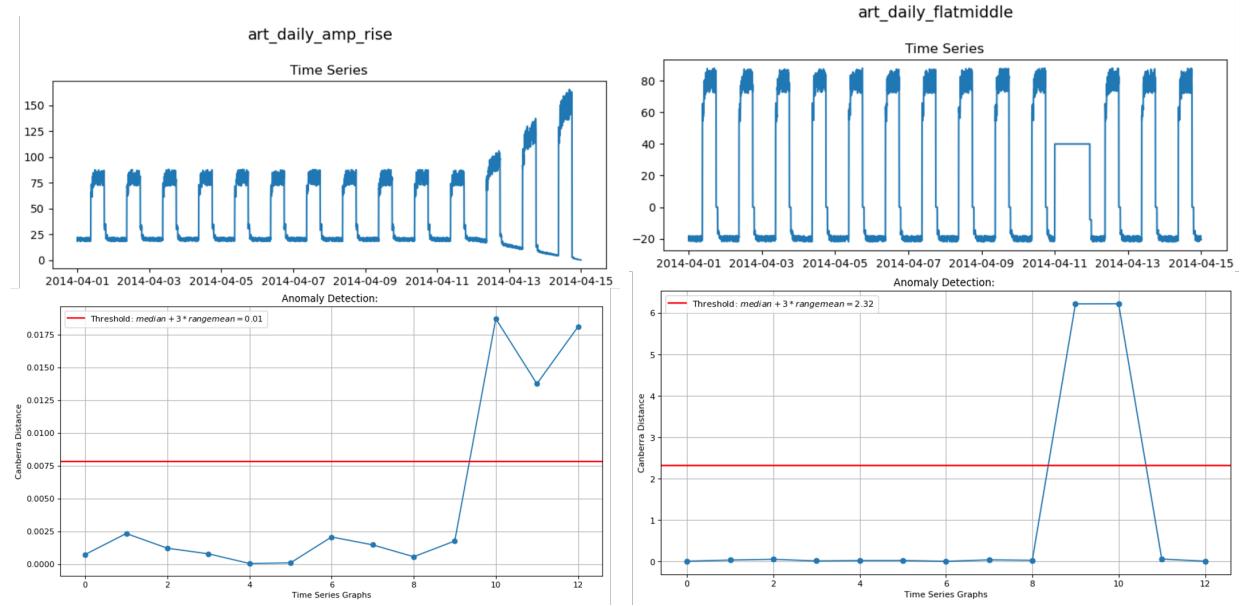
(b) Ausreißertyp Zunahme am Rauschen



(c) Ausreißertyp Einzelne Peaks

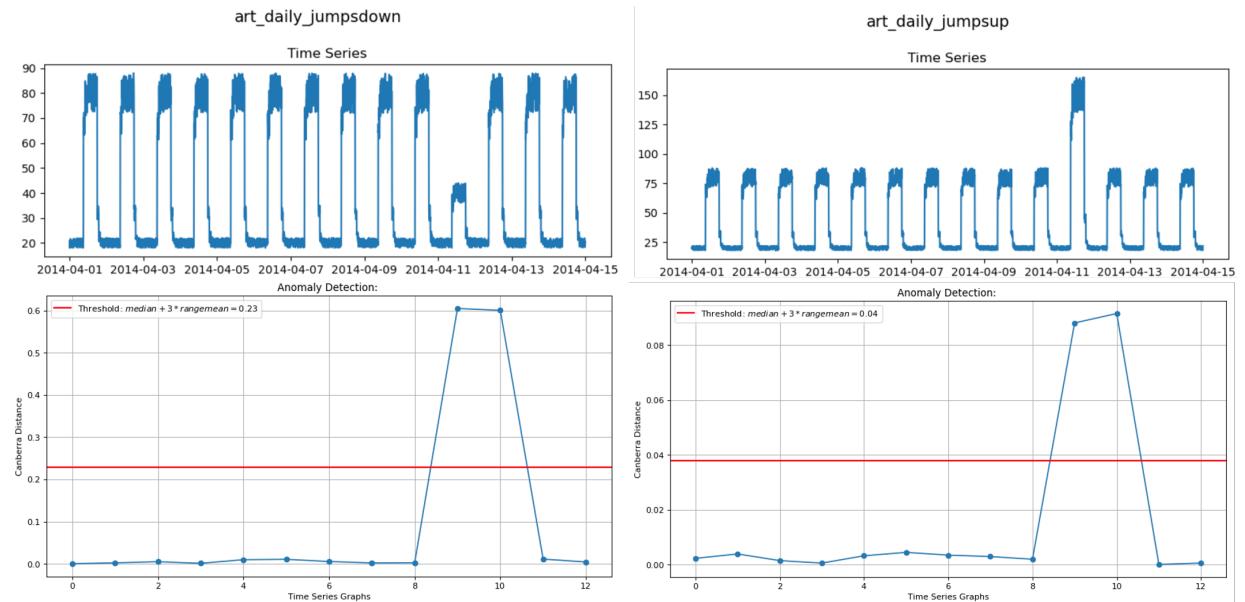


(d) Ausreißertyp Frequenzänderung



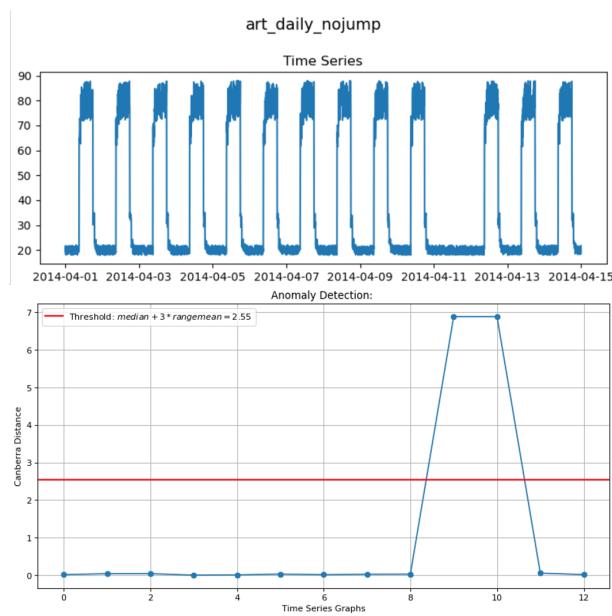
(e) Ausreißertyp Kontinuierliche Zunahme der Amplitude

(f) Ausreißertyp Zyklus Aussetzer



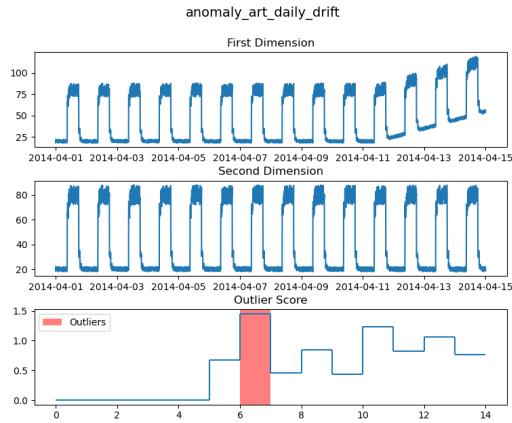
(g) Ausreißertyp Zyklus mit geringerer Amplitude

(h) Ausreißertyp Zyklus mit höherer Amplitude

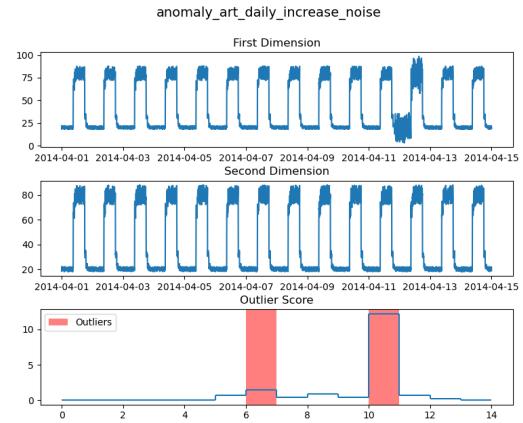


(i) Ausreißertyp Signal-Aussetzer

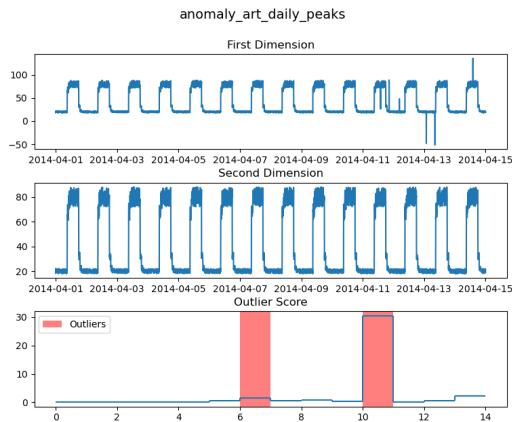
## Zweidimensionales Signal



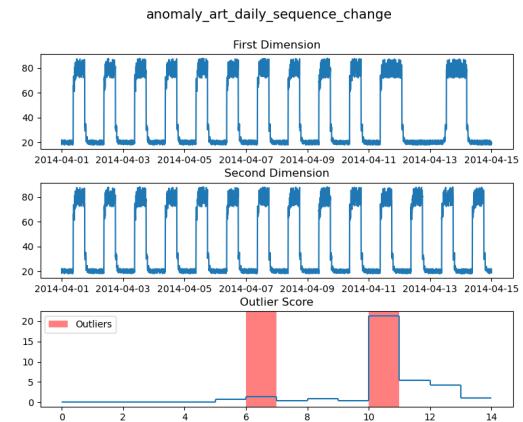
(a) Ausreißertyp Signal Drift



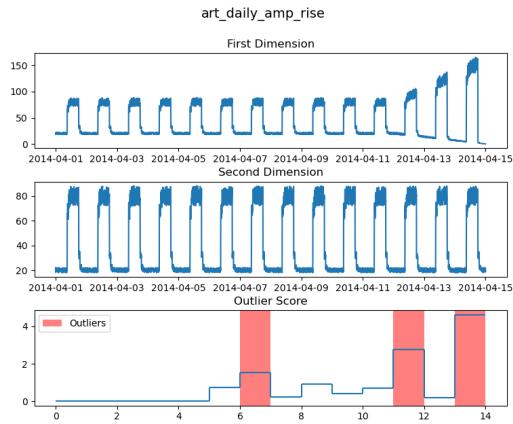
(b) Ausreißertyp Zunahme an Rauschen



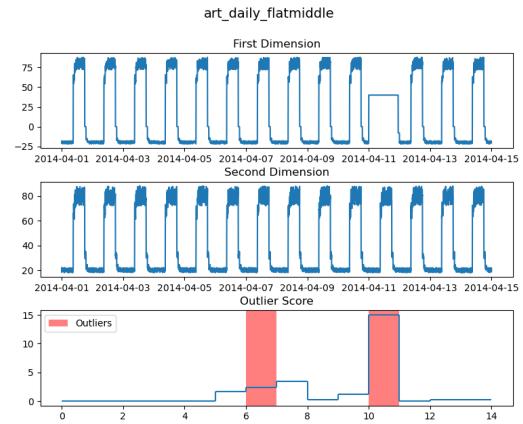
(c) Ausreißertyp Einzelne Peaks



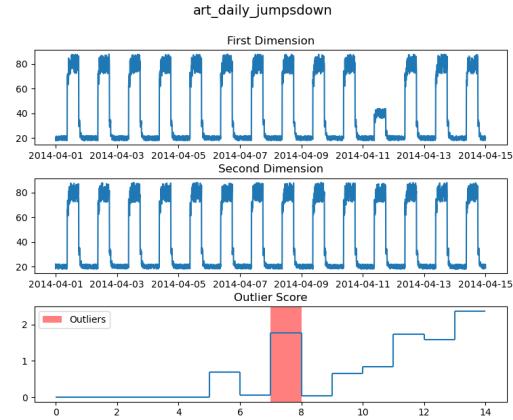
(d) Ausreißertyp Frequenzänderung



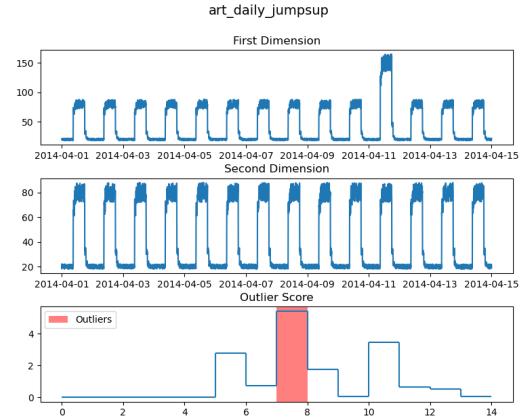
(e) Ausreißertyp Kontinuierliche Zunahme der Amplitude



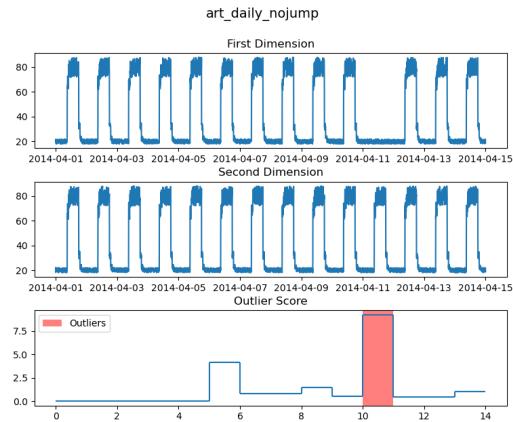
(f) Ausreißertyp Zyklus-Aussetzer



(g) Ausreißertyp Zyklus mit geringerer Amplitude

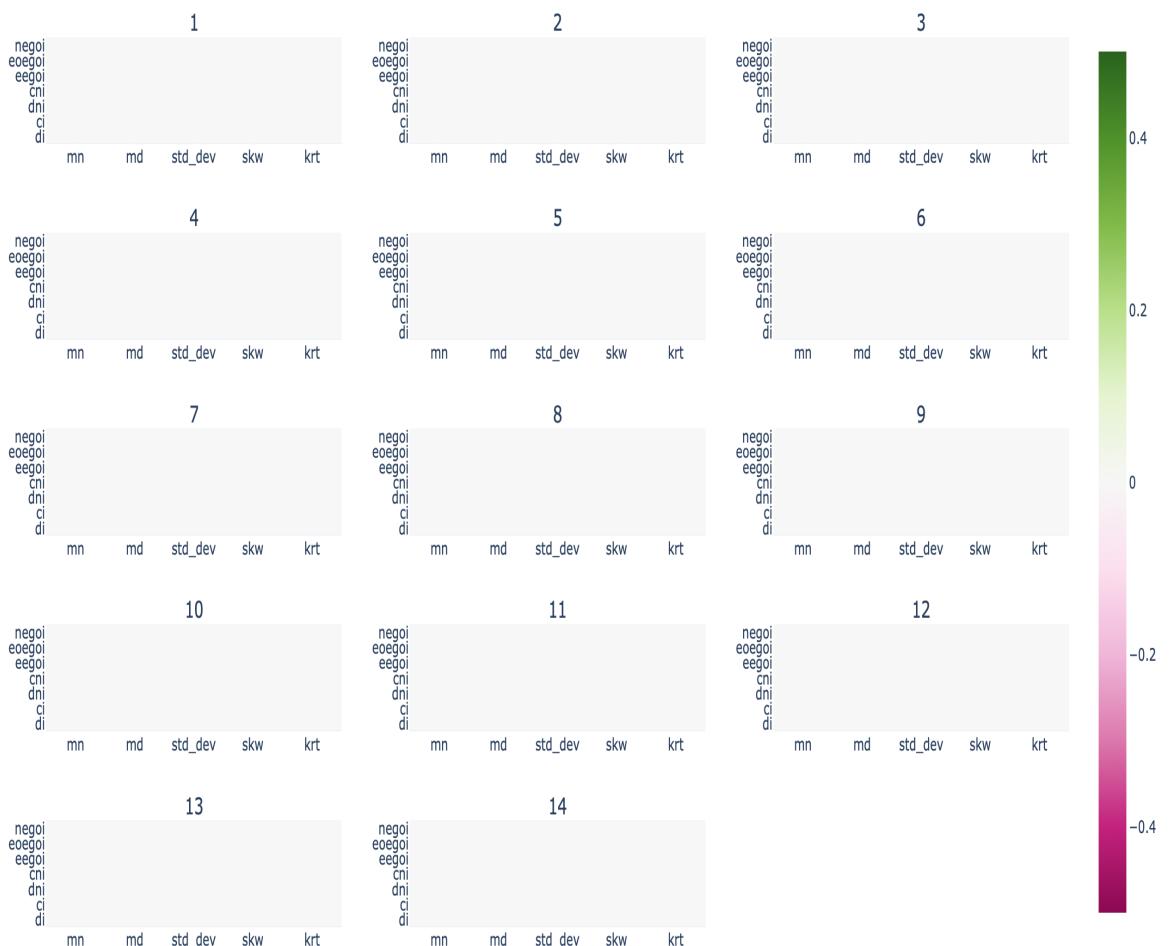


(h) Ausreißertyp Zyklus mit höherer Amplitude

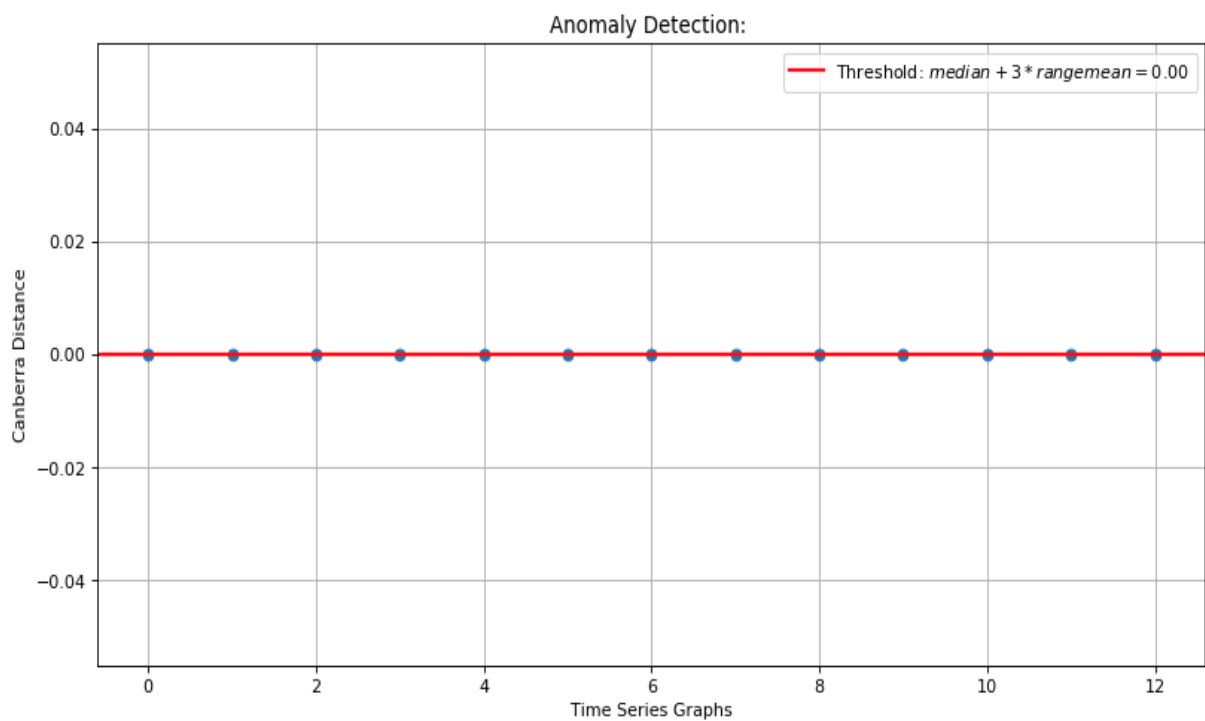


(i) Ausreißertyp Signal-Aussetzer

## Ergebnisse vollständiger Graphen



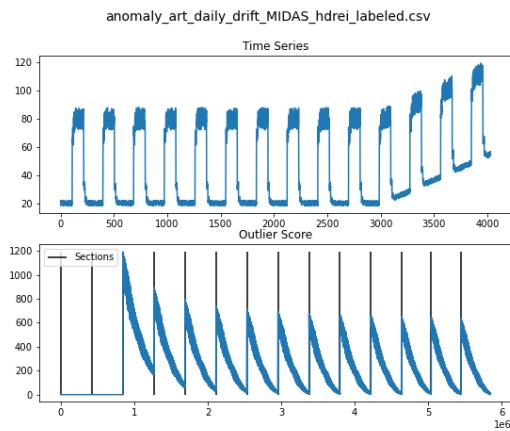
**Abb. B.-2:** Signaturvektoren der Zeitreihe mit vollständigen Graphen



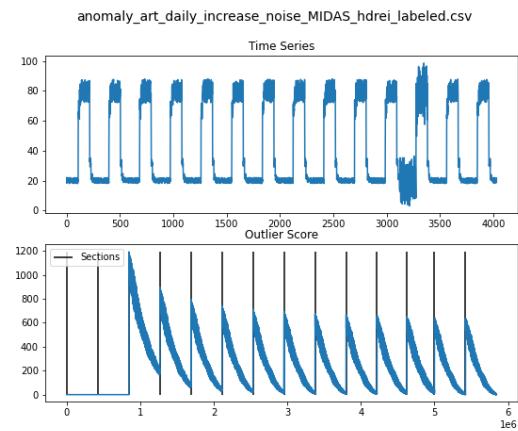
**Abb. B.-1:** Ausreißer-Score der vollständigen Graphen

## C MIDAS

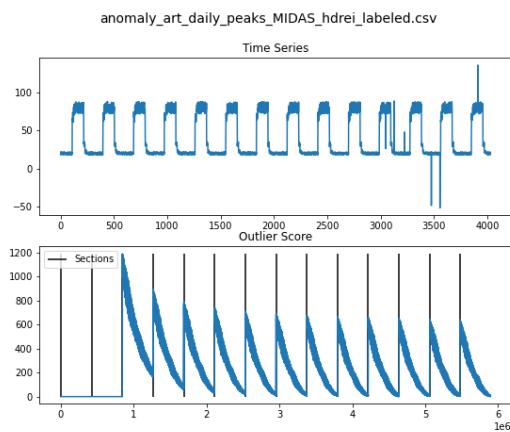
### Eindimensionales Signal



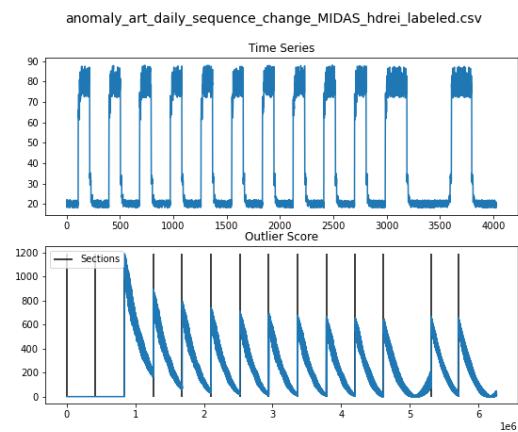
(a) Ausreißertyp Signal Drift



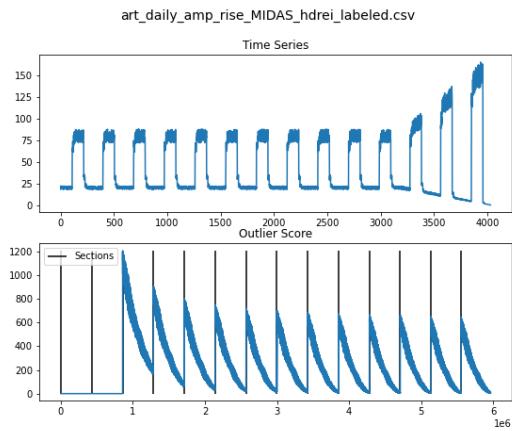
(b) Ausreißertyp Zunahme an Rauschen



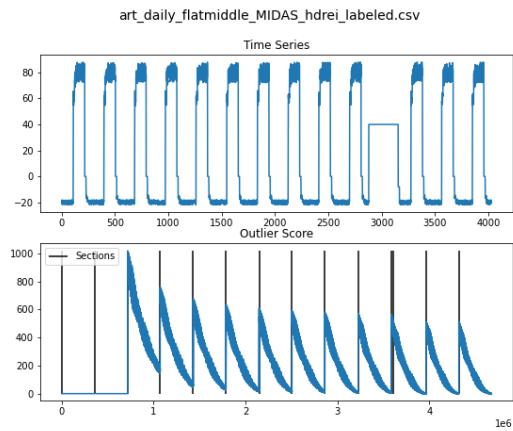
(c) Ausreißertyp Einzelne Peaks



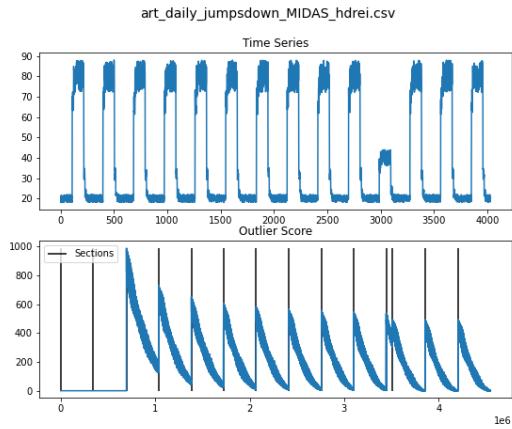
(d) Ausreißertyp Frequenzänderung



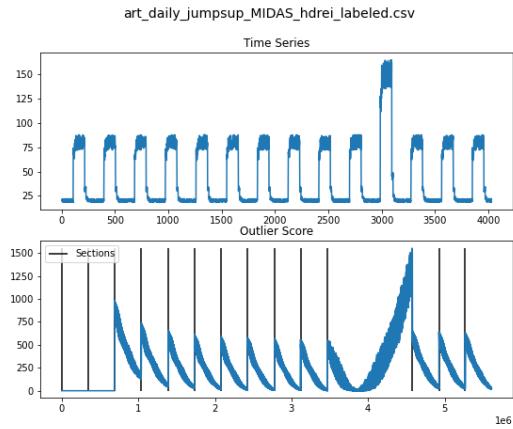
(e) Ausreißertyp Kontinuierliche Zunahme der Amplitude



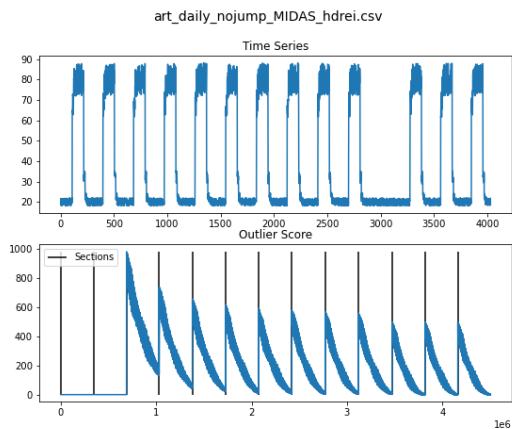
(f) Ausreißertyp Zyklus-Aussetzer



(g) Ausreißertyp Zyklus mit geringerer Amplitude



(h) Ausreißertyp Zyklus mit höherer Amplitude



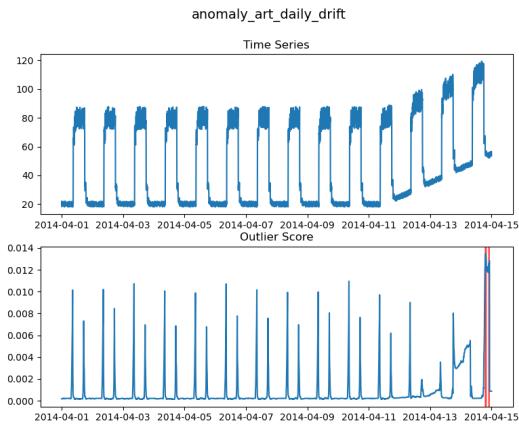
(i) Ausreißertyp Signal-Aussetzer

| Ausreißertyp                          | Dateiname                         | Bewertung |
|---------------------------------------|-----------------------------------|-----------|
| Einzelne Peaks                        | anomaly-art-daily-peaks           | -         |
| Zunahme an Rauschen                   | anomaly-art-daily-increase-noise  | -         |
| Signal Drift                          | anomaly-art-daily-drift           | -         |
| Kontinuierliche Zunahme der Amplitude | art-daily-amp-rise                | -         |
| Zyklus mit höherer Amplitude          | art-daily-jumpsup                 | **        |
| Zyklus mit geringerer Amplitude       | art-daily-jumpsdown               | -         |
| Zyklus-Aussetzer                      | art-daily-flatmiddle              | -         |
| Signal-Aussetzer                      | art-daily-nojump                  | -         |
| Frequenzänderung                      | anomaly-art-daily-sequence-change | -         |

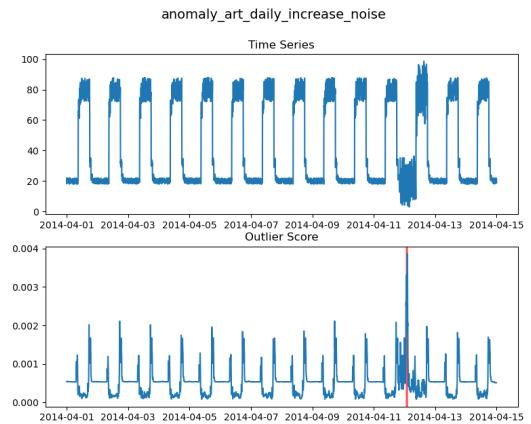
**Tab. C.1:** Bewertung des MIDAS-Algorithmus bzgl. der Erkennung von verschiedenen Ausreißertypen in Zeitreihen

## D Isomap

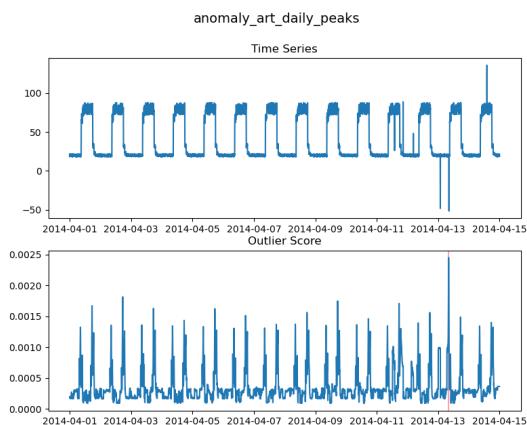
### Eindimensionales Signal



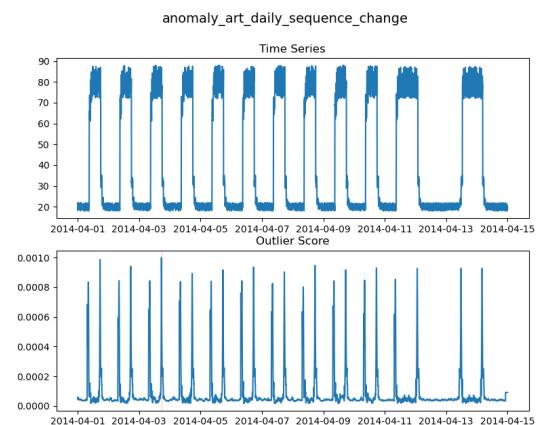
(a) Ausreißertyp Signal Drift



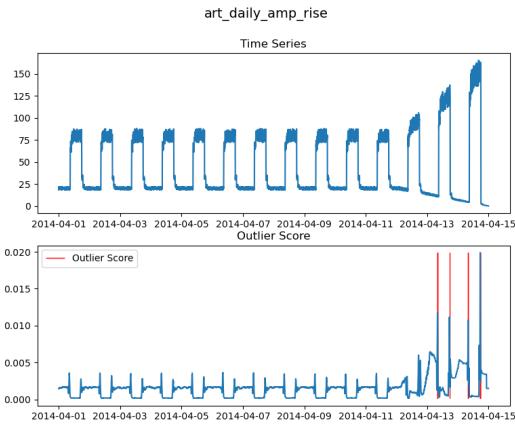
(b) Ausreißertyp Zunahme an Rauschen



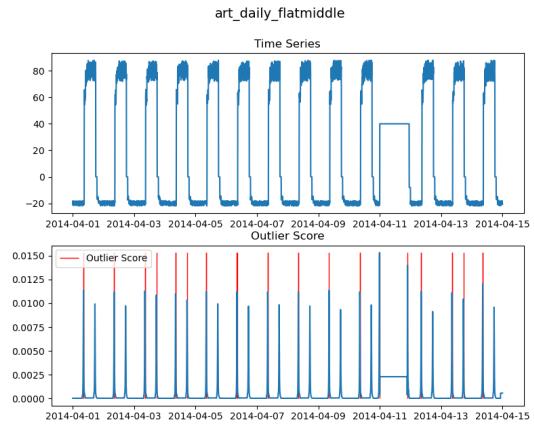
(c) Ausreißertyp Einzelne Peaks



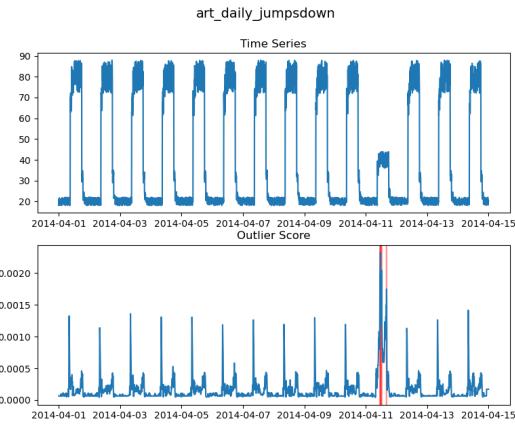
(d) Ausreißertyp Frequenzänderung



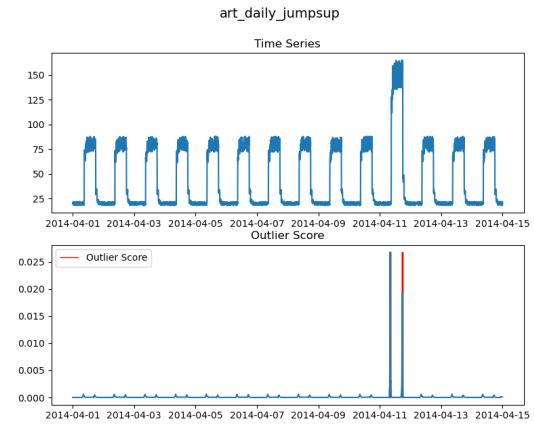
(e) Ausreißertyp Kontinuierliche Zunahme der Amplitude



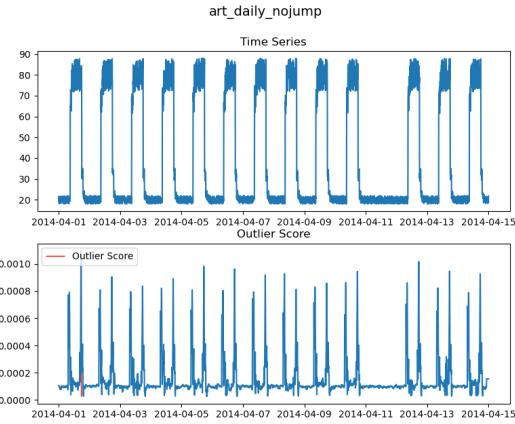
(f) Ausreißertyp Zyklus-Aussetzer



(g) Ausreißertyp Zyklus mit geringerer Amplitude



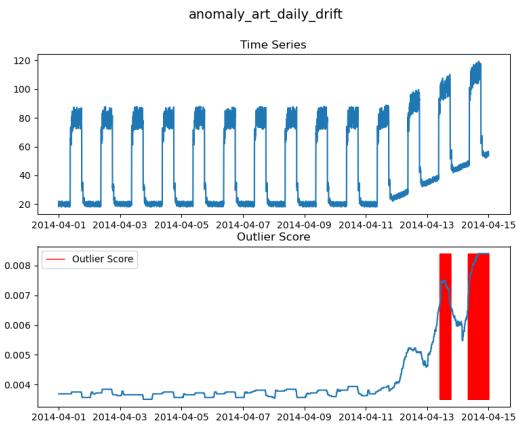
(h) Ausreißertyp Zyklus mit höherer Amplitude



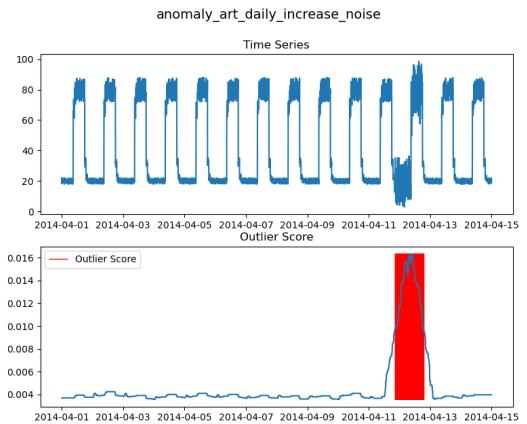
(i) Ausreißertyp Signal-Aussetzer

## E Percolation

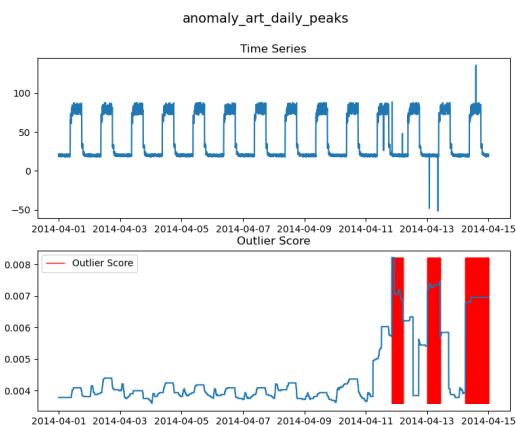
### Eindimensionales Signal



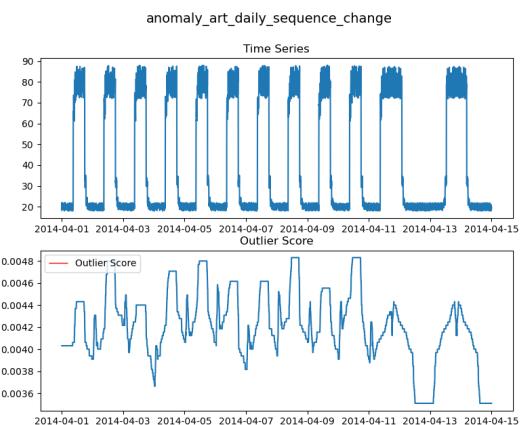
(a) Ausreißertyp Signal Drift



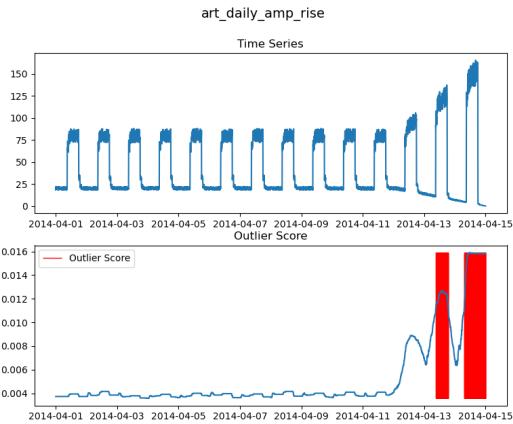
(b) Ausreißertyp Zunahme an Rauschen



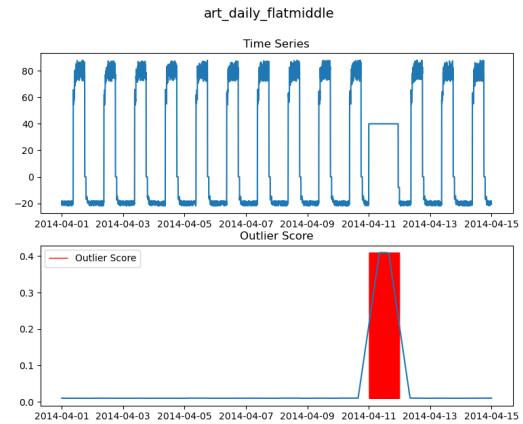
(c) Ausreißertyp Einzelne Peaks



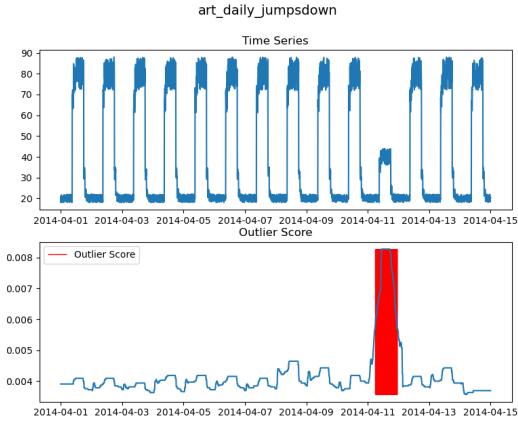
(d) Ausreißertyp Frequenzänderung



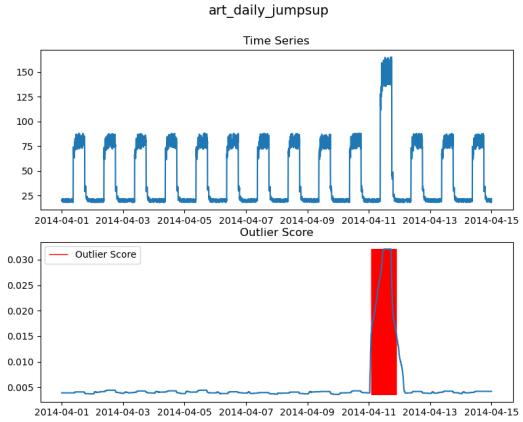
(e) Ausreißertyp Kontinuierliche Zunahme der Amplitude



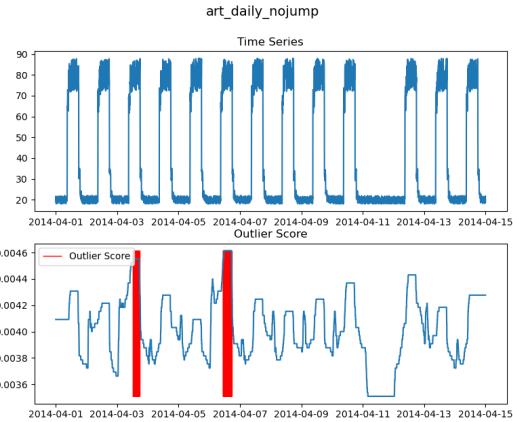
(f) Ausreißertyp Zyklus-Aussetzer



(g) Ausreißertyp Zyklus mit geringerer Amplitude



(h) Ausreißertyp Zyklus mit höherer Amplitude



(i) Ausreißertyp Signal-Aussetzer

## Literaturverzeichnis

- [1] Abt, S. and Baier, H. [2014], Are We Missing Labels? A Study of the Availability of Ground-Truth in Network Security Research, in ‘2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)’, pp. 40–55.
- [2] Ahmad, S., Lavin, A., Purdy, S. and Agha, Z. [2017], ‘Unsupervised real-time anomaly detection for streaming data’, *Neurocomputing* **262**, 134–147. Online Real-Time Learning Strategies for Data Streams.  
**URL:** <https://www.sciencedirect.com/science/article/pii/S0925231217309864>
- [3] Akoglu, L., McGlohon, M. and Faloutsos, C. [2010], oddball: Spotting Anomalies in Weighted Graphs, in M. J. Zaki, J. X. Yu, B. Ravindran and V. Pudi, eds, ‘Advances in Knowledge Discovery and Data Mining’, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 410–421.
- [4] Amil, P., Almeira, N. and Masoller, C. [2019], ‘Outlier Mining Methods Based on Graph Structure Analysis’, *Frontiers in Physics* **7**, 194.  
**URL:** <https://www.frontiersin.org/article/10.3389/fphy.2019.00194>
- [5] Berlingerio, M., Koutra, D., Eliassi-Rad, T. and Faloutsos, C. [2012], ‘NetSimile: A Scalable Approach to Size-Independent Network Similarity’, *CoRR* **abs/1209.2684**.  
**URL:** <http://arxiv.org/abs/1209.2684>
- [6] Bhatia, S., Hooi, B., Yoon, M., Shin, K. and Faloutsos, C. [2020], MIDAS: Microcluster-Based Detector of Anomalies in Edge Streams, in ‘AAAI 2020 : The Thirty-Fourth AAAI Conference on Artificial Intelligence’.
- [7] Cha, S.-H. [2007], ‘Comprehensive Survey on Distance/Similarity Measures Between Probability Density Functions’, *Int. J. Math. Model. Meth. Appl. Sci.* **1**.
- [8] Cheng, H., Tan, P., Potter, C. and Klooster, S. [2008], A Robust Graph-Based Algorithm for Detection and Characterization of Anomalies in Noisy Multivariate Time Series, in ‘2008 IEEE International Conference on Data Mining Workshops’, pp. 349–358.
- [9] Cormode, G. and Muthukrishnan, S. [2004], An Improved Data Stream Summary: The Count-Min Sketch and Its Applications, pp. 29–38.
- [10] Eswaran, D. and Faloutsos, C. [2018], SedanSpot: Detecting Anomalies in Edge Streams, pp. 953–958. Die Supplementary-Dokumentation wurde ebenfalls genutzt.
- [11] Lippmann, R., Haines, J., Fried, D., Korba, J. and Das, K. [2000], Analysis and Results of the 1999 Darpa Off-Line Intrusion Detection Evaluation, pp. 162–182.
- [12] Lovric, M., ed. [2011], *International Encyclopedia of Statistical Science*, Springer Berlin Heidelberg.  
**URL:** <https://doi.org/10.1007/978-3-642-04898-2>

- [13] Marks, Robert [2020], ‘Enron Timeline’. Letzter Zugriff : 13.03.2021.  
**URL:** <https://www.agsm.edu.au/bobm/teaching/BE/Enron/timeline.html>
- [14] Ranshous, S., Shen, S., Koutra, D., Harenberg, S., Faloutsos, C. and Samatova, N. F. [2015], ‘Anomaly detection in dynamic networks: a survey’, *Wiley Interdisciplinary Reviews: Computational Statistics* **7**(3), 223–247.  
**URL:** <https://doi.org/10.1002/wics.1347>
- [15] scikit-learn developers [2020], ‘sklearn.manifold.Isomap’. Letzter Zugriff : 13.03.2021.  
**URL:** <https://scikit-learn.org/stable/modules/generated/sklearn.manifold.Isomap.html>
- [16] Tenenbaum, J. B., Silva, V. d. and Langford, J. C. [2000], ‘A Global Geometric Framework for Nonlinear Dimensionality Reduction’, *Science* **290**(5500), 2319–2323.  
**URL:** <https://science.sciencemag.org/content/290/5500/2319>
- [17] Uzun, B., Kielman, J. and Erz, M. [2020], ‘Anomalie-Erkennung in Graphen’. nicht publiziert.
- [18] Xu, X., Yuruk, N., Feng, Z. and Schweiger, T. A. J. [2007], SCAN: A Structural Clustering Algorithm for Networks, in ‘Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining’, KDD ’07, Association for Computing Machinery, New York, NY, USA, p. 824?833.  
**URL:** <https://doi.org/10.1145/1281192.1281280>