der Bundeswehr
Universität München

Profilzuordnung über soziale Netze anhand von Metadaten

Dipl.-Inform. Robert Rödler

Vollständiger Abdruck der von der Fakultät für Informatik der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Gutachter:

1. Prof. Dr. Wolfgang Hommel
2. Prof. Dr. Arno Wacker

Die Dissertation wurde am 25.11.2021 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Informatik am 19.04.2022 angenommen. Die mündliche Prüfung fand am 25.05.2022 statt.

Kurzfassung

Profilzuordnung über soziale Netze anhand von Metadaten

Seit der Entwicklung sozialer Netze hat sich ihre Größe, Nutzerzahl und der Funktionsumfang schnell vergrößert. Zudem haben die meisten eine entsprechende Nische für sich entdeckt, wodurch es inzwischen mehrere hundert soziale Netze gibt. Daher ist es auch nicht verwunderlich, dass bereits 2016 eine Studie zu dem Ergebnis gekommen ist, dass eine Person im Durchschnitt in sieben sozialen Netzen angemeldet ist. Da ein Nutzer in einem sozialen Netz eine Menge persönlicher Informationen speichert und hinterlässt, gibt es eine Vielzahl von Bestrebungen, um diese Daten in einem Gesamtprofil zusammenzuführen. Diese Daten sind für Empfehlungssysteme, Marketing, Personalmanagement, aber auch Polizei und Geheimdienste höchst interessant. Klassische Profilzuordnungsverfahren basieren meist auf Profilattributen oder auf der Netzstruktur. Im Rahmen dieser Arbeit soll ein neuer Ansatz gewählt werden, der in dieser Form bisher nicht zum Einsatz kam: Die alleinige Abstützung der Verfahren auf öffentlich zugängliche Metadaten.

Im Rahmen dieser Dissertation wird daher untersucht, inwiefern sich zwei oder mehr Profile in unterschiedlichen sozialen Netzen ein und derselben Person zuordnen lassen und all dies nur anhand von Metadaten. Hierzu werden zunächst im Rahmen der Problembeschreibung die zu klärenden Forschungsfragen definiert, diese unter anderem anhand von Szenarien konkretisiert und entsprechende Anforderungen an ein Verfahren zur Zielerreichung definiert. Eine ausführliche Analyse des aktuellen Standes der Technik der Profilzuordnung und auch artverwandter Themen im Bereich sozialer Netze wird zur Abgrenzung dieser Arbeit durchgeführt. Anhand eines Metamodells werden die in einem sozialen Netz verfügbaren und abrufbaren Metadaten eingeführt und erläutert und basierend auf diesen Erkenntnissen werden drei Ansätze hinsichtlich Zielerreichung evaluiert. Dabei wird zum einen identifiziert, welche Metadaten sich überhaupt für die Profilzuordnung eignen, und zum anderen, wie viele davon benötigt werden. Es konnte gezeigt werden, dass selbst geringe Mengen Metadaten bereits eine nahezu 100%ige Zuordnungsgenauigkeit erzielen können. Umso wichtiger ist es, dass sich Nutzer dessen bewusst sind. Daher rundet eine Betrachtung nötiger Maßnahmen zur Verhinderung der erläuterten Ansätze und damit zur Sicherstellung des persönlichen Dateschutzes diese Arbeit ab.

Schlagwörter: Soziale Netze, Profilzuordnung, Metadaten, Zeitstempel, Geotags

Abstract

Profile Matching across Online Social Networks based on Meta Data

Since the development of social networks, their size, number of users and range of functions have rapidly increased. In addition, most of them have discovered a corresponding niche for themselves, as a result of which there are now several hundred social networks. It is therefore not surprising that a study in 2016 came to the conclusion that an average person is registered in seven social networks. Since a user stores and leaves a lot of personal information on a social network, there are numerous efforts to bring this data together in an overall profile. This data is extremely interesting for recommendation systems, marketing, personnel management, but also the police and secret services. Classic profile matching methods are mostly based on profile attributes or on the network structure. Within the scope of this work, a new approach is to be chosen that has not been used in this form so far. All approaches make only use of publicly available metadata.

As part of this dissertation, it is therefore investigated to what extent two or more profiles in different social networks can be matched to one and the same person and all this only on the basis of metadata. For this purpose, the research questions to be clarified are first defined in the context of the description of the problem, these are concretized using scenarios, among other things, and corresponding requirements for a method for achieving the goal are defined. A detailed analysis of the current state of the art of profile matching and related topics in the area of social networks is carried out to delimit this work. Using a meta model, the metadata available and retrievable in a social network are introduced and explained and, based on these findings, three approaches with regard to target achievement are evaluated. On the one hand, it identifies which metadata is suitable for profile matching and on the other hand, how much of it is required. It could be shown that even small amounts of metadata can achieve an almost 100% matching accuracy. It is all the more important that users are aware of this. Therefore, a consideration of the necessary measures to prevent the approaches explained and thus to ensure personal data protection rounds off this work.

Key words: social networks, profile matching, metadata, timestamps, geo-tags

Inhaltsverzeichnis

1. Einleitung **9**
1.1. Preisgabe privater Daten . . . 11
1.2. Metadaten-Definition . . . 11
1.3. Beiträge dieser Arbeit . . . 12
1.3.1. Skalierbare und verlässliche Profilzuordnung . . . 12
1.3.2. Erkennung von Fake-Profilen und Identitätsdiebstahl . . . 12
1.3.3. Botnet Erkennung . . . 13
1.4. Inhalt und Aufbau . . . 15

2. Problemstellung **17**
2.1. Ziel der Arbeit . . . 17
2.1.1. Metadaten-Extraktion . . . 17
2.1.2. Profilzuordnung . . . 17
2.2. Herausforderungen . . . 18

3. Szenarien **21**
3.1. Identitätsdiebstahl . . . 21
3.2. Fake-Profil . . . 22
3.3. Botnetze . . . 24

4. Anforderungsanalyse **27**
4.1. Anforderungen an ein Verfahren zur Profilzuordnung . . . 27
4.1.1. Keine direkte Nutzerbeeinflussung . . . 27
4.1.2. Verwendung von Metadaten . . . 28
4.1.3. Daten öffentlich zugänglich . . . 29
4.1.4. Skalierbarkeit . . . 30
4.1.5. Auswertung . . . 30
4.1.6. Verlässlichkeit . . . 31
4.2. Kategorisierung . . . 32
4.3. Zusammenfassung . . . 33

5. Stand der Technik **35**
5.1. Soziale Netze . . . 35
5.1.1. Analyse, Messung und Überwachung . . . 35
Meinungs- und Trenderkennung . . . 36
Ereigniserkennung . . . 36
Vorhersagen . . . 37
Geotags und ortsbasierte soziale Netze . . . 37
5.1.2. Schlussfolgern zusätzlicher Daten . . . 38
5.2. Profilzuordnung . . . 38
5.2.1. Attributübereinstimmung . . . 39
5.2.2. Netzstruktur . . . 40
5.2.3. Textanalyse . . . 41
5.2.4. Kombinationen . . . 41
5.2.5. Metadaten . . . 42
5.3. Mobilfunk und GPS Traces . . . 44
5.4. Privatsphäre in sozialen Netzen . . . 44
5.4.1. Ortsbasierte Verfahren . . . 45
5.4.2. Ansätze zur Verbesserung . . . 45
5.4.3. Fake-Profil- und Identitätsdiebstahl-Erkennung . . . 46
5.5. Bedrohungen . . . 46
5.5.1. Social Engineering . . . 46
5.5.2. Bots . . . 47
Fake-Profile und Spam . . . 47
Boterkennung . . . 48
5.6. Delta bisheriger Verfahren gegenüber dieser Arbeit . . . 48
5.7. Vergleich der Verfahren . . . 50

6. Metadaten Erfassung **55**
6.1. Metamodell . . . 55
6.2. Extrahierbare Metadaten . . . 57
6.2.1. IDs . . . 58
6.2.2. URLs . . . 59
6.2.3. Zeitstempel . . . 60
6.2.4. Geotags . . . 60
6.2.5. Areas . . . 62
6.2.6. Weitere Ressourcen-bezogene Metadaten . . . 63
6.2.7. Nutzerprofil-bezogene Metadaten . . . 64
6.3. Auswahl der sozialen Netze für die Evaluation . . . 65
6.3.1. Größe und Popularität . . . 65
6.3.2. Zugänglichkeit der Daten . . . 66
6.3.3. Wahrscheinlichkeit von Profilbeziehungen . . . 67
6.3.4. Verfügbarkeit von Metadaten . . . 68
6.3.5. Twitter . . . 68
6.3.6. Instagram . . . 69

6.3.7. Youtube . . . 70
6.4. Zusammenfassung . . . 70

7. Rahmenbedingungen der Profilzuordnung 71
7.1. Grundlagen . . . 71
7.1.1. Twitter-IDs . . . 71
7.1.2. Instagram-IDs . . . 72
7.2. Datensätze . . . 74
7.2.1. Profildaten . . . 74
7.2.2. Ground-Truth-Daten . . . 74
Verlässliche Profilzuordnung . . . 74
About.me . . . 75

8. Zuordnung anhand des zeitlichen Nutzerverhaltens 77
8.1. Datensatz . . . 77
8.2. Vorhersage des zeitlichen Nutzungsverhaltens . . . 79
8.2.1. Naiver Ansatz . . . 80
8.2.2. Tageweiser Ansatz . . . 80
8.3. Evaluation . . . 82
8.4. Zusammenfassung und Schlussfolgerung . . . 88

9. Profilzuordnung anhand von Zeitdifferenzen 91
9.1. Nutzungsmöglichkeiten und deren zeitlichen Abhängigkeiten . . . 91
9.1.1. Manuelles Posten . . . 91
9.1.2. Automatisches Posten . . . 92
9.1.3. Bot in einem Netz ohne automatisierte Benachrichtigung . . . 94
9.1.4. Bot in einem Netz mit automatisierter Benachrichtigung . . . 94
9.1.5. Posten eines Identitätsdiebes . . . 96
9.1.6. Zusammenfassung . . . 97
9.2. Prinzip der Nutzung von Zeitdifferenzen . . . 98
9.3. Datensatz . . . 99
9.3.1. Profilzuordnung . . . 99
9.3.2. Munich Bot Challenge . . . 101
9.4. Zuordnungsverfahren . . . 102
9.5. Evaluation . . . 103
9.5.1. Profilzuordnung . . . 103
9.5.2. Boterkennung . . . 105
9.6. Zusammenfassung . . . 108

10. Geobasierte Profilzuordnung 109
10.1. Datensatz . . . 109
10.2. Schrittweises Vorgehen . . . 109
10.2.1. Analyse der Aktivitätszentren . . . 109
Ergebnisse aus der Analyse der Zentren und Radien . . . 111

Schlussfolgerungen . . . 115
10.2.2. Vergleich der Aktivitätszentren . . . 115
Ergebnisse des Aktivitätszentrenvergleichs . . . 116
Schlussfolgerungen . . . 118
10.2.3. Vergleich auf Geotag-Ebene . . . 118
Erhöhung der Aussagekraft durch virtuelle Datensätze . . . 119
Auswertung auf Ebene der Geotags . . . 119
Ergebnisse der Geotag-weisen Auswertung . . . 122
Schlussfolgerungen . . . 129
10.3. Zusammenfassung . . . 129

11. Gewichtung und Aggregation der Verfahren 131
11.1. Aggregation der Teilergebnisse . . . 131
11.2. Ermittlung der Gewichtung . . . 132
11.3. Zusammenfassung . . . 132

12. Schutzmaßnahmen gegen Profilzuordnung 133
12.1. Zeit-basierte Schutzmaßnahmen . . . 133
12.1.1. Schutzmaßnahmen im Hinblick auf das Nutzungsverhalten . . . 133
12.1.2. Schutz vor Profilzuordnung durch Zeitdifferenzen . . . 134
12.2. Geo-basierte Schutzmaßnahmen . . . 134
12.3. Zusammenfassung . . . 135

13. Zusammenfassung und Ausblick 137
13.1. Einordnung der wissenschaftlichen Fragestellungen . . . 137
13.2. Abgleich der Anforderungserfüllung . . . 137
13.3. Beantwortung der Fragestellungen . . . 140
13.4. Weitergehende Forschungsarbeiten . . . 141

Tabellenverzeichnis 143

Abbildungsverzeichnis 145

Literatur 147

A. Anhang 173
A.1. Verfügbare Metadaten bei Twitter . . . 173
A.2. Ergänzende Diagramme der Geotag-weisen Auswertung . . . 175
A.2.1. Ergebnisse der einzelnen Metriken . . . 175
A.2.2. Top-3-Trefferliste . . . 176
A.3. Veröffentlichungen im Rahmen dieser Dissertation . . . 177

KAPITEL 1

Einleitung

Soziale Netze sind heute allgegenwärtig, auf nahezu jeder Website findet sich ein *Like-Button* bspw. von Facebook oder vergleichbare Interaktionselemente anderer sozialer Netze. Doch was ist ein soziales Netz? Boyd et al. [1] definieren dies als Web-basierten Dienst, der es Individuen erlaubt, öffentliche bzw. halb-öffentliche Profile innerhalb eines abgegrenzten Systems anzulegen, Listen von anderen Mitgliedern, zu denen eine Verbindung besteht, zu veröffentlichen und das Betrachten und Durchsuchen ihrer Verbindungsliste und derer die von anderen Mitgliedern innerhalb des Systems angelegt wurden. Die Art und Benennung dieser Verbindungen variiert dabei in Abhängigkeit vom Kontext der Seite.

Unter einem Profil versteht man im Kontext dieser Arbeit zum einen eine Profilseite, auf der Nutzer eines sozialen Netzes persönliche Informationen veröffentlichen bzw. teilen können. Zu dort veröffentlichten Informationen zählen beispielsweise Daten wie Name, Geburtsdatum, Hobbys, Verweise auf andere Profilseiten in anderen sozialen Netzen und ein Profilfoto. Zum anderen werden auch die Interaktionen mit dem sozialen Netz im Rahmen dieser Arbeit unter Profil verortet. Hierzu zählen beispielsweise eingestellte Inhalte wie Nachrichten, Posts, Annotierungen, Tags, Fotos bzw. Bilder und Videos. Nur sehr wenige soziale Netze erlauben die Möglichkeit, dass ein Nutzer mehr als eine Profilseite verwaltet, daher ist ein Profil gleichbedeutend mit einem eindeutigen Benutzerprofil, oft auch als Account bezeichnet, welches durch eine Benutzerkennung geschützt ist.

Um Mitglied in einem sozialen Netz zu werden, muss sich ein Nutzer dort anmelden bzw. registrieren. Gäste haben abhängig vom Anbieter meist keine oder nur partielle Leserechte. Nach der Registrierung können Mitglieder alle Funktionen des Netzes nutzen, dennoch können Mitglieder meist die Leserechte für ihre Profile einschränken, sodass diese beispielsweise nur für Mitglieder der Verbindungsliste dieses Nutzers zugänglich sind.

Soziale Netze erfüllen das Bedürfnis vieler Menschen zur Selbstdarstellung, weshalb ihr Wachstum stetig zunimmt. Facebook als das größte Netz, zählte am 31. Dezember 2016 bereits mehr als 1,8 Milliarden aktive Nutzer pro Monat [2]. Auch andere soziale Netze wie Twitter mit 313 Millionen oder Instagram mit über 600 Millionen Nutzern wachsen unaufhaltsam

[3] [4]. Aufgrund der großen Anzahl an Nutzern und der Fülle der von ihnen verbreiteten Informationen machen sich viele Forscher diese Daten zu nutze. Twitter-Daten werden zum Beispiel genutzt, um Erdbeben zu detektieren [5], die Ausbreitung der Grippe zu überwachen [6] oder Wahlergebnisse vorauszusagen [7]. Aber auch die Vorhersage von Aktienkursen [8], der Ort und die Zeit eines Verbrechens [9] oder das Auffinden von Schwachstellen in Software-Systemen [10] sind Gegenstand aktueller Forschung.

Als Alleinstellungsmerkmal setzen die meisten sozialen Netze auf eine Spezialisierung ihres Angebots. Daher gibt es beispielsweise Netze für Bilder und Fotos (Flickr, Instagram), für Videos (Youtube), Kurznachrichten (Twitter), Standortdaten (Foursquare) und viele weitere mehr.

Die Spezialisierung sozialer Netze führt dazu, dass viele Nutzer nicht nur bei einem, sondern bei mehreren Netzen Mitglied sind. Derzeit ist laut [11] davon auszugehen, dass ein Nutzer durchschnittlich bei sieben sozialen Netzen registriert ist. Besonders für Marketingzwecke sind die Kenntnisse über die verschiedenen Netze, in denen ein Nutzer angemeldet ist, von hohem Wert. So lassen sich umfangreiche Informationen über Zielgruppen und deren Interessen in Erfahrung bringen. Das Interesse von Nachrichtendiensten besteht schlicht in der Sammlung möglichst vieler Daten und Informationen und der Beziehungen untereinander, im Idealfall würden dabei auch die regionale Rechtsprechung und entsprechende Datenschutzgesetze berücksichtigt, um Straftäter und Terroristen zu ermitteln. Aufgrund der Allgegenwärtigkeit von sozialen Netzen nutzen immer mehr Arbeitgeber, in den USA bereits über 60% [12], die Möglichkeiten dieser Netze, um Kandidaten bereits vor dem Bewerbungsgespräch zu überprüfen und gegebenenfalls auszusortieren. Auch Firmen haben diese Marktlücke erkannt und bieten entsprechende Dienstleistungen zur Überprüfung eines Kandidaten anhand seiner Profile in sozialen Netzen an, beispielsweise [13].

Verfahren zur Zuordnung von Profilen zum selben Nutzer werden bereits eingesetzt. Dennoch basieren diese Ansätze, so sie nur auf öffentlich zugänglichen Daten arbeiten, auf der Annahme, dass Nutzer korrekte Daten in ihren Profilen nutzen. Hierzu werden beispielsweise die Namen und weitere Attribute, die in den Profilen hinterlegt sind, gegeneinander abgeglichen. Schreibfehler und häufig auftretende Namen führen hierbei zu Problemen. Auch wenn ein Nutzer gezielt Fake-Profile anlegt oder die Profildaten von jemand anderem, beispielsweise einem Mobbing-Opfer oder einem Prominenten, kopiert, versagen diese Verfahren.

In dieser Arbeit wird ein Verfahren entwickelt, welches die Zuordnung mehrerer Profile zur selben Person erlaubt, basierend auf Metadaten, die keiner direkten Kontrolle des Nutzers unterliegen. Dies erlaubt die Zuordnung mehrerer Profile in verschiedenen sozialen Netzen zu einem Nutzer, aber auch die Erkennung von Fake-Profilen und Identitätsdiebstahl. Darüber hinaus werden die Detektion von Spambotnetzen in den Netzen und die Bestimmung von Profilen zur Steuerung von Botnetzen, so hierzu mehr als ein Profil genutzt wird, ermöglicht.

1.1. Preisgabe privater Daten

Viele Menschen veröffentlichen private Daten in sozialen Netzen. Um besonders viel Aufmerksamkeit hervorzurufen, werden von den Nutzern stetig neue Informationen veröffentlicht. Solange diese Daten nur engen Freunden zugänglich sind, geht von ihnen kaum Gefahr aus, viele Nutzer verzichten jedoch auf entsprechende Einstellungen [14]. Darüber hinaus lassen die Privatsphäreneinstellungen der sozialen Netze meist zu wünschen übrig. Entweder stehen wichtige Funktionen zur Einschränkung nicht bereit, oder sind tief in den Konfigurationseinstellungen versteckt, so dass sie von den Nutzern nicht gefunden werden [15] [16].

Die Preisgabe privater Daten in sozialen Netzen ist umso kritischer, wenn daraus weitreichende Folgen entstehen können. Auch wenn diese über mehrere Profile gestreut werden, bietet dies wie zuvor erläutert keinen Schutz mehr. Private Daten können zu unterschiedlichen Zwecken missbraucht werden, wenn sie in die falschen Hände gelangen. Der Einbruch in die eigenen vier Wände sei hier exemplarisch für eine Vielzahl an Folgen genannt, siehe [17]. Einbrecher nutzen aus, dass unvorsichtige Nutzer bekannt geben, dass sie sich beispielsweise gerade im Urlaub im Ausland befinden. Selbst ein Strandfoto kann bereits diese Information liefern. Da nützt es auch nichts, wenn die Adresse nur in einem anderen Netz hinterlegt ist.

Es können nicht nur materielle Schäden entstehen: [18] erwähnt, dass es Ansätze gibt, Nutzer anhand ihrer Tweetfrequenz auf psychopathische Veranlagung hin zu untersuchen. Solche Ansätze entbehren jedweder Logik und sind auch nicht wissenschaftlich fundiert; dennoch eingesetzt, können sie den Ruf und dadurch das Leben eines Menschen immens schädigen.

1.2. Metadaten-Definition

Die in dieser Arbeit vorgestellten Algorithmen basieren auf der Nutzung von Metadaten. Der Grund ist, dass Daten, die der Nutzer selbst definieren kann, wie beispielsweise Namen, Adressen, Hobbys usw., nicht geeignet sind für Profile, die bewusst suggerieren sollen, einer anderen Person zu gehören.

Die National Information Standards Organization [19] definiert Metadaten sinngemäß wie folgt: Metadaten sind strukturierte Informationen, die beschreiben, erklären, lokalisieren oder es anderweitig erleichtern, eine Informationsquelle abzurufen, zu verwenden oder zu verwalten.

Es werden drei Hauptarten von Metadaten unterschieden, siehe [19]:

- **Beschreibende Metadaten** beschreiben Ressourcen, um diese leichter entdecken und identifizieren zu können. Beispielsweise Autor, Schlüsselwörter oder im Kontext sozialer Medien Geotags.
- **Strukturelle Metadaten** kennzeichnen, wie zusammengesetzte Objekte vereinigt werden. Beispielsweise, wie Seiten zu einem Buch angeordnet werden müssen.

- **Administrative Metadaten** liefern Informationen zur Verwaltung einer Ressource. Beispielsweise, wie und wann diese erzeugt wurde, welcher Dateityp vorliegt und wer Zugriff hat.

1.3. Beiträge dieser Arbeit

Der Kern der Arbeit ist die Entwicklung eines Verfahrens zur Zuordnung von mehreren Profilen zu einer Person. Damit können sowohl Profile verschiedener sozialer Netze, die der Spezialisierung der Netze geschuldet sind, dem selben Nutzer zugeordnet werden, als auch mehrere Profile im gleichen Netz, so genannte Fake-Profile, beispielsweise zum Zwecke des Identitätsdiebstahls, erkannt werden.

1.3.1. Skalierbare und verlässliche Profilzuordnung

Soziale Netze haben Millionen von Nutzern, aus diesem Grund ist die Skalierbarkeit ein entscheidender Faktor für die Praxistauglichkeit des Verfahrens. Methoden des maschinellen Lernens erfordern, um verlässliche Ergebnisse zu erzielen, annotierte Ground-Truth-Daten. Entsprechende Datensätze, besonders zur repräsentativen Abbildung aller Eigenarten der Profile eines Netzes, sind jedoch nicht verfügbar. Zudem ist die Wahrscheinlichkeit von False-Positives immens, da bei dieser Anzahl an Profilen die Profilattribute stark auseinander laufen. Um ein skalierbares Verfahren zu erhalten, wurden Methoden der Statistik, Schnittmengenbetrachtungen, verschiedenen Distanzmaße und Mustererkennung implementiert, die eine geringe Laufzeitkomplexität aufweisen.

Diese verschiedenen Ansätze werden durch Experimente mit Ground-Truth-Datensätzen auf ihre Eignung zur Ermittlung von Profilen gleichen Nutzerverhaltens hin, untersucht. Anhand dieser Resultate wurde eine spezifische Gewichtung für jedes einzelne Verfahren, so es geeignet war, ermittelt und eine Methode zur Aggregation dieser Techniken bestimmt.

Um eine verlässliche Profilzuordnung zu erreichen, wurden verschiedene Arten und Mengen an Metadaten sowie Kombinationen daraus evaluiert. Basierend auf diesen Resultaten werden Empfehlungen gegeben, welche Daten die genauesten Ergebnisse versprechen. Hierbei wurde ebenso berücksichtigt, welche Mengen an Metadaten aus den betrachteten sozialen Netzen extrahiert werden können.

1.3.2. Erkennung von Fake-Profilen und Identitätsdiebstahl

Die Erkennung erfolgt vollständig anhand von Metadaten. Typische Attribute von Profilseiten sozialer Netze können von Nutzern beliebig verändert und manipuliert werden. Dies gilt jedoch nicht für Metadaten. Zwar kann ein Nutzer beeinflussen, zu welcher Zeit er einen Eintrag tätigt, nicht jedoch, welcher Zeitstempel gespeichert und angezeigt wird. Zudem kann dieser im Nachhinein nicht mehr verändert werden. Lediglich die Löschung des Eintrages und damit die vollständige Entfernung des Zeitstempels ist in den meisten sozialen Netzen möglich. Aus diesem Grund können auch Profile einer bestimmten Person zugeordnet werden, die bewusst

falsche Attribute im Profil hinterlegt hat.

Die Gründe für so genannte Fake-Profile sind vielfältig. Die nachfolgende Liste betrachtet verschiedene Gründe wozu Fake-Profile genutzt werden, erhebt jedoch keinen Anspruch auf Vollständigkeit:

- **Mobbing:** Es werden Gerüchte über eine Person in die Welt gesetzt, um deren Ruf zu schädigen. Empfänger der Nachrichten sind gewöhnlich Bekannte der gemobbten Person.
- **Stalking:** Der Profilinhaber möchte nicht, dass eine bestimmte Person Zugriff auf sein Profil bekommt. Diese Person nutzt jedoch ein gefälschtes Profil, um eine andere Identität zu suggerieren und so dennoch Einblick in das Profil zu erhalten.
- **Hassreden:** Es werden Personen, Minderheiten und Randgruppen beschimpft und diffamiert.
- **Propaganda:** Verbreitung von linkem, rechten, terroristischem oder anderweitig unerwünschtem Gedankengut.
- **Identitätsdiebstahl:** Im Unterschied zum Stalking gibt sich eine Person nicht für irgendeine andere, sondern für eine ganz bestimmte Person aus. Ziel ist es, einen Profilinhaber, der mit dem eigentlichen Identitätsinhaber bekannt ist, zum Aufruf bestimmter Seiten, beispielsweise für Phishing oder Whaling, oder zur Preisgabe von Informationen, so genanntes Social Engineering, zu bewegen.

Ermittlungsbehörden tun sich bei strafbaren Handlungen in sozialen Netzen oft schwer, den Täter zu ermitteln. Dies liegt zum einen daran, dass die Zuordnung einer IP-Adresse zu einem Anschluss nur bei Kapitalverbrechen legal ist, und zum anderen befindet sich der Firmensitz der sozialen Netze meist außerhalb des Staatsgebiets, in dem die Straftat erfolgt ist, sodass die Firmen meist nicht gezwungen werden können, entsprechende Daten offenzulegen, siehe [20].

Das in dieser Arbeit entwickelte Verfahren erlaubt die Zuordnung eines Fake-Profils einem realen Profil, so der Täter eines besitzt. Dies ermöglicht Strafverfolgungsbehörden, die wahre Identität des Täters zu ermitteln oder zumindest auf einen kleinen Personenkreis einzuschränken.

1.3.3. Botnet Erkennung

Botnetze und deren Fähigkeiten sind ein großes Übel im Internet. Ein Botnetz ist ein Zusammenschluss vieler mit Schadsoftware infizierter PCs und anderer rechnergestützter Geräte. Auch Geräte des Internet of Things werden zunehmend zu so genannten Zombies versklavt [21]. Botnetze werden beispielsweise für den Versand von Spam oder die Ausführung von distributed Denial of Service (DDoS) Attacken eingesetzt.

Ein Botnet wird typischerweise über eine so genannte Command-and-Control-Infrastruktur gesteuert. Über diese werden sowohl die Bots mit neuen Befehlen versorgt als auch Daten von

diesen abgegriffen. Es gibt diverse Typen von Command-and-Control-Infrastrukturen, die sich besonders in der Art der Kommunikation unterscheiden. Der Internet Relay Chat (IRC) basiert auf mehreren Servern, die untereinander verbunden sind und Chat-Räume zur Verfügung stellen. Ein Botmaster, der Betreiber des Botnetzes, erstellt dort einen entsprechenden Raum, zu dem sich die Zombies verbinden. Hierdurch werden alle Bots zeitnah erreicht und Befehle können ohne Verzögerung ausgeführt werden.
Kommt eine Webanwendung zum Einsatz, wird keine fortwährende Verbindung gehalten, sondern in regelmäßigen Abständen auf neue Befehle geprüft.
Peer-to-Peer (P2P)-Kommunikation bedeutet, dass es keine zentrale Command and Control Infrastruktur gibt. Stattdessen verbinden sich die Zombies untereinander. Um Befehle absetzen zu können, verbindet sich der Botmaster zu einem Bot und überträgt die Befehle. Der Bot benachrichtigt nun die Bots, die ihm bekannt sind; diese verfahren genau so. Auf diese Weise werden in kurzer Zeit alle Bots erreicht und der Botmaster läuft nicht Gefahr, dass die Infrastruktur abgeschaltet werden kann.

IRC- und P2P-Kommunikation haben den Nachteil, dass ihr Datenverkehr leicht identifizierbar ist. Ein zentraler Server mit Webanwendung entspricht einem Single Point of Failure, beispielsweise kann der Server abgeschaltet oder die Adresse blockiert werden. Daher wird versucht, die Steuerung der Bots in legitimen Datenverkehr zu verstecken. Soziale Netze bieten sich hierzu an, da aufgrund der vielen Nutzer deren Datenverkehr gewöhnlich toleriert und nicht eingeschränkt oder blockiert wird. Daher setzen diverse Botnetze auf die Kommunikation mittels sozialer Netze. Da einzelne Profile leicht gelöscht werden können, nutzt ein Botmaster mehrere zur Kommunikation mit den Zombies [22] [23] [24].

Das Verfahren zur Zuordnung von mehreren Profilen zu einem Nutzer erkennt solche Steuerungsprofile, so dass diese alle zeitgleich gelöscht und hierdurch das Botnetz außer Betrieb genommen werden kann.

Darüber hinaus verbreiten Botnetze nicht mehr nur Spam in Form von E-Mails, sondern auch immer mehr als Nachrichten oder Posts in sozialen Netzen, siehe unter anderem [25] [26] [27]. Da sich die Programmierer solcher Spambots meist nicht die Mühe machen, die zeitliche Verteilung dieser Spam-Nachrichten zufällig erscheinen zu lassen, ist eine Identifizierung einfach anhand der zeitlichen Verteilung möglich [28] [29]. Durch das entwickelte Verfahren können so Profile identifiziert werden, die ein ähnliches Verhalten wie andere Spambots aufweisen. So können die Profile, die von einem Botnetz zum SpamVersand missbraucht werden, identifiziert und gesperrt werden. Anhand unterschiedlichem zeitlichem Verhalten lassen sich sogar verschiedene Botnetze voneinander abgrenzen. Solche Erkenntnisse können zukünftig auch Wahlkämpfe transparenter machen, da sogar Parteien den Einsatz von Spambots planen, vgl. [30].

1.4. Inhalt und Aufbau

Diese Arbeit ist nach Themen folgendermaßen gegliedert. Kapitel 2 schärft die Ziele der Arbeit, erläutert die zu klärenden Forschungsfragen und beschreibt die dabei zu meisternden Herausforderungen und zu beachtenden Anforderungen. Eine Übersicht von Szenarien bei denen die in dieser Arbeit entwickelten Ansätze zum Einsatz kommen könnten, zeigt Kapitel 3. Darauf aufbauend erfolgt in Kapitel 4 eine Anforderungsanalyse an die zu entwickelnden Verfahren. Der Stand der Technik wird im Detail in Kapitel 5 betrachtet und bewertet. Hierbei erfolgt sowohl eine Analyse bisheriger Profilzuordnungsansätze als auch artverwandter Themen und Methoden, beispielsweise zur Bot-Erkennung in sozialen Netzen.

Kapitel 6 klärt anhand eines adaptierten Metamodells, welche Metadaten für die Profilzuordnung anhand der definierten Anforderungen geeignet sind und stellt diese im Detail vor. Die Rahmenbedingungen in weitere grundlegende Informationen für die weitere Arbeit werden dann im Kapitel 7 eingeführt. In den nächsten Kapiteln werden drei verschiedene Ansätze für die Profilzuordnung vorgestellt und evaluiert. In Kapitel 8 wird anhand historischer Daten versucht das zukünftige Nutzerverhalten vorherzusagen. Ein Verfahren, welches anhand von Zeitdifferenzen verknüpfter Interaktionen eine Profilzuordnung vornimmt, wird in Kapitel 9 vorgestellt. Das dritte vorgestellte Verfahren in Kapitel 10 basiert auf der Analyse von Geotags, dabei werden Profile anhand von Distanzen zwischen Geotags zugeordnet. Kapitel 11 gibt dann eine Empfehlung, wie die Ergebnisse der drei vorgestellten Verfahren am besten zusammengefasst werden können.

Mögliche Maßnahmen zum Schutz der Privatssphäre in sozialen Netzen und insbesondere gegen Informationsgewinn aus der Korrelation öffentlich verfügbarer Daten werden in Kapitel 12 diskutiert. Kapitel 13 fasst die Ergebnisse dieser Arbeit zusammen und gibt einen Ausblick auf zukünftige Forschungsaktivitäten in diesem Bereich. Darüber hinaus enthält dieses Kapitel eine Auflistung der Veröffentlichung, die im Rahmen dieser Arbeit entstanden sind.

KAPITEL 2

Problemstellung

In diesem Kapitel werden die Forschungsfragen detailliert erläutert und die resultierenden Herausforderungen und Anforderungen an das Verfahren definiert.

2.1. Ziel der Arbeit

Der Schwerpunkt der Arbeit liegt darauf zu zeigen, dass mehrere (mindestens zwei) Profile ein und dem selben Nutzer nur anhand der Auswertung von Metadaten zugeordnet werden können. Die basierend auf dieser Anforderung entwickelten Fragestellungen werden in den folgenden Unterabschnitten betrachtet.

2.1.1. Metadaten-Extraktion

Da Metadaten keine bewusst von einem Nutzer generierten Daten sind, stellt sich die Frage, welche Metadaten durch entsprechende Nutzerinteraktionen generiert werden. Im Kontext dieser Arbeit insbesondere die Metadaten, die öffentlich zugänglich sind. Metadaten, die nur das soziale Netz zur Strukturierung oder Verwaltung nutzt und selbst vom generierenden Nutzer nicht eingesehen werden können, werden im weiteren Verlauf dieser Arbeit nicht betrachtet.

Die Vielzahl verschiedener sozialer Netze wirft auch die Frage auf, welche Überschneidungen der Metadatentypen netzübergreifend extrahiert werden können. Zu berücksichtigen ist ebenfalls, ob diese Metadaten Unterschiede, beispielsweise im Hinblick auf die Genauigkeit, aufweisen. Unterschiedliche Kodierungen beispielsweise von Datums- und Uhrzeit-Angaben werden hierunter nicht berücksichtigt. Eine solche Unterscheidung ist im Hinblick auf das erarbeitete Verfahren überflüssig, da entsprechende Umwandlungen von diversen frei verfügbaren Programmbibliotheken automatisiert vorgenommen werden können.

2.1.2. Profilzuordnung

Schwerpunkt dieser Arbeit ist die Klärung der Fragen, anhand welcher Metadaten sich mehrere Profile demselben Nutzer zuordnen lassen. Geklärt wird dabei, welche Arten von Metada-

ten hierfür geeignet und wie viele Daten dafür erforderlich sind. Des Weiteren werden die Eigenschaften, Beziehungen und Korrelationen zwischen den Metadaten von Beiträgen in sozialen Onlinenetzen bestimmt, die eine Zuordnung möglich machen. Darüber hinaus wird ermittelt, wie hoch die zu erzielende Genauigkeit in Abhängigkeit zur gewählten Kombination aus Metadaten ist.

2.2. Herausforderungen

Die nachfolgend betrachteten Herausforderungen unterstreichen die Komplexität der Fragestellungen in dieser Arbeit:

- **Extraktion von Metadaten**: Soziale Netze verdienen mit dem Verkauf der Nutzerdaten und mit auf den Nutzer angepasster Werbung ihr Geld [31]. Auch wenn Schnittstellen für Entwickler bereitgestellt werden, die die Attraktivität des Netzes steigern sollen, so sind die Anbieter dennoch bestrebt, einen massenhaften Abgriff ihrer Daten zu verhindern. Aus diesem Grund sind für alle Entwicklerfunktionen Limits definiert, die festlegen, wie oft eine Funktion in einem Zeitintervall maximal aufgerufen werden darf und meist existiert zusätzlich eine obere Grenze, wie weit zurück Daten abgefragt werden können. Dies kann eine zeitliche oder mengenbasierte Begrenzung sein, beispielsweise kann bei Twitter über die `user_timeline`-Funktion der Entwicklerschnittstelle nur auf die jüngsten 3.200 Tweets zugegriffen werden [32].

- **Zeitliche und örtliche Lücken der Daten**: Metadaten in sozialen Netzen werden durch Nutzerinteraktion generiert. Aber nur wenn die Nutzerinteraktion zu öffentlich zugänglichen Informationen führt, beispielsweise die Erstellung eines Posts, Kommentars, Tweets oder ähnlichem, sind auch die zugehörigen Metadaten öffentlich zugänglich. Dies bedeutet, dass obwohl ein Nutzer den ganzen Tag die Profile seiner Freunde liest, keine öffentlich zugänglichen Metadaten generiert werden. Es handelt sich dabei also nur um Momentaufnahmen, die von einem Nutzer zu unterschiedlichen Uhrzeiten und meist an verschiedenen Orten ausgelöst werden. Dies unterscheidet die Daten, die aus einem sozialen Netz extrahiert werden können, beispielsweise von Mobilfunk-Traces [33].

- **Variierende Genauigkeit**: Abhängig vom sozialen Netz können beispielsweise Zeitstempel mit unterschiedlichen Genauigkeiten zugänglich sein. Netz A liefert einen Zeitstempel basierend auf Millisekunden, Netz B nur auf Minutenbasis. Bei der Betrachtung von Geotags kann dies auch innerhalb eines Netzes variieren. Die Arbeit [34] zeigt, dass in Twitterdaten Geotags mit einer bis hin zu acht Nachkommastellen vorkommen könne.

- **Geringe Anzahl der Daten**: Abhängig von der Art der Metadaten kann die Anzahl deutlich unter der Beschränkung der Abfrageschnittstelle liegen. Beispielsweise können Tweets mit Geotags versehen sein, es besitzt jedoch nicht annähernd jeder Tweet ein Geotag. Zum Anteil an geogetaggten Tweets variieren die Angaben sehr stark. Beispielsweise ist in [35] der Anteil mit unter 0,42% angegeben, in [36] mit 1,7% und in [37] mit 2,02%.

- **Großer Zeitraum der Daten**: Der Zeitraum, der durch die Daten abgedeckt wird, resultiert aus dem Verhältnis an der Menge abfragbarer Daten und der Intensität der Nutzerinteraktion. Es gibt Nutzer, die keine Möglichkeit auslassen, um etwas zu teilen und wenn es nur der Musiktitel ist, der gerade bei ihnen läuft. Dies kann auch vollautomatisiert erfolgen, so dass hierfür keine Interaktion mehr notwendig ist. In solchen Fällen sind mehrere hundert Datensätze pro Tag keine Seltenheit. Im Falle von Twitter beispielsweise, mit einem Limit von 3.200 Datensätzen, kann so der beobachtbare Zeitraum auf wenige Tage sinken. Im Gegensatz hierzu veröffentlichen manche Nutzer nur 2-3 Posts am Tag; damit ist eine Zeitspanne von drei Jahren abgedeckt.

- **Immense Anzahl an Nutzern**: Sollen die Profile eines Nutzers identifiziert werden, so müssen alle Profile des zu betrachtenden sozialen Netzes analysiert werden, um sicherzugehen, dass alle Profile gefunden werden. Dies resultiert in einer enormen Menge an Datensätzen, die zum einen die Auswertung verzögern, da jeder einzeln betrachtet werden muss, und zum anderen eine große Herausforderung für die entwickelten Verfahren darstellt, da diese entsprechend präzise differenzieren können müssen.

- **Zusammenhänge der Daten**: Die Zusammenhänge zwischen den verschiedenen Metadaten und den Metadaten aus verschiedenen sozialen Netzen sind weitgehend unerforscht, so dass entsprechende Verfahren entwickelt und evaluiert werden müssen, die eine Zuordnung ermöglichen. Die wenigen Veröffentlichungen, die solche Betrachtungen durchgeführt haben, fokussieren jeweils nur auf Teilaspekte und weisen meist noch weitere Einschränkungen auf. Diese werden im Kapitel 5 im Detail betrachtet und gegen diese Arbeit abgegrenzt.

KAPITEL 3

Szenarien

Die folgenden Abschnitte erläutern Szenarien, in denen das in dieser Arbeit beschriebene Verfahren zur Erkennung und / oder der Identifizierung des Urhebers sinnvoll und gewinnbringend eingesetzt werden kann. Anhand der Szenarien werden im darauffolgenden Kapitel die Anforderungen an das Verfahren zur Profilzuordnung für die unterschiedlichen Anwendungsfälle erarbeitet.

Bei der klassischen Profilzuordnung ist häufig eine monetäre Motivation auszumachen, beispielsweise im Bereich Marketing oder Empfehlungssystemen, eine derartige Motivation steht jedoch bei dieser Arbeit nicht im Vordergrund. Das Ziel der Arbeit ist die sozialen Netze ein wenig sicherer zu machen. Daher werden zwar die Verfahren mitunter an klassischen Profilzuordnungsszenarien demonstriert, aber einer der Mehrwerte soll in der Erkennung und Verhinderung der nachfolgend erörterten Szenarien liegen. Daher werden, da die nachfolgenden Verfahren mangels entsprechender Ground-Truth-Datensätze, nicht direkt evaluiert werden können, zumindest dahingehende und anwendungsbezogene Anregungen gegeben. Nachfolgend werden nun Szenarien vorgestellt, bei denen stets jemand versucht mindestens einer Person "Schaden" zuzufügen.

3.1. Identitätsdiebstahl

Abbildung 3.1 zeigt ein Beispiel von Identitätsdiebstahl in sozialen Netzen. Alice hat in diesem Szenario ein Profil auf Foursquare. Der Identitätsdieb, Mallory genannt, besitzt ein Profil bei Twitter und legt zusätzlich eine Kopie von Alices Profil bei Twitter an. Hierzu meldet sich dieser dort mit einer beliebigen E-Mail-Adresse an und übernimmt alle öffentlich sichtbaren Informationen von Alice.

Typischerweise nimmt dieses Profil auch Kontakt zu den Freunden auf, die Alice bei Foursquare hat, und bittet, die Freundschaftsanfrage zu akzeptieren. Der Angreifer hat nun mehrere Möglichkeiten, weiter zu verfahren. Typischerweise nutzt er entweder den Kontakt zu Alices Freunden, um Nachrichten zu verschicken und Inhalte zu veröffentlichen, die Alices Ruf schaden. Zum anderen kann der Angreifer Social-Engineering-Methoden bei Alices Freunden

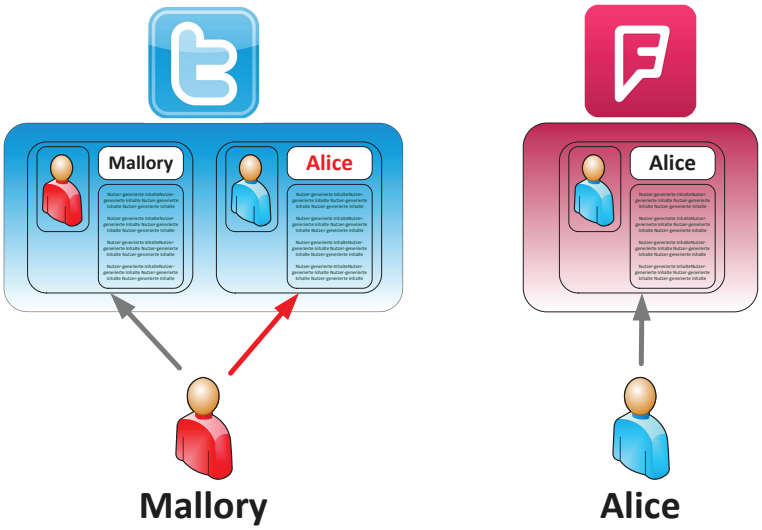


Abbildung 3.1.: Szenario Identitätsdiebstahl

anwenden. Häufig werden diese angeschrieben, dass eine Notlage beispielsweise im Urlaub besteht, weil das Smartphone, sämtliche Dokumente, Geld- und Kreditkarten und Bargeld gestohlen wurde, daher wird Geld benötigt, um wieder nach Hause kommen zu können. Es wird daher meist darum gebeten, mittlere dreistellige Beträge, zum Beispiel über Western Union, dorthin zu senden. Der Angreifer macht sich hierbei zu nutze, dass Alice in ihrem Profil bekannt gegeben hat, dass sie in den Urlaub fährt.

Ziel des in dieser Arbeit vorgestellten Verfahrens ist es, in diesem Szenario nicht das geklonte Profil zu finden, da dies über eine einfache Namenssuche möglich ist, sondern stattdessen den Angreifer, Mallory, zu identifizieren. Hierzu ist es erforderlich, Gemeinsamkeiten zwischen den beiden Profilen unter Mallorys Kontrolle zu detektieren. Da die Profile inhaltlich und im Hinblick auf den Freundeskreis keine Gemeinsamkeiten aufweisen, ist eine Einbeziehung der Profilseite oder der eingestellten Inhalte nicht zielführend. Da hierbei auch ein Straftatbestand vorliegen kann, muss das Ergebnis genau genug sein, um Strafverfolgungsbehörden als Indiz dienen zu können.

3.2. Fake-Profil

In den Abbildungen 3.2 und 3.3 sind die typischen Anwendungsfälle von Fake-Profilen dargestellt.

In Abbildung 3.2 registriert Bob zu seinem eigentlichen Profil ein zusätzliches Fake-Profil. Dieses nutzt er, um Hassreden, Propaganda oder linkes, rechtes, terroristisches oder anderweitig unerwünschtes Gedankengut zu verbreiten. Um hierbei anonym zu bleiben und keine Rückschlüsse auf sich oder sein weiteres Profil zuzulassen, verwendet er zufällige ausgewählte

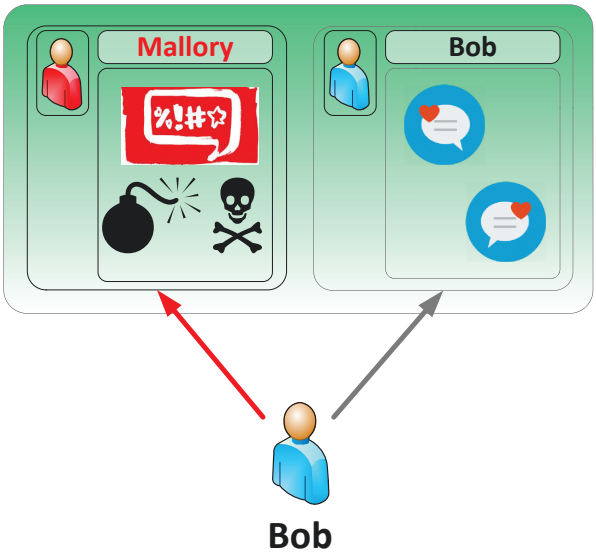


Abbildung 3.2.: Szenario Fake-Profil für Hassreden

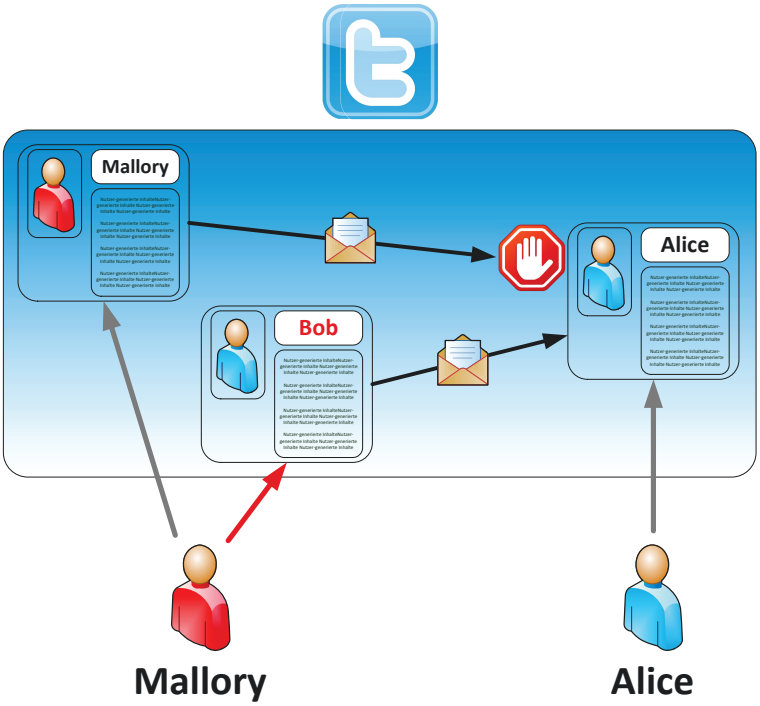


Abbildung 3.3.: Szenario Fake-Profil für Stalking

Namen und Profilattribute. Ohne Analyse des Nutzerverhaltens ist auch hier keine Zuordnung möglich, bedingt durch die nicht existente Schnittmenge der Profilattribute und Freunde.

Eine zweite Variante von Fake-Profilen ist in Abbildung 3.3 dargestellt. Alice hat Mallory geblockt, hierfür kann es verschiedene Ursachen geben, beispielsweise anzügliches Verhalten, unmoralische Angebote oder andere Gründe. Damit Mallory nun weiter Kontakt zu Alice aufnehmen kann und weiterhin Einsicht in ihre Profilseite hat, nutzt er ein Fake-Profil, im Beispiel auf den Namen Bob. In der Kommunikation gibt er sich nicht als Mallory zu erkennen; so hält Alice ihn für einen legitimen Freund. Dies erlaubt es Mallory, Alice weiterhin zu stalken oder zu überwachen, oder die Informationen von ihrem Profil anderweitig gegen sie zu verwenden.

3.3. Botnetze

Die Szenariobeschreibung zu Botnetzen lässt sich ebenfalls in zwei typische Anwendungsbereiche unterteilen, diese sind in den Abbildungen 3.4 und 3.5 dargestellt.

Die erste Abbildung 3.4 zeigt die Verteilung von Spam mittels einer großen Anzahl an Fake-Profilen. Diese werden zentral von Mallory gesteuert, es handelt sich also um ein Spambotnetz. Da der Versand von einer zentralen Instanz gesteuert wird, weisen alle hierzu genutzten Profile das gleiche Nutzungsverhalten auf und können hieran detektiert werden.

Viele Menschen wollen um jeden Preis auffallen; diese Tatsache hat zu einem neuen Geschäftsmodell geführt. Hierbei zahlt ein Nutzer dem Betreiber eines Botnetzes für eine entsprechende Anzahl an Followern bzw. Freunden Geld. Hierfür kommen ähnliche Botnetze wie für den Spamversand zum Einsatz.

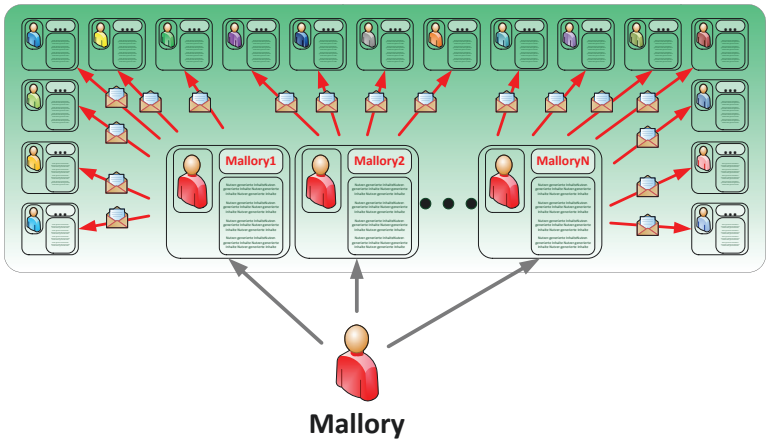


Abbildung 3.4.: Szenario Spamverteilung mittels eines Botnetzes

Im zweiten Anwendungsfall der Botnetzkontrolle, dargestellt in Abbildung 3.5, wird ein Botnetz, beispielsweise für DDoS-Angriffe genutzt. Die Bots sind hierbei auf einer Vielzahl an Rechnern

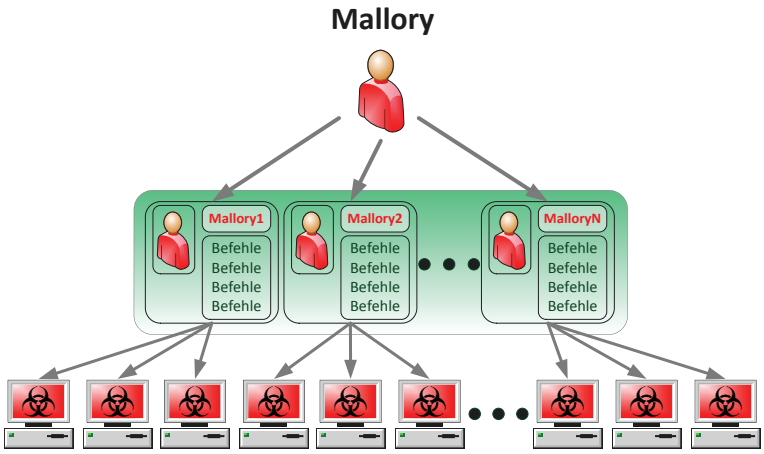


Abbildung 3.5.: Szenario Botnetzkontrolle mittels Profile sozialer Netze

im Internet verteilt. Um keinen auffälligen Datenverkehr zu generieren, der leicht geblockt werden kann, erfolgt die Kommunikation über HTTP oder HTTPS. Hierzu werden bestimmte Profilseiten in sozialen Netzen kontaktiert, da soziale Netze von einer Vielzahl an Nutzern verwendet werden und mehrere IP-Adressen nutzen, ist eine Blockierung der entsprechenden IP-Adressen nicht ohne weiteres möglich.

Mallory verteilt auf den entsprechenden Profilen, die von den Bots in regelmäßigen Abständen kontaktiert werden, neue Befehle an das Botnetz. Hierbei kann es sich um Angriffsbefehle aber beispielsweise auch um den Anstoß eines Updatevorgangs handeln. Um keinen Single Point of Failure zu erzeugen, wird nicht nur ein Profil, sondern es werden diverse genutzt, wobei jeder Bot eine Liste der Profile enthält und zufällig eines auswählt. Wird eine darin definierte Profilseite aufgerufen und festgestellt, dass diese nicht mehr existiert oder anderweitige Probleme beim Aufruf bestehen, wird ein anderes Profil kontaktiert. Diese Profilliste ist über entsprechende Befehle aktualisierbar, daher ist es essentiell, alle Profilseiten gleichzeitig zu entfernen, um das Botnetz lahmzulegen. Dies gelingt mit dem in dieser Arbeit vorgestellten Verfahren: Da alle Profile die gleichen Befehle im gleichen Zeitraum absetzen, weisen diese auch das gleiche, detektierbare Verhalten auf.

KAPITEL 4

Anforderungsanalyse

Im Rahmen dieses Kapitels erfolgt eine Anforderungsanalyse dahingehend welche Anforderungen im Kontext der Profilzuordnung anhand von Metadaten zu berücksichtigen und zu erfüllen sind. Hierunter kann eine Art Anforderungskatalog verstanden werden, der im weiteren Verlauf der Arbeit auf Erfüllung hin überprüft wird.

4.1. Anforderungen an ein Verfahren zur Profilzuordnung

Die nachfolgenden Abschnitte definieren eine Reihe von Anforderungen an das zu entwickelnde Verfahren, die aus den Szenarien und den Zielen dieser Arbeit resultieren.

4.1.1. Keine direkte Nutzerbeeinflussung

Unabhängig davon, ob ein Angreifer ein Profil mit gestohlenen Informationen, ein Fake-Profil oder ein Profil zur Botnetzsteuerung oder Spamversand anlegt, ist davon auszugehen, dass er sämtliche Profilattribute in einer Form wählen wird, die keine Rückschlüsse auf seine wahre Identität zulassen. Aus diesem Grund ist es essentiell, die Zuordnung anhand von Daten vorzunehmen, auf die ein Nutzer keinen direkten Einfluss hat.

Anforderung 1: Keine Nutzung von Profilattributen *Das Verfahren darf aufgrund der Manipulierbarkeit keine Profilattribute für die Zuordnung einbeziehen.*

Zudem wird ein entsprechender Angreifer für das Fake-Profil, abhängig vom Einsatzzweck, keine oder andere Freunde in das Profil aufnehmen. Wenn das Profil beispielsweise für Spamversand gedacht ist, so werden zufällige Fremde ausgewählt und als Freunde hinzugefügt, da die sozialen Netze inzwischen diverse Vorsichtsmaßnahmen getroffen haben und so Profile, die massenweise Nachrichten versenden, aber keine Freunde haben, leicht als Spamversender enttarnen können. Ist das Ziel jedoch die Kontrolle eines Botnetzes, so sind keine Freunde erforderlich, jedoch könnten die Kontrollprofile untereinander Freundschaften schließen, um unauffälliger zu wirken.

Anforderung 2: Keine Nutzung der Netzstruktur *Die Analyse der Netzstruktur bzw. der benachbarten Knoten eines Profils verfälscht für die vorgestellten Szenarien das Ergebnis zum*

schlechteren, da der Angreifer die Freunde und Nachbarn des Profils vollständig frei wählen kann, und darf daher nicht in das Ergebnis einbezogen werden.

Eine Analyse der vom Nutzer eingestellten Inhalte auf typische Muster, beispielsweise des Schreibstils anhand von Worthäufigkeiten oder typischen Schreibfehlern, stellt ebenfalls kein eindeutiges Indiz dar. Die Inhalte können irgendwo kopiert sein, zudem ist die Genauigkeit nur für sehr geringe Nutzerzahlen, kleiner 1.000 praktikabel. Der Berechnungsaufwand ist aufgrund der häufig mehreren 1.000 analysierten Features im Vergleich zum Nutzen sehr hoch. Lediglich für die Erkennung von mehreren Profilen zur Steuerung eines Botnetzes könnte ein solcher Ansatz ein positives Ergebnis liefern, falls die veröffentlichten Befehle in jedem Profil identisch sind. Dies könnte jedoch leicht durch entsprechende Kodierung des Befehls, beispielsweise mittels des Profilnamens, umgangen werden. Ansonsten könnten die Anbieter sozialer Netze solche Profile auch durch eine einfache Datenbankabfrage identifizieren und entfernen, falls durch die Analyse eines Schadprogramms auch nur ein Profil erkannt werden konnte.

Anforderung 3: Keine Textanalysen *Um die Genauigkeit der Ergebnisse hoch und den Berechnungsaufwand gering zu halten, darf ein Verfahren zur Profilzuordnung keine Textanalysen nutzen.*

Werden manipulierbare Attribute oder Daten miteinbezogen, reduziert dies im Falle von Fake-Profilen die Wahrscheinlichkeit einer korrekten Zuordnung. Selbst Benutzernamen von sozialen Netzen stellen keine verlässliche Quelle dar, besonders da manche Netze auch das mehrfache Ändern von Nutzernamen erlauben, siehe [38]. Deshalb ist der vollständige Verzicht auf Daten, die ein Nutzer direkt beeinflussen kann, essentiell für diese Arbeit. Eines der Ziele des in dieser Arbeit vorgestellten Verfahrens ist die Detektion von Spam- und Steuerungsprofilen von Botnetzen. Um diese aufspüren zu können, ist es essentiell, das Verfahren nach der Selektion eines Profils weiterhin auf das gleiche Netz anwenden und weitere entsprechende Profile detektieren zu können. Dies schließt Verfahren die auf Usernamen oder der Netzstruktur basieren aus, da hierbei keine vollständige Übereinstimmung möglich ist.

Anforderung 4: Zuordnung im gleichen Netz möglich *Das Verfahren muss geeignet sein, um geklonte Profile bzw. Profile, die ein identisches Verhalten aufweisen, im gleichen sozialen Netz aufzuspüren.*

4.1.2. Verwendung von Metadaten

Der vorangehende Abschnitt definiert Anforderungen, welche Daten nicht miteinbezogen werden dürfen. Um dennoch eine Profilzuordnung, besonders im Hinblick auf die definierten Szenarien, zu ermöglichen, ist die Auswertung von Metadaten essentiell. Im Gegensatz zu den vorgenannten Profilinformationen kann ein Nutzer zwar beispielsweise beeinflussen, wann er einen Post erstellt, hat jedoch keine Möglichkeit, die Uhrzeit zu manipulieren oder nachträglich zu verändern. Zudem unterliegt ein Nutzer in der Regel einem typischen Tagesablauf, so dass die gezielte Vortäuschung einer anderen Zeitzone oder eines anderen Tagesablaufs bereits an Arbeits- und Schlafzeiten scheitert. Darüber hinaus war bisher eine Zuordnung anhand von

Zeitstempeln nicht möglich, so dass sich ein Nutzer auch nicht bewusst ist, dass er dennoch anhand dieser Daten identifiziert werden kann.

Anforderung 5: Nutzung von Zeitstempeln *Aufgrund der nachträglichen Unveränderbarkeit und des nur bedingt frei wählbaren Zeitpunktes der Erstellung, stellen Zeitstempel, als eine Art von Metadaten, eine geeignete Information zur Zuordnung von Profilen dar und sind hierfür zu nutzen.*

Eine weitere Art an Metadaten, Geotags, erlauben vielfältige Rückschlüsse, beispielsweise durch die Ortsbestimmung oder die Genauigkeit, die Endgeräte-spezifisch ist, und stellen daher eine wichtige Informationsquelle aus dem Bereich der Metadaten dar. Diese werden vom Endgerät direkt an das soziale Netz übertragen, ohne dass ein Nutzer Einfluss auf die übertragenen Werte nehmen könnte. Er kann lediglich den Versand von Geotags unterbinden, diese jedoch nicht manipulieren.

Anforderung 6: Nutzung von Geotags *Geotags liefern verschieden Merkmale, die auch als Ausschlusskriterium für verschiedene Aspekte genutzt werden können, daher ist deren Nutzung essentiell.*

Darüber hinaus existieren verschiedene Metadaten, die von sozialem Netz zu Netz variieren können. Eine Auswertung dieser Daten kann die Ergebnisse signifikant verbessern.

Anforderung 7: Einbeziehung weiterer Metadaten *Soweit ein soziales Netz weitere Metadaten zur Verfügung stellt, sind diese in die Auswertung miteinzubeziehen.*

4.1.3. Daten öffentlich zugänglich

Das in dieser Arbeit entwickelte Verfahren soll es jedem erlauben zu prüfen, inwiefern die eigenen Profile korrekt einem selbst zugeordnet werden können. So kann jeder Nutzer prüfen, wie durchschaubar seine Verwendung sozialer Netze ist und hat eine Einsicht, welche Daten innerhalb kürzester Zeit über ihn aggregiert werden können. Kapitel 12 bietet für diese Nutzer Empfehlungen, um solche Zuordnungen zu erschweren.

Öffentlich zugänglich bedeutet im Kontext dieser Arbeit, dass eine Anmeldung bei dem entsprechenden sozialen Netz erforderlich sein darf, nicht jedoch beispielsweise eine akzeptierte Freundschaftsanfrage, um ein Profil einsehen zu können. Zum einen müssten massenhaften Freundschaftsanfragen verschickt werden und dies unter Vorspiegelung falscher Tatsachen, um das Gegenüber zu bewegen, diese auch zu akzeptieren. Zum anderen würde ein solches Verfahren keine effiziente Abfrage ermöglichen, wenn stets auf die Akzeptanz dieser Meldungen gewartet werden müsste.

Auch die Nutzungsbedingungen vieler sozialer Netze verbieten den exzessiven Versand von Nachrichten, zu denen auch Freundschaftsanfragen gehören. Um nicht gegen diese zu verstoßen, beschränkt sich die Arbeit auf öffentlich zugängliche Daten. Zudem wird ein Versuch, mit-

tels vorgenannter Weise massenhaft Daten abzugreifen, gewöhnlich automatisiert verhindert, da diverse Schwellwerte typischen Nutzerverhaltens deutlich überschritten werden, und der hierfür verwendete Zugang gesperrt.

Anforderung 8: Nutzung öffentlich zugänglicher Daten *Ein Versuch der massenhaften Datenausleitung von geschützten Profildaten aus einem sozialen Netz verstößt in mehreren Punkten gegen deren Nutzungsrichtlinie, daher dürfen für das Verfahren keine geschützten Informationen notwendig sein.*

Um die Schnittstellen der Netze nutzen zu können, die eine Abfrage von Daten ermöglichen, ist eine Anmeldung erforderlich. Da jedoch kein Nutzer behelligt oder auch nur über die Abfrage informiert wird, werden die auf diesem Wege erhaltenen Daten als öffentlich zugänglich angesehen.

4.1.4. Skalierbarkeit

Die Größe heutiger sozialer Netze erfordert ein stark skalierbares Verfahren. Zum einen darf die Komplexität eines einzelnen Vergleichs zwischen zwei Profilen nicht zu hoch, zum anderen sollte eine parallele Abarbeitung möglich sein.

Verfahren des maschinellen Lernens sind aufgrund ihrer Komplexität ungeeignet. Zudem müssten diese für jeden Nutzer, dessen Profile ermittelt werden sollen, einzeln trainiert werden, da das Nutzungsverhalten eines jeden Menschen zu variabel ist, um dies generisch abbilden zu können. Des weiteren benötigen Verfahren des maschinellen Lernens eine Vielzahl an Datensätzen für das Training. Der Startpunkt des Profilzuordnungsverfahrens besteht jedoch aus einem einzelnen Profil, zu dem weitere gefunden werden sollen, so dass ein effektives Training nicht möglich ist.

Der Einsatz von Klassifikatoren scheidet aufgrund der vorgenannten Aspekte ebenfalls aus. Das Ergebnis eines Klassifikators mag im Durchschnitt gute Ergebnisse erzielen, bei der Betrachtung einzelner Nutzer ist das Ergebnis jedoch nie optimal, da die Optimierung anhand aller Nutzer erfolgt ist.

Anforderung 9: Keine Klassifikatoren *Ein Einsatz von Klassifikatoren und anderen Methoden des maschinellen Lernens, ist für einzelne Nutzer betrachtet nie optimal und daher darf kein solches Verfahren bei der Profilzuordnung zum Einsatz kommen.*

4.1.5. Auswertung

Für die Auswertung werden verschiedenste Analysen und Eigenschaften von Metadaten und Profilen ausgewertet. Aus diesem Grund muss für die Entscheidungsfindung eine Gewichtung erfolgen, da einzelne Aspekte entscheidender und aussagekräftiger sind als andere. Diese Gewichtung kann dabei entweder statisch oder in Abhängigkeit eines der ausgewerteten Parameter erfolgen.

Anforderung 10: Gewichtung *Die Aggregation der Ergebnisse verschiedener Analysen wird abhängig von der Aussagekraft der einzelnen Aspekte zur Erzielung genauerer Resultate gewichtet.*

Die verschiedenen, ausgewerteten Aspekte werden nicht nur einzeln, sondern auch kombiniert betrachtet. Beispielsweise lassen sich zusätzliche Schlüsse ziehen, wenn Geotags und Zeitstempel nicht nur einzeln, sondern zusätzlich auch kombiniert analysiert werden.

Anforderung 11: Kombinierte Auswertung *Es werden nicht nur Einzelbetrachtungen der Aspekte durchgeführt, sondern diese zusätzlich auf gewinnbringende Kombinationsmöglichkeiten überprüft und diese in die Auswertung miteinbezogen.*

4.1.6. Verlässlichkeit

Aufgrund der Art der detektierbaren Profile, beispielsweise Fake-Profile, Profile zur Steuerung von Bots oder auch Spambot-Profile, ist eine hohe Verlässlichkeit essentiell. Wenn entsprechende Profile erkannt und dem sozialen Netz gemeldet werden, muss ausgeschlossen sein, dass Profile unbeteiligter Nutzer gelöscht oder anderweitig in Mitleidenschaft gezogen werden. Auch rechtliche Schritte sind beispielsweise aufgrund von mit Fake-Profilen begangenen Straftaten denkbar; hierbei muss sichergestellt sein, dass kein unbeteiligter Dritter in Rechtsstreitigkeiten verwickelt wird. Zum einen träfe es den Falschen, zum anderen könnte der Täter gewarnt werden und seine Spuren verwischen. Eine rechtliche Betrachtung dieser Aspekte kann aufgrund mangelnder Expertise im juristischen Bereich in dieser Arbeit nicht erfolgen.

Aufgrund der ausgewerteten Merkmale bzw. Metadaten der Profile ist die Auswertung für Menschen schwer nachzuvollziehen, da diese sich vorwiegend auf Profilattribute, Fotos oder Freunde konzentrieren würden. Daher muss das Ergebnis genau genug sein, dass keine Nachprüfung bzw. Verfeinerung durch einen Nutzer des Systems erforderlich ist.

Anforderung 12: Keine Verfeinerung notwendig *Für diese Arbeit wird die Anforderung so definiert, dass die korrekte Zuordnung in der Top-10-Trefferliste enthalten sein muss.*

Um die Ergebnisse, aufgrund der möglichen Verschiedenartigkeit im Hinblick auf Profilattribute, Fotos und Freunde zu verifizieren, ist die Nutzung eines Ground-Truth-Datensatzes unerlässlich. Ansätze, die dies nicht gewährleisten, ordnen mit großer Wahrscheinlichkeit Profile, die Teil eines Identitätsdiebstahls sind, dem tatsächlichen Profil des Opfers zu. Dies würde den Identitätsdiebstahl weiter verschleiern und das Profil als legitim verifizieren, obwohl es von einem Angreifer kontrolliert wird. Dies würde dem Angreifer in die Hände spielen und sollte unbedingt vermieden werden.

Anforderung 13: Evaluation mit Ground-Truth-Datensatz *Um die Verlässlichkeit und Genauigkeit zu zeigen und Falschzuordnungen erkennen zu können, ist für die Evaluation ein Ground-Truth-Datensatz heranzuziehen.*

Soziale Netze wie Twitter oder Instagram haben heutzutage Nutzerzahlen im dreistelligen Millionenbereich oder Facebook sogar im Milliardenbereich. Daher ist es essentiell notwendig, dass das erarbeitete Verfahren entsprechend gut skaliert, um auch bei solchen Nutzerzahlen noch verlässliche Ergebnisse zu erzielen.

Anforderung 14: Evaluation mit Datensatz realistischer Größe *Das Verfahren muss entsprechend skalierbar sein, daher wird zur Evaluation ein Datensatz mit mindestens 10^7 Nutzern verwendet.*

4.2. Kategorisierung

Die in den vorigen Abschnitten definierten Anforderungen lassen sich in drei Kategorien einteilen. Forderungen an die zu verwendenden Daten, die zu implementierende Architektur und die Evaluation. Die Anforderungen aus den zu verwendenden Daten basieren auf den Erfordernissen zur Zielerreichung der Szenarien. Die zu implementierende Architektur betreffenden Punkte ergeben sich aus der Notwendigkeit, große Profilmengen verarbeiten und dennoch ein genaues Ergebnis erzielen zu können. Anforderungen an die Evaluation stellen sicher, dass das Verfahren hält, was es verspricht, die Ergebnisse also entsprechend verlässlich sind und die Falsch-positiv-Rate gleich oder nahe Null ist.

Tabelle 4.1.: Kategorisierung der Anforderungen

	Daten
1	Keine Nutzung von Profilattributen
2	Keine Nutzung der Netzstruktur
3	Keine Textanalysen
4	Zuordnung im gleichen Netz möglich
5	Nutzung von Zeitstempeln
6	Nutzung von Geotags
7	Einbeziehung weiterer Metadaten
8	Nutzung öffentlich zugänglicher Daten
	Architektur
9	Keine Klassifikatoren
10	Gewichtung
11	Kombinierte Auswertung
12	Keine Verfeinerung notwendig
	Evaluation
13	Evaluation mit Ground-Truth-Datensatz
14	Evaluation mit Datensatz realistischer Größe

4.3. Zusammenfassung

In diesem Kapitel wurden Anforderungen an ein Verfahren zur Profilzuordnung definiert. Grundlage hierfür sind die verschiedenen Szenarien, in denen das Verfahren gewinnbringend eingesetzt werden kann. Die Anforderungen entfallen auf drei Kategorien, an die zu verwendenden Daten, die die Eignung der verschiedenen Profildaten betreffen, die zu implementierende Architektur, die eine entsprechend umfangreiche Analyse und eine stark reduzierte Ergebnismenge liefert, und die Evaluation, um die Funktionsweise und die Verlässlichkeit zu zeigen.

KAPITEL 5

Stand der Technik

Soziale Netze stehen seit ihrem Aufkommen im Mittelpunkt der Forschung. Sie ermöglichen die Analyse und Auswertung der Daten von Millionen von Nutzern und erlauben so Schlussfolgerungen, die nicht nur lokale, sondern auch internationale oder globale Gültigkeit besitzen.

In diesem Kapitel wird der aktuelle Stand der Forschung im Bereich sozialer Netze und, im Speziellen, im Gebiet der Profilzuordnung zu einem Nutzer betrachtet. Artverwandte Themen, beispielsweise die Privatsphäre betreffend oder den Bereich der Botdetektion, die ebenfalls Gegenstand dieser Arbeit sind, werden ebenfalls beleuchtet.

5.1. Soziale Netze

Boyd und Ellison [1] definieren in ihrer Arbeit den Begriff des sozialen Netzes, siehe hierzu auch Kapitel 1, und geben einen historischen Überblick über die Entwicklung und Gründungsdaten bekannter Netze. Viele Personen unterstellen der Nutzung von sozialen Netzen einen negativen Einfluss auf die Entwicklung von Jugendlichen oder generell eine schädliche Auswirkung auf die sozialen Kompetenzen aller Vielnutzer. Die Studien [39] [40] zeigen jedoch, dass das Gegenteil der Fall ist. Es wurden Studenten untersucht, die in nicht unerheblichem Maße Facebook genutzt haben. Das Ergebnis ist, dass sich die Nutzung des sozialen Netzes auf die Zufriedenheit, das gesellschaftliche Engagement und die politische Teilnahme dieser Studenten positiv ausgewirkt hat.

5.1.1. Analyse, Messung und Überwachung

Neben mehreren Büchern, die sich allgemein mit der Analyse von sozialen Netzen befassen [41] [42], existieren diverse Arbeiten, die sich auf einzelne Netze und bestimmte Aspekte fokussieren. Beispielsweise [43] [44] [45] [46] [47] [48] analysierten Twitter, [49] [50] [51] Facebook, [52] [53] [54] [55] Foursquare oder andere Netze [56]. Darüber hinaus gibt es Arbeiten, die ihre Erkenntnisse aus dem Vergleich mehrerer Netze gewinnen. Benevenuto et al. [57] analysiert das Nutzerverhalten in sozialen Netzen, darunter Hi5, LinkedIn, MySpace and

Orkut. Ihre Arbeit eröffnet Einblicke, wie oft und wie lange Leute mit den Netzen verbunden sind und welche Aktivitäten und Abfolgen ein Nutzer dort typischerweise ausführt. In [58] kombinieren die Autoren zwei Datensätze aus sozialen Netzen, von Youtube und Twitter, um ein Gesamtbild zu erstellen, wer welche Videos anschaut und dies auf Twitter teilt. Lucia, Akcora und Ferrari [59] analysierten das Gesprächsverhalten in Twitter und Facebook und stellten fest, dass die Like- bzw. Retweet-Rate von der Geoposition des Erstellers eines Posts abhängt. Die Arbeit [60] analysiert sechs verschiedene soziale Netze hinsichtlich zeitlichem und thematischem Teilungsverhalten. Fang und Chang [61] analysieren anhand von zeitlichen und räumlichen Signalen die Möglichkeit der Zuordnung zwischen dem Inhalt eines Tweets und einer oder mehrerer Entitäten, die einen Eintrag bei Wikipedia besitzen beispielsweise Sehenswürdigkeiten.

Meinungs- und Trenderkennung

Der Bereich der Meinungs- und Trenderkennung wurde ausführlich untersucht. Bing Liu gibt in seiner Arbeit [62] eine Einführung und umfangreichen Überblick über die Techniken und Möglichkeiten von Sentiment-Analysen und Meinungserkennung. Pak und Paroubek [63] zeigen, wie für Sentiment-Analysen durch das automatische Sammeln von Twitter-Daten ein geeigneter Korpus zustande kommt. Dieser wurde aus sprachlicher Sicht untersucht und die Ergebnisse präsentiert. In [64] wird ein Meinungsbildungs-Rahmenwerk präsentiert, welches sich aus drei Bausteinen zusammensetzt. Der automatischen Themen-, Emotions- und Meinungserfassung, Agenten-basierten Simulation und Informationsflussmodellierung und der Modellierung von Meinungsnetzen. Bodendorf und Kaiser präsentieren in ihrer Arbeit [65] basierend auf Analysen sozialer Netze und Texten ein Verfahren zur Identifikation von Meinungsführern und Meinungstrends, um das Prinzip der Meinungsbildung besser zu verstehen.

TwitterMonitor [66] ist ein System zur Trenderkennung in Twitter. Das System identifiziert Trends in Echtzeit und bietet zusätzlich eine Beschreibung der Themen. Hotho et al. [67] beschreiben das Problem der Datenflut und, dass viele diesem Problem mit sozialen Lesezeichen Tools begegnen. Die Nutzer dieser Werkzeuge definieren ihre eigenen Strukturen, eine Volks-Taxonomie oder Folksonomy genannt. Die Autoren stellen basierend auf einem adaptierten PageRank-Algorithmus einen Ansatz der Trenderkennung in diesen Folksonomies vor. In [68] werden Techniken und Methoden zur Erkennung und Identifikation von Trends in Streaming-Daten betrachtet und untersucht.

Ereigniserkennung

Weng, Yao, Leonardi und Lee [69] betrachten in ihrer Arbeit ausführlich die Erkennung von Ereignissen im Twitter-Datenstrom. In [70] wird ein Verfahren zur Ereigniserkennung basierend auf Netzen von Schlüsselwörtern und bekannter Erkennungsmethoden aus dem Bereich der Sozialen-Netz-Analyse vorgeschlagen. Die Arbeiten [5] [71] betrachten die Erkennung von Erdbeben anhand von Twitter-Streaming-Daten. Dies ermöglicht eine Erkennung in Echtzeit. Jain et al. [72] konzentrieren sich auf zeitliche Aspekte des Tweeting-Verhaltens und setzen diese in

Bezug zu aufkommenden Themen in Twitter. Die Autoren nehmen an, dass Nutzer von ihrem typischen Nutzungsverhalten abweichen, wenn ein wesentliches Ereignis auftritt. Tweets von Nutzern, die zu einer bestimmten Zeit typischerweise nicht twittern, erhalten so mehr Gewicht bei einem aufkommenden Thema.

Vorhersagen

Dominguez et al. versuchen in ihrer Arbeit [73], das Datenstromvolumen bzw. die Anzahl der darin enthaltenen Tweets von Twitters Samplestream durch die Nutzung von künstlichen neuronalen Netzen vorherzusagen. Zusätzlich wird ein Modell vorgeschlagen, um die Anzahl der Tweets in einem bestimmten Zeitfenster zu prognostizieren. Die Veröffentlichung [74] untersucht die Vorhersagefähigkeit durch die Erfassung von Nutzerverhalten, indem diese als Computereinheiten, die Informationen verarbeiten, modelliert werden. Hierzu werden zwei gegensätzliche Modellierungsparadigmen angewendet und evaluiert. In [75] analysieren Song et al. SINA Weibo, das bekannte chinesische soziale Netz. Dieses bietet unter anderem die gleichen Funktionalitäten wie Twitter. Die Autoren versuchen in der Arbeit vorherzusagen, ob eine Nachricht weitergeleitet, was bei Twitter geretweetet heißt, wird oder nicht.

Asur und Huberman [76] nutzen das Geschwätz von Twitter, um die Kasseneinnahmen für Filme vorauszusagen. Die Autoren zeigen, dass ein einfaches Modell basierend auf der Rate mit der Tweets zu bestimmten Themen erstellt werden, marktbasierte Prädiktoren übertreffen. Die Arbeiten [8] [77] betrachten darüber hinaus die Vorhersagbarkeit des Aktienmarktes anhand der Stimmung in Twitter.

Geotags und ortsbasierte soziale Netze

Bei Geotags handelt es sich um Metainformationen, daher erfolgt an dieser Stelle ein kurzer Abriss von Arbeiten, die sich mit Geotags, aber auch mit ortsbasierten Analysen und Verfahren auseinandersetzen. Die Arbeit [78] verwendet geogetaggte Tweets aus der Gegend von Seattle über einen Zeiraum von zwei Monaten und zeigt Möglichkeiten der bildlichen Analyse anhand von zeitlichen und örtlichen Aspekten. Das Kleine-Welt-Phänomen [79] wird in der Arbeit [80] mit Blick auf die Möglichkeiten und Eigenschaften sozialer Netze betrachtet. Darüber hinaus analysieren die Autoren beispielsweise die durchschnittlichen Distanzen zwischen Freunden. Eine umfangreiche Studie zur visuellen Analyse des Bewegungsverhaltens von Foursquare-Nutzern wurde in [81] durchgeführt. In [82] wird ein Clustering-Verfahren vorgestellt, welches anhand von semantischen Annotierungen Gegenden und Nutzer in Gruppen einteilt. Anhand des Inhalts von Tweets wird in der Arbeit [83] versucht, den Aufenthaltsort des Nutzers zu bestimmen. Scalleto et al. [84] präsentieren in ihrer Arbeit einen graphbasierten Ansatz, um soziale Netze mit Ortsinformationen zu untersuchen. Darüber hinaus werden Metriken vorgestellt, die charakterisieren wie geographische Distanzen soziale Strukturen beeinflussen. In [85] zeigen die Autoren ein Hidden-Markov-basiertes Modell, um Tweetinhalte und Nutzerbewegungen für das Geotagging zusammenzuführen. Naoto et al. [86] schlagen ein Verfahren vor bei dem der Postingort eines Tweets als Feature für die Analyse von Nutzerklassen herangezogen wird. Mai Ren untersucht in ihrer Masterarbeit [87] die

Auswirkungen der Standortmanipulation auf ortsbasierte soziale Netze.

Weitere Arbeiten zu diesem Themenbereich sind [88] [89] [90] [91] und [92]. Des weiteren behandeln diverse Veröffentlichungen das Thema ortsbasierter sozialer Netze, beispielsweise [93] [94] und [95].

5.1.2. Schlussfolgern zusätzlicher Daten

In [96] zeigen die Autoren, wie anhand von Informationen aus dem Internet Profile sozialer Netze rekonstruiert werden können. Hierzu wurden zufällig ausgewählte Profile aus Twitter gecrawlt, Daten im Internet gesucht und aggregiert und anschließend mit dem ursprünglichen Twitter-Profil abgeglichen. Mislove et al. [97] schlussfolgern nicht hinterlegte Attributinformationen eines Profils. Hierzu werden anhand der Graphstruktur eines Netzes die Attribute der Freunde betrachtet und anhand dieser auf die fehlenden Informationen geschlossen. In den Arbeiten [98] [99] [100] [101] [102] [103] werden Standort, Wohnort oder Herkunftsorte mithilfe verschiedener Verfahren geschlussfolgert. Die Veröffentlichungen [104] [105] schließen auf zukünftige Bewegungsziele, nutzen hierfür jedoch keine Daten sozialer Netze, sondern basieren auf GPS-Daten. In [106] und auch von anderen Autoren in [107], letztgenannte Arbeit wurden zudem in [108] fortgesetzt, werden fehlende Attribute durch Einbeziehen der Attribute von Freunden und anhand des Verhaltens eines Nutzers geschlussfolgert. Laut Autoren im Gegensatz zu früheren Verfahren, wo nur jeweils eine der beiden Quellen herangezogen wurde. Alekseev et al. versuchen in ihrer Arbeit [109] zunächst das Interesse eines Nutzers für ein Themenfeld zu messen. Im nächsten Schritt werden Vorhersagen hinsichtlich Alter und Geschlecht von Nutzern evaluiert. Vorhersagen zu Freundschaften und Beziehungen werden in [110] anhand von Bewegungsprofilen vorgenommen.

5.2. Profilzuordnung

Dieser Abschnitt behandelt den Stand der Technik der Profilzuordnung in sozialen Netzen. Die folgenden Unterpunkte gliedern die Arbeiten in die verwendeten Verfahren. Verfahren die generierte Inhalte (wie Tags, Fotos, etc.) miteinbeziehen, werden hier im Bereich der Attributübereinstimmung verortet. Ein Vergleich der nachfolgend vorgestellten Verfahren mit dieser Arbeit erfolgt in den Tabellen 5.1 bis 5.4.

Die Arbeit [111] nutzt die von Foursquare bereitgestellte Funktion, mit der Nutzer auf ihre Profile in anderen sozialen Netzen verweisen können, und untersucht die Konsistenz der verfügbaren Informationen zwischen diesen Profilen. In [112] machen die Autoren darauf aufmerksam, dass es schwer ist an Ground-Truth-Daten zu gelangen, da alte Datensätze zum einen entweder nicht mehr verfügbar sind oder aber nicht mehr die notwendige Relevanz besitzen und auch aus datenschutzrechtlichen Überlegungen kritisch sind. Daher schlagen die Autoren ein Sampling Verfahren zur Generierung entsprechender Testdatensätze für Profilzuordnungsansätze vor und evaluieren dieses. Kaushal et al. untersuchen in [113] den Einfluss des Nutzerverhaltens auf Datensätze für maschinelles Lernen. Hierzu wurde mittels

Ground-Truth-Daten beispielsweise Abweichungen in Nutzer- und Displaynamen untersucht.

Anforderungen an verlässliche Profilzuordnungsverfahren, insbesondere im Hinblick auf soziale Netze mit mehreren Hundertmillionen Nutzern, werden in [114] betrachtet und hergeleitet. Das Themenfeld der Profilzuordnung wird in [115] umfassend analysiert. Beginnend bei State-of-the-Art Algorithmen, über Bewertungsmethoden, bis hin zu repräsentativen Datensätzen. Dabei werden auch verwandte Forschungsthemen, offene Probleme und zukünftige Forschungsschwerpunkte diskutiert. Eine zweite Arbeit die ebenfalls einen sehr umfassenden Blick auf das Thema der Profilzuordnung wirft und auch ähnliche Schwerpunkte setzt ist [116]. Eine kurze Übersicht über Techniken der Profilzuordnung ist darüber hinaus in [117] zu finden. Eine sehr umfassendes Review hat zudem Kaushal im Rahmen seiner Dissertation erstellt, siehe [118].

5.2.1. Attributübereinstimmung

Zafarani und Liu [119] ordnen Profile über verschiedene Webseiten zu. Dies erfolgt allein anhand der Benutzernamen. Die Autoren zeigen mit ihrer Arbeit, dass diese hierfür geeignet sind. Eine weitere Arbeit [120] ordnet Profile einzig anhand von Benutzernamen zu. Neben weiteren Aspekten analysieren die Autoren verschiedene Verfahren zum Überprüfen von Strings auf Ähnlichkeit. Darüber hinaus werden auch Gegenmaßnahmen diskutiert. In [121] werden diverse Profilinformationen für die Identifizierung weiterer Profile genutzt. Hierzu bedienen sich die Autoren eines Klassifizierungsverfahrens und verwenden eine variierende Gewichtung in Abhängigkeit der betrachteten Attribute. Eine umfangreiche Betrachtung von Ähnlichkeitsmetriken für Strings und Semantiken erfolgt in [122]. Darüber hinaus wurde auch eine unterschiedliche Gewichtung von Attributen analysiert. Eine Kombination aus Profilattributen und der Netzstruktur wird in [123] zur Profilzuordnung vorgeschlagen. Der Beitrag der Arbeit besteht jedoch hauptsächlich aus einer Methode zum Schließen auf fehlende Attribute. Soltani und Abhari [124] nutzen Ähnlichkeitsmaße, Onlinedienste und eine Gewichtung der Attribute um Profile zuzuordnen. Abhängig vom Typ der Daten, persönliche Identitäten, soziale Identitäten und relationale Identitäten, werden die Ähnlichkeitsmaße und die API Aufrufe ausgewählt. Eine umfassende Prüfung von Ähnlichkeitsmetriken für Profilattribute wurde in [125] durchgeführt. Dies schließt Levenshtein, Jaro Winkler, Jaccard, Soundex und weitere Ähnlichkeitsmaße mit ein. Eine ähnliche Betrachtung von Ähnlichkeitsmetriken für Strings wird in [126] präsentiert. Eine tiefgreifendere Prüfung erfolgt in [127]. Zusätzlich erfolgt eine Gewichtung der Attribute um eine effektivere Zuordnung zu erzielen. Hierzu wird jedes Attribut betrachtet und eine subjektive Gewichtungsmethode darauf angewendet. In [128] versuchen die Autoren ebenfalls anhand von Profilinformationen Profile zuzuordnen. Bedingt durch die sehr kleinen Datensätze mit nur wenigen Hundert Profilen sind die Erbebnisse jedoch kaum übertragbar. Kaushal et al. [129] präsentieren fünf Methoden für die Profilzuordnung. Diese stützen sich jedoch nahezu ausschließlich auf den verfügbaren Profilinformationen ab. Methoden zur Profilzuordnung mittels Klassifikator werden in [130] und [131] vorgestellt, in [132], [133] oder [134] auch, beschränken sich aber lediglich auf die Nutzernamen und ggf. Displaynamen. Ein entsprechende Frameworks für unüberwachte Profilzuordnung mit und ohne Klassifikation werden in [135] bzw. [136] vorgestellt. Eine Arbeit die die Ähnlichkeiten zwischen Profilinformationen analysiert und für Profilzuordnung nutzbar

macht, aber noch keine Evaluation enthält, wird in [137] präsentiert. Sokhin et al. [138] schlagen ein Profilzuordnungsverfahren ausschließlich basierend auf den frei zugänglichen Bildern der Nutzer vor. Das Themenfeld der Profilattribute und der entsprechenden Möglichkeiten der Profilzuordnung damit, werden detailliert in der Dissertation von Frau Paridhi Jain beleuchtet, siehe [139]. Kojima et al. [140] errechnen für die Profilzuordnung die Ähnlichkeiten in der räumlichen Verteilung der Freunde gemäß deren Profilinformation. Evaluation erfolgt mit sehr kleinem Datensatz.

Weitere Arbeiten und Verfahren zur Zuordnung von Profilen anhand von Profilattributen wurden in [141] [142] [143] [144] [145] [146] [147] [148] [149] [150] [151] [152] und [153] betrachtet. Alle referenzierten Arbeiten in diesem Abschnitt werden in Tabelle 5.1 einander gegenüber gestellt.

5.2.2. Netzstruktur

Eine der meistzitierten Arbeiten dieser Kategorie ist [154]. Anhand der Behauptung der Autoren und aufgrund des Erscheinungsjahres ist davon auszugehen, dass dies die erste Veröffentlichung war, die Profile anhand der Netzstruktur zugeordnet hat. Zusätzlich ist eine umfangreiche Zusammenfassung ähnlicher Techniken enthalten. Allerdings ist die Ground-Truth des verwendeten Datensatzes nicht gegeben oder nur mit Einschränkungen, da hierfür eine von den Autoren selbst gewählte Abbildung zwischen den Daten zweier Netze verwendet wird. Verschiedene Algorithmen zur Zuordnung der Netzstruktur zweier sozialer Netze wurden in [155] evaluiert. Die Arbeit [156] betrachtet die Möglichkeit die in der Forschung meist eingesetzten anonymisierten Datensätze von sozialen Netzen einander anhand der Netzstruktur zuzuordnen und stellt ein entsprechendes Verfahren vor. Die Netzstruktur wird ebenfalls in [157] genutzt, um Profile zuzuordnen. Zudem präsentiert die Arbeit einen Ansatz, um bei Nutzern ein Bewusstsein für diese Art von Informationsgewinnung zu wecken. In [158] wird ein Graph-basierter Ansatz für die Profilzuordnung genutzt mit dem Ziel eine Suchmaschine für die Nutzeridentifizierung zu entwickeln. Tang et al. [159] und [160] versuchen mit zwei verschiedenen Verfahren Vorhersagen hinsichtlich Beziehungen verschiedener Nutzer untereinander vorherzusagen. Ein Ansatz zur Identifizierung von Accountpaaren die einem Betrüger gehören wird in [161] vorgestellt. Hierzu wird ein Graph-basiertes Profilzuordnungsverfahren entwickelt. Im Gegensatz zu vielen Verfahren wo ein Wissen über eine Menge initialer Profilpaare erforderlich ist, wird in [162] und [163] ein unüberwachtes Verfahren vorgestellt, welches dieses initiale Wissen nicht benötigt. In [164] wird ein Verfahren vorgestellt, welches sich die Nähe zwischen den Nutzern und ihren Freunden zu Nutze macht. Diese Nähe wird dabei anhand von Aufmerksamkeitsmechanismen der sozialen Netze errechnet. Ein zwei-stufiges Verfahren zur Profilzuordnung wird in [165] vorgeschlagen. Zunächst werden die Netze geclustert und Ähnlichkeiten errechnet und erst danach wird versucht Nutzer zwischen zwei Clustern zuzuordnen. Liu et al. [166] schlagen ein drei-stufiges Verfahren vor, um ähnliche Gruppen in sozialen Netzen zu identifizieren. Dabei kommen zunächst Random Walks zum Einsatz, gefolgt von der Extraktion von Ähnlichkeits-Features und dem ermitteln der Gruppenähnlichkeit. Bei den Graph-basierten Profilzuordnungsverfahren kommen des weiteren verschiedenste Ansätze zum Einsatz wie ein Random Forest Klassifikator

[167], Graph-basierte neuronale Netze [168] und [169], Community-erhaltende Netzeinbettung [170], neuronalen Tensornetzwerken [171], einem Deep-Learning Ansatz [172], einem Deep-Reinforcement-Learning Ansatz [173], einem Algorithmus zur lokalen Expansionsausbreitung [174] und ein Ansatz mit Nutzung der Einflüsse der Nachbarn innerhalb eines Netzes und Netz-übergreifend [175].

Weitere Arbeiten und Verfahren zur Zuordnung von Profilen anhand der Netzstruktur wurden in [176] [177] [178] [179] [180] [181] [182] [183] [184] [185] [186] betrachtet. Alle referenzierten Arbeiten in diesem Abschnitt werden in Tabelle 5.2 einander gegenüber gestellt.

5.2.3. Textanalyse

Das in [187] vorgestellte Verfahren basiert größtenteils auf Textanalysen, dennoch wird zusätzlich ein Profilattribut ausgewertet, nämlich die User-ID. Die Autoren versuchen, Nutzer anhand ihres Tagging-Verhaltens und ihrer User-IDs zu identifizieren. Trotz guter Evaluationsergebnisse ist das Verfahren nicht repräsentativ aufgrund einer geringen Anzahl an ausgewerteten Datensätzen. Narayanan et al. [188] liefern einen Beitrag zur Identifizierung von Autoren. Verschiedene Klassifikatoren werden betrachtet und evaluiert. Für jeden Text werden 1.188 Merkmale für die Klassifikation extrahiert, der Text selbst wird nicht weiter analysiert. Novak, Raghavan and Tomkins [189] nutzen die Verteilungen von Worten, Rechtschreibfehlern, Satzzeichen und Emoticons als Merkmale. Profile werden anhand dieser Merkmale mittels Clustering-Verfahren in aussagekräftige Gruppen eingeteilt. In der Arbeit [190] erfolgt eine Zuordnung von Profilen zwischen Flickr und del.icio.us. Hierzu werden Tags und Tag Clouds der Nutzer analysiert und anhand des Tagging-Verhaltens zugeordnet. In [191] wurde eine umfangreiche Studie zur Profilzuordnung anhand von Textanalysen durchgeführt. Hierzu wurden verschiedene Features definiert und in mehreren Schritten die Größen der analysierten Datensätze erhöht.

5.2.4. Kombinationen

Goga betrachtet in ihrer Arbeit [192] die verschiedenen Möglichkeiten, Profile aus verschiedenen sozialen Netzen einem Nutzer zuordnen zu können. Dabei werden verschiedene Verfahren basierend auf Profilattributen, Zeitstempeln und Geotags betrachtet. Eine genauere Beschreibung der Arbeit erfolgt im nächsten Abschnitt. Die Autoren der Arbeit [193] nutzen alle der vorgenannten Verfahren und versuchen, diese zu kombinieren. Dies schließt String-basierte, Stil-basierte, Zeitprofil-basierte und Netzstruktur-basierte Verfahren mit ein. Aufgrund der Komplexität der Verfahren wurde jedes nur oberflächlich untersucht. Jain et al. [194] nutzen Inhalts- und Netzstruktur-basierte Verfahren, um zu einem Twitter-Profil das passende Facebook-Profil zu ermitteln. Liu et al. [195] stellen das Framework HYDRA vor, welches mittels heterogener Verhaltensmodellierung Profile zuordnet. Hierzu werden die Profilattribute, der Nutzer-generierte Inhalt und das Verhalten, beispielsweise Likes, Freunde hinzufügen und weitere Aspekte einbezogen.
In [196] wird in einem zwei-stufigen Ansatz zunächst mittels der Netzstruktur die Kandidatenmenge reduziert und im Anschluss die Profilattribute für die finale Profilzuordnung ausgewertet, dabei handelt es sich um eine Weiterentwicklung der Arbeit aus [197]. Ein

Ansatz mit umgekehrter Reihenfolge ist in [198] erläutert. Wang et al. [199] präsentieren einen Deep-Learning-basierten Ansatz für die Profilzuordnung unter Nutzung der Netzstruktur und Profilattribute. Deep-Learning kommt auch bei [200] zum Einsatz, allerdings werden abweichende Informationen zur Profilzuordnung herangezogen. Da die Arbeit äußerst kurz gehalten ist, wird sie für den Vergleich der Ansätze nicht herangezogen. Cao et al. [201] nutzen hierfür einen Bootstrapping Ansatz und Liu et al. [202] hierarchischen, kaskadierenden Ansatz maschinellen Lernens. In der Arbeit [203], welche auf den Ergebnissen aus [204] aufbaut, wird ein Verfahren basierend auf iterativer Abgleichen zwischen den Profilen mehrerer sozialer Netze vorgeschlagen. Hierzu werden insbesondere Nutzer die ihre Profile untereinander verlinken herangezogen.

Weitere Arbeiten die Attribut- und Graph-basierte Profilzuordnung kombinieren sind [205] [206] [207] [208] [209] und [210].

Wie sich Nutzerinformationen verteilen und wie diese aggregiert und analysiert werden können, untersucht [211]. Zu diesem Zweck werden Profilattribute und Tags, die beispielsweise Bildern zugeordnet sind, kombiniert. Auf den gleichen Eingangsdaten setzt auch die Arbeit [212] auf. Ein zwei-stufiges Verfahren unter Einbeziehung der Profilattribute und einer Textanalyse wird in [213] vorgestellt. Ein Ansatz der viele Profilinformationen aber auch Zeitstempel und eine rudimentäre Textanalyse, Häufigkeit spezifischer Symbole, verwendet, wird in [214] vorgestellt. Hazimeh et al. [215] nutzen neben Profilattributen auch zurückliegende Ereignisse und insbesondere seltene Lebensereignisse, wie Abschlüsse, Hochzeiten, ein neuer Job, die meist in mehreren Netzen mitgeteilt werden.

In [216] wird ein Verfahren basierend auf Methoden maschinellem Lernens für die Profilzuordnung vorgeschlagen, welches sich auf der Netzstruktur und auf Textanalysen abstützt. In [217] werden Algorithmen entwickelt mit dem Ziel eine effiziente Quantifikation des Profilzuordnungsrisikos vornehmen zu können. Dazu werden Attribute, Textanalysen, Zeitstempel und die Netzstruktur miteinbezogen.

Alle referenzierten Arbeiten in diesem Abschnitt werden in Tabelle 5.3 einander gegenüber gestellt.

5.2.5. Metadaten

Die Autoren der Arbeit [218] schließen auf soziale Bindungen anhand von örtlichem und zeitlichem Zusammentreffen von Nutzern. Hierzu wird ein Raster verwendet, um zu analysieren, welche Flickr-Nutzer die gleiche Zelle in einem begrenzten Zeitfenster besucht haben. Nutzer mit mehreren Zusammentreffen waren häufig befreundet. Die Arbeiten [219] und [192] versuchen Profile anhand von Geotags und Zeitstempeln mittels Klassifikatoren zuzuordnen. Geotags werden hierzu auf Postleitzahlen reduziert und die Kombinationen von Postleitzahlen der Profile miteinander verglichen, zudem wurden verschiedene Rastergrößen von 1x1 km^2 bis hin zu 12 km^2 evaluiert. Zeitstempel werden nur in einem Zeitfenster von maximal fünf Sekunden ausgewertet. Aufgrund der kurzen Dauer werden nur automatisierte Nachrichten

erfasst; diese werden auch inhaltlich analysiert, da automatisierte Nachrichten anhand der Formulierung und weiterer Faktoren identifiziert werden können. Ziel der Arbeit ist auch keine möglichst eindeutige Zuordnung, sondern eine Reduzierung auf eine Größe, die von einem Nutzer auswertbar ist. In einem der vorgestellten Beispiele würden 750 Profilpaare zur Analyse durch einen Nutzer verbleiben. Zudem wurden für die Evaluation nur kleine Datensätze verwendet. Ein Teilaspekt der Arbeit [193] ist die Verwendung von Zeitprofil-basierten Verfahren. Aufgrund der oberflächlichen Betrachtung nimmt die Genauigkeit schnell mit der Größe des Datensatzes ab und beträgt beispielsweise bei 50 Nutzern 70% und bei 1.000 Nutzern nur noch 43%.

Eine weitere Arbeit die sich selbst mit [219] vergleicht ist [220]. Dabei werden Profile anhand von generierten Einträgen zugeordnet. Hierzu werden räumliche, zeitliche und inhaltliche Features ausgewertet. Die inhaltliche Betrachtung ist dabei als eine einfach Textanalyse ausgestaltet. Für die Auswertung an sich wird auf Methoden maschinellen Lernens zurückgegriffen. Größter Schwachpunkt der Arbeit ist, dass zwar erläutert wird wie die Datensätze für die Evaluation zustande kommen aber keine weiteren Informationen, wie beispielsweise die Datensatzgröße, genannt werden. Dies führt dazu, dass die Ergebnisse so nicht bewertbar sind.

Die Arbeit [221] nutzt im Schwerpunkt Zeitstempel und weitere Informationen des Eintrages dem der Zeitstempel zugeordnet ist. Dazu gehören geographische Daten, Text, Tags, Fotos und den echten bzw. Nutzernamen. Auch hier wird nicht ausschließlich auf Metadaten zurückgegriffen. Darüber hinaus sind die für die Evaluation herangezogenen Datensätze mit 1.358 Profilen pro Netze äußerst klein.

In [222] wird ein Framework vorgestellt, bei dem eine Menge an Geopositionen mit Zeitstempel einer Menge an Textbeschreibungen der Position mit Zeitstempel zugeordnet werden. Xu et al. [223] präsentieren ein Verfahren zum Zuordnen von Nutzertrajektorien. Eine Trajektorie ist dabei als eine zeitlich geordnete Menge von Geokoordinaten und Zeitstempeln definiert. Für die Zuordnung wird ein Raster genutzt. Darüber hinaus werden nur sehr kleine Datensätze für die Evaluation herangezogen. Die Arbeit [224] fokussiert auf die Profilzuordnung zwischen zwei Orts-basierten sozialen Netzen und dem räumlichen und zeitlichen Anmeldeverhalten. Im Gegensatz zu einem festen Raster kommen hier unregelmäßig geformte Aufenthaltszonen zum Einsatz. Auch hier wird nur ein sehr kleiner Datensatz für die Evaluation genutzt. Mittels ortsbasierten Hashing Verfahren werden in [225] die Nutzertrajektorien bestimmt. In Anschluss werden die Nutzer mit ähnlichen Trajektorien mit hoher Wahrscheinlichkeit in gleiche Zellen einsortiert. Aus den Zellen generieren sich dann die zu vergleichenden Kandidatenpaare. Auch diesem Verfahren muss die geringe Datensatzgröße angekreidet werden. Ein vergleichbarer Ansatz zu vorgenanntem ist [226], er besitzt bezogen auf die Datensatzgröße auch die gleiche Schwäche. In [227] wird ein Algorithmus vorgestellt, welcher anhand eines Ähnlichkeitsmaßes für jedes Kandidatenpaar einen Wert erreichnet und im Anschluss mittels eines Bipartiten Graphen ermittelt, ob es der gleiche Nutzer ist. Evaluation erfolgt mit sehr kleinem Datensatz. Chen et al. [228] nutzen in ihrer Arbeit eine Mischerteilung für die Abbildung der Zeitstempel, dies bedeutet allerdings einen gewissen Informationsverlust. Im Gegensatz zu einer Rasterung

wird hier ein Clustering-Verfahren angewendet, dieses ist zwar nicht so starr, wie ein Raster, dennoch können einzelne Punkte aus den Clustern herausfallen und werden nicht korrekt in eine Zuordnung miteinbezogen. Zudem geht das Verfahren mitunter von relativ hohen Aktualisierungsraten der Position aus. Die verwendeten Datensätze sind mit weniger als 1.000 Nutzern extrem klein.

Mögliche Gründe für die kleinen Datensätze der Evaluation einiger vorgenannter Verfahren können entweder eine stark abnehme Trefferwahrscheinlichkeit sein oder aber das Verfahren skaliert schlecht, da sämtliche Daten im Speicher gehalten werden müssen oder einen hohen Overhead im Speicher generieren und damit nicht für große Datensätze anwendbar sind.

Alle referenzierten Arbeiten in diesem Abschnitt werden in Tabelle 5.4 einander gegenüber gestellt.

5.3. Mobilfunk und GPS Traces

Harrington und Cahill [229] nutzen neben GPS die Daten verschiedener Sensoren, um den Zustand des Irischen Straßensystems zu überwachen und beispielsweise Staus zu detektieren. Die Arbeiten [230] [231] [232] [233] [234] [235] [236] [237] [238] und [239] nutzen Mobilfunk- oder GPS-Daten für Bewegungsmustererkennung. Im Gegensatz zu Geotags aus sozialen Netzen liefern jedoch Mobilfunk- bzw. GPS-Traces, solange eine Funkverbindung besteht, fortwährend Daten. Geotags sind lediglich eine Momentaufnahme. In [240] und [241] werden anhand von Mobilfunk- bzw. GPS-Daten spezifische Profile der Nutzer generiert. Li et al. [242] vergleichen mit GPS-Empfängern ausgestattete Nutzer anhand deren Standortverläufen. In den Arbeiten von Huandong Wang et al. [243], [244] und [245] werden Algorithmen hinsichtlich der Zuordnung verschiedener anonymer Mobilfunk-Traces zu einem Individuum erprobt. Weitere Arbeiten dieser Forschungsgruppe mit ähnlichem Fokus aber unter Nutzung verschiedener Ansätze sind [246], [247] und [248].

5.4. Privatsphäre in sozialen Netzen

In Zeiten, wo Milliarden von Nutzern private Informationen im Internet teilen, spielt die Privatsphäre eine immer entscheidendere Rolle, um zu verhindern, dass jeder diese Informationen einsehen kann. Diverse Studien und Arbeiten befassen sich daher mit dem Thema der Privatsphäre in sozialen Netzen, dazu zählen [249] [250] [251] [14] [252] [253] [254] [255] [256] und [257]. Diese Arbeiten betrachten zum einen die Möglichkeiten, die Privatsphäre zu umgehen, aber auch Studien zur Diskrepanz zwischen der gewünschten Privatsphäre und den vorgenommenen Einstellungen innerhalb der sozialen Netze fallen darunter.

In [258] zeigen die Autoren ein Verfahren auf, das es erlaubt, von veröffentlichten Datensätzen aus sozialen Netzen, in denen die Benutzernamen anonymisiert wurden, wieder eine Beziehung zu den eigentlichen Profilen herzustellen. Puglisi et al. [259] betrachten in ihrer Arbeit das Zeitverhalten und die sich daraus für die Privatsphäre ergebenen Risiken. Ein Ansatz zur

Verhinderung von Profilzuordnung mittels Graph-basierter Methoden wird in [260] erläutert. Ein Maß für die Verlinkbarkeit von Profilen wird in [261] vorgestellt. Ein vergleichbares Maß wir auch in [262] präsentiert, mit dem Fokus Awareness bei den Nutzer zu erzeugen. In [263] wird ein Framework präsentiert, welches einen Nutzer unterstützt, die Verlinkbarkeit seiner Profile zu kontrollieren.

Die nachfolgenden Arbeiten stellen Reviews bzw. Surveys zu ausgewählten Themen dar. Dazu gehören *Re-Identification* Attacken [264], Identifizierung von Verwundbarkeiten und Verminderung der Datenschutzrisiken von Beigi et al. [265], [266] und einem zusätzlichen Fokus auf geteilte Multimediainhalte von Rathore et al. [267], Privatsphäre im Bereich von Mobilfunk Traces [268].

5.4.1. Ortsbasierte Verfahren

Dieser Unterpunkt betrachtet im speziellen Aspekte der Privatsphäre, die sich aus der Nutzung von ortsbasierten Diensten oder Geotags ergeben. Die Arbeit [269] gibt hierzu einen umfassenden Überblick über Methoden der Anonymisierung von Standortdaten, aber auch entsprechender Verfahren, um diese zu brechen. In [270] zeigen die Autoren wie anonymisierte Traces korrekt einem Nutzer zugeordnet werden können. Hierzu werden soziale Netze als Seitenkanal genutzt, die es ermöglichen, Verbindungen im Netzgraph einem Treffen in den Traces zuordnen. Hoh et al. [271] [272] stellen ein Verfahren zur Sicherstellung der Anonymität von GPS-Traces vor. In [273] zeigen die Autoren wie sich anhand öffentlich verfügbarer Positionsmetadaten Wohnort und Arbeitsort ermitteln lassen.

Darüber hinaus existieren weitere Verfahren, die die Privatsphäre im ortsabhängigen Kontext beleuchten, darunter [274] [275] [276] [277] [278] und [279].

5.4.2. Ansätze zur Verbesserung

Aufgrund der umfangreichen Forschungarbeit im Bereich der Privatsphäre von sozialen Netz Nutzern betrachteten mehrere Arbeiten Möglichkeiten zur Verbesserung dieser. Hierunter fallen unter anderem [280] [281] und [282]. Die vorgenannten Verfahren stellen Anwendungen vor, um soziale Netze sicherer zu machen und den Abfluss von Informationen zu verhindern.

Balduzzi, Platzer und Holz [283] verwendeten einen Datensatz mit über 10 Millionen E-Mail Adressen, mit denen die Freundesuchfunktion von diversen sozialen Netzen gefüttert wurden. Hierdurch konnten die Autoren über 1,2 Millionen Profile crawlen. Aufgrund der Empfehlungen in dieser Arbeit und der Autoren implementierten diese Netze entsprechende Limitierungen der Suchfunktion, so dass in einem Zeitfenster nur noch eine begrenzte Anzahl an Freunden durch E-Mail Adressen gesucht werden kann. In [284] wird das Konzept der sozialen Netze mit erweitertem Datenschutz vorgestellt. Diese zeichnen sich dadurch aus, dass dem Nutzer die Risiken bewusst gemacht werden, dieser die Einstellungen entsprechend anpassen kann, Zugriffsberechtigungen von Anwendungen auf Attributebene konfiguriert werden können und diese auch aufzeigen, zu welchem Zweck die Daten verarbeitet werden, und die Daten des

Nutzers sein Eigentum bleiben und nicht auf den Betreiber des sozialen Netzes übergehen. Stein, Chen und Mangla präsentieren in ihrer Arbeit [285], wie Facebook selbst Bedrohungen begegnet. Es werden dabei Echtzeit-Überprüfungen und Klassifikatoren erläutert, die bei jeder Lese- und Schreiboperation zum Einsatz kommen.

5.4.3. Fake-Profil- und Identitätsdiebstahl-Erkennung

Die Arbeit [286] stellt eine Anwendung vor, die auf Facebook Fake-Profile erkennt und die Sicherheits- und Privatsphäreneinstellungen des Nutzers optimiert. Die Erkennung von Fake-Profilen erfolgt durch eine einfache Heuristik. Hierzu werden diverse Eigenschaften eines Profils, beispielsweise die Anzahl der Nutzer, die Anzahl der Posts oder die Anzahl getaggter Fotos ausgewertet. Conti, Poovendran und Secchiero [287] versuchen, Identitätsdiebstahl zu erkennen. Hierzu analysierten sie die typische Wachstumsrate eines sozialen Netz-Profils. Darüber hinaus versucht ein Angreifer, nahe Freunde des Opfers zu meiden, da diese das Fake-Profil erkennen könnten, was sich auf die Netzstruktur auswirkt. Anhand dieser Eigenschaften ermitteln die Autoren bösartiges Verhalten. Weitere Arbeiten [288] [289] [290] nutzen Methoden und Techniken der Analyse sozialer Netze, um Fake-Profile und/oder Identitätsdiebstahl zu detektieren. Kontaxis et al. [291] stellen ein Rahmenwerk vor, welches geklonte Profile identifiziert. Die Evaluation erfolgte anhand von LinkedIn. Ein weiteres Rahmenwerk wird in [292] präsentiert. Der Survey [293] setzt sich mit der Erkennung kompromittierter Accounts auseinander.

5.5. Bedrohungen

Fire, Goldschmidt und Elovici präsentieren in ihrer Arbeit [294] umfangreiche Betrachtungen der Bedrohungen in sozialen Netzen. Darüber hinaus geben die Autoren einen Überblick über die von Betreibern sozialer Netze, Sicherheitsfirmen und Forschern erarbeiteten Ansätze und Verfahren, um den betrachteten Bedrohungen zu begegnen. In [295] wird evaluiert, wie leicht mittels Identitätsdiebstahl private Profile gecrawlt werden können. Hierzu werden automatisch Profile kopiert und Freundschaftsanfragen an die Freunde des ursprünglichen Profils geschickt. Wurden die Anfragen akzeptiert, hatten die Autoren Zugriff auf die Daten des privaten Profils. Ein weiteres Verfahren kopiert Profile in sozialen Netzen, in denen der Besitzer des Ausgangsprofils nicht angemeldet ist, jedoch die Freunde des ursprünglichen Profils. Im Review [296] liegt der Fokus auf Betrügereien in sozialen Netzen. Zunächst wird eine Typologie von Betrügereien vorgestellt und im Anschluss werden diese im Detail erläutert und der Stand der Technik hinsichtlich deren Erkennung behandelt. Einen ähnlichen Ansatz enthält [297] wobei hier der Fokus auf verschiedenen Angriffen und entsprechenden Verteidigungsmechanismen liegt.

5.5.1. Social Engineering

Lauinger et al. [298] nutzen einen Bot für automatisiertes Social Engineering. Der Bot schreibt eine Person A an; sobald A antwortet, schickt der Bot die Nachricht an B. Die Antwort von B wird vom Bot an A weitergeleitet. Hierdurch kommt eine Kommunikation zwischen zwei Menschen zustande. Dennoch kann der Bot als Man-in-the-Middle beispielsweise den Text manipulieren oder Links einfügen. Da die Gegenseite das Gefühl hat, die Nachricht bzw. der

Link kommt vom Gegenüber, ist die Wahrscheinlichkeit des Anklickens deutlich größer. Die Arbeit [299] nutzt Bots für die langwierigen Schritte des Social Engineering, wodurch dies ein günstiger und attraktiver Angriff wird. In [300] untersuchten die Autoren, welche Eigenschaften einen Einfluss auf die Wahrscheinlichkeit der Akzeptanz von Freundschaftsanfragen und damit auf den Erfolg von Social-Engineering-Angriffen auf Facebook haben. Hierzu wurden unter anderem Aspekte wie die Anzahl der Freunde, die Menge des Inhalts eines Profils oder ein guter Schreibstil betrachtet. Irani, Balduzzi und Balzarotti [301] stellen in ihrer Arbeit das Konzept von rückwärtsgerichtetem Social Engineering vor. Hierbei geht die Kontaktanfrage an das Opfer nicht von einem Angreifer aus, sondern dieser macht sich die Funktionen zum Auffinden von Freunden eines sozialen Netzes zu Nutze, so dass das Opfer die Anfrage an den Angreifer schickt. Da die Anfrage dabei vom Opfer ausgeht, ergibt sich ein starkes Vertrauensverhältnis zwischen Opfer und Angreifer.

5.5.2. Bots

Boshmaf et al. evaluieren in ihrer Arbeit [302] die Verwundbarkeit sozialer Netze gegenüber der Infiltration von Bots. Hierzu adaptierten die Autoren ein traditionelles Web-basiertes Botdesign und betrieben eine Gruppe von Bots, gesteuert durch eine Command-and-Control-Infrastruktur im sozialen Netz Facebook.

Fake-Profile und Spam

In [303] charakterisieren die Autoren Spam in Twitter und fanden heraus, dass 8% von 25 Millionen untersuchten URLs aus Tweets auf Phishing- und Malware-Seiten verweisen. Darüber hinaus wurden Profile anhand der Zielseite der URLs und den entsprechenden Einträgen auf Blacklists nach Spam-Kampagnen geclustert. Bosma, Meij und Weerkamp [304] schlagen ein Rahmenwerk zur automatischen Detektion von Spam vor. Ihr Ansatz basiert auf den Daten von Nutzer-generierten Spamberichten und es werden hierzu drei verschiedene Modelle evaluiert. Die Arbeit [305] beschreibt eine Möglichkeit zur Erkennung von Spam- und Fake-Profilen. Hierzu werden einzig die topologischen Eigenschaften der sozialen Netze genutzt, dies bedeutet, dass das beschriebene Verfahren Profile erkennt, die sich zufällig mit anderen verbinden. Das eingesetzte Verfahren nutzt hierzu die Erkennung der dadurch entstandenen Anomalien. In [306] werden die Verfahren zur Erkennung von Spammern auf Twitter analysiert. Zusätzlich wird auch eine Taxonomie zur Einteilung der Verfahren vorgestellt. Die Arbeit [307] werden Daten von Twitter gesammelt, um im Rückblick diese mit Fokus auf suspendierte Accounts auszuwerten. Dabei werden auch die Tools, Techniken und die Supportinfrastruktur näher betrachtet. Traditionelle Klassifikatoren werden in [308] für die Spamerkennung bei Twitter herangezogen. Die Arbeit [309] betrachtet den Schwarzmarkt hinter Spam und Fake-Profilen in sozialen Netzen. Mohammadrezaei et al. schlagen in [310] ein Verfahren zur Erkennung von Fake-Profilen auf der Basis der Ähnlichkeit der Freundesnetze eines Nutzers vor. Hierzu werden diverse Metriken herangezogen, um diese Ähnlichkeit zu berechnen. Möglichkeiten zur Erkennung von bösartigen Profilen wird in [311] vorgestellt. Hierbei liegt der Fokus auf Profilen, die Attribute und Fotos von legitimen Profilen kopieren und für ihr Profil nutzen.

Eine Übersicht über verschiedene Verfahren zur Fake-Profilerkennung wird in [312] und [313] gegeben, in letzterem wird insbesondere auch auf die Herausforderungen und Limitierungen der Verfahren eingegangen, in [314] liegt der Fokus auf der Detektion von Spammern.

Boterkennung

Radziwill und Benton nutzen in ihrer Arbeit [315] Zeitkarten, um zu entscheiden, ob ein Tweet von einem Bot generiert wurde. Hierzu werden Muster zwischen der Ankunft mehrerer Tweets eines menschlichen Nutzers, Nutzern die Terminierungsdienste verwenden und Bots analysiert. In der Arbeit [316] wird eine Methode präsentiert, die es ermöglicht, zu entscheiden, ob ein Twitter-Profil automatisiertes Verhalten zeigt, also von einem Bot kontrolliert wird und dies nur anhand der Zeitstempel der Tweets. Die Autoren gehen davon aus, dass die Aktivitäten eines Bots zeitliche Muster aufweisen, die dazu führen, dass die zeitliche Verteilung der Tweet-Erzeugung im Hinblick auf Minuten und Sekunden im Gegensatz zu Menschen nicht zufällig ist. Webb et al. [317] nutzen gesellige Honeypots, um das Verhalten, Strategien und Taktiken von Spammern zu analysieren und Spam zu verfolgen und zu überwachen. Die Autoren erkannten hierdurch verschiedene Eigenschaften, die eine automatische Identifizierung von Spam ermöglichen. In [318] wird die Arbeit mit geselligen Honeypots fortgesetzt und mit Techniken des maschinellen Lernens kombiniert, um Spam zuverlässig zu erkennen. Die Autoren der Arbeit [319] setzten ebenfalls die Arbeit von [317] fort und konnten durch eine Kollaboration mit Twitter 15.857 Spamprofile entfernen. Einen KI-basierten Deep Learning Ansatz zur Botdetection nutzen die Autoren in [320]. In [321] wird ein Boterkennungssystem, inklusive der zugrunde liegenden Vorgehensweise, vorgestellt, welches jeden Tag hunderte bis tausende von Bots identifiziert und diese in online verfügbaren Reports dokumentiert. Die Arbeiten daran wurden in [322] fortgesetzt und mündeten in der Dissertation des Erstautors [323].

5.6. Delta bisheriger Verfahren gegenüber dieser Arbeit

Es existieren nur zwei aussagekräftige Arbeiten, deren Datenbasis auf Metadaten basiert. Die weiteren im vorherigen Abschnitt vorgestellten und in der Tabelle 5.4 verglichenen Verfahren arbeiten mit Datensätzen, die so klein sind, oft nur ein bis zweitausend Profile oder noch weniger, dass diese Datensätze so gewählt zu sein scheinen, dass gute Ergebnisse erzielt werden. Sie werden daher im Rahmen dieser Arbeit als nicht bewertbar angesehen und damit nicht weiter betrachtet.

Die Arbeiten [219] und [192] sind als eine Arbeit zu betrachten, da [192] mehrere Arbeiten der Autoren, darunter auch [219] in einer Dissertation zusammenfasst, jedoch keine weiteren Erkenntnisse zu diesem Themenbereich beiträgt.

Die Arbeit [218] rastert die Welt in verschieden große Zellen, in die Geotags von Fotos des sozialen Netzes Flickr einsortiert werden. Ziel ist, Bekanntschaften und Freundschaften zu identifizieren, indem Geotags mehrerer Nutzer in einem Zeitfenster von 24 Stunden in der gleichen Rasterzelle gezählt werden. Werden mehrere Übereinstimmungen detektiert, wird von

einer Freundschaft ausgegangen. Das Verfahren bietet jedoch gegenüber dieser Arbeit folgende Nachteile:

- Bei einer Rasterung können auch nahe beieinanderliegende Geotags, bedingt durch fest definierte Grenzen, in unterschiedlichen Zellen einsortiert werden, wodurch die Trefferquote abnimmt.

- Der Datensatz enthält Daten von 490.000 Nutzern mit durchschnittlich 77,5 Geotags. Das hier vorgestellte Verfahren erfordert deutlich geringere Mengen an Geodaten eines Nutzers.

- Die Autoren berichten von einer deutlichen Steigerung der Wahrscheinlichkeit einer Beziehung bereits bei drei gemeinsamen Vorkommen. Da der Datensatz Nutzer auf der ganzen Welt enthält, ergibt sich die Wahrscheinlichkeitssteigerung dadurch, dass zwei Personen in der Nähe mit größerer Wahrscheinlichkeit befreundet sind, als wie wenn eine der Personen am anderen Ende der Welt lebt.

- Die Arbeit liefert für diverse Parameter Statistiken darüber, wie viel Prozent korrekt zugeordnet werden konnten, verschweigt aber gänzlich, wie viele korrekt zugeordnete Profile zu diesem Prozentsatz führen. Die Autoren geben an, dass viele Flickr-Nutzer ihre Freundesliste nicht öffentlich zugänglich machen bzw. die Funktion gar nicht nutzen. Dies reduziert die Ground-Truth und die Datensatzgröße deutlich, hierzu fehlen jedoch Angaben.

- Keine Erkennung von Botnetzen oder Identitätsdiebstahl, keine Profilzuordnung mehrerer Profile in verschiedenen Netzen zu einem Nutzer.

Das in [219] beschriebene Verfahren ist von allen betrachteten Ansätzen dem in dieser Arbeit präsentierten am ähnlichsten. Dennoch ist das Ziel der Arbeit, nur zu zeigen, dass es möglich ist, daher ist das Verfahren nur rudimentär und mit diversen Einschränkungen umgesetzt, diese sind:

- Die Zuordnung von Zeitstempeln erfolgt nur in einem Zeitbereich von maximal fünf Sekunden. Auf diese Weise können nur automatisch generierte Nachrichten zugeordnet werden. Die Autoren beschreiben, dass nur wenige Nutzer von dieser Funktion Gebrauch machen. Weitere Analysen fanden im Hinblick auf Zeitstempel nicht statt bzw. führten zu keinem Ergebnis.

- Geotags werden entweder gerastert oder in die entsprechende Postleitzahl gewandelt. Postleitzahlen sind jedoch nicht weltweit ohne weiteres nutzbar und eine Rasterung führt zu dem Problem, welches für [218] bereits erläutert wurde.

- Es wurden Datensätze für fünf amerikanische Städte genutzt, kein gemeinsamer Datensatz, wodurch die Größe und die Komplexität reduziert wurde. Die Ground-Truth ist nur für etwa sechs Prozent des Datensatzes gegeben.

- Die Verfahren werden einzeln betrachtet. Eine Kombination findet im Anschluss statt, hierbei wird jedoch zusätzlich die verwendete Sprache miteinbezogen, was gegen die alleinige Nutzung von Metadaten dieser Arbeit spricht. Zudem kommen zur Beurteilung der Kombination Klassifikatoren zum Einsatz. Hierbei wird für jede Zusammenstellung zweier sozialer Netze ein eigener Klassifikator verwendet.
- Das Verfahren sieht vor, nur eine Vorauswahl zu treffen, so dass ein Nutzer, in einem gegebenen Beispiel noch 750 Profile, von Hand durchgehen und das Ergebnis verfeinern bzw. das entscheidende Profil auswählen muss.
- Erlaubt keine Identifikation von Botnetzen, Fake-Profilen oder Identitätsdiebstahl.

5.7. Vergleich der Verfahren

Die nachfolgende Tabelle 5.1 gibt einen Überblick über die in diesem Kapitel vorgestellten Verfahren zum Zuordnen von Profilen anhand der im Kapitel 4 aufgestellten Anforderungen.

Tabelle 5.1.: Vergleich bisheriger Verfahren (nur Attribut-bezogene) mit dieser Arbeit. ✓ : Eigenschaft erfüllt, ○ : Eigenschaft teilweise erfüllt, ✗ : Eigenschaft nicht erfüllt.

Veröffentlichung	keine Attribute	keine Struktur	keine Textanalyse	Zeitstempel	Geotags	Gewichtung	Groundtruth	keine Verfeinerung	kein Klassifikator	Datensatz [h]
[119]	✗	✓	✓	✗	✗	✗	✗	✓	✓	$\ll 10^6$ [b]
[120]	✗	✓	✓	✗	✗	✗	○[d]	✓	✗	$\ll 10^6$ [c]
[121]	✗	✓	✓	✗	✗	✓	✗	✓	✗	$< 10^5$
[122]	✗	✓	✓	✗	✗	✓	○[a]	✓	✓	$< 10^3$
[123]	✗	○[e]	✓	✗	✗	✗	✗	✓	✓	$\ll 10^6$
[124]	✗	○[e]	✓	✗	✗	✓	✗	✓	✓	$< 10^3$
[125]	✗	○[e]	✓	✗	✗	✗	✗	✓	✗	$\ll 10^6$
[126]	✗	✓	✓	✗	✗	✗	✗	✓	✗	$< 10^5$
[127]	✗	✓	✓	✗	✗	✓	✓	✓	✓	$\ll 10^4$
[141]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$< 10^4$
[142]	✗	○[e]	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[143]	✗	✓	✓	✗	✗	✓	✓	✓	✓	$< 10^4$
[144]	✗	✓	✓	✗	✗	✓	✓	✓	✓	$\ll 10^2$
[145]	✗	✓	✓	✗	✗	✗	✓	✓	✗	$\ll 10^7$
[146]	✗	✓	✓	✗	✗	✓	✓	✓	✗	$\ll 10^7$
[153]	✗	○[e]	✓	✗	✗	✗	○[d]	✓	✗	$< 10^6$
[129]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$\ll 10^6$
[128]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$\ll 10^3$
[130]	✗	✓	✓	✗	✗	✗	✓	✓	✗	$< 10^4$
[147]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$\ll 10^4$
[132]	✗	✓	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[131]	✗	✓	✓	✗	✗	✗	✓	✓	✗	$\ll 10^4$
[135]	✗	○[e]	✓	✗	✗	✗	✓	✓	✗	$< 10^7$
[136]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$< 10^5$
[133]	✗	✓	✓	✗	✗	✗	✓	✓	✗	$\ll 10^5$
[137]	✗	✓	✓	✗	✗	✓	? [i]	✓	✓	? [i]
[134]	✗	✓	✓	✗	✗	✓	✓	✓	✗	$\ll 10^4$
[148]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$\ll 10^3$
[149]	✗	✓	✓	✗	✗	✗	✗	✗	✗	$\ll 10^2$
[138]	✗	✓	✓	✗	✗	✗	✓	✓	✗	$\ll 10^4$
[139]	✗	✓	✓	✗	✗	✓	✓	✓	✗	$\ll 10^6$
[150]	✗	✓	✓	✗	✗	✓	✓	✓	✗	$\ll 10^3$
[151]	✗	✓	✓	✗	✗	✓	✓	✓	✗	$\ll 10^5$
[152]	✗	✓	✓	✗	✗	✓	✓	✓	✗	$\ll 10^5$
[140]	✗	✓	✓	✗	✗	✗	✓	✓	✓	$\ll 10^3$
Diese Arbeit	✓	✓	✓	✓	✓	✓	✓	✓	✓	$\gg 10^7$

[a] Datensatz selbst generiert.
[b] Datensatzgröße bezieht sich auf Benutzernamenpaare.
[c] Klassifikator mit Datensatzgröße 10 Millionen trainiert.
[d] Ground-Truth nur für eine Teilmenge vorhanden.
[e] Struktur nur Anzahl und ggf. Namen der Freunde.
[f] Betrachtung nur der Nutzernamen.
[g] Siehe Beschreibung.
[h] $\ll$ bedeutet kleiner als die Hälfte.
[i] Enthält keine Evaluation.

Tabelle 5.2.: Vergleich bisheriger Verfahren (nur Graph-basierte) mit dieser Arbeit. ✓ : Eigenschaft erfüllt, ○ : Eigenschaft teilweise erfüllt, ✗ : Eigenschaft nicht erfüllt.

Veröffentlichung	keine Attribute	keine Struktur	keine Textanalyse	Zeitstempel	Geotags	Gewichtung	Groundtruth	keine Verfeinerung	kein Klassifikator	Datensatz [h]
[154]	○[f]	✗	✓	✗	✗	✓	✗	✓	✓	10^6
[155]	○[f]	✗	✓	✗	✗	✗	✗	✓	✓	$\ll 10^7$
[156]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[157]	✓	✗	✓	✗	✗	✗	○[d]	✓	✗	$\ll 10^6$
[158]	✓	✗	✓	✗	✗	✗	○[a]	✓	✓	$\ll 10^5$
[159]	✓	✗	✓	✗	✗	✗	○[a]	✓	✓	$\ll 10^5$
[160]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[161]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^5$
[176]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^8$
[162]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$< 10^5$
[167]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[168]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^3$
[164]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$< 10^4$
[177]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^4$
[170]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$< 10^4$
[171]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^4$
[178]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[172]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^4$
[179]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$< 10^4$
[166]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^8$
[180]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^4$
[181]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^4$
[182]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^5$
[169]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^4$
[165]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^4$
[173]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^7$
[183]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^4$
[174]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[184]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^5$
[185]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^5$
[175]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^5$
[186]	✓	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^5$
[163]	✓	✗	✓	✗	✗	✗	✓	✓	✓	$< 10^4$
Diese Arbeit	✓	✓	✓	✓	✓	✓	✓	✓	✓	$\gg 10^7$

[a] Datensatz selbst generiert.
[b] Datensatzgröße bezieht sich auf Benutzernamenpaare.
[c] Klassifikator mit Datensatzgröße 10 Millionen trainiert.
[d] Ground-Truth nur für eine Teilmenge vorhanden.
[e] Struktur nur Anzahl und ggf. Namen der Freunde.
[f] Betrachtung nur der Nutzernamen.
[g] Siehe Beschreibung.
[h] $\ll$ bedeutet kleiner als die Hälfte.

Tabelle 5.3.: Vergleich bisheriger Verfahren (sonstige nicht Metadaten-basierte) mit dieser Arbeit. ✓ : Eigenschaft erfüllt, ○ : Eigenschaft teilweise erfüllt, ✗ : Eigenschaft nicht erfüllt.

Veröffentlichung	keine Attribute	keine Struktur	keine Textanalyse	Zeitstempel	Geotags	Gewichtung	Groundtruth	keine Verfeinerung	kein Klassifikator	Datensatz [h]
[187]	○[f]	✓	✗	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[188]	✓	✓	✗	✗	✗	✗	✓	✓	✗	$< 10^6$
[189]	✓	✓	✗	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[190]	✓	✓	✗	✗	✗	✗	✗	✓	✓	$\ll 10^4$
[191]	✓	✓	✗	✗	✗	✗	✓	✓	✓	$\leq 10^5$
[205]	✗	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^4$
[196]	✗	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^7$
[206]	✗	✗	✓	✗	✗	✗	✓	✓	✗	$< 10^5$
[198]	✗	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^5$
[197]	✗	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^7$
[201]	✗	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[207]	✗	✗	✓	✗	✗	✗	✗	✓	✗	?[i]
[199]	✗	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[208]	✗	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[209]	✗	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^4$
[202]	✗	✗	✓	✗	✗	✗	✗	✓	✗	$\ll 10^5$
[204]	✗	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^7$
[203]	✗	✗	✓	✗	✗	✗	✓	✓	✓	$\ll 10^7$
[193]	✗	✗	✓	✓	✗	✗	✓	✓	✓	10^4
[195]	✗	✗	✓	✗	✗	✓	✓	✓	✗	$\ll 10^8$
[210]	✗	✗	✓	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[212]	✗	✓	✗	✗	✗	✗	✓	✓	✗	$< 10^4$
[211]	✗	✓	✗	✗	✗	✗	✓	✓	✗	$\ll 10^6$
[213]	✗	✓	✗	✗	✗	✗	✓	✓	✗	$\ll 10^5$
[216]	✓	✗	✗	✗	✗	✗	✗	✓	✗	$\ll 10^6$
[217]	✗	✗	✗	✓	✗	✗	✓	✓	✗	$\ll 10^5$
[194]	✗	✗	✗	✗	✗	✗	✓	✓	✓	$< 10^4$
[215]	✗	✓	✗	✓	✗	✗	✓	✓	✗	$\ll 10^4$
Diese Arbeit	✓	✓	✓	✓	✓	✓	✓	✓	✓	$\gg 10^7$

[a] Datensatz selbst generiert.
[b] Datensatzgröße bezieht sich auf Benutzernamenpaare.
[c] Klassifikator mit Datensatzgröße 10 Millionen trainiert.
[d] Ground-Truth nur für eine Teilmenge vorhanden.
[e] Struktur nur Anzahl und ggf. Namen der Freunde.
[f] Betrachtung nur der Nutzernamen.
[g] Siehe Beschreibung.
[h] $\ll$ bedeutet kleiner als die Hälfte.
[i] Nur Anzahl der Tweets aber nicht die Anzahl der Nutzer.
[j] Veröffentlichung enthält keine entsprechende Angabe.

Tabelle 5.4.: Vergleich bisheriger Verfahren (nur im Schwerpunkt Metadaten-basierte) mit dieser Arbeit. ✓ : Eigenschaft erfüllt, ○ : Eigenschaft teilweise erfüllt, ✗ : Eigenschaft nicht erfüllt.

Veröffentlichung	keine Attribute	keine Struktur	keine Textanalyse	Zeitstempel	Geotags	Gewichtung	Groundtruth	keine Verfeinerung	kein Klassifikator	Datensatz [h]
[222]	✓	✓	✗	✓	✓	✗	✓	✓	✗	$\ll 10^4$
[214]	✗	✓	✗	✓	✗	✗	✓	✓	✓	$\ll 10^5$
[220]	✓	✓	✗	✓	✓	✗	✓	✓	✗	?[j]
[223]	✓	✓	✓	✗	○[g]	✗	✓	✓	✓	$\ll 10^4$
[224]	✓	✓	✓	✗	○[g]	✗	✓	✓	✓	$\ll 10^4$
[225]	✓	✓	✓	✗	✓	✗	✓	✓	✓	$\ll 10^4$
[226]	✓	✓	✓	✗	✓	✗	✓	✓	✓	$\ll 10^5$
[227]	✓	✓	✓	✗	✓	✗	✓	✓	✓	$\ll 10^4$
[228]	✓	✓	✓	○[g]	○[g]	✓	✓	✓	✓	$\ll 10^3$
[221]	○	✓	✓	✓	✓	✗	✓	✓	✗	$\ll 10^4$
[218]	✓	✓	✓	○[g]	○[g]	✗	✓	✓	✓	$\ll 10^7$
[219] [192]	✓	✓	○[g]	○[g]	○[g]	○[g]	○[d]	✗	○[g]	$< 10^6$
Diese Arbeit	✓	✓	✓	✓	✓	✓	✓	✓	✓	$\gg 10^7$

[a] Datensatz selbst generiert.
[b] Datensatzgröße bezieht sich auf Benutzernamenpaare.
[c] Klassifikator mit Datensatzgröße 10 Millionen trainiert.
[d] Ground-Truth nur für eine Teilmenge vorhanden.
[e] Struktur nur Anzahl und ggf. Namen der Freunde.
[f] Betrachtung nur der Nutzernamen.
[g] Siehe Beschreibung.
[h] $\ll$ bedeutet kleiner als die Hälfte.
[i] Nur Anzahl der Tweets aber nicht die Anzahl der Nutzer.
[j] Veröffentlichung enthält keine entsprechende Angabe.

KAPITEL 6

Metadaten Erfassung

Dieses Kapitel gibt zum einen anhand eines Metamodells einen Überblick über die Metadaten, die innerhalb sozialer Netze anfallen und zum anderen, wie diese Metadaten bzw. Gesetzmäßigkeiten zwischen ihnen für die Profilzuordnung instrumentalisiert werden können.

6.1. Metamodell

Es existiert eine Vielzahl an sozialen Netzen und nahezu alle dieser Netze spezialisieren sich auf einen Aspekt oder kombinieren verschiedene Aspekte, die kaum oder noch gar nicht von anderen Netzen abgedeckt werden. Dennoch ist es möglich, die Summe der sozialen Netze in einem Metamodell abzubilden. Ein Modell beschreibt bzw. stellt einen konkreten Sachverhalt oder Ablauf dar. Nach [324] werden Metamodelle eingesetzt, um die Struktur von Modellen eines eingeschränkten Einsatzbereichs formalisiert zu beschreiben. Ein Metamodell stellt somit die Abstraktion eines oder mehrerer konkreter Modelle dar.

Die Autoren von [325] beschäftigen sich in ihrer Arbeit mit der Frage, wie Experten in sozialen Netzen gefunden werden können. Hierzu definieren sie unter anderem ein vereinfachtes Metamodell sozialer Netze, welches in Abbildung 6.1 dargestellt ist. Auch wenn der Kontext von [325] in keiner Verbindung zu dieser Arbeit steht, ist das vorgestellte Metamodell sozialer Netze so allgemein und generisch gehalten, dass es auch für die Betrachtungen dieser Arbeit anwendbar ist.

Die Definition eines *Nutzerprofils* deckt sich weitestgehend mit der in dieser Arbeit verwendeten Definition, als die Summe aller Interaktionen mit dem sozialen Netz. Lediglich die Profilseite ist im Kontext dieses Metamodells als *Ressourcen-Container* zu verstehen, daher bezieht sich auch jedes Profil auf mindestens einen Container. Da das *Nutzerprofil* sämtliche Nutzerinteraktionen repräsentiert, gehen die Aktivitäten *annotieren, besitzen* und *erzeugen* auch von diesem aus. Diese beziehen sich auf eine *Ressource*, im Kontext dieses Modells fällt hierunter alles, was von einem Nutzer unter anderem erzeugt, verfasst oder hochgeladen wurde, beispielsweise Tweets, Nachrichten, Beiträge, Bilder oder Videos. Ein *Ressourcen-Container* kann *Ressourcen* enthalten, erbt jedoch gleichzeitig die Eigenschaften einer *Ressource*, so dass

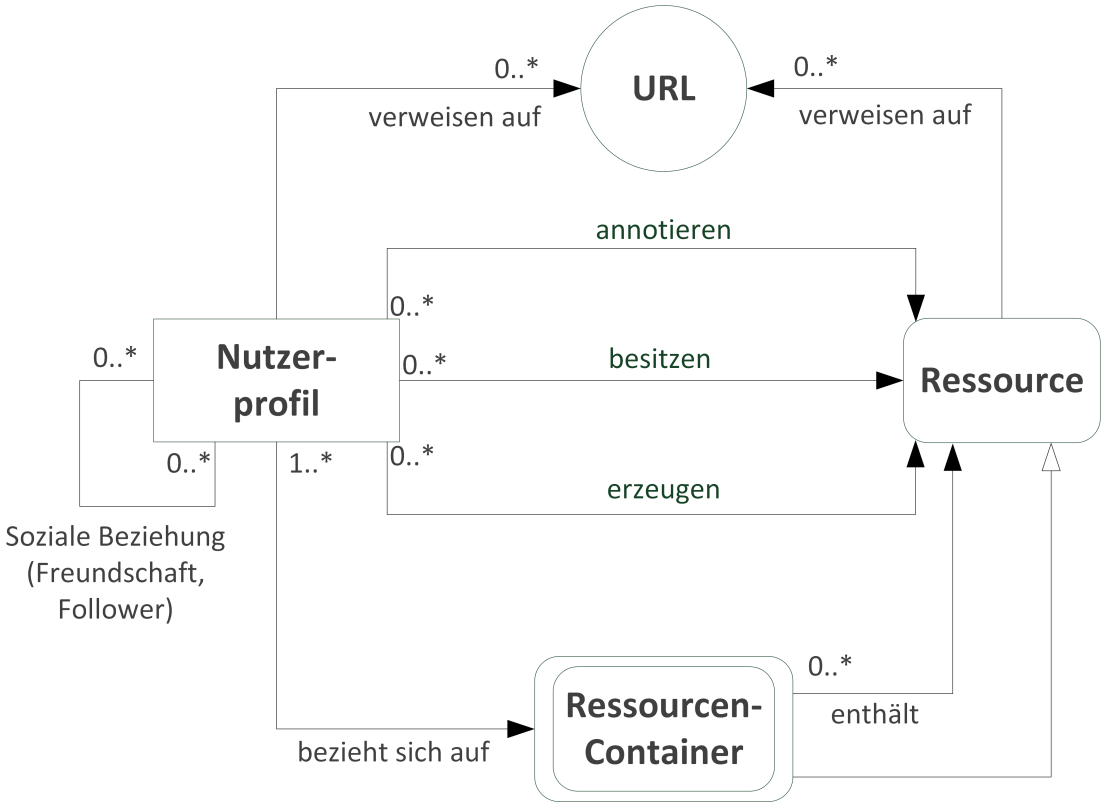


Abbildung 6.1.: Metamodell eines sozialen Netzes, vergleiche [325].

auch diesen ein *Nutzerprofil annotieren, besitzen* oder *erzeugen* kann. Nutzerprofile können auch soziale Bindungen untereinander aufweisen, beispielsweise Freundschaften oder einen Follower-Status wie bei Twitter üblich. Ein *Nutzerprofil* bezieht sich auf mindestens einen *Ressourcen-Container*, dies kann einerseits die Profilseite sein aber auch Zugehörigkeiten beispielsweise zu Gruppen bedingen einen Verweis auf einen *Ressourcen-Container* der Gruppen-spezifische *Ressourcen* enthält. Sowohl *Nutzerprofile* als auch *Ressourcen* können eine *URL* enthalten bzw. darauf verweisen. Diese *URLs* verweisen auf Webseiten die weitere Informationen zum *Nutzerprofil*, der *Ressource* oder dem *Ressourcen-Container* enthalten können.

Abbildung 6.2 zeigt das vorgestellte Metamodell zudem als Entity-Relationship-Modell mit Chen-Notation, was die Darstellung vereinfacht und es ermöglicht, dieses im nächsten Abschnitt mit Attributen zu versehen. An der Semantik hat sich im Vergleich zur vorhergehenden Darstellung aus Abbildung 6.1, abgesehen von der nicht dargestellten Vererbung der Ressourceneigenschaften an den Ressourcen-Container, nichts geändert. Dies ist jedoch für die weiteren Betrachtungen auch nicht notwendig.

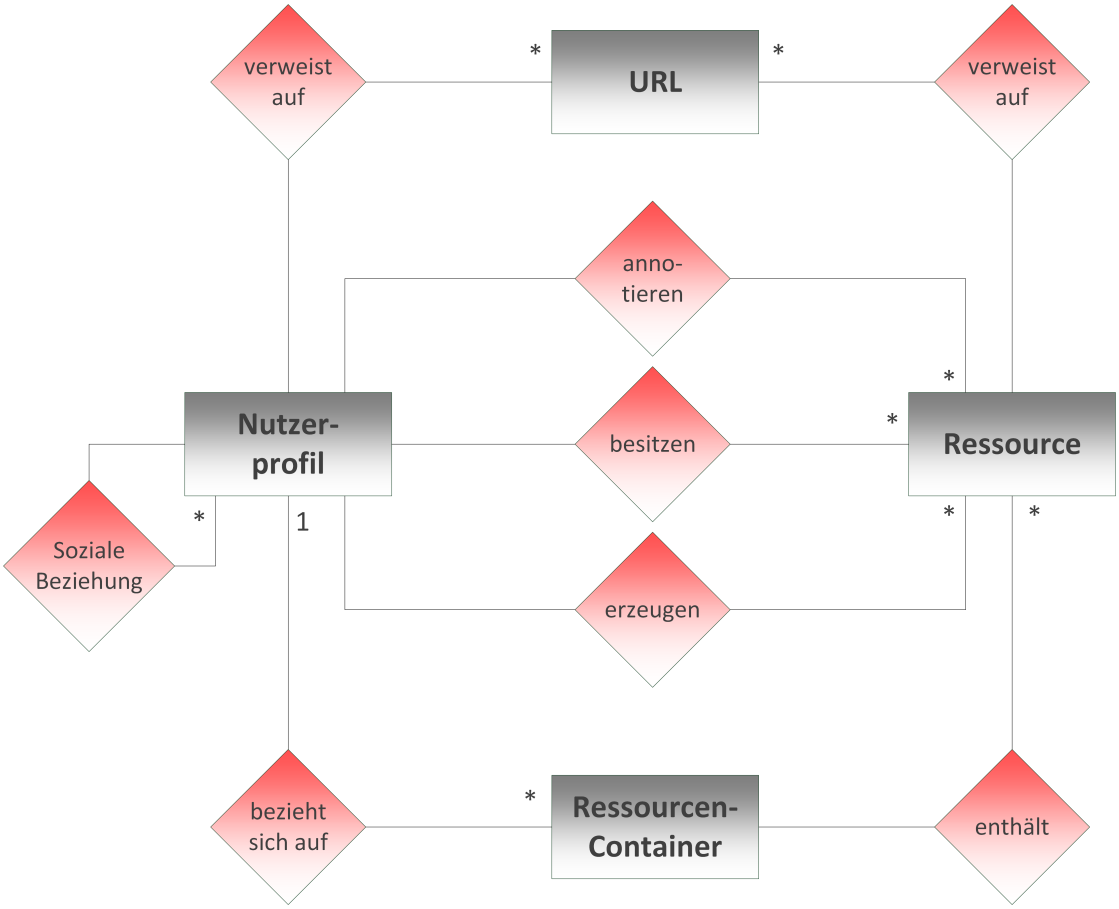


Abbildung 6.2.: Das vorgestellte Metamodell eines sozialen Netzes als Entity-Relationship-Diagramm in Chen-Notation.

6.2. Extrahierbare Metadaten

Dieser Abschnitt gibt einen Überblick über die extrahierbaren Metadaten anhand von Beispielen. Für die in dieser Arbeit herangezogenen Netze erfolgt eine Betrachtung der von diesen zur Verfügung gestellten Metadaten im weiteren Verlauf dieses Kapitels.

Abbildung 6.3 zeigt einen Ausschnitt aus dem Entity-Relationship Diagramm aus Abbildung 6.2. Dieser Ausschnitt wurde beispielhaft mit Attributen ergänzt, die in sozialen Netzen verfügbar sind. Ein Attribut ist hierbei als ein Metadatum zu sehen. Zu beachten ist, dass in diesem Beispiel nicht nur eine Annotierung verschiedene Daten liefert, sondern auch das Nutzerprofil mehrere Daten bereithält, die für eine Profilzuordnung zweckmäßig sein können. Darüber hinaus ist dieses Beispiel ebenso auf die Zweige *besitzen* und *erzeugen* des Entity-Relationship Diagramms anwendbar.

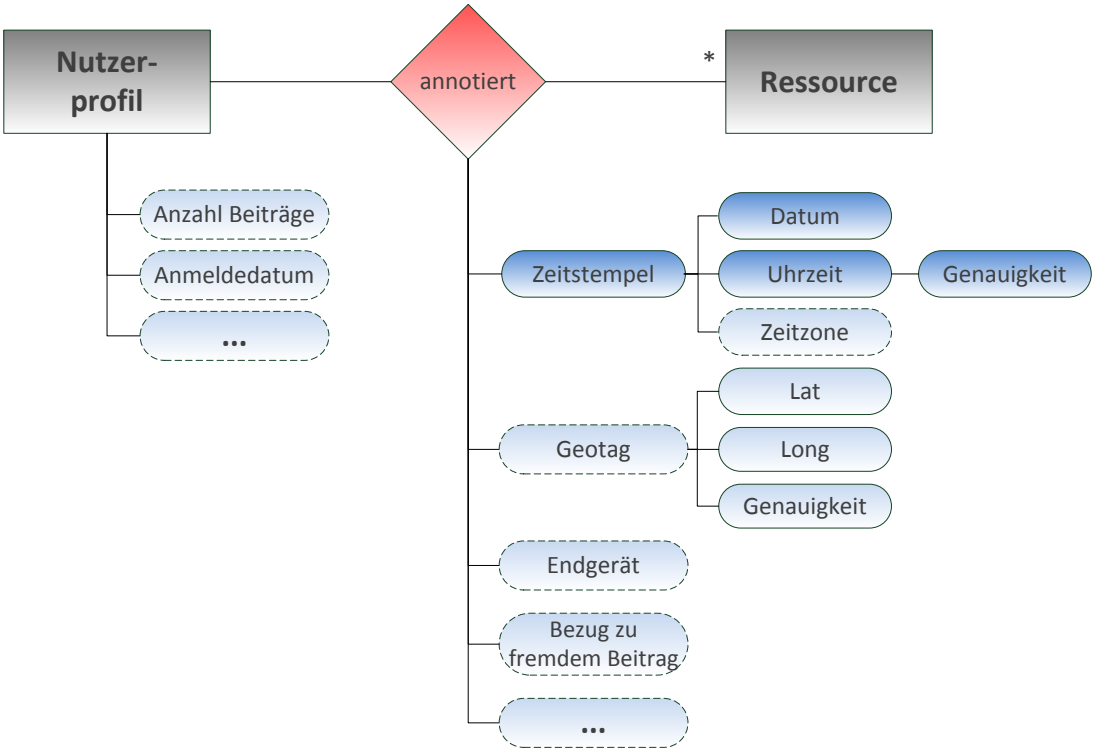


Abbildung 6.3.: Ausschnitt des Entity-Relationship-Diagramms mit beispielhaft ergänzten Attributen.

Dunkel eingefärbte Attribute, welche mit einer durchgezogenen Linie umrandet sind, stellen hierbei Attribute dar, die immer vorhanden sind. Hellblaue Attribute, mit einer gestrichelten Linie umrandet, sind optional; hier hängt es vom Nutzer und dem sozialen Netz ab, ob diese Informationen zur Verfügung stehen. Ist die Linie durchgezogen, so ist dieses Attribut vorhanden, wenn das optionale Attribut, von dem es abhängt, vorhanden ist.

Die nachfolgenden Abschnitte gehen auf verschiedene, häufig oder sogar immer zur Verfügung stehende Metadaten ein und beleuchten, wie diese für Profilzuordnungen eingesetzt werden können bzw. welche Rückschlüsse diese ermöglichen.

6.2.1. IDs

Identification Numbers oder kurz IDs finden sich in sozialen Netzen für nahezu jede Art von Ressource, beispielsweise User-IDs, Media-IDs, Tweet-IDs usw. Der Grund ist, dass die Speicherung der Daten eines sozialen Netzes typischerweise in Datenbanken erfolgt. Hierfür ist für jeden Datensatz eine eindeutige Adressierung erforderlich. Dies erfolgt typischerweise über IDs. Diese repräsentieren innerhalb der Datenbank den Primärschlüssel, werden jedoch auch auf den Websiten zur Adressierung eingesetzt. Dies erspart eine Übersetzung der

verschiedenen Adressierungsschemata und macht Webanfragen effizienter.

In kleinen und mittelgroßen Datenbanken erfolgt die Vergabe einer ID inkrementell. Hierdurch ergibt sich zwangsläufig eine chronologische Ordnung der IDs, daher spricht man auch von einer logischen Uhr. Es kann anhand einer ID zwar meist nicht der absolute Zeitpunkt ermittelt werden, wann diese vergeben wurde, aber sie ermöglicht es, grob auf einen Zeitraum zu schließen bzw. diesen abzuschätzen.

Eine inkrementelle ID-Vergabe bedeutet jedoch, dass bei der Abarbeitung ein Flaschenhals entstehen kann, aufgrund einer einzigen, zentralen Instanz. Daher wurde, beispielsweise bei Twitter, wo dies nicht von vornherein bedacht wurde, 2010 nachträglich ein ID-Schema eingeführt, das eine parallele Abarbeitung ermöglicht. Vergleichbare Methoden wurden auch von anderen Netzen übernommen. Dabei können im Aufbau von ausgewählten oder sogar allen IDs auch der Vergabezeitstempel und weitere Informationen kodiert sein. Eine detaillierte Beschreibung von Twitters und Instagrams ID-Schema ist im Abschnitt 7.1 enthalten, siehe hierzu auch [326] und [327].

In seltenen Fällen werden IDs auch mittels eines Hashes oder unbekannten Algorithmus erzeugt. Dies ist beispielsweise bei Youtube der Fall. Video-IDs bestehen aus einer quasi-zufälligen Zeichenkette. Da Youtube eines der wenigen sozialen Netze ist, wo alles öffentlich zugänglich ist, soll so verhindert werden, dass Videos systematisch gecrawlt werden. Dies verhindert, dass anhand der IDs eine chronologische Ordnung bestimmt werden kann.

6.2.2. URLs

Unified Ressource Locator (URLs) stellen einen Sonderfall dar. Dabei handelt es sich nicht um reine Metadaten, sondern es hängt von der Betrachtungsweise ab. Zwar kann ein Nutzer die URLs, die er verschickt, selbst wählen, insbesondere wenn diese im Fließtext übertragen werden, allerdings stellt ein zufälliger Verweis nicht zwangsläufig eine gültige Ressource dar. Der Nutzer kann bei Domains, die unter seiner Kontrolle stehen, zwar nahezu beliebige URLs generieren, wenn man jedoch von unabhängig kontrollierten Domains ausgeht, kann ein Nutzer nur auf vorhandene Ressourcen verweisen. Dies schränkt den Raum gültiger URLs daher stark ein. Hinzu kommt, dass eine URL weitere Metadaten enthalten kann. Beispielsweise enthält eine URL von Instagram, die ein Foto verlinkt, auch die entsprechende Media-ID. Aus dieser wiederum lassen sich Informationen wie Zeitstempel extrahieren. Der Aufbau einer Instagram URL sieht folgendermaßen aus: `https://www.instagram.com/p/BQchHqQAQhl`. Die letzten elf Zeichen entsprechen der Media-ID kodiert im Base64url Format. Abbildung 7.2 im Abschnitt 7.1.2 zeigt beispielhaft die Umwandlung und die enthaltenen Informationen der Media-ID und damit auch der URL. Darüber hinaus sind potentiell Metadaten in der Ressource, auf die verwiesen wird, enthalten. Beispielsweise kann der Erstellzeitpunkt einer Webseite abgefragt werden. So es sich nicht um eine dynamisch generierte Seite handelt, dann entspricht die Metainformation genau dem Zeitpunkt der Anfrage, können unter anderem hieraus weitere Informationen gewonnen werden.

6.2.3. Zeitstempel

Zeitstempel können in diversen Darstellungsformaten kodiert werden, siehe hierzu auch die entsprechende ISO-Norm 8601 [328], und enthalten die Informationen, die auch in Abbildung 6.4 dargestellt sind.

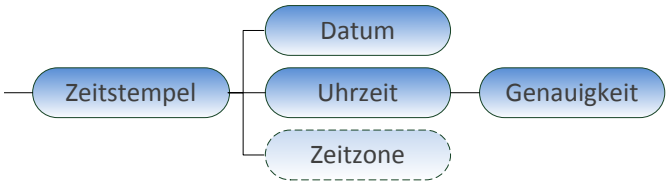


Abbildung 6.4.: Informationen eines Zeitstempels.

Die beinhalteten Informationen eines Zeitstempels sind das Datum und die Uhrzeit. Wobei die Uhrzeit in unterschiedlicher Genauigkeit vorliegen kann, beschränkt auf die Stunden und Minuten mit oder ohne Sekunden oder sogar bis auf die Millisekunde genau. Für die Analysen dieser Arbeit ist eine möglichst hohe Genauigkeit wünschenswert. Darüber hinaus kann die Zeitzone im Zeitstempel enthalten sein, ist jedoch optional, beispielsweise als numerische Abweichung des Offsets zu UTC oder als textuelle Angabe MEZ.

Neben verschiedenen Darstellungsvarianten von Zeitstempeln können diese in unterschiedlichen Formaten abrufbar sein. Auf einer Website ist gewöhnlich das Datum und die Uhrzeit angegeben, wird jedoch ein soziales Netz mittels einer öffentlichen API angesprochen, wird der Zeitstempel meist als Unixzeit zurückgeliefert. Die Unixzeit ist die Anzahl an Sekunden die seit dem 01.01.1970 00:00 Uhr UTC vergangen sind. Vereinzelte soziale Netze nutzen nicht die Unixzeit sondern zählen die Sekunden seit einem selbstgewähltem Zeitpunkt. Um solche Zeitstempel in die Unixzeit zu konvertieren, muss ein entsprechender Wert zum Zeitstempel des sozialen Netzes addiert werden.

6.2.4. Geotags

Ein Geotag beinhaltet die Informationen, die in Abbildung 6.5 dargestellt sind, wobei einzelne Attribute optional sind.
Generell kann ein Geotag auch einzelne oder eine Kombination der hier optional dargestellten Attribute ohne Längen- und Breitengrade, Longitude (Long) und Latitude (Lat) enthalten. Im Rahmen dieser Arbeit liegt der Fokus jedoch auf maschinell erstellten Geotags. Da hierfür mittels GPS Längen- und Breitengrad ermittelt werden, wird in dieser Arbeit ein Geotag mit den Mindestinformationen Längen- und Breitengrad und der Genauigkeit dieser Werte, definiert. Eine Koordinate bestehend aus Längen- und Breitengrad entspricht einem Bereich im World Geodetic System (WGS), einem globalen Referenzsystem, welches in der Version WGS 84 bei GPS zum Einsatz kommt [329]. Das WGS 84 definiert den Äquatorradius der Erde mit 6.378,137 km [330]. Hierdurch lässt sich die Auflösung eines Geotags bzw. die Länge eines Kreisbogens l

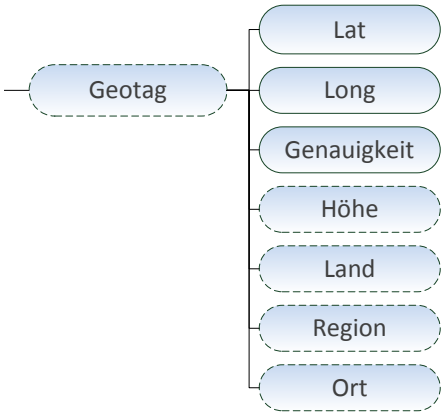


Abbildung 6.5.: Informationen eines Geotags.

Tabelle 6.1.: Genauigkeit von Geotags in Abhängigkeit der Nachkommastellen

Stellen	Grad	Kreisbogenlänge
0	1	111,32 km
1	0,1	11,13 km
2	0,01	1,11 km
3	0,001	111,32 m
4	0,0001	11,13 m
5	0,00001	1,11 m
6	0,000001	111,32 mm
7	0,0000001	11,13 mm
8	0,00000001	1,13 mm
9	0,000000001	0,11 mm

in Abhängigkeit des Gradbereichs α und damit der Genauigkeit anhand der folgenden Formel ermitteln:

$$l = \Pi * 6.378,137km * \frac{\alpha}{180°}$$

Die Tabelle 6.1 zeigt die Auflösung einer Geo-Koordinate in Abhängigkeit von der Anzahl der Nachkommastellen. Die Kreisbogenlänge bestimmt dabei den Bereich, der durch das Geotag repräsentiert wird, da diese Werte sowohl für Längen- als auch für Breitengrad gelten. In der Theorie ergibt sich so eine quadratische Fläche, aufgrund der Kugelform der Erde nimmt die Breite mit abnehmender Distanz zu den Polen jedoch ab, so dass sich eine entsprechende Trapezform ergibt.

Die Verteilung der Anzahl an Nachkommastellen zeigt Tabelle 6.2 anhand der Geotags aus einem Twitter-Datensatz vom Zeitraum 14.-15. August 2015. Die Verteilung zeigt, dass über 98,5 % aller Geotags eine Auflösung von 11,13 m oder weniger aufweisen, also noch genauer sind.

Tabelle 6.2.: Verteilung der Geotag-Genauigkeit im Bezug auf die Nachkommastellen anhand eines Twitter-Datensatzes vom 14.-15. August 2015 [34]

Stellen	% von Tweets
1	0,278
2	0,496
3	0,632
4	5,237
5	17,850
6	72,878
7	1,177
8	1,453

6.2.5. Areas

Eng verwandt mit Geotags sind Areas. Dabei handelt es sich um eine Kombination aus zwei Geotags, die ein Rechteck aufspannen, also keinen Punkt, sondern eine Fläche definieren. Wobei eine Punktdefinition nicht ausgeschlossen ist, dann sind beide Geotags identisch. Die zugehörigen Informationen sind in Abbildung 6.6 dargestellt.

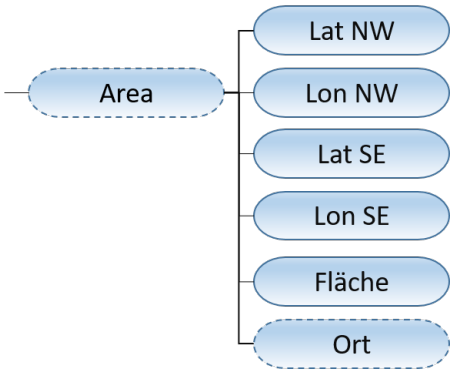


Abbildung 6.6.: Informationen einer Area.

Typischerweise definiert ein Geotag den nordwestlichen (NW) und ein weiteres den südöstlichen (WE) Punkt des aufgespannten Rechtecks. Daraus lässt sich stets die abgedeckte Fläche anhand der bereits in Tabelle 6.2 erläuterten Strecken des Kreisbogenmaßes näherungsweise berechnen. Der Ort ist optional. Dieser kann etwas darüber aussagen, was sich dort befindet, bspw. eine Sehenswürdigkeit.

Die Tabelle 6.3 gibt einen Überblick über die typische Ausdehnung von Areas. Hierzu wurde getrennt für Latitude und Longitude die Differenzen zwischen NW und SE Koordinaten ermittelt und entsprechend ihrem Delta erfasst. Dabei wurden 7.464.898 Areas ausgewertet. Bei etwa 1,1% der Areas handelt es sich um Punktkoordinaten, die beiden Geotags sind also identisch.

Das häufigste anzutreffende Delta liegt zwischen 0,1 und 0,2 Grad, was in etwa 11 bis 22 km entspricht.

Tabelle 6.3.: Verteilung der Area Flächenabdeckung anhand eines gecrawlten Twitter-Datensatzes

Abdeckung	**% Lat**	**cum. % Lat**	**% Lon**	**cum. % Lon**
Geotag	1,121851	1,121851	1,121851	1,121851
>0 & <=0,001	0,000027	1,121877	0,000067	1,121918
>0,001 & <= 0,002	0,001393	1,123271	0,000482	1,122400
>0,002 & <= 0,003	0,005466	1,128736	0,002585	1,124985
>0,003 & <= 0,004	0,032727	1,161463	0,010851	1,135836
>0,004 & <= 0,005	0,027663	1,189125	0,010034	1,145870
>0,005 & <= 0,006	0,041635	1,230760	0,017334	1,163204
>0,006 & <= 0,007	0,081810	1,312570	0,028051	1,191255
>0,007 & <= 0,008	0,074803	1,387373	0,016249	1,207505
>0,008 & <= 0,009	0,078420	1,465794	0,027315	1,234819
>0,009 & <= 0,01	0,145548	1,611342	0,066016	1,300835
>0,01 & <= 0,02	1,792161	3,403503	1,030007	2,330842
>0,02 & <= 0,03	2,590806	5,994308	1,663961	3,994803
>0,03 & <= 0,04	2,846683	8,840992	2,149982	6,144786
>0,04 & <= 0,05	3,315022	12,156013	2,056465	8,201251
>0,05 & <= 0,06	4,096131	16,252144	2,389155	10,590406
>0,06 & <= 0,07	3,452278	19,704422	2,889591	13,479997
>0,07 & <= 0,08	3,143646	22,848068	3,119225	16,599222
>0,08 & <= 0,09	3,766401	26,614469	2,712643	19,311865
>0,09 & <= 0,1	3,332785	29,947254	2,781512	22,093376
>0,1 & <= 0,2	25,328799	55,276053	23,959684	46,053061
>0,2 & <= 0,3	11,170976	66,447030	13,386211	59,439272
>0,3 & <= 0,4	7,295572	73,742602	9,163782	68,603054
>0,4 & <= 0,5	5,061436	78,804037	7,001676	75,604730
>0,5 & <= 0,6	3,045521	81,849558	3,712830	79,317561
>0,6 & <= 0,7	3,766589	85,616146	1,986377	81,303937
>0,7 & <= 0,8	0,959879	86,576026	2,992821	84,296758
>0,8 & <= 0,9	0,329690	86,905715	1,121234	85,417992
>0,9 & <= 1,0	0,682796	87,588511	0,795831	86,213824
>1,0	12,411489	100,000000	13,786176	100,000000

6.2.6. Weitere Ressourcen-bezogene Metadaten

In diesem Abschnitt werden verschiedene Metadaten diskutiert, die aus manchen sozialen Netzen extrahiert werden können. Da diese keine so aussagekräftigen und vielfältig auswertbaren Informationen beinhalten, erfolgt deren Betrachtung in der nachfolgenden Liste:

- **Quelle**: Dieses Attribut gibt Aufschluss darüber, auf welchem Weg eine Ressourcen-bezogene Aktion durchgeführt wurde. Dies kann beispielsweise eine bestimmte Client-anwendung, ggf. deren Versionsstand, auf einem Smartphone oder die Webseite des sozialen Netzes sein.

- **Endgerät**: Bestimmte Clientanwendungen übertragen Informationen über das verwendete Endgerät, beispielsweise um welches Endgerätemodell es sich handelt. Dies kann auch Informationen über das verwendete Betriebssystem einschließen.

- **Bezug zu fremdem Beitrag**: Der Bezug zu einem fremden Beitrag ist insofern relevant, als dass anhand des Beitrages, auf den sich bezogen wird, eine Zeitdifferenz zwischen beiden Ereignissen ermittelt werden kann. Ist diese Differenz hinreichend gering, ist von einer automatisierten Reaktion auszugehen. Erfolgt diese im gleichen Netz, so liegt der Verdacht nahe, dass es sich um einen Bot handelt. Bei unterschiedlichen kann dies ein automatischer Verweis eines Nutzers auf seinen neu eingestellten Inhalt in einem anderen Netz hindeuten und damit ein potentieller Profile-Match. Eine detaillierte Betrachtung dieses Zusammenhangs erfolgt im nächsten Kapitel.

6.2.7. Nutzerprofil-bezogene Metadaten

Zu den Ressourcen-bezogenen Metadaten kommen noch Nutzerprofil-bezogene hinzu. Diese fallen nicht bei einem Ereignis an, so dass potentiell nur ihr aktueller Wert ermittelt werden kann. Twitter beispielsweise liefert jedoch die folgenden Metadaten auch bei jedem API-Abruf, teils auch mit dem aktuellen Stand zum Zeitpunkt der Ressourcen-bezogenen Aktion, die über die API abgefragt wird, mit. Nachfolgende Liste fasst die Nutzerprofil-bezogenen Metadaten zusammen:

- **Anzahl Beiträge**: Anhand der Anzahl an Beiträgen lässt sich abschätzen, wie aktiv dieses Profil genutzt wird. Dies erlaubt Rückschlüsse auf das ungefähre Anmeldedatum anhand des aktuellen Verhaltens und der durchschnittlich durchgeführten Aktionen.

- **Anmeldedatum**: Das Anmeldedatum lässt Rückschlüsse zu, beispielsweise ob ein Profil für exzessiven Spamversand genutzt wird bzw. wurde. Wenn das Profil schon länger existiert, ist davon auszugehen, dass es nicht negativ aufgefallen ist, sonst hätte das entsprechende soziale Netz den Account mit hoher Wahrscheinlichkeit bereits gelöscht. In Kombination mit der Anzahl der Beiträge, lässt sich die durchschnittliche Anzahl an Aktionen pro Tag ermitteln. Besonders hohe Werte können hierbei dazu dienen, Bots zu identifizieren.

- **Zeitzone**: Die Zeitzone, so diese im Profil hinterlegt ist, ist durch den Nutzer festlegbar. Um diese zu verwenden zu können, sollte deren Korrektheit mithilfe von Geotags verifiziert werden. Umgekehrt kann anhand von Zeitstempeln ungefähr die Zeitzone geschätzt werden, deutliche Abweichungen von der angegebenen Zeitzone deuten auf ein Fake-Profil hin.

- **Verifiziertes Profil**: Bestimmte soziale Netze bieten die Möglichkeit, das eigene Profil zu verifizieren. Dies kann auf unterschiedliche Weisen erfolgen. Beispielsweise dadurch, dass

eine Kopie oder eindeutige Informationen des Personalausweises eingeschickt werden oder an die hinterlegte Adresse ein Brief verschickt wird. Verifizierte Profile werden nach erfolgreicher Überprüfung entsprechend kenntlich gemacht. Die Wahrscheinlichkeit, dass es sich bei einem verifizierten Profil um eine Fälschung handelt, ist folglich als weitaus geringer anzusehen.

6.3. Auswahl der sozialen Netze für die Evaluation

Für die Evaluation der Verfahren in dieser Arbeit musste die Auswahl sozialer Netze aufgrund deren Vielzahl eingegrenzt werden. Das Extrahieren der Metadaten und deren Speicherung ist für eine größere Anzahl an Netzen in diesem Rahmen nicht möglich. Auch der Berechnungsaufwand wächst drastisch, daher wurde die Anzahl der sozialen Netze für die Evaluation auf drei begrenzt.

Für die Auswahl dieser drei Netze wurden die folgenden Kriterien herangezogen. Die Eingrenzung erfolgte hierbei in der nachfolgend aufgeführten Reihenfolge.

- **Größe und Popularität**: Das soziale Netz sollte eine ausreichend großen Nutzerzahl aufweisen, welche auch direkt von dessen Popularität bestimmt wird. Dies ist notwendig, um die Qualität der Ergebnisse entsprechend beurteilen zu können. Finden sich nur wenige Nutzer, reduziert dies zum einen die Möglichkeiten, die in Frage kommen, zum anderen ist der Unterschied zwischen den Nutzern um so größer, da diese im Schnitt weiter auseinander leben, was sich auf Geotags und Zeitstempel auswirkt.

- **Zugänglichkeit der Daten**: Um den Prozess der Datenbeschaffung möglichst effizient zu gestalten, ist es erforderlich, dass das Netz eine entsprechende API bereitstellt, die ohne Autorisierung durch Nutzer angefragt werden kann. Darüber hinaus sollten möglichst wenig Anfragen erforderlich sein, um die Daten eines Nutzers vollständig zu erhalten, da dies aufgrund entsprechender Limitieren den Beschaffungsprozess stark verlangsamt.

- **Wahrscheinlichkeit von Profilbeziehungen**: Damit auch entsprechend detektierbare Profilbeziehungen wahrscheinlich sind, sollten Netze mit möglichst unterschiedlichen Einsatzgebieten gewählt werden, da nicht davon auszugehen ist, dass ein Nutzer ein und dasselbe auf mehreren Netzen tut.

- **Verfügbarkeit von Metadaten**: Um die Verfahren entsprechend zu evaluieren, ist es für jede Art von Metadaten erforderlich, dass entsprechende Daten von mindestens zwei sozialen Netzen verfügbar sind. Dennoch wird eine gewisse Diversität der Metadaten angestrebt, um ggf. entsprechende Korrelationen zu detektieren bzw. Abbildungen aufeinander zu ermöglichen.

6.3.1. Größe und Popularität

Tabelle 6.4 gibt einen Überblick über soziale Netze mit mehr als 100 Millionen aktiven Nutzern pro Monat. Einzelne dieser Netze veröffentlichen keine aktuellen Nutzerzahlen, diese sind daher

entweder veraltet und liegen wahrscheinlich höher oder wurden von Experten ermittelt oder geschätzt.

Tabelle 6.4.: Übersicht sozialer Netze mit einer Nutzerzahl von mehr als 100 Millionen aktiven Nutzern pro Monat. Ein * bedeutet, dass das Netz keine oder keine aktuellen Nutzerzahlen veröffentlicht.

Netz	Nutzer in Mio.		Nutzungsland
Facebook	1.860	[2]	global
Youtube	1.000	[331]	global
Qzone	632	[332]	China
Instagram	600	[4]	global
Tumblr	550*	[333]	global
Twitter	313	[3]	global
Baidu Tieba	300*	[334]	China
Sina Weibo	297	[335]	China
Pinterest	150	[336]	global
YY	142	[337]	China
Google+	111*	[338]	global
LinkedIn	106	[339]	global

- **global** : Netze dieser Kategorie sind typischerweise in den USA beheimatet. Auch wenn die Nutzerzahlen im Ländervergleich stark schwanken können, so ist der Zugriff prinzipiell weltweit möglich.
- **China** : Diese sozialen Netze haben ihren Ursprung in China. Trotz der immensen Nutzerzahlen sind fast ausschließlich Chinesen Mitglieder.

Aufgrund der Sprachbarriere und der Tatsache, dass der Zugriff von außerhalb Chinas auf Netze dieses Landes sehr eingeschränkt ist oder sogar blockiert wird, ist die Nutzung für die Evaluation dieser Arbeit unmöglich. Daher werden diese im weiteren Verlauf nicht weiter betrachtet.
Die Anzahl der Profile von Google+ ist zwar sehr hoch, die aktiv genutzte Zahl liegt jedoch nur bei ca. 1%, vgl. [340]. Ohne Nutzung gibt es keine Metadaten. Für die weitere Betrachtung kommt daher auch Google+ nicht in Frage und wurde während dieser Arbeit durch Google wegen der geringen Nutzerzahlen eingestellt [341].

6.3.2. Zugänglichkeit der Daten

Tabelle 6.5 gibt einen Überblick über soziale Netze mit mehr als 100 Millionen aktiven Nutzern pro Monat und einer Wertung der Abfragbarkeit der Daten bzw. Metadaten. Die Zugänglichkeit lässt sich herbei in die folgenden Kategorien aufgliedern.

- **+** : Diese Kategorie der Zugänglichkeit trifft auf soziale Netze zu, deren Seiten ohne explizite Einschränkung eines Nutzers, so diese überhaupt möglich ist, typischerweise

Tabelle 6.5.: Übersicht sozialer Netze mit einer Nutzerzahl von mehr als 100 Millionen aktiven Nutzern pro Monat und einer Wertung der Abfragbarkeit der Daten bzw. Metadaten.

Netz	Zugänglichkeit
Facebook	-
Youtube	+
Instagram	o
Tumblr	+
Twitter	+
Pinterest	+
LinkedIn	-

vollständig ohne Anmeldung einsehbar sind. Darüber hinaus kann eine öffentliche API verfügbar sein, die zwar Limitierungen aufweisen kann, im Bezug auf die Häufigkeit der Anfragen, nicht jedoch auf einen bestimmten Personenkreis, der eine Anwendung explizit autorisiert haben muss.

- **o** : In diese Kategorie fallen soziale Netze die entweder öffentlich einsehbar sind oder eine API bereitstellen, die im Hinblick auf den anfragbaren Personenkreis keine Einschränkungen aufweist.

- **-** : Soziale Netze dieser Kategorie sind nicht ohne Anmeldung einsehbar. Facebook ermöglicht seinen Nutzern, diese Einschränkung aufzuheben. Hiervon machen gewöhnlich vor allem Firmen Gebrauch. Außerdem existiert keine öffentliche API oder es sind nur die Profile von Nutzern einsehbar, die die anfragende Anwendung explizit autorisiert haben.

Aufgrund der schlechten Zugänglichkeit der Daten bei Facebook und LinkedIn werden diese für die Evaluation nicht herangezogen.

6.3.3. Wahrscheinlichkeit von Profilbeziehungen

Tabelle 6.6.: Übersicht über die verbliebenen sozialen Netze die für die Evaluation infrage kommen und deren Fokussierung.

Netz	Nutzung
Youtube	Video
Instagram	Foto
Tumblr	Blog
Twitter	Microblog
Pinterest	Foto

- **Video**: Typische Nutzung dieser Netze ist das Anschauen und Zurverfügungstellen von Videos. Dies können aus allen Bereichen kommen oder auf ein Themengebiet eingegrenzt sein.
- **Foto**: Auf diesen Netzen veröffentlichen Nutzer Bilder und Fotos, um sie mit Freuden und Bekannten zu teilen. Häufig erfolgt jedoch keine Eingrenzung auf bestimmte Personengruppen, so dass diese für alle einsehbar sind.
- **Blog**: Ein Blog ist vergleichbar mit einem öffentlichen Tagebuch. Nutzer schreiben über Dinge, die sie bewegen und beschäftigen. Darüber hinaus gibt es auch Themenblogs, wo ein Nutzer über Aspekte eines oder mehrerer Themen schreiben. Microblogs als Spezialform von Blogs unterscheiden sich darin, dass die Länge einer Nachricht stark limitiert ist. Das Limit bei Twitter seit Gründung lag bei 140 Zeichen. Es wurde inzwischen auf 280 Zeichen angehoben, dennoch zwingt diese Länge Nutzer, sich kurz und prägnant auszudrücken, siehe [342].

Wie bereits erläutert, ist davon auszugehen, dass die Wahrscheinlichkeit von Profilzuordnungen innerhalb eines Nutzungstyps sehr gering ausfällt. Aus diesem Grund wurde Pinterest im Vergleich zu Instagram, bedingt durch die deutlich geringere Größe und Popularität, aus der Kandidatenmenge entfernt. Eine parallele Nutzung von Blogs und Microblogs tritt häufiger auf, dennoch wurde zur Eingrenzung Twitter der Vorzug gegeben. Grund ist, dass die Datenzugänglichkeit besser und die abzufragenden Datenmengen deutlich geringer ausfallen. Denn um möglichst alle Metadaten zu erhalten, müssen auch die Nutzerinhalte abgerufen werden. Hierbei birgt die Zeichenlimitierung entscheidendes Einsparpotential.

6.3.4. Verfügbarkeit von Metadaten

Die Verfügbarkeit der häufigsten und für Profilzuordnung am geeignetsten Metadaten für die drei verbleibenden Netze, Twitter, Instagram und Youtube ist in Tabelle 6.7 dargestellt.

- ✓ : Dieses Metadatum ist für jedes Element, dem es sinnvoll zugeordnet werden kann, existent und kann abgefragt werden.
- ○ : Informationen dieser Kategorie sind optional bzw. nur manchmal verfügbar. Es hängt hierbei von den Einstellungen des Nutzers oder der Art der Nutzung ab, ob diese Informationen abrufbar sind.
- ✗ : Diese Metadaten werden entweder nicht erhoben und gespeichert oder sind zumindest nicht abfrag- oder ermittelbar.

6.3.5. Twitter

Twitter stellt eine Vielzahl an Metadaten zur Verfügung, die über den Umfang in Tabelle 6.7 hinausgehen. Im Abschnitt A.1 ist beispielhaft der Datensatz eines einzelnen Tweets enthalten, der aufzeigt, welche Metadaten darin enthalten sind. Aufgrund des Umfangs der verfügbaren Daten und der Leichtigkeit der Datenabfrage stellt Twitter die ideale Plattform für jedwede

Tabelle 6.7.: Übersicht extrahierbarer und nutzbarer Metadaten der für die Evaluation ausgewählten sozialen Netze

Metadatum		**Twitter**	**Instagram**	**Youtube**
chronologische	User-IDs	✓	○	✗
	Ressourcen-IDs	✓	✓	✗
Zeitstempel	Datum	✓	✓	✓
	Uhrzeit	✓	✓	✓
	Genauigkeit	ms	ms	ms
	Zeitzone	✓	✓	✓
Geotag	Lat / Long	○	○	○
	Genauigkeit	○	○	○
	Höhe	✗	✗	○
	Land	○	○	✗
	Region	○	○	✗
	Ort	○	○	✗
Quelle	Client	✓	✗	✗
	Endgerät	✗	✗	✗
Bezug zu fremdem Inhalt		○	○	○
Profil	Anzahl Beiträge	✓	○	○
	Anmeldedatum	✓	✗	✓
	verifiziert	✓	✗	○

Analysen im Kontext sozialer Netze dar. Twitter bietet auch einen eigenen API Zugang für Forscher, allerdings ist inzwischen bei Twitter generell eine Freischaltung erforderlich. Einfach anmelden und den API Zugang aktivieren, wie noch vor wenigen Jahren funktioniert nicht mehr. Es muss eine Art Antrag mit Begründung gestellt werden.

6.3.6. Instagram

Der verfügbare Datenumfang bei Instagram ist nicht annähernd mit dem von Twitter vergleichbar. Nichtsdestotrotz ist es ein stark frequentiertes Netz. Dies führt dazu, dass zwar pro Interaktion mit dem Netz wenige Metadaten gespeichert werden, aber von diesen dafür viele Werte zur Verfügung stehen. Dies ist natürlich besonders bei Metadaten relevant, die über eine Zählvariable, bspw. Anzahl Fotos, hinausgehen. Besonders zu nennen sind hier Zeitstempel oder Geotags. Geotags sind jedoch nur verfügbar, wenn ein Nutzer diese dem Bild explizit hinzufügt. Instagram hat erst kürzlich seine API durch neue ersetzt, was unter anderem zu einem eingeschränkteren Funktionsumfang und damit beschränkterem Zugriff auf die Metadaten führt, zumindest für private Profile. Zudem ist wie bei Twitter eine explizite Freischaltung von Instagram notwendig.

6.3.7. Youtube

Wie bei Instagram hat auch Youtube seine APIs kürzlich angepasst. Auch hier ist zunächst eine Freischaltung notwendig. Einige der mit ○bezeichneten Metadaten sind nicht nur optional. Sie lassen sich nicht direkt, sondern nur über Umwege ermitteln. Beispielsweise ist laut API Dokumentation die Anzahl an Videos nicht Teil der Nutzerprofilabfrage. Über entsprechende Listenfunktionen sollte sich das allerdings ermitteln lassen.

6.4. Zusammenfassung

In diesem Abschnitt wurde anhand eines Metamodells die häufigsten und sinnvoll für die Profilzuordnung einsetzbaren Metadaten eingeführt. Darüber hinaus wurde eine Auswahl der für die Evaluation zu nutzenden sozialen Netze hergeleitet. Aufgrund von Vorfällen wie dem Skandal um Boston Analytica [343], haben einige soziale Netze ihre Maßnahmen hinsichtlich Datenschutz verstärkt. Dies wirkt sich stark auf den Analysebereich sozialer Netze aus, da der Zugang zu den Daten insgesamt erschwert wird. Aus diesem Grund kommt Youtube im Rahmen der Arbeit nicht zum Einsatz, auch wenn es hier als mehr oder weniger geeignet bewertet wird.

KAPITEL 7

Rahmenbedingungen der Profilzuordnung

Nachdem im vorangegangenen Kapitel die Metadaten identifiziert wurden, die sich potentiell für Profilzuordnungen eignen, werden in diesem Kapitel die Rahmenbedingungen der Verfahren diskutiert, die in den nachfolgenden Kapitel detailliert werden. Darüber hinaus werden Grundlagen, deren Kenntnis für mehrere Verfahren erforderlich sind, im Vorfeld erläutert und die verwendeten Datensätze vorgestellt.

7.1. Grundlagen

Es gibt Eigenheiten bestimmter sozialer Netze, die es erst ermöglichen, bestimmte Metadaten zu erhalten. Hierzu zählt beispielsweise ein Zeitstempel mit Millisekundengenauigkeit. Typischerweise sind Datumsangaben auf Webseiten auf eine Genauigkeit von Minuten, bestenfalls von Sekunden beschränkt. Wie nun dennoch entsprechend genaue Zeitstempel für manche Netze erhalten werden können, zeigen die nachfolgenden Unterabschnitte. Da dieses Wissen für mehrere Ansätze dieser Arbeit relevant ist, wird es in der Beschreibung der Verfahren als Grundwissen vorausgesetzt.

7.1.1. Twitter-IDs

Twitters Tweet-IDs werde seit der Umstellung von 32-Bit- auf 64-Bit-Integer-Werte nicht mehr inkrementell erzeugt, sondern nach einem Schema generiert. Nach diesem Schema setzt sich eine Tweet-ID aus vier Einzeldaten zusammen. Deren Bitrepräsentation wird nach dem Schema in Abbildung 7.1 aneinander gereiht.

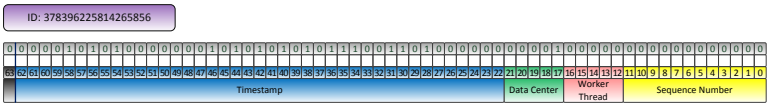


Abbildung 7.1.: Twitters Tweet-ID-Aufbau anhand der Beispiel ID 378396225814265856.

Tabelle 7.1 fasst das Tweet-ID-Schema tabellarisch zusammen und die nachfolgende Aufzählung erläutert die Einzeldaten genauer:

Tabelle 7.1.: Aufbau einer Tweet-ID.

Feld	Bits	Anzahl Bits	Anzahl mögl. Werte
Sequenznummer	0-11	12	4096
Workerthread	12-16	5	32
Datacenter	17-21	5	32
Zeitstempel	22-62	41	2.199.023.255.552
Reserviertes Bit	63	1	2, ist aber immer 0

- **Reserviertes Bit**: Das typische Format, in dem Tweet-Daten übertragen werden, ist JSON. Da dieses nicht zwischen Integer-Werten mit und ohne Vorzeichen unterscheidet, wird, um negative Zeitstempel zu vermeiden, das erste Bit stets auf 0 gesetzt.

- **Zeitstempel**: Der bekannte UNIX-Zeitstempel entspricht der Anzahl an Sekunden seit dem 1. Januar 1970 00:00:00 UTC. Twitters ID-Schema nutzt das gleiche Prinzip, zählt jedoch die Millisekunden. Im Gegensatz zum UNIX-Zeitstempel begann Twitter am 4. November 2010 um 01:42:54 UTC zu zählen. Dies entspricht dem Moment, als dieses ID-Schema aktiviert wurde. Um also einen Tweet ID-Zeitstempel in einen UNIX-Zeitstempel zu konvertieren, muss der Wert 1288834974657 addiert und das Ergebnis durch 1000 dividiert werden. Mit den verfügbaren 41 Bit kann Twitter einen Zeitraum von ungefähr 69 Jahren abdecken.

- **Datacenter**: Dieser Wert identifiziert ein konkretes Rechenzentrum von Twitter, in dem der entsprechende Workerthread den Tweet verarbeitet hat. Hierdurch kann Twitter bis zu 32 Rechenzentren betreiben, ohne das Schema anpassen zu müssen.

- **Workerthread**: Ein Workerthread ist die Instanz, die Tweets verarbeitet. Die ID der Workerthreads ist nur in Kombination mit dem Rechenzentrum eindeutig. Twitter kann damit 32 Workerthreads pro Rechenzentrum betrieben.

- **Sequenznummer**: Um die Rolle der Sequenznummern zu verstehen, muss man sich in Erinnerung rufen, dass die Zeitstempel eine Millisekunden-Genauigkeit besitzen. Dies würde jedem Workerthread erlauben, genau einen Tweet pro Millisekunde abzuarbeiten. Um dieses Limit aufzuheben, wurde eine Sequenznummer eingeführt. Diese ermöglicht eine inkrementelle Nummerierung für Tweets, die in einer Millisekunde von einem Workerthread verarbeitet werden. Aufgrund der Länge von 12 Bit können so theoretisch 4096 Tweets von einem Thread pro Millisekunde abgearbeitet werden.

Dieses ID-Schema wurde von Twitter im Laufe der Zeit auch auf weitere IDs angewandt. Beispielsweise werden inzwischen auch Nutzer-IDs auf diese Weise generiert.

7.1.2. Instagram-IDs

Instagram verwendet das gleiche Prinzip und ein ähnliches Schema wie Twitter für seine Media-IDs. Diese Media-IDs werden auch in der URL der entsprechenden Seite kodiert. Als

Beispiel sei hier die URL `https://www.instagram.com/p/BQchHqQAQhl/` genannt. Die 11 alphanumerischen Zeichen nach dem Prefix `https://www.instagram.com/p/` stellen die Media-ID dar. Diese wird in URLs mit Base64url kodiert.

Neben diesem URL-Schema verwendet Instagram auch lange URLs, diese bestehen aus dem gleichen Prefix, gefolgt von 39 Zeichen. Bei den Analysen für diese Arbeit lag der Anteil der langen Version bei etwa 22%, vgl. [327]. Da der Unterschied dieser URL-Schemata nicht dokumentiert ist, wird angenommen, dass diese Unterscheidung zum Schutz der Privatsphäre erfolgt. Bei stichprobenartigen Analysen hat sich herausgestellt, dass diese Medien vorwiegend von privaten Profilen stammen. Nachdem die Media IDs, nach einem festem Schema generiert werden, könnte es möglich sein, diese zu erraten. Dies könnte durch die lange Version verhindert werden. Hierdurch könnten nur Personen das Bild aufrufen, die für die Einsicht in das Profil autorisiert oder denen die URL eines Bildes zugänglich gemacht wurde. Analysen im Rahmen dieser Arbeit ergaben, dass die ersten 11 Zeichen der langen Version inhaltlich den 11 Zeichen der kurzen Version entsprechen. Diese werden nachfolgend erläutert und sind grafisch in Abbildung 7.2 dargestellt.

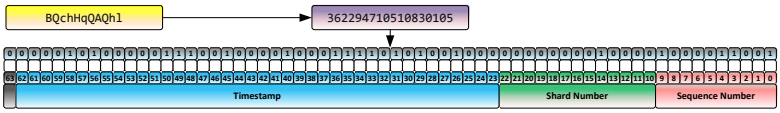


Abbildung 7.2.: Instagrams Media-ID-Aufbau anhand der Beispiel-ID 362294710510830105.

Tabelle 7.2.: Aufbau einer Media-ID.

Feld	Bits	Anzahl Bits	Anzahl mögl. Werte
Sequenznummer	0-9	12	1024
Shard Nummer	10-22	5	8192
Zeitstempel	23-62	41	1.099.511.627.776
Reserviertes Bit	63	1	2, ist aber immer 0

Tabelle 7.2 fasst dies tabellarisch zusammen. Die Einzeldaten werden nachfolgend im Detail vorgestellt, vgl. auch [344].

- **Reserviertes Bit**: Im Gegensatz zu Twitter, die ein solches reserviertes Bit nutzen, erwähnt Instagram dieses nicht, um zu verhindern, dass der Zeitstempel negativ wird. Dies schließt aber die spätere Nutzung nicht aus, da dies erst in einer entfernten Zukunft relevant wird, wenn der Zeitstempel groß genug wird. Der Instagram-ID-Generierungscode weist Variablendeklaration und Spaltendefinitionen des Datenbankschemas mit Vorzeichen auf. Um aber die zeitliche Sortierbarkeit, was ein Hauptgrund für die Nutzung des neuen ID-Schemas war, sicherstellen zu können, ist das reservierte Bit nötig.

- **Zeitstempel**: Das von Instagram genutzte Prinzip für Zeitstempel ist mit dem von Twitter identisch. Aber im Gegensatz hierzu führte Instagram dieses ID-Schema erst am 24. Au-

gust 2011 um 21:07:01 und 721 Millisekunden ein. Um also hieraus den UNIX Timestamp errechnen zu können, muss der Wert 1314220021721 addiert werden.

- **Shard Nummer**: Bei Sharding handelt es sich um eine horizontale Partitionierung von Datenbanken. Im Gegensatz zu vertikaler Partitionierung, wo Spalten oder ganze Tabellen auf zusätzliche Server verteilt werden, kennt hier jeder Server das gesamte Datenbankschema und nur die Zeilen werden über die verfügbaren Datenbankserver verteilt.
  Laut Instagram, vgl. [344], werden die Daten anhand der User-ID auf die Shards verteilt. Dies bedeutet, dass alle Daten eines konkreten Nutzers, wie Bilder und Likes, auf einem einzelnen Server vorgehalten werden können. Dies führt zu einer besseren Performance im Vergleich zu vertikaler Partitionierung und reduziert den notwendigen Aufwand für Loadbalancing.

- **Sequenznummer**: Die Sequenznummer ermöglicht wie bei Twitter die Erstellung mehr als einer ID pro Millisekunde. Im Gegensatz zu Twitter wird diese jedoch nicht für jede Millisekunde von Null beginnend inkrementiert, sondern die Inkrementierung erfolgt fortlaufend und wird bei Erreichen des Maximalwertes auf Null zurückgesetzt.

7.2. Datensätze

Im Rahmen dieser Arbeit werden zwei Typen von Datensätzen verarbeitet. Zum einen Profildaten mehrerer sozialer Netze, zwischen denen die Profilzuordnung erfolgt und so genannten Ground-Truth-Daten. Dies sind verlässliche Informationen über die korrekte Profilzuordnung der Profildaten.

7.2.1. Profildaten

Da für jedes Verfahren teils unterschiedliche Metadaten erforderlich sind und sich hierdurch die verwendeten Profildatensätze unterscheiden, werden deren Eigenschaften im Detail im Abschnitt des entsprechenden Verfahrens erläutert.

7.2.2. Ground-Truth-Daten

Für die Erhebung der Groundtruth-Daten wurden für diese Arbeit zwei Methoden herangezogen. Zum einen eine verlässliche Profilzuordnung, die eine variable Zuordnungsgenauigkeit bietet und entsprechend parametrisiert wurde, dass sichergestellt ist, dass es sich um korrekte Zuordnungen handelt. Das Prinzip entspricht dabei dem des Verfahrens aus Abschnitt 9. Zum anderen gibt es soziale Netze, die dazu dienen, sich der Öffentlichkeit vorzustellen. Diese bieten häufig auch die Möglichkeit, Informationen über weitere soziale Netze, in denen der Nutzer angemeldet ist, im eigenen Profil anderen zur Verfügung zu stellen.

Verlässliche Profilzuordnung

Um nicht zu viel vorweg zu greifen, an dieser Stelle nur eine kurze Erklärung hierzu. Es wird häufig die Möglichkeit genutzt, nahezu zeitgleich beispielsweise ein Bild bei Instagram zu posten

und einen Tweet mit dem Link zu dem Bild zu versenden. Wird die zeitliche Differenz zwischen diesen beiden Ereignissen entsprechend klein gewählt, so kann davon ausgegangen werden, dass es sich um eine korrekte Zuordnung und nicht um einen Bot handelt. Für die Erhebung der Ground-Truth-Daten wurde eine Differenz von einer Sekunde festgelegt; Details, warum diese Zeit nicht von Bots unterboten werden kann, folgen im Abschnitt des Verfahrens 9.

About.me

Bei About.me handelt es sich genau genommen nicht um ein soziales Netz, sondern um einen persönlichen Webhosting-Service. Ziel ist es, den Benutzern eine einfache Plattform zu bieten, auf der sie zu ihren diversen Onlineidentitäten verlinken können. Ein Nutzerprofil zeichnet sich dadurch aus, dass alle Informationen auf nur einer Seite dargestellt werden, was das Crawling der Daten sehr vereinfacht.

Da Profile auf About.me öffentlich zugänglich sind, kann jeder allein durch die Nutzung einer Suchmaschine Fakeprofile unter seinem Namen finden und entsprechend intervenieren. Eine Nutzung im Rahmen von Identitätsdiebstahl ist daher nicht zu erwarten. Sollte der unwahrscheinliche Fall eintreten, sind diese Profile leicht aufzuspüren. Daher eignen sich die dort hinterlegten Daten ideal als Ground-Truth-Datensatz.

Datensatz Der gecrawlte Ground-Truth-Datensatz setzt sich aus Daten zu Accounts in sozialen Netzen von 174.707 Personen zusammen. Die nachfolgende Tabelle gibt hierbei einen Überblick über die Anzahl der vertretenen Profile bestimmter sozialer Netze.

Tabelle 7.3.: Häufigkeit einzelner sozialer Netz am About.me Datensatz.

Netz	Häufigkeit Anzahl	Häufigkeit %
Twitter	103.565	59,28
Facebook	81.003	46,37
Instagram	63.885	36,57
Linkedin	84.133	48,17
Youtube	31.767	18,18
Wordpress	17.795	10,18
Flickr	13.991	8,01
Tumblr	22.779	13,04
GooglePlus	46.186	26,44
Foursquare	10.059	5,76
Vimeo	9.592	5,49

Da sich diese Arbeit mit der Profilzuordnung über soziale Netze beschäftigt, ist besonders das paarweise Auftreten von sozialen Netzen entscheidend. Dies vorwiegend für die Evaluation ausgewählten Netze, Twitter, Instagram und Youtube. Tabelle 7.4 zeigt die Anzahl der Nutzer für die jeweils die Daten von zwei bzw. allen drei Netzen vorliegen.

Tabelle 7.4.: Häufigkeit einzelner sozialer Netze im About.me Datensatz.

Netz	Häufigkeit Anzahl	Häufigkeit %
Twitter - Instagram	54.240	31,05
Twitter - Youtube	28.019	16,04
Instagram - Youtube	18.980	10,86
Twitter - Instagram - Youtube	17.745	10,16

Der Anteil am Datensatz, der sowohl ein Twitter- als auch ein Instagram-Profil besitzt, entspricht 31%. Hierbei beträgt der Anteil an Twitter-Nutzern, die auch einen Instagram Account haben, 52,37%, der Anteil an Instagram-Nutzern, die einen Twitter-Account haben, 84,90%. Für Youtube sieht das Verhältnis folgendermaßen aus, 27,05% der Twitter-Nutzer besitzen einen Youtube- und 88,20% der Youtube-Nutzer einen Twitter-Account. Zwischen Instagram und Youtube ist die Verteilung wie folgt, 29,71% der Instagram-Nutzer besitzen einen Youtube-, respektive 59,75% der Youtube-Nutzer einen Instagram-Account. Der Anteil für den Besitz von Profilen in allen drei Netzen, 17,13% für Twitter, 27,78% für Instagram und 5,86% für Youtube.

Twitter besitzt in diesem Datensatz mit Abstand den größten Anteil, hierdurch ergeben sich auch zwangsläufig hohe Anteile an Nutzern anderer Netze mit einem Twitter-Account. Die Wahrscheinlichkeit, dass ein Nutzer einen Twitter-Account besitzt, wenn dieser bereits aktives Mitglied bei Instagram oder Youtube ist, beträgt also, zumindest für diesen Datenstaz, ungefähr 85% oder mehr.

KAPITEL 8

Zuordnung anhand des zeitlichen Nutzerverhaltens

In diesem Kapitel wird versucht herauszufinden, wie vorhersehbar das Nutzungsverhalten von Mitgliedern sozialer Netze ist. Hierzu wurde anhand eines Twitter-Datensatzes mit simplen Methoden versucht vorherzusagen, wann ein Nutzer den nächsten Tweet absetzt. Ziel ist herauszufinden, ob die Vorhersagbarkeit ausreichend ist, um gegebenenfalls das Nutzungsverhalten zwischen zwei Profilen miteinander abgleichen zu können oder für andere Verfahren die Menge infrage kommender Profile zu reduzieren. Hierzu werden zunächst der verwendete Datensatz und dann die genutzten Verfahren vorgestellt und im Anschluss die Ergebnisse der Evaluation präsentiert.

8.1. Datensatz

Für diesen Datensatz wurde mithilfe des Twitter-Sample-Streams am 25.05.2016 eine Liste von User-IDs gesammelt. Diese enthielt mehr als eine Million User-IDs. Da diese Anzahl zu groß für das Abfragen der Tweets war, wurde die Menge zuerst auf circa 10% der ersten User-IDs in der Liste reduziert und aus den verbliebenen 100.000 IDs wurden zufällig 10.000 User-IDs ausgewählt. Für diese Profile wurden die verfassten Tweets abgefragt. Da Profile mit möglichst vielen Tweets benötigt wurden, wurden Profile mit weniger als 500 Tweets herausgefiltert. Vereinzelt wurden mehrere Tweets in der gleichen Millisekunde beobachtet. Da dies allein technisch gewollt schwer realisierbar ist, wurden Tweets mit einem Abstand von weniger als einer Sekunde zueinander entfernt. Mögliche Ursache könnte in der Pufferung von Tweets zu Zeiten der Umstellung auf das neue ID-Schema bei Twitter gewesen sein. Dies erklärt aber nicht die maximale Anzahl an Tweets in der gleichen Millisekunde eines Nutzers in Höhe von 1.110. Da dies äußerst ungewöhnlich ist, wurden, wie erläutert, entsprechende Tweets entfernt.

Die Eigenschaften des Datensatzes werden durch die Abbildungen 8.1, 8.2 und 8.3 näher dargestellt. Abbildung 8.1 zeigt die Anzahl an Tweets pro User-ID. 500 bildet aufgrund der erläuterten Filterung die untere Schranke, 3.200 die Obere, da dies das Maximum an abfragbaren Tweets pro User-ID bei Twitter darstellt. Da es bei diesem Ansatz insbesondere um die Betrachtung des zeitlichen Verhaltens geht, wurden die Zeitstempel der Tweets detaillierter betrachtet. Abbildung 8.2 zeigt die Zeitspanne vom ersten bis zum letzten erhaltenen Tweet

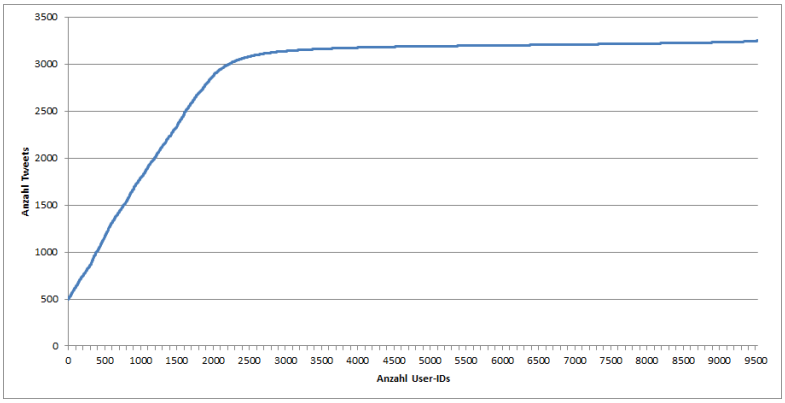


Abbildung 8.1.: Anzahl an Tweets für die ausgewählten User-IDs, aufsteigend sortiert.

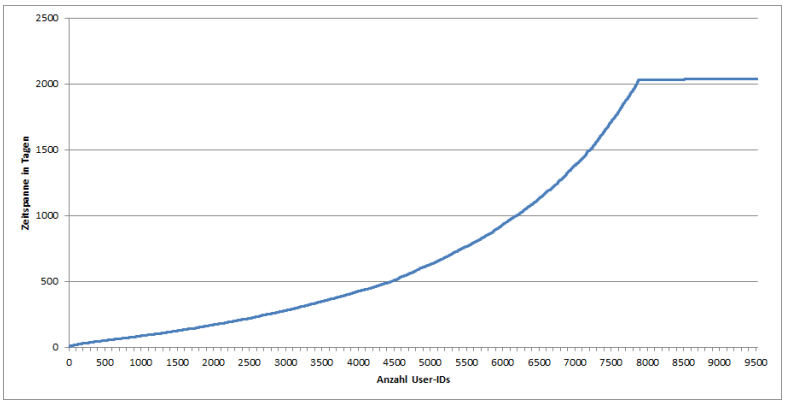


Abbildung 8.2.: Abgedeckte Zeitspanne vom ersten bis zum letzten Tweet in Tagen, aufsteigend sortiert.

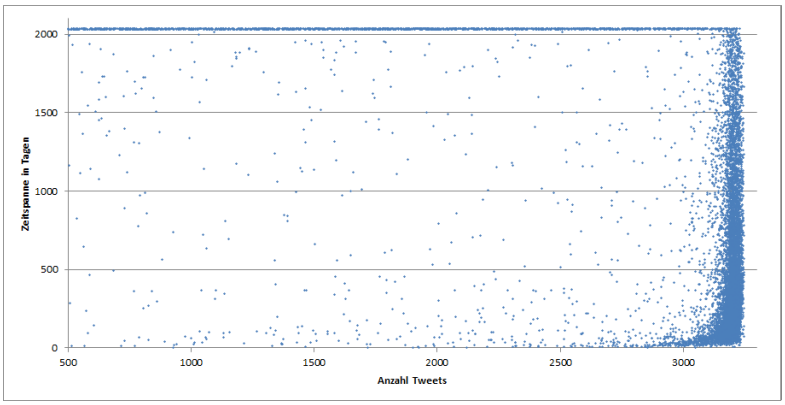


Abbildung 8.3.: Anzahl an Tweets im Verhältnis zur abgedeckten Zeitspanne, aufsteigend nach Anzahl Tweets sortiert.

für die jeweiligen User-IDs. Die obere Schranke bildet hierbei die Umstellung des Twitter-ID-Schemas, was zum Abfragezeitpunkt 2.035 Tage zurücklag. In der Abbildung 8.3 werden nun die beiden zuvor betrachteten Abbildungen ins Verhältnis gesetzt. Die untere und die oberen Schranken sind identisch mit den Daten beiden vorangegangenen Abbildungen.

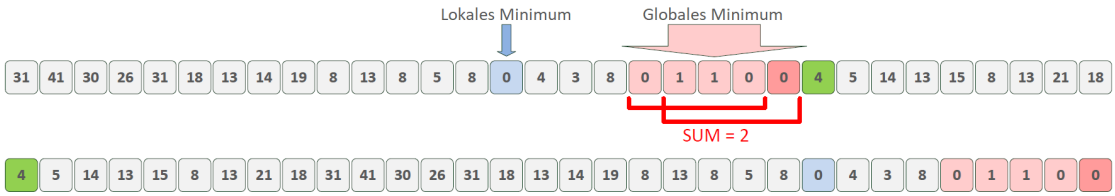


Abbildung 8.4.: Prinzipielles Vorgehen des Normalisierungsschrittes.

Da für dieses Verfahren nur die Zeitstempel der Tweets relevant sind, diese tageweise analysiert werden sollten und die Zeitzone nicht verlässlich ermittelt werden konnte, war eine Normalisierung der Zeitstempel notwendig. Das hierfür eingesetzte Verfahren ist in 8.4 dargestellt. Alle Zeitstempel eines Nutzers wurden auf ein Array projiziert, wobei jede Zelle einer Viertelstunde entspricht. Hierbei kann sich beispielsweise eine Verteilung wie in der oberen Zeile der Abbildung ergeben. Danach wurde im Array schrittweise nach dem Minimum von vier zusammenhängenden Zellen gesucht. Durch die Betrachtung von nicht nur einer Zelle soll sichergestellt werden, dass ein globales Minimum anstelle eines lokalen gefunden wird. Wenn die Summe der vier Zellen im nächsten Schritt identisch mit dem vorherigen Schritt ist, wird die rechte Grenze des globalen Minimums um eine Zelle erweitert. Dies ist in der Abbildung durch die roten Klammern und die dunklere rote Zelle angedeutet. Nach der Ermittlung des globalen Minimums, wird die rechte Grenze des Minimums, die dunklere rote Zelle, als Tageswechsel angenommen und die durch diese Zelle repräsentierte Anzahl an Millisekunden von allen Zeitstempeln abgezogen. Das führt zu einer korrekten tageweisen Anordnung der Zeitstempel, wie sie in der unteren Zeile der Abbildung dargestellt ist, kann aber leider abhängig von der realen Zeitzone des Nutzers zu einer Verschiebung um einen Tag führen. Beispielsweise werden die Zeitzonen UTC+11 und UTC-11 nicht auf die gleichen Wochentage gemappt. Da aber die Wochentage nicht separat betrachtet werden, ist es für diesen Ansatz irrelevant.

Nach dem Filtern verblieben 9.525 User im Datensatz, mit insgesamt 27.428.510 Tweets. Dies entspricht durchschnittlich 2879,6 Tweets pro Nutzer.

8.2. Vorhersage des zeitlichen Nutzungsverhaltens

Bei diesem Verfahren wird mittels einer Heuristik versucht, das zeitliche Nutzungsverhalten vorherzusagen. Zunächst wird auf einer Teilmenge des Datensatzes ”gelernt”, um dann zu versuchen die nächsten Tweets, die noch im Datensatz enthalten sind, vorherzusagen. Da dies der erste Versuch ist, Vorhersagen zu machen, wurde dabei auf einzelne Aspekte fokussiert, d.h. es wurden mitunter Informationen miteinbezogen, die nicht hätten bekannt sein können,

beispielsweise wurde bei der Vorhersage berücksichtigt, wie viele Tweets ein Nutzer an diesem Tag abgesetzt hat. Eine genauere Erläuterung hierzu erfolgt später. Zu Beginn erfolgte der Versuch der Vorhersage mittels eines naiven Algorithmus und in Verbindung dazu erfolgte eine tageweise Betrachtung. Das Ergebnis jedes Algorithmus wurde in fünf Stufen festgehalten. Dabei wurde das Delta zwischen vorhergesagter Zeit und dem entsprechenden Tweet in die Kategorien: kleiner einer Viertelstunde, kleiner einer halben Stunde, kleiner einer Stunde, kleiner zwei Stunden und kleiner vier Stunden. Zur Vergleichbarkeit der Verfahren wurde auch eine zufällige Vorhersage implementiert, um zeigen zu können, um welchen Prozentsatz die Verfahren jeweils besser abschneiden als eine rein zufällige Vorhersage.

8.2.1. Naiver Ansatz

Beim naiven Ansatz wird die durchschnittliche Zeit zwischen zwei Tweets ermittelt und angenommen, dass der nächste Tweet auch in diesem zeitlichen Abstand verfasst wird. Um die durchschnittliche Zeit zwischen zwei Tweets zu berechnen wurden verschiedene Zeitfenster genutzt, von 1-10, 15, 20, 25, 35, 50, 75, 100 und 200 der vorangegangenen Tweets. Da für jeden Nutzer mindestens 500 Tweets vorliegen, verschiebt sich das Fenster der für den durchschnittlichen Abstand herangezogenen Tweets mit jeder Vorhersage.

8.2.2. Tageweiser Ansatz

Hierunter fallen verschiedene Ansätze die die Zeitstempel Tag-basiert auswerten. Zum einen wird versucht vorherzusagen, ob noch ein Tweet am gleichen Tag erfolgen wird, zum anderen wurden zwei Methoden erprobt, die eine zeitliche Vorhersage für einen weiteren Tweet durchführen. Alle Ansätze wurden über den gesamten Datensatz getestet und getrennt, entweder nur für Tweets oder nur für Retweets.

Ein weiterer Tweet an diesem Tag?

Dieser Ansatz versucht vorauszusagen, ob noch ein weiterer Tweet (oder Retweet) an diesem Tag versendet wird. Das Verfahren nutzt dazu eine Historie. Diese ist derart implementiert, dass sie durch ein Array abgebildet wird, wobei jede Zelle einem 15 Minuten Zeitfenster entspricht. Das Array enthält jeweils die gerasterte Zeit der letzten Tweets an jedem Tag als Lerndatensatz. Während der Ausführung werden bereits vorhergesagte Tweets in diesem Lerndatensatz ergänzt. Die Vorhersage wird zum einen anhand des Mittelwertes des Arrays und zum anderen anhand des Maximums ermittelt. In der Evaluation wird gezeigt, welcher Wert besser für die Vorhersage geeignet ist. Eine Zufallsvorhersage wurde aufgrund des binären Charakters der Vorhersage nicht umgesetzt.

Wann erfolgt der nächste Tweet?

Für beide hier getesteten Verfahren wurden die täglichen Datensätze in vier Kategorien eingeteilt. In Tage mit einem, zwei, drei und vier oder mehr Tweets am Tag. Dazu wurden Informationen genutzt, die im Rahmen einer realen Vorhersage im Vorfeld nicht bekannt sind.

Bei einem vollständigen Vorhersage-Verfahren würde auch versucht, die Anzahl der Tweets am nächsten Tag vorherzusagen.

Um die Vorhersage transparenter zu gestalten, wurden nicht nur die Tage nach der Anzahl der Tweets kategorisiert, sondern auch die Tweets selbst. Folgende Kategorien wurden dabei definiert:

- **Single**: Ein einzelner Tweet, nur einer an diesem Tag.
- **Erster**: Der erste Tweet an einem Tag.
- **Letzter**: Der letzte Tweet an einem Tag.
- **Mitte**: Alle Tweets zwischen erstem und letztem.

Ringpuffer-Verfahren Für jede der vier Tweet-Kategorien wurde ein Ringpuffer implementiert, der eine limitierte Anzahl an Tweets bzw. Zeitstempeln speichern kann. Lediglich der Ringpuffer für die mittleren Tweets speichert eine definierte Anzahl an Arrays. Die Charakteristik eines Ringpuffers ist, dass die ältesten Elemente durch die Neuen überschrieben werden, falls die maximale Speicherkapazität erreicht ist. Ansonsten wird das neue Element in einer freien Zelle des Puffers abgelegt. Die maximale Anzahl der Speicherplätze der Puffer wird vor Ausführung definiert. Das Verfahren wurde für alle Größen der Puffer von 1-20 Speicherzellen durchgeführt. Der Algorithmus beginnt mit der Vorhersage sobald die Zeitstempel von X Tagen im Ringpuffer abgelegt wurden. Dabei entspricht X der maximalen Größe der Puffer. Dadurch wird eine initiale Befüllung der Puffer sichergestellt, um überhaupt eine Vorhersage durchführen zu können. Die nachfolgende Liste beschreibt, wie die Vorhersagen für die unterschiedlichen Tages-Kategorien errechnet werden.

- **1**: Berechnet den Durchschnitt der *Single* Zeitstempel im entsprechenden Ringpuffer. Wenn der Puffer leer ist, wird der Puffer der *Erster* Zeitstempel verwendet.
- **2**: Der erste Tweet wird anhand des Durchschnitts des *Erster* Puffers ermittelt, falls dieser leer ist, aus dem *Single* Puffer. Die zweite Vorhersage erfolgt aus dem *Letzter* Puffer, falls dieser leer ist, wird der zuvor errechnete auch hier angenommen.
- **3**: Die Vorhersage für den ersten und letzten Tweet erfolgt wie zuvor. Der *Mitte* Zeitstempel wird anhand des Mittelwertes des *Mitte* Puffers vorhergesagt. Falls dieser leer ist, wird der Mittelwert von den Vorhersagen für den ersten und letzten Tweet herangezogen.
- **4+**: Die Vorhersage für den ersten und letzten Tweet erfolgt wie zuvor. Für die *Mitte* Tweets erfolgt die Vorhersage anhand des Mittelwertes der n-ten Zeitstempel im *Mitte* Puffer. Falls dieser leer ist, wird die Zeitspanne zwischen erstem und letzten Tweet in die notwendige Anzahl gleich dimensionierter Intervalle geteilt und entsprechend als Vorhersage genutzt.

Maximum Arrayzell-Verfahren Bei diesem Verfahren kommen anstatt von Ringpuffern Arrays zum Einsatz. Daher wird für jede der Tweet-Kategorien das Auftreten eines Tweets in einer definierten Zeitspanne gezählt. Alle Zeitstempel werden dabei auf Intervalle fester Länge gemappt. Beispielsweise wenn ein Intervall mit 15 Minuten definiert ist, beträgt die Array-Größe $24/(60/15) = 96$. Der Algorithmus wird für alle Teiler von 60 (Minuten) ausgeführt, was zu Intervallgrößen von 1-6, 10, 12, 15, 20, 30 und 60 Minuten führt. Die Vorhersage an sich erfolgt wie beim Ringpuffer-Verfahren. Es wird lediglich anstelle des Mittelwertes des Ringpuffers, das Maximum des entsprechenden Arrays herangezogen. Nachdem jede Zelle ein Intervall abbildet, wird für die Vorhersage die Mitte des Intervalls genutzt. Wenn eine Berechnung fehlschlägt, da ein Array noch nicht befüllt ist, werden die Alternativen gemäß dem Ringpuffer-Verfahren verwendet.

Wochenweiser Ansatz

Die hier implementierten Verfahren sind vergleichbar mit den Tag-basierten Algorithmen. Aber anstelle jeden Tag gleich zu behandeln, wird hierbei der Wochentag mit berücksichtigt. Dadurch wird es möglich, unterschiedliches Verhalten, beispielsweise am Wochenende, in die Vorhersage miteinzubeziehen. Auch hier wurde ein Verfahren zur Vorhersage, ob noch ein Tweet erstellt wird, und zwei Verfahren zur zeitlichen Vorhersage umgesetzt. Außer der wochenweisen Betrachtung sind es die gleichen Methoden mit dem Unterschied, dass sieben Ringpuffer bzw. Arrays für jede Tweet-Kategorie verwendet werden.

8.3. Evaluation

In diesem Abschnitt werden nun die Ergebnisse der zuvor in der Theorie erläuterten Verfahren präsentiert. Abhängig vom eingesetzten Verfahren, hat die maximale zeitliche Abweichung des erwarteten Tweets unterschiedliche Grenzwerte. Beispielsweise beträgt die maximale Abweichung bei den Tag-basierten Ansätzen 12 Stunden, da nur die Zeit und nicht das Datum für die Evaluation herangezogen werden. Nachdem nur innerhalb eines Tages Vorhersagen gemacht werden, beträgt auch die zeitliche Abweichung für die Wochen-basierten Verfahren 12 Stunden.

Tabelle 8.1.: Durchschnittsergebnisse der Vorhersage, ob ein weiterer Tweet an diesem Tag folgt (R richtig, F falsch)

Tweets	**Maximum**		**Durchschnitt**	
	% **Tag R**	% **Tag F**	% **Tag R**	% **Tag F**
Alle	82,8242	17,1758	82,1045	17,5911
Nur Tweets	80,1340	19,8341	79,3684	20,3662
Nur Retweets	70,6275	29,0696	69,2038	30,3181

Tabelle 8.1 zeigt die Ergebnisse beider Verfahren der Vorhersage, ob ein weiterer (Re-)Tweet an diesem Tag erfolgen wird. In allen Fällen ist das Verfahren, welches auf den Maxima basiert

dem Verfahren mit Durchschnittswerten überlegen. Die Vorhersage ist in fast 83% korrekt, was deutlich über den 50% einer zufälligen Vorhersage liegt. Interessanterweise fallen die Ergebnisse nur für Tweets oder nur für Retweets schlechter aus. Eine korrekte Vorhersage erfolgt für Retweets in etwa 70% und für Tweets in etwa 80% der Fälle. Das zeigt, dass die Vorhersage von Retweets herausfordernder ist. Da eine Kombination von Tweets und Retweets das Ergebnis verbessert, kann angenommen werden, dass die Nutzung von Twitter regelmäßig und nicht nur mit der Absicht einen Tweet zu verschicken erfolgt. Dies ist daran zu erkennen, dass die Nutzung nur mit der Absicht einen Tweet zu verschicken dazu führen würde, dass Retweets immer innerhalb kurzer Zeit auf Tweets folgen würden. Damit würden diese das Ergebnis nicht verbessern, potentiell sogar verschlechtern, da zwischen Tweet und Retweet möglicherweise eine sehr kurze, aber bis zum nächsten Tweet wieder eine lange Zeitspanne liegt.

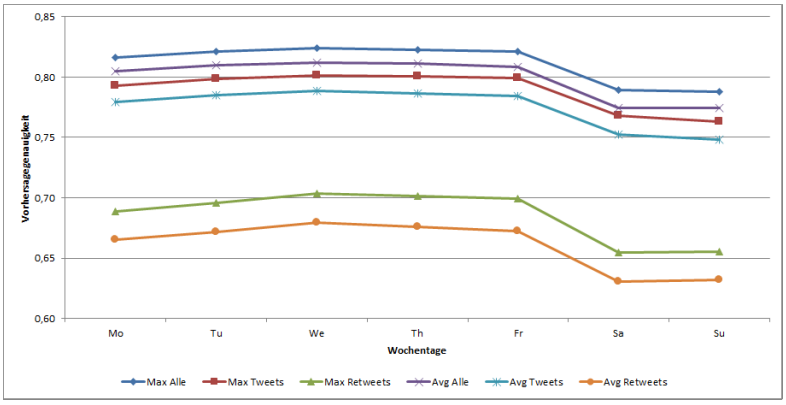


Abbildung 8.5.: Ergebnisse der Vorhersage, ob ein weiterer Tweet erfolgt, aufgeteilt auf Wochentage.

Die Abbildung 8.5 zeigt die Ergebnisse der Vorhersage, ob weitere Tweets am gleichen Tag erfolgen, aufgeteilt nach Wochentagen und für den vollständigen Datensatz, also Tweets und Retweets. Da die Ergebnisse des auf Maxima basierenden Verfahrens besser abschneiden als die Nutzung der Durchschnittswerte, liegt auf diesen in der weiteren Analyse der Fokus. Das Diagramm zeigt eine deutliche Verschlechterung der Vorhersagegenauigkeit am Wochenende. Hintergrund dürfte sein, dass am Wochenende, durch die für die meisten Leute entfallende Arbeit, weniger Routine im Tagesablauf enthalten ist. Interessanterweise wird die beste Vorhersage am Mittwoch mit 82,4% und die schlechteste der Arbeitstage am Montag mit 81,6% erreicht. Es ist anzunehmen, dass am Montag viele Leute später beginnen (Pendler) oder aufgrund eines anstrengenden Sonntags bzw. zugunsten eines langen Wochenendes Urlaub genommen haben. All das führt zu weniger Routine im Tagesverlauf. Nichtsdestotrotz sind 78,7% am Sonntag, als die schlechteste Vorhersage im laufe der Woche immer noch ein sehr gutes Ergebnis. Der Durchschnittswert des auf Maxima basierenden Ansatzes für alle Wochentage beträgt 81,1%, dies liegt geringfügig unter den 83% des Tage-weisen Verfahrens. Eine Möglichkeit hierfür liegt in dem kleineren Datensatz bei Vorhersagebeginn, da

der Trainingsdatensatz virtuell in sieben Datensätze aufgeteilt wird, einen für jeden Wochentag.

Die nachfolgenden Abschnitte präsentieren und diskutieren die Ergebnisse der verschiedenen Zeit-Vorhersageverfahren. Die gestrichelten Linien in den nachfolgenden Abbildungen repräsentieren die Ergebnisse der zufälligen Vorhersage. Die Einfärbung der Zeitintervalle ist identisch mit den anderen Vorhersageverfahren. Die Ergebnisse der zufälligen Vorhersage sind für alle Vorhersageverfahren identisch und sind in 8.2 dargestellt.

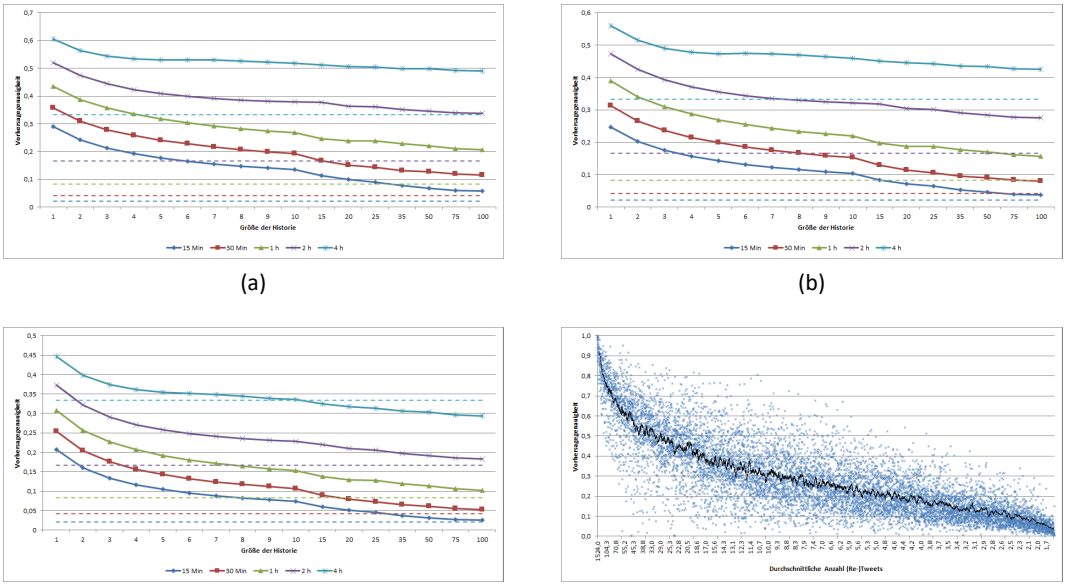
Tabelle 8.2.: Ergebnisse der zufälligen Vorhersage.

Zeitspanne	Wahrscheinlichkeit
15 Minuten	2,0833%
30 Minuten	4,1667%
1 Stunde	8,3333%
2 Stunden	16,6667%
4 Stunden	33,3333%

Die Trefferwahrscheinlichkeit der zufälligen Vorhersage entspricht dem Verhältnis der doppelten Zeitspanne im Vergleich zu einem ganzen Tag, da die Vorhersage als Treffer gewertet wird, sobald die zeitliche Distanz zum aktuell betrachteten Zeitstempel kleiner als das entsprechende Zeitintervall. Beispielsweise für das 15 Minuten Intervall werden alle Vorhersagen als Treffer gewertet, die im Zeitraum von 15 Minuten vor bis 15 Minuten nach dem Zeitstempel liegen. Daraus ergibt sich ein 30 Minuten Zeitfenster und 30 Minuten im Verhältnis zu 24 Stunden entspricht 2,0833%.

Die Abbildungen 8.6 a), b) und c) zeigen die Ergebnisse des naiven Vorhersageverfahrens für den gesamten Datensatz, nur Tweets bzw. nur Retweets. Die Diagramme zeigen, dass die Historie so klein wie möglich sein sollte. Je größer sie ist, um so schlechter werden die Ergebnisse. Die Ergebnisse an sich sind überraschend gut, die 15 Minuten Vorhersage zum Beispiel ist fast um den Faktor 14 besser als die zufällige Vorhersage. Da bei diesem Verfahren nicht mit so guten Ergebnissen zu rechnen war, ist davon auszugehen, dass Nutzer mit vielen Tweets pro Tag das Ergebnis stark zum positiven hin beeinflussen, da bei vielen Tweets der Zeitraum zwischen zwei Tweets oft kleiner oder nur geringfügig größer ist als 15 Minuten. Dies führt zu vielen korrekten Vorhersagen innerhalb eines Tages und nur zu sehr wenigen Falschen im Fall eines Tagwechsels. Abbildung 8.6 d) verdeutlicht das durch Darstellung des Verhältnisses zwischen dem Anteil korrekter Vorhersagen (y-Achse) und dem durchschnittlichen Aufkommen an (Re-)Tweets (x-Achse). Die Trendlinie (schwarz) zeigt diesen Zusammenhang sehr deutlich auf. Je geringer die Anzahl an Tweets, umso schlechter fallen die Ergebnisse aus.

Die Unterschiede in den Ergebnissen zwischen dem gesamten Datensatz und einer Unterscheidung zwischen nur Tweets bzw. nur Retweets sind für alle weiteren Betrachtungen ähnlich, daher wird im weiteren Verlauf darauf verzichtet, diese getrennt voneinander zu



(a) (b)

(c) (d)

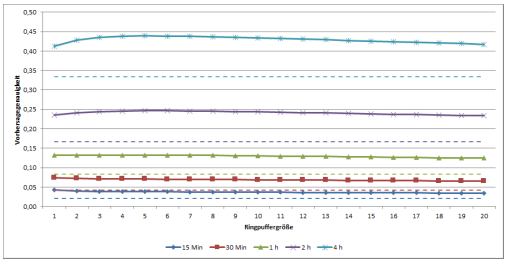
Abbildung 8.6.: Ergebnisse des naiven Vorhersageverfahrens für den gesamten Datensatz a), nur Tweets b) und nur Retweets c). Das Verhältnis zwischen der Genauigkeit der Vorhersage und der durchschnittlichen Anzahl an Tweets pro Tag zeigt d).

betrachten.

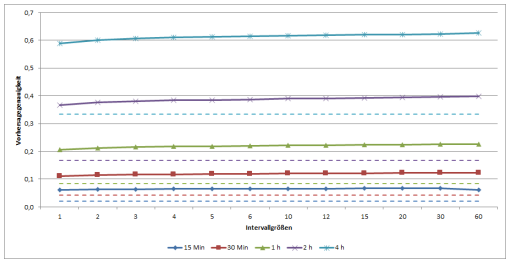
Die Abbildungen 8.7 zeigen die Ergebnisse für die tageweise Vorhersage mittels Ringpuffer a) und der Nutzung des Maximum Arrayzell-Verfahrens b). Das Arrayzell-Verfahren erzielt bessere Ergebnisse als die Nutzung eines Ringpuffers. Daraus kann geschlossen werden, dass die Abstraktion in Zeitslots für diesen Anwendungsfall besser geeignet ist, als die konkreten Werte aus dem Ringpuffer. Weitere Unterschiede bestehen ansonsten zwischen den Verfahren nicht.

Abbildung 8.7 c) zeigt die Ergebnisse des Maximum Arrayzell-Verfahren im Verhältnis zur durchschnittlichen Anzahl an (Re-)Tweets pro Tag. Im Unterschied zur Abbildung 8.6 d) weisen die Ergebnisse ein beständiges Verhalten unabhängig von der Anzahl an Tweets pro Tag auf. Daher zeigt das Maximum Arrayzell-Verfahren bessere Ergebnisse für Nutzer mit einer geringen Anzahl an Tweets als das naive Verfahren.

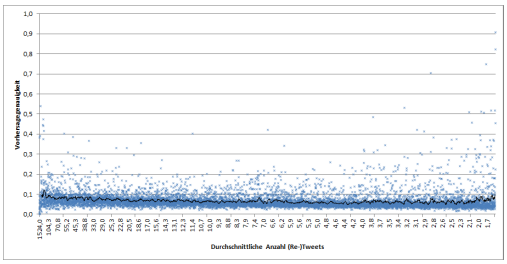
Die Ergebnisse der wochenweisen Betrachtung sind in den Abbildungen 8.8 dargestellt. a) zeigt die Ergebnisse für einen Ringpuffer der Größe 1, dieser zeigt die besten Ergebnisse für Vorhersagen mit einer Genauigkeit von 15 Minuten und b) die Ergebnisse für einen Ringpuffer der Größe 5, da dieser für eine Genauigkeit von 4 Stunden am besten abschneidet. Interessanterweise zeigen die Diagramme einen kleinen Peak am Freitag, was am stärksten für das Zeitintervall von 4 Stunden sichtbar wird. Grund könnten insbesondere Aktivitäten sein,



(a)



(b)



(c)

Abbildung 8.7.: Ergebnisse für die tageweise Vorhersage mittels Ringpuffer a) und der Nutzung des Maximum Arrayzell-Verfahrens b). c) zeigt die Ergebnisse des Maximum Arrayzell-Verfahren im Verhältnis zur durchschnittlichen Anzahl an (Re-)Tweets pro Tag.

die nach der Arbeit aufgrund des bevorstehenden Wochenendes durchgeführt werden. Die Ergebnisse der anderen Wochentage variieren untereinander nur minimal.

Die Diagramme c), d) und e) in Abbildung 8.8 zeigen die Ergebnisse des Maximum Arrayzell-Verfahrens, c) für ein Intervall von 1 Minute, d) 20 Minuten und e) 60 Minuten. Wie bereits bei der tageweisen Auswertung zeigt auch hier der Maximum Arrayzell-Ansatz bessere Ergebnisse als das Ringpuffer Äquivalent. Die Diagramme zeigen keinen Peak am Freitag, sondern eine Verschlechterung an Samstagen und Sonntagen. Grund könnte sein, dass der Arrayzell-Ansatz bei geringeren Variationen im Tagesverlauf, so wie an Wochentagen gegeben, besser abschneidet als bei stärkeren Variationen an Wochenenden. Das ergibt sich aus der Natur des Verfahrens, welches den Zeitslot mit dem höchsten Aufkommen auswählt. Bei stärkeren Variationen erhöht sich jedoch die Wahrscheinlichkeit, dass der vorherzusagende Zeitstempel stärker vom Maximum abweicht als normal. Daraus ergibt sich auch, dass in diesen Fällen das Maximum möglicherweise nicht so klar definiert ist.

Die Abbildungen 8.9 und 8.10 zeigen die Resultate aller betrachteten Zeitvorhersage-Verfahren für die besten bzw. die schlechtesten Ergebnisse. Die besten bzw. schlechtesten bedeutet, dass die Werte aus der Gesamtheit aller evaluierten Parameter der Verfahren ermittelt wurden. Dabei wurde immer der gesamte Datensatz, Tweets und Retweets, betrachtet. In beiden Abbildungen ist die Kurve mit den schlechtesten Ergebnissen die zufällige Vorhersage,

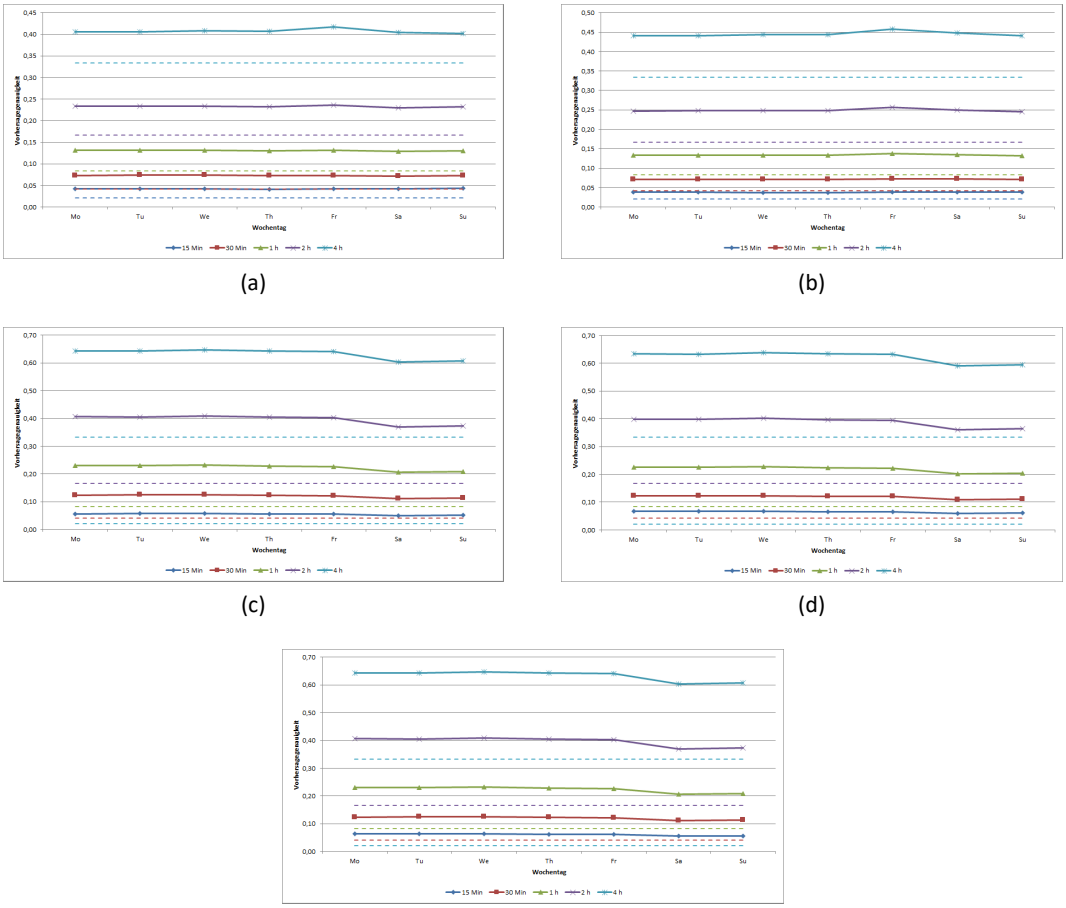


Abbildung 8.8.: Ergebnisse für die wochenweise Vorhersage mittels Ringpuffer Größe 1 a) und Größe 5 b) und der Nutzung des Maximum Arrayzell-Verfahrens mit Intervallen von 1 Min c), 20 Min d) und 60 Min e).

daraus folgt, dass jedes Verfahren in allen evaluierten Fällen besser abschneidet als eine zufällige Vorhersage. Nachdem zwischen jeder der fünf Vorhersagekategorien, 15 Minuten bis 4 Stunden, das Intervall verdoppelt wird, zeigen die Kurven der Diagramme, mit Ausnahme des naiven Ansatzes, ein exponentielles Wachstum. Der naive Ansatz zeigt nur ein lineares Wachstum. Es ist unklar, ob sich aufgrund des hohen Startwertes das exponentielle Wachstum relativiert oder ob es an der Charakteristik des Verfahrens liegt. Abbildung 8.9 illustriert die guten Ergebnisse des naiven Ansatzes, nichtsdestotrotz zeigt das Maximum Arrayzell-Verfahren für das 4 Stunden Intervall bessere Ergebnisse. Insgesamt zeigt die wochenweise Auswertung bessere Ergebnisse als die tageweise. Das zeigt, dass die individuelle Behandlung jedes Wochentages einen Mehrwert und dadurch bessere Ergebnisse generiert. Abbildung 8.10 zeigt, dass bei Betrachtung der schlechtesten Ergebnisse das Maximum Arrayzell-Verfahren im Vergleich zum naiven Ansatz weitaus besser abschneidet. Insbesondere die tageweise

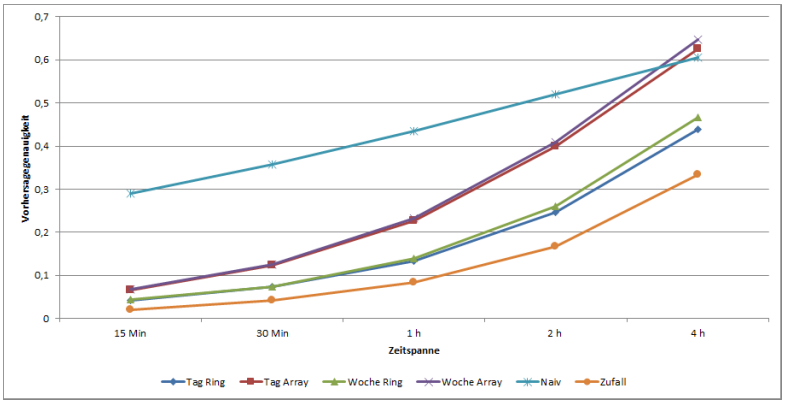


Abbildung 8.9.: Alle evaluierten Zeitvorhersage-Verfahren mit den besten Trefferwahrscheinlichkeiten im Vergleich zueinander.

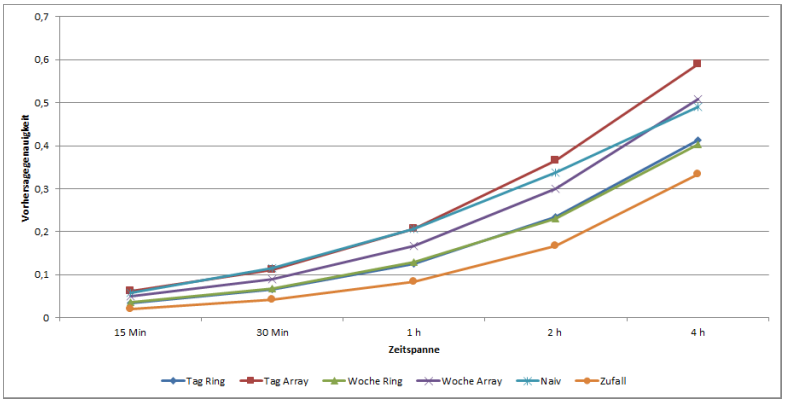


Abbildung 8.10.: Alle evaluierten Zeitvorhersage-Verfahren mit den schlechtesten Trefferwahrscheinlichkeiten im Vergleich zueinander.

Auswertung zeigt in allen Kategorien bessere Ergebnisse gegenüber dem naiven Ansatz. Das Ringpuffer-Verfahren schneidet besser ab als eine zufällige Vorhersage, aber deutlich schlechter als die anderen Verfahren.

8.4. Zusammenfassung und Schlussfolgerung

In diesem Kapitel wurde gezeigt, dass es unter gewissen Annahmen und Randbedingungen in Grenzen möglich ist, das zeitliche Nutzerverhalten bei Twitter vorherzusagen. Gute Ergebnisse konnten in diesem Kontext dennoch nur für ausgesprochene Vielnutzer erzielt werden und dies auch nur bedingt durch die in diesem Fall vergleichsweise großen Zeitintervalle, die für die Trefferermittlung herangezogen wurden.

Insgesamt kann man jedoch festhalten, dass die erzielten Ergebnisse, auf die Gesamtheit aller

Nutzer betrachtet, im Hinblick auf die Anwendung im Bereich der Profilzuordnung zu ungenau sind. Die Verfahren könnten einen geringen Beitrag bei einer Ergebnisverfeinerung liefern, als primäre Zuordnungsalgorithmen sind sie nicht geeignet.

KAPITEL 9

Profilzuordnung anhand von Zeitdifferenzen

Mit der Nutzung mehrerer sozialer Netze geht meist auch der Wunsch einher, Inhalte in einem Netz zu veröffentlichen und diese zusätzlich in einem anderen zu verbreiten bzw. darauf zu verweisen. Postet beispielsweise ein Nutzer ein Video bei Youtube oder ein Bild bei Instagram und besitzt er zudem ein Profil bei Twitter, ist die Wahrscheinlichkeit hoch, dass er diesen Inhalt dort zusätzlich bewirbt. Hierdurch ergibt sich eine zeitliche Abfolge, Posten des Inhalts in einem Netz und anschließend die Verbreitung in einem anderen. Dieser zeitliche Zusammenhang lässt sich für Profilzuordnungen aber beispielsweise auch die Boterkennung nutzen. Zu beachten ist bei diesem Verfahren, dass davon ausgegangen wird, dass auf den entsprechenden Inhalt in einem anderen Netz zum Beispiel durch Nutzung einer URL verwiesen wird, auch wenn dies nicht an jeder Stelle Erwähnung findet. Teilaspekte dieses Kapitels wurden in [327] veröffentlicht.

9.1. Nutzungsmöglichkeiten und deren zeitlichen Abhängigkeiten

Die folgenden Abschnitte geben einen Überblick über verschiedene Abläufe und Nutzungsweisen, die zu zeitlich voneinander abhängigen Ereignissen führen.

9.1.1. Manuelles Posten

Abbildung 9.1 zeigt ein solches Beispiel. Alice postet im *sozialen Netz 1* einen beliebigen Inhalt. Nach dem Absenden und dem Empfang der Daten des Netzes erfolgt eine interne Verarbeitung, das Speichern eines Mediums, das Eintragen in einer Datenbank und die Generierung entsprechender IDs inklusive zugehöriger Zeitstempel. Dies kann von einigen hundert Millisekunden bis hin zu wenigen Sekunden dauern. Anschließend wird das Hinzufügen der Informationen zu Alices Profil bestätigt und eine entsprechende URL für den direkten Aufruf dieses neuen Eintrages zur Verfügung gestellt. Nun kann Alice beginnen einen Post in einem anderen Netz, *Soziales Netz 2* vorzubereiten und diese URL anzuhängen. Die Erstellung des neuen Posts kann von einigen Sekunden bis hin zu wenigen Minuten dauern, daher die

graphische Unterbrechung. Anschließend wird dieser Post an das Netz versendet, es erfolgt dort ebenfalls eine interne Verarbeitung, bei der auch die Zeitstempel generiert werden. Das Netz bestätigt Alice die erfolgreiche Aufnahme der Informationen. Zwischen den beiden Zeitpunkten, zu denen die Zeitstempel der Inhalte generiert wurden, in der Abbildung am Ende der internen Verarbeitungen mit roten Linien gekennzeichnet, ist eine gewisse Zeit vergangen. Dies wird mit dem Pfeil zwischen beiden Linien verdeutlicht. Die Unterbrechung deutet eine potentiell längere Dauer aufgrund der notwendigen Nutzeraktivitäten an. Bei einer händischen Übernahme der URL und der anschließend noch notwendigen Inhaltserstellung, beispielsweise der Tweet-Formulierung, kann von einem zeitlichen Abstand von mindestens 20 bis 30 Sekunden ausgegangen werden, wobei die maximale Ausdehnung nicht beschränkt ist, da eine URL auch erst Jahre später verbreitet werden könnte.

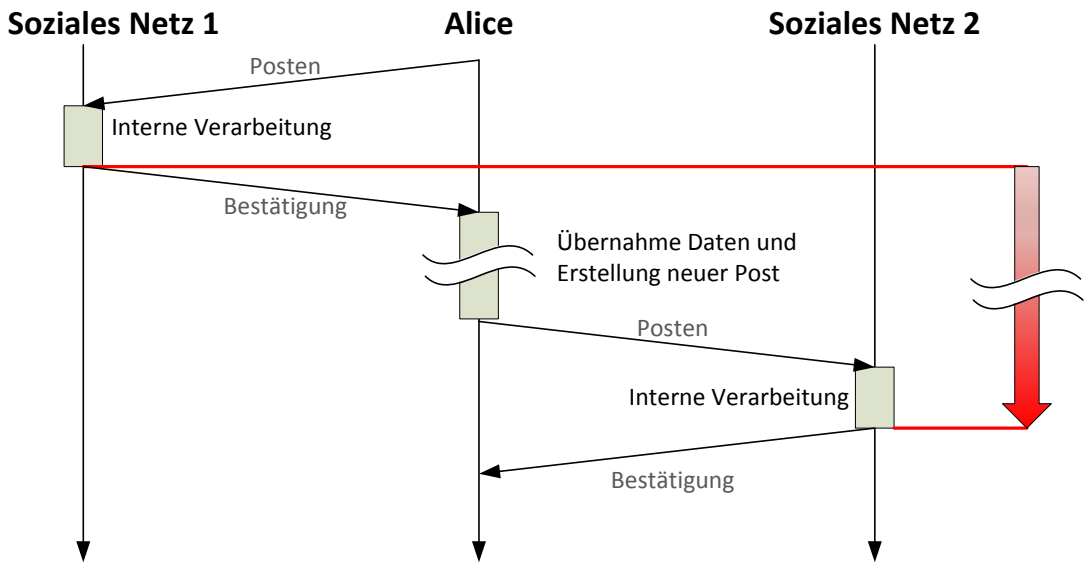


Abbildung 9.1.: Zeitlicher Ablauf des Postens in unterschiedlichen sozialen Netzen bei manuellem Übertrag der URL oder des Inhalts.

9.1.2. Automatisches Posten

Der Prozess des manuellen Postens von Inhalten in mehreren sozialen Netzen ist aufwändig. Daher verwenden viele Nutzer Dienste und Apps wie IFTTT, siehe [345]. IFTTT, ausgesprochen *If This Then That*, ermöglicht die Erstellung von Regeln, die bei Auslösen eines Triggers automatisch bestimmte Aktionen abarbeiten. Eine Regel ermöglicht beispielsweise bei Posten eines Fotos auf Instagram automatisch diesen Inhalt auch bei Twitter zu veröffentlichen mit einem Verweis, einer URL, zu dem entsprechenden Inhalt bei Instagram. IFTTT bietet hierbei mehr als 250 Regeln für diverse soziale Netze.

Abbildung 9.2 zeigt im oberen Bereich den eben skizzierten Ablauf, der erforderlich ist, um in zwei Netzen zu posten, wobei der zweite Eintrag auf den ersten verweist. Die Aktion *Übernahme Daten für nächsten Post* wird hierbei von der IFTTT-App übernommen, wobei auch eine Abarbeitung auf Servern eines Dienstanbieters möglich ist. Im unteren Bereich des Bildes ist der Fall dargestellt, dass auf den Verweis verzichtet und der Eintrag zeitgleich in zwei Netzen veröffentlicht wird. Die Nutzung von IFTTT führt, neben der Arbeitsersparnis für den Nutzer, zu äußerst geringen zeitlichen Unterschieden der beiden Posts. Hierbei konnten Zeitdifferenzen von weniger als einer Sekunde beobachtet werden. Das gleichzeitige Posten führt zu noch kleineren Differenzen, da die Erstellung der Zeitstempel auch gleichzeitig erfolgen kann. Unterschied ist, bei IFTTT ist die Reihenfolge vorgegeben. Nachdem ein Bild bei Instagram veröffentlicht wurde, erfolgt ein entsprechender Tweet. Im Gegensatz dazu, kann bei gleichzeitigem Posten nicht vorhergesagt werden, welcher Eintrag den früheren Zeitstempel bekommt. Der fehlende Verweis auf das andere Objekt erschwert bereits die Auswertung deutlich, da hierdurch das Referenzobjekt erst aus der Menge aller Daten im infrage kommenden Zeitraum herausgesucht werden muss. Und der infrage kommende Zeitraum ist hierbei nicht nur die Zeit nach, sondern auch vor dem Veröffentlichungszeitrum des zugehörigen Posts.

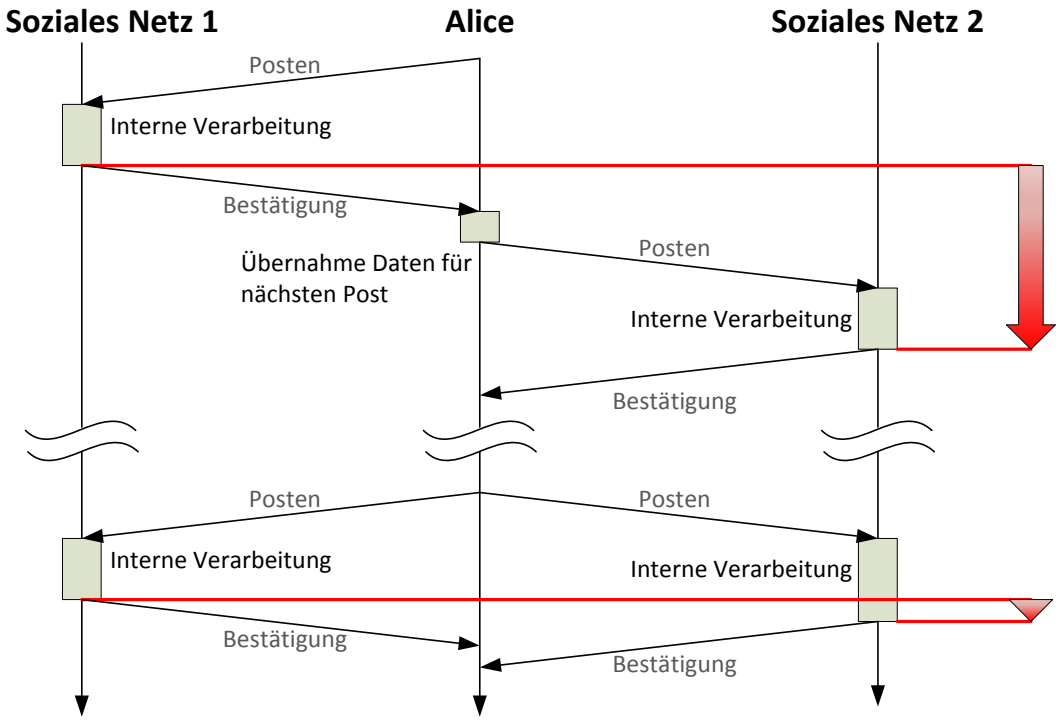


Abbildung 9.2.: Zeitlicher Ablauf des Postens in unterschiedlichen sozialen Netzen bei Nutzung von Tools wie IFTTT.

9.1.3. Bot in einem Netz ohne automatisierte Benachrichtigung

Im Gegensatz zu einem Nutzer verbreitet ein Bot Inhalte gewöhnlich nicht in einem anderen sozialen Netz, sondern im gleichen Netz, wo die Informationen zuerst gepostet wurden. Der Ablauf aus Sicht eines Bots unterscheidet sich lediglich in einem entscheidenden Punkt vom Ablauf des manuellen Vorgangs. Der Unterschied besteht in der Verzögerung, die auftritt, bis der Bot Kenntnis über den neuen Inhalt erlangt, siehe Abbildung 9.3. Bei Twitter ist dies eine äußerst kurze Zeitspanne, da hier beispielsweise einer definierten Menge an Personen "gefolgt"werden kann. Das heißt, ein Bot kann Twitter bei der Anfrage an einen Streaming-Endpunkt eine Liste von bis zu 200 User-IDs übergeben. Solange der Stream zwischen Twitter und Bot besteht, laufen alle öffentlichen Tweets der spezifizierten Nutzer über den Stream zum Bot. Hierbei ist mit Verzögerungen von maximal wenigen hundert Millisekunden zu rechnen. Vergleichbare Möglichkeiten bieten auch andere Netze aber längst nicht alle.

Instagram bietet die Möglichkeit des "Folgens" per Stream oder Push-Benachrichtigung beispielsweise nicht, hier kann sich ein Bot nicht automatisch bei neuen Inhalten benachrichtigen lassen. Dieser muss periodisch auf neue Inhalte prüfen, siehe hierzu auch die Grafik 9.5, allerdings ist davon auszugehen, dass bei zu häufigen Anfragen, beispielsweise alle paar Sekunden, ein Block der IP-Adresse von Instagram erfolgen wird. Die Verzögerung, bis ein Bot Kenntnis über neue Inhalte erlangt, ist daher für soziale Netze, die keine Schnittstelle zur automatisierten Benachrichtigung bieten, schwer abzuschätzen.

9.1.4. Bot in einem Netz mit automatisierter Benachrichtigung

Die Nutzung von Bots kommt besonders häufig bei Twitter vor, Hauptgrund ist die bereits genannte Möglichkeit, zeitnah über neue Inhalte benachrichtigt zu werden. Hier retweeten Bots häufig, entweder Inhalte von spezifizierten Nutzern und/oder zu bestimmten Themen. Hierbei können die Tweets sowohl inhaltlich unverändert aber auch manipuliert, beispielsweise durch Wortersetzungen retweetet werden, aber auch Tweets gegensätzlicher Meinungen werden als Reaktion auf neue Inhalte eines unbeliebten Urhebers, aus Sicht des Boterstellers, retweetet. Die Reaktion eines Bots erfolgt fast ausschließlich nicht als eigenständiger Tweet, sondern als Retweet, so dass der Ursprungstweet ermittelbar und sogar in den zugehörigen (Meta-)Informationen des Retweets enthalten ist. Aufgrund der kurzen Benachrichtigungszeiten bei Twitter ergeben sich Unterschiede zwischen Tweet und Retweet eines Bots von einigen Millisekunden bis hin zu wenigen Sekunden. Bei anderen Netzen können geringfügig größere Zeitunterschiede auftreten, dies hängt von den Benachrichtigungsmöglichkeiten dieser Netze und deren Umsetzungen ab.

Aufgrund der kurzen Zeitunterschiede zwischen Ursprungstweet und dem zugehörigen Retweet lassen sich Twitter-Bots leicht identifizieren. Grund hierfür ist, dass hierbei ein Bezug zwischen zwei Ereignissen besteht, der keinen typischen Usecase darstellt und damit die Nutzung von Diensten wie IFTTT (nahezu) ausgeschlossen werden kann. Ein Nutzer, der Informationen verbreiten möchte, antwortet nicht auf eigene Tweets. Auch wenn dieser Abschnitt sich

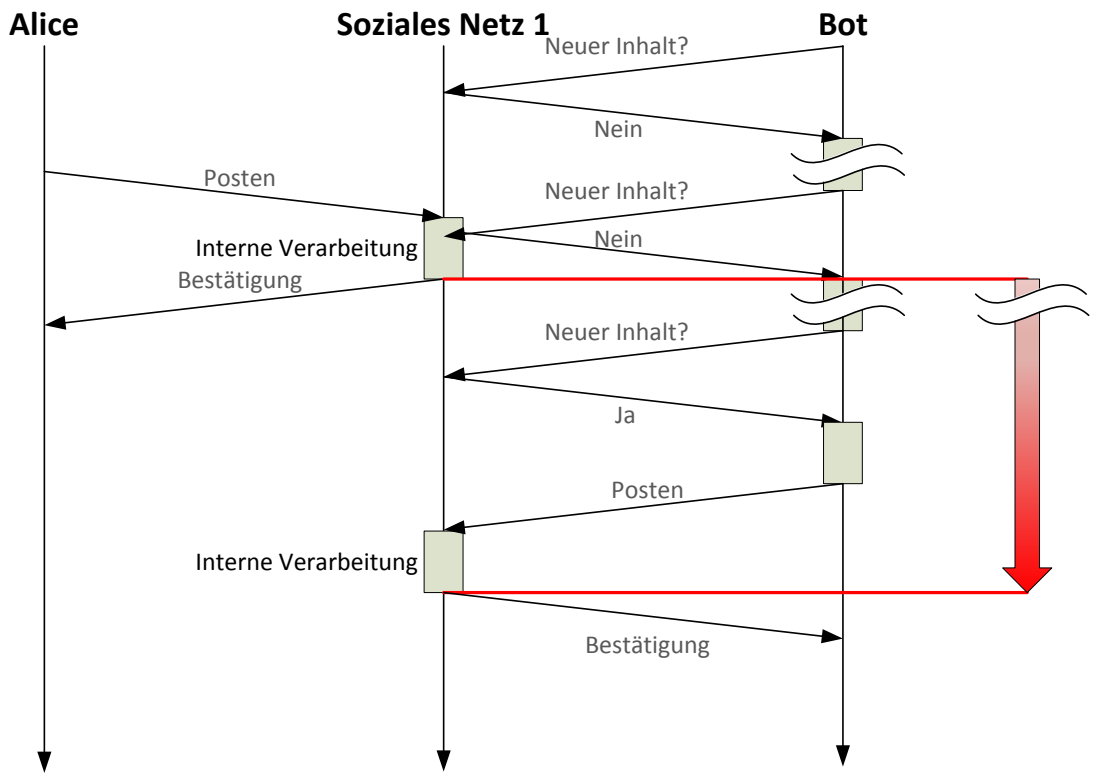


Abbildung 9.3.: Zeitlicher Ablauf des Postens eines Bots ohne automatisierte Benachrichtigung.

wesentlich auf Twitter fokussiert, so sind diese Aussagen dennoch auch auf andere Netze mit automatischer Benachrichtigung übertragbar.

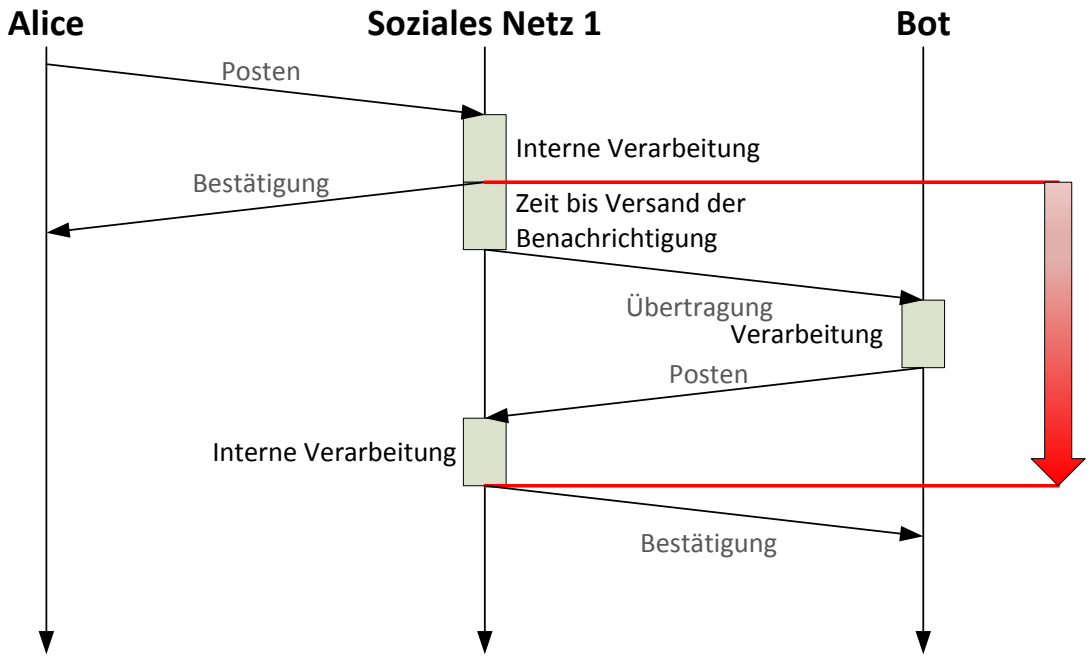


Abbildung 9.4.: Zeitlicher Ablauf des Postens eines Bots bei automatisierter Benachrichtigung.

9.1.5. Posten eines Identitätsdiebes

Anders sieht dies bei Identitätsdiebstahl aus. Will der Dieb, um unauffälliger zu agieren, Inhalte des Bestohlenen aus anderen Netzen in sein Profil übernehmen, ist er gezwungen, periodisch das Profil des Opfers auf neue Inhalte zu prüfen. Da solche Inhalte, abhängig vom Netz, nur wenige Male am Tag oder seltener gepostet werden können, erfolgen wie in Abbildung 9.5 gezeigt, viele Anfragen, ohne, dass eine Änderung stattgefunden hätte. Zudem ist die Wahrscheinlichkeit hoch, dass die Anfrage mit größerem zeitlichen Abstand nach dem Post erfolgt. Sobald der Identitätsdieb einen neuen Inhalt des Opfers bemerkt hat, wird dieser ggf. noch geändert oder manipuliert, bevor er auf dem Profil des Diebes gepostet wird. Dies führt ebenfalls zu zeitlichen Verzögerungen. Im Vergleich zu manueller und besonders zu automatischer Inhaltsübernahme ist der Zeitunterschied in diesem Fall deutlich größer. Große Zeitunterschiede können zwar auch bei manueller Übernahme auftreten, allerdings auch kurze. Zeitunterschiede von wenigen Minuten sind bei einem Identitätsdieb jedoch nicht zu erwarten. Diese Profile können daher durch Auswertung im Hinblick auf die minimalen zeitlichen Abstände identifiziert werden. Von der Nutzung eines Bots ist auch nicht auszugehen, da der Dieb potentiell den Inhalt der Nachricht abwandeln muss, um nicht aufzufallen bzw.

enttarnt zu werden.

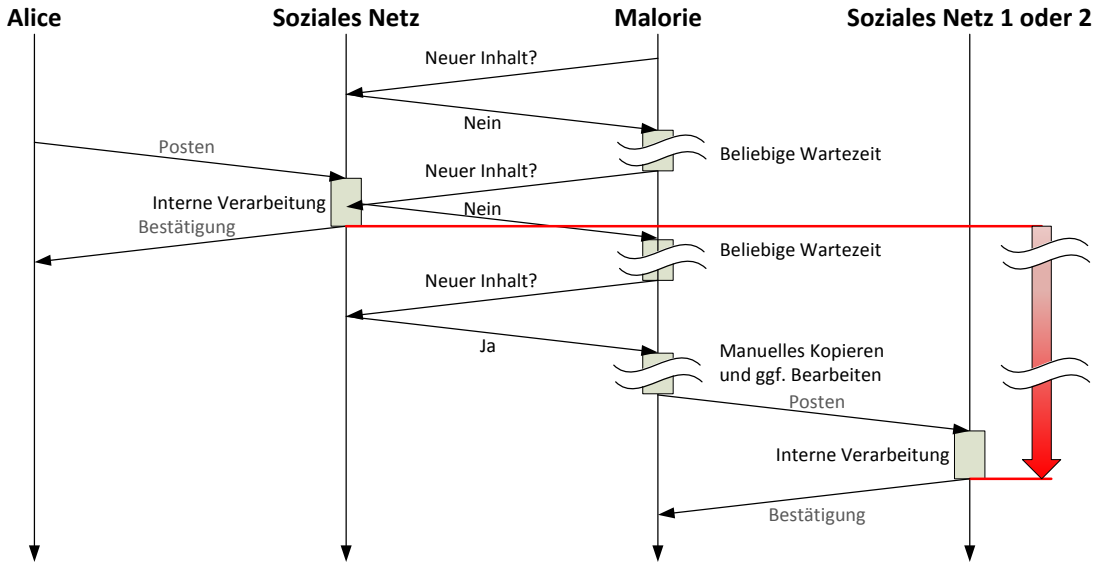


Abbildung 9.5.: Zeitlicher Ablauf des Postens in unterschiedlichen sozialen Netzen im Falle von Identitätsdiebstahl.

9.1.6. Zusammenfassung

In den vorangegangenen Abschnitten wurden verschiedene Konstellationen für das zweimalige Posten schwerpunktmäßig in unterschiedlichen, aber auch für das gleiche soziale Netz untersucht. Die zeitlichen Rahmenbedingungen, die Zeitdifferenzen zwischen diesen zwei Posts, der beschriebenen Abläufe sind in Tabelle 9.1 zusammengefasst.

Bei dem Vorgang des manuellen Postens, dem händischen Übertragen eines Inhalts von einem sozialen Netz in ein anderes, kann von einer deutlichen Verzögerung ausgegangen werden, in der Tabelle mit $>\sim$*10 Sekunden* bezeichnet. Dieser Wert ist eine Schätzung besonders zügigen Arbeitens. Beim Versuch, hierin einen Rekord aufzustellen, kann der Wert unterboten werden, dies erfordert aber eine Vorbereitung, innere Anspannung und Konzentration, die für so alltägliche Dinge alles andere als zu erwarten ist. Daher liegt der Durchschnitt deutlich höher.

Anders verhält es sich bei automatischem Posten. Hier sind Zeitdifferenzen unter einer Sekunde nicht ungewöhnlich, der begrenzende Faktor ist besonders die Übertragungszeit der Informationen. Deshalb ist auch im Durchschnitt nur von wenigen Sekunden auszugehen.

Sind Bots in sozialen Netzen ohne Möglichkeiten zur automatisierten Benachrichtigung bei neuen Inhalten aktiv, so ergibt sich zwar eine geringe Wahrscheinlichkeit, dass die minimale

Zeitdifferenz im Rahmen des automatischen Postens liegt, allerdings ist im Durchschnitt von einigen Sekunden bis hin zu Minuten auszugehen. Grund ist die Notwendigkeit der periodischen Anfrage und der damit einhergehenden Gefahr einer IP-Sperrung, wenn die Periode hierfür zu kurz gewählt ist.

In Netzen, die Funktionen zur automatischen Benachrichtigung bieten, beispielsweise Twitter, ist die minimale und die durchschnittliche Zeitdifferenz im gleichen Rahmen angesiedelt wie beim automatischen Posten durch einen Nutzer. Unterschied hierbei ist häufig, dass beispielsweise bei Twitter ein Bot neue Inhalte, die auf Twitter veröffentlicht werden, auch bei Twitter retweetet. Ein Vorgehen, das es ermöglicht, Inhalte in kurzer Zeit zu verbreiten, aber das bei einem Nutzer keine Verwendung findet, da dieser mit jedem Post die gleiche Zielgruppe erreichen würde.

Im Falle von Identitätsdiebstahl fallen die Zeitunterschiede hingegen sehr groß aus. Dies liegt daran, dass der Dieb periodisch auf neue Inhalte prüfen muss. Da es sich hierbei nicht um einen Bot, sondern einen Nutzer handelt, der beispielsweise auch schlafen oder arbeiten gehen muss, ist durchschnittlich mit wenigen Stunden zu rechnen. Minimal werden $\gg$ 30 Sekunden genannt, dies ist jedoch nur zufällig zu erreichen.

Tabelle 9.1.: Vergleich der Zeitunterschiede für die in diesem Abschnitt beschriebenen Abläufe zwischen ersten und zweiten Post.

Ablauf	**minimale Zeitdifferenz**	**durchschnittliche Zeitdifferenz**
manuelles Posten	> $\sim$10 Sekunden	wenige Minuten
automatisches Posten	> 0 Sekunden	wenige Sekunden
Bot: Netz ohne Benachrichtigung	> 0 Sekunden	einige Sekunden bis Minuten
Bot: Netz mit Benachrichtigung	> 0 Sekunden	wenige Sekunden
Identitätsdiebstahl	$\gg$ 30 Sekunden	Stunden

9.2. Prinzip der Nutzung von Zeitdifferenzen

Die zu erwartenden Zeitunterschiede wurden im vorangegangen Abschnitt im Detail erläutert. Die nachfolgenden Ausführungen bauen hierauf auf.

Das Prinzip der Nutzung von Zeitdifferenzen ist, anhand der Zeitunterschiede zweier Posts in unterschiedlichen Netzen, von denen einer auf den anderen verweist, zu entscheiden, ob es eine valide Profilzuordnung ist. Valide bedeutet, dass beide verwendeten Profile dem gleichen Nutzer zugehörig sind. Dies ist insbesondere bei der Nutzung von Diensten wie IFTTT möglich, da keine andere Möglichkeit besteht, derart kurze Reaktionszeiten zu erreichen.

Andererseits lassen sich auch Bots detektieren, da diese innerhalb des gleichen sozialen Netzes aktiv sind, und vergleichbare Zeitdifferenzen generieren, so das Netz automatische

Benachrichtigungen ermöglicht. Auch ohne automatische Benachrichtigungen bleiben die Zeitdifferenzen klein genug, um einen Nutzer von einem Bot zu unterscheiden, da die Spannweite der zu beobachtenden Reaktionszeiten bei einem Bot deutlich begrenzter als bei einem Nutzer ist.

Nach dem gleichen Prinzip lässt sich auch Identitätsdiebstahl detektieren. Hierbei sind die Reaktionszeiten immer sehr groß und nur in seltenen Ausnahmefällen erfolgt eine Reaktion zeitnah. Dies unterscheidet sich auch zum manuellen Posten, da hier nicht immer, aber häufig, beide Posts nacheinander ausgeführt werden, wodurch im Vergleich zu einem Identitätsdieb weitaus kürzere Reaktionszeiten auftreten.

9.3. Datensatz

Zur Evaluation dieses Verfahrens wurden getrennt voneinander zwei Datensätze betrachtet, einer kam im Rahmen der Veröffentlichung [327] zur Profilzuordnung, der andere im Rahmen der Munich Bot Challenge zur Boterkennung des Munich Center for Internet Research der Bayerischen Akademie der Wissenschaften zum Einsatz, siehe [346].

9.3.1. Profilzuordnung

Zur Evaluation dieses Verfahrens wurde ein Datensatz von Twitter herangezogen, der im Zeitraum vom 13. bis 20. Februar 2017 gesammelt wurde. Hierzu wurde Twitters Filterstream als Parameter eine den vollständigen Koordinatenraum-abdeckende Geoboundingbox übergeben. Auf diese Weise können alle Tweets, die ein Geotag enthalten, gesammelt werden, solange nicht Twitters 1%-Grenze überschritten wird. Diese Grenze sorgt dafür, dass nicht mehr als 1% der Tweets über einen Stream erhalten werden können.

Für dieses Verfahren ist kein Datensatz nötig, der Geotags enthält, so ist dieser aber auch für andere Verfahren nutzbar. Von den empfangenen Tweets enthalten 31% mindestens eine URL. Diese wurden für die Evaluation dieses Verfahrens ausgewählt, dabei verblieben 27.496.623 Tweets von 3.546.332 verschiedenen Nutzern. Tabelle 9.2 gibt einen Überblick über alle Domains der enthaltenen URLs, die mindestens 20.000 mal beobachtet wurden.

Interessanterweise kann man anhand der Häufigkeit der Domains aus Tabelle 9.2 keine Rückschlüsse auf die Häufigkeit der Nutzung dieser Webseiten und sozialen Netze ziehen. Sonst müssten Einträge wie Facebook oder Youtube an der Spitze dieser Liste stehen.

Die große Anzahl an Twitter-URLs geht wahrscheinlich auf die Tatsache zurück, dass im Falle von Retweets die URL des initialen Tweets im Retweet enthalten ist. Der zweitgrößte Anteil entfällt mit fast 21% auf Instagram. Es bietet sich an, diese für Profilzuordnungen zu nutzen, daher erfolgt die Evaluation dieses Verfahrens auch anhand der Zuordnung zwischen Twitter und Instagram.

Tabelle 9.2.: Übersicht über beobachtete Domains der beiden Datensätze

Pos	Domain	# of URLs	% of URLs
1	twitter.com	12,337,243	44.868
2	www.instagram.com	5,725,515	20.823
3	www.swarmapp.com	3,272,405	11.901
4	bit.ly	1,726,929	6.281
5	path.com	528,843	1.923
6	youtu.be	243,280	0.885
7	ln.is	200,909	0.731
8	www.youtube.com	192,224	0.699
9	www.trendinalia.com	152,532	0.555
10	goo.gl	143,091	0.520
11	dlvr.it	88,297	0.321
12	untp.beer	79,649	0.290
13	www.facebook.com	57,992	0.211
14	www.trendsmap.com	57,674	0.210
15	central132.cl	48,220	0.175
16	511ny.org	45,111	0.164
17	toplocalnow.com	43,670	0.159
18	curiouscat.me	39,970	0.145
19	soundcloud.com	35,368	0.129
20	www.periscope.tv	35,213	0.128
21	j.mp	34,285	0.125
22	www.careerarc.com	33,305	0.121
23	open.spotify.com	31,236	0.114
24	bitly.com	22,815	0.083
25	cards.twitter.com	20,957	0.076
-	Other	2,299,890	8.364

Der Datensatz enthält 5.725.515 Instagram URLs, die von 1.435.806 Nutzern stammen. Dies entspricht fast vier URLs pro Nutzer. Nach einer allgemeinen Validitätsüberprüfung der URLs, ob diese einem gültigen URL-Schema entsprechen, verblieben 5.720.098 URLs für den Evaluationsdatensatz. Dies entspricht einer Reduktion von unter 0,95‰.

Alle gültigen Instagram-URLs wurden zwischen Ende März und Anfang April 2017 abgefragt, um die zugehörige Instagram-User-ID zu erhalten und die Gültigkeit der URL zu überprüfen, da die alleinige Konformität zu einem URL-Schema keine Aussage darüber erlaubt, ob diese URL jemals existiert hat. Nachdem aber die Abfrage der Instagram-URLs erst etwa sechs Woche nach dem Sammeln der Tweets erfolgt ist, wurden potentiell bereits wieder Inhalte offline genommen, was zu Fehlern führte, da die Datei nicht gefunden werden konnte. Es wird angenommen, dass es sich im Falle von aufgetretenen Fehler um bereits offline genommene Inhalte handelt, da es keinen Sinn ergibt, eine imaginäre URL mit korrekter Struktur zu posten.

Hieraus kann kein Vorteil gezogen werden und dürfte, so dies überhaupt vorkommt, eine äußerst seltene Ausnahme darstellen.

Neben dem erfolgreichen Aufruf einer Seite und Datei-nicht-gefunden-Fehlermeldungen trat noch eine weitere Kategorie auf. Für eine nicht unerhebliche Anzahl an Anfragen wurde ein HTML-Fehlercode empfangen, diese machten es erforderlich, eine URL erneut anzufragen. Durch wiederholende Abfragen konnten am Ende alle URLs in die beiden Kategorien erfolgreich bzw. Datei-nicht-gefunden einsortiert werden. Diesen Umstand gilt es beim produktiven Einsatz dieses Profilzuordnungsverfahrens zu berücksichtigen.

Tabelle 9.3 zeigt das Ergebnis der Abrufversuche. Über 92% aller URLs konnten erfolgreich abgerufen werden. Da weniger als 8% der angefragten URLs am Ende einen Datei nicht gefunden Fehler liefert, wird angenommen, dass es sich hierbei um offline genommene Inhalte und nicht um ungültige URLs handelt. Durch die bereits erwähnten HTML-Fehler-Codes waren 347.610 zusätzliche Anfragen erforderlich, was einem Anstieg um fast 6,1% entspricht.

Tabelle 9.3.: Übersicht der erforderlichen Abrufversuche und notwendige Iterationen zur Eingruppierung aller URLs in die Kategorien erfolgreich und Datei nicht gefunden. Spalten mit HTML enthalten die Anzahl der empfangenen HTML Fehler Codes.

Iteration	# Erfolg	# Fehler	# HTML	% Erfolg	% Fehler	% HTML
1	4,938,126	434,362	292,687	86.329	7.594	5.117
2	276,856	15,831	41,994	79.646	4.554	12.081
3	38,966	3,028	10,582	70.947	5.513	19.267
4	9,993	589	2,347	77.291	4.556	18.153
5	2,254	93	0	96.037	3.963	0.000
Ergebnis	5,266,195	453,903		92.065	7.935	

9.3.2. Munich Bot Challenge

Vom 6. Juli 2017 bis 22. September 2017 führte das MCIR, Munich Center for Internet Research der Bayerischen Akademie der Wissenschaften, die Munich Bot Challenge durch. Dabei handelte es sich um einen öffentlichen Wettbewerb zur Entwicklung neuartiger Boterkennungsmethoden. Für die Evaluation der eingereichten Methoden wurde eine Liste zu untersuchenden Twitterprofile veröffentlicht. Diese enthielt 1.075.439 Twitter User-IDs. Für die Auswahl der Kandidatenmenge wurden alle Follower der folgenden drei Profile (Profilname auf Twitter in Klammern), des deutschen Regierungssprechers (*RegSprecher*), des damaligen Kanzlerkandidaten Martin Schulz (*MartinSchulz*) und der Technischen Universität München (*TU_Muenchen*) ausgewählt. Da hierbei eine gewisse Überschneidung bestand, reduzierte sich die Anzahl auf 1.026.728 eindeutige User-IDs. Eine Übersicht, wie sich diese Profile zusammensetzen, gibt Tabelle 9.4.

Tabelle 9.4.: Übersicht über die Zusammensetzung der Profilmenge des Munich Bot Challenge Datensatzes.

Profiltyp	Anzahl
Gelöschte oder gesperrte Accounts	1.325
Protected Accounts	65.048
Accounts ohne Tweets	306.334
Analysierbare Accounts	654.021

Für die Erstellung des Datensatzes wurden die Timelines der analysierbaren Profile abgerufen, wobei maximal die letzten 3.200 Tweets eines Users abfragbar sind. Der gesammelte Datensatz enthält 341.394.982 Elemente, davon 164.998.213 Tweets, 125.269.618 Retweets und 51.127.152 Replies. Dies entspricht 48,330591%, 36,693456% bzw. 14,9759529% der gesamten Tweetmenge. Auf einen Nutzer entfallen somit durchschnittlich 252,28 Tweets, 191,54 Retweets und 78,17 Replies.

Für die Auswertung der Verfahren musste eine Liste dieser IDs abgegeben werden, wobei für jede ID ein Wahrscheinlichkeitswert zwischen 0, kein Bot, und 1, ein Bot, zu nennen war. Nicht mehr verfügbare Profile sollten mit -1 gekennzeichnet werden.

9.4. Zuordnungsverfahren

Alle Instagram-URLs, auch nicht mehr abfragbare aufgrund eines Datei-nicht-gefunden-Fehlers, wurden, wie bereits in Abschnitt 7.1.2 erläutert, decodiert und Informationen wie der Erstellungszeitstempel in einer Datenbank gespeichert. Hierbei mussten 247 URLs entfernt werden, die Teil der Liste der nicht gefundenen Inhalte sind, da deren Zerlegung zu negativen Zeitstempeln führte. Dies ist nur durch ungültige URLs erreichbar, es könnte sich hierbei aber beispielsweise um einen Copy & Paste-Fehler handeln. Wird am Ende der URL ein Zeichen zu viel angehängt, wird die ID als entsprechend größer interpretiert, wodurch auch der Zeitstempel sich vergrößert und in den negativen Bereich abrutschen kann. Ergänzend zu den Instagram-IDs wurde dies, vgl. Abschnitt 7.1.1, für die zugehörigen Tweet-IDs vorgenommen. Hierdurch erhält man zwei Zeitstempel, jeweils den Zeitpunkt der Erzeugung des Instagram-Posts und des Tweets auf Twitter, beide bis auf die Millisekunde genau. Dies ermöglicht Rückschlüsse unter Einbeziehung der Erkenntnisse über die unterschiedlichen Nutzerverhalten aus Abschnitt 9.1.

Für dieses Verfahren ist prinzipiell auch erstmal keine Anfrage an Instagram erforderlich. Alle benötigten Informationen können aus der URL bzw. den beiden IDs extrahiert werden. Erst wenn eine konkrete Zuordnung zweier User-IDs zueinander erfolgen soll, muss diese bei Instagram ermittelt werden. Für bereits erfolgte Zuordnungen kann dies jedoch unterbleiben. Da die Twitter-User-ID immer vorliegt, können bereits erfolgte Zuordnungen aussortiert und nur sporadisch auf deren Gültigkeit überprüft werden. Hierdurch ist dieses Verfahren sehr

schnell und weist nur einen geringen Berechnungsaufwand auf.

Zu berücksichtigen ist jedoch, dass nicht anhand eines einzelnen Tweets Zuordnungen stattfinden sollten, um *false Positives* auszuschließen. Es besteht die Gefahr, dass jemand, der beispielsweise ein Bild tweetet, das ihm gut gefällt, diesem Profil fälschlicherweise zugeordnet wird. Dies sollte aber durch die entsprechenden Zeitdifferenzen offensichtlich sein und abgefangen werden. Zudem kommt dies, wie später noch gezeigt wird, sehr selten vor. Es ist dennoch ein geeigneter Grenzwert an beobachteten Tweets zu einem konkreten Instagram Profil zu definieren, bei dessen Erreichen eine gültige Zuordnung angenommen wird.

Das Verfahren zur Boterkennung unterscheidet sich nur marginal vom Ansatz der Profilzuordnung. Unterschied ist lediglich, dass nicht eine Tweet-ID und eine Instagram-Media-ID hinsichtlich Zeitdifferenz analysiert werden, sondern zwei Tweet-IDs, die des Tweets und des darauf folgenden Retweets. Bei entsprechend geringem zeitlichen Abstand kann von einem Bot ausgegangen werden.

9.5. Evaluation

In diesem Abschnitt werden die Ergebnisse des Verfahrens für die eingangs vorgestellten Datensätze präsentiert. Zuerst werden die Ergebnisse des Profilzuordnungsdatensatzes erläutert um im Anschluss auf die Ergebnisse der Boterkennung einzugehen.

9.5.1. Profilzuordnung

Für den ersten Datensatz wurden die Zeitunterschiede zwischen den Tweet-Zeitstempel und den entsprechenden Instagram-Zeitstempeln analysiert. Das Ergebnis ist in Tabelle 9.5 dargestellt. Jede Zeile definiert eine bestimmte Zeitspanne zwischen Instagram- und Twitter-Zeitstempel und die Anzahl an Tweets, die in die entsprechende Kategorie fallen. Die letzte Spalte kumuliert den Prozentsatz jeder Zeile, dadurch ist es einfach, den Anteil an Tweets seit dem Instagram Post für jedes Zeitintervall abzulesen.

Offensichtlich ist es nur eine Frage der Aktualität, warum Instagram-Inhalte auf Twitter geteilt werden. Über 75% aller Instagram-URLs wurden innerhalb von drei Sekunden nach der Veröffentlichung auf Instagram getweetet, fast 90% nach fünf Sekunden. Wie bereits erwähnt, kommt es äußerst selten vor, dass ein Nutzer durch Instagram scrollt und ein Bild, das ihm gut gefällt, tweetet. Dies lässt sich leicht daran zeigen, dass über 98% aller URLs innerhalb einer Stunde und über 99% innerhalb eines Tages geteilt werden. Bilder, die älter als ein Jahr waren, wurden nur 677 mal geteilt, das ist so gut wie nichts.

In Tabelle 9.5 wurde zur besseren Lesbarkeit auf eine Unterscheidung zwischen kurzen und langen Instagram-URLs verzichtet. Der Vollständigkeit halber sind diese jedoch in Abbildung 9.6 grafisch aufbereitet. Es gibt nur geringe Unterschiede, aber allgemein lässt sich sagen, dass der

Tabelle 9.5.: Übersicht der Zeitunterschiede zwischen der Veröffentlichung auf Instagram und Twitter

Zeitdifferenz	# Tweets	% Tweets	cum. % Tweets
t <= 1s	208.224	3,640	3,640
1s < t <= 2s	2.646.224	46,262	49,902
2s < t <= 3s	1.467.924	25,663	75,565
3s < t <= 4s	638.606	11,164	86,729
4s < t <= 5s	169.911	2,970	89,699
5s < t <= 10s	174.527	3,051	92,750
10s < t <= 1m	166.259	2,907	95,657
1m < t <= 1h	139.569	2,440	98,097
1h < t <= 1d	61.860	1,081	99,178
1d < t <= 1wk	21.561	0,377	99,555
1wk < t <= 1mo	10.588	0,185	99,740
1mo < t <= 1y	14.168	0,248	99,988
t > 1y	677	0,012	100,000

Zeitunterschied für lange URLs signifikant kleiner ist. Nichtsdestotrotz ist die durchschnittliche Differenz für kurze URLs 35.656,4 Sekunden bzw. 9,9 Stunden und für lange URLs 36.698,0 Sekunden bzw. 10,2 Stunden, was der Erwartung zuwiderläuft. Allerdings ist die Aussagekraft dieser Werte aufgrund des massiven Einflusses älterer Zeitstempel gering. Betrachtet man nur Zeitstempel kleiner einer Stunde, was ungefähr 98% entspricht, wird dies offensichtlicher. Der Durchschnitt hier beträgt für kurze URLs 21,0 Sekunden, im Gegensatz zu 18,0 Sekunden für lange URLs. Folglich ist der Durchschnitt für kurze URLs und der gewählten Teilmenge ungefähr 16,67% größer.

Die Annahme, dass der tweetende Nutzer typischerweise identisch ist mit dem Nutzer auf Instagram, wird untermauert durch die Anzahl an URLs, die von mindestens zwei verschiedenen User-IDs getweetet wurden. Tabelle 9.6 gibt einen Überblick über die Anzahl an URLs, auf die dies zutrifft. Offensichtlich ist es ein sehr geringer Teil aller URLs, betroffen sind nur 470. Hinzu kommt, dass einige dieser URLs nicht auf ein Bild, sondern auf Profilseiten oder die Instagram Webseite an sich, beispielsweise die URL mit 32 verschiedenen Twitter-User-IDs, verweisen. Nachdem diese URLs keine Media-ID und damit keinen Zeitstempel enthalten, sind diese Teil der wegen Ungültigkeit aussortierten URLs. Die dritte Spalte der Tabelle enthält die Anzahl an URLs, die tatsächlich auf eine Media-ID verweisen. Der Datensatz enthält 5.687.409 eindeutige Media-IDs, davon wurden 444 von mehr als einem Nutzer getweetet. Dies entspricht einem Anteil von 0,078‰. Daher ist die Wahrscheinlichkeit einer URL, von mehr als einem Nutzer getweetet zu werden, nahezu Null. Das bedeutet, dass selbst Fans typischerweise nicht die Fotos von Prominenten teilen, denen sie folgen.

Eigentlich gibt es keinen Grund, eine URL mehr als einmal zu teilen, da Twitters Timeline es erlaubt, die letzten paar hundert Tweets eines Nutzers einzusehen. Außerdem erreicht jeder

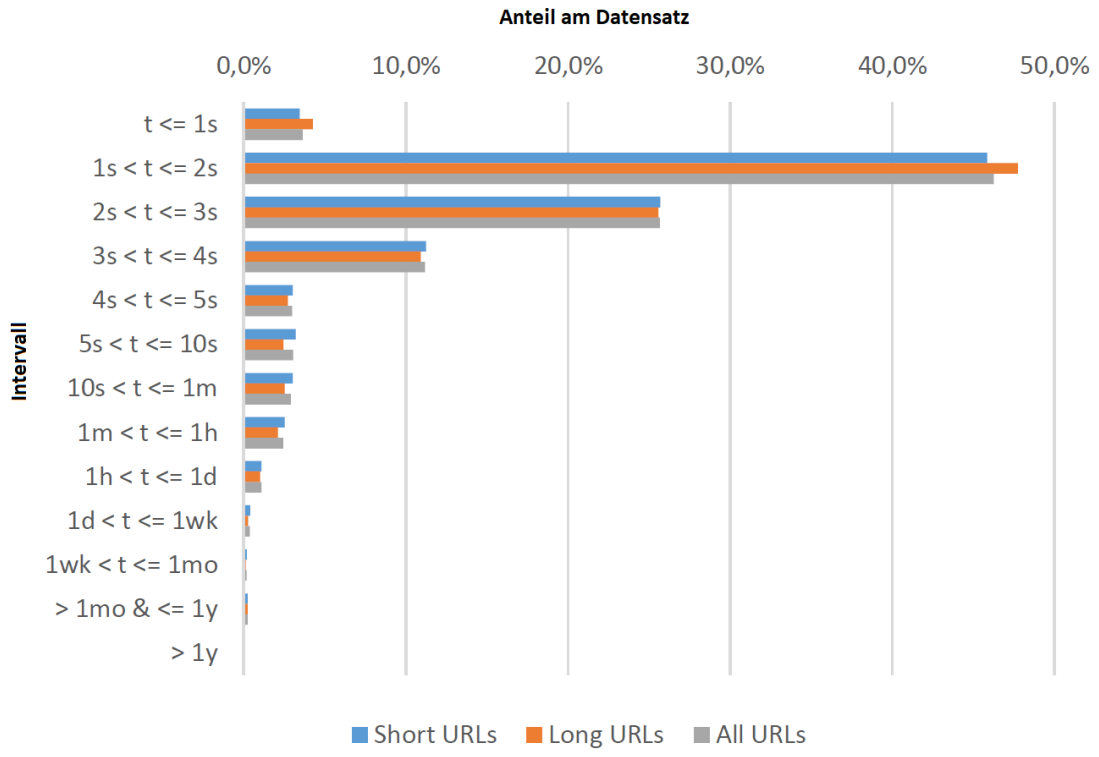


Abbildung 9.6.: Grafische Darstellung der Zeitunterschiede inklusive der getrennten Betrachtung der Verteilung von kurzen und langen Instagram-URLs.

Tweet nur die Follower dieses Users. Trotzdem kommt dies, wenn auch selten, vor. Nur 0,94% aller URLs sind Duplikate. Tabelle 9.7 gibt eine Übersicht von URLs, die von einem Nutzer mehr als einmal getweetet wurden. Aufgrund der Anzahl der Einträge wurde die Tabelle zweispaltig ausgeführt. Der erste Wert einer Zeile gibt die Häufigkeit an, wie oft eine einzelne URL beobachtet wurde. Der zweite Wert enthält die Anzahl der hiervon betroffenen URLs und der dritte Wert die Anzahl der Nutzern, von denen dies ausgeht. Die letzte Zeile der Tabelle, enthält die Summe betroffener URLs als auch der eindeutigen User-IDs, von denen dieses Verhalten ausgeht. Von den 17.312 Nutzern, die Duplikate getweetet haben, sind 2.568 Wiederholungstäter, die mehr als einmal eine URL mehrfach getweetet haben. 390 sogar fünf mal oder noch öfter.

9.5.2. Boterkennung

Für die Boterkennung wurde die zeitliche Differenz zwischen einem initialen Tweet und einem darauffolgenden Retweet bzw. Reply des Munich Bot Challenge Datensatzes ausgewertet, um Profile zu detektieren, deren Reaktionszeit die eines Menschen unterschreitet.

Tabelle 9.6.: Anzahl der beobachteten URLs von mindestens zwei unterschiedlichen Twitter-User-IDs.

Eindeutige User-IDs	# der URLs	# der Media-URLs
32	1	-
26	1	1
11	1	-
6	4	2
5	3	2
4	8	4
3	17	17
2	435	418
$\sum$	470	444

Tabelle 9.7.: Anzahl mehr als einmal beobachteter URLs von einzelnen Nutzern: EZ: einzelne, ED: eindeutige

# EZ URL	# von URLs	# ED User-IDs	# EZ URL	# von URLs	# E User-IDs
33	1	1	12	6	6
31	1	1	11	9	6
27	1	1	10	15	11
25	1	1	9	37	24
22	1	1	8	50	29
19	1	1	7	47	27
18	4	3	6	95	66
17	8	5	5	173	122
16	8	5	4	478	300
15	2	2	3	1,723	1,169
14	9	5	2	21,666	16,491
13	8	5	$\sum$	24,344	17,312

Die Analyse erfolgte nach gleichem Schema und identischen Zeitintervallen wie für die Profilzuordnung, allerdings getrennt für Retweets und Replies. Tabelle 9.8 zeigt die Verteilung über die verschiedenen Intervalle für Retweets. Im Vergleich zur Verteilung des Profilzuordnungsdatensatzes fällt auf, dass die durchschnittliche Verzögerung deutlich größer ist. Dies resultiert daraus, dass im Profilzuordnungsdatensatz, wie erwartet, vorwiegend automatisch-generierte Tweets enthalten sind, was für diesen Datensatz aber die Ausnahme darstellt und die Existenz generierter Retweets im Rahmen der Boterkennung erst nachgewiesen werden soll.

Aufgrund der geringen Anteils von Retweets im Zeitraum unter 10 Sekunden von ungefähr 0,2%, ist deutlich zu erkennen, dass die Anzahl an Bots in diesem Datensatz entweder sehr gering, oder die verwendeten Bots bereits entsprechende Gegenmaßnahmen implementiert

haben, so dass ein Retweet erst nach einer Zufallsgenerator-gesteuerten Wartezeit erfolgt. Der Großteil aller Retweets, über 80%, sind nicht älter als 24h bei deren Erstellung, 90% nicht älter als eine Woche.

Tabelle 9.8.: Übersicht der Zeitunterschiede zwischen Veröffentlichung eines Tweets und eines darauf basierenden Retweets.

Zeitdifferenz	# Retweets	% Retweets	cum. % Retweets
t <= 1s	2.941	0,002356	0,002356
1s < t <= 2s	1.258	0,001008	0,003364
2s < t <= 3s	1.870	0,001498	0,004861
3s < t <= 4s	8.074	0,006468	0,011329
4s < t <= 5s	17.248	0,013816	0,025145
5s < t <= 10s	218.695	0,175181	0,200326
10s < t <= 1m	6.010.342	4,814450	5,014776
1m < t <= 1h	51.777.793	41,475441	46,490217
1h < t <= 1d	50.971.223	40,829356	87,319573
1d < t <= 1wk	11.274.337	9,031055	96,350628
1wk < t <= 1mo	2.296.231	1,839344	98,189972
1mo < t <= 1y	1.736.683	1,391131	99,581103
t > 1y	522.949	0,418897	100,000000

Tabelle 9.9 zeigt die Verteilung für Replies. Auch hier zeigt sich ein nur sehr geringer Anteil offensichtlich automatisch generierter Tweets. Nur etwas mehr als 0,05% aller Replies erfolgen innerhalb von 10 Sekunden. Die Dauer bis zur Erstellung eines Replies ist wie erwartet aufgrund der nötigen Eingabe einer Antwort, bei Fokussierung auf die ersten 60 Sekunden nach Tweeterzeugung, größer als für Retweets. Im Gegensatz dazu sind Replies insgesamt jedoch aktueller, da fast 69% aller Replies innerhalb der ersten Stunde versandt werden, Retweets nur etwas mehr als 46%. Dies wird noch deutlicher, bei Betrachtung des Anteils innerhalb von 24h, dies sind für Replies fast 95%. Der Anteil nach einer Woche ist nur halb so groß wie für Retweets, nach einem Jahr sogar nur ein Drittel.

Die Anzahl detektierter Bots ist vergleichsweise gering im Vergleich zu Annahmen, dass bis zu 15% der Twitterprofile Bots sind. Dies kann mehrere Ursachen haben, die ohne Anspruch auf Vollständigkeit nachfolgend genauer beleuchtet werden:

- **Stichprobe der Profile zu gering:** Im Rahmen der Munich Bot Challenge wurden, um die Abarbeitung im gegebenen Zeitraum zu ermöglichen, lediglich drei initiale Profile ausgewählt, deren Follower analysiert werden sollten. Diese Anzahl ist potentiell zu gering, um ein realistisches Bild der deutschsprachigen Bots zu erhalten.

- **Globale Verteilung nicht gleichmäßig:** Für viele Veröffentlichungen wurden vorwiegend englisch bzw. amerikanisch-sprachige Profile ausgewertet. Eine Untersuchung der Botak-

Tabelle 9.9.: Übersicht der Zeitunterschiede zwischen der Veröffentlichung eines Tweets und eines darauf basierenden Replies.

Zeitdifferenz	# Replies	% Replies	cum. % Replies
t <= 1s	944	0,001880	0,001880
1s < t <= 2s	398	0,000793	0,002672
2s < t <= 3s	308	0,000613	0,003286
3s < t <= 4s	676	0,001346	0,004632
4s < t <= 5s	999	0,001990	0,006622
5s < t <= 10s	23.351	0,046505	0,053126
10s < t <= 1m	3.487.294	6,945087	6,998213
1m < t <= 1h	31.130.861	61,998368	68,996581
1h < t <= 1d	12.792.318	25,476418	94,472999
1d < t <= 1wk	2.028.308	4,039457	98,512457
1wk < t <= 1mo	410.132	0,816794	99,329512
1mo < t <= 1y	272.904	0,543499	99,872751
t > 1y	63.895	0,127249	100,000000

tivitäten über die verschiedenen Länder und Sprachen ist bisher nicht umfassend erfolgt. Was für amerikanische Profile richtig ist, muss nicht auch für deutsche gelten.

- **Implementierte Gegenmaßnahmen:** Es besteht die Möglichkeit, dass aufgrund der Bestrebungen der Betreiber sozialer Netze, Bots zu verbannen, Bots bereits entsprechende Gegenmaßnahmen für den hier gewählten Ansatz implementiert haben. Dies lässt sich jedoch nicht verifizieren.

Der genaue Grenzwert zur Entscheidung, ob es sich um einen Bot handelt, liegt wahrscheinlich im Bereich von etwa 5 Sekunden. Für eine genaue Festlegung ist jedoch eine Evaluation anhand von Ground-Truth-Daten notwendig, die in Ermangelung eines solchen Datensatzes an dieser Stelle leider nicht durchgeführt werden kann.

9.6. Zusammenfassung

In diesem Kapitel wurden die Möglichkeiten der Profilzuordnung und der Boterkennung anhand von Zeitstempeln bzw. Zeitdifferenzen behandelt. Hierzu wurden zuerst die Grundlagen typischer Nutzungsszenarien geschaffen und daraus die Auswirkungen auf die Zeitdifferenzen abgeleitet. Darauf aufbauend wurde das Prinzip der Nutzung von Zeitdifferenzen im Detail erläutert. Es wurden zwei Datensätze, jeweils einer für die Profilzuordnung und Boterkennung, vorgestellt und im Rahmen der Evaluation die Ergebnisse detailliert diskutiert.

Es konnte gezeigt werden, dass sich dieser Ansatz für beide Verfahren hervorragend eignet. Nichtsdestotrotz konnte die Evaluation in Ermangelung von Ground-Truth-Daten nicht vollumfänglich abgeschlossen werden.

KAPITEL 10

Geobasierte Profilzuordnung

Dieses Kapitel behandelt die Nutzung von Geotags zur Profilzuordnung. Dabei wird ein Algorithmus schrittweise erarbeitet. Die Erkenntnisse eines jeden Schrittes dienen zur Verfeinerung der Ergebnisse und der Planung der weiteren Vorgehensweise. Zuvor wird jedoch der verwendete Datensatz näher betrachtet.

10.1. Datensatz

Basierend auf dem About.me-Datensatz, welcher bereits in 7.2.2 näher analysiert wurde, erfolgte das Crawling für den hier genutzten Datensatz. Hierzu wurden die Twitter-Profile aus dem About.me-Datensatz extrahiert und alle zu dieser Zeit verfügbaren Tweets gecrawlt. Von den enthaltenen 103.565 Twitter-Profilen konnten 86.792 erfolgreich gecrawlt werden. Die Tweets von 16.773 Profilen konnten nicht ermittelt werden. Hierfür gab es mehrere Ursachen. Entweder waren die Profile privat, wurden bereits gelöscht oder enthielten keine Tweets. Von den 86.792 Profilen konnten in Summe 144.116.436 Tweets extrahiert werden. Dies entspricht etwa 1.660 Tweets pro Profil. Von diesen 144 Millionen Tweets enthalten bei weitem nicht alle Geotags. Geotags sind lediglich in 3.633.433 Tweets enthalten, dies entspricht einem Anteil von etwa 2,52% und einem Durchschnitt von knapp 42 Tweets pro Profil. Da von den 86.792 Profilen allerdings nur 32.828 Profile überhaupt Geotags enthalten, ändert sich das Verhältnis auf über 110 Tweets mit Geotag pro Profil.

10.2. Schrittweises Vorgehen

Der Algorithmus wurde schrittweise entwickelt; entsprechend ist dieses Kapitel aufgebaut. Zunächst werden das allgemeine Vorgehen erläutert und Zwischenergebnisse präsentiert. Auf der Basis dieser Zwischenergebnisse erfolgt dann jeweils die Herleitung des nächsten Schrittes.

10.2.1. Analyse der Aktivitätszentren

Der erste Schritt, um sich einen ersten Überblick über den Datensatz und die typische Nutzung von Geotags zu verschaffen, war die Analyse des Datensatz im Hinblick auf Aktivitätszentren. Im

Kontext dieser Arbeit wird unter einem Aktivitätszentrum ein Ort mit gehäuften Geotags eines spezifischen Nutzers verstanden. Dies könnte beispielsweise der Arbeits- oder Wohnort sein, typischerweise ein Ort, wo dieser Nutzer relativ viel Zeit verbringt, kann aber auch deutlich weiter gefasst sein, beispielsweise die Stadt in der der Nutzer lebt und wo er an diversen Stellen Tweets mit Geotags verfasst hat.

Zur Analyse von Aktivitätszentren wurden für jeden Nutzer alle Tweets mit Geotags ausgewertet. Dabei wurde sowohl der Mittelpunkt aller Koordinaten berechnet als auch eine durchschnittliche Distanz zu diesem Mittelpunkt. Anhand der größten beobachteten Distanz zum Mittelpunkt wurde ein Radius eines Kreises ermittelt, der alle Geotags mit einschließt. Um Ausreißer, beispielsweise Urlaubsaufenthalte, filtern zu können, wurden im nächsten Schritt die Anzahl der Geotags stufenweise reduziert. Dies in der Art, dass stets die Geotags, die am weitesten vom Zentrum entfernt waren, für die weitere Auswertung außer Acht gelassen wurden. Es wurden daher schrittweise die Geotags reduziert, so dass die 1%, 2,5%, 5%, 10%, 15%, 20%, 25%, 30%, 40% und 50% der entferntesten Geotags entfallen sind. Anhand der Reduktionsschritte wären mindestens 200 Geotags pro Profil notwendig. Da sich die Anzahl der Profile mit dieser Anzahl an Geotags nur auf 5.234 beläuft, wurden Profile ab 5 Geotags zugelassen, auch unter Berücksichtigung, dass dort nicht bei jedem Schritt eine Reduktion stattfindet. Dies ist jedoch auch der Grund, warum keine noch größeren Reduktionsschritte als 50% durchgeführt wurden. Es sollte vermieden werden, dass Profile nur noch ein oder zwei Geotags im Rahmen der Auswertung aufweisen. Es wird davon ausgegangen, dass mindestens drei Geotags vorhanden sein sollten. Dies deckt sich auch mit den Ergebnissen aus [219], dort wurden die Geotags, wie in Abschnitt 5.6 erläutert, in die entsprechenden Postleitzahlen umgewandelt. Ab einer Menge von drei Postleitzahlen konnten bereits gute Matchingerfolge erzielt werden.

Um das vorgehen anschaulicher zu gestalten, wurde das prinzipielle Vorgehen in Abbildung 10.1 dargestellt. Gezeigt wird das schrittweise Entfernen einzelner Geotags und der damit einhergehenden Veränderung der Ausdehnung, als auch der Verschiebung des Zentrums. Dabei sind Geotags gelb, das Zentrum rot und der Radius grün gezeichnet.

Abbildung 10.1.: Darstellung des prinzipiellen Vorgehens bei der Analyse der Aktivitätszentren.

Ziel dieses Analyseschritts war die Ausdehnung der Aktivitätszentren zu ermitteln bzw. in welchem Radius typischerweise die Nutzung von sozialen Netzen stattfindet und damit auch,

wo sich der Nutzer normalerweise aufhält. Die entsprechenden Ergebnisse werden im nächsten Abschnitt näher beleuchtet.

Ergebnisse aus der Analyse der Zentren und Radien

In diesem Abschnitt werden die Zwischenergebnisse aus der Analyse der Aktivitätszentren vorgestellt und erläutert. Hierzu werden zunächst die Radien der Aktivitätszentren näher beleuchtet, um im Anschluss auf die durchschnittlichen Distanzen eingehen zu können.

Die nachfolgenden Diagramme sind folgendermaßen aufgebaut: Die y-Achse entspricht dem Radius bzw. der Distanz in km. Die x-Achse gibt Aufschluss darüber, wie viele Geotags noch betrachtet wurden. Diese errechnen sich also anhand der von 100% subtrahierten Reduktionsschritte, wie im vorherigen Abschnitt erläutert. Anhand der Farbcodierung ist ablesbar, wie viele Geotags zu einem Nutzer mindestens vorliegen. Die nachfolgende Tabelle 10.1 gibt Aufschluss darüber, wie viele Profile in den fünf Gruppen enthalten sind.

Tabelle 10.1.: Umfang der ausgewerteten Profile anhand der Anzahl der Geotags.

mind. # Geotags	# Profile
Alle (>= 5)	25.070
>= 25	16.640
>= 50	12.678
>= 100	8.861
>= 250	4.190

Das erste Diagramm, Abbildung 10.2, zeigt die durchschnittlichen Radien in Abhängigkeit der außer Acht gelassenen Geotags. Da die Geotags aussortiert werden, die am weitesten von den errechneten Zentren entfernt liegen, nehmen die Radien kontinuierlich ab. Im Gegensatz zu den weiteren Diagrammen ist hier zu beachten, dass die y-Achse eine logarithmische Skalierung aufweist. Ohne aussortierte Geotags, 100% auf der x-Achse, fällt auf, dass Nutzer, deren Geotaganteil sehr hoch ist, auch im Urlaub stärker davon Gebrauch machen. Dies ist daran erkennbar, dass die durchschnittlichen Radien mit der Anzahl der Geotags entsprechend der Farbcodierung stark zunimmt. Mit fortschreitender Reduktion gleichen sich die Radien jedoch nahezu an, hier sind nur noch geringfügige Abweichungen sichtbar.

Der Vollständigkeit halber sind in Abbildung 10.3 auch die errechneten Maximalwerte der Radien dargestellt, siehe Abbildung 10.3. Hier wird deutlich, dass an entfernten Orten meist nicht nur ein oder zwei Geotags abgesetzt werden. Dadurch ergibt sich eine stufenweise Reduktion des Radius, allerdings nur bei größeren Mengen nicht mit einbezogener Geotags.

Auf die Darstellung der Minimalwerte wurde verzichtet, da diverse Nutzer so nah beieinanderliegende Geotags genutzt haben, dass der Radius gleich Null oder zumindest nahezu Null ist. Dies wird in Tabelle 10.2 verdeutlicht. Aufgeführt ist jeweils die Anzahl an

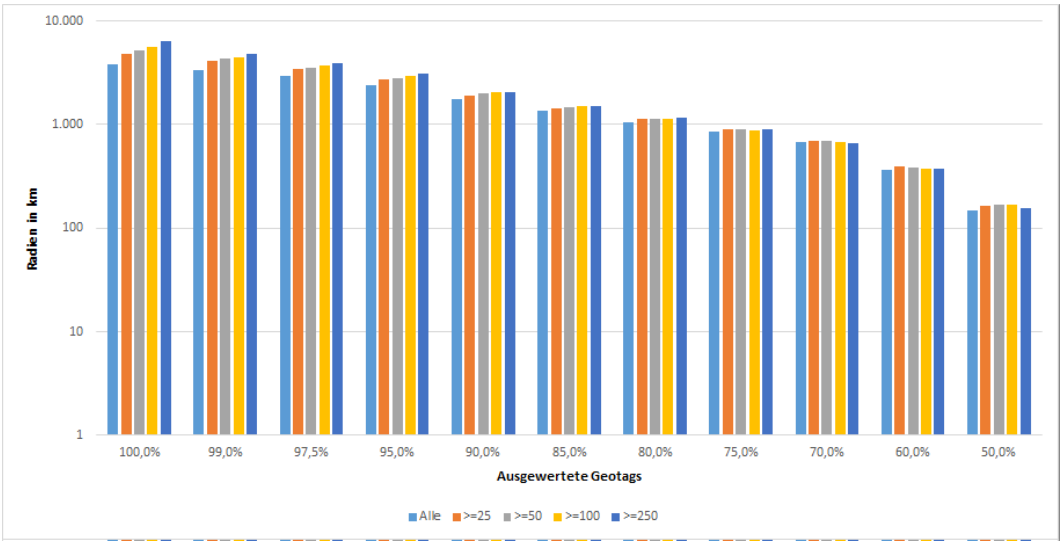


Abbildung 10.2.: Durchschnittswerte der berechneten Radien in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung.

Profilen, deren Radius Null oder kleiner gleich 0,001 ist; 0,001 entspricht dabei einem Meter. Dabei werden wie in den Diagrammen die fünf Häufigkeitskategorien unterschieden, um zu zeigen, dass dies nicht nur für Profile mit fünf Geotags beobachtet werden kann.

Tabelle 10.2.: Umfang der ausgewerteten Profile anhand der Anzahl der Geotags.

mind. # Geotags	# Radius <= 0,001	# Radius = 0.0
Alle (>= 5)	120	28
>= 25	25	1
>= 50	15	0
>= 100	9	0
>= 250	4	0

Ein ähnliches Bild wie für die Radien zeigt sich bei den durchschnittlichen Distanzen zwischen den Geotags. Abbildung 10.4 zeigt die Durchschnittswerte der durchschnittlichen Distanzen, die für jeden Nutzer berechnet wurden. Die Werte fallen dabei deutlich schneller ab, da der Einfluss der großen Distanzen durch die kontinuierliche Reduktion fortwährend abnimmt, für die Radiusberechnung jedoch nur eine verbleibende große Distanz bereits den Wert stark erhöht. Auch hier zeigt sich, dass zunächst mit größerer Anzahl an Geotags auch die durchschnittliche Distanz eine Größere ist. Dieser Effekt gleicht sich jedoch zu Beginn der Reduktion, bei etwa 95%, aus und dreht sich bereits bei 90% um. Dieses Verhältnis bleibt bis zur untersten Reduktionsstufe von 50% erhalten. Dort besitzen die Profile mit den meisten Geotags die geringsten durchschnittlichen Distanzen. Dies lässt vermuten, dass Vielnutzer von Geotags

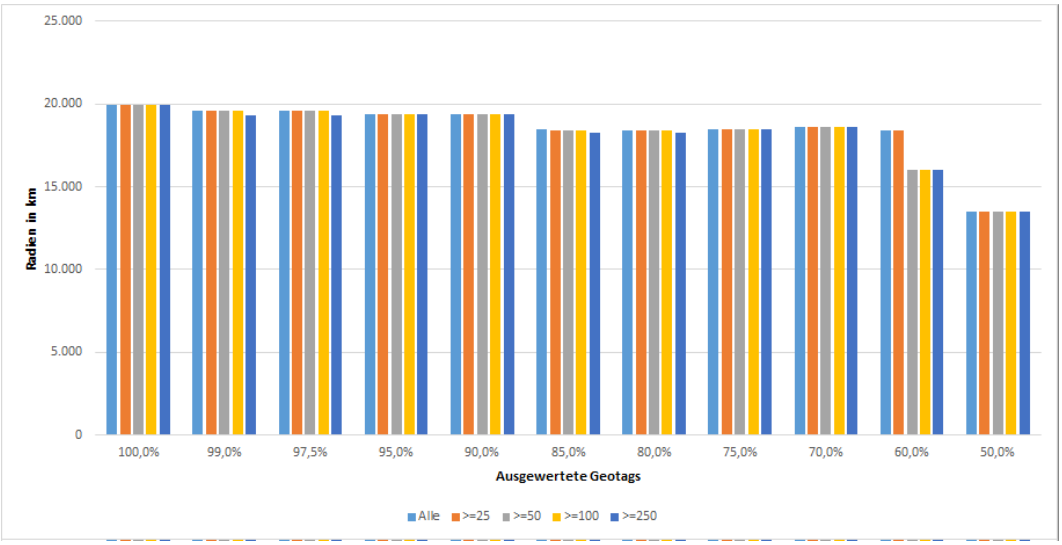


Abbildung 10.3.: Maximalwerte der berechneten Radien in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung.

tendenziell diese auch vermehrt an Orten nutzen, wo sie sich oft aufhalten, beispielsweise zuhause oder in der Arbeit. Wohingegen Nutzer, die nur spärlich Gebrauch von Geotags machen, dies wohl eher an besonderen Orten tun, zum Beispiel bei Sehenswürdigkeiten oder in einer Bar mit Freunden.

Betrachtet man die maximalen Werte der durchschnittlichen Distanzen, siehe Abbildung 10.5, ist das Bild ein anderes. Da hier jedoch immer nur ein Wert stellvertretend für die ganze Gruppe, kategorisiert nach Anzahl Geotags, steht, darf man diesen einen Maximalwert nicht überbewerten. Hier zeigt sich von Beginn an eine größere Distanz für die Gruppe mit nur mindestens fünf Geotags. Und das Verhältnis bleibt in etwa bis zum maximalen Reduktionsschritt bestehen. Bei nur noch 50% Geotags ist der Maximalwert der Nutzer mit mindestens 250 Geotags sogar weitaus geringer.

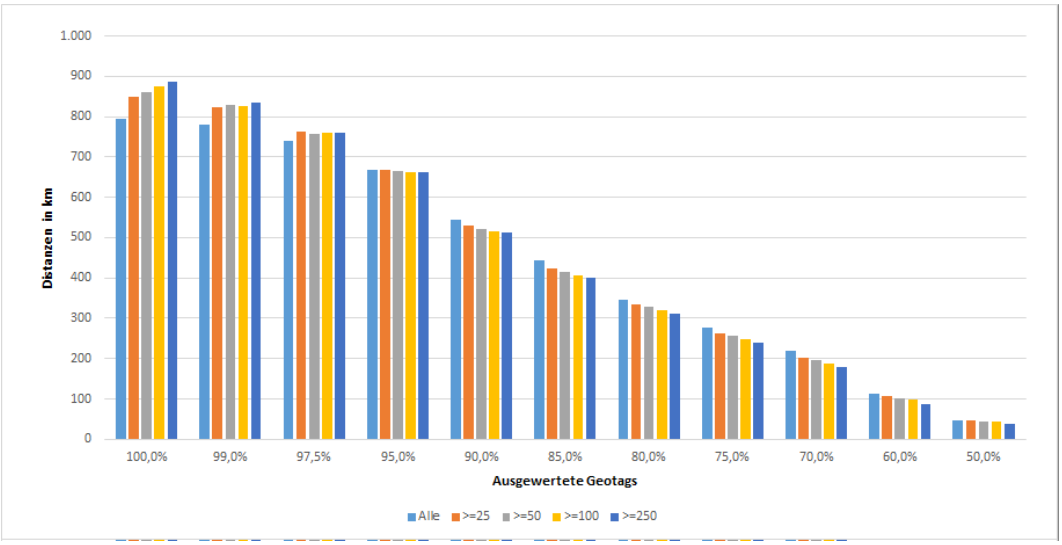


Abbildung 10.4.: Durchschnittswerte der berechneten Distanzen in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung.

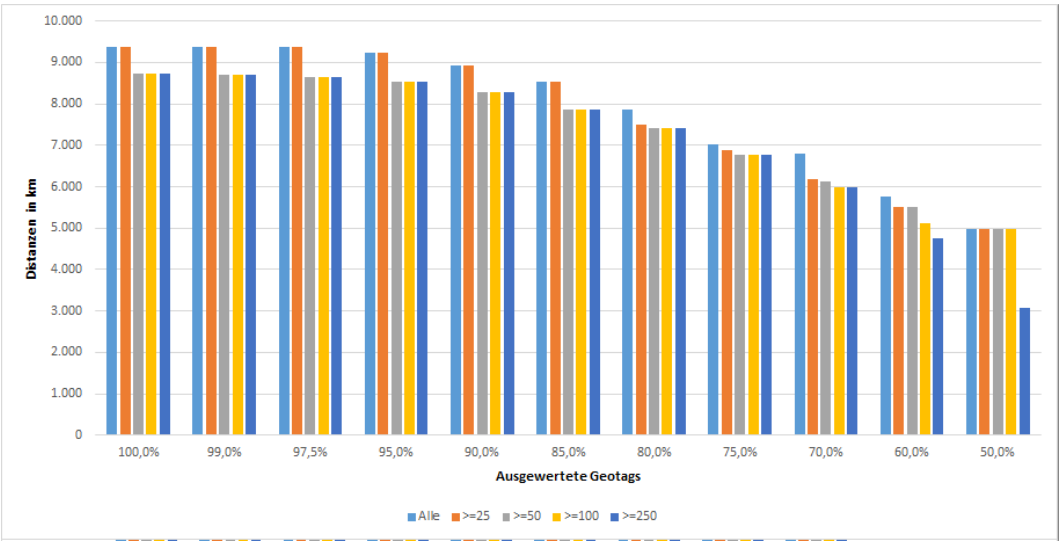


Abbildung 10.5.: Maximalwerte der berechneten Distanzen in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung.

Schlussfolgerungen

Nachfolgende Auflistung fasst die relevanten Schlussfolgerungen aus der Analyse der Aktivitätszentren für das weitere Vorgehen bzw. den weiteren Analysebedarf zusammen:

- Ein Reduktionsschritt ist essentiell notwendig und ermöglicht, die Geotags zu identifizieren, die dem Aktivitätszentrum des Nutzers am nächsten sind.
- Reduktionsschritte, die über 50% hinausgehen, wären wünschenswert, da davon auszugehen ist, dass so die Radien der Aktivitätszentren weiter eingeschränkt werden könnten. Dies kollidiert jedoch mit dem Ziel, dass drei Geotags nach der Reduktion verbleiben sollen und eine weitere Einschränkung der Profilmenge nicht erfolgen soll. Spätere Analysen werden ergeben, ob eine Reduktion um 50% ausreichend ist. Die durchschnittlichen Distanzen lassen dies jedoch erwarten, da beispielsweise 20 km zwischen Arbeits- und Wohnort heutzutage keine Seltenheit mehr darstellen.
- Dennoch sind für erfolgreiches Profilematching die entfernten Geotags miteinzubeziehen, da je weiter entfernt ein Geotag erstellt wurde, dies die Profilmenge mit vergleichbarem Aktivitätszentrum stark einschränkt.

10.2.2. Vergleich der Aktivitätszentren

Aufbauend auf den Analysen und Ergebnissen zu den Aktivitätszentren wurde im nächsten Schritt untersucht, wie nahe die Zentren der verschiedenen Nutzer beieinanderliegen. Hierzu wurden die 27.050 Profile jeweils gegen alle anderen verglichen und die jeweiligen Distanzen zwischen den Aktivitätszentren, für die bereits bekannten Reduktionsstufen (1%, 2,5%, 5%, 10%, 15%, 20%, 25%, 30%, 40% und 50%), analysiert und ausgewertet.

Das Vorgehen ist in Abbildung 10.6 dargestellt. Zu sehen ist wie der Abstand zweier Zentren zueinander ermittelt wird. Dabei sind Geotags gelb bzw. blau, die Zentren rot und die Radien grün gezeichnet. Um die Zentren den Geotags (gelb bzw. blau) zuordnen zu können, sind diese in der entsprechenden Farbe umrandet.

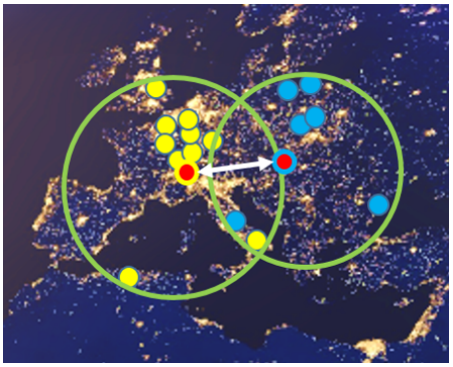


Abbildung 10.6.: Visualisierung des Vorgehens beim Vergleich der Aktivitätszentren.

Für 25.070 Profile ergeben sich so rechnerisch $\frac{1}{2} * 25.070 * (25.070 - 1) =$ 314.239.915 durchzuführende Vergleiche. Bei einem produktiven Einsatz lassen sich hier jedoch diverse Optimierungen implementieren, um diese Arbeitslast zu reduzieren. Dies ist auch erforderlich, da 25.070 noch eine vergleichsweise kleine Datenmenge ist, wenn man es mit den typischen Nutzerzahlen von sozialen Netzen vergleicht. Wenn man anhand der Zentren filtert und alles ausschließt, was beispielsweise 100km oder weniger entfernt liegt, lässt sich die Arbeitslast stark verringern.

Ergebnisse des Aktivitätszentrenvergleichs

Die erzielten Ergebnisse der vielen Vergleiche sind in Tabelle 10.3 gelistet. Hierbei gibt die Spalte eins Auskunft über die gefilterte Distanz und alle weiteren Spalten, entsprechend den Reduktionsstufen, der Anzahl berücksichtigter Geotags. Bedingt durch die hohe Zahl von Reduktionsstufen als auch von Distanzfiltern, ist es nicht möglich, die Tabelle vollständig nebeneinander darzustellen.

Tabelle 10.3.: Abstände der verglichenen Profile.

Distanz	100%	99%	97,50%	95%	90%	85%
>1000	91,605759%	91,595018%	91,558712%	91,486266%	91,333448%	91,178193%
<=1000	8,394241%	8,404982%	8,441288%	8,513734%	8,666552%	8,821807%
<=100	0,287902%	0,296118%	0,316043%	0,355676%	0,438904%	0,519521%
<=10	0,012585%	0,014010%	0,017970%	0,026173%	0,045271%	0,069589%
<=1	0,000289%	0,000339%	0,000443%	0,000683%	0,001352%	0,002447%
<=0.1	0,000015%	0,000015%	0,000016%	0,000016%	0,000025%	0,000047%
<=0.01	0,000009%	0,000009%	0,000009%	0,000010%	0,000013%	0,000021%
<=0.001	0,000009%	0,000009%	0,000009%	0,000010%	0,000013%	0,000020%

Distanz	80%	75%	70%	60%	50%
>1000	91,006653%	90,893525%	90,802624%	90,666789%	90,635899%
<=1000	8,993347%	9,106475%	9,197376%	9,333211%	9,364101%
<=100	0,597479%	0,668397%	0,725532%	0,847664%	0,941379%
<=10	0,101290%	0,130829%	0,163441%	0,228138%	0,291770%
<=1	0,004187%	0,006099%	0,008177%	0,014243%	0,021557%
<=0.1	0,000071%	0,000098%	0,000145%	0,000230%	0,000399%
<=0.01	0,000024%	0,000030%	0,000041%	0,000061%	0,000118%
<=0.001	0,000024%	0,000028%	0,000040%	0,000060%	0,000116%

Um die Ergebnisse aus Tabelle 10.3 besser veranschaulichen zu können, sind diese graphisch in Abbildung 10.7 aufbereitet. In der Abbildung sind die Zusammenhänge besser erkennbar, bedingt durch die logarithmische Skalierung der y-Achse, aber die Werte schlecht ablesbar. Das Diagramm zeigt die Ergebnisse der Tabelle, wobei die Reduktionsstufen auf der x-Achse

und die Prozentwerte auf der y-Achse angetragen sind. Durch die Farbcodierung werden die verschiedenen Distanzen der Profile zueinander visualisiert. Nimmt man nun zum Beispiel die unterste Linie, diese entspricht dem Anteil an Profilvergleichen, der einen Abstand von 0,001 Kilometer, also einem Meter oder darunter, ergeben hat. Die Linie steigt mit der fortschreitenden Reduktion von Geotags an. Grund hierfür ist, dass durch den Einfluss weit entfernter Geotags die Zentren erstmal weltweit verstreut sind; erst durch die Reduktionen nähern sie sich stark den bewohnten Zentren wie Großstädten an. Dies bedeutet, dass Profile von Personen, die nahe beieinander wohnen, auch erst als solche erkannt werden, wenn die Geotags aus den Fernreisen entfernt sind. Die Annäherung der Zentren an bewohnte Gebiete führt dazu, dass das eben beschriebene Verhalten zu einem Anstieg aller Linien mit Ausnahme der >1000 km Linie führt. Deren Anteil nimmt ab; diese Abnahme ist bedingt durch die logarithmische Skalierung, aber so gering, dass dies nur anhand der Tabelle erkennbar ist.

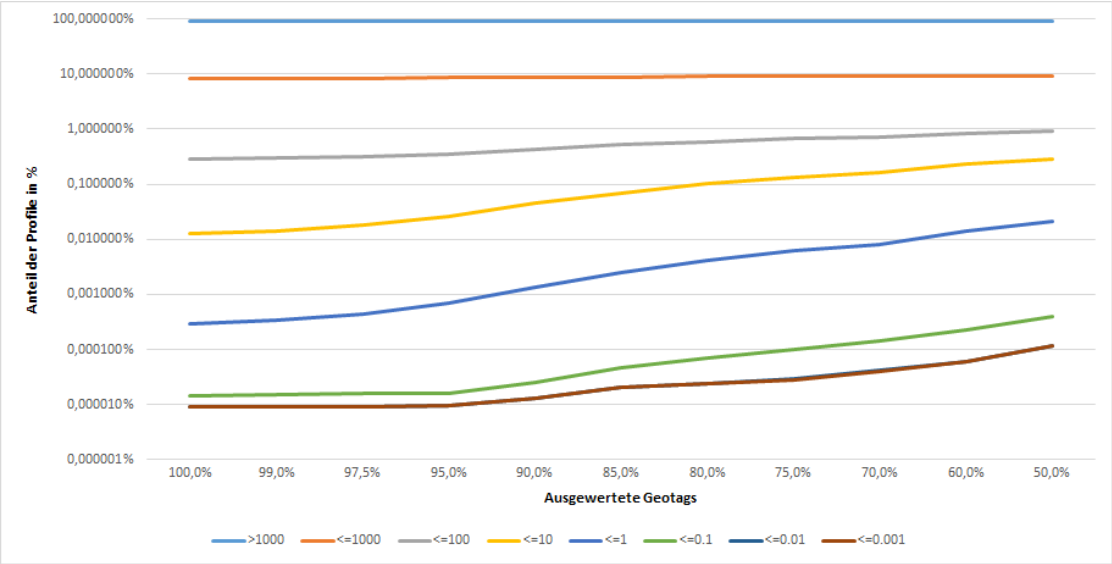


Abbildung 10.7.: Prozentsatz der Profile laut y-Achse mit den aufgeführten Abständen zueinander, siehe Farbcodierung laut Legende. X-Achse entspricht den bekannten Reduktionsstufen.

Um die Eignung dieses Vorgehens bewerten zu können, erfolgte eine manuelle Analyse der gefundenen Übereinstimmungen, welche für den Reduktionsschritt von 50% nur eine Distanz zwischen den Aktivitätszentren von 10 Metern oder weniger ergaben. Hierzu wurden die Profile zuerst entsprechend gruppiert, falls es in diesem Bereich mehrere Treffer gab. Tabelle 10.4 zeigt, wie häufig welche Gruppengröße aufgetreten ist. Da der Datensatz mit 25.070 Profilen vergleichsweise klein ist, war nicht zu erwarten, dass hierbei viele Übereinstimmungen gefunden werden. Daher ist es umso mehr überraschend, Gruppengrößen von bis zu 19 Profilen zu finden. Eine mögliche Erklärung ist, dass der Datensatz nicht die komplette Bandbreite typischer Nutzer abbildet. Da die Quelle der Profile der About.me Datensatz ist, sind dort nur Nutzer enthalten, die versiert im Umgang mit sozialen Netzen sind und diese zur

Selbstpräsentation oder zur Werbung für ihre Arbeit nutzen.

Tabelle 10.4.: Anzahl der Profile deren Aktivitätszentren eine Distanz von unter 10 Metern zueinander haben und wie oft dies vorkommt.

# Profile	# Vorkommen
2	45
3	6
4	4
5	2
6	1
7	2
9	1
19	1

Schlussfolgerungen

Nachfolgende Auflistung fasst die relevanten Schlussfolgerungen aus der Analyse der Vergleiche der Aktivitätszentren für das weitere Vorgehen bzw. den weiteren Analysebedarf zusammen:

- Eine Analyse auf Geotag-Ebene ist essentiell notwendig, da die Reduktion auf ein Aktivitätszentrum so stark von einzelnen Geotags, die weit entfernt z. B. im Urlaub generiert wurden, beeinflusst werden.

- Eine Einbeziehung von Aktivitätszentren eignet sich jedoch sehr gut als ersten Filterschritt. Haben beispielsweise die beiden Kreise zu vergleichender Profile, die sich aus den Aktivitätszentren und den Distanzen zum jeweiligen entferntesten Geotag ergeben, keine Schnittmenge, so kann davon ausgegangen werden, dass hierbei kein Match vorliegt bzw. mit einem Geo-basierten Verfahren kein Matching möglich ist. Daher können diese für eine weitere Analyse im Rahmen einer Profilzuordnung ausgeschlossen werden.

10.2.3. Vergleich auf Geotag-Ebene

Nachdem im vorangegangenen Schritt die Distanzen zwischen den Aktivitätszentren untersucht wurden, wird in diesem Schritt die Analyse auf Ebene der Geotags durchgeführt. Um für den zu entwickelnden Algorithmus auch eine Aussagekraft in dicht besiedelten Gebieten sicherzustellen, wird eine Methode eingesetzt, die im Rahmen dieser Arbeit als *virtuelle Datensätze* bezeichnet wird. Dies ist notwendig, da die Anzahl an Profilen mit ausreichender Menge an Geotags im verwendeten Datensatz hierfür nicht ausreichend ist. Die Profile aus 10.1 sind weltweit verteilt, aber entsprechende Nutzerzahlen können bereits in Kleinstädten erreicht werden. Daher ist es nötig eine vergleichbare Datenbasis zu schaffen. Die Funktionsweise der gewählten Methode wird in nachfolgendem Abschnitt im Detail betrachtet.

Erhöhung der Aussagekraft durch virtuelle Datensätze

Wie bereits erläutert, sind zur Prüfung eines Geo-basierten Profilematching Verfahrens Daten eines dicht besiedelten Gebietes heranzuziehen. Nur so kann sichergestellt werden, dass das Verfahren auch bei großen sozialen Netzen und der damit einhergehenden großen Anzahl an Nutzern funktionsfähig ist. Da entsprechende Datensätze nicht öffentlich zur Verfügung stehen und auch nur unter größtem Aufwand gecrawlt werden könnten, müssen diese synthetisch erzeugt werden.

Die einfachste Methode, Datensätze mit Geokoordinaten zu erzeugen, ist die Nutzung eines Zufallszahlengenerators. Dies führt jedoch unweigerlich zu zufälligen Anordnungen der Geotags und kann dadurch nicht einem vergleichbaren menschlichen Profil entsprechen. Ein menschliches Profil weist beispielsweise Häufungen der Koordinaten auf. Dies können der Wohn- oder Arbeitsort, ein Sportverein, eine Bar oder ein Restaurant sein. Diese Zusammenhänge lassen sich durch reine Zufallszahlen nicht abbilden.

Eine Alternative zu Zufallszahlen könnte sein, zufällig entsprechende Häufungspunkte zu generieren und die Koordinaten teilweise entsprechend dort anzusiedeln. Dies würde versuchen, vergleichbare Muster menschlicher Profile zu generieren, allerdings ohne die Sicherheit, dass dies tatsächlich menschlichem Verhalten entspricht. Zudem ist der Ansatz sehr aufwändig.

Im Rahmen dieser Arbeit wurde daher eine dritte Variante gewählt. Da der genutzte Datensatz zwar nicht ausreichend Profile enthält, diese jedoch von realen Nutzern stammen, wurden diese zur Darstellung von dichter Besiedelung herangezogen. Das Prinzip ist in Abbildung 10.8 verdeutlicht. Soll beispielsweise am Aktivitätszentrum *A*, der umliegenden gelben Punkte, eine Profilzuordnung evaluiert werden, so werden alle anderen Profile des Datensatzes dorthin transformiert. Es wird also von jedem Profil des Datensatzes das Aktivitätszentrum errechnet und dieses, im Beispiel Punkt *B*, auf das Aktivitätszentrum Punkt *A* transformiert. Auf diese Weise werden die Mittelpunkte der Aktivitäten von über 20.000 Profilen übereinander gelegt. Dieses Vorgehen wird im Rahmen dieser Arbeit als virtuelle Datensätze bezeichnet.

Auswertung auf Ebene der Geotags

Nachfolgend wird das Vorgehen bei der Auswertung bzw. Zuordnung auf Geotag-Ebene im Detail betrachtet. Dabei wurde auch die Zuordnung zweier Teilmengen eines Profils zueinander untersucht. Um hierfür ausreichend Geotags zu erhalten, wurden zunächst Profile ausgewählt, die mindestens 10 Geotags enthielten. Diese wurden für einen gegenseitigen Abgleich in zwei Teilmengen aufgeteilt. Um hierbei die Reproduzierbarkeit sicherstellen zu können, wurden die Geotags abwechselnd einer der beiden Mengen zugewiesen.

Jedes Profil wurde mit jedem anderen Profil auf Geotag-Ebene verglichen, lediglich für den Fall des Selbstabgleichs, erfolgte, wie beschrieben, die Aufteilung in zwei Teilmengen. Um hierbei eine dichte Besiedelung und die damit zusammenhängende Datenbasis zu simulieren,

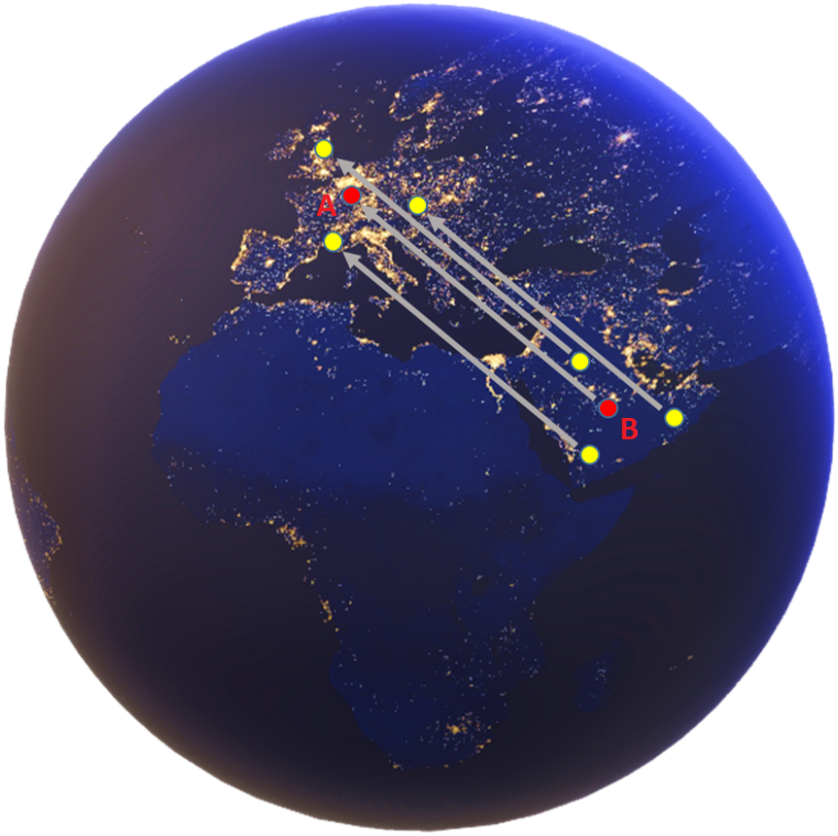


Abbildung 10.8.: Prinzip der virtuellen Datensätze.

kamen wie beschrieben virtuelle Datensätze zum Einsatz. Von allen Profilen besitzen 21.638 Profile mindestens 10 Geotags. Hierdurch ergibt sich eine virtuelle Datensatzgröße von 21638^2 Profilen, was theoretisch über 468 Millionen virtuellen Nutzern entspricht. Das Delta zwischen den Aktivitätszentren zweier zu vergleichender Profile wurde entsprechend auch beim Vergleich der Geotags untereinander berücksichtigt. Für den Vergleich wurde ein Profil ausgewählt und der Reihe nach für jedes Geotag mit allen Geotags des zu vergleichenden Profils die Distanz zwischen den beiden Geotags ermittelt. Der erhaltene Distanzwert wurde dann in folgende Intervalle kategorisiert. Distanz gleich null, Geotags sind also identisch; die folgenden Werte sind jeweils als obere Schranke des Intervalls zu verstehen, das Intervall entspricht also $\leq$ der nachfolgenden Werte: 1 m, 5 m, 10 m, 25 m, 50 m, 75 m, 100 m, 250 m, 500 m, 750 m, 1 km, 2,5 km, 5 km, 7,5 km, 10 km, 25 km, 50 km, 75 km, 100 km. Zur Vollständigkeit wurden zuletzt alle Vergleiche mit Distanzen $>$ 100 km erfasst.

Das Vorgehen beim Geotag-weisen Vergleich ist in Abbildung 10.9 dargestellt. Abgebildet ist der Vergleich aller blauen Geotags eines Nutzers mit drei exemplarischen Geotags des gelben

Nutzers. Dies erfolgt Schrittweise bis alle Geotags miteinander verglichen sind.

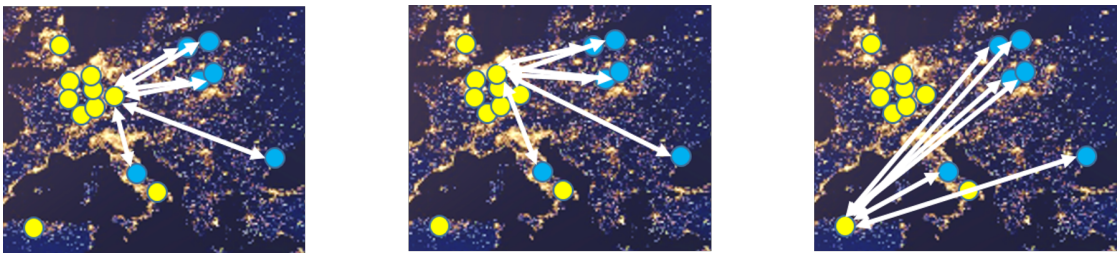


Abbildung 10.9.: Visualisierung des Vorgehens beim Vergleich der Geotags zweier Nutzer.

Nachdem alle Geotags miteinander verglichen und in die verschiedenen Intervalle einsortiert wurden, wurde eine Metrik benötigt, die die Vorkommen in den 21 Intervallen zu einem Messwert aggregieren kann. Hierbei sollte eine hohe Übereinstimmung durch einen möglichst kleinen, im Idealfall null, und geringe Übereinstimmung durch einen hohen Wert, nach oben offen, abgebildet werden. Dies erlaubt es zu prüfen, wie viele Vergleiche ggf. besser abgeschnitten haben. Dies erfolgt, indem nun der erzielte Wert eines Profilvergleichs mit sich selbst, also den beiden disjunkten Teilmengen, herangezogen und die Anzahl an Vergleichen ermittelt wird, deren Ergebnisse geringer ausgefallen sind. Zusätzlich wird auch ermittelt, wie häufig dieser Wert noch aufgetreten ist. Beispielsweise gibt es vielleicht keinen besseren Profilvergleich, aber zehn die den gleichen Wert aufweisen und damit als Kandidaten gleichwertig sind.

Auch hier wurde schrittweise vorgegangen. Es wurde nicht nur jeweils die Metrik auf alle 21 Intervalle zusammen angewandt, sondern mit aufsteigender Distanz. Es wurden also 21 Werte ermittelt, jeweils für dieses und die Intervalle mit geringerer Distanz, beispielsweise wird der Messwert für Intervall 16 aus den Intervallen 1 bis 16 gebildet.

Da im Vorfeld nicht bekannt war, welche Metrik gute Ergebnisse erzielen würde, wurden verschiedene Ansätze, A1 bis A4 kumulierend und A1 O bis A4 O nicht kumulierend, erprobt. Die Formeln der verwendeten Metriken, kumulierend oder nicht bezieht sich nur auf die Eingabeparameter, sind nachfolgend aufgeführt.

$$A1 = \sum_{i=0}^{x} \frac{Anzahl[i]}{\sum_{k=0}^{i} Anzahl[k]} * Raster[i] \tag{10.1}$$

$$A2 = \sum_{i=0}^{x} \frac{Anzahl[i]}{\sum_{k=0}^{i} Anzahl[k]} * \frac{1}{Raster[i]} \tag{10.2}$$

$$A3 = \sum_{i=0}^{x} \frac{Anzahl[i]}{\sum_{k=0}^{i} Anzahl[k]} * Raster[i] * k \tag{10.3}$$

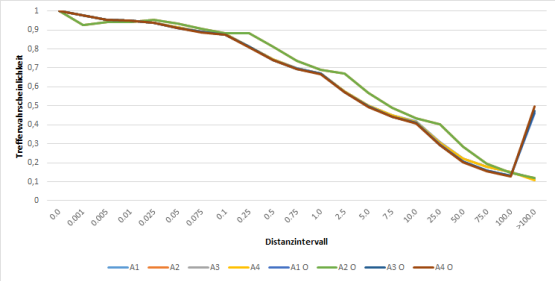
$$A4 = \sum_{i=0}^{x} \frac{Anzahl[i]}{\sum_{k=0}^{i} Anzahl[k]} * Raster[i]^2 \tag{10.4}$$

Die Metriken setzen sich zusammen aus einer Summe $\sum_{i=0}^{x}$ wobei x dem Intervallschritt entspricht für den die Metrik berechnet werden soll. Um bei dem kurzen Beispiel aus dem vorherigen Absatz zu bleiben, beispielsweise 16. $Anzahl[x]$ entspricht der ermittelten Übereinstimmungen für das Intervall x. Hier besteht auch der Unterschied zwischen kumulierend und nicht kumulierend. Bei kumulierend sind alle positiven Vergleiche unterhalb der oberen Intervallgrenze enthalten, bei nicht kumulierend nur die Anzahl zwischen oberer und unterer Intervallgrenze. Beispiel: $Anzahl[1]$ enthält 1 Treffer, $Anzahl[2]$ enthält 2 Treffer. $Anzahl[2]$ bei kumulierend entspricht dem Wert 3 (1+2), bei nicht kumulierend nur dem Wert 2. Die $\sum_{k=0}^{i} Anzahl[k]$ im Nenner setzt dabei die Treffer ins Verhältnis und sorgt für eine Werteverteilung des Bruches zwischen 0 und 1. $Raster[i]$ entspricht dabei jeweils der oberen Schranke des Intervalls [i] in km mit den Besonderheiten, dass für das erste Intervall, Grenze null, ein Wert von 0.0001 km (10cm) und für alle Distanzen größer 100 km pauschal mit 200 km gerechnet wurde. Dies ist erforderlich, um bei der Metrik A2 keine Division durch null zu erhalten bzw. alle Werte außerhalb der definierten Intervalle in die Berechnung miteinbeziehen zu können.

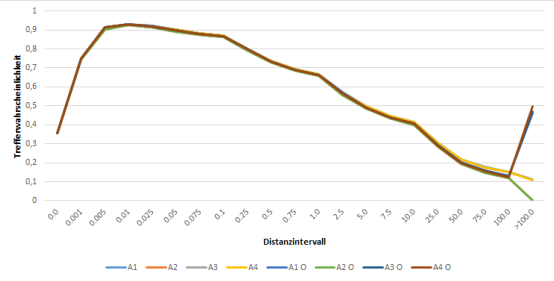
Ergebnisse der Geotag-weisen Auswertung

In den nachfolgenden Abschnitten erfolgt die Präsentation der Ergebnisse der Geotag-weisen Auswertung. Hierzu wurden die im vorherigen Abschnitt erläuterten Metriken herangezogen. Zusätzlich wurde zum einen für den Gesamtdatensatz eine Auswertung und zum anderen für die Intervalle mit <25, ≥25, ≥50, ≥100 und ≥250 Geotags durchgeführt. Gemäß der Anforderung 12, siehe Abschnitt 4.1.6, wurde definiert, dass der korrekte Treffer in der Top-10-Trefferliste enthalten sein muss. Daher wurde die Auswertung für Top-1, Top-3 und Top-10 Treffer durchgeführt und dies zusätzlich auch unter Berücksichtigung gleich bewerteter Profile. Beispielsweise ist der kleinste Wert bei der Auswertung ein Top-1-Treffer, existieren aber noch 10 andere Profile mit dem gleichen Wert, so schafft es dieses Profil gerade nicht in die Top-10-Trefferliste inklusive gleich Bewerteter, da 11 Profile identisch bewertet sind.

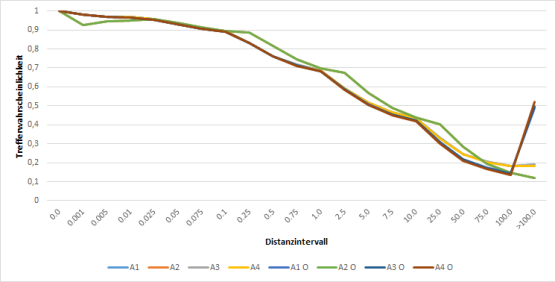
Die Diagramme in Abbildung 10.10 zeigen die Auswertung für den Gesamtdatensatz. Hierbei enthält die linke Spalte die Top-1, Top-3 und Top-10-Trefferlisten, wohingegen die rechte Spalte die jeweilige Trefferliste inklusive der Berücksichtigung identisch bewerteter Profile zeigt. Ohne die Berücksichtigung identisch bewerteter Profile ist die Trefferquote bei der



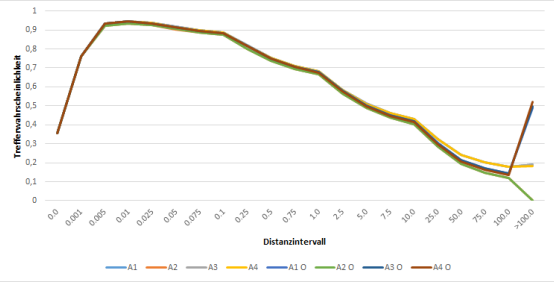
(a)



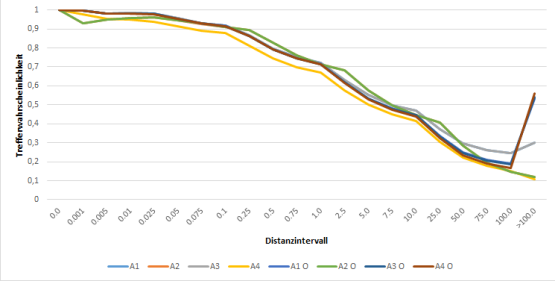
(b)



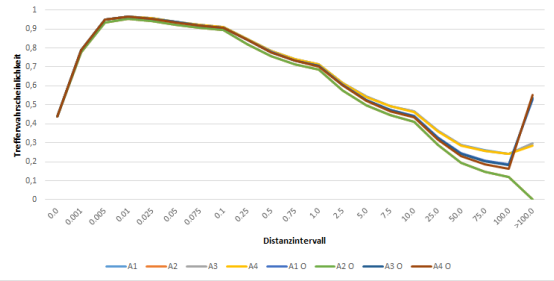
(c)



(d)



(e)



(f)

Abbildung 10.10.: Ergebnisse der Geotag-weisen Auswertung für den Gesamtdatensatz. a), b) und c) zeigen die Ergebnisse für die Top-1, Top-3 und Top-10-Trefferliste, wohingegen b), d) und e) jeweils die Trefferlisten inklusive identisch bewerteter Profile zeigen.

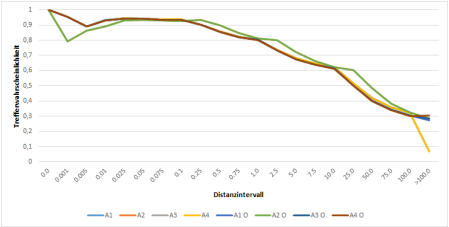
Auswertung für die ersten Intervalle nahe eins und fällt dann erst ab. Hintergrund ist, dass für die ersten Intervalle nur wenige Profile Geotag-Vergleiche in diesem Distanzbereich aufweisen. Insbesondere Geotags innerhalb eines Profils sind hierbei jedoch häufig vertreten, so dass insbesondere die geteilten Profile wieder korrekt einander zugeordnet werden. Zum Vergleich dazu fallen beim Blick auf die Diagramme mit Berücksichtigung identischer Bewertungen für die ersten Intervalle nur mittelmäßige Ergebnisse auf. Grund hierfür ist, dass aufgrund der geringen Anzahl von Treffern in diesen Intervallen viele Profile die gleiche Anzahl an Treffern aufweisen, häufig eins, wodurch es zu identischen Bewertungen kommt. Falls davon mehr als neun weitere Profile existieren, fällt diese Bewertung aus allen, einschließlich der Top-10-Trefferliste mit der Berücksichtigung identisch bewerteter, heraus.

Insgesamt lässt sich sagen, dass die Trefferwahrscheinlichkeit mit der Anzahl berücksichtigter Intervalle abfällt. Die Kurvenverläufe für die Top-1, Top-3 und Top-10-Trefferlisten-Diagramme unterscheiden sich nur geringfügig. Zu sehen ist eine leichte Verschiebung auf der y-Achse um wenige Prozent hin zu leicht steigender Trefferwahrscheinlichkeit. Das leichte Sägezahnmuster der Kurven ist auf die Staffelung der Distanzintervalle zurückzuführen.

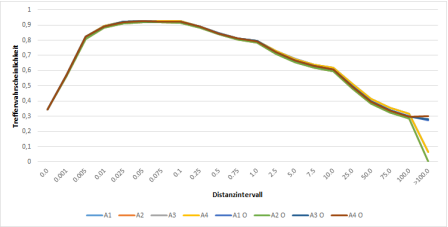
Bei der genaueren Analyse der Diagramme fällt auf, dass sich die verschiedenen Metriken nur geringfügig in der Trefferwahrscheinlichkeit unterscheiden. Die nicht kumulierenden Metriken machen erst beim letzten Intervallschritt einen Unterschied, dem Schritt in dem alle Vergleiche gezählt wurden, die über 100 km voneinander entfernt waren. Dadurch erfolgt ein Sprung von nur ungefähr 15% auf über 50% Trefferquote.

Zu erwähnen ist noch, dass besonders Metrik A2 auffällig ist. Durch ihre Formel erfolgt im Gegensatz zu den anderen Metriken eine Abschwächung statt einer stärkeren Gewichtung der Intervalle für sehr nahe Entfernungen. Dies führt zum einen dazu, dass diese Metrik bei den ersten Intervallen schlechtere Ergebnisse als die sonstigen Metriken erzielt, im Mittelfeld geringfügig besser als die sonstigen Metriken und am Ende wieder schlechter abschneidet. Die drei anderen Metriken (A1, A3 und A4) weichen nur geringfügig voneinander ab. So geringfügig, dass aufgrund der Reihenfolge der Darstellung der Linien der Verlauf der Metriken A1 und A1 O vollständig von den Linien der anderen Metriken verdeckt wird.

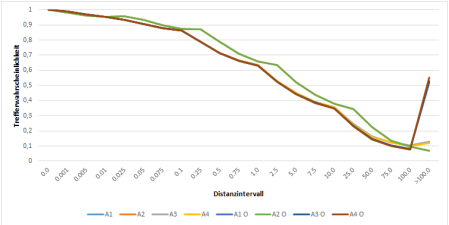
Neben den Untersuchungen für den gesamten Datensatz, erfolgte die Analyse für die Profile gemäß den Intervallen mit <25, ≥25, ≥50, ≥100 und ≥250 Geotags. Die Ergebnisse der Top-1-Trefferliste (links) und der Top-1-Trefferliste einschließlich identisch bewerteter Profile (rechts) ist in Abbildung 10.11 dargestellt. Dabei lässt sich feststellen, dass die Diagramme der Top-1-Trefferliste mit zunehmender Anzahl an Geotags eine schlechtere Trefferwahrscheinlichkeit aufweisen. Erst unter Einbeziehung des letzten Distanzintervalls springt die Trefferquote von teilweise nahe Null nach oben. Dabei werden beispielsweise für Profile mit mehr als 250 Geotags dann abhängig von der Metrik Trefferquoten von bis zu 67 % erzielt. Bei den Diagrammen für Profile mit mehr als 250 Geotags ist darüber hinaus zu beachten, dass die Trefferquote für das erste Distanzintervall null beträgt, da für keines der Profile eine so geringe Abweichung beim Geotag Vergleich beobachtet wurde.



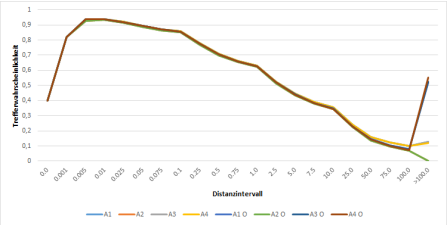
(a)



(b)

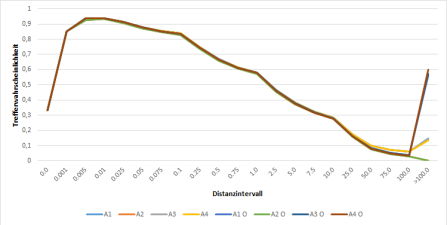


(c)

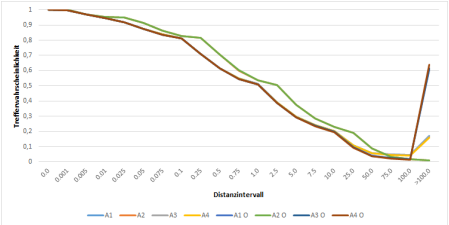


(d)

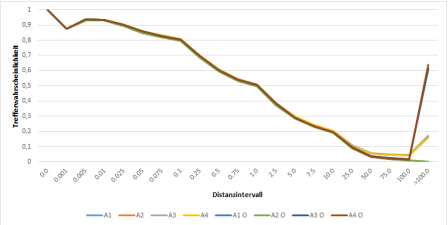
(e)



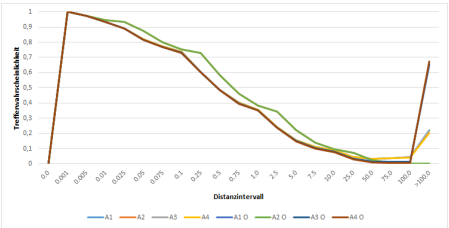
(f)



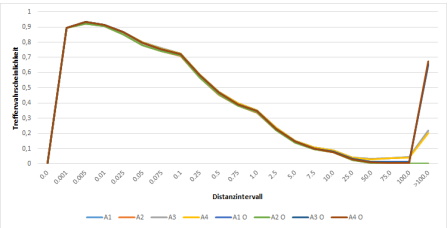
(g)



(h)

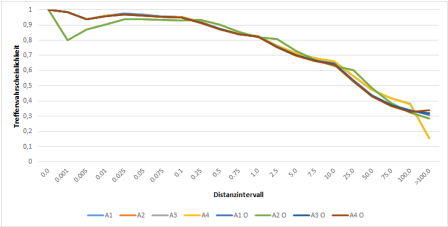


(i)

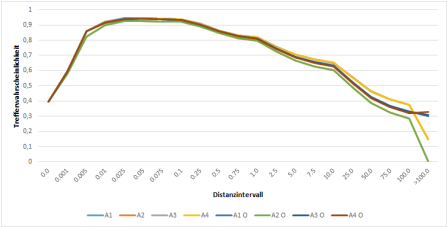


(j)

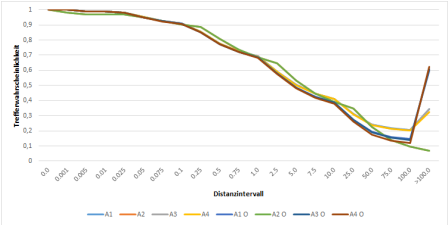
Abbildung 10.11.: Ergebnisse der Geotag-weisen Auswertung für Profile mit weniger als 25 (a+b) mind. 25 (c+d), 50 (e+f), 100 (g+h) und 250 (i+j) Profilen und einem genauen Treffer (links) und ohne gleich bewertete Treffer (rechts).



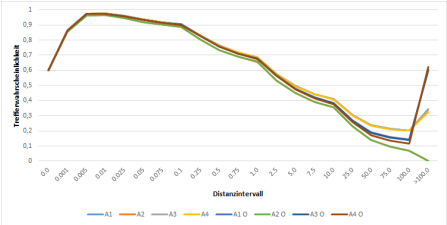
(a)



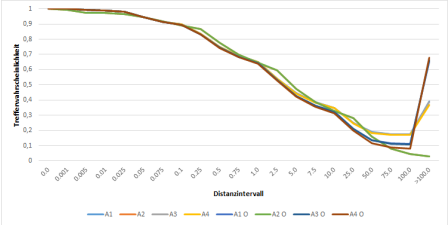
(b)



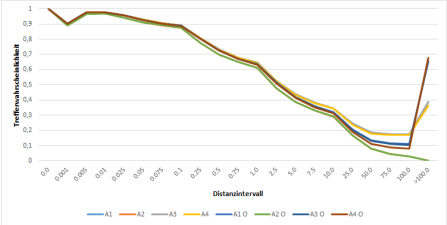
(c)



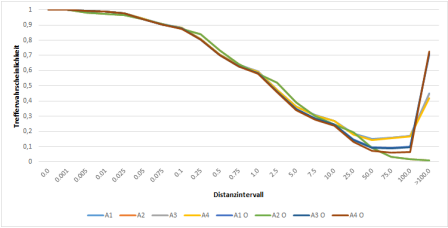
(d)



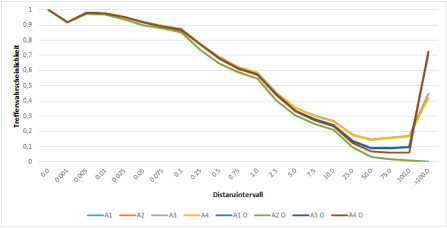
(e)



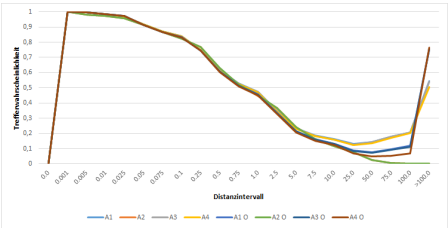
(f)



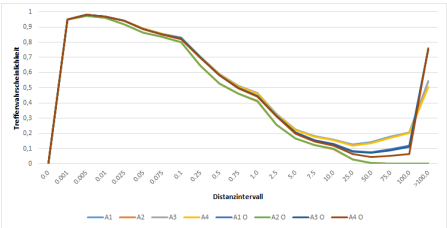
(g)



(h)



(i)



(j)

Abbildung 10.12.: Ergebnisse der Geotag-weisen Auswertung für Profile mit weniger als 25 (a+b) mind. 25 (c+d), 50 (e+f), 100 (g+h) und 250 (i+j) Profilen und Treffer unter den Top Zehn (links) und inklusive gleich bewerteter Treffer (rechts).

Die Diagramme aus 10.11 für die Top-1-Trefferliste inklusive gleich bewerteter Profile sieht den Diagrammen auf der linken Seite sehr ähnlich, der Unterschied findet sich insbesondere bei den ersten Distanzintervallen. Aufgrund der geringen Anzahl von Treffern für die geringen Distanzen, kommt es hier häufig zu mehreren gleich bewerteten Treffern. Beispielsweise erhalten für das erste Distanzintervall alle Profile mit nur einem Treffer in diesem Intervall die gleiche Bewertung und wenn dies mehr als eines ist, fallen diese alle aus der Wertung. Dies führt dann mitunter zu Kurven, die bei nur 30%-40% beginnen. Lediglich bei der Kurve für Profile mit mehr als 100 Geotags ist dies nicht zu beobachten, da es nur ein Profil in dieser Kategorie gibt, bei dem ein Treffer in diesem Distanzintervall aufgetreten ist.

Da gemäß Anforderung 12, siehe Abschnitt 4.1.6, ein Match so definiert wurde, dass der Treffer in der Top-10-Trefferliste enthalten sein muss, wird der Fokus auf die Top-10-Trefferlisten gesetzt. Diese sind in den Diagrammen der 10.12 zu sehen. Auf die Betrachtung der Top-3-Trefferlisten wird daher an dieser Stelle verzichtet, die Diagramme sind der Vollständigkeit halber aber im Anhang unter A.2.2 enthalten.

Die Kurvenverläufe sind nahezu identisch mit dem Top-1-Trefferlisten, unabhängig von der Betrachtung gleich bewerteter. Es erfolgt lediglich ein leichter Shift hin zu etwas besseren Trefferwahrscheinlichkeiten. Zudem erfolgt eine stärkere Separierung der Kurven der verschiedenen Metriken untereinander.

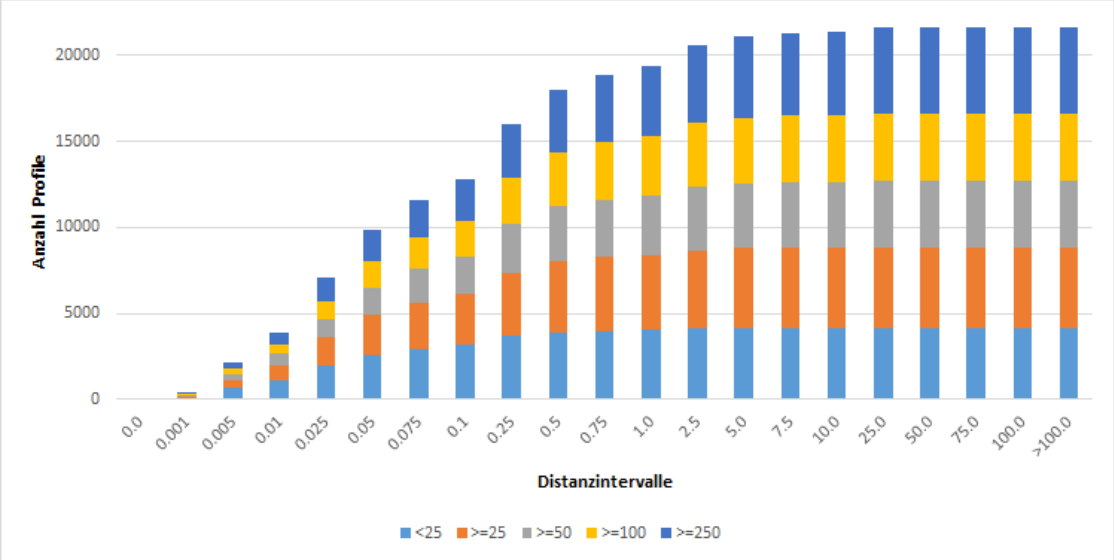


Abbildung 10.13.: Anzahl der Profile anhand derer eine korrekte Zuordnung geprüft werden konnte.

Die bisher vorgestellten Diagramme werden durch die Anzahl der Profile mit einem Treffer im entsprechenden Distanzintervall relativiert. Da beispielsweise für das erste Distanzintervall nur für Profilvergleiche, die dort mindestens einen Treffer hatten, geprüft werden kann, ob

eine korrekte Profilzuordnung erfolgt ist, ist die Profilmenge dort relativ gering. Dies führt indirekt zu vergleichsweise hohen Trefferquoten für die ersten Distanzintervalle, was leicht an den abfallenden Kurven für die steigenden Distanzintervalle nachvollzogen werden kann. Um daher die Trefferquoten korrekt bewerten zu können, müssen diese mit den Profilhäufigkeiten verglichen werden. Die Profilhäufigkeiten sind, farblich markiert nach den Intervallen der Anzahl an Geotags, in Abbildung 10.13 dargestellt. Um die Legende schlank halten zu können, ist hinsichtlich Anzahl an Geotags nur die untere Schranke als Text enthalten, ggf. ist als obere Schranke das nächste Intervall anzunehmen. Beispiel: Intervall ≥100, enthält alle Profile die 100 bis einschließlich 249 Geotags enthalten.

Tabelle 10.5.: Zusammenfassung der Trefferwahrscheinlichkeiten für die Top-10 inklusive identisch bewerteter Profile

Metrik	**Trefferwahrscheinlichkeit**					
	<25	**≥25 < 50**	**≥50 < 100**	**≥100 < 250**	**≥250**	**≥Alle**
A1	14,6%	34,4%	38,9%	44,8%	54,4%	29,8%
A2	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
A3	14,6%	34,1%	38,6%	44,5%	53,9%	29,6%
A4	14,6%	32,4%	36,5%	41,8%	50,6%	28,3%
A1 O	30,3%	59,8%	65,4%	70,6%	75,2%	53,0%
A2 O	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
A3 O	30,9%	60,4%	66,0%	71,2%	75,5%	53,6%
A4 O	32,7%	62,2%	67,8%	72,6%	76,2%	55,4%

Tabelle 10.6.: Zusammenfassung der Trefferwahrscheinlichkeiten für die Top-10 exklusive identisch bewerteter Profile

Metrik	**Trefferwahrscheinlichkeit**					
	<25	**≥25 < 50**	**≥50 < 100**	**≥100 < 250**	**≥250**	**≥Alle**
A1	15,6%	34,5%	39,0%	44,9%	54,5%	30,2%
A2	28,3%	6,9%	2,8%	0,8%	0,1%	11,8%
A3	15,6%	34,3%	38,7%	44,6%	54,0%	30,0%
A4	15,6%	32,6%	36,6%	41,9%	50,6%	10,9%
A1 O	30,8%	59,9%	65,4%	70,6%	75,2%	53,2%
A2 O	28,3%	6,9%	2,8%	0,8%	0,1%	11,8%
A3 O	32,1%	60,6%	66,1%	71,3%	75,6%	54,0%
A4 O	33,8%	62,4%	67,9%	72,7%	76,3%	55,8%

Auch wenn nun die hohen Trefferwahrscheinlichkeiten für die ersten Distanzintervalle in einem anderen Licht erscheinen, so ist auf die Gesamtmenge der Distanzintervalle eine erreichte Genauigkeit von über 50% für einen Top-10-Treffer unter Berücksichtigung identisch bewerteter Profile ein sehr gutes Ergebnis. Die Trefferwahrscheinlichkeiten sind der Übersichtlichkeit halber

in Tabelle 10.5 zusammenfasst. Metrik A2 besitzt die Eigenart, dass viele Profile identisch bewertet werden. Dies führt dazu, dass die Trefferwahrscheinlichkeit 0,0% beträgt, da stets mehr als zehn identisch bewerteter Profile vorhanden sind.

Um dies zu verdeutlichen, zeigt Tabelle 10.6 die Trefferwahrscheinlichkeiten für die Top-10-Trefferliste ohne Berücksichtigung identisch bewerteter Profile. Hierin zeigt sich auch der Umstand für Metrik A2, dass zwar Profile für die Top-10-Trefferliste korrekt zugeordnet werden, diese aber dann unter Berücksichtigung der identisch bewerteten Profile entfallen. Zu beachten ist an dieser Stelle, dass entgegen dem Trend für die anderen drei Metriken, die Trefferwahrscheinlichkeit mit der Anzahl an Geotags abnimmt.

Schlussfolgerungen

Aus den Ergebnissen des vorangegangenen Abschnitts lassen sich die folgenden Schlüsse ziehen:

- Es konnte gezeigt werden, dass eine Profilzuordnung anhand von Geotags auch ohne Rückgriff auf Raster, Postleitzahlen oder vergleichbares mitunter sehr erfolgreich umsetzbar ist.
- Das eingesetzte Verfahren der virtuellen Datensätze simuliert für jedes Profil eine vergleichsweise hohe Anzahl weiterer Profile mit gleichem Aktivitätszentrum. Dies lässt sich in etwa mit einer Großstadt gleichsetzen. Da nicht jeder Ort so stark besiedelt ist, kann für reale Datensätze sogar noch mit einer Verbesserung der Trefferwahrscheinlichkeiten gerechnet werden.

10.3. Zusammenfassung

In diesem Kapitel wurde durch schrittweises Vorgehen ein Verfahren zur Profilzuordnung anhand von Geotags entwickelt. Zuerst wurden hierzu die Aktivitätszentren und die Ausbreitung der Geotags untersucht. Im nächsten Schritt erfolgte ein Abgleich der Distanzen zwischen den Aktivitätszentren. Um für den finalen Analyseschritt ein dicht besiedeltes Gebiet zu simulieren, wurde das Verfahren der virtuellen Datensätze entwickelt. Dabei wurden alle Profile hinsichtlich ihrer Aktivitätszentren jeweils an einen gemeinsamen Ort verschoben. Dies entspricht theoretisch einem Datensatz von circa 468 Million Profilen.

Im letzten Schritt wurden die mit den Aktivitätszentren verschobenen Geotags miteinander verglichen. Dabei wurde stets der Datensatz des zu matchenden Profils geteilt und eine korrekte Zuordnung geprüft. Dabei konnten gute Ergebnisse jenseits der 50% erzielt werden.

KAPITEL 11

Gewichtung und Aggregation der Verfahren

In diesem Kapitel werden die Erkenntnisse hinsichtlich einer möglichen Gewichtung und Aggregation der vorgestellten Profilzuordnungsverfahren vorgestellt und gegenüber den ursprünglichen Anforderungen aus 4 abgegrenzt.

11.1. Aggregation der Teilergebnisse

Gemäß Anforderung 11 aus Kapitel 4 sollen nicht nur Einzelbetrachtungen durchgeführt werden, sondern diese auch auf gewinnbringende Kombinationsmöglichkeiten hin überprüft werden. Eine mögliche Aggregation der Ergebnisse ist stark von der Aussagekraft der einzelnen Verfahren abhängig. Daher erfolgt nachfolgend eine kurze Zusammenstellung zur Gültigkeit der Ergebnisse der vorgestellten Verfahren:

- **Zeitverhalten**: Vorhersagbarkeit zumindest mit einfachen Verfahren quasi nicht existent. Damit ist die Eignung der Ergebnisse für eine Aggregation mit anderen Verfahren nicht gegeben. Die Aussagekraft ist so gering, dass dadurch die Fehlerrate eines aggregierten Ergebnisses nur ansteigen und damit die Nutzung keinen Mehrwert generieren würde. Daher kommt das Verfahren für eine Aggregation nicht infrage.

- **Zeitdifferenz**: Das Zeitdifferenz-Verfahren hingegen liefert abhängig vom zu wählenden Grenzwert eine fast 100 prozentige Trefferquote mit einer quasi nicht existenten Falsch-Positiv-Rate. Kann das Verfahren angewendet werden, also werden URLs eines anderen sozialen Netzes automatisiert versendet, so ist keine Aggregation nötig, die Aussagekraft des Verfahrens kann nicht noch weiter verbessert werden. Für Fälle in denen diese Bedingung nicht erfüllt ist, ist die Aussagekraft entsprechend Null, wodurch dann keine Verbesserung der Trefferquote hinsichtlich einer Aggregation zu erzielen wäre. Daher kommt auch für dieses Verfahren eine Aggregation nicht infrage.

- **Positionsabgleich**: Das einzige Verfahren, das eine Trefferwahrscheinlichkeit bzw. eine Trefferliste mit absteigender Trefferwahrscheinlichkeit zurückliefert ist der Positionsabgleich. Aufgrund von Trefferwahrscheinlichkeiten von circa 50% würde dieses Verfahren auch als einziges stark von einer Aggregation profitieren. Angesichts der Eigenarten der beiden anderen Verfahren, kann diese jedoch nicht stattfinden.

Im Ergebnis ist eine Aggregation der Verfahren, entgegen der ursprünglich definierten Anforderung, so nicht sinnvoll möglich. Stattdessen ist eine Auswahl der Verfahren abhängig von den Eigenschaften der vorliegenden Daten zielführender. Hierzu bietet sich ein einfacher Entscheidungsbaum, in Abhängigkeit der verfügbaren Metadaten, an.

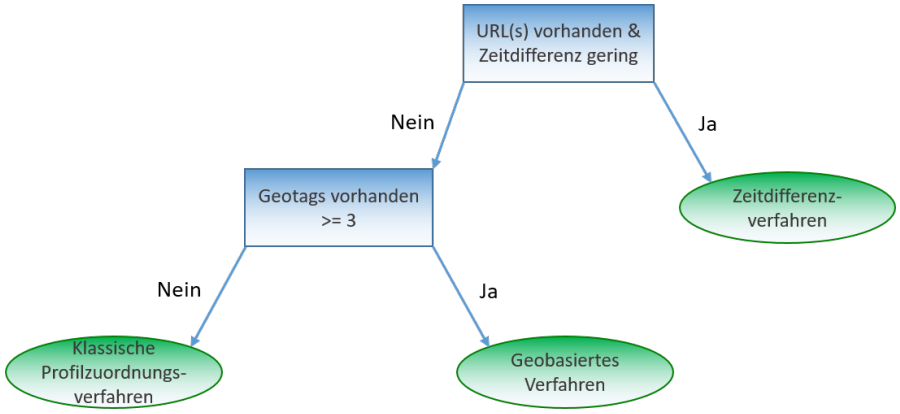


Abbildung 11.1.: Entscheidungsbaum für die Auswahl eines Profilzuordnungsverfahrens

Abbildung 11.1 zeigt den Entscheidungsbaum für die Auswahl der in dieser Arbeit untersuchten Verfahren. Ist die Auswahl nicht erfolgreich, weil die Bedingungen nicht erfüllt sind, so müsste auf klassische Profilzuordnungsverfahren, wie sie im Kapitel 5 vorgestellt wurden, zurückgegriffen werden. Zunächst wird aber geprüft, ob das Zeitdifferenzverfahren eingesetzt werden kann, falls nicht, wird die Nutzung des Geo-basierten Verfahrens geprüft. Und nur wenn dieses auch nicht eingesetzt werden kann, kommt die Rückfalloption zum Einsatz. Rückfalloption deshalb, da die klassischen Profilzuordnungsverfahren nicht Gegenstand dieser Arbeit sind.

11.2. Ermittlung der Gewichtung

Um eine Gewichtung der Ergebnisse vornehmen zu können ist Grundvoraussetzung, dass diese aggregiert werden können. Da aber, wie im vorherigen Abschnitt erläutert, keine Aggregation durchgeführt werden kann, muss auch auf eine Gewichtung der Ergebnisse verzichtet werden.

11.3. Zusammenfassung

Die Charakteristika der entwickelten Profilzuordnungsverfahren unterscheiden sich derart voneinander, dass die ursprünglich vorgesehenen Schritte der Aggregation und Gewichtung in dieser Form nicht durchgeführt werden können. Stattdessen wurde ein Entscheidungsbaum konstruiert, der anhand entsprechender Kriterien die Auswahl der Verfahren vornimmt.

KAPITEL 12

Schutzmaßnahmen gegen Profilzuordnung

Nachdem in den vorangegangenen Kapiteln Verfahren der Profilzuordnung diskutiert wurden, werden in diesem Kapitel Empfehlungen gegeben, eine entsprechende Profilzuordnung zu verhindern. Dieser und vergleichbare Aspekte die Privatsphäre betreffend wurden bereits umfangreich in der Literatur, und diese im Abschnitt 5.4, beleuchtet. Die folgenden Ausführungen mögen teilweise bereits in der in Abschnitt 5.4 zitierten Literatur so oder ähnlich erwähnt worden sein, basieren an dieser Stelle aber einzig und allein auf den Erkenntnissen aus dieser Arbeit. Dabei wird unterschieden zwischen Maßnahmen, die eine Zeit-basierte, und Maßnahmen, die eine Geo-basierte Zuordnung ermöglichen.

12.1. Zeit-basierte Schutzmaßnahmen

Wie in den Kapiteln 8 und 9 gezeigt, schwankt die Qualität der Ergebnisse im Hinblick auf eine mögliche Profilzuordnung sehr stark in Abhängigkeit des Verfahrens und dem Verhalten eines Nutzers.

12.1.1. Schutzmaßnahmen im Hinblick auf das Nutzungsverhalten

Wie gezeigt wurde, ist es nicht ohne weiteres möglich, das Nutzungsverhalten für eine Profilzuordnung zu instrumentalisieren. Insbesondere für Nutzer mit wenigen Interaktionen mit einem sozialen Netz am Tag zeigen die Verfahren sehr überschaubare Ergebnisse. Von daher ist an dieser Stelle keine grundlegende Maßnahme oder Verhaltensänderung notwendig. Anders mag es aussehen, wenn die Interaktionen immer zur gleichen Zeit stattfinden sollten, beispielsweise weil man sich dann in einer Pause befindet, dann wird die Menge zu betrachtender Daten und Nutzer stark eingeschränkt, wodurch ein entsprechender Zuordnungsversuch als weitaus erfolgversprechender anzusehen ist.

Liegt ein stark vorhersehbares Verhalten vor, so sollten gewisse Maßnahmen umgesetzt werden. Ein sich wiederholendes Ereignis, (fast) immer zur gleichen Uhrzeit, ragt in diesem Fall dann doch aus der Masse heraus und könnte gegebenenfalls auch durch Outlier-Detektion-Verfahren erkannt werden. Auch die Interpretation eines extrem ausgeprägten vorhersagbaren

Verhaltens als Bot, entweder durch das soziale Netz selbst oder durch eine externe Instanz, ist denkbar. Um dem entgegenzuwirken, bieten manche Apps eine Funktion zum zeitversetztem Senden an. Als Beispiel sei hier auf eine Twitter-eigene App namens TweetDeck verwiesen, siehe hierzu [347]. Darin kann ein Tweet verfasst und ein beliebiges Datum und eine beliebige Uhrzeit definiert werden, zu deren Zeitpunkt der Tweet dann verschickt wird. Auf diese Weise lässt sich das vorhersagbare Verhalten beliebig verändern und verschleiern, zum Beispiel können auch typische Schlafenszeiten zum Tweet-Versand genutzt werden. Dadurch wird nicht nur die Vorhersagbarkeit reduziert, sondern auch weitere Informationen wie die genannten Schlafens- oder auch Arbeitszeiten, eine Abschätzbarkeit der Zeitzone, etc. sind für andere nur schwer oder gar nicht mehr ermittelbar.

12.1.2. Schutz vor Profilzuordnung durch Zeitdifferenzen

Der in dieser Arbeit vorgestellte Zeit-basierte Matching-Ansatz wertet insbesondere sehr geringe Zeitunterschiede in sozialen Netzen aus, typischerweise zusätzlich gekennzeichnet dadurch, dass ein Link auf einen generierten Inhalt in einem anderen Netz enthalten ist. Ermöglicht wird dies durch die inzwischen häufige Nutzung von Diensten wie IFTTT [345].

Eine Schutzmaßnahme gegen das in dieser Arbeit beschriebene Profilzuordnungsverfahren könnte der Verzicht auf entsprechende Dienste sein. Der Verzicht darauf führt allerdings zu entsprechenden Komforteinbußen bei den Nutzern und würde nur auf geringe Akzeptanz stoßen. Eine weitere Variante wäre der Verzicht auf den Link zum eigenen Inhalt in einem anderen sozialen Netz, allerdings will der Nutzer ja gerade darauf aufmerksam machen. Daher ist die Empfehlung, wenn auf die beiden vorgenannten Aspekte nicht verzichtet werden kann, eine entsprechende zeitliche Verzögerung einzubauen. Diese Verzögerung sollte zufällig ermittelt werden, mit einem Minimum von einigen Minuten bis hin zu mehreren Stunden. Nur so wird bei einer Auswertung dies nicht als automatisches Verhalten erkannt. Das Maximum der Verzögerungsspanne von mehreren Stunden ist notwendig und sollte wenn möglich noch größer gewählt werden, damit die Spanne ausreichend groß ist, dass auch eine fremde Person die Inhalte entdecken und dazu twittern könnte. Zusätzlich könnten gelegentliche Verweise auf Inhalte anderer Nutzer diesen Effekt noch verstärken. Andernfalls ist zwar die zeitliche Differenz bzw. Varianz groß, da aber trotzdem immer nur auf Inhalte des gleichen Nutzers verwiesen wird, stellt dies weiterhin zumindest ein Indiz für einen möglichen Match dar. Wenn ein Nutzer dutzende oder hunderte Links zu ein und dem selben Profil in einem anderen sozialen Netz twittert, ist es ansonsten weiterhin naheliegend, dass zwischen diesen beiden Profilen eine Beziehung besteht.

12.2. Geo-basierte Schutzmaßnahmen

Wie bei dem Zeit-basierten Profilzuordnungsverfahren mittels Zeitdifferenzen wäre auch hier natürlich die sinnvollste Schutzmaßnahme auf die entsprechende Funktion, in diesem Fall Geotags, gänzlich zu verzichten. Im Fall von Geotags büßt man auch keinen Komfort ein,

lediglich den Nachweis, tatsächlich an Ort und Stelle gewesen zu sein. Da auch hierauf nicht alle Nutzer verzichten wollen, ist es zumindest ratsam, Geotags nur in einem sozialen Netz zu benutzen, so kann keine Zuordnung zu einem anderen sozialen Netz erfolgen. Darüber hinaus sollten Geotags nicht an Orten benutzt werden, die beispielsweise dem Wohn- oder Arbeitsort entsprechen, hierdurch ergeben sich weitere Risiken. Beispielsweise, dass, sollte man nicht in einem Hochhaus wohnen, die Anzahl an Personen die ebenfalls in diesen Bereichen twittern können, sehr überschaubar ist. Das bedeutet, dass dadurch das Risiko für eine korrekte Profilzuordnung massiv erhöht wird. Zudem droht auch die Gefahr von Einbrüchen, wenn man im sozialen Netz Urlaubsbilder teilt und im Vorfeld Geotags von seinem Wohnort versendet hat. Ganz besonders dann, falls es sich in einem solchen Fall beispielsweise um ein Einfamilienhaus handelt.

Wirklich interessant für Follower sind sowieso nur Geotags von beispielsweise Sehenswürdigkeiten, so dass diese die Möglichkeit haben, den Ort selbst zu besuchen. Freunde und gegebenenfalls Bekannte kennen den Wohnort und benötigen hierzu kein Geotag. Allen anderen sollte man es nicht auf die Nase binden. Wie erläutert, geht man damit deutliche Risiken ein.

Allerdings besteht immer die Gefahr, dass eine Einstellung falsch gesetzt wurde oder vergessen wurde eine Option für den nächsten Tweet abzuwählen, was dazu führen kann, dass ein Geotag geteilt wird, obwohl dies gar nicht beabsichtigt war. Dies fällt auch nicht immer im Nachgang auf, so dass diese Information potentiell unbewusst dann doch im Netz verfügbar ist. Wenn der Nutzer auch nur wenig aktiv ist, in diesem sozialen Netz, können solche Nachrichten auch Jahre später noch auffindbar sein.

Eine komfortable Lösung, um diese Risiken zu vermeiden ist das Prinzip des Geofencing. Darunter versteht man das automatisierte Auslösen von Aktionen bei einem Überschreiten von definierten Grenzen. Dabei können beispielsweise beliebige Flächen oder Bereiche definiert werden, bei deren Betreten oder Verlassen eine Aktion ausgelöst wird. Apples iOS Smartphone Betriebssystem unterstützen diese Funktion prinzipiell seit langem und benachrichtigen eine App über das Überschreiten, für Android stehen zumindest entsprechende Apps bereit.

Wie kann diese Funktion jetzt helfen die Privatsphäre zu schützen? Es kann beispielsweise ein Bereich um den Wohnort und ein Bereich um den Arbeitsplatz definiert werden und sobald diese Bereiche betreten werden, wird die Nutzung von Geotags abgeschaltet. Der Nutzer muss sich diesbezüglich um nichts mehr kümmern und muss dennoch keine Angst haben aus Versehen seinen Wohn- oder Arbeitsort zu verraten.

12.3. Zusammenfassung

In diesem Kapitel wurden mehrere Maßnahmen erläutert die die Profilzuordnungsmethoden dieser Arbeit entsprechend abmildern oder auch verhindern können. Nichtsdestotrotz existieren darüber hinaus noch weitere Maßnahmen der Profilzuordnung, so dass es keinen

hundertprozentigen Schutz dagegen geben kann, solange ein Nutzer in mehreren sozialen Netzen aktiv ist. Die einzige absolut sichere Methode wäre auf die Nutzung sozialer Netze zu verzichten. Da dies jedoch für viele Menschen heutzutage undenkbar ist, bieten die vorgenannten Maßnahmen zumindest gegen automatisierte Profilzuordnungsversuche einen grundlegenden Schutz. Daher lautet die Empfehlung möglichst alle genannten Maßnahmen umzusetzen.

KAPITEL 13

Zusammenfassung und Ausblick

In diesem Kapitel werden die Ergebnisse der Arbeit zusammengefasst. Darauf aufbauend erfolgt ein Abgleich der definierten Anforderungen an ein Verfahren zur Profilzuordnung. Die Forschungsfragen werden aufgegriffen und zusammenfassend beantwortet. Abgeschlossen wird das Kapitel mit einem Ausblick in Form noch offener Fragestellungen und weitergehenden Forschungsarbeiten.

13.1. Einordnung der wissenschaftlichen Fragestellungen

Im Bereich der Profilzuordnung wird bereits seit circa 2009 geforscht, wen man von den Jahreszahlen der Veröffentlichungen ausgeht. Einer breiten Masse ist das Thema aber erst durch das Bekanntwerden der Überwachungs- und Spionageaffäre 2013, als Edward Snowden eine Vielzahl streng geheimer NSA Dokumente publik machte, bewusst geworden. Dabei wurde unter anderem bekannt, dass die Informationen verschiedener Internetkonzerne aggregiert wurden, um Profile und Informationen über verschiedenste Personen zu sammeln.

13.2. Abgleich der Anforderungserfüllung

Aggregation und Gewichtung hätten nach Anforderungserhebung in Kapitel 4 die letzten Schritte der Profilzuordnung dargestellt. Auch wenn diese nicht wie geplant durchgeführt werden konnten, erfolgt in diesem Abschnitt eine Bewertung der dort definierten Anforderungen hinsichtlich ihres Erfüllungsgrades. Tabelle 13.1 zeigt die Anforderungen aus Kapitel 4 mit einer Einschätzung der Anforderungserfüllung. In nachfolgender Auflistung wird auf die entsprechenden Anforderungen genauer eingegangen und auch die Bewertung der Anforderungserfüllung begründet.

- **Keine Nutzung von Profilattributen**: Es ist keine Nutzung von Profilattributen erfolgt. Diese wurden auch nicht gecrawlt, so dass eine Nutzung gar nicht möglich gewesen wäre. Daher wird dieser Punkt als voll erfüllt gewertet.

Tabelle 13.1.: Anforderungserfüllung. ✓ : Anforderung erfüllt, ○ : Anforderung teilweise erfüllt, ✗ : Anforderung nicht erfüllt.

	Daten	
1	Keine Nutzung von Profilattributen	✓
2	Keine Nutzung der Netzstruktur	✓
3	Keine Textanalysen	✓
4	Zuordnung im gleichen Netz möglich	✓
5	Nutzung von Zeitstempeln	✓
6	Nutzung von Geotags	✓
7	Einbeziehung weiterer Metadaten	○
8	Nutzung öffentlich zugänglicher Daten	✓
	Architektur	
9	Keine Klassifikatoren	✓
10	Gewichtung	✗
11	Kombinierte Auswertung	✗
12	Keine Verfeinerung notwendig	✓
	Evaluation	
13	Evaluation mit Ground-Truth-Datensatz	○
14	Evaluation mit Datensatz realistischer Größe	✓

- **Keine Nutzung der Netzstruktur**: Auch die Netzstruktur wurde nicht erfasst und hätte damit nicht für eine Auswertung genutzt werden können. Damit ist auch dieser Punkt voll erfüllt.

- **Keine Textanalysen**: Textanalysen wurden nicht durchgeführt, die Nutzer-generierten Inhalte wurden nicht gespeichert, damit ist dieser Punkt erfüllt.

- **Zuordnung im gleichen Netz möglich**: Sowohl das Zeitdifferenz- als auch das geobasierte Verfahren lassen sich auch auf Profile aus dem gleichen sozialen Netz anwenden. Für das Zeitdifferenzverfahren wurde dies im Rahmen der Boterkennung nachgewiesen, siehe 9.5.2, und für das geobasierte Verfahren wurde dies beispielsweise im Rahmen des Vergleichs der Aktivitätszenten, siehe 10.2.2, gezeigt. Die Tabelle 10.4 zeigt dabei Profile, deren Aktivitätszentren nahezu übereinstimmen. Für die 19 Fälle mit gleichem Zentrum haben die Tweets stets eine URL für ein Restaurant, ein Geschäft oder ähnliches enthalten. Bei einer manuellen Recherche wurde an einer Koordinate, die sich in den Listen der Geotags häufig wiederholt hat, eine Marketing Agentur aufgefunden. Dies wird als Nachweis der Anwendbarkeit gewertet, auch die Evaluation auf Geotag-Ebene untermauert dies. Daher wird dieser Punkt als voll erfüllt gewertet.

- **Nutzung von Zeitstempeln**: Das Zeitdifferenzverfahren basiert neben URLs ausschließlich auf Zeitstempeln, zudem wurde eine weitergehende Nutzung von Zeitstempeln im Rahmen der Analyse des zeitlichen Nutzerverhaltens erprobt. Damit ist dieser Punkt voll erfüllt.

- **Nutzung von Geotags**: Im Rahmen des geobasierten Zuordnungsverfahrens kommen ausschließlich Geotags zum Einsatz. Damit ist auch dieser Punkt voll erfüllt.
- **Einbeziehung weiterer Metadaten**: Eine über die Nutzung von Zeitstempeln und Geotags hinausgehende Einbeziehung von Metadaten erfolgt lediglich in Form von URLs. Diese stellen jedoch, wie in Abschnitt 6.2.2 erläutert, einen Graubereich dar. Sie entsprechen keinen klassischen Metadaten. Daher wurde diese Anforderung nur als teilweise erfüllt erachtet.
- **Nutzung öffentlich zugänglicher Daten**: Alle Daten, die im Rahmen dieser Arbeit genutzt wurden, konnten, ggf. unter Zuhilfenahme generierter Nutzeraccounts, da ansonsten die Nutzung entsprechender API-Funktionen nicht möglich ist, gecrawlt werden. Damit werden diese als öffentlich zugängliche Daten angesehen, da ein prinzipielles Einsehen auch ohne Nutzeraccount möglich ist, diese waren nur für das systematische Crawling erforderlich. Dieser Punkt ist damit voll erfüllt.
- **Keine Klassifikatoren**: Alle untersuchten Profilzuordnungsverfahren kommen ohne Klassifikatoren aus. Von daher ist diese Anforderung voll erfüllt.
- **Gewichtung**: Wie im vorangegangenen Abschnitt erläutert, kann aufgrund der Eigenschaften der entwickelten Profilzuordnungsverfahren keine Gewichtung vorgenommen werden. Aus diesem Grund ist diese Anforderung als nicht erfüllt bewertet.
- **Kombinierte Auswertung**: Wie im Abschnitt 11.1 erläutert, ist auch eine Aggregation der Ergebnisse der Verfahren aufgrund deren Charakteristik nicht möglich. Ein Entscheidungsbaum ist hierfür ein geeigneteres Vorgehen. Daher muss auch dieser Punkt als nicht erfüllt bewertet werden.
- **Keine Verfeinerung nötig**: Für das Zeitdifferenzverfahren entfällt ein Verfeinerungsschritt vollständig, da aufgrund der einbezogenen Daten und einem entsprechend gewählten Schwellwert nur ein direkter Match infrage kommt. Da gemäß Definition dieser Anforderung ein Match in den Top-10 enthalten sein muss, was für das geobasierte Verfahren in über 50% der Fälle zutreffend ist, wird diese Anforderung als erfüllt bewertet.
- **Evaluation mit Ground-Truth-Datensatz**: Da das Verfahren des zeitlichen Nutzerverhaltens zu ungenau für die Profilzuordnung ist, erfolgte hierfür auch keine diesbezügliche Evaluation. Für das Zeitdifferenzverfahren ist die Ground-Truth implizit durch die geringen Zeitdifferenzen gegeben. Dies wird auch durch die äußerst geringe Anzahl an Profilen auf die von mehr als einem Nutzer verwiesen wird, untermauert. Für das geobasierte Verfahren kamen virtuelle Datensätze zum Einsatz und die Datenreihe jeweils eines Nutzers wurde auf zwei aufgeteilt, um zu prüfen, ob diese Teile einander korrekt zugeordnet werden. Daher liegt hier eine Ground-Truth vor. Da die Erfüllung jedoch nur für das geobasierte Verfahren garantiert ist, wurde die Anforderung als teilweise erfüllt gewertet.
- **Evaluation mit Datensatz realistischer Größe**: Für das Zeitdifferenzverfahren ist die Größe des Datensatzes unerheblich, da kein Abgleich mit allen Profilen erfolgen muss. Das Verfahren ist damit für beliebig große Datensätze ohne Einschränkungen hinsichtlich

Genauigkeit anwendbar. Für das geobasierte Verfahren wurde durch die Nutzung von virtuellen Datensätzen eine Profilmenge von über 468 Millionen simuliert. Dies entspricht schon einem sehr großen Netz und wird daher als realistisch angesehen. Daher wird diese Anforderung als voll erfüllt bewertet.

In Summe sind damit zehn der 14 Anforderungen voll, zwei teilweise und zwei nicht erfüllt. Insgesamt wurden also über 70% als voll erfüllt und der Rest jeweils zu gleichen Teilen als teilweise bzw. nicht erfüllt bewertet.

13.3. Beantwortung der Fragestellungen

In diesem Abschnitt werden die wissenschaftlichen Fragestellungen aus Kapitel 2 aufgegriffen und anhand der gewonnenen Erkenntnisse aus der Arbeit beantwortet. Die Beantwortung erfolgt in etwas angepasster Reihenfolge, da die Erkenntnisse aufeinander aufbauen.

Welche öffentlich zugänglichen Metadaten durch Nutzerinteraktion generiert werden? Anhand eines Metamodells wurden zunächst generisch ausgewählte Metadaten näher analysiert. Dabei wurde zum einen deren Eigenarten aber auch die daraus möglichen Schlussfolgerungen diskutiert. Im nächsten Schritt wurden die für die Evaluation geeigneten sozialen Netze anhand ihrer Metadaten-Verfügbarkeit ausgewählt, näher betrachtet und einander gegenübergestellt.

Welche Überschneidungen der Metdadatentypen können netzübergreifend extrahiert werden? Die vorgenannte Gegenüberstellung der sozialen Netze zeigt in tabellarischer Form Metadatenüberschneidungen für die zuvor ausgewählen Netze. Aufgrund von stark gestiegender Datenschutzmaßnamen ist allerdings festzuhalten, dass der Zugriff auf die Daten sozialer Netze, dies schließt auch Metadaten mit ein, heutzutage weitaus restriktiver ist, als noch vor wenigen Jahren. Wobei nicht zwangsläufig der Funktionsumfang eingeschränkt wurde, sondern die Hürden zur Nutzung der API erhöht wurden. Bei allen drei betrachteten sozialen Netzen ist hierfür inzwischen eine explizite Freischaltung erforderlich. Das heißt ein solcher Zugang muss explizit beantragt und kann nicht wie noch vor wenigen Jahren einfach aktivert werden wenn man einen Account hat.

Welche Arten von Metadaten eignen sich für die Profilzuordnung? Anhand von drei verschiedenen Ansätzen wurde gezeigt, dass Zeitstempel für sich betrachtet keine ausreichende Aussagekraft besitzen. Auch für den Großteil weiterer Metadaten, für sich allein betrachtet, ist nicht davon auszugehen, dass die Aussagekraft für eine eindeutige Zuordnung ausreichend ist., da die Spanne möglicher Werte zu gering ist. Diese eignen sich aber beispielsweise für zusätzliche Filterschritte, um die Komplexität zu reduzieren. Einzige Ausnahme, die für sich genommen eine Zuordnung zulässt, die im Rahmen der Arbeit identifiziert werden konnte, sind Geotags.

Welche Beziehungen und Korrelationen von Metadaten ermöglichen eine Profilzuordnung? Entgegen der Einzelbetrachtung, wo Zeitstempel als alleiniges Kriterium als nicht aussagekräftig genug bewertet wurden, konnte gezeigt werden, dass demgegenüber ein Zeitstempel und ein

verweisendes Element, wie eine URL, eine Tweet-ID oder Media-ID, woraus sich ein zweiter Zeitstempel ermitteln lässt), schon ausreichend sein können. Wobei das verweisende Element nicht selbst den Zeitstempel enthalten muss, auch wenn dies die Sache deutlich erleichtert, ist es ausreichend wenn das Ziel des Verweises einen entsprechend abfragbaren Zeitstempel besitzt. Diese Art der Kombination erlaubt nicht nur eine Profilzuordnung, sondern lässt sich beispielsweise auch für die Boterkennung einsetzen.

Wie viele Daten sind hierfür erforderlich? Abhängig von der Art der Metadaten, kann bereits eine einmalige Kombination aus zwei Metadaten, wie eben für Zeitstempel und ein verweisendes Element erläutert, völlig ausreichend sein, um eine Profilzuordnung vorzunehmen. Wenn die Aussagekraft geringer ausfällt, beispielsweise für Geotags, konnte dennoch nachgewiesen werden, dass bereits fünf Geotags ausreichend sein können. Dennoch hat die Evaluation gezeigt, dass mit einer höheren Anzahl an Geotags auch eine deutlich bessere Genauigkeit erzielt werden kann.

Wie hoch ist die zu erzielende Genauigkeit? Die zu erzielende Genauigkeit ist stark vom verwendeten Ansatz abhängig. Für die Kombination aus Zeitstempel und verweisendes Element ist eine 100%ige Genauigkeit möglich. Voraussetzung dafür ist, dass das Delta zwischen den beiden Zeitstempeln, des genannten und dem des Elements auf das verwiesen wurde, so gering ausfällt, dass bedingt durch die Signallaufzeiten eine Beteiligung Dritter ausgeschlossen ist. Mit ansteigendem Delta nicht die Genauigkeit ab, wobei innerhalb weniger Sekunden immernoch von nahezu 100% ausgegangen werden kann. Für Geotags konnte immerhin eine Genauigkeit von durchschnittlich über 55% erzielt werden, wenn man das Ergebnis auf Profile mit mindestens 250 Geotags einschränkt, sind es über 76%.

13.4. Weitergehende Forschungsarbeiten

Im Rahmen der Arbeit wurden viele Aspekte der Profilzuordnung anhand von Metadaten behandelt. Nichtsdestotrotz bieten Metadaten so viele Möglichkeiten, dass nicht alle umfassend in dieser Arbeit behandelt werden konnten. Daher bieten sich mehrere Richtungen für zukünftige Forschungsarbeiten an:

- Die im Rahmen der Arbeit entwickelten Ansätze und die damit erzielbaren Ergebnisse weisen derzeit keine Optimierungen auf. Beispielsweise könnten durch einbeziehen weiterer (z.B. Geotag-Genauigkeit) oder der vollen Ausnutzung ausgewerteter (Geotags als geographischen Filter) Metadaten die Kandidatenmenge signifikant reduziert werden. Dies sollte zum einen die Genauigkeit erhöhen und Gleichzeit die Komplexität und damit den Rechenaufwand reduzieren.

- Ein Teil der vorgestellten Szenare aus Kapitel 3 konnten aufgrund fehlender Ground-Truth-Daten nicht im Detail untersucht werden. Hier besteht weiterer Forschungsbedarf und es ist ggf. auch eine Erhebung entsprechender Evaluationsdaten erforderlich. Diese könnten entweder durch Umfragen oder evt. auch durch eine Kooperation mit einem sozialen Netz erfolgen, so dieses anhand seiner Erfahrungen Aussagen dazu tätigen kann. Sobald

entsprechende Daten vorliegen, besteht die Möglichkeit die existierenden Verfahren daraufhin zu optimieren bzw. eigenständige, spezialisierte Verfahren zu entwickeln.

- Die Daten, die ein Nutzer im Internet und im speziellen in sozialen Netzen hinterlässt, werden immer mehr. Daher kommt dem Datenschutz eine immer größere Rolle zu. Auch wenn im Rahmen dieser Arbeit Empfehlungen gegeben wurden, wie die hier vorgestellten Verfahren umgangen bzw. deren Anwendung verhindert werden kann, so ist die Bedrohung einer ungewollten Profilzuordnung nicht gebannt. Insbesondere durch eine Kombination klassischer Profilzuordnungsverfahren mit den Ansätzen und Ideen aus dieser Arbeit ergibt sich hier weiterer Klärungsbedarf, welche Maßnahmen notwendig sind um zu verhindern, dass solche Verfahren auf einen selbst angewendet werden.

Tabellenverzeichnis

4.1. Kategorisierung der Anforderungen 32

5.1. Vergleich bisheriger Verfahren (nur Attribut-bezogene) mit dieser Arbeit 51
5.2. Vergleich bisheriger Verfahren (nur Graph-basierte) mit dieser Arbeit. 52
5.3. Vergleich bisheriger Verfahren (sonstige nicht Metadaten-basierte) mit dieser Arbeit. 53
5.4. Vergleich bisheriger Verfahren (nur im Schwerpunkt Metadaten-basierte) mit dieser Arbeit. 54

6.1. Genauigkeit von Geotags in Abhängigkeit der Nachkommastellen 61
6.2. Verteilung der Geotag-Genauigkeit im Bezug auf die Nachkommastellen anhand eines Twitter-Datensatzes vom 14.-15. August 2015 [34] 62
6.3. Verteilung der Area Flächenabdeckung anhand eines gecrawlten Twitter-Datensatzes 63
6.4. Übersicht sozialer Netze mit einer Nutzerzahl von mehr als 100 Millionen aktiven Nutzern pro Monat. Ein * bedeutet, dass das Netz keine oder keine aktuellen Nutzerzahlen veröffentlicht. 66
6.5. Übersicht sozialer Netze mit einer Nutzerzahl von mehr als 100 Millionen aktiven Nutzern pro Monat und einer Wertung der Abfragbarkeit der Daten bzw. Metadaten. 67
6.6. Übersicht über die verbliebenen sozialen Netze die für die Evaluation infrage kommen und deren Fokussierung. 67
6.7. Übersicht extrahierbarer und nutzbarer Metadaten der für die Evaluation ausgewählten sozialen Netze 69

7.1. Aufbau einer Tweet-ID. 72
7.2. Aufbau einer Media-ID. 73
7.3. Häufigkeit einzelner sozialer Netz am About.me Datensatz. 75
7.4. Häufigkeit einzelner sozialer Netze im About.me Datensatz. 76

8.1. Durchschnittsergebnisse der Vorhersage, ob ein weiterer Tweet an diesem Tag folgt (R richtig, F falsch) 82
8.2. Ergebnisse der zufälligen Vorhersage. 84

9.1. Vergleich der Zeitunterschiede für die in diesem Abschnitt beschriebenen Abläufe zwischen ersten und zweiten Post. 98
9.2. Übersicht über beobachtete Domains der beiden Datensätze 100
9.3. Übersicht der erforderlichen Abrufversuche und notwendige Iterationen zur Eingruppierung aller URLs in die Kategorien erfolgreich und Datei nicht gefunden. Spalten mit HTML enthalten die Anzahl der empfangenen HTML Fehler Codes. 101
9.4. Übersicht über die Zusammensetzung der Profilmenge des Munich Bot Challenge Datensatzes. 102
9.5. Übersicht der Zeitunterschiede zwischen der Veröffentlichung auf Instagram und Twitter 104
9.6. Anzahl der beobachteten URLs von mindestens zwei unterschiedlichen Twitter-User-IDs. 106
9.7. Anzahl mehr als einmal beobachteter URLs von einzelnen Nutzern. 106
9.8. Übersicht der Zeitunterschiede zwischen Veröffentlichung eines Tweets und eines darauf basierenden Retweets. 107
9.9. Übersicht der Zeitunterschiede zwischen der Veröffentlichung eines Tweets und eines darauf basierenden Replies. 108

10.1. Umfang der ausgewerteten Profile anhand der Anzahl der Geotags. 111
10.2. Umfang der ausgewerteten Profile anhand der Anzahl der Geotags. 112
10.3. Abstände der verglichenen Profile. 116
10.4. Anzahl der Profile deren Aktivitätszentren eine Distanz von unter 10 Metern zueinander haben und wie oft dies vorkommt. 118
10.5. Zusammenfassung der Trefferwahrscheinlichkeiten für die Top-10 inklusive identisch bewerteter Profile 128
10.6. Zusammenfassung der Trefferwahrscheinlichkeiten für die Top-10 exklusive identisch bewerteter Profile 128

13.1. Anforderungserfüllung. ✓ : Anforderung erfüllt, ○ : Anforderung teilweise erfüllt, ✗ : Anforderung nicht erfüllt. 138

Abbildungsverzeichnis

3.1. Szenario Identitätsdiebstahl 22
3.2. Szenario Fake-Profil für Hassreden 23
3.3. Szenario Fake-Profil für Stalking 23
3.4. Szenario Spamverteilung mittels eines Botnetzes 24
3.5. Szenario Botnetzkontrolle mittels Profile sozialer Netze 25

6.1. Metamodell eines sozialen Netzes, vergleiche [325]. 56
6.2. Das vorgestellte Metamodell eines sozialen Netzes als Entity-Relationship-Diagramm in Chen-Notation. 57
6.3. Ausschnitt des Entity-Relationship-Diagramms mit beispielhaft ergänzten Attributen. 58
6.4. Informationen eines Zeitstempels. 60
6.5. Informationen eines Geotags. 61
6.6. Informationen einer Area. 62

7.1. Twitters Tweet-ID-Aufbau anhand der Beispiel ID 378396225814265856. 71
7.2. Instagrams Media-ID-Aufbau anhand der Beispiel-ID 362294710510830105. . . 73

8.1. Anzahl an Tweets für die ausgewählten User-IDs, aufsteigend sortiert. 78
8.2. Abgedeckte Zeitspanne vom ersten bis zum letzten Tweet in Tagen, aufsteigend sortiert. 78
8.3. Anzahl an Tweets im Verhältnis zur abgedeckten Zeitspanne, aufsteigend nach Anzahl Tweets sortiert. 78
8.4. Prinzipielles Vorgehen des Normalisierungsschrittes. 79
8.5. Ergebnisse der Vorhersage, ob ein weiterer Tweet erfolgt, aufgeteilt auf Wochentage. 83
8.6. Ergebnisse des naiven Vorhersageverfahrens 85
8.7. Ergebnisse der tageweisen Vorhersage mittels Ringpuffer bzw. Array 86
8.8. Ergebnisse der wochenweisen Vorhersage mittels Ringpuffer bzw. Array 87
8.9. Alle evaluierten Zeitvorhersage-Verfahren mit den besten Trefferwahrscheinlichkeiten im Vergleich zueinander. 88
8.10. Alle evaluierten Zeitvorhersage-Verfahren mit den schlechtesten Trefferwahrscheinlichkeiten im Vergleich zueinander. 88

9.1. Zeitlicher Ablauf des Postens in unterschiedlichen sozialen Netzen bei manuellem Übertrag der URL oder des Inhalts. 92
9.2. Zeitlicher Ablauf des Postens in unterschiedlichen sozialen Netzen bei Nutzung von Tools wie IFTTT. 93
9.3. Zeitlicher Ablauf des Postens eines Bots ohne automatisierte Benachrichtigung. 95
9.4. Zeitlicher Ablauf des Postens eines Bots bei automatisierter Benachrichtigung. 96
9.5. Zeitlicher Ablauf des Postens in unterschiedlichen sozialen Netzen im Falle von Identitätsdiebstahl. 97
9.6. Grafische Darstellung der Zeitunterschiede inklusive der getrennten Betrachtung der Verteilung von kurzen und langen Instagram-URLs. 105

10.1. Darstellung des prinzipiellen Vorgehens bei der Analyse der Aktivitätszentren. . 110
10.2. Durchschnittswerte der berechneten Radien in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung. 112
10.3. Maximalwerte der berechneten Radien in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung. 113
10.4. Durchschnittswerte der berechneten Distanzen in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung. 114
10.5. Maximalwerte der berechneten Distanzen in km in Abhängigkeit von der Anzahl verworfener Geotags in % und der pro Nutzer insgesamt vorhandenen Geotags, siehe Farbcodierung. 114
10.6. Visualisierung des Vorgehens beim Vergleich der Aktivitätszentren. 115
10.7. Prozentsatz der Profile laut y-Achse mit den aufgeführten Abständen zueinander, siehe Farbcodierung laut Legende. X-Achse entspricht den bekannten Reduktionsstufen. 117
10.8. Prinzip der virtuellen Datensätze. 120
10.9. Visualisierung des Vorgehens beim Vergleich der Geotags zweier Nutzer. 121
10.10 Ergebnisse der Geotag-weisen Auswertung für alle Profile 123
10.11 Ergebnisse der Geotag-weisen Auswertung für Profile mit mind. 25, 50, 100 und 250 Profilen und einem genauen Treffer 125
10.12 Ergebnisse der Geotag-weisen Auswertung für Profile mit mind. 25, 50, 100 und 250 Profilen und Treffer unter den Top Zehn 126
10.13 Anzahl der Profile anhand derer eine korrekte Zuordnung geprüft werden konnte. 127

11.1. Entscheidungsbaum für die Auswahl eines Profilzuordnungsverfahrens 132

A.1. Metadaten eines Tweets 174
A.2. Ergebnisse der Geotag-weisen Auswertung für alle Profile mit Top 1, Top 3, Top 10 und Top 1, Top 3 und Top 10 inklusive gleich bewerteter Treffer 175
A.3. Ergebnisse der Geotag-weisen Auswertung für Profile mit mind. 25, 50, 100 und 250 Profilen und Treffer unter den Top Drei 176

Literatur

[1] d. m. boyd und N. B. Ellison. „Social Network Sites: Definition, History, and Scholarship“. In: *Journal of Computer-Mediated Communication* 13.1 (2007), S. 210–230. ISSN: 1083-6101. DOI: 10.1111/j.1083-6101.2007.00393.x.

[2] Facebook. *Company Info | Facebook Newsroom*. URL: http://newsroom.fb.com/company-info/ (abgerufen am 06. 03. 2017).

[3] Twitter. *Company | About*. URL: https://about.twitter.com/company (abgerufen am 06. 03. 2017).

[4] Instagram. *Our Story – Instagram*. URL: https://instagram-press.com/our-story/ (abgerufen am 06. 03. 2017).

[5] P. S. Earle, D. C. Bowden und M. Guy. „Twitter earthquake detection: earthquake monitoring in a social world“. In: *Annals of Geophysics* 54.6 (2012).

[6] E. Aramaki, S. Maskawa und M. Morita. „Twitter catches the flu: detecting influenza epidemics using Twitter“. In: *Proceedings of the conference on empirical methods in natural language processing*. Association for Computational Linguistics. 2011, S. 1568–1576.

[7] A. Tumasjan u. a. „Predicting elections with twitter: What 140 characters reveal about political sentiment.“ In: *ICWSM* 10 (2010), S. 178–185.

[8] A. Mittal und A. Goel. „Stock prediction using twitter sentiment analysis“. In: *Standford University, CS229 (2011 http://cs229.stanford.edu/proj2011/GoelMittal-StockMarketPrediction UsingTwitterSentimentAnalysis.pdf)* (2012).

[9] M. S. Gerber. „Predicting crime using Twitter and kernel density estimation“. In: *Decision Support Systems* 61 (2014), S. 115–125.

[10] D. Kergl, R. Roedler und G. D. Rodosek. „Detection of Zero Day Exploits Using Real-Time Social Media Streams“. In: *Advances in Nature and Biologically Inspired Computing*. Springer, 2016, S. 405–416.

[11] J. Mander. *Internet users have average of 7 social accounts:* URL: https://www.globalwebindex.net/blog/internet-users-have-average-of-7-social-accounts (abgerufen am 07. 03. 2017).

[12] CareerBuilder. *Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade - CareerBuilder:* URL: http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=4/28/2016&siteid=cbpr&sc_cmp1=cb_pr945_&id=pr945&ed=12/31/2016 (abgerufen am 20. 10. 2016).

[13] S. I. Corp. *Home - Social Intel:* URL: http://www.socialintel.com/ (abgerufen am 20. 10. 2016).

[14] R. Gross und A. Acquisti. „Information revelation and privacy in online social networks". In: *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM. 2005, S. 71–80.

[15] H. R. Lipford, A. Besmer und J. Watson. „Understanding Privacy Settings in Facebook with an Audience View." In: ().

[16] M. Madejski, M. Johnson und S. M. Bellovin. „The failure of online social network privacy settings". In: *Department of Computer Science, Columbia University, Tech. Rep. CUCS-010-11* (2011).

[17] K. Blair. *New Survey: Burglars Use Social Media to Plan Crimes | SocialTimes:* URL: http://www.adweek.com/socialtimes/new-survery-burglars-use-social-media-to-plan-crimes/80480 (abgerufen am 20. 10. 2016).

[18] S. Krempl. *heise online Polittalk: Gute Programmierer essen viel Lakritze | heise online:* URL: http://www.heise.de/newsticker/meldung/heise-online-Polittalk-Gute-Programmierer-essen-viel-Lakritze-3354094.html (abgerufen am 19. 10. 2016).

[19] N. Press. „Understanding metadata". In: *National Information Standards* 20 (2004).

[20] A. Z. *Haftung und Vollstreckung:* URL: http://www.informatik.uni-oldenburg.de/~iug11/rf/vollzug_haftung.html (abgerufen am 21. 10. 2016).

[21] T. Greene. *Largest DDoS attack ever delivered by botnet of hijacked IoT devices | Network World:* URL: http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html (abgerufen am 21. 10. 2016).

[22] P. Burghouwt, M. Spruit und H. Sips. „Detection of Covert Botnet Command and Control Channels by Causal Analysis of Traffic Flows". In: *Cyberspace Safety and Security: 5th International Symposium, CSS 2013, Zhangjiajie, China, November 13-15, 2013, Proceedings*. Hrsg. von G. Wang u. a. Cham, 2013, S. 117–131.

[23] Y. Boshmaf u. a. „Design and analysis of a social botnet". In: *Computer Networks* 57.2 (2013), S. 556–578.

[24] E. J. Kartaltepe u. a. „Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures". In: *Applied Cryptography and Network Security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010. Proceedings*. Hrsg. von J. Zhou und M. Yung. Berlin, Heidelberg, 2010, S. 511–528.

[25] C. Lumezanu und N. Feamster. „Observing Common Spam in Twitter and Email“. In: *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*. IMC ’12. Boston, Massachusetts, USA, 2012, S. 461–466. ISBN: 978-1-4503-1705-4.

[26] G. Stringhini, C. Kruegel und G. Vigna. „Detecting spammers on social networks“. In: *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM. 2010, S. 1–9.

[27] T. Warren. *First Click: Twitter spam is out of control | The Verge:* URL: http://www.theverge.com/2016/8/30/12707554/first-click-twitter-spam-is-out-of-control (abgerufen am 21. 10. 2016).

[28] C. M. Zhang und V. Paxson. „Detecting and analyzing automated activity on twitter“. In: *International Conference on Passive and Active Network Measurement*. Springer. 2011, S. 102–111.

[29] N. M. Radziwill und M. C. Benton. „Bot or Not? Deciphering Time Maps for Tweet Interarrivals“. In: *arXiv preprint arXiv:1605.06555* (2016).

[30] n tv.de. *Der Tag: AfD setzt für Wahlen 2017 auf Social Bots - n-tv.de:* URL: http://mobil.n-tv.de/der_tag/AfD-setzt-fuer-Wahlen-2017-auf-Social-Bots-article18908766.html?campaign_id=A100 (abgerufen am 21. 10. 2016).

[31] C. Hoffman. *Facebook Makes Money Out Of Your Data – Why Shouldn’t You?:* URL: http://www.makeuseof.com/tag/facebook-makes-money-out-of-your-data-why-shouldnt-you/ (abgerufen am 22. 10. 2016).

[32] Twitter. *GET statuses/user_timeline | Twitter Developers:* URL: https://dev.twitter.com/rest/reference/get/statuses/user_timeline (abgerufen am 22. 10. 2016).

[33] F. Calabrese u. a. „Understanding individual mobility patterns from urban sensing data: A mobile phone trace example“. In: *Transportation research part C: emerging technologies* 26 (2013), S. 301–313.

[34] R. Roedler, D. Kergl und G. D. Rodosek. „Profile Matching Across Online Social Networks Based on Geo-Tags“. In: *Advances in Nature and Biologically Inspired Computing*. Springer, 2016, S. 417–428.

[35] Z. Cheng, J. Caverlee und K. Lee. „You are where you tweet: a content-based approach to geo-locating twitter users“. In: *Proceedings of the 19th ACM international conference on Information and knowledge management*. ACM. 2010, S. 759–768.

[36] D. Thom u. a. „Using large scale aggregated knowledge for social media location discovery“. In: *2014 47th Hawaii International Conference on System Sciences*. IEEE. 2014, S. 1464–1473.

[37] S. H. Burton u. a. „” Right time, right place” health communication on Twitter: value and accuracy of location information“. In: *Journal of medical Internet research* 14.6 (2012), e156.

[38] P. Jain und P. Kumaraguru. „@ i to@ me: An anatomy of username changing behavior on twitter“. In: *arXiv preprint arXiv:1405.6539* (2014).

[39] S. Valenzuela, N. Park und K. F. Kee. „Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation1". In: *Journal of Computer-Mediated Communication* 14.4 (2009), S. 875–901.

[40] C. Steinfield, N. B. Ellison und C. Lampe. „Social capital, self-esteem, and use of online social network sites: A longitudinal analysis". In: *Journal of Applied Developmental Psychology* 29.6 (2008), S. 434–445.

[41] J. Scott. *Social network analysis*. Sage, 2012.

[42] C. C. Aggarwal. „An introduction to social network data analytics". In: *Social network data analytics*. Springer, 2011, S. 1–15.

[43] B. Hecht u. a. „Tweets from Justin Bieber's heart: the dynamics of the location field in user profiles". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2011, S. 237–246.

[44] D. Correa, A. Sureka und R. Sethi. „WhACKY!-What anyone could know about you from Twitter". In: *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on*. IEEE. 2012, S. 43–50.

[45] E. Altman und Y. Portilla. „Geo-linguistic fingerprint and the evolution of languages in Twitter". In: *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on*. IEEE. 2012, S. 1–6.

[46] T. Fujisaka, R. Lee und K. Sumiya. „Discovery of user behavior patterns from geo-tagged micro-blogs". In: *Proceedings of the 4th International Conference on Uniquitous Information Management and Communication*. ACM. 2010, S. 36.

[47] K. Zoltán und S. Johann. „Semantic analysis of microposts for efficient people to people interactions". In: *2011 RoEduNet International Conference 10th Edition: Networking in Education and Research*. IEEE. 2011, S. 1–4.

[48] E. Kouloumpis, T. Wilson und J. D. Moore. „Twitter sentiment analysis: The good the bad and the omg!" In: *Icwsm* 11 (2011), S. 538–541.

[49] J. K. Ahkter und S. Soria. „Sentiment analysis: Facebook status messages". In: *Unpublished master's thesis, Stanford, CA* (2010).

[50] J. Ugander u. a. „The anatomy of the facebook social graph". In: *arXiv preprint arXiv:1111.4503* (2011).

[51] M. Gjoka u. a. „Walking in facebook: a case study of unbiased sampling of OSNs". In: *Infocom, 2010 Proceedings IEEE*. IEEE. 2010, S. 1–9.

[52] J. Lindqvist u. a. „I'm the mayor of my house: examining why people use foursquare-a social-driven location sharing application". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM. 2011, S. 2409–2418.

[53] H. Cramer, M. Rost und L. E. Holmquist. „Performing a check-in: emerging practices, norms and'conflicts' in location-sharing using foursquare". In: *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*. ACM. 2011, S. 57–66.

[54] M. A. Vasconcelos u. a. „Tips, dones and todos: uncovering user profiles in foursquare“. In: *Proceedings of the fifth ACM international conference on Web search and data mining*. ACM. 2012, S. 653–662.

[55] A. Noulas u. a. „An Empirical Study of Geographic User Activity Patterns in Foursquare.“ In: *ICwSM* 11 (2011), S. 70–573.

[56] Y.-Y. Ahn u. a. „Analysis of topological characteristics of huge online social networking services“. In: *Proceedings of the 16th international conference on World Wide Web*. ACM. 2007, S. 835–844.

[57] F. Benevenuto u. a. „Characterizing user behavior in online social networks“. In: *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*. ACM. 2009, S. 49–62.

[58] A. Abisheva u. a. „Who watches (and shares) what on youtube? and when?: using twitter to understand youtube viewership“. In: *Proceedings of the 7th ACM international conference on Web search and data mining*. ACM. 2014, S. 593–602.

[59] W. Lucia, C. G. Akcora und E. Ferrari. „Multi-dimensional conversation analysis across online social networks“. In: *Cloud and Green Computing (CGC), 2013 Third International Conference on*. IEEE. 2013, S. 369–376.

[60] B. H. Lim u. a. „# mytweet via Instagram: Exploring user behaviour across multiple social networks“. In: *Advances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on*. IEEE. 2015, S. 113–120.

[61] Y. Fang und M.-W. Chang. „Entity linking on microblogs with spatial and temporal signals“. In: *Transactions of the Association for Computational Linguistics* 2 (2014), S. 259–272.

[62] B. Liu. „Sentiment analysis and opinion mining“. In: *Synthesis lectures on human language technologies* 5.1 (2012), S. 1–167.

[63] A. Pak und P. Paroubek. „Twitter as a Corpus for Sentiment Analysis and Opinion Mining.“ In: *LREc*. Bd. 10. 2010, S. 1320–1326.

[64] P. Sobkowicz, M. Kaschesky und G. Bouchard. „Opinion mining in social media: Modeling, simulating, and forecasting political opinions in the web“. In: *Government Information Quarterly* 29.4 (2012), S. 470–479.

[65] F. Bodendorf und C. Kaiser. „Detecting opinion leaders and trends in online social networks“. In: *Proceedings of the 2nd ACM workshop on Social web search and mining*. ACM. 2009, S. 65–68.

[66] M. Mathioudakis und N. Koudas. „Twittermonitor: trend detection over the twitter stream“. In: *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*. ACM. 2010, S. 1155–1158.

[67] A. Hotho u. a. „Trend detection in folksonomies“. In: *International Conference on Semantic and Digital Media Technologies*. Springer. 2006, S. 56–70.

[68] J. Benhardus und J. Kalita. „Streaming trend detection in twitter“. In: *International Journal of Web Based Communities* 9.1 (2013), S. 122–139.

[69] J. Weng und B.-S. Lee. „Event Detection in Twitter.“ In: *ICWSM* 11 (2011), S. 401–408.

[70] H. Sayyadi, M. Hurst und A. Maykov. „Event detection and tracking in social streams.“ In: *Icwsm*. 2009.

[71] T. Sakaki, M. Okazaki und Y. Matsuo. „Earthquake shakes Twitter users: real-time event detection by social sensors“. In: *Proceedings of the 19th international conference on World wide web*. ACM. 2010, S. 851–860.

[72] M. Jain u. a. „Temporal analysis of user behavior and topic evolution on Twitter“. In: *Big Data Analytics*. Springer, 2013, S. 22–36.

[73] G. Dominguez u. a. „Stream Volume Prediction in Twitter with Artificial Neural Networks.“ In: *ICPRAM (2)*. 2012, S. 488–493.

[74] D. Darmon u. a. „Predictability of user behavior in social media: Bottom-up v. top-down modeling“. In: *Social Computing (SocialCom), 2013 International Conference on*. IEEE. 2013, S. 102–107.

[75] G. Song, Z. Li und H. Tu. „Forward or ignore: User behavior analysis and prediction on microblogging“. In: *Advanced Research in Applied Artificial Intelligence*. Springer, 2012, S. 231–241.

[76] S. Asur und B. A. Huberman. „Predicting the future with social media“. In: *Web Intelligence and Intelligent Agent Technology (WI-IAT), 2010 IEEE/WIC/ACM International Conference on*. Bd. 1. IEEE. 2010, S. 492–499.

[77] J. Bollen, H. Mao und X. Zeng. „Twitter mood predicts the stock market“. In: *Journal of Computational Science* 2.1 (2011), S. 1–8.

[78] G. Andrienko u. a. „Thematic patterns in georeferenced tweets through space-time visual analytics“. In: *Computing in Science and Engineering* 15.3 (2013), S. 72–82.

[79] S. Milgram. „The small world problem“. In: *Psychology today* 2.1 (1967), S. 60–67.

[80] D. Liben-Nowell u. a. „Geographic routing in social networks“. In: *Proceedings of the National Academy of Sciences of the United States of America* 102.33 (2005), S. 11623–11628.

[81] R. Krüger, D. Thom und T. Ertl. „Semantic enrichment of movement behavior with foursquare–A visual analytics approach“. In: *IEEE transactions on visualization and computer graphics* 21.8 (2015), S. 903–915.

[82] A. Noulas u. a. „Exploiting Semantic Annotations for Clustering Geographic Areas and Users in Location-based Social Networks.“ In: *The social mobile web* 11 (2011), S. 02.

[83] Z. Cheng, J. Caverlee und K. Lee. „You are where you tweet: a content-based approach to geo-locating twitter users“. In: *Proceedings of the 19th ACM international conference on Information and knowledge management*. ACM. 2010, S. 759–768.

[84] S. Scellato u. a. „Distance Matters: Geo-social Metrics for Online Social Networks.“ In: *WOSN*. 2010.

[85] Z. Liu und Y. Huang. „Where are You Tweeting? A Context and User Movement Based Approach“. In: *Proceedings of the 25th ACM International on Conference on Information and Knowledge Management*. 2016, S. 1949–1952.

[86] N. Takeda und Y. Seki. „Twitter User Classification with Posting Locations“. In: *International Conference on Asian Digital Libraries*. Springer. 2016, S. 297–310.

[87] M. Ren. „Location Cheating: A Security Challenge to Location-based Social Network Services“. In: (2011).

[88] Z. Zhang u. a. „On the validity of geosocial mobility traces“. In: *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*. ACM. 2013, S. 11.

[89] J. Goldenberg und M. Levy. „Distance is not dead: Social interaction and geographical distance in the internet era“. In: *arXiv preprint arXiv:0906.3202* (2009).

[90] M. Dredze u. a. „Carmen: A twitter geolocation system with applications to public health“. In: *AAAI Workshop on Expanding the Boundaries of Health Informatics Using AI (HIAI)*. Citeseer. 2013, S. 20–24.

[91] J. Cranshaw u. a. „Bridging the gap between physical location and online social networks“. In: *Proceedings of the 12th ACM international conference on Ubiquitous computing*. ACM. 2010, S. 119–128.

[92] J. Liu u. a. „Multi-scale population and mobility estimation with geo-tagged tweets“. In: *Data Engineering Workshops (ICDEW), 2015 31st IEEE International Conference on*. IEEE. 2015, S. 83–86.

[93] E. Cho, S. A. Myers und J. Leskovec. „Friendship and mobility: user movement in location-based social networks“. In: *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 2011, S. 1082–1090.

[94] S. Scellato u. a. „Socio-Spatial Properties of Online Location-Based Social Networks.“ In: *ICWSM* 11 (2011), S. 329–336.

[95] L. Humphreys. „Mobile social networks and social practice: A case study of Dodgeball“. In: *Journal of Computer-Mediated Communication* 13.1 (2007), S. 341–360.

[96] E. Aïmeur, G. Brassard und P. Molins. „Reconstructing profiles from information disseminated on the internet“. In: *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*. IEEE. 2012, S. 875–883.

[97] A. Mislove u. a. „You are who you know: inferring user profiles in online social networks“. In: *Proceedings of the third ACM international conference on Web search and data mining*. ACM. 2010, S. 251–260.

[98] L. Backstrom, E. Sun und C. Marlow. „Find me if you can: improving geographical prediction with social and spatial proximity“. In: *Proceedings of the 19th international conference on World wide web*. ACM. 2010, S. 61–70.

[99] M. D. Lieberman und J. Lin. „You Are Where You Edit: Locating Wikipedia Contributors through Edit Histories.“ In: *ICWSM*. 2009.

[100] D. Thom u. a. „Using large scale aggregated knowledge for social media location discovery“. In: *2014 47th Hawaii International Conference on System Sciences*. IEEE. 2014, S. 1464–1473.

[101] J. Krumm. „Inference attacks on location tracks“. In: *International Conference on Pervasive Computing*. Springer. 2007, S. 127–143.

[102] C. A. Davis Jr u. a. „Inferring the location of twitter messages based on user relationships“. In: *Transactions in GIS* 15.6 (2011), S. 735–751.

[103] J. Mahmud, J. Nichols und C. Drews. „Where Is This Tweet From? Inferring Home Locations of Twitter Users.“ In: *ICWSM* 12 (2012), S. 511–514.

[104] L. Liao u. a. „Learning and inferring transportation routines“. In: *Artificial Intelligence* 171.5 (2007), S. 311–331.

[105] J. Krumm und E. Horvitz. „Predestination: Inferring destinations from partial trajectories“. In: *International Conference on Ubiquitous Computing*. Springer. 2006, S. 243–260.

[106] J. Jia u. a. „AttriInfer: Inferring User Attributes in Online Social Networks Using Markov Random Fields“. In: *Proceedings of the 26th International Conference on World Wide Web*. WWW '17. Perth, Australia: International World Wide Web Conferences Steering Committee, 2017, S. 1561–1569. ISBN: 9781450349130. DOI: 10.1145/3038912.3052695.

[107] N. Z. Gong und B. Liu. „You Are Who You Know and How You Behave: Attribute Inference Attacks via Users' Social Friends and Behaviors“. In: *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, S. 979–995. ISBN: 978-1-931971-32-4.

[108] N. Z. Gong und B. Liu. „Attribute Inference Attacks in Online Social Networks“. In: *ACM Trans. Priv. Secur.* 21.1 (Jan. 2018). ISSN: 2471-2566. DOI: 10.1145/3154793.

[109] A. Alekseev und S. Nikolenko. „Word embeddings for user profiling in online social networks“. In: *Computación y Sistemas* 21.2 (2017), S. 203–226.

[110] M. Backes u. a. „Walk2friends: Inferring Social Links from Mobility Profiles“. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. Dallas, Texas, USA: Association for Computing Machinery, 2017, S. 1943–1957. ISBN: 9781450349468. DOI: 10.1145/3133956.3133972.

[111] Y. Chen u. a. „Understanding cross-site linking in online social networks“. In: *Proceedings of the 8th Workshop on Social Network Mining and Analysis*. ACM. 2014, S. 6.

[112] M. Edwards u. a. „Sampling labelled profile data for identity resolution“. In: *2016 IEEE International Conference on Big Data (Big Data)*. 2016, S. 540–547. DOI: 10.1109/BigData.2016.7840645.

[113] R. Kaushal, S. Gupta und P. Kumaraguru. „Investigation of Biases in Identity Linkage DataSets“. In: *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. SAC '20. Brno, Czech Republic: Association for Computing Machinery, 2020, S. 1861–1868. ISBN: 9781450368667. DOI: 10.1145/3341105.3374015.

[114] O. Goga u. a. „On the reliability of profile matching across large online social networks“. In: *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM. 2015, S. 1799–1808.

[115] K. Shu u. a. „User identity linkage across online social networks: A review“. In: *Acm Sigkdd Explorations Newsletter* 18.2 (2017), S. 5–17.

[116] L. Xing u. a. „A Survey of Across Social Networks User Identification“. In: *IEEE Access* 7 (2019), S. 137472–137488. DOI: 10.1109/ACCESS.2019.2942840.

[117] A. Viswam und G. Darsan. „A STUDY ON IDENTIFYING SIMILAR USERS ACROSS MULTIPLE SOCIAL MEDIA SITES“. In: (2017).

[118] R. Kaushal und P. Kumaraguru. „A Systematic Review on User Identity Linkage across Online Social Networks“. In: (2020).

[119] R. Zafarani und H. Liu. „Connecting Corresponding Identities across Communities.“ In: *ICWSM*. Citeseer. 2009.

[120] D. Perito u. a. „How unique and traceable are usernames?“ In: *Privacy Enhancing Technologies*. Springer. 2011, S. 1–17.

[121] J. Vosecky, D. Hong und V. Y. Shen. „User identification across multiple social networks“. In: *Networked Digital Technologies, 2009. NDT'09. First International Conference on*. IEEE. 2009, S. 360–365.

[122] E. Raad, R. Chbeir und A. Dipanda. „User profile matching in social networks“. In: *Network-Based Information Systems (NBiS), 2010 13th International Conference on*. IEEE. 2010, S. 297–304.

[123] C. G. Akcora, B. Carminati und E. Ferrari. „Network and profile based measures for user similarities on social networks“. In: *Information Reuse and Integration (IRI), 2011 IEEE International Conference on*. IEEE. 2011, S. 292–298.

[124] R. Soltani und A. Abhari. „Identity matching in social media platforms“. In: *Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2013 International Symposium on*. IEEE. 2013, S. 64–70.

[125] O. Peled u. a. „Entity matching in online social networks“. In: *Social Computing (SocialCom), 2013 International Conference on*. IEEE. 2013, S. 339–344.

[126] W. Cohen, P. Ravikumar und S. Fienberg. „A comparison of string metrics for matching names and records“. In: *Kdd workshop on data cleaning and object consolidation*. Bd. 3. 2003, S. 73–78.

[127] Y. Na u. a. „User identification based on multiple attribute decision making in social networks“. In: *Communications, China* 10.12 (2013), S. 37–49.

[128] S. Sarker, W. Franz und M. T. Nayeem. „Automatic Individual Information Aggregation using Publicly Available Social Media Data“. In: *2019 22nd International Conference on Computer and Information Technology (ICCIT)*. 2019, S. 1–6. DOI: 10.1109/ICCIT48885.2019.9038402.

[129] R. Kaushal, V. Ghose und P. Kumaraguru. „Methods for User Profiling across Social Networks“. In: *2019 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*. 2019, S. 1572–1579. DOI: 10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00231.

[130] A. Esfandyari u. a. „User identification across online social networks in practice: Pitfalls and solutions“. In: *Journal of Information Science* 44.3 (2018), S. 377–391.

[131] W. Zeng u. a. „User Identification Based on Integrating Multiple User Information across Online Social Networks“. In: *Security and Communication Networks* 2021 (2021).

[132] Y. Li u. a. „User Identification Based on Display Names Across Online Social Networks“. In: *IEEE Access* 5 (2017), S. 17342–17353. DOI: 10.1109/ACCESS.2017.2744646.

[133] Y. Li u. a. „Matching user accounts across social networks based on username and display name“. In: *World Wide Web* 22.3 (2019), S. 1075–1097.

[134] L. Xing u. a. „Behavioral habits-based user identification across social networks“. In: *Symmetry* 11.9 (2019), S. 1134.

[135] Z. Zhong u. a. „Colink: An unsupervised framework for user identity linkage“. In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Bd. 32. 1. 2018.

[136] W. Ahmad und R. Ali. „Social Account Matching in Online Social Media using Cross-linked Posts“. In: *Procedia Computer Science* 152 (2019). International Conference on Pervasive Computing Advances and Applications- PerCAA 2019, S. 222–229. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2019.05.046.

[137] M. VIDYAVIHAR. „Identity Resolution across Different Social Networks using Similarity Analysis“. In: *International Journal on Recent and Innovation Trends in Computing and Communication* 5.8 (), S. 26–30.

[138] T. Sokhin, N. Butakov und D. Nasonov. „User Profiles Matching for Different Social Networks Based on Faces Identification“. In: *International Conference on Hybrid Artificial Intelligence Systems*. Springer. 2019, S. 551–562.

[139] P. Jain und P. Kumaraguru. „Automated methods for identity resolution across online social networks“. Diss. 2016.

[140] K. KOJIMA, K. IKEDA und M. TANI. „Short Paper: User Identification across Online Social Networks Based on Similarities among Distributions of Friends' Locations“. In: *2019 IEEE International Conference on Big Data (Big Data)*. 2019, S. 4085–4088. DOI: 10.1109/BigData47090.2019.9006186.

[141] F. Carmagnola, F. Osborne und I. Torre. „User data distributed on the social web: how to identify users on different social systems and collecting data about them“. In: *Proceedings of the 1st international workshop on information heterogeneity and fusion in recommender systems*. ACM. 2010, S. 9–15.

[142] A. Malhotra u. a. „Studying user footprints in different online social networks“. In: *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*. IEEE Computer Society. 2012, S. 1065–1070.

[143] F. Carmagnola und F. Cena. „User identification for cross-system personalisation“. In: *Information Sciences* 179.1 (2009), S. 16–32.

[144] F. Orlandi, J. Breslin und A. Passant. „Aggregated, interoperable and multi-domain user profiles for the social web“. In: *Proceedings of the 8th International Conference on Semantic Systems*. ACM. 2012, S. 41–48.

[145] R. Zafarani und H. Liu. „Connecting users across social media sites: a behavioral-modeling approach“. In: *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 2013, S. 41–49.

[146] P. Jain, P. Kumaraguru und A. Joshi. „Other Times, Other Values: Leveraging Attribute History to Link User Profiles across Online Social Networks“. In: *Proceedings of the 26th ACM Conference on Hypertext & Social Media*. ACM. 2015, S. 247–255.

[147] M. Wang u. a. „De-anonymizing Social Networks User via Profile Similarity“. In: *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*. 2018, S. 889–895. DOI: 10.1109/DSC.2018.00142.

[148] V. Belov u. a. „An integrated approach to mapping user profiles on social networks“. In: (2020).

[149] A. Mbarek, S. Jamoussi und A. BenHamadou. „Tuser 3: A Profile Matching Based Algorithm Across Three Heterogeneous Social Networks“. In: *International Conference on Advanced Data Mining and Applications*. Springer. 2020, S. 191–206.

[150] S. Garg, S. K. Raghuwanshi und P. D. Singh. „User profile matching and identification using TLBO and clustering approach over social networks“. In: *Harmony Search and Nature Inspired Optimization Algorithms*. Springer, 2019, S. 979–987.

[151] A. Halimi und E. Ayday. „Profile Matching Across Online Social Networks“. In: *International Conference on Information and Communications Security*. Springer. 2020, S. 54–70.

[152] Q. Ma u. a. „Joining user profiles across online social networks: From the perspective of an adversary“. In: *Advances in Social Networks Analysis and Mining (ASONAM), 2016 IEEE/ACM International Conference on*. IEEE. 2016, S. 178–185.

[153] M. Motoyama und G. Varghese. „I seek you: searching and matching individuals in social networks“. In: *Proceedings of the eleventh international workshop on Web information and data management*. ACM. 2009, S. 67–75.

[154] A. Narayanan und V. Shmatikov. „De-anonymizing social networks“. In: *Security and Privacy, 2009 30th IEEE Symposium on*. IEEE. 2009, S. 173–187.

[155] D. Chen, B. Hu und S. Xie. „De-anonymizing social networks“. In: *CS224W Course Project Writup* (2012).

[156] J. Zhang und S. Y. Philip. „Multiple anonymized social networks alignment“. In: *Data Mining (ICDM), 2015 IEEE International Conference on*. IEEE. 2015, S. 599–608.

[157] Y. Shen und H. Jin. „Controllable information sharing for user accounts linkage across multiple online social networks“. In: *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management*. ACM. 2014, S. 381–390.

[158] H. Van Pham und V. T. Nguyen. „A Novel Approach Using Context Matching Algorithm and Knowledge Inference for User Identification in Social Networks“. In: *Proceedings of the 4th International Conference on Machine Learning and Soft Computing*. ICMLSC 2020. Haiphong City, Viet Nam: Association for Computing Machinery, 2020, S. 149–153. ISBN: 9781450376310. DOI: 10.1145/3380688.3380708.

[159] R. Tang u. a. „Interlayer link prediction in multiplex social networks: an iterative degree penalty algorithm“. In: *Knowledge-Based Systems* 194 (2020), S. 105598.

[160] R. Tang u. a. „Interlayer Link Prediction in Multiplex Social Networks Based on Multiple Types of Consistency between Embedding Vectors“. In: *arXiv preprint arXiv:2008.05212* (2020).

[161] N. Hernandez u. a. „Fraud De-Anonymization for Fun and Profit“. In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’18. Toronto, Canada: Association for Computing Machinery, 2018, S. 115–130. ISBN: 9781450356930. DOI: 10.1145/3243734.3243770.

[162] X. Zhou u. a. „Structure based user identification across social networks“. In: *IEEE Transactions on Knowledge and Data Engineering* 30.6 (2017), S. 1178–1191.

[163] X. Zhou u. a. „An unsupervised user identification algorithm using network embedding and scalable nearest neighbour“. In: *Cluster Computing* 22.4 (2019), S. 8677–8687.

[164] T. Ma u. a. „Friend closeness based user matching cross social networks“. In: *Mathematical Biosciences and Engineering* 18.4 (2021), S. 4264–4292.

[165] J. Zhang u. a. „Two-Stage User Identification Based on User Topology Dynamic Community Clustering“. In: *Complexity* 2021 (2021).

[166] X. Liu u. a. „We Know Who You Are: Discovering Similar Groups Across Multiple Social Networks“. In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50.7 (2020), S. 2693–2704. DOI: 10.1109/TSMC.2018.2826555.

[167] J. Ma u. a. „De-anonymizing social networks with random forest classifier“. In: *IEEE Access* 6 (2017), S. 10139–10150.

[168] W. Zhang u. a. „Graph Neural Networks for User Identity Linkage“. In: *CoRR* abs/1903.02174 (2019). arXiv: 1903.02174.

[169] R. Wang u. a. „User identity linkage across social networks by heterogeneous graph attention network modeling“. In: *Applied Sciences* 10.16 (2020), S. 5478.

[170] X. Guo u. a. „User Identity Linkage Across Social Networks via Community Preserving Network Embedding“. In: *Australasian Conference on Information Security and Privacy*. Springer. 2020, S. 621–630.

[171] X. Guo u. a. „User Identity Linkage Across Social Networks Based on Neural Tensor Network“. In: *International Conference on Security and Privacy in New Computing Environments*. Springer. 2020, S. 162–171.

[172] F. Zhou u. a. „DeepLink: A Deep Learning Approach for User Identity Linkage“. In: *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 2018, S. 1313–1321. DOI: 10.1109/INFOCOM.2018.8486231.

[173] X. Li u. a. „RLINK: Deep reinforcement learning for user identity linkage“. In: *World Wide Web* 24.1 (2021), S. 85–103.

[174] Y. Zhang u. a. „A local expansion propagation algorithm for social link identification“. In: *Knowledge and Information Systems* 60.1 (2019), S. 545–568.

[175] Z. Huang, X. Li und Y. Ye. „Aligning Users Across Social Networks via Intra and Inter Attentions“. In: *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data*. Springer. 2020, S. 162–169.

[176] J. Zhang u. a. „MEgo2Vec: Embedding Matched Ego Networks for User Alignment Across Social Networks“. In: *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*. CIKM '18. Torino, Italy: Association for Computing Machinery, 2018, S. 327–336. ISBN: 9781450360142. DOI: 10.1145/3269206.3271705.

[177] S. Fu u. a. „A multi-granularity representation learning framework for user identification across social networks“. In: *International Joint Conference on Rough Sets*. Springer. 2019, S. 507–521.

[178] W. Zhao u. a. „Learning to Map Social Network Users by Unified Manifold Alignment on Hypergraph“. In: *IEEE Transactions on Neural Networks and Learning Systems* 29.12 (2018), S. 5834–5846. DOI: 10.1109/TNNLS.2018.2812888.

[179] A. Cheng u. a. „User Alignment via Structural Interaction and Propagation“. In: *2018 International Joint Conference on Neural Networks (IJCNN)*. 2018, S. 1–8. DOI: 10.1109/IJCNN.2018.8489228.

[180] L. Liu u. a. „Structural Representation Learning for User Alignment Across Social Networks“. In: *IEEE Transactions on Knowledge and Data Engineering* 32.9 (2020), S. 1824–1837. DOI: 10.1109/TKDE.2019.2911516.

[181] J. Liu u. a. „User Identification Cross Multiple Social Media Platform with Revised Input Output Network Embedding Framework“. In: *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. 2019, S. 422–426. DOI: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00086.

[182] C. Zheng, L. Pan und P. Wu. „CAMU: Cycle-Consistent Adversarial Mapping Model for User Alignment across Social Networks“. In: *IEEE Transactions on Cybernetics* (2021), S. 1–12. DOI: 10.1109/TCYB.2021.3064294.

[183] X. Li u. a. „Aligning users across social networks by joint user and label consistence representation“. In: *International Conference on Neural Information Processing*. Springer. 2019, S. 656–668.

[184] M. Wang u. a. „User Profile Linkage Across Multiple Social Platforms“. In: *International Conference on Web Information Systems Engineering*. Springer. 2020, S. 125–140.

[185] Y. Wang u. a. „User identity linkage across social networks via linked heterogeneous network embedding“. In: *World Wide Web* 22.6 (2019), S. 2611–2632.

[186] T. Zhou u. a. „Retrofitting Embeddings for Unsupervised User Identity Linkage“. In: *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer. 2020, S. 385–397.

[187] T. Iofciu u. a. „Identifying Users Across Social Tagging Systems.“ In: *ICWSM*. 2011.

[188] A. Narayanan u. a. „On the feasibility of internet-scale author identification“. In: *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE. 2012, S. 300–314.

[189] J. Novak, P. Raghavan und A. Tomkins. „Anti-aliasing on the web“. In: *Proceedings of the 13th international conference on World Wide Web*. ACM. 2004, S. 30–39.

[190] M. N. Szomszor, I. Cantador und H. Alani. „Correlating user profiles from multiple folksonomies“. In: *Proceedings of the nineteenth ACM conference on Hypertext and hypermedia*. ACM. 2008, S. 33–42.

[191] M. Almishari, E. Oguz und G. Tsudik. „Trilateral large-scale osn account linkability study“. In: *2016 AAAI Fall Symposium Series*. 2016.

[192] O. Goga. „Matching user accounts across online social networks: methods and applications“. Diss. LIP6-Laboratoire d'Informatique de Paris 6, 2014.

[193] F. Johansson, L. Kaati und A. Shrestha. „Detecting multiple aliases in social media“. In: *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. ACM. 2013, S. 1004–1011.

[194] P. Jain, P. Kumaraguru und A. Joshi. „@ i seek'fb. me': identifying users across multiple online social networks“. In: *Proceedings of the 22nd international conference on World Wide Web*. ACM. 2013, S. 1259–1268.

[195] S. Liu u. a. „Hydra: Large-scale social identity linkage via heterogeneous behavior modeling“. In: *Proceedings of the 2014 ACM SIGMOD international conference on Management of data*. ACM. 2014, S. 51–62.

[196] H. Li u. a. „Privacy leakage via de-anonymization and aggregation in heterogeneous social networks“. In: *IEEE Transactions on Dependable and Secure Computing* (2017).

[197] H. Li u. a. „Hybrid De-Anonymization across Real-World Heterogeneous Social Networks“. In: *Proceedings of the ACM Turing 50th Celebration Conference - China*. ACM TUR-C '17. Shanghai, China: Association for Computing Machinery, 2017. ISBN: 9781450348737. DOI: 10.1145/3063955.3063988.

[198] J. Ma u. a. „Balancing User Profile and Social Network Structure for Anchor Link Inferring Across Multiple Online Social Networks“. In: *IEEE Access* 5 (2017), S. 12031–12040. DOI: 10.1109/ACCESS.2017.2717921.

[199] F. Wang u. a. „Deep-Learning-based Identification of Influential Spreaders in Online Social Networks“. In: *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*. Bd. 1. 2019, S. 6854–6858. DOI: 10.1109/IECON.2019.8927419.

[200] C. Cai u. a. „Capturing Deep Dynamic Information for Mapping Users across Social Networks“. In: *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 2019, S. 146–148. DOI: 10.1109/ISI.2019.8823341.

[201] X. Cao und Y. Yu. „BASS: A Bootstrapping Approach for Aligning Heterogenous Social Networks“. In: *Machine Learning and Knowledge Discovery in Databases*. Hrsg. von P. Frasconi u. a. Cham: Springer International Publishing, 2016, S. 459–475. ISBN: 978-3-319-46128-1.

[202] Q. Liu, Y. Du und T. Lu. „User Identity Linkage Across Social Networks“. In: *International Conference on Computer Engineering and Networks*. Springer. 2018, S. 600–607.

[203] G. Quercini u. a. „Liaison: reconciliation of individuals profiles across social networks“. In: *Advances in Knowledge Discovery and Management*. Springer, 2017, S. 229–253.

[204] N. Bennacer u. a. „Matching user profiles across social networks“. In: *International Conference on Advanced Information Systems Engineering*. Springer. 2014, S. 424–438.

[205] S. Feng u. a. „User Identification across Social Networks Based on Global View Features“. In: *2017 14th Web Information Systems and Applications Conference (WISA)*. 2017, S. 93–98. DOI: 10.1109/WISA.2017.36.

[206] Z. Fang u. a. „A co-training method for identifying the same person across social networks“. In: *2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. 2017, S. 1412–1416. DOI: 10.1109/GlobalSIP.2017.8309194.

[207] W. M. Campbell u. a. „Cross-Domain Entity Resolution in Social Media“. In: *CoRR* abs/1608.01386 (2016). arXiv: 1608.01386.

[208] C. Kong, B.-X. Chen und L.-P. Zhang. „DEM: Deep Entity Matching Across Heterogeneous Information Networks“. In: *Journal of Computer Science and Technology* 35.4 (2020), S. 739–750.

[209] S. Li, W. Liang und X. Zhang. „Recognize the Same Users across Multiple Online Social Networks“. In: *International Conference on Computing and Information Technology*. Springer. 2017, S. 327–336.

[210] L. Wang u. a. „Factor Graph Model Based User Profile Matching Across Social Networks“. In: *IEEE Access* 7 (2019), S. 152429–152442. DOI: 10.1109/ACCESS.2019.2948073.

[211] F. Abel u. a. „Interweaving public user profiles on the web“. In: *User Modeling, Adaptation, and Personalization*. Springer, 2010, S. 16–27.

[212] D. Zhao u. a. „An Improved User Identification Method Across Social Networks Via Tagging Behaviors“. In: *2018 IEEE 30th International Conference on Tools with Artificial Intelligence (ICTAI)*. 2018, S. 616–622. DOI: 10.1109/ICTAI.2018.00099.

[213] S. Gu u. a. „A Novel Two-Stage Framework for User Identification Across Social Networks“. In: *2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD)*. 2019, S. 266–270. DOI: 10.1109/ICAIBD.2019.8836981.

[214] K. Deng u. a. „A User Identification Algorithm Based on User Behavior Analysis in Social Networks“. In: *IEEE Access* 7 (2019), S. 47114–47123. DOI: 10.1109/ACCESS.2019.2909089.

[215] H. Hazimeh u. a. „SocialMatching++: A Novel Approach for Interlinking User Profiles on Social Networks.“ In: *PROFILES@ ISWC*. 2017.

[216] D. Chatzakou u. a. „User Identity Linkage in Social Media Using Linguistic and Social Interaction Features“. In: *12th ACM Conference on Web Science*. WebSci ’20. Southampton, United Kingdom: Association for Computing Machinery, 2020, S. 295–304. ISBN: 9781450379892. DOI: 10.1145/3394231.3397920.

[217] A. Halimi und E. Ayday. „Efficient Quantification of Profile Matching Risk in Social Networks Using Belief Propagation“. In: *European Symposium on Research in Computer Security*. Springer. 2020, S. 110–130.

[218] D. J. Crandall u. a. „Inferring social ties from geographic coincidences“. In: *Proceedings of the National Academy of Sciences* 107.52 (2010), S. 22436–22441.

[219] O. Goga u. a. „Exploiting Innocuous Activity for Correlating Users Across Sites“. In: *Proceedings of the 22Nd International Conference on World Wide Web*. WWW ’13. Rio de Janeiro, Brazil: International World Wide Web Conferences Steering Committee, 2013, S. 447–458. ISBN: 978-1-4503-2035-1.

[220] Y. Li, Z. Zhang und Y. Peng. „A solution to tweet-based user identification across online social networks“. In: *International Conference on Advanced Data Mining and Applications*. Springer. 2017, S. 257–269.

[221] S. Isaj, N. B. Seghouani und G. Quercini. „Profile reconciliation through dynamic activities across social networks“. In: *International Conference on Advanced Information Systems Engineering*. Springer. 2019, S. 126–141.

[222] J. Shao u. a. „Locate Who You Are: Matching Geo-location to Text for Anchor Link Prediction“. In: *CoRR* abs/2104.09119 (2021). arXiv: 2104.09119.

[223] Q. Xu u. a. „Algorithm research for user trajectory matching across social media networks based on paragraph2vec“. In: *AIP Conference Proceedings*. Bd. 1955. 1. AIP Publishing LLC. 2018, S. 040056.

[224] F. Ding u. a. „User Identity Linkage across Location-Based Social Networks with Spatio-Temporal Check-in Patterns“. In: ().

[225] Y. Li u. a. „Matching User Accounts across Large-scale Social Networks based on Locality-sensitive Hashing“. In: ().

[226] F. Basik, H. Ferhatosmanoglu und B. Gedik. „SLIM: Scalable Linkage of Mobility Data“. In: *CoRR* abs/2004.05951 (2020). arXiv: 2004.05951.

[227] C. Riederer u. a. „Linking Users Across Domains with Location Data: Theory and Validation“. In: WWW ’16. Montréal, Québec, Canada: International World Wide Web Conferences Steering Committee, 2016, S. 707–719. ISBN: 9781450341431. DOI: 10.1145/2872427.2883002.

[228] W. Chen u. a. „Exploiting Spatio-Temporal User Behaviors for User Linkage“. In: *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*. New York, NY, USA: Association for Computing Machinery, 2017, S. 517–526. ISBN: 9781450349185.

[229] A. Harrington und V. Cahill. „Route profiling: putting context to work“. In: *Proceedings of the 2004 ACM symposium on Applied computing*. ACM. 2004, S. 1567–1573.

[230] F. Giannotti u. a. „Trajectory pattern mining“. In: *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 2007, S. 330–339.

[231] Y. Zheng u. a. „Learning transportation mode from raw gps data for geographic applications on the web“. In: *Proceedings of the 17th international conference on World Wide Web*. ACM. 2008, S. 247–256.

[232] K. Laasonen. „Clustering and prediction of mobile user routes from cellular data“. In: *European Conference on Principles of Data Mining and Knowledge Discovery*. Springer. 2005, S. 569–576.

[233] Y. Zheng u. a. „Mining interesting locations and travel sequences from GPS trajectories“. In: *Proceedings of the 18th international conference on World wide web*. ACM. 2009, S. 791–800.

[234] M. C. Gonzalez, C. A. Hidalgo und A.-L. Barabasi. „Understanding individual human mobility patterns“. In: *Nature* 453.7196 (2008), S. 779–782.

[235] M. Kim, D. Kotz und S. Kim. „Extracting a Mobility Model from Real User Traces.“ In: *INFOCOM*. Bd. 6. 2006, S. 1–13.

[236] S. Isaacman u. a. „Ranges of human mobility in los angeles and new york“. In: *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*. IEEE. 2011, S. 88–93.

[237] C. Song u. a. „Limits of predictability in human mobility“. In: *Science* 327.5968 (2010), S. 1018–1021.

[238] X. Xiao u. a. „Finding similar users using category-based location history“. In: *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM. 2010, S. 442–445.

[239] T. M. T. Do und D. Gatica-Perez. „The places of our lives: Visiting patterns and automatic labeling from longitudinal smartphone data“. In: *IEEE Transactions on Mobile Computing* 13.3 (2014), S. 638–648.

[240] M. A. Bayir, M. Demirbas und N. Eagle. „Discovering spatiotemporal mobility profiles of cellphone users“. In: *World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*. IEEE. 2009, S. 1–9.

[241] L. Liao u. a. „Building personal maps from GPS data“. In: *Annals of the New York Academy of Sciences* 1093.1 (2006), S. 249–265.

[242] Q. Li u. a. „Mining user similarity based on location history“. In: *Proceedings of the 16th ACM SIGSPATIAL international conference on Advances in geographic information systems*. ACM. 2008, S. 34.

[243] H. Wang u. a. „Anonymization and De-Anonymization of Mobility Trajectories: Dissecting the Gaps Between Theory and Practice“. In: *IEEE Transactions on Mobile Computing* 20.3 (2021), S. 796–815. DOI: 10.1109/TMC.2019.2952774.

[244] H. Wang u. a. „De-anonymization of mobility trajectories: Dissecting the gaps between theory and practice“. In: *The 25th Annual Network & Distributed System Security Symposium (NDSS'18)*. 2018.

[245] H. WANG u. a. „Linking Multiple User Identities of Multiple Services From Massive Mobility Traces“. In: ().

[246] J. Feng u. a. „DPLink: User Identity Linkage via Deep Neural Network From Heterogeneous Mobility Data“. In: *The World Wide Web Conference*. WWW '19. San Francisco, CA, USA: Association for Computing Machinery, 2019, S. 459–469. ISBN: 9781450366748. DOI: 10.1145/3308558.3313424.

[247] Z. Tu u. a. „A New Privacy Breach: User Trajectory Recovery From Aggregated Mobility Data“. In: *IEEE/ACM Transactions on Networking* 26.3 (2018), S. 1446–1459. DOI: 10.1109/TNET.2018.2829173.

[248] J. Feng u. a. „User Identity Linkage via Co-Attentional Neural Network From Heterogeneous Mobility Data“. In: *IEEE Transactions on Knowledge and Data Engineering* (2020), S. 1–1. DOI: 10.1109/TKDE.2020.2989732.

[249] F. Nagle und L. Singh. „Can friends be trusted? Exploring privacy in online social networks“. In: *Social Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in*. IEEE. 2009, S. 312–315.

[250] K. Rechert u. a. „User centric privacy in mobile communication scenarios“. In: *Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on*. IEEE. 2011, S. 202–207.

[251] S. Creese u. a. „A data-reachability model for elucidating privacy and security risks related to the use of online social networks“. In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE. 2012, S. 1124–1131.

[252] M. Chew, D. Balfanz und B. Laurie. „(Under) mining Privacy in Social Networks“. In: (2008).

[253] B. Krishnamurthy und C. E. Wills. „On the leakage of personally identifiable information via online social networks“. In: *Proceedings of the 2nd ACM workshop on Online social networks*. ACM. 2009, S. 7–12.

[254] M. Netter u. a. „Privacy Settings in Online Social Networks–Preferences, Perception, and Reality“. In: *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE. 2013, S. 3219–3228.

[255] B. Krishnamurthy. „Privacy and online social networks: can colorless green ideas sleep furiously?“ In: *IEEE Security & Privacy* 11.3 (2013), S. 14–20.

[256] T. Okuno u. a. „Content-based de-anonymisation of tweets“. In: *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference on*. IEEE. 2011, S. 53–56.

[257] A. Ho, A. Maiga und E. Aïmeur. „Privacy protection issues in social networking sites“. In: *2009 IEEE/ACS International Conference on Computer Systems and Applications*. IEEE. 2009, S. 271–278.

[258] L. Backstrom, C. Dwork und J. Kleinberg. „Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography“. In: *Proceedings of the 16th international conference on World Wide Web*. ACM. 2007, S. 181–190.

[259] S. Puglisi, D. Rebollo-Monedero und J. Forné. „On the anonymity risk of time-varying user profiles“. In: *Entropy* 19.5 (2017), S. 190.

[260] G. G. Gulyás und S. Imre. „Hiding information against structural re-identification“. In: *International Journal of Information Security* 18.2 (2019), S. 125–139.

[261] M. Backes u. a. „On Profile Linkability despite Anonymity in Social Media Systems“. In: *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*. WPES ’16. Vienna, Austria: Association for Computing Machinery, 2016, S. 25–35. ISBN: 9781450345699. DOI: 10.1145/2994620.2994629.

[262] X. Li u. a. „A privacy measurement framework for multiple online social networks against social identity linkage“. In: *Applied Sciences* 8.10 (2018), S. 1790.

[263] R. Kaushal u. a. „Nudging nemo: Helping users control linkability across social networks“. In: *International Conference on Social Informatics*. Springer. 2017, S. 477–490.

[264] J. Henriksen-Bulmer und S. Jeary. „Re-identification attacks—A systematic literature review“. In: *International Journal of Information Management* 36.6 (2016), S. 1184–1192.

[265] G. Beigi und H. Liu. „Privacy in Social Media: Identification, Mitigation and Applications“. In: *CoRR* abs/1808.02191 (2018). arXiv: 1808.02191.

[266] G. Beigi und H. Liu. „A Survey on Privacy in Social Media: Identification, Mitigation, and Applications“. In: *ACM/IMS Trans. Data Sci.* 1.1 (März 2020). ISSN: 2691-1922. DOI: 10.1145/3343038.

[267] S. Rathore u. a. „Social network security: Issues, challenges, threats, and solutions“. In: *Information sciences* 421 (2017), S. 43–69.

[268] M. Fiore u. a. „Privacy in trajectory micro-data publishing: a survey“. In: *arXiv preprint arXiv:1903.12211* (2019).

[269] J. Krumm. „A survey of computational location privacy“. In: *Personal and Ubiquitous Computing* 13.6 (2009), S. 391–399.

[270] M. Srivatsa und M. Hicks. „Deanonymizing mobility traces: Using social network as a side-channel“. In: *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM. 2012, S. 628–637.

[271] B. Hoh u. a. „Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking“. In: *IEEE Transactions on Mobile Computing* 9.8 (2010), S. 1089–1107.

[272] B. Hoh u. a. „Preserving privacy in gps traces via uncertainty-aware path cloaking“. In: *Proceedings of the 14th ACM conference on Computer and communications security*. ACM. 2007, S. 161–171.

[273] K. Drakonakis u. a. „Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data“. In: *CoRR* abs/1901.00897 (2019). arXiv: 1901.00897.

[274] C. Bettini, X. S. Wang und S. Jajodia. „Protecting privacy against location-based personal identification“. In: *Workshop on Secure Data Management*. Springer. 2005, S. 185–199.

[275] K. Rechert u. a. „Reclaiming location privacy in mobile telephony networks—effects and consequences for providers and subscribers“. In: *IEEE Systems Journal* 7.2 (2013), S. 211–222.

[276] T. Pontes u. a. „We know where you live: privacy characterization of foursquare behavior“. In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM. 2012, S. 898–905.

[277] C. R. Vicente u. a. „Location-related privacy in geo-social networks“. In: *IEEE Internet Computing* 15.3 (2011), S. 20–27.

[278] G. Friedland und R. Sommer. „Cybercasing the Joint: On the Privacy Implications of Geo-Tagging.“ In: *HotSec*. 2010.

[279] T. Pontes u. a. „Beware of what you share: Inferring home location in social networks“. In: *2012 IEEE 12th International Conference on Data Mining Workshops*. IEEE. 2012, S. 571–578.

[280] M. Riesner und G. Pernul. „Provider-Independent Online Social Identity Management–Enhancing Privacy Consistently Across Multiple Social Networking Sites“. In: *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE. 2012, S. 800–809.

[281] E. Lalas, A. Papathanasiou und C. Lambrinoudakis. „Privacy and traceability in social networking sites“. In: *Informatics (PCI), 2012 16th Panhellenic Conference on*. IEEE. 2012, S. 127–132.

[282] G. G. Gulyás und S. Imre. „Using identity separation against de-anonymization of social networks“. In: *Trans Data Privacy (TDP)* 8.2 (2015), S. 113–140.

[283] M. Balduzzi u. a. „Abusing social networks for automated user profiling“. In: *International Workshop on Recent Advances in Intrusion Detection*. Springer. 2010, S. 422–441.

[284] E. Aimeur, S. Gambs und A. Ho. „Towards a privacy-enhanced social networking site“. In: *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE. 2010, S. 172–179.

[285] T. Stein, E. Chen und K. Mangla. „Facebook immune system“. In: *Proceedings of the 4th Workshop on Social Network Systems*. ACM. 2011, S. 8.

[286] M. Fire u. a. „Friend or foe? Fake profile identification in online social networks“. In: *Social Network Analysis and Mining* 4.1 (2014), S. 1–23.

[287] M. Conti, R. Poovendran und M. Secchiero. „FakeBook: detecting fake profiles in online social networks“. In: *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*. IEEE Computer Society. 2012, S. 1071–1078.

[288] G. Kolaczek. „An Approach to Identity Theft Detection Using Social Network Analysis“. In: *Intelligent Information and Database Systems, 2009. ACIIDS 2009. First Asian Conference on*. IEEE. 2009, S. 78–81.

[289] C. Perez u. a. „Spot 1.0: Scoring suspicious profiles on twitter“. In: *Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on*. IEEE. 2011, S. 377–381.

[290] C. Perez, M. Lemercier und B. Birregah. „A dynamic approach to detecting suspicious profiles on social platforms“. In: *2013 IEEE International Conference on Communications Workshops (ICC)*. IEEE. 2013, S. 174–178.

[291] G. Kontaxis u. a. „Detecting social network profile cloning“. In: *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*. IEEE. 2011, S. 295–300.

[292] M. R. Khayyambashi und F. S. Rizi. „An approach for detecting profile cloning in online social networks“. In: *e-Commerce in Developing Countries: With Focus on e-Security (ECDC), 2013 7th Intenational Conference on*. IEEE. 2013, S. 1–12.

[293] S. P. Velayudhan und M. S. B. Somasundaram. „Compromised account detection in online social networks: A survey“. In: *Concurrency and Computation: Practice and Experience* 31.20 (2019). e5346 cpe.5346, e5346. DOI: `https://doi.org/10.1002/cpe.5346`. eprint: `https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.5346`.

[294] M. Fire, R. Goldschmidt und Y. Elovici. „Online social networks: threats and solutions“. In: *IEEE Communications Surveys & Tutorials* 16.4 (2014), S. 2019–2036.

[295] L. Bilge u. a. „All your contacts are belong to us: automated identity theft attacks on social networks“. In: *Proceedings of the 18th international conference on World wide web*. ACM. 2009, S. 551–560.

[296] M. Apte, G. K. Palshikar und S. Baskaran. „Frauds in online social networks: A review“. In: *Social networks and surveillance for society* (2019), S. 1–18.

[297] S. R. Sahoo und B. B. Gupta. „Classification of various attacks and their defence mechanism in online social networks: a survey“. In: *Enterprise Information Systems* 13.6 (2019), S. 832–864.

[298] T. Lauinger u. a. „Honeybot, Your Man in the Middle for Automated Social Engineering.“ In: *LEET*. 2010.

[299] M. Huber u. a. „Towards automating social engineering using social networking sites“. In: *Computational Science and Engineering, 2009. CSE'09. International Conference on*. Bd. 3. IEEE. 2009, S. 117–124.

[300] A. Algarni, Y. Xu und T. Chan. „Social engineering in social networking sites: the art of impersonation“. In: *Services Computing (SCC), 2014 IEEE International Conference on*. IEEE. 2014, S. 797–804.

[301] D. Irani u. a. „Reverse social engineering attacks in online social networks“. In: *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer. 2011, S. 55–74.

[302] Y. Boshmaf u. a. „The socialbot network: when bots socialize for fame and money“. In: *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM. 2011, S. 93–102.

[303] C. Grier u. a. „@ spam: the underground on 140 characters or less“. In: *Proceedings of the 17th ACM conference on Computer and communications security*. ACM. 2010, S. 27–37.

[304] M. Bosma, E. Meij und W. Weerkamp. „A framework for unsupervised spam detection in social networking sites“. In: *European Conference on Information Retrieval*. Springer. 2012, S. 364–375.

[305] M. Fire, G. Katz und Y. Elovici. „Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies“. In: *Human Journal* 1.1 (2012), S. 26–39.

[306] B Sharmila und A Soumya. „SOCIAL NETWORKS FOR SPAMMER DETECTION AND RECOGNITION OF FAKE USERS“. In: ().

[307] K. Thomas u. a. „Suspended Accounts in Retrospect: An Analysis of Twitter Spam“. In: *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*. IMC ’11. Berlin, Germany, 2011, S. 243–258.

[308] M. McCord und M. Chuah. „Spam Detection on Twitter Using Traditional Classifiers“. In: *Autonomic and Trusted Computing: 8th International Conference, ATC 2011, Banff, Canada, September 2-4, 2011. Proceedings*. Hrsg. von J. M. A. Calero u. a. Berlin, Heidelberg, 2011, S. 175–186.

[309] K. Thomas u. a. „Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse“. In: *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. 2013, S. 195–210.

[310] M. Mohammadrezaei, M. E. Shiri und A. M. Rahmani. „Identifying fake accounts on social networks based on graph analysis and classification algorithms“. In: *Security and Communication Networks* 2018 (2018).

[311] M. S. Raja und L. A. Raj. „Detection of Malicious Profiles and Protecting Users in Online Social Networks“. In: *Wireless Personal Communications* (2021), S. 1–18.

[312] D. Ramalingam und V. Chinnaiah. „Fake profile detection techniques in large-scale online social networks: A comprehensive review“. In: *Computers & Electrical Engineering* 65 (2018), S. 165–177.

[313] P. K. Roy und S. Chahar. „Fake Profile Detection on Social Networking Websites: A Comprehensive Review“. In: *IEEE Transactions on Artificial Intelligence* 1.3 (2020), S. 271–285. DOI: 10.1109/TAI.2021.3064901.

[314] F. Masood u. a. „Spammer Detection and Fake User Identification on Social Networks“. In: *IEEE Access* 7 (2019), S. 68140–68152. DOI: 10.1109/ACCESS.2019.2918196.

[315] N. M. Radziwill und M. C. Benton. „Bot or Not? Deciphering Time Maps for Tweet Interarrivals“. In: *arXiv preprint arXiv:1605.06555* (2016).

[316] C. M. Zhang und V. Paxson. „Detecting and analyzing automated activity on twitter“. In: *Passive and Active Measurement*. Springer. 2011, S. 102–111.

[317] S. Webb, J. Caverlee und C. Pu. „Social Honeypots: Making Friends With A Spammer Near You.“ In: *CEAS*. 2008.

[318] K. Lee, J. Caverlee und S. Webb. „Uncovering social spammers: social honeypots + machine learning“. In: *Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval*. ACM. 2010, S. 435–442.

[319] G. Stringhini, C. Kruegel und G. Vigna. „Detecting spammers on social networks“. In: *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM. 2010, S. 1–9.

[320] S. S. Sengar u. a. „Bot Detection in Social Networks Based on Multilayered Deep Learning Approach“. In: *Sensors & Transducers* 244.5 (2020), S. 37–43.

[321] N. Chavoshi, H. Hamooni und A. Mueen. „Identifying correlated bots in twitter“. In: *International conference on social informatics*. Springer. 2016, S. 14–21.

[322] N. Chavoshi, H. Hamooni und A. Mueen. „On-Demand Bot Detection and Archival System“. In: *Proceedings of the 26th International Conference on World Wide Web Companion*. WWW ’17 Companion. Perth, Australia: International World Wide Web Conferences Steering Committee, 2017, S. 183–187. ISBN: 9781450349147. DOI: 10.1145/3041021.3054733.

[323] N. Chavoshi. „Mining Temporal Activity Patterns On Social Media“. In: (2018).

[324] ITWissen.info. *Metamodell :: meta model :: ITWissen.info:* URL: http://www.itwissen.info/definition/lexikon/Metamodell-meta-model.html (abgerufen am 18. 12. 2016).

[325] A. Bozzon u. a. „Choosing the right crowd: expert finding in social networks“. In: *Proceedings of the 16th International Conference on Extending Database Technology*. ACM. 2013, S. 637–648.

[326] D. Kergl, R. Roedler und S. Seeber. „On the endogenesis of Twitter’s Spritzer and Gardenhose sample streams“. In: *Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on*. IEEE. 2014, S. 357–364.

[327] R. Roedler, D. Kergl und G. D. Rodosek. „Content Driven Profile Matching Across Online Social Networks“. In: *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*. ASONAM ’17. Sydney, Australia: ACM, 2017, S. 1049–1055. ISBN: 978-1-4503-4993-2. DOI: 10.1145/3110025.3110095.

[328] I. ISO. „8601: 2004“. In: *Data elements and interchange formats–Information interchange–Representation of dates and times* 3 (2004).

[329] N. G.-I. Agency. *World Geodetic System:* URL: https://www.nga.mil/ProductsServices/GeodesyandGeophysics/Pages/WorldGeodeticSystem.aspx (abgerufen am 20. 12. 2016).

[330] N Imagery. *M. Agency,"Department of defense world geodetic system 1984, its definition and relationships with local geodetic systems," Department of Defense World Geodetic System 1984, Its Definition and Relationships With Local Geodetic Systems, vol*. Techn. Ber. NIMA Technical Report TR8350. 2, 2000.

[331] YouTube. *Press room - YouTube:* URL: https://www.youtube.com/yt/press/ (abgerufen am 06. 03. 2017).

[332] C. I. Watch. *WeChat MAUs grew to 846 million in Q3 2016*. URL: https://www.chinainternetwatch.com/19277/tencent-q3-2016/ (abgerufen am 06. 03. 2017).

[333] S. Kemp. *Digital in 2017 Global Overview*. URL: https://de.slideshare.net/wearesocialsg/digital-in-2017-global-overview (abgerufen am 07. 03. 2017).

[334] C. I. Watch. *Baidu Tieba News & Insights*. URL: https://www.chinainternetwatch.com/tag/baidu-tieba/ (abgerufen am 07. 03. 2017).

[335] C. I. Watch. *Weibo Performance Overview in Q3 2016*. URL: https://www.chinainternetwatch.com/19275/weibo-q3-2016/ (abgerufen am 07. 03. 2017).

[336] B. Silbermann. *150 million people finding ideas on Pinterest | Pinterest Blog:* URL: https://blog.pinterest.com/en/150-million-people-finding-ideas-pinterest (abgerufen am 07. 03. 2017).

[337] Y. Inc. *YY Reports Second Quarter 2016 Unaudited Financial Results*. URL: https://globenewswire.com/news-release/2016/08/17/864987/0/en/YY-Reports-Second-Quarter-2016-Unaudited-Financial-Results.html (abgerufen am 07. 03. 2017).

[338] S. Denning. *Has Google+ Really Died?* URL: https://www.forbes.com/sites/stevedenning/2015/04/23/has-google-really-died/#718c0f31466c (abgerufen am 07. 03. 2017).

[339] L. C. C. Team. *LinkedIn Announces Third Quarter 2016 Results:* URL: https://press.linkedin.com/site-resources/news-releases/2016/linkedin-announces-third-quarter-2016-results (abgerufen am 07. 03. 2017).

[340] E. Kühl. *Google+ schließt langsam den Sargdeckel*. URL: http://www.zeit.de/digital/internet/2015-07/google-plus-youtube-pflicht-ende (abgerufen am 18. 11. 2017).

[341] B. Smith. *Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+*. URL: https://www.blog.google/technology/safety-security/project-strobe/ (abgerufen am 11. 03. 2020).

[342] A. Rosen. *Tweeting Made Easier*. URL: https://blog.twitter.com/official/en_us/topics/product/2017/tweetingmadeeasier.html (abgerufen am 18. 11. 2017).

[343] S. Meredith. *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. URL: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html (abgerufen am 12. 07. 2021).

[344] I. Engineering. *Sharding & IDs at Instagram*. URL: http://instagram-engineering.tumblr.com/post/10853187575/sharding-ids-at-instagram (abgerufen am 24. 03. 2017).

[345] IFTTT. *IFTTT helps your apps and devices work together - IFTTT*. URL: https://ifttt.com/ (abgerufen am 09. 12. 2017).

[346] M. M. C. for Internet Research der Bayerischen Akademie der Wissenschaften. *Munich Bot Challenge*. URL: http://mcir.digital/munich-bot-challenge/ (abgerufen am 03. 01. 2018).

[347] Twitter. *TweetDeck*. URL: https://tweetdeck.twitter.com/ (abgerufen am 19. 05. 2021).

[348] T. Economist. *What's in a tweet*. URL: https://www.economist.com/graphic-detail/2011/09/29/whats-in-a-tweet (abgerufen am 15. 07. 2021).

ANHANG A

Anhang

Nachfolgend sind ergänzende Informationen zu konkreten Sachverhalten einzelner Abschnitte zu finden.

A.1. Verfügbare Metadaten bei Twitter

Die Grafik A.1 zeigt den Aufbau eines Tweets, wie er früher von Twitter zur Verfügung gestellt wurde, siehe auch [348]. Der Aufbau ist inzwischen nicht mehr aktuell, allerdings haben sich vorwiegend die Struktur, Reihenfolge und die Formatierung der unterschiedlichen Daten geändert. Daher gibt diese Grafik einen guten Überblick über die Art und Menge der darin enthaltenen Metadaten.

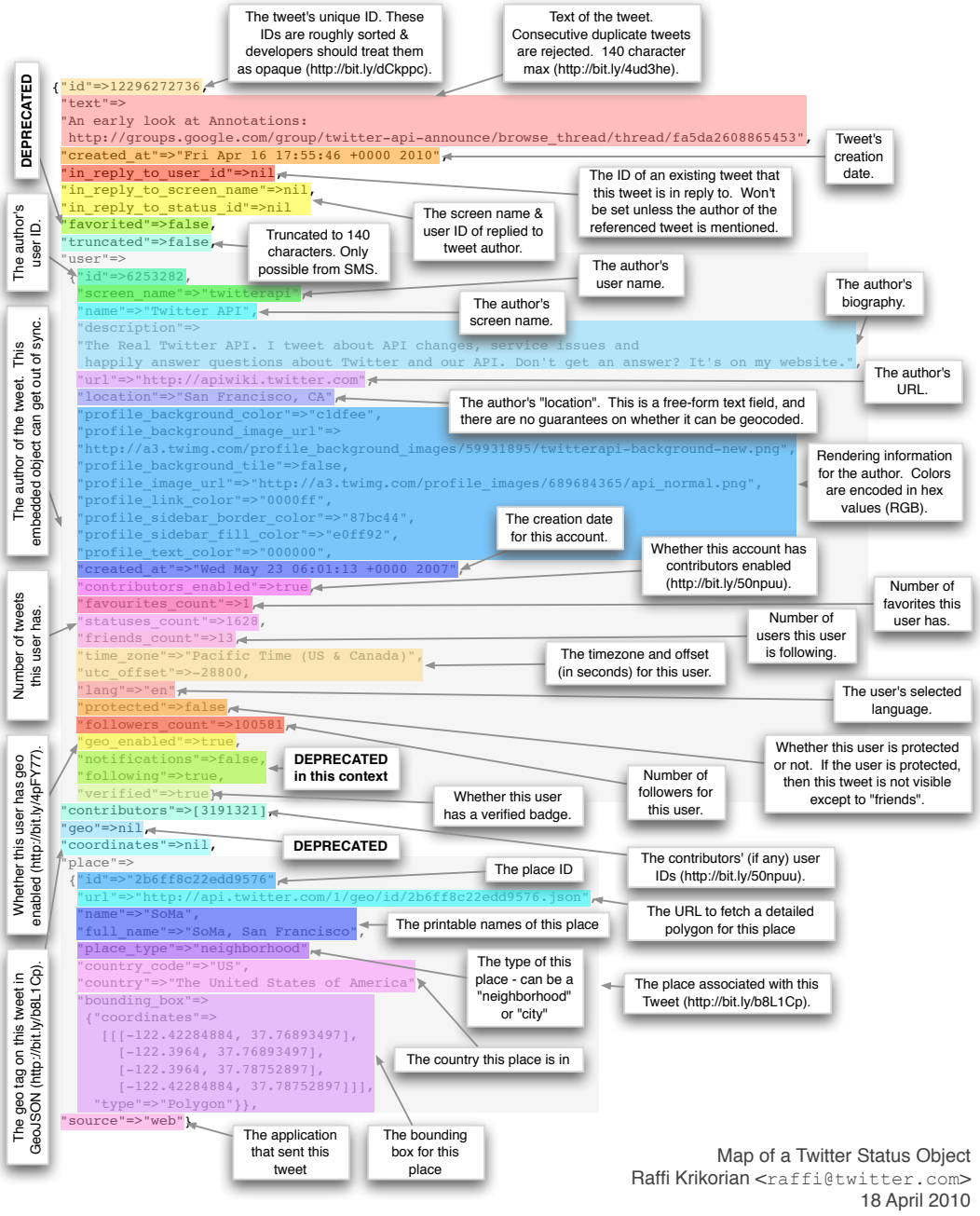
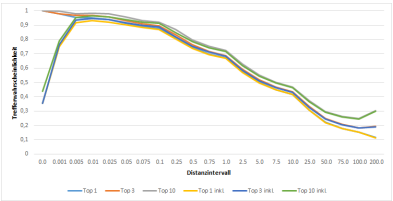


Abbildung A.1.: Metadaten eines Tweets

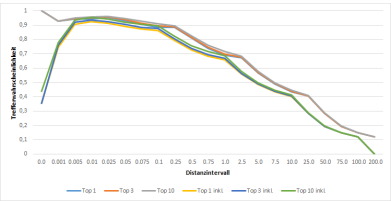
A.2. Ergänzende Diagramme der Geotag-weisen Auswertung

In diesem Abschnitt sind ergänzende Diagramme der geobasierten Profilzuordnung ohne weitere Erklärung aufgeführt. Auf diese wird an geeigneter Stelle im entsprechenden Kapitel verwiesen.

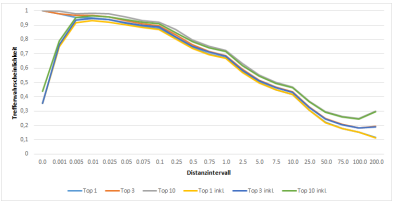
A.2.1. Ergebnisse der einzelnen Metriken



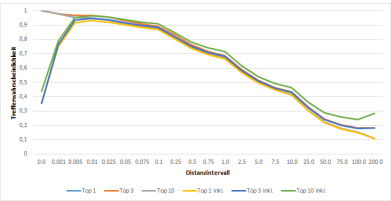
(a)



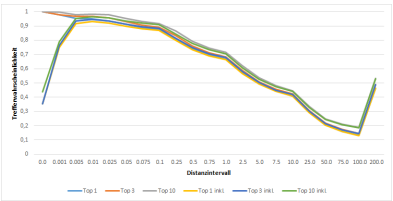
(b)



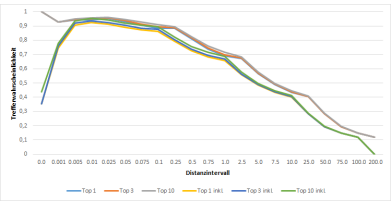
(c)



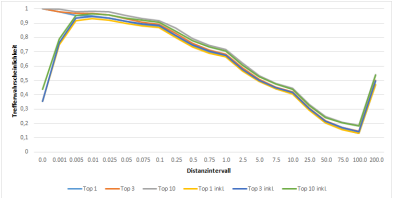
(d)



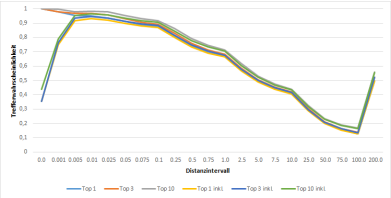
(e)



(f)



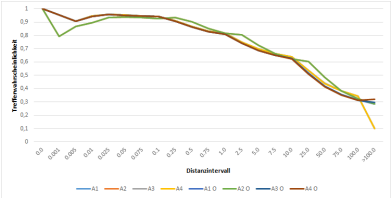
(g)



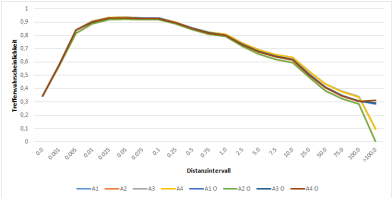
(h)

Abbildung A.2.: Ergebnisse der Geotag-weisen Auswertung für alle Profile mit Top 1, Top 3, Top 10 und Top 1, Top 3 und Top 10 inklusive gleich bewerteter Treffer. a) A1, b) A2, c) A3, d) A4, e) A1 O, f) A2 O, g) A3 O und h) A4 O

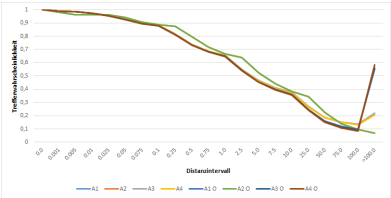
A.2.2. Top-3-Trefferliste



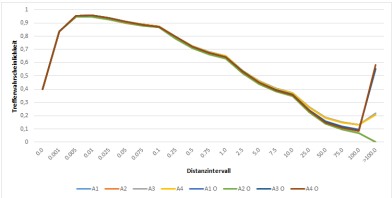
(a)



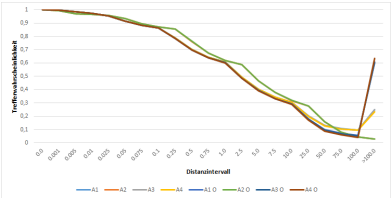
(b)



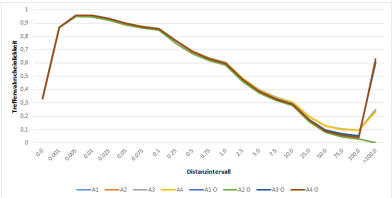
(c)



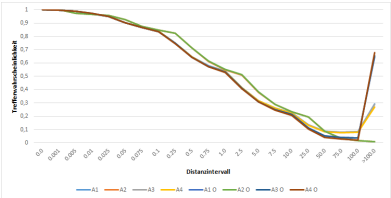
(d)



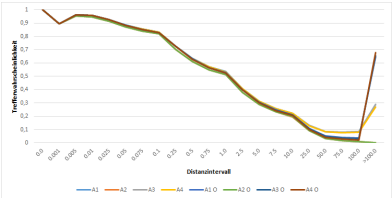
(e)



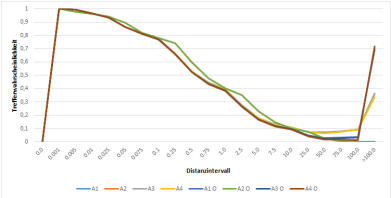
(f)



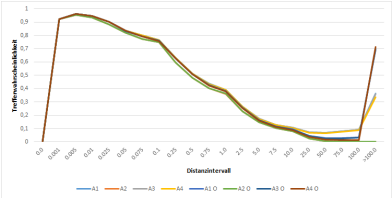
(g)



(h)



(i)



(j)

Abbildung A.3.: Ergebnisse der Geotag-weisen Auswertung für Profile mit weniger als 25 (a+b) mind. 25 (c+d), 50 (e+f), 100 (g+h) und 250 (i+j) Profilen und Treffer unter den Top Drei (links) und inklusive gleich bewerteter Treffer (rechts).

A.3. Veröffentlichungen im Rahmen dieser Dissertation

Im Rahmen dieser Arbeit sind mehrere Veröffentlichungen entstanden, welche nachfolgend aufgelistet sind:

- **On the endogenesis of Twitter's Spritzer and Gardenhose sample streams**
  D Kergl, R Roedler, S Seeber
  2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)
- **Profile Matching Across Online Social Networks Based on Geo-Tags**
  R Roedler, D Kergl, GD Rodosek
  Advances in Nature and Biologically Inspired Computing
- **Detection of Zero Day Exploits Using Real-Time Social Media Streams**
  D Kergl, R Roedler, GD Rodosek
  Advances in Nature and Biologically Inspired Computing
- **Content driven profile matching across online social networks**
  R Roedler, D Kergl, GD Rodosek
  Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017
- **Towards internet scale quality-of-experience measurement with twitter**
  D Kergl, R Roedler, GD Rodosek
  IFIP International Conference on Autonomous Infrastructure, Management and Security
- **VulMap: Global information security vulnerabilities IEEE CNS 17 poster**
  D Kergl, R Roedler, GD Rodosek
  2017 IEEE Conference on Communications and Network Security (CNS)