

Privatheit durch Manipulation der Datenqualität

Alexander Delp
AlexanderDelp@gmx.net

Übersicht. Immer neue Möglichkeiten der personalisierten Datensammlung machen es erforderlich, die Privatsphäre des Einzelnen speziell in der IT-Welt zu schützen. Im Rahmen des Seminars „Informationsverwaltung in Sensornetzwerken“ befasst sich diese Arbeit mit verschiedenen Ansätzen, Privatheit durch Manipulation der Datenqualität zu gewährleisten. Dabei soll sowohl auf zufallsbasierte Verfahren, als auch auf strategisch vorgehende Verfahren eingegangen werden, deren Vor- und Nachteile gezeigt und gegenüber gestellt werden.

Schlüsselwörter: Privatheit, Privatsphäre, Datenschutz

1 Einführung

Sowohl Verbesserungen im Bereich etablierter Technologien (wie zum Beispiel die Integration von WLAN-Adaptoren in immer kleinere Geräte), als auch die – zum Teil aus den Verbesserungen resultierende – Entwicklung neuer Technologien (wie zum Beispiel „Ambient Intelligence“ [1] oder „location-based Services“ [2]) erhöhen die Menge und Genauigkeit der messbaren, personalisierten Attribute der realen Welt. Dies ermöglicht einen steigenden Grad an Komfort und Sicherheit. Das Erkennen von Handlungsabsichten einer Person in einem Raum oder möglichen Gefahrensituationen beim Steuern eines Fahrzeuges und die automatische Reaktion von Computersystemen darauf sind hier nur zwei denkbare Beispiele.

Neben diesen gewünschten Effekten bergen die immer größer werdenden Fähigkeiten, personalisierte Daten zu sammeln, auch Gefahren für den Einzelnen durch fortschreitendes Eindringen Dritter in seine Privatsphäre: Das Erstellen von Bewegungs-, Verhaltens- und Besitzprofilen wird mit den ansteigenden Datenmengen immer einfacher und genauer.

Im so genannten Volkszählungsurteil leitet das Bundesverfassungsgericht ein „Recht auf informationelle Selbstbestimmung“, definiert als die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“, aus dem allgemeinen Persönlichkeitsrecht und der Unantastbarkeit der menschlichen Würde ab [3]. Auch die Vereinten Nationen erklären den „willkürlichen Eingriff in die Privatsphäre“ als menschenunwürdig [4]. Die Forderung nach dem Schutz der Privatsphäre ist somit keine unbegründete Erscheinung, sondern hat, neben der Wahrung der persönlichen Bedürfnisse des Einzelnen, auch eine starke rechtliche Verankerung.

Aufgrund der Dringlichkeit im Bereich des Schutzes der Privatsphäre gibt es einige Ansätze, die Privatsphäre zu schützen bei der gleichzeitig weiterhin bestehenden Möglichkeit, personenbezogene Daten zu erheben und zu verarbeiten. Viele dieser

Ansätze lassen sich mit dem Begriff „Zufallsverfahren“ überschreiben, da sie versuchen, durch zufälliges Verändern der Ausgangsdaten das Erkennen von Mustern durch geeignete Verfahren zu ermöglichen, aber die genauen Ausgangsdaten zu verschleiern [5]. Die Hauptprobleme liegen hier in der beschränkten Nutzbarkeit der resultierenden Daten oder der Möglichkeit, durch mathematische Verfahren die Ausgangsdaten erheblich anzunähern [6, 7]. Die zweite Art der hier vorgestellten Verfahren versucht, die Daten durch Erzeugung von Klassen auf den Wertebereichen der Attribute zu entpersonalisieren [8, 9].

Zunächst werden genauere Beispiele für erhobene personalisierte Daten und den daraus resultierenden Gefahren für den Einzelnen gegeben, um die Dringlichkeit dieser Betrachtungen zu verdeutlichen. Drei in dieser Arbeit relevante Begriffe werden in Kapitel 3 eingeführt. Kapitel 4 befasst sich dann mit der Vorstellung der hier behandelten Verfahren und der kritischen Hinterfragung ihrer Einsetzbarkeit. Kapitel 5 beschließt diese Arbeit mit einer Zusammenfassung und einem Blick auf mögliche Folgearbeiten.

2 Aktuelle Beispiele

Nicht nur explizit werden persönliche Daten von ihrem Besitzer zur Speicherung und Verarbeitung freigegeben. Im alltäglichen Leben werden zum Beispiel durch Kamerasysteme oder Datenweitergabe von Unternehmen ohne die Unterrichtung des Besitzers Daten erhoben und verarbeitet.

2.1 Toll Collect

Das Sensornetz des Toll Collect Systems des gleichnamigen Unternehmens Toll Collect, das am 01.01.2005 für die stichprobenartige Überwachung der LKW Maut auf Deutschen Autobahnen nach lang anhaltenden anfänglichen technischen Schwierigkeiten eingeführt wurde, besteht aus TollCheckern des Unternehmens VITRONIC und etwa 300 mobilen Teams. In etwa 300 dieser TollChecker sind auf Deutschen Autobahnen in Mautkontrollbrücken im Einsatz (Abbildung 1). Das System arbeitet dabei im fließenden mehrspurigen Autobahnverkehr und erlaubt unter anderem die Klassifizierung passierender Fahrzeuge nach Größe und Vorhandensein von Anhängern, als auch die automatische Kennzeichenerkennung nationaler und internationaler Nummernschilder [10].

Der in dieser Betrachtung relevante Teil ist dabei das Kamerasystem, das in den TollCheckern integriert ist. Bei einer aktiven Mautkontrollbrücke nimmt es von jedem passierenden Fahrzeug – sowohl LKW als auch PKW – zunächst ein Foto auf und führt eine Klassifizierung des Fahrzeugs durch.

Die gesetzlichen Grundlagen des Toll Collect Systems schreiben vor, dass pro Jahr nur 10 Millionen Stichproben genommen werden dürfen und, dass ausschließlich Daten von mautpflichtigen Fahrzeugen gespeichert und nur für die Nutzung in diesem Bereich verwendet werden dürfen: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig.“ [11].

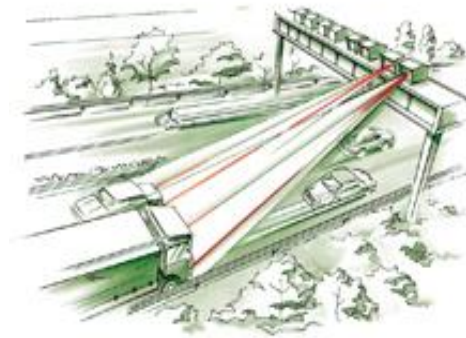


Abbildung 1: Skizze einer Mautkontrollbrücke mit TollChecker im fließenden mehrspurigen Autobahnverkehr.

Als Reaktion auf die Fahndung im Fall des Mordes an der Schülerin Anna S. im Juli 2006 wurde in der Politik „eine Nutzung der Mautdaten zur Strafverfolgung in eng definierten Einzelfällen, beschränkt auf schwere Straftaten“ [12] für die Polizei diskutiert. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar verneint zwar die Zustimmung zu einer zusätzlichen Speicherung der erhobenen Mautdaten, um eine solche Nutzung zur Strafverfolgung jedoch sinnvoll zu machen, müsste das Gesetz dahingehend geändert werden, dass alle Mautkontrollbrücken permanent jedes Fahrzeug aufnehmen und diese Fotos mit Zusatzdaten wie Wagentyp, Nummernschild, Zeitpunkt und vielleicht sogar Personalien der Insassen auf Vorrat für nicht mautspezifische Zwecke speichern dürfen.

Abgesehen davon, dass dieser Einsatz des Systems in den ursprünglichen Gesetzesformulierungen explizit ausgeschlossen wurde, würden sich dann für jeden, der auf einer Deutschen Autobahn verkehrt, zwei Datenschutzprobleme stellen: Das Speichern von Daten auf Vorrat entspricht dem Kritikpunkt von Datenschützern, dass jeder zunächst als potentieller Täter gilt und nicht nur Daten von verdächtigen Personen erhoben werden. Das zweite Problem liegt in der Tatsache an sich, dass das Gesetz geändert werden muss, um die erhobenen Daten für weitere Zwecke zugänglich zu machen. Wo ist die Grenze dieser Lockerung? Denkbar wäre auch eine Nutzung der Daten für das Finanzamt, das Sozialamt, Unternehmen der Automobilbranche (für Werbezwecke) oder beliebige weitere Institutionen.

2.2 Anti-Terror-Kampf

Ein weiterer akuter Brennpunkt für den Schutz der Privatsphäre bei der Erhebung von Daten besteht seit dem Anschlag auf das World Trade Center am 11.09.2001. Der internationale Kampf gegen den Terrorismus hat viele Staaten (zum Beispiel die USA unter dem Begriff der „Total Awareness“ und Deutschland mit dem Anstreben einer „Anti-Terror-Datei“) dazu veranlasst, eine große Menge an Daten zu sammeln (Daten aus der Finanzwelt, dem Gesundheitswesen und der Kommunikation sind hier nur ein

paar Beispiele [7]), um möglichst früh terroristische Anschläge vorhersehen und verhindern zu können. Auch hier ist das Speichern der Daten auf Vorrat ein wichtiger Bestandteil des Vorgehens.

So haben die USA seit dem Anschlag Zugriff auf die Daten des Unternehmens SWIFT, das weltweit für über 7800 Finanzunternehmen die Transaktionsübermittlung abwickelt. Auch die Passagierdatensätze von Flugunternehmen, welche persönliche Daten über den Passagier, seine Firma und das Flugunternehmen beinhalten, sind den USA frei zugänglich. Diese Zugriffsmöglichkeiten wurden den USA ohne richterlichen Beschluss von den beteiligten Unternehmen freiwillig gewährt. Eine konkrete offizielle Reaktion der Europäischen Union erfolgte jeweils erst sehr spät: In einer Entscheidung vom 30.05.2006 hat der Europäische Gerichtshof festgestellt, dass keine Zuständigkeit der EU-Kommission im Bereich der Passagierdatensätze besteht. Die Überwachung der SWIFT Datensätze durch die USA wurde in einer Resolution vom 06.07.2006 vom EU-Parlament verurteilt [16].

2.3 Auswirkungen im Alltag

In unserem Alltag sind schon heute eine große Zahl an Sensornetzen integriert, die viele personenbezogene Daten sammeln können, aber bewusst nicht als solche wahrgenommen werden. Mit dem Fortschreiten der technologischen Möglichkeiten werden diese Netze immer zahlreicher und größer und deren Möglichkeiten umfassender (wie man an den bereits erwähnten Technologien der „Ambient Intelligence“ und der „location-based Services“ sehen kann).

Das Sammeln von Daten über Personen beginnt bei einfachen Technologien wie eMail-Minern oder Kundenkarten. Verbreitete Systeme wie die Sicherheitsüberwachung von Parkhäusern und Supermärkten stellen flächendeckende optische Sensornetze dar und auch jeder Bankautomat hat eine integrierte Kamera. Theoretisch besteht bei all diesen Technologien die Möglichkeit der Personenerkennung. Jedes Gerät, das über eine kabellose Verbindung verfügt, gibt zu jedem eingewählten Zeitpunkt seine Position preis: Ein Handy den Mast, ein WLAN-Adapter den Hotspot, an dem es/er angemeldet ist.

Mit diesen zwei allgegenwärtigen Arten an Sensornetzwerken ist nun bereits eine Personenerkennung und -verfolgung (durch konsekutive Messung des Standortes – Abbildung 2) möglich, ohne dass die betroffene Person darüber unterrichtet werden würde oder sich darüber wirklich im Klaren wäre. Auch die Erkennung von Besitz über RFID-Chips, Kaufverhalten eines Kunden oder andere Wege kann für den Besitzer Nachteile mit sich bringen. Diese können sich in großen Mengen an unerwünschter Werbung äußern, negative Auswirkungen bei Einstellungsgesprächen oder auf öffentlichen Ämtern (wenn persönliche Daten über den Besitz, das Verhalten oder auch die Erkrankungsgeschichte einer Person ohne Weiteres in Erfahrung gebracht werden können) sein, oder bis hin zu der Gefahr, ein leichtes Opfer für Straftaten zu werden (über Besitz-, Verhaltens- und Bewegungsprofile), reichen.



Abbildung 2: Beispiel einer Personenverfolgung mittels konsekutiver Messung des Standortes.

Zu diesen sehr allgemeinen kommen immer mehr spezielle Netze und Technologien, wie zum Beispiel „Body Area Networks“, „Ambient Intelligence“ oder der „Smart Kindergarten“, die personalisierte Daten aus immer mehr Bereichen sammeln können.

Generell ist es möglich, Wissen über eine Person zur Machtausübung über sie zu missbrauchen. Je mehr Informationen über eine Person verfügbar sind, um so genauer kann eine unerwünschte Bewertung oder sogar Verhaltensvorhersage dieser durch Dritte erfolgen.

Nimmt man nun diese ganzen Nachteile, die man durch (freiwillige oder unfreiwillige) Freigabe persönlicher Daten in Kauf nimmt, auf die eine Seite und die Vorteile der dadurch realisierten Dienste und Technologien, die durch kontextsensitive System im Bereich des Komforts und durch frühzeitige Verbrechens- und Unglückserkennung im Bereich der Sicherheit liegen, auf die andere, so wird der Trade-Off deutlich, den man bei dieser Problematik eingehen muss: Werden keine Daten freigegeben, so muss man auf viel(e) Dienste, Komfort und Sicherheit verzichten. Werden wiederum 'zu viele' Daten freigegeben, so liefert man sich unerwünschten bis gefährlichen Situationen aus.

3 Begriffseinführungen

Im Folgenden werden drei Begriffe eingeführt, die für das Verständnis der Verfahrensbehandlung im darauf folgenden Kapitel relevant sind: „Datengranularität“, „k-Anonymität“ und „location-based Services“.

3.1 Datengranularität

Die Datengranularität knüpft direkt an den in 2.3 erarbeiteten Trade-Off an. Daten sollten immer genau in der Granularität freigegeben werden, wie sie den gewünschten Dienst gerade noch ermöglichen. Der Wahlspruch lautet hier: „So wenig wie möglich, so viel wie nötig.“.

Ein Dating-Service benötigt von der Adresse seiner Kunden nur den Stadtnamen um seinen Dienst korrekt erbringen zu können. Eine Angabe der Straße wäre nicht zweckmäßig. Für ein Taxiunternehmen reicht eine Straßenecke aus, ein Lieferdienst sollte die vollständige Hausanschrift zur Verfügung haben, da eine Lieferung sonst nur mit Mehraufwand möglich wäre.

Eine Sonderstellung nimmt hier – wie in anderen Gebieten des Datenschutzes auch – ein Notfall ein. Der Wunsch nach Datenschutz tritt zunächst in den Hintergrund, da die Gesundheit (oder das Leben an sich) einen größeren Wert als die Wahrung der Privatsphäre darstellt. Stürzt eine Person in ihrem Haus und bleibt danach regungslos liegen (was zum Beispiel durch Sensoren im Teppich festgestellt werden könnte), so wäre eine Übermittlung von zusätzlichen Daten an einen Notarzt, wie dem Stockwerk und der genauen Wohnung, durchaus sinnvoll.

Abbildung 3 zeigt für dieses Beispiel die Datengranularität von Adressdaten für verschiedene Dienste. Sie genügt der Forderung des obigen Wahlspruchs „So wenig wie möglich, so viel wie nötig.“

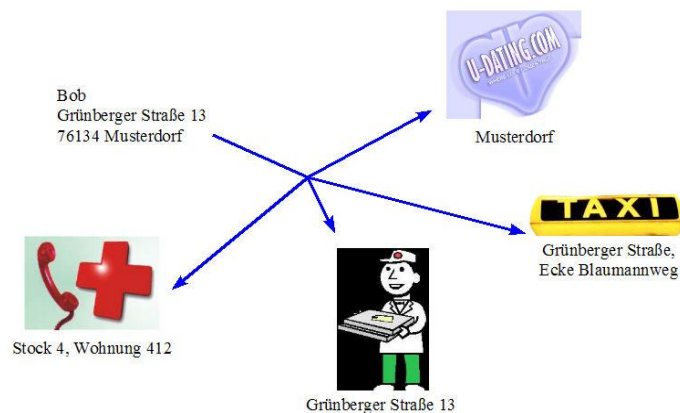


Abbildung 3: Beispiel für Datengranularität für verschiedene Dienste anhand eines Adressdatensatzes.

3.2 k-Anonymität

'Vollständige Anonymität' („Anonymität“ - aus dem Griechischen für „Namenlosigkeit“ [13]), also bezogen auf die gesamte Menschheit, ist in den meisten Fällen nicht möglich. Sobald auch nur ein Attribut einer Person X bekannt ist, schränkt dies die Menge der Personen ein, unter denen sich X befinden muss. Ein einfaches Beispiel hierzu ist eine schwarze Haarfarbe: Alle Menschen, die keine schwarze Haarfarbe haben, können bereits davon ausgeschlossen werden, X zu sein. X ist nur noch in der Menge der Personen mit schwarzen Haaren anonym. Natürlich ist diese Menge noch sehr groß. Im Allgemeinen kann aber (vor allem von einem Computersystem) zunächst keine Aussage darüber getroffen werden, wie 'groß' die verbleibende Anonymität ist. „X hat schwarze Haare und wohnt in Musterdorf.“ könnte bereits eine eindeutige Identifikation sein, obwohl weder Name, noch Adresse, noch ein anderes, leicht als identifizierend erkennbares, Attribut von X gegeben ist.

Um mit dieser Problematik zurecht zu kommen, führt man die Eigenschaft der k-Anonymität ein. Ein Objekt ist k-anonym in Bezug auf eine gegebene Attributmenge genau dann, wenn es mindestens k-1 weitere Objekte gibt, von denen es auf dieser Attributmenge nicht unterschieden werden kann [9].

Mit dieser Definition erreicht man zweierlei Dinge: Mit dem Beschränken auf eine feste Attributmenge wird explizit festgelegt, dass andere, das Objekt eventuell

genauer identifizierende Attribute, nicht berücksichtigt werden (dies wird noch eine Rolle beim „Spatial and Temporal Cloaking Algorithm“ in Kapitel 4 spielen: es wird keine Aussage über eventuell identifizierende Anfrageinhalte getroffen). Das Zweite das man erreicht ist, dass durch das Sicherstellen, dass es mindestens $k-1$ weitere, dem System bekannte Objekte gibt, die von dem zu anonymisierenden Objekt nicht unterschieden werden können, in der realen Welt mindestens ebenfalls $k-1$ solcher Objekte bestehen. Es kann zwar keine Aussage über die Vollständigkeit der Objekte im System getroffen werden, aber in der realen Welt können nur mehr als $k-1$ solcher Objekte existieren, nicht weniger (gegeben die Daten im System sind korrekt). Die k -Anonymität ist also auf jeden Fall gewährleistet, anders als in dem Fall des schwarzhäarigen Musterdorfbewohners, für den keine k -Anonymität im System geprüft wurde.

Abbildung 4 zeigt ein Beispiel, in dem die Beispieldatensätze auf der Attributmenge {'Name', 'Geburtsdag', 'PLZ'} für $k=3$ k -anonymisiert werden und das Attribut 'IQ' somit nicht mehr zwischen den grün, beziehungsweise den blau eingefärbten Personen entschieden werden kann.

Name	Geburtsdag	PLZ	IQ	Name	Geburtsdag	PLZ	IQ
Alice	01.12.1978	76131	90	*	1978	761**	90
Bob	22.07.1978	76137	60	*	1978	761**	60
Eve	12.01.1977	69514	88	*	1977	6951*	88
Carth	19.07.1977	69514	120	*	1977	6951*	120
Wayne	30.03.1978	76127	115	*	1978	761**	115
Zoe	03.05.1977	69516	137	*	1977	6951*	137

Abbildung 4: Links: Die ursprünglichen Beispieldatensätze. Rechts: Auf der Attributmenge {'Name', 'Geburtsdag', 'PLZ'} $k=3$ k -anonymisierte Datensätze. Jeder Wert des Attributs 'IQ' ist zwischen $k=3$ Personen nicht mehr entscheidbar.

3.3 Location-based Service

Ein location-based Service stellt einen kontextsensitiven Dienst zur Verfügung, wobei der Kontext dem Standort des Sensors entspricht.

Stellt man eine Anfrage an den Dienst, so übermittelt man ihm den aktuellen Standort und die Daten der Anfrage. Mögliche Bereiche dafür sind die Livenavigation (also Navigation unter Berücksichtigung der aktuellen Verkehrsverhältnisse), die Hotelsuche in der Umgebung, interaktive Stadtführer oder Ähnliches. Eine Anfrage könnte etwa so aussehen: (Längengrad, Breitengrad, „Gib mir alle Hotels mit freien Zimmern im Umkreis von 5km.“) und von einem PDA, Handy oder ähnlichen Endgerät abgesendet werden.

Eine etwas andere Form würde zum Beispiel in der Erstellung aktueller Wetter- oder Verkehrskarten zum Einsatz kommen. Statt einer Anfrage könnte ein Auto, das sich laut Navigationssystem auf einer Autobahn befindet, sich nur vereinzelt kurze Strecken mit geringer Geschwindigkeit vorwärts bewegt und dessen Regensensoren die Scheibenwischer aktiviert haben, folgenden Datensatz versenden: (Längengrad, Breitengrad, „A5“, „Stau“, „Regen“). Auf diese Weise wäre es dem Dienstgeber möglich, eine sehr aktuelle Wetter- und Verkehrskarte zu unterhalten. Auch im

Bereich der Unfallvorbeugung könnten zum Beispiel Gefahrenkarten unterhalten werden, die unter Anderem häufige Vollbremsungen an einer Kreuzung berücksichtigen.

4 Verfahren

In diesem Kapitel werden verschiedene Verfahren zur Manipulation der Datenqualität vorgestellt und kritisch auf ihre Einsetzbarkeit hinterfragt. Zunächst wird mit den zufallsbasierten Verfahren „Value Distortion“ und „Data Swapping“ begonnen. Anschließend wird das „Value Class Membership“-Verfahren allgemein und anhand zweier Anwendungsmöglichkeiten (dem „Spatial and Temporal Cloaking Algorithm“ und dem „MiniGIS“-Operator) behandelt.

Das generelle Anliegen dieser Verfahren ist es, personalisierte Daten so zu entpersonalisieren, dass deren Weitergabe kontextsensitive Diensterbringung (wie location-based Services) und Mustererkennung (wie Association Rules, Classification oder Clustering) ermöglichen und gleichzeitig den Schutz der Privatsphäre des Datenbesitzers gewährleisten.

Nach Gruteser und Grunwald ist dem Schutz der Privatsphäre genüge getan, wenn – in ihrem Beispiel – die Verfolgung einer Person mit Hilfe der freigegebenen Daten nur mit vergleichbarem Aufwand wie dem der Verfolgung mit traditionellen Methoden zu erreichen ist [9]. Unter traditionellen Methoden versteht man zum Beispiel das Beschatten einer Person oder das Anbringen eines Peilsenders an ihrem Wagen. Diese Definition ist angemessen, da der darüber hinausgehende Schutz eines Systems durch eben solche traditionellen Methoden umgangen werden kann und somit keine Verbesserung der generellen Datenschutzsituation darstellt.

Eine wichtige Grundvoraussetzung für alle Verfahren ist, dass mehrere Anfragen auf die selben Ausgangsdaten auch stets die selben veränderten Daten ergeben müssen. Andernfalls wären alleine durch mehrfaches Anfragen und anschließende Mittelwertbildung schon Rückschlüsse auf die Ausgangsdaten möglich.

4.1 Value Distortion

Verfahren. Das Value Distortion-Verfahren [5, 6, 15] basiert auf der Verschleierung der sensitiven Ausgangswerte mit Hilfe von Zufallszahlen. Zu diesem Zweck wird zwischen die Quelle der Werte und deren Weitergabe ein Zufallsgenerator geschaltet, der zu jedem Wert einen Zufallswert einer vorgegebenen Verteilung addiert, bevor diese Summe weitergegeben wird.

Es wird der Wert von $x_i + y_i$ statt vom Ausgangswert x_i weitergegeben, wobei y_i eine Zufallszahl aus einer bestimmten Verteilung ist. Hierbei sind zwei Verteilungen möglich:

- **Gleichverteilung**, bei der y_i in $[-\alpha, +\alpha]$ liegt,
- **Normalverteilung** mit dem Erwartungswert $\mu=0$ und der Standardabweichung σ .

Die Ausgabe wird für jedes Element vermerkt, um Rückschlüsse durch mehrere gleiche Anfragen mit unterschiedlichen Ergebnissen zu verhindern.

Seien die Ausgangsdatenwerte x_1, x_2, \dots, x_n n unabhängige, gleichverteilte Stichproben der Verteilung X und y_1, y_2, \dots, y_n n unabhängige Stichproben der Verteilung Y , dann ist das Rekonstruktionsproblem unter Kenntnis von $x_1 + y_1, x_2 + y_2, \dots, x_n + y_n$ und der kumulativen Verteilungsfunktion $F_Y(y)$ von Y die Abschätzung der Verteilungsfunktion $F_X(x)$ der Ausgangsdaten aus den verschleierte Daten. Es wird jedoch nur die Verteilung der Ausgangsdaten rekonstruiert, nicht die Ausgangsdaten selbst. Somit ist eine Mustererkennung auf den verschleierte Werten möglich, die Ausgangsdaten sollen jedoch nicht mehr aus den verschleierte Daten hervorgehen.

Bewertung. Eine erste Einschränkung dieses Verfahrens ist die Tatsache, dass es nur auf numerische Attribute angewendet werden kann.

Verschleiert man sehr wenige Werte, so können die Ausgangsdaten in der Tat nicht mehr errechnet werden. Allerdings macht auch eine Mustererkennung auf wenigen Datensätzen wenig Sinn. Erst ab einer großen Menge an Daten kann man die Mustererkennung gewinnbringend einsetzen. Hier liegt jedoch auch der mathematische Angriffspunkt an das Verfahren: Man kann sich Eigenschaften von Zufallsmatrizen zu eigen machen, um die Ausgangsdaten in sehr guter Qualität wieder aus den verschleierte Daten zu errechnen. Fasst man die erhaltenen Daten als Zufallsmatrix auf, kann man über die Betrachtung des Leistungsdichtespektrums (ähnlich wie bei der Rauschunterdrückung in der Signalverarbeitung) einen erheblichen Teil des Rauschens durch die aufaddierten Zufallszahlen wieder entfernen. Eine exakte mathematische Rückrechnung auf die Ausgangsdaten ist zwar so nicht möglich, die Unsicherheit eines jeden Wertes kann jedoch sehr stark reduziert werden (Abbildung 5).

[15] gibt einen Rauschfilteransatz an, der eine gute Annäherung an die Ausgangsdaten ermöglicht. Ein ausreichender Schutz der Ausgangsdaten ist somit nicht mehr gewährleistet. Unter diesem Gesichtspunkt sollte das Verfahren in dieser Form und ohne Überarbeitung der mathematischen Grundlagen nicht mehr angewendet werden.

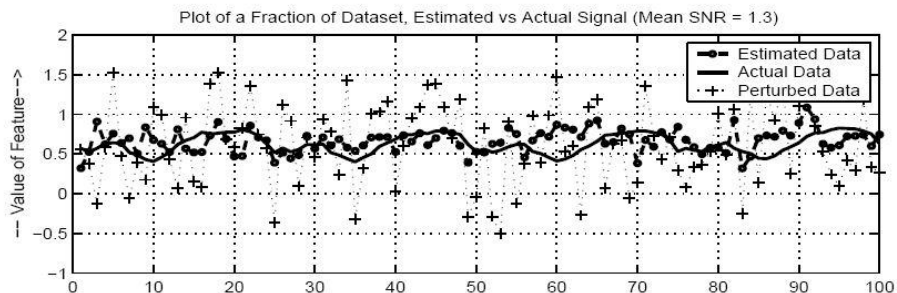


Abbildung 5: Abschätzung der Ausgangsdaten von mit Value Distortion verwischten Audiodaten.

4.2 Data Swapping

Verfahren. Das Data Swapping ist ein sehr einfaches Verfahren, bei dem zwischen verschiedenen Datensätzen Attributwerte untereinander ausgetauscht und dann die so veränderten Datensätze weitergegeben werden.

Das Austauschen funktioniert dabei in der Form, dass die Werte eines sensitiven Attributs paarweise vertauscht werden. Je nach Anforderung kann dieser Schritt (mit einer jeweils neuen Zuordnung) mehrfach durchgeführt werden. Danach verfährt man mit den anderen sensitiven Attributen ebenso.

Auf den ausgegebenen Datensätzen können dann einfache Operationen auf einzelnen Attributen, wie zum Beispiel Aufsummieren oder Existenzprüfung von Werten, ausgeführt werden.

Bewertung. Ein Vorteil dieses Verfahrens ist, dass es auf beliebige Attributstypen angewendet werden kann, da nur ihre existierenden Ausprägungen vertauscht werden.

Ein weiterer Vorteil besteht darin, dass durch eine große Anzahl an Vertauschungen ein sehr hoher Grad an Anonymität erreicht werden kann, wenn die Daten gut verteilt liegen. Es ist jedoch abhängig von den zugrunde liegenden Ausgangsdaten: Liegen sehr viele gleiche Werte vor, so ist eine Veränderung eines Datensatzes durch Vertauschung unwahrscheinlicher.

Der große Nachteil an diesem Verfahren ist jedoch, dass durch ein unkontrolliertes Vertauschen von Attributwerten Abhängigkeiten zwischen den Attributen verloren gehen und somit ausgefeiltere Mining-Techniken wie Association Rules, Clustering oder Classification unmöglich werden. Aus dem selben Grund können Datensätze nach der Vertauschung auch inkonsistent werden. So repräsentieren („Opel“, „Corsa“, „rot“) und („Mercedes“, „SL“, „silber“) Objekte der realen Welt, ein („Opel“, „SL“, „schwarz“) jedoch nicht.

Aufgrund seines großen Nachteils, ist das Data Swapping Verfahren für die meisten Anwendungsgebiete in dieser Form nicht geeignet. Wenn es darum geht einfache Zähloperationen auf Attributen durchzuführen, würden auch sortierte Wertelisten ausreichen, die in ihrer Erstellung erheblich weniger Rechenleistung erfordern, als das mehrfache Vertauschen aller Werte.

4.3 Value Class Membership

Verfahren. Grundsätzlich funktioniert das Value Class Membership-Verfahren, indem der Definitionsbereich eines Attributs in disjunkte, nicht notwendiger Weise gleichgroße Intervalle (Klassen) unterteilt wird und statt einem genauen Attributwert nur noch das Intervall, in das der Wert fällt, weitergegeben wird.

Die Intervalle können nach verschiedenen Strategien statisch oder dynamisch erzeugt werden, also zum Beispiel zum Implementierungszeitpunkt, zur Laufzeit oder unter Berücksichtigung des aktuellen Datenbestandes. Je nach dem welche Strategie verwendet wird, kann man verschiedene Ziele mit diesem Verfahren realisieren. Durch sie wird auch ein Trade-Off zwischen dem Berechnungsaufwand und der erreichten Güte der Anonymisierung gesteuert. Weitere Ziele, die mit verschiedenen Strategien erreicht werden können sind die k-Anonymität von Datensätzen oder die optimale Granularität von Ausgabedaten. Anhand des „Spatial and Temporal

Cloaking Algorithms“ [9] wird das Value Class Membership-Verfahren im Folgenden genauer erläutert.

Spatial and Temporal Cloaking Algorithm. Der Aufbau des Szenarios ist wie folgt: Ein location-based Service bietet für registrierte Teilnehmer über eine Software im Bordcomputer ihrer Autos die Möglichkeit, Anfragen über verschiedene Unternehmen in der aktuellen Umgebung zu stellen. Anfragen sind der Form „Gib mir alle Hotels/Banken/Restaurants/... in meiner aktuellen Umgebung, die freie Zimmer haben/in der Cashgroup sind/freie Tische haben/...“.

Die Anfragen werden nicht direkt vom Endgerät an den location-based Service gesendet, sondern zunächst an einen Anonymity Server, der mittels des Spatial and Temporal Cloaking Algorithms k-Anonymität für den Sender gewährleistet, bevor er die Anfrage an den location-based Service weiterleitet. Von diesem nimmt er die Antwort wiederum entgegen und sendet diese an das Endgerät. Das Mapping von Anfrage, beziehungsweise Antwort auf ein Endgerät wird ausschließlich im Anonymity Server für die Rückübermittlung der Antwort gespeichert. Der Anonymity Server wird von einer Trusted Third Party gestellt, bei der jeder Teilnehmer angemeldet sein muss.

Erreicht wird die k-Anonymität, indem Intervalle über die Raumkoordinaten („spatial“), beziehungsweise über die Zeit („temporal“) in der Form gebildet werden, dass in dem angegebenen Intervall neben dem Absender der Anfrage noch mindestens k-1 weitere Teilnehmer waren. Ein Beobachter, der die Anfrage an den location-based Service liest, kann somit nicht entscheiden, von welchem dieser mindestens k Endgeräte sie stammt.

Der Spatial Cloaking Algorithm läuft dabei wie folgt ab:

(1) Das aktuelle Intervall ist zunächst das gesamte Gebiet, das von dem Anonymity Server behandelt wird.

(2) Das aktuelle Intervall wird in gleichgroße Quadranten zerlegt und als nächstes der Quadrant mit dem Endgerät der Anfrage betrachtet.

(3) Sind in diesem Quadranten mindestens k Endgeräte vorhanden, so wird dieser das aktuelle Intervall und der Algorithmus fährt mit (2) fort. Sind nicht mehr mindestens k Endgeräte in diesem Quadranten, endet der Algorithmus und gibt das letzte aktuelle Intervall zurück.

Das Beispiel in Abbildung 6 zeigt den Ablauf für k=2.

Der Temporal Cloaking Algorithm betrachtet ein gegebenes räumliches Intervall, in dem zum Zeitpunkt T eine Anfrage gestellt wurde, über die Dauer des Zeitintervalls $[T-t_a, T+t_b]$ ob innerhalb dieser Zeitspanne mindestens k Endgeräte in diesem räumlichen Intervall gewesen sind.

Die Positions- und Zeitdaten, die der Anonymity Server an den location-based Service weiterleitet, sind der Form $([x_1, x_2], [y_1, y_2], [t_1, t_2])$ und garantieren, dass dieses Raum/Zeit-Intervall auf mindestens k Endgeräte zu traf.

Bewertung. Die Güte des Value Class Membership-Verfahrens ist sehr von der Strategie, mit der die Klassen gebildet werden, abhängig. Sie ist die Abstimmung zwischen Güte auf der einen, und Aufwand zur Berechnung der Rückgabeklasse auf der anderen Seite. Somit hat das Verfahren eine grundlegende Eigenschaft für den Einsatz in verschiedensten Bereichen. Generell kann das Verfahren auf alle Arten von

Attributen angewendet werden und auf sehr szenariospezifische Problemstellungen eingehen.

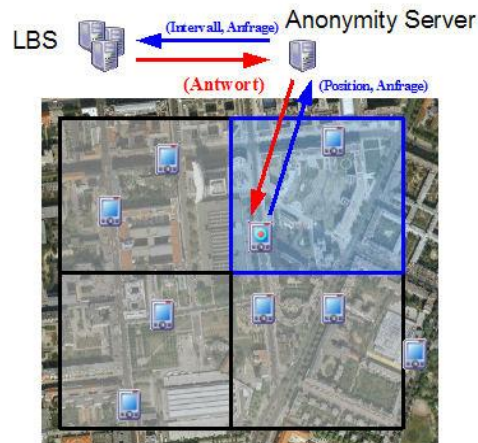


Abbildung 6: Der Anonymity Server berechnet für die gestellte Anfrage das blaue Quadrat als Intervall, das für das anfragende Endgerät $k=2$ k -Anonymität gewährleistet.

Wie man anhand des Spatial and Temporal Cloaking Algorithms sehen kann, kann k -Anonymität – sofern sie möglich ist und die Strategie darauf ausgelegt ist – gewährleistet werden. Auch eine optimale Granularität der Daten kann mit einer entsprechenden Strategie (siehe nächste Verfahren „MiniGIS“) erreicht werden.

Neben diesem sehr großen Vorteil des Verfahrens gibt es jedoch auch dadurch entstehende Probleme. Um einen optimalen Schutz zu gewährleisten, muss man eine szenario- und datenspezifische Erstellung der Klassen planen, was mit einem großen Aufwand verbunden ist. Betreibt man diesen Aufwand nicht und verwendet zum Beispiel statische Intervalle, so können durchaus Rückschlüsse auf die Daten getroffen werden. Auch der hier vorgestellte Spatial Cloaking Algorithm hat dieses Problem (Abbildung 7): Bei einer bekannten Unterteilung der Intervalle, kann das Wählen eines größeren Quadranten durch den Anonymity Server Rückschlüsse auf den kleineren, nicht gewählten Quadranten zulassen. Würden drei der vier kleineren Quadranten (1, 2, 3) das k -Anonymitäts-Kriterium erfüllen, jedoch einer (4) nicht, so könnte man die Anfrage diesem Quadranten aufgrund der Wahl des größeren Quadranten zuordnen.

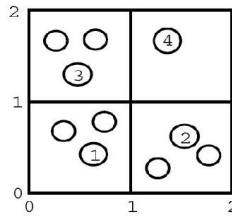


Abbildung 7: Bei ungünstiger Verteilung der Daten und bekannter Unterteilung der Intervalle können Rückschlüsse möglich sein: Eine Anfrage von (4) liefert – im Vergleich zu allen anderen Anfragen – ein größeres Intervall, um $k=3$ k -Anonymität zu gewährleisten.

Ein weiteres Problem besteht darin, dass eine gleichmäßige Verteilung von vielen Daten über den gesamten Wertebereich optimal wäre. In spärlichen Bereichen werden die Intervalle sehr groß, eventuell sogar unbrauchbar. Aus diesem Grund wurde der Spatial Cloaking Algorithm auch um das zeitliche Intervall erweitert. Während in Großstädten durchaus genügend Teilnehmer auf den Straßen unterwegs sind, um brauchbare Intervallgrößen zu erreichen, wird dies auf abgelegeneren Strecken zunehmend schwieriger.

Vor allem im vorgestellten Spatial and Temporal Cloaking-Szenario kommt ebenfalls als Kritikpunkt hinzu, dass eine Trusted Third Party benötigt wird, um das Anonymisieren durchzuführen. Zwar wird diese Instanz in jedem Fall benötigt, jedoch fällt sie meistens mit dem Besitzer der Daten (zum Beispiel dem Datenbanksystem, aus dem die Daten ausgelesen werden) zusammen.

4.4 MiniGIS

Verfahren. Der MiniGIS-Operator [8] („GIS“ steht für „Geographic Information Server“) ist ein sehr spezialisiertes Verfahren. Es erlaubt das lokale Anpassen der Granularität von Positionsdaten vor der Übermittlung. Im Prinzip kann man es ebenfalls wieder in die Klasse der Value Class Membership-Verfahren einordnen, da es die aktuellen Positionskordinaten in Ortsklassen überführt.

Das Vorgehen bei diesem Verfahren ist wie folgt: Zunächst ermittelt man passiv seine aktuelle Position per GPS oder einem System wie Place Lab [14]. Auf die so erhaltenen Koordinaten wendet man lokal den MiniGIS Operator an, der sie – je nach gewünschter Granularität – umrechnet. Die mögliche Ausgaben dabei bestehen aus zwei Teilen. Der erste gibt die Beziehung zur ausgewählten Ortsklasse an: „Distance to“, „nearest to“ und „at“. „Distance to“ berechnet die Entfernung von der aktuellen Position zum gewünschten Ort, „nearest to“ gibt das nächstgelegene Element der gewählten Ortsklasse und „at“ den tatsächlichen Aufenthaltsort zurück. Der zweite Teil gibt die gewünschte Granularität der Ortsangabe (weiter oben als Ortsklasse bezeichnet) an. Er sagt, ob die Ausgabe als Koordinaten, Platz, Stadt, Postleitzahl, Region, Land oder Kontinent aufgelöst werden soll. Prinzipiell sind Umrechnungen von allen Ortsklassen in alle anderen möglich – für den Schutz der Privatsphäre wirklich interessant, ist jedoch nur die Transformation in eine gröbere Ortsangabe. Die dem System bekannten Orte können sowohl aus öffentlichen Quellen, wie den

geografischen Datenbanken von USGS („U. S. Geological Survey“) oder GeoNET, als auch aus selbst definierten Orten aufgebaut werden.

Bewertung. Im Gegensatz zum Spatial and Temporal Cloaking Algorithm setzt sich dieses Verfahren eine optimal an die Bedürfnisse des Empfängers anpassbare Granularität der Ortsdaten zum Ziel. Entweder per Hand oder per automatisierter Umrechnung der Koordinaten (in zum Beispiel die aktuelle Stadt vor dem Senden einer Anfrage an einen location-based Service) wird hier die Granularität lokal angepasst. Es wird kein externer Dienst für das Anonymisieren benötigt. Aufgrund der geringen Größe des Operators in Verbindung mit einer (aus Platzgründen auf die aktuelle Umgebung beschränkten) Datenbank, kann dieses Verfahren auch auf PDAs und Handys zum Einsatz kommen.

Aufgrund des passiven Charakters der Positionsermittlung mittels GPS, Place Lab oder ähnlichen Systemen, wird auch in diesem ersten Schritt keinerlei Information preis gegeben.

Der größte Vorteil dieses Verfahrens (die rein lokale Umrechnung) ist auch gleichzeitig sein größter Nachteil: Aufgrund des Fehlens von Betrachtungen über andere Personen in dem angegebenen Gebiet kann keinerlei Aussage über eine k-Anonymität getroffen werden: Das Endgerät könnte durchaus das einzige sein, das sich zu einem Zeitpunkt zum Beispiel „at Musterdorf“ aufhält. Hier sei jedoch darauf hingewiesen, dass dies in diesem Fall auch nicht angestrebt wird. Ein Dienst soll mit den minimal-granularen Ortsdaten gespeist werden, mit denen er gerade noch funktionieren kann. Würde die Granularität weiter verringert werden, um zum Beispiel auf k-Anonymität einzugehen, so könnte dieser Dienst nicht mehr in Anspruch genommen werden.

5 Zusammenfassung und Ausblick

Es wurden einige Beispiele für extreme und für alltägliche Probleme mit personalisierten Daten aufgezeigt und dadurch die Notwendigkeit des Schutzes der Privatsphäre verdeutlicht. Auch wenn ein rechtlicher Anspruch darauf besteht, so werden Verstöße in dieser Richtung meist nicht geahndet (siehe Anti-Terror-Kampf oder auch den alltäglichen Verkauf von Adressen durch Unternehmen).

Vor allem die vorgestellten Zufallsverfahren zur Manipulation der Datenqualität haben sich als weniger brauchbar herausgestellt. Dies hat zwei Gründe: Zum Einen kann die zufällige Vertauschung von Daten eine Strukturhaltung nicht gewährleisten, zum Anderen kann das Verändern von Daten mit Zufallszahlen meist keine ausreichende Sicherheit bieten. In diesem Bereich sind weitere Anstrengungen nötig, um für dieses Verfahren entweder neue mathematisch sichere Modelle zu entwickeln, oder um sie mathematisch als prinzipiell unbrauchbar zu beweisen.

Ein größeres Potential kommt den strategisch vorgehenden Ablegern des Value Class Membership-Verfahrens zu. Wie gezeigt wurde, gibt es bereits Ansätze, die auf die wichtigen Eigenschaften „k-Anonymität“ und „minimal nötige Granularität“ hinarbeiten. Im Fall des Spatial and Temporal Cloaking Algorithms müssen jedoch noch genauere Betrachtungen über die Unterteilung der einzelnen Abschnitte getroffen werden, um Vorhersagen über mögliche Sicherheitslücken treffen zu können, bevor das Verfahren Verwendung findet.

Sowohl der Spatial and Temporal Cloaking Algorithm, als auch der MiniGIS-Operator haben noch eine Problematik, für deren Lösung sich vielleicht ein verteiltes System von Endgeräten anbieten könnte: Im zuerst genannten Fall wird eine Trusted Third Party benötigt. Der MiniGIS-Operator kann überhaupt keine Aussage über den Grad der Anonymität machen. In wie weit ein vorgehen mittels Kommunikation unter den Endgeräten hier zu einer Verbesserung führt, muss jedoch noch genauer untersucht werden.

Es kristallisiert sich vor allem auf dem Gebiet des Schutzes der Privatsphäre heraus, gefundene Lösungen stets kritisch zu hinterfragen, da eine unentdeckte Lücke (wie bei dem Value Distortion-Verfahren) zum Verlust der Privatsphäre von Personen führen kann. Eine umfassende Betrachtung der mathematischen Grundlagen eines entwickelten Systems sind unumgänglich.

Literaturverzeichnis

1. Sadeh, N. M., Gandon, F. L., Kwon, O. B.: Ambient Intelligence: The MyCampus Experience. Carnegie Mellon University Technical Report (CMU-ISRI-05-123). 2005.
2. Rao, B., Minakakis, L.: Evolution of Mobile Location-Based Services. Communication of the ACM, Volume 46, Issue 12. 2003.
3. Bundesverfassungsgericht: BVerfGE 65, 1 – Volkszählung. 1983.
4. United Nations: Universal Declaration of Human Rights. 1948.
5. Agrawal, R., Ramakrishnan, S.: Privacy-Preserving Data Mining. ACM SIGMOND Record, Volume 29, Issue 2. 2000.
6. Kargupta, H., Datta, S., Wang, Q., Sivakumar, K.: On the Privacy Preserving Properties of Random Data Perturbation Techniques. Third IEEE International Conference on Data Mining, 2003. 2003.
7. Dutta, H., Kargupta, H., Sivakumar, K., Datta, S.: Analysis of Privacy Preserving Random Perturbation Techniques: Further Explorations. Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society, Washington, DC. 2003.
8. Hong, J. I., Landay, J. A.: An Architecture for Privacy-Sensitive Ubiquitous Computing. Proceedings of the Second International Conference on Mobile Systems, Applications, and Services, Boston, MA. 2004.
9. Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. Proceedings of the First International Conference on Mobile Systems, Applications, and Services. 2002.
10. VITRONIC Dr.-Ing. Stein Bildverarbeitungssysteme GmbH: Maut erheben und kontrollieren. www.vitronic.de. 10.01.2007.
11. ABMG: Gesetz über die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen. 2002.
12. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar. Interview in der Hessischen Niedersächsischen Allgemeinen vom 02.08.2006. 2006.
13. Meyers großes Taschenlexikon in 25 Bänden, Auflage 7. 1999.
14. Gloor, T.: Ortsbestimmung mit Place Lab. Distributed Systems Seminar – ETH Zürich. 2005.
15. Datta, S., Kargupta, H., Sivakumar, K.: Homeland Defense, Privacy-Sensitive Data Mining, and Random Value Distortion. Proceedings of the SIAM Workshop on Data Mining for Counter Terrorism and Security. 2003.
16. Weichert, T.: US-Behörden kontrollieren weltweite Banktransaktionsdaten von SWIFT. Homepage des Unabhängigen Landesentrums für Datenschutz Schleswig-Holstein (www.datenschutzzentrum.de), Stand 10.07.2006. 2006.