

Technische Universität Dresden
Fakultät Verkehrswissenschaften "Friedrich List"
Institut für Verkehrstelematik
Professur Informationstechnik für Verkehrssysteme

Studienarbeit

Untersuchungen zellbasierter Ortungsverfahren hinsichtlich Genauigkeit und Energieeffizienz

eingereicht von
Herrn cand.-Ing. Jonas Bechtel

verantwortlicher Hochschullehrer:

Prof. Dr.-Ing O. Michler, TU Dresden

Betreuer:

Dipl.-Ing Florian Giersch, TU Dresden

und

Dipl.-Ing Paul Schwarzbach, TU Dresden

Dresden, zum 15. Juni 2017

Bibliographischer Nachweis

Jonas Bechtel

Untersuchungen zellbasierter Ortungsverfahren hinsichtlich Genauigkeit und Energieeffizienz

Studienarbeit, Technische Universität Dresden

Fakultät Verkehrswissenschaften "Friedrich List"

Zeit der PDF-Erzeugung: sh: ./nice_date.sh: Datei oder Verzeichnis nicht gefunden

Gefundene parallele Projektversion: cat: ../../version/version.number: Datei oder Verzeichnis nicht gefunden

Variante: noreach

Abstract/Kurzfassung (als Autorenreferat)

bla

bla

bla

(TODO!!)

Thesen

These 1: GPS ist in der Stadt ungenau.

These 2: WLAN und andere Technologien (Bluetooth, Mobilfunk) verbrauchen weniger Energie als GPS (Dieser Aspekt ist insbesondere für mobile Anwendungen interessant.)

These 3: Mit Zellortung (WLAN, Bluetooth, Mobilfunk) kann man in der Stadt seine Position sehr genau und in Echtzeit bestimmen.

These 4: Smartphones lassen sich leicht als Messsystem einsetzen.

Inhalt

Synonyme und Abkürzungen und Glossar	VIII
1 Einleitung	1
2 Grundlegendes	2
2.1 Digitale Signalübertragung	2
2.1.1 Funktionsweise mit ä und ö (mit a und o)	2
2.1.2 Energieverbrauch	3/Y
2.2 Technik: WLAN	Z
2.3 Technik: Mobilfunk	Z
2.4 Technik: Bluetooth	Z
2.5 Technik: Zellortung	Z
2.6 Technik: Satellitenortung	Z
2.6.1 Ansatz	Z
2.6.2 Aufbau	Z
2.6.3 Funktionsweise von GPS	_UNKOWN! (CH 2.6.3)
2.6.4 Funktionsweise der anderen Systeme	_UNKOWN! (CH 2.6.4)
2.6.5 Fehler	_UNKOWN! (CH 2.6.5)

Synonyme und Abkürzungen und Glossar

An verschiedenen Stellen im Projekt werden unterschiedliche Begriffe für dieselbe Sache verwendet. Damit sich der Leser gut in dem Projekt zurechtfindet, sind hier die entsprechenden Begriffe aufgelistet:

USB = Universal Serial Bus – Universelle Schnittstelle mit weiter Verbreitung zum Anschluss von Geräten, Abfragen der Fähigkeiten der angeschlossenen Geräte und Kommunikation mit den Geräten über virtuelle Kanäle.

WLAN-Station – ein (im Sinne der Studienarbeit möglichst nicht ortsveränderliches) Gerät, das nach dem IEEE-802.11-Standard funkt.

WLAN-AP = Wireless Access Point = Basisstation – Eine i. d. R. nicht ortsveränderliche WLAN-Station, die den Zugang zum Internet (oder seltener zu unabhängigen Netzwerken) bereitstellt.

WLAN-Adapter = WLAN-Empfänger – Gerät, mit dem in dieser Arbeit (mit WLAN-Scans und/oder WLAN-Paketdumps) die umgebenden WLAN-Netze gefunden werden. Es handelt sich um die handelsüblichen WLAN-Chips oder WLAN-USB-Adapter.

WLAN-Netz = Tautologie von **WLAN = Wireless Local Area Network** – lokales Funknetz nach einem Standard der IEEE-802.11-Familie, das sich aus einer oder mehreren Basisstationen zusammensetzt.

RLS = rls = Rudolf-Leonhard-Straße

LH DD = Landeshauptstadt Dresden

Frame = Paket – Datensequenz, die in einem Stück von einem WLAN-Gerät versendet wird.

WLAN-Scan = WLAN-Suchlauf – Nutzung der i. d. R. hardwareseitigen Funktion des WLAN-Adapters, auf allen verfügbaren Kanälen WLAN-Netze zu suchen.

WLAN-Paketdump – Nutzung der bei vielen WLAN-Adaptern verfügbaren Funktion, alle Pakete auf dem aktuell eingestellten Kanal zu empfangen.

Einplatinencomputer = Messcomputer = Raspberry Pi 3 Model B (Messfahrten 2,3,4) bzw. Raspberry Pi Model B (Messfahrt 1)

LSA = Lichtsignalanlage – das beinhaltet die lokale Steuerlogik einer Kreuzung von Individualverkehrsstraßen inklusive der angeschlossenen Ampeln und Sensoren.

M3 = Messfahrt 3

M4 = Messfahrt 4 (Aus dieser Messfahrt wurde das Fingerprinting gespeist)

Scan = Suchlauf – Durchschalten aller technisch verfügbaren Frequenzen und gleichzeitig hören, auf welcher Frequenz welche Stationen funken.

DOP = GDOP = Geometric Dilution of Precision – geometrische Verzerrung des Messfehlers

LOS = line-of-sight – ein in der Funktechnik verwendeter Begriff für die direkte hindernisfreie Übertragungslinie einer elektromagnetischen Welle auf dem kürzesten Weg zwischen dem Empfänger und dem Sender.

NLOS = non-line-of-sight – ein in der Funktechnik verwendeter Begriff für eine Übertragungslinie einer elektromagnetischen Welle, die entweder durch Hindernisse, die in die Fresnel-Zone hereinragen, gestört ist und/oder die an einem großen Gegenstand/Gebäude reflektiert wird und anschließend den Empfänger erreicht.

NMEA = National Marine Electronics Association

NMEA-Daten = NMEA-Zeilen – zeilenweise Daten, die nach dem Standard NMEA 0183 für die Kommunikation zwischen Ortungsgeräten formatiert sind.

csv-Daten – csv steht für "comma separated values". Das Dateiformat dazu ist sehr einfach aufgebaut: die verschiedenen Messwerte (in Zeilen und Spalten angeordnet) sind als lesbarer Text gespeichert, wobei die Quell-Zeilen mithilfe von Zeilenumbrüchen getrennt werden und die Quell-Spalten mithilfe von Kommata getrennt werden. Das Zeichen zur Spaltentrennung kann variieren, manchmal wird auch ein Semikolon oder ein Punkt verwendet.

INS = inertial navigation system = Intertiales Navigationssystem – Die Technik, sich von einem

Startpunkt aus zu bewegen und anhand bordeigener Messgeräte (d. h. ohne Positionsmeldungen von außen) den eigenen Fahrtverlauf so zu erfassen, dass man ihn nachträglich auf einer Landkarte einzeichnen kann. Typischerweise wird dazu eine Kombination aus einem/mehreren Gyroskop(en) für die Erfassung der Richtungsänderungen und Beschleunigungssensoren oder Odometern für die Erfassung der zurückgelegten Distanz verwendet.

GPS = Global Positioning System – ein von den Vereinigten Staaten von Amerika betriebenes Satellitennavigationssystem

DGPS = Differential GPS – lokal gemessene Abweichung der GPS-Signallaufzeiten vom erwarteten Wert. Mit den DGPS-Daten können die empfangenen Signale zeitlich korrigiert werden und somit wird die Genauigkeit der GPS-Ortung insgesamt erhöht.

Zellortung = Zellbasierte Ortung – Ortung anhand von Funkstationen mit bekanntem Ort. Explizit nicht ist damit die Erkennung von Handys durch die Basisstationen gemeint.

SMD = Surface mounted device – elektronisches Bauelement, das auf die Leiterplatte gelegt wird und dort verlötet wird. Meist kleiner als die ältere Variante (THT = through-hole-technique, hier wird das Bauteil durch die Löcher der Leiterplatte gesteckt und an der Rückseite verlötet.)

IC = Integrated circuit – eine sehr kleine, sehr fein strukturierte mehrschichtige Siliziumfläche, die nach der Produktion als SMD-Bauteil, d. h. in einem Plastikgehäuse vergossen mit Beinchen oder Kontaktflächen verkauft wird. In der deutschen Allgemeinsprache werden ICs häufig als "Chips" bezeichnet. Allerdings ist der Begriff "Chip" in der englischsprachigen Industrie die Kurz-Bezeichnung für SMD-Widerstände.

OFDM = Orthogonal frequency division multiplexing – für dieses Modulationsverfahren werden die Signale auf vielen Frequenzen übertragen, die alle eine kleine Differenz zur Trägerfrequenz haben. Obwohl die Frequenzen sehr ähnlich sind, reagieren die ausgesendeten Wellen z. B. bei Reflektionen an Hauswänden unterschiedlich, weswegen die Wahrscheinlichkeit, dass eine gut nutzbare Frequenz dabei ist, sehr hoch ist.

CSMA/CA = carrier-sense multiple-access/collision avoidance – Ein Fehlerschutzmechanismus für leitungsgebundene oder Funk-Übertragungen, wenn das Übertragungsmedium mehrere nicht von vorneherein absehbar verbundene Geräte hat. In der CA-Variante beobachtet die Hardware das Übertragungsmedium, bis kein fremdes Signal zu erkennen ist und sendet erst dann das eigene Signal.

CSMA/CD = carrier-sense multiple-access/collision detection – Ein Fehlerschutzmechanismus für leitungsgebundene oder Funk-Übertragungen, wenn das Übertragungsmedium mehrere nicht von vorneherein absehbare verbundene Geräte hat. In der CD-Variante sendet die Hardware das eigene Signal. Der Empfänger untersucht anschließend, ob mehrere Sender gleichzeitig gesendet haben und bittet ggf. um eine Übertragungswiederholung.

TDMA = time-division multiple-access – Die Bezeichnung für die Methode, ein gemeinsam genutztes Medium (Luft, Netzkabel) in Zeitbereiche aufzuteilen, die den teilnehmenden Geräten zugeteilt werden.

1 Einleitung

Sie halten meine Studienarbeit zu einem Thema in Ihren Händen, das ich kurz "Haltelinie" nenne, denn der Anlass zu der Studienarbeit war eine intelligente Ampel-Vorankündigung, die es zwar schon in App-Form gibt, aber noch Schwächen hat. Eine dieser Schwächen, auf die eben diese Studienarbeit abzieht, ist die bislang nur unscharf beantwortete Frage: "Zu welcher Kreuzung gehört die vor mir liegende Haltelinie und wie viele Zentimeter ist sie noch entfernt?"

Die GPS-Ortung ist zwar an vielen Stellen sehr genau (in der Stadt ein geringer einstelliger Fehler in Metern), aber es gibt auch hohe Häuserschluchten, in denen die GPS-Empfänger ein "schlechtes Bild" abliefern. Genau in diesen Häuserschluchten sind aber viele WLAN-Netze zu erwarten. Der Ortungsteil der Studienarbeit konzentriert sich deswegen auf eine solche Stelle, die in Dresden zu finden war.

Besonders bemerkenswert und deswegen schon hier genannt ist die Berücksichtigung einer möglichen Unterteilung der Ortung in eine Längsrichtung und eine Querrichtung, denn diese beiden Ortungsrichtungen haben im Stadtverkehr einen unterschiedlichen Satz an verkehrstelematischen Anwendungen.

Falls Sie nur diesen Text vor sich haben, nicht aber die Projektdateien: unter dem folgenden Link stelle ich das Projektverzeichnis als tar.bz2-Archiv ins Internet: <http://jbechtel.de/site/Tools/HALTELINIE/>

Die Aufgabe

TODO: ggf. nochmal die Aufgabe in eigenen Worten beschreiben.

Reinnehmen: Annahme Zielgenauigkeit: besser als GPS (dadurch werden Systemparameter/-auswahl festgelegt.)

2 Grundlegendes

2.1 Digitale Signalübertragung

Die digitale Signalübertragung ist eine Technik mit einem sehr hohen analogen Anteil. Die Bezeichnung „digital“ kommt daher, dass die Sendedaten digital an die Sendeschaltung übergeben werden und aus der Empfängerschaltung digital herauskommen.

2.1.1 Funktionsweise mit ä und ö (mit a und o)

Die allgemeine Funktionsweise einer digitalen Signalübertragung unterscheidet sich wenig bei den in dieser Studienarbeit behandelten Techniken. Deswegen kann das Prinzipbild eines Mobiltelefon, siehe Abbildung 2.1, als allgemein bezüglich der Funktechnik angesehen werden.

Nach der Vorverarbeitung/Modulation wird das Signal in den weitgehend analogen Hochfrequenz-Bereich übertragen und gesendet. Die Hochfrequenz-„Baugruppen“ (heutzutage sind viele Baugruppen auf einem IC = Integrated Circuit integriert, weswegen eher von Hochfrequenzteilen gesprochen werden kann) sind: Frequenzkreise, Mischer und Verstärker. Die Frequenzkreise stellen eine synchronisierte Frequenz bereit, welche von außen steuerbar sein muss, damit der Kanal ausgewählt werden kann. Die Mischer übertragen das Signal auf den Zielkanal, also in die Zielfrequenz. Die Verstärker (engl. amplifier; in der Abbildung 2.1 als nach rechts/links zeigende Dreiecke dargestellt) müssen bei hohen Frequenzen eine möglichst starke und möglichst lineare Verstärkung realisieren. Eine nichtlineare Verstärkung führt zu Störsignalen (engl. noise) auf falschen Frequenzen. Da mit den genannten Anforderungen kein linearer Verstärker realisierbar ist, ist zwischen Verstärker und Antenne ein Filter nötig, der das Nutzsignal wieder leicht abschwächt und die

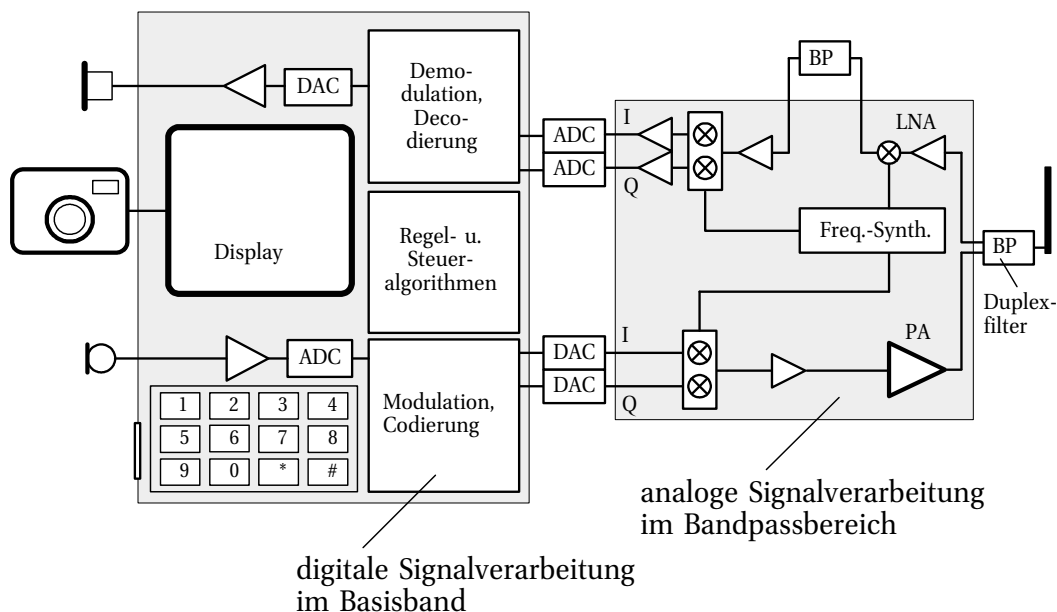


Abbildung 2.1: Digitale Signalübertragung bei einem Mobiltelefon. Der Originaltitel der Grafik ist „Blockschaltbild eines Handys“; sie ist von Seite 84 aus [Nuszkowski 2012] übernommen.

Die nach links/rechts gerichteten Dreiecke sind Verstärker, darunter „LNA“ = „low noise amplifier“ = sehr linearer Verstärker und „PA“ = „power amplifier“ = Verstärker für „große“ Leistungen. „BP“ steht für „Bandpass“, gemeint ist ein Filter, der die Störfrequenzen stark abschwächt und die Arbeitsfrequenzen (= Trägerfrequenzen) nur geringfügig abschwächt. „ADC“ = „Analog-to-digital converter“ und „DAC“ = „Digital-to-analog converter“. Die Mischer sind vom Grundprinzip Multiplikatoren, deswegen sind sie hier in der Abbildung als eingekreistes Kreuz dargestellt.

Eidesstattliche Erklärung

Störsignale stark abschwächt.

2.1.2 Energieverbrauch

Ein allgemeingültiger Energieverbrauch einer digitalen Signalübertragung (oder einer Berechnung o. ä.) ist schwer anzugeben, da er sehr stark von der technischen Realisation der Standards und diversen Seiteneffekten abhängt. Dies war auch an dem Quellenstudium in den Computerzeitschriften und Arbeiten abzulesen: die Verwendung bestimmter Techniken beansprucht die sonstigen Komponenten der Computer/Geräte. Trotzdem lassen sich die folgenden allgemeinen Überlegungen anstellen:

Zum Einen unterscheiden sich die Empfangs- und Versand-Richtung kaum im Energieverbrauch, was an der niedrigen erlaubten Sendeleistung und der aufgrund der hohen Frequenz aufwändigen Schaltung liegt, sodass der Schaltungs-Verbrauch viel größer als die eigentliche Sendeleistung ist.

Der Hochfrequenz-Teil ist der Haupt-Energieverbraucher der in dieser Arbeit beschriebenen Funktechniken. Insbesondere, um die Verstärker überhaupt realisieren zu können, müssen viele, teils energieintensive, schaltungstechnische Tricks angewandt werden.

Zum Anderen ist die Vorverarbeitung und die Modulation eines Sendesignals bzw. Nachverarbeitung eines Empfangssignals manchmal energieaufwändig (z. B. der Korrelationsschritt bei der Satellitenortung oder die Kanalschätzung bei OFDM-Übertragungen) (OFDM = Orthogonal frequency division multiplexing)

Der Technikzeitschriftenverlag Heise hat in [Labs 2010]/[Labs 2012]/[Spier 2016] für konkrete Motorola- und Samsung-Smartphones empirische Energieverbrauchswerte bestimmt; außerdem hat ein Konferenz-Paper [Carroll 2010] exakte komponentenweise Messungen zu einem Openmoko-Smartphone vorgenommen. Diese Messungen sind in Tabelle 2.1 zusammengefasst. Der übersichtlichen Zusammenfassung standen unterschiedliche Nutzungsbenennungen und teils fehlende Definitionen entgegen. In dieser Arbeit wurde streng nach den in den Artikeln gegebenen Definitionen gearbeitet, auch wenn sie nicht immer sinnvoll schienen. Es ist noch bemerkenswert, dass die verschiedenen Techniken unterschiedlich viel Strom verbrauchen, der aber immer im Kontext mit dem Datendurchsatz gesehen werden muss. So gibt [Carroll 2010] für die Speicherbausteine auch Effizienzwerte mit der Einheit Mebibyte/Joule an. Bei den Funkübertragungstechniken wurden solche Werte nicht angegeben, was daran gelegen haben könnte, dass ein zusätzlicher softwareseitiger Messschritt nötig gewesen sein könnte.

Weiterhin bemerkenswert ist die Aussage am Schluss von [Carroll 2010], dass solch detaillierte Energieverbrauchsanalysen durch den offenen Charakter der Openmoko-Plattform ermöglicht wurden und bei üblichen kommerziellen Smartphones nur in geringerem Umfang durchführbar sind.

Bei der Betrachtung der Tabelle fällt auf, dass ein WLAN-Suchlauf ähnlich viel Strom wie eine WLAN-Datenübertragung verbraucht. Außerdem wird in [Carroll 2010] beschrieben, dass der Stromverbrauch des GPS-Bauelements (der Firma u-Blox) unabhängig von der Anzahl der gefundenen Satelliten oder anderen Zustandsindikatoren ist. (Die beiden Tabellenwerte sind je für die Konfiguration mit/ohne externer Antenne angegeben. Weiterhin wird in der genannten Arbeit davon ausgegangen, dass der GPS-Energieverbrauch nach einem erfolgreichen Fix zurückgeht, was nur aufgrund einer fehlerhaften Ansteuerung durch das Smartphone nicht passiert.) Beide Beobachtungen sind dadurch zu erklären, dass der analoge Hochfrequenzteil (Bandpassbereich) der Schaltung immer aktiv ist, unabhängig von der Art oder Menge der zu übertragenden Daten.

2.2 Technik: WLAN

TODO:

- 2,4x GHz und 5,x GHz
- Kanäle in Deutschland, Kanäle in den USA, Kanäle anderswo
- Stationen,
- Modi: Ad Hoc, Mesh, Station
- Beacons: alle 100 s
- Frequenz teils überbelegt.
- Schnellabschaltung ?
- WLANp

2.3 Technik: Mobilfunk

TODO

- **GSM: ~850 MHz, 1600 MHz?**
- **Andere Standards:**
- **Masten**
- **Registrierung, IMEI**

2.4 Technik: Bluetooth

TODO

- **Schnelles Kanalhopping**
- **2,4 GHz?**

2.5 Technik: Zellortung

- **Basierend auf den o. g. Technologien**
- **Existierende Verbreitung**
- **Unterscheidung Indoor/Outdoor**
- **LoRAN?**
- **Verschiedene Algorithmen**

2.6 Technik: Satellitenortung

2.6.1 Ansatz

TODO

2.6.2 Aufbau

Die Architektur der gängigen Satellitenortungs-Systeme fasst treffend, wenn auch einschränkend als Satellite-"Navigation" bezeichnend, [Tauscher 2015] zusammen:

„Ein Satellitennavigationssystem ermöglicht dem Nutzer die Bestimmung seiner Position. Weltweit existieren unterschiedliche dieser satellitengestützten Systeme, deren prinzipieller Aufbau [...] ähnlich ist. Sie bestehen, wie Abbildung 2.2 zeigt, aus drei Segmenten: Dem Raumsegment, dem Bodensegment