# Fünf Milliarden vernetzte Sensoren: Chancen und Gefahren

Matthias Hollick und Delphine Christin
Technische Universität Darmstadt, Fachbereich Informatik
Fachgebiet Sichere Mobile Netze – SEEMOO
Mornewegstr. 32, 64293 Darmstadt
{matthias.hollick;delphine.christin}@seemoo.tu-darmstadt.de

***Abstract*—Sensornetze die durch Nutzerbeteiligung und auf Basis von Mobiltelefonen etabliert werden – *Partizipative Sensornetze* – eröffnen eine Reihe von Chancen, bergen aber auch eine Reihe von Gefahren. Dieser Beitrag stellt eine Auswahl von Anwendungen für Partizipative Sensornetze dar und identifiziert genutzte Sensormodalitäten. Mögliche Risiken mit dem Fokus auf dem Schutz der Privatsphäre der Nutzer werden eingeführt und offene Forschungsfragen in diesem Bereich benannt.**

## I. Motivation

Mobile Netze und mobile Endsysteme haben in der jüngeren Vergangenheit unsere Gesellschaft in allen Bereichen des täglichen Lebens durchdrungen und geprägt. Aktuelle Statistiken sagen voraus, dass die Anzahl von Mobilfunknutzern die Grenze von 5 Milliarden im Jahr 2011 überschreiten wird[1]. Gleichzeitig ist die Anzahl der aktiven Nutzer von (mobilen) Online Sozialen Netzen (OSN) ein Indiz für die Bereitschaft von Nutzern in virtuellen Gemeinschaften mitzuwirken; für das OSN Facebook liegt diese Anzahl zu Anfang 2011 bei über 500 Millionen aktiver Nutzer – bei stark steigender mobiler Nutzung[2].

Zur selben Zeit verfügen moderne Mobiltelefone (Smartphones) über eine Vielzahl von Sensoren und sind daher prinzipiell in der Lage, großflächige Sensornetze zu realisieren:

- Sensoren zur Lokalisierung – GPS, Triangulierung oder Zellen-basierte Positionsbestimmung via Bluetooth, Wi-Fi oder GSM/UMTS
- Bild- und Videosensoren – Kamera(s)
- Audiosensoren – Mikrofon(e)
- Bewegungs-, Temperatur-, Feuchte-, Näherungssensoren, Kompass, Near Field Communication, etc.

[1] www.gsmworld.de
[2] www.facebook.com

Diese vielfältigen Sensoren können ergänzt werden um dedizierte Sensoren, die zusätzliche Messdaten erheben (z.B. Luftschadstoffmessungen durch Sensoren für Ozon, Feinstaub, $CO_2$, etc.) und die Plattform Mobiltelefon als Kommunikationskomponente nutzen.

Im Gegensatz zu traditionellen Sensornetzen, die überwiegend für spezialisierte Anwendungen zum Einsatz kommen, bieten diese partizipativen Sensornetze die Chance auch dort Messwerte zu erfassen, wo dedizierte Sensornetze aus Kostengründen nicht ausgebracht werden. Ebenso steigt die Abdeckung des Sensornetzes in partizipativen Netzen mit der Anzahl der teilnehmenden Nutzer. Der Aufbau und Betrieb dieser Netze bedarf jedoch der Zustimmung und Mitwirkung der Nutzer, was auch in der Definition von Participatory Sensing nach (Burke et al., 2006) Ausdruck findet:

*"Participatory sensing will task deployed mobile devices to form interactive, participatory sensor networks that enable public and professional users to gather, analyze and share local knowledge."*

Ein Zielkonflikt zwischen dem Schutz der Privatsphäre und dem Nutzen der partizipativen Anwendung besteht. Im Folgenden stellen wir ausgewählte repräsentative Anwendungen für partizipative Sensorrnetze vor und klassifizieren diese. Wir betrachten die einzelnen Sensormodalitäten in partizipativen Sensornetzen und benennen mögliche Bedrohungen für die Privatsphäre der Nutzer.

## II. Anwendungen für Partizipative Sensornetze

Wir unterscheiden zwischen Mensch-zentrierten und Umwelt-zentrierten Anwendungen in partizipativen Sensornetzen. Im Folgenden geben wir eine kurze Übersicht über ausgewählte repräsentative Anwendungen beider Klassen. Eine ausführliche Liste der genannten Literaturreferenzen ist auf Anfrage bei den Autoren erhältlich.

### A. Mensch-zentrierte Anwendungen

Mensch-zentrierte Anwendungen nutzen Sensoren, um Daten über die Nutzer selbst zu erheben und entweder dem individuellen Nutzer oder einer Gruppe von Nutzern einen Mehrwert zu verschaffen. Dieser Klasse enthält:

1) Anwendungen zur Überwachung des *persönlichen Gesundheitszustandes* wie DietSense (Reddy et al., 2007), MobAsthma (Kanjo et al., 2009) oder SenSay (Siewiorek et al., 2003)
2) Anwendungen zur *Charakterisierung der Wechselwirkung von Nutzern und Umwelt* wie PEIR - Personal Environmental Impact Report (Mun et al., 2009)
3) Anwendungen zu *Sport und Fitness* wie BikeNet (Eisenman et al., 2009), Biketastic (Shilton, 2009) oder SkiScape (Eisenman and Campbell, 2006; Eisenman et al., 2006)
4) Anwendungen um *Mobile Soziale Medien* mit Echtzeit-Sensordaten zu erweitern wie Micro-Blog (Gaonkar et al., 2008) oder CenceMe (Miluzzo et al., 2008; Musolesi et al., 2008)
5) Anwendungen zur *Überwachung von Preisen* wie LiveCompare (Deng and Cox, 2009) oder PetrolWatch (Dong et al., 2008)

### B. Umwelt-zentrierte Anwendungen

Umwelt-zentrierte Anwendungen nutzen Sensoren, um ein Umweltmonitoring durchzuführen. Anwendungsklassen umfassen:

1) Die Überwachung der *Luftqualität* wie Haze Watch (Carrapetta et al. 2011), PollutionSpy (Kanjo et al., 2009) oder (Paulos et al., 2007).
2) *Umgebungslärmmessungen* wie NoiseTube (Maisonneuve et al., 2009), Ear-Phone (Rana et al., 2010) oder NoiseSpy (Kanjo et al., 2009).
3) Anwendungen, die die *Qualität von Straßen* dokumentieren oder aktuelle *Verkehrsflussinformationen* bzw. auf deren Basis optimierte *Routenempfehlungen* liefern wie Nericell (Mohan et al., 2008), CarTel (Hull et al., 2006) oder GreenGPS (Ganti et al., 2010).

## III. Privatsphäre in Partizipativen Sensornetzen

Der Schutz der Privatsphäre der Teilnehmer in partizipativen Sensornetzen ist ein wichtiger Aspekt, der über die Akzeptanz und damit schlussendlich den Nutzen dieser Netze entscheidet. Es ist festzustellen, dass existierende Anwendungen teilweise mehr Sensormodlitäten erfassen, als für die Kernanwendung nötig (vgl. Tabelle). Einige der genannten Ansätze benennen das Problem des Schutzes der Privatsphäre, allerdings gibt es bisher nur vereinzelt Lösungsansätze um diese zu schützen. Als Stand der Technik können zentrale Lösungen seitens des Anbieters der Anwendungsplattform gelten, dem man letztlich vertrauen muss, dass er die Daten ausreichend vor dem Zugriff Dritter schützt (z.B. indem Daten anonymisiert werden, Rohdaten nicht veröffentlicht werden, beantwortete Anfragen keine Rückschlüsse auf Nutzer zulassen, etc.).

| | Time | Location | Pictures | Sound samples | Acceleration | Pollution data | Biometric data |
|---|---|---|---|---|---|---|---|
| DietSense | x | x | x | x | | | |
| MobAsthma | x | x | | | | x | x |
| SenSay | x | x | | | x | | |
| PEIR | x | x | | | | | |
| BikeNet | x | x | | x | x | x | x |
| BikeStatic | x | x | | x | x | | |
| SkiScape | x | x | | x | x | | |
| Micro-Blog | x | x | x | x | x | | x |
| CenceMe | x | x | x | x | x | | |
| LiveCompare | x | x | x | | | | |
| PetrolWatch | x | x | x | | | | |
| Haze Watch | x | x | | | | x | |
| PollutionSpy | x | x | | | | x | |
| (Paulos et al.) | x | x | | | | x | |
| NoiseTube | x | x | | x | | | |
| Ear-Phone | x | x | | x | | | |
| NoiseSpy | x | x | | x | | | |
| SoundSense | x | x | | x | | | |
| MoVi | x | x | | x | x | | |
| Nericell | x | x | | x | x | | |
| CarTel | x | x | x | | x | x | |
| GreenGPS | x | x | | | | | |

Gleichzeitig kann festgestellt werden, dass eine Reihe von bisher ungelösten Fragen in dem genannten Kontext existieren. Beispielhaft sollen an dieser Stelle genannt werden: Die Abwägung zwischen Anonymität/Pseudonymität vs. Integrität der erfassten Daten; Garantien für den erreichbaren Schutz der Privatsphäre; Nutzerschnittstellen, um den Schutz (bzw. die Bedrohung) transparent für den Nutzer zu machen sowie ihm Eingriffsmöglichkeiten zu bieten das Schutzlevel festzulegen.

## IV. Zusammenfassung

Partizipative Sensornetze versprechen vielfältige Anwendungen, die es erlauben, die physikalische Welt in die virtuelle Welt einzubetten, indem sie Sensordaten in bislang unerreichter Auflösung und Abdeckung erfassen können. Gleichzeitig gefährden diese Anwendungen die Privatsphäre der Nutzer, die sich aktiv an diesen Sensornetzen beteiligen.

## Danksagung

Diese Arbeit wurde durch LOEWE CASED (www.cased.de) unterstützt.