

Das Netz der bewegten Dinge

Die Vernetzung der Dinge (Internet of Things oder kurz IoT) findet in vielen Bereichen statt, wie zum Beispiel der vernetzte Kühlschrank, der selbstständig Lebensmittel bestellt, oder der Fernzugriff mittels Smartphone auf verschiedene Geräte, wie Überwachungskameras, Beleuchtung oder die Heizung, oder Personenwaagen, die das eigene Gewicht auf Facebook posten etc.. Alle genannten Beispiele sind unbewegliche Dinge die im Internet of Things vernetzt sind.

Ein eigenes Anwendungsfeld ist das Netz der bewegten Dinge (Internet of Moving Things, IoMT). Das sind Geräte/Dinge, die vernetzt und zudem in irgendeiner Form in Bewegung sind, wie zum Beispiel Roboter, (autonome) Fahrzeuge, oder auch Dinge die Menschen mit sich herumtragen, wie etwa Smartphones, smarte Kleidung oder andere Wearables. Durch die Vernetzung können sich diese Dinge/Geräte selbst (Geschwindigkeit, Bewegungsrichtung, aber auch ihre Umgebung vermessen (Temperatur, Geräusche, Bodenbeschaffenheit, Luftverschmutzung etc.). Im Smart City Bereich sollen so auch die Vorteile von edge-, fog- oder [Cloud-computing](#) genutzt werden (Cao et al. 2020).

In der Robotik könnte die Vernetzung z. B. über Cloud-Dienste zum Austausch gesammelter Daten, „Lernerfahrungen“ bzw. Algorithmen genutzt werden. Interessante Anwendungsfelder für das Internet der bewegten Dinge ergeben sich vor allem im Bereich der Mobilität. Viele Neuwagen unterstützen bereits den SIM-Karten-Standard, Tendenz steigend. Das ermöglicht die Vernetzung der Fahrzeuge untereinander, aber auch zum Hersteller. Ferndiagnostik, Echtzeitnavigation und verschiedene Infotainment-Services können so zur Verfügung gestellt werden und sollen den Fahrkomfort und das Fahrerlebnis verbessern. Weitere potentielle Vorteile ergeben sich über die Datensammlung des Mobilitätsverhaltens, welches für ein effizienteres Verkehrssystem genutzt werden könnte. Neben der Steigerung der Effizienz im Verkehrssektor, verspricht man sich durch die zunehmende Vernetzung der Fahrzeuge auch eine erhöhte Verkehrssicherheit.

Die zunehmende Vernetzung hat aber nicht nur Vorteile. Es stellt sich die Frage, wie das Grundrecht auf informationelle Selbstbestimmung geschützt werden kann, vor allem im Hinblick auf die Nutzung der Daten durch Dritte (Krieger-Lamina 2016). Die Vernetzung eröffnet zudem potentielle Einfallstore für HackerInnen, was gravierende Auswirkungen haben kann. 2015 haben zwei Hacker auf diese Gefahr hingewiesen. Sie haben es geschafft einen zwei Tonnen schweren SUV zu kapern. Es war ihnen somit möglich das Fahrzeug gänzlich zu steuern, angefangen bei der Klimaanlage hin zu Lenkbewegungen und sogar das Bremsen war möglich.¹ 2016 wiesen Hacker auf eine Sicherheitslücke eines Elektroautoherstellers hin.

¹ [wired.com/video/hackers-wireless-jeep-attack-stranded-me-on-a-highway](https://www.wired.com/video/hackers-wireless-jeep-attack-stranded-me-on-a-highway).

Sie konnten aus einer Entfernung von 19 km auf das Fahrzeug zugreifen. Nach einem Update wurde die Sicherheitslücke beseitigt.² Das Tencent Keen Security Lab hat Anfang 2019 den „Autopiloten“ eines bekannten Elektroautoherstellers mittels kleiner weißer Aufkleber, die auf der Fahrbahn angebracht wurden, ausgetrickst. Der Autopilot des Fahrzeugs wurde so dazu gebracht auf die Gegenfahrbahn zu wechseln.³ Dieses Beispiel zeigt anschaulich, dass die eingesetzten Machine-Learning-Systeme nicht fehlerfrei sind. Ob die zunehmende Vernetzung der (bewegten) Dinge solche Situationen verhindern und nicht wohlmöglich neue Einfallstore eröffnen würde, bleibt eine offene Frage.

Auch auf Österreichs Straßen sind bereits Fahrzeuge unterwegs, die vernetzt sind. Bestrebungen, Österreich zu einem Vorreiter der neuen Mobilfunkgenerationen zu machen, hätten einen förderlichen Einfluss auf die zunehmende Vernetzung bewegter Dinge, zumal es ein explizites Ziel ist, diese Technologie in der digitalen Verkehrsinfrastruktur einzusetzen (BMVIT 2018). Das Ziel hierbei ist es, die Effizienz und Sicherheit auf österreichischen Straßen zu erhöhen und zugleich die internationale Wettbewerbsfähigkeit der Unternehmen zu gewährleisten, bspw. in der Automobilzulieferindustrie.

Mit den genannten Beispielen kristallisieren sich neue Handlungsfelder im Bereich der IT-Sicherheit und vor allem des Datenschutzes heraus. Darüber hinaus sollte auch bedacht werden, wie mit der steigenden Abhängigkeit von dieser Vernetzung umzugehen ist, oder konkret, wie Mobilität zukünftig funktioniert, wenn Mobilfunknetze einmal ausfallen.⁴

Zitierte Literatur

- BMVIT, 2018, 5G-Strategie Österreichs Weg zum 5G-Vorreiter in Europa, April 2018, Wien: Bundesministerium für Verkehr, Innovation und Technologie: [info.bml.gv.at/service/publikationen/telekommunikation/5gstrategie---oesterreichs-weg-zum-5g-vorreiter-in-europa.html](https://www.bml.gv.at/service/publikationen/telekommunikation/5gstrategie---oesterreichs-weg-zum-5g-vorreiter-in-europa.html).
- Cao, H.; Wachowicz, M. A (2020) Holistic Overview of Anticipatory Learning for the Internet of Moving Things: Research Challenges and Opportunities. *ISPRS Int. J. Geo-Inf.*, 9, 272. [mdpi.com/2220-9964/9/4/272/pdf](https://www.mdpi.com/2220-9964/9/4/272/pdf).
- Krieger-Lamina, J., 2016, Vernetzte Automobile. Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen. Endbericht, 2016-08-31, Wien: Institut für Technikfolgen-Abschätzung (ITA): <http://epub.oew.ac.at/ita/ita-projektberichte/2016-02.pdf>.

² [zdnet.de/88279165/tesla-model-s-sicherheitsforscher-hacken-elektroauto-aus-der-ferne/?inf_by=5a03063e681db8cf478b467d](https://www.zdnet.de/88279165/tesla-model-s-sicherheitsforscher-hacken-elektroauto-aus-der-ferne/?inf_by=5a03063e681db8cf478b467d).

³ futurezone.at/produkte/kleine-sticker-auf-der-strasse-lassen-tesla-auf-gegenfahrbahn-wechseln/400453735.

⁴ Siehe dazu auch das Forschungsprojekt ISIDOR, das sich mit den Folgen eines lang andauernden und großflächigen Ausfalls Internet-basierter Dienste und Infrastrukturen befasste: oew.ac.at/ita/projekte/isidor-was-geht-ohne-internet. Der abschließende Projektbericht wird ab Dezember 2022 verfügbar sein.