
Studiengang: Informationstechnik

# Entwicklung eines externen Sensornetzes mit WLAN Kopplung und Visualisierung

## Studienarbeit

Im Rahmen der vierten Praxisphase

Abgabedatum Irgendwann 2015


| | |
|---|---|
| Verfasser | Maik Maier, Nicolai Staege |
| Matrikelnummer | 4050846, 4615051 |
| Kurs | TINF12B3 |

# Erklärung

Gemäß §5 (3) der „Studien- und Prüfungsordnung DHBW Technik“ vom 22. September 2011.

Ich habe die vorliegende Studienarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet.

Karlsruhe, Datum

Unterschrift

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Listings

# Abkürzungsverzeichnis

| | |
|---|---|
| **IoT** | Internet of Things |
| **SPOT** | Small Programmable Object Technology |
| **I/O** | Input/Output |
| **USB** | Universal Serial Bus |
| **M2M** | Machine-to-Machine |
| **MHz** | Megahertz |
| **CPU** | Central Processing Unit |
| **SRAM** | Static Random Access Memory |
| **G** | G-Kraft - Gewichtskraft |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **USART** | Universal Asynchronous Receiver Transmitter |
| **$I^2C$** | InterIntegrated Circuit |
| **mA** | Milli-Ampere |
| **EEPROM** | Electrically Erasable Programmable Read-Only Memory |
| **LED** | Licht-emittierende Diode |
| **RGB** | Rot, Grün und Blau |

# Kapitel 1

# Einleitung und Intention

Der Computer ist mittlerweile zum festen Bestandteil im alltäglichen Leben geworden. Mit ihm können viele Aufgaben wie Recherchen, komplexe Rechnungen und Kommunikation vereinfacht und schnellstmöglich erledigt werden. Während vor einigen Jahren noch der Desktop-PC die beliebteste Wahl darstellte, geht der Trend mittlerweile in Richtung der mobilen Endgeräte wie z.B. Smartphone, Laptop oder auch Tablet. Menschen wollen sich nicht an einen Ort binden, an dem sie ihren Computer benutzen können und sehnen sich nach dem Wunsch, dass alle Alltagsgegenstände per Smartphone oder Tablet kontrollierbar werden.

Diese Vernetzung aller elektronischen Geräte in einem Haushalt wird als "Internet of Things"(kurz IoT) bezeichnet. Die grundsätzliche Idee besteht darin, dass alle elektronischen Geräte wie z.B. Kühlschrank, Backofen u.a. miteinander kommunizieren können und der Nutzer über sein mobiles Endgerät alle Daten der vernetzten Geräte einsehen und diese auch auf seinen Wunsch hin steuern kann. Nähere Informationen zu IoT folgen im nächsten Kapitel.

Zur beispielhaften Demonstration des Aufbaus eines solchen Netzes elektronischer Geräte beschäftigt sich diese Studienarbeit mit Oracle SunSpot, einem Sensornetzwerk bestehend aus 2 Sensoren und einer Basisstation. Im Folgenden wird die Inbetriebnahme und Programmierung dieser Sensoren vorgenommen und die darin enthaltene Technik erklärt. Ziel der Studienarbeit ist es, mit Hilfe von SunSpot eine rudimentäre Raumüberwachung zu programmieren, indem bewegte Fenster oder Türen bei Abwesenheit des Besitzers der Wohnung erkannt werden, die Basisstation die Werte sammelt und sie an den Besitzer meldet.

## 1.1 Ziel dieser Arbeit

Hier werden wir das Ziel dieser Arbeit sowie das erwartete Ergebnis niederschreiben. Im Fazit kann hierauf Bezug genommen werden, um rückblickend den Erfolg dieser Arbeit zu messen.

# Kapitel 2

# Internet of Things

Als im Februar 1946 ENIAC, der erste elektronische sowie programmierbare Universalrechner vorgestellt wurde, wog dieser 27 Tonnen und füllte einen gesamten Raum. Für private Anwendungen waren diese Rechnersysteme nicht geeignet. Mit der voranschreitenden Entwicklung werden Computer immer kleiner und leistungsfähiger. Es erschließen sich immer neue Anwendungen von Computersystemen, die hauptsächlich den Menschen in seinem Alltagsleben unterstützen sollen.

Rund um 1990, als das Internet kommerzialisiert und somit für jeden zugänglich wurde, begann eine rasante Entwicklung neuer Technologien. Bis heute hat es unsere Arbeitsweise sowie unser Privatleben verändert und dieser Trend schreitet ungebremst voran.

Mit dem Web 2.0 wurden Webseiten interaktiv sowie Videos und Bilder im Internet eine Selbstverständlichkeit. Soziale Netzwerke verbinden die Nutzer durch verschiedenste Arten der Kommunikation. Dieses sich immer weiter aufspannende Kommunikations- und Informationsnetz, erreicht nun auch unsere kleinsten elektronischen Geräte.
Das Haus wird durch ein komplexes Sicherheitssystem überwacht, die Tür benötigt nur den Fingerabdruck um sich automatisch zu öffnen, der Fernseher reagiert auf Spracheingaben und in der Zukunft erstellt der Kühlschrank autonom den Einkaufszettel.

All diese Informationen werden über das Internet zu einer zentralen Sammelstelle oder dem Menschlichen Akteur zugespielt, das Internet of Things (IoT) ist entstanden.

## 2.1 Geschichte

Etwa um 1982 ärgerten sich drei Studenten der School of Computer Science, an der Carnegie Mellon University über den Getränkeautomaten ihres Instituts. An manchen Tagen liefen sie zu dem Automaten und erhielten entweder keine Getränke, oder zu warme, da diese erst kürzlich nachgefüllt wurden. Um diese Problematik zu lösen entwickelten die Studenten John Zsarnay neue Hardware die mit Software von David Nichols und Ivor Durham die Füllstände, sowie die Temperatur der Getränke überwachte [Car98].
Über den damals an der Universität vorhandenen Vorgänger des Internets, das sogenannte Arpanet konnte direkt beim Automaten der aktuelle Status nachgefragt werden. Dieser antwortete zum Beispiel mit:

```
1 >                    EMPTY    EMPTY    1h 3m
2 >                    COLD     COLD     1h 4m
```

Hiermit informierte der Automat darüber, dass kalte Getränke in der mittleren sowie linken Schiene vorhanden seien, die Getränke der rechten Schiene jedoch noch warm seien. Die angegebene Zeit informierte darüber, wie lange die Getränke sich bereits im Automat befanden. Nach drei Stunden nahm der Automat an Getränke seien ausreichend gekühlt.

Bereits 1991 schrieb der Amerikanische Informatiker Mark Weiser eine Vision, wie technische Geräte der Zukunft untereinander vernetzt sein könnten [Wei91]. Den Namen IoT erhielt das ganze jedoch erst 1999.

## 2.2 Ziele und Anwendungsbeispiele

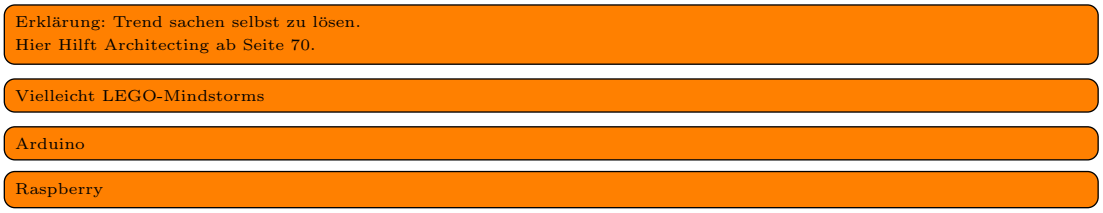
Aus Spielereien und purem Erfindergeist wurden in wenigen Jahren eine ganze Industrie, die sich heute nur mit Produkten des IoT beschäftigt. Es entstanden bereits viele Projekte, denen man im Alltag begegnet, ohne sie Wahrzunehmen. Diese lassen sich in 3 Hauptkategorien unterteilen, die gleichzeitig die Ziele des IoTs darstellen:

- Automatisierung
- Informationsgewinnung über bessere Vernetzung
- Entertainment

In der folgenden Tabelle haben sind einige der Erfolgreichsten davon Zusammengestellt.

- Umweltsensoren (Temperatur Feuchtigkeit Erschütterung Lautstärke Luftzusammensetzung)
- Lichtsteuerung
- Haushaltshilfen
- Bestandsaufnahme / Nachfuhrkontrolle
- Überwachungsfunktionen
- „Smart Signs“ - Autobahn
- Entertainment
- Haussteuerung
- Prozessüberwachung (Ventile, Flussraten usw.)
- Diagnose / Lebensüberwachung usw.

## 2.3 Do It Yourself - Trend




## 2.4 Sicherheitsaspekte

Über das Internet werden immer mehr Informationen versendet. Ein kleiner Bestandteil hiervon sind auch die Informationen die verschiedene Geräte des IoTs untereinander austauschen. Diese automatisch abgewickelte Machine-to-Machine (M2M)-Kommunikation stellt ein hohes Sicherheitsrisiko für Unternehmen und Privatpersonen dar. Durch einen gezielten Angriff könnten personenbezogene oder sicherheitsrelevante Informationen an die Öffentlichkeit gelangen. Aufgrund dessen müssen sich die Verantwortlichen die Frage stellen, wie man mit dieser Herausforderung in der Zukunft umgeht.

Sicherheitsexperten sind sich bereits heute einig, dass das IoT ein enormes Risiko darstellt [Wil15]. Für Privatpersonen äußert sich das hauptsächlich in der Sicherheit ihrer Elektronischen Geräte. So musste der Automobilhersteller BMW kürzlich ein Softwareupdate für seine Automobile mit dem ConnectedDrive-System ausliefern, da es Hackern ohne Spuren zu hinterlassen gelungen war, die Türen mittels Smartphones zu öffnen [ZEI15].

Zusätzlich zur Beschädigung oder Entwendung von Eigentum durch Hacker besteht ein Risiko private Informationen zu verlieren. Gerade Informationen wie E-Mail-Adressen oder Passwörter stehen in großem Interesse der Hacker. Solche könnten über ein privates IoT entwendet werden und für weitere Cyber-Kriminelle Aktionen genutzt werden.

Auch Firmen müssen sich die Risiken bewusst machen, die sie durch die Benutzung von IoT-Geräten eingehen. Oftmals nutzen Unternehmen IoT-Systeme als Infrastrukturkomponenten über die sie einen Service betreiben. Solche Netze stellen einen Idealen Angriffspunkt für Wirtschaftsspionage oder Denial of Service - Attacken dar

DO NOT USE THIS: IS COPIED:

Die Sicherheitsexperten sind sich heute bereits einig, dass die Sicherheitsbedrohungen des Internet der Dinge enorm hoch sind und diese möglicherweise sogar die Verbreitung dieser Systeme erheblich verzögern kann. Da die IoT-Systeme wichtige Infrastrukturkomponenten darstellen, sind diese natürlich ein hervorragendes Ziel für eine Wirtschaftsspionage, Denial of Service- und andere Angriffen. Ein weiterer wichtiger Aspekt ist die bereits von den Datenschützern geäußerte Sorge, dass durch IoT noch mehr persönliche Daten in den Netzen verfügbar sein werden, die möglicherweise Ziele für Cyber-Kriminelle darstellen.

Man muss bei Bewertung der Sicherheitsanforderungen für das Internet der Dinge jedoch im Auge behalten, dass sich diese Technologie erst im Anfangsstadium befindet und viele Aspekte heute noch nicht absehbar sind. Das IoT wird sich auch nicht über Nach entwickeln, sondern allmählich an Bedeutung gewinnen. Einige Dinge sind bereits mit dem Internet verbunden, aber wir werden zukünftig einen Boom an autonomen Maschinen erleben, die eigenständig ihre Informationen untereinander austauschen.

Die erwartete explosionsartige Zunahme der IoT-Komponenten und -Objekten, welche mit anderen Maschinen/Objekten bzw. Menschen in Echtzeit (oder annähender

Echtzeit) ihre Daten austauschen, muss die Sicherheit in einer M2M-Welt zu einem festen Bestandteil der Lösung werden.

Zu den wichtigsten Sicherheitsüberlegungen bei IoT gehört, dass jedes Objekt, sei es ein LKW, ein Automaten oder eine Medizinflasche, zu ein Teil der Netzwerkumgebung wird. Das IOT sorgt für die virtuelle Präsenz eines physischen Objekts. Diese virtuelle Präsenz interagiert mit anderen Geräten und tauscht Kontextinformationen aus. Auf Basis dieser Informationen treffen die Geräte ihre logischen Entscheidungen. Da diese Objekte zukünftig fester Bestandteil einer vernetzten Umgebung sind, müssen wir erkennen, dass diese Geräte ihre physische Sicherheit verlieren. Viele diese Geräte werden jedoch in unwirtlichen Umgebungen installiert und können dadurch von nicht autorisierten Person leicht erreicht werden. Angreifer können die Daten möglicherweise abfangen, mitlesen oder verändern. Mit handelsüblichen IoT-Geräten lassen sich die Daten somit für jeden beliebigen Zweck manipulieren. Dies ist bei der Risikobetrachtung dieser neuen Komponenten einzukalkulieren.

Vor Jahren wurden die klassischen PC-Drucker gegen netzwerkfähige Geräte ausgetauscht. Dadurch wurde aus einem klassischen Arbeitsgerät ein Sicherheitsrisiko. Jeder Netzwerkdrucker verfügt über einen integrierten (Web) Server. Greift man über einen Browser auf das Gerät zu, erhält man die komplette Steuerung über das Gerät. Standardmäßig verfügen die meisten Netzwerkdrucker über ein "BlankPasswort. Die Passworte können geändert werden, wenn der Administrator seine Hausaufgaben korrekt erledigt. Ein weiteres Problem mit diesen Geräten ist das Patch/Upgrade-Management. Die integrierten Server sind anfällig für Angriffe. Ein Patch/Upgrade eines in einem netzwerkfähigen Druckers ist keine einfache Sache. In der Regel muss hierbei ein Firmware-Upgrade vorgenommen werden. Damit ist der Besitzer/Administrator auf den jeweiligen Hersteller des netzwerkfähigen Druckers angewiesen. Stellt dieser keine neue Firmware zur Verfügung, dann bleiben die Sicherheitsprobleme im Drucker bestehen. Die integrierten Server und die Probleme der Patches/Upgrades sind zwei Problembereiche, die auch bei IoT-Komponenten auf uns zukommen.

Es geht nicht um Panikmache, denn Sicherheitsvorfälle von IoT-Implementierungen sind bereits bekannt geworden. Die meisten Beispiele stammen jedoch aus Labor -oder Testumgebungen. Da diverse Bedrohungen bereits Realität sind, wundert es doch, dass diese in der Öffentlichkeit kaum wahrgenommen werden. Erst kürzlich haben Forscher zwei Autos gehackt und drahtlos die Bremsen deaktiviert und die Lichter ausgeschaltet - alles außerhalb der Kontrolle des Fahrers. In einem anderen Fall wurde das GPS-Signal manipuliert und die Frachtschiffe auf einen

falschen Kurs gelockt. Auch die Home Control Hubs sind sehr verletzlich, so dass die Angreifer die Heizung, die Beleuchtung, die Stromzufuhr und die Türschlösser manipuliert werden können. Auch lassen sich industriellen Steuerungssysteme ist das drahtlose Netzwerk und der Sensoren leicht hacken.

Gehackt Fernseher, Videokameras und Baby-Phones gehören heute quasi zum Alltag und hegen natürlich die Bedenken gegenüber diesen Geräten, hinsichtlich der Privatsphäre und der Datensicherheit. Früher manipulierte man die Stromzähler im Haus um "kostengünstigän elektrische Energie zu kommen. Heute muss man nur noch über das Internet in diese Geräte einbrechen und schon ist die nächste Stromrechnung öptimiert.

In einem kürzlich erschienenen Artikel sprach der Autor von einer "gehackt Glühbirne". So absurd diese Vorstellung klingt, so realitätsnah sind jedoch deren Wirkungen. Ein Wurm, der eine große Anzahl von diesen im Internet verfügbaren IoT-Geräten infiziert, kann über ein Botnetz jede beliebige Information einsammeln und für diese für seine Zwecke missbrauchen. Ein weiteres Angriffsszenario zielt auf die verfügbare Bandbreite ab. Mit einem gezielten DDoS (Distributed Denial-of-Service) Angriff lassen sich alle IT-Komponenten vom Netz nehmen. Oder man stelle sich vor, alle kompromittierten IoT-Geräte in einem Unternehmen greifen gezielt mit hohen Anfrageraten auf die Steuerungsrechner zu und bringen diesen zum Erliegen bzw. zum Absturz.

Das Internet der Dinge schafft somit relativ komplexe sicherheitspolitische Herausforderungen für die Unternehmen. Als autonome Maschinen sind diese in der Lage, mit anderen Maschinen zu interagieren und selbständig Entscheidungen zu treffen. Diese Entscheidungen haben direkte Auswirkungen auf die reale Welt. Wir kennen ähnliche Probleme mit automatischen Trading-Systemen in Banken. Ein kleines Softwareproblem kann bereits zum Absturz ganzer Börsensystem führen und kann zu Folgekosten im Millionenbereich führen.

Alle IT Systeme lassen sich fehlertolerant auslegen bzw. aufbauen. Da die genutzte Software von Menschen die fehlbar sind, programmiert wurden, können auch auf einem vermeintlich ßicherenSSystem immer wieder Fehler auftreten.

Sicherheitsbedrohungen von IoT-Systemen haben direkte Auswirkungen auf eine Menge von Menschen. Wenn die Sicherheit eines der aktuellen IT-System ausfällt können werden eventuell ein paar hundert Kreditkartendaten gestohlen oder ein Politiker bloßgestellt. Alles kein großes Problem. Stellen wir uns stattdessen vor, ein zentrales Leistungssystem wird gehackt und die Einbrecher schaltete das Licht eines Teils oder einer ganzen Stadt während der Morgenstunden aus. Tausende von Menschen stecken auf einmal in den U-Bahnen unter der Erde in

völliger Dunkelheit fest und die Produktionsbetriebe dieser Stadt können keine Waren mehr herstellen. Der Unterschied zwischen den beiden Angriffsszenarien massiv. Mit Hilfe von IoT interagiert die virtuelle Welt mit der physischen Welt und dies erfordert ein höheres Sicherheitsniveau.

In der derzeitigen IoT-Entwicklungsphase werden noch traditionelle Sicherheitslösungen im IoT-Markt vorausgesetzt. Das Netzwerk stellt in diesem Fall noch alle Sicherheitsfunktionen bereit. Erst in der nächsten Entwicklungsphase wird die Netzwerksicherheit durch zusätzliche IoT-Sicherheitsfunktionen (welche auf Chip-Ebene, auf einer SIM-Karte oder auf M2M-Modulen integriert sind) ergänzt. Ein Zukunftsszenario sieht vor, dass die M2M-Anwendungen eines Tages sämtliche Sicherheitsrisiken abdecken und eine vollkommen eigenständige Sicherheitslösung bereitstellen.

Das Internet der Dinge formuliert wesentliche Fragen zur Sicherheit neu. Den Verlust der Privatsphäre, die künftige Vermischungen von persönlichen und betrieblichen Daten und das Monitoring. Der Verlust der Privatsphäre hängt vom jeweiligen Aufenthaltsort (im Unternehmen, Unterwegs oder Zuhause) der betreffenden Person und dessen Handlungen (beispielsweise welches Produkt die Person gerade erwirbt) ab. Die meisten Nutzer von Handys halten diese Geräte rund um die Uhr betriebsbereit und sind permanent im Mobilfunknetz eingebucht. Anhand der Mobilfunkmasten lassen sich unsere Bewegungen bereits heute permanent verfolgen. Anhand der aktuellen Verbrauchsdaten eines intelligenten Stromzählers lässt sich darauf schließen, ob ein Nutzer sich in seinem Haus oder Unterwegs befindet. Der Stromverbrauch lässt auch Rückschlüsse zu, ob wir Nachtschwärmer oder Frühaufsteher sind.

Die Trends des ITK-Markts wie beispielsweise Cloud Computing, Mobilität und Big Data, wirkt sich auf die Sicherheitsanforderungen der Unternehmen und den Risikobetrachtungen direkt aus und beeinflussen auch die Sicherheitsanforderungen der M2M-Architekturen. Bei der Vermischungen von persönlichen und betrieblichen Daten stehen wir vor der gleiche Herausforderung, wie wir sie vom Einsatz der mobilen Technologien am Arbeitsplatz und dem Bring Your Own Device (BYOD) Trend her kennen. Smartphones gehören heute zum Arbeitsalltag. In manchen Fällen werden die Geräte vom Unternehmen, in anderen Fällen vom jeweiligen Nutzer beschafft. Natürlich gibt es inzwischen auch für die BYOD-Probleme technische Lösungen, wie beispielsweise die Datenverschlüsselung und die Möglichkeit zum Remote Löschen von Informationen. Letztere Lösung wirft jedoch einige rechtliche Probleme auf: Darf das Unternehmen legal die Daten eines Anwenders auf dessen privaten Gerät löschen?

Die enorme Anzahl von IoT-Geräten und -Gegenständen, die zukünftig durch M2M in die Kommunikationsnetze angeschlossen werden, integrieren die Unternehmensabläufe noch tiefer in die Unternehmenskommunikation. Big Data wird nicht nur ein Schlagwort ohne Hülle sein, sondern durch das Internet der Dinge mittelfristig in jedem Unternehmen an Relevanz gewinnen. Aus diesem Grund ist es notwendig, dass sich die Unternehmen auf Basis einer wohldefinierten Risikoanalyse die Themen Datensicherheit, Vertrauen und Privatsphäre untersuchen und auf Basis dieser Ergebnisse eine entsprechende Sicherheitspolitik ableiten.

Die von den Marktanalysten für das Jahr 2020 vorausgesagten 50 Milliarden IoT-Komponenten legen die Grundlage für eine umfassend "vernetzte Gesellschaft". In den verbleibenden sieben Jahren, müssen daher die IT-Branche sowie die zuständigen Standardisierungsgremien für tragfähige und nachhaltige Rahmenbedingungen schaffen, damit sich die Bedürfnisse der "digitalen Unternehmenünd der "digitalen Bürgerïn der nächste Generation von M2M/IoT-Lösungen wiederfinden.

Sicherheitsnormen für das Internet der Dinge Das Internet der Dinge beruht auf dem Konzept der Identitäten. Diese schließen sowohl reale Nutzer als auch "Dinge"(Objekte) ein. Daher erscheint es zwingend notwendig, also, dass sich die Hersteller von IoT/M2M-Komponenten auf verbindliche Identity-Standards einigen. Dies beinhaltet die allgemeingültige Definition von Elementen und deren Identitäten, ein standardisiertes Modell zur Objekt-Identifikation und Authentifizierung. Erst die Verabschiedung von Standard-Kommunikationsprotokollen für IoT ebnet den Weg in den Mainstream. Beispiele hierfür sind das Message Queuing Telemetrie Traffic (MQTT) Protokoll, dem M2M Äquivalent zu HTTP. Ebenso müssen Mechanismen gefunden werden, die eine Interoperabilität zwischen verschiedenen Objekten und Services garantiert

Es müssen die Fehler der Datenkommunikation vermieden werden. Die Sicherheit darf nicht mehr nachträglich an die eigentlichen Kommunikationsfunktionen angeflanscht werden.

Sicherlich werden die Sicherheitsfunktionen nicht von Anfang an in die IoT-Objekte integriert werden. Dies hat oft den Grund, dass meist ein Mangel an lokalen Ressourcen oder Kapazitäten besteht. Die Sicherheit wird daher zuerst in den zuständigen Web-Diensten implementiert werden, welche direkt vor dem Objekt arbeiten und deren Funktionalität bereitstellen. Die jeweiligen Objekte werden sich auf die Themen Integrität der Nachrichten und der Absicherung der Kommunikationsflüsse konzentrieren. Mit den Entwicklungsfortschritten . wird

die Sicherheit näher an das Objekt heranrücken und eines Tages direkt auf der Chip-Ebene eingebettet werden.

# Kapitel 3

# Theoretische Grundlagen

In diesem Kapitel erklären wir kurz, dass wir in den folgenden Unterkapiteln Grundlagen erklären. Worum es sich hierbei handelt können Sie den folgenden Kapiteln entnehmen.

## 3.1 Wireless Sensor Networks

Hier wird alles zu Wireless Sensor Networks erklärt. Bisher steht das erst als Gerüst.

### 3.1.1 Ubiquitäres Rechnen

1988 verwendete Mark Weiser erstmals den Begriff 'ubiquitous computing' (dt. ubiquitäres Rechnen), um seine Vision nach einem stets verfügbaren Rechensystem, welches dem Nutzer unsichtbar erscheinen soll, zum Ausdruck zu bringen. Der Computer soll sich so in den Alltag integrieren, dass die Menschen ihn gar nicht mehr bemerken. Nach seiner Vorstellung verbessere das ubiquitäre Rechnen die Erfahrungen, die man mit Computern macht, da die Rechner dem Nutzer nahtlos verfügbar gemacht werden, ohne dabei effektiv sichtbar zu sein.

Weiser zufolge sind die besten Technologien diejenigen, die scheinbar verschwinden, tatsächlich jedoch nur in den Hintergrund geraten und unsichtbar werden. Der Mensch soll nicht in der Welt des Computers leben, sondern der Rechner soll sich in die Welt des Menschen integrieren. In Lichtschaltern, Thermostaten, Stereoanlagen und Backöfen werden bereits heute kleine Rechner verbaut, die helfen sollen, den Alltag zu erleichtern und die Idee des 'Internet of

Things' weiter zu verfolgen.

Da Ubiquitäres Rechnen zuverlässig und unsichtbar funktionieren soll, ist die Technologie der unsichtbaren Rechenmodule von großer Bedeutung. Voraussetzungen sind z.B. leistungsstarke Prozessoren, ausreichend Speicherplatz, drahtlose Kommunikation, Sensoren und Aktoren (die z.B. mit der Umwelt und dem Menschen interagieren). Der Mensch muss nicht für alle Anwendungsfälle von ubiquitärem Rechnen direkt eingebunden werden, da die Systeme auch autonom arbeiten können [WB12].

### 3.1.2 Motivation von Sensornetzen

Sensornetze sind sehr flexibel und können unter anderem dafür eingesetzt werden, um

- Umwelteinflüsse wahrzunehmen ('sensing')
- Umwelteinflüsse zu verarbeiten und zu analysieren ('computing')
- Daten zu übertragen ('transport')
- Netzwerke für verteile Systeme aufzubauen ('networking')
- Die Umwelt zu beeinflussen und zu verändern ('actuation')

Für viele Anwendungsfälle und Szenarien, in denen mit der Umwelt interagiert wird, soll die Benutzung von drahtlosen Sensornetzen zukünftig ausgebaut und etabliert werden. Der Einsatz von Sensornetzen kann dabei verschiedene Motivationen und Anforderungen haben:

- Direkte Interaktion mit Menschen ist nicht möglich oder nicht erforderlich (z.B. bei Überwachung einer Maschine in der Industrie)
- Der Mensch soll nur im Notfall alarmiert werden (z.B. in Notfällen oder wenn die Sensoren bestimmte Schwellenwerte erreichen)
- Es handelt sich um ein autonomes System, welches nur Selten das Handeln eines Menschen erfordert

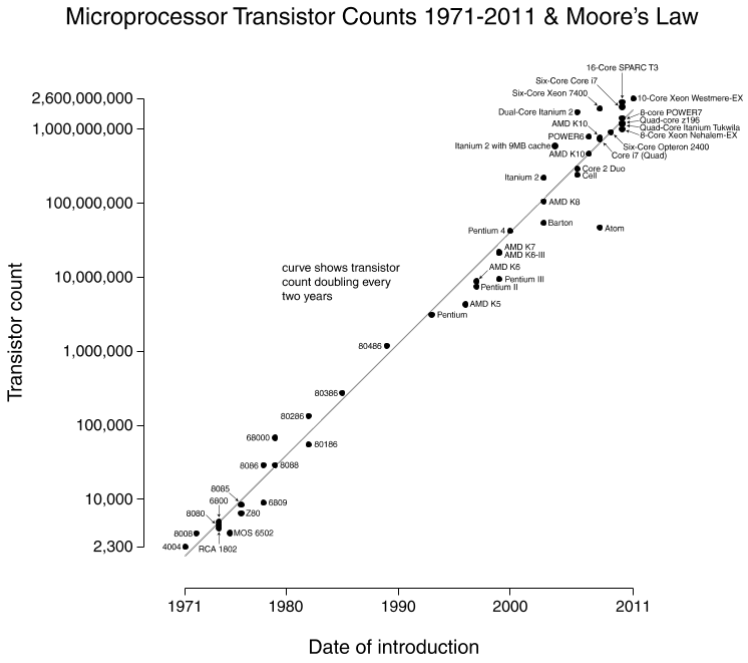



Abbildung 3.1: Mikroprozessoren-Transistoren im Laufe der Zeit [Wgs]

Eine weitere Motivation der Verwirklichung von drahtlosen Sensornetzen ist der Technologiefortschritt, der es möglich macht, immer kleinere Rechengeräte mit mehr Leistung herzustellen und miteinander zu vernetzen. Um diesen Fortschritt zu verdeutlichen, formulierte Gordon Moore 1965 ein Gesetz, welches besagt, dass sich die Anzahl der integrierten Schaltkreise auf einem Mikroprozessor alle 18-24 Monate verdoppelt. Im Gegensatz zu den Anzahl der Schaltkreise steigt die Rechenleistung der Prozessoren allerdings nicht linear an, da immer mehr Schaltkreise für den Cache des Prozessors verwendet werden, was nur geringfügig der Leistungssteigerung dient. Das Ende der Gültigkeit des Mooreschen Gesetzes wurde schon des öfteren wegen unüberwindbarer technischer Grenzen vorausgesagt, diese wurden jedoch bisher alle mit dem Einsatz neuer technischen Mittel und Materialien überwunden. Momentan schätzt der Halbleiterhersteller Intel, welcher 1968 von Moore mitbegründet wurde, dass das Mooresche Gesetz noch mindestens bis 2023 seine Gültigkeit behält. Mittlerweile existieren beim Konzern sogar explizite Pläne, die das Einhalten des Mooreschen Gesetzes sicherstellen sollen. [WB12] [Kah12] [Tuo02].

### 3.1.3 Bestandteile

Um die Kommunikation der einzelnen Knoten untereinander zu koordinieren, gibt es neben den normalen Sensoren weitere Bestandteile eines 'Wireless Sensor Network'.

Aktoren werden dazu benötigt, um das Sensornetz Einfluss auf die Umwelt nehmen zu lassen.

'Aggregating Nodes' werden dazu gebraucht, um die Daten von verschiedenen Sensoren zu sammlen, zu verarbeiten und zu kombinieren.

'Sink Nodes' sammeln die Daten von verschiedenen Sensoren und geben diese an die Basisstation bzw. das Backend-System weiter.

Backend-Systeme dienen zu weiteren Verarbeitung und Analyse der Daten. Diese sind von Vorteil, wenn z.B. komplexere Berechnungen durchgeführt werden sollen oder die Daten langfristig gespeichert werden sollen.

### 3.1.4 Topologien

Bei einem Aufbau eines Sensornetzes stellt sich grundsätzlich die Frage, wie die einzelnen Sensoren miteinander Verbindungen aufbauen und kommunizieren sollen. Ein solche Verbindungsstruktur nennt sich in der Informatik 'Topologie'. Da das Sensornetz insgesamt zuverlässig arbeiten soll, Kosten und Komplexität jedoch gering gehalten werden sollen, wurden speziell für die drahtlosen Sensornetze neue Ansätze im Bereich der Topologie erforscht. Im folgenden sollen 4 Topologie-Alternativen näher erläutert werden.

Peer-to-Peer Netzwerke erlauben es, das jeder Knoten im Netz (in unserem Fall der Sensor) mit jedem anderen Knoten direkt Kontakt aufnehmen kann. Jedes 'Peer-Gerät' ist gleichzeitig Client und Server gegenüber anderen Knoten im Netzwerk.

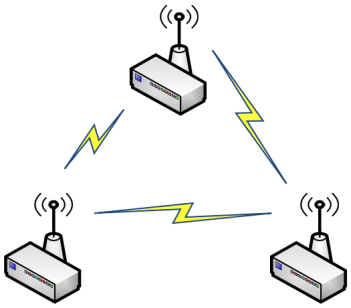


Abbildung 3.2: Peer-To-Peer Netzwerk [Kos09]

Bei der Stern-Topologie sind die Sensoren an ein zentrales Kommunikationsgerät angebunden. In diesem Fall kommunizieren die einzelnen Knoten nicht direkt miteinander. Jegliche Art von Kommunikation wird über das zentrale Gerät (auch Hub genannt) geroutet. Der Hub wird hier als Server betrachtet, wohingegen die Knoten (Sensoren) die Clients darstellen.

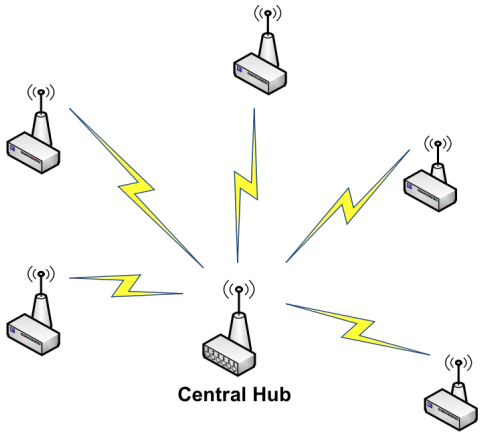



Abbildung 3.3: Stern Netzwerk [Kos09]

Die Baum-Topologie stellt eine Hybridvariante aus Peer-to-Peer und Stern dar. Sie nutzt einen sogenannten 'Root-Knoten' als zentraler Router. Eine Ebene darunter liegen die Hubs, an denen wie in der Stern-Topologie die Sensoren angebunden sind.

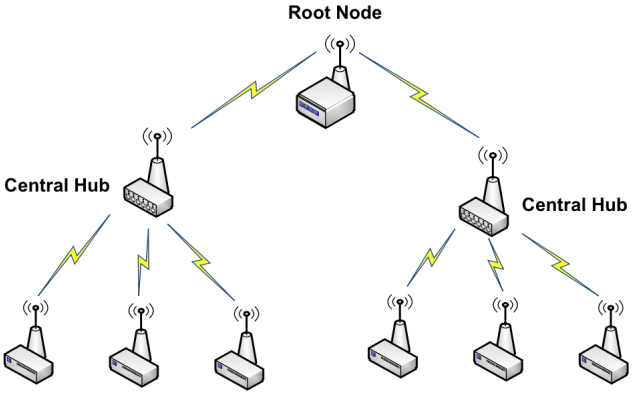



Abbildung 3.4: Baum Netzwerk [Kos09]

Eine weitere Mögliche Variante ist ein vermaschtes Netz. Die Knoten sind untereinander ohne zentralen Hub verbunden und die Daten werden einfach von Knoten zu Knoten weitergesendet, bis sie ihr gewünschtes Ziel erreicht haben [Kos09].

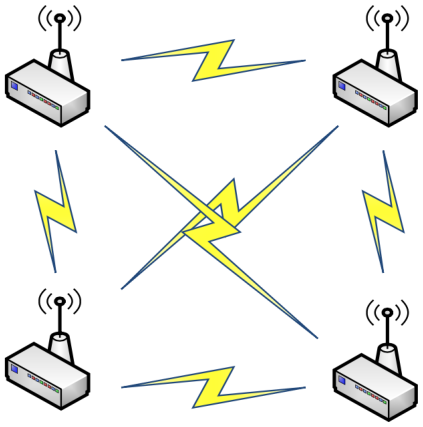


Abbildung 3.5: Vermaschtes Netzwerk [Kos09]

### 3.1.5 Schwierigkeiten

Beim Planen eines drahtlosen Sensornetzwerkes stellen sich vermehrt eine Schwierigkeiten heraus, die zu berücksichtigen sind. Viele dieser Schwierigkeiten sind auch untereinander abhängig und beeinflussen gleichzeitig die verwendete Elektronik, physikalische Aspekte, Rechenleistung oder auch Lebensdauer eines Sensors.

Die erste Schwierigkeit, die es bei einem Sensor zu betrachten gilt, ist die Versorgung des Sensors mit Energie. Dazu gibt es unterschiedliche Ansätze, wie z.B.

die Versorgung des Sensors mit Batterien. Dies hat allerdings den Nachteil, dass deren Lebenszyklus beschränkt ist und Batterien früher oder später ausgetauscht werden müssen. Ein Akkumulator eignet sich hier schon besser, allerdings bleibt die Frage, wie der Akkumulator mit neuem Strom versorgt werden soll.

In Zusammenhang mit dieser Fragestellung ist die Betrachtung der möglichen Gewinnung oder Rückgewinnung von Energie durch den Sensor von Vorteil. Wie kann ein Sensor Energie gewinnen, ohne dass er damit direkt versorgt werden muss? Möglichkeiten wäre die Gewinnung von Solarenergie durch den Sensor, das Nutzen von Temperaturunterschieden in der Umwelt, die Rückgewinnung der Bewegungsenergie (z.B. durch Wind o.ä.) oder das Ausnutzen von Erschütterungen und Vibrationen. Diese Möglichkeiten sollten nur in Betracht gezogen werden, wenn der Sensor eine lange Lebensdauer mit sich bringen soll. Ist der Einsatz der Sensoren in absehbarer Zeit vorüber, lohnt es sich aus Produktions- und Kostengründen die begrenzte Lebenszeit des Sensors hinzunehmen, um ihn danach z.B. durch neue Sensoren auszutauschen.

Ein weiterer wichtiger Aspekt im Bereich Energie ist die Energieeffizienz. Dabei sollen alle Teile in einem Sensorknoten möglichst effizient nutzen, um die Energie sinnvoll und langsam aufzubrauchen. Nicht nur der Sensor selbst spielt dabei eine wichtige Rolle, sondern auch wie das Netzwerk um ihn herum aufgebaut und genutzt wird. Folgende Aspekte spielen bei der Energieeffizienz eine erhebliche Rolle:

- Wahrnehmen der Daten durch die Sensoren
- Verarbeitung der Daten
- Sicherung der Daten
- Übertragung der Daten
- Empfang von Daten

Damit der Energieverbrauch weiter eingeschränkt werden kann, sollten Sensoren nur aktiv sein, wenn sie wirklich benötigt werden. Ansonsten sollten sie sich in einen Sleep- bzw. Energiesparmodus begeben, um Energie zu sparen. Des Weiteren wäre zur ausschließlichen Wahrnehmung der Umgebung ein "Controller- bzw. Sensormodus und zum Senden und Empfangen von Daten ein "Radio bzw.

Übertragungsmodus von Vorteil.

Eine weitere Schwierigkeit, die sich stellt, ist der Einsatz bzw. die Verteilung der Sensoren in der Umwelt und ihre Selbstverwaltung. Die Knoten könnten entweder zufällig in der Umgebung platziert oder systematisch angeordnet werden. Hier entscheidet der jeweilige Anwendungszweck, wobei das systematische Platzieren der Sensoren meistens sinnvoller und effizienter ist. Des Weiteren sollte unterschieden werden, ob aktive oder passive Sensoren eingesetzt werden sollen. Auch hier muss je nach Anwendungsfall unterschieden werden. Passive Sensoren eignen sich besser, wenn Daten nur erfasst und übermittelt werden sollen. Aktive Sensoren sollten eingesetzt werden, wenn auf die Erfassung der Daten eine eventuelle Aktion bzw. Reaktion mit der Umwelt erforderlich ist.

Sensoren sollten bestimmte Informationen über sich selbst und ihre Nachbarn wissen bzw. ermitteln können. Dazu gehören unter anderem ihre eigene Position, die Ortung der Nachbarknoten und ihre Identifikation, ihre eigene Knotenkonfiguration und ihre kürzeste Route zu einer Basisstation. Denn sobald ein Sensornetz einmal in Betrieb genommen wurde, muss es in der Lage sein, sich autonom betreiben und verwalten zu können. Dazu zählen die Anpassung an veränderte Umweltbedingung und das Kompensieren von Fehlern. Beim Ausfall eines Sensors soll das Sensornetz weiterhin aktiv und funktionsfähig bleiben.

Auch in Hinsicht auf die Sicherheit gibt es einige Aspekte zu betrachten. Manche Sensornetzwerke übertragen empfindliche und kritische Informationen, was sie zu einem beliebten Angriffsziel macht. Sie können sowohl von innen, von außen als auch direkt an den Knoten angegriffen werden. Es stellt sich als schwierig heraus, solche Netzwerke vor Angriffen zu schützen, da sie entfernt und selbstständig arbeiten, drahtlos kommunizieren und meistens keine speziellen Sicherheitsfeatures besitzen. Dies ist aus Energie-, Kostengründen und Gründen der Form und Größe der Sensoren meist nicht realisierbar. Übliche Sicherheitstechniken sind meist nicht durchführbar, da den Knoten üblicherweise die Rechen-, Kommunikations- und Speicherressourcen fehlen. Man braucht neu entwickelte Sicherheitsmechanismen für Sensornetze, die spezielle Lösungen für die Erkennung von Eindringlingen, Verschlüsselung, Schlüsselverwaltung und Verteilung und Registrierung von neuen Knoten besitzen, sodass die Ressourcen der Sensoren ausreichen und das Sicherheitskonzept realisierbar ist [WB12].

### 3.1.6 Adhoc-Netzwerke

Inhalt kommt hier auch noch rein.

### 3.1.7 IEEE 802.15.4

Und hier kommt ebenfalls noch Inhalt rein.

## 3.2 SunSPOT

Die Firma Oracle besitzt im Rahmen seiner Java-Technologie eine Vormachtstellung im Bereich der Smartphones. Auf der Welt sind schätzungsweise über eine Milliarde Smartphones mit der Java-Technologie lizenziert. [Hor08]
Ziel von Oracle ist es, auch in den zukunftsnahen Technologien mit ihrer Programmiersprache Java auszustatten und diese Produkte zu etablieren.

Ein erster Schritt in diese Richtung is das von Oracle entwickelte “SunSPOT“-Sensornetzwerk. SunSPOT bedeutet “Sun Small Programmable Object Technology“ und ist eine Plattform für Java-basierte drahtlose Sensornetzwerke. Sie bestätigt den Trend, dass in immer kleiner werdenden Geräten zunehmend leistungsfähigere Technologien eingesetzt werden. Dabei ist wichtig, dass jene Geräte, am Besten drahtlos, miteinander kommunizieren können und jederzeit von überall auf der Welt steuerbar bleiben. Das SunSPOT Starter Paket besteht aus einer Basisstation und 2 Sensoren.

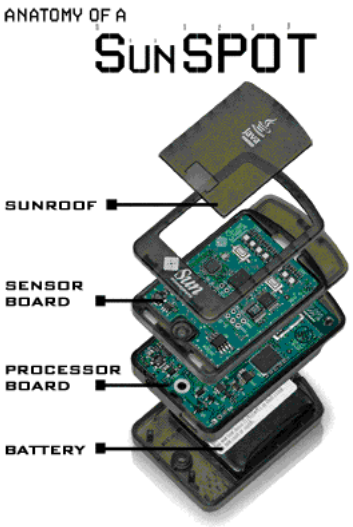



Abbildung 3.6: Anatomie eines Standard SunSPOT-Sensors [Uni]

Die Hardware der SunSPOT-Sensoren ist modular aufgebaut. Das bedeutet, dass man die verfügbaren Boards frei nach Belieben aufeinander stecken und somit verbinden kann. Dabei können maximal bis zu 3 Boards + Stromversorgung miteinander verknüpft werden. [Hor08]

### 3.2.1 Technische Daten

Das sogenannte eSPOT Prozessor-Board besitzt in der aktuellsten Version eine 400 MHz 32-bit ARM CPU von Atmel, zusammen mit einem Flashspeicher von 8 Megabytes und einem Megabyte SRAM Hauptspeicher. Weiterhin ist es ausgestattet mit einem Radio Transceiver basierend auf IEEE 802.15.4 und einer USB 2.0 - Full Speed Schnittstelle. Der im SunSPOT integrierte Akkumulator hat eine Leistungsfähigkeit von 770mAh. Der maximale Energieverbrauch liegt zwischen 40-100 mA, abhängig von der Nutzung der integrierten LEDs, des Transceivers und anderer angeschlossener Geräte. [Hor08] [Ora10b]

Der SunSPOT-Sensor wird dazu standardmäßig mit dem eDemo Sensor Board ausgeliefert. Dieses Board besitzt in der aktuellen Version einen 2G/4G/8G 3-Achsen-Beschleunigungssensor, einen Lichtsensor, 8 RGB 24bit LEDs, einen Infrarot-Sender & Empfänger, ein kleiner Lautsprecher, 2 Knopfschalter, 4 analoge Eingänge, 4 I/O Pins, diverse weitere $I^2C$- und USART-Interfaces, einen EEPROM und 4 100mA Ausgangspins, mit denen es möglich ist, den SunSPOT-Sensor z.b. an weitere Lautsprecher oder andere Geräte anzuschließen. [Hor08] [Ora10a]

Weitere Boards, welche man nach Bedarf dazustecken kann, sind das eProto-Board, ein Board welches direkte Zugriffe auf das Prozessorboard ermöglicht und einen SD-Kartenslot besitzt, damit man die Daten dauerhaft speichern kann, das eSerial Board zum Verbinden via RS232 und das eFlash SD-Kartenleser Board. [Hor08]

# Kapitel 4

# Praktische Arbeiten mit SunSPOT

Das ist das normale Todo, inline.
Mit dem \newline Befehl erzwingt man eine neue Zeile.

In diesem Kapitel werden wir die praktischen Arbeiten, die wir mit SunSPOTS durchführen erläutern. Dies wird in zwei Unterkapiteln durchgeführt. Man sollte damit das hier besser aussieht auch viel Text haben. Wenn nur eine Zeile unterstrichen ist sieht das nicht ganz so gut aus.

Also das hier ist ein Improvement und ist einfach in einer anderen Farbe.

Das nach dem \unsure Befehl folgende wird bis zum Zeilenende rot unterstrichen.

## 4.1 Erste Schritte

Hier erläutern wir unsre ersten Schritte im Praktischen Teil der Studienarbeit.

## 4.2 Implementierung einer Raumüberwachung

### 4.2.1 Idee

Hier kommt die Idee die wir hatten hin.

### 4.2.2 Visualisierung der Information

Beschreibung der Visualisierung unserer durch das Sensornetz gesammelter Informationen.

# Kapitel 5

# Zusammenfassung

Hier kommt die Zusammenfassung des Projektes hin. Diese besteht aus Beschreibung, Vorgehensweise und Ergebnis. Insgesamt umfasst sie etwa eine Seite.

# Anhang

## Beispielergebnis Bedienungsanleitungen

Manchmal benutzt man Worte wie Hamburgefonts, Rafgenduks oder Handgloves, um Schriften zu testen. Manchmal Sätze, die alle Buchstaben des Alphabets enthalten - man nennt diese Sätze »Pangrams«. Sehr bekannt ist dieser: The quick brown fox jumps over the lazy old dog. Oft werden in Typoblindtexte auch fremdsprachige Satzteile eingebaut (AVAIL® and Wefox™ are testing aussi la Kerning), um die Wirkung in anderen Sprachen zu testen. In Lateinisch sieht zum Beispiel fast jede Schrift gut aus. Quod erat demonstrandum. Seit 1975 fehlen in den meisten Testtexten die Zahlen, weswegen nach TypoGb. 204 § ab dem Jahr 2034 Zahlen in 86 der Texte zur Pflicht werden.

# Literaturverzeichnis


[Car98] Carnegie Mellon University Computer Science Department: *The Only Coke Machine on the Internet*. https://www.cs.cmu.edu/~coke/history_long.txt, Juni 1998

[Hor08] Horan, Bernard: *Sun SPOTs*. https://www.dropbox.com/sh/l2kch3izg7lwdpl/AADjbAi2ukAjtaZY8zVzMpdHa/IoT/sunspot.pdf, 2008

[Kah12] Kahle, Christian: *Intel: Mooresches Gesetz gilt noch mind. 10 Jahre*. http://winfuture.de/news,72001.html, September 2012

[Kos09] Kosmerchock, Steven: *Wireless Sensor Network Topologies*. http://www.k5systems.com/TP0001_v1.pdf, 2009

[Ora10a] Oracle Corp.: *Sun$^{TM}$ SPOT eDEMO Technical Datasheet Rev 8.0*. http://www.sunspotworld.com/docs/Yellow/edemo8ds.pdf, Oktober 2010

[Ora10b] Oracle Corp.: *Sun$^{TM}$ SPOT Main Board Technical Datasheet Rev 8.0*. http://www.sunspotworld.com/docs/Yellow/eSPOT8ds.pdf, Oktober 2010

[Tuo02] Tuomi, Ilkka: *The lives and deaths of moores law*. http://firstmonday.org/ojs/index.php/fm/article/view/1000/921, November 2002

[Uni] University of Southern California: *Standardmäßiger Aufbau eines SunSPOT-Sensors*. http://anrg.usc.edu/ee579_2012/Group07/img/spotanatomy.jpg,

[WB12] Wolf, Lars ; Büsching, Felix: *Wireless Sensor Networks - Introduction and Applications*. https://www.dropbox.com/sh/l2kch3izg7lwdpl/AABu1b-vt8FCuUD2iU905F0ca/IoT/

RecentTopics_Chapter02_WSN-Introduction-and-Applications.pdf, 2012

[Wei91] Weiser, Mark: *The Computer for the 21st Century*. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html, September 1991

[Wgs] Wgsimon: *Mooresches Gesetz*. http://commons.wikimedia.org/wiki/User:Wgsimon#mediaviewer/File:Transistor_Count_and_Moore%27s_Law_-_2011.svg,

[Wil15] Willems, Eddy: *IoT: The Internet of Things... ehm... / Ein Balance-Akt zwischen Benutzbarkeit und Sicherheit?!* https://tcadistribution.wordpress.com/tag/sicherheitsexperten/, März 2015

[ZEI15] ZEIT ONLINE, dpa, AFP, rav: *Hacker konnten BMW-Türen jahrelang per Handy öffnen*. http://www.zeit.de/mobilitaet/2015-01/bmw-hacker-sicherheit, Januar 2015

# Notes