Vom Internet der Computer zum Internet der Dinge

Friedemann Mattern, Christian Flörkemeier
ETH Zürich

Es wird in wenigen Jahrzehnten kaum mehr Industrieprodukte geben, in welche die Computer nicht hineingewoben sind.
Karl Steinbuch, 1966

Das Internet der Dinge steht für eine Vision, in der das Internet in die reale Welt hinein verlängert wird und viele Alltagsgegenstände ein Teil des Internets werden. Dinge können dadurch mit Information versehen werden oder als physische Zugangspunkte zu Internetservices dienen, womit sich weitreichende und bis dato ungeahnte Möglichkeiten auftun.

Die Vision

Die Vision vom Internet der Dinge beruht auf der Extrapolation des anhaltenden und uns fast zur Selbstverständlichkeit gewordenen Fortschritts von Mikroelektronik, Kommunikationstechnik und Informationstechnologie. Indem aufgrund ihrer abnehmenden Größe und ihres ständig zurückgehenden Preises und Energiebedarfs immer mehr Prozessoren, Kommunikationsmodule und andere Elektronikkomponenten in Gegenstände des täglichen Gebrauchs integriert werden, dringt Informationsverarbeitung, gekoppelt mit Kommunikationsfähigkeit, fast überall ein, sogar in Dinge, die zumindest auf den ersten Blick keine elektrischen Geräte darstellen. Damit rückt die bereits Anfang der 1990er-Jahre von Mark Weiser mit „Ubiquitous Computing“ [33] bezeichnete Vorstellung einer umfassenden Informatisierung und Vernetzung der Welt und ihrer vielen Gegenstände in greifbare Nähe. Diese schleichende aber nachdrückliche Entwicklung eröffnet große Chancen für Wirtschaft und Privatleben, birgt jedoch auch Risiken und stellt zweifellos eine gewaltige technische und gesellschaftliche Herausforderung dar.

Eine zentrale Rolle kommt in dieser Vision den „smarten“ (bzw. „intelligenten“) Objekten zu: Ausgestattet mit Informations- und Kommunikationstechnik und angebunden an den Cyberspace mit seinen mächtigen Diensten erhalten alltägliche Gegenstände eine neue Qualität: Diese können über Sensoren ihren Kontext wahrnehmen, sich miteinander vernetzen, auf Internetservices zugreifen und mit dem Menschen interagieren. Eine derartige, idealerweise nicht sichtbare „digitale Aufrüstung“ klassischer Gegenstände ergänzt deren physische Funktion um die flexiblen Fähigkeiten digitaler Objekte und schafft damit einen substanziellen Mehrwert. Vorboten dieser Entwicklung kündigen sich bereits an: Immer mehr Geräte wie Nähmaschinen, Heimtrainer, elektrische Zahnbürsten, Waschmaschinen, Stromzähler oder Fotokopierer werden „informatisiert“ und mit einer Netzschnittstelle ausgestattet. Drahtlos mit dem Laptop oder direkt mit dem Internet verbunden, erhalten sie so eine erweiterte Funktionalität.

Durch eine Internetanbindung lässt sich auch der Zustand von Geräten und Dingen aus der Ferne einfach ermitteln, und Informationssysteme können aktuelle Daten über physische Objekte und Vorgänge sammeln. Insbesondere können damit viele Realweltaspekte in bisher unerreichter Granularität und zu fast verschwindenden Kosten „gemessen“ werden, was sie oft erst im Detail verständlich macht und einer rationalen Lenkung und Bewirtschaftung zuführt [10]. Indem so automatisch, schnell und in informierter Weise auf Ereignisse der Realität reagiert werden kann, eröffnen sich nicht nur neue Möglichkeiten im Umgang mit komplexen oder kritischen Situationen, sondern dies erlaubt auch die Optimierung vielfältiger Wirtschaftsprozesse sowie die Bereitstellung ganz neuer Dienste, welche durch die

zeitnahe Interpretation von Daten aus der physischen Welt ökonomischen und gesellschaftlichen Nutzen stiften.

Für die oben skizzierte Vision hat sich der eingängige Begriff „Internet der Dinge" herausgebildet, der allerdings interpretationsbedürftig ist. Denn das Wort „Internet" kann dabei entweder nur als Metapher verstanden werden – analog dazu, wie wir Menschen das Web benutzen, kommunizieren bald auch Dinge auf irgendeine Art miteinander, verwenden Dienste, stellen Daten bereit und generieren dadurch einen Mehrwert – oder es kann im technischen Sinne enger aufgefasst werden, indem ein Protokollstack für den IP-Standard auf smarten Dingen (bzw. auf „Proxies" als deren Stellvertreter im Netz) postuliert wird. Eine weitere Interpretation erfährt das Internet der Dinge im Logistikbereich [3]: Dort versteht man darunter ein selbstorganisierendes Logistiknetz, das RFID (Radio Frequency Identification) als Technologie zur berührungslosen automatischen Identifikation von Transporteinheiten nutzt, sodass diese sich in Eigenregie durch Netzwerke von Warenumschlagplätzen bewegen können – sinnbildlich analog zu den Datenpaketen im gleichermaßen dezentral strukturierten Internet der Computer.

Populär wurde der Begriff vom Internet der Dinge durch das Wirken des Auto-ID Center am Massachusetts Institute of Technology (MIT), das ab 1999 eine firmenübergreifende RFID-Infrastruktur entwarf und propagierte.[1] Dessen Mitgründer und damaliger Leiter Kevin Ashton wird 2002 im Forbes Magazine mit „we need an internet for things, a standardized way for computers to understand the real world" [26] zitiert. Der Beitrag trägt den Titel „The internet of things" und stellt damit die erste dokumentierte Verwendung des Terminus im wörtlichen Sinne dar[2]; auf Deutsch taucht „Internet der Dinge" im gleichen Jahr auf [23]. In sinngemäßer Weise wird der Begriff aber bereits 1999 von Neil Gershenfeld vom MIT Media Lab in seinem populärwissenschaftlichen Buch „Wenn die Dinge denken lernen" [14] gebraucht: „Es kommt mir so vor, als sei das rasante Wachstum des WWW nur der Zündfunke einer viel gewaltigeren Explosion gewesen. Sie wird losbrechen, sobald die Dinge das Internet nutzen".

In den vergangenen Jahren hat sich der Begriff „Internet der Dinge" dann schnell verbreitet: 2005 fand er sich bereits in Buchtiteln [8, 19], und 2008 wurde die erste wissenschaftliche Konferenz dazu veranstaltet [12]. Von der europäischen Politik wurde der Terminus zunächst zwar nur im Zusammenhang mit RFID verwendet, die Namen der von der EU-Kommission veranstalteten RFID-Konferenzen waren jedoch durchaus programmatisch: „From RFID to the Internet of Things" (2006) und „RFID: Towards the Internet of Things" (2007). Ein spezifischer Aktionsplan der EU-Kommission zum Internet der Dinge aus dem Jahr 2009 versteht dann schließlich das Internet der Dinge im Sinne des allgemeinen Wandels des Internets „von einem Computernetz zu einem Netz untereinander verbundener Gegenstände" [6].

Grundlagen

Aus technischer Sicht steht hinter dem Internet der Dinge nicht eine einzelne Technologie oder eine spezifische Funktionalität; vielmehr tragen mehrere sich ergänzende sowie teilwei-

[1] Schon im ersten *White Paper* des Auto-ID Center [25] deutet sich allerdings eine über RFID hinausgehende Vision an: „The Center is creating the infrastructure […] for a networked physical world. […] A well known parallel to our networked physical world vision is the Internet."

[2] Kevin Ashton merkte dazu allerdings im Juni 2009 an: „I'm fairly sure the phrase *Internet of Things* started life as the title of a presentation I made at Procter & Gamble in 1999" [2].

se konvergierende Technikentwicklungen zu einem Funktionsbündel bei, welches in seiner Gesamtheit eine neue Qualität hervorbringt [9]. Zu diesen Funktionen gehören:

- *Kommunikation und Kooperation:* Objekte verfügen über die Möglichkeit zur Vernetzung mit Ressourcen im Netz oder sogar untereinander, um Daten und Dienste gegenseitig zu nutzen und ihren Zustand zu aktualisieren. Relevant sind hier vor allem funkbasierte Technologien wie GSM oder UMTS, Wi-Fi, Bluetooth, ZigBee und diverse absehbare Weiterentwicklungen, insbesondere im Bereich der Wireless Personal Area Networks (WPAN).
- *Adressierbarkeit:* Objekte im Internet der Dinge können über einen Discovery-, Look-up- oder Namensdienst gefunden und angesprochen und damit aus der Ferne abgefragt oder beeinflusst werden.
- *Identifikation:* Objekte sind eindeutig identifizierbar. RFID, NFC (Near Field Communication) oder optisch erkennbare Strichcodes stellen beispielsweise Technologien dar, mit denen – unter Zuhilfenahme eines „Mediators", wie etwa eines RFID-Lesers oder eines Mobiltelefons – sogar passive Dinge identifiziert werden können. Die Identifikation ermöglicht die Verknüpfung des Objekts mit zugehörigen Informationen, die auch von einem Server geholt werden können, sofern der Mediator mit dem Netz verbunden ist (vgl. Abb. 1).
- *Sensorik:* Objekte sammeln Informationen über ihre Umgebung, zeichnen diese auf, melden sie weiter oder reagieren direkt darauf.
- *Effektorik:* Objekte besitzen Effektoren zur Einwirkung auf die Umwelt (wie etwa Aktuatoren, die elektrische Signale in mechanische Arbeit umwandeln), womit ferngesteuert über das Internet Prozesse der Realität beeinflusst werden können.
- *Eingebettete Informationsverarbeitung:* Smarte Objekte besitzen einen Prozessor oder Mikrocontroller sowie Speicherkapazität. Damit kann beispielsweise sensorische Information verarbeitet und interpretiert werden, oder Produkte können ein „Gedächtnis" hinsichtlich ihrer Nutzung bekommen.
- *Lokalisierung:* Dinge kennen ihren physischen Aufenthaltsort oder sind für andere lokalisierbar. Hierfür kann GPS oder das Mobilfunknetz verwendet werden; aber auch Ultraschallzeitmessungen, UWB (Ultra-Wide Band), Funkbaken (z.B. benachbarte WLAN-Basisstationen oder RFID-Lesegeräte mit bekannten Koordinaten) und optische Technologien kommen zum Einsatz.
- *Benutzungsschnittstelle:* Smarte Objekte können in geeigneter Weise (direkt oder auch indirekt, etwa via Smartphone) mit Menschen kommunizieren. Relevant sind hierfür auch innovative Interaktionsparadigmen wie beispielsweise „tangible user interfaces" oder flexible Displays auf Polymerbasis, aber auch Methoden aus den Bereichen Sprach-, Bild- und Gestenerkennung.

Für konkrete Anwendungszwecke ist allerdings meist nur ein Teil dieser Funktionen nötig, zumal deren Realisierung in ökonomischer und technischer Hinsicht (z.B. bezüglich der Energieversorgung) oft aufwendig ist. So konzentrieren sich derzeit beispielsweise Logistikanwendungen auf die mittels RFID bzw. Strichcodes vergleichsweise billig erzielbare Identifikation und grobe Lokalisierung (Position der letzten Lesestation) von Objekten, und nur in wenigen Fällen werden dabei auch Sensordaten (z.B. zur Überwachung der Kühlkette) oder eingebettete Prozessoren genutzt. Einen anderen bedeutenden Anwendungsbereich stellen funkbasierte Sensornetze für die großräumige Überwachung dar. Hier stehen naturgemäß Sensorik und Kommunikationsfähigkeit zusammen mit einer minimalen lokalen Informationsverarbeitung im Vordergrund.

Insbesondere im Zusammenhang mit RFID lassen sich bereits Vorboten kommunizierender Alltagsgegenstände erkennen – wenn etwa die Schlüsselkarte über kurze Distanz mit der Hotelzimmertür kommuniziert oder der Skipass mit dem Drehkreuz vor dem Schlepplift. Noch deutlicher wird dies bei einem smarten Spielkartentisch, der den Spielverlauf anhand der ausgespielten (und „gechippten“) Karten verfolgt [11]. Bei allen diesen Anwendungen handelt es sich allerdings noch um dedizierte Systeme; von einem „Internet“ im Sinne eines offenen, skalierbaren und standardisierten Systems kann man dabei nicht sprechen.

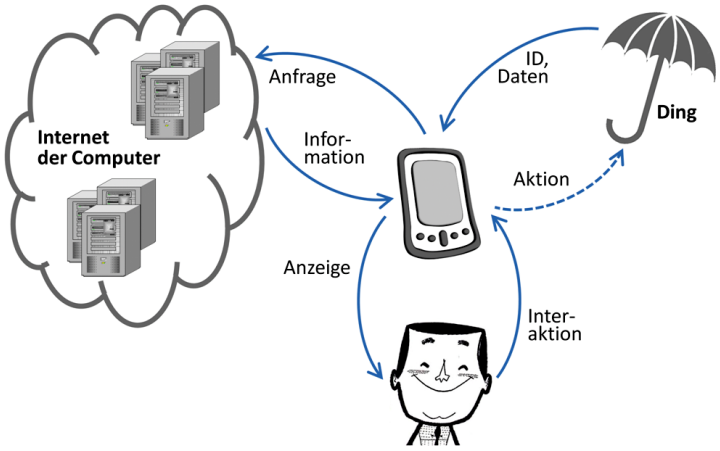

Abbildung 1. Das Smartphone als Mediator zwischen Mensch, Ding und Internet.

Indem nun aber Funkkommunikationsmodule immer kleiner und billiger werden, IPv6 sich zunehmend durchsetzt, Flash-Speicherchips hoher Kapazität zur Verfügung stehen, der Energiebedarf von Prozessoren pro ausgeführter Instruktion laufend zurückgeht und Handys mit optischer Strichcodeerkennung, NFC und Touchscreen ausgestattet werden – und diese damit eine Mittlerrolle im Dreieck Mensch, Ding und Internet einnehmen können (Abb. 1) –, wandelt sich langsam das Paradigma vom Internet der Dinge: Von der Fernidentifikation von Objekten und einem Internet „mit“ Dingen gelangt man zu einem System, wo (mehr oder weniger) smarte Gegenstände tatsächlich mit Nutzern, mit Internetdiensten und sogar untereinander kommunizieren. Dieses neue Potenzial der Dinge eröffnet spannende Perspektiven und interessante Anwendungsmöglichkeiten; damit einher gehen aber auch gewichtige Anforderungen an die zugrundeliegenden Technologien und Infrastrukturen. Für ein Internet der Dinge müssen diese Infrastrukturen effizient, skalierbar, verlässlich, sicher und vertrauenswürdig sein; aber auch allgemeinen gesellschaftlichen und politischen Erwartungen entsprechen, breit anwendbar sein und unter Berücksichtigung ökonomischer Aspekte betrieben werden können.

Treiber und Erwartungen

Was treibt die Entwicklung zu einem Internet der Dinge voran? Alleine schon der evolutionäre Fortschritt der Informations- und Kommunikationstechnik lässt kontinuierliche Produktverbesserungen zu, bei denen immer mehr Dinge kommunikationsfähig werden, wodurch deren Funktionalität erweitert und ergänzt wird. Beispiele hierfür sind Navigationsgeräte, die Meldungen über Verkehrsereignisse aus der Ferne beziehen und für die Sprachausgabe mit dem Autoradio kooperieren; Fotokameras, die sich zum Austausch von Bildern mit einem benachbarten Netbook verbinden; Reifendrucksensoren, die ihre Werte an das Armaturenbrett schicken, oder elektronische Bilderrahmen, die mit dem smarten Haushaltsstromzähler

kommunizieren, um neben den Familienfotos auch die Strombilanz der hauseigenen Solaranlage in graphisch hübsch aufbereiteter Weise darzustellen.

Bald dürfte es oft auch ökonomischer sein, Geräte statt mit klassischen Bedienungselementen und Anzeigen mit einer „unsichtbaren" Funkschnittstelle wie NFC, WLAN oder ZigBee auszurüsten und damit die Interaktionskomponente in das Web oder auf das Handy zu exportieren. Von dieser Entwicklung profitieren dann auch smarte Dinge, die bislang keine Möglichkeit hatten, ihren Zustand der Umwelt zu offenbaren, weil sie für traditionelle Nutzungsschnittstellen zu klein sind oder, wie etwa bei einem Herzschrittmacher oder einem Kleidungsstück, andere Gründe (Unzugänglichkeit, Ästhetik etc.) dagegen sprechen. Ausgehend davon ist es dann in technischer Hinsicht ein eher kleiner, aber konsequenter Schritt, wenn sich smarte Objekte statt nur mit Browser oder Handy auch mit Internetservices verbinden oder sogar untereinander vernetzen.

Zunehmend rücken mittlerweile auch größere und visionäre Anwendungsszenarien in den Bereich des prinzipiell Möglichen, die zwar eine komplexere Infrastruktur, höhere Investitionen und eine aufwendige Kooperation mehrerer Beteiligter erfordern, die aber entweder gesellschaftlich wünschenswert erscheinen oder längerfristig ganz neue Dienstleistungen (und damit Verdienstmöglichkeiten) versprechen. Zur ersten Kategorie gehören beispielsweise die Kommunikation von Autos untereinander zur Steigerung der Verkehrssicherheit, Möglichkeiten zur rationelleren Verwendung von Energie im Haus, indem etwa einzelne Haushaltsgeräte unmittelbar Auskunft über ihre Stromkosten geben [34], oder das „ambient assisted living" mit der Erwartung, das alltägliche Leben älterer Menschen unaufdringlich zu unterstützen.

Beispiele der zweiten Kategorie wären ein virtuelles Fundbüro [13], bei dem schwache Hilferufe verloren gegangener Dinge von einer mobilen Infrastruktur wahrgenommen werden, oder Sachversicherungen, wo das Risiko oft besser abgeschätzt (und evtl. sogar vermindert) werden kann, wenn die versicherte Sache „smart" ist [7]. Dies kann etwa eine dynamische Autohaftpflichtversicherung sein, die ihre Prämie nicht nur von der Kilometerleistung („pay as you drive"), sondern vom individuellen Risiko abhängig macht. Somit könnten sich überhöhte Geschwindigkeit, gewagte Überholmanöver oder ein Ausflug bei unsicheren Straßenverhältnissen direkt in den Versicherungskosten niederschlagen [4].

Generell ist zu erwarten, dass mit dem Internet der Dinge zunehmend hybride Produkte entstehen, die sich aus klassischer physischer Leistung und neuer Informationsleistung zusammensetzen. Wenn Gegenstände Zugangspunkt für passende (bzw. in ihnen „verankerte") Services darstellen, können Produkte beispielsweise Nutzungsempfehlungen und Wartungshinweise geben, über Garantieleistungen Auskunft erteilen oder auf ergänzende Produkte hinweisen. Ferner kann der digitale Mehrwert eigener Erzeugnisse diese nicht nur von physisch ähnlichen Fabrikaten der Konkurrenz absetzen und Kunden stärker an eigene Zusatzdienste und dazu kompatible Nachfolgeprodukte binden, sondern er schützt außerdem vor Plagiaten, da die an einen Gegenstand gekoppelten Dienste nur schwer nachzuahmen sind. Schließlich ergeben sich auch ganz neue Möglichkeiten, wenn Produkte selbsttätig mit anderen Gegenständen in der Nähe kooperieren – der smarte Kühlschrank mag zum Beispiel dann auf Vorrat stärker herunterkühlen, wenn der „intelligente" Stromzähler billige Energie signalisiert, die von anderen Haushaltsgeräten zurzeit nicht benötigt wird.

Ein weiterer Treiber für das Internet der Dinge stellt die „real world awareness" von Informationssystemen dar: Indem auf relevante physische Ereignisse zeitnah reagiert wird, können Unternehmen ihre Prozesse optimieren – mittlerweile schon klassisch ist in diesem

Sinne die Verwendung der RFID-Technik im Logistikbereich. Anders ausgedrückt: Durch die Erhöhung der „Sehschärfe“ von Informationssystemen ist ein besseres Management der Vorgänge möglich, womit typischerweise eine Effizienzsteigerung und Kostenreduktion verbunden ist [10].

Im Prinzip sind solche Telemetrieanwendungen zwar nichts Neues, doch war dies in der Vergangenheit wegen der eher aufwendigen Technik auf spezielle Fälle beschränkt (wie etwa Induktionsschleifen in Straßen, die zur Optimierung der Ampelsteuerung den Verkehrsfluss an einen zentralen Rechner melden). Inzwischen lohnt es sich aber beispielsweise auch für Heizöllieferanten, aus der Ferne den Füllstand der Öltanks bei den Kunden abfragen zu können (um die Route einzelner Tanklaster bestmöglich planen zu können), oder für Betreiber von Getränke- und Zigarettenautomaten, den Zustand ihrer Verkaufsautomaten (Befüllungsgrad, Fehlfunktionen etc.) über Funkmodems in Erfahrung zu bringen [30]. Auch das mittlerweile im Energiewirtschaftsgesetz verbriefte Recht, eine monatliche Stromrechnung mit den tatsächlichen Verbrauchswerten zu bekommen, lässt sich heutzutage wirtschaftlich nur noch mit fernauslesbaren Haushaltsstromzählern („smart meter“) erreichen.

Besitzt ein smarter Gegenstand eine geeignete Funkschnittstelle (z.B. NFC), dann kann der Nutzer via Handy mit ihm interagieren. Wie oben erwähnt, genügt oft in den Fällen, wo lediglich Informationen zum Objekt angezeigt werden sollen, die bloße Identifikation des Gegenstands (Abb. 1). Kann mit einem Smartphone z.B. der Strichcode eines Supermarktartikels gelesen werden, so lassen sich damit automatisch weitere Daten aus dem Netz holen und auf dem Handydisplay dem Bild des Gegenstands überlagern [1]. Mit der so erreichten „augmented reality“ können nützliche Zusatzinformationen zum Produkt aus unabhängigen Quellen angezeigt werden, z.B. eine auf das persönliche Profil zugeschnittene Allergiewarnung oder eine Nährwertampel. Möglich wird aber auch ein „political shopping“ (Anzeige des Herstellungslandes, eines Gütesiegels oder des CO_2-Footprints) oder das „self checkout“ im Supermarkt.

Smartphones stellen auf diese Weise Fenster für Gegenstände bereit und wirken als Browser für das Internet der Dinge – mit dem Vorteil, dass das Handy manches über die aktuelle Situation weiß (z.B. den momentanen Ort oder das Profil des Besitzers) und dass das „Zeigen“ auf den betroffenen Gegenstand die manuelle Eingabe einer Internetadresse oder eines Suchbegriffs überflüssig macht, der Vorgang also sehr schnell und bequem abläuft. Es erscheint damit vorstellbar, dass in Zukunft eine solche lokale Informationsmöglichkeit über Dinge in Reichweite als genauso wichtig angesehen wird wie heute das „weltweite“ Web oder dass sie gar mit diesem verschmilzt.

Zusammengefasst verbinden sich folgende Erwartungen mit dem Internet der Dinge: Aus *wirtschaftlicher Sicht* eine Effizienzsteigerung von Unternehmensprozessen und eine Kostenreduktion in der Warenlogistik sowie im Servicebereich (durch Automatisierung und Verlagerung zum Kunden); ferner eine verbesserte Kundenbindung und -ansprache sowie neue Geschäftsmodelle mit smarten Dingen und damit verbundenen Dienstleistungen. Interessant aus *gesellschaftlicher und politischer Sicht* ist die allgemeine Steigerung der Lebensqualität durch eine umfassendere Informationsmöglichkeit von Konsumenten und Bürgern, durch eine bessere Betreuung Hilfsbedürftiger mittels smarter Assistenzsysteme sowie durch eine Erhöhung der Sicherheit, etwa im Straßenverkehr. In *individueller Hinsicht* zählen vor allem Dienstleistungen rund um smarte Objekte und das Internet der Dinge, die das Leben angenehmer, unterhaltsamer, unabhängiger und sicherer machen – letzteres z.B. durch die Lokalisierung abhandengekommener Dinge (bzw. Haustiere oder gar Mitmenschen). Alle

diese Möglichkeiten haben natürlich auch eine Kehrseite – hierüber wird weiter unten noch zu sprechen sein.

Technologische Herausforderungen

So interessant viele der oben skizzierten Anwendungsmöglichkeiten und Szenarien auch sein mögen – die Ansprüche an die zugrundeliegenden Technologien sind dabei gewaltig. Der Weg vom Internet der Computer hin zu einem Internet der Dinge als fernes und etwas undeutliches Ziel kann daher nur schrittweise gegangen werden. Neben der Erwartung, dass die Technik sehr billig werden muss, wenn tatsächlich eine große Zahl von Gegenständen mitspielen soll, ist man dabei unter anderem mit folgenden Herausforderungen konfrontiert:

- *Skalierbarkeit:* Ein Internet der Dinge hat potenziell einen viel größeren Gesamtumfang als das klassische Internet der Computer. Andererseits kooperieren Dinge meist in einem lokalen Umfeld. Grundfunktionalitäten wie Kommunikation und service discovery müssen daher sowohl in einem kleinräumigen als auch im globalen Umfeld effizient funktionieren.
- *„Arrive and operate":* Smarte Alltagsgegenstände sollen nicht als Computer wahrgenommen werden, die erst konfiguriert und vom Nutzer an die jeweilige Situation angepasst werden müssen. Über die spontane Vernetzung hinaus müssen mobile und oft nur sporadisch genutzte Dinge sich selbst organisieren und konfigurieren und sich in die jeweilige Umgebung einpassen.
- *Interoperabilität:* Die Welt der Dinge ist äußerst heterogen, entsprechend wird in einem Internet der Dinge auch die jeweilige Ausstattung mit Informations- und Kommunikationstechnik sehr variabel ausfallen und ganz unterschiedlichen Bedingungen (Energiebudget, benötigte Kommunikationsbandbreite etc.) unterliegen. Dennoch sollte nach weitgehend gleichartigen Prinzipien und Standards kommuniziert und kooperiert werden. Dies gilt insbesondere auch für die Adressierung der Objekte, die möglichst nach einem einheitlichen Schema erfolgen sollte, was sich ja auch im klassischen Internet mit dem IP-Standard bewährt hat.
- *Discovery:* In dynamischen Umgebungen müssen geeignete Dienste für Dinge automatisch identifiziert werden, was eine semantisch adäquate Beschreibung der Funktionalität voraussetzt. Ferner werden Nutzer zu Produkten passende Informationen erhalten und dafür Suchmaschinen nutzen wollen, die Dinge finden oder Auskunft über den Zustand eines Gegenstands geben.
- *Softwarekomplexität:* Einerseits müssen, wie bei den klassischen eingebetteten Systemen, die Softwaresysteme in den smarten Objekten mit knappen Ressourcen auskommen, andererseits muss eine umfangreichere Softwareinfrastruktur („Middleware") im Netz und auf Hintergrundservern die Dinge an der Front verwalten und mit Dienstleistungen unterstützen.
- *Datenvolumen:* Bei einigen Anwendungsszenarien wird nur selten und wenig kommuniziert, bei anderen (Sensornetze, Logistik, großflächige „real world awareness" etc.) fallen aber bei zentralen Netzknoten oder Servern sehr große Datenmengen an.
- *Intelligente Dateninterpretation:* Um Nutzer smarter Dinge zu unterstützen, möchte man den mit Sensoren ermittelten lokalen Kontext möglichst gut interpretieren; um als Dienstanbieter aus den verteilt anfallenden Daten einen Gewinn zu ziehen, möchte man aus diesen verallgemeinerbare Schlüsse ziehen. Aus Daten einen Nutzen, Sinn und Wert zu generieren, ist allerdings keineswegs trivial.
- *Sicherheit und Privatsphärenschutz:* Neben den aus dem Internet bekannten Sicherheits- und Schutzaspekten (wie Vertraulichkeit der Kommunikation, Authenti-

zität und Vertrauenswürdigkeit der Kommunikationspartner, Integrität der Nachricht) werden in einem Internet der Dinge noch weitere Anforderungen wichtig: Dingen möchte man vielleicht nur selektiv Zugriff auf gewisse Dienste geben, Dinge sollen nicht immer oder mit jedem anderen in unkontrollierter Weise kommunizieren, und Geschäftsvorgänge mit smarten Objekten sollen vor Einblicken der Konkurrenz geschützt werden.

- *Fehlertoleranz:* Die Welt der Dinge ist viel dynamischer und mobiler als die Welt der Computer, die Kontextbedingungen können sich rasch und in unvorhergesehener Weise ändern. Dennoch sollte man sich auf das Funktionieren verlassen können. Redundanz auf vielen Ebenen und eine automatische Anpassung an veränderte Bedingungen ist daher notwendig, um das Internet der Dinge robust und vertrauenswürdig auszugestalten.
- *Energieversorgung:* Typischerweise sind Dinge beweglich und nicht an das Stromnetz angebunden, sie müssen also ihre „smartness" energieautark erzielen. Passive RFID-Transponder benötigen zwar keine eigene Energiequelle, dafür ist ihre Funktionalität und die erzielbare Kommunikationsreichweite aber auch sehr eingeschränkt. Batterien und Akkumulatoren andererseits sind in vielen Szenarien „lästig", da sie groß und schwer sind, vor allem aber einen manuellen Unterhalt erfordern. Leider macht die Batterietechnik vergleichsweise eher langsame Fortschritte, und das „energy harvesting", also das Erzeugen von Strom aus der Umgebung (mittels Temperaturdifferenzen, Vibrationen, Luftströmungen, Licht etc.), ist bei den meisten interessanten Szenarien für den Energiebedarf heutiger Elektroniksysteme noch zu unergiebig.

  Die Hoffnungen konzentrieren sich daher auf zukünftige Low-Power-Prozessoren und Kommunikationseinheiten für eingebettete Systeme, die mit deutlich weniger Energie auskommen. Stromspartechniken betreffen dabei nicht nur die Hardware- und Architekturebene, sondern auch die Software, etwa bei der Implementierung von Protokollstacks, wo mit jedem einzelnen zu übermittelnden Byte gegeizt wird. Allerdings gibt es immerhin bereits batterielose Funksensoren, die ihre Messwerte einige Meter weit melden können. Die dazu nötige Energie beziehen sie wie RFID-Systeme aus der Ferne oder aus dem Messvorgang, indem beispielsweise piezoelektrische oder pyroelektrische Materialien bei Druck- bzw. Temperaturmessungen eingesetzt werden.
- *Interaktion und Nahbereichskommunikation:* In vielen Anwendungsszenarien genügt eine Funkkommunikation über Distanzen von wenigen Zentimetern – wenn beispielsweise ein Gegenstand mit einem anderen Objekt berührt wird oder der Nutzer sein Handy an den Gegenstand hält. Für so kurze Entfernungen wird nur sehr wenig Energie benötigt, die Adressierung vereinfacht sich (da oft nur ein einziges Ziel infrage kommt) und die Gefahr des Mithörens durch andere ist typischerweise ausgeschlossen. Ein Beispiel ist NFC, das analog zu RFID die induktive Kopplung verwendet. Bei der Kommunikation ist ein Partner im sogenannten aktiven Modus, der andere kann im passiven Modus sein. Aktive NFC-Einheiten sind klein genug, um beispielsweise in einem Mobiltelefon untergebracht zu werden; passive Einheiten sind analog zu RFID-Transpondern noch wesentlich kleiner, billiger und benötigen keine eigene Energiequelle.
- *Funkbasierte Kommunikation:* Etablierte Funktechnologien wie GSM, UMTS, Wi-Fi und Bluetooth sind unter energetischen Gesichtspunkten vielfach weniger gut geeignet; neuere und in Entwicklung befindliche WPAN-Standards wie ZigBee haben zwar eine geringere Bandbreite, kommen dafür aber mit deutlich weniger Energie aus.

RFID und das EPC Network

RFID (Radio Frequency Identification) dient primär der Identifikation von Gegenständen aus einigen Metern Entfernung, wobei zur Abfrage der Identitätsnummern eine typischerweise stationäre „Lesestation“ per Funk mit kleinen an den Objekten angebrachten batterielosen Transpondern („Funketiketten“) kommuniziert. Neben Identifikation und Kommunikation als zwei für ein Internet der Dinge wichtige Grundfunktionen wird durch RFID (bei bekannter Position der Lesestation) auch die grobe Lokalisierung von Objekten ermöglicht.

Noch Ende der 1990er-Jahre kam die RFID-Technik nur in Nischenbereichen zum Einsatz, etwa zur Tieridentifikation, zur Zugangskontrolle oder in Autowegfahrsperren. Hohe Transponderpreise und fehlende Standards behinderten eine größere Verbreitung. Mittlerweile hat sich das Anwendungsfeld jedoch deutlich erweitert, was vor allem dem 1999 am MIT gegründeten Auto-ID-Center zu verdanken ist. Diese Institution und ihre Nachfolgeorganisation EPCglobal haben die Vision von kostengünstigen, standardisierten Transpondern, die Milliarden von Alltagsgegenständen identifizieren, konsequent weiterverfolgt und die Technologie gemeinsam mit kommerziellen Anbietern fortentwickelt. Der heutige Einsatz in den Lieferketten von Handelsriesen wie Wal-Mart oder Metro ist ein Ergebnis dieser Strategie. Dies ist ein bemerkenswerter Erfolg; die Entwicklung der RFID-Technik und die Realisierung damit verbundener Anwendungen zeigen jedoch auch auf, mit welchen prinzipiellen Schwierigkeiten und Herausforderungen bei der Ausbildung eines eigentlichen Internets der Dinge zu rechnen ist.

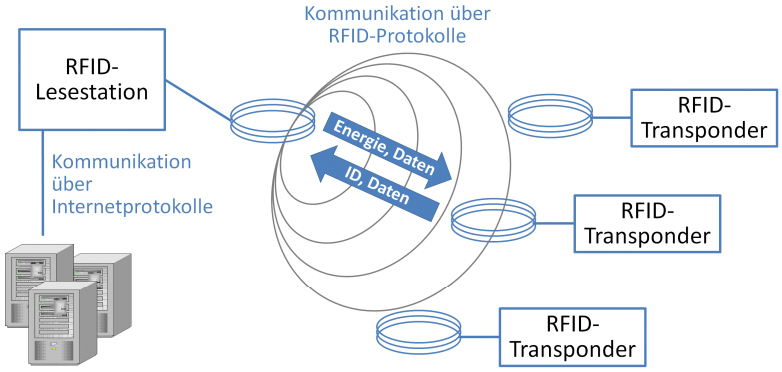

Abbildung 2. RFID-Kommunikationsprinzip.

Die RFID-Weiterentwicklung der vergangenen Jahre spiegelt sich sowohl im technischen Fortschritt als auch in der Kostenreduktion und Standardisierung wider. So liegt die Leistungsaufnahme von Transpondern der neusten Generation unter 30 µW, wodurch unter günstigen Bedingungen Reichweiten von bis zu zehn Metern möglich sind. Die zunehmende Miniaturisierung hat außerdem dazu geführt, dass die Kosten von einfachen RFID-Transpondern bei hohen Stückzahlen auf unter fünf Cent gesunken sind. Große Fortschritte sind auch bei der Standardisierung erzielt worden, wo heute mit dem Funkprotokoll ISO 18000-6C, welches häufig auch als „EPCglobal Gen2“ bezeichnet wird, ein von mehreren Herstellern unterstütztes, leistungsstarkes Kommunikationsprotokoll den Markt dominiert und Interoperabilität garantiert.

Der hohe Kostendruck und der Verzicht auf eine Batterie in den Transpondern führt dazu, dass RFID-Kommunikationsprotokolle aufgrund zu knapper Ressourcen nicht auf den etablierten Internetprotokollen aufbauen können. So besteht ein typischer RFID-Mikrochip nur aus einigen zehntausend Transistoren, enthält keinen Mikrocontroller und hat nur

minimale Speicherkapazität – meist nur wenige Bytes. Anstatt über eine Batterie wird ein passiver RFID-Mikrochip vom Lesegerät drahtlos mit Energie versorgt. Da dabei aufgrund von „Funklöchern“ die Energieversorgung häufig unterbrochen sein kann, wird die Übertragung größerer Datenpakete vermieden – mit typischerweise nur 128 Bits sind diese wesentlich kürzer als IP-Pakete. Alltagsgegenstände, die in einem Internet der Dinge mithilfe der RFID-Technik angesprochen werden sollen, werden sich daher nicht direkt wie Internetknoten verhalten. Vielmehr wird auf den letzten Metern ein bezüglich der knappen Ressourcen sowie widrigen Umstände der physischen Welt hochoptimiertes Funkprotokoll verwendet. Das Gateway zwischen den beiden Protokollwelten stellt dabei das RFID-Lesegerät dar. Im Umfeld der RFID-Technik sind hier TCP- und HTTP-basierte Protokolle entwickelt worden, mit denen die Lesegeräte konfiguriert und die damit erfassten Daten der Gegenstände über das Internet verteilt werden können.

Ein Hauptanwendungsgebiet von RFID ist die Warenlogistik. Mussten in diesem Bereich bisher betriebliche Informationssysteme von Menschenhand über Tastatur oder Strichcodeleser mit Daten „gefüttert“ werden, können mithilfe der RFID-Technik die Daten logistischer Einheiten nun automatisch, ohne Zeitverzögerung und zu einem Bruchteil der Kosten erfasst werden. Durch die konsequente Weiterentwicklung kommt die RFID-Technik mittlerweile aber nicht mehr nur in der Handelslieferkette zum Einsatz, sondern auch in zahlreichen anderen Anwendungsfeldern, denen noch vor Jahren keine große Beachtung geschenkt wurde. So wird RFID beispielsweise in Bibliotheken zur Verwaltung von Büchern und Medien eingesetzt, aber auch in Fabriken zur Lokalisierung von Werkzeugen und anderem mobilen Inventar oder prototypisch sogar in Kleidergeschäften, wo mithilfe von RFID-Systemen sichergestellt wird, dass die Regale stets aufgefüllt sind.

Generell dominieren auf der Anwendungsseite noch die sogenannten „Closed-Loop-Applikationen“. Bei einer zu frühen Einführung von RFID-Systemen in „Open-Loop-Applikationen“, wie dem Einsatz in Lieferketten mit vielen verschiedenen Partnern mit unterschiedlichen wirtschaftlichen Interessen, hat sich die daraus resultierende organisatorische Komplexität schnell als Problem herausgestellt. Es ist daher zweckmäßiger, RFID zunächst nur innerhalb einer einzigen Organisation, vielleicht sogar geographisch begrenzt, zu nutzen. Bei einer solchen „Closed-Loop-Anwendung“ lassen sich die Kosten unmittelbar dem eigenen Effizienzgewinn und Mehrwert gegenrechnen, und technologische Herausforderungen sind oft einfacher zu meistern. Übertragen auf das allgemeine Internet der Dinge heißt dies, dass mit „globalen“ Anwendungen, die die Kooperation vieler verschiedener Parteien bedingen, nicht schon bald und nicht als erstes zu rechnen ist. Vielmehr dürften auf der Basis von standardisierten Schnittstellen zunächst lokale Anwendungen realisiert werden, die dann erst zu einem späteren Zeitpunkt zusammengeführt werden.

Langfristig werden so auch Infrastrukturen wie das „EPC Network“ eine wichtige Rolle spielen [32]. Das EPC Network ist nach dem „Electronic Product Code“ (EPC) benannt, der als strukturierte Kennung jeden produktbezogenen RFID-Transponder eindeutig auszeichnet. Das Ziel des EPC Network ist es, nicht nur die Objektidentifizierung mittels RFID-Technik zu ermöglichen, sondern auch die Weiterverarbeitung und den Austausch der damit erfassten Daten zu vereinfachen. Eine wesentliche Komponente stellt dabei der EPCIS-Standard dar, der heute schon von vielen Softwareherstellern unterstützt wird. Er definiert Ereignisse, durch welche die von Lesegeräten erfassten RFID-Daten mit Kontextinformationen verknüpft werden. So liefern EPCIS-Ereignisse nicht nur eine Antwort auf die Frage, wann und wo ein bestimmter Transponder erfasst wurde, sondern auch Informationen zum zugehörigen Geschäftsvorgang bzw. Anwendungsereignis. Die kontextbezogene Dateninterpretation, die

zur Generierung der EPCIS-Ereignisse führt, bleibt dabei der anwendungsspezifischen Geschäftslogik überlassen.

Der EPCIS-Standard definiert neben den EPCIS-Ereignissen auch eine Schnittstelle, mit der nach EPCIS-Ereignissen in sogenannten Repositories gesucht werden kann. Kennt man diejenigen Repositories, in denen Informationen zu einem bestimmten RFID-Transponder abgespeichert sind, dann kann beispielsweise die „Spur“ des damit markierten Objekts zurückverfolgt werden. In der Praxis ist man aber bei solchen globalen Informationsszenarien mit einer Vielzahl von Problemen konfrontiert. So wird normalerweise nicht jedes Repository bekannt sein, in dem Daten zu einem Objekt abgelegt sind, und eine globale Suche über alle Repositories wird bei weiter steigender Zahl unrealistisch. In vielen Fällen unterliegen die gespeicherten Daten auch dem Geschäftsgeheimnis und sind nicht allgemein zugreifbar – selbst das Wissen, ob eine Firma zu einem bestimmten Objekt Informationen hat, kann dabei bereits vertraulich sein. Diese Schwierigkeiten zeigen, dass auf dem Weg zu einem Internet der Dinge, das solche globalen Anfragen unterstützt, noch viele Herausforderungen hinsichtlich Anwendbarkeit, Skalierbarkeit und Sicherheit zu bewältigen sind.

IP auf Dingen

Wenn in einem zukünftigen Internet der Dinge Alltagsgegenstände über das Internet ansprechbar und kontrollierbar werden, dann sollte idealerweise nicht wie heute bei RFID auf spezielle Kommunikationsprotokolle zurückgriffen werden, sondern die Dinge sollten sich wie normale Internetknoten verhalten; also eine IP-Adresse bekommen und zur Kommunikation mit anderen smarten Objekten und Netzknoten das Internet Protocol (IP) implementieren – und zwar aufgrund der großen Zahl benötigter Adressen gleich in der neueren IPv6-Version mit 128-Bit-Adressen.

Die Vorteile IP-fähiger Dinge liegen auf der Hand, selbst wenn die Objekte nicht weltweit offen zugreifbar gemacht werden, sondern nur in einem kontrollierten Intranet zum Einsatz kommen: Es kann unmittelbar auf vorhandene Grundfunktionalität wie globale Interoperabilität, netzweite Datenpaketzustellung (forwarding, routing), Datentransport über ganz unterschiedliche physikalische Medien, Namensverwaltung (URL, DNS) oder Netzmanagement aufgebaut werden; die Nutzung vorhandener Internetdienste und Anwendungen durch smarte Objekte wird einfach, umgekehrt können diese als vollwertige Internetteilnehmer auch von überall her angesprochen werden, und nicht zuletzt lassen sich dadurch wichtige Protokolle höherer Schichten wie beispielsweise HTTP einfach realisieren. IPv6 bietet auch die interessante Möglichkeit der automatischen Adresskonfiguration, sodass sich smarte Objekte in autonomer Weise selbst eine Adresse zuweisen können.

Bis vor kurzem schien allerdings eine vollständige IP-Unterstützung einfacher Dinge aufgrund der benötigten Ressourcen (Prozessorleistung, Energie) und damit auch aus Kostengründen illusorisch zu sein; propagiert wurde vielmehr ein indirekter Anschluss smarter Objekte an das Internet über Proxies oder Gateway-Rechner. Der Nachteil solcher nicht allgemein standardisierter Lösungen ist jedoch, dass durch die Protokollumsetzung auf proprietäre Verfahren „auf den letzten Metern“ die Ende-zu-Ende-Funktionalität verloren geht und Gateways zusätzlich Komplexität erzeugen, was diese Vorgehensweise hinsichtlich Installation, Betrieb und Wartung aufwendig macht.

Inzwischen gibt es aber nicht nur 16-Bit-Mikrocontroller mit ausreichend Speicher, die weniger als 400 µW/MIPS benötigen, sondern auch TCP/IPv6-Stacks, die mit 4 kB RAM und 24 kB Flash-Speicher auskommen [17]. Genauso entscheidend sind aber auch funk-

basierte Kommunikationsstandards wie IEEE 802.15.4, die die Ebenen unterhalb von IP abdecken und eine relativ geringe Leistungsaufnahme bedingen – ZigBee-Implementierungen benötigen z.B. ca. 20 bis 60 mW (bei 1 mW Sendeleistung, 10 bis 100 m Reichweite und einer Datenübertragungsrate von 250 kbit/s), wobei im Arbeitszyklus der Anwendung die Funkeinheit aus Energiespargründen meist nur kurzzeitig betrieben wird. Auf diese Weise wird mit AA-Batterien („Mignonzellen“) die Bereitstellung einer bescheidenen, für viele Zwecke aber schon ausreichenden Rechenleistung und Funkkommunikation über viele Monate hinweg möglich.

Die sich damit abzeichnenden Möglichkeiten haben in jüngster Zeit zu einigen Maßnahmen bei Firmen und Standardisierungsgremien geführt: Um die Implementierung und Nutzung von IP für ressourcenarme Geräte wie Funksensoren, Verbrauchszähler und andere smarte Objekte zu propagieren, wurde Ende 2008 von Atmel, Cisco, Intel, SAP, Sun Microsystems und weiteren Unternehmen die Firmenallianz „IP for Smart Objects“ (IPSO) gegründet. Konkreter befasst sich die Arbeitsgruppe „IPv6 over Low Power Wireless Area Networks“ (6LoWPAN) der Internet Engineering Task Force (IETF) mit dem Problem, IPv6 durch den 802.15.4-Funkstandard zu unterstützen [18]. Dies ist eine technische Herausforderung, da (aufgrund der geringeren Datenrate sowie der höheren Störanfälligkeit und Bitfehlerrate der Funkkommunikation) die maximale Länge von 802.15.4-Datenrahmen nur 127 Bytes beträgt, aber alleine der Header von IPv6-Paketen (im Wesentlichen wegen der jeweils 16 Bytes langen Quell- und Zieladresse) schon 40 Bytes groß ist und unfragmentierte IPv6-Pakete sogar bis zu 1280 Bytes groß werden können.

Um in effizienter Weise IPv6-Kommunikation mit Funknetzen zu ermöglichen, wurde daher eine Protokollanpassungsschicht definiert, die im Wesentlichen vier Aspekte behandelt: Die Einbettung von IPv6-Paketen in 802.15.4-Rahmen, die Fragmentierung von langen Paketen zu Folgen solcher Rahmen, die zustandslose Komprimierung des Paketkopfes (auf typischerweise nur 6 Bytes) sowie das Weiterleiten („forwarding“) von IPv6-Paketen über Multihop-Funkstrecken. Die starke Komprimierungsmöglichkeit des IPv6-Headers beruht darauf, dass 802.15.4-Knoten vorwiegend innerhalb ihres eigenen Funknetzes kommunizieren, sodass in diesem Fall die meiste Information aus dem gemeinsamen Kontext oder den umgebenden 802.15.4-Rahmen rekonstruiert werden kann und wesentlich kürzere lokale Adressen verwendet werden können.

Der Arbeitsgruppenvorschlag wurde inzwischen als „Internet proposed standard“ RFC 4944 veröffentlicht, eine darauf basierende Implementierung ist in [17] beschreiben. 2009 erklärte die ZigBee-Allianz, diesen „native IP support“ bei zukünftigen ZigBee-Spezifikationen zu berücksichtigen, „allowing seamless integration of Internet connectivity into each product“.

Das Web der Dinge

Eine konsequente Weiterentwicklung des Prinzips, das dem Internet der Dinge zugrunde liegt, stellt die Nutzung des World Wide Web und seiner vielfältigen Technologien als Infrastruktur für smarte Objekte dar. Bereits vor einigen Jahren propagierten Kindberg et al. mit dem Cooltown-Projekt die Idee, physische Objekte mit URLs zu markieren, die z.B. mit einer Infrarotschnittstelle ausgelesen werden können und auf Webseiten mit Informationen und Services zu den jeweiligen Objekten verweisen [20]. Eine andere prinzipielle Möglichkeit der Webnutzung besteht darin, smarte Objekte in eine standardisierte Webservice-Architektur (mit Normen wie SOAP und WSDL) einzubinden – in der Praxis erweist sich dies jedoch für einfache Objekte als zu aufwendig und zu komplex.

Statt auf die klassische Webservice-Technologie setzt die in jüngster Zeit entstandene „Web of Things“-Initiative [15] daher auf einfache eingebettete HTTP-Server sowie auf Web 2.0-Techniken. Moderne Webserver guter Funktionalität (mehrere gleichzeitige Verbindungen, Vermittlung von dynamisch generiertem Inhalt, Ereignismeldung über „server push“) kommen, bei geschickter schichtübergreifender Optimierung von TCP/HTTP, mit 8 kB Speicher und ohne Betriebssystemunterstützung aus, sind also sogar für kleinste eingebettete Systeme wie Chipkarten geeignet – womit das Kunststück eines „high level API on a low power device“ gelingt [5]. Da beim Internet der Dinge eingebettete Webserver im Allgemeinen weniger Ressourcen besitzen als Web-Clients in Form von Browsern oder Handys, erweist sich die AJAX-Technologie („Asynchronous JavaScript and XML”) als vorteilhaft, mit der Arbeitslast vom Server teilweise in den Client verlagert werden kann.

Typischerweise werden beim Web of Things smarte Objekte und deren Dienste mittels URLs adressiert und über eine einfache Schnittstelle mit wenigen, wohldefinierten Operationen (GET, PUT etc.) angesprochen; als Kommunikationsprotokoll wird HTTP genutzt. Daten, die ein Objekt ins Web sendet, werden entweder in Form eines strukturierten XML-Dokumentes dargestellt oder als maschinell (per JavaScript) direkt evaluierbares JSON-Objekt ausgeliefert. Diese Darstellungen sind nicht nur für Maschinen, sondern bei entsprechender Wahl der Auszeichnungselemente und Variablennamen ebenso für Menschen verständlich; über Mikroformate lassen sie sich auch mit semantischen Informationen anreichern.

Smarte Objekte können auf diese Weise jedoch nicht nur im Web kommunizieren, sondern auch eine nutzungsfreundliche Repräsentation von sich selbst bereitstellen, sodass über normale Webbrowser mit ihnen interagiert werden kann und (via Links, die auf andere, damit zusammenhängende Dinge verweisen) die Welt der smarten Dinge mit ihren vielfältigen Beziehungen exploriert werden kann. Auf solchen „repräsentativen“ Webseiten lassen sich auch dynamisch generierte Realweltdaten der smarten Objekte darstellen, die dann mit dem ganzen Instrumentarium an allgemein verfügbaren Web 2.0-Tools weiterverarbeitet werden können. So lassen sich beispielsweise Dinge (über ihre digitale Repräsentation) einerseits wie Webseiten indexieren, hinsichtlich ihrer Eigenschaften von Nutzern googeln oder als Referenz weiterreichen, andererseits können die physischen Objekte selbst aktiv werden und ein Blog führen oder sich per Twitter gegenseitig informieren. Was zunächst wie eine etwas abwegige Anthropomorphisierung klingt, hat eine praktische Bedeutung: Es wird das Web mit seinen Diensten als eine ubiquitäre Middleware zur einfachen Realisierung neuer Funktionalität und innovativer Anwendungen für smarte Dinge genutzt. Möchte man etwa den Zustand der Waschmaschine im Keller verfolgen, so abonniert man in einem Web-Client ihren Atom-Feed, der über wesentliche Zustandsänderungen informiert, oder man erklärt sich gleich zum „Follower“ ihres Tweets.

In verallgemeinerter Weise können mit einem Mashup-Editor Ereignis- und Datenströme von physischen Objekten miteinander (sowie mit Services im Web) verbunden und so neue Funktionalität erzeugt werden. Ein Beispiel soll das verdeutlichen: Die meisten Flugzeuge sind mit Funkbaken („ADS-B“) ausgestattet, die ein bis zwei Mal pro Sekunde auf 1090 MHz ein kurzes Datenpaket aussenden, das im Umkreis von wenigen 100 km empfangen werden kann. Dieses enthält neben der Flugkennung die aktuelle Position, Höhe, Geschwindigkeit sowie die Steig- oder Sinkrate des Flugzeugs. Unter http://radar.zhaw.ch findet man dazu ein Mashup, bei dem auf Karten von Google Maps die Flugbahnen der Flugzeuge im Großraum Zürich (einschließlich dem Südwesten Deutschlands sowie Teilen von Frankreich und Österreich) in Echtzeit visualisiert werden (vgl. Abb. 3; die Größe des Schattens und seine Nähe zum Flugzeugsymbol symbolisiert die Flughöhe). Dies wird mit weiteren Daten aus verschiedenen Quellen (z.B. www.flightstats.com) angereichert, sodass durch

Klicken auf ein Flugzeugsymbol außerdem noch Angaben wie Fluggesellschaft, Abflug- und Zielflughafen, erwartete Ankunftszeit etc. dargestellt werden.

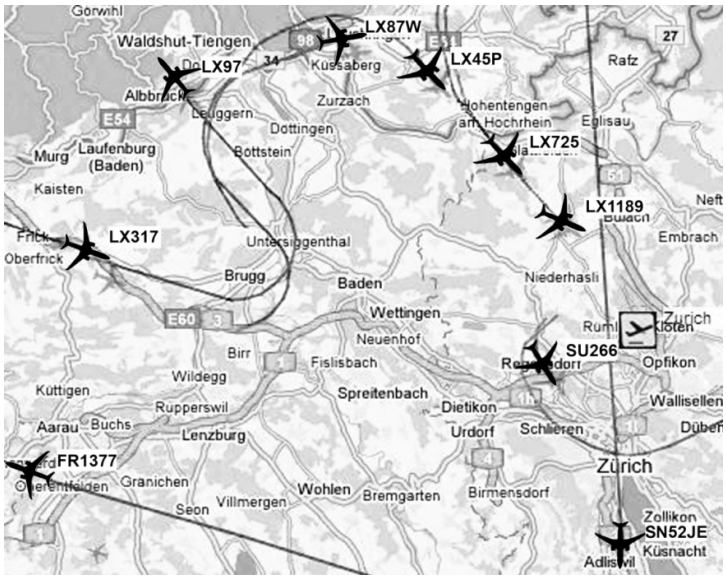

Abbildung 3. Ein Mashup zur Visualisierung von Flugbahnen im Großraum Zürich [22].

Auch wenn Flugzeuge keine kleinen „Allerweltsdinge“ im Sinne der ultimativen Vision des Internets der Dinge sind, demonstriert das Beispiel in hübscher Weise das Potenzial der Verbindung von physischer Welt mit dem Cyberspace. Ein „bodenständigeres“ physisches Mashup, bei dem mittels „intelligenter“ Steckdosen und Web-Technologie der Stromverbrauch von Geräten wie Kühlschrank, Wasserkocher und PC-Bildschirm auf Webbrowsern visualisiert wird, ist in [15] beschrieben.

Preisgünstige eingebettete Webschnittstellen dürften schon in naher Zukunft, unabhängig von der Langfristvision eines Internets der Dinge, vielfältige Anwendungsmöglichkeiten eröffnen. Ein Beispiel stellt das Gebiet der Hausautomatisierung dar: Zur Energieeinsparung und Kostenreduktion oder – insbesondere im privaten Bereich – zur Erhöhung des Komforts und der Sicherheit werden dabei in einem Gebäude über Temperaturfühler, Bewegungsmelder und andere Sensoren vielfältige Aspekte wie Beleuchtung, Heizung, Lüftung, Rollläden und Schließanlagen gesteuert, was eine Kommunikationsfähigkeit dieser Einheiten bedingt. Hierfür wurden in der Vergangenheit diverse Standards, wie beispielsweise der Europäische Installationsbus (EIB), entwickelt, doch blieb die Einrichtung eine teure Angelegenheit; auch muss die Konfiguration, Parametrisierung und Adresszuordnung der Einheiten vor Ort durch Experten mittels spezieller Software erfolgen.

Als standardisierte und preiswerte Massentechnologie verspricht hier die Web- und Internettechnologie Abhilfe, auch weil damit bewährte Konzepte aus der Netzwelt (wie beispielsweise Autokonfiguration oder Netzmanagementwerkzeuge) eingesetzt werden können und mittels Webschnittstellen eine einfache Fernwartung über Webbrowser möglich wird. Aufbauend darauf könnte dann mit smarten Haushaltsgeräten („Web 2.0 ready“), WLAN-fähigen Stromzählern und weiteren drahtlos kommunizierenden und sich selbst integrierenden Gadgets schrittweise vielleicht auch der alte Traum (oder Albtraum?) des „intelligenten Hauses“ Realität werden…

Gesellschaftliche und politische Fragen

Schon längst ist das Internet von einem rein informatischen zu einem soziotechnischen System mutiert, das eine soziale, gestalterische und politische Dimension aufweist. Die hohe Bedeutung der über die Technik hinausgehenden Gesichtspunkte gilt erst recht für die Weiterentwicklung zu einem Internet der Dinge, das diesen Aspekten eine ganz neue Qualität hinzufügt [16]. Neben den weiter oben angesprochenen positiven Erwartungen stellen sich hinsichtlich möglicher Konsequenzen daher auch einige kritische Fragen.

Viele Punkte der öffentlichen Diskussion, die Akzeptanz oder Ablehnung betreffen, lassen sich dabei den klassischen Dualismen „Sicherheit – Freiheit“ und „Komfort – Datenprivatheit“ zuordnen. Insofern unterscheiden sich die Debatten dazu nicht grundsätzlich von den bekannten Auseinandersetzungen um Kundenkarten, Videoüberwachung oder E-Pass. Wie früher schon beim Thema „RFID“ [31] artikuliert sich das Unbehagen primär in Bezug auf die persönlichen Daten, die automatisch anfallen und ohne Zustimmung und eigenes Wissen von Fremden zu unbekannten und potenziell schädlichen, die individuelle Freiheit einschränkenden Zwecken genutzt werden könnten.

Und tatsächlich steht die Privatsphäre unter Druck: Smarte Gegenstände könnten eine Unmenge von Daten anhäufen, nur um uns perfekt zu dienen. Da dies typischerweise unaufdringlich im Hintergrund geschieht, können wir uns dann nie ganz sicher sein, ob wir bei irgendwelchen Handlungen nicht „observiert“ werden. Eine einzelne Beobachtung mag für sich genommen noch harmlos sein – aber wenn in einem Internet der Dinge verschiedene solche Erkenntnisse zusammengeführt und an Externe weitergeleitet werden, kann dies unter Umständen eine folgenschwere Verletzung der Privatsphäre nach sich ziehen.

Unabhängig von der Datenschutzproblematik stellt sich auch die Frage, wem im Einzelfall die vielen automatisch erhobenen und maschinell interpretierten Realweltdaten gehören, die durchaus einen bedeutenden wirtschaftlichen oder auch gesellschaftlichen Wert haben könnten, und wer darüber die Verfügungsgewalt hat und welcher ethische und rechtliche Rahmen dabei gilt.

Ein weiterer kritischer Aspekt ist die Technologiedependenz. In der Wirtschaft, aber auch in der Gesellschaft, haben wir uns heute schon stark von der allgemeinen Verfügbarkeit des elektrischen Stroms abhängig gemacht – seltene „Blackouts“ blieben bislang glücklicherweise ohne gravierende Folgen. Aber funktionieren in Zukunft viele eher alltägliche Dinge nur noch dann ordnungsgemäß, wenn von diesen aus Zugriff auf das Internet besteht, dann entsteht eine noch größere Abhängigkeit von der zugrundeliegenden Technik. Wenn diese versagt, wofür unterschiedliche Gründe – Entwurfsfehler, Materialdefekte, Sabotage, Überlastung, Naturkatastrophen, Krisensituationen etc. – denkbar sind, dann kann sich dies desaströs auf Wirtschaft und Gesellschaft auswirken. Selbst einen nur von übermütigen Teenagern programmierten Virus, der befallene Alltagsgegenstände weltweit verrückt spielen lässt und dadurch sicherheitskritische, lebensbedrohende oder gar politisch brisante Situationen provoziert, möchte man sich lieber nicht vorstellen.

Auch individuell kann man sich durch Dinge, die aus der Ferne kontrolliert werden, in eine unerwünschte Abhängigkeit begeben und die Souveränität verlieren. Und selbst ohne böse Absicht mögen sich unsere eigenen smarten Gegenstände nicht immer so verhalten, wie wir es uns wünschen, sondern wie diese „glauben“, dass es für uns am besten wäre – womit eine subtile Form des Technikpaternalismus droht [27]. Das zeitnahe Feedback, das uns smarte Dinge über sich selbst oder das uns Assistenzinstrumente wie Smartphones und Augmented-Reality-Brillen über unsere Umgebung und unser Handeln geben können, ist ebenfalls eine

zwiespältige Angelegenheit: Einerseits kann uns dies zum Guten und Nützlichen animieren (wie der Smiley im smarten Badezimmerspiegel, der das Zähneputzen mit der elektrischen Bürste kommentiert), andererseits aber auch beispielsweise zu unnützen Impulskäufen verführen.

Mittlerweile hat das Internet der Dinge auch die Politik erreicht. In einer Studie für das Projekt „Global Trends 2025“ [24] des US-amerikanischen „National Intelligence Council“ wird mit „foreign manufacturers could become both the single-source and single-point-of failure for mission-critical Internet-enabled things“ [28] nicht nur vor einer kritischen Abhängigkeit der Nation gewarnt, sondern auch gleich die sicherheitspolitische Dimension durch eine Verlängerung des Cyberwars in die Realität angesprochen: „U.S. law enforcement and military organizations could seek to monitor and control the assets of opponents, while opponents could seek to exploit the United States“ [29].

Bei der Europäische Kommission wird schon laut, wenn auch noch etwas vage, über das Problem der „Governance“ des zukünftigen Internets der Dinge nachgedacht. Dabei geht es um die Frage, wie in einem solchen System das allgemeine öffentliche Interesse sichergestellt werden kann und wie verhindert werden kann, dass zu stark zentralisierte Strukturen entstehen oder die regulatorische Macht über das Internet der Dinge exklusiv bei einer, wie es wörtlich heißt, „spezifischen Autorität“ zu liegen kommt.

Der oben bereits erwähnte Aktionsplan der Europäischen Kommission zum Internet der Dinge [6] hat allerdings auch heftige emotionale Gegenreaktionen ausgelöst, als dieser im Onlinemagazin „Telepolis“ [21] mit dem Aufmacher „Der kurze Weg zur kollektiven Zwangsentmündigung“ kritisch kommentiert wurde (Tenor des Artikels: Das Internet der Dinge würde viel Geld kosten, das der Verbraucher zu zahlen hätte, und der Nutzen würde gering sein). In Leserkommentaren zum Beitrag wird das Internet der Dinge als „zwangsvernetzte Welt“ und „gigantische Klapsmühle“ bezeichnet; es würde uns „vollkommen abhängig von Technik und den Herrschenden“ machen und die „Aufgabe aller Freiheiten“ bedeuten. Die Entwicklung wird sogar als Perversion des Internets und seiner vorgeblichen politischen Mission apostrophiert: „Ein Medium, was zur Befreiung der Menschheit entstanden ist und dazu dienen soll, könnte also dazu missbraucht werden, die totale Kontrolle zu errichten“.

Auch wenn diese Extremmeinungen nicht repräsentativ sind, so kann man doch festhalten: Damit ein Internet der Dinge wirklich Nutzen stiftet, bedarf es mehr als nur mikroelektronisch aufgerüsteter und miteinander kooperierender Gegenstände. Ebenso nötig sind sichere und verlässliche Infrastrukturen, geeignete ökonomische und rechtliche Rahmenbedingungen sowie ein gesellschaftlicher Konsens darüber, wie die neuen technischen Möglichkeiten verwendet werden sollen. Hierin liegt eine große Aufgabe für die Zukunft.

Danksagung. Unser Dank gilt Christof Roduner und Kay Römer für konstruktive Kritik sowie Elgar Fleisch für viele interessante Diskussionen und spannende gemeinsame Projekte zum Internet der Dinge.

Literatur

1. Adelmann, R., Langheinrich, M., Floerkemeier, C. (2006) A Toolkit for Bar-Code-Recognition and -Resolving on Camera Phones – Jump Starting the Internet of Things. Proc. Workshop Mobile and Embedded Interactive Systems. In: Hochberger, C., Liskowsky, R. (Hrsg) Informatik 2006 – Informatik für Menschen, Band 2, GI Lecture Notes in Informatics (LNI) 94, pp 366–373
2. Ashton, K. (2009) That ‚Internet of Things‘ Thing. RFID Journal, www.rfidjournal.com/article/print/4986

3. Bullinger, H.J., ten Hompel, M. (Hrsg) (2007) Internet der Dinge. Springer-Verlag
4. Coroama, V. (2006) The Smart Tachograph – Individual Accounting of Traffic Costs and Its Implications. In: Fishkin, K.P., Schiele, B., Nixon, P., Quigley, A.J. (eds) Proc. Pervasive 2006, LNCS 3968, Springer-Verlag, pp 135–152
5. Duquennoy, S., Grimaud, G., Vandewalle, J.-J. (2009) Smews: Smart and Mobile Embedded Web Server. Proc. Int. Conf. on Complex, Intelligent and Software Intensive Systems, pp 571–576
6. Europäische Kommission (2009) Internet der Dinge – ein Aktionsplan für Europa. KOM(2009) 278, http://eur-lex.europa.eu/LexUriServ/site/de/com/2009/com2009_0278de01.pdf
7. Fleisch, E., Bechmann, T. (2002) Ubiquitous Computing – Wie „intelligente Dinge“ die Assekuranz verändern. Versicherungswirtschaft 57(8):538–541
8. Fleisch, E., Mattern, F. (Hrsg) (2005) Das Internet der Dinge. Springer-Verlag
9. Fleisch, E., Thiesse, F. (2008) Internet der Dinge. In: Kurbel, K., Becker, J., Gronau, N., Sinz, E., Suhl, L. (Hrsg) Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon, www.enzyklopaedie-der-wirtschaftsinformatik.de
10. Fleisch, E. (2009) What is the Internet of Things? When Things Add Value. White paper, ETH Zurich, www.im.ethz.ch/education/HS09/Fleisch_2009_IOT.pdf
11. Floerkemeier, C., Mattern, F. (2006) Smart Playing Cards – Enhancing the Gaming Experience with RFID. In: Magerkurth, C., Chalmers, M., Björk, S., Schäfer, L. (eds) Proc. 3rd Int. Workshop on Pervasive Gaming Applications – PerGames 2006, pp 27–36
12. Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., Sarma, S.E. (eds) (2008) The Internet of Things. First International Conference, IOT 2008, LNCS 4952, Springer-Verlag
13. Frank, C., Bolliger, P., Mattern, F., Kellerer, W. (2008) The Sensor Internet at Work: Locating Everyday Items Using Mobile Phones. Pervasive and Mobile Computing 4(3):421–447
14. Gershenfeld, N. (1999) Wenn die Dinge denken lernen. Econ
15. Guinard, D., Trifa, V., Wilde, E. (2010) Architecting a Mashable Open World Wide Web of Things. TR ETH Zürich, www.vs.inf.ethz.ch/publ/papers/WoT.pdf
16. Herzog, O., Schildhauer, T. (Hrsg) (2009) Intelligente Objekte: Technische Gestaltung – wirtschaftliche Verwertung – gesellschaftliche Wirkung. Reihe „acatech diskutiert“, Springer-Verlag
17. Hui, J., Culler, D. (2008) IP is Dead, Long Live IP for Wireless Sensor Networks. Proc. 6th Int. Conf. on Embedded Networked Sensor Systems (SenSys), pp 15–28
18. Hui, J., Culler, D., Chakrabarti, S. (2009) 6LoWPAN – Incorporating IEEE 802.15.4 into the IP architecture. Internet Protocol for Smart Objects Alliance, white paper # 3
19. International Telecommunication Union (2005) The Internet of Things. ITU
20. Kindberg, T., Barton, J., Morgan, J., Becker, G., Caswell, D., Debaty, P., Gopal, G., Frid, M., Krishnan, V., Morris, H., Schettino, J., Serra, B., Spasojevic, M. (2002) People, Places, Things: Web Presence for the Real World. Mobile Networks and Applications 7(5):365–376
21. Kollmann, K. (2009) Das „Internet of Things“ – Der kurze Weg zur kollektiven Zwangsentmündigung. Telepolis, 27.07.2009, www.heise.de/tp/r4/artikel/30/30805/1.html
22. Kramarz, D., Loeber, A. (2007) Visualisierung von Transponder-Daten mittels Mashup. Diplomarbeit, Zürcher Hochschule für Angewandte Wissenschaften
23. Mattern, F. (2002) Vom Handy zum allgegenwärtigen Computer: Szenarien einer informatisierten Welt. In: Analysen der Friedrich-Ebert-Stiftung zur Informationsgesellschaft 6, http://library.fes.de/fulltext/stabsabteilung/01183.htm
24. National Intelligence Council (2008) Global Trends 2025: A Transformed World. www.dni.gov/nic/NIC_2025_project.html
25. Sarma, S., Brock, D.L., Ashton, K. (2000) The Networked Physical World. TR MIT-AUTOID-WH-001, MIT Auto-ID Center
26. Schoenberger, C.R. (2002) The internet of things. Forbes Magazine, March 18
27. Spiekermann, S., Pallas, F. (2007) Technologiepaternalismus – Soziale Auswirkungen des Ubiquitous Computing jenseits von Privatsphäre. In: Mattern, F. (Hrsg) Die Informatisierung des Alltags – Leben in smarten Umgebungen, Springer-Verlag, S 311–325
28. SRI Consulting Business Intelligence (2008) Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests out to 2025. www.fas.org/irp/nic/disruptive.pdf

29. SRI Consulting Business Intelligence (2008) Disruptive Civil Technologies, Appendix F: The Internet of Things (Background). www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf
30. Tellkamp, C., Kubach, U. (2005) Nutzenpotenziale smarter Maschinen am Beispiel von Verkaufsautomaten. In: Fleisch, E., Mattern, F. (Hrsg) Das Internet der Dinge, Springer-Verlag, S 251–260
31. Thiesse, F. (2005) Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung. In: Fleisch, E., Mattern, F. (Hrsg) Das Internet der Dinge, Springer-Verlag, S 363–378
32. Thiesse, F., Floerkemeier, C., Harrison, M., Michahelles, F., Roduner, C. (2009) Technology, Standards, and Real-World Deployments of the EPC Network. IEEE Internet Computing 13(2):36–43
33. Weiser, M. (1991) The Computer for the 21st Century. Scientific American 265(9):66–75
34. Weiss, M., Mattern, F., Graml, T., Staake, T., Fleisch, E. (2009) Handy feedback: Connecting smart meters with mobile phones. Proc. 8th Int. Conf. on Mobile and Ubiquitous Multimedia (MUM 2009)