From the Internet of Computers to the Internet of Things

Friedemann Mattern and Christian Floerkemeier

Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich
{mattern,floerkem}@inf.ethz.ch

Abstract. This paper[1] discusses the vision, the challenges, possible usage scenarios and technological building blocks of the "Internet of Things". In particular, we consider RFID and other important technological developments such as IP stacks and web servers for smart everyday objects. The paper concludes with a discussion of social and governance issues that are likely to arise as the vision of the Internet of Things becomes a reality.

Keywords: Internet of Things, RFID, smart objects, wireless sensor networks.

> *In a few decades time, computers will be interwoven into almost every industrial product.*
>
> Karl Steinbuch, German computer science pioneer, 1966

1 The vision

The Internet of Things represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. An Internet of Things makes computing truly ubiquitous – a concept initially put forward by Mark Weiser in the early 1990s [29]. This development is opening up huge opportunities for both the economy and individuals. However, it also involves risks and undoubtedly represents an immense technical and social challenge.

The Internet of Things vision is grounded in the belief that the steady advances in microelectronics, communications and information technology we have witnessed in recent years will continue into the foreseeable future. In fact – due to their diminishing size, constantly falling price and declining energy consumption – processors, communications modules and other electronic components are being increasingly integrated into everyday objects today.

"Smart" objects play a key role in the Internet of Things vision, since embedded communication and information technology would have the potential to revolutionize

[1] This paper is an updated translation of [19].

the utility of these objects. Using sensors, they are able to perceive their context, and via built-in networking capabilities they would be able to communicate with each other, access Internet services and interact with people. “Digitally upgrading” conventional object in this way enhances their physical function by adding the capabilities of digital objects, thus generating substantial added value. Forerunners of this development are already apparent today – more and more devices such as sewing machines, exercise bikes, electric toothbrushes, washing machines, electricity meters and photocopiers are being “computerized” and equipped with network interfaces.

In other application domains, Internet connectivity of everyday objects can be used to remotely determine their state so that information systems can collect up-to-date information on physical objects and processes. This enables many aspects of the real world to be “observed” at a previously unattained level of detail and at negligible cost. This would not only allow for a better understanding of the underlying processes, but also for more efficient control and management [7]. The ability to react to events in the physical world in an automatic, rapid and informed manner not only opens up new opportunities for dealing with complex or critical situations, but also enables a wide variety of business processes to be optimized. The real-time interpretation of data from the physical world will most likely lead to the introduction of various novel business services and may deliver substantial economic and social benefits.

The use of the word “Internet” in the catchy term “Internet of Things” which stands for the vision outlined above can be seen as either simply a metaphor – in the same way that people use the Web today, things will soon also communicate with each other, use services, provide data and thus generate added value – or it can be interpreted in a stricter technical sense, postulating that an IP protocol stack will be used by smart things (or at least by the “proxies”, their representatives on the network).

The term “Internet of Things” was popularized by the work of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which in 1999 started to design and propagate a cross-company RFID infrastructure.[2] In 2002, its co-founder and former head Kevin Ashton was quoted in Forbes Magazine as saying, “We need an internet for things, a standardized way for computers to understand the real world” [23]. This article was entitled “The Internet of Things”, and was the first documented use of the term in a literal sense[3]. However, already in 1999 essentially the same notion was used by Neil Gershenfeld from the MIT Media Lab in his popular book “When Things Start to Think” [11] when he wrote “in retrospect it looks like the rapid growth of the World Wide Web may have been just the trigger charge that is now setting off the real explosion, as things start to use the Net.”

In recent years, the term “Internet of Things” has spread rapidly – in 2005 it could already be found in book titles [6, 15], and in 2008 the first scientific conference was held in this research area [9]. European politicians initially only used the term in the context of RFID technology, but the titles of the RFID conferences “From RFID to the Internet of Things” (2006) and “RFID: Towards the Internet of Things” (2007) held by the EU Commission already allude to a broader interpretation. Finally, in

[2] The Auto-ID Center’s first white paper [22] already suggested a vision that extended beyond RFID: “The Center is creating the infrastructure […] for a networked physical world. […] A well known parallel to our networked physical world vision is the Internet.”

[3] Kevin Ashton commented in June 2009: “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].

2009, a dedicated EU Commission action plan ultimately saw the Internet of Things as a general evolution of the Internet "from a network of interconnected computers to a network of interconnected objects" [5].

2 Basics

From a technical point of view, the Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

- *Communication and cooperation:* Objects have the ability to network with Internet resources or even with each other, to make use of data and services and update their state. Wireless technologies such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and various other wireless networking standards currently under development, particularly those relating to Wireless Personal Area Networks (WPANs), are of primary relevance here.
- *Addressability:* Within an Internet of Things, objects can be located and addressed via discovery, look-up or name services, and hence remotely interrogated or configured.
- *Identification:* Objects are uniquely identifiable. RFID, NFC (Near Field Communication) and optically readable bar codes are examples of technologies with which even passive objects which do not have built-in energy resources can be identified (with the aid of a "mediator" such as an RFID reader or mobile phone). Identification enables objects to be linked to information associated with the particular object and that can be retrieved from a server, provided the mediator is connected to the network (see Figure 1).
- *Sensing:* Objects collect information about their surroundings with sensors, record it, forward it or react directly to it.
- *Actuation:* Objects contain actuators to manipulate their environment (for example by converting electrical signals into mechanical movement). Such actuators can be used to remotely control real-world processes via the Internet.
- *Embedded information processing:* Smart objects feature a processor or microcontroller, plus storage capacity. These resources can be used, for example, to process and interpret sensor information, or to give products a "memory" of how they have been used.
- *Localization:* Smart things are aware of their physical location, or can be located. GPS or the mobile phone network are suitable technologies to achieve this, as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known coordinates) and optical technologies.
- *User interfaces:* Smart objects can communicate with people in an appropriate manner (either directly or indirectly, for example via a smartphone). Innovative interaction paradigms are relevant here, such as tangible user interfaces, flexible polymer-based displays and voice, image or gesture recognition methods.

Most specific applications only need a subset of these capabilities, particularly since implementing all of them is often expensive and requires significant technical effort. Logistics applications, for example, are currently concentrating on the approximate localization (i.e. the position of the last read point) and relatively low-cost identification of objects using RFID or bar codes. Sensor data (e.g. to monitor cool chains) or embedded processors are limited to those logistics applications where such information is essential such as the temperature-controlled transport of vaccines.

Forerunners of communicating everyday objects are already apparent, particularly in connection with RFID – for example the short-range communication of key cards with the doors of hotel rooms, or ski passes that talk to lift turnstiles. More futuristic scenarios include a smart playing card table, where the course of play is monitored using RFID-equipped playing cards [8]. However, all of these applications still involve dedicated systems in a local deployment; we are not talking about an “Internet” in the sense of an open, scalable and standardized system.

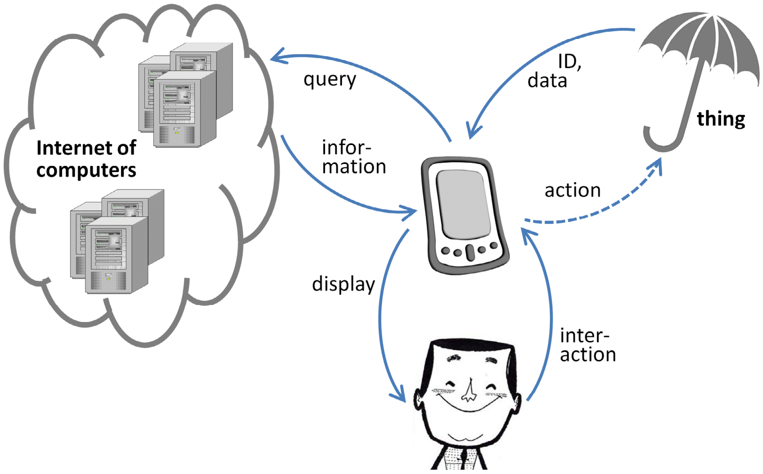

Figure 1. The smartphone as a mediator between people, things and the Internet.

But these days wireless communications modules are becoming smaller and cheaper, IPv6 is increasingly being used, the capacity of flash memory chips is growing, the per-instruction energy requirements of processors continues to fall and mobile phones have built-in bar code recognition, NFC and touch screens – and can take on the role of intermediaries between people, everyday items and the Internet (see Figure 1). All this contributes to the evolution of the Internet of Things paradigm: From the remote identification of objects and an Internet “with” things, we are moving towards a system where (more or less) smart objects actually communicate with users, Internet services and even among each other. These new capabilities that things offer opens up fascinating prospects and interesting application possibilities; but they are also accompanied by substantial requirements relating to the underlying technology and infrastructure. In fact, the infrastructure for an Internet of Things must not only be efficient, scalable, reliable, secure and trustworthy, but it must also conform with general social and political expectations, be widely applicable and must take economic considerations into account.

3 Drivers and expectations

What is driving the development of an Internet of Things? One important factor is the mere evolutionary progress of information and communications technology which is enabling continuous product improvements. Examples of this include navigation devices that receive remote road traffic messages, cameras that connect to a nearby netbook to exchange photos, tire pressure sensors that send their readings to the car's dashboard, and electronic photo frames that communicate with household electricity meters and display not only family photos but also illustrative graphs showing the power being generated by domestic solar panels.

Instead of giving devices conventional operating controls and displays, it can soon be more cost-effective to fit them with an "invisible" wireless interface such as NFC, WLAN or ZigBee and export their interaction components to the Web or a mobile phone. This development will also benefit smart things that were previously unable to disclose their state to their surroundings, either because they were too small for conventional user interfaces or for other reasons (such as inaccessibility or aesthetics) – examples include pacemakers or items of clothing. From here it is a small but logical step for smart objects to connect to Internet services instead of just to browsers or mobile phones, and even to network with each other.

Larger and more visionary application scenarios are increasingly moving into the realm of what is possible. Although they require a more complex infrastructure, greater investment and cooperation between multiple partners, they can be socially desirable or offer the prospect of novel services with significant profit potential. The first category includes cars communicating with each other to improve road safety, ways of using energy more rationally in the home by cooperating energy-aware household devices [20], and "ambient assisted living" aimed at unobtrusively supporting elderly people in their everyday lives.

Examples of the second category include a virtual lost-property office [10], where a mobile infrastructure would pick up feeble cries for help from lost things, or property insurance where the risk can often be better assessed (and possibly even reduced) if the insured item is "smart". This might be a dynamic car insurance that makes your premium dependent not only on how far you drive ("pay as you drive"), but also on the individual risk. Speeding, dangerous overtaking and driving in hazardous conditions would then have a direct impact on the insurance costs [3].

In general, we can expect the Internet of Things to give rise to increasing numbers of hybrid products that provide both, a conventional physical function and information services. If objects become access points for relevant services, products will be able to provide recommendations for use and maintenance instructions, supply warranty information or highlight complementary products. Furthermore, the digital added value of a company's products can be used not only to differentiate them from physically similar competing products and tie customers to the company's additional services and compatible follow-on products, but can also be used to protect against counterfeit products. Completely new opportunities would arise if products independently cooperated with other objects in their proximity. For example, a smart fridge might reduce its temperature when the smart electricity meter indicates that cheap power is available, thus avoiding the need to consume energy at a later stage when electricity is more expensive.

Another driver for the Internet of Things is the real-world awareness provided to information systems. By reacting promptly to relevant physical events, companies can optimize their processes, as typically illustrated by the use of RFID in logistics applications. Or to put it another way, by increasing the "visual acuity" of information systems, it is possible to manage processes better, typically increasing efficiency and reducing costs [7].

Although such telemetry applications are nothing new in principle, they have previously been restricted to special cases due to the costly technology involved (such as inductive loops in roads that transmit traffic conditions to a central computer in order to optimize the sequencing of traffic lights). Due to diminishing cost and technical progress, many other application areas can now benefit from an increased awareness of real-world processes. For example, it is now becoming worthwhile for suppliers of heating oil to remotely check how full customers' oil tanks are (to optimize the routes of individual fuel tankers), and for operators of drinks and cigarette machines to establish the state of their vending machines (how full they are, any malfunctions, etc.) via a wireless modem.

If a smart object possesses a suitable wireless interface (e.g. NFC), the user can interact with the object via a mobile phone. As mentioned above, when only information about the object is to be displayed, it is often sufficient simply to identify the object in question (Figure 1). For example, if the bar code on a supermarket item can be read using a smartphone, additional data can automatically be retrieved from the Internet and displayed on the phone [1]. The "augmented reality" achieved in this way can be used to display helpful additional information on the product from independent sources, for example a personally tailored allergy warning or nutritional "traffic lights". Political shopping would also be possible (displaying an item's country of origin, seal of approval or CO_2 footprint), as would self-checkouts in supermarkets.

Smartphones can thus provide displays for physical objects and act as browsers for the Internet of Things – with the added benefit that the phone knows something about the current situation (such as the current location or the user's profile). "Pointing" at the object in question also removes the need to manually input an Internet address or search term, making the process extremely quick and easy. It appears conceivable that in the future the ability to obtain information about nearby things will be considered just as important as the "worldwide" Web is today, or that this ability will even become part of the Web.

In summary, the following expectations can be associated with the Internet of Things: from a *commercial point of view*, increased efficiency of business processes and reduced costs in warehouse logistics and in service industries (by automating and outsourcing to the customer), improved customer retention and more targeted selling, and new business models involving smart things and associated services. Of interest from a *social and political point of view* is a general increase in the quality of life due to consumers and citizens being able to obtain more comprehensive information, due to improved care for people in need of help thanks to smart assistance systems, and also due to increased safety, for example on roads. From a *personal point of view*, what matters above all are new services enabled by an Internet of Things which would make life more pleasant, entertaining, independent and also safer, for example by locating things that are lost, such as pets or even other people.

4 Technological challenges

While the possible applications and scenarios outlined above may be very interesting, the demands placed on the underlying technology are substantial. Progressing from the Internet of computers to the remote and somewhat fuzzy goal of an Internet of Things is something that must therefore be done one step at a time. In addition to the expectation that the technology must be available at low cost if a large number of objects are actually to be equipped, we are also faced with many other challenges, such as:

- *Scalability:* An Internet of Things potentially has a larger overall scope than the conventional Internet of computers. But then again, things cooperate mainly within a local environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small-scale and large-scale environments.
- *"Arrive and operate":* Smart everyday objects should not be perceived as computers that require their users to configure and adapt them to particular situations. Mobile things, which are often only sporadically used, need to establish connections spontaneously, and organize and configure themselves to suit their particular environment.
- *Interoperability:* Since the world of physical things is extremely diverse, in an Internet of Things each type of smart object is likely to have different information, processing and communication capabilities. Different smart objects would also be subjected to very different conditions such as the energy available and the communications bandwidth required. However, to facilitate communication and cooperation, common practices and standards are required. This is particularly important with regard to object addresses. These should comply with a standardized schema if at all possible, along the lines of the IP standard used in the conventional Internet domain.
- *Discovery:* In dynamic environments, suitable services for things must be automatically identified, which requires appropriate semantic means of describing their functionality. Users will want to receive product-related information, and will want to use search engines that can find things or provide information about an object's state.
- *Software complexity:* Although the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems, a more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them.

- *Data volumes:* While some application scenarios will involve brief, infrequent communication, others, such as sensor networks, logistics and large-scale "real-world awareness" scenarios, will entail huge volumes of data on central network nodes or servers.
- *Data interpretation:* To support the users of smart things, we would want to interpret the local context determined by sensors as accurately as possible. For service providers to profit from the disparate data that will be generated, we would need to be able to draw some generalizable conclusions from the interpreted sensor data. However, generating useful information from raw sensor data that can trigger further action is by no means a trivial undertaking.
- *Security and personal privacy:* In addition to the security and protection aspects of the Internet with which we are all familiar (such as communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity), other requirements would also be important in an Internet of Things. We might want to give things only selective access to certain services, or prevent them from communicating with other things at certain times or in an uncontrolled manner; and business transactions involving smart objects would need to be protected from competitors' prying eyes.
- *Fault tolerance:* The world of things is much more dynamic and mobile than the world of computers, with contexts changing rapidly and in unexpected ways. But we would still want to rely on things functioning properly. Structuring an Internet of Things in a robust and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.
- *Power supply:* Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. In many scenarios, batteries and power packs are problematic due to their size and weight, and especially because of their maintenance requirements. Unfortunately, battery technology is making relatively slow progress, and "energy harvesting", i.e. generating electricity from the environment (using temperature differences, vibrations, air currents, light, etc.), is not yet powerful enough to meet the energy requirements of current electronic systems in many application scenarios.

  Hopes are pinned on future low-power processors and communications units for embedded systems that can function with significantly less energy. Energy saving is a factor not only in hardware and system architecture, but also in software, for example the implementation of protocol stacks, where every single transmission byte will have to justify its existence. There are already some battery-free wireless sensors that can transmit their readings a distance of a few meters. Like RFID systems, they obtain the power they require either remotely or from the measuring process itself, for example by using piezoelectric or pyroelectric materials for pressure and temperature measurements.
- *Interaction and short-range communications:* Wireless communication over distances of a few centimeters will suffice, for example, if an object is touched by another object or a user holds their mobile against it. Where such short

distances are involved, very little power is required, addressing is simplified (as there is often only one possible destination) and there is typically no risk of being overheard by others. NFC is one example of this type of communication. Like RFID, it uses inductive coupling. During communication, one partner is in active mode and the other can be in passive mode. Active NFC units are small enough to be used in mobile phones; passive units are similar to RFID transponders and are significantly smaller, cheaper and do not need their own power source.

- *Wireless communications:* From an energy point of view, established wireless technologies such as GSM, UMTS, Wi-Fi and Bluetooth are far less suitable; more recent WPAN standards such as ZigBee and others still under development may have a narrower bandwidth, but they do use significantly less power.

5 RFID and the EPC network

RFID (Radio Frequency Identification) is primarily used to identify objects from a distance of a few meters, with a stationary reader typically communicating wirelessly with small battery-free transponders (tags) attached to objects. As well as providing two important basic functions for an Internet of Things – identification and communication – RFID can also be used to determine the approximate location of objects provided the position of the reader is known.

At the end of the 1990s, RFID technology was restricted to niche applications such as animal identification, access control and vehicle immobilizers. High transponder prices and a lack of standards constituted an obstacle to the wider use of the technology. Since then, however, its field of application has broadened significantly, mainly thanks to MIT's Auto-ID Center, which was founded in 1999. The Auto-ID Center and its successor organization EPCglobal have systematically pursued a vision of cheap, standardized transponders identifying billions of everyday objects, and they have developed the necessary technology jointly with commercial partners. The use of RFID technology in the supply chains of retail giants such as Wal-Mart and Metro is the result of these efforts. While the adoption by major retailers represents a remarkable success, the evolution of RFID and its associated infrastructure technologies in recent years also highlights challenges involved in realizing an Internet of Things in the broader sense of the term.

The development of RFID over recent years is reflected not only in technical progress but also in cost reductions and standardization. For example, the power consumption of the latest generation of transponders is less than 30 μW, with reading distances of up to ten meters possible under favorable conditions. Increasing miniaturization has also led to a unit price of close to five cents for bulk orders of simple RFID transponders. Major progress has also been made in the field of standardization, with the ISO 18000-6C RFID protocol – also referred to as EPCglobal Gen2 – being supported by several manufacturers, dominating the market and guaranteeing interoperability.

High cost pressure and the absence of batteries in transponders means that RFID communications protocols cannot be based on established Internet protocols due to a scarcity of resources. For example, a typical RFID microchip merely consists of a few hundred thousand transistors, contains no microcontroller and has minimal storage capacity – usually just a few bytes. Instead of using a battery, passive RFID microchips are supplied with power remotely from a reading device. Since the power supply can frequently be interrupted due to "field nulls", the transmission of large data packets is avoided – at 128 bits, these are typically much shorter than IP packets. Everyday objects that are to be addressed in an Internet of Things using RFID technology will therefore not behave in exactly the same way as Internet nodes. Instead, it is likely that a highly optimized wireless protocol will be used over the last few meters due to scarce resources and the adverse conditions encountered in the physical world. The RFID reader would act as a gateway between the two different protocols. TCP and HTTP-based protocols have been developed for use in RFID environments, where they are used to configure readers and distribute the data captured via the Internet.

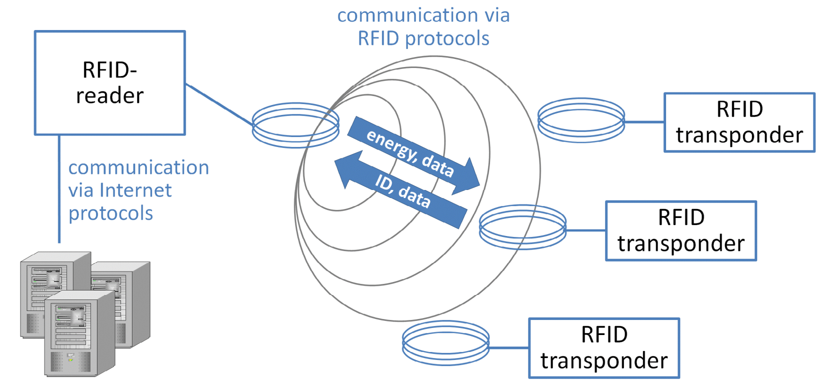

Figure 2. RFID communication.

One key application area for RFID is logistics. Whereas previously information systems had to be "hand-fed" with data via a keyboard or bar code reader, data relating to logistics units can now be captured automatically, without delay and at a fraction of the cost using RFID technology. The systematic development of RFID technology now means it is used not only in the commercial supply chain, but also in numerous other application areas. For example, RFID is used to manage books and media in libraries, to locate tools and other portable inventory items in factories, and even in the apparel industry, where RFID systems ensure that the retail store shelves are regularly replenished with the appropriate clothing items.

Most of the RFID applications deployed are closed-loop applications. When RFID systems are introduced in open-loop applications such as supply chains involving many different partners with different commercial interests, the resulting organizational complexity can rapidly become a problem. It is therefore advisable to use RFID initially within a single organization, and perhaps even within a limited geographical area. In such closed-loop applications, costs can be directly offset against added value and gains in efficiency, and technological challenges are often easier to overcome.

Transferred to the general Internet of Things vision, this means that we are unlikely to see "global" applications requiring cooperation between many different partners any time soon. It is thus important to use standardized interfaces to implement local applications, which can then be combined at a later point in time.

In the long term, infrastructure such as the EPC network will play an important role [28]. The EPC network takes its name from the "Electronic Product Code" – a structured identifier that uniquely identifies each individual product-related RFID transponder. The aim of the EPC network is not only to enable RFID technology to identify objects, but also to simplify the processing and exchange of the data captured. The EPCIS standard represents a fundamental part of this network, and is already supported by many software manufacturers. It defines events that can be used to link the RFID data captured by readers with contextual information. For example, EPCIS events cannot only tell when and where a particular transponder was detected, but also provide information on associated business processes or application events. Custom, application-specific business logic is used for the contextual data interpretation that results in the generation of EPCIS events.

In addition to defining EPCIS events, the EPCIS standard also defines an interface that can be used to search for such events in repositories. If the repositories that hold information on a particular RFID transponder are known, one can follow the "trail" of the object to which it is attached. In practice, however, there are numerous problems associated with this type of global information scenario. For example, one would not normally know all of the repositories that held data relating to a given object, and a global search of all repositories would be unrealistic as their numbers grow. In many cases, the data would be commercially confidential and not generally accessible – even the fact that a company possesses information relating to a particular object may itself be confidential. These difficulties show that there are still many challenges relating to applicability, scalability and security that need to be overcome before we can achieve an Internet of Things that supports such global queries.

6 IP for things

If, in a future Internet of Things, everyday objects are to be addressed and controlled via the Internet, then we should ideally not be resorting to special communications protocols as is currently the case with RFID. Instead, things should behave just like normal Internet nodes. In other words, they should have an IP address and use the Internet Protocol (IP) for communicating with other smart objects and network nodes. And due to the large number of addresses required, they should use the new IPv6 version with 128-bit addresses.

The benefits of having IP-enabled things are obvious, even if the objects in question are not going to be made globally accessible but instead used in a controlled intranet environment. This approach enables us to build directly on existing functionality such as global interoperability, network-wide data packet delivery (forwarding and routing), data transport across different physical media, naming services (URL, DNS) and network management. The use of IP enables smart objects to use existing Internet services and applications and, conversely, these smart objects can be addressed from anywhere since they are proper Internet participants. Last but not least, it will be easy to use important application layer protocols such as HTTP. IPv6 also provides the interesting capability of automatic address configuration, enabling smart objects to assign their own addresses.

Until recently, however, the prospect of full IP support for simple things appeared illusory due to the resources required (such as processor capacity and energy) and thus the costs involved. Instead, it was suggested to connect smart objects to the Internet indirectly via proxies or gateways. But the disadvantage of such non-standardized solutions is that end-to-end functionality is lost because standardized Internet protocols would be converted to proprietary protocols over the last few meters. Gateways would also generate added complexity, making installation, operation and maintenance time-consuming and costly.

However, there are now not only 16-bit microcontrollers with sufficient storage that require less than 400 μW/MIPS, but also TCP/IPv6 stacks that can operate with 4 kB RAM and 24 kB flash memory [13]. Equally important are wireless communications standards such as IEEE 802.15.4 that cover the layers below IP and consume relatively little power – ZigBee implementations require approximately 20 to 60 mW (for 1 mW transmission power, a range of 10 to 100 meters and a data transmission rate of 250 kbit/s). Whenever possible, the wireless unit is being used for short periods of time only in order to save energy. This approach enables AA batteries to provide a modest level of computing power and wireless communication that is nevertheless sufficient for many purposes over many months.

The opportunities that this opens up have recently led to companies and standards committees adopting various measures. At the end of 2008, Atmel, Cisco, Intel, SAP, Sun Microsystems and other companies founded the “IP for Smart Objects” (IPSO) corporate alliance to promote the implementation and use of IP for low-powered devices such as radio sensors, consumption meters and other smart objects. More specifically, the “IPv6 over Low Power Wireless Area Networks” (6LoWPAN) working group set up by the Internet Engineering Task Force (IETF) is addressing the problem of supporting IPv6 using the 802.15.4 wireless communication standard [14]. This is a technical challenge because the maximum length of 802.15.4 data frames is only 127 bytes due to lower data rate, higher susceptibility to failure and bit error rate of wireless communications. The IPv6 packet header alone is 40 bytes long (primarily due to the source and target addresses each being 16 bytes long), and unfragmented IPv6 packets can be up to 1280 bytes long.

To make IPv6 communications function efficiently in wireless networks, a protocol modification layer has been defined that essentially deals with four issues – embedding IPv6 packets in 802.15.4 frames, fragmenting long packets to fit these frames, statelessly compressing packet headers (typically to just 6 bytes), and forwarding IPv6 packets via multihop wireless routes. It is possible to compress the IPv6 header so drastically because 802.15.4 nodes communicate mainly within their own wireless network, and therefore most of the information can be reconstructed from the general context or the surrounding 802.15.4 frames and considerably shorter local addresses can be used.

The working group’s proposal has now been published as proposed Internet standard RFC 4944, and an implementation based on this is described in [13]. In 2009, the ZigBee Alliance announced it would be incorporating this “native IP support” into future ZigBee specifications, “allowing seamless integration of Internet connectivity into each product”.

7 The Web of things

One logical development of the Internet of Things is to leverage the World Wide Web and its many technologies as an infrastructure for smart objects. Several years ago, Kindberg et al. put forward the idea of marking physical objects with URLs that could, for example, be read using an infrared interface and cross-reference Web pages containing information and services on the objects in question [16]. Another fundamental way of using the Web is to incorporate smart objects into a standardized Web service architecture (using standards such SOAP and WSDL), although in practice this might be too expensive and complex for simple objects.

Instead of conventional Web service technology, the recently established “Web of Things” initiative [12] uses simple embedded HTTP servers and Web 2.0 technology. Modern Web servers with a sufficient feature set (support for several simultaneous connections, an ability to transmit dynamically generated content, and “server push” event reporting) can make do with 8 kB memory and no operating system support thanks to clever cross-layer TCP/HTTP optimization. These web server implementations are therefore suitable for even tiny embedded systems such as smart cards, where they provide a high level API to a low power device [4]. Since embedded Web servers in an Internet of Things generally possess fewer resources than Web clients such as browsers on personal computers or mobile phones, AJAX technology (Asynchronous JavaScript and XML) has proved to be a good way of transferring some of the server workload to the client.

In the Web of Things, smart objects and their services are typically addressed via URLs and controlled via a simple interface using a few well-defined HTTP operations such as GET and PUT. The data that objects transmit to the Web usually takes the form of a structured XML document or a JSON object that is machine-readable (using JavaScript). These formats can be understood not only by machines but also by people, provided meaningful markup elements and variable names are used. They can also be supplemented with semantic information using microformats.

In this way, smart objects can not only communicate on the Web but also create a user-friendly representation of themselves, making it possible to interact with them via normal Web browsers and explore the world of smart things with its many relationships (via links to other related things). Dynamically generated real-world data on smart objects can be displayed on such “representative” Web pages, and can then be processed using the extensive functionality of widely available Web 2.0 tools. For example things could, via their digital representations, be indexed like Web pages, users could “google” their properties, or they could be passed on as references. The physical objects themselves could become active and keep blogs or update each other using social networking tools like Twitter. Although this may sound like an odd humanizing of inanimate objects, it is of practical significance. The Web and its services are being used as ubiquitous middleware – facilitating the implementation of new functionality and innovative applications for smart things. So if, for example, your washing machine is in the basement and you want to monitor its progress, you could subscribe to its atom feed on a Web client and get information on major state changes, or follow its tweets on Twitter.

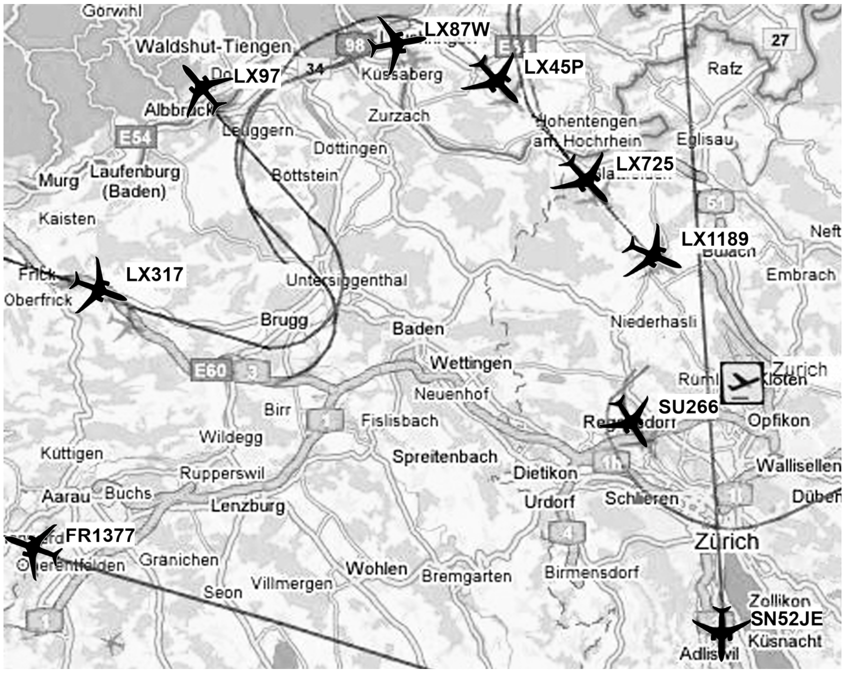

Figure 3. A mashup displaying flight paths around Zurich [18].

In a more generalized way, a mashup editor can be used to link event and data streams from physical objects with each other (and with Web services). Here is an example to illustrate this: most planes are equipped with radio beacons (“ADS-B”) that transmit a short data packet once or twice per second at 1090 MHz, which can be received within a range of a few hundred kilometers. In addition to the plane’s identifier, this packet contains its current position, height, speed and rate of climb or descent. At http://radar.zhaw.ch one can find a mashup that uses Google maps to display the real-time flight paths of planes around Zurich in Switzerland (see Figure 3; the size of the shadow and its proximity to the plane symbol indicates altitude). This mashup is enriched with additional data from various sources such as www.flightstats.com. Clicking on the plane symbol now also results in a display of details such as the airline, departure and destination airports, expected arrival time, etc.

Although planes are not small “everyday objects” as envisaged in an ultimate Internet of Things, this example convincingly illustrates the potential for connecting the physical world with cyberspace. A more “down-to-earth” physical mashup is described in [12] which displays the energy consumption of appliances such as fridges, kettles and PC screens on Web browsers by using smart power sockets and Web technology.

Regardless of the long-term vision of an Internet of Things, cheap embedded Web interfaces could soon open up a wide variety of application opportunities. Take the example of household automation, for instance. To save energy and reduce costs or – particularly in private homes, to increase comfort and security – temperature sensors, motion detectors and other types of sensors will control many different aspects of buildings such as lighting, heating, ventilation, shutters and locking systems. To do so, these units need to be able to communicate. In the past, a variety of standards were developed, such as the European Installation Bus (EIB), but installation was still a rather costly business; and configuring, parameterizing and assigning addresses to the units had to be done in situ by experts using special software.

Since it is cheap, standardized and widely available, Web and Internet technology could be the answer here. Such an approach would allow for the use of tried-and-tested network concepts (such as auto-configuration and network management tools), and remote maintenance would be possible using standard Web browsers and interfaces. With smart household devices ("Web 2.0-ready"), WLAN-enabled electricity meters and other wirelessly communicating and self-integrating gadgets, it might then be possible to gradually realize the old dream (or perhaps nightmare?) of the "smart home"…

8 Social and political issues

The Internet has long since changed from being a purely informational system to one that is socio-technological and has a social, creative and political dimension. But the importance of its non-technological aspects is becoming even more apparent in the development of an Internet of Things, since it adds an entirely new quality to these non-technological aspects. So in addition to the positive expectations mentioned above, several critical questions need to be asked with regard to possible consequences.

Much of the public debate on whether to accept or reject the Internet of Things involves the conventional dualisms of "security versus freedom" and "comfort versus data privacy". In this respect, the discussion is not very different from the notorious altercations concerning store cards, video surveillance and electronic passports. As with RFID [27], the unease centers primarily on personal data that is automatically collected and that could be used by third parties without people's agreement or knowledge for unknown and potentially damaging purposes.

And personal privacy is indeed coming under pressure. Smart objects can accumulate a massive amount of data, simply to serve us in the best possible way. Since this typically takes place unobtrusively in the background, we can never be entirely sure whether we are being "observed" when transactions take place. Individual instances of observation might seem harmless enough, but if several such instances were to be amalgamated and forwarded elsewhere, this could under certain circumstances result in a serious violation of privacy.

Irrespective of the data protection issues, there is also the question of who would own the masses of automatically captured and interpreted real-world data, which could be of significant commercial or social value, and who would be entitled to use it and within what ethical and legal framework.

Another critical aspect is that of dependence on technology. In business and also in society generally we have already become very dependent on the general availability of electricity – infrequent blackouts have fortunately not yet had any serious consequences. But if everyday objects only worked properly with an Internet connection in the future, this would lead to an even greater dependence on the underlying technology. If the technology infrastructure failed for whatever reason – design faults, material defects, sabotage, overloading, natural disasters or crises – it could have a disastrous effect on the economy and society. Even a virus programmed by some high-spirited teenagers that played global havoc with selected everyday objects and thus provoked a safety-critical, life-threatening or even politically explosive situation could have catastrophic consequences.

Remotely controlled things could also cause us to become dependent and lose our supremacy on a personal level. And even with no ill intent, our own smart objects might not behave as we would wish, but rather as they "believe" is best for us – presaging a subtle type of technological paternalism [24]. The prompt feedback that smart things can give us about themselves or that helpful tools such as smartphones and augmented reality spectacles can give us about our environment is also a mixed blessing. While it can encourage us to do good, useful things (such as an animated smiley in a smart bathroom mirror that praises us for brushing our teeth properly with the electric toothbrush), it can also seduce us into making unnecessary impulse purchases.

The Internet of Things has now arrived in politics. A study for the "Global Trends 2025" [21] project carried out by the US National Intelligence Council states that "foreign manufacturers could become both the single source and single point of failure for mission-critical Internet-enabled things" [25], warning not only of the nation becoming critically dependent on them, but also highlighting the national security aspect of extending cyberwars into the real world: "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" [26].

The European Commission is reflecting vocally but somewhat vaguely on the problem of governance for a future Internet of Things. The issue here is how to safeguard the general public interest and how to prevent excessively powerful centralized structures coming into being or the regulatory power of the Internet of Things falling exclusively into the hands of what they describe as a single "specific authority".

The European Commission's action plan on the Internet of Things [5] mentioned above has also provoked a huge emotional backlash, as critically noted in the German "Telepolis" [17] online magazine with its lead story entitled "A brief route to collective incapacitation" (the tone of the article is that the Internet of Things would cost a lot of money, that consumers would have to pay for it, and that its benefits would be small). Readers' comments on the article describe the Internet of Things as a "world of enforced networking" and a "gigantic funny farm"; it would make us "totally dependent on technology and those in power" and would mean "surrendering all freedom". It was even called a perversion of the Internet and its alleged political mission:

"a medium that was developed to free mankind and that should be used for this purpose could hence be misused in order to establish total control".

Although these extreme opinions are not representative, it must be said that for an Internet of Things to be truly beneficial requires more than just everyday objects equipped with microelectronics that can cooperate with each other. Just as essential are secure, reliable infrastructures, appropriate economic and legal conditions and a social consensus on how the new technical opportunities should be used. This represents a substantial task for the future.

Acknowledgements. Our thanks go to Christof Roduner and Kay Römer for their constructive criticism, and to Elgar Fleisch for many interesting discussions and fascinating joint projects on the Internet of Things.

References

1. Adelmann, R., Langheinrich, M., Floerkemeier, C.: 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. (eds.) Informatik 2006 – GI Lecture Notes in Informatics (LNI) 94, pp. 366–373 (2006)
2. Ashton, K.: That 'Internet of Things' Thing. RFID Journal, www.rfidjournal.com/article/print/4986 (2009)
3. Coroama, V.: 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, pp. 135–152 (2006)
4. Duquennoy, S., Grimaud, G., Vandewalle, J.-J.: Smews: Smart and Mobile Embedded Web Server. Proc. Int. Conf. on Complex, Intelligent and Software Intensive Systems, pp. 571–576 (2009)
5. European Commission: Internet of Things – An action plan for Europe. COM(2009) 278, http://eur-lex.europa.eu/LexUriServ/site/en/com/2009/com2009_0278en01.pdf (2009)
6. Fleisch, E., Mattern, F.: (eds.) Das Internet der Dinge. Springer (2005)
7. Fleisch, E.: What is the Internet of Things? When Things Add Value. Auto-ID Labs White Paper WP-BIZAPP-053, Auto-ID Lab St. Gallen, Switzerland (2010)
8. Floerkemeier, C., Mattern, F.: 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 (2006)
9. Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., Sarma, S.E.: (eds.) The Internet of Things. First International Conference, IOT 2008, LNCS 4952, Springer (2008)
10. Frank, C., Bolliger, P., Mattern, F., Kellerer, W.: The Sensor Internet at Work: Locating Everyday Items Using Mobile Phones. Pervasive and Mobile Computing 4(3):421–447 (2008)
11. Gershenfeld, N.: When Things Start to Think. Henry Holt and Company (1999)
12. Guinard, D., Trifa, V., Wilde, E.: Architecting a Mashable Open World Wide Web of Things. TR CS-663 ETH Zürich, www.vs.inf.ethz.ch/publ/papers/WoT.pdf (2010)
13. Hui, J., Culler, D.: IP is Dead, Long Live IP for Wireless Sensor Networks. Proc. 6th Int. Conf. on Embedded Networked Sensor Systems (SenSys), pp. 15–28 (2008)
14. Hui, J., Culler, D., Chakrabarti, S.: 6LoWPAN – Incorporating IEEE 802.15.4 into the IP architecture. Internet Protocol for Smart Objects Alliance, white paper # 3 (2009)
15. International Telecommunication Union: The Internet of Things. ITU (2005)

16. 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.: People, Places, Things: Web Presence for the Real World. Mobile Networks and Applications 7(5):365–376 (2002)
17. Kollmann, K.: Das „Internet of Things" – Der kurze Weg zur kollektiven Zwangsentmündigung. Telepolis, www.heise.de/tp/r4/artikel/30/30805/1.html (2009)
18. Kramarz, D., Loeber, A.: Visualisierung von Transponder-Daten mittels Mashup. Diplomarbeit, Zürcher Hochschule für Angewandte Wissenschaften (2007)
19. Mattern, F., Floerkemeier, C.: Vom Internet der Computer zum Internet der Dinge. Informatik-Spektrum 33(2):107–121 (2010)
20. Mattern, F., Staake, T., Weiss, M.: ICT for Green – How Computers Can Help Us to Conserve Energy. Proc. e-Energy 2010, ACM, pp. 1–10 (2010)
21. National Intelligence Council Global Trends 2025: A Transformed World. www.dni.gov/nic/NIC_2025_project.html (2008)
22. Sarma, S., Brock, D.L., Ashton, K.: The Networked Physical World. TR MIT-AUTOID-WH-001, MIT Auto-ID Center (2000)
23. Schoenberger, C.R.: The internet of things. Forbes Magazine, March 18 (2002)
24. Spiekermann, S., Pallas, F.: Technology paternalism – wider implications of ubiquitous computing. Poiesis & Praxis 4(1):6–18 (2006)
25. SRI Consulting Business Intelligence: Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests out to 2025. www.fas.org//nic/.pdf (2008)
26. SRI Consulting Business Intelligence: Disruptive Civil Technologies, Appendix F: The Internet of Things (Background). www.dni.gov/nic/PDF_GIF_confreports//_F.pdf (2008)
27. Thiesse, F.: RFID, Privacy and the Perception of Risk: A Strategic Framework. The Journal of Strategic Information Systems 16(2):214–232 (2007)
28. Thiesse, F., Floerkemeier, C., Harrison, M., Michahelles, F., Roduner, C.: Technology, Standards, and Real-World Deployments of the EPC Network. IEEE Internet Computing 13(2):36–43 (2009)
29. Weiser, M.: The Computer for the 21st Century. Scientific American 265(9):66–75 (1991)