



THE INTERNET OF THINGS: TECHNOLOGICAL AND SOCIAL ASPECTS

Grzegorz Sowa, Alina Marchlewska

IT Institute, University of Social Sciences, Łódź, Poland
g22sowa@gmail.com, amarchlewska@spoleczna.pl

Abstract

The basic idea of the Internet of Things is the presence around us of a variety of things – such as RFID tags, sensors, actuators, mobile phones, etc. – which are able to interact with each other and cooperate with their neighbors to reach common goals. Semantic oriented IoT visions have also been proposed. The number of items involved in the future Internet is destined to become extremely high. Therefore, issues pertaining how to represent, store, interconnect, search, and organize information generated by the IoT will become very challenging. In this context, semantic technologies will play a key role. And creative approaches to visualizing data – humans are far better than computers at seeing patterns – frequently prove integral to the process of creating knowledge. From a privacy perspective, IoT is challenging because it operates in private settings, like homes, and presents an attack target that is harder to secure.

Key words: Internet of Things, RFID systems, Big Data, privacy, user interface

1 Introduction

The development of information technology has brought about universal information access and measurements. This can be explained by way of a simple example: the measurement of time. We often continue to wear watches; clocks hang on the wall largely for decorative purposes. Yet time is displayed on mobile phones as a basic non-core function. And it is also displayed on electric ovens, microwaves, computer screens, television screens, television decoders, weather stations, in the car – wherever we look, we will see the current time. The everyday items that surround us have functions that cross over, and they are driven by electronic devices of a level of complexity similar to that of computers. The items are often connected to external networks – even a simple weather station may be synchronising with a central clock somewhere in Europe. And of course computer-smartphone-tablets make automatic updates not only of the date and time but of their operating systems or anti-virus protection.

Another noteworthy characteristic is the connection of these devices to the internet, which enables them to communicate with each other. This creates completely new technological potential; we are not far away from a refrigerator which can let us know by mobile phone when its stock of a product has fallen below a prescribed minimum, allowing you to make that same order in a shop. This is what the Internet of Things looks like, and it is fast becoming a reality. There are several features of this phenomenon that are worth a closer look. Our starting point is with the technical solutions, which are already quite advanced, although some standards are still to be developed. One interesting aspect here is the problem of analysing the large amounts of data which are a by-product of these systems - the problem of 'big data' takes on a new dimension. Another issue is that of the interface. All the devices have an interface – even if it is only a standard time display. These need to be carefully designed – and this must be done from the starting-point of the needs and capabilities of users and not of the limitations of hardware or software which are ever-decreasing. Today's interface designers must be psychologists, sociologists and artists and not just specialists. And lastly let us not omit to consider security issues and the protection of personal data.

2 The concept of the Internet of Things

The Internet of Things (IoT) is formed as a result of the presence around us of a variety of devices such as RFID tags, sensors, actuators and smartphones, which when covered in a uniform addressing scheme can work together pursuing common tasks. Linking the sensors and control systems of the various devices creates an opportunity to exchange information between different platforms with a uniform standard. This brings potential for the development of innovative systems. Such an objective is achieved via comprehensive measurement, data analysis and information presentation, usually with the use of cloud computing [Atzori, 2010, p.1].

3 The technology and architecture of the Internet of Things

As is the case in conventional computer networks, the Internet of Things is built in layers. At the lowest level, that of hardware, we have firstly the measuring and implementing components: RFID tags and implanting components (actuators) associated with wireless WSN (Wireless Sensor Network) networks and NFC (Near Field Communication) networks. The key elements are the 'spims' – self-sufficient objects whose positions can be tracked over time. This category includes 'smart items' which provide wireless connectivity and memory and that are autonomous in action [Fritzche, 2015, p. 20].

Such equipment fulfils basic functions:

- Identification and storage of information (RFID)
- Communication (WNS)
- Information processing
- Physical communication, control and operations

A general overview of the layers of the Internet of Things can be presented as follows:

- Application layer
- Intermediary layer ('middleware')
- Internet layer
- Access goals layer ('access gateway')
- Technology layer ('hardware')

The intermediary layer - 'middleware' - provides an interface between the hardware and the applications. In recent years, there has been a proliferation of service-orientated architecture (SOA), which allows the creation of applications with well-defined components. This layer is responsible for the management of devices and information, the filtering and aggregation of data, semantic analysis, and access control.

The application layer includes various relevant solutions e.g. in the fields of logistics, healthcare, environmental protection [Bandyopadhyay, 2011, p. 5].

The internet of the future will be very different to the one that we know today. Currently, communication is generally host-to-host, and we mainly use the network for acquisition or publication of information. However, the networks of the future will be built around the data itself: this assumes that both the data and queries to it will be self-addressing and self-routable (have built-in protocols). Such features already exist of course in the object-orientated programming era. Research carried out by Koponen's team suggested the need for change in addressing practises in the Internet. They proposed replacing the hierarchical DNS system into a 'flat' one, in which names and addresses would include everything above the IP layer; each object ('thing') would have its own address and be available on the Internet. This proposal is called DONA: Data-Orientated Network Architecture [Koponen, 2010, p. 2]. Internet \emptyset is spoken of differently here, in terms of a transformation of today's 'internet devices' in the 'Internet of Things'. The IPSO (Internet Protocol for Smart Objects) was developed by this team.

A recent UN report [Botterman, 2009] states that in the coming era humans will be a minority of recipients and senders of data on the Internet; most communication will be between smart objects. The basic concepts in the field of the Internet of Things are the oriented network and object, but the overriding approach (semantic-orientated) focuses on meaning [Botterman, 2009, p.

8]. While network and web approaches are focussed on protocols and programming languages, the semantic approach focuses on the meaning of the data and how the information can be represented.

The semantic layer includes [Atzori, 2010, p. 3]:

- Semantic technologies
- Inferences based on data
- Semantic environmental regulations
- Semantic middleware

Two components made possible the early applications of the Internet of Things: the RFID - Radio Frequency Identification and the WSN - Wireless Sensor Network. RFID is still the key technology due to technological maturity, low costs, and strong resulting support enterprises [Pang, 2013, p. 43]. Passive and active RFID chips are widely used in logistics and are gradually replacing bar codes in commerce. WSN networks combine sensors and implanting components (actuators) in the network and integrate them with higher level systems throughout the net. However it is already apparent that a wider spectrum of technologies supporting the Internet of Things has been created: Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) are now elementary components that combine the world of things with the digital world. The development of supporting platforms such as Wireless Identification and Sensing Platforms (WISP) is significant.

Sensor nodes transmit their data (location, temperature, movement) to the so-called 'sink' – a special node that collects information. Such measurement nodes are lightweight, inexpensive and easy to install and maintain but their capabilities are limited. Their constituent elements are: power, processing unit, communication and sensing element. It is possible to create a network of thousands of sensors that gathers, processes and analyses information. The principal relevant issues are: energy efficiency, scalability, reliability and resistance to interference.

Sensors gather information about objects and processes and events. Technically they are transducers which convert physical signals into electronic impulses. Sensors link the physical world to digital measurements of real processes and events, and convert them into a form that can be stored and processed. Placing a large number of sensors in many places brings great benefits – from improvements in logistics to enhanced levels of safety. Sensor networks sometimes contain implementing components that manipulate the real world, such as boiler switches.

There is a distinction between active sensors that are equipped with an external power supply, and passive ones that obtain their energy from the measured object e.g. by infrared waves. Another classification is for sensors that are resistive, capacitive, inductive or piezoelectric.

A comparison of technologies is presented in this table:

Table 1. Comparison between RFID systems, wireless sensor networks, and RFID sensor networks. Source: [Atzori 2010, p. 5].

technology	pro- cessing	collecting of information	communica- tion	range (metres)	power	durabil- ity	Size	standard
RFID	No	No	assymetric	10	harvested	unlim- ited	very small	ISO 1 8000
WSN	Yes	Yes	peer-to-peer	100	battery	up to 3 yrs	small	IEEE 802.15.4
RSN	Yes	Yes	assymetric	3	harvested	unlim- ited	small	none

Smart objects are those objects in our surroundings which we can identify – address and communicate with. Examples of such objects are [Nguyen, 2015, p. 58]:

- Smart key: contains an RFID tag, so that it is possible, for example, among other functions, to find its location
- Smart lighting: linked to a wireless controller that allows different settings, such as on/off
- Smart plate: able to identify the types of meals that are placed on it and to transmit this information to a database about the dietary behaviour of the user
- Smart air conditioning: scans data on the number of people in a room thus facilitating automatic temperature control
- Smart fridge: keeps track of stored products thus enabling automatic re-ordering [The Only Fridge as Smart as You, 2015]

4 Typical applications

In transport and logistics, communications and sensors (video, sonar, radar, induction loops and magnetometers) that enable the exchange of information between cars, and between cars and the store, are already in common use. They enable traffic jams and journey times to be reduced. Sensors placed in cars and trains, and on their routes, can provide information to a collision avoidance system, monitor the transport of hazardous materials and help in directing vehicles (assisted driving). Each step of the logistics chain (design, purchasing, production, transportation, storage, sales, after-sales service) can be monitored and reinforced with the help of RFID tags. Real-time visibility of a company’s operations and customers can bring about more efficient

supply chain management. It is possible to determine the location of goods being transported, their status, time of delivery, and any delays or errors [Xiao, 2011, p. 4].

An example within the field of environmental monitoring would be the tracking of perishable food goods at every stage (collection, processing, transportation, storage and consumption) to ensure supply chain efficiency. Temperature and humidity can be monitored/controlled at every stage. Another important application is tracking of the status of major engineering structures such as bridges or pipelines, which facilitates their maintenance. The incorporation of sensors that enable fast collection of measurement data in hard to reach places is possible during the construction phase.

In the field of healthcare, the ability to identify moving objects and people (e.g. children) brings about significant safety improvements. Identifying patients prevents confusion and provides an up-to-date treatment record. Specialised indicators of temperature, pressure and breathing can be used to monitor patients and, in combination with wireless networks, provide information about their health status in real time. This information can be displayed where it is needed, reducing the number of medical errors. Most of the sensors used in medicine are placed on the bodies of patients and it is possible to use them in patients' own homes, allowing them a safe life under medical supervision.

Recently, attention has been focussed on a rather startling issue. The aim of protecting individuals' privacy is straightforward; rather murkier is the use of so-called persuasion technologies which shape correct behaviour (from the point of view of, for example, patient care or the environment [Fogg, 2009]. A simple example of such a technology is already prevalent; beeping that reminds us of the need to fasten seat-belts in cars or dashboard display of information about current fuel consumption. The idea here is to influence the behaviour of users ('educating them') without compulsion or forcing them to do anything. Another example, and an amusing one, is a doll which behaves like a baby and demands constant attention in order to discourage teens from early parenthood [Fogg, 2009, str. 4].

5 The Internet of Things and Big Data

A problem specific to the Internet of Things is the huge amount of data collected by different measuring devices. Such data collection and, particularly, sound interpretation of the data is no longer possible using traditional tools – we are dealing with the issue of 'Big Data'. The growth in data has been unimaginable (in 2012 data from sensors was ten times greater in volume than total Internet traffic in 2000 [Richards, 2013, p. 1]).

However, this increase in the amount of collected and processed data is only an external symptom. More significant is the change in approaches to the calculation of results. Traditional experimental science is based around controlled experiments; current approaches are about recognizing patterns within chaotic incoming data and seeking to understand them. This approach is referred to as ‘data dredging’. In other words, we make the assumption that there is information lying within the data, even if we cannot yet understand it. Counter-intuitively, an active role for human operators here is often critical. ‘A creative approach to visualising data – people are much better at pattern recognition than computers – often proves to be crucial in the creation of knowledge’ [Shaw, 2014 p. 30].

Examples of meaningful discoveries of completely non-obvious patterns of behaviour have been given e.g. the deduction that a woman is pregnant based on the type of deodorant she purchases.

There is an interesting analogy here to another field of ‘big data’ – that of the analysis of social media. ‘The huge amount of information created by Internet users offers new potential for social analysis. The tools for analysing this data are still just beginning to be developed. Tools for monitoring social networking sites are already a major source of marketing information. However, we are dealing with a form of digital divide; only the reviews of customers who are online matter. From the standpoint of social marketing that’s simply an issue for commerce, but unrepresentative social research (e.g. electoral polling) is a political problem. The issue is of course well-known and it has been noticed for a long time that, for example, telephone users are not a good representative sample. Yet these days the temptation to limit oneself to analysing more easily available digital information is even greater.’ [Sowa, 2012, p. 13]

6 Protecting privacy in the era of the Internet of Things

RFID tags attached/worn by users create a completely new social world. When meeting someone we can automatically exchange information straight-away, we can provide live updates to social networking data about our location and activities. Such data can be used to communicate with other users or be saved as a digital diary. Of course, access to such information should be restricted. There are already sophisticated algorithms in practise which allow, for example, the identification of a person based on her behaviour patterns: how she moves, how she uses a mouse, etc. [Ziegler, 2015, p. 102].

Another example of an application is in security. We can find lost objects; a user can also be kept informed when an object (e.g. a valuable painting) changes its usual position.

Unfortunately, the Internet of Things is extremely sensitive to hacker attack [Atzori, 2010, p. 2]. Firstly, most of its components are inactive most of the time; they are also readily physically accessible. Wireless communication is easy to wiretap and most of the hardware components have little computing capability and so cannot effectively use sophisticated programming methods as a defence. Authentication is difficult – that requires infrastructure and servers that exchange information – it is hard to imagine it in place for RFID tags at present. Similarly, it is difficult to control for accurate data integrity. Several solutions have been proposed, based generally on the principle of a hierarchy of nodes, with those at higher levels treated as normal Internet nodes and made subject to normal authentication procedures.

Privacy and data protection are currently at the forefront of attention, and policy is ‘privacy at the design stage’ (Privacy by design – PbD). Internet of Things system designers are required to incorporate personal data protection considerations as early as possible, especially in the field of smart homes, and before the system is completely constructed [Urquart, 2016, p. 7]. What is essential here is the time and manner in which legal regulations will be made. This pyramid of regulatory strategies is interesting [Urquart, 2016, p. 13]:

- Self-regulation
- Forced self-regulation
- Organised self-regulation with discreet penalty
- Organised self-regulation with public penalty

And a pyramid of sanctions:

- Persuasion
- Letter of warning
- Civil trial
- Criminal trial
- Suspension of licence
- Removal of license

While learning from previous experience we are currently trying to keep up with current regulations for the development of the technology. In October 2014 a conference in Mauritius adopted a resolution on Big Data and the Internet of Things. The main recommendations were:

- Implement privacy at the design stage
- Transparency in data collection, processing and transmission
- Define the purpose of data collection
- Obtaining consent, limiting access
- Collecting only the data that is needed
- Data made available to those concerned, possible to correct and make changes to profiles
- Data anonymity if possible

In this day and age, the choice between safety and privacy has become critical.

7 The interface of the Internet of Things

The prevalence in the 1980s of last-century personal computers with popular computer applications (word processors, spreadsheets etc.) meant that literally everyone was a potential computer user. This was a drastic contrast with an earlier era where a very few computers were in use by professionals. This universality of usage led to an increase in the importance of interfaces, the development of which was as rapid as the development of the equipment itself; they were in fact the major component of software. Traditional interfaces based on a keyboard and drop-down menu (still in use) were replaced largely by GUI interfaces, where icons supplement or replace text. Still under development are voice interfaces, and more recently interfaces based on the interpretation of gestures (Gestalt User Interfaces).

In the era of the Internet of Things we make contact with new devices that continuously measure and observe our surroundings. In the past they operated independently (as thermostats, boilers and refrigerators), now they will be part of the Internet, and will exchange information. Interfaces different to the graphical user interfaces that we are used to will become necessary. Different types of 'responsive objects' are being researched. One of them is the touch-based interface TUI - Tangible User Interface [Sharlin, 2004]. Basically it is a digital world adaption of physical contact with the driven object. But here automation brings with it new opportunities: an object can change visually e.g. shapes can give us information about their state, can vibrate etc.

The concept has its own history. Kurt Koffka wrote in 1935: 'To a primitive man each thing tells us what it is and what is to be done with it: fruit says: 'Eat me', water says 'Drink me', thunder says 'Fear me' and a woman says 'Love me''. [Koffka, 1935, p. 3]

Freedom of manoeuvre (DOF – degree of freedom) is essential to interface design and so is linking it to the controlled object. From this point of view mouse cursor control has promising properties – its movements correspond exactly to the movements of the cursor. But it is not suitable for steering a model airplane, for example, moving in three-dimensional space [Sharlin, 2004, p. 2].

Intricate relationships between different systems increase the complexity of the design. One can imagine, for example, a system which supports the care of patients living at home detecting depression and deciding to increase light levels, whilst another application that manages energy gauges that nothing is moving in the house – it is empty and lights should be put out. When overly complex devices communicate directly with each other using wireless net-

works, mistakes in print execution by a neighbouring printer are common [Alur, 2015, p. 9].

This brings us to the idea of Cyber-Physical-Human Systems (CPHS) systems. In addition to a set of computing devices that communicate with each other and affect the physical environment, a place for the user must be found – for a person who must be meaningfully integrated into the control loops. A human must be able to intervene, interact with and use these systems.

The visualisation of information is an essential part of most applications because of the need to communicate with their users. Measurements which are not incorporated are useless. The purpose of visualisation is to provide information drawn from raw data. They must be presented in such a way that the user can utilise them. A simple example is the representation of real-world objects as virtual ones that can be depicted, accessible and show their states. Their representation can be physical or – more commonly – virtual. The basic devices in use here are smartphones, tablets and notebooks.

8 Conclusions

The Internet of things brings with it a qualitative change for the development of computer science. Computers are not only ubiquitous but are beginning to communicate directly with each other. This creates enormous opportunities to improve our quality of life but, as usual, also poses new risks. A car that reminds us constantly to fasten our seatbelts can be troublesome enough; a plate that vibrates unpleasantly when we place our pork knuckle onto it is perhaps a step too far. Maybe not everything that is technically possible is worth pursuing.

References

1. Alur, R., Berger E., Drobnis A.W., Fix L., Fu K., Hager G. D., Lopresti D., Nahrstedt K., Mynattm E., Patel S., Rexford J., Stankovic J., A., Zorn B., 2015, *Systems Computing Challenges in the Internet of Things*, Computer Community Consortium, September 22
2. Atzori L., Iera A., Morabito G., 2010, *The Internet of Things: A survey*, Computer Networks 54 (2010) 2787–2805
3. Bandyopadhyay D., 2011, Sen J., *Internet of Things - Applications and Challenges in Technology and Standardization*, Wireless Personal Communications, May 2011, Volume 58, Issue 1, pp 49-69
4. Botterman M., May 2009, *Internet of Things: An Early Reality of the Future Internet*, Report of the Internet of Things Workshop, Prague, Czech Republic
5. Fogg, B. J., Cuellar, G. & Danielson, D., 2009, *Motivating, influencing, and persuading users: an introduction to captology*. In A. Sears & J. A. Jacko (Eds.),

- Human-computer interaction. Fundamentals (pp. 109-122). London: CRC Press. Taylor & Francis Group
6. Fritzsche B., 2015, *Revealing the Invisible - Information Visualization in the Internet of Things Era*, Human Computer Interaction in the Internet of Things Era, Hauptseminar Medieninformatik SoSe
 7. Technical Report LMU-MI-2015-2, September, 2015 ISSN 1862-5207, 2015
 8. Gershenfeld N., Krikorian R., Cohen D., 2004, *The internet of things*, Scientific American 291 (4) (2004) 76–81.
 9. Koffka K., 1935, *Principles of Gestalt psychology*, New York
 10. Koponen T., Chawla M., Byung-Gon Chun, Ermolinskiy A., Kye Hyun Kim, Shenker S., Stoica I., August 2007, *A Data-Oriented (and Beyond) Network Architecture*, in: Proceedings of ACM SIGCOMM'07, Kyoto, Japan
 11. *Mauritius Declaration on the Internet of Things*, 14 October 2014, 36th International Conference of Data Protection and Privacy Commissioners, Balaclava
 12. Nguyen M., 2015, *Designing Smart Interactions for Smart Objects*, Human Computer Interaction in the Internet of Things Era, Hauptseminar Medieninformatik SoSe 2015, Technical Report LMU-MI-2015-2, September, 2015 ISSN 1862-5207
 13. Pang Z., 2013, *Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being*, Doctoral Thesis in Electronic and Computer Systems KTH – Royal Institute of Technology Stockholm, Sweden
 14. Richards N. M., King J. H., 2013, *Three Paradoxes of Big Data*, September 3, 66 STAN. L. REV. ONLINE 41
 15. Rieder A., 2015, *Health and Everyday Life: The Potential of Self-Monitoring in Managing the Own Health*, Human Computer Interaction in the Internet of Things Era, Hauptseminar Medieninformatik SoSe 2015, Technical Report LMU-MI-2015-2, September, 2015 ISSN 1862-5207
 16. Sharlin E., Watson B., Kitamura Y., Kishino F., Itoh Y., 2004, *On tangible user interfaces, humans and spatiality*, Personal and Ubiquitous Computing, 8(5): 338-346
 17. J. Shaw., 2014, *Why big data is a big deal*, Harvard Magazine
 18. Sowa G., Filutowicz Z., Paszkowski J., 2012, *Social Media Monitoring Tools, Computer Methods in Practice*; W-wa, ISBN 978-83-60434-94-9
 19. *The Only Fridge as Smart as You*, 2015, to Launch at CES, GE Appliances Pressroom LAS VEGAS—January 5