DEVICES IN THE INTERNET OF THINGS

DAVID BOYLE, ROMAN KOLCUN, ERIC YEATMAN

IoT – definitions and explanations

The Internet of Things – or IoT – is a term that captures the imagination of the technology- savvy across society. Its mention is typically met with a nod to comprehension. But, as the team from Imperial College, London explains, there lacks a ubiquitously agreeable and satisfactory definition of precisely what IoT means.

There are numerous examples of Internet-connected devices. These include smartphones, 'smart' appliances in homes, cars, personal health and fitness trackers, and so on. All of these are representative Internet of Things (IoT) technologies – and yet there are innumerable potentially connected things[1]. These examples are taken from the automotive and consumer electronics industries, but the basic concept extends to industrial monitoring, control and manufacturing processes, historically referred to as supervisory control and data acquisition (SCADA) and machine-to-

[1] Where 'things' in this context may extend to systems and processes, natural and man-made.

machine (M2M) type systems. There are many potential applications in the utilities, critical infrastructure monitoring and control and environmental monitoring [1].

This article charts the device-level technologies used in the creation of the IoT, including hardware, software and communications. We disambiguate and explain these technologies based on their suitability to application design, provide a comprehensive overview of the state-of-the-art, describe what is achievable today, and tentatively explore the future of connected things.

IoT's origins

IoT's emergence coincided with the development and popularisation of radio frequency identification (RFID) technology - originally described as a replacement for the barcode in mainstream media. Whilst being more costly than barcodes, RFID boasted significant advantages, such as the communicable range, ability to write data to a tag, and the possibility of reading multiple tags more efficiently with a single reader.

Pioneering work in the field was conducted at the Massachusetts Institute of Technology Auto-ID Center, founded in 1999, where initial work in RFID, the roots of which date back to World War II, was reconceived to make use of Internet computing, offloading workload at the tag/reader to the cloud, and ultimately making the technology cheaper and scalable. Later, that effort was divided along commercial and research lines as the utility and practicality of the technology, specifically in 'track and trace' logistics applications, were supported and adopted by industrialists. Credit is often attributed to Kevin Ashton, a co-founder of the Auto-ID Center, for coining the phrase 'Internet of Things' – albeit that the facts may be disputable.

RFID[2] is now just one of many component IoT technologies. Arguably, today's use of the term speaks more to Mark Weiser's prior articulation of ubiquitous computing. In the late 1980s and early 1990s, Weiser described this wave of computing technology as one that would 'recede into the background of our lives', where future human computer interaction models would be entirely different, ultimately subconscious and intuitive [2, 3]. We have arrived at a situation where it is practically trivial to integrate computation and communication into any manufactured thing, and it is equally feasible to connect and technologically perceive natural things using communicable sensors. Furthermore, it is possible to react to, and control the environment using embedded computing devices coupled with actuators – switches or valves, for example. This can be done manually from a remote location, or may be entirely automated.

Entire fields of research and development, including but not limited to networked embedded systems, Internet computing, 'Big Data', wireless communication, sensor networks, distributed systems, real-time systems, and cyber-physical systems, are synergised in IoT scenarios. Typically, the primary differentiators are application-level requirements and their related criticalities. There are a number of common component technologies. In every case, IoT applications require a minimum of the following: computation, communication, storage and energy. Application-level specifics determine which sensors and actuators are required, in addition to a host of other considerations including physical dimensions and environmental survivability, communications technology (including network architecture and environment, range, density, quality of service, etc.), computational and storage requirements, and energy provision[3]. Ultimately, the design space is enormous, and complexity is difficult to effectively overcome.

Evolving IoT devices

Thorough comprehension of functional and non-functional requirements is necessary to develop an effective, efficient design specification for an IoT device. Non-functional requirements are significantly more challenging to adequately address, whereas functional requirements simply describe what the device should do. In many cases, the functional requirements are trivial. It is beyond the scope of this article to fully address the design space for IoT devices and applications. Rather, we overview the devices that are now considered Internet of Things technology. Given the large design space and complexity, there are numerous barriers to entry. As a result, many types of device have been adopted as practical de facto hardware development platforms across a number of communities. These span:

- Research communities, like those in networked embedded systems wherein the tendency is to adopt 'mote'-class (i.e. highly constrained) devices.
- Hacker and maker communities that are typically based on open source designs, coupled with the emergence of education-oriented platforms.

In each case, intermediary 'operating systems', designed to simplify their programming by masking hardware complexity, are typically used. From an industry perspective, IoT devices are typically sold as products to the consumer market. Their technical specifications are often not fully disclosed, but they do rely on well-defined standards to ensure the necessary interoperability – for example, a smart appliance connecting to the Internet using the home WiFi connection.

The majority of devices are characterised as single board computers. In each case, devices are integrated microsystems that have all of the building blocks of a typical computer, including computational, storage and communications capabilities, in addition to numerous input and output possibilities. The final design for a market-ready product will likely be as efficient and cost-effective as possible in terms of design, but include sufficient redundancy to support software updates and potential shifts in standards.

Since the early 2000s [4], the wireless sensor network (WSN) community has worked with highly constrained devices characterised by limited energy, storage, communications (range and bandwidth), packet loss, etc. These characteristics are, in combination, typically resultant in 'mote'

[2] It is worth noting that RFID is not a single technology, and may refer to passive (and/or active) low, high or ultra-high frequency, and other hybrid systems that provide additional features.

[3] There are significant challenges surrounding data management, storage and search resulting from the multitude of connected devices. These aspects are beyond the scope of this article.

class devices. Incremental improvements to hardware components have led to net energy efficiency improvements (e.g. combined microcontroller and radio transceiver integrated on a single chip – i.e. System on Chip), increased computation for equivalent or less energy, more storage, etc. Algorithms and protocols have been developed to further improve efficiency and reliability. The literature is awash with surveys concerning these types of devices, including numerous efforts to develop modular systems to reduce the redesign burden and improve the time taken to prototype applications.

The 'maker' movements have focused on open source hardware, such as the Arduino (https://www.arduino.cc/) community – which, including hardware and software, has found its way into a number of start-up businesses. Enthusiasts in the open source space have worked with embedded Linux boards such as the Gumstix (https://www.gumstix.com/) and BeagleBone (http://beagleboard.org/). Those on the educational side have sought to reduce the barriers to entry in terms of cost and simplification – for example, the Raspberry Pi, which has also garnered a significant following in the maker community.

Industrialists have increasingly tended to incorporate monitoring systems into their operations. These were known as SCADA systems (e.g. using networked programmable logic controllers). Cellular connectivity has also been adopted, where M2M was a key enabling technology exploiting early cellular communications technologies. Both are now converging on IoT – either as "Industry 4.0" in Europe or cyber-physical systems in general (where there is control or actuation in the loop).

Communication: wired and wireless networks and standards

Wireless connectivity has been central to the development of many IoT standards.

A flavour of the relevant standards, many of which have been driven and contributed to by researchers in the wireless and sensor networks fields, is presented in the 'IoT standards and specifications' box. Some technical details relevant to a number of the wireless communications options for IoT devices are given in the 'Wireless IoT' box.

IoT standards and specifications

Standards and industrial specifications govern the main approaches and architectures in the design of IoT applications. The most important of these standards relate to communication; where the physical communications layer (i.e. the wireless medium) is specified with regard to the electromagnetic spectrum.

The IEEE 802.15.4 – 2003 Standard for Low Rate Wireless Personal Area Networks is one of the most important in the wireless sensor network domain, a constituent IoT technology. It specifies the physical and medium access control layers for radio modules that operate in the industrial, scientific and medical (i.e. unlicensed) bands, at 433MHz, 868 / 915MHz and 2.4GHz. The IEEE 802.15 WPAN Task Group 4 developed and released it during its investigation of a low data rate solution with long lasting (multi-year) battery life, and reasonably low complexity.

In contrast to WiFi (IEEE 802.11) and Bluetooth (originally IEEE 802.15.1), IEEE 802.15.4 offers lower data rates and lower power operation over similar, or greater distances (depending on band and transceiver power setting). This allows for applications with smaller bandwidth requirements, such as embedded sensing and control, to run on batteries (or ambient harvested energy) for extended periods (potentially up to decades, depending on environmental and operational conditions).

It is essential to understand the conceptual layers of the communications 'stack'. This is due to the intricate relationships between application level requirements and what is feasible given certain communications configurations and architectures. Neither the traditional Transmission Control Protocol / Internet Protocol nor OSI layered models are ideally suited to describing wireless sensor network type communications and applications abstractions. The former is perhaps the more appropriate, with specific sub-layering defined as necessary.

A noteworthy standardisation effort has been to bring IPv6 to wireless sensor networks. The Internet Engineering Task Force is responsible for most of this work. Specifically, the IPv6LoWPAN, Routing over Low Power and Lossy Networks (RoLL), and Constrained Restful Environments (CoRE) groups have been instrumental in developing standards to translate and compress IPv6 for IEEE 802.15.4 networks, develop appropriate routing capabilities, and enable URI-based interaction with embedded devices from web browsers, respectively. RoLL and CoRE are responsible for the development of RPL and CoAP, respectively, neither of which necessitate the use of a wireless communications medium.

There are several industrial alliances seeking to promote standards and specifications relevant to IoT devices. These include LoRA (www.lora-alliance.org), which focuses on LPWAN, the Internet Protocol for Smart Objects Alliance (IPSO, www.ipso-alliance.org), Thread (www.threadgroup.com), which focuses on reliability, security, efficiency and compatibility of smart home devices, the AllSeen Alliance (www.allseenalliance.org) that promotes interoperability amongst IoT devices, processes and systems at scale, and the Open Interconnect Consortium (www.openinterconnect.org).

Devices with wired connections to the Internet can also be part of the IoT. Indeed,

Standard	Version	Date	Frequency (GHz)	Bandwidth (MHz)	Data Rate	Modulation	Typical Range	Licenced	Example Chipset(s)
IEEE 802.11	ac	2013	5	20,40, 80,160	7.2 (min) - 867 (max) Mbps	QAM	35 m	No	Broadcom BCM43460
	n	2009	2.4	20,40	7.2 (min) - 150 (max) Mbps	QAM	35 m	No	
IEEE 802.15.4	2006	2006	2.4	2	250 kbps	O-QPSK	Up to 250 m	No	TI CC2520 TI CC2538
		2006	0.868	0.6	20 kbps	BPSK	Up to some km	No	Coronis Wavecard868
Bluetooth Low Energy (Bluetooth Smart)	4.0	2010	2.4	2	1 Mbps	GFSK	<100m	No	TI CC2541 u-blox OLS425 / OLP245

Table 1: Examples of IoT wireless connectivity options

Wireless IoT

Many IoT applications use short range (i.e. from tens of metres up to hundreds of metres) wireless communications technologies. Connection to the Internet is then achieved via gateway devices and longer range communications.

Much of the work carried out in the wireless sensor network research community has made use of radio transceivers designed to comply with licence-free industrial, scientific and medical (ISM-band) standards. Most significantly, the IEEE 802.15.4-2003 standard, which underlies WirelessHART (http://en.hartcomm.org/) and ZigBee (http://www.zigbee.org/), resulted in wide availability of a many compliant integrated circuits from major manufacturers (including Analog Devices, Texas Instruments, etc.). These operate in the 433MHz, 868 / 915MHz and 2.4GHz bands, and led to an explosion of practical WSN research. More recently, system-on-chip solutions, i.e. those that integrate a microcontroller and radio transceiver in a single piece of silicon, have been developed.

These offer similar functionality for incrementally improved communications efficiency and significantly improved computational efficiency. Similarly, Bluetooth Low Energy (aka Bluetooth Smart) and ANT/ANT+ (https://www.thisisant.com/) have been developed to support low-power, high data rate applications, and are typically found in consumer electronic health, fitness and lifestyle applications available today.

Data rates and communication range depend largely on the frequency of communication, and are traded accordingly. Longer transmission distances typically result in lower data rates (and increased antenna size). Recent advances using multiple antennae that exploit multipath propagation allow for bandwidth increases, thus throughput, to be achieved.

For the purposes of comparison, a selection of wireless technologies suitable for a range of IoT applications is given in Table 1. It is evident that for any application, the requirements must be understood prior to selecting an appropriate communications method. Trade-offs are inevitable, and it is likely that a range of solutions will co-exist in the future.

many standards relevant to IoT are designed independent of the particular physical communications medium and associated medium access control protocols. This makes for seamless interoperability at higher layers of the conceptual protocol stacks, and eases connectivity concerns in integrated applications.

Software in IoT Devices

A number of approaches exist to developing software for IoT devices. As the computing power available increases, the ease with which one may program the device tends to improve. The fewer resources that are available, the closer the software developer must get to the hardware. This is also true as the constraints placed on operation become more severe.

To reduce the complexity of programming devices, operating systems and associated programming languages have been designed or adapted to suit the embedded environment. These operating systems provide numerous advantages, such as the ability to reuse trusted code modules that perform standard duties (such as managing concurrency and interrupts, and medium access control, for example).

Considering the more computationally powerful single board computers, certain flavours of Linux have been developed, such as Yocto (https://www.yoctoproject.org/). High-end boards with significant processing capabilities are capable of running full-blown operating systems. Recently, mobile operating systems, such as Android, have been used, and stripped down versions have been touted by the big developers, such as Google's Brillo (https://developers.google.com/brillo/?hl=en) - marketed as an OS for IoT devices. Educational, more constrained, devices like the Raspberry Pi has its own Raspbian flavour of Linux.

Wireless sensor network-type devices have evolved over the past decade with support from two leading OS communities, namely TinyOS [4] and Contiki [5], initially developed at Berkeley and the Swedish Institute of Computer Science, respectively. Each has attracted a global development community, however it appears as if Contiki is likely to emerge as the dominant OS for Internet connected devices of this type. There are well-supported and tested implementations for each of the relevant standards mentioned in Sidebar 1 available in both of these operating systems. There are some other noteworthy community-driven efforts in this space, including FreeRTOS (http://www.freertos.org/), OpenWSN (https://code.google.com/p/openwsn/) and RIOT (http://www.riot-os.org/).

AUTHORS' CONCLUSIONS

Perhaps one of the most important, yet infuriating, conclusions that can be drawn is that any modern computing problem or solution can lay claim to being relevant to the Internet of Things. From a devices perspective, it is easier than ever to connect a sensor, a controller, or a mundane household item to the Internet. On the other hand, there are still significant challenges to be overcome. With regard to industrial applications with strict performance requirements, multiple constraints, and often-difficult operational environments, work is far from complete [6]. And so to a final comment on projections of the absolute number of connected Internet-connected devices in the coming years: many commentators predict 50 billion by 2020. There will be this many at the very least!

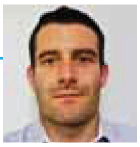
REFERENCES

1. Holler, J., Tsiatsis, V., Mulligan, C., Avesand, S., Karnouskos S., Boyle, D. 'From Machine-to-machine to the Internet of Things: Introduction to a New Age of Intelligence', 2014, Academic Press.
2. Weiser, M. 'The computer for the twenty-first century'. Sci. Am, Sept. 1991), 94-104.
3. Weiser, M. 'Some computer science issues in ubiquitous computing'. Commun. ACM 36, 7.
4. Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister. K., (2000) 'System architecture directions for networked sensors'. In Proceedings of the ninth international conference on Architectural support for programming languages and operating systems (ASPLOS IX). ACM, New York, NY, USA, 93-104.
5. Dunkels, A., Gronvall, B., Voigt, T., (2004) 'Contiki - a lightweight and flexible operating system for tiny networked sensors' in Local Computer Networks, 29th Annual IEEE International Conference on, 455-462.
6. Teich, J., 'Hardware/Software Codesign: The Past, the Present, and Predicting the Future,' in Proceedings of the IEEE, vol.100, Special Centennial Issue, pp.1411-1430, 2012

ABBREVIATIONS

CoRE	Constrained Restful Environments
IoT	Internet of Things
M2M	Machine-to-Machine
RFID	Radio Frequency Identification
RoLL	Routing over Low Power and Lossy Networks
SCADA	Supervisory Control and Data Acquisition
WSN	Wireless Sensor Network

ABOUT THE AUTHORS



Dr David Boyle

David is a Research Fellow in the Department of Electrical and Electronic Engineering at Imperial College London. He received his PhD in Electronic and Computer Engineering from the University of Limerick, Ireland, in 2009. A member of the Optical and Semiconductor Devices Group, and contributing to the Digital Economy Laboratory, his research interests lie at the intersection of applied complex sensing, actuation and control systems (cyber-physical systems), Internet of Things, data analytics, and digital economy.

Dr Roman Kolcun

Roman is a Research Associate in the Department of Electrical and Electronic Engineering at Imperial College London. He received his Master and Doctoral Degrees from Department of Computing, Imperial College London, working with the Adaptive Emergent Systems Engineering group. His main research interests include wireless sensor networks, distributed query processing, cyber-physical systems, embedded systems, communication protocols, and Internet of Things.

Professor Eric Yeatman

Eric is a Professor of Micro-Engineering and Head of the Department of Electrical and Electronic Engineering at Imperial College London. He has published more than 200 papers and patents on optical devices and materials, micro-electro-mechanical systems (MEMS), and other topics. His current research interests are in energy sources for wireless devices, radio frequency and photonic MEMS, and sensor networks.

ITP INSIGHT CALL

Want to talk to the author?

To discuss this article and its content, join in the ITP Insight Call on 8 February, 2016.

To book onto the call visit: https://www.theitp.org/calendar/