Moving from Sensors to Smart Objects

Xing Liu and Orlando Baiocchi
Institute of Technology
University of Washington Tacoma
Tacoma, USA
E-mails: {xingliu8,baiocchi}@uw.edu

***Abstract*—The Internet of Things connects the physical world together. From the standpoint of the Internet of Things, the connected physical world can be modelled as a family of interactive smart objects which incorporate sensors, actuators, computing hardware and software. This paper discusses how smart objects can be built on top of sensors and actuators. The paper also reviews technologies that are employed to implement smart objects and the Internet of Things.**

Keywords*— *Internet of Things, IoT, sensors, smart objects

I. INTRODUCTION

Internet of Things (IoT) has attracted enormous attention with its huge potential of applications in every aspect of our lives. Broad efforts have been made by industries, governments, and the academia to make IoT a reality. New IoT hardware and software products are being released rapidly.

IoT connects the physical world together. Among all the services IoT provides, “monitor and control” makes the most part. This requires the use of sensors and actuators. For this reason, people tend to think that IoT is a network of sensors and actuators. However, IoT researchers have found that it makes more sense to consider IoT as a network of smart objects which can operate autonomously, and such smart objects are the building blocks of the Internet of Things [1][2].

If IoT can be considered as a network of smart objects, then numerous questions can be raised. For example, what is a smart object? What is the relationship between smart objects and sensors/actuators? What do smart objects do? What are the enabling technologies for smart objects?

This paper tries to answer the above questions. The paper is organized into seven sections. Section II of the paper gives a brief overview about the Internet of Things. Section III discusses sensors and smart sensors. Section IV is a general introduction to smart objects. A detailed examination of smart objects is given in Section V. Section VI provides an overview on emerging technologies in IoT and smart objects. Conclusions are given in Section VII.

II. THE INTERNET OF THINGS

A. *Definition of IoT*

According to the IEEE [3], “an IoT is a network that connects uniquely identifiable ‘things’ to the Internet. The ‘things’ have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the ‘thing’ can be collected and the state of the ‘thing’ can be changed from anywhere, anytime, by anything”.

We can infer from the above IEEE definition that IoT can be modeled as a network of objects (things). These objects are identifiable, networked, programmable, and controllable, can sense and actuate, and can exchange information with each other.

B. *IoT Applications*

The industry is investing heavily on IoT. It is interesting to observe that many IoT applications and products are termed using the word “smart”. Application examples are “smart cities” and “smart homes”. Product examples are “smart thermostats” and “smart microwaves”. The phrase “Internet of Things” has also been “customized” for different application fields. For example, when the IoT concept is applied to manufacturing, it’s called the “Industrial Internet of Things”. CISCO moved further by coining the term “IoE” – the “Internet of Everything”. Other examples include the “Social Internet of Things” and the “Web of Things” (WOT).

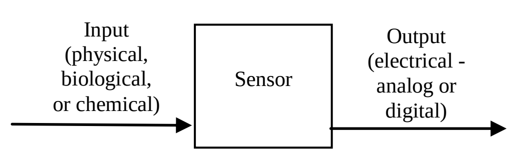
III. SENSORS

A. *Sensors*

According to NIST, a sensor is a transducer that converts a physical, biological or chemical parameter into an electrical signal and can return digital data [4]. Sensors are an important part of our lives, ranging from home automation to industrial automation. Common sensors are temperature sensors, humidity sensors and gas sensors. An example is the HDC1080 made by Texas Instruments’ [5]. HDC 1080 is a low power, high accuracy module that contains a digital humidity sensor and a temperature sensor.

The input/output relationship of a sensor can be represented using Fig.1.

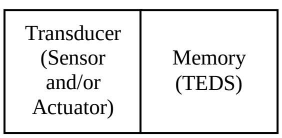
Fig.1 Sensor for measuring physical, biological, or chemical parameters



B. *Smart Sensor and Smart Transducers*

It was interesting to discover that the term "smart transducers" was created long before the concepts of IoT became widespread. The IEEE defined "smart transducers" in 1997 in its standard IEEE 1451 [6]. Transducers include both sensors and actuators. IEEE believed that a simple transducer could just accomplish the operations of measuring or driving something, whereas a smart transducer should also be able to tell people what they are, how to calibrate them, and who made them. Therefore, the IEEE 1451 standard requires that transducers be augmented with a memory device. This memory device stores a Transducer Electronic Data Sheet (TEDS) which contains transducer identification, calibration, correction data and manufacturer-related information. The objective of the IEEE 1451 standard is to allow transducer data to be accessed from wired or wireless computer networks. A smart transducer that meets the requirement of the IEEE 1451 standard is shown Fig.2.

Fig. 2 An IEEE 1451 smart transducer



IV. Smart Objects

A. *What Are Smart Objects*

Kortuem et al [1] defined smart objects as autonomous physical and/or digital objects that have sensing, processing, and networking capabilities, and carry application logic. "They make sense of their local environment and interact with human users. They sense, log, and interpret what's occurring within themselves and the world, act on their own, intercommunicate with each other, and exchange information with people" [1]. Kortuem et al also pointed out that the Internet of Things could be considered to be a loosely coupled and decentralized system of smart objects. Although numerous other researchers had slightly different definitions on smart objects, Kortuem et al's definition seemed to have broad acceptance and has been frequently referenced.

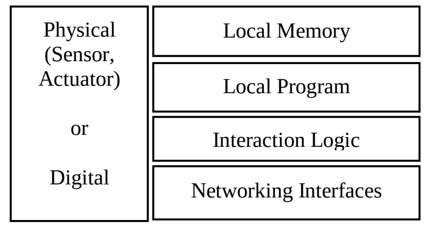
A close look at the Kortuem definition, key smart object attributes can be identified and are summarized in Table 1.

Table 1 Defining attributes of smart objects

- Physical (or virtual);
- With network interface;
- Sensing and actuating capabilities;
- Local data storage;
- Local processing;
- Able to interact with other objects and/or humans

Based on the attributes in Table 1, a smart object can be represented using several compositional elements as indicated in Fig.3.

Fig.3 Compositional elements of a smart object



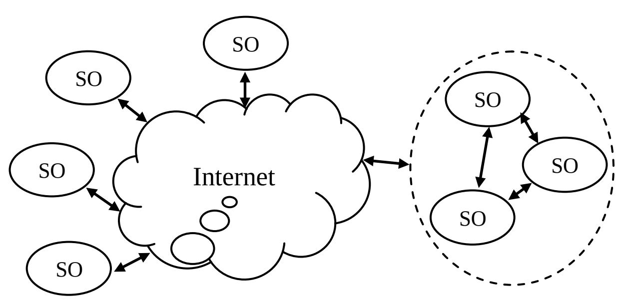
It is now clear that the main differences between the smart sensors (as defined by IEEE 1451) and smart objects are: 1). Smart objects can contain actuators (so a smart object is a smart transducer); 2). Smart objects can be digital; 3). Smart objects can interact with each other and with humans (which the IEEE smart transducers are not able to do).

Although the definition of smart objects sounds that they are hugely powerful, the current common understanding of the IoT community is that smart objects should be "constrained devices" that have constraints on energy, bandwidth, memory, size and cost [7][8].

B. *Internet of Things and Smart Objects*

When smart objects are considered to be building blocks of IoT, an IoT system can be represented using Fig.4.

Fig. 4 Internet of Things as a system of smart objects (SOs)



Smart objects can interact with each other locally through a local network, can form a group to interact with the Internet, and can interact with each other remotely through the Internet "anywhere, anytime".

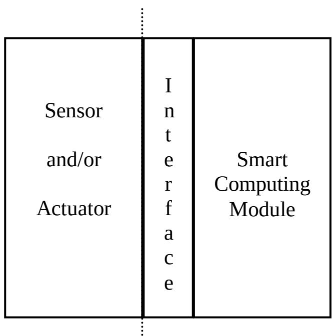
The IoT smart objects can be used to cover the earth, monitor everything, and take control actions whenever necessary. With IoT, the earth is now not only covered by the so called "information highways" as it used to be, but also by the physical entities that are networked and that communicate with each other. For this reason, some people compare IoT as "the skin of the earth", others call IoT "the nervous system of the earth".

V. Detailed Examination of Smart Objects

A. Hardware and Software for Smart Objects

Careful examination of Fig.3 reveals that a smart object can be divided into two modules: a sensor/actuator module and a smart computing module. The smart computing module consists of local memory, local program, interaction logic, and networking interfaces. The two modules are linked with a local interface, as shown in Fig.5.

Fig.5 A smart object depicted as two modules and a local interface



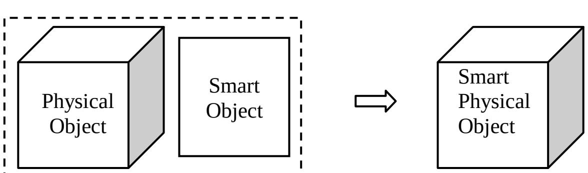
The reason of dividing a smart object into two modules and a local interface is that usually the smart computing module and the local interface can be manufactured on a single integrated circuit (IC) chip. However, it is often difficult to have the sensors and actuators manufactured on the same IC chip because many of them can be large in size, such as electro-magnetic sensors and motors.

The smart computing module is typically implemented as an IC chip with an embedded system that has constrained resources. Application software, and even a tiny operating system can be stored on the chip, together with a networking software stack.

B. Smart Objects as Smartness Enablers

The smart object shown in Fig.5 can be attached to any existing real-life physical object to "empower" that physical object with smartness, as shown in Fig.6.

Fig.6 Smart object as a "smartness" enabler

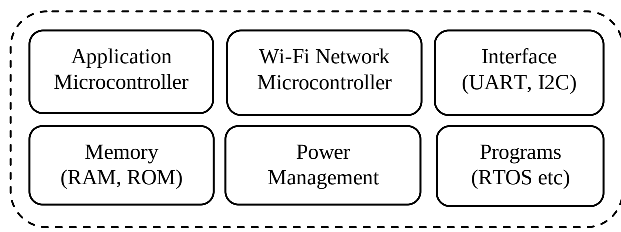


What Fig.6 means is that, a smart object can be attached to an existing physical object to make it a "smart physical object". Based on this rule, a smart object can be added to a door lock to make it a smart lock. Similarly, a smart object can be added to a microwave to make it a "smart microwave".

A similar idea was proposed by Beigl and Gellersen [9] who designed a hardware board named "Smart-It". The Smart-It board is a generic computing device which is envisioned to be able to become as small as a "label" in the future. What this means is that, in the future, people can stick a Smart-It "label" to any existing physical object to get a smart physical object.

Such label-like "smartness enabler" is already available on the market (although the product is not as "flexible" as a label). For example, the Texas Instruments CC3200 IoT chip is well qualified as a smartness enabler, as shown in Fig.7.

Fig.7 Texas Instruments' CC3200 IoT SoC chip (9mm x 9mm)



C. Local Processing in Smart Objects

The Local Program element in a smart object performs a number of tasks locally. Tasks include signal processing - data from sensors have noises which should be filtered out. Other tasks can be local data calibration, local data interpretation and local decision making and local actuation action generation. There can also be a task such as local "health condition" monitoring of the smart physical object, as well as tasks that help smart physical objects adapt to environmental changes.

D. Interfacing Technologies for Smart Objects

The local interface between the smart computing module and the sensor/actuator module inside a smart object is usually wired. Typical wired interfaces are 1). Universal asynchronous receiver/transmitter (UART); 2). General-purpose input/output (GPIO); 3). Analog-to-digital converter (ADC); 4). Digital-to-analog converter (DAC); 5). Inter-integrated circuit (I2C); 6). Integrated interchip sound (I2S).

Although the networking interfaces between smart objects can be wired as well, such as Ethernet, they are usually wireless. Typical between-object wireless technologies include BlueTooth, Wi-Fi, ZigBee, NFC, RFID, and Z-Wave [10].

E. *Advantages of Using Smart Objects*

There are several advantages in designing IoT systems based on smart objects. Energy saving is one of them. Smart objects are usually powered by battery. Communication interfaces between smart objects are usually wireless which consumes the most energy while transmitting data. Limiting most processing local to the objects saves considerable amount of energy. The second advantage is automation. IoT smart objects are autonomous and self-governed. They operate independently and can collaborate with other objects globally.

F. *Challeneges of Using Smart Objects*

There are a number of challenges when building a smart object-based IoT system [11]. Smart objects are often constrained devices and are usually powered by battery. Frequently they are working in real-time mode. These are the main causes of the challenges.

Power is the first challenge, although localizing processing reduces wireless power usage. The use of battery in IoT smart objects demands power efficiency. Efforts should be made to minimize smart object wake-up time and other operations. Incorporating energy harvesting technologies into smart object design should be further investigated.

The second challenge is connectivity. Currently a large number of networking technologies are being employed in connecting physical devices together and to the Internet. Some of these technologies are proprietary. Other technologies are not IP based. Smart object-based IoT demands interoperability. This expects open standards to be used at different communication levels.

Security and privacy is of big concern for smart object based IoT systems. How to build secure smart objects and secure IoT systems are under extensive research [12].

G. *Smart Object Communication Patterns*

Tschofenig et al [8] suggested that four communication patterns exist in IoT smart object communications.

The first one is object-to-object communication which usually occurs when smart objects are connected within the same local network. Objects talk to other objects directly without going through an application server. Currently communication technologies used by smart objects in this pattern are Bluetooth, Z-Wave, ZigBee, and Wi-Fi.

The second pattern is object-to-cloud communication. In this pattern smart objects connect directly to a cloud service in an application service provider. Communication technologies employed in this pattern are Ethernet, Wi-Fi and cellular radios.

The third pattern is object-to-application layer gateway (ALG). In this pattern, smart objects connect to a cloud service through an ALG service. Communication technologies between smart objects and the ALG are Bluetooth, ZigBee and Wi-Fi. Communication technologies between the ALG and the cloud service are IP-based networks.

The last pattern is back-end data sharing. This pattern enables users to analyze smart object data in combination with data from other sources on the application service provider.

VI. EMERGING TECHNOLOGIES FOR IOT ANS SMART OBJECTS

As pointed out previously, smart object based IoT involves a wide range of industries and uses deployment platforms with different embedded technologies and cloud computing technologies. The main challenge is developing efficient communication protocols that will allow constrained devices to communicate with servers via the existing Internet infrastructure. There are already newly proposed protocols at each level of communications.

Table 2 shows a mapping between the set of protocols designed for Internet of Things/Web of Things (IoT/WoT) and their counterpart in existing Internet/Web protocols.

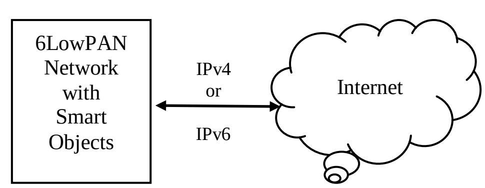
Table 2 Communication Protocols for Smart Objects and IoT

Internet/Web	**IoT/WoT**
XML	*Web Objects*
HTTP	*CoAP*
TLS	*DTLS*
TCP	*UDP*
IPv6	*6LowPAN*

A. *6LowPAN*

Prior to (and also during) the IoT era, extensive research has been carried out on wireless sensor networks (WSN) based on the IEEE 802.15.4 standard. IoT researchers hope that low-power IEEE 802.15.4 small devices be able to work with the Internet Protocol and participate in IoT. A new standard named 6LowPAN was proposed. 6LowPAN stands for "IPv6 over Low-Power Wireless Personal Area Networks". It is an IETF open standard defined in RFC 6282 [13]. Essentially, 6LowPAN defines an adaption layer above the MAC layer that assists numerous non-IP devices to work with IP based networks. 6LowPAN is now used much further beyond assisting IEEE 802.15.4 devices. It is also being adapted for Sub-1 GHz low-power RF, Bluetooth Smart (Bluetooth LE), power line control (PLC) and low-power Wi-Fi. The idea of 6LowPAN is shown in Fig.8.

Fig.8 Connecting low power smart objects to the Internet via 6LowPAN



B. UDP

In networking, TCP/IP has connection states and is suitable for applications requiring delivery reliability. The price for the benefit is high overhead and delay time. Therefore, TCP/IP is not suitable for real-time and deterministic applications.

On the contrary, UPD does not possess the overhead [14]. UDP packets can be sent right after the underlying physical devices have generated them without delay. This leads to reduced local memory use, less network traffic, and improved response time. Therefore, UDP is preferred for IoT smart object communications.

C. DTLS

The DTLS (Datagram Transport Layer Security) protocol provides communications privacy for datagram protocols [15]. DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides end-to-end security guarantees. Secure CoAP (see next section below) mandates DTLS to be used for authenticated and confidential communication.

D. CoAP

CoAP [16] stands for Constrained Application Protocol. It was designed for resource-constrained devices to be used in IoT and is for communications at the application layer. It runs over the UDP protocol. CoAP provides a REST (Representational State Transfer) interface similar to HTTP. Resources are available via Universal Resource Identifiers (URIs).

E. The Web of Things (WoT)

The WoT is an application layer technology that uses web technologies to enable communications between smart objects. It hides the physical and transport layer protocols used by smart objects. In WoT, objects are represented as resources that can be interacted with REST-style communications. Smart physical devices made by different manufacturers can have the standard Web API and can be integrated come out of the box.

VII. Conclusions

This paper has reviewed research on sensors, smart sensors, smart objects, and IoT. Efforts have been made to clarify the concepts and their relationships in the "IoT family". In addition, the paper has reviewed the emerging technologies that are needed to build smart objects and the Internet of Things.

References

[1] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart Objects as Building Blocks for the Internet of Things", IEEE Internet Computing, vol.14, No.01, pp: 44-51, 2010.

[2] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, "Architectural Considerations in Smart Object Networking", Request for Comments: 7452, Internet Architecture Board (IAB), March 2015.

[3] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)", IEEE Internet of Things Initiative, May 27, 2015. DOI=http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. Accessed August 13, 2016.

[4] NIST, "What is a sensor?", Definitions – Sensors, http://www.nist.gov/el/isd/ieee/definitions.cfm. Accessed August 13, 2016.

[5] Texas Instruments, "HDC1080 Low Power, High Accuracy Digital Humidity Sensor with Temperature Sensor", DOI=http://www.ti.com/product/HDC1080. Accessed September 3, 2016.

[6] IEEE, The IEEE 1451.4 Standard for Smart Transducers, https://standards.ieee.org/develop/regauth/tut/1451d4.pdf. 1997. Accessed August 13, 2016.

[7] H. Tschofenig and J. Arkko, Internet Architecture Board (IAB), "Report from the Smart Object Workshop", Request for Comments 6574, April 2012.

[8] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, "Architectural Considerations in Smart Object Networking", Internet Architecture Board (IAB), Request for Comments 7452, March 2015.

[9] M. Beigl and H. Gellersen, "Smart-Its: An Embedded Platform for Smart Objects", Smart Objects Conference (sOc). Vol. 2003. 2003.

[10] D. Kovacs, "Communication Technologies for Smart Objects", Ubiquitous Computing Seminar FS2014, Student report, ETH Zurich, 2014.

[11] Texas Instruments, "Challenges in the Internet of Things", http://www.ti.com/ww/en/internet_of_things/iot-challenges.html. Accessed Sept. 3, 2016.

[12] A. Skarmeta, J. L. Hernández-Ramos, J. B. Bernabe, "A required security and privacy framework for smart objects", ITU Kaleidoscope conference, Barcelona, Spain, 9-11 December 2015.

[13] J. Olsson, "6LoWPAN demystified", Texas Instruments, Oct. 2014, DOI=http://www.ti.com/lit/wp/swry013/swry013.pdf. Accessed Sept. 1, 2016.

[14] B. Cole, "UDP and the embedded wireless Internet of Things", www.embedded.com, Oct. 11, 2011. DOI= http://www.embedded.com/electronics-blogs/cole-bin/4229531/UDP---the-embedded-wireless--Internet-of-Things-#. Accssessd Sept.1, 2016.

[15] M. Petit-Huguenin, G. Salgueiro, August 2014, "Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN)", Internet Engineering Task Force (IETF), Request for Comments: 7350, August 2014.

[16] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)", Request for Comments: 7252, Internet Engineering Task Force (IETF), June 2014.

[17] K. Kajimoto, R. Matsukura, J. Hund, M. Kovatsch, and K. Nimura, "Web of Things (WoT) Architecture", Unofficial Draft 02 September 2016, W3C, 2016.

[18] D. Raggett, "The Web of Things", DOI= https://www.w3.org/2015/07/15-dsr-wot.pdf. Accssessd Sept.1, 2016.

[19] D. Raggett, "BUILDING THE WEB OF THINGS", https://www.w3.org/blog/2015/05/building-the-web-of-things/, 24 May 2015. Accssessd Sept.4, 2016.

[20] D. Guinard, "Web of Things vs Internet of Things: 1/2", http://webofthings.org/2016/01/23/wot-vs-iot-12/, January 23, 2016.

[21] List of automation protocols, https://en.wikipedia.org/wiki/List_of_automation_protocols. Accessed September 4, 2016.

[22] W3C, "Web of Things at W3C", DOI= https://www.w3.org/WoT/. Accessed August 13, 2016.