The Internet of Things

The Internet of Things

Connecting Objects to the Web

Edited by
Hakima Chaouchi

ISTE

WILEY

First published 2010 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd 2010

The rights of Hakima Chaouchi to be identified as the author of this work have been asserted by her in accordance with the Copyright, Designs and Patents Act 1988.

Library of Congress Cataloging-in-Publication Data

The Internet of things : connecting objects to the web / edited by Hakima Chaouchi.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-84821-140-7
1. Ubiquitous computing. 2. Computer networks. 3. Radio frequency identification systems. I. Chaouchi, Hakima.
QA76.5915.I67 2010
004--dc22

2010003706

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-140-7

Printed and bound in Great Britain by CPI Antony Rowe, Chippenham and Eastbourne.

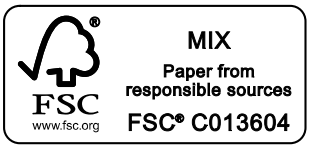

Table of Contents

Preface xi

Chapter 1. Introduction to the Internet of Things 1
Hakima CHAOUCHI

1.1. Introduction 1
1.2. History of IoT 3
1.3. About objects/things in the IoT 7
1.4. The identifier in the IoT 9
1.5. Enabling technologies of IoT 13
1.5.1. Identification technology 15
1.5.2. Sensing and actuating technology 17
1.5.3. Other technologies 18
1.5.4. Connected objects' communication 19
1.6. About the Internet in IoT 21
1.7. Bibliography 32

Chapter 2. Radio Frequency Identification Technology Overview 35
Ayyangar Ranganath HARISH

2.1. Introduction 35
2.2. Principle of RFID 36
2.3. Components of an RFID system 41
2.3.1. Reader 41
2.3.2. RFID tag 44
2.3.3. RFID middleware 45

2.4. Issues 48
2.5. Bibliography 52

Chapter 3. Wireless Sensor Networks: Technology Overview 53
Thomas WATTEYNE and Kristofer S.J. PISTER

3.1. History and context. 53
3.1.1. From smart dust to smart plants 54
3.1.2. Application requirements in modern WSNs. 55
3.2. The node 60
3.2.1. Communication 60
3.2.2. Computation 63
3.2.3. Sensing 63
3.2.4. Energy 64
3.3. Connecting nodes 64
3.3.1. Radio basics. 64
3.3.2. Common misconceptions 66
3.3.3. Reliable communication in practice: channel hopping. 67
3.4. Networking nodes 70
3.4.1. Medium access control 71
3.4.2. Multi-hop routing 80
3.5. Securing communication 88
3.6. Standards and Fora 89
3.7. Conclusion 91
3.8. Bibliography 91

Chapter 4. Power Line Communication Technology Overview 97
Xavier CARCELLE and Thomas BOURGEAU

4.1. Introduction 97
4.2. Overview of existing PLC technologies and standards . . 98
4.2.1. History of PLC technologies 99
4.2.2. Different types of in-home PLC technologies. 100
4.2.3. Security 109
4.2.4. Performances of PLC technologies 110
4.2.5. Standards and normalization 112
4.3. Architectures for home network applications 114
4.3.1. Architecture for a high bit-rate home network application 115

4.3.2. Architecture for low bit-rate home network application . . . 117
4.4. Internet of things using PLC technology . . . 120
4.4.1. Connecting objects in the indoor environment . . . 121
4.4.2. Interoperability of connecting objects in the home environment . . . 124
4.5. Conclusion . . . 127
4.6. Bibliography . . . 127

Chapter 5. RFID Applications and Related Research Issues . . . 129
Oscar BOTERO and Hakima CHAOUCHI

5.1. Introduction . . . 129
5.2. Concepts and terminology . . . 129
5.2.1. Radio-frequency identification . . . 130
5.2.2. Transponder (tag) classes . . . 132
5.2.3. Standards . . . 134
5.2.4. RFID system architecture . . . 136
5.2.5. Other related technologies . . . 138
5.3. RFID applications . . . 139
5.3.1. Logistics and supply chain . . . 139
5.3.2. Production, monitoring and maintenance . . . 140
5.3.3. Product safety, quality and information . . . 141
5.3.4. Access control and tracking and tracing of individuals . . . 142
5.3.5. Loyalty, membership and payment . . . 143
5.3.6. Household . . . 143
5.3.7. Other applications . . . 144
5.4. Ongoing research projects . . . 144
5.4.1. Hardware issues . . . 145
5.4.2. Protocols . . . 146
5.5. Summary and conclusions . . . 152
5.6. Bibliography . . . 153

Chapter 6. RFID Deployment for Location and Mobility Management on the Internet . . . 157
Apostolia PAPAPOSTOLOU and Hakima CHAOUCHI

6.1. Introduction . . . 157
6.2. Background and related work . . . 159

6.2.1. Localization 159
6.2.2. Mobility management. 164
6.3. Localization and handover management relying on RFID 169
6.3.1. A technology overview of RFID 169
6.3.2. How RFID can help localization and mobility management 170
6.3.3. Conceptual framework 172
6.4. Technology considerations 176
6.4.1. Path loss model. 176
6.4.2. Antenna radiation pattern 177
6.4.3. Multiple tags-to-reader collisions 177
6.4.4. Multiple readers-to-tag collisions 178
6.4.5. Reader-to-reader interference 179
6.4.6. Interference from specific materials. 181
6.5. Performance evaluation 181
6.5.1. Simulation setup 181
6.5.2. Performance results 183
6.6. Summary and conclusions 187
6.7. Bibliography 188

Chapter 7. The Internet of Things – Setting the Standards . . 191
Keith MAINWARING and Lara SRIVASTAVA

7.1. Introduction 191
7.2. Standardizing the IoT 193
7.2.1. Why standardize? 193
7.2.2 What needs to be standardized?. 194
7.3. Exploiting the potential of RFID 196
7.3.1. Technical specifications 196
7.3.2. Radio spectrum and electromagnetic compatibility . . 201
7.4. Identification in the IoT 202
7.4.1. A variety of data formats. 203
7.4.2. Locating every thing: IPv6 addresses 208
7.4.3. Separating identifiers and locators in IP: the HIP . . . 210
7.4.4. Beyond the tag: multimedia information access 211
7.5. Promoting ubiquitous networking: any where, any when, any what 212
7.5.1. Wireless sensor networks 213
7.5.2. Networking the home 215
7.5.3. Next generation networks 216
7.6. Safeguarding data and consumer privacy 217

7.7. Conclusions 220
7.8. Bibliography 220

Chapter 8. Governance of the Internet of Things 223
Rolf H. WEBER

8.1. Introduction 223
8.1.1. Notion of governance 223
8.1.2. Aspects of governance 224
8.2. Bodies subject to governing principles 225
8.2.1. Overview 225
8.2.2. Private organizations 226
8.2.3. International regulator and supervisor 229
8.3. Substantive principles for IoT governance 233
8.3.1. Legitimacy and inclusion of stakeholders 233
8.3.2. Transparency 234
8.3.3. Accountability 236
8.4. IoT infrastructure governance 239
8.4.1. Robustness 239
8.4.2. Availability 240
8.4.3. Reliability 241
8.4.4. Interoperability 242
8.4.5. Access 244
8.5. Further governance issues 246
8.5.1. Practical implications 246
8.5.2. Legal implications 247
8.6. Outlook 248
8.7. Bibliography 248

Conclusion 251

List of Authors 261

Index 263

Preface

Services designed over the Internet evolved depending on the needs identified from person-to-person interaction, such as email or phone services to meet other interactions, such as person-to-machine, machine-to-person and, lately, machine-to-machine where no human interaction is needed; thus building ubiquitous and pervasive computing. Such a computing system started a long time ago with the ambition of offering all-pervading computing to automate tasks and build a smart world. Introducing radio-frequency identification (RFID) technology in building new services over the network has pushed what is called the “Internet of Things” (IoT) as a meeting point between the real world and the virtual world, especially when combined with other technologies, such as sensor technology or mobile communication.

IoT appears to be one step further on the path to ubiquitous computing. This is possible with the introduction of RFID or sensor technologies, but also other technologies such as robotics, nanotechnology and others. These technologies make the Internet of things services an interdisciplinary field where most of the human senses are somehow reproduced and replaced in the virtual world.

So, what is meant by the Internet of things? From the economical point of view, it is about designing new services and generating new revenue streams in the communication value chain. This is not straightforward however, as lots of technical issues have been raised that need to be solved before an effective deployment of the new

envisioned services. From the technical point of view, it is about connecting new devices, called objects or things, and investigating the issues related to connecting these objects with the network in order to develop exploitable applications. To tackle these issues, it is important to understand what the Internet and things mean in the IoT, knowing that, depending on the research community, the meaning and the related issues might be different.

A thing or an object in the IoT is described as any item from our daily life that is enhanced with some computing and/or communication capabilities. For instance, items or objects with RFID or sensor technologies will become connected objects. These objects, depending on the application, might range from a size as small as an atom or as large as a building; they might be fixed or mobile, such as a car; they might be inanimate or animate, such as animals or humans. These objects joining an IoT service will have an electronic identification, such as an RFID. Objects or things are also new electronic devices interacting with the real-world environment, such as sensors.

Conventional communicating devices, such as laptops, computers and phones might be considered to be objects. In our book, we exclude these classical devices from the object list since they do not directly enable interaction with the real-world environment. Other objects, such as consumer electronic products like a TV or a fridge have already been introduced in the communication chain via other technologies, such as power line communication technology. IoT will clearly have to allow the connectivity of a large number and different types of objects. This means that it has to face the heterogenity and scalability of the communication framework in order to build the envisioned applications. These applications will orchestrate the real environment-related new functionalities of identifying, locating, sensing and acting, thus building the task automation and environmental task monitoring expected by the IoT.

Currently RFID technology and sensor technology are promising, very close-to-market applications, since they offer the new functionalities of identifying and sensing, respectively. Sensor

technology and sensor networks for phenomenon monitoring have interested the telecommunication research community earlier than RFID technology, which evolved in the retail product chain for product tracking and only recently joined the telecommunication value chain. Some recent examples show the development of RFID-based systems to help vision-impaired people to be guided on buses and enhance museum visits with smart phones and RFID. Combining RFID, sensor, and mobile communications appears to be very promising and will enable more applications to contribute in building the IoT. Although already used, these technologies need to be improved from security, privacy, performance and scalability points of view.

On the other hand, the Internet in the IoT might also have different interpretations. The obvious interpretation, which is more direct, refers to the current Internet adapted to these new objects' connectivity needs. Current Internet is that of connected nodes using a TCP/IP (the internet protocol suite) protocol stack with IP addressing and routing capabilities. Usually, the Internet model runs a TCP/IP stack in the connected device or offers the possibility of designing corresponding gateways to specific nodes or networks.

Connecting objects to the current Internet involves adapting the TCP/IP stack to the resources of the objects. This is what is proposed by the Internet Engineering Task Force with the 6LoWPLAN protocol stack for sensor networks. It also means designing gateways connecting the objects to the Internet, as might be done with connecting RFID objects to the Internet via gateways.

Another view of the IoT involves designing a new communication model, different from TCP/IP. This would be a new Internet, also called future Internet, where it is possible to adapt the communication model to the context, traffic constraints, resource limitations and so on. Note that designing the network of the future (or future Internet) is one of the major research goals of the current networking research community, where better network adaptation than the current Internet is expected.

In the long run, the IoT appears to be one of the leading paths to this goal since it challenges the current Internet model with new needs of object connectivity: such as identification, naming and addressing, scalability, heterogenity, resource limitation, new traffic modeling, etc.

While waiting for the future Internet, the current Internet operators show a great interest in the concretization of unlimited IoT services. They are welcoming any new and attractive internet services generating new traffic to be transported by the Internet or all-IP network that already offers one network model for multiservice support, such as voice, data and multimedia services.

Designing services involving real-world things' and objects' interaction and communication through the Internet is therefore highly encouraged under the condition of solving all the related issues of security and privacy and of connecting billions of objects to the Internet directly or through gateways. These gateways can be simple or intelligent gateways, capable of interpreting the traffic needs at the entrance of the network.

The current objects' resources such as memory, processing and battery in tiny objects are very limited and cannot run the current Internet communication model which means that these objects will use an adapted version of the Internet model, a proprietary communication system that will be seen as a heterogenous one from the Internet, and thus needs a gateway to benefit from the forwarding of traffic.

Of course, the traffic that will be generated by these object-based applications will have different expectations from the network. In fact, until now voice was considered the most difficult object to transport since it was used over a circuit-switched forwarding system designed to match its expectation. Now the traffic generated by these specific IoT applications will have to be modeled and need to be satisfied, probably partially by the current Internet and totally by the future Internet. For instance, if an "*actuate*" is ordered remotely via the network, the traffic priority should match the emergency of this

action. Also the packet size should be adapted to this new type of information. Similarly to the voice application, with the IoT-generated traffic, the packet design and priority of the packets will have to be specified to match the traffic requirement.

It is clear that plenty of technical, research, economic and societal issues are correlated with the IoT. In this book *The Internet of Things*, we have tried to bring together the up-to-date knowledge associated with what a connected object means, what Internet means in the IoT, and what the technical challenges (see Chapter 1) are with a more network-related view.

The book, also describes what the enabling technologies of the IoT are; the closest to the market are described in detail. These are mainly RFID (Chapter 2) for identifying and tracking the objects, and sensors (Chapter 3) for sensing the environment and actuating. Both RFID and sensor technologies use wireless connectivity.

This book additionally describes power line communication technology (Chapter 4) used for home networking. This applies the idea of building smart homes by connecting smart objects at home, such as a fridge and TV. This idea emerged before we started to use the IoT terminology, which was pushed more with RFID-connecting objects. Services developed in home networking are also part of the IoT services, but do not have the same connectivity issues as RFID or sensors, which are tiny devices with limited resources, mainly battery power.

This book, discusses the applications and research issues related to RFID (Chapter 5). It also proposes to look at other RFID technology usage in improving some network-related functionalities, such as location and mobility (Chapter 6). Finally, setting the standards and the governance of the IoT is discussed in Chapters 7 and 8.

We are not ignoring other issues related to the IoT, such as the need for high-performance computing to face scalability, the need for even faster processing and the limits of component physics in increasing the speed of processors, to face the expected billion

connected objects generating traffic in the network. Moreover, research disciplines will have to work and interact with the networking community to build ubiquitous computing and design the IoT services and networking.

Hakima CHAOUCHI

April 2010