SIMONE CIRANI | GIANLUIGI FERRARI
MARCO PICONE | LUCA VELTRI

INTERNET *of* THINGS

ARCHITECTURES, PROTOCOLS AND STANDARDS

WILEY

Internet of Things

Internet of Things

Architectures, Protocols and Standards

Simone Cirani
Caligoo Inc., Chicago, IL, USA

Gianluigi Ferrari
Department of Engineering and Architecture
University of Parma, Parma (PR), Italy

Marco Picone
Caligoo Inc., Chicago, IL, USA

Luca Veltri
Department of Engineering and Architecture
University of Parma, Parma (PR), Italy

WILEY

This edition first published 2019

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office
The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Cirani, Simone, 1982- author. | Ferrari, Gianluigi, 1974- author. | Picone, Marco, 1984- author. | Veltri, Luca, author.
Title: Internet of things : architectures, protocols and standards / Simone Cirani, Taneto, Gattatico (RE), Italy, Ph.D., Gianluigi Ferrari, Ph.D., Marco Picone, Gattatico (RE), Italy Ph.D., Luca Veltri, Ph.D., Parma (PR), Italy.
Description: First edition. | Hoboken, NJ : Wiley, 2019. |
Identifiers: LCCN 2018021870 (print) | LCCN 2018028978 (ebook) | ISBN 9781119359685 (Adobe PDF) | ISBN 9781119359708 (ePub) | ISBN 9781119359678 (hardcover)
Subjects: LCSH: Internet of things.
Classification: LCC TK5105.8857 (ebook) | LCC TK5105.8857 .C55 2019 (print) | DDC 004.67/8–dc23
LC record available at https://lccn.loc.gov/2018021870

Cover design by Wiley
Cover image: © shulz/iStockphoto

Set in 10/12pt WarnockPro by SPi Global, Chennai, India

10 9 8 7 6 5 4 3 2 1

"Machines take me by surprise with great frequency."
(Alan Mathison Turing)

I would like to dedicate this work: To Paola, the love of my life, my hero, my strength. You are what I live for. To my wonderful mom and dad. You have always supported me. You gave me everything. You taught me the value of work and commitment. You gifted me with your love. You are always in my heart and thoughts. To my fantastic sisters, who have always been an example. You believed in me and blessed me with your love, joy, and laughs. To my grandma, you will always have a special place in my heart. You are an incredible inspiration. I miss you. To Jonas, who has taught me the passion for knowledge, exploration, and science. To Emil and Emma, I wish you all the best. I am proud of you. I will never say thanks enough. I love you all. Thanks to Marco, Gianluigi, and Luca, I am really proud and honored to have worked and researched with you. I am so proud of what we have achieved in these years. Finally, thanks to all my colleagues, old and new, who contributed to make this book happen in one way or another.
Simone Cirani

To the women of my life, Anna, Sofia, and Viola: You fill my heart and brighten my days.
Gianluigi Ferrari

To Eleonora and my parents, Antonio and Marina, who are always by my side in every choice and decision. A special thanks to all the people who worked with us, supported our vision, and shared the challenges during these years.
Marco Picone

To my family.
Luca Veltri

Contents

Preface *xv*

1 Preliminaries, Motivation, and Related Work *1*
1.1 What is the Internet of Things? *1*
1.2 Wireless Ad-hoc and Sensor Networks: The Ancestors without IP *2*
1.3 IoT-enabled Applications *3*
1.3.1 Home and Building Automation *3*
1.3.2 Smart Cities *4*
1.3.3 Smart Grids *4*
1.3.4 Industrial IoT *5*
1.3.5 Smart Farming *7*

2 Standards *9*
2.1 "Traditional" Internet Review *9*
2.1.1 Physical/Link Layer *10*
2.1.1.1 IEEE 802.3 (Ethernet) *11*
2.1.1.2 IEEE 802.11 *12*
2.1.2 Network Layer *14*
2.1.2.1 IPv6 and IPv4 *14*
2.1.3 Transport Layer *17*
2.1.3.1 TCP and UDP *19*
2.1.4 Application Layer *21*
2.1.4.1 HTTP *21*
2.1.4.2 AMQP *22*
2.1.4.3 SIP *23*
2.2 The Internet of Things *25*

2.2.1 Designing the Architecture of an IP-based Internet of Things *26*
2.2.2 Physical/Link Layer *28*
2.2.2.1 IEEE 802.15.4 and ZigBee *28*
2.2.2.2 Low-power Wi-Fi *30*
2.2.2.3 Bluetooth and BLE *31*
2.2.2.4 Powerline Communications *32*
2.2.3 Network Layer *33*
2.2.3.1 The 6LoWPAN Adaptation Layer *34*
2.2.4 Transport Layer *34*
2.2.5 Application Layer *34*
2.2.5.1 CoAP *35*
2.2.5.2 CoSIP Protocol Specification *60*
2.3 The Industrial IoT *76*

3 Interoperability *79*
3.1 Applications in the IoT *79*
3.2 The Verticals: Cloud-based Solutions *80*
3.3 REST Architectures: The Web of Things *81*
3.3.1 REST: The Web as a Platform *82*
3.3.1.1 Resource-oriented Architectures *83*
3.3.1.2 REST Architectures *84*
3.3.1.3 Representation of Resources *84*
3.3.1.4 Resource Identifiers *85*
3.3.1.5 Statelessness *86*
3.3.1.6 Applications as Finite-state Machines *86*
3.3.1.7 Hypermedia as the Engine of Application State *86*
3.3.2 Richardson Maturity Model *88*
3.3.2.1 Level 0: the Swamp of POX *88*
3.3.2.2 Level 1: Resources *90*
3.3.2.3 Level 2: HTTP Verbs *90*
3.3.2.4 Level 3: Hypermedia *95*
3.3.2.5 The Meaning of the Levels *97*
3.4 The Web of Things *97*
3.5 Messaging Queues and Publish/Subscribe Communications *98*
3.5.1 Advantages of the Pub/Sub Model *99*
3.5.2 Disadvantages of the Pub/Sub Model *100*
3.5.3 Message Queue Telemetry Transport *100*
3.5.3.1 MQTT versus AMQP *101*

3.6 Session Initiation for the IoT *102*
3.6.1 Motivations *102*
3.6.2 Lightweight Sessions in the IoT *104*
3.6.2.1 A Protocol for Constrained Session Initiation *106*
3.6.2.2 Session Initiation *106*
3.6.2.3 Session Tear-down *108*
3.6.2.4 Session Modification *108*
3.7 Performance Evaluation *109*
3.7.1 Implementation *109*
3.7.2 Experimental Results *111*
3.7.3 Conclusions *114*
3.8 Optimized Communications: the Dual-network Management Protocol *115*
3.8.1 DNMP Motivations *115*
3.8.2 Related Work *117*
3.8.3 The DNMP Protocol *118*
3.8.4 Implementation with IEEE 802.15.4 and IEEE 802.11s *123*
3.8.4.1 LPLT Networking *123*
3.8.4.2 HPHT Networking *123*
3.8.4.3 Node Integration *124*
3.8.5 Performance Evaluation *125*
3.8.5.1 Experimental Setup *125*
3.8.5.2 Operational Limitations of IEEE 802.15.4 *126*
3.8.6 IEEE 802.15.4-controlled Selective Activation of the IEEE 802.11s Network *129*
3.8.7 Conclusions *130*
3.9 Discoverability in Constrained Environments *131*
3.9.1 CoRE Link Format *131*
3.9.1.1 CoRE Link Format: Discovery *132*
3.9.1.2 Link Format *133*
3.9.1.3 The Interface Description Attribute *135*
3.9.2 CoRE Interfaces *135*
3.9.2.1 Sensor *136*
3.9.2.2 Parameter *137*
3.9.2.3 Read-only Parameter *137*
3.9.2.4 Actuator *137*
3.10 Data Formats: Media Types for Sensor Markup Language *138*
3.10.1 JSON Representations *141*
3.10.1.1 Single Datapoint *141*

3.10.1.2 Multiple Datapoints *142*
3.10.1.3 Multiple Measurements *142*

4 Discoverability *145*
4.1 Service and Resource Discovery *145*
4.2 Local and Large-scale Service Discovery *146*
4.2.1 ZeroConf *151*
4.2.2 UPnP *152*
4.2.3 URI Beacons and the Physical Web *152*
4.3 Scalable and Self-configuring Architecture for Service Discovery in the IoT *154*
4.3.1 IoT Gateway *156*
4.3.1.1 Proxy Functionality *156*
4.3.1.2 Service and Resource Discovery *158*
4.3.2 A P2P-based Large-scale Service Discovery Architecture *159*
4.3.2.1 Distributed Location Service *160*
4.3.2.2 Distributed Geographic Table *161*
4.3.2.3 An Architecture for Large-scale Service Discovery based on Peer-to-peer Technologies *162*
4.3.3 Zeroconf-based Local Service Discovery for Constrained Environments *167*
4.3.3.1 Architecture *167*
4.3.3.2 Service Discovery Protocol *168*
4.3.4 Implementation Results *170*
4.3.4.1 Local Service Discovery *171*
4.3.4.2 Large-scale Service Discovery *175*
4.4 Lightweight Service Discovery in Low-power IoT Networks *178*
4.4.1 Efficient Forwarding Protocol for Service Discovery *180*
4.4.1.1 Multicast through Local Filtered Flooding *181*
4.4.2 Efficient Multiple Unicast Forwarding *183*
4.5 Implementation Results *185*

5 Security and Privacy in the IoT *191*
5.1 Security Issues in the IoT *192*
5.2 Security Mechanisms Overview *196*
5.2.1 Traditional vs Lightweight security *196*
5.2.1.1 Network Layer *197*
5.2.1.2 Transport Layer *199*

5.2.1.3 Application Layer *201*
5.2.2 Lightweight Cryptography *202*
5.2.2.1 Symmetric-key LWC Algorithms *203*
5.2.2.2 Public-key (Asymmetric) LWC Algorithms *206*
5.2.2.3 Lightweight Cryptographic Hash Functions *210*
5.2.2.4 Homomorphic Encryption Schemes *213*
5.2.3 Key Agreement, Distribution, and Security Bootstrapping *214*
5.2.3.1 Key Agreement Protocols *215*
5.2.3.2 Shared Group-key Distribution *215*
5.2.3.3 Security Bootstrapping *216*
5.2.4 Processing Data in the Encrypted Domain: Secure Data Aggregation *217*
5.2.5 Authorization Mechanisms for Secure IoT Services *219*
5.3 Privacy Issues in the IoT *222*
5.3.1 The Role of Authorization *222*
5.3.2 IoT-OAS: Delegation-based Authorization for the Internet of Things *227*
5.3.2.1 Architecture *227*
5.3.2.2 Granting Access Tokens *229*
5.3.2.3 Authorizing Requests *231*
5.3.2.4 SP-to-IoT-OAS Communication: Protocol Details *231*
5.3.2.5 Configuration *232*
5.3.3 IoT-OAS Application Scenarios *232*
5.3.3.1 Network Broker Communication *233*
5.3.3.2 Gateway-based Communication *235*
5.3.3.3 End-to-End CoAP Communication *235*
5.3.3.4 Hybrid Gateway-based Communication *235*

6 Cloud and Fog Computing for the IoT *237*
6.1 Cloud Computing *237*
6.2 Big Data Processing Pattern *238*
6.3 Big Stream *239*
6.3.1 Big-stream-oriented Architecture *243*
6.3.2 Graph-based Processing *247*
6.3.3 Implementation *251*
6.3.3.1 Acquisition Module *251*
6.3.3.2 Normalization Module *253*
6.3.3.3 Graph Framework *254*
6.3.3.4 Application Register Module *255*

6.3.4 Performance Evaluation *257*
6.3.5 Solutions and Security Considerations *262*
6.4 Big Stream and Security *263*
6.4.1 Graph-based Cloud System Security *266*
6.4.2 Normalization after a Secure Stream Acquisition with OFS Module *268*
6.4.3 Enhancing the Application Register with the IGS Module *269*
6.4.4 Securing Streams inside Graph Nodes *273*
6.4.5 Evaluation of a Secure Big Stream Architecture *277*
6.5 Fog Computing and the IoT *281*
6.6 The Role of the IoT Hub *283*
6.6.1 Virtualization and Replication *285*
6.6.1.1 The IoT Hub *285*
6.6.1.2 Operational Scenarios *287*
6.6.1.3 Synchronization Protocol *290*

7 The IoT in Practice *303*
7.1 Hardware for the IoT *303*
7.1.1 Classes of Constrained Devices *305*
7.1.2 Hardware Platforms *307*
7.1.2.1 TelosB *307*
7.1.2.2 Zolertia Z1 *307*
7.1.2.3 OpenMote *310*
7.1.2.4 Arduino *313*
7.1.2.5 Intel Galileo *315*
7.1.2.6 Raspberry Pi *318*
7.2 Software for the IoT *321*
7.2.1 OpenWSN *321*
7.2.2 TinyOS *322*
7.2.3 FreeRTOS *323*
7.2.4 TI-RTOS *323*
7.2.5 RIOT *324*
7.2.6 Contiki OS *325*
7.2.6.1 Networking *325*
7.2.6.2 Low-power Operation *326*
7.2.6.3 Simulation *326*
7.2.6.4 Programming Model *327*
7.2.6.5 Features *328*

7.3 Vision and Architecture of a Testbed for the Web of Things *328*
7.3.1 An All-IP-based Infrastructure for Smart Objects *330*
7.3.2 Enabling Interactions with Smart Objects through the IoT Hub *332*
7.3.2.1 Integration Challenges *334*
7.3.3 Testbed Access and Security *335*
7.3.3.1 The Role of Authorization *335*
7.3.4 Exploiting the Testbed: WoT Applications for Mobile and Wearable Devices *336*
7.3.5 Open Challenges and Future Vision *338*
7.4 Wearable Computing for the IoT: Interaction Patterns with Smart Objects in RESTful Environments *340*
7.4.1 Shaping the Internet of Things in a Mobile-Centric World *340*
7.4.2 Interaction Patterns with Smart Objects through Wearable Devices *342*
7.4.2.1 Smart Object Communication Principles *342*
7.4.2.2 Interaction Patterns *343*
7.4.3 Implementation in a Real-world IoT Testbed *345*
7.4.3.1 Future Vision: towards the Tactile Internet *348*
7.5 Effective Authorization for the Web of Things *349*
7.5.1 Authorization Framework Architecture *353*
7.5.1.1 System Operations *353*
7.5.2 Implementation and Validation *357*

Reference *359*

Index *381*

Preface

The Internet of Things or, as commonly referred to and now universally used, IoT has two keywords: things and Internet. The very idea of IoT consists allowing things to connect to the (existing) Internet, thus allowing the generation of information and, on the reverse, the interaction of the virtual world with the physical world. This book does not attempt to be an exhaustive treaty on the subject of IoT. Rather, it tries to present a broad view of the IoT based on the joint research activity at the University of Parma, mainly in the years between 2012 and 2015 (when all the authors were affiliated with the same Department of Information Engineering), especially in the context of the EU FP7 project CALIPSO (Connect All IP-based Smart Objects!, 2012–2014). In particular, we present, in a coherent way, new ideas we had the opportunity to explore in the IoT ecosystem, trying to encompass the presence of heterogeneous communication technologies through unifying concepts such as interoperability, discoverability, security, and privacy. On the way, we also touch upon cloud and fog computing (two concepts interwoven with IoT) and conclude with a practical view on IoT (with focus on the physical devices). The intended audience of the book is academic and industrial professionals, with good technical skills in networking technologies. To ease reading, we have tried to provide intuition behind all presented concepts.

The contents of the book flow from a preliminary overview on the Internet and the IoT, with details on "classical" protocols, to more technical details. The synopsis of the book can be summarized as follows: The *first chapter* introduces IoT in general terms and illustrates a few IoT-enabled applications, from home/building automation to smart farming. The *second chapter* contains an overview of relevant standards (e.g. Constrained Application Protocol, CoAP), presented

according to the protocol layers and parallelizing the "traditional" Internet and the IoT, with a final outlook on industrial IoT. *Chapter three* focuses on interoperability, a key concept for IoT, highlighting relevant aspects (e.g. Representational State Transfer (REST) architectures and Web of Things) and presenting illustrative applications (e.g. the Dual-network Management Protocol (DNMP) allowing the interaction of IEEE 802.11s and IEEE 802.15.4 networks). At the end of Chapter three, we preliminarily also discuss discoverability in constrained environments (with reference to the CoRE Link Format); this paves the way to *Chapter four*, which dives into the concept of discoverability (both in terms of service and resource discovery), presenting a few of our research results in this area. *Chapter five* is dedicated to security and privacy in the IoT, discussing proper mechanisms for IoT in a comparative way with respect to common mechanisms for classical Internet. In *Chapter six*, we consider cloud and fog computing, discussing concepts such as big stream processing (relevant for cloud-based applications) and the IoT Hub (relevant for fog-based applications). Finally, *Chapter seven* is an overview of hands-on issues, presenting relevant hardware devices and discussing a Web-of-Things-oriented vision for a test bed implementation.

We remark that the specific IoT protocols, algorithms, and architectures considered in this book are "representative," as opposed to "universal." In other words, we set to write this book mainly to provide the reader with our vision on IoT. Our hope is that this book will be interpreted as a starting point and a useful comparative reference for those interested in the continuously evolving subject of the IoT.

It is our pleasure to thank all the collaborators and students who were with us during the years of research that have led to this book, collaborating with the Wireless Adhoc and Sensor Networks (WASN) Lab of Department of Information Engineering of the University of Parma, which has lately been "rebranded," owing to this intense research activity, as the IoT Lab at the Department of Engineering and Architecture. We particularly thank, for fundamental contributions, Dr. Laura Belli, Dr. Luca Davoli, Dr. Paolo Medagliani, Dr. Stefano Busanelli, Gabriele Ferrari, Vincent Gay, Dr. Jérémie Leguay, Mattia Antonini, Dr. Andrea Gorrieri, Lorenzo Melegari, and Mirko Mancin. We also thank, for collaborative efforts and useful discussions, Dr. Michele Amoretti, Dr. Francesco Zanichelli, Dr. Andrzej Duda, Dr. Simon Duquennoy, Dr. Nicola Iotti, Dr. Andrea G. Forte, and Giovanni Guerri. Finally, we express our sincere gratitude to Wiley

for giving us the opportunity to complete this project. In particular, we are indebted to Tiina Wigley, our executive commissioning editor, for showing initial interest in our proposal; we are *really* indebted to Sandra Grayson, our associate book editor, who has shown remarkable patience and kindness, tolerating our delay and idiosyncrasies throughout the years of writing.

Parma, July 2018

Simone Cirani
Gianluigi Ferrari
Marco Picone
Luca Veltri

1

Preliminaries, Motivation, and Related Work

1.1 What is the Internet of Things?

The Internet of Things (IoT) encapsulates a vision of a world in which billions of objects with embedded intelligence, communication means, and sensing and actuation capabilities will connect over IP (Internet Protocol) networks. Our current Internet has undergone a fundamental transition, from hardware-driven (computers, fibers, and Ethernet cables) to market-driven (Facebook, Amazon) opportunities. This has come about due to the interconnection of seamingly disjoint intranets with strong horizontal software capabilities. The IoT calls for open environments and an integrated architecture of interoperable platforms. Smart objects and cyber-physical systems – or just "things" – are the new IoT entities: the objects of everyday life, augmented with micro-controllers, optical and/or radio transceivers, sensors, actuators, and protocol stacks suitable for communication in constrained environments where target hardware has limited resources, allowing them to gather data from the environment and act upon it, and giving them an interface to the physical world. These objects can be worn by users or deployed in the environment. They are usually highly constrained, with limited memory and available energy stores, and they are subject to stringent low-cost requirements. Data storage, processing, and analytics are fundamental requirements, necessary to enrich the raw IoT data and transform them into useful information. According to the "Edge Computing" paradigm, introducing computing resources at the edge of access networks may bring several benefits that are key for IoT scenarios: low latency, real-time capabilities and context-awareness. Edge nodes (servers or micro data-centers on the edge) may act as an interface to data

Internet of Things: Architectures, Protocols and Standards, First Edition.
Simone Cirani, Gianluigi Ferrari, Marco Picone, and Luca Veltri.

streams coming from connected devices, objects, and applications. The stored Big Data can then be processed with new mechanisms, such as machine and deep learning, transforming raw data generated by connected objects into useful information. The useful information will then be disseminated to relevant devices and interested users or stored for further processing and access.

1.2 Wireless Ad-hoc and Sensor Networks: The Ancestors without IP

Wireless sensor networks (WSNs) were an emerging application field of microelectronics and communications in the first decade of the twenty-first century. In particular, WSNs promised wide support of interactions between people and their surroundings. The potential of a WSN can be seen in the three words behind the acronym:

- "Wireless" puts the focus on the freedom that the elimination of wires gives, in terms of mobility support and ease of system deployment;
- "Sensor" reflects the capability of sensing technology to provide the means to perceive and interact — in a wide sense — with the world;
- "Networks" gives emphasis to the possibility of building systems whose functional capabilities are given by a plurality of communicating devices, possibly distributed over large areas.

Pushed on by early military research, WSNs were different from traditional networks in terms of the communication paradigm: the address-centric approach used in end-to-end transmissions between specific devices, with explicit indication of both source and destination addresses in each packet, was to be replaced with an alternative (and somewhat new) data-centric approach. This "address blindness" led to the selection of a suitable data diffusion strategy – in other words, communication protocol – for data-centric networks. The typical network deployment would consist of the sources placed around the areas to be monitored and the sinks located in easily accessible places. The sinks provided adequate storage capacity to hold the data from the sources. Sources might send information to sinks in accordance with different scheduling policies: periodic (i.e., time-driven), event specific (i.e., event-driven), a reply in response to

requests coming from sinks (i.e., query-driven), or some combination thereof.

Because research focused on the area, WSNs have typically been associated with ad-hoc networks, to the point that the two terms have almost become – although erroneously so – synonymous. In particular, ad-hoc networks are defined as general, infrastructure-less, cooperation-based, opportunistic networks, typically customized for specific scenarios and applications. These kinds of networks have to face frequent and random variations of many factors (radio channel, topology, data traffic, and so on), implying a need for dynamic management of a large number of parameters in the most efficient, effective, and reactive way. To this end, a number of key research problems have been studied, and solutions proposed, in the literature:

- self-configuration and self-organization in infrastructure-less systems;
- support for cooperative operations in systems with heterogenous members;
- multi-hop peer-to-peer communication among network nodes, with effective routing protocols;
- network self-healing behavior providing a sufficient degree of robustness and reliability;
- seamless mobility management and support of dynamic network topologies.

1.3 IoT-enabled Applications

The IoT touches every facet of our lives. IoT-enabled applications are found in a large number of scenarios, including: home and building automation, smart cities, smart grids, Industry 4.0, and smart agriculture. In each of these areas, the use of a common (IP-oriented) communication protocol stack allows the building of innovative applications. In this section, we provide a concise overview of potential applications in each of these areas.

1.3.1 Home and Building Automation

As the smart home market has seen growing investment and has continued to mature, ever more home automation applications have

appeared, each designed for a specific audience. The result has been the creation of several disconnected vertical market segments. Typical examples of increasingly mainstream applications are related to home security and energy efficiency and energy saving. Pushed by the innovations in light and room control, the IoT will foster the development of endless applications for home automation. For example, a typical example of an area of home automation that is destined to grow in the context of the IoT is in healthcare, namely IoT-enabled solutions for the physically less mobile (among others, the elderly, particulary relevant against a background of aging populations), and for the disabled or chronically ill (for instance, remote health monitoring and air-quality monitoring). In general, building automation solutions are starting to converge and are also moving, from the current applications in luxury, security and comfort, to a wider range of applications and connected solutions; this will create market opportunities. While today's smart home solutions are fragmented, the IoT is expected to lead to a new level of interoperability between commercial home and building automation solutions.

1.3.2 Smart Cities

Cities are complex ecosystems, where quality of life is an important concern. In such urban environments, people, companies and public authorities experience specific needs and demands in domains such as healthcare, media, energy and the environment, safety, and public services. A city is perceived more and more as being like a single "organism", which needs to be efficiently monitored to provide citizens with accurate information. IoT technologies are fundamental to collecting data on the city status and disseminating them to citizens. In this context, cities and urban areas represent a critical mass when it comes to shaping the demand for advanced IoT-based services.

1.3.3 Smart Grids

A smart grid is an electrical grid that includes a variety of operational systems, including smart meters, smart appliances, renewable energy resources, and energy-efficient resources. Power line communications (PLC) relate to the use of existing electrical cables to transport data and have been investigated for a long time. Power utilities have been using this technology for many years to send or receive (limited amounts of)

data on the existing power grid. Although PLC is mostly limited by the type of propagation medium, it can use existing wiring in the distribution network. According to EU's standards and laws, electrical utility companies can use PLC for low bit-rate data transfers (with data rates lower than 50 Kbps) in the 3–148 kHz frequency band. This technology opens up new opportunities and new forms of interactions among people and things in many application areas, such as smart metering services and energy consumption reporting. This makes PLC an enabler for sensing, control, and automation in large systems spread over relatively wide areas, such as in the smart city and smart grid scenarios. On top of PLC, one can also adopt enabling technologies that can improve smart automation processes, such as the IoT. For instance, the adoption of the PLC technology in industrial scenarios (e.g., remote control in automation and manufacturing companies), paves the way to the "Industrial IoT". Several applications have been enabled by PLC technology's ability to recover from network changes (in terms of repairs and improvements, physical removal, and transfer function) mitigating the fallout on the signal transmission.

Nevertheless, it is well known that power lines are far from ideal channels for data transmission (due to inner variations in location, time, frequency band and type of equipment connected to the line). As a result there has been increasing interest in the joint adoption of IoT and PLC paradigms to improve the robustness of communication. This has led to the suggestion of using small, resource-constrained devices (namely, IoT), with pervasive computing capabilities, and internet standard solutions (as proposed by Internet standardization organizations, such as IETF, ETSI and W3C). Such systems can be key components for implementing future smart grids.

1.3.4 Industrial IoT

The Industrial Internet of Things (IIoT) describes the IoT as used in industries such as manufacturing, logistics, oil and gas, transportation, energy/utilities, mining and metals, aviation and others. These industries represent the majority of gross domestic product among the G20 nations. The IIoT is still at an early stage, similar to where the Internet was in the late 1990s. While the evolution of the consumer Internet over the last two decades provides some important lessons, it is unclear how much of this learning is applicable to the IIoT, given its unique scope and requirements. For example, *real-time* responses are

often critical in manufacturing, energy, transportation and healthcare: real time for today's Internet usually means a few seconds, whereas real time for industrial machines involves sub-millisecond scales. Another important consideration is reliability. The current Internet embodies a "best effort" approach, which provides acceptable performance for e-commerce or human interactions. However, the failure of the power grid, the air traffic control system, or an automated factory for the same length of time would have much more serious consequences.

Much attention has been given to the efforts of large companies such as Cisco, GE, and Huawei, and government initiatives such as Industrie 4.0 in Germany. For example:

- GE announced that it realized more than $1 billion in incremental revenues in 2014 by helping customers improve asset performance and business operations through IIoT capabilities and services.
- The German government is sponsoring "Industrie 4.0", a multi-year strategic initiative that brings together leaders from the public and private sectors as well as from academia to create a comprehensive vision and action plan for applying digital technologies to the German industrial sector.
- Other European countries have their own industrial transformation projects in which the IIoT takes center stage, such as Smart Factory (the Netherlands), Industry 4.0 (Italy), Industry of the Future (France), and others.
- China has also recently launched its "Made in China 2025" strategy to promote domestic integration of digital technologies and industrialization.

As the IIoT gains momentum, one of the biggest bottlenecks faced is the inability to share information between smart devices that may be speaking different "languages". This communication gap stems from the multiple protocols used on factory floors. So, while you can put a sensor on a machine to gather data, the ability to push that information across a network and ultimately "talk" with other systems is a bit more difficult. Standardization is therefore a key aspect of the IIoT.

The IIoT's potential payoff is enormous. Operational efficiency is one of its key attractions, and early adopters are focused on these benefits. By introducing automation and more flexible production techniques, for instance, manufacturers could boost their productivity by as much as 30%. In this context, three IIoT capabilities must be mastered:

- *sensor-driven computing*: converting sensed data into insights (using the industrial analytics described below) that operators and systems can act on;
- *industrial analytics*: turning data from sensors and other sources into actionable insights;
- *intelligent machine applications*: integrating sensing devices and intelligent components into machines.

1.3.5 Smart Farming

Modern agriculture is facing tremendous challenges as it attempts to build a sustainable future across different regions of the globe. Examples of such challenges include population increase, urbanization, an increasingly degraded environment, an increasing trend towards consumption of animal proteins, changes in food preferences as a result of aging populations and migration, and of course climate change. A modern agriculture needs to be developed, characterized by the adoption of production processes, technologies and tools derived from scientific advances, and results from research and development activities.

Precision farming or smart agriculture is an area with the greatest opportunities for digital development but with the lowest penetration, to date, of digitized solutions. The farming industry will become arguably more important than ever before in the next few decades. It could derive huge benefits from the use of environmental and terrestrial sensors, applications for monitoring the weather, automation for more precise application of fertilizers and pesticides (thus reducing waste of natural resources), and the adoption of planning strategies for maintenance.

Smart farming is already becoming common, thanks to the application of new technologies, such as drones and sensor networks (to collect data) and cloud platforms (to manage the collected data). The set of technologies used in smart farming are as complex as the activities run by farmers, growers, and other stakeholders in the sector. There are is a wide spectrum of possible applications: fleet management, livestock monitoring, fish farming, forest care, indoor city farming, and many more. All of the technologies involved revolve around the concept of the IoT and aim at supporting farmers in their decision processes through decision-support systems. They involve real-time data at a level of granularity not previously possible. This

enables better decisions to be made, translating into less waste and an increase in efficiency.

Communication technologies are a key component of smart agriculture applications. In particular, wireless communication technologies are attractive, because of the significant reduction and simplification in wiring involved. Various wireless standards have been established. One can group these into two main categories, depending on the transmission range:

- *Short-range communication*: including standards for:
  – wireless LAN, used for Wi-Fi, namely IEEE 802.11
  – wireless PAN, used more widely for measurement and automation applications, such as IEEE 802.15.1 (Bluetooth) (IEEE, 2002) and IEEE 802.15.4 (ZigBee/6LoWPAN) (IEEE, 2003).

  All these standards use the instrumentation, scientific and medical (ISM) radio bands, typically operating in the 2.400–2.4835 GHz band.
- *Long-range communication*: including the increasingly important sub-gigahertz IoT communication techologies, such as LoRA, in the 868–870 MHz band. These trade data transmission rates (on the order of hundreds of kbit/s) for longer transmission ranges.

Communication technologies can be also classified according to the specific application:

- environmental monitoring (weather monitoring and geo-referenced environmental monitoring)
- precision agriculture
- machine and process control (M2M communications)
- facility automation
- traceability systems.

2

Standards

2.1 "Traditional" Internet Review

The original idea of the Internet was that of connecting multiple independent networks of rather arbitrary design. It began with the ARPANET as the pioneering packet switching network, but soon included packet satellite networks, ground-based packet radio networks and other networks. The current Internet is based on the concept of open-architecture networking (an excellent overview of the history of the Internet is in an article by Leiner *et al.* [1]). According to this original approach, the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with the other networks through a meta-level "internetworking architecture". The use of the open systems interconnect (OSI) approach, with the use of a layer architecture, was instrumental in the design of interactions between different networks. The TCP/IP protocol suite has proven to be a phenomenally flexible and scalable networking strategy. Internet Protocol (IP) (layer three) provides only for addressing and forwarding of individual packets, while the transport control protocol (TCP; layer four), is concerned with service features such as flow control and recovery when there are lost packets. For those applications that do not need the services of TCP, the User Datagram Protocol (UDP) provides direct access to the basic service of IP.

In practice, the seven-layer architecture foreseen by the ISO-OSI protocol stack has been replaced by a five-layer IP stack. This is typically referred to as the TCP/IP protocol stack, because the TCP is the most-used protocol in the transport layer and IP is the almost ubiquitous in the network layer. The three upper layers of the

Internet of Things: Architectures, Protocols and Standards, First Edition.
Simone Cirani, Gianluigi Ferrari, Marco Picone, and Luca Veltri.

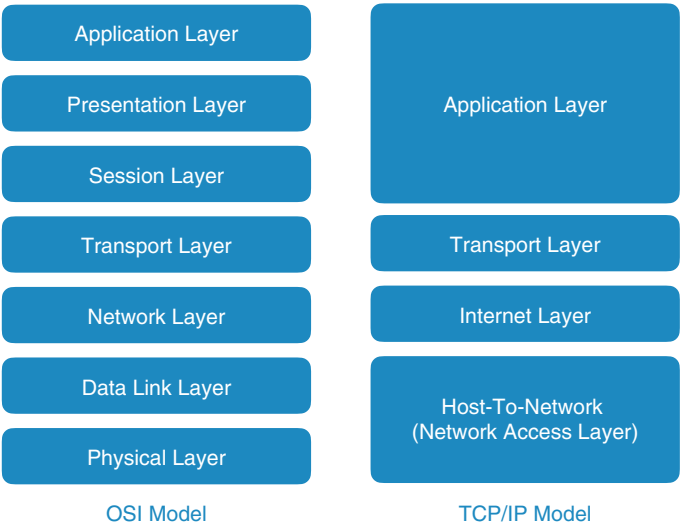

Figure 2.1 Communication protocol stacks: traditional seven-layer ISO-OSI stack (left) versus four-layer TCP/IP stack (right).

ISO-OSI protocol stack – the session (layer five), presentation (layer six), and application (layer seven) – converge in a single (fifth) layer in the TCP/IP protocol stack, namely The layered architecture of the Internet (according to the ISO-OSI and TCP/IP models) is shown in Figure 2.1.

In the following, we summarize the main communication protocols used in the various layers of the ISO-OSI communication protocol stack. In particular, we will outline:

- at the physical/link layer (L1/L2), the IEEE802.3 (Ethernet) and IEEE 802.11 (Wi-Fi) protocols;
- at the network layer (L3), IPv4 and IPv6;
- at the transport layer (L4), TCP and UDP;
- at the application layer (L5), Hypertext Transfer Protocol (HTTP) and Session Initiation Protocol (SIP).

2.1.1 Physical/Link Layer

In this subsection, we focus on two relevant communication protocols for physical/link (PHY/MAC) layers, namely the IEEE 802.3 standard