The Internet *of* Things

Key Applications and Protocols

OLIVIER HERSENT | DAVID BOSWARTHICK | OMAR ELLOUMI

WILEY

ETSI World Class Standards

THE INTERNET OF THINGS

THE INTERNET OF THINGS

KEY APPLICATIONS AND PROTOCOLS

Olivier Hersent
Actility, France

David Boswarthick
ETSI, France

Omar Elloumi
Alcatel-Lucent, France

ETSI World Class Standards

WILEY
A John Wiley & Sons, Ltd., Publication

This edition first published 2012

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Hersent, Olivier.
The internet of things : key applications and protocols / Olivier Hersent, David Boswarthick, Omar Elloumi.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-119-99435-0 (hardback)
1. Intelligent buildings. 2. Smart power grids. 3. Sensor networks. I. Boswarthick, David. II. Elloumi, Omar. III. Title.
TH6012.H47 2012
681′.2–dc23

2011037210

A catalogue record for this book is available from the British Library.

ISBN: 9781119994350 (H/B)

Typeset in 10.5/13pt Times by Aptara Inc., New Delhi, India

Contents

List of Acronyms

6LoWPAN	6LoWPAN is the acronym of IPv6 over Low power Wireless Personal Area Networks and the name of a working group in IETF
ACL	Access Control List
ACSE	Association Control Service Element
AER	All Electric Range
AFE	Analog Front End
AIB	Application Layer Information Base
AIS	Application Interworking Specification
AMI	Automatic Metering Infrastructure
ANSI	American National Standards Institute
AODV	Advanced Ad-Hoc On-Demand Distance Vectoring
AP	Application Process
APDU	Application Protocol Data Unit
API	Application Programming Interface
aPoC	Application Point of Contact
APS	Application Support Sublayer
APSDE-SAP	Application Support Sublayer Data Entity Service Access Point
APSME-SAP	Application Support Sublayer Management Entity Service Access Point
APSSE-SAP	Application Support Sublayer Security Entity Service Access Point
ARIB	Association of Radio Industries and Businesses is a standardization organization in Japan
ASDU	Aps Service Data Unit
ASK	Amplitude-Shift Keying
BbC	KNX Backbone Controller
BCI	Batibus Club International
BEV	Battery Electric Vehicle
BO	Beacon Order
BPSK	Binary Phase Shift Keying
BTT	Broadcast Transaction Table

CAN	Controller Area Network
CAP	Contention Access Period
CBC MAC	CBC Message Authentication Code
CC	Consistency Check
CCA	Clear Channel Assessment
CCM*	Extension of Counter with CBC-MAC Mode of Operation
CD range	Charge Depleting Range
CENELEC	European Committee for Electrotechnical Standardization
CER	Communication Error Rate
CFP	Contention Free Period
CI	Control Information
CNF	M-Bus CONFIRM Message
CRC	Cyclical Redundancy Check
CRL	X.509 Certificate Revocation List
CRUD	Create, Read, Update, Delete
CS mode	Charge Sustaining Mode
CSL	Coordinated Sampled Listening
CSMA	Carrier-Sense, Multiple Access
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
D device	ETSI M2M device without local M2M capabilities and interfaced to a gateway via the mId interface
D' device	ETSI M2M device implementing ETSI M2M capabilities and the mId interface to the network domain (does not interface via a gateway)
DA	Device Application
DAG	Direct Acyclic Graph
DAG root	A Node within the DAG that has no outgoing edge
DAO	Destination Advertisement Object
DER	Distinguished Encoding Rule
dIa	ETSI M2M Reference point between an application and ETSI M2M service capabilities
DIB	Data Information Block
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DLL	Data Link Layer the layer 2 specified in the seven-layer OSI model
DLMS	Device Language Message Specification is a specification for Data exchange for meter reading, tariff and load control
DODAG	Oriented Direct Acyclic Graph
DODAG Version	Specific iteration ("Version") of a DODAG with a given DODAGID
DODAGID	The identifier of a DODAG Root
DR	Demand Response

DRH	Data Record Header
DSSS	Direct Spread Spectrum Destination
DTSN	Destination Advertisement Trigger Sequence Number
ED	Energy Detection
EFF	Extended Frame Format
EHS	European Home System
EIB	European Installation Bus
EIBA	The European Installation Bus Association
EMC	Electromagnetic Compatibility
EMS	Energy Management System
EN 50065-1	CENELEC standard for Powerline transmission on low-voltage electrical installations in the frequency range 3 to 148,5 kHz
EP	Enforcement Point
EPID	Extended PAN ID
ESI	Energy Services Interface
ESP	Energy Service Portal
eTag	Entity Tag
ETSI	European Telecommunications Standards Institute is an independent, nonprofit, standardization organization in the telecommunications industry
ETSI PLT	The ETSI Powerline working group
EUI	Extended Unique Identifier
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Charging Equipment
EXI	Efficient XML Interchange Encoding
FCC	Federal Communications Commission
FFD	Full Function Device
FHSS	Frequency Hopping Spread Spectrum
FLiRS	Frequently Listening Routing Slave
FSK	Frequency-shift keying is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave
GA	Gateway Application
GBA	Generic Bootstrapping Architecture
GCM	Galois/Counter Mode
GMO	Gateway Management Object
GO	Group Object
GRE	Gestionnaire de réseau de transport
GRIP	Gateway Remote Interface Protocol
HC	Header Compression
HEV	Hybrid Electric Vehicle

HLS	High-Level Security
HomePlug Alliance	The HomePlug Alliance is a group of electronics manufacturers, service providers, and retailers that establishes standards for power line communication
IANA	Internet Assigned Number Authority
I-Band	Industrial Band, see ISM
IC	Interface Class
IEC TC13	International Electrotechnical Commission, Technical Committee 13
IEEE	The Institute of Electrical and Electronics Engineers
IEEE 1901	IEEE 1901 is an IEEE working group developing a global standard for high speed Powerline communications
IEEE 802.15.4	IEEE 802.15.4-2006 is a standard that specifies the physical layer and media access control for low-rate wireless personal area networks
IEEE P1901.2	IEEE 1901.2 is an IEEE working group developing a Powerline communications standard for metering applications
IETF	Internet Engineering Task Force
IHD	In Home Display
IID	Interface Id
IO	Interface Object
IPHA	IP Host Application
IPHC	IP Header Compression
IPSO	Internet Protocol for Smart Objects is a industry alliance promoting Internet of Objects
ISM	Industrial Scientific and Medical
ISO	International Organization for Standardization
ISP	Intersystem Protocol
ITS	Intelligent Transport System
ITU	International Telecommunication Union is the specialized agency of the United Nations which is responsible for information and communication technologies
ITU G.9972	ITU G.9972 (also known as G.cx) is a recommendation developed by ITU-T that specifies a coexistence mechanism for networking transceivers
ITU G.hn	G.hn is the common name for ITU recommendation G.9960, a home network technology standard being developed under the International Telecommunication Union
ITU G.hnem	An ITU project addressing the home networking aspects of energy management
LC	Line Coupler
LDN	Logical Device Name

LLC	Logical Link Control layer
LLN	Low Bitrate and Lossy Network
LLS	Low-Level Security
LN	Logical Name
LonWorks	LonWorks is a networking platform created to control applications The platform is built on a protocol created by Echelon Corporation
LowPAN	Low-power Wireless Personal Area Networks
LQI	Link Quality Information
LRWBS	Low Rate Wide Band Services are emerging services on Powerline transmitting in the 2–4 MHz band
LV-MV	Low Voltage (less than 600 Volts) and Medium Voltage (in the order of magnitude of 20 000 Volts)
M2M	Machine-to-Machine
MAC	Media Access Control
MAS	M2M Authentication Server
MCPS	MAC Common Part Sublayer
MCPS-SAP	MAC Common Part Service Access Point
MDU	Multidwelling Unit
mIa	Reference Point between a M2M application and the M2M Service Capabilities in the Networks and Applications Domain
MIC	Message Integrity Protection Code
mId	Reference point between an M2M Device or M2M Gateway and the M2M Service Capabilities in the Network and Applications Domain
MLDE	MAC Layer Management Entity
MLME-SAP	MAC Layer Management Entity Service Access Point
MP2P	Multipoint To Point Traffic
MSBF	M2M Service Bootstrap Function
MSP	Manufacturer Specific Profile
MTU	Maximum Transmission Unit
NA	Network Application
NAN	Neighborhood Area Network
NAPT	Network Address and Port Translation
NIB	Network Information Base
NIF	Node Information Frame
NIP	Network Interworking Proxy
NIST	National Institute of Standards and Technology is a measurement standards laboratory in USA
NLDE-SAP	Network Layer Data Entity Service Access Point
NLME	Network Layer Management Entity
NLME-SAP	Network Layer Management Entity Service Access Point
NLSE-SAP	Network Layer Security Entity Service Access Point

NREL	National Renewable Energy Laboratory
NRZ	Nonreturn to Zero
NUD	Neighbor Unreachability Detection
OBIS	Object Identification System
OCP	Objective Code Point
OF	Objective Function
OFDM	Orthogonal Frequency-Division Multiplexing
OOK	On-off keying the simplest form of modulation that represents digital data as the presence or absence of a carrier wave
O-QPSK	Offset-Quadrature Phase-Shift Keying
OSI	Open Systems Interconnections
OTA	Over-the-Air
OUI	Organizationally Unique Identifier
P2MP	Point to Multipoint Traffic
PAA	PANA Authentication Agent
PaC	PANA Client
PAN	Personal Area Network
PAN ID	Personal Area Network Identifier
PANA	Protocol for Carrying Authentication for Network Access
PCT	Programmable Communicating Thermostat
PEV	Plug-in Electric Vehicle
PHEV	Plug-in Hybrid Electric Vehicle
PHR	Physical Header
PHY	Physical Layer
PIB	PAN Information Base
PIO	Prefix Information Option
PLC	Powerline Communication
PLT	Powerline Technology
PN	Parent Node
PoC	Point of Contact
PRE	PANA Relay Element
PRIME	Powerline Intelligent Metering Evolution
PSDU	Physical Service Data Unit
PSEM	Protocol Specification for Electric Metering
PSSS	Parallel Spread Spectrum modulation
PWM	Pulse Width Modulation
Rank	A node's individual position relative to other nodes with respect to a DODAG root
REQ	M-Bus REQUEST message
REST	Representational State Transfer
RFD	Reduced Function Device
RIT	Receiver-Initiated Transmission

ROLL	Routing over Low-power and Lossy network
RPF	Reverse Power Flow
RPL	RPL IPv6 Routing Protocol over Low-power and Lossy Networks
RPL Instance	A set of one or more DODAGs that share a RPLInstanceID
RPLInstanceID	A unique identifier within a RPL LLN. DODAGs with the same RPLInstanceID share the same Objective Function
RSP	M-Bus RESPOND Message
RTE	Réseau Transport Electricité
RTU	Remote Terminal Unit
RZtime	Rendezvous Time
SA	Secure Association
SAP	Service Access Point
S-Band	Scientific Band, *see* ISM
SCDE	Secured Connection Protocol
SCL	Service Capability Layer
SCME	SCoP Management Entity
SCoP	SCoP Data Entity
SCPT	Standard Configuration Property Type
SCSS	SCoP Security Service
SDP	SECC Discovery Protocol
SDU	Service Data Unit
SECC	Supply Equipment Communication Controller
SFD	Start Frame Delimiter
SHR	Synchronous Header
SKKE	Symmetric-Key Key Exchange
SLAAC	IPv6 Stateless Address Autoconfiguration
SN	Short Name
SND	M-Bus SEND Message
SNVT	Standard Network Variable Type
SoC	System on Chip
SUN	Smart Utility Network
TDMA	Time division multiple access is a channel access method for shared medium networks
TL	Transport Layer
TLS	Transport Layer Security
ToU	Time of Use
TP1	KNX Twisted Pair Physical Media
TSCH	Time-Synchronized Channel Hopping
TSO	Transmission System Operator
UC	Upgrade Client
UID	Unique Node Identifier
U-NII	Unlicensed National Information Infrastructure

UNVT	User Network Variable Type
US	Upgrade Server
V2GTP	Vehicle to Grid Transfer Protocol
VIB	Value Information Block
VIF	Value Information field, see M-Bus
WADL	Web Application Description Language
xAE	Application Enablement M2M Service Capability
xBC	Compensation Broker M2M Service Capability
XCAP	Extensible Markup Language (XML) Configuration Access Protocol (RFC 4825)
xCS	Communication Selection M2M Service Capability
xHDR	History and Data Retention M2M Service Capability
xIP	Interworking Proxy M2M Service Capability
xRAR	Reachability, Addressing and Repository M2M Service Capability
xREM	Remote Entity Management M2M Service Capability
xSEC	Security M2M Service Capability
xTM	Transaction Management M2M Service Capability
xTOE	Telco Operator Exposure M2M Service Capability
ZBD	ZigBee Bridge Device
ZC	ZigBee Coordinator
ZCL	ZigBee Cluster Library
ZCP	ZigBee Compliant Platform
ZDO	ZigBee Device Object
ZDP	ZigBee Device Profile
ZED	ZigBee End Device
Zero-crossing	In alternating current, the zero-crossing is the instantaneous point at which there is no voltage present
ZGD	ZigBee Gateway Device
ZigBee Alliance	ZigBee Alliance is a group of companies that maintain and publish the ZigBee standard
ZIPT	ZigBee IP Tunneling Protocol
ZR	ZigBee Router
ZSE	ZigBee Smart Energy

Introduction

Innovation rarely comes where it is expected. Many governments have been spending billions to increase the Internet bandwidth available to end users . . . only to discover that there are only a limited number of HD movies one can watch at a given time. In fact, there are also a limited number of human beings on Earth.

The Internet is about to bring us another ten years of surprises, as it morphs into the "Internet of Things" (IoT). Your mobile phone and your PC are already connected to the Internet, maybe even your car GPS too. In the coming years your car, office, house and all the appliances it contains, including your electricity, gas and water meters, street lights, sprinklers, bathroom scales, tensiometers and even walls[1] will be connected to the IoT. Tomorrow, several improvements will be made to these appliances such as not heating your house if hot weather is forecast, watering your garden automatically only if it doesn't rain, getting assistance immediately on the road, and so on. These improvements will facilitate our lives and utilize natural resources more efficiently.

Why is this happening now? As always, there is a combination of small innovations that, together, have reached a critical mass:

- Fieldbus technologies, using proprietary protocols and standards (LON, KNX, DALI, CAN, ModBus, M-Bus, ZigBee, Zwave . . .), have explored many vertical domains. Gradually, these domains have started to overlap as use cases expanded to more complex situations, and protocols have emerged to facilitate interoperability (e.g., BACnet). But in many ways, current fieldbus deployments continue to use parallel networks that do not collaborate. The need for a common networking technology that would run over any physical layer, like IP, has become very clear.
- Despite the need for a layer 2 independent networking technology for fieldbuses, IP was not considered as a possible candidate for low-bitrate physical layers typically used in fieldbus networks, due to its large overheads. But the wait is now over: with 6LoWPAN not only has IP technology found its way onto low-bitrate networks but – surprise, surprise – it is IPv6 ! As an additional bonus, the technology comes with a state-of-the-art, standardized IP level mesh networking protocol, which makes multiphy

[1] Sensors for structural monitoring.

mesh networking a reality: finally different layer 2 fieldbus technologies can collaborate and form larger networks.

- Today, local fieldbus networks optimize the HVAC[2] regulation in your office and perhaps your home, with sophisticated algorithms. The energy-efficiency regulation for new building construction has created a need for even more sophisticated algorithms, like predictive regulation that takes into account weather forecasts or load shifting that incorporates the CO_2 content of electricity. In many automation sectors, the current state-of-the-art tool requires the local fieldbus to collaborate with hosted centralized applications and data sources. The technology required to enable this progressed in steps: oBix introduced the concept of a uniform (REST) interface to sensor networks, ETSI M2M added the management of security and additional improvements required in large-scale public networks.

The industry was only missing a really, really compelling business case to trigger the enormous amount of R&D that will be required to integrate all these technologies and build a bulletproof Internet of Things.

This business case is coming from the energy sector:

- The accelerated introduction of renewable-energy sources in the overall electricity production park brings an increasing degree of randomness to the traditionally deterministic supply side.
- In parallel, the mass introduction of rechargeable electric and hybrid vehicles is making the demand side more complex: EVs are roaming objects that will need to authenticate to the network, and will require admission control protocols.

The current credo of electricity operators “demand is unpredictable, and our expertise is to adapt production to demand”, is about to be reversed into “production is unpredictable, and our expertise is to adapt demand to production”.

As the rules of the game change, the key assets of an energy operator will no longer be the means of production, but the next-generation communication network and information system, which they still need to build entirely, creating an enormous market for mission-critical M2M technology. This dramatic change of how electricity will be distributed prefigures the more general evolution of the Internet towards the Internet of Things, where telecom operators and network-based application developers will have an increasing impact on our everyday lives, including the things that we touch and use.

This book targets an audience of engineers who are involved or want to get involved in large-scale automation and smart-grid projects and need to get a feel for the “big picture”.

Many such projects will involve interfaces with existing systems. We included detailed overviews of many legacy fieldbus and automation technologies: BACnet, CAN, LON, M-Bus/wMBUS, ModBus, LON, KNX, ZigBee, Z-Wave, as well as C.12 and

[2] Heating, ventilation and air conditioning.

DLMS/COSEM metering standards. We also cover in detail two common fieldbus physical layers: 802.15.4 and PLC.

This book will not make you an expert on any of these technologies, but provides enough information to understand what each technology can or cannot do, and the fast-track descriptions should make it much easier to learn the details by yourself.

The future of fieldbus protocols is IP: we introduce 6LoWPAN and RPL, as well as the first automation protocol to have been explicitly designed for 6LoWPAN networks: ZigBee SE 2.0. We also provide an introduction to the emerging ETSI M2M standard, which is the much-awaited missing piece for service providers willing to provide a general-purpose public M2M infrastructure, shared by all applications.

I would like to thank Paul Bertrand, the inventor of the lowest-power PLC fieldbus technology to date (WPC) and designer of the first port of 6LoWPAN to PLC for accepting to write – guess what – the Powerline Communications chapter of this book. I am also grateful for the C.12 and DLMS chapters that were provided by Jean-Marc Ballot (Alcatel), and required a lot of documentation work.

Despite my efforts, there are probably quite a few errors remaining in the text, but there would have been many more without the help of the expert reviewers of this book: Cedric Chauvenet for 6LoWPAN/RPL, Mathieu Pouillot for ZigBee, Juan Perez (EPEX) for the smart-grid section, François Collet (Renault) for EV charging, Alexandre Ouimet-Storrs for his insights on energy trading, and the companies who provided internal documentation or reviews: Echelon for LON (with special thanks to Bob Dolin, Jeff Lund, Larry Colton and Mark Ossel), and Sigma Designs for Z-Wave. I am also grateful to Benoit Guennec and Baptiste Vial (Connected Object), who supplied me with the temperature and consumption profiles of their homes and shared their field experience with Z-Wave. Please let me know of remaining errors, so that we can improve the next edition of this book, at olivier.hersent@actility.com.

Gathering and reading the documentation for this book has been an amazing experience discovering new horizons and perspectives. I hope you will enjoy reading this book as much as I enjoyed writing it.

Olivier Hersent

Part One

M2M Area Network Physical Layers