A Practical Guide to Power Line Communications

This excellent resource synthesizes the theory and practice of power line communication (PLC), providing a straightforward introduction to the fundamentals of PLC as well as an exhaustive review of the performance, evaluation, and security of heterogeneous networks that combine PLC with other means of communications. It advances the groundwork on PLC, a tool with the potential to boost the performance of local networks, and provides useful worked problems on, for example, PLC protocol optimization. Covering the PHY and MAC layers of the most popular PLC specifications, including tutorials and experimental frameworks, and featuring many examples of real-world applications and performance, it is ideal for university researchers and professional engineers designing and maintaining PLC or hybrid devices and networks.

Christina Vlachou is Senior Research Scientist at Hewlett Packard Enterprise Laboratories.

Sébastien Henri is Senior Software Engineer at Cisco Meraki.

A Practical Guide to Power Line Communications

CHRISTINA VLACHOU
Hewlett Packard Enterprise Laboratories

SÉBASTIEN HENRI
Cisco Meraki

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108835480
DOI: 10.1017/9781108890823

First published 2022

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

ISBN 978-1-108-83548-0 Hardback

Contents

Preface

Having spent eight years on research of power line communications (PLC), we observed a significant gap between industry and academia, especially on the configuration and management of PLC devices. From the industry perspective, there are a few open source tools for configuration and measurement of PLC. However, unlike Wi-Fi chipsets, there is no open source firmware. Measurement and configuration of commercial devices require a lot of reverse engineering. From the academia perspective, there are many analytical and measurement works, which often do not get compared to or implemented on commercial devices due to the tools' limitations and obfuscated firmware. During our doctoral theses, we developed an experimental framework on commercial devices as well as analysis tools for PLC. Performance analysis is useful for network optimizations and for ensuring scalability in multiuser deployments. Yet, models have to be validated against experimental results, and chipset configuration is essential for implementing any optimizations. To help users and researchers address these issues, we have decided to write this book to share our knowledge and methods to configure, manage, analyze, and evaluate PLC networks.

Our book mainly focuses on the IEEE 1901 standard, on which the vast majority of commodity PLC devices are based. We first provide an understanding of the standard, giving the most important features of physical (PHY) and medium-access control (MAC) layers. Understanding how data flows and is modulated and transmitted over the electrical wires is crucial for evaluating PLC performance. The standard is about 1600 pages and describes two types of PLC networks: the Internet access networks and the indoor enterprise/residential PLC networks. Hence IEEE 1901 stations can be deployed in-building or over power line distribution cables. The two deployments differ in topology, protocols, and channel quality, which differentiates also the PHY and MAC features. In our book, we focus on broadband indoor PLC networks, which work at low voltage and are very popular in residential environments.

The book is divided into three parts. First, we present the channel models and PHY layer of PLC devices. We explain how data flows are modulated into analog signals transmitted over the electrical wires and how these signals propagate. The attenuation and noise experienced by PLC signals are different and more complex than those of Wi-Fi. This yields a different PHY layer design with adaptive and periodic modulation with respect to the alternate current (AC). The MAC layer of PLC is also more complex than Wi-Fi. Similarly to Wi-Fi, PLC is a broadcast medium; hence stations have to resolve collisions when they transmit simultaneously. But owing to the specificities of power lines, PLC MAC introduces an additional variable that creates different levels of multiuser efficiency and short-term fairness. We present a detailed experimental framework for configuring and measuring performance of PLC commercial devices. We discuss how to measure PHY- and MAC-layer metrics, configure topology and security mechanisms, and write new tools for these functionalities.

In the second part of the book, we present a performance evaluation of the PHY and MAC layers on a testbed of nineteen stations. We explore the spatial and temporal variation of capacity and provide guidelines for link metric estimation in hybrid PLC/Wi-Fi networks. Then, we present efficiency and throughput models of the MAC layer and analyze the multiuser performance and configurations. In this second part, we provide experimental guidelines to reproduce the experiments.

In the third part of the book, we discuss security, management, and other applications of PLC. We present the processes of creating secure PLC networks, new station authentication and association, and potential security attacks on PLC. Finally, we discuss the IEEE 1905.1 standard for heterogeneous networks where several technologies, such as PLC and Wi-Fi, coexist. We detail the most important features of heterogeneous networks. We conclude the book by providing new research directions and open problems of PLC. Throughout the book, we compare Wi-Fi and PLC, as they are technologies often used simultaneously in heterogeneous networks. The PHY and MAC layers of PLC have differences that can benefit the network in terms of coverage, throughput, latency, and security.

The book can be useful for PLC researchers, users who would like to optimize PLC performance, engineers working on new PLC devices, and computer networking classes. Our book is intended for both a general audience with little networking background and an advanced audience with a Wi-Fi, PLC, or networking background. To distinguish the parts of the book for the advanced audience, we introduce sections for further reading using the symbol. The book is also intended to be used as a guide for PLC testbed development, configuration, and measurement. When applicable, we provide experimental guidelines to reproduce our results or network configurations using the symbol.

This book is a product of eight years of research on PLC; a significant part of this research was carried out under the supervision of Professor Patrick Thiran and Professor Albert Banchs. We thank them for their guidance and advice on Chapters 5 and 6. Patrick supervised our theses and helped us with the analysis and performance evaluation of PLC. Albert has helped us with the throughput model of the PLC MAC layer. The performance evaluation of PLC was done at École polytechnique fédérale de Lausanne (EPFL), Switzerland, on a testbed that Julien Herzen had initially developed for Wi-Fi networks. We thank Julien for his help with the testbed and the inauguration of PLC devices on it. Finally, we thank Can Karakuş for his feedback on the book.

We hope that the book will serve as a practical guide on teaching PLC, new research directions on PLC, and development of new PLC commercial devices.

Cambridge University Press & Assessment
978-1-108-83548-0 — A Practical Guide to Power Line Communications
Christina Vlachou , Sébastien Henri
Frontmatter
More Information

Abbreviations

AC alternating current
ACK acknowledgment
AES advanced encryption standard
AFE analog front end
AGC automatic gain control
ALME abstraction layer management entity
AP access point
ARP address resolution protocol
ARQ automatic repeat request
ASCII American standard code for information interchange
BBF bidirectional burst flag
BBT beacon backoff time
BC backoff counter
BDF beacon detect flag
BIFS burst interframe space
BLE bit loading estimate
bps bits per second
Bps bytes per second
BPSK binary phase-shift keying
CA channel access
CBC cypher block chaining
CCo central coordinator
CFP contention-free period
CFS contention-free session
CIFS contention interframe space
CMDU control message data unit
CMG CTS-MPDU gap
CP contention period
CRC cyclic redundancy check
CSC channel-switching cost
CSMA/CA carrier sense multiple access with collision avoidance
CTS clear to send

CW contention window
D/A digital-to-analog converter
DAK device access key
dB decibel
dBm decibel of measured power referenced to one milliwatt
DC deferral counter
DPLL digital phase-locked loop
DPW device password
DSNA device-based security network association
DTEI destination terminal equipment identifier
EIFS extended interframe space
EKS encryption key select
EMI electromagnetic interference
EPFL École polytechnique fédérale de Lausanne
ETH Ethernet
ETT expected transmission time
ETX expected transmission count
FC frame control
FCCS frame control check sequence
FDM frequency division multiplexing
FEC forward error correction
FFT fast Fourier transform
FID fragment identifier
FL frame length
Gbps gigabits per second
G.hn specification for home networking
GHz gigahertz
GI guard interval
GP GreenPHY
GUI graphical user interface
HD high definition
HD-PLC high-definition power line communication alliance
HF high frequency
HLE higher layer (above MAC) entity
HPAV HomePlug AV
HPGP HomePlug Green PHY
Hz hertz
IARU International Amateur Radio Union
ICV integrity check value
IEEE Institute of Electrical and Electronics Engineers
IFFT inverse fast Fourier transform
IFS interframe space
IMC impedance mismatch compensation
IoT Internet of Things

IP Internet protocol
IPTV IP television
ISI intersymbol interference
ISP intersystem protocol
ITU International Telecommunication Union
ITU-T ITU Telecommunication Standardization Sector
IV initialization vector
kbps kilobits per second
KCD key carrying device
kHz kilohertz
LAN local area network
LDPC low-density parity check codes
LID link identifier
LLDP link layer discovery protocol
LN logical network
LTE long-term evolution 4G mobile communications standard
m meters
MAC medium-access control
Mbps megabits per second
MCF multicast flag
MCS modulation and coding scheme
MHz megahertz
MID message identifier
MIMO multiple input and multiple output
MLME MAC layer management entity
MM management message
MNBC multinetwork broadcast
MNBF multinetwork broadcast flag
MoCA Multimedia over Coax Alliance
MPDU MAC protocol data unit
MPTCP transport control protocol
MRTFL maximum reverse transmission frame length
ms millisecond
μs microsecond
MSDU MAC service data unit
NEK network encryption key
NFCNK near-field communication network key
NID network identifier
NMK network membership key
NMK-SC network membership key – simple connect
NPW network password
NVRAM nonvolatile random access memory
OFDM orthogonal frequency-division multiplexing
OFDMA orthogonal frequency-division multiple access

PB physical block
PBC push-button configuration
PBCS physical block check sequence
PBKDF password-based key derivation function
PC personal computer
PCP priority code point
PE protective earth
PHY physical layer
PIB parameter information block
PKCS public-key cryptography standard
PLC power line communications
PLME physical layer management entity
PPB pending physical block
PPDU physical protocol data unit
PRS priority resolution slot
PSD power spectral density
QAM quadrature amplitude modulation
QoS quality of service
QPSK quadrature phase shift keying
QUIC Quick UDP Internet connections
RCG RTS/CTS gap
RF radio frequency
RI roll-off interval
RIFS response interframe space
ROBO robust modulation schemes for IEEE 1901
RSC recursive systematic convolutional
RSNA robust security network association
RSSI received signal strength indicator
RTS request to send
RTT round trip time
s second
SACK selective acknowledgment
SC simple connect
SHA secure hash algorithm
SIFS short interframe space
SISO single input and single output
SL security level
SME station management entity
SNID short network identifier
SNR signal over noise ratio
SoF start of frame
SSID service set identifier
SSN sequence segment number
STEI source terminal equipment identifier

SVD single-value decomposition
SWM sliding-window method
TCC turbo convolutional coder
TCP transport control protocol
TDM time division multiplexing
TDMA time division multiple access
TEI terminal equipment identifier
TEK temporary encryption key
TIA Telecommunications Industry Association
TLV type length value
TTL time-to-live
TV television
UCPK user-configured passphrase
UDP user datagram protocol
UIS user interface station
UKE unicast key exchange
UPA Universal Powerline Association
USA United States of America
USAI unassociated station advertisement interval
VLAN virtual local area network
VLC visible light communication
VoIP Voice over IP
WiMAX worldwide interoperability for microwave access
WPA Wi-Fi protected access
WPS Wi-Fi protected setup
WSC Wi-Fi simple configuration
XOR exclusive or