Advances in Information Security 108

Javier Hernandez Fernandez
Aymen Omri
Roberto Di Pietro

Physical Layer Security in Power Line Communications

Fundamentals, Models and Applications

Springer

Advances in Information Security

Volume 108

The purpose of the *Advances in Information Security* book series is to establish the state of the art and set the course for future research in information security. The scope of this series includes not only all aspects of computer, network security, and cryptography, but related areas, such as fault tolerance and software assurance. The series serves as a central source of reference for information security research and developments. The series aims to publish thorough and cohesive overviews on specific topics in Information Security, as well as works that are larger in scope than survey articles and that will contain more detailed background information. The series also provides a single point of coverage of advanced and timely topics and a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook.

Javier Hernandez Fernandez • Aymen Omri •
Roberto Di Pietro

Physical Layer Security in Power Line Communications

Fundamentals, Models and Applications

Springer

Javier Hernandez Fernandez
Iberdrola Innovation Middle East
Doha Qatar, Qatar

Aymen Omri
Iberdrola Innovation Middle East
Doha Qatar, Qatar

Roberto Di Pietro
CEMSE Division
King Abduallah University of Science and Technology (KAUST)
Thuwal, Saudi Arabia

ISSN 1568-2633 ISSN 2512-2193 (electronic)
Advances in Information Security
ISBN 978-3-031-57348-4 ISBN 978-3-031-57349-1 (eBook)
https://doi.org/10.1007/978-3-031-57349-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To our dear families.

Foreword

Power line communications (PLC) has drawn increasing interest in recent years due to its potential to provide wireline communications services using existing power-line infrastructure. A key issue arising in the use of PLC is that power-line infrastructure was not designed originally for communications purposes and, as an open medium, is generally not secured against potential eavesdropping and other security breaches. Physical layer security (PLS) has emerged in recent years as an alternative or companion technology to more traditional methods of communications security, especially for securing networks of low-complexity devices such as those envisioned for many applications of PLC. Consequently, there has been a considerable amount of work on the application of PLS in PLC in recent years, and this book provides, for the first time, a comprehensive treatment of the state-the-art of this field. It also serves as a very useful introduction to PLC itself, with the initial chapters providing a concise review of the state-of-the art in PLC. By examining the entire range of issues arising in this context, the authors provide readers with the tools to understand and potentially develop PLS techniques for application in PLC networks. This book is an excellent resource for those interested in learning about the potential of PLS to help secure PLC networks, and for those who merely want to learn more about PLC technology. Its breadth and depth of coverage, and its expert insights, make it a singular contribution to the field.

Princeton, NJ, USA
December, 2023

H. Vincent Poor
Michael Henry Strater University Professor
Princeton University

Preface

We live in an ever increasingly interconnected and digitally dependent world, where the critical infrastructure that sustains our modern way of life still shows a worrying degree of vulnerability. In this scenario, the power line communications (PLC) technology and associated paradigms have the potential to emerge as a linchpin, serving as the nervous system that facilitates the seamless flow of information between various components of our energy grid. Moreover, given their pervasiveness, their possible usages are yet to be fully discovered. For instance, PLC could be the silver bullet to provide IoT with the long-sought connectivity grail, or being an enabler for the edge cloud.

Whatever the usages will be, already today, in the realm of PLC, given the convergence of power systems and communication technologies, robust security measures are a pre-requisite—though intertwined with challenges and constraints.

We felt the need to produce this book in an attempt to both unravel the complexities and safeguard the confidentiality, integrity, and availability of power line communications. In particular, we intended to not only clarify the fundamental principles of physical layer security in PLC, but also to provide practical insights into mitigating risks and fortifying resilience.

This book is intended for engineers, researchers, and practitioners struggling with the multifaceted dimensions of cybersecurity in our energy infrastructure. The clarity of the language is accompanied by a rigorous treatment of the topics, and findings are supported by extensive simulations, showing the viability of the several offered solutions, also through the exposition of compelling use cases.

We hope our readers will find this book useful and inspiring, enjoying it at least as much as we enjoyed the research journey that has led to its publication.

Doha, Qatar — Javier Hernandez Fernandez
Doha, Qatar — Aymen Omri
Jeddah, Saudi Arabia — Roberto Di Pietro
May, 2024

Acknowledgments

We extend our gratitude to Iberdrola for their support.

Additionally, we acknowledge the valuable assistance of our colleagues Dr. Gabriele Oligeri, Muhammad Irfan, Abdulah Youssef Jarouf, Ayman Al-Kababji, Dr. Imene Mecheter, and Mohammad Khorasani.

Contents

Acronyms

AMI	Advanced Metering Infrastructure
ARIB	Association of Radio Industries and Businesses
ASC	Average Secrecy Capacity
AWGN	Additive White Gaussian Noise
BB-PLC	Broadband Power Line Communication
BER	Bit-Error Rate
BGR	Bit Generation Rate
BMR	Bit Mismatch Rate
BPSK	Binary Phase Shift Keying
CDR	Connection Detection Rate
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPRI	China Electric Power Research Institute
CFR	Channel Frequency Response
CIR	Channel Impulse Response
CNN	Convolutional Neural Network
CSI	Channel State Information
CSRF	Cross-Site Reference Forgery
CSS	Cross-Site Scripting
CTF	Channel Transfer Function
CUSUM	Cumulative Sum Control Chart
DAA	Destination Address Alteration
DAK	Direct Access Key
DCSK	Differential Chaos Shift Keying
DER	Distributed Energy Resource
DES	Data Encryption Standard
DFC	Dynamic Flow Concept
DL	Deep Learning
DNS	Domain Name System
DoS	Denial of Service
DSO	Distribution System Operator

EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EST	Effective Secrecy Throughput
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
FCC	Federal Communications Commission
FDD	Frequency-Division Duplexing
FDR	Frequency Domain Reflectometry
FIR	Finite Impulse Response
FNDP	False Negative Detection Probability
FPDP	False Positive Detection Probability
G.hn	Gigabit Home Networking
G.hn-MIMO	Gigabit Home Networking-Multiple-Input and Multiple-Output
G3-PLC	3rd Generation Power Line Communication
HAN	Home Area Networks
HD-PLC	High Definition-Power Line Communication
HIF	High Impedance Fault
IBFD	In-Band Full-Duplex
IDA	Information Dispersal Algorithm
IDFT	Inverse Discrete Fourier Transform
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISP	Internet Service Providers
ITU	International Telecommunication Union
KDR	Key Disagreement Rate
KGR	Key Generation Rate
LF SGPLC	Low Frequency Smart Grid Power Line Communications
LO	Length Overflow
MAC	Medium Access Control
MF SGPLC	Medium Frequency Smart Grid Power Line Communications
MIMO	Multiple-Input and Multiple-Output
NAN	Near-me Area Network
NB-PLC	Narrowband Power Line Communication
NDSO	National Standard Developing Organizations
NEK	Network Encryption Key
NMK	Network Membership Key
NOMA	Non-Orthogonal Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
PDF	Probability Distribution Function
PER	Packet Error Rate
PHEV	Plug-in Hybrid Electric Vehicle
PKI	Public Key Infrastructure
PL	Power Line

PL ID	Physical Layer Identification
PLC	Power Line Communication
PLM	Power Line Modem
PLS	Physical Layer Security
PNR	Passive Network Reconnaissance
PRIME	Power Line Intelligent Metering Evolution
RC	Rogue Commands
RF	Radio Frequency
RGB	Red Green Blue
RI	Rogue Interloper
RSA	Rivest Shamir Adleman
RSSI	Received Signal Strength Indicators
SC	Secrecy Capacity
SDO	Standard Development Organization
SDP	Successful Detection Probability
SEE	Secrecy Energy Efficiency
SEM	Standard Error of the Mean
SINR	Signal-to-Interference-Plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SPDG	Successful Path Detection Gain
SPDP	Successful Path Detection Probability
SQLi	Structured Query Language Injection
SR	Secrecy Rate
SSTP	Secure and Successful Transmission Probability
ST	Secrecy Throughput
TDD	Time-Division Duplexing
TDoA	Time Difference of Arrival
TEM	Transverse Electromagnetic
TL	Transmission Line
ToA	Time of Arrival
TSM	Transport Sequence Modification
UF	Unavailable Function
UNB-PLC	Ultra Narrowband Power Line Communication
VCIR	Virtual Channel Impulse Response
WCR	Wiretap Code Rate

Chapter 1
Introduction

Abstract Although Power Line Communication (PLC) technology has a long history, its broader acceptance and deployment have only gained momentum in recent years, primarily due to its applications in industrial settings. For years, various standardization organizations and industrial associations have been working towards making PLC a widely accepted and secure communication technology. Despite its quick adoption, there has not been much focus on the security of PLC, particularly regarding physical layer techniques, with current measures mostly relying on traditional cryptographic principles. This book provides an in-depth analysis of PLC Physical Layer Security (PLS), examining its techniques, features, and limitations. It also introduces novel metrics and reviews existing ones to deliver a comprehensive security performance assessment of PLC networks. This introductory chapter presents an overview of PLS in PLC and outlines the structure and scope of the remaining chapters of the book.

1.1 Power Line Communication

The Power Line Communication (PLC) industry has seen tremendous advances in the past few years. Fueled by the deployment of smart meters and the rise of the Internet of Things (IoT), PLC technology has experienced a significant growth spurt. At the same time, advances in communication technologies have enabled wider and higher-throughput networks, which can support numerous applications beyond metering and monitoring. For those applications that rely on PLC networks, the opportunities for novel uses of such technologies have ushered in a new era where previously unthinkable implementations are becoming increasingly common.

The potential of PLC comes from its ability to leverage existing power lines and wiring infrastructure for data transmission. This makes it cost-effective and reliable compared to other wired or wireless communication systems. Moreover, the introduction of multiple protocols, such as Power Line Intelligent Metering Evolution (PRIME) or G.hn, has made deploying PLC increasingly easier. As a piece of evidence, a 2022 report indicated that the deployment of smart meters in the

J. Hernandez Fernandez et al., *Physical Layer Security in Power Line Communications*, Advances in Information Security 108,
https://doi.org/10.1007/978-3-031-57349-1_1