Data-Driven Modeling of Cyber-Physical Systems using Side-Channel Analysis

Sujit Rokka Chhetri
Mohammad Abdullah Al Faruque

Data-Driven Modeling of Cyber-Physical Systems using Side-Channel Analysis

Springer

Sujit Rokka Chhetri
Department of Electrical Engineering
and Computer Science
University of California
Irvine, CA, USA

Mohammad Abdullah Al Faruque
Department of Electrical Engineering
and Computer Science (EECS)
University of California
Irvine, CA, USA

ISBN 978-3-030-37961-2 ISBN 978-3-030-37962-9 (eBook)
https://doi.org/10.1007/978-3-030-37962-9

We dedicate this book to our family.

Preface

Cyber-physical systems (CPS) consist of a unique integration of discrete cyber-domain processes and continuous physical domain components. Current modeling approaches use extensive first-principle approaches to derive the various components of CPS. However, it is difficult to model some of the stochastic phenomenon (such as environmental variation, physical process variation, etc.) of CPS using the first-principle approach. Hence, in this book we have explored a data-driven modeling approach for CPS and present various methodologies for modeling security and creating virtual replica or digital twin of the physical system. Furthermore, we will also present new algorithms to handle complex non-Euclidean data for modeling the CPS. More specifically, the book will present and exploration of the unintended emissions from the physical domain of the CPS to infer various cyber-domain states.

This book provides a new perspective on modeling the cyber-physical system using a data-driven approach. It covers the use of state-of-the-art machine learning and artificial intelligence algorithms for modeling various aspects of the CPS. It provides insight on how a data-driven modeling approach can be utilized to take advantage of the relation between the cyber and the physical domain of the CPS for aiding the first-principle approach in capturing the stochastic phenomenon affecting the CPS.

The books book provides a practical use case of the data-driven modeling approach for securing the CPS, presenting novel attack models, building and maintaining the digital twin of the physical system. Furthermore, it also provides novel data-driven algorithms to handle non-Euclidean data. In summary, this book presents a novel perspective for modeling the CPS.

The first-principle based approach for modeling the CPS is complex and time-consuming. Below we present three major reasons for proposing a new book in this area:

- Due to the advancement of machine learning and artificial intelligence algorithms, there has been a huge leap in performing data-driven modeling. However, to the best of our knowledge, there are no books covering the data-driven modeling of the CPS to aid in capturing the stochastic phenomenon affecting CPS.

- The book presents some practical application for securing the CPS as well as building the digital twin of the physical twin of CPS. The digital twin is expected to be one of the pillars for next generation of CPS. Hence, this book provides timely coverage of building and maintaining the digital twins of CPS.
- The book also provides novel algorithms for handling not just Euclidean data but also non-Euclidean data. These algorithms will thus demonstrate how the next generation of digital twins may be made more cognitive by allowing it to process and extract information from complex and higher dimensional data.

Some of the unique features of the book can be listed as follows:

- Only book covering the data-driven modeling of the CPS utilizing the unique relation between the cyber and the physical domain.
- Coverage of machine learning and artificial intelligence algorithms for data-driven modeling of the CPS.
- Practical use case of the data-driven modeling approach for security and building digital twin of the CPS.
- Well-structured and comprehensive book chapters covering the breadth and depth in data-driven modeling of CPS.

Irvine, CA, USA Sujit Rokka Chhetri
Irvine, CA, USA Mohammad Abdullah Al Faruque

Acknowledgments

We would like to thank all the current and past members of Advanced Integrated Cyber-Physical Systems (AICPS) lab at the University of California of Irvine for contributing to the research and content of this book. We are really grateful for your help and support.

Contents