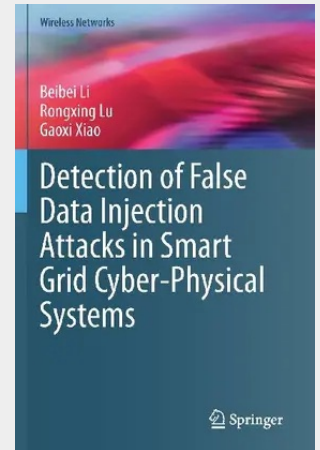


Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems

This book discusses cybersecurity issues of smart grid cyber-physical systems, focusing on the detection techniques against false data injection attacks. The authors discuss passive and proactive techniques that combat and mitigate two categories of false data injection attacks, false measurement data injections and false command data injections in smart grid cyber-physical systems. These techniques are easy to follow for either professionals or beginners. With this book, readers can quickly get an overview of this topic and get ideas of new solutions for false data injections in smart grid cyber-physical systems. Readers include researchers, academics, students, and professionals.

- Presents a comprehensive summary for the detection techniques of false data injection attacks in smart grid cyber-physical systems;
- Reviews false data injections for either measurement data or command data;
- Analyzes passive and proactive approaches to smart grid cyber-physical systems.

Introduction.- Foundations and Related Literature.- SPNTA: Stochastic Petri-Net-Based Reliability Analysis under Topology Attacks.- DHCD: Distributed Host-Based Collaborative Detection for FDI Attacks.- DDOA: Dirichlet-Based Detection for Opportunistic Attacks.- PFDD: On Feasibility and Limitations of Detecting FDI Attacks Using DFACTS.- Conclusion.



106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030586744
Medium: Buch
ISBN: 978-3-030-58674-4
Verlag: Springer
Erscheinungstermin: 07.11.2021
Sprache(n): Englisch
Auflage: 1. Auflage 2020
Serie: Wireless Networks
Produktform: Kartoniert
Gewicht: 277 g
Seiten: 157
Format (B x H): 155 x 235 mm

