Preface

Electrical energy storage is a key of modern and future life. The consumption of electrical energy (i.e. the use of air conditioning, audio and video devices or electric heating) is increasing every year due; firstly, to the increase of the population and secondly by the appearance of new form of consumption, such as electric cars. The dilemma with this increase consumption is, how to ensure the balance between supply and demand for electricity at all times? To address this problem, the idea of placing the new generation of smart grids to control this energy has appeared in recent literature in different flavors in order to provide electric power supply secure, sustainable and competitive to consumers. In addition, the revolution in smart grid involves a significant change in side of the consumer where consumers will also become producer with the ability of energy storage such as in the vehicle battery, or as a local generation sources such as photovoltaic panels.

The smart grid develops modern solutions for the next-generation network and digital communication in which many systems and subsystems are interconnected to provide services from end-to-end network between various actors and between intelligent devices that are deployed there. Within each network, a hierarchical structure is composed of different types of networks, such as the HANs (Home Area Networks), the BANs (Building Area Networks), the IANs (Industrial Area Networks), the NANs (Neighborhood Area Networks), the FANs (Field Area Networks), and the WANs (Wide Area Networks). In addition, large societies propose the use of cloud computing in smart grid applications connected with the electrical control center.

The main problem in the development of a smart grid is not located at the physical medium but mainly in delivery of reliability and security. The possibility of fitting with active or passive attacks in smart grid network is great to divulge privacy and disrupt energy (e.g. Wormhole Attack, False Data Injection Attack, Black Hole Attack, Grey Hole Attack, DoS Attack, Physical Layer Attack, Colluding Adversary Attack, Routing Table Overflow Attack etc.). Therefore, the security requirements, including authentication, accountability, integrity, non-repudiation, access control and confidentiality should be paid more attention in the future for high performance smart grids. This book will cover the current scope of various methodologies and mechanisms in the theory and practice of security, privacy, intrusion detection, and applied cryptography in smart grid communications in one place.

This book is organized as follows:

- Section 1 introduces the vulnerabilities, threats, and attacks in smart grid communications;
- Section 2 deals with authentication, privacy, and interoperability in smart grid communications;
- Section 3 presents intrusion detection systems and cryptography solutions for securing smart grid communications;
- Section 4 discusses smart energy and network management in smart grid.
In more detail:


This book aims to be an essential reference source, building on the available literature in the field of smart grid security in developing countries while providing for further research opportunities in this dynamic field. We hope it serves as a reference for technology developers and managers to adopt and implement smart grid platforms in developing nations across the globe.

Mohamed Amine Ferrag  
Guelma University, Algeria

Ahmed Ahmim  
University of Larbi Tebessi, Algeria