Computers and Electrical Engineering 000 (2018) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Cyber-security in smart grid: Survey and challenges☆

Zakaria El Mrabet[a,b,*], Naima Kaabouch[a], Hassan El Ghazi[b], Hamid El Ghazi[b]

[a] Department of Electrical Engineering, Upson Hall II, University of North Dakota, 243 Centennial Drive, Grand Forks, ND 58202, USA
[b] STRS Lab, National Institute of Posts and Telecommunication, Rabat, Morocco

ARTICLE INFO

Article history:
Received 12 May 2017
Revised 12 January 2018
Accepted 12 January 2018
Available online xxx

Keywords:
Smart grid
Cyber-attacks
Vulnerabilities
Confidentiality
Availability
Integrity
Accountability
Intrusion detection system
Cryptography
Network security

ABSTRACT

Smart grid uses the power of information technology to intelligently deliver energy by using a two-way communication and wisely meet the environmental requirements by facilitating the integration of green technologies. The inherent weakness of communication technology has exposed the system to numerous security threats. Several survey papers have discussed these problems and their countermeasures. However, most of these papers classified attacks based on confidentiality, integrity, and availability, but they excluded the accountability. In addition, the existing countermeasures focus on countering some specific attacks or protecting some specific components, but there is no global approach to secure the entire system. In this paper, we review the security requirements, provide descriptions of several severe cyber-attacks, and propose a cyber-security strategy to detect and counter these attacks. Lastly, we provide some future research directions.

1. Introduction

Traditional electrical distribution systems are used to transport electrical energy generated at a central power plant by increasing voltage levels and then delivering it to the end users by reducing voltage levels gradually. However, this electricity grid has major shortcomings, including the inability to include diverse generation sources such as green energy, high cost and expensive assets, time-consuming demand response, high carbon emission, and blackouts. For example, a study conducted by researchers at the Berkeley National Laboratory in 2004 showed that power interruptions cost the American economy approximately $80 billion per year; other estimates indicate a higher cost of $150 billion per year [1]. It is evident that these critical problems cannot be addressed with existing electricity grid. Smart grid promises to provide flexibility and reliability by facilitating the integration of new power resources (such as renewable energy, wind, and solar energy), enabling corrective capabilities when failures occur, reducing carbon footprint, and reducing energy losses within the grid.

The smart grid is a system based on communication and information technology in the generation, delivery, and consumption of energy power. It uses the two-way flow of information to create an automated and widely distributed system that has new functionalities such as, real-time control, operational efficiency, grid resilience, and better integration of renew-

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. R. C. Poonia.

* Corresponding author: Department of Electrical Engineering, Upson Hall II, University of North Dakota, 243 Centennial Drive, Grand Forks, ND 58202, USA.

E-mail addresses: zakaria.elmrabet@ad.ndus.edu (Z.E. Mrabet), naima.kaabouch@engr.und.edu (N. Kaabouch), elghazi@inpt.ac.ma (H.E. Ghazi), h.elghazi@inpt.ac.ma (H.E. Ghazi).

https://doi.org/10.1016/j.compeleceng.2018.01.015
0045-7906/

able technology which will decrease carbon footprint [2]. However, risks can still exist in the smart grid. Any interruptions in power generation could disturb smart grid stability and could potentially have large socio-economic impacts. In addition, as valuable data are exchanged among smart grid systems, theft or alteration of this data could violate consumer privacy. Because of these weaknesses, smart grid has become the primary target of attackers [1], which attracted the attention of government, industry, and academia.

Several research papers have been published that provide an overview of the prevailing problems related to cyber security in smart grid infrastructure [3–7]. In [3], the authors presented a study of the challenges present in smart grid security. They classified attacks based upon the type of the network, namely, home area network (HAN), neighborhood area network (NAN), and wide area network (WAN). In addition, they presented the impact of each attack on the information security: confidentiality, integrity, and availability (CIA). In [4], the authors discussed security challenges in the smart grid system, especially those related to connectivity, trust, customer privacy, and software vulnerabilities. The authors provided also an overview of the existing security solutions, particularly network security, data security, key management, network security protocols, and compliance checks. Another study focused on public networks has been conducted in [5]. This paper described a protection framework of smart grid based on a public network. This framework was composed of three layers, main station, communication network, and terminals. In [6], the authors discussed the security requirements and possible threats on the smart grid. These threats were classified into three categories: people and policy, platform, and network threats. In [7], the authors classified attacks based on the CIA requirements, and they described several countermeasures, including network security, cryptographic, secure protocols, and secure architecture.

While these survey papers provide various classifications of attacks on smart grid, most of them are based on confidentiality, integrity, or availability. However, they excluded the accountability requirement which is another important criterion that ensures the tractability of every action performed by any entity in the system. In addition, blended and sophisticated attacks such as Stuxnet, Duqu, and Flame [1] can compromise all of the security parameters at the same time. Therefore, such attacks are usually excluded from these classification systems. Furthermore, countermeasures and security solutions were presented individually for each smart grid's component, and there is no global approach to combine all security mechanisms to secure the entire system.

This paper provides an overview of the current status and future directions of the smart grid cyber-security. The remainder of this paper is organized as follows. First, we present an overview of the smart grid's features, its conceptual model, key components, and network protocols. Next, we review cyber-security objectives in the smart grid and we describe a new classification of cyber-attacks based on a method used by hackers or penetration testers. This method allows one to better understand the process used by hackers to compromise the smart grid system security. Then, we propose a global cyber-security approach which includes a number of detection techniques and countermeasures to protect the entire system. Some challenges and future directions are discussed in the last section.

2. Smart grid overview

2.1. Smart grid's features

The main benefits expected from the smart grid are increasing grid resilience and improving environmental performance. Resilience indicates the capability of a given entity to resist unexpected events and recover quickly thereafter [1]. Today, grid resilience as a feature has become non-negotiable, especially when power interruptions can potentially impact the economy. Smart grid promises to provide flexibility and reliability by enabling additional dispersed power supply, facilitating the integration of new resources into the grid, and enabling corrective capabilities when failures occur. Moreover, smart grid systems are expected to enable electric vehicles as replacements for conventional vehicles, reducing energy used by customers and reducing energy losses within the grid.

2.2. Smart grid's conceptual model

According to the National Institute of Standard and Technology (NIST) [2], a smart grid is composed of seven logical domains: bulk generation, transmission, distribution, customer, markets, service provider, and operations, each of which includes both actors and applications. Actors are programs, devices, and systems whereas applications are tasks performed by one actor or more in each domain. Fig. 1 shows the conceptual model of smart grid and the interaction of actors from different domains via a secure channel.

Within the customer domain, the main actor is the end user. Generally, there are three types of customers: home, commercial/building, and industrial. In addition to consuming electricity, these actors may also generate, store, and manage the use of energy. This domain is electrically connected to the distribution domain and communicates with the distribution, operation, service provider, and market domains [2].

In the market domain, actors are the operators and participants in the electricity markets. This domain maintains the balance between electrical supply and the demand. In order to match the production with demand, the market domain communicates with energy supply domains which include the bulk generation domain and distributed energy resources (DER) [2]. The service provider domain includes the organizations that provide services to both electrical customers and utilities. These organizations manage services such as billing, customer account, and use of energy. The service provider

Please cite this article as: Z.E. Mrabet et al., Cyber-security in smart grid: Survey and challenges, Computers and Electrical Engineering (2018), https://doi.org/10.1016/j.compeleceng.2018.01.015