Computers and Electrical Engineering 68 (2018) 499–512

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An efficient Intrusion Detection System against cyber-physical attacks in the smart grid☆

Mohamed Attia[a,*], Sidi Mohammed Senouci[a], Hichem Sedjelmaci[b], El-Hassane Aglzim[a], Daniela Chrenko[c]

[a] DRIVE EA1859, University of Bourgogne Franche-Comté, Nevers F58000, France
[b] IRT SystemX, Paris-Saclay, France
[c] University of Technology at Belfort-Montbéliard, Belfort 90010, France

ARTICLE INFO

Keywords:
Intrusion Detection System (IDS)
State estimation
Smart grid
DoS attack
Price manipulation attack

ABSTRACT

Without robust security mechanisms, the smart grid remains vulnerable to many attacks that can cause serious damages. Since state estimation is a critical entity to monitor and control electricity production and distribution, intruders are more attracted by this entity in order to disrupt the smart grid reliability. In this context, we propose an Intrusion Detection System (IDS) architecture to detect lethal attacks with a focus on two smart grid security issues: (i) Firstly, against integrity issue with price manipulation attack, we propose a Cumulative Sum (CUSUM) algorithm that detects this attack even with granular price changes; (ii) Secondly, the availability issue with Denial of Service (DoS) attack against which we develop an efficient method to monitor and detect any misbehaving node. Performance evaluations show the robustness of the proposed IDS system compared to existing mechanisms. The achieved detection rate is above 95% and the false positive rate is below 5%.

1. Introduction

Today, electric power distribution is made possible by the power distribution grid; a system of transmission mediums that allows electricity to be transferred from the point of generation to consumers like homes, offices or industries. The electrical grid is expected to evolve to a new grid paradigm: the smart grid that uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network. A smart grid is an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers, and those that do both – in order to optimize the production, supply as well as the consumption of electricity and provide several features to its customers [1]. This smartness comes from the usage of Information and Communication Technologies (ICT) [2], where data is exchanged between three main levels, as described with more details in the proposed architecture in Section 3. The first level is Home Area Network (HAN), which is composed by consumer's appliances like smart meters and connected devices. The second level, known as Neighborhood Area Network (NAN), is the aggregator where consumers' information is aggregated to be transmitted to the upper level. Finally, the last level is the control center where all data are analyzed.

Though, all smart grid features and advantages will be useless if this system is highly vulnerable to different kinds of attacks that

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. N. K. Yadhav.

* Corresponding author.
E-mail addresses: mohamed.attia@u-bourgogne.fr (M. Attia), Sidi-Mohammed.Senouci@u-bourgogne.fr (S.M. Senouci), hichem.sedjelmaci@irt-systemx.fr (H. Sedjelmaci), el-hassane.aglzim@u-bourgogne.fr (E.-H. Aglzim), daniela.chrenko@utbm.fr (D. Chrenko).

https://doi.org/10.1016/j.compeleceng.2018.05.006
Received 30 September 2017; Received in revised form 3 May 2018; Accepted 4 May 2018

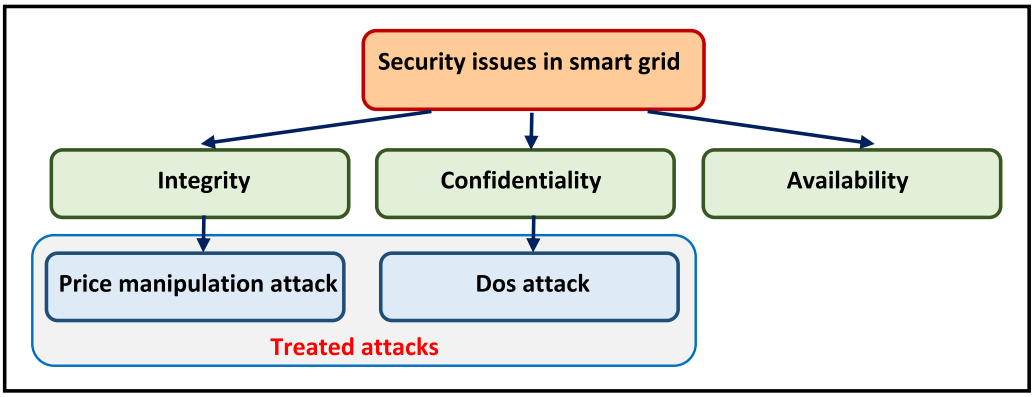

Fig. 1. Security issues in smart grid and classification of treated attacks.

can turn those features to catastrophic results beginning by non-satisfying consumers' needs, disrupting the electricity grid and in some cases causing serious physical damages to the utility grid or even intermediate stakeholders and end consumers' equipment [3].

As shown in Fig. 1, three main security objectives should be addressed in the smart grid: availability, integrity and confidentiality [4,5]. Among lethal attacks targeting availability in smart grid, there are *traffic flooding*, where the attacker aims to delay message transmission [6], *buffer flooding*, in which the intruder sends many false events in order to flood the aggregator's buffer [7] and *jamming attack,* where the attacker jams the power price for a period to make a great change in consumers' behavior [8]. All those attacks are categorized as *Denial-of-Service (DoS) attacks* where intruders aim to degrade the communication performance and prevent different stakeholders from useful information [9]. Besides, the control center will be unable to extract proper estimation of the electricity consumed and then will be pushed to take wrong decisions to produce energy and supply it to the appropriate regions.

Concerning confidentiality issue, there are many attacks presented in literature like eavesdropping communication channels in power networks to intercept useful data using traffic analyzers [10] or wiretappers (i.e. equipment used to eavesdrop channels) [11]. For the integrity issue, *false data injection (FDI) attacks* are heavily threatening the smart grid and can be introduced at different levels. For example, we mention *load redistribution attack* where the attacker compromises critical nodes to alter the load distribution and make serious damages [12]. Furthermore, *price manipulation attack* is one of the stealthy attacks that can occur and threat the smart grid information integrity and has a dangerous effect on the demand response equilibrium. This attack can cause huge changes in the demanded and/or consumed power, which may disorder the smart grid stability [13]. This kind of attack is known under different names in the literature like price information falsification [13], fabrication of price messages and false price injection [14].

With these kinds of attacks, the attacker may act in three levels: first, the attacker may target the control center or pretend that he is the control center and send a fake pricing. However, this task is not easy to the attacker since the control center is strongly robust against attacks because of its paramount role to collect information and make decisions. Furthermore, it has a huge computation capacity and can therefore integrate sophisticated security algorithms. That is why, it is fair to consider that this entity is trustful and cannot be threatened. Second, the attacker can target the aggregator node where he can alter the price information or block access to this node and thereafter create a fake access point. Third, the attacker can act at the level of the customer site by modifying the pricing information in the smart meter. This disturbance can be made by either the modification of *price information* or a *jamming attack* where the intruder can prevent the customer from receiving the right price information [9]. These kinds of attacks can cause many problems like lines failure [14] or financial losses [15].

The state estimation is a paramount entity that enhances the efficiency and reliability of the smart grid. It provides the estimation of the electricity production and consumption states in real time based on meter measurements. For this reason, we focus our work to deal with attacks that target especially the state estimation since they are lethal and can make greater damages compared to other attacks [16]. Hence, this paper focuses on *price manipulation attack* and develops a detection model based on Cumulative Sum (CUSUM: a sequential analysis technique used for monitoring change detection) algorithm. Moreover, an abnormal behavior detection algorithm is proposed to identify *DoS attacks*. Our added value draws its strength from the fine selection of the algorithm parameters obtaining a high accuracy rate. Furthermore, the proposed models rely on a lightweight detection algorithm since it is based on simple but efficient rules and equations to fit with all nodes especially those with restricted computation capacity like smart meters.

The main contributions in this paper are summarized as follows:

- A taxonomy is constructed to classify attacks targeting integrity and availability in smart grid.
- A new smart gird architecture with hierarchical IDS agents deployment is proposed.
- A *price manipulation attack* detection algorithm is developed based on CUSUM algorithm. It can detect this attack even with granular price change, which is not possible using traditional security mechanisms.
- An efficient method is developed to monitor and detect any misbehaving node to counter *DoS attacks*.

The remainder of this paper is organized as follows: an overview of the related works is presented in Section 2. Section 3