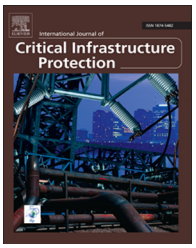
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Exposing vulnerabilities in electric power grids: An experimental approach

*Luigi Coppolino**, Salvatore D'Antonio, Luigi Romano*

University of Naples "Parthenope," Centro Direzionale di Napoli Is. C4, 80143 Naples, Italy

ARTICLE INFO

Article history:
Received 6 December 2012
Received in revised form
29 November 2013
Accepted 23 January 2014
Available online 30 January 2014

Keywords:
Smart grids
Phasor measurement units
Synchrophasors
Phasor data concentrators
Security assessment

ABSTRACT

During the past few years, coordinated and targeted cyber attacks of unprecedented levels of sophistication have been conducted against critical infrastructures. Simple experiments and probes are now turning into concerted cyber operations, carried out for profit or political reasons. Examples of critical infrastructures include airports, railway networks, hospitals, energy plants and networks and dams. Among these, electric power grids are possibly the most critical assets, since virtually all the critical infrastructures strongly depend on power distribution networks for their operation. To improve the accuracy and coherence of supervisory control and data acquisition/energy management systems (SCADA/EMSs), utility operators are increasingly integrating emerging technologies for power data collection. This paper presents the results of a thorough security analysis of two key enabling technologies used for data collection in power grids: (i) phasor measurement units (PMUs) also known as synchrophasors and (ii) phasor data concentrators (PDCs). Evidence is provided to demonstrate that these technologies are vulnerable to traditional cyber attacks (due to weaknesses such as the lack of encrypted communications channels and weak password policies), as well as to emerging cyber attacks (due to the lack of input validation and sanitization).

1. Introduction

The principal security goals for information technology (IT) assets are confidentiality, integrity and availability of data, services and communications systems. In the case of smart grids, cyber security requirements are particularly challenging to implement because they are imposed by the power domain as well as by the IT domain. Security strategies for the smart grid must guarantee both the resilience of the power infrastructure and the privacy of consumer information. The U.S. National Institute of Standards and Technology (NIST) [26] has produced a report entitled "Guidelines for Smart Grid Cyber Security" that presents a cyber security strategy and architecture. The document identifies the following risks to the grid:

- Vulnerabilities and exposure to attacks and unintentional errors due to the increasing complexity of the grid.
- Novel vulnerabilities generated by the interconnection of different networks.
- Vulnerabilities and weaknesses caused by disruptions of the communications network and the introduction of malicious software/firmware and/or compromised hardware.
- Increased numbers of entry points and paths available for potential adversaries to exploit.

*Corresponding author.
E-mail address: luigi.coppolino@uniparthenope.it (L. Coppolino).

1874-5482/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2014.01.003

- Threats to data confidentiality and integrity caused by interconnected systems that can increase the amount of private information exposed and the risk when data are aggregated.
- New vulnerabilities introduced by the use of new technologies.
- Potential for compromise of data integrity, including customer privacy breaches due to increases in the collected data.

Reports by McAfee [16] and Symantec [31] discuss how critical infrastructures [1,6] are exposed to cyber attacks. The McAfee report describes "Night Dragon," a major hacking initiative originating from China that specifically targeted power grids. The NIST report [26] identifies a number of research and development themes that must be addressed in the near future; these include phasor measurement unit security and protection.

Phasor measurement units (PMUs) and phasor data concentrators (PDCs) are key technologies used for power grid monitoring. A PMU, also known as a synchrophasor, is a device that measures the electrical waves on a power grid using a common time source for synchronization. A PDC is a node where phasor data from a number of PMUs or PDCs are correlated and output as a single stream to other applications. An assessment of the status of the power distribution network can be obtained by correlating information collected by multiple PMUs deployed in a single power grid.

Power grids are rapidly evolving to smart grids. According to the European Commission [28], 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 efficiently deliver sustainable, economic and secure electricity supplies."

Smart grids support new paradigms for power generation, consumption and delivery by leveraging advanced information and communications technologies and frameworks. A smart grid network (Fig. 1) incorporates several functional units. Each consumer hosts a smart controller and meter that are connected to a collector node. The collector node receives inputs from several end-points and transmits them to a utility station via the Internet. The utility is in charge of transmitting data to the distribution and transmission systems, typically via an intranet connection. The utility interacts with consumers by commanding their smart controllers and meters.

Given that power grids are evolving towards smart grids, successful attacks against the IT layers of a power grid could have a dramatic impact in the future, when smart grid architectures will include reconfiguration mechanisms that trigger automated actions when anomalous behavior [5] is detected in a power grid [33]. In this context, ensuring the integrity of measurements is of paramount importance, since their alteration could result in incorrect reconfiguration actions, and possibly monetary losses and blackouts with unpredictable cascading effects that could affect multiple countries [7,9,15]. A key project that is investigating the use of synchrophasor technology for power grid monitoring is NASPI (NASPInet) [8], an effort involving the North American Electric Reliability Corporation (NERC) [18], the U.S. Department of Energy and North American consumers and utilities. Another project is the Frequency Monitoring Network (FNET) [34], which seeks to detect power system anomalies using frequency disturbance recorders (FDRs) and information management systems (IMSs).

This paper presents the results of a security analysis conducted on two key technologies that enable data collection in power grids, namely synchrophasor devices and PDCs.

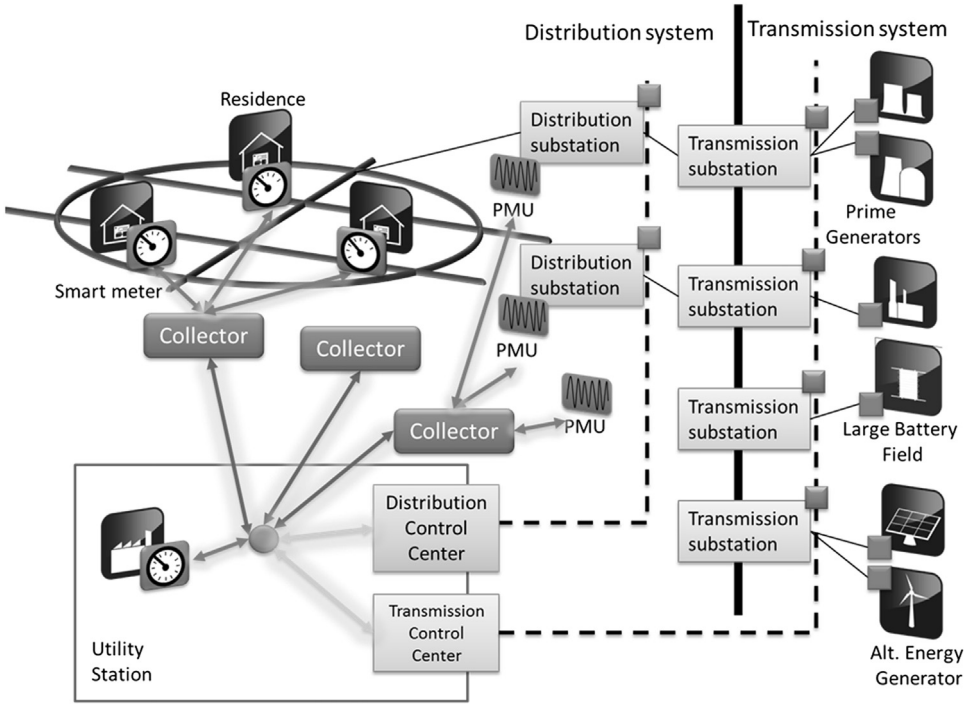


Fig. 1 – Schematic representation of a smart grid.