Chapter 5
Early Detection and Recovery Measures for Smart Grid Cyber-Resilience

Ismail Butun
https://orcid.org/0000-0002-1723-5741
Chalmers University of Technology, Sweden & Konya Food and Agriculture University, Turkey & Royal University of Technology, Sweden

Alparslan Sari
University of Delaware, USA

ABSTRACT

The internet of things (IoT) has recently brought major technological advances in many domains, including the smart grid. Despite the simplicity and efficiency that IoT brings, there are also underlying risks that are slowing down its adoption. These risks are caused by the presence of legacy systems inside existing infrastructures that were built with no security in mind. In this chapter, the authors propose a method for early-stage detection of cyber-security incidents and protection against them through applicable security measures. This chapter introduces security techniques such as anomaly detection, threat investigation through a highly automated decision support system (DSS), as well as incident response and recovery for smart grid systems. The introduced framework can be applied to industrial environments such as cyber-threats targeting the production generator as well as the electricity smart meters, etc. The chapter also illustrates the framework's cyber-resilience against zero-day threats and its ability to distinguish between operational failures as well as cyber-security incidents.

DOI: 10.4018/978-1-7998-7468-3.ch005

INTRODUCTION

Cybersecurity has a very important role in information and computing technology (ICT) systems, such as ensuring the reliability and safety of the provided services. This is a non-trivial task hence cybersecurity of the systems is difficult to maintain and operate when compared to all other services being provided. One of the prominent reasons is that the traditional cyber-security solutions are becoming obsolete as many vulnerabilities are being discovered by hackers every day (such as in the case of Zero-day attacks) on the systems and networks that are being used today.

Apart from the ICT domain, cybersecurity in the power domain is even more important and difficult due to the diverse networking and communication technologies used which exposes the whole energy grid to be vulnerable to cyber-attacks and hacks. Recent history has taught us that cybersecurity in the power domain (including industrial networks) has utmost importance as the resulting failures and enforced accidents (cyber incidence-related disasters such as explosions) might be life-threatening to the people.

For instance, Stuxnet is a malware initially distributed over Microsoft (MS) Windows platforms. It became recognized after it attacked the Iranian nuclear reactor in June 2010. It attacked Siemens programmable logic controllers (PLCs) step-7 software through computers that are running MS Windows. Stuxnet specifically attacked the PLCs that are operating in Iranian nuclear facilities: 1) By gathering industrial systems' information, 2) initiating a sequence to cause centrifuges to enter in a super fast-spinning mode, 3) eventually the catastrophic events ended up by which the centrifuges have torn themselves apart and destroyed their surrounding structures (Karnouskos, 2011).

Smart Grid is also not resistant to cyber-attacks (Butun, dos Santos, 2020). It can be both targeted at the controller side (command capture attacks on electric utility providers) and distributor side (manipulation attacks on the billing). In a modern factory (e.g. that produces paper polishing material from marble dust), one can observe that several automated machinery equipments is armed with IIoT sensors and actuators for an illustration). Some of the equipment is mainly composed of: grinders, mixers, heaters, conveyor bands. These IIoT sensors and actuators facilitate mainly three functions (Forsström, 2018):

1. Digitized on-the-go remote monitoring and control of equipment.
2. Optimization of machines within a production line (monthly or annual) due to collected short/long-term process-related data.
3. Instant alarming and shutting down of the equipment in the case of emergency situations.