Chapter 42
Detecting Synchronization Signal Jamming Attacks for Cybersecurity in Cyber-Physical Energy Grid Systems

Danda B. Rawat
Howard University, USA

Brycent A. Chatfield
Georgia Southern University, USA

ABSTRACT

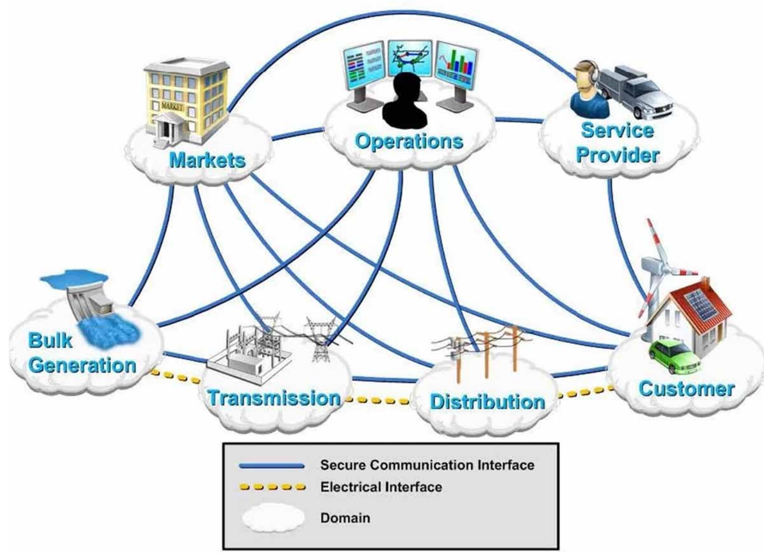
The transformation of the traditional power grid into a cyber physical smart energy grid brings significant improvement in terms of reliability, performance, and manageability. Most importantly, existing communication infrastructures such as LTE represent the backbone of smart grid functionality. Consequently, connected smart grids inherit vulnerabilities associated with the networks including denial of service attack by means of synchronization signal jamming. This chapter presents cybersecurity in cyber-physical energy grid systems to mitigate synchronization signal jamming attacks in LTE based smart grid communications.

INTRODUCTION

Traditional power grids undoubtedly play a critical role in the functioning of society. thus, common luxuries such as computers, cellular phones, tablets, television, music, and most importantly, power within homes are enjoyed daily. Energy demands by consumers, industries, and civilians alike, remain a daily challenge in terms of efficiency. There is no real-time interaction between consumers and utility providers in traditional energy grids. The transformation of traditional energy networks to cyber physical smart energy grids can assist in revolutionizing the energy industry in terms of reliability, performance, and manageability in almost real-time (Rawat, 2015, (Rawat, Rodrigues, & Stojmenovic, 2015)). In

DOI: 10.4018/978-1-7998-2466-4.ch042

Figure 1. Seven domains of smart cyber-physical grid
Source: NIST Smart Grid Model, 2010



cyber physical smart energy grid, there are seven domains associated with the design. These domains include: bulk generation, transmission, distribution, customer, markets, service provider, and operations as in Figure 1. The first four domains are to feature two-way power and information flow whereas the latter three consist of information collection and power management.

The vastness of the smart grid, as aforementioned, is a major parameter that must be orchestrated in a highly distributed and hierarchal manner to achieve efficient and reliable communication. Communications in cyber physical smart grid is divided into three tiers: Home Area Networks, Neighborhood Area Networks, and Wide Area Networks as shown in Figure 2.

A Home Area Network (HAN) consists of all appliances residing in a consumer's premise. Smart appliances within the premise transmit real-time power usage to a smart utility meter serving as the HAN gateway node. Real-time power usage along with pricing provided by utility companies grants consumers real-time insight of their power bill along with knowledge of which devices are consuming the most power.

Neighborhood Area Network (NAN) compiles all data transmitted from HANs. NAN provides the opportunity for utility companies to control end user devices, send real time commands, and control the distribution grid devices [2, 10, 11]. Another function of NAN is delivering information provided by HANs to Wide Area Networks (WAN).

WAN collects information from NANs to that is ultimately delivered to utility companies through variety of technologies such LTE cellular, WiMAX, etc. The WAN also cover power generation to transmission.

Drastic differences in latency requirement for the smart grid, in comparison to the internet, are indicative of how critical the delays are within the smart energy grid. Performance wise, internet focuses on high throughput and fairness amongst users. Power communication focuses to ensure reliable, secure, real-time message delivery instead of focusing on throughput.