# Attacks, vulnerabilities and security requirements in smart metering networks

ABSTRACT

A smart meter is one of the core components in Advanced Metering Infrastructure (AMI) that is responsible for providing effective control and monitor of electrical energy consumptions. The multifunction tasks that a smart meter carries out such as facilitating two-way communication between utility providers and consumers, managing metering data, delivering anomalies reports, analyzing fault and power quality, simply show that there are huge amount of data exchange in smart metering networks (SMNs). These data are prone to security threats due to high dependability of SMNs on Internet-based communication, which is highly insecure. Therefore, there is a need to identify all possible security threats over this network and propose suitable countermeasures for securing the communication between smart meters and utility provider office. This paper studies the architecture of the smart grid communication networks, focuses on smart metering networks and discusses how such networks can be vulnerable to security attacks. This paper also presents current mechanisms that have been used to secure the smart metering networks from specific type of attacks in SMNs. Moreover, we highlight several open issues related to the security and privacy of SMNs which we anticipate could serve as baseline for future research directions.

**Keyword**: Smart metering networks; Smart grid; Security attacks; Privacy