Advanced Metering Infrastructure Based on Smart Meters in Smart Grid

Trong Nghia Le, Wen-Long Chin,
Dang Khoa Truong and Tran Hiep Nguyen

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/63631

Abstract

Due to lack of situational awareness, automated analysis, poor visibility, and mechanical switches, today's electric power grid has been aging and ill-suited to the demand for electricity, which has gradually increased, in the twenty-first century. Besides, the global climate change and the greenhouse gas emissions on the Earth caused by the electricity industries, the growing population, one-way communication, equipment failures, energy storage problems, the capacity limitations of electricity generation, decrease in fossil fuels, and resilience problems put more stress on the existing power grid. Consequently, the smart grid (SG) has emerged to address these challenges. To realize the SG, an advanced metering infrastructure (AMI) based on smart meters is the most important key.

Keywords: advanced metering infrastructure, communications, security, smart grid, smart meters

1. Introduction

An electric power grid is a network of power generators, transmission lines, transformers, and distribution/relay systems to provide its consumers (residential, industrial, and commercial) with the power they need. Currently, electrical energy is generated in centralized power plants and transported over a long-distance transmission network to distribution networks before reaching the end consumers via communication and power flows in only one direction, i.e., from power plants to the customers, which is collectively called an electric grid. After many decades of development, it has been realized that various utilities can interconnect to achieve greater reliability of overall power system by compensating for unexpected failures as well as disconnections from power devices, i.e., transmission lines and generators.

In an electric grid, generation, transmission, and distribution of power should be precisely coordinated. **Figure 1** depicts various sections in today's electric grid, which consists of four areas that are generation, transmission, distribution, and customers [1]. Generation involves the production of electricity from energy sources such as wind and solar farms, coal plants, and hydroelectric dams. Because generators cannot be located too close to population centers for safety, legal, and financial reasons, the electric grid needs transmission lines to carry the electricity over long distances (often more than hundreds of miles). Distribution includes taking the electricity from transmission lines and delivering it to the customers. Typically, an electricity distribution system includes medium voltage power lines (below 50 kV), substations, and transformers, starting at the transmission substations and ending at the meters of customers. A substation consists of a bus to split up the power into different regions, step-down transformers, relays, and circuit breakers, which are designed to disconnect the substation from different distribution lines or from the power grid when necessary. The same transmission substation can deliver the power at different voltages to different regions, and the power might be further stepped down in several stages to reach 7200 V. A transformer is used to reduce voltage from 7200 to 240 V at each customer site. Two wires from the trans-

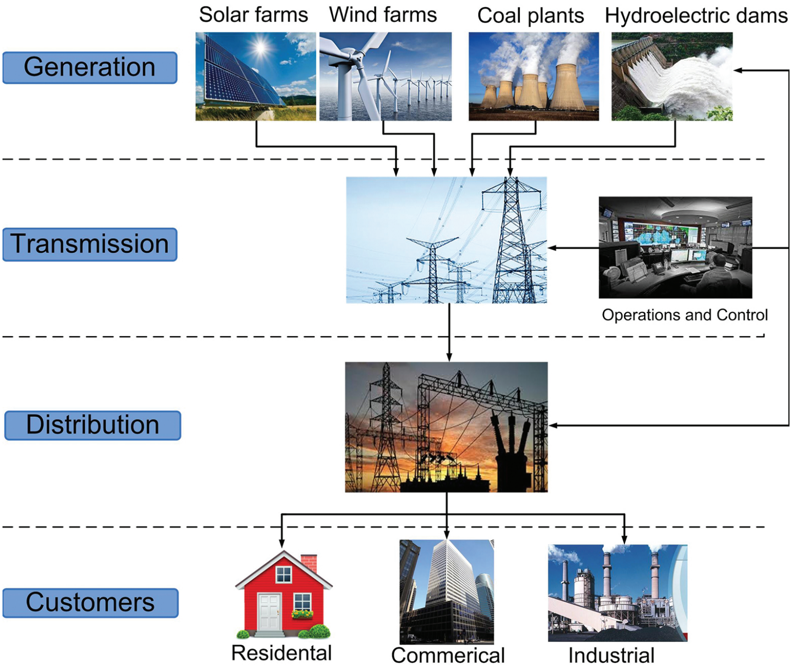

Figure 1. Typical electric power grid [1].

former are used to connect to power meters at a building or house, each carrying 120 V. These two wires are 180° out of phase, resulting in 240 V, which allows customers to use both 240 and 120 V appliances.

Due to the lack of situational awareness and automated analysis, today's electric power grid has been aging and ill-suited to the fast growing demand for electricity in the twenty-first century [2]. For example, in the United States, the consumption and demand for electricity have increased by 2.5% annually over the past 20 years [3]. Besides, the global climate change and greenhouse gas emissions on the Earth caused by the electricity and transportation industries [4] put more stress on the existing power grids. Consequently, a new concept of next-generation electric power system is urgently needed to address these challenges, which motivates the proposal of smart grid (SG).

The SG can be viewed as a superposition of communication networks on the electric grids. Hence, it can improve efficiency, reliability, safety, and security of electricity supply to the customers, with a seamless integration of renewable and alternative energy sources, such as photovoltaic systems, wind energy, biomass power generation, tidal power, small hydropower plants, and plug-in hybrid electric vehicles, through automated control and modern communications technologies [5]. In SG, various components in these four areas of the electric grid are linked together via two-way communications and power flows to provide interoperability among them. Thus, consumers can not only draw power but also supply surplus power to the grid using smart meters that enable monitoring and measuring of these bidirectional flows. This new infrastructure could potentially produce millions of alternate micro-energy sources and allow improved load balancing through instantaneous electricity demand information exchanges, which could help power plants match their output to demand with the help of information generated from metering, sensing, and monitoring.

To realize the SG, an advanced metering infrastructure (AMI) based on smart meters is the most important key. The AMI is the system that collects and analyzes data from smart meters using two-way communications, and giving intelligent management of various power-related applications and services based on that data. The AMI is the deployment of a metering solution with two-way communications to the electric meter. The implementation of AMI is widely seen as the first step in the digitalization of the electric grid control systems. Recently, AMI has gained great attraction in both industry and commerce due to the accurate improvement in online meter reading and control. The AMI is the architecture for automated two-way communications between smart utility meters and utility companies. The AMI includes smart meters, e.g., electric, gas, and heat meters, at customer premises, access points, communication backbone network between customer and service providers, and data management systems to measure, collect, manage, and analyze the data for further processing. The smart meter can identify power consumption in much more detail than a conventional meter and periodically send the collected information back to the utility company for load monitoring and billing purposes. Besides, the data from smart meter readings are also critical for the control center to implement Demand/Response mechanism. By using smart meters, customers can control their power consumption and manage how much power they are using, particularly managing the peak load. Hence, through customer participation, the utility companies can likely provide electricity at lower and even rates for all their customers, and the consequent carbon dioxide emission will decrease. Despite the increase in the utilization of AMI, there has been very little assessment or research and development effort to identify the security needs for such systems. Hence, the aim of this chapter is to offer a comprehensive description about AMI based on smart meters in SG. In addition, the issues on security, major challenges, and solutions in AMI in SG are also proposed.

2. Smart meter architecture

Smart meter is an advanced energy meter that supports two-way communications compared with a conventional energy meter. Hence, it can measure the energy consumption data of a consumer and then transmits added information to the utility companies to support decentralized generation sources and energy storage devices, and bill the customer accordingly. Besides, smart meters can receive information about electricity price and commands from utility companies and then deliver them to consumers. In practice, smart meters can read energy consumption information of customers in real time, such as values of voltage, frequency, and phase angle, and then they securely communicate the information to control centers. By using bidirectional communication of data, smart meters can collect information regarding the electricity consumption values of customer premises. Data collected by smart meters is a combination of parameters such as a unique meter identifier, timestamp of the data, and the electricity consumption values. Based on the information, smart meters can monitor and execute control commands for all home devices and appliances at the customer's premises remotely as well as locally. Besides, smart meters can communicate with other meters in their reach using home area network (HAN) to collect diagnostic information about appliances at the customer as well as the distribution grid. Moreover, smart meters can be programmed such that, only power consumed from the utility grid is billed whereas the power consumed from

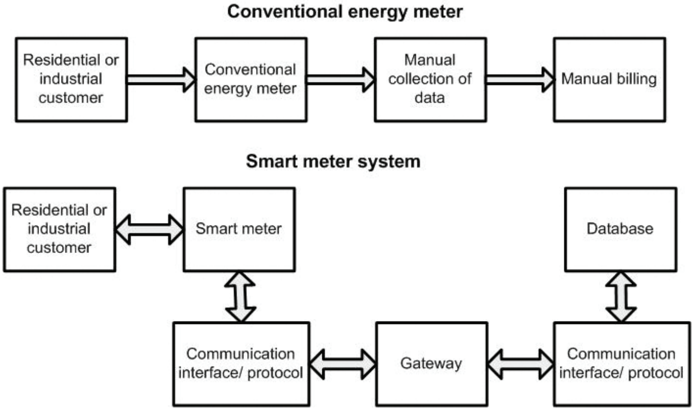
Conventional energy meter
Residential or industrial customer
Conventional energy meter
Manual collection of data
Manual billing
Smart meter system
Residential or industrial customer
Smart meter
Database
Communication interface/ protocol
Gateway
Communication interface/ protocol

Figure 2. Architectural model of conventional energy meter and smart meter.

the distributed generation sources or storage devices owned by the customers is not billed. As a result, they can limit the maximum electricity consumption, and can terminate or reconnect electricity supply to any customer remotely [6]. **Figure 2** shows an architectural model of a conventional energy meter and a smart meter.

A smart meter system includes various control devices and sensors to identify parameters and situations in SG and then it transfers the collected data to the control center or provides command signals to the devices in the home of customers. The collected electricity consumption data from all devices of customers on a regular basis helps the utility companies to manage electricity demand/response more efficiently and also to provide useful information to the customers about the cost-efficient methods to use their appliances. Besides, smart meters can be programmed to maintain a schedule for operation of the home devices and control operation of other appliances accordingly, i.e., to control light, heat up water in swimming pool, air conditioning, washing machine, and other appliances [7]. In addition, by integrating smart meters in electricity grid, utility companies can detect and identify electricity theft and unauthorized consumption in view of improving the power quality and distribution efficiency [8]. Hence, smart meters would play an extremely important role in monitoring the performance and the energy usage characteristics of the load on the electricity distribution grid in the future.

Typically, smart meters implement two major functions, which are communication and measurement [9]. Hence, each meter is equipped with two subsystems as communication and metrology, respectively. The communication part includes security and encryption that define the suitable data transmission approach. The metrology varies depending on multiple characters such as measured phenomenon, technical requirements, region, accuracy, applications, and level of data security. Regardless of the type or quantity of their measurement, smart meters should have six basic functionalities as mentioned [10], which include the following:

Quantitative measurement: Smart meters have to accurately measure the quantity of the medium by using various topologies, physical principles, and approaches.

Control and calibration: Smart meters should be providing ability to compensate the small variations according to each system type.

Security communication: The meters have ability receiving operational commands and sending stored data as well as upgrades for its firmware trustworthily.

Power management: Smart meters have to help the system to exactly maintain its functionality when the primary source of energy is lost.

Display: Smart meters will send and display information usage of electricity energy to customers for billing in real time. Besides, the information of real time consumption displayed on smart meters helps customers to manage their demand efficiently.

Synchronization: Typically, smart meters transmit data of customers to the collector systems or central hubs for billing and data analysis. Hence, timing synchronization is very important for reliable transmission of data, particularly in case of wireless communication.

As a result, based on smart meters, utility companies can provide highly reliable, readily accessible, flexible, and cost-effective energy services to their consumers by combining advantages of both small distributed power generators and large centralized generators. Moreover, demand side management techniques require that these companies have to collect large quantity of data from smart meters in real time. One of key components to implement this concept is advanced metering infrastructure, which collects and analyzes data from smart meters, and gives intelligent management of various power-related applications and services based on that data. In next section, we present AMI based on smart meters.

3. AMI based on smart meters in SG

3.1. AMI architecture

AMI is a main mechanism for the realization of other smart grid applications to deliver operational and business benefits across the utility. AMI is the system that collects and analyzes data from smart meters using two-way communications between user domain and utility domain, and gives intelligent management of various power-related applications and services based on that data. The implementation of AMI is widely seen as the first step in the digitalization of the electric grid control systems. AMI's main functionalities encompass power measurement facilities, assisting adaptive power pricing and demand side management, providing self-healing ability, and interfaces for other systems. Recently, AMI has gained great attraction in both industry and academia due to the accurate improvement in online meter reading and control. AMI helps for financial benefits, improved services, and opportunities for consideration of environmental concerns.

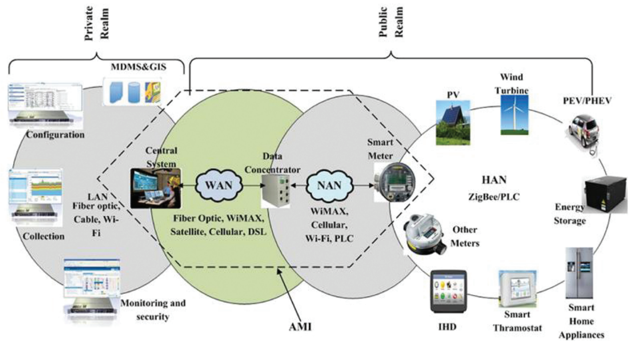

Figure 3. AMI overview architecture.

The AMI includes smart meters, e.g., electric, gas, and heat meters, at customer premises, access points, communication backbone networks between customers and service providers, and data management systems to measure, collect, manage, and analyze the data for further processes. These AMI components are usually located in various networks [11] and different realms such as public and private ones [12]. In AMI systems, smart meters are regarded as the key interfaces for physical, information, and social domains of the smart grid. **Figure 3** shows AMI overview architecture that is integrated in a broader context of power generation, transmission, distribution, and customer using HAN, neighborhood area network (NAN), and wide area network (WAN).

From this figure, we can see that the smart meter is a key device for consumers because it is responsible for monitoring and recording power consumption of home appliances. HAN provides connections between home appliances, other integrated systems such as rooftop photovoltaic system, distributed sensors, plug-in electric vehicle/plug-in hybrid electric vehicle, in-home display (IHD), smart thermostat, etc., and the smart meter. For communicating among these constituents, power line communications (PLCs) or wireless communications, such as ZigBee, 6LowPAN, Z-wave, and others can be utilized. NAN provides communication links between a number of individual smart meters and a data concentrator using WiMAX or cellular technologies. A number of data concentrators are connected to a central system (it also is called an AMI headend) in the utility side through WAN. Typically, WAN consists of two interconnected networks, i.e., the core networks and backhaul networks. The core networks provide connections to the control center and commonly use fiber optics or cellular networks to guarantee high data rates and low latency. The backhaul networks handle the broadband connections to NANs and monitoring devices. Applying cognitive radio (CR) technology in backhaul networks contributes to reducing the cost for investment and enhancing the flexibility, capacity, and coverage. Typically, the AMI headend, which is located in the utility side, includes geographic information system (GIS), configuration system, meter data management system (MDMS), etc. These subsystems can utilize a local area network (LAN) for intercommunication. In the next section, we present detail in AMI communications infrastructure.

3.2. AMI communications infrastructure

In AMI, the smart meter can identify power consumption in much more detail than a conventional meter and periodically send the collected information back to the utility company for load monitoring and billing purposes. In addition, the data from smart meter readings are also critical for the control center to implement demand response mechanisms. Using smart meters, customers can control their power consumption and manage how much power they are using, particularly managing the peak load. Hence, through customer participation, the utility companies can likely provide electricity at a lower rate for all their customers, and the consequent carbon dioxide emission will be decreased. Typically, existing AMIs collect data from smart meters and sensors with intervals of 15 min, the collected data are huge and important, and it is estimated that a moderately sized city with 2 million homes could generate 22 GB of meter data every day [13], and is referred to as "Big Data," easily overwhelming best planned data center capacity in a fairly short time. In particularly, MDMS with the analytical tools is considered the central module of the management system. Besides, MDMS has to ensure complete and accurate Big Data from customer to the management modules under possible interruptions at lower layers by performing validation, estimation and editing on the AMI data. Moreover, the distribution network automation system, which collects up to 30 samples per second per sensor for real-time control of SG [14], third-party systems, such as storages or distributed energy resources, connected to the grid, and asset management system responsible for communication among central command are also sources created Big Data in SG. As a result, the communication backbone networks should be reliable, secure, scalable, and cost-effective enough to meet the requirements in terms of bandwidth and latency to communicate the data.

In [15], by deploying an AMI, reliability, operational efficiency, and customer satisfaction can be achieved. This chapter also suggested several additional benefits gained in the AMI, such as managing power quality and asset management to improve service of the utility company. However, a robust communication backbone for the AMI data transmissions was not provided in the chapter. In particular, the AMI communication models include thousands of smart meters, multiple access points, and a mesh network, which is formed between smart meters for data routing purposes using industrial, scientific, and medical (ISM) frequency bands. Meanwhile, the aggregated data are routed to the utility company by access points mostly using licensed bands. The reliability and security of data communications between AMI components suffer from crowded and noisy ISM bands in urban areas. Packet losses, performance degradation, latency, and signal interferences are some of the consequences of heterogeneous spectrum characteristics of the crowded wireless communications. Moreover, the use of licensed bands to communicate the data between access points and utility companies requiring extra costs, which is another obstacle to deploy AMI in SG. Consequently, providing a robust communication backbone is sometimes hardly achievable, and it also comes with some obstacles for implementation of AMI in SG.

Several works investigated integrated communication technologies for the communication backbone of AMI. For example, mesh, Ethernet, and cellular AMI network topologies for SG have been proposed in [16–18]. In [16], the authors proposed mesh networks with a transmission architecture based on ZigBee, because the ZigBee protocol was integrated into smart meters by many AMI vendors, such as Itron, Elster, and Landis Gyr. The operation of ZigBee under an unlicensed spectrum makes it easy to implement network, being a standardized protocol based on the IEEE 802.15.4 standard. Nevertheless, ZigBee also has its own disadvantages, i.e., the transmission distance is limited, the rate of data transmission is low, and the capability to penetrate the barriers is weak due to non-line-of-sight transmission. Moreover, ZigBee may cause interferences to other appliances, which operate in the identical 2.4 GHz ISM frequency band, such as IEEE 802.11 wireless local area networks (WLANs), WiFi, Bluetooth, and Microwave. Inefficiencies of AMI based on ZigBee will arise when transmission distances increase. High levels of internetwork coordination are necessary in the deployment of new mesh networks. Improved alternatives of AMI mesh networks utilize IEEE 802.11 (a, b, g, n) protocols. However, such networks only support transmission distances ranging from 50 to 200 m, which is also problematic for robust metropolitan area coverage. To increase the transmission distances in the metropolitan areas and security of data communications between AMI components, in [17], the authors discussed communication infrastructure based on

Ethernet. The proposed method can support automated meter readings, customer home appliance connections, distribution automation, and substation automation. However, AMI based on Ethernet is not always affordable. In addition, the wireline systems can be challenging to rapid redeployment, particularly in emergency situations. To overcome this problem, the authors in [18] proposed a framework for Radio frequency (RF) mesh networking interfaced with high-speed access networks such as WiMAX. In the framework, the AMI smart meters are capable of two-way communications over a 900 MHz wireless mesh network back to a collection point at the substation. A private high-speed access network, which typically can be fiber or an existing cellular network such as WiMAX, will be then utilized to connect the substation to the corporate network. However, the AMI network topology based on cellular network or fiber for SG brings in extra costs to the utility companies and customers. Especially, the AMI interfaces for future proprietary protocols were not proposed in the framework. Ideally, AMI interfaces should be upgraded via software without hardware modifications to save time and cost.

4. Security in AMI

AMI security is required to protect both communication networks and power grid, because these two systems need to ensure their availability of access as well as survivability in different scenarios. However, the security of communication networks and power grid differ in several ways. In a communication network, latency needs to be limited and bandwidth needs to be guaranteed, whereas data manipulation (placement of false data), destruction of data, and unauthorized access should be prevented. On the other hand, security of a power grid needs to ensure reliability, power quality, and stability. Despite these differences, security between the two systems must be coordinated because the power grid and communication network can be used to launch attacks against each other. For instance, because the power supply in SG will be controlled by instantaneous users, information, manipulation of usage data could create a fictitious grid imbalance leading to voltage variations that can create large-scale failures. Similarly, if the state information of the grid is poisoned, the grid could be destabilized with a potential for physical damage. Physical damage could occur through overheating of transformers and relays or through voltage fluctuations in appliances. Due to the critical role of AMI in the SG, AMI security is special importance for the security of the SG. Given importance in AMI security, in [19] the authors discuss the security issue from two major aspects: maintaining the privacy of consumer's information and resilience of system against cyber or external attacks. Besides, the authors in [20] propose security in AMI using key management scheme for communication system. We can summarize these aspects as follows.

4.1. Privacy of end user's information

In AMI, smart meters are capable of collecting information of customers in every 15 min. However, current technologies even allow for collecting the data with intervals of minute [21]. Hence, if attackers analyze the data, they can achieve “consumer profiling” with an alarmingly high accuracy, for example, they know how many people live in the house, type of devices, duration of occupancy, ability of security and alarming systems. The profiling allows the attackers to extract behavior of customers without the need of using computer-aided tools or sophisticated algorithms. The authors in [21] have shown that they can identify the use of major devices in a house of customer by analyzing cumulative energy consumption data from the smart meter with a 15 min interval. Molina-Markham et al. [22] use the current general statistical schemes to identify the usage pattern from AMI data, which is valuable to third parties, such as entertainment agencies, insurance companies, and government authorities. In AMI of SG, you can access the network data using your name and address information collected and stored for billing purpose. From the detailed information, the process can backfire if it is used without your consent.

To discuss the importance of privacy, it is necessary to consider electrical behavior of an appliance while it is operating, which is defined as load signature (LS) because each appliance has different measurable behaviors. For example, consumption behavior of each electrical appliance is a signature, which could be measured at meter point. Typical variables are current, voltage, and power or energy. To protect the customers’ privacy, a common method is to make it impossible for unauthorized parties to differentiate between load patterns and signatures. The authors in [23] proposed “load signature moderation” technique to facilitate customers’ privacy protection by reshaping the overall pattern of data to make differentiating between load patterns and signatures impossible. This technique combines three methods, which are smoothing, hiding, and mystifying consumption, utilizing cooperation of grid and storage/ battery as power source. The method is also defined as “undetectability” in [24].

4.2. Security against external cyber or physical attacks

The AMI-Sec Task Force, which is formed by security domain experts, industry leaders and standards bodies, developed the requirements for AMI security [25]. It provides guidance and security controls to organizations developing or implementing AMI solutions. According to the report in [25], security requirements for AMI system include confidentiality, integrity, and availability (or resilience to DoS attacks). Hence, the security for AMI system should satisfy the requirements as follows:

- **Confidentiality:** In the AMI, the metrology and consumption information communications have to meet confidentiality requirements to protect the customer's privacy and business information. This means physical theft of smart meters to access the stored information, unauthorized access to the data, as well as customer's access to other customers’ data should be prevented. At AMI headend, only authorized systems are permitted to access to specific customer's information.

- **Integrity:** The AMI system should ensure the integrity of transmitted messages, as the operation of the AMI is dependent on the integrity of communicated information. Integrity in AMI means that the transmitted data from the meter to the utility as well as control commands from the utility to the meter and the received data from smart meters are maintained and protected from any changes such as malicious modification, insertion, deletion, or replay. The integrity of data can be ensured by using cryptographic techniques to prevent hackers from pretending they are authorized entities and issue commands to perform their attacks. In AMI, smart meters have to detect cyber-attacks and ignore all issued control commands from attacker to protect the integrity of SG.

- **Availability:** The assurance that any network resources, such as data, bandwidth, and equipment, will always be available to any authorized entity. One of the important functions of the availability is to prevent denial-of-service (DoS) attacks, energy starvation, and selfishness. Hence, AMI components should protect against or limit the effects of DoS attacks. The AMI system should restrict the ability of internal or external users to launch DoS attacks against other AMI components or networks. Besides, the main reason for unavailability of data is component failure, such as communication failure (due to interference, cut cables, path degeneration, loss of bandwidth, network traffic, etc.), software problem, physical damage, or human tampering with the meter.

- **Accountability:** Also known as nonrepudiation or nondenial. Accountability techniques prevent either receiver or sender from denying a message by ensuring that undeniable proof will exist to verify the truthfulness of any claim of an entity. Accountability is specifically important for billing purpose as well as responses to control signals and in the actual metrology data. In AMI, the accountability requirement is a major concern, because different devices are usually owned by different entities, for example, service providers, customers, and they are manufactured by different vendors. To ensure accountability, time synchronization across AMI network as well as accurate time stamp of collected data is vital.

Based on the security requirements for AMI system was mentioned, security in AMI is very complex. Hence, just a single solution is insufficient for securing AMI. The authors in [22] present the threats to the security in AMI and then they propose some technologies as well as policies to improve the system's security.

4.3. Security in AMI using key management scheme

A typical AMI involves smart meters, HAN, NAN, WAN, and MDMS. For secure communication between these entities, confidentiality, integrity, and authentication should be guaranteed in the first place. Meanwhile, availability is also a critical requirement that should be fulfilled due to the high availability of electrical power. Besides, the AMI system must implement intelligent applications, such as dynamic electricity pricing, demand response, and real-time measuring/monitoring. Hence, AMI should be able to support different communication types (i.e., unicast, multicast and broadcast communications) for both customers and the utility companies to propagate information between the utility and smart meters [26]. Measured data are usually unicast communication from smart meters to the utility companies. Meanwhile, electricity pricing information is communicated multicast or broadcast from the utility to smart meters. Demand response program information is transmitted broadcast to all customers. As a result, by using the key management scheme for the AMI system, unicast, multicast, and broadcast communications should be able to securely and efficiently deliver [20].

To meet the security requirements for AMI, an underlying key management scheme is needed to generate and update keys for secure message transmission and authentication. Unfortunately, existing key management schemes designed for IT systems are simply inapplicable for AMI infrastructure in SG due to the reasons as follows:

- AMI is a complex heterogeneous system, which includes various entities with different computing ability, storage, and communication capability. In AMI, the smart meters are typical resource-constrained appliances, which have limited computation and storage capability. Meanwhile, the MDMS has high computing ability and plenty of storage resources. Hence, AMI utilizes the key management scheme, which not only achieves the security requirements of the system, but also accommodates this imbalance in its existing resources.

- Typically, AMI in SG is built based on combining IT systems with electric power system. Thus, problems of AMI are unique that are not encountered in traditional electric power system as well as IT systems. For example, electric power service demands the high availability, which is the same high availability of the security schemes in IT systems. The availability of electric power service and IT systems is considered as DoS attacks. As a result, the key management scheme must been designed with mechanisms to protect against DoS attacks. Additionally, the key management scheme has ability to support various modes of data transmission used in AMI.

- Because AMI may consist of a huge number of smart meters. Hence, the key management protocol has to open with scalable ability for such a big system.

Currently, in [26, 27], the authors propose key management schemes in AMI for SG. However, these schemes cannot completely satisfy the above requirements of security. For example, the authors in [26] present a new key management scheme for AMI, but this method is vulnerable to DoS attacks and inefficient in key management for a big system. In [27], the authors propose the key management scheme using physically unclonable functions to guarantee the security requirements of the system; however, the method is designed without open protocol with scalable ability for the big size of AMI. To overcome these problems, a hybrid key management scheme for AMI is proposed in [20] by integrating public key cryptosystem with symmetric cryptosystem. In this hybrid scheme, the elliptic curve cryptosystems are utilized to achieve efficient session key generation and trusted authentication. Besides, to generate and update group keys efficiently, the authors employ a specially designed key hierarchy.

Based on the security requirements of AMI, the system structure, and required availability, a key security technology using trusted computing methodologies and public key infrastructure (PKI) is proposed in [28]. By combining PKI technologies with trusted computing elements, the method is the most desirable solution for SG security as well as AMI. However, the method is complex, especially in the big system. To reduce the complexity of the method, the authors propose a technology utilizing the four major technical elements, namely automated trust anchor security, PKI standards, SG PKI tools, and certificate attributes. In [29], the authors complement a novel technical element to reduce the complexity of PKI security, which is device attestation. The proposed method includes the PKI elements into the overall security architecture to achieve a cost-effective and comprehensive solution for AMI security in SG. Besides, the trusted computing elements are utilized to guarantee that a malware cannot to access to the software processing devices. The main functionality of trusted computing is to allow any devices, which want to join a grid network, to verify that authorized code runs on that system. The adoption of strict code signing standards by SG suppliers and operators was also suggested in [28]. Mechanisms for enforcing such standards have been put forward by the Trusted Computing Group and have been also well documented and available in the literature. The works in the literature concluded that security solution in SG requires a holistic method, which combines trusted computing techniques with PKI technologies based on industry standards. In the holistic method, PKI technical elements, such as trust anchor security, attribute certificates, and certificate lifecycle management tools, are the existing technologies tailored specifically to result in an optimal solution for SG networks. To achieve the optimal solution for secure SG networks, the primary step should be taken is to propose a cohesive set of standards and requirements for AMI security.

The authors in [29] articulated the security threats to transmission and distribution (T&D) automation systems. They mentioned that vulnerabilities in power T&D automation systems exist at multiple levels, including components, protocols, and networks. An attack process involves three steps: access, discovery, and control. First, the attacker gains access to the SCADA system through a connection with the corporate network or through a virtual private network (VPN). Subsequently, the attacker studies the behaviors of the system and finally launches an attack. The authors pointed out that the current security solutions are focused mainly on information technology (IT) but not on control systems, and that there are different needs for them, making IT security solutions ineffective. They suggested to decouple the controls from security in order to make it accessible for legacy systems that do not have inherent security. Their work is mainly a conjecture without clear evidence or comparison with other approaches.

5. Challenges and solutions in AMI

Such a complex system undoubtedly presents many challenges. In this section, the challenges and solutions in AMI are identified in two domains including security and communications between networks.

5.1. Challenges and solutions in security of AMI

5.1.1. Challenges

5.1.1.1. Difficulty to identify large-scale catastrophic failures

In AMI security, the primary challenge stems from the high-level dependence between grid components, such that seemingly independent random events can aggregated to yield large-scale catastrophic failures in the grid. High complexity in AMI increases the probability of flaws, and unintended access points increase the possibility of attacks induced failure, especially in an adversary model, in which attacks are readily replicated, thus propagating the failures. In addition, new entities, such as electric vehicles and DER, are expected to be incorporated in the grids. However, researches on security raised up by the incorporations have received very limited attention. Hence, it is very difficult to identify and address the new failure modes in such systems before they become large-scale problems.

5.1.1.2. Dependence between electric grids and communication networks of AMI

We understand the threats to the communication networks of AMI and power grids, and we understand to some extent how the threats associated with the SG communication infrastructure impact on the power grid. However, it is unclear how the threats in the power grids can affect the communication networks of AMI.

5.1.1.3. Challenge to detect network-based threats

The most serious challenge comes from the ubiquitous connectivity in the equipment, software, and controls in AMI. Network-based threats may propagate quickly to overwhelm the whole network of AMI. In addition, the universal connectivity and multiple access points make AMI more vulnerable to attacks (such as DoS). We need to rely on automated detection schemes to respond to network-based threats.

5.1.1.4. Intrusion detection, prevention, and recovery for AMI

Typically, DoS is one of the most dangerous attacks against AMI. If such attack cannot be detected and quarantined early enough, it will risk the failure of the functionality in most critical infrastructure and threaten AMI. Hence, we need new methods for risk assessment based on prior knowledge in order not to introduce further delays in the overall system. Besides, in case that an attack cannot be identified and prevented, appropriate intrusion recovery techniques must be implemented to remedy the consequences of the attack on the critical infrastructure of AMI.

5.1.1.5. Key management techniques for AMI

Today, the majority of key management schemes were proposed only for secure communications within the SG, to address the issues on key establishment for the communicating entities within SCADA systems to protect critical messages, such as near-real-time information, pricing signals, and feedback data regarding energy consumption of customers. In fact, very few studies have been carried out on key management schemes for the AMI. Hence, in the future, researchers should focus on the proposal of novel key management techniques specifically designed for the AMI.

5.1.2. Solutions

5.1.2.1. Security analysis

It is important to develop a risk/security analysis process that can autonomously detect faults to limit the damages to communications of AM. In addition to the analysis of causes and effects of different threats on the electric grid, we need to establish comprehensive failure scenarios that include the impacts of multiple threats simultaneously. The risks include those associated with interactions among cyberspace and physical systems. It will not be possible to consider all possible combinations of threats. Consequently, an automated test system of taking into account different failures (attacks) in both cyberspace and physical systems will be an important additional source for mapping all of the threats and studying their behaviors. Contingency analysis is already performed for analyzing the stability of AMI. However, that will need to be expanded to incorporate the risks due to threats coming from various communication networks in AMI. More precise detection techniques that use multiple factors for accurately predicting threats will need to be devised to reduce false-alarm probability. Based on the previous risk analysis, the algorithms can autonomously detect the faults in AMI to limit the damages caused by degraded security performance.

5.1.2.2. Security standards

On the other hand, international security standards and legislations are also needed for communications in AMI. Currently, there are numerous independent efforts to develop security standards and legislations. Security standards being developed need to be future-proof, considering futuristic applications, operations, and energy markets. Standard test scenarios need to be developed for the researchers developing the algorithms, as well as for equipment manufacturers for detecting security attacks and failure scenarios at the interfaces between power grid and communication networks of AMI. Moreover, we should establish standardized testing requirements for the security in all applications and protocols of AMI. It is also essential to create auditing requirements to ensure compliance with security legislations for utilities, equipment manufacturers, and generators for local, national, and regional regulatory bodies.

5.5.2.3. Quantum key distribution in AMI

The use of quantum key distribution (QKD) can help improve the security of communications in an AMI. Quantum communication is an emerging technology with potential applications to the power grids. QKD has been proposed as an approach to improve the security of communications between the power grids, and it could be implemented over existing fiber-optic channels and free-space optical communication links, within generation systems and power distribution networks. Quantum communication employs a fundamentally different technique from most of traditional communicationtechnologies, and it works based on the physics of entangled quantum states as a fundamental resource. The classical cyber security techniques depend on physical protection of communication channels, and they need complex computational techniques to encrypt transmitted data and protect its confidentiality. The observation of quantum communication measurements fundamentally disturbs the system, alerting the receiver for the changes in the channel. QKD has rapidly matured and is now providing commercial applications by several companies around the world. Researchers are exploring its applications in more challenging and interesting scenarios, including AMI. One potential usage in AMI is quantum location verification. Because today's power system components tend to be stationary, quantum communication techniques could potentially be used to improve the security with regard to the identification of the location of a smart meter. This adds another level of security by ensuring that a smart meter placed at a fixed location in the power grid is truly at that location and is not being spoofed. There are potentially many other applications of quantum communication techniques that might become useful to ensure the security in AMI [1].

5.1.2.4. Cross-layer design for attacks detection

Cross-layer design for attacks detection in communications of AMI based on CR technology is another new research topic. To realize a secure communications of AMI based on CR, security should prevail every other aspects of the whole system design, and be integrated into every system component. AMI security includes the protection of both communication networks and power grids to ensure availability and survivability. The detection techniques based on higher layer introduce an overhead in the network, which could potentially affect timely delivery of critical messages in the SG, resulting in instabilities. Thus, our earlier work proposed a cross-layer design for primary user emulation attacks detection without burdening the networks with extra overhead [30]. In this work, to completely identify primary user emulation attacks and primary users (PU) at PHY layer over multipath Rayleigh fading channels in mobile CR networks, cross-layer intelligent learning capability of secondary user (SU) was exploited to establish radio-frequency fingerprint (i.e., channel-tap power) databases by combining the accuracy and capability of higher layer authentication [31] with a quick detection algorithm on PHY layer [32].

5.2. Challenges and solutions in communications

5.2.1. Challenges

Depending on the characteristics of HAN, NAN, and WAN, different communication technologies are utilized efficiently. For example, in a small area as customers’ home, HANs use ZigBee, Bluetooth, or PLC to communicate data between devices. Besides, WiMAX, or WiFi is utilized to build NAN based on wireless mesh topology, and fiber optics or broadband cellular networks are adopted for WANs. However, these traditional communication methods bear the high costs for investment, operation, and maintenance, which are incapable of meeting the requirements and challenges in SG. It has been recognized that CR is a promising technology to construct a more advanced communication infrastructure for SG. By using dynamic spectrum access technique, CR networks solve the problem of scarce spectrum and poor allocation of traditional spectrum policies, and support increasing demand for applications based on wireless communications in SG [33]. In [34], the authors propose the use of CR technology to address the communication requirements, standardization, and security problems of SG communications. There are many benefits brought in by introducing CR into SG. In [35], by using CR technology, it can support energy- and spectrum-efficient designs, as well as avoiding interference and adapting the data throughput, i.e., CR communication over license-free bands is employed in the HANs to coordinate heterogeneous wireless technologies, whereas CR communications over licensed bands is employed in the NANs and WAN to dynamically access unoccupied spectrum opportunities [36].

Moreover, to address aforementioned problems in AMI communications infrastructure (Section 3.2), CR technology can be suitable for AMI communication system. In [37], the authors proposed to enhance a routing protocol for low power and lossy networks (RPL) for CR-enabled AMI networks, i.e., CORPL [38]. This protocol provides novel modifications to RPL to address the routing challenges in CR environments, such as reliable and low latency data delivery, along with protecting the PUs and meeting the requirements of secondary networks. Results show that CORPL improves the reliability of the network while reducing harmful interferences to PUs by up to 50%, as well as reducing the deadline violation probability for delay sensitive traffic. The authors in [39] proposed to use a cloud computing data center as a central communication and optimization infrastructure supporting a CR network of AMI smart meters that is called netbook advance metering infrastructure (Net-AMI). The proposed system is extensible and can easily handle thousands of variations in power systems, communication protocols, control, and energy optimization protocols. By placing new CR antennas on existing cellular antenna towers, vast geographical coverage can be achieved. Moreover, remote software upgrades allow modifications of existing networks components, AMI interfaces, and Net-AMI smart meters in a flexible and amorphous manner using CR technology. In [40], the authors modeled the AMI as a SU in CR-based SG systems based on the IEEE802.22 wireless regional area network (WRAN) [41], which supports the unlicensed operation of SUs with spectrum sensing technologies in VHF/UHF TV broadcast bands from 54 to 862 MHz. The authors also investigated a beam-forming method based on minimum mean squared error (MMSE) to suppress self-interferences in smart meter channels. In [42], the authors proposed a CR-based SG using wireless access communication of line and substation monitoring system addressing the system implementation issues, such as communication efficiency and energy supply in AMI.

As part of the end-user facilities, AMIs can also be efficiently realized with the help of CR technology. For example, by using CR technology, AMI can self-configure and deploy in coexisting wireless networks at various customer premises easily. Based on the spectrum-aware capability of CR, smart meters and equipment in AMI can be easily deployed at the remote sides to achieve reliable and seamless communications between AMIs and the control center of utility company. The cognitive sensor network (CSN) nodes designed with consideration of energy and price limitations in remote monitoring can be the main components for efficient realization of wireless AMI.

However, when we apply CR technology in communications of AMI, we have to face some challenges.

(1) Communications between cognitive HANs and NANs

The challenges to implement communications between CR-based HANs and NANs can be identified as follows.

- **The lack of spectrum holes of licensed bands for data transmissions from smart devices:** In CR-based SG networks, the communications between HANs and NANs are realized by connecting HAN gateways (HGWs) and NAN gateway (NGW). A NGW connects many HGWs from various HANs using licensed bands in an opportunistic manner. However, a SG system generates vast amount of data coming from smart devices. Hence, it might happen that there are no enough spectrum holes of licensed bands to be used for the data transmissions, as there might be times or locations where vacant bands are not available. Moreover, a great challenge in HANs is to internetwork various customer equipment provided by different manufacturers using different standards such as WiFi, ZigBee, WRAN, and Bluetooth.
- **Delay of traffics and real-time capability:** Bidirectional data transmissions between NANs and HANs must meet real-time requirements. The data transmissions involve many types of data, which have different levels of time requirements. For example, the real-time data exchanges between IEDs and other power devices in a large distributed area should ensure that all decisions are made by the control centers in a timely manner, such as controlling or monitoring data, so that demand response can be realized in the customer ends; whereas some other data are transmitted in a periodic manner, such as power consumption data of households. The various types of data also bring in a major challenging issue due to low-speed transmission characteristics and inherent sensing delays of CR. Moreover, the SU in CR must continuously monitor radio spectrum usage to give the precedence to the PU. Therefore, the random interruption of SU traffic will unavoidably cause packet losses and delays in sending SU data. As a result, the communications in a CR network are normally unreliable, and it is a great challenge to support real-time applications.
- **AMI self-configuration:** HANs connect many smart devices to achieve optimum energy consumption and to implement demand response and AMIs. Smart meters, energy management systems (EMSs), and smart devices installed in all customer premises are part of the AMI. The AMI will enable these smart devices to communicate with the utility operated control centers to control their operations at a given time and thus implement demand-side management for the utility. However, the number and characteristics of the smart meters and devices change randomly according to the preferences of customers, who can install new smart meters and devices or remove old smart appliances in an unpredictable manner. Hence, the AMI must have self-configuration ability to ensure online update and effectively monitor the random changes of these smart appliances.

(2) Communications between cognitive NANs and WANs

The challenges to implement communications between cognitive NANs and WANs are identified in the sequel.

- **Limited WAN coverage area due to the use of ISM bands:** The communications between NANs and WANs are built up based on cognitive base stations. Hence, there is also the problem of a shortage of licensed bands for opportunistic access. However, the ISM bands are not suitable for the communications between NANs and WANs because the coverage area of WAN is larger, whereas the ISM bands are suitable for short-range transmissions.

- **Service reliability using TV white space (TVWS) to connect NANs and WANs:** Another serious challenge using TVWS to connect NANs and WANs is service reliability. In spite of dynamic frequency switching and multi-channel utilization, which can solve the reliability problems, the SU using TVWS is considered as a fundamental issue, in which the SU have to postpone its connections with TVWS if it detects the existence of an incoming PU. New methods to mitigate the unreliability caused by inherent cognitive characteristics of SG communications in the licensed bands remains to be proposed.

- **Scalability:** The scalability feature of WAN connections using wired communication technologies in AMI is limited due to high maintenance and installation costs. Hence, wireless communication technologies are suitable for wide area communications in AMI because of its flexibility. However, to achieve scalability in wireless technologies, we have to add more wireless routers and access points to AMI network, so the installation costs will increase.

5.2.2. Solutions

5.2.2.1. Communications between cognitive HANs and NANs

In order to facilitate the communications between cognitive HANs and NANs, we suggest to use the following techniques.

- **Hybrid spectrum access method to extend the coverage of WANs:** As spectrum holes of the licensed bands may not be enough to transmit a massive amount of data, the communications between HANs and NANs may temporarily operate in the license-free bands (i.e., ISM bands) with lower communication rates. In the method, data transmissions between HGWs and a NGW are considered using a hybrid spectrum access. As a result, the communications between HANs and NANs can improve reliability. As using hybrid spectrum access, the HGWs operate as cognitive nodes in the communication networks and they employ the spectrum sensing method to find vacant spectrum bands. However, if spectrum sensing time of HGWs is too long, then the rest of time to transmit data is short, so the throughput of the networks will be reduced. To solve the problem of HGWs, a scheme to decide when to stop spectrum sensing and when to access ISM bands was proposed in [43] based on the expected throughput performance. In this case, ISM bands are introduced as backup bands for communications to improve service reliability of SG applications. If this condition happens frequently, more NGWs can be installed to utilize space diversity.

- **CR-based AMI self-configuration:** As part of the end-user facilities, AMIs can also be efficiently realized with the help of CR technology. By using CR technology, AMI can self-configure in order to coexist wireless networks at different customer premises. With the spectrum-aware communication capability, smart meters and equipment in AMI can be easily deployed at the remote sides to achieve reliable and seamless communications between AMIs and the control center of utility company. This is a major opportunity for efficient implementation of wireless AMI in remote monitoring.

5.1.1.1. Communications between cognitive NANs and WANs

To ensure reliable and scalable communications between cognitive NANs and WANs, we identify the approaches as listed in the sequel.

- **WAN coverage area extension to improve reliability:** First, we can use hybrid access modes of licensed and leased bands to extend the coverage area of WANs and improve service reliability. The utilities can lease some radio bands, which are used as backup bands, at a low cost from a telecommunication operator. The hybrid access mode between the leased and licensed bands is intelligently scheduled and seamlessly switched, so that it can improve quality of service (QoS) of data communications, thus benefiting both utilities and users. In this sense, NGWs operate as cognitive nodes, which use spectrum sensing methods to find vacant spectrum bands in communication networks of AMI. After given certain sensing times, the NGWs will choose leased spectrum bands to communicate data with base station, whereas these NGWs still find vacant spectrum bands to use them opportunistically. When the data transmission rate of the leased spectrum bands is higher than that of the cognitive licensed spectrum bands, SUs will stop spectrum sensing and access the leased bands to transmit collected data. On the contrary, if the transmission rate of the leased bands is lower than that of cognitive licensed bands, then SUs will find vacant spectrums and access the cognitive licensed bands to transmit data for achieving a higher throughput. However, the number of the leased spectrum bands is very limited and they also serve as backup bands in emergency situations to transmit critical data. Hence, the NGWs have to spectrum sensing periodically to release the leased spectrum bands once a vacant spectrum band is identified. In NANs, the available unoccupied spectrum bands are scarce in urban areas, whereas abundant in rural areas, because the amount of data traffic in urban areas is much larger than that in rural areas. Therefore, the leased bands, which are distributed to a NAN in urban areas, should be more than that distributed to a NAN in rural areas. Moreover, a leased spectrum band can be shared by several NANs without causing interference to each other if the service area of a WAN is very large. Similarly, the leased bands are utilized as backup bands for communications to improve service reliability of SG applications. Besides, we can use cooperative communications to extend the coverage and improve service reliability. Other available wireless and wireline technologies, such as wireless cellular networks, internet, and fiber optics, should also interoperate with cognitive NANs and WANs to make SG more resilient, scalable, and reliable in an economical manner. For example, currently, the mobile communications have been implemented via both cellular networks and IPv6 mobile ad hoc networks (MANETs), so that we can utilize the MANETs to transmit noncritical data.

- **Scalability:** The CR technology creates an opportunity to increase scalability with a low cost. For example, IEEE 802.22 standard has unique features, such as geo-location, spectrum sensing, and intra-system coexistence for CR-based operations. The standard operating in TVWSs from 54 to 862 MHz permits broadband wireless access to wide range rural areas without interference with the PUs. Using IEEE 802.22 standard, coverage area of base station can be 33 km if customer premises equipment operates at power level of 4 W. When higher power levels are allowed, the coverage area can be increased to 100 km [34].

6. Conclusions and future visions of AMI

AMI based on smart meters in SG has been identified, and their state-of-the-art research activities were reviewed. In addition, the issues on security of AMI in SG have also been discussed. Future SG should comprise intelligent monitoring systems to keep a track of all electricity flows and a huge amount of collected data from smart devices as well. Hence, it must be flexible and resilient to accommodate new requirements in an economical manner. To achieve these goals, communications in AMI based on CR will certainly play an important role for infrastructures of the SG. Moreover, by using AMI, SG can support real-time traffic delivery with stringent the quality of service requirements of real-time applications. The major challenges on evolutional path toward SG and solutions are also identified in this chapter. With AMI, SG should preserve its interoperable and secured communications within a hybrid system where both new and legacy grids coexist. Therefore, AMI in SG should be built up on open protocols with a common notion of security and standard. Besides, advanced research topics, such as artificial neuron network and Fuzzy theory, can also apply to the intelligent monitoring systems to improve the ability of AMI. Moreover, accurate state estimation methods need to propose in the future to detect blind false data injection attacks because accurate state estimation is of paramount importance to maintain normal operations of AMI. Typically, a bad data detection system is used to ensure the integrity of state estimation and to filter faulty measurements introduced by device malfunctions or malicious attacks. However, in [44], we prove that blind false data injection attacks using the principal component analysis approximation method without the knowledge of Jacobian matrix and the assumption regarding the distribution of state variables can bypass the bad data detection system to inject fault data in the system. In the future, the architecture of AMI not only aims at seamless integration of various existing smart metering products, but also other software systems used by power utilities (i.e., outage, energy and distribution management systems, etc.). Hence, new solutions aim at enabling flexible integration of metering devices and their grouping in form of *virtual meters* through hierarchically organized software structures and flexible standardized communication interfaces.

Author details

Trong Nghia Le[1], Wen-Long Chin[2*], Dang Khoa Truong[1] and Tran Hiep Nguyen[1]

*Address all correspondence to: wlchin@mail.ncku.edu.tw

1 Le Quy Don Technical University, Hanoi, Vietnam

2 National Cheng Kung University, Tainan, Taiwan, ROC

References

[1] IEEE Smart Grid Research. IEEE Vision for Smart Grid Communications: 2030 and Beyond. IEEE Vision for Smart Grid Communications:. May 2013; Chapter 1; 3–22.

[2] V.C. Gungor, B. Lu, and G.P. Hancke. Opportunities and challenges of wireless sensor networks in smart grid. IEEE Trans. Ind. Electron. Oct. 2010;57(10):3557–3564.

[3] U.S. Department of Energy. [Online]. Available at: http://www.oe.energy.gov. 2011.

[4] A.Y. Saber and G.K. Venayagamoorthy. Plug-in vehicles and renewable energy sources for cost and emission reductions. IEEE Trans. Ind. Electron. Apr. 2011;58(4):1229–1238.

[5] P. Siano, C. Cecati, C. Citro, and P. Siano. Smart operation of wind turbines and diesel generators according to economic criteria. IEEE Trans. Ind. Electron. Oct. 2011;58(10): 4514–4525.

[6] D.G Hart. Using AMI to realize the smart grid. in Proc. IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. July 2008;:1–2.

[7] R. Gerwen, S. Jaarsma, and R. Wilhite. Smart metering. [Online]. Available at: http://www.leonardo-energy.org/webfm_ send/435.

[8] S.S.S.R. Depuru, L. Wang, and V. Devabhaktuni. A conceptual design using harmonics to reduce pilfering of electricity. IEEE PES General Meeting; Minneapolis; MN. July 2010; 1–7.

[9] R.R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar . Application of Advanced Metering Infrastructure in Smart Grids. 2014 22nd Mediterranean Conference on Control and Automation (MED); Palermo. 2014;:822–828.

[10] Silicon Laboratories, Inc. Smart Metering Brings Intelligence and Connectivity to Utilities, Green Energy and Natural Resource Management. Rev.1.0. Available at: http://www.silabs.com/Support%20Documents/TechnicalDocs/Designing-Low-Power-Metering-Applications.pdf. August, 2013.

[11] R. Berthier, W. H. Sanders, and H. Khurana. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm); MD*. 2010;:350–355.

[12] R. Shein. Security measures for advanced metering infrastructure components. in Proc. *2010 Asia-Pacific Power and Energy Engineering Conference* (APPEEC); Chengdu. 2010;:1–3.

[13] S. Rusitschka, K. Eger, and C. Gerdes. Smart Grid Data Cloud: A Model for Utilizing Cloud Computing in the Smart Grid Domain. First IEEE International Conference on Smart Grid Communications; Gaithersburg, MD. 2010;:483–488.

[14] Anderson, C. Zhao, C. Hauser, V. Venkatasubramanian, D. Bakken and A. Bose. A virtual smart grid. IEEE Power & Energy Magazine. December 13, 2011;9(6):49–57.

[15] D. Backer. Power Quality and Asset Management The Other “Two-Thirds” of AMI Value. 2007 IEEE Rural Electric Power Conference; Rapid City, SD. May 2007;:6–8.

[16] S. W. Luan, J. H. Teng, S. Y. Chan, and L. C. Hwang. Development of a smart power meter for AMI based on zigbee communication. *2009 International Conference on Power Electronics and Drive Systems (PEDS); Taipei*. 2009;:661–665.

[17] W. Luan, D. Sharp, and S. Lancashire. Smart grid communication network capacity planning for power utilities. *IEEE PES T&D 2010*; New Orleans, LA, USA. 2010;:1–4.

[18] B. Reid. Oncor electric delivery smart grid initiative. *2009 62nd Annual Conference for Protective Relay Engineers*; Austin, TX. 2009;:8–15.

[19] R.R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar. A survey on advanced metering infrastructure. Int. J. Electr. Power Energy Syst. Dec. 2014;63:473–484.

[20] Z. Wan, G. Wang, Y. Yang, and S. Shi. SKM: scalable key management for advanced metering infrastructure in smart grids. IEEE Trans. Ind. Electron. Dec. 2014;61(12): 7055–7066.

[21] Murrill BJ, Liu EC, Thompson II, RM.. Smart Meter Data: Privacy and Cyber security. Congressional Research Service; USA. 2012; 1–45.

[22] Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D. Private memoirs of a smart meter. Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building; ACM, 2010; 61–66.

[23] G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda. Privacy for smart meters: towards undetectable appliance load signatures. In: Proc IEEE International Conference on Smart Grid Communications, Gaithersburg, MD. 2010.

[24] Pfitzmann A, Hansen M.. A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. 2010. Online: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[25] The Advanced Security Acceleration Project. Security profile for advanced metering infrastructure. AMI-Sec Task Force, TN, Tech. Rep. Jun. 2010.

[26] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He. A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Trans. Ind. Electron. 2013;60(10):4746–4756.

[27] M. Nabeel, S. Kerr, X. Ding, and E. Bertino. Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions. Purdue University, Tech. Rep. 2012.

[28] A.R. Metke, and R.L. Ekl. Security technology for smart grid networks. IEEE Trans. Smart Grid. 2010;1(1):99–107.

[29] D. Wei, Y. Lu, P. Skare, M. Jafari, K. Rohde, and M. Muller. Power infrastructure security: fundamental insights of potential cyber attacks and their impacts on the power grid. Part of project Protecting Intelligent Distributed Power Grids against Cyber Attacks for DoE: 35, 2010. [Online]. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.152.1832.

[30] T.N. Le, W.L. Chin, and W.C. Kao. Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks. IEEE Commun. Lett. May 2015;19(5):782–799.

[31] C. N. Mathur, and K. P. Subbalakshmi. Digital signatures for centralized DSA networks. *2007 4th IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA. 2007;:1037–1041.

[32] W.L. Chin, T.N. Le, C.L. Tseng, W.C. Kao, C.S. Tsai, and C.K. Kao. Cooperative detection of primary user emulation attacks based on channel-tap power in mobile cognitive radio networks. Int. J. Ad Hoc Ubiquitous Comput. 2014;15(4):263–274.

[33] J. Wang, M. Ghosh, and K. Challapali. Emerging cognitive radio applications: a survey. IEEE Commun. Mag. Mar. 2011;49(3):74–81.

[34] A. Ghassemi, S. Bavarian, L. Lampe. Cognitive Radio for Smart Grid Communications. First IEEE International Conference on Smart Grid Communications (SmartGrid-Comm); Gaithersburg, MD. 2010;:297–302.

[35] Vineeta and J. K. Thathagar. Cognitive radio communication architecture in smart grid reconfigurability. *2012 1st International Conference on Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN)*; Surat, Gujarat, India. 2012;:1–6.

[36] Y. Han, J. Wang, Q. Zhao, and P. Han. Cognitive information communication network for smart grid. *2012 IEEE International Conference on Information Science and Technology*; Hubei. March 2012;:847–850.

[37] A. Aijaz, H. Su, A.H. Aghvami. CORPL: a routing protocol for cognitive radio enabled AMI networks. IEEE Trans. Smart Grid. Jan. 2015;6(1):477–485.

[38] T. Winter. IPv6 routing protocol for low power and lossy networks. Internet Engineering Task Force, RFC 6550. Mar. 2012. [Online]. Available at: http://www.rfc-editor.org/rfc/rfc6550.txt.

[39] K. Nagothu, B. Kelley, M. Jamshidi, A. Rajaee. Persistent NetAMI for microgrid infrastructure using cognitive radio on cloud data center. IEEE Syst. J. 2012;6(1):4–15.

[40] S. Chang, K. Nagothu, B. Kelley, M.M. Jamshidi. A beamforming approach to smart grid systems based on cloud cognitive radio. IEEE Syst. J. 2014;8(2):461–470.

[41] IEEE Draft Standard for Information Technology - Telecommunications and information exchange between systems - Wireless Regional Area Networks (WRAN) - Specific requirements - Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands. IEEE P802.22/D3.0. March. 2011.

[42] B. Li, B. Zhang, J. Guo and J. Yao. Study on Cognitive Radio Based Wireless Access Communication of Power Line and Substation Monitoring System of Smart Grid. 2012 International Conference on Computer Science and Service System (CSSS); Nanjing. 2012;:1146–1149.

[43] F. Liu, J. Wang, Y. Han, P. Han. Cognitive radio networks for smart grid communications. 9th Asian Control Conference (ASCC); Istanbul. 2013;:1–5.

[44] Z.H. Yu and W. L. Chin. Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans. Smart Grid. May 2015;6(3):1219–1226.