A survey on Advanced Metering Infrastructure

CrossMark

Ramyar Rashed Mohassel, Alan Fung, Farah Mohammadi, Kaamran Raahemifar *

Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON M5B 2K3, Canada

ABSTRACT

This survey paper is an excerpt of a more comprehensive study on Smart Grid (SG) and the role of Advanced Metering Infrastructure (AMI) in SG. The survey was carried out as part of a feasibility study for creation of a Net-Zero community in a city in Ontario, Canada. SG is not a single technology; rather it is a combination of different areas of engineering, communication and management. This paper introduces AMI technology and its current status, as the foundation of SG, which is responsible for collecting all the data and information from loads and consumers. AMI is also responsible for implementing control signals and commands to perform necessary control actions as well as Demand Side Management (DSM). In this paper we introduce SG and its features, establish the relation between SG and AMI, explain the three main subsystems of AMI and discuss related security issues.

Crown Copyright © 2014 Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/3.0/).

1. Introduction

With emerging challenges and issues in the energy market of the 21st century, changes in the electrical systems are inevitable. The changes in the conventional ways of generation, transmission and distribution of power have brought along new challenges. The challenges to power industry include (but are not limited to): introduction of Distributed Energy Resources (DER), improvement of delivered power quality, environmental concerns over conventional and centralized methods of power generation, privacy of

consumer's information and security of the system against external cyber or physical attacks, economics of power systems, from maintenance costs to equipment renovation and network expansion and last but not least, needs for better control schemes for complex system. The developed control schemes shall be able to address numerous uncertainties due to load distribution and integration of new sources of energy, as well as integration of electrical storage systems into the grid [1]. For many years utility providers have been concerned about the power quality and the economy of power system; however, security and privacy of information are the newly emerging challenges due to the incorporation of new technologies. Utilization of DER as renewable energy plays an important role in sustainability of the system. Although DERs are part of the solution, they are not easy to use since they add to the complexity of the control system. To address some of these challenges, Europe and North America modernized their energy generation and distribution systems and switched to Smart Grid (SG).

While the first electrical grids date back to the late 1800s, the 1960s were the golden era of power grids in developed countries. In this era, the distribution network's penetration rates and their load delivery capacity were high, reliability and quality of delivered power were satisfactory and centralized power generation in fossil, hydro and nuclear plants were technically and economically boomed. The last decades of the 20th century experienced an increase in electric demand due to the introduction of new consumers, such as entertainment industry, and dependency on electricity as the main source of heat and ventilation. The latter was due to the increasing price of fossil fuels. Furthermore, there was

significant fluctuation in the rate of energy consumption. With increased demand at peak times, more generation plants were required to avoid voltage drops and decline in power quality. However, the new plants were costly. On the other hand, the consumption rates were lower at night time causing an unbalanced consumption that left the plants' production capacity idle. Therefore, to promote a more even consumption pattern, the electricity industry tried to encourage its consumers to manage their consumption through offered incentives by changing its approach to Demand Side Management (DSM). The 21st century came along with innovations and advancements in different sectors that allow enhancement of Smart Grid concept. The improvements in Information Technology and communication industries along with introduction of smart sensors eliminated the restriction of precise consumption measurement for each consumer and allowed adaptive billing mechanisms to financially motivate consumers shift their consumption to off peak times. Improvement in renewable energies such as wind, solar, tidal or geothermal, combined by environmental concerns led to integration of these technologies into electrical systems to form decentralized generation. Electrical storage systems were also developed to address power management issues [2].

Smart Grids modernized the traditional concept and functionality of electrical grids by using Information Technology to obtain network components' data, from power producers to consumers, and use it properly to maximize the efficiency and reliability of the system. There is no clear or fully agreed boundary and definition for intelligence of a Smart Grid, as there are a number of factors involved in designing such a system. However, it is unanimous that for an efficient SG design interaction among three fields of communication, control and optimization is essential. The ideal Smart Grid design should address reliability, adaptability and prediction issues [1–3]. It should also address the challenges to load handling and demand adjustment, incorporation of advanced services, flexibility and sustainability, end to end control capability, market enabling, power and service quality, cost and asset optimization, security, performance, self-healing and restoration [1–3]. Since the introduction of SG, many studies in both industry and academia have been conducted in an attempt to put the concept into practice. Although the achievements are huge, there is still plenty of room for improvement. While SG has addressed some of the initial challenges, it has introduced new ones.

This survey introduces the AMI technology and its current status, as the foundation of SG, which is responsible for collecting all the data and information from loads and consumers. To the best of our knowledge, no previous published work has been dedicated to AMI, its building blocks and the critical issues relevant to the technology. The authors' motivation was to introduce AMI and present the related information in one consolidated, yet abridged work, in a simple and easy to understand language. The hope is that this paper provides basic information regarding AMI to future researchers, utility companies, technicians and manufactures.

2. Advanced Metering Infrastructure (AMI)

2.1. Introduction

To achieve an intelligent grid, a succession of sub-systems should be realized. The solid establishment and functionality of each sub-system is instrumental in overall SG performance, as each layer's output serves as the feed for the next layer. Fig. 1 depicts this relationship and summarizes the role of each sub-system in development of the grid [4].

AMI is not a single technology; rather, it is a configured infrastructure that integrates a number of technologies to achieve its
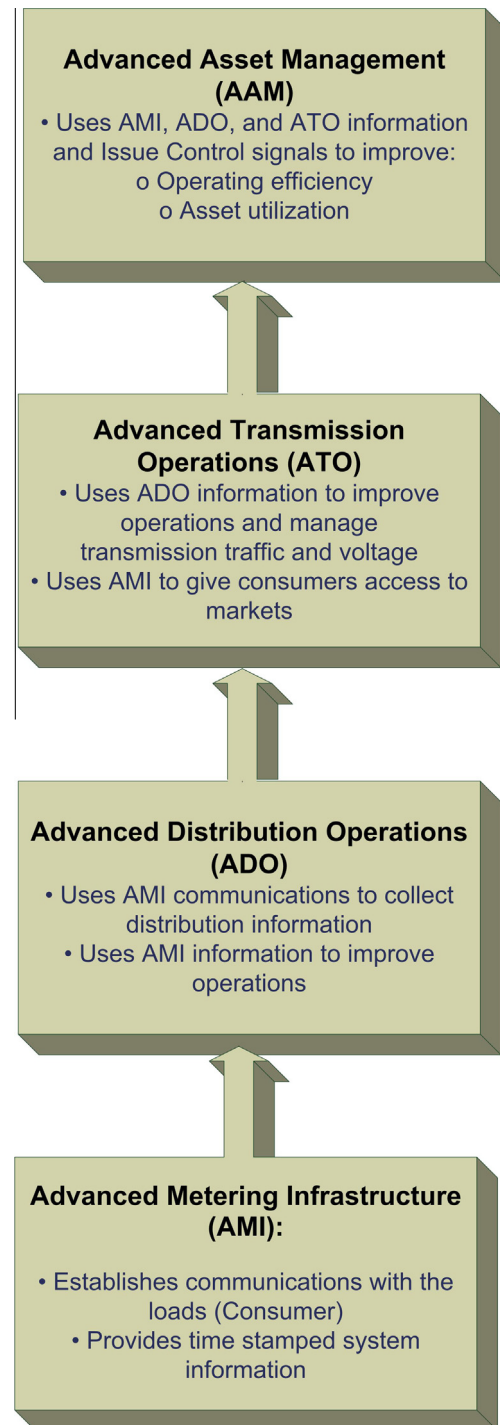
Fig. 1. An overview of Smart Grid sub-system sequence.

goals. The infrastructure includes smart meters, communication networks in different levels of the infrastructure hierarchy, Meter Data Management Systems (MDMS), and means to integrate the collected data into software application platforms and interfaces [4]. As shown in Fig. 2, the customer is equipped with an advanced solid state electronic meter that collects time-based data. These meters can transmit the collected data through commonly available fixed networks, such as Broadband over Power Line (BPL), Power Line Communications, Fixed Radio Frequency, as well as public networks such as landline, cellular and paging. The metered consumption data are received by the AMI host system.
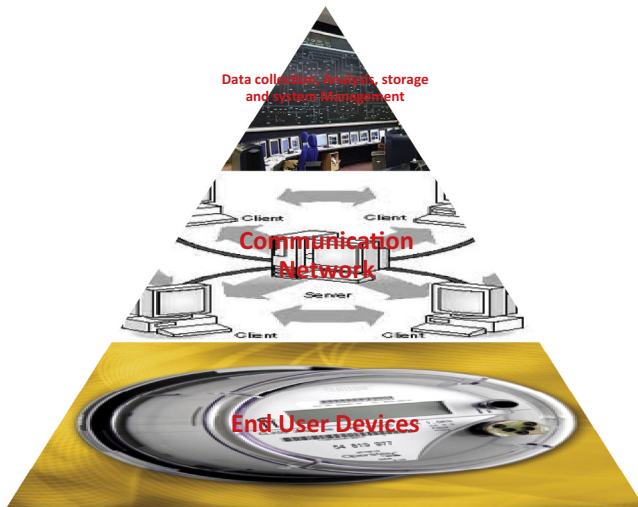
Fig. 2. Schematic representation of AMI.

Subsequently, it is sent to a MDMS that manages data storage and analysis and provides the information in a useful form to the utility service provider.

AMI enables a two-way communication; therefore, communication or issuance of command or price signal from the utility to the meter or load controlling devices are also possible [5].

2.2. Sub-systems of AMI

AMI is not limited to electricity distribution; it covers gas and water networks too. Although the infrastructures for metering different forms of energy are very similar in several aspects, they still differ in some traits. . Electric meters are typically fed from the same electric feed that they are monitoring. This is not the case for gas and water meters. Flow meters are typically powered by stored energy, i.e., batteries; therefore, have utilization constraints. These constraints are more evident in communication since power is needed for transmitting and receiving signals. Meters also have embedded controllers to manage the metering sensor, a display unit, and a communication module which is generally a wireless transceiver. Technical aspects of AMI are wide and vast; therefore, in this paper we only cover issues associated with utilization of AMI in electrical Smart Grids.

2.2.1. Smart devices

End user devices are comprised of state-of-the-art electronic hardware and software capable of data collection or measurement in desired time intervals and time stamping. These devices have an established communication with remote data center and are capable of transmission of such information to various parties in required time slots set by system administrator. Unlike Automatic Meter Reading (AMR), communication in AMI is bidirectional; therefore, smart devices or load controlling devices can accept command signals and act accordingly. At the consumer level, a smart device is a meter that communicates consumption data to both the user and the service provider. In-Home Displays (IHD) illustrate the smart devices' data to consumers; making them aware of their energy usage. Utility (electricity, gas, water) pricing information supplied by the service provider enables load controlling devices (e.g. smart thermostats) to regulate consumption based on pre-set user criteria and directives. Where Distributed Energy Resources (DER) or storages are available, the system can come up with an optimized solution in terms of share of each source in answering the demand.

From the measured phenomenon point of view, smart meters have three distinct categories in broadest view: electrical, fluid, and thermal. There are also a number of sensors or devices that measure factors like humidity, temperature and light which contribute in utility consumption. The sensors could be expanded based on the needs and desire of user or system designer, considering their cost and functionality. Home automation systems deal with the proper selection, placement and utilization of various sensors within the home premises. Smart meters have two functions: measurement and communication, and therefore each meter has two sub-systems: metrology and communication. The metrology part varies depending on a number of factors including region, measured phenomenon, required accuracy, level of data security, application. There are also multiple factors, including security and encryption, which define the suitable communication method. There are a number of essential functionalities meters should have regardless of the type or quantity of their measurement. These functionalities include [6]:

- *Quantitative measurement:* the meter should be able to accurately measure the quantity of the medium using different physical principles, topologies and methods.
- *Control and calibration:* although varies based on the type, in general, the meter should be able to compensate the small variations in the system.
- *Communication:* sending stored data and receiving operational commands as well as the ability to receive upgrades of firmware.
- *Power management:* in the event of a primary source of energy going down, the system should be able to maintain its functionality.
- *Display:* customers should be able to see the meter information since this information is the base for billing. A display is also needed as demand management at customer end will not be possible without the customer's knowledge of the real time consumption.
- *Synchronization:* timing synchronization is critical for reliable transmission of data to central hub or other collector systems for data analysis and billing. Timing synchronization is even more critical in case of wireless communication.

Based on the aforementioned remarks, key features of smart electricity meters can be summarized as follows:

- Time-based pricing.
- Providing consumption data for consumer and utility.
- Net metering.
- Failure and outage notification.
- Remote command (turn on/off) operations.
- Load limiting for Demand Response purposes.
- Power quality monitoring including: phase, voltage and current, active and reactive power, power factor.
- Energy theft detection.
- Communication with other intelligent devices.
- Improving environmental conditions by reducing emissions through efficient power consumption.

2.2.2. Communication

Smart meters should be able to send the collected information to the analyzing computer and to receive operational commands from operation center. Therefore, standard communication is an important part of AMI. Considering the number of users and smart meters at each center, a highly reliable communication network is required for transferring the high volume of data. Design and selection of an appropriate communication network is a meticulous

process which requires careful consideration of the following key factors [7]:

- Huge amount of data transfer.
- Restriction in accessing data.
- Confidentiality of sensitive data.
- Representing complete information of customer's consumption.
- Showing status of grid.
- Authenticity of data and precision in communication with target device.
- Cost effectiveness.
- Ability to host modern features beyond AMI requirements.
- Supporting future expansion.

Various topologies and architectures can be used for communication in Smart Grids. The most practiced architecture is to collect the data from groups of meters in local data concentrators, and then transmit the data using a backhaul channel to central command where the servers, data storing and processing facilities as well as management and billing applications reside [4]. As different types of architectures and networks are available for realization of AMI, there are various mediums and communication technologies for this purpose as well. Examples are:

- Power Line Carrier (PLC).
- Broadband over Power Lines (BPL).
- Copper or optical fiber.
- Cellular.
- WiMax.
- Bluetooth.
- General Packet Radio Service (GPRS).
- Internet.
- Satellite.
- Peer-to-Peer.
- Zigbee.

At AMI level, devices within the premises of the house communicate with each other as well as the utility network through smart meters. This network, in short, could be called in-home network. At upper layer, the Home Area Networks (HAN) communicates with the utility provider, forming another network that could be called utility network.

HANs connect smart meters, smart devices within the home premises, energy storage and generation (solar, wind, etc.), electric vehicles as well as IHD and controllers together. Since their data flow is instantaneous rather than continuous, HANs required bandwidth vary from 10 to 100 Kbps for each device, depending on the task. The network however, should be expandable as the number of devices or data rate may increase to cover office buildings or large houses. The calculated reliability and accepted delay are also based on the consideration that the loads and usage are not critical. Given the above requirements and considering the short distances among nodes that enable low power transmission, wireless technologies are the dominant solutions for HANs. These technologies include 2.4 GHz WiFi, 802.11 wireless networking protocol, ZigBee and HomePlug [8]. Zigbee is based on the wireless IEEE 802.15.4 standard and is technologically similar to Bluetooth. Home Plug, on the other hand, transmits data over the electrical wiring existing at the home. There is still no unique standard or practice for in-home communication in the market; however, Zigbee, and to lesser extent Home plug and ZWave, are the dominant solutions. Advantages of Zigbee include providing wireless communication, low power consumption, flexibility and economic efficiency. The main disadvantage of Zigbee is the low bandwidth. In commercial buildings, a wired technology named BACnet is the prominent communication protocol. Recently, a wireless version of BACnet

has become available using short range wireless networks such as Zigbee.

As shown in Fig. 3, utility networks have four levels: core backbone, backhaul distribution, access points and HAN. The smart meters typically act as the access points. HANs will connect to the access points in their immediate above layers. The information will then be taken from access points to aggregation points through backhaul distribution. Although aggregation points are usually local substations, they could be communication towers too. The requirement for this network is the same as HANs; however, network topology is important in this regard. If data from each appliance is to be transferred to aggregation point, then a higher bandwidth is needed. Backup power is not required for smart meters as they are not considered critical; however, backup power is needed at aggregation points. Currently, PLC addresses the communication needs between in-home system and aggregation points. If communication at the aggregation point is meant to be distributed to each, or most of the smart devices inside the home rather than the meter, then higher rate of transfer and more bandwidth is needed which PLC would not be able to provide. The Advantages of PLCs are their low cost and expansion and penetration in utility provider's territory. Their disadvantages however, include the low bandwidth of up to 20Kbps, and data distortion around transformers which necessitates bypassing transformer points using other techniques. PLC is more or less the prominent practice in current market due to the aforementioned advantages and also because this grid is already up and running, minimizing the deployment cost.

PLC is specifically valuable in remote locations where the number of nodes (consumers) is relatively low and no wireless (cellular, GPRS) coverage is available. When either the number of nodes increases or metering intervals decrease, then higher bandwidths are required to achieve higher data resolutions for control or Demand Response (DR) reasons. The aforementioned, along with availability of reliable wireless technologies in urban areas, led to utilization of Mesh networks. In Mesh networks, in order to propagate information to the end point, each node is responsible for collecting its own data, as well as relaying the information by other nodes in the network. The wireless mesh networks are mainly owned and operated by utility companies. These networks are capable of supporting up to 900 MHz through unlicensed radio spectrums. As the demand for bandwidth increases, broad band technologies such as IEEE 802.16e, mobile WiMAX and broadband PLC are going to play a key role in newer installations. Today, the Long Term Evolution (LTE) standard for wireless technology is believed to answer the market's demand. LTE enables high speed, high capacity wireless communication with good Quality of Service (QoS) as well as low latency. These characteristics make LTE suitable for critical applications in SG as well as for Neighborhood Area Networks, Wide Area Networks, substation automation and many more. The improved version of LTE, LTE-Advanced, has higher capacity with increased peak data rate of 1 Gbps for the downlink and 500 Mbps for the uplink, higher spectral efficiency, increased number of simultaneously active subscribers, and improved performance at cell edges [9]. It has been estimated [10] that by 2020 the annual LTE-based communication nodes shipment will surpass 5 million units.

Table 1 compares some of the available communication technologies [11].

Although utility providers are aware of the potential of LTE application, a number of obstacles should be lifted before LTE dominates the market. Cost and spectrum are the two main factors that prevent utility companies from adopting private LTE networks. On the other hand they are hesitant to rely on public LTE networks. For many years, utility companies have used specific DR applications that utilize private communication networks by default. These companies argue that the higher resilience against natural
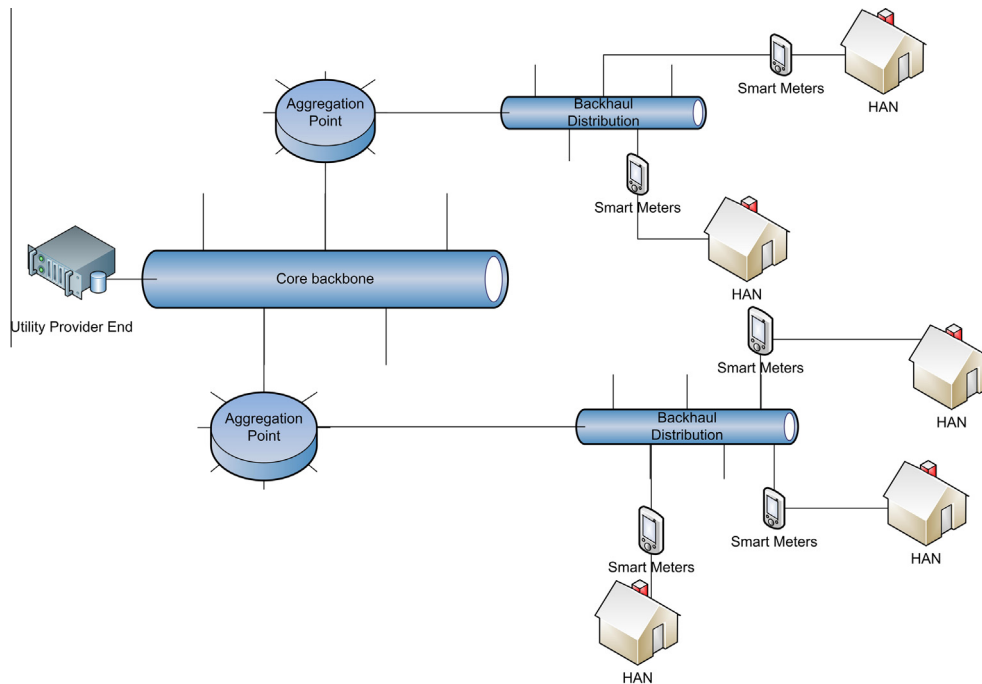
Fig. 3. Overview of utility network.

Table 1
Comparing the different features of available communication technologies for AMI.

	LTE-A	3G (HSPA+)	PLC	802.22
Latency (ms)	<5	<50	<10	<20
Data rate (Mbps) Download/upload	1000/ 500	28/11	3/3	18/18
Range (km)	100	10	5	100
Main disadvantage	–	Limited number of supported connections	Alternate technology (bypass) needed at transformers	No QoS due to faulty spectrum sensing

disasters, the ability to maintain service throughout a utility's service territory, avoidance of prioritization of other services when recovering from outages and the cost of service make the private networks a superior option over commercial services. More and more commercial service providers are partnering with utilities to provide communications for Smart Grid applications. They have encouraged many technological changes, such as the general movement toward integrated platforms and open standards for utility communication functions thus facilitated opportunities for qualitatively better communication systems [8].

2.2.3. Data Management System

At the utility provider end, a system for storing and analyzing the data for billing purposes is needed. It should also handle DR, consumption profile and real time reactions to changes and emergencies in the grid. Modules of such multi modular structure are listed below [3]:

- Meter Data Management System.
- Consumer Information System (CIS), billing system, and the utility website.
- Outage Management System (OMS).
- Enterprise Resource Planning (ERP), power quality management and load forecasting systems.
- Mobile Workforce Management (MWM).
- Geographic Information System (GIS).
- Transformer Load Management (TLM).

MDMS could be considered the central module of the management system with the analytical tools required for communication with other modules incorporated within it. It also has the responsibility to perform validation, editing and estimation on the AMI data to ensure accurate and complete flow of information from customer to the management modules under possible interruptions at lower layers. In existing AMIs with data collection intervals of 15 min, the collected data is huge and in order of terabytes referred to as "Big Data" [12]. Managing and analyzing such Big Data requires special tools. Sources of data in Smart Grids, not necessarily electrical grid, that create the Big Data are as follows:

- AMI (smart meters): collecting consumption data at given frequency.
- Distribution network automation system: collecting data for real-time control of the system that could be up to 30 samples per second per sensor [13].
- Third-party systems connected to the grid, e.g. storages, Distributed Energy Resources or electric vehicles.
- Asset management: communication between central command and smart components in the network including updating firmware.

Different vendors have different definitions for MDMS and design their system based on their specific concept. Therefore, the number or types of additional features or applications vary from one vendor to another. Some developed MDMS systems make

the data available only for use by other applications, while other products include additional application suites in their system. Regardless of features or complexity, all MDMS suites should be able to address three demands: improvement and optimization of operation of utility grids, improvement and optimization of utility management, and enabling customer engagement. Data analytics have become one of the hottest topics in Smart Grids. The purpose is to use all the available data from inside and outside of the grid, connect them together with available data analysis and data mining techniques, and extract useful information for decision makings. From an infrastructure and hardware point of view, the following components are necessary for such a system [12]:

- *Data center infrastructure:* the building hosting the system and all related auxiliary systems, i.e., backup power, ventilation, etc.
- *Servers:* hardware needed for data handling.
- *Storage system:* all hardware needed for storing data and connecting with other hardware in the system.
- *Data base system:* software needed for data analysis.
- *Virtualization systems:* allow more efficient use of discrete storage and computing resources.

Since the collected data contains critical personal as well as business information, the storage facilities should be disaster proof and all required back up and contingency plans for different scenarios should be carefully designed for them. The cost associated with such provisions is huge. Virtualization and cloud computing have been suggested as a solution for this problem [14]. Virtualization allows all available resources to be merged together in order to improve the efficiency and return on investment; however, it requires additional technology and complexity. Cloud computing enables access to virtual resources in different locations; yet, it brings serious concern regarding the security of data. Cloud computing can also be problematic since different regulations and laws apply to the data collected in different locations. Cloud computing however, reduces the cost of special purpose data centers as it uses the capacity of different service providers.

3. Security challenges in AMI

As the number of smart meters increase exponentially, security issues associated with SG and AMI grow substantially from within the system as well as outside. Detailed information of customers' consumption is critical as it can reveal their life style. Transmission of data over long distance as well as storing the data in various places for re-transmission or analysis can also create vulnerabilities in terms of data theft or manipulation. The price signal and commands received at consumer end are also potential areas for cyber and physical attack for the purpose of espionage, damaging infrastructure or power theft. Furthermore, consumer's peace of mind is critical in the success of smart meters and expansion of AMI. If consumers believe that their personal data is used against their will, or experience poor service or power quality due to external manipulation of the system by unauthorized parties or hackers, then they most likely resist the implementation of AMI. Potential health hazards and higher bills after installation of such smart meters will also affect the consumers' decision. The government is taking these issues seriously and is working on procedures to guarantee customers' privacy of information. The government is also launching campaigns to increase the public's knowledge on smart meters and to address their legitimate concerns regarding health and cost issues. Utility companies as well as installation technicians are also playing an important role in this regard.

Given its importance, in this paper we discuss the security issue from three different aspects: maintaining the privacy of consumer's information, resilience of system against cyber or external attacks, and the power theft.

3.1. End user's privacy

Conventional meters were only capable of measuring and displaying the aggregate consumption. The data was collected manually in intervals defined by utility company for billing. Smart meters however, are capable of collecting information with higher frequencies, i.e., every 15 min. Initial AMI deployed projects in Ontario, Canada, sustain readings at intervals of 5 to 60 min [15]. Current technologies even allow for measurements every minute [16]. By analyzing smart meter's data, it is possible to perform "consumer profiling" with an alarmingly high accuracy. Examples range from how many people live in the house, duration of occupancy, type of appliances, security and alarming systems, to inferring special conditions such as medical emergencies or new born baby.

Profiling allows extracting residents' behavior even without utilization of sophisticated algorithms and computer aided tools. Murrill and colleagues [16] have shown that it is possible to identify the use of major appliances in a house, by analyzing only a 15 min interval cumulative energy consumption data. Molina-Markham et al. [18] have shown that with the current general statistical schemes it is possible to identify the usage pattern from AMI data even without the detailed signatures of appliances or previous training.

This data is valuable to third parties, from insurance companies to entertainment agencies and government authorities. Once you have access to the network data in AMI or SG, you will also have access to the customer's name and address information collected and stored for billing purpose. Although obtaining detailed information is one of the objectives of SG, the process can backfire when such detailed information is collected and used without the customers' consent.

The importance of privacy will be clearer when one takes into account the number of households covered by AMI, currently and in the future. It is expected that by 2015, as many as 65 million smart meters will be operating in the United States [16]. In Ontario, Canada, as one of the pioneers in AMI deployment, 4.7 million smart meters have been commissioned and 3.8 million Ontarians are being billed on Time Of Use system as of February 2012 [17]. To discuss the users' privacy in more details, it is necessary to define Load Signature (LS) first. LS falls into the premises of Electric Load Intelligence (ELI) which is a broad term describing state of studying detailed usage pattern of electric loads for developing intelligent applications to augment value of electricity. In simple form, ELI is the act of collecting consumption data of customers for detailed analysis purposes for modern application usage such as AMI and SG. LS could be defined as electrical behavior of a device while in operation. Each device has different measurable behaviors. From consumption point of view, there is a unique attribute or "signature" in each electrical device consumption behavior that could be measured at meter point. Typical variables are voltage, current and energy or power. One way to protect the consumers' privacy is to make it impossible for unauthorized parties to distinguish load patterns and signatures. Kalogridis et al. [19] introduced "load signature moderation" technique to facilitate consumers' privacy protection. The technique basically re-shapes the overall pattern of data to make distinguishing load patterns and signatures impossible. The technique incorporates three methods of hiding, smoothing and mystifying consumption using combination of grid and storage/battery as power source. Pfitzmann et al. [20] defined the whole procedure as "undetectability".

There are legal discussions associated with data collection in AMI and SG in some countries. For example, in Canada Information and Privacy Commissioner of Ontario has issued guidelines for building privacy into smart meters data management system. The commissioner tried to address the privacy of information in the three domains that are involved in SG and AMI: IT, business practices and networked infrastructures. It is mentioned that there is no single formulation to cover security requirements in all these fields and each domain has its own requirements, measures and considerations. Therefore, by introducing the following seven fundamental principles that form the "Privacy by Design" (PbD) concept, commissioner aimed at ensuring freedom of choice and personal control over one's information, as well as gaining a sustainable competitive advantage for organizations.

1. *Proactive not Reactive; Preventative not Remedial:* PbD approach is proactive rather than reactive. This means PbD anticipates and prevents privacy invasive events before they happen.
2. *Privacy as the Default Setting:* the idea is to have privacy part of the default setting of the system. In this case, the consumer does not need to activate the privacy setting as it is built into the system by default.
3. *Privacy Embedded into Design:* privacy will be embedded into the design and architecture of the systems rather than being a separate practice or technology attached to the system. Privacy will be an integral part of the system without affecting its overall functionality or diminishing with time.
4. *Full Functionality — Positive-Sum, not Zero-Sum:* PbD seeks to provide all legitimate interests and objectives in a win–win approach, not through a dated, zero-sum approach where unnecessary trade-offs are made. PbD avoids showing false contradiction in its approach, such as privacy vs. security, demonstrating that it is possible to have both.
5. *End-to-End Security — Full Lifecycle Protection:* PbD will be embedded into the system prior to collection of the first bit of information and will be extended throughout the entire lifecycle of the collected data. The aforementioned ensures that all data are securely retained and if needed securely destroyed at the end of the process.
6. *Visibility and Transparency — Keep it Open:* PbD seeks to assure all stakeholders that the system operates according to the stated promises and objectives regardless of their business practices or used technologies, and it is open to independent verification. System components and operations will be visible and transparent to users and providers.
7. *Respect for User Privacy — Keep it User-Centric:* PbD requires designers and operators to keep customers satisfied by offering strong privacy defaults, appropriate notification, and user-friendly options.

3.2. Security against external cyber or physical attacks

There is a relatively big difference between AMI and SG in terms of communication and network needs and requirements due to their functionality, components, range and architecture. Understanding the communicational needs of each layer is important in determining suitable technology for deployment of each application or layer of the grid/network. Six applications or layers play role in SG: Advanced Metering Infrastructure, Demand Response, wide-area situational awareness, Distributed Energy Resources and storage, electric transportation, and distribution grid management [8]. Many security requirements in AMI are the same as those of typical IT networks; however, there are some unique security requirements that are described below:

Confidentiality: Confidentiality can be translated as privacy of customer's consumption pattern and information which was discussed before. In brief, the metrology and consumption information shall remain confidential. This means physical theft of meter to access the stored data, unauthorized access to the data by other connected automated systems through gateways, as well as customer's access to other customers' information should be prevented. At AMI head end, customer information shall remain confidential and only authorized systems will have access to specific sets of data.

Integrity: Although the head end of AMI in utility provider's premises is in a physically secured environment, its multiple interfaces with many other systems make it vulnerable by nature. Integrity in AMI is applicable to the transmitted data from meter to the utility as well as control commands from utility to the meter. Integrity means preventing changes in the data received from meter, and in the commands sent to the meter. Hackers aim to breach the integrity of the system, pretending they are authorized entities and issue commands to carry out their attacks. In comparison with electromechanical meters, smart meters are resilient against physical or cyber-attacks. Smart Meters should also be able to detect cyber attacks and ignore all issued control commands to avoid breach in the integrity of the system.

Availability: Availability concerns vary based on the type of information communicated in the system. Some data are not critical; therefore, they can be collected in bigger time intervals, and the estimated values can be used instead of the actual ones. However, sometimes it is important that the actual values be collected in very short time intervals, e.g. every minute. The main reason for unavailability of data is component failure. Component failure may be due to physical damage, software problem, or human tampering with the meter. Communication failure can also be a source of unavailability. There are many reasons for communication failure such as interference, cut cables, path degeneration, loss of bandwidth, network traffic, etc.

Accountability: Also known as non-repudiation or non-denial, accountability means that the entities receiving the data will not deny receiving it and vice versa, i.e., if the entities did not receive the data, they cannot state they have done so. This is specifically important from financial point of view in AMI as well as in the actual metrology data and responses to control signals. Accountability requirement is particularly a concern, because different components of an AMI system are usually manufactured by different vendors and owned by different entities, i.e., customers, service providers, etc. Accurate time stamp of information as well as time synchronization across AMI network is also important in accountability. Audit logs are the most common way to ensure accountability; however, these audit logs are vulnerable themselves as explained in the next section. In the smart meters all metered values, changes to the parameters and tariffs should be accountable since they are the basis for billing.

More information on the aforementioned terms is available in ISO/IEC standard. ISO/IEC Information Security Management Systems (ISMS) standards, introduced the international ISO/IEC 27000 series named: Information technology-Security techniques-Information Security Management Systems-Overview and vocabulary. ISO/IEC 27000 presents the entire ISMS standards and gives the readers an overview of the family. It also provides a glossary of fundamental terms and definitions used in the ISO/IEC 27000 family.

The attacks against AMI should be studies from another perspective too: the attackers and their motivations. This is especially important when it comes to designing counter measures. Table 2 categorizes attackers and their motivation for this purpose.

It is evident that a single solution is not sufficient for securing the network. Cleveland [21] discussed the threats to the system's security as well as some technologies and policies that can be used to improve the system's security. Security risk assessment of

Table 2
AMI potential attackers, their motivation and the tools they use.

Attacker	Motivation	Tool
Customers	Personal reasons	Personal knowledge or assistance from criminals
Criminals	Financial, sabotage or terroristic	Creating software and hardware to tamper with AMI
Insiders	Various	Unethical use of the system's trust, illegal use of their authority and knowledge
Institutions	Using private information for various reasons, denial of service	Using expertise, authority, resources and vulnerabilities of system or its components

assets, security compliance reporting or security attack litigation are a few methods that can be used to ensure customers' security. Other security technologies including (but not limited to): Intrusion Detection Systems (IDS), firewalls with Access Control List (ACL), Network and System Management (NSM) or Public Key Infrastructure (PKI).

To conclude, some of the security constraints in AMI are [21]:

- Smart meters must be revenue grade certified. This makes changes and upgrades to counter security vulnerabilities difficult.
- Smart meters are generally installed in insecure locations as they have to be easily reached; therefore, physical security of meters is hard to achieve.
- Some sections of the AMI network are carried out by low bandwidth technologies such as Zigbee, WiFi or PLC while other sections are high bandwidth with high traffic. Therefore, the throughput will have a negative effect on security attempts as sending large certificates to all meters with high frequency would not be possible.
- Some AMI networks use public communication services such as cellular networks. These networks have limited security compared to networks especially designed for certain purposes.
- The functionality of the overall system requires many other systems to have access to the AMI data at the utility end. In order to have a uniform security over the network, these systems will need to have coordinated security policies and technologies. The aforementioned is difficult to achieve since in many cases different systems are owned and operated by different entities.

3.3. Power theft

Electrical losses can happen at every stage; generation, passing through step-up transformers and switch gears, transmission, distribution, and utilization. Generally, losses during generation are technically definable, while losses in transmission and distribution are hard to quantify. Losses can also be categorized as technical and Non-Technical Loss (NTL). A technical loss could be calculated; however, a NTL is hard to measure. Nevertheless it is possible to calculate a NTL if the technical loss is known.

Total Energy Loss = Energy Supplied − Bills paid

Total Energy Loss = NTL + TL

NTL = Energy Supplied − Bills Paid − TL

NTL during Transmission and Distribution (T&D) of electricity is difficult to detect, calculate and prevent, causing a major problem for utility. Technical loss is considered natural because of power dissipation in lines and components. It is estimated that T&D loss worldwide is more than the total installed generation capacity of Germany, UK and France. The annual global loss is about $25 billion. Recovering as little as 10% of the annual global loss could result in about 83000 GWh of recovered electric energy, and reduce carbon dioxide emissions by 9.2 million tons annually [22]. Smith [23] states that NTL forms 10–40% of the total generation capacity of developing countries. Given the aforesaid statistics,

it is interesting to know that power theft accounts for a major portion of NTL. Technically, power theft can cause overload on generators, which may lead to over voltage since utility providers do not have an estimate of real consumption. This can cause trip in generation units and result in black outs. Since sufficient reactive power is necessary in order to have a good power factor and flat voltage over the feeders, power theft can make total load flow calculations faulty and make Volt-Ampere Reactive compensation difficult.

Traditionally, the electro-mechanical meters used for metering purposes offered little or no security and were easy to manipulate. Theft in electro-mechanical meters may be realized using the following methods [24]:

- Direct connection to distribution lines.
- Grounding the neutral wire.
- Attaching a magnet to electromechanical meter.
- Stopping the coil from rotating by blocking it.
- Damaging the rotating coil i.e. by hitting it.
- Reversing input output connections.

Using smart meters can eliminate or minimize the aforementioned issues. Smart meters are capable of recording zero readings and informing the utility companies through AMI. In the second theft method mentioned above, smart meter assumes that the circuit is not closed and does not perform reading. The rotating coil is not the case any more in smart meters, so the other methods are also not the case for smart meters [24]. There are also more complex techniques for power theft that do not involve the meter directly. Current Transformer (CT) tampering is one of them. CTs are generally used to match the grid current rating with the meter rating for meters of large loads. Secondary side wires of CTs are generally insulated; however, it is possible to damage this insulation and tap these wires. Based on the number of wires tampered, the meter can be forced to read less or even zero current amounts. The other method is to exchange the position of damaged wires, causing phase shift and altering the meter reading.

Table 3 summarizes theft techniques in conventional meters and their effect on smart meters.

Some of the stealing techniques used in electro-mechanical meters work in systems with smart meters and AMI too. Meddling with data can happen at three different stages: (i) during data collection, (ii) when data is stored in the meter, and (iii) as the data transits across the network. Meddling with data during collection can happen with both conventional and smart meters. Interfering with data at the other two stages can only happen with smart meters. Mclaughlin et al. [25] created an "attack tree" depicting possible ways of power theft, as shown in Fig. 4. The authors say that the different methods of power theft can be translated into forge demand or manipulation of demand data.

In comparison with conventional systems, AMI makes tampering meters more difficult using data loggers. The loggers are capable of recording power outages to the meter or inversion of power flow. Attackers planning to use inversion or disconnecting techniques need to also erase the logged events stored in the meter. Therefore, its removal falls into the second category of tampering with stored data in the meter. If attackers access the stored data of smart meter they will have complete control over the meter as

Table 3
Theft techniques in conventional meters and their corresponding counter measure in smart meters.

| Theft technique	Effect	Counter measure in smart meters
Direct connection to distribution lines	Zero reading at the meter	Capable of recording zero readings and informing utility provider through AMI
Grounding the neutral wire	Energy meter assumes the circuit is not complete and does not measure	Capable of recording zero readings and informing utility provider through AMI
Attaching a magnet to electromechanical meter	Magnetic field effects the coil's motion and makes it move slowly or even stop	No rotating coil in smart meters
Blocking the coil and preventing its rotation	Affects the coil's motion and makes it move slowly or even stop	No rotating coil in smart meters
Damaging the rotating coil i.e. by hitting it	Affects the coil's motion and makes it move slowly or even stop	No rotating coil in smart meters
Reversing input/output connections	The coil starts moving in reverse direction, which is also a method to create lower reading	No rotating coil in smart meters
Current Transformer (CT) wire tampering	By damaging wires' insulation at secondary side and taping them. Based on the number of wires tampered, the meter can be forced to read less or even zero	Tamper proof enclosure
Current Transformer (CT) phase shift	Changing the position of damaged wires can cause phase shift which alters the meter reading	Tamper proof enclosure
In three phase meters, neutral is kept open and only one out of three phases is used	Electromechanical meter assumes that no energy is passing through it to the customer	Earth Leakage (EL) indicator flashes
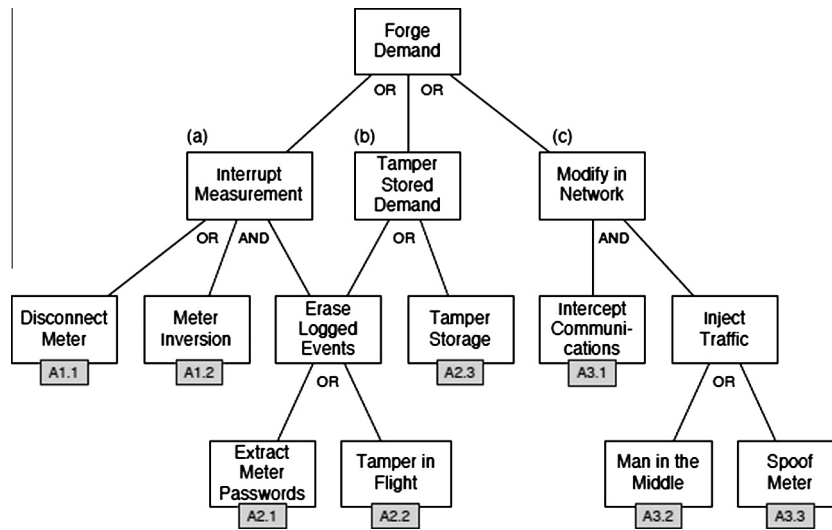
Fig. 4. Attack tree in power theft.

the Time of Use tariffs, received or executed commands, event logs, consumption and time stamps, and the firmware reside there. In usual cases of power theft, the firmware and whole stored data in the meter is not the point of interest for attackers; rather manipulating stored total demand and auditing logs is sufficient for them. This requires meter's password.

In another scenario, the data could be altered while it is being transferred over the network. This comprises of injecting false data into the system, or intercepting communications within the infrastructure. This type of attack is possible at each node of the infrastructure. If the attack takes place at an aggregation point or backhaul link, the data for a set of meters or consumers will be compromised. To do so, attackers need to either interpose on the backhaul link, or access to communication channel to modify or inject false data between meter and utility. As AMI can use cryptography and authentication for communication, attackers need to obtain encryption keys which are stored in the meter. If the authentication and encryption processes or the integrity protocol between meter and utility are not done correctly, attackers can use spoofing techniques to send their fake demand values or event log to the utility end. If the authentication process is faulty but an encrypted communication exists between meter and utility, then a node between meter and utility on the backhaul is needed by attacker to mimic meter for the utility and vice versa during the

encrypted communication to obtain cryptographic keys. This form of attack is called Man In the Middle [25].

Different techniques have been developed and introduced to estimate and locate power theft. These techniques either utilize smart meters or work independently, e.g. Central Observer Meter proposed [26], Genetic Algorithm-Support Vector Machines [27], Power Line Impedance [28], and Harmonic Generator [22]. A number of mathematical approaches are also introduced to detect power theft. Support Vector Machine Linear, Support Vector Machine-Radial Basis Function, Artificial Neural Network-Multi Layer Perceptrons and Optimum Path Forest classifier are among them [24].

4. Complimentary topics

4.1. Standards and protocols

Communication within a network requires a universal language and agreed standards. Although it might look complicated and difficult to gather all players together under one roof, much of the work has been already done. Major existing protocols for building automation include: ZigBee, ZWave, BACnet, LonTalk, Modbus, C-Bus, 1-Wire, xPL, xAP, x10, VSCP, oBIX and few others. For

Automatic Meter Reading (AMR) the domination is with ZigBee, Modbus, M-Bus, DLMS/IEC62056, IEC61107 and ANSI C.12.18.

DLMS/COSEM is the common language in AMR/AMI or generally, Demand Side Management for participating partners. DLMS or Device Language Message Specification is a generalized concept for abstract modeling of communication entities. COSEM or Companion Specification for Energy Metering sets the rules, based on existing standards, for data exchange with energy meters. The role and function of DLMS/COSEM can be defined as:

1. An object model to view the functionality of the meter as seen at its interface(s).
2. An identification system for all metering data.
3. A messaging method to communicate with the model and to convert the data to a series of bytes.
4. A transporting method to relay the information from the metering equipment to the data collection system

DLMS has been developed and maintained by DLMS User Association. The association has been co-opted by the IEC TC13 WG14 to create the international version of the DLMS as IEC 62056 series of standards. In this joint work, the DLMS User Association provides maintenance, registration and conformance testing services for this new international standard, while COSEM includes a set of specifications that defines the Transport and Application Layers of the DLMS protocol [29].

DLSM has four sets of specifications:

- *Green Book:* describes the architecture and protocols.
- *Yellow Book:* covers all the questions concerning conformance testing.
- *Blue Book:* describes the COSEM meter object model and the object identification system.
- *White Book:* contains the glossary of terms.

For a product conformity to DLMS Yellow Book means conformance to IEC62056 set of standards. The IEC TC13 WG 14 groups the DLMS specifications under the common heading: "Electricity metering - Data exchange for meter reading, tariff and load control".

- IEC 62056-21: Direct local data exchange (3d edition of IEC 61107) describes how to use COSEM over a local port (optical or current loop).
- IEC 62056-42: Physical layer services and procedures for connection-oriented asynchronous data exchange.
- IEC 62056-46: Data link layer using HDLC protocol.
- IEC 62056-47: COSEM transport layers for IPv4 networks.
- IEC 62056-53: COSEM Application layer.
- IEC 62056-61: Object identification system (OBIS).
- IEC 62056-62: Interface classes.

4.2. Sub-metering

Bulk metering measures the total energy used by the entire building or site, including the common areas and amenities. The total amount is then divided among the building's residents based on a factor, e.g. the size of residential units. This is an unfair method of billing since someone may live in a larger unit but have smaller energy consumption, and vice versa. Sub-metering, as opposed to bulk-metering, denotes measuring utility consumption for individual units in a residential complex or Heating, Ventilation and Air Conditioning System (HVAC) in a commercial complex. The aim is to have accurate utility consumption for precise billing. The advantage of this system is that consumers have to pay only for the energy they consumed. Sub-meter's data could also be indicative of

equipment performance with regard to economic and comfort standards. In brief, while smart metering provides data longitudinally, sub-metering provides consumption data laterally thus, increasing the resolution of the acquired data. This is specifically suitable for operation and maintenance personnel and the occupants, as they can plan for their operational needs, fine tuning and consumption relatively. A report by Navigant Consulting Ltd. [30] suggests that sub-metering in the multi-residential buildings reduced the average electricity consumption by 34% for non-electrically heated buildings, and by 27% for electrically heated buildings. There are a few technologies and techniques that can reduce this amount of consumption without major costs and changes in the network. The following, is the benefits of sub-metering according to the National Science and Technology Council [31]:

- Identifying performance improvements and guiding preventive maintenance.
- Enabling quick response to failures of components, assuming the meters are linked to an Energy Management System or a Building Management System.
- Supporting life cycle financial planning by developing a dataset for trend analysis.
- Focusing accountability for building operations on the facilities department, encouraging building managers to control energy and water consumption.
- Verifying savings from energy and water improvement projects.
- Helping to compile baseline energy use for setting contractual terms with an energy service company.
- Helping with energy and water upgrades in buildings by comparing usage in similar facilities.
- Facilitating charge-backs to departments or other campus units to encourage energy and water efficiency measures.
- Providing data to building occupants to promote awareness about the effect of their behavior on energy and water consumption.
- Lowering peak demand charges on electrical utility bills through virtual aggregation of different sub-meters.

4.3. Costs

Costs associated with the deployment of AMI arise from three sources:

- Smart devices at user points.
- Communication network.
- Data collection, analysis, storage and system management.

Implementation of each of the abovementioned layers requires specific hardware and software. Once the software is designed for the system, further expansion is possible with minimum cost. Since designers consider contingencies, the main expansion costs would be related to the end point devices, probable extra hardware for communication, data collection and storage facilities. These costs could also be reduced by careful consideration of contingencies during initial design and implementation.

The continuous advancements in electronics and digital systems further reduces the cost of both the smart meters and communication and data collection facilities making it difficult to calculate a valid capital deployment cost. However, it is possible to estimate a percentage for different segments in the overall deployment cost of the AMI. Regardless of the maintenance cost or potential costs due to the regional and environmental laws and regulations, the deployment cost for AMI is on the falling edge. Fig. 5 shows the AMI deployment cost in different sectors as reported by Electric Power Research Institute [5].
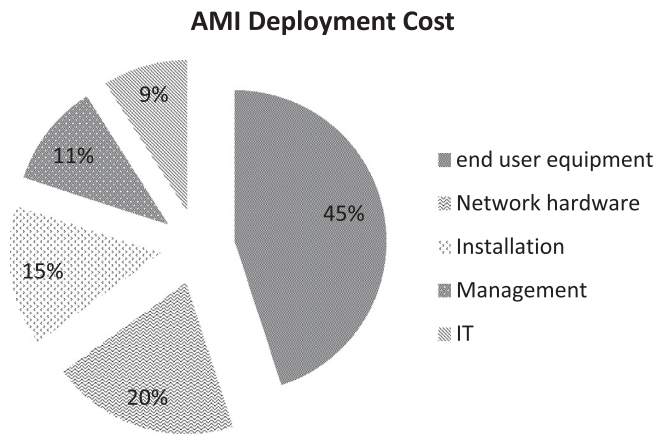
AMI Deployment Cost

Fig. 5. AMI deployment cost.

4.4. Batteries

Meters are generally considered to have the life span of 15–20 years. However, low power requirement and high battery performance are necessary to allow such life span.

The current dominant battery technology for AMI application is lithium battery chemistries, namely lithium-thionyl chloride or Li-SOCl2. Lithium batteries are disposable and have lithium as their anode. Different chemistries of these batteries come with different types of cathodes and electrolytes. In lithium-thionyl chloride batteries, the cell contains a liquid mixture of thionyl chloride ($SOCl_2$) and lithium tetrachloroaluminate ($LiAlCl_4$) which act as the cathode and electrolyte, respectively. These types of batteries have large energy density suitable for extremely low-current applications where long life is necessary, and generally are not available for individual consumers. The primary use of these batteries is in commercial and industrial applications where the batteries cannot be replaced by the consumers.

From the battery chemistries available, Lithium thionyl chloride (LiSOCL2) offers the highest specific energy (energy per unit weight) and energy density (energy per unit volume). Lithium's large electric potential is instrumental in high energy density of this type of batteries, and also contributes to their high voltage which is typically 2.7–3.9 VDC. Lithium cells use a non-aqueous electrolyte which enables certain lithium batteries to operate in extreme temperatures of $-55\,°C$ to $125\,°C$. For AMI applications Bobbin cells lithium batteries are the best. These batteries consist of one cylinder of cathode surrounded by one cylinder of anode material. The small common surface area results in low rate discharge and can deliver approximately 30% more energy than the equivalent spiral cells. Bobbin cells are used for AMI because they have the highest energy density and voltage, operate in a wide temperature range, and have an extremely low annual self-discharge. The- disadvantages of this type of battery however, are their limited current capability and the resulting passivation effect that may further limit their use in high current applications [32,33]. As a two-way communication is needed in AMI meters, higher current pulses are essential. While retailers come up with different solutions to improve the performance of their batteries and to address the aforementioned issues, so far the lithium thionyl chloride batteries remain the best available option for AMI applications.

The specific features of an ideal battery for AMI application are:

- *End life indicator/alarm:* it is necessary for the operator to know the proper time of battery replacement. Without such notification, the utility companies would pay huge costs for unnecessary battery replacements
- *High energy density:* typically 3.6 V and 19 Ah

- Wide operating temperature range: the current LiSOCL2 batteries operate in the temperature range of $-50\,°C$ to $+85\,°C$
- *Low self-discharge:* typically 0.5 to 1 percent per year
- *Extended life expectancy:* batteries' life expectancy is very much dependant on the external factors such as environmental conditions, communication topology and devices, measured quantity, etc. However, an ideal battery for AMI application should have a minimum life expectancy of 12 or 15 years. Considering the huge cost for battery replacement in a network, some utility providers even require a minimum life expectancy of 20 years.

Silicon Labs [6] suggests that each battery could cost over a dollar for the meter provider. Assuming that a typical "D" size Li-SOCl2 battery can provide 16–19 amp-hours with steady-state system current of 10 micro amps costing 50 to 75 cents per amp-hour in high volume of sales, the fuel cost of a meter during its desired life span of 20 years is:

10 micro amps * 24 h/day * 365 day/year * 20 years * $0.75 amp/hour = $1.31 in battery/system cost. This means even when there is no need for battery replacement, the system owners should consider at least $1.31 as the "fuel" cost of each meter with life expectancy of 20 years.

Silicon Labs [34] estimates the price of a battery used in water or gas meter application is about $15. Every year retailers ship millions of meters. The aforementioned highlights the importance of optimized power consumption to minimize the cost.

5. Conclusion

The 21st century brought great technological advancements in the field of electrical energy distribution and utilization. These advancements face many challenges and require novel tools and approaches to tackle these challenges. Advanced Metering Infrastructure is one such tool. Thanks to the innovations and developments in electronics, instrumentation, communication and data handling, an infrastructure has been materialized that can perform real time data acquisition from consumers, transmit the data and return the executive commands to the loads. This valuable tool allows the operators and utility companies to have firsthand information on the status of their network for planning and performance optimization purposes. The acquired data could also be utilized for consumption regulation, at both consumer and provider's ends. Diagnostic and notification tools provided by AMI, such as leak detection in water and gas networks or cyber or physical attacks detection, can save millions of dollars in damage prevention and maintenance cost for energy providers and consumers. The possibility of incorporating advanced services such as fire detection or notification and monitoring via mobile apps further increased the networks' value and attracted public attention towards the SG and AMI. Enhanced security for transmitted information and delivered power is another advantage of AMI. Furthermore, AMI allows the users to better control their consumption pattern. It also offers higher power quality and stability.

Our survey shows that Advanced Metering Infrastructure is a relatively new concept which needs improvement in the areas of communication, data analysis and control schemes. However, taking into the account the global energy market's situation and environmental concerns that motivates governments, companies and consumers to fuel AMI research and utilization, the prospect of AMI looks promising.

References

[1] Momoh JA. Smart grid design for efficient and flexible power networks operation and control. In: Power Systems Conference and Exposition, PSCE '09. IEEE/PES; 2009. p. 1–8.

[2] The History of Electrification: The Birth of our Power Grid, Edison Tech Center. <http://edisontechcenter.org/HistElectPowTrans.html> [accessed November, 2013].

[3] SAIC Smart Grid Team for The Energy Policy Initiatives Center. San Diego smart grid study final report. University of San Diego School of Law; 2006.

[4] National Energy Technology Laboratory for the U.S. Department of Energy. Advanced metering infrastructure, NETL modern grid strategy; 2008.

[5] Electric Power Research Institute (EPRI). Advanced metering infrastructure (AMI); 2007.

[6] Silicon Laboratories, Inc. Smart metering brings intelligence and connectivity to utilities, green energy and natural resource management. Rev.1.0. <http://www.silabs.com/Support%20Documents/TechnicalDocs/Designing-Low-Power-Metering-Applications.pdf> [accessed August, 2013].

[7] Depuru SSSR, Wang L, Devabhaktuni V. Smart meters for power grid: challenges, issues, advantages and status. Renewable and sustainable energy reviews; 2011. p. 2736–42.

[8] US Department of Energy. Communications requirements of smart grid technologies; October 5, 2010.

[9] Agilent Technologies. Introducing LTE-Advanced; 2011 <http://cp.literature.agilent.com/litweb/pdf/5990-6706EN.pdf> [accessed May, 2014].

[10] Navigant Research. LTE Networks for Smart Grid Applications; 2013.

[11] Fischione C. Toward a development of LTE for smart energy systems. Scandinavian workshop on test-bed based wireless research, Stockholm; November, 2013.

[12] Deign J, Salazar CM. Data management and analytics for utilities. FC Business Intelligence Ltd.; 2013.

[13] Anderson D, Zhao C, Hauser C, Venkatasubramanian V, Bakken D, Bose A. A virtual smart grid. IEEE power & energy magazine; December 13, 2011. p. 49–7.

[14] Cohen R. Is cloud computing really cheaper? Forbes; 2012 <http://www.forbes.com/sites/reuvencohen/2012/08/03/is-cloud-computing-really-cheaper/> [accessed August, 2013].

[15] Cavoukian A. Privacy by design. Take the challenge. Information and privacy commissioner of Ontario, Canada; 2009.

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

[17] Information and Privacy Commissioner of Ontario, Canada. Building Privacy into Ontario's Smart Meter Data Management System: A Control Framework; 2012.

[18] Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D. Private memoirs of a smart meter; 2010.

[19] Kalogridis G, Efthymiou C, Denic SZ, Lewis TA, Cepeda R. Privacy for smart meters: towards undetectable appliance load signatures. In: Proc IEEE international conference on smart grid communications, Gaithersburg, Maryland; October 2010.

[20] Pfitzmann A, Hansen M. A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management; 2010.

[21] Cleveland FM. Cyber security issues for advanced metering infrastructure (AMI). In: IEEE power and energy society general meeting: conversion and delivery of electrical energy in the 21st century; 2008. p. 1–6.

[22] Depuru SSSR, Wang L, Devabhaktuni V. Electricity theft: overview, issues, prevention and a smart meter based approach to control theft. Energy Policy 2009;39:1007–15.

[23] Smith TB. Electricity theft—comparative analysis. Energy Policy 2003;32:2067–76.

[24] Anas M, Javaid N, Mahmood A, Raza SM, Qasim U, Khan ZA. Minimizing electricity theft using smart meters in AMI; 2012.

[25] McLaughlin S, Podkuiko D, McDaniel P. Energy theft in the advanced metering infrastructure. In: Critical information infrastructures security. Lecture notes in computer science, vol. 6027. 2010. p. 176–87.

[26] Bandim CJ, Alves JER, Pinto AV, Souza FC, Loureiro MRB, Magalhaes CA, et al. Identification of energy theft and tampered meters using a central observer meter: a mathematical approach. In: Proceedings of the IEEE PES transmission and distribution conference and exposition, Rio de Janeiro, Brazil; September, 2003. p. 163–8.

[27] Nagi J, Yap KS, Tiong SK, Ahmed SK, Mohammad AM. Detection of abnormalities and electricity theft using genetic support vector machines. In: Proceedings of the IEEE region 10 conference TENCON, Hyderabad, India; January, 2009. p. 1–6.

[28] Pasdar A, Mirzakuchaki SA. Asolution to remote detecting of illegal electricity usage based on smart metering. In: Proceedings of the international workshop on soft computing applications, Oradea, Romania; August, 2007. p. 163–7.

[29] DLMS User Assosiation, <http://www.dlms.com>.

[30] Navigant Consulting Ltd. for EnerCare Connections Inc. Evaluation of the impact of sub-metering on multi residential electricity consumption and the potential economic and environmental impact on Ontario; 2012.

[31] National Science and Technology Council Committee on Technology. Submetering of building energy and water usage; 2011.

[32] Jacobs S. Smart Power for AMI Smart Meters. WaterWorld; 2013 <http://www.waterworld.com/articles/print/volume-28/issue-8/advanced-metering-infrastructure/smart-power-for-ami-smart-meters.html> [accessed August, 2013].

[33] Pilarzyk J. White paper – lithium carbon monofluoride coin cells in real-time clock and memory backup applications. rayovac.com. Rayovac Corporation; 2007.

[34] Silicon Laboratories, Inc. How to design smart gas and water utility meters for the utmost in power efficiency. Rev. 1.1; 2013 <http://www.silabs.com/Support%20Documents/TechnicalDocs/Low-Power-MCU-Metering.pdf> [accessed August, 2013].