A Survey on Advanced Metering Infrastructure and its Application in Smart Grids

Ramyar Rashed Mohassel[1], Alan S. Fung[2], Farah Mohammadi[3], and Kaamran Raahemifar[4]
[1,3,4] Department of Electrical and Computer Engineering, [2] Department of Mechanical and Industrial Engineering
Ryerson University
Toronto, Canada
[1]rrashedm@ryerson.ca; [2]alanfung@ryerson.ca, [3]fmohamma@ee.ryerson.ca; [4]kraahemi@ryerson.ca

***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 the 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 intends to focus on AMI, which is responsible for collecting all the data and information from loads and consumers, as the foundation for SG. AMI is also responsible for implementing control signals and commands to perform necessary control actions, including Demand Side Management (DSM). In this paper we introduce SG and its features, establish the relation between SG and AMI, explain three main subsystems of AMI and discuss related security issues.**

Keywords—Advanced metering; smart metering; AMI; Smart Grid.

I. INTRODUCTION

With emerging challenges and issues in the 21st century energy market, changes in the electrical systems are inevitable. The challenges to the 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 along with security of the system against external cyber or physical attacks, economics of power systems (from maintenance costs to equipment renovation and network expansion) and the need for better control schemes for complex systems[1]. Europe and North America have both modernized their energy generation and distribution systems and switched to Smart Grid (SG) as a solution to such challenges.

While the first electrical grids date back to the late 1800s, the 1960s were the golden era of power grids in developed countries. During this era, the penetration rates of the distribution network 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 boomed, technically and economically. The last decades of the 20th century experienced an increase in electricity demand due to introduction of new consumers, such as entertainment systems and dependence on electricity as the main source of heating, cooling and ventilation (HVAC). Furthermore, the rate of energy consumption experienced significant fluctuation. 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, consumption rates were lower at night causing unbalanced consumption that left 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 and by changing its approach to Demand Side Management (DSM). The 21st century came along with innovations and advancements in different sectors that allowed enhancement of Smart Grid concept. The improvements in Information Technology (IT) 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 shifting their consumption to off-peak times. Improvements in electrical storages and renewable energies such as wind, solar, tidal or geothermal, combined with environmental concerns, led to the integration of these technologies into electrical systems to form the decentralized generation concept [2].

Smart Grids modernized the traditional concept and functionality of electrical grids by using IT to obtain data from network components, from power producers to consumers, and use them properly to maximize the efficiency and reliability of the system. There is no clear boundary and definition for intelligence of a Smart Grid, since a number of factors are 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 [1,2,3]. It should also address the challenges to load handling and demand adjustment, incorporation of advanced services, flexibility, sustainability, end-to-end control capability, market enabling, power and service quality, cost and asset optimization, security, performance, self-healing and restoration [1,2,3].

II. ADVANCED METERING INFRASTRUCTURE (AMI)

A. AMI and Smart Grid

To achieve an intelligent grid, a string of sub-systems should be realized. The solid establishment and functionality of each sub-system is crucial in the overall SG performance, since each layer's output serves as the feed for the next layer.

978-1-4799-3010-9/14/$31.00 ©2014 IEEE

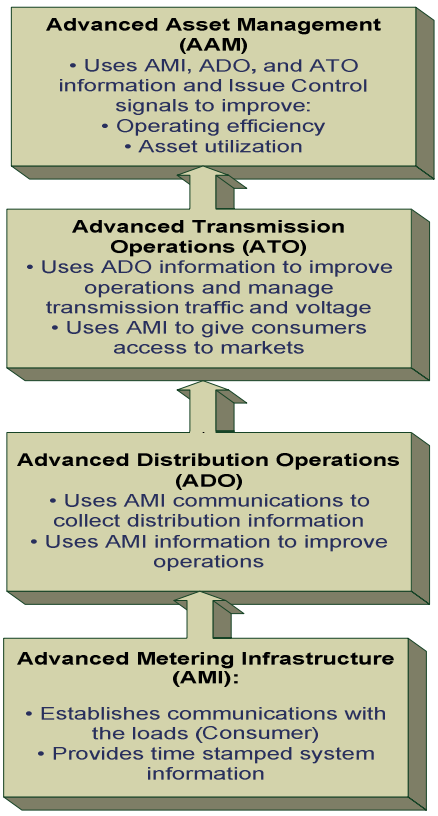

Fig. 1. Smart Grid sub-system sequence overview

Fig.1 depicts this relationship and summarizes the role of each sub-system in development of the grid [4].

B. Definition

Unlike SG, AMI cannot be defined in a single sentence. AMI is not a single technology; rather it is a configured infrastructure that integrates a number of technologies to achieve its goals. The infrastructure includes smart meters at the consumer end, communication networks at different levels of the infrastructure hierarchy to connect two ends, Meter Data Management Systems (MDMS) and the means to integrate the collected data into software application platforms and interfaces at utility provider or head end [4]. 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. The metered data are received by the AMI host system. Subsequently, they are sent to a MDMS that manages data storage, analyzes and provides the information in a useful form to the utility service provider. AMI enables two-way communication; therefore, communication or issuance of command or price signals from the utility provider to the meter or load controlling devices are also possible [5].

III. SUB-SYSTEMS OF AMI

AMI is not limited to electricity distribution; it also covers gas and water networks. Although the infrastructures for metering different forms of energy consumption are similar, there are slight differences between them. Electric meters are typically fed from the same electric supply that they are monitoring whereas 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. In this paper we only cover issues associated with utilization of AMI in Smart Grids.

A. Smart devices

End user devices are comprised of state-of-the-art electronic hardware and software, capable of time stamping and of data collection or measurement in desired time intervals. These systems have established communication with remote data center and are capable of transmitting such information to various parties in time slots required and set by the system administrator. Unlike Automatic Meter Reading (AMR), communication in AMI is bi-directional; therefore, smart devices or load controlling devices can accept command signals and act accordingly. At the consumer level, smart meters communicate consumption data to both the user and the service provider. In-Home Displays (IHD) display data from the smart device so that consumers are aware of their energy usage. Utility pricing information supplied by the service provider enables load control devices (e.g. smart thermostats) to regulate consumption based on pre-set user criteria and directives. Where 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.

Smart meters have three distinct categories in broadest view: electrical, fluid and thermal. There are also a number of sensors that measure factors such as humidity, temperature and light all of which contribute to utility consumption. The sensors could be expanded based on the needs and desire of user or system designer, considering their cost and functionality. Smart meters have two functions: measurement and communication; therefore, each meter has two sub-systems: metrology and communication. The metrology part varies depending on a number of factors including region, measured phenomenon, accuracy, technical requirement, level of data security, application, etc. There are also multiple factors, including security and encryption that define the suitable communication method. There are some essential functionalities meters should have, regardless of the type or quantity of their measurement, including [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 it varies based on the type, the meter should be able to compensate the small variations in the system.

Communication: the ability to send stored data and receiving operational commands as well as upgrades for firmware.

Power management: in the event of loss of primary source of energy, the system should be able to maintain its functionality.

Display: customers should be able to see the meter's information since this information is the basis for billing. A display is also needed as demand management at customer end will be impossible without the customer's knowledge of the real time consumption.

Synchronization: timing synchronization is critical for reliable transmission of data to the central hub or other collector systems for data analysis and billing. Timing synchronization is even more critical in case of wireless communication.

Thus, key features of smart electricity meters are 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 (phase, voltage and current, active and reactive power, power factor), energy theft detection, communication with other intelligent devices and improving environmental conditions by reducing emissions through efficient power consumption.

B. Communication

Smart meters should be able to send the collected information to the analyzing computer and to receive operational commands from the operation center. Therefore, standard two-way communication is an important part of AMI. Considering the number of users and smart meters at each end point, 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, restricting data access, confidentiality of sensitive data, showing status of grid, cost effectiveness, authenticity of data along with precision in communication with target device, ability to host modern features beyond AMI and future expansion.

There are various topologies for communication in SG. The most practiced architecture is to collect the data from groups of meters in local data concentrators and then transmit them using a backhaul channel to central command, where the servers, data storing and processing facilities as well as management and billing applications reside [4]. Since different types of architecture and networks are available for realization of AMI, there are various mediums and communication technologies for this purpose as well: Power Line Carrier (PLC), Broadband over power lines (BPL), copper or optical fiber, cellular, WiMax, Bluetooth, GPRS, Peer-to-Peer, Zigbee and a few others. At AMI level, communications are between devices in a home while at upper layer, they occur between Home Area Networks (HAN) and the utility provider. These two, in short, could be called in-home and utility networks.

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 varies 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. HomePlug, on the other hand, transmits data over the existing electrical wiring at the home. There is still no unique standard or practice for in-home communication on the market; however, Zigbee and to lesser extent HomePlug 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. 2, 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 the layers immediately above them. The information will then be taken from access points to aggregation points through backhaul distribution. Although aggregation points are usually local substations, they could also be communication towers. 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 the aggregation point, then a higher bandwidth is needed. Backup power is not required for smart meters as they are not considered critical; however, it is needed at aggregation points. Currently, Power Line Carrier (PLC) addresses the communication needs between the 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 to the meter, then higher rate of transfer and more bandwidth is needed that would exceed the capacity of PLC to support the communication required. 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 that necessitates re-routing via other techniques. PLC is 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 of

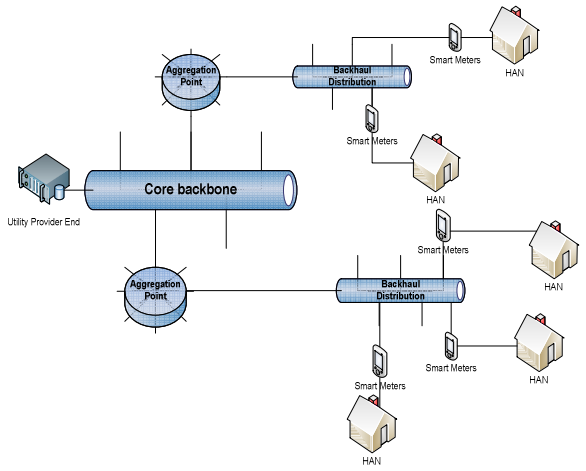

Fig. 2. Overview of utility network

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, broadband technologies such as IEEE 802.16e, mobile WiMAX and broadband PLC (BPL) are going to play a key role in newer installations. For many years, utility companies have used specific DR applications that utilize private communications networks by default. These companies argue that the higher resilience against natural 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 and have encouraged many technological changes, such as the general movement toward integrated platforms and open standards for utility communication functions. They have thus facilitated opportunities for qualitatively better communication systems [8].

C. Data Management System

At the utility provider end, a system should exist to store and analyze the data for billing purposes. It should also handle DR, consumption profile and real time reactions to changes and emergencies in the grid. Modules of such multi modular structure include [3]:

- Meter Data Management System (MDMS)
- Consumer Information System (CIS), billing systems, 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 (VEE) on the AMI data to ensure accurate and complete flow of information from customer to the management modules despite possible interruptions at lower layers. In existing AMIs with data collection intervals of 15 minutes, the amount of collected data is huge and in the order of terabytes, referred to as "Big Data" [9]. Managing and analyzing such Big Data requires special tools. Sources of data in Smart Grids, not necessarily the electrical grid, that create the Big Data are as follows: AMI (smart meters); distribution network automation system (collecting data for real-time control of the system that could be up to 30 samples per second per sensor [10]); third-party systems connected to the grid, e.g. storages or DER; and, finally, asset management system, which is responsible for 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 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 SG. The purpose is to use all the available data inside and outside of the grid, connect them together with available data analysis and data mining techniques, and extract useful information for decision making. From the infrastructure and hardware point of view, the necessary components of such a system are [9]: data center infrastructure which is the building hosting the system and all related auxiliary systems, i.e., backup power, ventilation, etc.; servers and hardware needed for data handling; storage system; database software needed for data analysis and virtualization systems, which allow more efficient use of discrete storage and computing resources.

Since the collected data is very important, utility providers are vigilant about data storage. The storage facilities should be disaster proof, and all required back up and contingency plans for different scenarios should be carefully designed. The cost associated with such provisions is huge. Virtualization and cloud computing have been suggested as a solution for this problem [11]. 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; however, there are serious concerns 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 does however reduce the cost of special

purpose data centers by using the capacity of different service providers.

IV. Security 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 of it. Transmission of data via communication channels over long distance, as well as storing it 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 potential areas for cyber and physical attacks for the purpose of espionage, damaging infrastructure or power theft. Furthermore, if consumers suspect their personal data is being used without their will and consent or experience problems in services or power quality due to external manipulation of the system by unauthorized parties or hackers, they are likely to resist the implementation and expansion of AMI. Given its importance, we address three different aspects of the security issue.

A. Privacy of end user's information

Conventional meters were only capable of measuring and displaying aggregate consumption. The data needed to be collected manually at intervals defined by the utility company for billing. Smart meters however, are capable of collecting information with higher frequencies, i.e., every 15 minutes. Initial AMI deployed projects in Ontario, Canada, sustain readings at intervals of 5 to 60 minutes [12]. Current technologies even allow for measurements every minute [13]. By analyzing the smart meter's data, it is possible to perform "consumer profiling" with alarmingly high accuracy. Examples range from how many people live in the house, duration of occupancy, types of appliances, security and alarming systems, to inferring special conditions, such as medical emergencies or a newborn baby. Once you have access to the network data in AMI or SG, you will also have access to the customer's name and address collected and stored for billing purpose. Based on the network's intelligence level or the number of smart technologies used by the consumer, it is possible to access to Internet Protocol (IP) addresses of devices at the consumer end. This data is valuable to third parties, from insurance companies to entertainment agencies and government authorities. Although obtaining detailed information is one of the objectives of SG, the process can back fire when such detailed information is collected and used without the consumers' consent. The importance of privacy will be clearer when one takes into account the present and future number of households covered by AMI. It is expected that by 2015, as many as 65 million smart meters will be operating in the United States [13]. 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 (TOU) system as of February 2012 [14]. Different researches and studies [13,15] have shown that profiling makes it possible to extract residents' behavior even without utilization of sophisticated algorithms and computer aided tools. Murrill and colleagues [13] have shown that it is possible to identify utilization of major appliances in a house, even by analyzing 15 minute interval cumulative energy consumption data. Molina-Markham et al. [15] have shown that with available general statistical schemes, it is possible to identify the usage patterns from AMI data, even without the detailed signatures of appliances or previous training. First, we will define Load Signature (LS). LS falls under the grouping of Electric Load Intelligence (ELI), which is a broad term describing the state of studying detailed usage pattern of electric loads for developing intelligent applications to enhance 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's consumption behavior that could be measured at meter point. Typical variables are voltage, current and energy or power. One way to protect the consumer's privacy is to make it impossible for unauthorized parties to distinguish load patterns and signatures. Kalogridis et al. [16] introduced the "load signature moderation" technique to facilitate the protection of consumer privacy. 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 a combination of grid and storage or battery as the power source. Pfitzmann et al. [17] defined the whole procedure as "undetectability".

There are legal discussions associated with data collection in AMI and SG in some countries. For example, The Information and Privacy Commissioner of Ontario, Canada has issued guidelines for building privacy into smart meters data management. 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" concept (PbD), the commissioner aimed to ensure freedom of choice and personal control over one's information, as well as gaining a sustainable competitive advantage for organizations [14].

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 ensure users that the highest level of privacy of their data is a rule in any given IT system or business practice. 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. 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. 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.

B. Security against external cyber or physical attacks

There is a relatively big difference between AMI and SG in terms of communication and network needs due to their functionality, components, range and architecture. Understanding the communicational needs of each network is important in determining suitable technology for deployment of each layer of the network. Six applications play a role in SG: AMI, DR, wide-area situational awareness, DER and storages, 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 described below:

Confidentiality: Confidentiality can be translated as privacy of customer's information as 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's information should remain confidential, and only authorized systems will have access to specific sets of data.

Integrity: Although the head end is physically in a secured environment, its multiple interfaces with many other systems make it vulnerable by nature. Integrity in AMI is applicable to the transmitted data from the meter to the utility as well as control commands from the utility to the meter. Integrity avoids any changes in the received data from meter, and in the commands sent to the meter. Hackers aim at the integrity of the system, pretending they are authorized entities and issue commands to carry out their attacks. Smart meters are resilient against physical and cyber-attacks. Meters will 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 at 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 at 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, 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 for billing as well as in the actual metrology data and responses to control signals. The 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 vital 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.

Based on what was mentioned, it is evident that just a single solution is insufficient for securing the network. Cleveland [18] showed the threats to the system's security as well as some technologies and policies that can be used to improve its security.

C. Power theft

Electrical losses can happen at every stage; generation, passing through transformers and switch gears, transmission, distribution, and utilization. Generally, losses during generation can be defined technically while losses in transmission and distribution are hard to quantify. Losses can also be categorized as Technical Loss (TL) 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 TL is known.

$$\textit{Total Energy Loss} = \textit{Energy Supplied} - \textit{Bills paid}$$

$$\textit{Total Energy Loss} = \textit{NTL} + \textit{TL}$$

$$\textit{NTL} = \textit{Energy Supplied} - \textit{Bills Paid} - \textit{TL}$$

NTL during Transmission and Distribution (T&D) of electricity is difficult to detect, calculate and prevent, causing a major problem for utility providers. 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 combined. 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 [19]. Smith [20] states that NTL forms 10-40% of the total generation capacity of developing countries. Given that, it should be said 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 don't have an estimate of real consumption. This can cause generation units to trip, and resulting 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 Volt-Ampere Reactive (VAR) 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 by [21]: direct connection to distribution lines, grounding the neutral wire, attaching a magnet to the housing, stopping the coil from rotating by blocking it, damaging the rotating coil by hitting it or reversing input and 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. In the case of grounding neutral wire, the smart meter assumes that the circuit is not closed and does not perform a 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.

However, some of the stealing techniques used in electro-mechanical meters do work in systems with smart meters and AMI. 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. [22] created an "attack tree", depicting possible ways of power theft (Fig. 3). The authors say that the different methods of power theft can be translated into forge demand.

In comparison with conventional systems, AMI makes tampering with meters more difficult by using data loggers. The loggers are capable of recording power outages to the meter or any inversion of power flow. Attackers planning to use inversion or disconnecting techniques need also to erase the logged events stored in the meter. If attackers access stored data of smart meter they will have complete control over the meter as the TOU tariffs, received or executed commands, event logs, consumption and time stamps, and firmware reside there. In usual cases of power theft, the firmware and whole stored data is not the point of interest for attackers. It suffices to manipulate stored total demand and audit logs. This requires the meter's password. In another scenario, the data could be altered while 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.

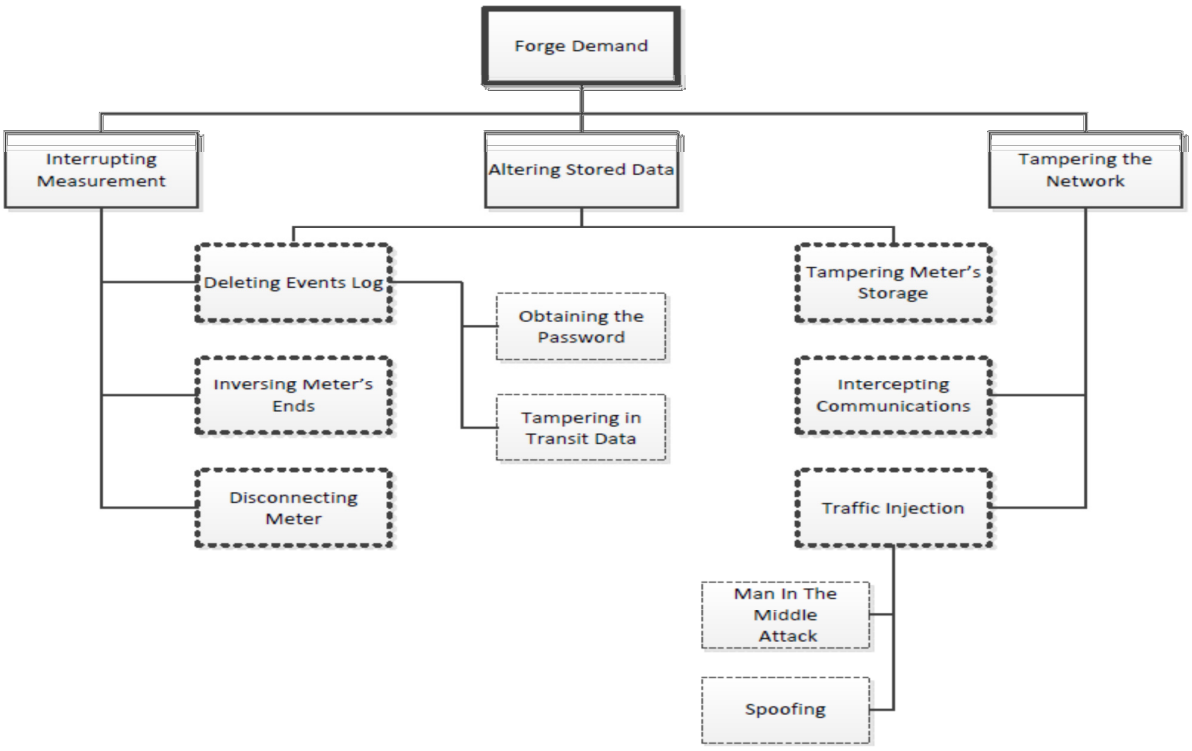

Fig. 3. Attack tree in power theft

If the authentication and encryption processes or the integrity protocol between meter and utility are not formed 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 the attacker needs a node between meter and utility on the backhaul to mimic the meter for the utility and vice versa during encrypted communication to obtain cryptographic keys. This form of attack is called Man In the Middle (MIM) [22].

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 [23], Genetic Algorithm-Support Vector Machines (GA-SVM) [24], Power Line Impedance [25], and Harmonic Generator [19]. A number of mathematical approaches have also been introduced to detect power theft. Among these approaches are the following: Support Vector Machine Linear (SVM-LINEAR), Support Vector Machine-Radial Basis Function (SVM-RBF), Artificial Neural Network- Multi Layer Perceptrons (ANN-MLP) and Optimum Path Forest classifier (OPF) are among them [21].

Perhaps adding a short Conclusion section will be ideal.

REFERENCES

[1] J.A. Momoh, "Smart Grid Design for Efficient and Flexible Power Networks Operation and Control," *Power Systems Conference and Exposition-PSCE'09,* pp.1-8, 2009.

[2] "The History of Electrification: The Birth of our Power Grid," Edison Tech Center. [online] Available at: 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. Available at: http://www.sandiego.edu/documents/epic/061017_SDSmartGridStudyFINAL.pdf

[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, Available at:

http://www.silabs.com/Support%20Documents/TechnicalDocs/Designing-Low-Power-Metering-Applications.pdf

[7] S.S.S.R.Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status", Renewable and Sustainable Energy Reviews, pp. 2736-2742, 2011.

[8] US Department of Energy, "Communications Requirements of Smart Grid Technologies," October 5, 2010.

[9] J. Deign, C.M. Salazar, "Data Management and Analytics for Utilities," *FC Business Intelligence Ltd*., 2013.

[10] D. Anderson, C. Zhao, C. Hauser, V. Venkatasubramanian, D. Bakken and A. Bose, "A virtual smart grid," *IEEE Power & Energy Magazine*, pp.49-57, December 13, 2011.

[11] R. Cohen, "Is cloud computing really cheaper? " Forbes, 2012, [online] Available at: http://www.forbes.com/sites/reuvencohen/ 2012/08/03/is-cloud-computing-really-cheaper/, accessed August, 2013.

[12] A. Cavoukian, "Privacy by Design...Take the Challenge," Information and Privacy Commissioner of Ontario, Canada, 2009.

[13] B.J. Murrill, E.C. Liu and R.M. Thompson II,"Smart Meter Data: Privacy and Cyber security," Congressional Research Service, 2012.

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

[15] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet and D. Irwin, "Private Memoirs of a Smart Meter," *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building BuildSys '10*, pp.61-66, 2010.

[16] G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," *First IEEE International Conference on Smart Grid Communications* (SmartGridComm), 2010.

[17] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," v0.33, 2010. Avilable at:

http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.32.pdf

[18] F.M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century,* pp.1-5, 2008 .

[19] S.S.S.R. Depuru, L. Wang and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy 39*, pp.1007-1015, 2009.

[20] T.B. Smith," Electricity theft—comparative analysis," *Energy Policy 32*, pp.2067–2076, 2003.

[21] M. Anas, N. Javaid, A. Mahmood, S.M. Raza, U. Qasim and Z.A. Khan, "Minimizing Electricity Theft using Smart Meters in AMI," 2012.

[22] S. McLaughlin, D. Podkuiko and P. McDaniel, "Energy Theft in the Advanced Metering Infrastructure," *4th International Workshop*, CRITIS 2009, Bonn, Germany, pp.176-187, 2009.

[23] C.J. Bandim, J.E.R. Alves, A.V. Pinto, F.C. Souza, M.R.B. Loureiro, C.A. Magalhaes and D.F. Galvez, "Identification of energy theft and tampered meters using a central observer meter: a mathematical approach," *Proceedings of the IEEE PES Transmission and Distribution Conference and Exposition*, Rio de Janeiro, Brazil, pp. 163–168, September, 2003.

[24] J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed and A.M. Mohammad, "Detection of abnormalities and electricity theft using genetic support vector machines," *Proceedings of the IEEE Region 10 Conference TENCON*, Hyderabad, India, pp. 1–6, January, 2009.

[25] A. Pasdar, S.A. Mirzakuchaki, "Asolution to remote detecting of illegal electricity usage based on smart metering," *Proceedings of the International Workshop on Soft Computing Applications*, Oradea, Romania, pp. 163–167, August, 2007.