PSERC

Communication Needs and Integration Options for AMI in the Smart Grid

Future Grid Initiative White Paper

Power Systems Engineering Research Center

Empowering Minds to Engineer the Future Electric Energy System

Communication Needs and Integration Options for AMI in the Smart Grid

Prepared for the Project "The Future Grid to Enable Sustainable Energy Systems" Funded by the U.S. DOE

White Paper Team

Vinod Namboodiri
Visvakumar Aravinthan
Ward Jewell
Wichita State University

PSERC Publication 12-05

March 2012

Information about this white paper

For information about this white paper contact:

Prof. Vinod Namboodiri
Wichita State University
Dept. of Electrical Engineering and Computer Science
210 Jabara Hall
Wichita, KS, 67260, USA
Vinod.Namboodiri@wichita.edu, 316-978-3922

Your feedback on the white paper will be welcomed. Send your comments to Vinod Namboodiri.

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: http://www.pserc.org.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
527 Engineering Research Center
Tempe, Arizona 85287-5706
Phone: 480-965-1643
Fax: 480-965-0745

Acknowledgements

This white paper was developed as one of nine white papers in the project "The Future Grid to Enable Sustainable Energy Systems: An Initiative of the Power Systems Engineering Research Center." This project is funded by the U.S. Department of Energy. More information about the Future Grid Initiative is available at the website of the Power Systems Engineering Research Center.

We express deep appreciation to the several reviewers who significantly contributed to the quality of this white paper, as listed below. Their identification here does not constitute endorsement regarding any of the contents of this report.

- Eve Schooler, Intel Corporation
- Abtin Keshavarzian, Robert Bosch Research and Technology Center
- Babak Karimi, Wichita State University

Executive Summary

This white paper analyzes the current state of communications for the advanced metering infrastructure (AMI) and recommends for discussion future actions needed to enable consumer participation in the smart grid. It describes the motivation for AMI, surveys the current state of the art and deployment status, and points out technical, policy, and other challenges in moving forward. This white paper emphasizes technical aspects and capabilities of communication technologies being considered for AMI and describes research challenges that need to be solved to hasten the realization of benefits attributed to the AMI application scenario.

On a global scale, the U.S. has made good progress in deploying the AMI, lagging behind only some European countries in terms of penetration and technical capabilities. In terms of actual communications technologies being used, there seems to be greater consensus on how to build home area networks (HANs) than "backhaul" links that carry data from smart meters to the control center. The consensus on HAN technologies and associated architectures comes about primarily due to the existence of such technologies in residences and commercial premises. Further research is required to evaluate the communication and control model and possible architectures for backhaul options, including infrastructure costs, communication medium, and scalability. In contrast, information security and privacy needs to be addressed more from a HAN perspective due to consumer involvement and their data. Additional challenges that need further research include scalable data collection and aggregation, medium contention resolution in dense deployments, and divergence of global technology adoption trends.

Future actions that are needed at a federal level in terms of communication needs and integration options for meeting AMI goals are the following:

(i) Encouraging more far-reaching investments in backhaul communication infrastructures and providing spectrum access for wireless communication,

(ii) Incentivizing consumers to embrace AMI initiatives and purchase AMI-capable loads, and

(iii) Developing information security and privacy regulations to protect consumers and guide utility reactions to threats and malicious behavior.

This version of the white paper will be revised in the coming weeks. Your feedback on the white paper will be welcomed. Send your comments to Vinod Namboodiri at Vinod.Namboodiri@wichita.edu.

Table of Contents

List of Figure

List of Tables

1. Motivation for AMI

The electric power industry is undergoing major changes in the twenty-first century. Significant developments are occurring in the areas of advanced measurements (synchrophasors, optical sensor technologies, etc.), improved communication infrastructures, renewable energy sources, and electric vehicles (EVs). These changes are expected to influence the way energy is consumed by customers. Advanced metering infrastructure (AMI) initiatives are a popular tool to incorporate these changes for modernizing the electricity grid, reducing peak loads, and meeting energy-efficiency targets. With the introduction of AMI technology, two-way communication between the smart meter (SM) and the control center, as well as between the smart meter and customer loads would be facilitated for many applications, including demand response, dynamic pricing, system monitoring, cold-load pick-up, and the mitigations of greenhouse gas emissions [1]. AMI technology captures and transmits energy use data to a collection point on an hourly or sub-hourly basis, in contrast to standard meters that provide total daily energy usage and a cumulative monthly bill [2].

There are many environmental and economic benefits to utilities, consumers, and society as a whole in adopting AMI technologies, which are summarized in the following subsections.

1.1 Benefits to utilities

Through demand response programs and load management, AMI allows electric utilities to shave peak use. Rather than change the output of a power station, the utilities can better balance the supply of electricity with the demand for electricity through pricing signals. Time-of-use pricing can allow customers to move their electricity consumption to off-peak times with lower rates. Critical peak pricing can enable utilities to charge much higher rates during peak hours of electricity consumption (for example, a hot summer afternoon) to prevent blackouts. An in-home AMI device can be used to provide such dynamically changing information and influence customer behavior. AMI can also provide power quality measurements (voltage sags and swells, harmonics distortion, voltage and current imbalances, and their event durations [3]) to the utility in more detail than that provided by kWh readings alone and, hence, can help plan network expansion and improve power quality. This is in addition to one of the originally conceived benefits of automated meter reading (AMR) where meter readings can be collected on a daily, hourly, or sub-hourly basis without the involvement of an operator. Additionally, AMI offers utilities the capability of building a better outage management system (OMS). Instead of customers calling to report outages, utilities will be able to detect and pinpoint an outage through the AMI communication link to smart meters. This, in turn, can result in shorter outages and more efficient and cost-effective outage restoration. More granular information on outages (especially useful for large-scale outages) will be available for future planning and grid design, and presentation to local and state authorities.

1.2 Benefits to customers/consumers

The AMI provides many benefits also to customers/consumers.[1] Real-time pricing allows consumers to move some of their electricity usage to periods of lower rates. This is especially beneficial to those who are flexible with their electricity use. In-home AMI devices also bring about better awareness by enabling benchmarking of energy usage. Consumers could see (through displays, cellular phones, etc.) how they consume electricity, which can lead to behavioral changes that are more energy efficient. A study in 2006 by the Environmental Change Institute at the University of Oxford showed that direct feedback to electricity customers can result in an energy conservation effect of 5-15% [4]. There could also be options for automated billing, possibly on a daily or sub-monthly basis, instead of one bill at the end of the month. Daily monitoring and/or billing can prevent unpleasant surprises and would allow the consumer to adjust his/her usage accordingly.[2] Finally, AMI can bring about the convenience of bundling the billing of electricity, water, and gas in the near future.

1.3 Benefits to society

Apart from utilities and consumers, the AMI benefits society in general. Financial and environmental gains are associated with conservation, reduced peak loads, and increased reliability. For example, lower operating and maintenance costs will result from improved system efficiency and reliability. The AMI would allow better integration of distributed energy sources and electric vehicles and, together with requiring less power generated due to peak shaving, a reduction in greenhouse gas emissions is expected.

A more detailed list of benefits to utilities, consumers, and society can be found in the 2008 NETL report on AMI [6]. With the benefits of AMI to utilities, consumers, and society as a whole apparent from this section, the next section provides a snapshot of the current deployment status of AMI in the U.S. and other countries, along with details of the communication technologies employed.

---

[1] The term "customer" is typically used when describing something from the standpoint of the utility. The term "consumer" is used when something is described from the standpoint of a user of electric power. There are some instances where both terms may apply, in which case we use them interchangeably.

[2] There has been recent federal oversight on how wireless carriers bill monthly; similar oversight may someday be applied to electric power charges [5].

2. Current Status of AMI

It is clear that AMI can provide many benefits to utilities, consumers, and society. This section details the status of current global AMI deployments, and discusses aspects such as smart meter penetration and the types of communication technologies employed to connect end-user loads to grid operator control centers for monitoring, control, and of course metering. Therefore this section will provide a useful reference point to judge how much further AMI deployments must go before most envisioned benefits are realized, and what issues need to be addressed in the future to enable such a scenario.

2.1 Overview of national and global deployment status

2.1.1 U.S. landscape

Results of the Advanced Metering and Demand Response Survey by FERC (2010 Survey, covering calendar year 2009) indicate that advanced metering penetration and potential peak load reductions from electric power demand response have increased significantly since the last survey in 2008 [7]. Advanced metering penetration (i.e., the fraction of all installed meters that are advanced meters) has reached approximately 8.7 percent in the United States, compared to approximately 4.7 percent in the 2008 FERC Survey (covering calendar year 2007). The upper Midwest, West, and Texas have advanced meter penetrations exceeding 13 percent, with electric cooperatives (which supply about 10% of electric power in the U.S.) having the largest penetration of nearly 25 percent among categories of organizations. Survey results also indicate that use of the internet predominates (> 60%) for residential and non-residential customers in how they obtain information on their electricity use.

2.1.2 International landscape

AMI deployments have grown significantly outside the U.S. as well, although data on smart meter penetration rates is harder to obtain. The question of what is “smart” is a fundamental one and seems to have varying interpretations across the globe.

While the European Union (EU) has set a smart meter target deployment of 80% by 2020, there is little talk about demand response, off-peak usage, and planning for electric vehicles. The main motivation in Europe for installing AMI such as smart meters appears to be limited to the operational efficiency of automatic meter reading (AMR). The diversity of EU member countries and country-specific goals is a big challenge in defining a common smart grid methodology [8]. The European Smart Metering Landscape report in [9] classifies EU countries and Norway into five categories: dynamic movers, market drivers, ambiguous movers, waverers, and laggards. These categories are based on the existence of a regulatory framework and/or a clear strategy for AMI. Dynamic mover countries such as Italy and Sweden have close to 100% advanced meter penetrations, but a large percentage of these only have unidirectional communication capabilities for automated meter reading. Only meters for larger customers can currently perform hourly metering and data handling with further investments required to increase reading frequencies for demand response and load-shifting applications.

In Canada, the provinces of Ontario and British Columbia have introduced mandatory requirements for smart electricity meters for all customers. The largest project involves AMI deployment. Hydro-Quebec plans to install close to 4 million metering points by 2017. Large-scale rollouts to residential customers have only recently begun in Japan and South Korea, but these countries seem to have a clear vision for the adoption of the technology over the course of this decade and could gain from the implementation experiences of early adopters. China is investing massively in the expansion of the nation's energy infrastructure by deploying more advanced electricity meters capable of two-way communication. This will reduce inter-operability issues of needing backwards compatibility to meters that are more limited and capable of only one-way communications. Australia and New Zealand began large-scale smart meter installations in 2009 and 2010, with their adoption driven by regulations in the case of Australia and by the main industry players in New Zealand. Brazil is among the leaders in AMI deployments in Latin America, with the preparation of regulations underway for widespread smart meter deployments throughout the country. With lower electricity consumption than countries such as the U.S. and in Europe, the market driver for such deployments in Brazil is income recovery through anti-tampering systems rather than energy conservation.

2.2 Communication technologies employed from utility control center to smart meters

A communication network for the power grid allows power utility companies to access electricity usage data and services remotely, regardless of their geographic position. Real-time monitoring of transmission and distribution lines for protection against natural disasters or even malicious attacks are all reasons to have a secure, reliable, and scalable communication network for the power grid. Several last-mile options are available for getting a communication network to be operational; broadband technologies such as digital subscriber line (DSL), fiber options (FTTX), and power line carrier (PLC) are some examples. All these technologies have their limitations, however, due to their fixed nature and lack of flexibility.

2.2.1 Power line carrier

When distribution feeders are considered, PLC is well suited because it is a no-cost medium for the utility and is spread along the distribution system. PLC has the potential to transmit data at a maximum rate of 11 kbit/s, and the maximum data rate can be achieved only in a narrow frequency range of 9 to 95 kHz [10]. This low rate of communication is not enough for supporting applications where large amounts of data may be transferred, for example, when a large number of smart meters connected to end-user loads send periodic information using the AMI.

Broadband over power line (BPL) has its limitations as well. The distribution system is consistently affected by voltage transients and harmonics that are unpredictable, and thus is prone to a high level of disturbance. High-frequency signals involved in BPL communication need to bypass transformers to avoid high attenuation [11]. The attenuation in a radial distribution feeder is high, and this would increase the number of regenerators needed. It is expected that a typical 20-mile-long rural feeder needs regenerators on the order of 30 to 100 [12]. Thus, even if the medium of communication is free in BPL, there are infrastructure costs involved. In addition, the high-frequency signals may cause problems by being blocked by voltage regulators, reclosers, and shunt capacitors that are common in long radial feeders [12].

Apart from the above-mentioned challenges of PLC-based technologies, their scalability, stability, and reliability are under scrutiny. Many deployments have been terminated in Australia, Russia, and the United States due to such concerns and the high costs involved [13]. Power line technologies, however, have an advantage that most of the upgrades needed are in substations, which is much easier than making changes at scattered geographic locations over the power grid. For this reason, some utilities rely on this approach as a first step in deploying AMI.

2.2.2 Wired technologies

Another option is to use dedicated wired communication; however, one issue with copper wire connections is interference and attenuation. Fiber optic cables would be a solution to the interference but would increase the cost. It should be noted that the investment required for a fiber optic network would be on the order of $10-100 million for 100 nodes [14]. Newly developing communities could install a fiber optic communication network close to the feeders, thus enabling the infrastructure to be shared for both the power grid and consumer communication needs. One of the advantages of this medium is that the utility would bear only the costs of the terminal equipment and for leasing the line, which would reduce the utility's costs and improve communication. On the other hand, the utility would not have control over the medium because, in most cases, it would not own the dedicated wired network, and would require physical connections that reduce flexibility.

Using the public switched telephone network (PSTN) is another option. It offers a highly reliable, simple, and relatively inexpensive solution and can be used for bi-directional communication. However, the PSTN option is limited by the communication bandwidth offered and the requirement of a telephone line at each meter premise. This is difficult in rural areas, especially in developing countries. The current trend in developed countries is to move away from PSTN to wireless technologies, further decreasing the future potential of being able to rely on dedicated telephone lines to customers. Nevertheless, PSTN could be useful in areas with limited coverage of other technologies.

2.2.3 Wireless

Wireless communication is a promising alternative for distribution-level communication. One of the important characteristics of wireless communication is the feasibility of communication without a physical connection between two nodes, thus ensuring continued connectivity even when local disruptions could bring down infrastructure such as electric poles.

Messaging over cellular networks

Short message service (SMS) is available through most cellular providers, and most users rely on it for sending short text messages. A smart meter could similarly send its reading as a short text message over periodic intervals. The technology allows bi-directional communication where grid operators could send control commands as text messages to the smart meter. Examples of the use of SMS over cellular networks can be found in work such as [15],[16]. The SIM card used in each terminal serves as a unique identifier for a customer. The biggest disadvantage of using such cellular services is the subscription costs owed to third-party carriers that provide the infrastructure. The scalability of this technology is also questionable when millions of meters send messages every 15 to 60 minutes due to the limited bandwidth of cellular technologies.

Table 2.1: Comparison of backhaul wireless communication technologies

Attribute	**WiMAX**	**Wi-Fi**	**ZigBee**	**GSM/UMTS**
Cost	High	Medium	Medium	High
Range	< 1 km, 4 km (rural)	100-200 m	70-100 m	1-2 mi
Max. Data Rate	70 Mbps	54 Mbps	250 kbps	20-800 kbps
Frequency Band	2-11, 10-66 GHz	2.4, 5 GHz	2.4, 5 GHz	700 MHz, 2.1 GHz
Band License	Free and Licensed	Free	Free	Licensed
Robustness	Medium	High	High	Low

Radio Frequency (RF) Technologies

Compared to cellular technologies, an advantage of using RF technologies is that these typically use unlicensed bands that do not incur any carrier costs to the utility. The utility must own only the terminal units, which are relatively cheap and could be integrated with cost-effective local processors. By using multi-hopping, the range of communication could be extended. Three current wireless technologies that are suitable for the long-haul communication from smart meters or data collectors to grid operator control centers are ZigBee, Wi-Fi, and WiMax.

The above-mentioned wireless technologies and their features are summarized in Table 2.1; this table also includes legacy cellular technology based on GSM/UMTS, which is now being upgraded to provide higher data rates.[3] ZigBee has the limitation of lower data rates, which could put into question its ability to handle long-haul communications with a large number of smart meters as sources. WiMax is a long-haul solution with a large communication range and high data rates, but it tends to be costlier. Wi-Fi is a shorter range technology such as ZigBee that could be used even for long-range communication by multi-hopping from one end to another. It provides high data rates and could be a cost-effective option if existing feeder infrastructure is re-used to mount multi-hopping points on electric poles. WiMax is a good alternative for rural areas where feeder sections between consecutive poles tend to be longer than the typical communication range of Wi-Fi. Range issues of Wi-Fi could be mitigated to some extent with improved receivers and directional antennas.

The disadvantages of wireless communication could be interference due to the presence of buildings and trees, which could result in the "multi-path effect" where signals arrive over different paths making the capture and decoding of the signal challenging. But careful planning and design can mitigate such effects. A major concern with a wireless medium is easy accessibility, which could result in security issues. This could be avoided by using security mechanisms presented in prior work like [17].

[3] The newer cellular technologies are commonly referred to as either 3G, 4G, or LTE, based on type and generation to which they belong.

Maintenance can also be harder with communication nodes scattered geographically compared to a power line solution.

2.3 Communication technologies employed in home area networks

With few customer premises enabled by smart meters, very limited practical HAN implementations exist currently. Many customers use energy management systems (EMS) as alternatives to monitoring their power usage and sending control commands through their computers or wireless-enabled phones. This white paper does not discuss such EMS separately and assumes that the smart meter could take on the role of current EMS and additionally communicate with individual loads for demand response, load control, and similar applications.

Table 2.2: Comparison of HAN Communication Technologies

Technology	Data-Rate (Mbps)	Range (meters)	Security	Cost
Ethernet	10-100	100	High	High
PLC	10-100	10-100	High	Medium
Bluetooth	0.7-2.1	10-50	Medium	Low
Wi-Fi	5-100	30-100	Low	Medium
Zigbee	0.02-0.2	10-75	Low	Low

Various wireless technologies such as Bluetooth, Wi-Fi (IEEE 802.11), and ZigBee (IEEE 802.15.4) can be used for implementing an HAN between the smart meter and various loads in the consumer premise. Wired options include Ethernet and PLC. Wired options provide considerable data rates and are inherently more secure than wireless technologies. However, technologies such as Ethernet involve extensive cabling costs and are less flexible than wireless technologies. The usage of PLC for HANs is still in the preliminary stages, and questions about its impact on power quality have not been answered yet. Wireless technologies on the other hand need to handle information security and customer privacy more carefully as they typically utilize a shared broadcast medium. Table 2.2 compares two wired technologies and three wireless technologies. The master-slave architecture of Bluetooth adds a limitation of seven slaves for every master node and can be a constraint in HAN implementation with more loads controlled. Wi-Fi radios provide higher data rates than any other wireless technology, but they consume a higher amount of power. ZigBee technology provides an adequate data rate for AMI communications and consumes less power compared to Wi-Fi, and has a larger communication range than Bluetooth that can cover a typical residence easily. ZigBee, however, is not found as ubiquitously in residences as Wi-Fi.

2.4 Current AMI status summary

On a global scale, the U.S. is behind only some European countries in AMI penetration and technical capabilities of deployments to provide benefits. There is greater understanding of the technologies most suitable for the HAN infrastructure compared to the backhaul links. This is partly due to the low investment required for deploying HANs and the existence of similar consumer networks. For the backhaul, power line technologies offer benefits of easy upgrades, but they also offer limited capabilities that will be a shortcoming over the long term. Wireless technologies meet most communications needs of today and for the near future, but they need to be carefully deployed to mitigate interference and security issues, and require greater infrastructure investments.

3. Discussion - General Requirements and Design Considerations for AMI Communications

This section discusses the impact of emerging communication technologies and applications on AMI deployments over the next decade or two. The issue of designing communication infrastructure to scale up with higher AMI penetration is considered, along with requirements for information security and privacy that are associated with consumer involvement in energy delivery.

Success of the smart grid vision depends on the effective design and implementation of a reliable and economic communication infrastructure at the distribution level. An ideal communication architecture will be flexible and resilient, reuse existing infrastructure of the distribution system to cut deployment and maintenance costs, and provide adequate communication bandwidth to handle large volumes of data and be scalable. Many types of communication techniques, with different levels of maturity, are being employed in emerging deployments by grid operators at the distribution level around the United States, Europe, and Asia. These deployments embody various communication solutions, but only a few have complete end-to-end bi-directional information and control capabilities. It is not yet clear what technology, or combination of technologies, can effectively meet the requirements for large-scale smart grid undertaking at the distribution level where greater automation and consumer participation in energy delivery is sought.

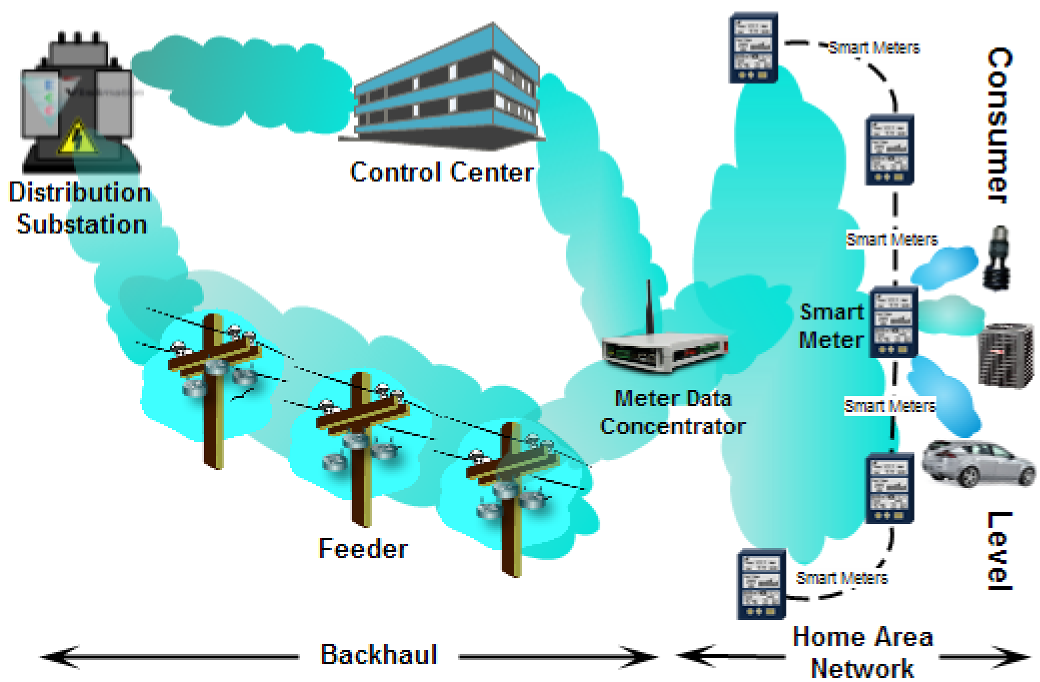

Figure 3.1: Communications for AMI at the distribution level. The communications infrastructure needed (indicated by links shown as clouds) can be divided into the following: (i) backhaul infrastructure communications possibly through feeders, and (ii) consumer/customer premise home area networks.

There are many communication technology and architecture options in deploying the AMI. As shown in Figure 3.1, the end-to-end communication infrastructure can be divided into two major phases: (i) the consumer level home area network (HAN) between a smart meter and various electrical equipment/appliances, (ii) the backhaul link that collects information from smart meters and carries it to the utility control center.

3.1 Backhaul communications infrastructure

The backhaul can either be a direct link from individual smart meters to the utility control center, or a link (or series of links) from a concentrator node, which aggregates data from multiple smart meters through some form of a mesh network, to the control center. There is reasonable consensus on using ZigBee-based star topologies in HANs [22],[21], and ZigBee or Wi-Fi based mesh topologies to collect and aggregate data at concentrators [18], but the technologies and topologies to be used for the backhaul is still an open problem. An approach of deploying the backhaul communication infrastructure is to create a network through the existing feeder infrastructure. This approach has the advantage of reducing costs by reusing existing infrastructure of electric poles and feeder lines if needed. Further, it can also integrate well with sensors deployed on feeder poles to improve distribution automation through applications such as automated fault location and self-healing feeders. Important design choices would include the type of communication technologies, the type of medium (wired or wireless), and whether to use direct links (single-hop communication) or relaying through other intermediate nodes (multi-hop communication). The long-haul communication network to smart meters could reuse existing feeder-level infrastructure to reduce costs.

The following list of requirements is important for any communication architecture to satisfy, but are of particular importance for the backhaul.

3.1.1 Low-latency communications

Any communication technology should be able to provide low-latency communications from the data generation or collection point to the eventual destination. Any control commands from grid operators should similarly reach smart meters and consumers with minimal delay. For the AMI application, a higher latency is tolerable for the data collected from smart meters to the control center, but there are control commands in the other direction (from the control center to smart meters) for controlling loads and remote connect/disconnect, which need to communicate immediately.

3.1.2 Low infrastructure development and maintenance costs

Modernizing the grid involves many upgrades. It is imperative that the cost of developing additional infrastructure is minimized by reusing existing infrastructure where possible. Thus, any communication technology used should be inexpensive, and be able to utilize existing infrastructure (such as feeder poles), and be easy to setup and reconfigure. The technology used should also preferably have low maintenance costs, including fees to third-party providers/carriers.

3.1.3 Scalability

The scale of possible deployments under a single grid operator at the distribution level for AMI could be on the order of hundreds of thousands of nodes or more when smart meters and end-user loads they connect to are included. Any communication technology and the services it provides should be scalable in terms of the technical features it provides, such as data carrying capacity and latency.

3.1.4 Privacy, information security, and network availability

With AMI fostering customer participation in energy delivery, ensuring privacy and information security in general is a challenge. This issue takes on greater dimensions if wireless technologies are involved due to their reliance on a shared broadcast medium. Further ensuring that the communication network is available for operation and control can be critical.

Additional considerations for designing a backhaul communication infrastructure that will reuse feeder-level infrastructure would involve deciding on an adequate communication range, taking into account distances between feeder poles at the distribution level, and the density at which communication nodes should be deployed on electric poles, taking into account costs and benefits. Applications such as the integration of EVs and renewables would require low-latency communications involving consumers and the utility. This would necessitate the inclusion of pervasive computing and communication technologies such as mobile consumer devices into the proposed communications infrastructure for consumer participation. Additional improvements specific to the AMI application will involve looking at the problem of collection and management of data from smart meters. By current standards, each smart meter sends a few kilobytes of data every 15 minutes to a smart meter [19], [20]. When this is scaled up to large numbers, many existing communication architectures will find it difficult to handle the data traffic due to limited bandwidth. Addressing this challenge requires contributions on the design of data aggregation/processing algorithms that preserve useful information from each consumer premise, but at the same time allow significant compression of the overall aggregate when the data is transmitted through the communications infrastructure.

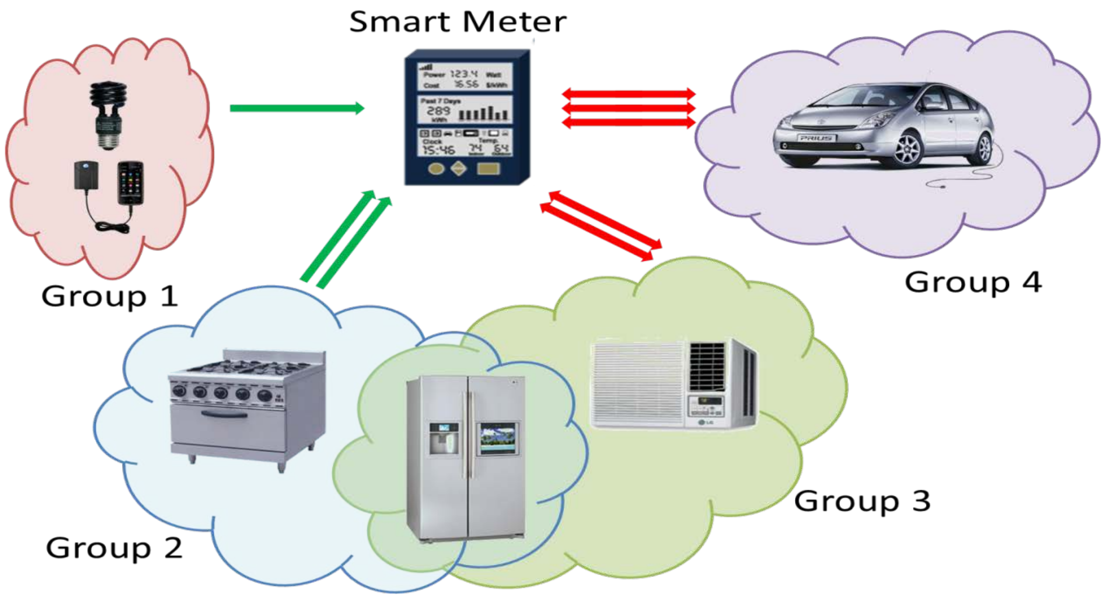

Figure 3.2: Communication and control model in HANs.

3.2 Home area network communications infrastructure

There are not too many HANs deployed today that connect appliances to a smart meter or energy management system that allows both communication and control capabilities. Thus, the rest of this section takes a more futuristic vision to HAN communication and control and discusses the primary challenge of security and privacy.

3.2.1 Communication and control model for HANs

At the consumer level—including residential, industrial, and commercial loads—loads could be connected to and controlled by a smart meter by being classified into different groups based on the nature of the load [21], as shown in Figure 3.2. Appliances/equipment in each group could be subjected to different restrictions on utilizing the grid. Communication between the smart meter and each load would be used to realize one-on-one control to regulate the operation of each device. For small loads (Group 1 in Figure 3.2), such as light bulbs, device chargers, etc., exerting control does not change the load profile significantly. Hence, they could be required to only send notifications of connection and disconnection. There could be larger loads such as stoves (Group 2 in Figure 3.2) which a consumer would want to use at any time and should not be controlled. For such "non-negotiable" loads, power usage and expected duration should be communicated to the smart meter. Large loads such as air conditioners and washers/dryers (Group 3 in Figure 3.2), for which usage could be controlled, should wait for acceptance from the smart meter to be switched on. These types of equipment/appliances will need to communicate extensive information such as expected load, expected duration of usage, and duration of availability. The decision to turn on a component will depend on the dynamic pricing and duration of availability. The last type of load is electric vehicles (EVs) which are new to the power grid. Since these are very large and stochastic in nature, it is vital for the smart meter to communicate with the EV in order to plan charging.

An issue to consider in deploying any communication technology is that most of the existing electrical devices to be controlled do not have any communication capabilities. With time, and further standardization activities, it is expected that such capabilities will become common. Thus, an intermediate step could be to enable power outlets with communication capabilities.

3.2.2 Requirements for security and privacy

Applications such as AMI which involve consumer participation would have to consider issues such as information security and privacy. The design of a secure communication and control model for home area networks that involves smart meters and end-user loads is an open research problem. For example, prior work [22] recommends ZigBee-based wireless communication as the best solution for HANs. Since wireless communication uses a shared medium, several threats in terms of information security and consumer privacy must be addressed in a common framework that can be agreed upon by grid operators and consumers. A key aspect that differentiates security in HANs from that of conventional local area networks is the presence of two different entities whose interests must be kept secure: (i) the grid operator, who must be sure that no one, including the consumer, can tamper with the measurement and control of appliances as agreed upon, and (ii) the consumer, whose privacy must be guarded at all times when the smart meter is collecting and relaying data, and whose personal appliance management preferences are honored at all times. Traditional local area network security protocols are based on a single-party application. No prior work seems to have been done for local area network security solutions under the presence of more than one stakeholder. There would have to be a re-definition of traditional security objectives such as confidentiality, integrity, availability, in terms of the HAN scenario, and mechanisms to provide secure authentication and time-sensitive communication services, along with an integrated framework addressing security and privacy vulnerabilities.

Two party dynamics

In traditional home area-based networks, the consumer is the only entity responsible for the operation of the network and acquiring benefits from the deployed applications. For example, consider the case of a home surveillance system. It is in the interest of the consumer that the network functions as intended. The consumer must correct any unintended behavior of the network. The HAN scenario has the additional dynamic of there being two parties with interests in the network. If the HAN does not function properly, it could prevent controlled appliances from operating at request. Similarly, a misbehaving network could take away the ability to manage load based on the utility requirements. Such network misbehavior could benefit one party at the expense of the other. Further distributed control that exists between two parties could allow a third party to threaten the security of the network by impersonating one or the other party, or both. It should be noted that capturing shared secrets among network entities is easier when more than one party is involved.

Security objectives

The following five main objectives can be identified to ensure a secure HAN.

• **Availability:** This objective is to ensure that network services are available and will survive possible attacks or failures that could occur. In the HAN scenario, resource depletion is typically not a concern when it comes to a resource such as energy, where both the smart meter and appliances are assumed to have access to grid power. But computation capabilities and memory constraints could be exploited by keeping these resources fully loaded, affecting the ability of the network to function as desired. Equipment failures may also be more common, especially with the low cost of HAN radios.

• **Confidentiality:** The goal of confidentiality is to ensure that any sensitive data is not disclosed to parties other than those involved in the communication process. In the HAN scenario, this could mean that apart from the customer and utility, no other party obtains access to the appliance usage behavior of the customer. Further the customer would prefer the utility to have only an aggregate view of power consumed.

• **Integrity:** This requirement is to ensure that a received message is not altered from the way it was transmitted by the sender. In the HAN scenario, this is important to allow timely and accurate control. If an attacker manages to change the source of the request, it could happen that the smart meter ends up communicating and controlling the wrong appliance.

• **Authentication:** Authentication is used by one node to identify another node or verify the source of origin of data in the network. Authentication is important for administrative tasks such as association, beaconing, and identifier collision. This is critical in the HAN scenario to ensure that a customer is sure of the authenticity of a smart meter with which its appliance is communicating, and for the smart meter to ensure that it is communicating only with the assigned customer's appliance.

• **Time sensitivity:** Any message delayed over a specific tolerable time frame may be of no use. A network must ensure relevance of communication by enforcing latency constraints. In the HAN scenario, a customer request for appliance operation must reach the smart meter in a timely manner; similarly, control commands from the smart meter to appliances must be timely to ensure scheduling practices of the smart meter.

Security objectives, such as fairness, which are common to more general wireless networks are not applicable in HAN because all appliances that compete for access to the medium belong to the same customer. Furthermore, the HAN network is expected to be used mainly as a control network and is not expected to be highly loaded in terms of bandwidth, thus providing no incentives for selfish behavior by nodes.

4. Future Needs

This section talks about the future research, policy, and standards needs in terms of communications for AMI. The time horizon for these needs can vary from a few years to a few decades.

4.1 Standards

Currently, the ANSI C12 standards target electric meters, but there is no way to verify compliance to the C12.22 standard or the C12.19 data tables it references. Currently, data collectors of major AMI suppliers do not support compliant meters from other meter suppliers. The C12.22 standard does not define any transport, network or lower-level layers and, at best, represents an application-level standard.

Standards bodies need to work on aspects such as communication and control in HANs, how and what appliances can be part of HANs, and how they are classified. Furthermore, standards such as DNP3 for smart meter communications need to be extended to allow options that can be used to increase or decrease the amount of data collected to deal with the varying scale of deployments. AMI smart meters offered by different vendors will be required to conform to standards established by American National Standards Institute (ANSI). Open standards may be the best way to drive down the cost of AMI deployments and provide utilities with the assurance that they can move forward with investments with one or a few vendors and not worry about a vendor's failure. The AMI-SEC task force is an effort in this direction that also includes creating guidelines for security in AMIs [23].

Network planning as it relates to the TCP/IP stack will be essential. Utilities should identify technologies and appropriate standards for both the HAN and backhaul. Interoperability testing will be essential, with the reliance on proprietary technologies minimized where possible. For each layer or combination of network layers, an effort should be made to identify open standards and use equipment that conforms to those standards. For example, the IEEE 802 standard specifies the physical and data link layers for technologies such as ZigBee and Wi-Fi, and is supported by many vendors. Usage of internet protocols at the network layer provides huge advantages in terms of field-proven protocols for network organization, management, and security.

4.2 Research needs

4.2.1 Infrastructure for scalable data collection and management

An important area of future research specific to the AMI application will involve looking at the problem of collection and management of data from millions of smart meters. By current standards, each smart meter sends a few kilobytes of data every 15 minutes to a smart meter [19], [20]. When this is scaled up to large numbers, many existing communication architectures will find it difficult to handle the data traffic due to limited bandwidth. Addressing this challenge requires contributions to the design of data aggregation/processing algorithms that preserve useful information from each consumer premise but at the same time allows significant compression of the overall aggregate when the data is transmitted through the communications infrastructure. The use of wireless communication technologies would also need contention resolution algorithms for utilizing shared spectrum. At the back end, cloud computing or other paradigms could be leveraged to store and share data across the various entities interested in the data.

- **Sharing and integration of infrastructure with other utilities**

Taking a step further, the electric grid AMI application can be extended for other billing needs involving water supply, heat, and gas. Such an integrated solution will require a more fundamental redesign of the way all of these consumer needs are supplied by utility companies. A common communication infrastructure can be used to read each meter and collect information that is then sent separately to each billing authority. A common data exchange standard such as the one developed by the DLMS user association could be used for this purpose [24]. Issues of how to share limited communication bandwidth across these diverse entities (an n-party scenario) would need additional research.

- **Integration with the Internet**

In the future, the communication infrastructure for AMI will probably need to be integrated with the internet such that AMI with smart meters and home appliances are just some of the nodes in the so-called "Internet of Things" (IOT). The IOT concept envisions everyday things such as clothes, grocery items, books, furniture, etc. to be connected to the internet along with electronic devices and appliances [25]. Technology will be pervasive, and decisions and management of energy will follow suit. Integration with the internet will require AMI nodes to be addressable in the IP format, assuming IP remains the protocol that is used in the future. The newer version of IP, IPV6, should have enough addresses available for integrating millions of such nodes, including those used as part of the AMI. Without AMI, the electric power grid had no capability to control the use of power by individual loads. With AMI, individual loads can be electronically controlled just such as an internet node can be addressed and data flow to it controlled. Thus, the power grid may need to evolve to information architectures similar to the internet.

- **Impact of emerging countries**

Whereas the U.S. has a pre-existing, reliable electrical grid infrastructure, there are some countries (e.g., India and China) where there exists some electrical grid infrastructure, although it is not as pervasive as in the U.S.. And of the infrastructure that exists, it may only offer unreliable (intermittent) or low-quality electricity. In many developing countries, the infrastructure that emerges may grow from the inside out; for example, through isolated microgrids. These alternate grid models may lead to alternate communications architectures than exist in the U.S. This is relevant to the U.S. communications architecture because a large number of people globally live in areas where alternate electric power infrastructures are emerging. Their Smart Grid solutions may predominate in the long run, or at very least may lead to "clean slate" opportunities that may not be available in the short term, but should be certainly considered for the longer term.

4.2.2 Impact of partial implementation

The benefits of AMI mentioned earlier in this white paper were mainly based on full AMI implementation in a region of interest. What is not clear is how much benefit can be realized with only partial implementation. This is an increasingly likely scenario with consumers having the right to opt out of smart meter deployments by utilities. PG & E in California is one example of a utility for which such an "opt-out" is possible. Modeling and analysis of such partial implementation scenarios needs to be added to the existing studies on AMI benefits. Such research should also consider different communication capabilities and constraints across geographic regions and operator domains. Even with 100% AMI penetration rates, acquired benefits could vary significantly based on degree of consumer participation and available communication technologies.

4.2.3 Information security and consumer privacy

With the greater integration of AMI devices to the internet, wide area network security threats to the application are expected to increase. This will require wide area networking security research to be done in conjunction with specific localized threats to the AMI. For example, smart meters would have to ensure not only consumer security and privacy within the HAN, but also protection from remote attacks from any part of the internet. Similarly, it should be possible to defend the power grid, as well as the internet as a whole, from compromised AMI nodes.

Figure 4.1 shows a list of possible remote and local attacks possible in the AMI scenario (additional details can be found in [21]). The degree of feasibility of each, and

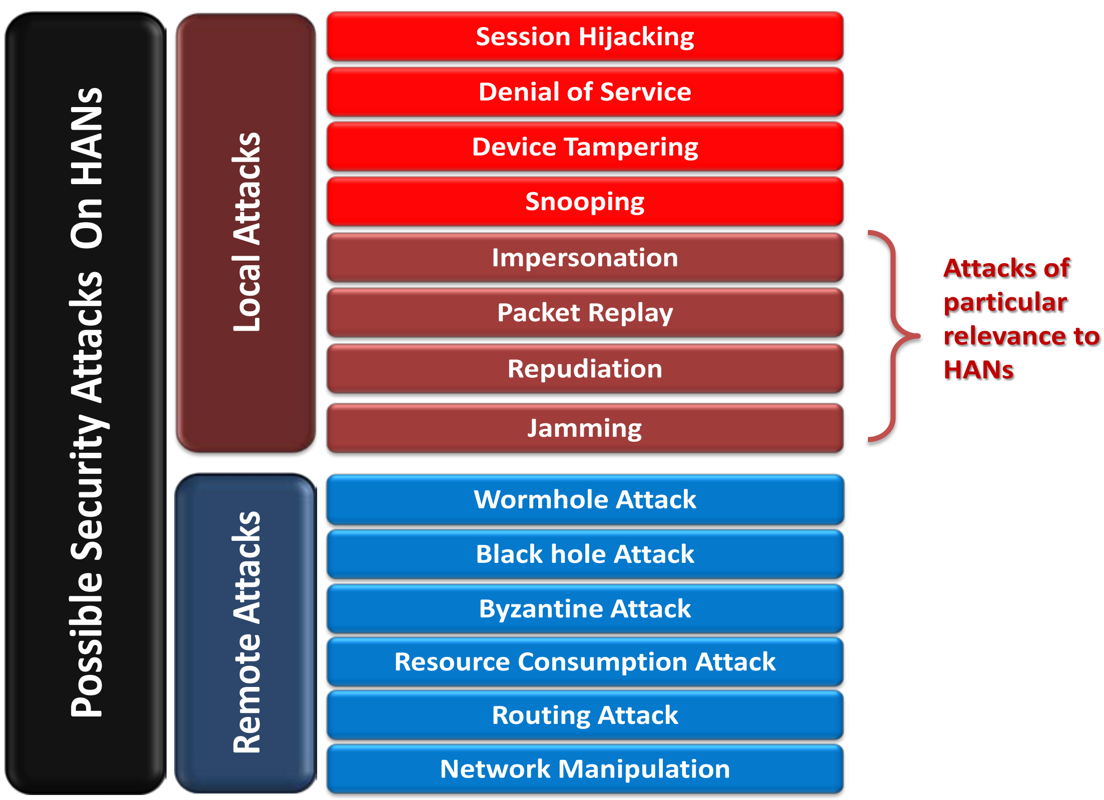

Figure 4.1: List of possible security attacks in AMI scenario.

possible solutions should be identified and then integrated into a common framework that can be agreed upon by both the utility and the customer. Some attacks, such as jamming, load impersonation, and replay attacks, are directly relevant to the HAN scenario, and solutions may need customer cooperation to be implemented.

4.2.4 Integration of communication technologies and their evaluation for emerging application requirements

Current approaches to satisfying communication needs take a "piecemeal" approach to meeting the needs of applications, where one type of communication solution is proposed for each application. A highly integrated communications infrastructure is required that is scalable, provides interoperability, improves consumer participation, and considers the issues of cyber-security and reliability beginning with the design phase. In general, the effectiveness of applications has not been studied under communication capacity and reliability constraints. The performance, and eventually success, of these applications would depend on the nature and level of these constraints. For example, the degree of consumer participation in energy delivery would depend on the type and quality of communication infrastructure available (including end-user devices) based on economic and geographical considerations. It becomes important to study the effects on smart grid applications at various levels of consumer participation. Emerging applications would need multiple communication technologies integrated to work together end-to-end from grid control centers to end-user loads. An evaluation of the need for overlap in communications among the various applications will enable better data aggregation across applications, and effective creation and utilization of common communication paths. With AMI deployments driven by regulations in many countries, it would make sense to design the AMI communication infrastructure in a way that supports other emerging applications as well.

For example, to reduce infrastructure costs, it may be worthwhile to design a single communications infrastructure that can be used for both the AMI application and general distribution system automation. Legacy distribution system automation has been confined to supervisory control and data acquisition (SCADA) systems at the primary distribution substations [26]. Integrating the communications infrastructure for AMI to include the feeder level of the distribution system beyond the substation would benefit applications such as self-healing feeders, feeder asset reliability, and integration of distributed sources.

4.3 Policy needs

4.3.1 Infrastructure investments

Due to the benefits of AMI, not only for utilities but also consumers and society in general, policies need to be put in place to encourage investments in infrastructure. Although utilities are expected to eventually have financial gains from the AMI application, they will need to be supported at the local, state, and federal levels for them to advance from "half-hearted" measures of AMI with limited capabilities to a "full-blown" investment in the AMI with full real-time bi-directional communication capabilities. This will prevent issues such as backwards compatibility and hasten the realization of benefits. Examples of such support could be tax incentives, subsidies for smart meters deployed, and usage of community communication networks (e.g., citywide Wi-Fi networks), where applicable. There is also a discussion about the FCC allocating spectrum for wireless communication needs for the smart grid. This will drive down infrastructure costs and hasten deployments. There is some discussion on whether this spectrum should be dedicated for utilities only, or shared with other entities [27]. At the consumer level, incentives must be provided for consumers to participate in the AMI, similar to that in other federal energy efficiency programs. For example, consumers should be encouraged to buy appliances with communication and control capabilities within their HANs. Furthermore, authorities, in conjunction with educational institutions, could step up educational efforts for consumers to help fully realize the benefits of AMI for everyone.

4.3.2 Information security and consumer privacy

It might have become apparent from this white paper that information security and privacy is one of the threats to the otherwise overwhelmingly beneficial AMI application scenario. The MIT report on the future of the electric grid [28] also considered HAN security and privacy as a critical challenge in achieving overall cyber security goals. Although much of the information sent through the AMI is not sensitive, data involving consumers must be safeguarded. Generally, customers own their data and there are clear privacy and security policies, and requirements for utilities to protect the data from any unauthorized access. Any access to the customer specific data must be authorized and approved by the specific customer. As such, utilities generally are considered "custodians of the customer's data". However, any customer-specific data can often be stripped away from the energy use data for general analysis.

Policies need to be in place on how utilities must handle, process, and store consumer data, and with whom they can share the information. Disputes arising among utilities and consumers would need third-party intervention that should be able to consult records of all control information exchanged between AMI nodes and the utility. These records, as well as some of the AMI devices, should be tamper-proof. For the benefit of utilities, regulations should be in place on how utilities can classify nodes as malicious and react by disconnecting power and/or communications. The utility should have the means (possibly through software at the smart meter) to ensure that all customer nodes participating in the HAN are following the rules of communication and control.

5. Conclusions

This white paper analyzed the current state of communication infrastructure for AMI and recommended future actions needed to enable and fully realize the benefits of consumer participation in smart grids. On a global scale, the U.S. has made good progress in deploying AMI, lagging behind only some European countries. There also seems to be better consensus on moving beyond AMR alone to realizing the benefits of AMI, which is not necessarily the case in many countries.

In terms of actual communications technologies being relied upon, there seems to be more consensus on how to build HANs rather than backhaul links. This is probably due to the fact that HANs are more or less an extension of consumer communication networks that exist today. Proven technologies in that space, such as ZigBee and Wi-Fi, seem to satisfy all communication requirements and do not need large infrastructure investments.[4] There is a fair agreement on the use of a gateway or hub architecture for HAN technologies. On the other hand, many more players, technology options, and architectures are available for backhaul links. Options that are more far reaching with greater capabilities require big infrastructure investments; options are available that seem to satisfy most current needs without big investment. Due to such diverging options for backhaul communications, there is greater flux in decision-making in this area. This is one area where policy could guide decisions one way or the other, and encourage investments that could serve the nation for many decades. Further research is required to evaluate such options and possible communication architectures. Replicating the success of the internet for AMI would require greater cross-disciplinary research work between the fields of communications/networking and power systems.

In contrast, information security and privacy needs to be addressed more from a HAN perspective due to involvement of consumers and their data. Both parties, the utility and the consumer, have different stakes in securing their HANs, and solutions must address the concerns of both parties without leaving any vulnerability for a third party to exploit. Future research in this area, along with policies on how to handle misbehavior and breach of consumer privacy, is needed. Wide-area network attacks could be addressed similarly to the approaches used for the internet, but they would still need research expertise in the power systems area to identify vulnerabilities and application requirements and define service-quality levels.

In summary, the future actions needed nationally in terms of communication needs and integration options for meeting AMI goals are as follows: (i) encouraging more far-reaching investments in backhaul infrastructure and providing spectrum access for wireless communication, (ii) incentivizing consumers to embrace AMI initiatives and adopt AMI-capable loads, and (iii) information security and privacy regulations to protect consumers and guide utility reactions to threats and malicious behavior.

---

[4] The author received feedback from multiple industry reviewers that appliance manufacturers are not clear on a technology of choice and may implement more than in one, or rely on technology “bridges” to meet future adoption trends that may emerge. For example, HAN technology uncertainty has led to some appliance manufacturers such as LG including both Wi-Fi and ZigBee in their products. The report by the Association of Home Appliance Manufacturers (AHAM) found at www.**aham**.org/ht/a/GetDocumentAction/i/5069 talks about the possible choices moving forward.

6. References

[1] U.S. Department of Energy. (2008) What the Smart Grid Means to Americans. by Consumer Advocates group in a series of books of Smart Grid stakeholder groups. [Online]. Available: http://www.doe.gov/sites/prod/files/oeprod/DocumentsandMedia/ConsumerAdvocates.pdf, last retrieved October 27, 2011.

[2] Demand Response and Advanced Metering Coalition (DRAM), "Overview of advanced metering technologies and costs," April 2004. [Online]. Available: http://www.drsgcoalition.org/resources/whitepapers/DRAM White Paper 2004-04.pdf, last accessed on October 27, 2011.

[3] G. Heydt, "Electric power quality: a tutorial introduction," Computer Applications in Power, IEEE, vol. 11, no. 1, pp. 15 –19, January 1998.

[4] S. Darby, "The effectiveness of feedback on energy consumption: A review for DEFRA of the literature on metering, billing and direct displays," vol. 22nd, April 2006. [Online]. Available: http://www.powerwatch.com/doc/smart-metering-report.pdf, last accessed October 27, 2011.

[5] Amy Schatz, "Cellphone users to get billing alerts under new voluntary standards," The Wall Street Journal. [Online]. Available: http://online.wsj.com/article/SB10001424052970203658804576635053172551850.html, last accessed on October 27, 2011.

[6] National Energy Technology Laboratory, "Advanced Metering Infrastructure," February 2008. [Online]. Available: http://www.netl.doe.gov/smartgrid/refshelf.html, last accessed October 27, 2011.

[7] Federal Energy Regulatory Commission (FERC), "Assessment of demand response and advanced metering," Staff Report, February 2011. [Online]. Available: http://www.ferc.gov/legal/staffreports/2010-dr-report.pdf, last accessed on October 27, 2011.

[8] B. Heile, "Surveying the international AMI landscape." [Online]. Available: http://www.elp.com/index/display/articledisplay/3987256252/articles/utility-automation-engineering-td/volume-15/Issue 7/Features/Surveying the International AMI Landscape.html, last accessed on October 27, 2011.

[9] Smart Regions, "European smart metering landscape report," 2011. [Online]. Available: http://www.smartregions.net/default.asp?SivuID=26927, last accessed on October 27, 2011.

[10] M. Bauer, W. Plappert, C. Wang, and K. Dostert, "Packet-oriented communication protocols for smart grid services over low-speed PLC," in IEEE International Symposium on Power Line Communications and Its Applications, March 2009, pp. 89–94.

[11] T. Tran-Anh, P. Auriol, and T. Tran-Qouc, "Distribution network modeling for power line communication applications," in International Symposium on Power Line Communications and Its Applications, April 2005, pp. 361–365.

[12] S. E. Collier, "Delivering broadband internet over power lines: what you should know," in Rural Electric Power Conference, May 2004, pp. 1–11.

[13] T. Khalifa, K. Naik, and A. Nayak, “A survey of communication protocols for automatic meter reading applications,” Communications Surveys Tutorials, IEEE, vol. 13, no. 2, pp. 168 –182, quarter 2011.
[14] G. N. Ericsson, “Communication requirements-basis for investment in a utility wide-area network,” IEEE Trans. on Power Delivery, vol. 19, no. 1, pp. 92–95, January 2002.
[15] H. Tan, C. Lee, and V. Mok, “Automatic power meter reading system using GSM network,” in Power Engineering Conference, 2007. IPEC 2007. International, December 2007, pp. 465–469.
[16] A. Abdollahi, M. Dehghani, and N. Zamanzadeh, “SMS-based reconfigurable automatic meter reading system,” in Control Applications, 2007. CCA 2007. IEEE International Conference on, October 2007, pp. 1103 –1107.
[17] B. Brown, “802.11: the security differences between b and i,” Potentials, IEEE, vol. 22, no. 4, pp. 23–27, Oct.-Nov. 2003.
[18] P. Kulkarni, and S. Gormus, and Fan Zhong and B. Motz, “A self-organising mesh networking solution based on enhanced RPL for smart metering communications”, in World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on, pp. 1–6, June 2011.
[19] D. Bernaudo et al., “SmartGrid/AEIC AMI interoperability standard guidelines for ANSI C12.19 / IEEE 1377 / MC12.19 end device communications and supporting enterprise devices, networks and related accessories,” The Association of Edison Illuminating Companies, Meter and Service Technical Committee report version 2, November 2010. [Online]. Available: http://www.aeic.org/meter service/AEICSmartGridStandardv2-11-19-10.pdf
[20] E. E. Queen, “A discussion of smart meters and RF Exposure Issues, Edison Electric Institute (EEI), 2011, A Joint Project of the EEI and AEIC Meter CommitteesWashington, D.C, March, http://www.aeic.org/meterservice/smartmetersandrf031511.pdf,” Tech. Rep.
[21] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, “Wireless AMI application and security for controlled home area networks,” in Proceedings of the Power and Energy Society (PES) General Meeting, ser. IEEE PES GM, 2011.
[22] C. Bennett and D. Highfill, “Networking AMI Smart Meters,” November 2008, pp. 1–8.
[23] “AMI-SEC task force overview,” OpenSG users group. [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec/default.aspx, last accessed on November 1, 2011.
[24] “DLMS user association.” [Online]. Available: http://www.dlms.com, last retrieved October 27, 2011.
[25] L. Atzori, A. Iera, and G. Morabito, “The internet of things: a survey,” Computer Networks, vol. 54, pp. 2787–2805, October 2010.
[26] J. Northcote-Green and R. Wilson, Control and automation of electric power distribution systems. CRC Press, September 2006.
[27] K. Fehrenbacher, “AEP Calls for Dedicated Wireless Spectrum for Smart Grid,” GigaOM, August 25, 2009; and Utilities Telecom Council, “Dedicated Spectrum for Utilities—Frequently Asked Questions,” http://www.utc.org/utc/dedicatedspectrum-utilities-frequently-asked-questions

[28] "The Future of the Electric Grid: An interdisciplinary MIT study", 2011. [Online] Available: http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf