The New Frontier of Communications Research: Smart Grid and Smart Metering

Zhong Fan, Georgios Kalogridis, Costas Efthymiou, Mahesh Sooriyabandara, Mutsumu Serizawa, and Joe McGeehan
Toshiba Research Europe Limited, Telecommunications Research Laboratory
32 Queen Square, Bristol, BS1 4ND, UK
{zhong.fan, george, costas, mahesh, mutsumu.serizawa, joe}@toshiba-trel.com

ABSTRACT

This paper discusses some of the challenges and opportunities of communications research in the area of smart grids and smart metering. It is clear that the communications research community has been actively seeking the 'next big thing' after interests in recent hot topics such as cognitive radio, cooperative communications, and MIMO have more or less peaked. We argue that the new initiative on smart grid worldwide provides an ideal opportunity for communication and networking researchers to apply various existing technologies as well as inventing new ones in this exciting area.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design - Wireless communication

General Terms

Management, Security, Standardization.

Keywords

Wireless communications, smart grid, security.

1. INTRODUCTION

Communications research, especially wireless communications research, is at a cross road. Although the whole industry is comparatively healthy and moving forward at full-speed towards 4G (IEEE 802.16m, 3GPP LTE-A, etc.) in spite of the recession, research seems to be stagnating. For example, at a recent VTC conference, a panel on "the PHY layer is dead" attracted a lot of attention from both academia and industry [1]. For the past few years, the wireless research community has embraced a number of hot topics in different layers of the communications stack, such as MIMO, cooperative relaying, ad hoc networks, and cognitive radio, just to name a few. Research on these topics has produced some successful outputs, e.g. new standards like IEEE 802.11n and 802.16m, new products and applications like mesh networking (FON-type services), etc. However, it is clear that the majority of this research has peaked and the community is desperately searching for new growth points and the 'next big thing'. Fortunately, the recent worldwide initiative on smart grids can provide an ideal opportunity for communication engineers to apply solutions to new problems and invent new technologies.

A smart grid is an *intelligent* electricity network that integrates the actions of all users connected to it and makes use of advanced information, control, and communication technologies to save energy, reduce cost and increase reliability and transparency. Recently, many countries have started massive efforts on research and developing smart grids. For example, the smart grid is a vital component of President Obama's comprehensive energy plan: the American Recovery and Investment Act includes $11 billion in investments to "jump start the transformation to a bigger, better, smarter grid".

In this paper, we discuss various challenges of communication systems in smart grid, as well as candidate solutions. The aim is to outline a big picture of possible research directions and stimulate interests in this area in the wider community.

The remainder of the paper is organized as follows. Section 2 discusses various technical challenges and issues in the communication network aspects of smart grid. Section 3 describes the security challenges of smart grid and Section 4 concludes the paper.

2. COMMUNICATION CHALLENGES AND ISSUES

While communications technology is seen as a great enabler for future smart grids, and indeed an essential component, there are a number of challenges that must first be overcome for fully robust, secure and functional smart grids and networks. Some of these challenges are discussed below. It is important to note that these challenges are very much intertwined, i.e. they affect each other and must be considered as parts of a bigger problem/challenge.

2.1 Interoperability

A key feature of smart grids is the interconnection of a potentially large number of disparate energy distribution networks, power generating sources and energy consumers. The components of each of these entities will need a way of communicating that will be independent of the physical medium used and also independent of manufacturers and type of devices. The communication architecture of the future smart grid is yet to be defined. As a result, multiple communication technologies and standards could

e-Energy '10, Apr 13-15, 2010, Passau, Germany

coexist in different parts of the system. For example, short-range wireless such as Bluetooth or UWB could be used for the interface between meter and end customer devices, IEEE 802.15.4 (ZigBee) and IEEE 802.11 (WiFi) could be used for smart meter interfaces in the home and local area network, and cellular wireless (e.g. GPRS, UMTS, or 4G technologies like 802.16m and LTE) could be used for the interface between meters and the central system. To this end, interoperability is essential for smart metering devices, systems, and communications architectures supporting smart grids. This has also been emphasized by the recent EU M/441 Mandate on smart grid [2].

It can be envisaged that in a complex system such as smart grid, heterogeneous communication technologies are required to meet the diverse needs of the system. Therefore, in contrast to conventional telecommunication standardization such as IEEE 802.11n or LTE, the standardization of communications for smart grid means making interfaces, messages and workflows interoperable. Instead of focusing on or defining one particular technology, it is more important to achieve agreement on usage and interpretation of interfaces and messages that can seamlessly bridge different standards or technologies. In other words, one of the main aims of communication standardization for smart grids is ensuring interoperability between different system components rather than defining these components (meters, devices or protocols) [3].

Based on the above reasoning, the smart grid poses new challenges and opportunities for communication researchers. An analogy would be the recent trend of wireless PHY researchers moving from the point-to-point research to the link level and network level (e.g. MIMO to network MIMO, cooperative diversity to network coding). In the case of smart grid, we may need to expand our networking research to the 'network of networks', taking into account real world constraints.

In this context, generic APIs (application programming interfaces) and middleware is a very useful enabling technology. The success of commercial deployment of smart metering and smart grid solutions will significantly depend on the availability of *open* and standard mechanisms that enable different stakeholders and vendors to interoperate and interface in a standard manner. Open interfaces serve many purposes and provide additional benefits in multi-stakeholder scenarios such as smart energy management in home and industrial environments. Further, open APIs provide the means for third parties not directly associated with the original equipment manufacturers to develop a software component which could add functionality or enhancements to the system. On the other hand, smart energy management solutions require access to more information ideally from different service providers and devices implemented by different vendors. Such information should be available and presented in a usable format to interested parties. Further, timing and specific configuration of measurements and controls are also critical for dynamic scenarios. Since support for different technologies and some level of cooperation over administrative boundaries are required, proprietary or widely simplified interfaces will not be sufficient in these scenarios. This situation can be improved by standard generic API definitions covering methods and attributes related to capability, measurement and configurations. The design of such APIs should be technology agnostic, light-weight and 'future-proof'.

2.2 Scalable internetworking solutions

Wireless sensor networks (WSN) research should be extended to smart grid and metering. WSN has been an active research topic for nearly ten years and has found many applications. Smart grid/metering appears to be a major application for WSN, especially along the line of Internet of things and machine-to-machine (M2M) communications. Existing industry efforts include IETF 6LoWPAN [10] and ROLL [11]. Based on smart metering user scenarios, the overall M2M network architecture, service requirements, and device capabilities are yet to be defined. Recently ETSI has established a new M2M technical committee to address these issues [4].

Internetworking between cellular networks and local area networks (e.g. WLAN) has received a lot of attention because of the need for seamless mobility and quality of service (QoS) requirements. Topics such as intelligent handover and connection management have been extensively investigated. In the context of smart grid, due to the extremely large scale nature of the network, the characteristics of the metering and control traffic carried in the network are not clearly known. For instance, it could be the case where 100,000 nodes (meters) generate meter traffic data every 10 minutes. As a result, how to design and provision a scalable and reliable network so that this data can be delivered to the central utility control in a timely manner is a challenging task. As traffic will be traversing different types of networks, interoperability is the key. Further, some of the traditional research topics may need to be revisited to cater for smart grid traffic, e.g. resource allocation, routing, and QoS. This is because the traffic that will be generated by e-energy type applications will likely be quite different to the traditional browsing/downloading/streaming applications that are in use today, with a mix of both real-time and non-real-time traffic being generated and distributed across different parts of a smart grid.

Interworking of communication protocols and dedicated smart metering message exchange protocols such as DLMS/COSEM [5] is an open research issue. The DLMS/COSEM standard suite has been developed based on two concepts: object modeling of application data and the Open Systems Interconnection (OSI) model. This allows covering the widest possible range of applications and communication media. Work has already started in the industry trying to address the issue of carrying DLMS data over various networks such as GPRS and power line communications (PLC) networks. Recently, the DLMS User Association also established a partnership with the Zigbee Alliance and the two organizations are working on tunneling DLMS/COSEM over Zigbee networks to support complex metering applications.

2.3 Self-organizing overlay networks

Because of the scale and deployment complexity of smart grids, telecommunication network systems supporting smart grids are likely to rely on the existing public networks such as cellular and fixed wired access technologies, as well as private and dedicated networks belonging to different administrative domains. The purpose of such networks can be seen not only as a communications medium to exchange monitoring and control information, but also as an enabler of new services and applications. In many ways, the complexity and heterogeneity

characteristics of smart grid communications networks will be similar to that of a wireless radio access network supporting voice and data services. However, stakeholder expectations, QoS requirements and load patterns will be significantly different from those of a typical mobile voice/data network because of the nature of the applications and services supported. Both will share, at least partially, problems related to managing and operating a complex and heterogeneous network where tasks such as network planning, operation and management functions, and network optimization are important. We believe that a 'self-organizing network' overlaid over existing infrastructure is the way forward to support wider deployment of smart grid systems. Such a self-organizing network should support functions such as communications resource discovery, negotiation and collaboration between network nodes, connection establishment and maintenance to provide the performance guarantees required by smart grid/metering applications.

2.4 Home networking challenges

Research on home networking has so far focused on providing multimedia applications with high QoS, zero-configuration, and seamless connectivity to home users. With the advent of smart grids, new features and system design principles have to be considered. For example, consider how to integrate smart meter or M2M gateway functions into the home gateway (e.g. WLAN AP or femtocell BS) in a cost-effective manner. Clearly, smart metering adds a new dimension to home networks, complicating the issue of interference management and resource provisioning.

With potentially every device and appliance in the home supplying energy related information to the smart meter/home gateway (and by extension, possibly to the energy supplier as well), it is easy to envisage an order of magnitude increase in the number of devices in each home that are able to communicate with each other and with the outside world. Today's homes may have 2-3 computers (desktop, laptop, smart phone) that are connected to the home network and to the Internet – tomorrow's smart grid/smart meter homes could have 20-30 or more appliances and devices connected to the same network. Although the preferred (wireless) networking standards for these devices have not yet been established, it is clear that there will be many more devices connected to whichever network is used. Although there has been much discussion in the networking community over the years of having "an IP address for every possible device" in the home and so on, the convergence of energy provision and communications may be the catalyst for this to actually become a reality.

Along with the many new devices that will be connected to home networks, new kinds of applications will undoubtedly emerge. The prime (and easy to envisage) application is the one of energy consumption monitoring within the home and other areas (offices, etc.). In this direction, there are proposals for load monitoring and real-time control from the utility companies' perspective. However, energy monitoring has the potential to grow into something far more significant than just measuring the energy consumed. With the current concerns over climate change and the very important need for energy efficiency in all areas, it follows that fine-granularity monitoring of energy usage in the home and other areas will become a necessity and much research will be required in automating methods for energy usage reduction in the home. Given that there is much perceived wastage in the way that we use appliances and devices today (e.g. leaving devices on standby, inefficient usage of washing machines and refrigerators, inefficient use of heating and cooling), there is plenty of scope for automated energy consumption methods.

3. SMART GRID SECURITY

Analyzing and implementing smart grid security is a challenging task, especially when considering the scale of the potential damages caused by attacks.

As compared to current grids, smart grids differ in that they interconnect smart grid components with a two-way communication network. For example, energy suppliers and customers exchange information in an interactive, real-time manner. This capability supports features such as load shedding, consumption management, distributed energy storage (e.g. in electric cars), and distributed energy generation (e.g. from renewable resources). Also, as previously discussed, the network could be implemented using a variety of media ranging from fiber optics/broadband (e.g. for meters to base control center networking), to Zigbee/WLAN (e.g. for home networking). Considering the need to fine-granularity smart metering monitoring (described in the previous section), the security of an advanced metering infrastructure (AMI) is of paramount importance.

Smart grid security risks and vulnerabilities can be identified by using a top-down or a bottom-up approach. The top-down approach analyzes well-defined user scenarios such as automated meter reading (AMR) billing, while the bottom-up approach focuses on well-understood security attributes and features such as integrity, authentication, authorization, key management, and intrusion detection. A classification of smart grid risks and vulnerabilities has recently been published by NIST [6].

The second step of a smart grid security assessment is the specification of security requirements ─ a comprehensive specification of AMI security requirements has been documented by OpenSG [7].

3.1 Privacy

The smart grid invasion of privacy is threatening as smart grid data infer directly where and when people were, and what they were doing. For example, smart meters can already collect a unique meter identifier, timestamp, usage data, and time synchronization every 15 to 60 minutes. Soon, smart meters will be able to collect outage, voltage, phase, frequency data, and detailed status and diagnostic information from networked sensors and smart appliances. Also, smart grid devices roaming in different utility systems – for example, driving an electric vehicle to visit family and recharging it while there – will require such information to be shared between more than one host utility.

The major benefit provided by the smart grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its Achilles' heel from a privacy viewpoint. As stated in a resolution drafted by the American National Association of Regulatory Utility Commissioners (NARUC) [8], it is clear that: "utility customer information can be used to differentiate utility services in a manner that creates added value to the customer". On

the other hand, "a balance has to be carefully considered between the appropriate pro-competitive role that utility customer information can play in new and developing markets and the privacy implications of using that information". To this end, customers should be permitted to choose the degree of privacy protection, with respect to both information outflows and inflows.

3.2 Security challenges

The most widely discussed smart grid security challenges concern the protection of smart metering data against unauthorized access and repudiation. This is an important requirement without which AMR data will not be trusted by either the utility providers or the customers. Solutions are required on different levels: end to end secure communication protocols need to be used, hardware components (e.g. smart meters) need to withstand physical attacks, the grid needs to detect forged/hacked components, smart meter software should be bug-free, etc [9].

We believe that AMI communication security requirements can be addressed by combining existing cryptographic protocols and tamper-proof hardware solutions, by exhaustively testing equipment and software against all sorts of attacks, and by adopting an open architecture for further testing and secure updating.

Also, it is equally important to develop mechanisms for protecting smart metering data against insider attacks. The use of open smart grid interfaces, as previously described, will create a gateway for multiple third parties (stakeholders) to access and process AMR data. We need to make sure that such insiders will access smart metering data in an authorized manner and will only use this data in an 'acceptable' manner.

Our vision is that security policies and legislation are not a panacea for privacy as they do not thwart attacks such as data privacy concessions: history teaches that 'legitimate' techniques for mining and exploiting data evolve quickly when there is a clear financial incentive. Hence, the problem of smart meter data access and usage needs to be further reviewed within different security domains:

Enforcement: Smart metering data should belong, in principle, to the users. For example, a digital rights management system could be used to allow utility providers to use the data in an 'acceptable' manner. Any use of personal data (acceptable or unacceptable) should not be repudiated.

Reaction: There should be mechanisms that will detect (in retrospect) misuse of smart metering data. These mechanisms should have regulatory support for counter-measures (e.g. penalties) against malicious parties.

The common challenge in all the above cases remains to design a system that will balance the trade-off between security and performance, i.e. use 'adequate' security strength while minimizing its power usage and cost overheads.

3.3 Secure integration

Smart grid security should not be seen as a standalone system. As heterogeneous communication systems converge, smart grid communications will start to integrate with ad hoc opportunistic networks, the Internet, etc. For example, a roaming smart grid customer may wish to initiate an authenticated flow of information between his smart meter at home and the smart meter in facilities he is temporarily using while being abroad. The same customer may wish to allow usage of such data by other parties in exchange for free entrance to the facilities, or he may wish to remain anonymous. In this scenario it is clear that integration of services and interfaces requires transparent and secure protocols.

One can envisage further challenges arising as smart grid communication systems integrate with other communication systems: home entertainment systems, medical communication systems, and traffic monitoring communication systems (e.g. via GPS), just to name a few.

4. CONCLUSION

In this paper we have presented the case that smart grid is a new frontier for communications and networking research. It poses many unique challenges and opportunities, e.g. interoperability, scalability, and security. The success of future smart grid depends heavily on the communication infrastructure, devices, and enabling services and software. Results from much existing communications research can be applied to the extremely large-scale and complex smart grid, which will become a killer application. We therefore envisage that smart grid will be an exciting research area for communication researchers for many years to come.

Due to space limitations, there are a number of important issues we have not discussed here in detail, e.g. power saving technologies, distributed/centralized data processing, and infrastructure management. In particular, an exciting research challenge is how the smart grid fits into the overall picture of the future Internet [12] currently under development.

5. REFERENCES

[1] M. Dohler et al., IEEE VTC-Spring'09 Panel, http://www.ieeevtc.org/vtc2009spring/panels.php#Panel02.

[2] EU M/441 Mandate, http://www.cen.eu/CENORM/Sectors/Sectors/Measurement/Smart+meters/index.asp.

[3] SMCG report: Response to M/441, Sept. 2009.

[4] ETSI TC M2M, http://portal.etsi.org/portal_common/home.asp?tbkey1=m2m.

[5] DLMS/COSEM, http: //www.dlms.com.

[6] A. Lee and T. Brewer, Smart grid cyber security strategy and requirements. NISTIR 7628, NIST, September 2009.

[7] AMI System Security Requirements. Technical Report, AMI-SEC TF, OpenSG, December 2008.

[8] Resolution Urging the Adoption of General Privacy Principles for State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information. NARUC, October 2009.

[9] P. McDaniel and S. McLaughlin, Security and Privacy Challenges in the Smart Grid. IEEE Security & Privacy, pages 72-74, May/June 2009.

[10] N. Kushalnagar et al., IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), RFC 4919, 2007.

[11] M. Dohler et al., Routing Requirements for Urban Low-Power and Lossy Networks, RFC 5548, 2009.

[12] D. Clark, Toward the design of a Future Internet, MIT technical report, 2009.