Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

> *"As we modernize the nation's electric infrastructure to make it smarter, more efficient, and more capable, we need to make it more secure from end to end."*
>
> Gary Locke
> U.S. Ambassador to China
> and Former Secretary of Commerce

The smart grid is a next-generation power system that is increasingly attracting the attention of government, industry, and academia. It is an upgraded electricity network that depends on two-way digital communications between supplier and consumer that in turn give support to intelligent metering and monitoring systems. Considering that energy utilities play an increasingly important role in our daily life, smart-grid technology introduces new security challenges that must be addressed. Deploying a smart grid without adequate security might result in serious consequences such as grid instability, utility fraud, and loss of user information and energy-consumption data. Due to the heterogeneous communication architecture of smart grids, it is quite a challenge to design sophisticated and robust security mechanisms that can be easily deployed to protect communications among different layers of the smart grid-infrastructure. In this article, we focus on the communication-security aspect of a smart-grid metering and control system from the perspective of cryptographic techniques, and we discuss different mechanisms to enhance cybersecurity of the emerging smart grid. We aim to provide a comprehensive vulnerability analysis as well as novel insights on the cybersecurity of a smart grid.

Introduction

The term "smart grid" generally refers to a next-generation power grid in which the generation, transmission, distribution, and management of electricity are upgraded and automated by incorporating advanced computing and communication technologies for improving the efficiency, reliability, economics, and safety of the grid. Loosely speaking, a smart grid is composed of a power grid and a two-way communication network for information retrieval and management. When compared to legacy and closed power-control systems, the smart grid is envisioned to establish a scalable, pervasive, and interactive communication infrastructure with new energy-management and demand-response capabilities. During the past few years, smart-grid metering and control systems have been widely deployed throughout the world. According to a new Navigant Research report (2013; tinyurl.com/m3qm7xx), the global market potential for smart-grid equipment manufacturers and solution providers will nearly double by 2020, reaching $73 billion in annual revenue and $461 billion in cumulative profit.

A smart grid brings great performance benefit to the power industry and enables end users to optimize their power consumption; however, the heavy dependence on communication networks has made smart grids vulnerable to a wide range of cyberspace threats. For example, it has been shown that security breaches in smart grids can result in a variety of serious consequences, from blackouts and physical damage of infrastructure to the leakage of customer information. Considering the vast scale and complex architecture of

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

a smart grid, it is not difficult to understand that the vulnerabilities associated with the smart-grid communication system may also be enormous. Those security vulnerabilities need to be properly addressed to ensure that smart grids are not only secure and function correctly, but that they also maximize their adoption and successfully fulfill the promise of smart-grid investment.

Although most of the architectures, frameworks, and roadmaps for smart grids have already been defined by the governments, industry, and academia, there are still many important security and privacy issues in smart-grid communications. These issues are now considered by governments and industry to be one of the highest priorities for smart-grid design, and they must be resolved before smart grids can be operationally ready for the market. In this article, we will present the high-level architecture of a smart-grid metering and control system, and we will describe typical cyberspace attacks on smart-grid communications. We also will summarize the security requirements, review some existing solutions, and highlight several important directions along this emerging research line.

The remainder of this article is organized as follows. First, we present the fundamental architecture and functionalities of a smart-grid metering and control system. Next, we focus on the security requirements for smart-grid communications, followed by a survey of current efforts made by the industry and academia to secure the smart-grid networks and devices. Finally, we propose several research areas and directions in smart-grid security and draw some conclusions.

Architecture

A typical smart-grid metering and control system, as illustrated in Figure 1, consists of a collection of meters/sensors and controllers/actuators that communicate with a substation/data-concentrator, a consumer or technician, and various third-party entities. The communication among different network entities is realized by high-speed wired or wireless links or a combination thereof. A smart-grid metering and control system has a layered network structure through which it collects data and controls the delivery of electricity.

The main functionalities of each component in a smart-grid metering and control system are as follows:

1. **Utility company:** connects to the substation network through the wide area network (WAN) interface and the communication channel might be Wi-Fi, satellite, 4G-LTE, Wi-Max, etc. The utility company is responsible for processing alarms and alerts, managing the meter data, and generating bills. Moreover, it may also provide a web portal that allows customers to view their monthly energy consumption and bills.

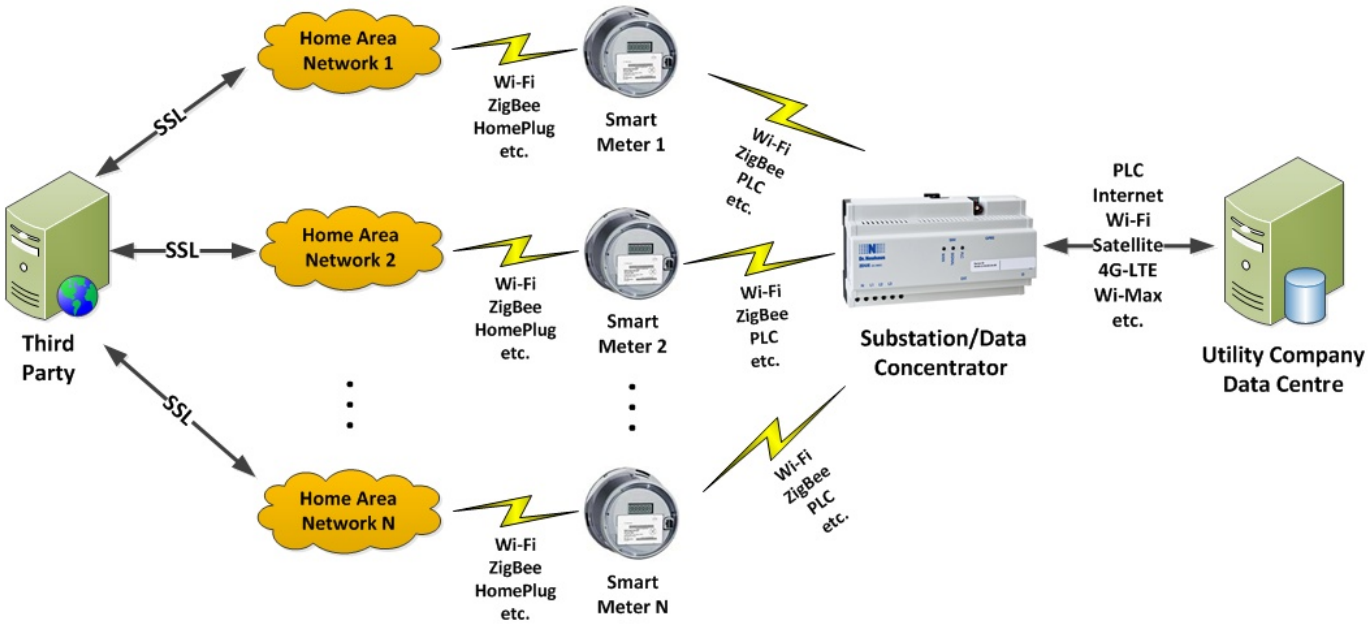

Figure 1. Architecture of a typical Smart-grid metering and control system

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

2. **Substation/data-concentrator network:** consists of a number of smart meters in a certain area as well as a data collector. The connection between smart meters and the data collector might through Wi-Fi, ZigBee, power line carrier (PLC), etc. Typically, the smart meters form a wireless mesh network and forward the meter readings to the data collector through multi-hop communications. The data collector then transmits the accumulated data to the utility company.

3. **Home area network (HAN):** provides the consumer access points to control and monitor the real-time power consumption. The HAN contains a home gateway that receives the power-consumption data from the smart meter and displays it on householder's devices (e.g., laptop, tablet, smartphone). Furthermore, the home gateway may send the power consumption data to a third party for other value-added services (e.g., efficiency advice, supplier selection). The HAN also includes a controller that enables householders to remotely control the status of their home appliances.

4. **Smart meter**: is composed of a microcontroller, a metrology board, and a communication board. Under the control of the microcontroller, the metrology board measures the real-time power consumption, and the meter data is transmitted to both the substation network as well as the home area network through the communication board. The connection between the smart meter and home appliances may be through Wi-Fi, ZigBee, Ethernet, HomePlug, Wireless M-Bus, etc. The smart meter may also contain a disconnection function that (if enabled) allows utility companies or customers to remotely connect or disconnect the home appliances and services.

5. **Third party:** relies on accurate meter readings to provide value-added services for householders, including power efficiency advice, supplier selection, etc. Those services will help householders to manage their power usage in a cost-effective way.

Requirements

The conventional power grid is composed of dedicated power devices that form closed networks with reliable and predicable communication links. In contrast, a smart-grid metering and control system relies on advanced wired and wireless communication networks, thereby inheriting all of the weaknesses and potential cyberspace vulnerabilities of general communication networks. The smart-grid metering and control system is becoming an increasingly common target for cyberspace attacks, and strong and robust security mechanisms are paramount for the prevention of financial fraud, environmental accidents, and a host of other potentially disastrous incidents. In this section, we discuss the major security concerns and requirements for smart-grid metering and control systems.

Efforts from standards bodies and organizations

A number of organizations have been actively working on the development of smart grid security requirements, as illustrated in Box 1. Among existing smart-grid standardization efforts, the NIST Framework and Roadmap for Smart Grid Interoperability Standards and its Interagency Report, "Guidelines for Smart Grid Cyber Security" (NIST IR 7628; tinyurl.com/yb6jpuw), represent the most comprehensive coverage of cyberspace security requirements in the smart grid.

All standards bodies consistently specify three high-level smart-grid security objectives: availability, integrity, and confidentiality. However, even though the standards bodies define the security requirements based on a fairly comprehensive set of use cases in the power industry, there is still a considerable gap between understanding the security requirements in the standards and applying them to design a secure-

Box 1. Examples of organizations working on smart-grid requirements

- Electric Power Research Institute (EPRI; epri.com)
- International Society of Automation (ISA; isa.org)
- IEEE 1402-2000 (tinyurl.com/ox786r8)
- International Electrotechnical Commission (IEC; iec.ch)
- National Energy Board (NEB, Canada; neb-one.gc.ca)
- North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP; nerc.com)
- National Institute of Standards and Technology (NIST; nist.gov)

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

smart grid metering and control system. It is extremely important for designers and practitioners of smart grids to gain deep understanding about a wide range of malicious attacks to the smart grid, as detailed below.

Availability

Availability refers to ensuring timely and reliable access to information, which is the primary security goal of a smart-grid metering and control system. Malicious attacks targeting availability can be considered as denial-of-service attacks (tinyurl.com/jzn67), which intend to delay, block, or even corrupt the communication in the system. In particular, due to the extensive adoption of wireless communication technologies in the smart grid, a jamming attack (tinyurl.com/km9sd9) that fills the wireless medium with noise signals has become the most typical form of physical-layer attack. The jamming attack is able to defer the transmission of messages and to distort the transmitted data signal. As a result, the legitimate receiver cannot recover messages out of the damaged data packets. Jamming attacks are more relevant and serious in the smart grid than other than other networking systems, because the smart grid involves essential resources for people's everyday lives. On the other hand, many man-in-the-middle attacks (tinyurl.com/fco32) can be launched only when the full or partial communication channels can be jammed. Examples include jamming then inserting false location information and jamming then delaying the transmission. Because the network traffic in the smart grid is generally time-critical, it is crucial to evaluate the impact of denial-of-service attacks and to design efficient and effective countermeasures to such attacks.

Integrity

Integrity refers to preventing or detecting the modification or destruction of information by unauthorized persons or systems. Malicious attacks targeting the integrity of a smart grid attempt to stealthily manipulate critical data such as meter readings, billing information, or control commands. Recent research (Liu et al., 2011; tinyurl.com/kzaxzdy) has demonstrated that a new class of attacks, called false data-injection attacks, are highly viable against the state estimation in electrical power grids. Based on the assumption that an attacker has compromised one or several smart meters and is able to access the current power-system configuration information, such attacks can successfully inject arbitrary bogus data into the monitoring centre, and at the same time, pass the data-integrity checking used in current state-estimate processes. Integrity protection can be achieved by authentication, certification, and attestation. More specifically, the smart devices and substation must authenticate each other's identity to thwart impersonation. Data certification of a message prevents modification of data during transmission. Data authentication with non-repudiation goes beyond certification by preventing the sender from claiming that it did not send the data. Substations use attestation to confirm that the memory contents (code and data) on a smart device have not been modified. The security services related to integrity are usually implemented using public-key cryptography, which requires a trusted third party that hosts a key-management service.

Confidentiality

Confidentiality refers to protecting personal privacy and proprietary information from unauthorized access. Malicious attacks targeting confidentiality aim at obtaining desirable information (e.g., power usage, customer's account information) through eavesdropping on communication channels in a smart-grid metering and control system. Although such attacks have negligible effects on the operation of the system, the transmission of fine-grained consumption data by smart meters has raised concerns about privacy. Research (Quinn, 2009; tinyurl.com/pc2st2e) has shown that the consumption data collected by smart meters reflects the use of all electric appliances by inhabitants in a household over time, and it allows criminals to make inferences about the behaviours, activities, or preferences of those inhabitants. Those privacy issues need to be addressed appropriately to reduce customers' fears about potential leakages of their information. Some best practices relating to privacy have been proposed for the design of smart grids (Cavoukian, 2010; tinyurl.com/27r43ds). An emerging trend is for the smart meters to aggregate usage data for billing purposes and support load-balancing and other monitoring functions through peer-to-peer protocols that preserve the consumer's privacy.

Current Approaches

Based on the security guidelines specified by the NIST and other standards bodies, both industry and academia have made efforts to address the challenging security issues in smart-grid metering and control systems by employing various cryptographic techniques. Here, we give an overview of several existing cyber-security solutions proposed by industry and academia for smart-grid communications.

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

Cybersecurity solutions from industry

In 2007 a large stakeholder community was assembled by the ZigBee Alliance to address the security issues in the smart grid; this community developed what is known as the ZigBee Smart Energy Profile (SEP; tinyurl.com/kjfl96m). The ZigBee SEP has been widely adopted as the communication infrastructure in home area networks. Regarding to the security, the ZigBee SEP specifies that each smart meter should be equipped with an Elliptic Curve Qu-Vanstone (ECQV; tinyurl.com/7v4f36a) implicit certificate before deployment. The ECQV certificate is much smaller than a traditional X.509 certificate (tinyurl.com/8e3zr), and it binds a meter's MAC address and manufacture identifier to an ECC key pair (tinyurl.com/egz7y). Although the ECQV certificate issuance has been addressed (Certicom; tinyurl.com/mbug9b), the certificate renewal and revocation processes are not defined in the ZigBee SEP.

For supervisory control and data acquisition (SCADA; tinyurl.com/jcrlz) systems, NIST (2010; tinyurl.com/mfrn42j) suggests AES, SHA-1, and RSA, and IEC 62351 (tinyurl.com/29tm8ll) specifies RSA-1024. However, it is now known that RSA is a poor choice for SCADA networks because of the high computation cost of RSA encryption and the limited computing power of SCADA devices. The Standards Council of Canada (tinyurl.com/m4najzg) and the European Union (tinyurl.com/kvmnswk) also define cybersecurity requirements for smart grids, but do not specify a suite of cryptographic algorithms to meet the requirements, except that the Standards Council of Canada specifies that SHA be used as the secure hash function. It remains an open research problem to find a set of cryptographic algorithms that provide the right combination of security and implementability for the smart-grid metering and control system.

Besides industry alliances and standards bodies, there are a number of manufacturers of smart devices for SCADA networks and meters for smart grids. Implementation details for these devices are generally considered proprietary information, but a few generalizations can be made. The cryptographic algorithms are implemented in software on a low-power 16-bit microprocessor. RSA-1024 or ECC-256/384 is used for public-key services. Symmetric key services use AES-128 or AES-256. Some devices use spread-spectrum modulation. Most smart-device manufacturers implement the security services themselves. A few companies have a hardware security module (HSM; tinyurl.com/7r9v6rv) or similar product that is independent of a specific smart device. SafeNet's PKI HSM (tinyurl.com/k6mbobz) provides public key cryptography with RSA-1024 and ECC-256/384, and symmetric-key cryptography with AES-256 to perform attestation, key management, encryption/decryption, and billing. GE Digital Energy (tinyurl.com/lsjyqsl) makes a family of wireless routers with AES-128 designed to connect to smart meters and controllers. Within Canada, Tofino Security's Industrial Security Solution (tofinosecurity.com) is a server-side software program combined with security devices that act as wired access points with encryption for meters and actuators. Bentek Systems' SCADALink SMX900 (tinyurl.com/mrj74mb) is a modular wireless remote-terminal-unit/modem that supports spread-spectrum communication, but does not appear to have any facilities for encryption, authentication, etc.

Cybersecurity solutions from academia

A critical component of smart grid security is key management, which will ensure the confidentiality, authenticity, and integrity of devices and communications within the grid. Most previous research focused on designing cryptographic protocols to provide certain security functionalities.

Efficient implementations of encryption schemes are essential for providing confidentiality in a smart grid. An experimental study about the performance of a symmetric-key cipher (i.e., DES-CBC) and a public-key cipher (i.e., RSA) on an intelligent electronic device (IED) called TS7250 has been conducted (Wang and Lu, 2013; tinyurl.com/mlzypxp), where the IED is used for sending the transformer status and receiving commands from the control centre. These experimental results show that the computational ability of an IED becomes a bottleneck for the delay performance when performing asymmetric-key cryptography. These authors also suggested that a symmetric-key approach is more suitable for real-time IED communications in power distribution and transmission systems.

Authentication is crucial to protect the integrity of data and devices in the smart grid. Due to the limited computational capabilities of devices, stringent timing requirements, and high data-sampling rates in the smart grid, traditional authentication schemes might not be applicable. Moreover, besides supporting basic data and device authentication, multicast authentication is another desirable feature due to the multicast nature of the smart-grid communication. A number of authentication schemes have been proposed in the literature for smart grids. Szilagyi and Koopman (2009: tinyurl.com/k8pwh46 and 2010: tinyurl.com/l93xwjs) proposed flexible and low-cost multicast authentication schemes

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

for embedded control systems. The basic idea is to verify truncated message authentication codes (MACs) across multiple packets, thereby achieving a good trade-off among authentication cost, delay performance, and tolerance to attacks. Wang and colleagues (2009; tinyurl.com/qxvb49v) proposed a fast multicast authentication scheme for time-critical messages in the smart grid. Their scheme is based on an efficient variant of a one-time signature (OTS) scheme. Although the proposed scheme is efficient in terms of computation, the public key size in an OTS-based scheme is quite large (i.e., on the order of 10KB). Hence, both communication and storage overhead are significant in this case. Lu and colleagues (2012; tinyurl.com/m3xfj5g) conducted an empirical study for a few data-origin authentication schemes in substation automation systems (SAS). These authors compared the performance of RSA, MAC, and OTS on a small-scale SAS prototype and concluded that the existing authentication schemes cannot be applied directly into the SAS due to insufficient performance considerations in response to application constraints.

The heterogeneous communication architecture of the smart grid has made the key management particularly challenging, and it is not practical to design a universal key-management scheme for the entire smart grid. The simplest way is to use a single key shared by all the meters in the smart grid. However, this solution will cause the single point of failure due to the lack of a tamper-proof module in smart meters. Beaver and colleagues (2002; tinyurl.com/qcgsgth) proposed an elementary key-establishment scheme called SKE for SCADA systems. Whereas the master-slave communications are secured by symmetric-key schemes, the peer-to-peer communications are protected by public-key schemes. However, the scheme proposed by these authors does not support efficient multicast and broadcast authentication in the smart grid. Dawson and colleagues (2006; tinyurl.com/lkkoxgb) proposed SKMA, a key management scheme for SCADA systems. These authors introduced a key-distribution centre (KDC) and each node maintains two types of long-term keys: node-to-KDC and node-to-node. A session key in SKMA is generated using the node-to-node key. Unfortunately, SKMA does not consider issues of multicast, key update, and revocation. Choi and colleagues described ASKMA (2009; tinyurl.com/mooapta) and ASKMA+ (2010; tinyurl.com/ml2kvqm) for key management in SCADA systems, respectively. Both schemes are designed based on the usage of a logical key hierarchy (LKH), which is able to achieve efficient key management among all nodes. In particular, ASKMA supports both multicast and broadcast authentication and the performance has been further improved in ASKMA+.

Although many encryption, authentication, and key-management schemes have been proposed, their performance does not seem to fulfill the stringent timing requirements of the smart grid. Therefore, fine-grained and advanced security protocols still need to be developed for protecting different communication networks in smart grids.

In a smart grid, the utility company needs the real-time power-consumption data for planning purposes as well as for providing accurate and authentic billing. For the utility company, the correctness of the calculated bills is the most important issue. However, from the customer's perspective, privacy is the main concern. Researchers have designed privacy-preserving billing protocols using advanced cryptographic techniques such as zero-knowledge proof (tinyurl.com/2z5blx) and homomorphic encryption (tinyurl.com/depohp). Bohil and colleagues (2010; tinyurl.com/mmfv5kt) proposed a privacy model for smart metering, in which a trusted third-party proxy is introduced to collect meter readings from individual customers and aggregate data before forwarding it to the utility company. Later on, Garcia and Jacobs (2012; tinyurl.com/kmxnnh7) proposed the use of homomorphic encryption to prevent the utility company from accessing the power consumption data of individual households. Using those advanced cryptographic techniques, utility companies only receive the commitments (tinyurl.com/ljgcasm) of the real-time power consumption instead of the raw data from smart meters, and customers can prove to the utility company that a utility bill has been correctly generated.

Besides research into addressing general privacy concerns for the smart grid, a number of researchers have been focusing on designing and implementing privacy-preserving billing protocols. Rial and colleagues (2011; tinyurl.com/lha6zpf) proposed a privacy-preserving billing protocol in which the power-consumption data is sent to the user along with other information from the smart meter, and the user computes the bill based on the pricing policy during each billing period. After that, the user sends the proof of correct computation to the utility company, where a homomorphic commitment scheme has been used to construct the proof. Kursawe and colleagues (2011; tinyurl.com/ldc7cfx) presented a set of protocols that can be used to privately compute aggregate meter measurements over defined sets of meters without revealing any additional information about the individual meter readings. Moreover, their

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

protocols also allow for detection of fraud and leakage as well as network management and statistical processing of meter measurements. Molina-Markham and colleagues (2012; tinyurl.com/mjyz2a8) implemented the privacy-preserving billing protocol proposed by Rial on a MSP430-based microcontroller and verified the feasibility of designing privacy-preserving smart meters using low-cost microcontrollers.

Future Outlook

The smart-grid metering and control system consists of heterogeneous wired and wireless networks and devices from various domains. Each sub-system in the smart grid currently follows the different standards and regulations and has distinct security requirements. In particular, the smart grid faces unique challenges stemming from the combination of stringent security requirements, limited computational resources, time-critical message delivery and responses, and the use of heterogeneous networks with multiple authentication and protection mechanisms. Although a lot of efforts have been made by industry and academia to address a wide range of security issues in the smart grid, there are still many challenges that need to be tackled before smart grids can be widely deployed. From the viewpoint of cryptographic technique, we highlight several research areas and directions that need to be further investigated.

A lightweight cipher suite for smart-grid devices
The tight cost and resource constraints inherent in mass deployments of smart-grid devices bring forward impending requirements for implementing a lightweight cipher suite that can perform strong authentication and encryption, and provide other security functionalities. Previous research has shown that using classical cryptographic algorithms that are designed for full-fledged computers has become the bottleneck in many smart-grid applications. In order to meet the stringent time requirements in a smart grid, it is highly desirable to standardize a set of lightweight symmetric-key and asymmetric-key ciphers for securing smart-grid applications.

Advanced key management for smart-grid networks
Encryption and authentication are crucial cryptographic processes in a smart grid, because they protect data integrity and confidentiality, and an efficient key-management scheme is the foundation that ensures the secure operation of a smart grid. Because a smart grid is composed of heterogeneous communication networks and involves symmetric-key and asymmetric-key cryptosystems, a large set of cryptographic keys need to be managed in an efficient manner. A sophisticated key-management framework needs to be designed to deal with security services as well as the seamless handover of those services across different sub-systems in the smart grid.

Privacy-preserving operations in smart-grid networks
Smart-grid communications have raised serious concerns about user privacy due to the possibility of inferring customers' behaviour and habits from the detailed energy usage information, which can lead to potential risks that consumers would be vulnerable to criminal activities and personal information leakage. Advanced privacy-preserving security schemes need to be developed and integrated into smart-grid networks to enable utility companies to perform the regular business operations such as customer billing only using aggregated power-consumption information. The real-time power consumption data should only be accessible by individual customers.

Conclusion

Smart-grid metering and control systems hold enormous promise for improving efficiency, convenience, and sustainability. However, the complicated and heterogeneous system architecture has made securing the smart grid particularly challenging. Cybersecurity in the smart-grid metering and control system is an important and rapidly evolving area that has attracted attention from government, industry, and academia. In this article, we introduced the high-level architecture of a smart-grid metering and control system, detailed the system's security requirements, summarized the recent efforts from industry and academia, and highlighted several areas and directions for further research. Our objective is to shed some light on cybersecurity in the smart grid and to trigger the close collaborations among government, industry, and academia.

Based on our discussion in this article, it is clear that implementing an integrated and fine-grained security solution that is able to address potential security and privacy issues in each sub-system of a smart grid is critical to guarantee its successful deployment. Moreover, the design of security solutions should take into account the salient features of the smart grid as well as the underlying power system. Looking to the future, the joint efforts from industry and academia will make the era of "smart energy" become reality at a staggering speed.

Security Challenges in Smart-Grid Metering and Control Systems

Xinxin Fan and Guang Gong

About the Authors

Xinxin Fan is a Research Associate in the Department of Electrical and Computer Engineering at the University of Waterloo, Canada. He holds a PhD degree in Electrical and Computer Engineering from the University of Waterloo, as well as a BSc degree in Applied Mathematics and an MEng degree in Information Systems and Telecommunication Engineering from Xidian University, China. His research interests range from fast and secure software and hardware implementations of cryptographic algorithms to the design and the analysis of security protocols for wireless and wireline networks.

Guang Gong is a Professor in the Department of Electrical and Computer Engineering at the University of Waterloo, Canada, and she is the Managing Director of the Centre for Applied Cryptographic Research at University of Waterloo. She holds a BSc degree in Mathematics, an MSc degree in Applied Mathematics, and a PhD degree in Electrical Engineering from universities in China. Dr. Gong has also held a fellowship at the Fondazione Ugo Bordoni, in Rome, Italy, and was Associate Professor at the University of Electrical Science and Technology of China. Her research interests are in the areas of sequence design, cryptography, and communication security.

Citation: Fan, X. and G. Gong. 2013. Security Challenges in Smart-Grid Metering and Control Systems. *Technology Innovation Management Review*. July 2013: 42–49.

Keywords: smart grid, cybersecurity, privacy, encryption, authentication