Secure Service Provision in Smart Grid Communications

Daojing He, Chun Chen, and Jiajun Bu, Zhejiang University

Sammy Chan, City University of Hong Kong

Yan Zhang, Simula Research Laboratory and University of Oslo

Mohsen Guizani, Qatar University

ABSTRACT

The smart grid provides a platform for third-party service providers to remotely monitor and manage energy usage for consumers. At the same time, the involvement of service providers brings a new set of security threats to the smart grid. In this article, we first identify the cyber security challenges on service provision in the smart grid. Then we present two main security issues related to service provision and provide potential solutions. The first one is to establish a secure communication procedure among the electric utility, consumers, and service providers. The second one is to provide a privacy-preserving yet accountable authentication framework among the smart grid entities without relying on any trusted third party. Finally, we suggest directions of future work on secure service provision by describing several open issues.

INTRODUCTION

An increasing demand for reliable energy supply and numerous technological advancements have motivated the development of smart grids. As the world's largest engineered system, the smart grid will expand the current capabilities of the electric grid's generation, transmission, and distribution systems to provide an infrastructure capable of handling future requirements for distributed generation, renewable energy sources, electric vehicles, and the demand-side management of electricity. A smart grid is composed of power infrastructure and communication infrastructure. The power infrastructure generates and distributes electricity to consumers. The communication infrastructure controls the power infrastructure and enables intelligent operation of the power grid. The success of the smart grid rests on a communication infrastructure that is secure, reliable, and cost effective.

Although deploying the smart grid has enormous social and technical benefits, several security and privacy concerns arise. The interconnection nature of the smart grid partially explains its success, since the network can be easily accessible by many people at different places. The reverse side of the coin of this success is the great weakness of the smart grid facing malicious attacks. Increasingly interconnected smart grids will unavoidably provide external access, which in turn can lead to compromise and infection of components.

Compared to current electrical grids, a new feature of smart grids is that more and more service providers will be involved that can monitor and manage the energy usage for their subscribed consumers by the existing communication network [1]. Service providers are needed because it is highly unlikely that consumers, even if they could understand their cost of energy or environmental impact, will be able to effectively manage their energy usage as it involves too many variables that may change frequently and requires specialized tools. For example, with the help of service providers, consumers react to price signals to achieve active load management [2]. However, the existence of service providers raises new questions about smart grid security. First, since customers (e.g., electric utilities and consumers) work closely with service providers to manage their energy usage, they need to share more information about how they use energy and thus expose themselves to privacy invasions. Second, the involvement of service providers adds significant complexity to the infrastructure, which in turn introduces numerous opportunities for attack exploitation. From the perspective of the defender, more complex systems require dramatically more effort to analyze and defend, because of the state-space explosion when considering combinations of events. The cyber security of the smart grid should not be compromised by service providers when they deliver existing or emerging services.

In the remainder of this article, we first introduce the structure of the smart grid, as well as general security threats it will have to face and the corresponding solutions. After giving an overview of secure service provision in the smart grid, we present two new and important security challenges due to the addition of service providers. The first is to establish a secure communication procedure among the electric utility, consumers, and service providers. The second is

0163-6804/12/$25.00 © 2012 IEEE

A wide variety of motivations exist for launching attacks on smart grids, ranging from economic reasons, to pranks, and all the way to terrorism. The emerging smart grid, while benefiting the benign participants (i.e., electric utilities, consumers, service providers), also provides opportunities for adversaries.

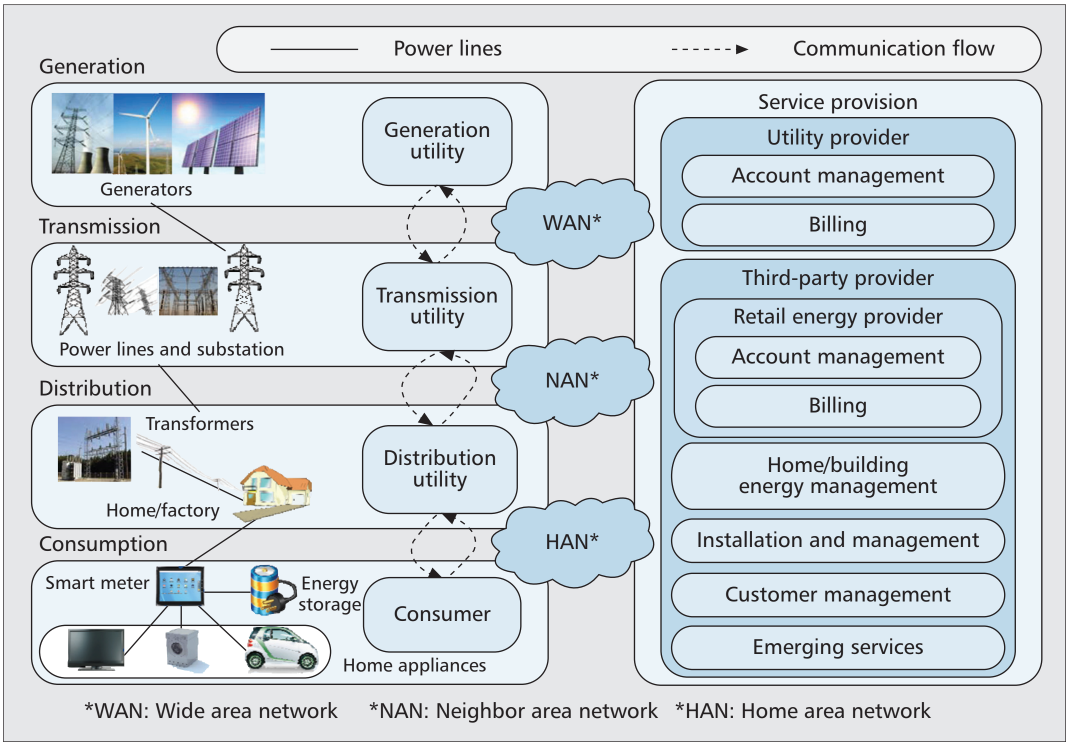

Figure 1. *An overview of the smart grid with various service providers.*

to provide a privacy-preserving yet accountable authentication framework among the smart grid entities without relying on any trusted third party. We also suggest solutions to these two issues. Finally, we conclude with some outstanding security issues that need further research work.

Cyber Security in Smart Grids

Overview of Smart Grids

As shown in Fig. 1, a smart grid consists of five components [3]:

- Generation: Power system generators produce electric power by different means such as hydropower, solar, wind, tidal forces, and other generation sources.
- Transmission: A very high voltage infrastructure transfers electrical energy from power plants to electrical substations.
- Distribution: Distribution networks step down voltage and delivers electricity from substations to consumers.
- Consumption: Energy consumers use the electric energy in a multitude of ways.
- Service provision: The service provider performs services to support the business processes of power system generators and consumers.

The home area network (HAN) is an important part of the smart grid communication network through which the consumers are able to communicate with service providers and electric utilities. In a HAN, there are typically a number of smart meters and electric appliances. A smart meter may also act as the gateway of a HAN. A neighbor area network (NAN) is formed under one substation where multiple HANs are hosted. Finally, a power plant may leverage a wide area network (WAN) to connect distributed NANs.

General Cyber Security Threats

A wide variety of motivations exist for launching attacks on smart grids, ranging from economic reasons (e.g., the consumers want to reduce electricity bills), to pranks, and all the way to terrorism (e.g., threatening people by controlling electricity and other critical resources). The emerging smart grid, while benefiting the benign participants (i.e., electric utilities, consumers, service providers), also provides opportunities for adversaries.

As shown in Fig. 2, there are four general categories of attacks on the communication network of smart grids [4]. *Interruption* occurs when a message is blocked to/from a particular service. Some examples are channel jamming and denial-of-service (DoS) attacks. *Interception* refers to an adversary eavesdropping on a message intended for a recipient. Some examples are traffic analysis and release of message contents. *Modification* refers to the action of intercepting and then transmitting a modified message to a particular service. An example is alteration of data. Fabrication refers to making up a message and inserting it into the normal message flow. Some examples are message forgery, service provider spoofing, and smart meter spoofing.

Cyber Security Properties and Approaches

There are some basic security properties for smart grids [4]. *Confidentiality* is the ability to keep secret or private information (e.g., meter data) from being disclosed to unauthorized parties. *Integrity* refers to the ability of the smart grid components (e.g., smart meter) to prevent an unauthorized user from modifying the information. *Authentication* is the process of ensuring that someone (e.g., service subscriber) or something is whom they claim to be. Authorization is the right to execute certain actions (e.g., reading a particular smart meter). *Privacy* means that one can keep some information solely to oneself. *Availability* refers to the ability of authorized users to obtain access to certain resources (e.g., electricity service) whenever needed. *Non-repudiation* refers to the ability to prevent someone who has performed a particular action (e.g., subscribing to value-added services) from denying what he/she has done.

There are commonly used cryptographic mechanisms to meet the basic security properties, which can be used to prevent the four categories of attacks. The standard way to ensure confidentiality is through encryption and decryption. Integrity checks are provided primarily through hash functions. Authentication is achieved either by using passwords in a peer-to-peer relationship or involving a certification agent (CA). For authorization approaches, they can be either identity-based or token-based. Identity-based approaches are typically associated with access control lists, while token-based approaches are also referred to as capability-based authorization. Privacy is provided via some privacy-aware cryptographic primitives (e.g., blind signature, ring signature and group signature). Some approaches (e.g., jamming detection mechanisms) to resist DoS and jamming attacks are used to achieve availability. Non-repudiation is provided primarily via the digital signature technique, which can be used to claim that an entity was uniquely responsible for a message or an action.

Secure Service Provision Overview

Service Provision

As shown in Fig. 1, service providers consist of a utility provider and a third-party provider. The former is an electric utility, while the latter is a company entirely separate from the electric utility. Typical applications in the service provider domain shown in Fig. 1, which are equivalent to the service applications specified by NIST [1], are discussed as follows:

- Account management denotes managing the supplier and customer business accounts.
- Billing indicates managing customer billing information, including sending billing statements and processing payments.
- Building/home energy management monitors and controls building/home energy usage and responds to smart grid signals while minimizing impact on building/home occupants.
- Installation and management denotes installing and maintaining various customer premises equipment that interact with the smart grid.
- Customer management indicates managing customer relationships by providing point of contact and resolution for customer issues and problems.
- Emerging services refer to all services and innovations that have yet to be created. These will be instrumental in defining the smart grid of the future.

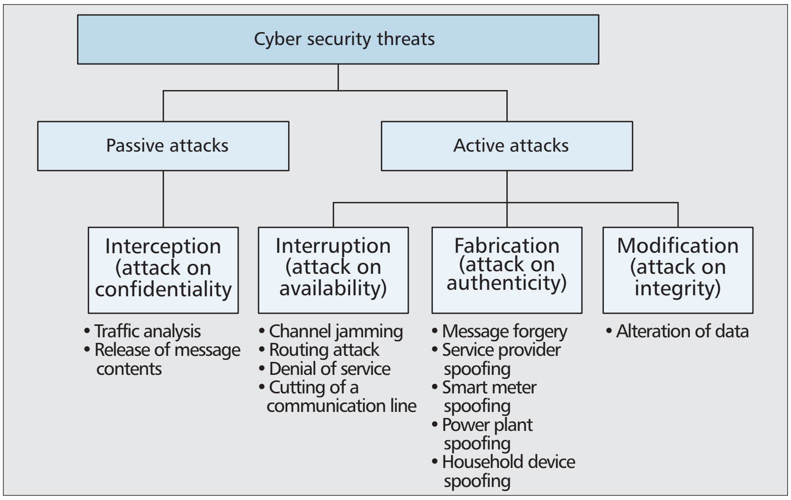
Cyber security threats
Passive attacks
Active attacks
Interception (attack on confidentiality)
Interruption (attack on availability)
Fabrication (attack on authenticity)
Modification (attack on integrity)
• Traffic analysis
• Release of message contents
• Channel jamming
• Routing attack
• Denial of service
• Cutting of a communication line
• Message forgery
• Service provider spoofing
• Smart meter spoofing
• Power plant spoofing
• Household device spoofing
• Alteration of data

Figure 2. *Cyber security threats on smart grid communications.*

Benefits from Service Providers

Service providers will create new and innovative services and products to meet the new requirements and opportunities presented by the evolving smart grids. The benefits brought by the presence of service providers in the deployment of smart grids include [1]:

- The development of a growing market for third parties to provide value-added services and products to customers and electric utilities.
- The decrease in cost of business services due to competition brought by the open market. For example, installation and management service providers are responsible for installing smart electric devices (e.g., smart meters), competitions among them will lower the price of installing smart meters.
- A decrease in purchased energy as customers become active participants in the power supply chain. For example, some farms now offset energy costs by producing electricity using solar panels and wind turbines. With the help of service providers, farmers can even sell excessive generated energy back to the utility, thereby further reducing, and possibly eliminating, energy costs.

Another example is home/building energy management based on dynamic pricing which can significantly reduce the electricity bill. During off-peak periods, electric power is relatively less expensive and thus can be used without restrictions (e.g., diverted to energy storage). On the other hand, during peak periods when the price is high, some appliances (e.g., washer, plug-in electric vehicle) will be powered by stored energy or turned off [3].

Design Principles of Secure Service Applications

Price information, meter data, control commands, software, total power consumption information (for billing), device information (e.g., device type and device ID), and subscription information (e.g., user registration and service related information) are the core information exchanged in service applications which we consider in this article. With the development of smart grids, while more types of information will be exchanged, these core infor-

Application category	Information type	Confidentiality/ privacy	Integrity/ authentication	Non-repudiation	Availability	Authorization
Customer management	Subscription	Intermediate	High	High	Low	N/A
	Software	N/A	High	N/A	N/A	Low
Installation and management	Subscription	Intermediate	High	High	Low	N/A
	Device information	High	N/A	N/A	Low	Intermediate
	Software	N/A	High	N/A	N/A	Low
Home/building energy management	Meter data	High	High	Intermediate	Low	Intermediate
	Commands	Low	High	Intermediate	High	Intermediate
	Subscription	Intermediate	High	High	Low	N/A
	Device information	High	N/A	N/A	Low	Intermediate
	Software	N/A	High	N/A	N/A	Low
	Price	Low	High	Intermediate	High	N/A
Billing	Total power consumption	Low	High	Intermediate	Low	Low
	Subscription	Intermediate	High	High	Low	N/A
	Software	N/A	High	N/A	N/A	Low
	Price	Low	High	Intermediate	High	Low
Account management	Subscription	Intermediate	High	High	Low	N/A
	Software	N/A	High	N/A	N/A	Low

Table 1. *Security level of the core information types with respect to cyber security properties in different service applications.*

mation types provide a comprehensive sample of security issues in service applications.

We now examine the security level of the core information types with respect to the main security properties in typical service applications. Here, we take home/building energy management and billing as examples.

Home/building energy management: Confidentiality of meter data and device information is very important, because such information exposes customer habits and behaviors. Certain activities, such as watching television, have detectable power consumption signatures. For all applications, confidentiality of software should not be critical because the security of the system should not rely on the secrecy of the software, but on the secrecy of the key materials. Except device information, integrity of all other core information is very important. For instance, injecting false prices, such as negative pricing, will lead to power shortage or other significant damages on the target region.

Billing: Confidentiality of total power consumption is not important, because it contains little information about user and corporate usage privacy. Confidentiality of price information should be non-critical, and service providers can simply broadcast price information to the residential meters. However, integrity of price information is very important because fake price information can generate huge financial impacts on electricity markets. Availability and non-repudiation of price information are critical due to serious financial and possibly legal implications.

Table 1 summarizes the security level of the core information types with respect to cyber security properties in different service applications. "High" implies that the property of certain information is very important/critical, and "medium" and "low" classify properties that are important and non-critical, respectively. Besides, "N/A" classifies properties that are not applicable. Based on this classification, designers of security protocols for specific applications can focus effort on the most critical issue first.

Secure Communication among Electric Utility, Consumers, and Service Providers

Figure 3a depicts the communication procedure among an electric utility, consumers, and service providers, which is advocated by recent research

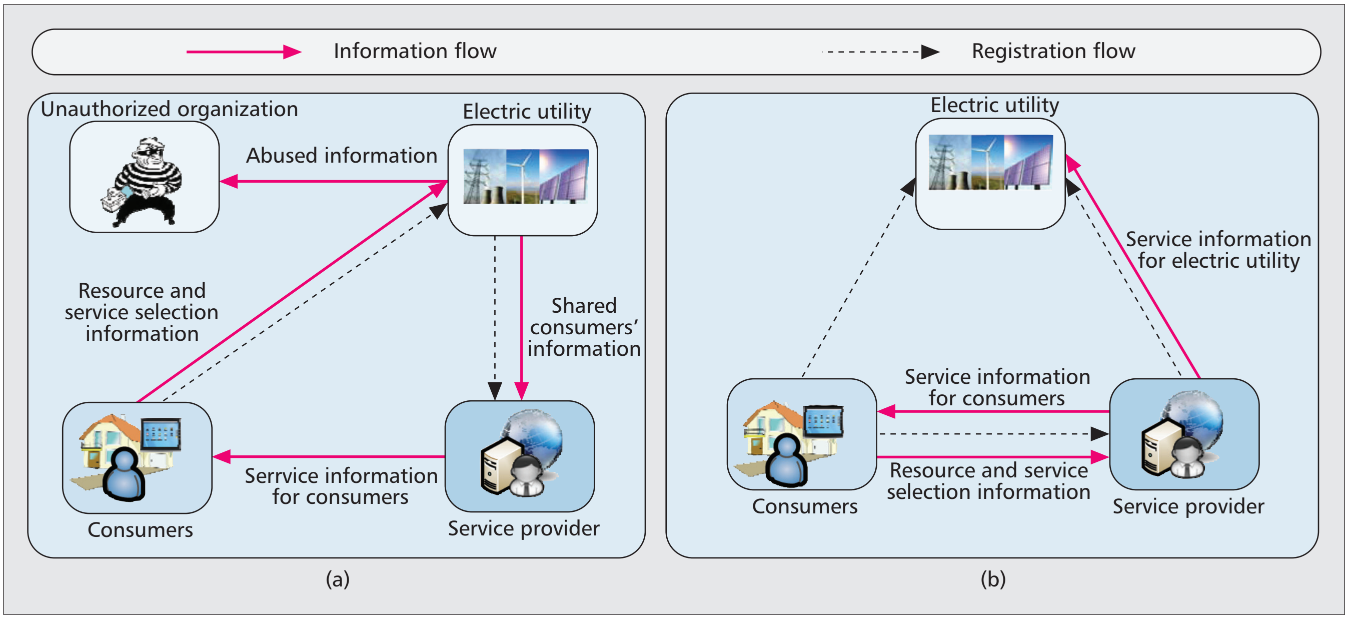
Information flow
Registration flow
Unauthorized organization
Electric utility
Abused information
Resource and service selection information
Shared consumers' information
Service information for consumers
Consumers
Service provider
(a)
Electric utility
Service information for electric utility
Service information for consumers
Resource and service selection information
Consumers
Service provider
(b)

Figure 3. *Secure communication procedure among electric utility, service providers, and consumers: a) traditional approach; b) the proposed approach.*

work [5]. Here, the service providers are companies entirely separated from the electric utility. A consumer interacts with the electric utility to select a service from a service provider and grants permission to the service provider by notifying the electric utility to share his/her information. Then, the electric utility interacts with the service provider to indicate the service requested by the consumer and provide the consumer's information. Such a communication procedure is inefficient as a consumer has to indirectly deliver his/her information to a service provider through the help of the electric utility. More importantly, it is insecure because the electric utility may share the consumer's information to other unauthorized organizations or misuse it for its own purposes. We consider home energy management service provider as an example. A consumer needs to submit real-time electric usage statistics and device information to the service provider through the electric utility. However, the electric utility may not need to know these information.

To address the security weakness and efficiency problem of the traditional communication procedure, a novel secure communication procedure is suggested as follows.

As shown in Fig. 3b, a consumer directly interacts with a service provider and submits his/her information. Then the service provider only needs to transmit the service information such as commands (e.g., cutting down the electric power of a particular consumer) to the electric utility. With the employment of the following public key infrastructure, a consumer will be able to directly establish contracts with service providers for individual electrical devices and use the smart meter to relay messages between internal devices and the service provider in a secure way. The electric utility acts as the authoritative CA in providing public key certificates for the smart grid entities (i.e., smart meters and service providers). Each smart meter chooses its public/private key pair and registers with the electric utility, and then obtains a public key certificate for its identity and public key. The public key certificate and the electric utility's public key are stored in every smart meter before installation. In order to be able to serve consumers, service providers follow the same procedures to obtain public key certificates for their identities and public keys. Then the service providers will be able to establish contracts with individual consumers for devices that they support. The smart meter will limit communication with only contracted service providers whose certificates are valid. To ensure the security of distributing public key certificates, instead of the electric utility, the law authority (e.g., local police office) can act as the CA in the smart grid. In a similar fashion, the electric utility registers with the law authority, and then obtains a public key certificate for its identity and public key.

In order to optimize the grid and manage the demand in a much more efficient way, consumers have to share information with the service providers. However, in some circumstances, consumers' information may be misused by some service providers. Therefore, the trust of service providers should be limited. Moreover, dishonest consumers and inside attackers should be pinpointed with the cooperation of the law authority. To address these challenges, it is suggested to deploy a novel privacy-preserving yet accountable authentication framework based on this new secure communication procedure. This will be discussed in detail in the next section.

Privacy-Preserving yet Accountable Authentication Framework

The creation of smart grids, especially as household devices become more and more intelligent and service providers become more involved in

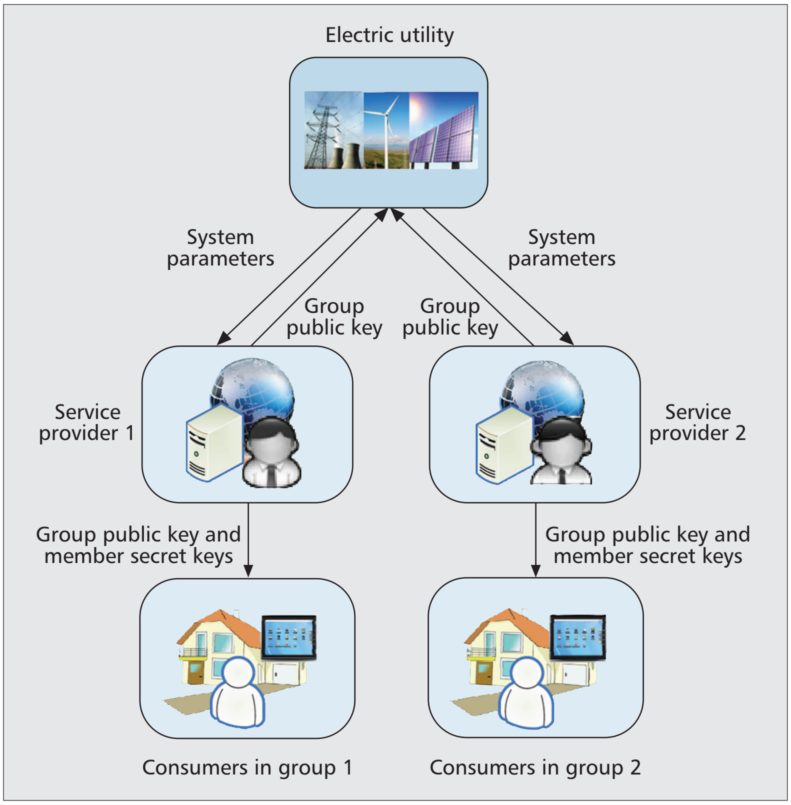

Figure 4. *Trust and key management model of the proposed privacy-preserving and accountable authentication framework.*

household power monitoring and management, brings more challenges with respect to security, privacy, and accountability:

Security: Due to the highly distributed and inherently insecure nature of wireless networks, it is essential for service providers to enforce access control to cope with free riders and malicious attacks. Dynamic access to the service providers should be subject to successful authentication based on properly pre-established trust between consumers and service providers.

Privacy: It is critical to provide adequate consumer privacy, especially in contexts such as smart meter privacy. Depending on the roles and the available resources, adversaries can be outsiders (e.g., eavesdroppers, other consumers) or insiders (e.g., service providers and the electric utility). The wide deployment of smart grids becomes possible only after the smart grid system provides the ability to maintain their desired level of anonymity.

Accountability: Dishonest consumers and inside attackers should be pinpointed with the cooperation of the law authority.

In addition, security and privacy of wireless/wired networks is usually achieved through a trusted third party such as key distribution or management center, but the establishment and maintenance of this entity in such a distributed environment is not trivial. Thus, achieving security, privacy, and accountability without involving any trusted third party is of the most concern in pushing the success of smart grids for their wide deployment and supporting value-added services.

We further illustrate the importance of the above requirements by considering the following application scenarios:

- We consider a service provider for energy consumption analysis as an example. Only authorized consumers who have registered with the service provider can get the service. The privacy of consumers must be guaranteed in the sense that the power usage reports of a consumer should be protected, while the law authority should be able to reveal the sender identity of the report for any disputed event.
- The electricity usage management service provider is responsible for managing a consumer's energy savings profile, and coordinating the smart grid demand response (DR) of all household devices and other DR products in the consumer's home [6]. For both billing purposes and avoiding abuse of service resources, it is also essential to prohibit free riders and only allow subscribed consumers to access the service. On the other hand, a subscriber might not want anyone including the service provider to associate his/her identity with the electricity usage information.

Related Studies in the Literature

Despite the necessity and importance, security and privacy research in the smart grid communication network is still in its early stages, especially with respect to an authentication framework with the involvement of service providers. In the literature, some schemes have been proposed for achieving security in the smart grid (e.g., [7, 8]). Identity-based cryptosystems have been demonstrated to be feasible for providing a zero-configuration encryption and authentication solution for end-to-end secure communications [7]. Based on public key cryptography, a model has been proposed to ensure the privacy and integrity of communicating parties within the smart grid [8]. We observe that protecting consumers' identity privacy and providing accountability have not been studied yet.

The existing privacy-aware cryptographic primitives are not applicable to achieve the goal discussed above. Ring signature and blind signature algorithms can only provide irrevocable anonymity, while here it demands user accountability and hence revocable anonymity. Group signature algorithms do provide revocable anonymity. That is, a group signature scheme allows any group member to sign a message on behalf of the group using its member secret key without revealing its identity. Any pair of signatures generated by the same group member cannot be linked together by any entity except the trusted group manager. Any signed message can be verified using the group public key. Moreover, different from blind signature and ring signature, in exceptional cases such as a legal dispute, a group signature can be opened by the group manager to reveal unambiguously the identity of the signature's originator. However, the revocation capability of group signature algorithms degrades consumer privacy protection because when directly applied to smart grids, either the electric utility or service providers, who usually serve as the group managers, will always be able to track each consumer. This is not desirable, especially in a smart grid where the electric utility and service providers are not highly trustworthy. According to the above analysis, it is clear that simultaneously achieving authentication, privacy, and accountability is still an open challenge in the smart grid communication network.

Our Proposed Approach

Figure 4 shows our proposed trust and key management model. It involves three kinds of entities: electric utility, service providers, and consumers organized in groups. Here, the service providers are companies entirely separate from the electric utility. Each consumer group is a collection of consumers according to contacted service provider. For example, a consumer group consists of all consumers who have registered to the same capacity bidding program service provider. Our protocol does not rely on the existence of a trusted third party, and thus is more feasible in practice. In this case, the trust of all entities is limited. Thus, any entity should be prevented from compromising user privacy. Each consumer group has one group manager (i.e., the service provider) responsible for distributing member secret keys, adding and removing consumers. Before accessing a service provider, each consumer has to enroll in the consumer group whose manager thus knows the real identity of the consumer. The electric utility generates the system parameters and group private key, and keeps the group private key secretly. Upon receiving a registration request from a service provider, the electric utility delivers the system parameters to this service provider. Then, as the group manager, the service provider generates the group public key. For the purpose of non-repudiation, the electric utility, service providers, and consumers sign on their messages under a standard digital signature scheme.

Such a key management scheme is based on the principle of "separation of powers" and possesses a number of salient features. First, from the point of view of access control, each legitimate consumer with a valid member secret key can generate a valid access credential (i.e., the group signature of a fresh access request). The validity of this access credential can be verified by the service provider through the group public key. Hence, access security is guaranteed. Second, our protocol divides the group private key and the mapping of the member secret keys to the identities of the consumers among two autonomous entities: the electric utility and service provider. Electric utility knows the group private key, but not the mapping of the member secret keys to the identities of the users; as the group manager, a service provider knows the mapping of the member secret keys to the identities of the consumers, but not the group private key. As a result, given an access credential generated by a consumer, neither the service provider nor the electric utility can determine consumer's identity or compromise his/her privacy. Therefore, user privacy is enhanced. Finally, with the help from both electric utility and user group manager, only the law authority can link any communication session to the corresponding consumer who is responsible. Thus, in case of service disputes or frauds, the law authority can precisely identify the responsible consumer and hold him/her accountable. Hence, user accountability can be attained as well.

To achieve the goal of the proposed framework, we need to modify the key generation and tracing phases of the existing construction of a group signature. Here, we choose the short group signature proposed by Boneh and Shacham [9] as an example, which is secure and considered to be best suited to wireless communication applications. As shown in Fig. 5, first, the electric utility generates the group private key *gmsk* (called the private key of the group manager in [9]) and system parameters, keeps the former secretly, and distributes the latter to each group manager (i.e., each service provider). With the system parameters, each group manager selects a random number γ as the private key, and then computes the group public key *gpk*. After that, the group manager delivers the group public key *gpk* to each group member. The group manager keeps the mapping between each individual consumer *i* and his/her corresponding member secret key $gsk_i = (A_i, x_i)$ (called a user's private key in [9]), where x_i is a number randomly picked for each user, and A_i is computed from x_i and γ. Also, signing and verification algorithms are kept same as the original group signature construction [9].

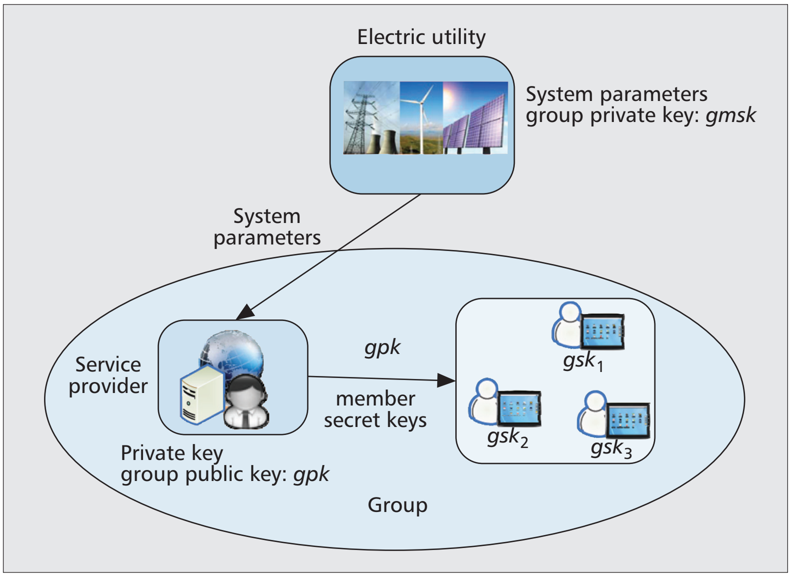

Figure 5. *The proposed privacy-preserving and accountable authentication framework based on Boneh's group signature scheme.*

It should be noted that in order to trace a consumer, one has to know the corresponding A_i value of the consumer's gsk_i. Only with such knowledge can one connect an access credential (i.e., signature generated by the consumer's member secret key) to the consumer and thus trace the consumer. With the proposed adoption on group signature construction, the electric utility knows the group private key, but does not know the mapping between the consumer and the user's member secret key. Thus, the electric utility cannot link a signature to the corresponding consumer who is responsible. The group manager knows the mapping between the consumer and the user's member secret key (A_i, x_i). But without knowing the group private key, the group manager cannot recover A_i, which essentially disables it from tracing a particular consumer by the signature he/she generated.

When the law authority decides to track a particular attacker who is responsible for a certain communication session, the law authority transmits the group signature to the electric utility, and the electric utility verifies that the group signature is

Governments need to establish a regimen of consumer and service provider protections in smart grids. Such rules should be tantamount to the Health Insurance Portability and Accountability Act for the health industry, in which laws would identify the rules of the road.

	Generate *gmsk* and system parameters	Compute *gpk*	Compute gsk_i	Sign	Verify	Track
Time (CPU = 1.6 GHz) (ms)	26.049	8.720	8.726	80.925	90.628	100.900
Time (CPU = 2.4 GHz) (ms)	17.491	5.871	5.734	54.199	60.647	67.653
Time (CPU = 3.1 GHz) (ms)	13.370	4.485	4.437	41.580	46.729	51.997

Table 2. *Running time for each phase of our proposed privacy-preserving and accountable authentication framework.*

valid, uses the group private key to obtain the consumer's A_i, and then reports A_i to the law authority. After that, the law authority delivers A_i to the user group manager, the manager can look up the mapping to find the corresponding consumer identity, and then reply to the law authority. At this point, with the help of the electric utility and the user group manager, only the law authority gets to know about which particular consumer is responsible for the communication session in audit.

Table 2 presents the measured running time for each phase of our proposed approach, which is tested on laptop PCs with different computational power. Type A pairings (./param/a.param) of the Pairing-Based Cryptography Library (version pbc-0.5.12) are used in our implementation. We have performed the same experiment 10,000 times and taken an average over them. Here we consider a 1.6-GHz laptop PC as an example. Generating a member secret key gsk_i, signing a 10-byte message, and computing a consumer's A_i (for tracking) take 8.726 ms, 80.925 ms, and 100.9 ms for a service provider, a consumer, and the electric utility, respectively. From the table, we can see that our framework is efficient in practice.

Conclusion and Open Issues

In this article, we argue that the involvement of service providers in the smart grid poses a series of new security and privacy challenges. We have proposed a new secure communication procedure among the smart grid entities. Compared with traditional approaches, the proposed procedure is superior in the aspects of security features and communication/computation efficiency. We have also proposed a mechanism to achieve privacy-preserving yet accountable authentication framework without relying on any trusted third party.

The work described above demonstrates that a rethinking of the commonly used methods is required to address the new security concerns. Thus, a concerted effort by the industry, the research community, and the policy makers is required to achieve the vision of a secure smart grid. Here, we point out some more important challenging issues that need to be addressed in the context of service provision security.

Establishment of Regimen of Consumer and Service Provider Protections

Governments of a nation (or region) need to establish a national (or regional) regimen of consumer and service provider protections in smart grids. Such rules should be tantamount to the HIPAA (Health Insurance Portability and Accountability Act) for the health industry, in which laws would identify the rules of the road for how sensitive data (e.g., subscription information, customer data) are collected, to whom they are exposed, and the consequences of information abuse. Because these laws will help customers, service providers, and electric utilities to assess risk, they could dramatically increase smart grid adoption.

An employee of electric utilities or service providers who is authorized to access smart grid system resources can execute actions that are difficult to detect and prevent. Moreover, privileged insiders know the deployed defense solutions well and hence can find ways to circumvent them. High accessibility to smart grid components provides opportunities to escalate an authorized access to a powerful attack [3].

For example, the Google PowerMeter service receives real-time usage statistics from installed smart meters. Subscribers to this service can visualize their usage via a customized web page. Although the final privacy policy of this service is yet to be announced, early versions have the possibility of allowing the company to use this information for commercial purposes. Besides this type of opt-in services, subscribers also have little control over the use of power information delivered to utility companies. Unfortunately, currently in the United States, there are no federal laws or regulations that clearly define the protections of energy usage data, and it is unclear how existing privacy laws apply to customer energy usage [2]. Thus, future works should consider how to establish a regimen for assessing such malicious insiders.

Effective Cybersecurity Solutions for Service Applications

Research and development of effective cyber security technologies require understanding current and emerging smart-grid infrastructure, particularly its constraints and opportunities. Depending on where the solution will be employed, developers should carefully consider the relevant security and efficiency requirements (e.g., integrity, scalability, adaptability). For example, currently, numerous security protocols exist in service applications, such as Secure Sockets Layer/Transport Layer Security protocols, Internet Protocol Security, and Secure Shell. However, these protocols are inapplicable on some low-power devices (e.g., consumer-owned home appliances) or constrained networks (e.g., HANs). Thus, lightweight protocols should be developed and deployed to secure service applications.

DoS/DDoS Resistance of Service Provision

Because service providers and customers (e.g., electric utilities and consumers) are connected over a heterogeneous network, an adversary can launch a DoS/distributed DoS (DDoS) attack against various grid components including smart meters, communication links, electric utilities, and service providers.

For service provision, DoS/DDoS attacks are of serious concern for two main reasons [10]. First, if the attack is successful, electricity supply can be stopped, the consequence of which would be extraordinarily disruptive. Second, the attacks are fundamentally more difficult to defend against or repel since they may take place outside the target. Compared to other areas, service provision in smart grids is more vulnerable to DoS/DDoS attacks due to the addition of service providers. More important, most existing DoS/DDoS defending techniques are inapplicable in service provisions. For example, one existing approach requires the attacked system to marshal the aid of other legitimate systems (i.e., service providers in this article) in the operational community and impose filters to discard the attacking traffic closer to its point of origin. However, service providers may not be willing to cooperate because they often belong to different owners.

For service provision, DoS/DDoS attacks are of serious concern for two main reasons. First, if the attack is successful, electricity supply can be stopped, the consequence of which will be extraordinarily disruptive. Second, the attacks are fundamentally more difficult to defend against or repel since they may take place outside the target.

Acknowledgment

This work was supported National Science Foundation of China (Grant No. 61070155), Program for New Century Excellent Talents in University (NCET-09-0685), the Fundamental Research Funds for the Central Universities (2012FZA5017), projects 217006/E20 funded by the Research Council of Norway, the European Commission FP7 Project EVANS (grant no. 2010-269323), and a grant from the Research Grants Council of the Hong Kong SAR, China (Project No. CityU 111208).

References

[1] NISTNIST, "Framework and Roadmap for Smart Grid Interoperability Standards," Release 1.0, NIST Special Publication 1108, Jan. 2010

[2] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy Mag.*, vol. 7, no. 3, May/June 2009, pp. 75–77.

[3] Y. Mo *et al.*, "Cyber-Physical Security of A Smart Grid Infrastructure," *Proc. IEEE*, vol. 100, no. 1, Jan. 2012, pp. 195–209.

[4] M. Humphrey, M. R. Thompson, and K. R. Jackson, "Security for Grids," *Proc. IEEE*, vol. 93, no. 3, Mar. 2005, pp. 644–52.

[5] P. Mithila, *Security and Privacy in Demand Response Systems in Smart Grid*, Master's thesis; http://csus-dspace.calstate.edu/xmlui/handle/10211.9/874, accessed May 28, 2012.

[6] T. J. Liu, W. Stirling, and H. O. Marcy, "Get Smart," *IEEE Power Energy Mag.*, vol. 8, no. 3, May/June 2010, pp. 66–78.

[7] H. K.-H. So *et al.*, "Zero-Configuration Identity-based Signcryption Scheme for Smart Grid," *Proc. IEEE SmartGridComm*, 2010, pp. 321–26.

[8] J. Naruchitparames, M. H. Gunes, and C. Y. Evrenosoglu, "Secure Communications in the Smart Grid," *Proc. IEEE CCNC*, 2011, pp. 1171–75.

[9] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," *Proc. Crypto '04*, 2004.

[10] S. D. Crocker, "Protecting the Internet from Distributed Denial-of-Service Attacks: A Proposal," *Proc. IEEE*, vol. 92, no. 9, Sept. 2004, pp. 1375–81.

Biographies

DAOJING HE (hedaojinghit@gmail.com) received his B.Eng. and M.Eng. degrees in computer science from Harbin Institute of Technology in 2007 and 2009, respectively. He is currently a Ph.D. student in the Department of Computer Science at Zhejiang University, P.R. China. His research interests include network and systems security. He is a Technical Program Committee member of many international conferences.

CHUN CHEN received a Bachelor's degree in mathematics from Xiamen University, China, in 1981, and Master's and Ph.D. degrees in computer science from Zhejiang University, China, in 1984 and 1990, respectively. He is a professor in the College of Computer Science and director of the Institute of Computer Software at Zhejiang University. His research activity is in image processing, computer vision, and embedded systems.

SAMMY CHAN received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994, he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994, he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

YAN ZHANG received a Ph.D. degree from Nanyang Technological University, Singapore. He is working with Simula Research Laboratory, Norway; and he is an adjunct associate professor at the University of Oslo, Norway. He is an associate editor or guest editor of a number of international journals. He serves as organizing committee chair for many international conferences. His research interests include resource, mobility, spectrum, energy, and data management in communication networks.

JIAJUN BU received B.S. and Ph.D. degrees in computer science from Zhejiang University, China, in 1995 and 2000, respectively. He is a professor in the College of Computer Science and deputy director of the Institute of Computer Software at Zhejiang University. His research interests include embedded systems, mobile multimedia, and data mining.

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] is currently a professor and associate vice president for Graduate Studies at Qatar University. He was chair of the CS Department at Western Michigan University from 2002 to 2006 and chair of the CS Department at the University of West Florida from 1999 to 2002. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. He received his B.S. (with distinction) and M.S. degrees in electrical engineering; M.S. and Ph.D. degrees in computer engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, New York. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial boards of six technical journals and is the founder and Editor-in-Chief of *Wireless Communications and Mobile Computing Journal* published by Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is also the founder and Steering Committee Chair of the annual International Conference of Wireless Communications and Mobile Computing (IWCMC). He is the author of seven books and more than 270 publications in refereed journals and conferences. He has guest edited a number of special issues in IEEE journals and magazines. He has also served as member, Chair, and General Chair of a number of conferences. He served as Chair of the IEEE Communications Society Wireless Technical Committee (WTC) and the TAOS Technical Committee. He was an IEEE Computer Society Distinguished Lecturer from 2003 to 2005. He is a Senior Member of ACM.