Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges

Xu Li, Inria Lille — Nord Europe
Xiaohui Liang, Rongxing Lu, and Xuemin (Sherman) Shen, University of Waterloo
Xiaodong Lin, University of Ontario Institute of Technology
Haojin Zhu, Shanghai Jiao Tong University

ABSTRACT

Smart grid has emerged as the next-generation power grid via the convergence of power system engineering and information and communication technology. In this article, we describe smart grid goals and tactics, and present a three-layer smart grid network architecture. Following a brief discussion about major challenges in smart grid development, we elaborate on smart grid cyber security issues. We define a taxonomy of basic cyber attacks, upon which sophisticated attack behaviors may be built. We then introduce fundamental security techniques, whose integration is essential for achieving full protection against existing and future sophisticated security attacks. By discussing some interesting open problems, we finally expect to trigger more research efforts in this emerging area.

INTRODUCTION

The August 2003 electrical blackout in North America affected over 100 power plants, paralyzed tens of millions of people's lives, and led to a $10 billion social cost. Investigations revealed that the failure was due to load imbalance in the electric power grid and lack of effective real-time diagnosis, among others. The function of the power grid is to deliver electricity from power plants to customers. Because electricity cannot be stored easily, load must be matched by the supply and transmission capacity of the grid. While swift advances in science and technology are triggering radical innovations in many fields, today's power grid is still grounded on a design more than 100 years old. It is composed of two parts: high-voltage transmission grid and medium-low-voltage distribution grid. The former is responsible for moving electricity from power plants to substations; the latter delivers electricity from substations to customers in local regions. The grid management system is an island of automation, implemented over closed dedicated networks running proprietary protocols. It contains a group of control centers. Each control center manages a regional grid spanning several substations, and has direct connections to the devices in the regional grid. The control center queries these substations about the grid operation status in turn; based on the collected information, it then adjusts power supply to meet the demands, and detects and responds to weaknesses or failures by instructing the control devices to take proper actions. Control centers collaborate to make decisions covering multiple regional grids.

With ubiquitous adoption of electronic devices and complex patterns of electricity usage, which were both hard to imagine in the past, the traditional power grid is undoubtedly outdated and does not meet our present growing demand for continuous stable electricity distribution. Specifically, its centralized management involves massive data exchanges and causes large data latency, and cannot satisfy the requirement for real-time monitoring and control; its one-way electricity distribution channels prevent the grid from accommodating customer-owned renewable power sources to improve power efficiency. In the recent decade, ever-increasing efforts on the development of next-generation power grid, known as *smart grid*, have been made in many countries. Under government-imposed open access policies, smart grid intends to combine the traditional isolated power system and public networks, and allows remote access by a wide variety of users. By having a communication and control layer, smart grid will enable local data processing, decentralized control, two-way electricity transmission, and reliability-efficiency-driven response. As summarized in Table 1, the ultimate goal of smart grid is to provide improved reliability (e.g., real-time diagnosis, self-healing, self-activating, automated outage management), efficiency (e.g., accommodation of future alternative, renewable power sources, active management of electric vehicle charging, cost-effective power generation, transmission, and distribution), and security (physical and cyber) [1]. Figure 1 presents an overall picture of smart grid.

Notably, as a part of the design consideration, smart grid will automate reliable power dis-

0163-6804/12/$25.00 © 2012 IEEE

tribution by engaging and empowering customers in utility management in addition to adopting advanced control and optimization mechanisms. It will expose customers' fine-grained electricity use information to utilities through the key elements, smart meters. Utilities are consequently able to apply different prices for power consumption based on the time of day and the season. They may even interfere with customers' power usage by pre-installed control switches in order to help flatten demand peaks. Consumers are allowed to access their own real-time use information through web services. In order to lower their own energy costs and enjoy uninterrupted activities, they are (hopefully) willing to use energy-efficient appliances and tend to shift power use from peak hours to non-peak hours.

Goal	Tactics
Reliability	Automated real-time monitoring and control of equipments; smart metering and dynamic pricing.
Efficiency	Accommodation of alternative power sources and smart appliances; active management of electric vehicle charging; optimized power generation, transmission and distribution
SecuritY	Improved monitoring; improved reliability; access control; authentication; privacy preservation; intrusion detection

Table 1. *Smart grid goals and tactics.*

Smart Grid Network Architecture

Smart grid network is the necessary communication platform for monitoring and controlling the grid operation. By generalizing previous proposals, e.g. [2–4], we present a hierarchical smart grid network structure including three layers, i.e. a residential network layer, a community network layer, and a regional network layer, as illustrated in Fig. 2.

At the bottom layer are *residential networks*, each corresponding to a distinct customer. A residential network has a star-like topology, composed of a smart meter at the center and a few control switches (if any exist) at the periphery. As the interface of the network, the smart meter provides real-time raw metering data to the control center at the top layer, and detailed energy usage and cost information to the customer. It also accepts control commands from the upper layers to connect/disconnect particular appliances (through pre-installed control switches) for load balancing purposes.

At the middle layer are *community networks*. A community network connects the residential networks, intelligent electric devices (IEDs), and remote terminal units (RTUs) in a neighborhood together. Data storage devices may additionally be included in the network to support networked storage, local fault diagnosis, and distributed decision making. There is a communication gateway in each community network. It manages the communication among the network elements, performs data aggregation, and bridges the bottom and top layers to allow data exchange. An example of a community network is the network in a smart community [5].

At the top layer are *regional networks*. A regional network connects the community networks, power plants, renewable power sources, substations, feeders, and other grid devices in a geographic region. Dedicated hub nodes may be deployed in the network to build a multiple-hop overlay structure for efficient and reliable data communication. A control center is implemented in each regional network. It provides supervisory control and data acquisition (SCADA) functionalities in the regional grid: collecting electricity usage data and grid operation status, detecting and responding to anomalies, and optimizing power generation, transmission, and distribution.

In the above presented architecture, each network is realized by high-speed wired or wireless links or a combination thereof, and runs IP-based communication protocols. Supporting IP allows devices with different physical details to

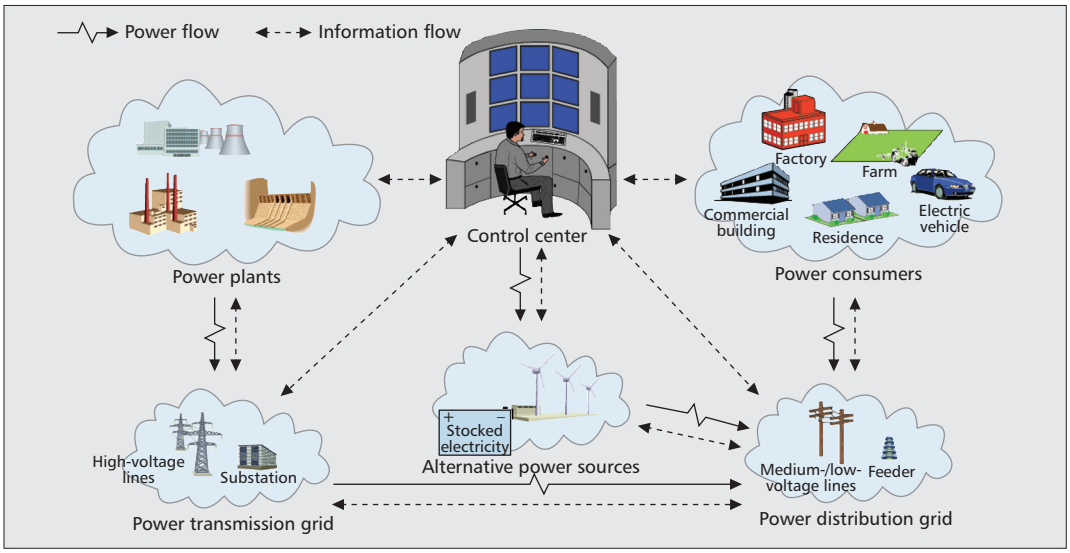

Figure 1. *An overall picture of smart grid.*

Through the Internet connections, customers may access their own electricity use and cost information, utilities may obtain electricity usage information at different granularities, and control centers may share data and coordinate to make inter-regional decisions.

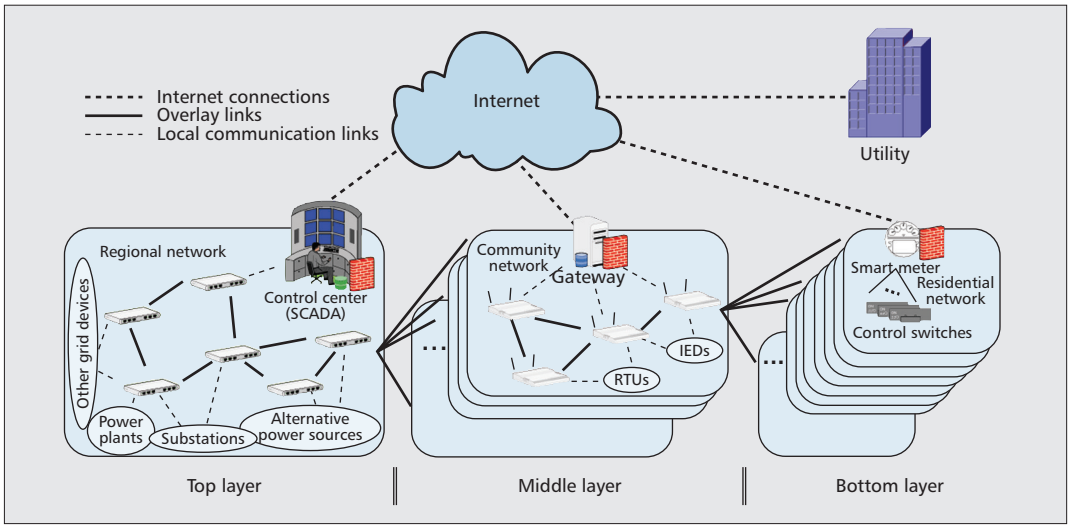

Figure 2. *Smart grid network architecture with a single regional network.*

be effortlessly integrated and managed in a unified way. Furthermore, control centers, community gateways, and smart meters are connected to the Internet. Through the Internet connections, customers may access their own electricity use and cost information, utilities may obtain electricity usage information at different granularities, and control centers may share data and coordinate to make interregional decisions.

Security Challenges in Smart Grid

With the elaborate smart grid architecture and composition as well as real-time grid operation status information, control centers may easily ensure power efficiency by applying optimization techniques to find the best power generation, transmission, and delivery strategies with respect to given constraints. In smart grid development, major challenges lie in the delivery of reliability and security.

Conventional power grid employs dedicated power devices, which are usually integrated with control and communication functionalities, and uses closed networks composed of reliable, predictable serial communication links. In contrast, smart grid will decouple the communication and control functionalities from power devices, and be modularized from the expendability and maintenance perspectives. Its components will largely be commercial off-the-shelf products from different companies that may have unknown incompatibilities, and adopt broadband communications and IP-like technologies which are error-prone and have nondeterministic behaviors. This transformation inevitably decreases *system operation reliability*. Faults caused by component incompatibility and communication failure will occur. In order to reduce greenhouse gas emissions, renewable but unstable power generation by, for example, photovoltaic cells and wind turbines will be accommodated in smart grid. Besides, to flatten load in the grid, power may be stocked during off-peak time and released, possibly at a different location, in peak time. These distributed power sources will cause reverse power flows and voltage variations in the grid, resulting in more severe *power distribution reliability* issues. Solving these reliability issues requires realization of wide-area measurement and control as well as improvement of real-time communication, diagnosis, and response mechanisms.

Since smart grid is a combination of the power grid and a communication network, security attacks may take place in both the physical space, as in the conventional power grid, and cyber space as in any communication network. A power device is traditionally located at a protected place (e.g,. substation) and controlled through physical contact or following proprietary protocols via dedicated wired communication links. In smart grid, a power device is often microprocessor-based and running public protocols, the specifications of which can be obtained readily (e.g., from the Internet) by anyone interested. Also, it may have a human-machine interface and very likely support wireless connection for easy access. The increased openness conveniences adversaries and brings additional security vulnerabilities to the grid. In conventional power grid, there is normally only one access point to the grid management system in a neighborhood. In smart grid, smart meters are massively deployed as access points, one per customer, in order to engage customers in utility management. They are connected to the Internet for ease of management. These access points are ideal portals for intrusions and malicious attacks. As computer communications is extensively used in the grid for implementing advanced monitoring and control, the grid becomes increasingly like a computer network, and as a result, all kinds of cyber attacks present in computer networks will have their analogs in smart grid, with the purpose of jeopardizing the grid system.

To conquer the above reliability and security challenges and realize the ambitious vision of smart grid, innovative research is expected in all aspects of smart grid, from high-level architecture design to low-level implementation detail.

In the sequel, we focus our attention on smart grid cyber attacks. We present an attack taxonomy, and discuss how to resist these attacks and enable secure smart grid communication.

Smart Grid Cyber Attacks

We present a taxonomy of basic cyber attacks in smart grid communication. In this taxonomy, there are four types of attacks: device attack, data attack, privacy attack, and network availability attack. These attacks are listed in Table 2. They have different objectives and are often the building blocks of more sophisticated attacks.

A *device attack* aims to compromise (control) a grid device. It is often the initial step of a sophisticated attack, in which the compromised device will be used to launch further attacks such as data attacks and network availability attacks toward the smart grid or perform malicious physical actuation (if the device is a control element). For example, a compromised IED such as a circuit breaker may break a circuit maliciously and cause power outage. Another example is that a compromised grid device might abruptly increase load to cause circuit overflow [6]. To resist device attacks, strict access control is necessary.

A *data attack* attempts to adversarially insert, alter, or delete data or control commands in the network traffic so as to mislead the smart grid to make wrong decisions/actions. One commonly observed data attack is that a customer jeopardizes the smart meter in order to reduce its electricity bill. Another example is that a compromised RTU is informed about a fault detected by a faulted circuit indicator (FCI) device, but it refuses to report the fault to the control center, resulting in increased outage time. To resist this attack, data integrity and authenticity must be protected, and effective intrusion detection mechanisms ought to be developed.

A *privacy attack* aims to learn/infer users' private information by analyzing electricity usage data. In smart grid, electricity usage information is collected multiple times per hour by smart meters so as to obtain fine-grained information about the grid status and improve grid operation efficiency. The detailed information may easily reveal customers' physical activities [7]. For example, in a residential setting, lack of electricity use for stove and microwave during a certain time period indicates that the home is not occupied. Using this information, physical attacks like robbery can be planned when nobody is at home. Clearly, such privacy-sensitive information must be protected from unauthorized access.

A *network availability attack* takes place in the form of denial of service (DoS). Its objectives are to use up or overwhelm the communication and computational resources of the smart grid, resulting in delay or failure of data communications. For example, an adversary may flood a control center with false information at very high frequency such that the control center spends most of the time verifying the authenticity of the information and is not able to timely respond to legitimate network traffic. Communication and control in smart grid are time critical. A delay of a few seconds may cause irreparable damage to the national economy and homeland security. A network availability attack must be handled effectively.

Name	Description
Device attack	It aims to compromise (control) a grid device. It is often the initial step of a sophisticated attack.
Data attack	It attempts to adversarially insert, alter or delete data in the network traffic so as to mislead smart grid to take wrong decisions.
Privacy attack	It aims to learn/infer users' private information by analyzing electricity usage data.
Network availability attack	It aims to use up or overwhelm the communication and computational resources of smart grid and to result in delay or failure of communication.

Table 2. *A taxonomy of basic cyber attacks in smart grid.*

Smart Grid Security Fundamentals

We now present the fundamental security techniques for defending the above basic cyber attacks in smart grid communication networks. These techniques are to be used in combination to provide full protection against existing or future sophisticated malicious attacks.

Access Control

In smart grid, typical system roles include operators, engineers, technicians, managers, and so on, and by regulation these roles have different access privileges to grid devices and system functionalities. Using role-based access control (RBAC) can obviously increase the system reliability and eliminate potential security threats. Existing RBAC schemes are designed for a single security domain (e.g., a regional network) and do not meet requirements of secure operations across multiple domains (e.g., interconnected regional networks). Cheung *et al.* [8] proposed an RBAC model specially tailored for smart grid, known as smart-grid role-based access control (SRAC). According to this model, the control center of each regional network maintains the security policy for all inside community networks and residential networks, and acts as an interface to communicate with outside users from other regional networks. Role hierarchy and role constraints are predefined in accordance with the real-life role relations and limitations. Some particular requirements are taken into consideration. For example, a role in a community network may take on some tasks belonging to another community network; a user may be assigned multiple roles, while conflict of interest of the roles must be prevented; the trust relationship between users of a home regional network and those of a foreign regional network is required for establishing a foreign-user network access policy. An XML-based security policy managing method was suggested, with respect

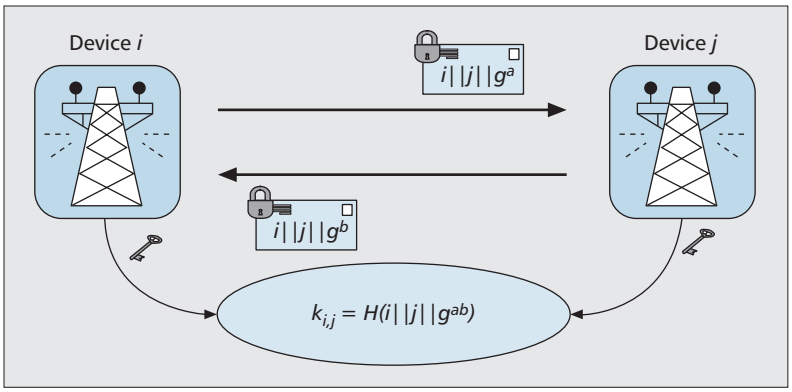

Figure 3. *Two-step mutual authentication [9].*

to syntax for elements and privilege assignment, syntax for foreign-interfacing role, and foreign-interfacing role assignment, for simplifying smart grid network security administrations. Through a case study, Cheung *et al.* showed that the proposed SRAC model is effective.

Authentication

The reliability and security of smart grid are subject to the integrity and authenticity of devices and data traffic in the grid. Device authentication is normally the first step of a data communication session, and its result is often a shared session key for encrypting and authenticating subsequent data packets and ensuring data integrity. Because of the delay-sensitive and traffic-intensive nature of smart grid communication, an authentication scheme should involve minimal message exchange between grid devices. Fouda *et al.* [9] proposed a lightweight two-step mutual authentication protocol by combining the public key encryption scheme and Diffie-Hellman key agreement scheme. Consider two arbitrary communicating grid devices i and j, as shown in Fig. 3. At the first step, i encrypts $i||j||g^a$ with j's public key (a is a random number), and sends the ciphertext to j. At the second step, j decrypts the received ciphertext and responds to i with a newly generated ciphertext on $i||j||g^b$ using i's public key (b is a random number). After these two steps, both devices i and j can calculate $g^{ab} = (g^a)b = (g^b)a$, and derive the shared session key as $k_{i,j} = H(i||j||\text{gab})$, where H: $\{0,1\}^* \rightarrow \mathbb{Z}_q^*$ is a publicly known hash function. Both of them are able to identify each other since the secrets g^a and g^b can be accessed only by each other. Because random numbers a and b are deleted after the generation of $k_{i,j}$, the compromise of either i's or j's long-term private keys does not affect the security of the previous session keys. Forward secrecy of the scheme is guaranteed, and economic and privacy loss due to compromised nodes can be largely reduced as a result.

Li and Cao [10] considered that in smart grid field devices often have limited storage space, and addressed the authentication problem from a storage load minimization perspective. They devised a new variant of the one-time signature (OTS) scheme. In traditional OTS [11], a device has a secret key $(s_1, s_2, \cdots, s_t)$ and the corresponding public key $(v_1, v_2, \cdots, v_t)$, where $v_i = f(s_i)$ and f is a one-way function. With a message m as input, the device calculates the hash value of m: $h = H(m) = h_1||h_2||\cdots||h_k$ in which each h_j is a $\log_2 t$-bit substring of $H(m)$ and interpreted as an integer $1 \le i_j \le t$. The device's signature on m is computed as $(s_{i1}, s_{i2}, \cdots, s_{ik})$. The security of this signature comes from the difficulty of finding such a message m' that all h_i' appearing in $H(m') = h_1'||h_2'||\cdots||h_k'$ has been used in previous signatures. Li and Cao extended this traditional scheme by applying a hash chain. For $1 \le i \le$ t, the device computes $f^{w+1}(s_i)$ corresponding to the secret key s_i and the public key, with $s_i \rightarrow f(s_i) \rightarrow \cdots \rightarrow f^{w+1}(s_i)$. After calculating all the i_js, it sorts them in decreasing order. If an i_j appears in the kth position in the sorted sequence, it will replace s_{ij} with $f^{w+1-k}(s_{ij})$ in the signature. The security level of the traditional OTS scheme is improved since a forgery attack has to generate such m' that the substrings in $H(m')$ follow a restricted order. For example, in the traditional OTS scheme if $H(m) = h_1|h_2|h_3$ is generated and a forgery attack finds $H(m') = h_2|h_1|h_3$, the forgery attack can succeed; whereas in the new variant, m' has to satisfy $H(m') = h_1|h_2|h_3$ in order for the attack to succeed. Analysis showed that under the same security level, the new OTS variant reduces the signature size by 40 percent and the storage load on receiver by a factor of 8.

Privacy Preservation

There are two types of metering data in smart grid communication, transmitted at a low frequency and a high frequency [12]. The low-frequency data contains a periodic power use summary, coarse enough not to cause privacy leakage. It may be sent to community gateways and then obtained by utilities for accounting and billing purposes. The high-frequency data contains specific power usage patterns and is destined to regional control centers for fine-grained real-time control and optimization. It is related to users' private lives and must be protected from utilities. According to this classification, Efthymiou and Kalogridis [12] proposed to assign each smart meter two IDs, one for low-frequency data transmission (LFID) and the other for high-frequency data transmission (HFID). The former is considered as a pseudonymous ID and open to utilities. The objective of privacy preservation is therefore to hide the link between high-frequency metering data and smart meters' HFIDs. A trusted third party, known as *escrow*, is assumed to be connected to the smart grid network. It knows the connection of a valid (HFID, LFID) pair, and assigns two public/private key pairs to each smart meter, corresponding to the HFID and LFID of the smart meter. As privacy can be protected by end-to-end encryption, Efthymiou and Kalogridis focused on the initial device registration process when a smart meter joins the smart grid. Registration is necessary for the grid and utilities to recognize and accept the readings of legislated smart meters. The idea is to register each smart meter through two separate steps. At the first step, the smart meter informs the utility about its LFID and the LFID public key, which in turn passes them to the proper community gateway. At the second step, the smart meter sends its HFID and HFID public key to the escrow, and the

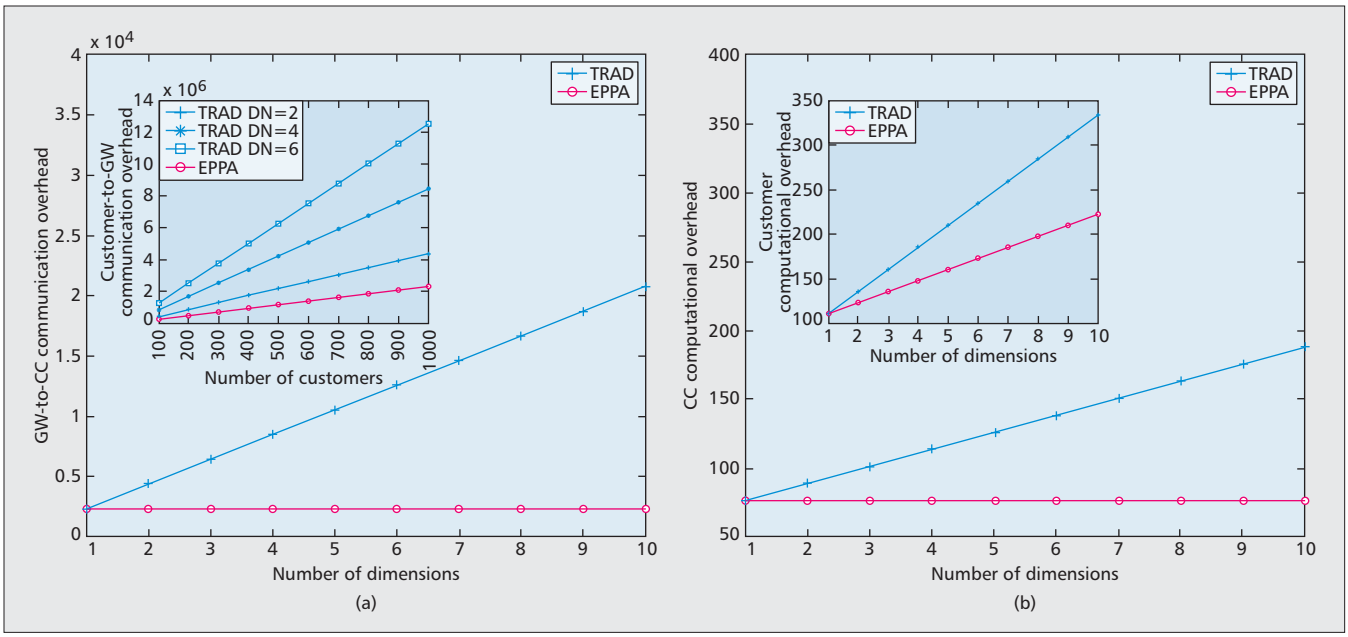

Figure 4. *Performance comparison: EPPA [13] vs. TARD. GW stands for community gateway; CC for control center. Communication overhead is measured in bits; computational overhead is measured by time in milliseconds.*

escrow forwards them to the control center. A random time interval is suggested between the two steps for breaking the correlation. Since the utility is not involved in the second step, the HFID remains unknown to the utility.

For simplicity, in the following we refer to high-frequency metering data (containing electricity usage patterns) as metering data. In [13], we noticed that metering data is often small in size, smaller than the plain text space of the encryption algorithm used. Each time when the data is encrypted, its size is increased to occupy the entire plain text space. As such information is transmitted by a massive number of smart meters, a large portion of the communication bandwidth is wasted, and transmission delay is increased as a result. Since in a regional network, smart metering data flows to the control center through community gateways, we reasonably suggested that community gateways aggregate received raw smart metering data and forward them in an integrated compact form to the control center. Each smart meter encrypts its readings using a secret key shared with the control center. Community gateways are not be able to access the content of metering data. To enable community gateways to perform data aggregation in this case, we further suggested that smart meters apply a homomorphic encryption technique. In this technique, a specific linear algebraic manipulation toward the plaintext is equivalent to another one conducted on the ciphertext. This unique feature allows community gateways to perform summation and multiplication based aggregation on received metering data without decrypting them.

Existing homomorphic encryption based data aggregation schemes consider one-dimensional data only. In smart grid, metering data is however multi-dimensional, for example, including the amount of energy consumed, and in which time period and for what purpose the consumption was, and so on. When multiple dimensions are present, these schemes will have to process every dimension separately and impose overwhelming processing load on smart meters and control centers, becoming less efficient in communication and in time. Under these circumstances, we proposed a novel Efficient and Privacy-Preserving Aggregation (EPPA) scheme [13] for smart grid communication based on homomorphic Paillier cryptosystem [14]. This scheme processes all the dimension data as a whole rather than separately, thus saving both computational overhead and communication cost, reducing data latency and improving real-time response capability. Below, we briefly describe EPPA and present its performance in comparison with the traditional scheme (referred to as TRAD) where no data aggregation is engaged. Detailed algorithm design and performance evaluation can be found in [13].

Assume that smart metering data has l dimensions. The control center obtains a public key (n, g) and a private key (λ, μ) using the input security parameters. According to the security parameters and the public key, it selects a proper super increasing sequence $\vec{a} = (a_1, a_2, \cdots, a_l)$ contains l primes. Further, it computes a sequence $\vec{g} = (g_1, g_2, \cdots, g_l)$, where $g_i = g^{a_i}$. It publishes $(n, \vec{g})$ and some other necessary information to smart meters, while keeping $(\lambda, \mu, \vec{a})$ and the other remaining information secretly. A smart meter i obtains $(n, \vec{g})$ by registering itself with the smart grid. Each time when it transmits a piece of l-dimensional metering data $\vec{d}_i = (d_{i1}, d_{i2}, \cdots, d_{il})$, it encrypts $\vec{d}_i$ into to a piece of one-dimensional cyphertext and transmits the cyphertext. During the encryption, it computes $C_i = (r_i^n \prod_{j=1}^{l} d_{ij}^{g_j}) \bmod n^2$ as the cyphertext, where r_i is a random integer.The cyphertext is delivered to the gateway of the community network that the smart meter belongs to. Let w represent the number of smart meters in the community network. The community gateway performs data

Each IDS module has two components: a classifier (for attack classification) and a recorder (for logging and accuracy evaluation). As in convention, either machine learning techniques or artificial immune systems may be applied for realizing the classifier.

aggregation on received cyphertext $\{C_1, C_2, \cdots, C_w\}$ as $C = (\prod_{i=1}^{w} C_i) \bmod n^2$. It forwards C to the control center. At the control center, the aggregated cypher text C is decrypted with the private key (λ, μ) to obtain a mixture data $M = (\sum_{j=1}^{l} a_i \sum_{i=1}^{w} d_{ij}) \bmod n$. Through simple calculus, the control center easily recovers each original piece of metering data $\vec{d}_j$ from M. Figure 4 shows that EPPA indeed has significantly less overhead than TRAD.

Intrusion Detection

The above security techniques are for smart grid to defend against attacks launched by an adversary outside the grid. If the adversary attacks the grid through some compromised devices, these techniques will lose their effectiveness. Intrusion detection mechanisms are necessary for identifying compromised devices. While existing network intrusion detection techniques may be applied to the smart grid network directly or with minor modification, below we introduce a generic IDS (intrusion detection system) framework and a DoS attack (i.e. network availability attack) detection technique, both designed particularly for smart grid communications.

Zhang *et al.* [2] proposed a hierarchical IDS framework, where an IDS module is installed distributedly along the network hierarchy, that is, on control centers, community gateways and smart meters, as shown in Fig. 2. The IDS module at the bottom layer accepts raw input from smart meters; the module at a higher layer accepts input only from the IDS module at the immediate lower layer. If an attack is detected by an IDS module, an alarm will be invoked at the corresponding layer. If a detection decision cannot be made at certain layer, it will be left for the upper layer to make, since the upper layer has a wider scope of knowledge. Each IDS module has two components: a classifier (for attack classification) and a recorder (for logging and accuracy evaluation). As in convention, either machine learning techniques or artificial immune systems may be applied for realizing the classifier. Zhang *et al.* suggested to apply Support Vector Machine or clonal selection to build the classifier. In either case, the classifier needs to be trained before put in use. Considering the difference of attacks likely happening at different layers, the training data will have a different concentration of attack types at each layer for a tradeoff of accuracy and time.

Authentication is performed between grid devices to ensure authenticity. It is a computation-intensive procedure generating noticeable delay and can become the target of DoS attack. Fadlullah *et al.* [3] proposed a predication based DoS attack defense mechanism. They assumed that some compromised grid devices launch DoS attack distributedly by frequently sending false data or authentication requests along the network hierarchy. Unusual activities such as device failures and authentication failures are monitored at every layer and reported to the control center. The control center models each malicious event as a Gaussian process, realized by a collection of random variables representing event features such as number of defective devices, malicious authentication ratio, and so on. It uses the collected reports as observations to form the prior beliefs of the Gaussian process. Using the prior beliefs and observations, it computes the posterior probability distributions of the Gaussian process through Gaussian process regression. The optimal parameters of the Gaussian process are obtained by maximizing the log likelihood of the training data with respect to the parameters. Then it is able to predict whether a DoS attack is going to happen, and to send early warning and instructions to the respective device so that the later can take appropriate actions (e.g. drop the data or authentication request) in advance to mitigate the forthcoming DoS attack.

Conclusions and Future Directions

In this article, we have studied the smart grid network architecture and discussed major challenges in smart grid development. We have also addressed the basic cyber attack behaviors in smart grid and offered several fundamental approaches to resist these behaviors. Below, we conclude the article by discussing several open problems and possible solutions, in accordance with the fundamental security techniques introduced previously. Our objective is to shed more light on the smart grid security and privacy issues and to trigger more research efforts along this emerging research line.

The role-based access control scheme [8] requires a pre-defined fixed role hierarchy. From flexibility and sustainability points of view, it is desirable to allow automatic access control policy generation to allow dynamic role addition and removal. One possible solution is to apply attribute-based, rather than role-based, access control. In such scheme, there is a pre-defined universal attribute sets, and each attribute is associate with certain access privileges. A social role is assigned with a number of attributes such that it obtains the corresponding access privileges. By combining attributes in different ways, different roles and therefore different access policies are created on the fly.

The authentication schemes [9, 10] both adopt public key cryptography without specifying how public keys are managed. Public key infrastructure (PKI) is a classic public key management system, where users obtain certificates (including public keys) from pre-defined certificate authorities (CAs) and CAs form a hierarchical structure. When PKI is used, each grid device obtains a certificate from a local CA. Two devices belonging to the same regional network may have certificates issued by different CAs and do not recognize each other's certificate. In this case, they have to consult with the common ancestor of the two CAs in the PKI hierarchy, leading to increased authentication delay. Fast authentication is an open problem. One possible solution is to use a cryptographic technique, known as re-signature. This technique enables two CAs to together initialize a computing device in the regional network, which can quickly translate a certificate issued by one of them to a certificate issued by the other.

For the sake of privacy preservation, each smart meter transmits two types of data, privacy-sensitive raw metering data (to the control center) and privacy-insensitive metering data summary (to the utility), both going through community gateways [12, 13]. Since summary data can be computed from raw data, its transmission is redundant. It is an interesting open problem to enable a community gateway to compute the summary without knowing the content of the raw data, and generate the result that is accessible by the utility. Solutions will reduce smart grid communication overhead, shorten data latency, and eventually improve smart grid reliability.

Compromised grid devices are severe security threats to the smart grid operation. They are to be detected by the installed intrusion detection systems [2, 3]. However, normal devices may behave selfishly and damage the grid operation as well. For example, customer-owned renewable power sources may suddenly stop providing electricity for its own benefit and lead to voltage variations in the grid. Detecting selfish renewable power sources is a unique problem in smart grid, and warrants deep investigation. One possible solution is to apply trust management for those devices, with respect to their power generation capabilities and constraints as well as their actual behaviors, and avoid using the devices with low trust ratings.

Acknowledgments

This research was partially supported by National Natural Science Foundation of China (Grant No. 61003218, 70971086.)

References

[1] H. Khurana *et al.*, "Smart-Grid Security Issues," *IEEE Security & Privacy*, vol. 8, no. 1, 2010, pp. 81–85.
[2] Y. Zhang *et al.*, "Distributed Intrusion Detection System in A Multi-Layer Network Architecture of Smart Grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2011, pp. 796–808.
[3] Z. M. Fadlullah *et al.*, "An Early Warning System against Malicious Activities for Smart Grid Communications," *IEEE Network*, vol. 25, no. 5, 2011, pp. 50–55.
[4] Y.-J. Kim *et al.*, "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid," *IEEE Commun. Mag.*, vol. 48, no. 11, 2010, pp. 58–65.
[5] X. Li *et al.*, "Smart Community: An Internet of Things Application," *IEEE Commun. Mag.*, vol. 49, no. 11, 2011, pp. 68–75.
[6] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2011, pp. 667–74.
[7] F.G. Marmol *et al.*, "Do Not Snoop My Habits: Preserving Privacy in the Smart Grid," *IEEE Commun. Mag.*, vol. 50, no. 5, 2012, pp. 166–72.
[8] H. Cheung *et al.*, "Role-based Model Security Access Control for Smart Power-Grids Computer Networks," *Proc. IEEE PESGM*, 2008, pp. 1–7.
[9] M. Fouda *et al.*, "A Light-Weight Message Authentication Scheme for Smart Grid Communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2011, pp. 675–85.
[10] Q. Li and G. Cao, "Multicast Authentication in the Smart Grid With One-Time Signature," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2011, pp. 686–96.
[11] L. Reyzin and N. Reyzin, "Better Than BiBa: Short One-Time Signatures with Fast Signing and Verifying," *Proc. ACISP*, 2002, pp. 144–53.
[12] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *Proc. SmartGridComm*, 2010, pp. 238–43.
[13] R. Lu *et al.*, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Trans. Parallel and Distributed Systems*, to appear.
[14] P. Paillier, "Public-Key Cryptosystems based on Composite Degree Residuosity Classes," *Proc. EUROCRYPT*, 1999, pp. 223–38.
[15] D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, 2011, pp. 375–81.

Biographies

Xu Li (xu.li@inria.fr) received a Ph.D. (2008) degree from Carleton University, Canada, an M.Sc. (2005) degree from the University of Ottawa, Canada, and a B.Sc. (1998) degree from Jilin University, China, all in computer science. Prior to joining Inria, France, as a research scientist, he held postdoctoral fellow positions at the University of Waterloo, Canada, Inria/CNRS, France, and the University of Ottawa, Canada. He is on the editorial boards of the Wiley *Transactions on Emerging Telecommunications Technologies*, *Ad Hoc & Sensor Wireless Networks*, and *Parallel and Distributed Computing and Networks*. He is/was a guest editor of a few journal special issues. His current research focuses on machine-to-machine communications and mobile social networks, along with over 50 different works published in refereed journals, conference proceedings, and books.

Xiaohui Liang [S'10] (x27liang@bbcr.uwaterloo.ca) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo. He is a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include security and privacy for e-healthcare systems and mobile social networks.

Rongxing Lu [S'09, M'11] (rxlu@bbcr.uwaterloo.ca) received a Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006 and a Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2012. He is currently a postdoctoral fellow with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xiaodong Lin [S'07, M'09, SM'12] (xiaodong.lin@uoit.ca) received a Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, China, in 1998 and a Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

Haojin Zhu [M'09] (zhu-hj@sjtu.edu.cn) received his B.Sc. degree (2002) from Wuhan University, China, his M.Sc. degree (2005) from Shanghai Jiao Tong University, China, both in computer science, and his Ph.D. in electrical and computer engineering from the University of Waterloo in 2009. He is currently an associate professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His current research interests include wireless network security and distributed system security. He received the SMC-Young Research Award (Rank B), Shanghai Jiao Tong University, November 2011. He was a co-recipient of best paper awards of IEEE ICC 2007 — Computer and Communications Security Symposium and Chinacom 2008 — Wireless Communication Symposium. He serves on the technical program committees for many international conferences such as INFOCOM, ICCCN, GLOBECOM, ICC, and WCNC.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] (xshen@bbcr.uwaterloo.ca) received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He is currently serving as an Editor-in-Chief for *IEEE Network*, *Peer-to-Peer Networks and Applications*, and *IET Communications*. He is a Fellow of Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.

It is an interesting open problem to enable a community gateway to compute the summary without knowing the content of the raw data, and generate the result that is accessible by the utility. Solutions will reduce smart grid communication overhead, shorten data latency, and eventually improve smart grid reliability.