Chapter 2
Background and Models

Abstract This chapter contextualizes the role of smart meters in smart grid initiatives around the world to show that the smart grid concept goes beyond energy supplier modernization. In addition, this chapter presents the security model and the privacy model for Privacy-Preserving Protocols (PPPs). Security is ensured by means of cryptography, and privacy is protected by aggregation of encrypted measurements.

Keywords Initiatives • Concept • Security • Privacy • Aggregation • Maps • Cryptography • Aggregation

2.1 Smart Grids Around the World

On the Internet, one can find many projects and governmental sites about smart grids. Smart Metering Projects Map in Google Maps[1] provides a good visualization of the number and distribution of smart grid initiatives around the world. Figure 2.1 shows a screen-shot of the map.[2] In addition, Fig. 2.2 gives us a zoomed-in view of smart grid initiatives in the European Union (EU). A triangle indicates a trial or pilot, and a circle indicates a project. The colors red, green, and blue represent initiatives for electricity, gas, and water, respectively. Red is the dominant color, thus indicating that the majority of the initiatives are directed to electricity. The initiatives are also classified as automatic meter reading (AMR), advanced metering infrastructure (AMI), and smart grid. The first aims mainly to collect measurements and send them to suppliers. The second aims to transform the metering systems into microcomputers connected in networks. The third aims to use additional technologies. The AMI is the new terminology and goes beyond AMR. In terms of technology, the idea of AMR is old [8]. However, it was renewed with the AMI, which integrates new features like remote control and two-way communication [6].

[1] http://maps.google.com/maps/ms?ie=UTF8&oe=UTF8&msa=0&msid=115519311058367534348.0000011362ac6d7d21187.

[2] On January 1, 2015.

F. Borges de Oliveira, *On Privacy-Preserving Protocols for Smart Metering Systems*,
DOI 10.1007/978-3-319-40718-0_2

Fig. 2.1 Smart Metering Projects Map—Google Maps

Fig. 2.2 Smart Metering Projects Map in EU—Google Maps

A smart grid can have even more than AMI, for instance, phasor measurement units (PMUs), distributed generation, and smart inverters. Information about interesting features of smart inverters can be found in [5].

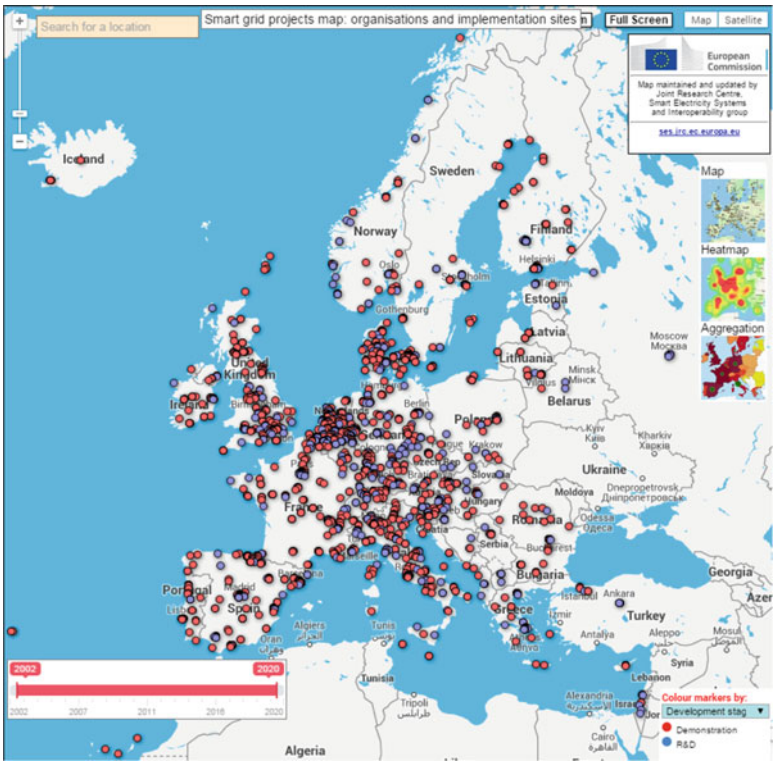

Fig. 2.3 Official Smart Metering Project Map in EU

Currently, many initiatives are taken to create smart grids. The EU aims to install smart meters in 80 % of households by 2020.[3] Figure 2.3 shows a screen-shot[4] of the official map[5] generated by European Commission's in-house science service. The map is interactive and can show information about initiatives associated with the EU outside of Europe, for instance, in the America. The EU also aims to reach at least 80 % reduction of greenhouse gas emission by 2050 in comparison with 1990 levels.[6] A survey of regulations in the EU electricity market may be found in [11]. This chapter does not present political regulation in depth because of its ephemeral nature. In particular, countries need to adapt their laws for modern smart metering systems. Particularly, Germany has made efforts to increase substantially the share of renewable and private energy production. Such efforts are known as *Energiewende*.

[3]Directive 2012/27/EU of 25 October 2012 published on the Official Journal L No.315, 25 Oct 2012.

[4]On January 1, 2015.

[5]http://ses.jrc.ec.europa.eu/.

[6]Energy roadmap 2050—EU—doi:10.2833/10759.

Fig. 2.4 Official Smart Metering Project Map in USA

The German Federal Office for Security in Information Technology, the free translation of Bundesamt für Sicherheit in der Informationstechnik (BSI), has defined that smart meter gateway has a secure module and may control many metering devices of different commodities in a neighborhood. Indeed, it controls the communication and centralizes the intelligence. To ensure security and privacy, the smart meter gateway has a secure module, like a Trusted Platform Module (TPM), and aggregates the measurements from many metering devices to ensure privacy, cf. Sect. 2.2.3. In addition, the prescription of the German BSI *Schutzprofil* for smart meters mitigates the risks by means of very restrictive legal measures.

The Department of Energy (DOE) of the United States of America (USA) also presents a map of investments in smart grids. Figure 2.4 shows a screen-shot of the official map[7] generated by the DOE.[8] In the USA, smart grid is a term applied to the power grid modernization due to its aging. Electrification is recognized as the greatest achievement of impact on quality of life and as uniquely critical system [7].

In contrast to the BSI model that can work with multiple commodities, the National Institute of Standards and Technology (NIST) has focused its standards on smart grid scenarios for energy suppliers. The NIST Framework and Roadmap for Smart Grid Interoperability Standards[9] presents a conceptual reference model to describe the interaction between the information network and the electric power network. In this standard, seven domains are defined as below.

Customers are the electricity consumers in the power network who may also be small generators for some periods.
Markets are parties involved in the electricity markets.

[7] On January 1, 2015.

[8] https://www.smartgrid.gov/recovery_act/project_information.

[9] NIST Special Publication 1108R2.

Service Providers are the organizations that provide services to customers and suppliers.
Operations is a domain in which actors manage the electric flow.
Bulk Generation is the set of large-scale electricity generators.
Transmission indicates the corporations responsible for the transmission of electricity in high voltage from distant power plants to distribution networks.
Distribution indicates the corporations responsible for distributing the electricity between the customers in the distribution power network.

NIST is one of the pioneers in smart grid privacy issues. In 2010, the guideline for Privacy and the Smart Grid[10] drew attention to the fact that the energy supplier can identify when customers turned on and turned off their appliances. The USA have made strong investment in smart meters and aim to have almost 52 million customers equipped with smart meters by 2015 [4]. In 2012,[11] suppliers in USA already had more than 43 million smart meters installed.

2.2 Security and Privacy Models

Security and privacy models for smart grid scenarios require the definition of some terminology. A PPP should have a usual secure model, but its privacy model goes further than the secure model. In fact, this section goes from the basis of the security to lay down the bases for a privacy model.

2.2.1 Terminology in PPPs

This book uses some specific terms as listed below. Others may be found in the Glossary at the end of this book or at the beginning in List of Acronyms, List of Abbreviations, or List of Symbols.

User is an abstraction of a customer with a smart meter running a PPP with a supplier. The user may buy or sell a commodity.
Supplier is an abstraction of bulk generator, transmission, distribution, operations, markets, and service providers.
Meter is an abbreviation of smart meter, which lies in a customer's property. Its function is to collect measurements from a commodity flow and to report them through an information network to a supplier. Meters can communicate in many ways, e.g., using wireless, power line communication, or Internet Protocol (IP).

[10] NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid.
[11] http://www.eia.gov/tools/faqs/faq.cfm?id=108&t=3.

Round (or round of measurement) is a period in which a supplier receives the encrypted measurements from every meter i. Normally, the meters considered in one round belong to the same neighborhood. The measurements are collected in a fixed interval or by a request of the supplier.

Measurement is the measured consumption or generation in watts collected by a meter i in the round j, and it is denoted as $m_{i,j}$. Normally, the interval between rounds is assumed to be short.

Consolidated consumption is the sum of the measurements $m_{i,j}$ in the round j, and it is denoted as c_j. Thus, c_j is the total of energy consumption or generation reported by all meters during one round j to their supplier, i.e.,

$$c_j \stackrel{\text{def.}}{=} \sum_{i=1}^{\tilde{\imath}} m_{i,j},$$

where $\tilde{\imath}$ is the number of meters in the aggregation.

Bill is a monetary consumption value of an invoice with respect to the electricity consumption or generation in a period, and it is denoted by $b_i^{\$}$, i.e.,

$$b_i^{\$} \stackrel{\text{def.}}{=} \sum_{j=1}^{\tilde{\jmath}} \text{Value}\left(m_{i,j}\right),$$

where $\tilde{\jmath}$ is the number of rounds until the billing process and $\text{Value}\left(m_{i,j}\right)$ is a function that transforms the measurements from watts into a monetary value with a price that floats over the time. Thus, the electricity has a time-based pricing.

Billed consumption is the balance of the consumption and generation in watts registered in the invoice of the meter i. This balance is denoted as b_i and given by

$$b_i \stackrel{\text{def.}}{=} \sum_{j=1}^{\tilde{\jmath}} m_{i,j}.$$

Note that the measurements can be positive or negative depending on whether there is consumption or generation. In addition, the time-based pricing might be different in buying or selling. Normally, the measurements $m_{i,j}$ are in watts, but they may also be in monetary units, if the meter i knows the current unit price.

2.2.2 Security Model

This section presents Shannon's security model [10] re-written in the context of smart grids. In this model, the meter i encrypts its measurement $m_{i,j}$, computes

$$\mathfrak{M}_{i,j} = \mathsf{Enc}\left(m_{i,j}\right),$$

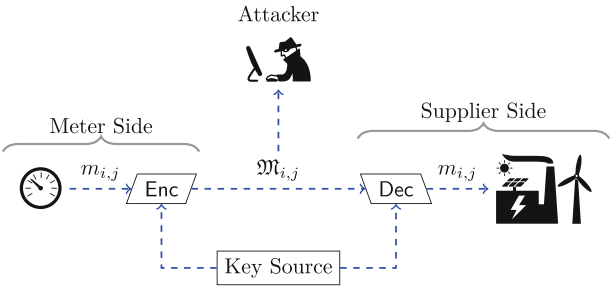

Fig. 2.5 Shannon's security model in the context of smart grids

and sends the encrypted measurement $\mathfrak{M}_{i,j}$ to the supplier, which decrypts as

$$m_{i,j} = \mathsf{Dec}\left(\mathfrak{M}_{i,j}\right).$$

The security model is composed of attack model and trust model. The former defines the capabilities assumed for the attackers. The latter defines the trust relationship between meters and their supplier with the corresponding changes to the attack model.

2.2.2.1 Attack Model

The attacker is very limited and can access only the encrypted measurement $\mathfrak{M}_{i,j}$. Note that there is no difference if the cryptographic scheme is either symmetric or asymmetric. However, Shannon's security model was created 27 years before the introduction of asymmetric cryptography [3]. Figure 2.5 depicts the attack model.

In this model, the attacker knows how the functions Enc and Dec work. The model does not allow hiding these functions, because security through obscurity is considered harmful. Hence, the attacker only does not know the keys and the measurement $m_{i,j}$. The security lies in the keys, which can be generated to create certificates with security and privacy without trusted third party (TTP) [1]. This work does not consider side-channel attack, fault attack, etc. A secure source generates the keys, used as input for the encryption and decryption functions. This source is not a TTP but a function or protocol as given in [1].

2.2.2.2 Trust Model

Usually, the meter i and its supplier are considered trusted. Thus, the meter measures the consumption correctly, computes Enc correctly, signs the result correctly, and sends the signed encrypted measurement directly to its supplier. The communication channel transmits the message without interruption and the supplier computes Dec correctly. There is no collusion.

Even with all these restrictions in the trust model, the attacker could infer information about the consumption if the encrypted measurements had a bijection with the measurements. The attacker could infer the encrypted measurement of zero watts and deduce when the customer is at home. To avoid such attack, the cryptographic function should be probabilistic.

2.2.2.3 Considerations About the Cryptographic Functions

In contrast to the well-known cryptographic functions that have the same encrypted measurement for the same measurement, we also have probabilistic encryption schemes that enable different encrypted measurements $\mathfrak{M}_{i,j}$ for the same measurement $m_{i,j}$. This is possible because probabilistic encryption schemes are based on additional parameters chosen by the meter. Such parameters are not necessary for the decryption function. Paillier cryptosystem [9] is an example of probabilistic encryption. In fact, if the meter i has the key k and a secret r, the encryption function should be written as

$$\mathfrak{M}_{i,j} = \mathsf{Enc}_{k,r}(m_{i,j}),$$

and the decryption function depends on the key $\bar{k}$ associated with k, thus the decryption function should be written as

$$m_{i,j} = \mathsf{Dec}_{\bar{k}}(\mathfrak{M}_{i,j}).$$

Moreover, if we have two secrets r_1 and r_2 such that $r_1 \neq r_2$, then

$$\mathsf{Enc}_{k,r_1}(m_{i,j}) \neq \mathsf{Enc}_{k,r_2}(m_{i,j}).$$

However,

$$\mathsf{Dec}_{\bar{k}}\left(\mathsf{Enc}_{k,r_1}(m_{i,j}) \odot \mathsf{Enc}_{k,r_2}(m_{i,j})\right) = m_{i,j} \oplus m_{i,j} = 2m_{i,j}, \tag{2.1}$$

for all $m_{i,j}$. Section 6.4.1 uses this property to show that additive homomorphic encryption primitives (AHEPs) are particular cases of Asymmetric DC-Nets (ADC-Nets). Note that the functions form a bijection between two groups. Equation (2.1) denotes the operation over the measurements $m_{i,j}$ and the encrypted measurements $\mathfrak{M}_{i,j}$ as $\oplus$ and $\odot$, respectively. Note that encryption and decryption functions of probabilistic encryption schemes are usually presented without the keys neither the random number.

According to Shannon's terminology, the encrypted measurement is called ciphertext and the measurement is called message. In this work, message has different concepts. Message may refer to other packets sent in the information network.

Once the security is ensured in a system, we can go to the next challenge.

2.2.3 Privacy Model

Ensuring privacy is more complicated than ensuring security. The privacy model works under the assumption that the security model and its components are robust, i.e., if a security assumption fails, privacy is impaired.

The privacy model can be constructed using two strategies, namely: pseudonyms and data aggregation. The latter is adopted in this book and is more efficient for smart grids than the former, cf. Sect. 3.1.2 or [2]. The former requires that the measurements are associated with pseudonyms and sent through an anonymity network. Note that pseudonyms should be randomly chosen and unlinkable with each other. In particular, cryptographically secure pseudorandom number generators (CSPRNGs) are already computationally expensive. The latter relies on the idea of a ballot box. In other words, each meter i encrypts its measurement $m_{i,j}$ and somehow the encrypted measurements $\mathfrak{M}_{i,j}$ from all meters i in the round j are aggregated generating an encrypted consolidated consumption $\mathfrak{C}_j$, s.t.

$$\mathfrak{C}_j = \prod_{i=1}^{\tilde{\imath}} \mathfrak{M}_{i,j} = \prod_{i=1}^{\tilde{\imath}} \mathsf{Enc}\left(m_{i,j}\right).$$

After the aggregation, the supplier decrypts the encrypted consolidated consumption resulting in the consolidated consumption c_j, s.t.

$$c_j = \mathsf{Dec}\left(\mathfrak{C}_j\right) = \sum_{i=1}^{\tilde{\imath}} m_{i,j}.$$

2.2.3.1 Attack Model

The attacker is more powerful in a privacy attack model than in a security attack model. The attacker has access to the encrypted consolidated consumptions $\mathfrak{C}_j$ and all information on the supplier side, including the cryptographic key to decrypt them. The key source is still secure and distributes the keys to the meters and the supplier, which can decrypt only the encrypted consolidated consumption $\mathfrak{C}_j$ or even an individual measurement $m_{i,j}$, depending on the PPP used and if the supplier receives such measurement. Since AHEPs enable the decryption of a single measurement $m_{i,j}$, the attacker cannot have access to an individual encrypted measurement $\mathfrak{M}_{i,j}$, if the PPP is based on an AHEP. Figure 2.6 depicts a model for privacy and its data aggregation in the context of smart grids. Figure 2.6 does not have edges indicating the bill $b_i^{\$}$. The supplier already knows $b_i^{\$}$ for each meter i in a non-smart grid. More information about bills is presented further.

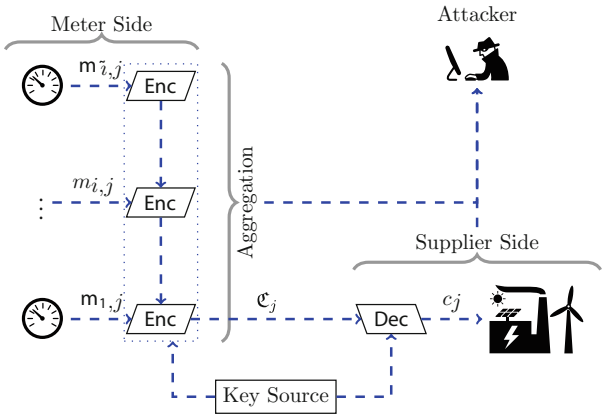

Fig. 2.6 Privacy model in the context of smart grids

2.2.3.2 Trust Model

In privacy trust models, we can define meters as trusted, honest-but-curious, or malicious. The first definition requires that meters behave correctly. This is a strong assumption, because machines might fail. The second requires that meters also behave correctly, but it will collect accessible information. In the honest-but-curious model, the attacker has no access to the communication channel during the aggregation process. However, it is clear that access to encrypted measurements $\mathfrak{M}_{i,j}$ should be denied for PPPs based on AHEPs. The third requires that meters might behave as an attacker. This is a safe, secure, and weak assumption, because factual or intentional failures can happen in real life. Parallel with these definitions, we could define meters as non-attackers, passive attackers, and active attackers, respectively.

For the privacy trust model, the supplier is malicious. This is a safe assumption for customers and even for the supplier, which do not need blindly to trust the employees.

Trusted meters measure the consumption correctly, compute Enc correctly, sign the result correctly, and send the signed encrypted measurements directly to their supplier. They do everything correctly.

Honest-but-curious also known as semi-honest meters behave like trusted meters, but they read information in the aggregation, if possible.

Malicious meters can fail to measure the correct consumption, can compute Enc wrongly, sign the result wrongly and send the signed encrypted measurements to their supplier and an attacker. The communication channel can transmit the messages with noise and interruption, and the supplier can compute Dec wrongly. Collusion is considered. Thus, an attacker has more information.

In contrast to previous work, this work presents PPPs taking in consideration that the meters might be malicious. Moreover, each meter and its supplier can verify the bill $b_i^{\$}$.

References

1. F. Borges, L.A. Martucci, M. Mühlhäuser, Analysis of privacy-enhancing protocols based on anonymity networks, in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)* (2012), pp. 378–383. doi:10.1109/SmartGridComm.2012.6486013
2. F. Borges et al., Secure and privacy-friendly public key generation and certification, in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (2014), pp. 114–121. doi:10.1109/TrustCom.2014.19
3. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inform. Theory **22**(6), 644–654 (1976). issn:0018-9448. doi:10.1109/TIT.1976.1055638
4. P. Fox-Penner, *Smart Power: Climate Change, the Smart Grid, and the Future of Electric Utilities* (Island Press, Washington, DC, 2010). isbn:9781597268097
5. F. Katiraei, C. Sun, B. Enayati, No inverter left behind: protection, controls, and testing for high penetrations of pv inverters on distribution systems. IEEE Power Energ. Mag. **13**(2), 43–49 (2015). issn:1540-7977. doi:10.1109/MPE.2014.2380374
6. S. Li, K. Choi, K. Chae, An enhanced measurement transmission scheme for privacy protection in smart grid, in *2013 International Conference on Information Networking (ICOIN)* (2013), pp. 18–23. doi:10.1109/ICOIN.2013.6496345
7. D. Novosel, V. Rabl, J. Nelson, A report to the U.S. DOE: IEEE shares its insights on priority issues [leader's corner]. IEEE Power Energ. Mag. **13**(2), 6–12 (2015). issn:1540–7977. doi:10.1109/MPE.2014.2374971
8. T.G. Paraskevakos, *Sensor monitoring device*. US Patent 3,842,208 (1974). http://www.google.com/patents/US3842208
9. P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in *Advances in Cryptology - EUROCRYPT 1999*, vol. 1592. Lecture Notes in Computer Science (Springer, Berlin, 1999), pp. 223–238. isbn:978-3-540-65889-4
10. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949). issn:0005-8580. doi:10.1002/j.1538-7305.1949.tb00928.x
11. J. Vasconcelos, Survey of regulatory and technological developments concerning smart metering in the European Union electricity market (2008). issn:1830-1541. http://hdl.handle.net/1814/9267

http://www.springer.com/978-3-319-40717-3

On Privacy-Preserving Protocols for Smart Metering Systems
Security and Privacy in Smart Grids
Borges de Oliveira, F.
2017, XXVII, 143 p. 41 illus., 37 illus. in color., Hardcover
ISBN: 978-3-319-40717-3