Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 32 (2014) 1087 – 1094

Procedia Computer Science

International Workshop on Recent Advances on Machine-to-Machine Communication (RAMCOM 2014)

Smart Metering privacy-preserving techniques in a nutshell

Hajer Souri[1,3*], Amine Dhraief[3], Syrine Tlili[3], Khalil Drira[1,2], Abdelfettah Belghith[3]

[1] *CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France*
[2] *Univ de Toulouse, INSA, F-31400 Toulouse, France*
[3] *HANA Group Lab., Univ de Manouba, Manouba, Tunisie*

Abstract

The legacy power grid has several limitations resulting in misuse and mismanagement of energy. The evolution of IT technologies have empowered revolutionizing the power grid and created the concept of the Smart Grid. Hence, the Smart Grid is considered as the integration of the latest information, communication and operational technologies with the traditional power grid in order to enhance energy management within a reliable, efficient network linking the diffirent grid actors from the consumer to the end-head system such as energy providers and billing services. Introducing new technologies into Smart Grid raises new issues, mainly security issues. Therefore, in this paper, after presenting the Smart Grid and the smart metering system, we present the security requirements of the Smart Grid and we highlight the user privacy concern as well as the different techniques proposed in literature to deal with it. Our main objective is to provide a study of the existing techniques preventing privacy disclosure.

Keywords: Smart Grid, AMI, security, privacy, Aggregation

1. Introduction

Providing energy to residential and industrial areas is among the most important requirements of modern society. Therefore,the energy management cycle must be carefully and accurately planned. Traditionally, manual meters are used to read consumption and are consulted periodically by special agents in order to perform billing. Such an inaccurate operation may lead to different errors and misuse of energy, in addition to the inconvenience for inhabitants. Therefore, it is useful to introduce smart meters which are able to communicate appropriately their consumption information to involved parties. The deployment of a smart metering system is beneficial to the whole power grid as it represents an important factor for energy management optimization.

Combining new technologies with the legacy power grid may introduce new challenges regarding its security. Mainly, it is assumed that once revealed smart meter readings may disclose private information about customers' daily life and habits. Recently, in Australia and Canada, a rapidly growing movement has been opposing the installation

* Corresponding author. Tel.: +216 23 659 417.
E-mail address: hajer.souri@hanalab.org

doi:10.1016/j.procs.2014.05.537

of new sophisticated meters. Smart meter opponents have chosen to retain their old analogic ones despite utilities' intimidation tactics. The disclosure of their own privacy is topping their concerns. Therefore, it is highly required to investigate in how to preserve the customer's own privacy while taking advantage from the use of new technologies in the power grid. Few research works have been launched in this context aiming to conceive efficient privacy-preserving protocols that fit with the Smart Grid features.

In this paper, we firstly give an overview of the Smart Grid and its different domains. Then, we compare the Smart Grid to the Internet as it is a potential network on which we could build the smart grid. We, also, briefly present the smart metering system. After that, we move to introducing the Smart Grid security requirements. A special focus is given to privacy in the Smart Grid. We identify the effect of revealing smart meter readings on the user's privacy. And then we present few techniques dealing with privacy-preserving requirement.

2. An overview of Smart Grid

The smart grid is the modernized version of the electrical grid. It uses the recent information, telecommunication and operational technologies to improve and optimize the traditional power grid. Smart Grid has several objectives. Mainly, it opts for automating and optimizing the operations of the electrical grid, in particular, energy transmission and distribution, data collection, billing, etc. Besides, via the adoption of flexible tariff policies, the accuracy of meters readings, the reliability, transparency and real-time delivery of messages, it aims to reduce the consumption costs and to optimize the management of energy. Self-healing capabilities is also an important requirement to be guaranteed in Smart Grid.

2.1. The Smart Grid domains

According to NIST[1], the Smart Grid involves seven different blocks called domains which are bulk generation, transmission, distribution, operation, market, customer, and service provider (Fig.1).

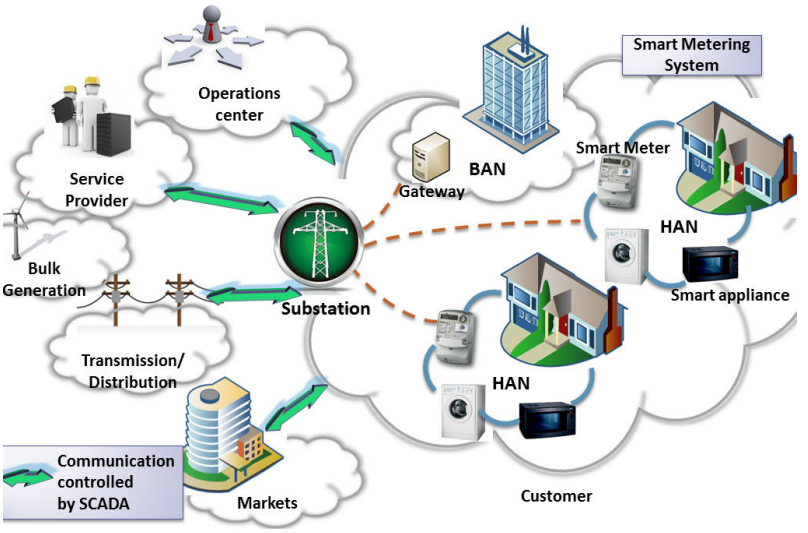

Fig. 1. Smart Grid domains

- Bulk generation: This domain is responsible for the generation of electricity in bulk. Generated electricity could be immediately distributed or stored for later distribution. Electricity resources could be either non-renewable

[1] National Institute of Standards and Technology

(like oil and coal) or renewable (like water, wind, sunlight, etc.). The bulk generation domain is connected to different other domains such as transmission and market domains.
- Transmission: Electricity is transmitted to the distribution domain via multiple substations and transmission lines.
- Distribution: This domain is responsible of delivering energy to the consumer domain according to user demands and energy availability.
- Operation: In this domain, the movement of electricity is managed in order to ensure an optimal and efficient transmission and distribution of electricity.
- Market: In this domain it is about balancing between the supply and the demand. Actually, this domain may contain different actors: electricity is provided by suppliers to traders who resell it to retailers who in turn distribute it to the consumers.
- Customer: The consumer is the end user of the energy; it could be either home (Home Area Network; HAN) or an entire building (Building Area Network; BAN), a private, commercial or industrial user. In addition to consuming energy, an end user could also store and generate energy via home installed equipments such as photovoltaic cells. The customer domain is also referred a smart metering system or also Advanced Metering Infrastructure (AMI). End users communicate with the different domains in order to reveal their consumption details, to perform billing and to forecast future consumption. Communication between this domain and the other domains is usuallly controlled by SCADA [1], a technology of monitoring and controlling large processes.
- Service provider: Services such as billing, system control, energy management, account management, etc. are provided by the service provider domain. It interacts with the different other domains in order to ensure the smooth management of the Smart Grid.

2.2. Smart Grid vs. Internet

In order to eventually establish future cooperation between Smart Grid and Internet, it is important to evaluate the different similarities and differences in term of requirements in both networks. Obviously, both structures are complex and hierarchical, yet, in term of requirements, both networks are fundamentally different. In fact, in the case of internet, what matters the most regarding performance is to guarantee high throughput and fairness between users [2]. However, when it comes to Smart Grid, it is about guaranteeing a secure, reliable and real time delivery of messages while the real time monitoring and management of the system is not required. Regarding traffic, the Internet usually provides best effort traffic with about 100 ms of delay required for delay-sensitive traffic such as VoP traffic. On the other side, in the Smart Grid, traffic flows are mostly periodic transmitting consumption related data between end users and utilities. Besides, its time requirements are more stringent as some kinds of messages delivery is constrained by 3 ms delay. As for the communication pattern, it is commonly known that Internet adopts the end-to-end model of communication while the Smart Grid supports a two-way communication model bottom-up (from meter to utilities) and top-down (from utilities to meter) and possibly peer-to-peer model in customer local networks. And unlike the Internet that uses the IP protocol suite for communication, the Smart Grid needs more sophisticated protocols guaranteeing mainly the low energy and low data rate requirements such as the IEEE 802.15.4g for the PHY layer [3].

Certainly, the Internet offers solutions enabling large-scale network deployment. The Smart Grid as one of these networks could be an eventual exploiter for Internet but some features must be revisited regarding time, security and law data rate/low energy requirements. Such requirements could be highlighted when focusing more on the customer domain: the smart metering system. In the next section we give an overview about the smart metering system features.

2.3. The Smart Metering System

The smart metering system, also called as the Advanced Metering Infrastructure (AMI), is the sensor network of the Smart Grid. Small and smart devices, gas, water and electricity meters, are installed in the end user side (residential and commercial buildings) in order to automatically sense and record accurate special data related to users energy consumption (energy consumption, time of use, etc.). Recorded data is then delivered to related utilities repeatedly (each minute, hour, billing period, etc.). Eventually, meters communicate their sensed measurements to a gateway

that gathers all the sensed data in the local area network and forward it to the outsider network. The local network bounded by the gateway is called Home/Building Area Network.

On the inside of this local network, the communication between the different devices is performed wirelessly for flexibility reasons. The smart devices used in the local network are battery-powered and have low computational capabilities, therefore this wireless communication should meet the requirements of low energy and low data-rate.

Such a system stands for automating fine-grained readings enabling the adoption of fine-grained and dynamic time-based pricing schemes. Thereby, the smart metering system is a crucial factor for the power grid management allowing the consumer to be more active and aware in the management of the energy consumption and able to take better-informed decisions when planning its use of energy.

2.4. Security requirements in Smart Grid

Providing secure and reliable delivery of messages is considered of high priority in the Smart Grid. Hence, to ensure such a critical information exchange in this network, it is important first to define the security requirements of the Smart Grid[2].

Availability is among the main security requirements. Actually, it is important to ensure a constant and continuous correct functioning in the Smart Grid by preventing any delay in delivering messages and any system disruption that may causes failure in delivering energy. Besides, access to and use of information have to be reliably and timely ensured.

Integrity is considered as another security requirement of high importance. In fact, any malicious unauthorized modification of information may lead to incorrect billing operations or incorrect power management decisions.

Confidentiality, the last important security requirement to mention, requires that unauthorized access to proper information and its disclosure to third parties should be prevented. In this context, it is assumed that disclosing information such as daily energy consumption by illegitimate third parties invades the user personal privacy.

Privacy, among others, is topping user's concerns as it is inconvenient to let third parties keeping an eye on its daily life details. In the remaining of this paper, we focus on the privacy concerns, and the different techniques proposed in literature to preserve it from disclosure.

3. Privacy

3.1. Privacy concerns

It is important firstly to define the term privacy in Smart Grid. Overall, privacy in Smart Grid is keeping the power use information of users out of the reach of other third parties in order to prevent disclosing the user living profile.

In the smart metering system, smart meters are the key element responsible of two-way communication between the consumer and the utilities, allowing the exchange of data related to pricing as well as consumption related information. Due to its automated and fine-grained nature, The data issued from a smart meter may reveal a lot about the user activities and behaviour when exposed to sophisticated data mining techniques. Possible extracted information could be:

- Energy consumption details
- Number of people in the house
- Residents presence or absence in the house
- Daily schedule (showers/ watching TV/ sleeping patterns)
- Information about household equipment
- Movement pattern inside the home in case of smart homes

Fig.2 shows a day-long electrical power usage trace extracted from a smart meter. A simple and intuitive observation allows as to learn several information about a consumer day-long activity. From the high variation of the curve we can deduce human activity in the house, and linking time with variation make it possible to deduce what are the activities being performed by the end user. It is possible with data mining techniques and power signature analysis to

have more accurate information about its activities. Certainly, many end users won't tolerate under any circumstance the disclosure of theis living profile to any third party.

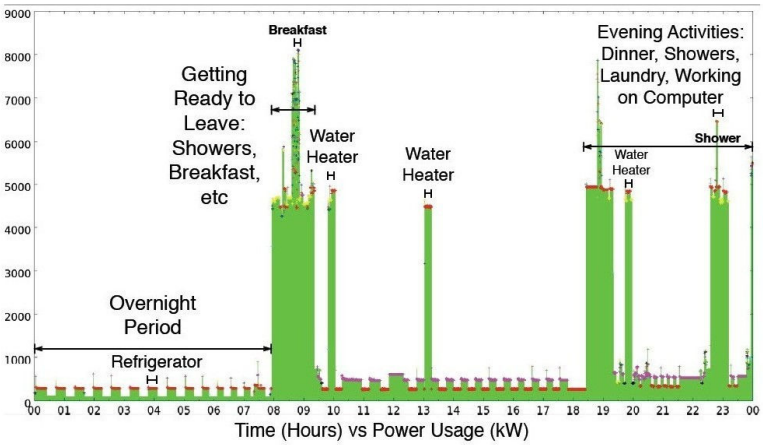

Fig. 2. Example of day-long power trace

Such behavioural information may interest different third parties such as social studies researchers as they can have an overview about people daily habits, security agents can use information for conducting criminal investigations or resolving legal disputes. It is also of high importance for criminals as they may pre-identify household items to steal as well as detect the absence of residents from home and then schedule their burglary. Therefore, it is of high importance to adopt powerful privacy preserving techniques to secure the smart metering system and protect the consumer daily life patterns from invasion.

3.2. Privacy preserving techniques: study and comparison

Many researchers have tackled the privacy issue and proposed different techniques to preserve the consumer privacy in the Smart Grid. Privacy preserving techniques could be divided into two categories; those using data aggregation and those without data aggregation. In Smart Grid, and to deal with the security issue, data aggregation is defined as gathering and computing data in order to preserve the anonymity of its origins. Aggregated data could be originated from different sensors, or it could be different readings from the same sensor. And in Smart Grid literature, such operation is usually computed in the gateway level and linked to other security techniques.

- Techniques with aggregation are usually locally centralized as we have a gateway that communicates with different smart meters before forwarding the aggregated data to the utilities. Besides, usually here the security logic is processed in the gateway level alleviating the smart meter from extra computational capabilities. But, the aggregator could be considered as a local single point of failure that may cause the disconnection of the local electric network if the aggregator fails.
- Techniques without aggregation are usually distributed, where smart meters communicates directly with the utilities. In this case, each smart meter is reinforced with extra computational capabilities allowing it to perform the security techniques on its side.

We have compared the studied approaches from a security perspective as well as computational costs perspective. We noticed that the aggregation techniques pose an availability concern as the aggregator represents a local single point of failure which may lead to a system disruption and failure in delivering messages and energy.

Most of the privacy preserving techniques may be affiliated under one of those two categories. In the remainder of this paper, we present several techniques of each category and then we draw two summary tables for comparison between them.

3.2.1. Privacy-preserving techniques using aggregation

Aggregation is often adopted in smart grid networks for different purposes; mainly to reduce the number of packets travelling between the AMI and utilities avoiding bandwidth exhaustion. But, in our study we are interested in the case where aggregation is used as a way of privacy preservation.

Several researches have coupled data aggregation with other privacy preserving techniques.In [4], authors assume that data issued from smart meters are multidimensional and could be classified into space related data and time related data. Therefore, they introduced the notions of space based aggregation and time based aggregation and then the Privacy-Preserving Nodes (PPNs) which play the role of aggregators collecting data from the different smart meters. In this work, data aggregation is used along with the Secret Sharing technique [5]. Secret Sharing is a cryptographic algorithm based on the idea of dividing a secret into shares that will be distributed among a group of parties. No one can reconstruct the secret unless it disposes of at least a defined number of shares. In this work, the meter readings are considered as secrets that will be divided and shared with different PPNs. PPNs perform homomorphic aggregation over received shares and then forward aggregated data to requesting consumers. The proposed architecture is locally distributed as aggregation is performed in different nodes which enable easy healing of the system in case of failure of nodes. Besides, the model is fault-tolerant as the initial shared information could be obtained even if some nodes which number is inferior to a certain threshold are compromised.

In [6], authors propose the use of Zero-Knowledge (ZK) proof protocols along with aggregation. Zero-Knowledge proofs allow one party to prove to another the correctness of a statement without revealing anything about the statement other than its veracity. Molina-Markham *et al.* used a zero-knowledge billing protocol allowing the smart meter to compute the bill and prove to the utility service that it is in conformity with the power consumption that remains unknown to it. A neighbourhood gateway periodically send an aggregated value of the neighbourhood consumption for future demand forecast and electricity generation planning. The proposed solution guarantees correct billing without unveiling customer energy consumption details to third parties. However, the technique is expensive in term of computational costs, it requires high computational capabilities to be granted to the Smart Meter.

Homomorphic cryptosystems also are widely used in security protocols mainly when using aggregation, especially because of their homomorphic additive and multiplicative proprieties *i.e.* the encryption scheme is additively homomorphic if the multiplication of cipher texts of n messages results in an encryption of the sum of these n messages. In [7], Lu *et al.* used the homomorphic Paillar system to encrypt communication between smart meter and utility center. Encrypted data is aggregated in intermediate aggregators that ignore the real value of the encrypted metering data. The solution proposed by Lu *et al.* could be considered as efficient in term of computational costs while guaranteeing that no third party would disclose the content of data travelling between the Smart Meter and the utility center. Security is provided in an end-to-end mode.

3.2.2. Privacy-preserving techniques without aggregation

When there is no gateway to aggregate data, we often resort to a third party that we consider as trustworthy. Such a trusted third party would be the only allowed party to identify the data origins and bind between them. Smart metering data are anonymized. In [8], authors differentiate between high and low frequency data and attribute an ID to each type; High Frequecy ID (HFID) and Low Frequecy ID (LFID). It is assumed that high frequency data could reveal different information about the end user when analysed with efficient techiques, mainly its life patterns and behaviour could be easily deduced. Therefore, they propose that such data, *i.e.* its HFID, should only be known by the trusted third party. However, low frequency data, *i.e.* data with LFID, could be known by all parties. Hence, data issued from smart meters keep anonymous to any untrusted parties including the utility center. To ensure the correctness of data, the connection between a valid HFID/LFID could be verified via the third trusted party.

In [9], authors use another technique to preserve the privacy of consumers in Smart Grid: the blind signature. The blind signature is a scheme that allows a person to get a message signed by another party without revealing any information about the message to the other party. Here, it is about blindly signing anonymous power credentials (authors used credential identities instead of user identity) used for daily power requests. Daily power consumption remains anonymous, user identity is only used at the end of each billing period when presenting all consumed credentials together.

In [10], the proposed technique aims to preserve the consumer's own privacy by the smart meter itself in the user side; the approach is referred to as user-centric privacy-preserving approach. The idea is that the only involved

communicating parties are the smart meter and the control center and they are the only ones that have the ability to get real reading values and match it to real identities. The control center is assumed to be fully trusted and secure. On the user side, the consumption messages are signed with Hash based MAC[2], assigned to pseudo-identities preventing intermediate substations to invade any meter related information. Then, messages are encrypted before being sent to the utility center.

The two tables below present a summary and a comparison of the approaches cited above. Tab. 1 verifies some security features while tab. 3.2.2 shows the evaluation of some performance metrics in each techniques.

Table 1. Security features of the privacy preserving techniques

Privacy preserving techniques comparison	Integrity	Confidentiality	Certification authority
Secret sharing [4]	Encryption	Encryption	No
ZK proof [6]	Encryption	Encryption	No
Homomorphic Cryptosystem [7]	BLS short signature [11]	end-to-end encryption	No
Third trusted party [8]	Timestamp, nonce, MAC, digital signature	Encryption, MAC	Yes
Blind signature [9]	Double encryption	Double encryption	No
User centric privacy [10]	Encryption, HMAC	Encryption	Yes

Table 2. Performance of the privacy preserving techniques

Privacy-preserving techniques comparison	Computational costs/delay	Overhead	Scalability
Secret sharing [4]	N/A	N/A	Yes
ZK proof [6]	Expensive costs	N/A	No (Smart Meter: prover, the company server: verifier)
Homomorphic Cryptosystem [7]	Not expensive	Low overhead	N/A
Third trusted party [8]	long setup time	N/A	N/A
Blind signature [9]	N/A	Depends on power usage	N/A
User centric privacy [10]	HAM signature verification delay: 368msec	20 bytes (8%)/ request message	N/A

4. Conclusion

Privacy in smart metering systems has been a serious concern to the different involved parties in the Smart Grid, mainly end-users. Special analysis of data issued from smart meters may reveal information about life patterns of users. Therefore, it is important to establish an efficient infrastructure that adopt security strategies guaranteeing the non disclosure of users private information.

In this paper, we first recalled some concepts related to Smart Grid such as domains and security requirements. Then we gave a special interest to the privacy concern and privacy-preserving techniques. we classified the privacy-preserving techniques into two categories on the basis of the use of aggregation: techniques using aggregation among others to provide privacy preservation and those that don't use aggregation between the end-users and utilities. For each category we presented three techniques along with their different features. Two drawn tables summed up different security and performance features of the privacy-preserving techniques.

[2] Message Authentication Code

It is worth mentioning that the existing research works, as asserted by the drawn tables, lack of in-depth performance evaluation of privacy-preserving protocols in terms of real implementation conditions. The Smart meters are devices of low computing capabilities, battery-powered and to be widely deployed. Hence, privacy preserving techniques should not exhaust meters ressources and capabilities and have to guarantee scalability of deployment. Related metrics should be carefully evaluated in order to guarantee the reliable and efficient functioning of smart meters.

References

1. Boyer, S.A.. *Scada: Supervisory Control And Data Acquisition*. USA: International Society of Automation; 4th ed.; 2009. ISBN 1936007096, 9781936007097.
2. Wang, W., Lu, Z.. Survey Cyber Security in the Smart Grid: Survey and Challenges. *Comput Netw* 2013;**57**(5):1344–1371. URL: http://dx.doi.org/10.1016/j.comnet.2012.12.017. doi:10.1016/j.comnet.2012.12.017.
3. Chang, K.H., Mason, B.. The ieee 802.15.4g standard for smart metering utility networks. In: *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. 2012, p. 476–480. doi:10.1109/SmartGridComm.2012.6486030.
4. Rottondi, C., Verticale, G., Capone, A.. Privacy-preserving smart metering with multiple data consumers. *Computer Networks* 2013;**57**(7):1699 – 1713. URL: http://www.sciencedirect.com/science/article/pii/S1389128613000364. doi:http://dx.doi.org/10.1016/j.comnet.2013.02.018.
5. Shamir, A.. How to share a secret. *Commun ACM* 1979;**22**(11):612–613. URL: http://doi.acm.org/10.1145/359168.359176. doi:10.1145/359168.359176.
6. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.. Private memoirs of a smart meter. In: *Proceedings of the 2Nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*; BuildSys '10. New York, NY, USA: ACM. ISBN 978-1-4503-0458-0; 2010, p. 61–66. URL: http://doi.acm.org/10.1145/1878431.1878446. doi:10.1145/1878431.1878446.
7. Lu, R., Liang, X., Li, X., Lin, X., Shen, X.S.. Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems* 2012;**23**(9):1621–1631. doi:http://doi.ieeecomputersociety.org/10.1109/TPDS.2012.86.
8. Efthymiou, C., Kalogridis, G.. Smart grid privacy via anonymization of smart metering data. In: *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. 2010, p. 238–243. doi:10.1109/SMARTGRID.2010.5622050.
9. Chim, T., Yiu, S., Hui, L.C.K., Li, V.K.. Privacy-preserving advance power reservation. *Communications Magazine, IEEE* 2012; **50**(8):18–23. doi:10.1109/MCOM.2012.6257522.
10. Chim, T., Yiu, S., Hui, L.C.K., Li, V.K.. Pass: Privacy-preserving authentication scheme for smart grid network. In: *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*. 2011, p. 196–201. doi:10.1109/SmartGridComm.2011.6102316.
11. Boneh, D., Lynn, B., Shacham, H.. Short signatures from the weil pairing. In: *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*; ASIACRYPT '01. London, UK, UK: Springer-Verlag. ISBN 3-540-42987-5; 2001, p. 514–532. URL: http://dl.acm.org/citation.cfm?id=647097.717005.