World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-3, Issue-2, August 2016 Pages 13-17

# Smart Meters - Keeping Users' Privacy

**Alves André Luiz ,Fonseca Keiko Veronica Ono**

***Abstract*—Electric power distribution systems are evolving toward more intelligent models allowing distribution organizations to have a perspective on how consumption is happening. However, these systems may allow for violation of consumer privacy, as they can identify the equipment in use, allowing for profiling of user activities. This work addresses the need to develop a mechanism to protect privacy, and presents an option for creating this protection for individual electric power consumer units through intermediate encryption of readings from these individual units, allowing suppliers access not to individual readings, but sum of their total.**

***Index Terms —smart grid; smart metering; homomorphic encryption; privacy***

## I. INTRODUCTION

Electric power generation, transportation and distribution systems have undergone, together with electric power consumption, changes in recent years due to the need to modernize the vast Power Grid (PG). According to [1], some 8% of all electric power produced is lost along transmission lines while another 20% of transmission and distribution capacity is destined for meeting demand at peak consumption, which comprises approximately 5% of the total transport time of this energy.

The evolution of the electric power system is called Smart Grid (SG) which, according to [2], is modern infrastructure applied throughout the electric power grid to improve efficiency, reliability and safety as well as smoothly integrate renewable and alternative energy sources through automated control and communication technology. According to [3], the SG is composed of a network of computers and powerful computers to monitor and manage the generation, transport, distribution and use of electric power.

The definition of Smart Grid according to the European regulatory council is "[...] an electricity network that can cost-efficiently integrate the behavior and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically-efficient, sustainable power systems with low losses and high levels of quality and security of supply and safety" [4]. According to the National Institute of Standards and Technology's conceptual model, the Smart Grid consists of seven domains: Mass Generation, Transmission, Distribution, Client, Markets, Service Providers and Operations. In order to interconnect all these domains, the communication network should be highly distributed and hierarchical, as affirmed by [5].

A system this size must have the capacity to automatically recuperate itself after a disturbance, provide energy without oscillations, failures or quality/reliability problems, should support alternative and renewable energy sources (solar, wind, tide, etc...) as well as maintain energy storage systems, have high monitoring standards and constant measurement throughout the entire system, while allowing users/consumers to take advantage of these features (see [6],[7],[8]and[9]).

If we follow these lines of thought, we can aim toward the possibility of suppliers being able to use information from periodical Smart Meter readings to control electric power demand.

The use of Smart Meters in electric power distribution systems gives rise to a new paradigm in the context of consumption analysis of consumer units, especially homes. The ease of measurement introduced by this system can, to a certain point, instantly determine consumption[1] at each consumer unit. However this places privacy into check, as it is possible to determine what happens inside each unit through analysis of the collected data. Electricity Suppliers (represented as ES in this paper) may need to obtain instant consumption for their demand control and planning.

The challenge of maintaining privacy while having access to this information on demand engenders some solutions. Given that the ES need information on demand for a group of consumer units as opposed to single units, the sum of the consumption will meet their needs. In this paper, we present a possible approach to address consumer unit privacy issues while meeting ES needs for demand. The solution is based on the work presented by [10].

## II. APPROACH

In [10], we are presented with a structure where Smart Meters (SM) communicate directly with ES as shown in Fig. 1, together with the mathematical calculations involved.

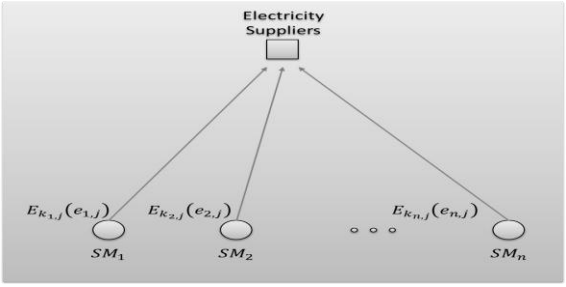


Fig.1: Basic approach – from [10]

[1] In this paper, "instant consumption" refers to consumption measured in small intervals of time like fractions of an hour.

**André Luiz Alves,** CPGEI - Engenharia Elétrica e Informática Industrial Universidade Federal Tecnológica do Paraná Curitiba, Brazil/.
**Keiko Veronica Ono Fonseca**, CPGEI - Engenharia Elétrica e Informática Industrial Universidade Federal Tecnológica do Paraná Curitiba, Brazil

The approach explained by [10] assumes that the ES will receive a reading $e_{ij}$ from the Smart Meter$SM_i$for a period jencrypted with a key$k_{ij}$. This key is encrypted and used only once and renewed for each reading received by the ES, which is unable to decipher the message but will be able to decrypt the sum of specific group's measurements. This is made possible by the process described below.

We used two graphic symbols here; the first $\oplus$, is used to denote a addition operation on simple texts, in this case individual readings for each SM, and the second,$\otimes$, represents an addition operation on encrypted values.

1. The ES receives periodical readings $e_{ij}$ encrypted with the key $k_{ij}$, i.e.,

$$E_{k_{ij}}(e_{ij}), \forall\, i,j$$

$$\left(\mathrm{E}_{\mathrm{k}_{1\mathrm{j}}}(\mathrm{e}_{1\mathrm{j}}), \mathrm{E}_{\mathrm{k}_{2\mathrm{j}}}(\mathrm{e}_{2\mathrm{j}}), \ldots, \mathrm{E}_{\mathrm{k}_{\mathrm{nj}}}(\mathrm{e}_{\mathrm{nj}})\right)$$

2. The ES performs the operation $\otimes_i E_{k_{ij}}(e_{ij})$ that will be equal to the equation defined by $E_K(\oplus_i e_{ij})$where $K = f(k_{1j}, k_{2j}, \ldots, k_{nj})$, or:

$$\otimes_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{E}_{\mathrm{k}_{\mathrm{ij}}}(\mathrm{e}_{\mathrm{ij}}) = \mathrm{E}_{\mathrm{K}}\left(\oplus_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{e}_{\mathrm{ij}}\right)$$

3. The key $K$ is transmitted one time to the ES.

## III. Grouping

We assume that the SMs are grouped according to the interests of the ES such as, for example, all the consumer units in a given building, on a street, or all the units served by a particular distribution transformer.

We can assume that all the SMs in one common group can communicate among themselves, regardless which physical means is used to do so. One SM will periodically assume the role of Local Concentrator (LC), which is assigned at random. The LC's job is to generate the key K and manage the group.

This work also assumes that the security requirements for message exchanges between the SM and ES are met by means of an authentication mechanism, therein guaranteeing the establishment of a secure channel. This begins with the establishment of a TLS connection in which the server is authenticated through a certificate. The server can be the ES or the LC.

## IV. Aggregation keys

According to the CMT model presented by [11], whose algorithm is shown inTable 1, the cryptography keys should be changed constantly. The LC receives the keys $k_{ij}$ during the first period of measurement (therefore j = 1) from all SMs in the group, aggregates these keys and sends their sum to the ES via a secure channel.

TABLE 1Castelluccia, Mykletun, Tsudik (CMT) algorithm

| | |
|---|---|
| Encryption | $Message\ m\ \in [0, M-1,]$<br>$randomly\ generated\ keystream$<br>$k \in [0, M-1]$<br>$c = (m + k)\ mod\ M$ |
| Decryption | $Dec(c, k, M) = c - k\ (mod\ M)$ |
| Aggregation | $Let\ c_1 = Enc(m_1, k_1, M)\ and$<br>$c_2 = Enc(m_2, k_2, M)$<br>$Fork = k_1 + k_2,$<br>$Dec(c_1 + c_2, k, M) = m_1 + m_2$ |

This process will be repeated every time there is a change in system topology, in other words, a new SM in the group, an SM that leaves the group (even if temporarily, which happens in the case of communication failure). This process will also be carried out every time the LC is changed. This model is shown mathematically in (2).

$$\mathrm{K} = \mathrm{f}(\mathrm{k}_{11}, \mathrm{k}_{21}, \ldots, \mathrm{k}_{\mathrm{n}1}) = \oplus_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{k}_{\mathrm{i}1} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{k}_{\mathrm{i}1} \qquad (2)$$

In order to maintain the value of K constant, the $k_{ij}$ values must have a relationship. To guarantee this, the LC organizes the SMs in the group with a virtual ring where one SM sends a value $\delta_{ij}$ to its successor.

In **Error! Reference source not found.**is a schematic representation of how this ring works. It should be mentioned here that any of the SMs may assume the role of LC, represented in this figure as $SM_m$. The value $\delta_{ij}$ is randomly generated each time and denominated by *differential iterative encryption key*.

Each SM generates a value $\delta_{ij}$which is sent to the next SM in the virtual ring and when it has these values the encryption key is assembled. This way, each encrypted key is defined according to (3). The LC is responsible for determining the successors of each SM.

$$\mathrm{k}_{\mathrm{ij}} = \mathrm{k}_{\mathrm{i}1} - \delta_{\mathrm{ij}} + \delta_{\mathrm{i}-1,\mathrm{j}} \qquad (3)$$

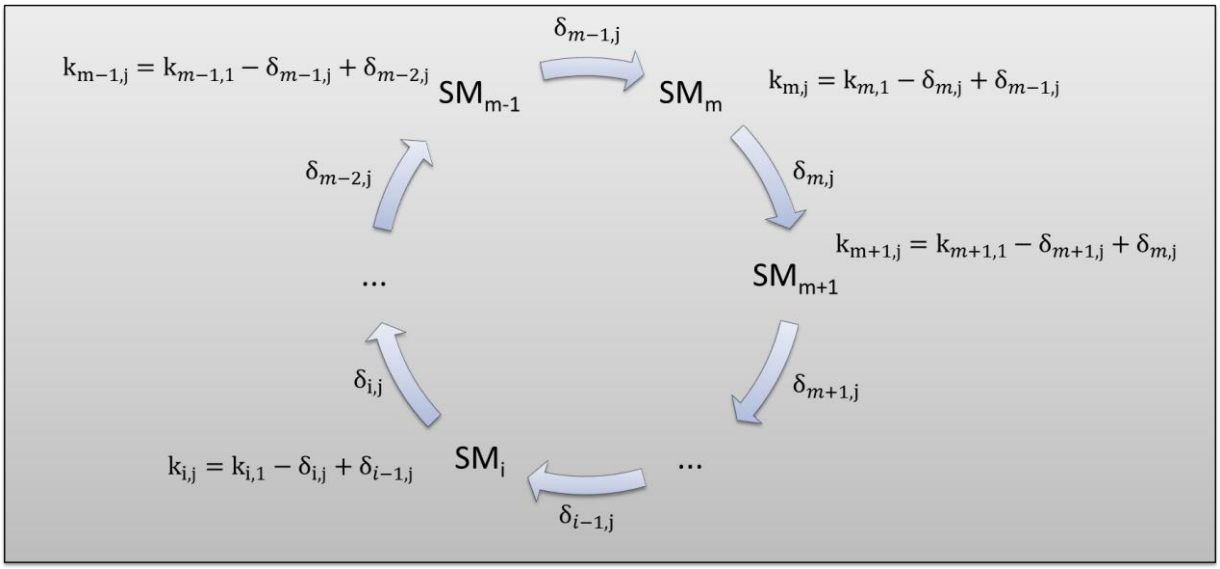


Fig.2: Smart meters ring: keys updating – adapted from **[10]**

## V. How it works

The process is begun when a $SM_i$ is connected to the grid for the first time and must receive a license from the ES. The SM in question sends an Enabling Request in the Grid to the ES via data which identify it. At the ES, the data of this SM are verified and if they are correctly registered, the ES sends back a license allowing it to continue the process. Next, the SM sends a message via Broadcast to the LC. If there is on response from the LC after a pre-determined number of attempts the SM will assume the role of LC. If an LC already exists in the group it will respond to the SM with a Token value which will identify it to the group. This Token is not related to the SM identifier with the ES. This Token value ($T_i$)is also sent to the ES. The Token's role is to identify the SM with the ES only for obtaining the group's instant consumption.

When the $SM_i$ receives the $T_i$, it responds to the LC with the encryption key value $k_{i1}$, which in turn responds by sending the identification of its successor $Sc_i$within the previously described virtual ring. After a previously determined interval of time, the LC processes the values $k_{i1}$to arrive at the value K as shown in (4).

$$K = \sum_{i=1}^{n} k_{i1} \quad (4)$$

Once the K value has been calculated, the LC sends the K, n and$T_i$ values to the ES, where n is the number of SMs present in the virtual ring. Whenever the network's topography changes, the process is repeated. The LC role is traded at random between the members of the group at random intervals. If the LC is the $SM_m$, then its successor will be the $SM_{m+1}$and its predecessor the $SM_{m-1}$.

The ES will begin the reading of instant consumption through a request made directly to the LC, which sends the value $\delta_{m,j}$to its successor. The smart meter $SM_{m+1}$sends the values $T_{m+1}$, and $E_{k_{m+1,j}}(e_{m+1,j})$to the ES and the value$\delta_{m+1,j}$to $SM_{m+2}$, its successor.

The values are sent from one member of the ring to the next until returning to $SM_m$which only then will send the encrypted consumption value.

After receiving the last value $E_{k_{1j}}(e_{1j})$the ES will obtain the entire group's consumption value through the equations shown in (5).

$$\otimes_{i=1}^{n} E_{k_{ij}}(e_{ij}) = \sum_{i=1}^{n} E_{k_{ij}}(e_{ij}) = \sum_{i=1}^{n}(e_{ij} + k_{ij}) = i{=}1 e_{ij} + i{=}1 k_{ij} = EK \oplus i{=}1 e_{ij} \quad (5)$$

And:

$$\otimes_{i=1}^{n} E_{k_{ij}}(e_{ij}) = \sum_{i=1}^{n} e_{ij} + K \quad (6)$$

The decryption function performed by the ES is given by (7).

$$D_K\left(E_K\left(\oplus_{i=1}^{n} e_{ij}\right)\right) = D_K\left(\otimes_{i=1}^{n} E_{k_{ij}}(e_{ij})\right)$$

$$= D_K\left(\sum_{i=1}^{n} e_{ij} + K\right) \quad (7)$$

Where K was sent by the LC and the values $E_{k_{ij}}(e_{ij})$ by the SMs. Thus, when K it is subtracted from (7) the group's instant consumption value is obtained ($\sum_{i=1}^{n} e_{ij}$).The model for this procedure is shown in Fig.3.

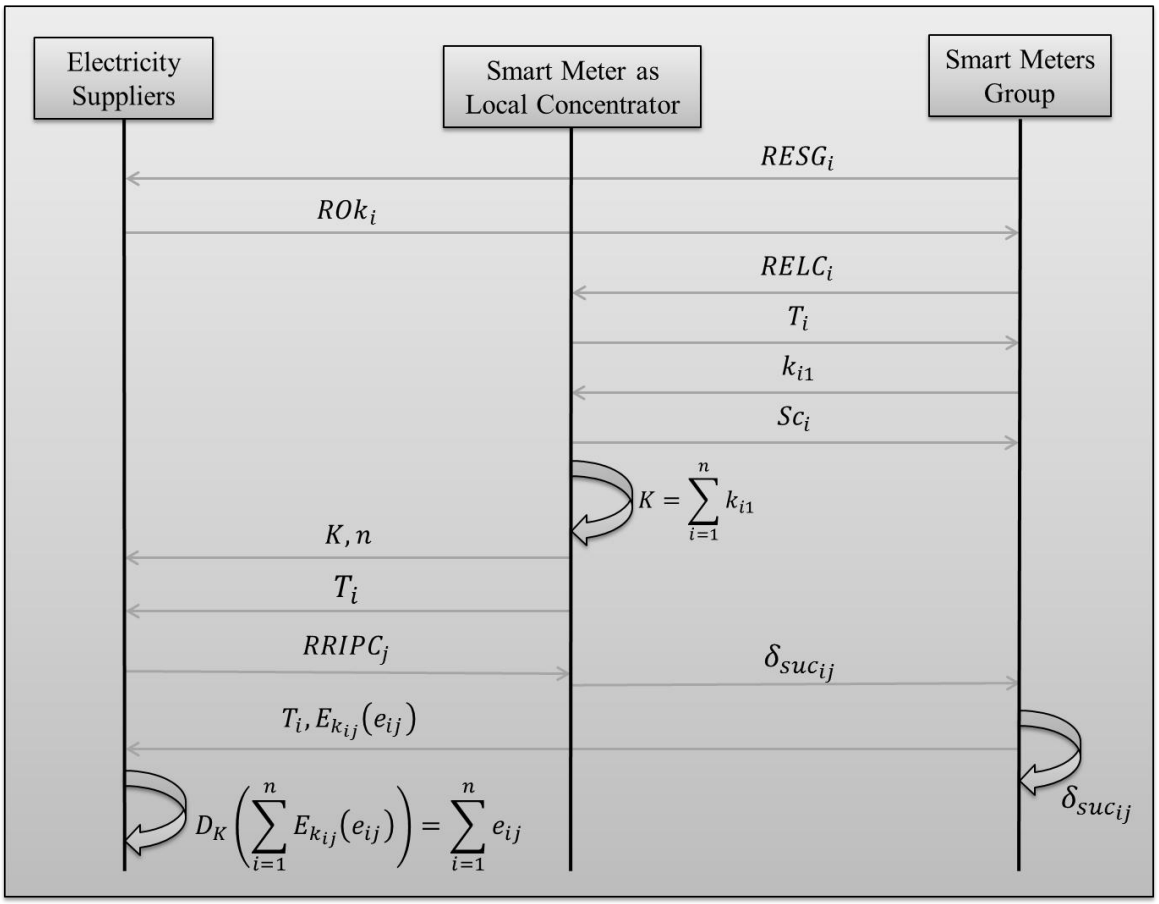


Fig.3: Proposed architecture

So when the ES makes a request for readings of instant values, it determines how long it will wait for the readings to be finished, in other words, it waits for an interval of time for theall SMs respond. When this interval is over, the ES will process the received data.

Supposing that the $SM_i$had one fault in its data link, then the virtual ring won't complete its cycle. The LC will be able to identify this error and restart the process, sending a request to all the SMs so they re-register with the LC, therefore isolating $SM_i$. When the error is fixed, the $SM_i$will emit a request for license to the LC.

In the case that$SM_i$ is the LC itself, the ES may be able to partially receive the readings but it will not receive the readings from $SM_i$. To resolve this problem, the ES determines an interval of time for receiving data. If by the end of this time interval one SM has failed to respond, the readings are not validated and the ES waits for the process to restart.

## VI. Conclusion

Transmission of instant energy consumption measurements from consumer units is carried out via a secure channel, guaranteeing the integrity and authenticity of the data transmitted. The data confidentiality question is resolved by the process itself. The Electricity Supplier (ES) receives the consumption data through an identifier that only the Local Concentrator (LC) knows, unlike readings for billing in which the ES must know the identity of each consumer unit. The rotation of the LC position also guarantees security as it unables outsiders to obtain data, which is key-encrypted and unreadable without the key, which is changed with every reading.

The Privacy-enhanced architecture for smart metering presented by [10], upon which this study is based, does not describe management of the Local Concentrator's functions and the dispatch of the keys between the consumer units belonging to the interest group. This brought about a proposal for an additional, improved mechanism for managing LC functions and the exchanges of messages between the Electricity Supplier and the Smart Meters, as well as the dispatch of the *differential iterative encryption key*between them as a guarantee of consumer privacy security.

## REFERENCES

[1] H. Farhangi, "The Path of the Smart Grud," *IEEE Power & Energy Magazine*, pp. 19-28, jan-fev 2010.

[2] V. C. Güngör, B. Lu and G. P. Hancke, "Opportunities and Chellenges of Wireless Sensor Network in Smart Grid," *IEEE Transactions on Industrial Electronics*, Vols. vol. 57, nº 10, pp. 3557-3564, oct. 2010.

[3] P. McDaniel and S. W. Smith, "Security and Privacy Challenges in the Smart Grid," *Security & Privacy*, Vols. vol. 7, nº 3, pp. 75-77, may-jun 2009.

[4] CEER, "status review of regulatory approaches to smart electricity grids," Bruxelles, 2011.

[5] W. Wang and L. Zhuo, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, pp. - no prelo, 2013.

[6] D. G. Hart, "Using AMI to Realize the Smart Grid," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, 2008.

[7] D. Yazar and A. Dunkels, "Efficient Application in IP-Based Sensor Networks," in *BuildSys' 09 Proceedings of the First ACM Worshop on Embedded Sensing Systems for Energy Efficiency in Buildings*, New York, 2009.

[8] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki and Y. Nozaki, "Toward Intelligent Machine-to-Machine Communications in Smart Grid," *IEEE Communicatoins Magazine*, pp. 60-65, apr. 2011.

[9] A. Ghassemi, S. Bavarian and L. Lampe, "Cognitive Radio for Smart Grid Communications," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaitherburg, 2010.

[10] F. G. Mármol, C. Sorge, R. Petrlic, O. Ugus, D. Westhoff and G. M. Pérez, "Privacy-enhanced architecture for smart metering," *International Journal of Information Security*, vol. 12, no. 2, pp. 66-82, April 2013.

[11] C. Castelluccia, E. Mykletun and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," *Mobile and Ubiquitous Systems: Networking and Services*, pp. 109-117, 2005.