Computer Communications 82 (2016) 95–101

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Efficient smart metering based on homomorphic encryption

N. Busom [a,*], R. Petrlic [b], F. Sebé [a], C. Sorge [b], M. Valls [a]

[a] Departament de Matemàtica, Universitat de Lleida, Avda. Jaume II, Lleida 69 E-25001, Spain
[b] CISPA, Saarland University, P.O. Box 15 11 50, Saarbrücken D-66041, Germany

ARTICLE INFO

Article history:
Received 23 March 2015
Revised 10 July 2015
Accepted 30 August 2015
Available online 8 September 2015

Keywords:
Encryption
ElGamal
Homomorphism
Privacy
Smart metering

ABSTRACT

Smart meters send fine-grained client electricity consumption readings to suppliers. Although this presents advantages for both entities, it results in a serious loss of privacy for customers. We present a monitoring-purpose system that preserves customers' privacy by homomorphically aggregating the consumptions of all n members of a neighborhood. The proposal has an efficient linear $O(n)$ communication cost and is proven to preserve customers' privacy even in the presence of a corrupted substation and some malicious smart meters. It requires neither secure communication channels nor a trusted third party (except for issuing public-key certificates). Computation on the smart meters is limited to modular exponentiations. These favorable properties come at the expense of increased computation cost on the electricity suppliers' side. We show that the computation is easily feasible for realistic parameter choices.

1. Introduction

1.1. Smart meters systems

Smart meters are a refined adaptation of traditional electricity meters. These devices record energy consumption in small intervals of time, for example every 30 min, and regularly communicate their readings to the utility for monitoring and billing purposes.

Since electricity cannot be stored in large quantities, it is highly useful for energy suppliers to keep track of the current energy consumption, as well as to know its trend. This way, they can adapt their trades at the energy exchange, and—in the long run—avoid the production of an electricity surplus. Smart metering is an appropriate technology for monitoring, measuring, and making predictions of energy utilization, which results in advantages both for energy suppliers and final customers. The former can elaborate an energy plan to avoid unnecessary energy production and try to promote electricity consumption in times of higher availability. The latter may benefit from different prices, more accurate billing, and better knowledge on consumption habits.

However, smart meters have raised concerns about being privacy invasive. Meter readings allow one to infer behavioral patterns such as the time at which a given customer leaves his home, switches on the washing machine, or goes to bed. For this reason, smart metering solutions should provide mechanisms for customer privacy preservation.

1.2. Related work

Research on smart metering privacy has tremendously increased over the last few years, starting in 2010 with publications highlighting the privacy problems introduced by smart metering [2]. Complete overviews—not including most recent research results—can be found in [9,12,15].

Proposals for privacy protection in smart metering can be classified according to the technique employed for providing privacy. Three main techniques exist:

- *Anonymization:* data are transmitted so that the link between electricity readings and the identity of customers is removed [8,10,21].
- *Perturbation:* each reading is transmitted after adding some random noise to it. Since this random noise will not be removed, such solutions have to be tuned to provide an appropriate trade-off between privacy and accuracy [1,2,14].
- *Aggregation:* smart meters are partitioned into communities that aggregate (add) their readings prior to transmitting them to the energy supplier [2,3,5,11,12,17–19,24,25]. Data can be aggregated by a trusted party or by making use of the homomorphic property of some cryptosystems. The homomorphic solutions require the use of secure computation techniques when some of the participants in the system may act dishonestly.

* Corresponding author. Tel.: +34 973 702 774; fax: +34 973 702 716.
E-mail addresses: nuria@matematica.udl.cat (N. Busom), ronald.petrlic@uni-saarland.de (R. Petrlic), fsebe@matematica.udl.cat (F. Sebé), christoph.sorge@uni-saarland.de (C. Sorge), magda@matematica.udl.cat (M. Valls).

http://dx.doi.org/10.1016/j.comcom.2015.08.016
0140-3664/

1.2.1. Anonymization-based proposals

Efthymiou and Kalogridis [8] propose that every smart meter has a high-frequency identity used for anonymous transmission of power consumption readings on a regular basis and another low-frequency identity that is used by the meter for transmissions of bills, computed on the smart meter based on the readings, to the electricity supplier in infrequent intervals. The relationship between those two identities is not known by the energy supplier, but only by an escrow party.

Petrlic [21] proposes the introduction of so-called collector systems within switchyards. Individual smart meters send their readings to the collector, which checks their authenticity, removes identifying information, and then forwards the readings to the electricity supplier. The proposal is complemented with the use of trusted computing to ensure integrity of the smart meters.

Finster and Baumgart [10] propose a system based on anonymization. It employs an anonymous peer-to-peer overlay network in its smart metering architecture. Each smart meter is in possession of a pseudonymous public key that has been previously certified anonymously by the grid operator. The smart meter then encrypts its meter reading value with the grid operator's public key and signs it with its private key. The value is then sent—together with the certificate—to the energy supplier over the overlay network.

1.2.2. Perturbation-based proposals

Bohli et al. [2] propose the addition of random noise with known finite variance and expectation by each individual smart meter. The values are then aggregated by the electricity supplier. While the sum is more precise than the individual readings, the authors conclude that large groups are required for the approach to provide sufficient privacy guarantees while giving the electricity supplier useful aggregated data.

Ács and Castelluccia [1] provide *differential privacy* by adding Laplacian random noise to the consumption measurements. The noisy measurements are sent to an aggregator that will add them obtaining a noisy overall consumption value. The system tolerates limited failures.

The general proposal of Shi et al. [23] on privacy-preserving aggregation of time-series data can be indeed applied to smart metering systems. This proposal combines perturbation-based techniques with data aggregation. Each meter adds noise to its reading before encrypting it. Afterwards, the encrypted values are transmitted to an aggregator which homomorphically aggregates them. At the end, the aggregator is able to obtain a noisy addition of data.

Jawurek and Kerschbaum [14] present a proposal for calculating diverse statistics (sums) of users' power consumption that provides differential privacy and fault-tolerance.

1.2.3. Aggregation-based proposals

The proposal we are presenting provides privacy by means of data aggregation employing an additive homomorphic cryptosystem. Next, we review some proposals using the same approach. The obvious approach of having a trusted third party computing the aggregation is already mentioned by Bohli et al. [2], but more advanced aggregation proposals have been published later.

García and Jacobs [11] were among the first to propose a privacy-friendly smart metering architecture based on additive homomorphic encryption. In their architecture, they consider a neighborhood with n smart meters. Each meter M_i, $i \in \{1, \ldots, n\}$, divides its energy reading m_i into n shares, m_{ij}, $j \in \{1, \ldots, n\}$, then encrypts each share m_{ij}, for $j \neq i$, under M_j's public key and sends the resulting ciphertexts to its substation *SSt*. Next, *SSt* homomorphically aggregates all $n-1$ shares encrypted under the public key of M_i and sends the result to it. Each M_i decrypts the received ciphertext and adds m_{ii} to it. Finally, it sends the result to *SSt*. The *SSt* computes the aggregated energy consumption by adding all the received results. In [11], each reading period requires the transmission of $O(n^2)$ ciphertexts.

The proposals by Shi et al. [23] and Xie and Zhang [25] require the presence of a trusted dealer that generates a set of random values that sum up to zero. During the set-up, each value is privately assigned to a different smart meter which will employ it for encrypting each of its readings prior to their transmission. Such a solution is not suitable for dynamic scenarios since each time a smart meter is added (or removed), the aforementioned set–up process must be executed from scratch. Moreover, the trusted dealer knows all the secret values so that, in case of corruption, it could obtain the individual measurements of all the smart meters.

Li et al. [18] and Lu et al. [19] present aggregation methods that preserve customers' privacy but only provide security against honest-but-curious attackers. In [18] a neighborhood of n meters is represented as a graph G whose vertices correspond to the meters and each edge represents an available wireless link. Then, a proper spanning tree of G rooting at the collector node is taken and the power consumption is recursively computed from children to parent nodes. The aggregation is performed using the additive homomorphic property of the Paillier cryptosystem. In [19], a centralized aggregating entity uses the Paillier cryptosystem to efficiently aggregate the collected data. The validity of data is provided by means of digital signatures using bilinear pairing cryptography.

Vetter et al. [24] suggest an approach that enables flexible server-side aggregation of smart meter readings. It combines homomorphic encryption with homomorphic message authentication codes for preserving customers' privacy. The energy consumptions are encrypted and stored in a database so that aggregation operations over time and other *selective* SQL-queries are possible. However, only aggregated values of at least one group of smart meters can be retrieved. The proposal requires the introduction of a trusted third party, which computes aggregate keys from the smart meters' secret keys (but is not involved in the transmission of individual values to the electricity supplier).

Gómez Mármol et al. [12] propose an architecture that allows the transmission of up-to-date electricity measurements to energy suppliers on a group basis, i.e. the data of individual users belonging to a group are *not* revealed in their approach. The solution is based on an additive homomorphic encryption scheme by Castelluccia et al. [3]. No trusted third party is needed, but only an untrustworthy aggregating node. Every smart meter encrypts its power consumption value with a homomorphic key. The encrypted meter value is then forwarded to the energy supplier. However, this value cannot be decrypted by the supplier, who is not in possession of the corresponding key. At this point, key aggregation comes into play. Each smart meter sends its homomorphic key to the aggregating node, who then aggregates all the received individual keys and sends forth only the aggregated key to the energy supplier. The energy supplier can now decrypt the aggregation of the *encrypted* meter readings with the aggregated key. This proposal presents some drawbacks derived from its high complexity due to the need for smart meters to implement TLS connections, group signatures, and anonymous credentials (depending on the attack scenarios).

Jung and Li [17] present several proposals for privacy-preserving sum and product calculation. They present a proposal for sum computation in which one of the parties (called *the aggregator*) computes a sum $\sum_{i=1}^{n} m_i$ being m_i the private input of party i. In the context of smart metering, the substation *SSt* would play the aggregator role while each smart meter would participate by providing its reading as input. Their proposal requires a set-up operation in which the parties are required to be arranged in a circle. When dealing with possible corrupted parties, the set-up operation consists of $k+1$ rounds for tolerating up to k colluding adversaries. If the amount of corrupted parties exceeded k, they would be able to obtain individual readings through a passive attack.