

Article

Enabling Privacy in Vehicle-to-Grid Interactions for Battery Recharging

Cristina Rottondi *, Simone Fontana and Giacomo Verticale

Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milano 20133, Italy;
E-Mails: simone.fontana@mail.polimi.it (S.F.); giacomo.verticale@polimi.it (G.V.)

* Author to whom correspondence should be addressed; E-Mail: cristinaemma.rottondi@polimi.it;
Tel.: +39-02-2399-3691; Fax: +39-02-2399-3413.

Received: 10 January 2014; in revised form: 13 April 2014 / Accepted: 21 April 2014 /

Published: 25 April 2014

Abstract: The diffusion of Electric Vehicles (EV) fostered by the evolution of the power system towards the new concept of Smart Grid introduces several technological challenges related to the synergy among electricity-propelled vehicle fleets and the energy grid ecosystem. EVs promise to reduce carbon emissions by exploiting Renewable Energy Sources (RESes) for battery recharge, and could potentially serve as storage bank to flatten the fluctuations of power generation caused by the intermittent nature of RESes by relying on a load aggregator, which intelligently schedules the battery charge/discharge of a fleet of vehicles according to the users' requests and grid's needs. However, the introduction of such vehicle-to-grid (V2G) infrastructure rises also privacy concerns: plugging the vehicles in the recharging infrastructures may expose private information regarding the user's locations and travelling habits. Therefore, this paper proposes a privacy-preserving V2G infrastructure which does not disclose to the aggregator the current battery charge level, the amount of refilled energy, nor the time periods in which the vehicles are actually plugged in. The communication protocol relies on the Shamir Secret Sharing threshold cryptosystem. We evaluate the security properties of our solution and compare its performance to the optimal scheduling achievable by means of an Integer Linear Program (ILP) aimed at maximizing the ratio of the amount of charged/discharged energy to/from the EV's batteries to the grid power availability/request. This way, we quantify the reduction in the effectiveness of the scheduling strategy due to the preservation of data privacy.

Keywords: smart grid; electric vehicles; vehicle privacy; vehicle-to-grid interactions

1. Introduction

The evolution of the electric power system toward the novel Smart Grid paradigm and the progressive concurrent electrification of transportation aimed at the reduction of carbon emissions rises various issues related to the interactions between the distribution network and the Electric Vehicles (EVs). Such category of vehicles includes battery/fuel cell-powered automobiles, as well as hybrid systems combining electricity generators and conventional gasoline engines [1,2]. Several investigations on the potential market penetration of EVs and on the impacts of their possible massive introduction have been carried out by the research community [3,4]: on one hand, the additional connected load capacity required to simultaneously recharge a huge number of EVs might significantly impact the energy consumption trend; on the other hand, the EVs' batteries represent a huge storage bank that can be exploited to flatten the typically unpredictable power generation patterns of Renewable Energy Sources (RESes) by accumulating energy in case of excessive power generation and transferring it back to the grid during peak-demand periods [5,6]. To enable such synergies between EVs and the Smart Grid, which are usually referred to as Vehicle-to-Grid (V2G) interactions, the introduction of an aggregator capable of coordinating the charging/discharging process for a huge fleet of vehicles has been proposed [7,8]: the role of such agent is to operate as middleman between the vehicle owner (who could not act as stakeholder on the electricity market due to the limited power capacity of a single vehicle) and the electrical utilities or system operators. Several business models for the aggregation entity have been studied, possibly taking into account the additional costs incurred by the EVs' owners due to the frequent battery charge/discharge and the introduction of financial incentives to encourage the owners to plug their vehicle when not in use [9,10]. However, V2G assumes that detailed information about the traveling habits of the vehicle owners are available at the aggregator, which can disclose sensitive data (e.g., presence in a certain location at a given time) and thus arises privacy concerns [11,12]: according to NIST [13], once a two-way communication between the EV and the charging station is established, there is currently no technical limitation to the amount and type of data that could be obtained from the EV's microcomputers which manages specific functions such as breaking, ignition systems, lighting controls, fuel delivery, on-board diagnostics, and so on. This could lead to potentially threatening consequences: for instance, burglars could track people's movements before attempting robberies, information about vehicle maintenance could be inferred and exploited for insurance and warranties, or companies could perform targeted marketing for car-related services.

The main contributions of our paper are:

- the design of a privacy preserving online framework which allows a set of Aggregators to collaboratively coordinate the charging/discharging process of the vehicles' batteries without learning the time periods in which the EVs are actually plugged-in and the current charge level of the batteries, nor the amount of refilled energy: every data is split in w parts called *shares* by means of the Shamir Secret Sharing (SSS) threshold cryptosystem and each share is given to a different Aggregator. The protocol ensures that a collusion of less than $t \leq w$ Aggregators cannot reconstruct the data.

- the definition of a set of security properties which capture the requirements of V2G interactions for battery recharge and the proof that such properties are satisfied by our proposed scheduling protocol.
- the formulation of a benchmark offline scheduling problem, which assumes full knowledge of the future travels of the users and of the battery-related information before the beginning of the scheduling horizon.
- the comparison of the performance of our privacy-friendly mechanism to the benchmark model. This way, we quantify the reduction in the effectiveness of the scheduling strategy due to incorporating data privacy preservation in the scheduling mechanism.

The benefits introduced by our privacy-friendly protocol are twofold: on one hand, it encourages the EV owners to take part in the scheduling optimization framework by protecting their personal data. Assuming an underlying business model which rewards the users that allow for the discharge of their EV's batteries, providing privacy in V2G interactions could therefore lead to significant cost savings for the individual users. On the other hand, the wider is the EV fleet participating to the protocol, the higher is the degree of flexibility experienced by the grid in the management of the power generation/consumption balancing, thus helping in a more effective compensation of the unpredictable power generation patterns of RESes.

The remainder of the paper is structured as follows: Section 2 provides an overview of the related literature, while some background notions about the SSS scheme are recalled in Section 3. The privacy-friendly scheduling infrastructure, the collaborative scheduling procedure and the associated communication protocol are discussed in Section 4. The security analysis of the proposed scheduling mechanism are presented in Section 5, while Section 6 introduces an Integer Linear Programming formulation for the optimal scheduling to be used as evaluation benchmark. The performance assessment of our proposed solution is discussed in Section 7. Final conclusions are drawn in the last Section.

2. Related Work

The design of EVs and the characterization of their interactions with the power grid has been widely investigated in the last decade: for a comprehensive survey on the impact of the introduction of EVs in the Smart Grid ecosystem, the reader is referred to [14], while a thorough overview on the economical and technical models of aggregator agents for EV fleets can be found in [15].

A substantial body of work investigates optimal and heuristic policies for the battery recharge of a population of EVs based on various approaches, ranging from game theory [16,17] to queuing theory [18,19], possibly associated with reinforcement learning techniques [20] or stochastic/fuzzy logic-based predictors [21]. Game models are suitable for scenarios involving multiple selfish entities, each one operating with the aim of optimizing his own utility function, and allow for possible negotiations among them. Conversely, in our framework we assume that the vehicle owners fully collaborate with the aggregator in order to achieve a common optimization goal in terms of balancing of the grid's power availability, without assumption of any economical incentives. Queuing models are employed to capture constraints such as limits on the maximum number of EVs to be charged

contemporaneously: our scenario assumes that the charging station is equipped with a sufficient number of plugs to serve the whole fleet without introducing additional waiting times.

However, none of the above papers addresses the privacy-related issues which are peculiar of the V2G scenario, which have been considered only by a few studies: Stegelmann and Kesdogann [22] enumerate the security requirements of a V2G infrastructure in presence of an untrusted aggregator, and formalize the model of an honest-but-curious attacker which tries to infer the traveling habits of the vehicle owners by linking the plugging/unplugging events at the charging stations in different locations. The same authors further refine such adversary model in [23] by integrating information regarding the charge level of the EV's batteries. We consider the same attacker model, and our solution ensures that the aggregators schedule the charging/discharging process without knowing the total amount of energy to be provided to the battery, nor the time periods in which the EV is actually plugged. The only information available at the aggregators is a priority tag which declares whether the EV must be necessarily charged or could also be discharged, according to the current battery charge level, which remains undisclosed.

Yang *et al.* [24] also assume a honest-but-curious aggregator model in a two-tiered structure including multiple local aggregators directly interacting with the vehicles and a central aggregator which interfaces the electricity market, and propose a rewarding scheme based on blind signature techniques, which ensures mutual authentication while preserving location and identity privacy, and allows for anonymous rewards. Our solution is based on Shamir Secret Sharing scheme, which is computationally less demanding, but requires the collaboration of multiple scheduling entities, thus introducing additional message exchanges among them (which would not occur in presence of a single aggregator).

Liu *et al.* propose in [25] a two-way anonymous payment system for EVs' battery charge/discharge providing traceability in case of car theft, while Nicanfar *et al.* [26] design a pseudonym-based authentication scheme, which ensures untraceability of the users' movements and assumes the presence of an external trusted entity in charge of recording the associations between pseudonyms and real identities to provide accountability for billing purposes. Though the security of the billing process is out of the scope of our contribution, similar protocols could be easily integrated in our infrastructure.

3. Background on Shamir Secret Sharing Scheme

Shamir Secret Sharing (SSS) scheme [27] is a cryptographic threshold scheme which allows multiple participants to reconstruct a secret by means of a collaborative procedure. To do so, the secret is split in w shares, which are given to the participants to the protocol: the secret can be recovered through cooperation of at least $t \leq w$ participants, where the threshold t is a system design parameter.

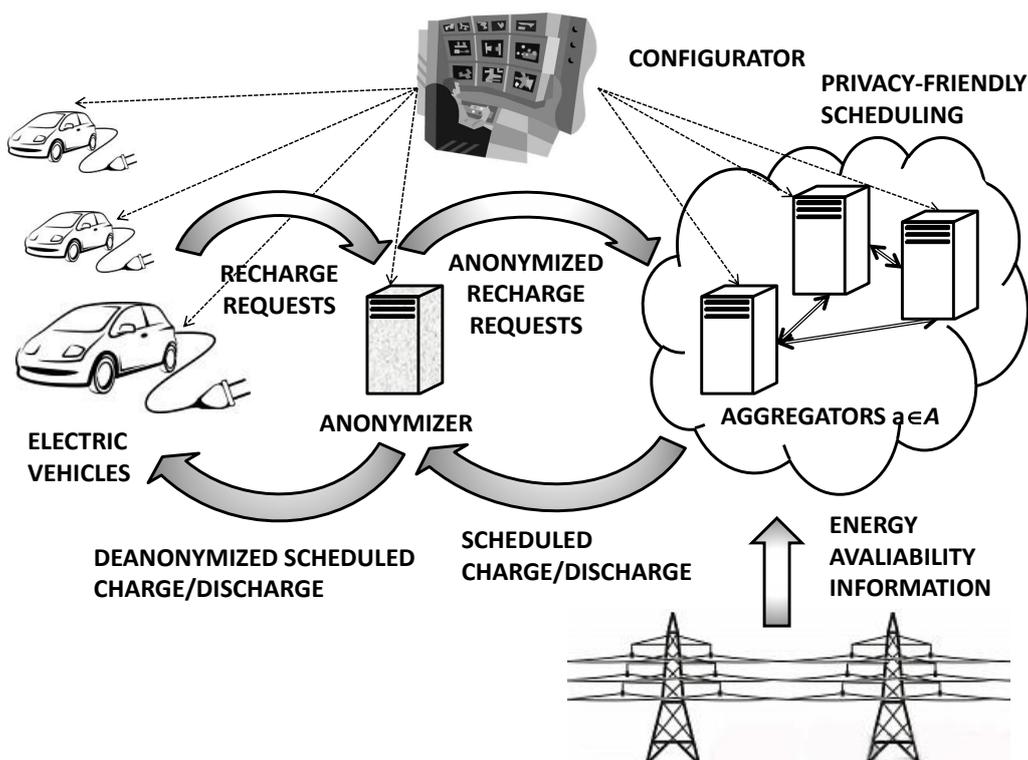
More in detail, the SSS scheme works as follows. Choose a prime number q and split the secret $m \in \mathbb{Z}_q$ in w shares (x_s, y_s) ($1 \leq s \leq w$) by selecting $t-1$ integer random numbers $\rho_1, \rho_2, \dots, \rho_{t-1}$ with uniform distribution in $[0, q-1]$ and calculating the s -th share as $y_s = m + \rho_1 x_s + \rho_2 x_s^2 + \dots + \rho_{t-1} x_s^{t-1} \pmod{q}$, where $x_s \in \mathbb{Z}_q$ is arbitrarily chosen. The secret can be reconstructed by interpolating at least t shares, using e.g., the Lagrange interpolation algorithm. The SSS scheme has homomorphic properties with respect to addition and multiplication, meaning that performing such operations on the shares and then recovering the result leads to the same result that would be obtained by computing the same operations on the secrets directly. The sum of two secrets can be independently calculated by a

single participant by summing the corresponding shares, while multiplication must be performed interactively by means of a collaborative procedure, e.g., as the one described in [28]. Therefore, any function expressed in terms of additions and multiplications can be calculated directly on the shares. In particular, several collaborative methods to perform the comparison of two secrets have been proposed (see e.g., [29,30]). In this paper, we will adopt the comparison protocol presented in [30], which works as follows: each party holding the s -th shares $(x_s, y_s), (x'_s, y'_s)$ of the secrets m and m' to be compared selects two big random numbers r_s, r'_s , which can multiplicatively hide $m - m'$, and a random bit $b_s \in \{0, 1\}$. The collaborative protocol enables each party to obtain a share of the quantity $c = (m - m') \prod_{s=1}^t (-1)^{b_s} r_s - \sum_{s=1}^t (-1)^{1-b_s} r'_s$. The result of the comparison can be computed by retrieving c , setting a bit e either to 0 in case $c > 0$ or to 1 otherwise (note that in a modulo n field negative numbers are represented by the upper half of the range $[0, n - 1]$), and calculating the result of the XOR operation $\xi = e \oplus b_1 \oplus \dots \oplus b_t$. $\xi = 0$ indicates that $m > m'$, while $\xi = 1$ indicates that $m \leq m'$. The reader is referred to [30] for additional details about the collaborative procedure and the proof of the correctness of the comparison protocol.

4. The Privacy-Friendly V2G Communication Framework

As depicted in Figure 1, our proposed architecture comprises a set of EVs, \mathcal{V} , a set of Aggregators, \mathcal{A} , which collaboratively schedule the charge/discharge of the EVs' batteries, and an Anonymizer which collects the messages sent by the EVs and replaces their IDs with pseudonyms before forwarding the messages to the Aggregators. The Anonymizer also receives the charge/discharge schedules from the Aggregators and communicates each of them to the addressed EV.

Figure 1. The privacy-friendly scheduling infrastructure.



We assume that:

- (1) Each EV is equipped with hardware and software (e.g., as described in [31,32]) enabling Internet access at any time.
- (2) A Configurator node is responsible for the setup of a suitable public-key infrastructure (e.g., as the one proposed in [33]).
- (3) The parties agree on a hybrid encryption algorithm $E(K_e, \cdot)$ and a corresponding decryption algorithm $D(K_d, \cdot)$. The hybrid scheme is assumed to be IND-CPA secure [34] (i.e., it ensures message indistinguishability under chosen plaintext attack) and uses state-of-the-art secure public key cryptography and symmetric cryptography to transmit messages of any size.
- (4) Each Aggregator $a \in \mathcal{A}$ has its own pair of public/private keys (K_e^a, K_d^a) and all the EVs know the public keys of the Aggregators.
- (5) All the communication channels between the EVs, the Anonymizer, and the Aggregators are confidential and authenticated.

We also assume that time is divided in a set of epochs \mathcal{I} of finite duration T (e.g., in the order of minutes) and that at the beginning of each epoch $i \in \mathcal{I}$ the system operator communicates the maximum amount g_i of power it can provide to recharge the Vehicles or it would need to discharge in order to satisfy the demands generated by other categories of critical loads (e.g., non-deferrable appliances). Such power supply/request curve is supposed to be public and known to all the Aggregators.

The design goal is to schedule the charge/discharge times of the EVs' batteries through a collaborative procedure in order to satisfy the customers' recharge requests while minimizing the difference between the power supplied (requested) by the grid and the power charged (discharged) to (from) the batteries, without exceeding the grid overall power availability (request).

A pictorial view of the exchanged messages between Vehicles and Aggregators is presented in Figure 2, while a list of the main symbols is provided in Table 1.

Figure 2. Data exchange during the battery charge/discharge scheduling procedure.

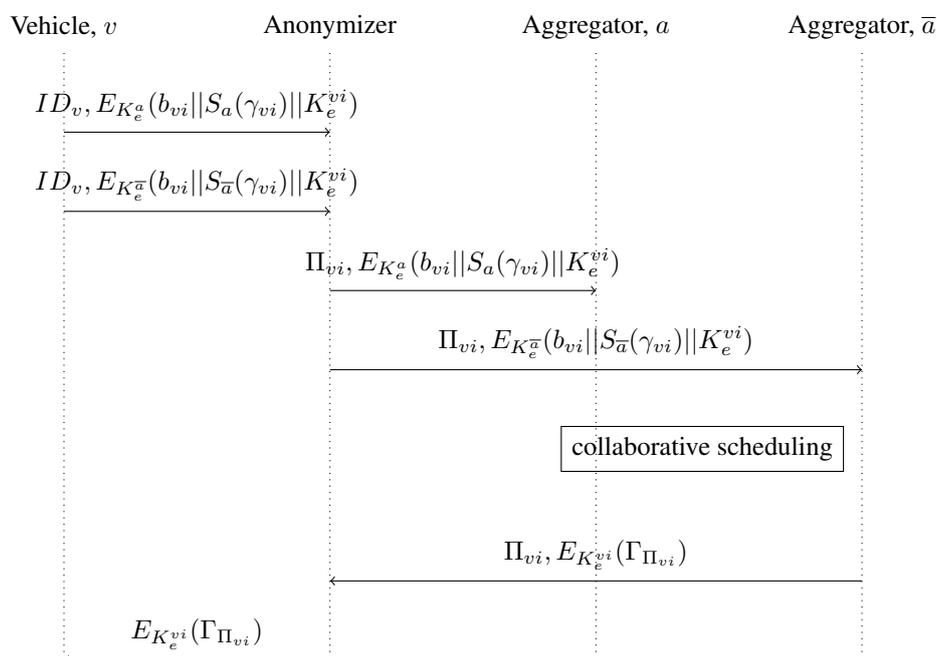


Table 1. List of main symbols.

Notation	Description
\mathcal{V}	set of Vehicles (v is an element of the set)
\mathcal{A}	set of Aggregators (a is an element of the set)
\mathcal{I}	set of time epochs (i is an element of the set)
r_v	battery charging rate of Vehicle v
b_{vi}	recharge priority indicator of Vehicle v at epoch i
l_{vi}	battery charge level of Vehicle v at epoch i
γ_{vi}	requested battery charge/discharge indicator of Vehicle v at epoch i
t_v	battery threshold level below which no discharge is accepted by Vehicle v
K_e^{vi}, K_d^{vi}	ephemeral encryption/decryption key-pair generated by Vehicle v at epoch i
ID_v	identifier of Vehicle v
Π_{vi}	pseudonym attributed to Vehicle v at epoch i
\mathcal{S}_i	set of the pseudonyms Π_{vi} at epoch i
Γ_{vi}	scheduled battery charge/discharge indicator of Vehicle v at epoch i

Whenever a new epoch i starts, each Vehicle $v \in \mathcal{V}$ initializes a parameter γ_{vi} either to 0, in case it is unable or unwilling to be charged/discharged (for instance because it is currently traveling or because its battery is already full) or to r_v , which indicates the Vehicle's charge/discharge rate. Moreover, v defines a threshold t_v indicating the level of charge below which no discharge is accepted by the customer. In a worst-case scenario, t_v equals the level of full battery charge, meaning that the customer does not allow for any discharge. Let l_{vi} be the battery charge level of v at the beginning of epoch i : if $l_{vi} < t_v$, v sets a priority bit b_{vi} to 1, otherwise to 0. Further, v generates an ephemeral keypair (K_e^{vi}, K_d^{vi}) , which is refreshed at every epoch. Then, v divides γ_{vi} in shares using a (w, t) -SSS scheme with parameters $t = w = |\mathcal{A}|$, thus obtaining $|\mathcal{A}|$ shares $S_1(\gamma_{vi}), \dots, S_{|\mathcal{A}|}(\gamma_{vi})$, and concatenates the priority bit b_{vi} and the ephemeral encryption key K_e^{vi} to each share $S_a(\gamma_{vi})$. For the sake of easiness, in this paper we set as SSS threshold $t = w$, meaning that all the Aggregators must collaborate to perform the charge/discharge scheduling procedure. However, to improve resiliency to faults and malfunctions, t could be lower than w . For a discussion on the correct dimensioning of t and w , the reader is referred to [35]. Finally, v encrypts $b_{vi} || S_a(\gamma_{vi}) || K_e^{vi}$ using the public key K_e^a for each Aggregator $a \in \mathcal{A}$ and sends the pair $ID_v, E_{K_e^a}(b_{vi} || S_a(\gamma_{vi}) || K_e^{vi})$ to the Anonymizer, where ID_v is the identity of Vehicle v .

Upon reception of the $|\mathcal{A}|$ messages sent by v , the Anonymizer replaces ID_v with a random pseudonym Π_{vi} , which is refreshed at every epoch, and forwards each pair $\Pi_{vi}, E_{K_e^a}(b_{vi} || S_a(\gamma_{vi}) || K_e^{vi})$ to the respective Aggregator a .

Let $\Gamma_{\Pi_{vi}}$ be the scheduling output of the Vehicle associated to the pseudonym Π_{vi} , which can be set by the Aggregators either to 1 if the Vehicle is scheduled for recharge, to -1 if it is scheduled for discharge, or to 0 otherwise. Moreover, let P_i be a variable which records the amount of power required for the charges/discharges scheduled during the current epoch i : positive values of P_i indicate that the grid must provide power to charge the batteries, while negative values indicate that the energy collected from the batteries is injected in the grid.

Algorithm 1 The Privacy-Friendly Scheduling Algorithm

```

1: On input of the epoch number  $i$  and of  $\Pi_{vi}, b_{vi}, S_a(\gamma_{vi}), K_e^{vi} \forall v \in \mathcal{V}$ 
2:  $\mathcal{S}_i \leftarrow \{\Pi_{vi} \forall v \in \mathcal{V}\}, \mathcal{V}_h \leftarrow \{\Pi_{vi} \in \mathcal{S}_i : b_{vi} = 1\}, \mathcal{V}_l \leftarrow \{\Pi_{vi} \in \mathcal{S}_i : b_{vi} = 0\}, \Gamma_{\Pi_{vi}} \leftarrow b_{vi} \forall \Pi_{vi} \in \mathcal{S}_i$ 
3:  $S_a(P_i) \leftarrow S_a(P_i) + \sum_{\bar{v}: \Pi_{\bar{v}} \in \mathcal{V}_h} (\gamma_{\bar{v}i})$ 
4: for all  $\Pi_{vi} \in \mathcal{V}_l$  do
5:   if  $g_i > 0$  then
6:     collaboratively compare  $P_i + r_v$  and  $g_i$ 
7:     if  $P_i + r_v < g_i$  then
8:        $S_a(P_i) \leftarrow S_a(P_i) + S_a(\gamma_{vi}), \Gamma_{\Pi_{vi}} \leftarrow 1$  {The grid provides enough energy to recharge  $v$ }
9:     else
10:      collaboratively compare  $P_i$  and  $g_i$ 
11:      if  $P_i > g_i$  then
12:         $S_a(P_i) \leftarrow S_a(P_i) - S_a(\gamma_{vi}), \Gamma_{\Pi_{vi}} \leftarrow -1$  { $v$  is discharged to reduce the amount of energy taken from the grid}
13:      end if
14:    end if
15:   else
16:     collaboratively compare  $P_i - r_v$  and  $g_i$ 
17:     if  $P_i - r_v > g_i$  then
18:        $S_a(P_i) \leftarrow S_a(P_i) - S_a(\gamma_{vi}), \Gamma_{\Pi_{vi}} \leftarrow -1$  { $v$  is discharged to inject energy from the battery to the grid}
19:     else
20:      collaboratively compare  $P_i$  and  $g_i$ 
21:      if  $P_i < g_i$  then
22:         $S_a(P_i) \leftarrow S_a(P_i) + S_a(\gamma_{vi}), \Gamma_{\Pi_{vi}} \leftarrow 1$  { $v$  is charged to reduce the excessive amount of energy provided by the batteries to the grid}
23:      end if
24:    end if
25:   end if
26: end for

```

Initially, a designated Aggregator \bar{a} sets P_i to 0, divides it in shares and distributes the shares $S_a(P_i)$ to the Aggregators. Once all the pseudonymized messages from every EV have been received by the Aggregators, each Aggregator a decrypts the incoming messages using its private key K_d^a and retrieves the triple $b_{vi}, S_a(r_v), K_e^{vi}$ for each Vehicle v , then it operates according to Algorithm 1 as follows:

- (1) It groups the EVs' pseudonyms in two sets \mathcal{V}_h and \mathcal{V}_l . The former set includes all the pseudonyms associated to Vehicles with $b_{vi} = 1$ which do not allow battery discharge, while all the other pseudonyms are grouped in \mathcal{V}_l . Note that the Vehicles whose pseudonyms are in \mathcal{V}_h are considered to have high charge priority, meaning that they will always be scheduled for recharge, regardless to the energy availability of the grid. Conversely, the Vehicles belonging to \mathcal{V}_l can be either charged/discharged or not, in order to meet the grid power offer/demand.

- (2) The recharge of each Vehicle with pseudonym $\Pi_{vi} \in \mathcal{V}_h$ is scheduled for the epoch i by setting $\Gamma_{\Pi_{vi}}$ to 1 and the total power amount P_i is updated by adding the corresponding share $S_a(\gamma_{vi})$. Note that the additions are performed directly on the shares, therefore the Aggregator operates without knowing the values γ_{vi} . In case $\gamma_{vi} = 0$, *i.e.*, v is not available for recharge/discharge, adding $S_a(\gamma_{vi})$ to $S_a(P_i)$ does not alter the current values of P_i .
- (3) For each Vehicle associated to a pseudonym $\Pi_{vi} \in \mathcal{V}_l$, if $g_i > 0$ (*i.e.*, the grid has a power surplus which can be used to recharge the batteries), the Aggregators collaboratively compare $P_i + \gamma_{vi}$ and g_i by means of the comparison protocol presented in [30]. Without loss of generality, we assume that the Aggregator \bar{a} is elected as responsible of defining the order of service of the vehicles in \mathcal{V}_l (which is randomly chosen at every epoch) and to communicate it to the other Aggregators. If the current power amount (including the recharge of v) does not exceed g_i , v is scheduled for recharge, otherwise a second collaborative comparison between P_i and g_i is performed: if P_i exceeds g_i (meaning that the current energy used to serve the Vehicles exceeds the grid's power availability), the discharge of v is scheduled, otherwise no charge/discharge takes place. Analogously, for $g_i < 0$, $P_i - \gamma_{vi}$ and g_i are collaboratively compared and in case $P_i - r_v$ exceeds g_i , the discharge of the battery of v is scheduled in order to reduce the amount of energy used for recharging, otherwise the Aggregators compare again P_i to g_i and if $P_i < g_i$ (*i.e.*, the total discharged energy exceeds the grid's needs), v is recharged. Conversely, in case $P_i \geq g_i$, no action is scheduled.

Once the scheduling procedure is concluded, \bar{a} sends to the Anonymizer the scheduling output $E_{K_e^{vi}}(\Gamma_{\Pi_{vi}})$ encrypted under the ephemeral encryption key of Vehicle v and the corresponding pseudonym Π_{vi} . The Anonymizer retrieves the identity ID_v of the Vehicle associated to Π_{vi} , forwards $E_{K_e^{vi}}(\Gamma_{\Pi_{vi}})$ to v , which obtains $\Gamma_{\Pi_{vi}}$ by decrypting the message with its private ephemeral key K_d^{vi} and schedules its battery charge/discharge accordingly.

5. Security Discussion

In this Section we discuss the adversarial model, state definitions of the privacy properties of our scheduling mechanism and provide proofs that such properties are guaranteed by our framework.

We assume that each Aggregator behave according to the *honest-but-curious* attacker model, meaning that it honestly executes the scheduling algorithm, but tries to obtain further information about the current battery levels of the EVs and the amount of refilled energy by performing arbitrary elaborations on the messages they receive, possibly colluding with other Aggregators (but not with the Anonymizer). The Anonymizer is also supposed to be *honest-but-curious*. Conversely, the EVs are assumed to be honest nodes.

We now define the property of **blindness**, which the proposed infrastructure satisfies.

Definition 1. *The scheduling infrastructure provides **blindness** if during any set of epochs \mathcal{I} a collusion of $\tilde{\mathcal{A}}$ Aggregators of cardinality $c < |\mathcal{A}|$ cannot relate b_{vi} to the identity ID_v of the Vehicle which generated it during any set of epochs \mathcal{I} and obtains no additional information with respect to what is implied by the knowledge of $(S_a(\gamma_{vi}), b_{vi})$ for each Aggregator $a \in \tilde{\mathcal{A}}$.*

More formally, we define the `Blind` experiment, involving a challenger \mathcal{C} controlling the Anonymizer node and a probabilistic polynomial-time adversary \mathcal{D} controlling the set of colluded Aggregators $\tilde{\mathcal{A}}$: $|\tilde{\mathcal{A}}| < \mathcal{A}$:

- (1) \mathcal{D} selects four sets of Vehicles $\mathcal{V}_0^h, \mathcal{V}_0^l, \mathcal{V}_1^h, \mathcal{V}_1^l \subseteq \mathcal{V}$: $b_{vi} = 1 \forall i \in \mathcal{I}, v \in \mathcal{V}_0^h, \mathcal{V}_1^h \wedge b_{vi} = 0 \forall i \in \mathcal{I}, v \in \mathcal{V}_0^l, \mathcal{V}_1^l \wedge |\mathcal{V}_0^h| = |\mathcal{V}_1^h| \wedge |\mathcal{V}_0^l| = |\mathcal{V}_1^l|$, the identifiers ID_v , the values γ_{vi} and the random numbers $\rho_1, \rho_2, \dots, \rho_{t-1}$ to be used to divide each γ_{vi} in shares for each Vehicle in $\mathcal{V}_0^h, \mathcal{V}_0^l, \mathcal{V}_1^h, \mathcal{V}_1^l$, and communicates them to \mathcal{C} .
- (2) \mathcal{C} selects a random bit $\bar{b} = \{0, 1\}$, generates the pseudonyms Π_{vi} and the shares $S_a(\gamma_{vi}) \forall i \in \mathcal{I}, a \in \tilde{\mathcal{A}}, v \in \mathcal{V}_{\bar{b}}^h, \mathcal{V}_{\bar{b}}^l$ and communicates them to \mathcal{D} .
- (3) \mathcal{D} outputs a bit \bar{b}' .

The architecture provides $|\mathcal{A}|$ -**blindness** if:

$$P(\bar{b}' = \bar{b} \mid \Pi_{vi}, S_a(\gamma_{vi}) \forall i \in \mathcal{I}, a \in \tilde{\mathcal{A}}, v \in \mathcal{V}_{\bar{b}}^h, \mathcal{V}_{\bar{b}}^l) = P(\bar{b}' = \bar{b}) = \frac{1}{2}$$

The proof that our proposed infrastructure is **blind** descends from the property of *perfect secrecy* of the SSS scheme [36] and can be constructed by straightforwardly extending the one provided in ([37], Theorem 3) for two sets of shares to a scenario with $|\mathcal{I}|(|\mathcal{V}_l| + |\mathcal{V}_h|)$ sets of shares. The theorem proves that, given two secrets m_0, m_1 , two sets of their shares $\mathcal{S}_0, \mathcal{S}_1$ of cardinality $t - 1$ and a random bit $\bar{b} \in \{0, 1\}$, the probability that an adversary provided with $m_{\bar{b}}, \mathcal{S}_0, \mathcal{S}_1$ can guess the correct value of \bar{b} is $1/2$.

Thus, it follows that:

$$P(\bar{b}' = \bar{b} \mid S_a(\gamma_{vi}) \forall i \in \mathcal{I}, a \in \tilde{\mathcal{A}}, v \in \mathcal{V}_{\bar{b}}^h, \mathcal{V}_{\bar{b}}^l) = P(\bar{b}' = \bar{b}) = \frac{1}{2}$$

The proof is completed by noting that the pseudonyms Π_{vi} are random numbers refreshed at every epoch, therefore the knowledge of Π_{vi} does not provide any advantage to \mathcal{D} : in particular, from the point of view of the collusion $\tilde{\mathcal{A}}$, if $b_{vi} = 1$ no Vehicle \bar{v} appears to be more likely to be the sender of b_{vi} than any other Vehicle $v \in \mathcal{V}_{\bar{b}}^h$. Analogously, if $b_{vi} = 0$, all the Vehicles in $\mathcal{V}_{\bar{b}}^l$ are equally likely to have generated b_{vi} . It follows that the collusion $\tilde{\mathcal{A}}$ obtains no information to reconstruct the succession of b_{vi} generated by a given Vehicle \bar{v} during the succession of epochs \mathcal{I} .

Definition 2. *The scheduling architecture is **oblivious** if the Anonymizer has no knowledge of the priority bit b_{vi} , the values γ_{vi} and the scheduling outputs $\Gamma_{\Pi_{vi}}$ in any epoch i .*

To formalize this property, we define the `Oblivious` experiment, which involves a challenger \mathcal{C} controlling the set of Aggregators and an adversary \mathcal{D} controlling the Anonymizer:

- (1) \mathcal{D} selects two Vehicles $v_0, v_1 \in \mathcal{V}$ and communicates to \mathcal{C} the priority bits b_{v_0i}, b_{v_1i} , the values $\gamma_{v_0i}, \gamma_{v_1i}$, and the random numbers $\rho_1, \rho_2, \dots, \rho_{t-1}$ to be used to divide $\gamma_{v_0i}, \gamma_{v_1i}$ in shares.
- (2) \mathcal{C} selects a random bit $\bar{b} = \{0, 1\}$, generates $E_{K_e^a}(b_{v_{\bar{b}}i} || S_a(\gamma_{v_{\bar{b}}i}) || K_e^{v_{\bar{b}}i}) \forall a \in \mathcal{A}$ and the encrypted scheduling output $E_{K_e^{v_{\bar{b}}i}}(o_{\Pi_{v_{\bar{b}}i}})$, and communicates them to \mathcal{D} .
- (3) \mathcal{D} outputs a bit \bar{b}' .

The architecture provides **obliviousness** if:

$$P(\bar{b}' = \bar{b} \mid E_{K_e}(b_{v\bar{b}i} \parallel S_a(\gamma_{v\bar{b}i}) \parallel K_e^{v\bar{b}i}) \forall a \in \mathcal{A}, E_{K_e^{v\bar{b}i}}(o_{\Pi_{v\bar{b}i}})) = P(\bar{b}' = \bar{b}) = \frac{1}{2}$$

Assuming that the cryptosystem $E(K_e, \cdot)$ ensures *message indistinguishability* (see Section 4), the property can be proved by contradiction: let us suppose that the adversary \mathcal{D} has more than negligible advantage in the Oblivious experiment. Since in Oblivious the adversary \mathcal{D} arbitrarily chooses the plaintext data and all the parameters of the SSS scheme, Oblivious is constructed analogously to the IND-CPA experiment [34]. Therefore, if \mathcal{D} has more than negligible advantage over randomness to guess \bar{b} in the Oblivious experiment, it also has a non-negligible advantage in the IND-CPA experiment, which violates the assumption of message indistinguishability under chosen plaintext.

Finally, it is worth discussing the correctness of our privacy-friendly scheduling protocol: at the end of the scheduling procedure, it results $S_a(P_i) = \sum_{\Pi_{vi} \in \mathcal{S}_i} \Gamma_{\Pi_{vi}} \cdot S_a(\gamma_{vi})$. Therefore, the overall energy usage reconstructed by means of the secret recovery procedure would be $P_i = \sum_{\Pi_{vi} \in \mathcal{S}_i} \Gamma_{\Pi_{vi}} \cdot \gamma_{vi}$. Since the value of $\Gamma_{\Pi_{vi}}$ is set based on the result of the comparison protocol presented in [30], which has been therein proved to be correct, it follows that the output of the privacy-friendly scheduling algorithm is the same that would be obtained by operating directly on the plaintexts.

6. Benchmark ILP Model

We now introduce an Integer Linear Programming formulation which finds the optimal battery charge/discharge schedule. Such model should be considered as an ideal benchmark, since it relies on future knowledge about the periods in which EVs are plugged in, the current battery level and the amount of energy to be refilled, which would impose great limitations to its applicability to a real scenario (e.g., by requiring the users to declare in advance their traveling periods for the next day).

Sets

- \mathcal{P} : set of recharge periods of the EVs (each vehicle $v \in \mathcal{V}$ has at least one recharge period within the optimization time span)
- \mathcal{I} : set of discretized epochs within the optimization time span

Parameters

- e_p : maximum amount of power to be provided during the recharge period p (given by the difference between the battery maximum capacity and the initial battery charge level l_v of the Vehicle v having the p -th recharge period)
- a_p : minimum amount of power to be provided during the recharge period p ($a_p = t_v - l_v$ if $l_v < t_v$, 0 otherwise)
- r_p : battery charge rate (per epoch) of the vehicle v having the p -th recharge period
- k_{pi} : it is 1 if epoch i belongs to the p -th recharge period, 0 otherwise
- g_i : maximum grid power supply (if $g_i > 0$) or demand (if $g_i < 0$) at epoch i
- u_i^+ : boolean indicator, it is 1 if $g_i \geq 0$, 0 otherwise
- u_i^- : boolean indicator, it is 1 if $g_i < 0$, 0 otherwise
- M : positive value, such as $M \gg \max_{i \in \mathcal{I}} |g_i|$

Variables

- x_{pi} : integer variable ($-1 \leq x_{pi} \leq 1$), it is 1(−1) if the battery of the vehicle associated to the p -th recharge period is recharged(discharged) at epoch i , 0 otherwise
- δ : indicates the minimum ratio of the power utilized (provided) for battery recharge (discharge), to the power supplied/requested by the grid

Objective function

$$\max \delta \quad (1)$$

Constraints

$$\sum_{i \in \mathcal{I}} k_{pi} r_p x_{pi} \leq e_p \quad \forall p \in \mathcal{P} \quad (2)$$

$$\sum_{i \in \mathcal{I}} k_{pi} r_p x_{pi} \geq a_p \quad \forall p \in \mathcal{P} \quad (3)$$

$$\sum_{p \in \mathcal{P}} k_{pi} r_p x_{pi} \leq g_i + M u_i^- \quad \forall i \in \mathcal{I} \quad (4)$$

$$\sum_{p \in \mathcal{P}} k_{pi} r_p x_{pi} \geq g_i - M u_i^+ \quad \forall i \in \mathcal{I} \quad (5)$$

$$\delta \leq \frac{\sum_{p \in \mathcal{P}} k_{pi} r_p x_{pi}}{g_i} \quad \forall i \in \mathcal{I} \quad (6)$$

The objective function maximizes the minimum ratio of the power requested by the aggregator to recharge the vehicles' batteries (or obtained by the aggregator by discharging them) to the power requested/offered by the grid. Constraints 2 and 3 limit the minimum/maximum amount of energy to be charged during each recharge period, while Constraints 4 and 5 avoid recharging batteries with more energy than the grid can provide or injecting excessive energy into the grid by discharging batteries during the periods of shortages. Finally, Constraints 6 set δ to the minimum normalized amount of scheduled power absorption/supply.

7. Performance Evaluation

We now evaluate our proposed scheduling mechanism in terms of computational complexity, message number and length, and compare its performance to the optimal results obtained by means of the ILP formulation presented in Section 6. Our implementation assumes a 256 bit-long modulo q for the SSS scheme and IDs/pseudonyms of 32 bits. The hybrid cryptosystem used for the share encryption is the RSA-KEM Key Transport Algorithm [38], which uses the RSA public key cryptosystem with modulo n of 1024 bits, the KDF2 key derivation function (based on SHA-1) and the AES-Wrap-128 key-wrapping scheme to communicate an ephemeral 128-bit-long key used to encrypt the samples $V(i)$ by means of the standard AES scheme operating in Cipher Block Chaining mode (CBC). The scheduling output destined to the EVs is assumed to be encrypted with the standard RSA public key cryptosystem.

7.1. Computational Complexity

We start evaluating the asymptotic number of incoming/outgoing messages at each node. As showed in Table 2, the number of messages exchanged by the Vehicles exhibits a linear dependence on the number of shares $|\mathcal{A}|$, while for the Anonymizer it depends linearly on both $|\mathcal{A}|$ and the number of EVs $|\mathcal{V}|$. Finally, for the Aggregators the dependence is linear in $|\mathcal{V}|$ and superlinear in $|\mathcal{A}|$ (due to the collaborative comparison procedure discussed in [30]).

Table 2. Asymptotic complexity in terms of incoming/outgoing messages per node for the scheduling of a single service request.

Node	Input	Output
Vehicle	$O(1)$	$O(\mathcal{A})$
Anonymizer	$O(\mathcal{A} \cdot \mathcal{V})$	$O(\mathcal{A} \cdot \mathcal{V})$
Aggregator	$O(\mathcal{A} ^2 \log_2 \mathcal{A} \cdot \mathcal{V})$	$O(\mathcal{A} ^2 \log_2 \mathcal{A} \cdot \mathcal{V})$

Table 3 reports the operations performed by each node for the scheduling of a single battery recharge. The computational cost of each operation is detailed in Table 4 based on [28,30]. The most demanding procedure is the share collaborative comparison performed by the Aggregators in multiple rounds depending on $|\mathcal{A}|$.

Table 3. Computational load at each node for the scheduling of a single service request.

Vehicle	1 random number generation modulo $n + \tilde{V}C_s(q) + \mathcal{A} C_e^{RSA-KEM}(n, 11) + C_d^{RSA}(n)$
Anonymizer	1 random number generation modulo 2^{32}
Aggregator	$C_d^{RSA-KEM}(n, 11) + 2C_c(q) + c_a(q) + C_e^{RSA}(n)$ (worst case)

see Table 4 for the cost details.

Finally, it is worth discussing the message length: each service request generated by an EV and forwarded by the Anonymizer consists on a 32 bit-long ID/pseudonym and a RSA-KEM encrypted message of 2624 bits, for a total length of 2656 bits. During the share comparison procedure, each share is in turn divided in $|\mathcal{A}|$ shares and redistributed among the Aggregators. In a worst case scenario in which all the EVs have low priority, each Aggregator sends/receives at most $|\mathcal{V}| \cdot |\mathcal{A}| \cdot (|\mathcal{A}| - 1)$ messages of 256 bits each (see [30] for further details) per comparison round (note that the number of rounds exhibits a logarithmic dependency on $|\mathcal{A}|$). Ultimately, the scheduling output for each EV Γ_{vi} is encrypted and forwarded to the Anonymizer together with the respective pseudonym, thus requiring $|\mathcal{V}|$ messages of $32 + 1024 = 1056$ bits each. In a scenario with $|\mathcal{A}| = 4$ and $|\mathcal{V}| = 1000$ the throughput per scheduling epoch experienced by each Aggregator would be approximately (worst case) 8.6 Mbit/epoch, of which 4.9 Mbit/epoch are due to the inter-Aggregators communications and 3.7 Mbit/epoch are due to the EVs-to-Aggregators communications). It follows that the inter-Aggregators communication burden, which would be avoided in case of a single scheduling entity directly accessing the raw data generated by the EVs, is an additional communication cost required by the privacy-preserving

approach. Such throughput values are compatible with state-of-the art communication technologies for V2G infrastructures.

Table 4. Detail of operation costs.

$C_s(x)$	cost of the generation of $ \mathcal{A} $ shares modulo x	$ \mathcal{A} (\mathcal{A} - 1)$ additions modulo x $ \mathcal{A} (\mathcal{A} - 1)$ multiplications modulo x $(\mathcal{A} - 1)$ random number generations modulo x
$C_a(x)$	cost of a share addition modulo x	1 addition modulo x
$C_l(x)$	cost of a share Lagrange interpolation modulo x	$O(\mathcal{A} ^2)$ multiplications modulo x
$C_m(x)$	cost of a share collaborative multiplication modulo x	$C_s(x) + (\mathcal{A} - 1)C_a(x) + 2$ multiplications modulo x , performed in 2 rounds
$C_c(x)$	cost of a collaborative comparison modulo x	2 random number generation modulo x + 1 random number generation modulo 2 2 exponentiations modulo q + 2 multiplications modulo x $2C_s(x) + (\mathcal{A} + 1)C_a(x) + O(\mathcal{A})C_m(x) + C_l(x)$, performed in $\lceil \log_2 \mathcal{A} \rceil$ rounds
$C_e^{RSA}(x)$	cost of an RSA encryption modulo x	1 exponentiation modulo x
$C_d^{RSA}(x)$	cost of an RSA decryption modulo x	1 exponentiation modulo x
$C_e^{RSA-KEM}(x, l)$	cost of an RSA-KEM encryption with RSA modulo x and AES encryption of a message of l blocks	1 random number generation modulo $x + C_e^{RSA}(x)$ 1 KDF2 key derivation and AES-Wrap-128 key wrapping l AES encryptions
$C_d^{RSA-KEM}(x, l)$	cost of an RSA-KEM decryption with RSA modulo x and AES decryption of a message of l blocks	$C_d^{RSA}(x)$ 1 KDF2 key derivation and AES-Wrap-128 key unwrapping l AES decryptions

7.2. Numerical Results

We compare the scheduling results obtained by our proposed protocol to the ILP benchmark model. We consider a scenario of a residential area of 1000 houses with peak power consumption of 3 kW [39], a windfarm (peak production of 8 MW [40]) and 1000 EVs (battery maximum capacity between 12.75 and 17 kWh, charging rate of 0.75 or 1 kW [14], minimum recharge threshold between 1.5 and 2 kWh). The behavior of each Vehicle v is modeled by means of a discrete random walk between 0 and 1 with state transition probability of 0.25. For each epoch, state 0 is mapped to $k_{vi} = 0$, while state 1 sets $k_{vi} = r_v$.

Note that, since the ILP model does not take into account the energy price, such price is assumed to be constant within the whole optimization time span and does not play any role in the scheduling strategy in both the optimal and the privacy-friendly approaches.

Results averaged over 365 days (each day is divided in 96 epochs of 15 min duration, see Figure 3 for an example of daily schedule) show that the running time of the privacy-friendly approach is significantly lower than the one of the ILP model (seconds vs. hours, see Table 5). The minimum power consumption-to-power availability ratio provided by our algorithm is on average lower than the optimal one, which is due to the fact that, in case g_i is negative, the privacy-friendly approach always schedules the recharge of high priority EVs, while the ILP model might postpone it according to the knowledge of their future traveling behavior. However, the degree of similarity (expressed in terms of Mean Square Error) between the curve of the grid power supply/request and the curve of the scheduled energy usage is not significantly worsened w.r.t. the optimal solution provided by the ILP formulation (only 0.2% increase, as reported in Table 5).

Figure 3. Comparison of optimal vs. privacy-friendly scheduled battery charges/discharges. Positive values indicate that the grid provides power to recharge the EVs’ batteries, while negative values indicate that power provided by the batteries is injected into the grid.

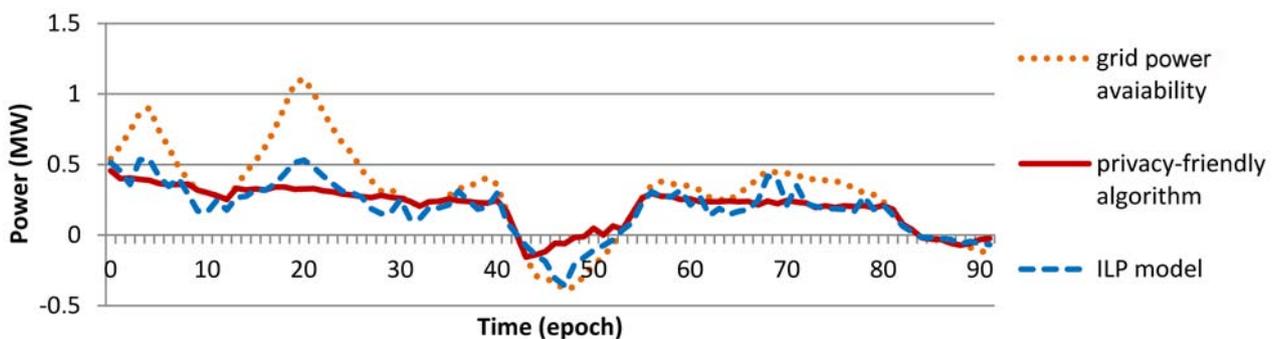


Table 5. Comparison of the performance of ILP vs. privacy-friendly scheduling.

Privacy-friendly S.					ILP				
Average	Max	Min	Aver. MSE	Time	Average	Max	Min	Aver. MSE	Time
-6.64	0.11	-167.98	4.72×10^{12}	0.6 s	0.03	0.48	-0.38	4.71×10^{12}	4 h

8. Conclusions

This paper proposes a privacy-preserving Vehicle-to-Grid communication infrastructure which schedules the battery charge/discharge times of electric vehicles without exposing the users’ traveling habits, the current battery level nor the amount of refilled energy. Performance in terms of computational times and gap w.r.t. the optimal schedule obtained by means of an Integer Linear Program shows the viability of the proposed privacy-friendly approach, which provides results not significantly dissimilar w.r.t. the optimal ones.

Acknowledgments

The authors thank Valeria Olivieri for her precious suggestions.

Author Contributions

Cristina Rottondi and Giacomo Verticale jointly designed the privacy preserving framework. Cristina Rottondi designed the associated protocol and the benchmark Integer Linear Program. The security assessment of the proposed infrastructure has been provided by Giacomo Verticale. Both the privacy-friendly protocol and the ILP model have been implemented and tested by Simone Fontana

Conflicts of Interest

The authors declare no conflicts of interest.

References

1. Chan, C.; Bouscayrol, A.; Chen, K. Electric, hybrid, and fuel-cell vehicles: Architectures and modeling. *IEEE Trans. Veh. Technol.* **2010**, *59*, 589–598.
2. Offer, G.; Howey, D.; Contestabile, M.; Clague, R.; Brandon, N. Comparative analysis of battery electric, hydrogen fuel cell and hybrid vehicles in a future sustainable road transport system. *Energy Policy* **2010**, *38*, 24–29.
3. Pieltain Fernandez, L.; Roman, T.; Cossent, R.; Domingo, C.; Frias, P. Assessment of the impact of plug-in electric vehicles on distribution networks. *IEEE Trans. Power Syst.* **2011**, *26*, 206–213.
4. Lopes, J.; Soares, F.; Almeida, P. Integration of electric vehicles in the electric power system. *IEEE Proc.* **2011**, *99*, 168–183.
5. Markel, T.; Kuss, M.; Denholm, P. Communication and control of electric drive vehicles supporting renewables. In Proceedings of the IEEE Vehicle Power and Propulsion Conference (VPPC '09), Dearborn, MI, USA, 7–10 September 2009; pp. 27–34.
6. Ekman, C.K. On the synergy between large electric vehicle fleet and high wind penetration—An analysis of the Danish case. *Renew. Energy* **2011**, *36*, 546–553.
7. Kempton, W.; Tomic, J.; Letendre, S.; Brooks, A.; Lipman, T. *Vehicle-to-Grid Power: Battery, Hybrid, and Fuel Cell Vehicles as Resources for Distributed Electric Power in California*; Working Paper Series ECD-ITS-Rr-1-03; Institute of Transportation Studies, University of California, Davis: Davis, CA, USA, 2001.
8. Brooks, A. Integration of electric drive vehicles with the power grid—a new application for vehicle batteries. In Proceedings of the Seventeenth Annual Battery Conference on Applications and Advances, Long Beach, CA, USA, 15–18 January 2002; pp. 239–254.
9. Kempton, W.; Marra, F.; Andersen, P.; Garcia-Valle, R. Business models and control and management architectures for EV electrical grid integration. In *Electric Vehicle Integration into Modern Power Networks*; Garcia-Valle, R., Peagas Lopes, J.A., Eds.; Power Electronics and Power Systems; Springer New York: New York, NY, USA, 2013; pp. 87–105.

10. Brooks, A. *Vehicle-to-Grid Demonstration Project: Grid Regulation Ancillary Service with a Battery Electric Vehicle*; Research Report to CARB; AC Propulsion: San Dimas, CA, USA, 2002.
11. Hoh, B.; Gruteser, M.; Xiong, H.; Alrabady, A. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Comput.* **2006**, *5*, 38–46.
12. Liao, L.; Patterson, D.J.; Fox, D.; Kautz, H. Learning and inferring transportation routines. *Artif. Intell.* **2007**, *171*, 311–331.
13. National Institute of Standards and Technology, The Smart Grid Interoperability Panel, Smart Grid Cybersecurity Committee. Guidelines for Smart Grid Cybersecurity: Volume 2, Privacy and the Smart Grid, Draft NISTIR 7628 Revision 1, 2013. Available online: <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628r1> (accessed on 1 January 2014).
14. Liu, R.; Dow, L.; Liu, E. A survey of PEV impacts on electric utilities. In Proceedings of the 2011 IEEE PES Innovative Smart Grid Technologies (ISGT), Hilton Anaheim, CA, USA, 17–19 January 2011; pp. 1–8.
15. Bessa, R.J.; Matos, M.A. Economic and technical management of an aggregation agent for electric vehicles: A literature survey. *Eur. Trans. Electr. Power* **2012**, *22*, 334–350.
16. Han, Y.; Chen, Y.; Han, F.; Liu, K. An optimal dynamic pricing and schedule approach in V2G. In Proceedings of the 2012 Asia-Pacific Signal Information Processing Association Annual Summit and Conference (APSIPA ASC), Hollywood, CA, USA, 3–6 December 2012; pp. 1–8.
17. Zou, S.; Ma, Z.; Liu, X. Distributed efficient charging coordinations for electric vehicles under progressive second price auction mechanism. In Proceedings of the 52nd IEEE Conference on Decision and Control (CDC), Firenze, Italy, 10–13 December 2013; pp. 550–555.
18. Li, G.; Zhang, X.P. Modeling of plug-in hybrid electric vehicle charging demand in probabilistic power flow calculations. *IEEE Trans. Smart Grid* **2012**, *3*, 492–499.
19. Alizadeh, M.; Scaglione, A.; Davies, J.; Kurani, K. A scalable stochastic model for the electricity demand of electric and plug-in hybrid vehicles. *IEEE Trans. Smart Grid* **2013**, *PP*, 1–13.
20. Di Giorgio, A.; Liberati, F.; Pietrabissa, A. On-board stochastic control of Electric Vehicle recharging. In Proceedings of the 52nd IEEE Conference on Decision and Control (CDC), Firenze, Italy, 10–13 December 2013; pp. 5710–5715.
21. Khayyam, H.; Abawajy, J.; Javadi, B.; Goscinski, A.; Stojcevski, A.; Bab-Hadiashar, A. Intelligent battery energy management and control for vehicle-to-grid via cloud computing network. *Appl. Energy* **2013**, *111*, 971–981.
22. Stegelmann, M.; Kesdogan, D. Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction. In *Public Key Infrastructures, Services and Applications*; Petkova-Nikova, S., Pashalidis, A., Pernul, G., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7163, pp. 75–90.
23. Stegelmann, M.; Kesdogan, D. Location privacy for vehicle-to-grid interaction through battery management. In Proceedings of the Ninth International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, USA, 16–18 April 2012; pp. 373–378.
24. Yang, Z.; Yu, S.; Lou, W.; Liu, C. P^2 : Privacy-preserving communication and precise reward architecture for V2G networks in smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 697–706.

25. Liu, J.; Au, M.; Susilo, W.; Zhou, J. Enhancing location privacy for electric vehicles (at the right time). In *Computer Security—ESORICS 2012*; Foresti, S., Yung, M., Martinelli, F., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7459, pp. 397–414.
26. Nicanfar, H.; Hosseini-zhad, S.; TalebiFard, P.; Leung, V.C.M. Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations. In *Proceedings of the IEEE INFOCOM, Turin, Italy, 14–19 April 2013*; pp. 3429–3434.
27. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613.
28. Bogdanov, D. *Foundations and Properties of Shamir's Secret Sharing Scheme, Research Seminar in Cryptography*; Institute of Computer Science, University of Tartu: Tartu, Estonia, 2007.
29. Nishide, T.; Ohta, K. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol. In *Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC '07)*, Beijing, China, 16–20 April 2007; Springer-Verlag: Berlin/Heidelberg, Germany, 2007; pp. 343–360.
30. Kerschbaum, F.; Biswas, D.; de Hoogh, S. Performance comparison of secure comparison protocols. In *Proceedings of the 20th International Workshop on Database and Expert Systems Application (DEXA '09)*, Linz, Austria, 31 August–4 September 2009; pp. 133–136.
31. Bychkovsky, V.; Hull, B.; Miu, A.; Balakrishnan, H.; Madden, S. A measurement study of vehicular internet access using *in situ* Wi-Fi networks. In *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom '06)*, Los Angeles, CA, USA, 24–29 September 2006; ACM: New York, NY, USA, 2006; pp. 50–61.
32. Pinart, C.; Sanz, P.; Lequerica, I.; García, D.; Barona, I.; Sánchez-Aparisi, D. DRIVE: A reconfigurable testbed for advanced vehicular services and communications. In *Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TridentCom '08)*, Innsbruck, Austria, 18–20 March 2008; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2008; pp. 16:1–16:8.
33. Bissmeyer, N.; Stubing, H.; Schoch, E.; Gotz, S.; Stotz, J.P.; Lonc, B. A generic public key infrastructure for securing Car-to-X communication. In *Proceedings of the 18th World Congress on Intelligent Transport Systems featuring ITS America's Annual Meeting and Exposition*, Orlando, FL, USA, 16–20 October 2011.
34. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*; Chapman & Hall/CRC: Boca Raton, FL, USA, 2007.
35. Rottondi, C.; Verticale, G.; Capone, A. Privacy-preserving smart metering with multiple data Consumers. *Comput. Netw.* **2013**, *57*, 1699–1713.
36. Stinson, D. *Cryptography Theory and Practice*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2005.
37. Rottondi, C.; Mauri, G.; Verticale, G. A protocol for metering data pseudonymization in smart grids. *Trans. Emerg. Telecommun. Technol.* **2013**, doi:10.1002/ett.2760.

38. Randall, J.; Kaliski, B.; Brainard, J.; Turner, S. *Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS)*; RFC 5990; RFC, Ed.; The Internet Engineering Task Force: Fremont, CA, USA, 2010.
39. Barker, S.; Mishra, A.; Irwin, D.; Cecchet, E.; Shenoy, P.; Albrecht, J. Smart*: An Open Data Set and Tools for Enabling Research in Sustainable Homes. In Proceedings of the 1st KDD Workshop on Data Mining Applications in Sustainability (SustKDD), Beijing, China, 12 August 2012.
40. Hong, T.; Pinson, P.; Fan, S. Global energy forecasting competition 2012. *Int. J. Forecast.* **2014**, *30*, 357–363.

© 2014 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).