Roaming Electric Vehicle Charging and Billing: an Anonymous Multi-User Protocol

DOI:
10.1109/SmartGridComm.2014.7007769

Document Version
Accepted author manuscript

Roaming Electric Vehicle Charging and Billing: an Anonymous Multi-User Protocol

Mustafa A. Mustafa and Ning Zhang
School of Computer Science
The University of Manchester
Oxford Road, Manchester, M13 9PL, UK
Email: {mustafm, nzhang}@cs.man.ac.uk

Georgios Kalogridis and Zhong Fan
Toshiba Research Europe Limited
Telecommunications Research Laboratory
32 Queen Square, Bristol, BS1 4ND, UK
Email: {george, zhong.fan}@toshiba-trel.com

***Abstract*—In this paper, we propose a secure roaming electric vehicle (EV) charging protocol that helps preserve users' privacy. During a charging session, a roaming EV user uses a pseudonym of the EV (known only to the user's contracted supplier) which is anonymously signed by the user's private key. This protocol protects the user's identity privacy from other suppliers as well as the user's privacy of location from its own supplier. Further, it allows the user's contracted supplier to authenticate the EV and the user. Using two-factor authentication approach a multi-user EV charging is supported and different legitimate EV users (e.g. family members) can be held accountable for their charging sessions. With each charging session, the EV uses a different pseudonym which prevents adversaries from linking the different charging sessions of the EV. On an application level, our protocol supports fair user billing, i.e. each user pays only for his/her own energy consumption, and an open EV marketplace in which EV users can safely choose among different remote host suppliers.**

I. Introduction

A Smart Grid (SG) is envisioned as the next generation electrical grid that can support two-way power and communication flows between different entities in the grid [1]. The purpose for using the SG is to make the grid (i.e. the available power resource management) more efficient, reliable and resilient.

Electric Vehicles (EVs) are recognised as a key element in the realization of the SG vision due to the fact that their batteries can potentially be used as a flexible and remote electricity storage. Although the battery technology has improved in recent years, the current EVs still have a limited battery capacity, which leads to the need for frequent chargings. As the locations of vehicles usually indicate the whereabouts of their users, the footprints left by EV chargings can be used by various entities, e.g. charging stations, for profiling users' EV usage and locations, thus breaching their privacy [2]–[4]. This rises the case for protecting EV users' privacy while supporting them to roam and charge their vehicles.

Existing privacy-preserving solutions in this context [5]–[14] rely on the use of a trusted third party (TTP) to protect EV users' privacy against charging stations. However, in these solutions, the TTP will know the exact locations and IDs of all the EVs. Moreover, these solutions do not support roaming EV charging or multi-user billing. Also when charging at a host location, depending on the amount of electricity generated from the host's Renewable Energy Source (RES) during the charging session, the roaming EV may get electricity supplied by the RES, by the grid, or by both RES and the grid (if RES has some stock but the stock is not sufficient for the EV's demand). Owing to these different possibilities, the payee of the payment made by the roaming EV user and the amount payable to the payee may vary. In other words, the user of a roaming EV may need to pay for the electricity to the host, to the host's supplier, or to both of them.

In this paper, we propose a novel secure roaming EV charging protocol that 1) supports multi-user utilization (i.e. fairer EV charging expenses sharing between legitimate EV users), and 2) fairer billing, for the host while protecting the privacy of both, i.e. the roaming EV user and the host.

The rest of the paper is organized as follows. Section II discusses the related work. Section III presents the design preliminaries for our solution. Our protocol is presented in Section IV, followed by its security and privacy analyses in Section V. We draw our conclusions in Section VI.

II. Related Work

Although the security and privacy issues in SG have received significant attentions in recent years [15]–[20], the issue of roaming EV charging and billing while preserving EV users' identity and location privacy has not been properly addressed. Privacy concerns in the EV charging context have been analysed in [2]–[5], but no solutions are proposed in the papers. A decentralized EV authentication solution was proposed in [6] and the same authors have also proposed a multi-domain architecture for Vehicle-to-Grid (V2G) communication using a hybrid public key infrastructure and hierarchical and peer-to-peer cross-certifications [7], but the solutions do not support roaming EV charging nor billing.

Context-aware EV authentication schemes have been proposed in [8]–[11]. The schemes can protect the confidentiality of EV charging related data, such as battery-status, charging mode (host/visitor) and roles (consumer/producer/storage), from charging stations, but no payment options are suggested as they are designed for collecting data for monitoring purposes. In [13] a secure and privacy-preserving protocol for communications in V2G networks has been proposed. The protocol utilizes the restrictive partially blind signature to protect the identities of the EV owners during a communication session. The use of a fresh pseudonym with each charging

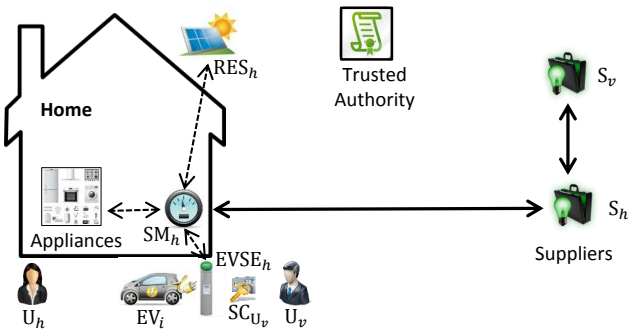

Fig. 1: The system architecture.

session was proposed in [12]. However, the scheme requires that the EV must obtain a new pseudonym from a trusted SG server before the next charging session, which could be difficult in areas where accessing such a server is difficult.

In some of the above solutions, EVs' real identities can be hidden from charging stations, but a TTP (e.g. SG server) is relied upon, so the TTP can obtain the locations and the real identities of all the EVs in the system. Moreover, the TTP authenticates only the EV or the user of the EV, but not both, thus leaving room for potential misuse of the system by dishonest users. Also, the existing proposals have not considered the case where users may recharge their EVs in locations that are not operated by their suppliers.

III. Preliminaries

This section details the system architecture, threat model, assumptions and security and privacy requirements used in the design of our solution. Table I depicts the notations.

A. System Architecture

Our system consists of the following entities (Fig. 1):

- Trusted Authority (TA): a trusted organization (e.g. an electricity market regulator) that initializes the system and certifies other entities' public keys;
- Electric Vehicle (EV): a battery-powered vehicle;
- EV Supply Equipment (EVSE): a device that connects an EV to the grid, measures the electricity used by the EV;
- User (U): a legitimate user of an EV who is responsible for paying for his/her EV charging sessions;
- Smart Card (SC): a tamper-proof hardware that stores its user's sensitive data, e.g. cryptographic keys;
- Supplier (S): a utility company that is responsible for supplying electricity to its customers (users);
- Smart Meter (SM): an advanced metering device that measures its user's electricity usage on his/her premises;
- Renewable Energy Source (RES): an electricity source (e.g. solar panel, wind turbine) located at a user's house.

B. Threat Model and Assumptions

- Users are not trustworthy. They may try to impersonate other users or modify data sent by EVs/SMs to avoid (reduce) payments for the electricity their EVs consume.
- Suppliers are honest but curious. They follow protocol specifications but may attempt to find out as much as possible information about competing suppliers' users.
- External entities are not trustworthy. They may intercept data in transit trying to access confidential data and/or alter the data in attempt to gain some financial advantages.
- EVSEs/SMs are tamper-proof and sealed. It is hard for their users to tamper with them successfully.
- Each user has a contract with a supplier, thus suppliers know their users' data used for billing purposes.
- Each supplier can securely deliver the electricity price data, $\mathrm{P_S} = \{\mathrm{P_S^{t_1}}, \ldots, \mathrm{P_S^{t_n}}\}$, to its users' SMs/EVSEs, where $\mathrm{P_S^{t_i}}$ denotes the price of electricity at timeslot t_i;
- Suppliers do not share their users' sensitive data;
- All the entities are time synchronised.

TABLE I: Notations

Symbols	Meanings
U_v, U_h	visitor (roaming EV user), host
S_v, S_h	contracted supplier of U_v, U_h
$\mathrm{SC}_{\mathrm{U}_v}$	smart card of U_v
SM_h, EVSE_h	smart meter of U_h, the EVSE of U_h
RES_h	RES located on the premises of U_h
EV_i, ID_i	ith electric vehicle, real identity of entity i
$\mathrm{PSID}_{\mathrm{EV}_{i,j}}$	jth pseudonym of the ith EV, $j = \{1, \ldots, n\}$
T_i, T_{ch}	time-stamp of entity i, EV charging duration
$\mathrm{P_S^{t_i}} \in \mathrm{P_S}$	electricity price during the ith timeslot
PK_i, SK_i	public, private key of entity i
$\mathrm{K}_{\mathrm{U}_v}$	secret key of U_v (shared between U_v and S_v)
$\mathrm{K}_{\mathrm{H}_h}$	secret key shared between SM_h and EVSE_h
Cert_i	digital certificate of entity i
C_i	ciphertext (encrypted data) generated by entity i
M_i or msg_i	message constructed by entity i
$E(\mathrm{K}, \mathrm{M})$	symmetric encryption of M with K,
$D(\mathrm{K}, \mathrm{M})$	symmetric decryption of M with K,
$Enc(\mathrm{PK}, \mathrm{M})$	asymmetric encryption of M with PK,
$Dec(\mathrm{SK}, \mathrm{M})$	asymmetric decryption of M with SK,
$\mathrm{Sig}_i(\mathrm{M})$	digital signature of entity i on M
$\mathrm{hmac_K(M)}$	keyed-hash value of M generated with K
$\mathrm{E}^{t_i}_{\mathrm{EVSE}_h}$, $\mathrm{E}^{t_i}_{\mathrm{SM}_h}$	consumption during t_i measured at EVSE_h, SM_h

C. Security and Privacy Requirements

(R1) Message authenticity: The recipient of a message should be assured that the message has not been altered during transit, is fresh and is indeed from the claimed source;

(R2) Confidentiality of users' data: Only authorized entities (the respective users and suppliers) can access users' data;

(R3) Roaming EV user's privacy preservation
  a) EV identity privacy: the identity of a roaming EV should only be disclosed to the EV user's supplier;
  b) user identity privacy: the identity of a roaming EV user should only be disclosed to his/her own supplier;
  c) location privacy: no entity should be able to link a roaming EV's location to the EV's or EV user's ID;
  d) session unlinkability: only a user's supplier should be able to link the charging sessions of the user/EV;

(R4) Fair billing: a user/supplier should only pay (charge) for the electricity it consumes (provides);

(R5) Minimum data disclosure: suppliers should only access data that is necessary for them to bill their users fairly;

TABLE III: User related data stored at suppliers

User	Smart Card	ID	Personal data	Accounting data	Certificate	Secret key	Legitimate EVs
U_a	SC_{U_a}	ID_{U_a}	$P.DATA_{U_a}$	$A.DATA_{U_a}$	$Cert_{U_a}$	K_{U_a}	EV_1, EV_2, ...
U_v	SC_{U_v}	ID_{U_v}	$P.DATA_{U_v}$	$A.DATA_{U_v}$	$Cert_{U_v}$	K_{U_v}	EV_i, ...
U_w	SC_{U_w}	ID_{U_w}	$P.DATA_{U_w}$	$A.DATA_{U_w}$	$Cert_{U_w}$	K_{U_w}	EV_i, ...
...	...	...	...	...	...	...	...

TABLE II: EV related data stored at suppliers

EV	ID	Pseudonyms	Legitimate users
EV_1	ID_{EV_1}	$\{PSID_{EV_{1,1}}, \ldots, PSID_{EV_{1,n}}\}$	$\{U_a, U_b, \ldots\}$
EV_2	ID_{EV_2}	$\{PSID_{EV_{2,1}}, \ldots, PSID_{EV_{2,n}}\}$	$\{U_a, U_l, \ldots\}$
...	...	...	...
EV_i	ID_{EV_i}	$\{PSID_{EV_{i,1}}, \ldots, PSID_{EV_{i,n}}\}$	$\{U_v, U_w\}$

IV. The Protocol

This section presents the multi-user anonymous roaming EV charging and billing protocol. The protocol consists of four phases: system initialization, EV registration, roaming EV pre-charging and roaming EV post-charging.

A. System Initialization

TA sets up the system as follows:

- TA generates a system public/private key pair, PK_{TA}/ SK_{TA}, keeps SK_{TA} secret, but publishes certified PK_{TA}.
- During the license acquisition process, each supplier, e.g. S_h, generates a distinct public/private key pair, PK_{S_h}/ SK_{S_h}. TA signs PK_{S_h} with SK_{TA}. This is done through the generation of a digital certificate for PK_{S_h}, $Cert_{S_h}$.
- During the SM manufacturing process, each SM, e.g. SM_h, generates a distinct public/private key pair, PK_{SM_h}/ SK_{SM_h}. PK_{SM_h} is certified by TA using SK_{TA} in the form of a digital certificate, $Cert_{SM_h}$. SM_h is equipped with $Cert_{SM_h}$ and SK_{SM_h} that is kept secret and tamper-proof. (Note that this is a status quo procedure.)
- During an SM installation, the digital certificate of its user's contracted supplier is installed onto the SM.
- During an EVSE installation, the EVSE establishes a shared secret (i.e. a symmetric key) with its user's SM.

B. EV Registration

Each EV owner registers his/her EV with his/her contracted supplier through a secure and authenticated communication channel. This EV registration phase has the following steps.

a) The EV owner, e.g. U_v, provides his/her supplier, S_v, with his/her identity, ID_{U_v}, and the EV's identity, ID_{EV_i};

b) S_v generates a public/private key pair, PK_{U_v}/SK_{U_v}, and a shared symmetric key, K_{U_v}, for the user, and a digital certificate, $Cert_{U_v}$, for PK_{U_v}, where $Cert_{U_v}$ contains ID_{U_v}, PK_{U_v}, ID_{S_v} and a digital signature of S_v on its content. SK_{U_v} is used for generating a digital signature by U_v, so the authenticity (including freshness and integrity) of any signed message by U_v can be verified by S_v using PK_{U_v}. K_{U_v} is used for encrypting the signature, so only S_v can access it. This is to protect U_v against exhaustive public key search attacks. Without this encryption an attacker eavesdropping the communication channel can access the user's signature and attempt to identify him/her by trying all users' public keys to verify the signature;

c) S_v issues the user a smart card (SC), SC_{U_v}, which is preloaded with $Cert_{U_v}$, SK_{U_v} and K_{U_v}. SC_{U_v} is tamper-resistant where SK_{U_v} and K_{U_v} are kept secret.

d) S_v generates a set of pseudonyms for ID_{EV_i}, $\{PSID_{EV_{i,1}}, \ldots, PSID_{EV_{i,n}}\}$, which is loaded to EV_i. For each charging session, EV_i will be using one of these pseudonyms, instead of its real identity (ID_{EV_i}). Only S_v will know the link between ID_{EV_i} and $\{PSID_{EV_{i,1}}, \ldots, PSID_{EV_{i,n}}\}$.

U_v may further provide S_v with the details of any other potential users of the EV (e.g. U_w - a family member). S_v may then contact U_w to obtain his/her data necessary for billing purposes. Tables II and III depict the EV and user related data, respectively, stored in the supplier's database.

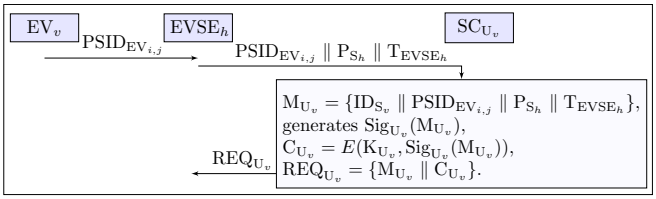

Fig. 2: Roaming EV charging request generation.

C. Roaming EV pre-Charging

Prior to each roaming EV charging session, the EV user should be granted with a permission to charge at a host location. This pre-charging phase includes two steps: roaming EV charging request generation and granting charging permission.

1) Roaming EV charging request generation: A roaming EV user uses his/her SC to generate a charging request at a host location. This step is shown in Fig. 2 and described below.

a) The roaming EV user, U_v, plugs his/her EV, EV_i, in the host's EVSE, $EVSE_h$. EV_i gets one of its pseudonyms, e.g. $PSID_{EV_{i,j}}$, and sends it to $EVSE_h$. To protect against EV substitution attacks, EV-EVSE communication link should be wired (i.e. via the charging cable) [5];

b) $EVSE_h$ receives $PSID_{EV_{i,j}}$, concatenates it with the electricity price of the host's supplier, $P_{S_h} = \{P_{S_h}^{t_1}, \ldots, P_{S_h}^{t_n}\}$, and its local time-stamp, and sends the result, $\{PSID_{EV_{i,j}} \| P_{S_h} \| T_{EVSE_h}\}$, to the roaming EV user's SC, SC_{U_v};

c) SC_{U_v} performs the following operations:
- it reads ID_{S_v} from $Cert_{U_v}$ stored on the card and constructs $M_{U_v} = \{ID_{S_v} \| PSID_{EV_{i,j}} \| P_{S_h} \| T_{EVSE_h}\}$;
- it reads SK_{U_v} and uses it to generate a signature on M_{U_v}, $Sig_{U_v}(M_{U_v})$, used by S_v to authenticate U_v;
- it reads K_{U_v} and uses it to encrypt $Sig_{U_v}(M_{U_v})$, i.e. $C_{U_v} = E(K_{U_v}, Sig_{U_v}(M_{U_v}))$.

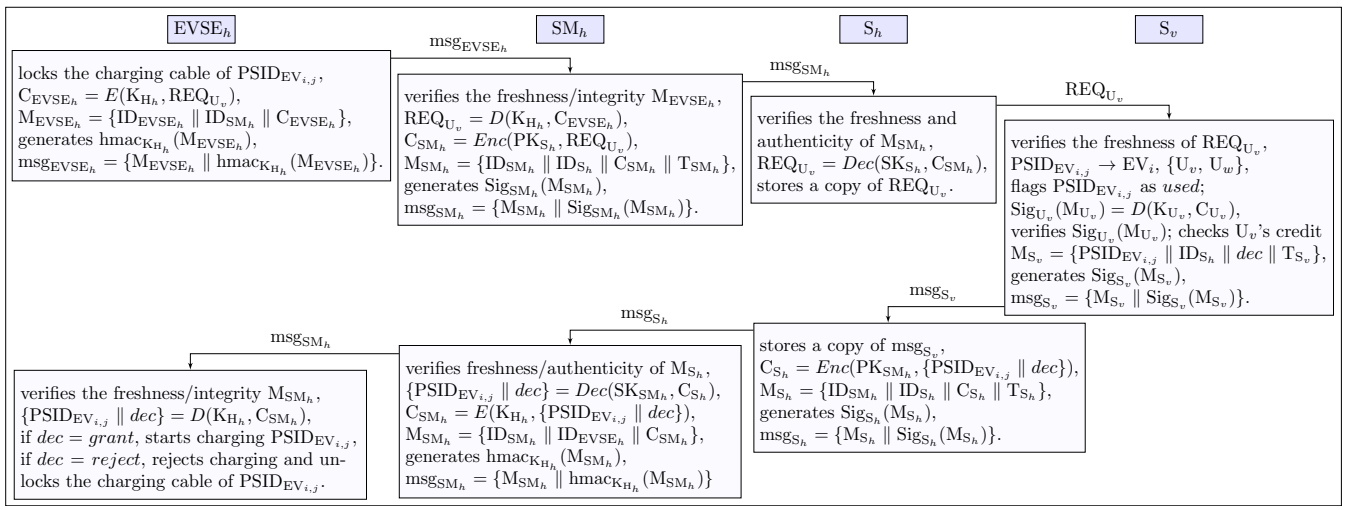

Fig. 3: Granting roaming EV charging permission.

– it constructs a charging request, i.e. $\text{REQ}_{\text{U}_v} = \{\text{M}_{\text{U}_v} \parallel \text{C}_{\text{U}_v}\}$, and sends it to EVSE_h;

2) Granting roaming EV charging permission: The charging request is sent to the roaming EV user's supplier, S_v, where S_v verifies the request, authenticates the roaming EV and its user, and based on the user's account balance, it grants (rejects) the request. This step is shown in Fig. 3 and described below.

a) Upon receiving REQ_{U_v}, EVSE_h,
   – locks the charging cable of EV_i, so the cable can remain securely plugged in during granting the charging permission (and during the charging process).
   – encrypts REQ_{U_v} with the secret key it shares with the host's SM (SM_h), K_{H_h}, generating $\text{C}_{\text{EVSE}_h} = E(\text{K}_{\text{H}_h}, \text{REQ}_{\text{U}_v})$;
   – constructs $\text{M}_{\text{EVSE}_h} = \{\text{ID}_{\text{EVSE}_h} \parallel \text{ID}_{\text{SM}_h} \parallel \text{C}_{\text{EVSE}_h}\}$;
   – generates a keyed-hash value of M_{EVSE_h} using K_{H_h}, $\text{hmac}_{\text{K}_{\text{H}_h}}(\text{M}_{\text{EVSE}_h})$, constructs $\text{msg}_{\text{EVSE}_h} = \{\text{M}_{\text{EVSE}_h} \parallel \text{hmac}_{\text{K}_{\text{H}_h}}(\text{M}_{\text{EVSE}_h})\}$ and sends $\text{msg}_{\text{EVSE}_h}$ to SM_h.

b) Upon receiving $\text{msg}_{\text{EVSE}_h}$, SM_h,
   – verifies the freshness and integrity of M_{EVSE_h};
   – decrypts C_{EVSE_h}, i.e. $\text{REQ}_{\text{U}_v} = D(\text{K}_{\text{H}_h}, \text{C}_{\text{EVSE}_h})$;
   – encrypts REQ_{U_v} with the public key of the host's supplier, S_h, i.e. $\text{C}_{\text{SM}_h} = Enc(\text{PK}_{\text{S}_h}, \text{REQ}_{\text{U}_v})$;
   – constructs $\text{M}_{\text{SM}_h} = \{\text{ID}_{\text{SM}_h} \parallel \text{ID}_{\text{S}_h} \parallel \text{C}_{\text{SM}_h} \parallel \text{T}_{\text{SM}_h}\}$
   – generates a signature on M_{SM_h}, $\text{Sig}_{\text{SM}_h}(\text{M}_{\text{SM}_h})$;
   – sends $\text{msg}_{\text{SM}_h} = \{\text{M}_{\text{SM}_h} \parallel \text{Sig}_{\text{SM}_h}(\text{M}_{\text{SM}_h})\}$ to S_h.

c) Upon receiving msg_{SM_h}, S_h,
   – verifies the authenticity of M_{SM_h} using PK_{SM_h};
   – decrypts C_{SM_h}, i.e. $\text{REQ}_{\text{U}_v} = Dec(\text{SK}_{\text{S}_h}, \text{C}_{\text{SM}_h})$;
   – stores a copy of REQ_{U_v} before forwarding it to S_v via a secure and authentic communication channel.

d) Upon receiving $\text{REQ}_{\text{U}_v} = \{\text{ID}_{\text{S}_v} \parallel \text{PSID}_{\text{EV}_{i,j}} \parallel \text{P}_{\text{S}_h} \parallel \text{T}_{\text{EVSE}_h} \parallel \text{C}_{\text{U}_v}\}$, S_v,
   – verifies the freshness of REQ_{U_v};
   – searches its database, Table II, to find the EV corresponding to $\text{PSID}_{\text{EV}_{i,j}}$, EV_i, and the EV's legitimate users, $\{\text{U}_v, \text{U}_w\}$; and flags $\text{PSID}_{\text{EV}_{i,j}}$ as $used$;
   – reads the secret keys of $\{\text{U}_v, \text{U}_w\}$ from its database, Table III, and finds the user whose key decrypts C_{U_v}, i.e. U_v, as $\text{Sig}_{\text{U}_v}(\text{M}_{\text{U}_v}) = D(\text{K}_{\text{U}_v}, \text{C}_{\text{U}_v})$;
   – verifies $\text{Sig}_{\text{U}_v}(\text{M}_{\text{U}_v})$, thus it is assured that the request was indeed initiated by U_v and stores REQ_{U_v};
   – checks if the account of U_v has a sufficient fund (credit) to cover the charging expenses and based on that it makes a decision, $dec = \{grant \vee reject\}$;
   – constructs $\text{M}_{\text{S}_v} = \{\text{PSID}_{\text{EV}_{i,j}} \parallel \text{ID}_{\text{S}_h} \parallel dec \parallel \text{T}_{\text{S}_v}\}$;
   – generates a signature on M_{S_v}, $\text{Sig}_{\text{S}_v}(\text{M}_{\text{S}_v})$;
   – sends $\text{msg}_{\text{S}_v} = \{\text{M}_{\text{S}_v} \parallel \text{Sig}_{\text{S}_v}(\text{M}_{\text{S}_v})\}$ to S_h.

e) Upon receiving msg_{S_v}, S_h,
   – stores a copy of $\text{msg}_{\text{S}_v} = \{\text{M}_{\text{S}_v} \parallel \text{Sig}_{\text{S}_v}(\text{M}_{\text{S}_v})\}$;
   – encrypts the decision with the public key of SM_h, $\text{C}_{\text{S}_h} = Enc(\text{PK}_{\text{SM}_h}, \{\text{PSID}_{\text{EV}_{i,j}} \parallel dec\})$;
   – constructs $\text{M}_{\text{S}_h} = \{\text{ID}_{\text{SM}_h} \parallel \text{ID}_{\text{S}_h} \parallel \text{C}_{\text{S}_h} \parallel \text{T}_{\text{S}_h}\}$
   – generates a signature on M_{S_h}, $\text{Sig}_{\text{S}_h}(\text{M}_{\text{S}_h})$;
   – sends $\text{msg}_{\text{S}_h} = \{\text{M}_{\text{S}_h} \parallel \text{Sig}_{\text{S}_h}(\text{M}_{\text{S}_h})\}$ to SM_h.

f) Upon receiving msg_{S_h}, SM_h,
   – verifies the authenticity of M_{S_h} using PK_{S_h};
   – decrypts C_{S_h} to obtain the decision, i.e. $\{\text{PSID}_{\text{EV}_{i,j}} \parallel dec\} = Dec(\text{SK}_{\text{SM}_h}, \text{C}_{\text{S}_h})$;
   – encrypts and integrity protects the decision (using K_{H_h}) before forwarding it to EVSE_h.

g) EVSE_h verifies the integrity of the cipertext before decrypting it to obtain the decision. If the decision is $grant$, EVSE_h starts the charging process. Otherwise, EVSE_h rejects the request and unlocks the charging cable.

D. Roaming EV post-Charging

This step ensures that, after each roaming EV charging, the roaming EV user's and the host's account balances are adjusted accordingly. Two steps are used to accomplish this: roaming EV charging termination and fair billing.

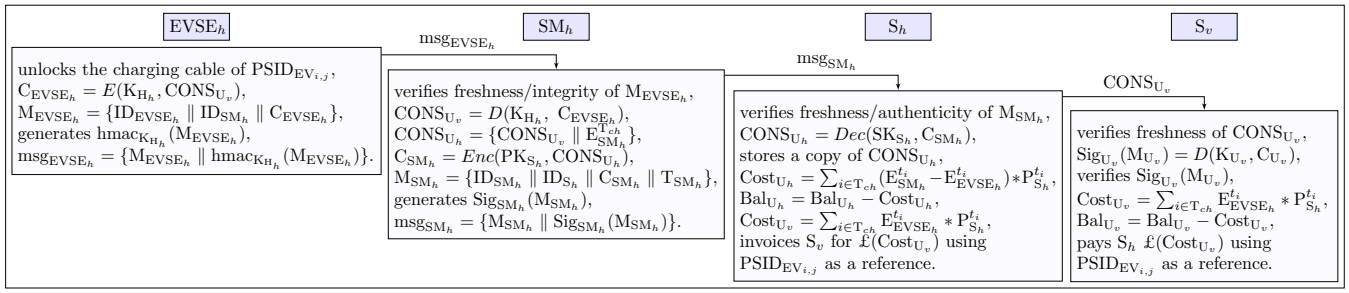

Fig. 5: Fair billing calculation.

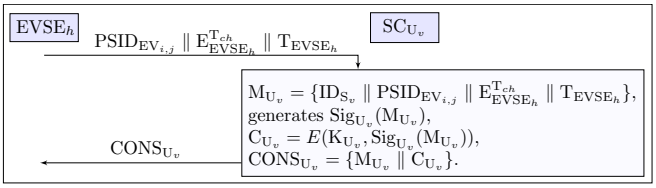

Fig. 4: Consumption report generation.

1) Roaming EV charging termination: Once the roaming EV is fully recharged or the user decides to terminate the charging process, he/she uses his/her SC to generate a consumption report which includes the amount of electricity the EV has consumed during the charging process.

As shown in Fig. 4, the report generation process is identical to the charging request generation process plotted in Fig. 2. The only difference is in the input data sent to SC_{U_v}, i.e. $EVSE_h$ replaces the electricity price data, i.e. P_{S_h}, with the electricity consumption data measured at $EVSE_h$ during the charging process, i.e. $E^{T_{ch}}_{EVSE_h} = \{E^{t_i}_{EVSE_h}, \ldots, \ldots\}$. SC_{U_v} performs the same operations and outputs the consumption report, $CONS_{U_v}$, which is sent to $EVSE_h$.

2) Fair billing: The consumption data measured at the host EVSE and SM during the EV charging are delivered to the host supplier where the host's cost is calculated and his/her account balance adjusted accordingly. Also, the data measured at the EVSE is forwarded to the roaming EV user's supplier where the user's cost is calculated and his/her account balance adjusted. This step is shown in Fig. 5 and described below.

a) Upon receiving $CONS_{U_v}$, $EVSE_h$ unlocks the EV's charging cable, encrypts and integrity protects $CONS_{U_v}$ using K_{H_h} and forwards the result, msg_{EVSE_h}, to SM_h.
b) Upon receiving and verifying msg_{EVSE_h}, SM_h recovers $CONS_{U_v}$ and constructs a consumption report of the host, $CONS_{U_h}$, which includes $CONS_{U_v}$ and the consumption data measured at the host's SM during the EV charging, $E^{T_{ch}}_{SM_h} = \{E^{t_i}_{SM_h}, \ldots, \ldots\}$. Then, SM_h encrypts and signs the report before forwarding the result, msg_{SM_h}, to S_h.
c) Upon receiving and verifying msg_{SM_h}, S_h recovers and stores a copy of $CONS_{U_h} = \{CONS_{U_v} \| E^{T_{ch}}_{SM_h}\}$ before sending $CONS_{U_v}$ to S_v. It then calculates the cost of the electricity consumed only by the host, i.e. $Cost_{U_h} = \sum_{i \in T_{ch}} (E^{t_i}_{SM_h} - E^{t_i}_{EVSE_h}) * P^{t_i}_{S_h}$, and adjusts his/her account balance accordingly, i.e. $Bal_{U_h} = Bal_{U_h} - Cost_{U_h}$. Note that $Cost_{U_h}$ could be negative (when the electricity used to charge the roaming EV comes from a RES located on the host's premises some of which would otherwise be sold back to the grid). In such cases, the host's balance increases, i.e. U_h is paid for the electricity which is generated locally and consumed by the roaming EV. S_h also calculates the cost of the electricity consumed by the roaming EV, i.e. $Cost_{U_v} = \sum_{i \in T_{ch}} E^{t_i}_{EVSE_h} * P^{t_i}_{S_h}$, and invoices S_v for £($Cost_{U_v}$) using PSID$_{EV_{i,j}}$ as a reference.
d) Upon receiving and verifying $CONS_{U_v}$, S_v recovers and verifies its user's signature, so it can be assured that $CONS_{U_v}$ was indeed generated by U_v. It then verifies the cost that has been calculated by S_h, i.e. $Cost_{U_v} = \sum_{i \in T_{ch}} E^{t_i}_{EVSE_h} * P^{t_i}_{S_h}$, and adjusts the account balance of U_v accordingly, i.e. $Bal_{U_v} = Bal_{U_v} - Cost_{U_v}$. Finally, S_v pays £($Cost_{U_v}$) to S_h using PSID$_{EV_{i,j}}$ as a reference.

V. Security and Privacy Analyses

This section presents (1) the informal security and privacy analyses and (2) the formal security validation of the protocol. The latter is done using the Automated Validation Internet Security Protocols and Application (AVISPA) tool [21].

A. Informal Analyses

Message authenticity: Each message communicated between SMs and suppliers contains a digital signature of the message originator. Assuming that a standard digital signature scheme is used (e.g. RSA, DSA) which is proven to be computationally secure, our protocol ensures message integrity, origin authentication and non-repudiation (satisfying R1). Also each message communicated between a user's SM and EVSE contains a HMAC generated with the use of a secret symmetric key shared only between the SM and the EVSE. Hence, any active attacks on data in transit can be detected and modified data discarded. Also, including a time stamp in each message ensures that all such messages received are fresh.

Confidentiality of charging data: The charging request and consumption reports are always communicated in an encrypted format (encrypted via a symmetric encryption scheme (e.g. AES) between EVSE and SM, and via an asymmetric scheme (e.g. RSA) between SMs and suppliers). Therefore, it is hard for any adversaries eavesdropping the communication channels to obtain any sensitive data (satisfying R2).

EV identity privacy: During a charging session the roaming EV uses a pseudonym (instead of its identity). As only the roaming EV user's supplier knows the mapping between the pseudonym and the EV's identity, it is the only entity able to find out the real identity of the roaming EV (satisfying R3a).

User identity privacy: During a charging session the identity of the roaming EV user is not used at all. As only the roaming EV user's supplier can obtain the user's signature, it is the only entity able to relate the charging session to a specific user. Note that this relation is necessary as the supplier is responsible for the user's billing management (satisfying R3b).

User/EV location privacy: During a charging session the host's supplier knows the charging location and obtains the identity of the supplier contracted by the roaming EV user and the pseudonym of the roaming EV but not the EV's and its user's identities. On the other hand, the supplier of the roaming EV user knows the EV's and its user's identities and obtains the identity of the host's supplier but does not get any information about the charging location. As there is no entity that knows 1) the real identities of the roaming EV and its user and 2) the charging location, we can say that location privacy of the roaming EV user is preserved (satisfying R3c).

Charging sessions unlinkability: In our protocol each EV is loaded with a sufficient number of pseudonyms. The EV uses a different pseudonym every time it executes a roaming charging. As these pseudonyms are random strings, it is hard for any unauthorised entity (e.g. host's supplier or eavesdropping adversaries) to relate different charging sessions of the same EV, or to find out if two charging sessions have been performed by the same EV (satisfying R3d).

Fair billing: While charging at a host's premises, a roaming EV may use electricity generated by the host's RES thus preventing the host from selling the electricity back to the grid. By collecting data from the host's EVSE and SM, the host's supplier can calculate the exact amount of electricity consumed only by the host, and the amount of electricity generated by the host's RES but consumed by the roaming EV during the EV charging session. Thus the host's supplier can calculate the correct cost/reward of/for its user. Thus, our protocol supports fair billing (satisfying R4).

Minimum data disclosure: In our protocol a roaming EV user's supplier only obtains the data necessary to bill the user and pay the correct supplier (i.e. proof that the request comes from a legitimate user who wants to charge a legitimate EV, the amount of electricity consumed, the price data and the host's supplier). There is no need for the supplier to learn the location and identity of the host, nor the source of the electricity consumed by the EV (i.e. the host's RES or grid). The host's supplier obtains only the data necessary to bill the host (i.e. the amount of electricity consumed by the roaming EV, the amount of electricity consumed/fed by the host and the roaming EV user's supplier). It does not need to learn the roaming EV's and its user's identities (satisfying R5).

Protection against lost SC or stolen EV: By using double authentications, i.e. user and EV authentications, our solution ensures that a charging process could only be applied to the EVs that are registered with, and initiated by, the users whose EVs are registered with their accounts. Thus, our protocol minimises the risks of unauthorised use of a lost/stolen SC/EV. To abuse the system, one has to steal both the SC and the EV. Optionally, each SC can also be password/pin code protected, thus further minimising the risk of unauthorised use of a SC. Even if the secret keys from a stolen SC are extracted, they will not be usable to charge EVs unregistered with the SC.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\SPAN\testsuite\results\Roaming_EV.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 2.62s
  visitedNodes: 607 nodes
  depth: 8 plies
```

(a) OFMC

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  C:\SPAN\testsuite\results\Roaming_EV.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 4712 states
  Reachable  : 656 states
  Translation: 0.11 seconds
  Computation: 0.09 seconds
```

(b) ATSE

Fig. 6: AVISPA results.

B. Formal Security Verification Using AVISPA

AVISPA [21] is a tool for automated validation of security properties of Internet protocols and applications. It has also been used for SG protocol verifications [12], [22], [23]. AVISPA uses the role-based High Level Protocol Specifications Language (HLPSL), for specifying protocols and their security properties, and integrates verification tools such as On-the-Fly Model-Checker (OFMC) and Constraint-Logic-based Attack Searcher (CL-AtSe) that implement a variety of automatic analysis techniques. The validation results of our protocol are presented in Fig. 6. Due to page limitation, only the main HLPSL code (in Fig. 7) is provided.

VI. Conclusion

In this paper, we have proposed a secure roaming EV charging protocol that supports fair billing while preserving EV user's ID and location privacy. With regard to privacy preservation, it can a) hide the user and EV ID from the host supplier (by a use of secure pseudonyms) and b) hide the user and EV location from the user's supplier. The protocol uses double authentication, i.e. the user's supplier first authenticates the EV and then its user, to support secure multi-user EV utilization and charging expenses sharing among different legitimate EV users and to reduce risks of the system being abused by both external perpetrators and internal entities. The protocol design has used the principle of minimum data disclosure to preserve EV users' ID and location privacy while facilitating fair billing for both EV users and their hosts. Informal security analyses and formal verification have shown that the protocol is secure and robust in achieving its goal.

Our next stage of research will be the introduction of 1) a more complex electricity pricing model, and 2) a new type of suppliers that are responsible for supplying electricity only to EVs, which should open up the electricity market and help innovation in optimizing the SG by smart EV prosumption.

```
role session( EVv,EVSEh,SCv,SMh,Sh,Sv,TA        : agent,
              PK_SCv,PK_SMh,PK_Sh,PK_Sv,PK_TA    : public_key,
              K_EVSEhSMh,K_SCvSv                 : symmetric_key,
              H                                  : hash_func,
              LEVSEh,LSMh,LSh,LSv                : text set)
def=
            local       SndEVv,RcvEVv,SndEVSEh,RcvEVSEh,SndSCv,RcvSCv,SndSMh,RcvSMh,SndSh,RcvSh,SndSv,RcvSv                          : channel(dy)
            const       sv_auth_scv,evseh_auth_smh,smh_auth_evseh,sh_auth_smh,smh_auth_sh,sv_auth_sh,sh_auth_sv,decsv,sigscv       : protocol_id
            composition
                           electric_vehicle(EVv,EVSEh,SndEVv,RcvEVv)
                        /\ electric_vehicle_supply_equipment(EVSEh,SCv,SMh,K_EVSEhSMh,H,SndEVSEh,RcvEVSEh)
                        /\ smart_card(SCv,EVSEh,SMh,Sh,Sv,K_SCvSv,H,PK_SCv,PK_TA,SndSCv,RcvSCv)
                        /\ smart_meter(SMh,EVSEh,Sh,Sv,TA,PK_SMh,PK_Sh,PK_TA,K_EVSEhSMh,H,SndSMh,RcvSMh)
                        /\ supplier_host(Sh,SMh,Sv,TA,PK_Sh,PK_SMh,PK_Sv,PK_TA,SndSh,RcvSh)
                        /\ supplier_visitor(Sv,EVSEh,SCv,SMh,Sh,TA,PK_Sh,PK_Sv,PK_TA,PK_SCv,K_SCvSv,SndSv,RcvSv)
end role

role environment()

def=
            local       LEVSEh,LSMh,LSh,LSv,PSDEVV,PSDSV                : text set
            const       scv,evv,evseh,smh,sh,sv,ta,i                    : agent,
                        pk_uv,pk_smh,pk_sh,pk_sv,pk_ta,pk_i             : public_key,
                        k_evsehsmh,k_evsehi,k_ismh,k_scvsv,k_isv,k_scvi : symmetric_key,
                        h                                               : hash_func

init        LEVSEh:= {} /\ LSMh:= {} /\ LSh:= {} /\ LSv:= {} /\ PSDEVV := {psid1_EVv,psid2_EVv,psid3_EVv} /\ PSDSV := {psid1_EVv,psid2_EVv,psid2_EVv}
            intruder_knowledge = {evv,evseh,smh,sh,sv,i,k_ismh,k_evsehi,k_isv,k_scvi,pk_smh,pk_sh,pk_sv,pk_ta,pk_i,inv(pk_i),h}
            composition
                          session(evv,evseh,scv,smh,sh,sv,ta,pk_uv,pk_smh,pk_sh,pk_sv,pk_ta,k_evsehsmh,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
                        /\ session(evv,evseh,scv,smh,sh,sv,ta,pk_uv,pk_smh,pk_sh,pk_sv,pk_ta,k_evsehsmh,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
                        % /\ session(i,evseh,scv,smh,sh,sv,ta,pk_uv,pk_smh,pk_sh,pk_sv,pk_ta,k_evsehsmh,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
                        % /\ session(evv,i,scv,smh,sh,sv,ta,pk_uv,pk_smh,pk_sh,pk_sv,pk_ta,k_ismh,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
                        % /\ session(evv,evseh,i,smh,sh,sv,ta,pk_i,pk_smh,pk_sh,pk_sv,pk_ta,k_evsehsmh,k_isv,h,LEVSEh,LSMh,LSh,LSv)
                        % /\ session(evv,evseh,scv,i,sh,sv,ta,pk_uv,pk_i,pk_sh,pk_sv,pk_ta,k_evsehi,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
                        % /\ session(evv,evseh,scv,smh,i,sv,ta,pk_uv,pk_smh,pk_i,pk_sv,pk_ta,k_evsehsmh,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
                        % /\ session(evv,evseh,scv,smh,sh,i,ta,pk_uv,pk_smh,pk_sh,pk_i,pk_ta,k_evsehsmh,k_scvsv,h,LEVSEh,LSMh,LSh,LSv)
end role

goal
            authentication_on sv_auth_scv       % the roaming EV user's supplier authenticates the user (his/her smart card)
            authentication_on evseh_auth_smh    % the host EVSE authenticates the message sent by the host SM
            authentication_on smh_auth_evseh    % the host SM authenticates the message sent by the host EVSE
            authentication_on sh_auth_smh       % the host supplier authenticates the message sent by the host SM
            authentication_on smh_auth_sh       % the host SM authenticates the message sent by the host supplier
            authentication_on sv_auth_sh        % the roaming EV user's supplier authenticates the message sent by the host supplier
            authentication_on sh_auth_sv        % the host supplier authenticates the message sent by the roaming EV user's supplier

            secrecy_of decsv                    % confidentiality of the decision for granting (rejecting) the roaming EV charging
            secrecy_of sigscv                   % confidentiality of the roaming EV user's signature
end goal

environment()
```

Fig. 7: The HLPSL code.

ACKNOWLEDGMENT

This research is supported by the Engineering and Physical Sciences Research Council (EPSRC) and Toshiba Research Europe Limited under Grant [EP/I501541/1].

REFERENCES

[1] H. Farhangi. The path of the smart grid. *Power and Energy Magazine, IEEE*, 8(1):18–28, Jan.-Feb. 2010.

[2] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M.A. Mustafa. Toward unified security and privacy protection for smart meter networks. *Systems Journal, IEEE*, PP(99):1–14, 2013.

[3] M.A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan. Smart electric vehicle charging: Security analysis. In *ISGT, IEEE PES*, Feb Feb. 2013.

[4] H. Chaudhry and T. Bohn. Security concerns of a plug-in vehicle. In *Innovative Smart Grid Technologies (ISGT), IEEE PES*, Jan 2012.

[5] A.C. Chan and J. Zhou. On smart grid cybersecurity standardization: Issues of designing with nistir 7628. *Communications Magazine, IEEE*, 51(1):58–65, Jan. 2013.

[6] B. Vaidya, D. Makrakis, and H.T. Mouftah. Efficient authentication mechanism for pev charging infrastructure. In *ICC, IEEE*, June 2011.

[7] B. Vaidya, D. Makrakis, and H.T. Mouftah. Security mechanism for multi-domain vehicle-to-grid infrastructure. In *GLOBECOM,IEEE,2011*.

[8] Hong Liu, Huansheng Ning, Yan Zhang, and L.T. Yang. Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid. *Smart Grid, IEEE Trans. on*, 3(4):1722–1733, Dec 2012.

[9] Hong Liu, Huansheng Ning, Yan Zhang, and M. Guizani. Battery status-aware authentication scheme for v2g networks in smart grid. *Smart Grid, IEEE Transactions on*, 4(1):99–110, March 2013.

[10] H. Liu, H. Ning, H. Zhang, Q. Xiong, and L.T. Yang. Role-dependent privacy preservation for secure v2g networks in the smart grid. *Information Forensics and Security, IEEE Trans. on*, 9(2):208–220, Feb 2014.

[11] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. Yang, and M. Guizani. Securing vehicle-to-grid communications in the smart grid. *Wireless Communications, IEEE*, 20(6):66–73, December 2013.

[12] H. Nicanfar, P. TalebiFard, S. Hosseininezhad, V.C.M. Leung, and M. Damm. Security and privacy of electric vehicles in the smart grid context: Problem and solution. In *Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, NY, USA, 2013. ACM.

[13] Huei-Ru Tseng. A secure and privacy-preserving communication protocol for v2g networks. In *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, pages 2706–2711, April 2012.

[14] Huaqun Guo, Yongdong Wu, Feng Bao, Hongmei Chen, and Maode Ma. Ubapv2g: A unique batch authentication protocol for vehicle-to-grid communications. *Smart Grid, IEEE Trans.*, 2(4):707–714, Dec 2011.

[15] IETF RFC 6272: Internet Protocols for the Smart Grid Internet: www.tools.ietf.org/html/draft-baker-ietf-core [24.04.2012].

[16] ETSI. Machine-to-machine communications (m2m); threat analysis and counter-measures to m2m service layer. Technical report, ETSI TR 103 167 V1.1.1, Aug. 2011.

[17] U.S. NIST, Guidelines for smart grid cyber security (vol. 1 to 3), NIST IR-7628, Aug. 2010.

[18] Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and C. L. Philip Chen. Cyber security and privacy issues in smart grids. *Communications Surveys Tutorials, IEEE*, 14(4):981–997, Fourth 2012.

[19] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart grid the new and improved power grid: A survey. *Communications Surveys Tutorials, IEEE*, 14(4):944–980, Fourth 2012.

[20] Zhong Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *Communications Surveys Tutorials, IEEE*, 15(1):21–38, First 2013.

[21] Avispa - automated validation of internet security protocols and applications. Internet: http://www.avispa-project.org/ [28.07.2014].

[22] H. Nicanfar and V.C.M. Leung. Multilayer consensus ecc-based password authenticated key-exchange (mcepak) protocol for smart grid system. *Smart Grid, IEEE Transactions on*, 4(1):253–264, March 2013.

[23] H. Nicanfar, P. Jokar, K. Beznosov, and V.C.M. Leung. Efficient authentication and key management mechanisms for smart grid communications. *Systems Journal, IEEE*, 8(2):629–640, June 2014.