Secure Optimal Itinerary Planning for Electric Vehicles in the Smart Grid

Achraf Bourass, Soumaya Cherkaoui, *Senior Member, IEEE*, and Lyes Khoukhi, *Member, IEEE*

***Abstract*—Although the number of electric vehicles (EVs) on the road has been steadily increasing in the last few years, the problems of autonomy and limited driving range of EVs still represent a big challenge for automotive industry. In this paper, we first propose a secure architecture where EVs and the smart grid exchange information for itinerary planning and charging time-slots' reservations at charging stations. The architecture ensures privacy, and includes authentication and authorization in order to secure EVs sensitive information. Second, we introduce a new scheme for EV itinerary planning, which takes into account the state-of-charge of the EV, its destination, and available charging stations on the road. The scheme minimizes the waiting time of the EV and its overall energy consumption to attain destination. MATLAB and CPLEX simulations were performed to show the performance of our proposed scheme. Simulation proved that our model is able to optimize paths in terms of energy consumption and waiting time.**

***Index Terms*—Electric vehicle (EV), itinerary planning, smart grid, waiting time.**

I. Introduction

Electric vehicles (EVs) are known for their economic and environmental benefits. EVs offer a transportation mean without greenhouse gas emissions, which cause significant pollution in urban areas. The global climatic contribution of an EV is estimated to 9 tones in terms of equivalent CO_2 over its entire lifespan, compared to an estimated 22 tones for its thermic vehicle counterpart. These economic and environmental benefits have made EVs a privileged mode of transportation for an increasing number of citizens; there are more than 500 000 registered EVs around the world and 2.7 million more EVs are expected to join the roads by 2018 [1].

Manuscript received February 12, 2017; revised May 21, 2017; accepted July 16, 2017. Date of publication September 18, 2017; date of current version December 1, 2017. This work was supported in part by Natural Sciences and Engineering Research Council of Canada and Quebec's Ministry of International Relations and La Francophonie under the Champlain Program. Paper no. TII-17-0261. *(Corresponding author: Soumaya Cherkaoui.)*

A. Bourass and S. Cherkaoui are with the INTERLAB, University of Sherbrooke, QC J1K 2R1, Canada (e-mail: Achraf.bourass@usherbrooke.ca; soumaya.cherkaoui@usherbrooke.ca).

L. Khoukhi is with the Autonomic Networking Environment, Charles Delaunay Institute, University of Technology of Troyes, Troyes 10300, France (e-mail: lyes.khoukhi@utt.fr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2017.2741347

Despite the increasing popularity of EVs, some of the important issues that restrain a mass adoption of EVs are the limited range of battery, the limited availability of charging stations (CSs), and the overall duration of the charging process.

Indeed, EVs charging times are significantly longer compared to those of conventional vehicles, leading to longer waiting time in the CSs. An EV charging time (service time) depends on the equipment of the CS and the nature of the batteries. In Level 3 stations, the fastest ones, the charging time can be as long as 30 mn, depending on the state-of-charge of the EV [2]. The waiting time depends on the number of vehicles waiting for service ahead of the EV and their cumulative charging times. In periods of peak demand for charging on the road, or in areas having only few CSs, issues of waiting time can become problematic. Another issue, which hinders EV mass adoption, is the so-called range-anxiety, where users fear that an EV will have insufficient battery range to reach its destination [3].

Parallel to the adoption of EVs, a new architecture of electric power grid, called the smart grid, is being deployed world-wide [4]. The smart grid offers many benefits, such as:

ensuring reliability, quality of energy, and security of different entities connected to the distribution grid;

integrating renewable energy sources;

minimizing disconnection times/durations; and

optimizing energy consumption at times of peak demand.

All these benefits are made possible with two-way communications with all entities involved in the grid.

In this paper, we propose an architecture where EVs wirelessly exchange information with the smart grid, more specifically the Grid System Operator (GSO), in order to assist them in planning their itinerary. Since the two-way communication between GSO and EVs can help third parties access sensitive information about both EVs (e.g., state of charge, position, battery capacity) and the smart grid (e.g., available charging time-slots at CSs), security mechanisms are needed. Therefore, the proposed architecture integrates a secure service architecture (SSA) [5], which ensures both confidentiality of communications and privacy of EVs. Further, the architecture integrates authentication and authorization mechanisms to allow EVs to reserve charging time-slots along their itineraries.

In order to plan the itinerary of an EV, we propose an optimization scheme, which takes into account the global occupancy of CSs on the road, the roadmap and road segment speeds, traffic density, together with the EV state-of-charge (SoC), position, and final destination. The scheme is used by the GSO to determine the optimal itineraries for the EV to attain its destination while minimizing its waiting time and total energy consumption to arrive to destination.

We suppose that the EVs communicate to the GSO their SoC, position, and destination. Based on this information, the GSO computes the optimal paths in terms of waiting time and energy consumption, and indicates to the EV the best CS choices.

The remainder of this paper is organized as follows: Section II presents related works. Section III presents our system model and the reservation process. Section IV describes the proposed secure architecture. Section V describes the reservation strategy algorithm. Section VI evaluates the proposed architecture with simulations for different scenarios. Finally, Section VII concludes the paper and suggests future works.

II. Related Work

A few works have addresses issues of planning strategies for EVs in the past years. Minimization of the waiting time of EVs in CSs along a road by using stochastic methods has been proposed in a previous work [6]. Another work looked at minimizing the time to join a CS by choosing the CS that has the minimum distance and occupancy time [7]. However, in both these works, the problem of itinerary planning based on destination and the reservation of charging time-slots were not addressed. Traffic density and road speed limits between EV current location and CSs were not considered neither.

In [8] and [9], the authors proposed two different algorithms for EV route planning in order to find the best routes in terms of energy consumption, by considering road topology and traffic conditions. However, these algorithms do not consider the available SoC of EV. In [10], battery constraints are considered in a route planning problem where the objective is to find the optimal path for EV in terms of energy or travel time. In [11], Rezgui *et al.* proposed a new communication protocol for the reservation process between EVs and the CSs. However, in [10] and [11], issues related to traffic and overall EV energy consumption were not considered.

In [12], the best path problem is modeled using a mathematical optimization problem where exchanging the EV battery at the stations is considered as an alternative solution to EV charging. The authors do not consider the time needed for battery exchange nor the waiting time at stations in their model.

In [13], Ruzmetov *et al.* proposed a scheduling algorithm of EVs at CSs based on the SoC, the travel distance to the stations and road traffic. However, this paper does not minimize the queuing time in the stations nor does it consider the destination location. In [14], a generalized multicommodity network flow was used in a multicriteria EV routing problem to minimize the cost and/or the time to reach the final destination. In [15], Mehar *et al.* proposed an architecture for EV planning by calculating the most economic path along the route in terms of energy consumption based on some information (e.g., status of CSs, EV position, destination, EV SoC, road conditions). The problem of waiting time at CSs was not addressed in [14] and [15] even though CSs may have significant queueing time. In [16], Akbari and Fernando focused on queuing time and the shortest path to assign an EV to a single CS; however, the work does not consider traffic, overall EV energy consumption, and destination position.

In recent works [17]–[24], security issues of EVs and smart grids have received significant attention. In [25], various types of attacks on vehicle-grid (V2G) connections were presented, such as denial of services, tampering with communication messages, and eavesdropping. In [26], a security architecture for smart grid is proposed where five main components are integrated: a secure grid overlay network, publisher–subscriber data delivery, low-latency transport protocols, and application programming and networked cache/storage. The authors focused on how to secure the infrastructure of the smart grid without special attention to interactions with EVs. Zhang *et al*. in [27] discussed security and privacy requirements for V2G networks and presented some security mechanisms for smart grids to protect EVs. In [28], a mechanism for securing EV communications with different grid entities is proposed; this mechanism aims at preventing attackers from executing Sybil attacks. In [29], Nicanfar *et al.* proposed an authentication scheme between EVs and CSs. This scheme aims at securing EV sensitive information based on EV pseudonyms to impede third parties from monitoring EV movements. In [30], Liu *et al.* proposed a battery status- aware scheme which aims at hiding the EV battery identity and preserving EV privacy. However, neither [29] nor [30] have considered issues regarding accounting and authorization. In [31] and [32], various schemes were presented which aim at ensuring the confidentiality of EV data. In [33], Liu *et al.* proposed an aggregated-proof-based privacy-preserving authentication scheme, aiming at protecting vehicles' battery identity. For the sake of preserving communication resources, vehicles can be authenticated by an aggregator in their scheme. All of the aforementioned schemes aimed at securing some aspects related to EV-grid interactions. However, to the best our knowledge, none of the previous works proposed solutions for jointly protecting the privacy of EVs, securing communications, and providing authorization to allow EVs access itinerary planning and charge scheduling.

In our paper, we propose a secure architecture, which ensures confidentiality of information, privacy for EVs, and authentication and authorization mechanisms for reserving charging slots at CSs.

III. System Architecture

Let us consider an EV travelling from a departure point to an arrival destination. The EV needs to plan its itinerary, so it makes a corresponding request to the GSO. As a response, the GSO determines the best itineraries for the EV which minimize the waiting time and overall energy consumption to attain destination. The GSO then indicates to the EV both the itinerary and the CSs where it should recharge its battery along the routes.

In our model, we consider that the EV can exchange information with the GSO through wireless communication technology (e.g., WiFi, DSRC, LTE, etc.). The exchanged information consists of SoC, destination, and current position. We also consider that GSO has a global view on the status of occupancy of CS along the road network. CS can exchange information with the

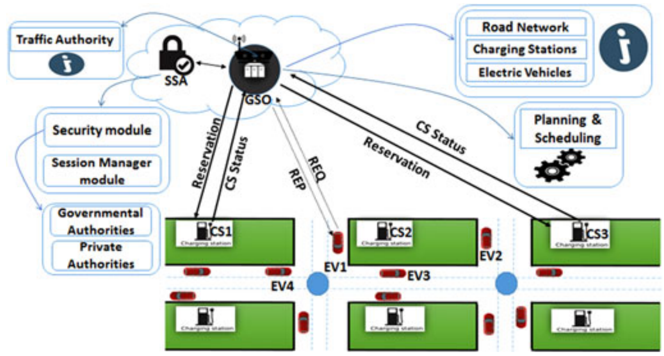

Fig. 1. Itinerary planning architecture.

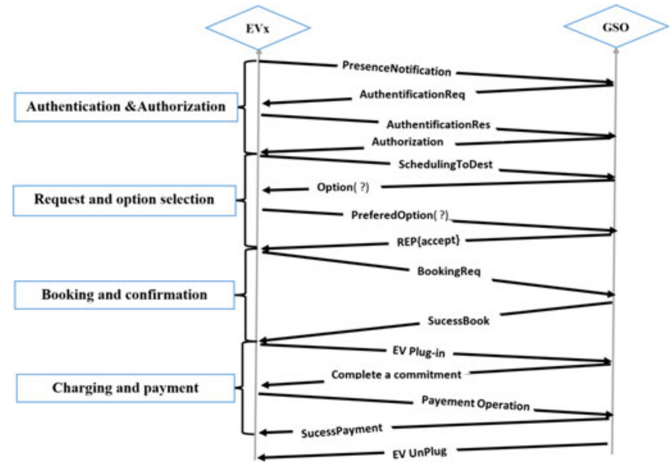

Fig. 2. Sequence diagram of the booking process.

GSO through wireless (mesh networks, LTE, etc.) or wired network technologies. The GSO is able to communicate with the traffic authority (TA), through wireless or wired network technologies, in order to obtain information about traffic in a real time.

The GSO manages different constraints and limitations imposed by EVs and CSs, to deliver optimal charging options and economic path planning, in terms of energy consumption, for EVs. The constraints imposed by EVs are generally related to: 1) their remaining SoC allowing them to attain a maximum distance without recharging their battery; and 2) the EVs destination, which poses a particular constraint about the trajectory to be travelled. Indeed, the suggested CSs should be as near as possible to the shortest path trajectory. For public CSs, the limitations are related mainly to their number, geographic distribution, and their charging capability (i.e., number of charging points or EV supply equipment, EVSE, at each station).

The GSO aims at computing the optimal paths for EVs which minimize their waiting time for charging, and the total energy consumption from source to destination. The GSO informs EVs about their optimal itineraries, together with the CS where they need to stop for charging. When an EV chooses an itinerary and confirms its choice to the GSO, the latter performs the appropriate reservations of charging time slots at the corresponding CS. Exchanges between the GSO and EVs are secured with the integration of SSA, to ensure the confidentiality of communications and privacy of EVs.

The proposed architecture is illustrated in Fig. 1, which shows the several components involved and their interaction. The GSO collects information (denoted with symbol "i" in Fig. 1) about the road network, road traffic, EVs, CS. It proposes itinerary plans for EVs and performs the corresponding reservations at CS.

SAA architecture integrates authentication and authorization mechanisms to allow EVs to reserve charging time-slots along their itineraries. The SSA architecture, its security modules, and mechanisms are detailed in Section IV.

Fig. 2 illustrates the messages exchanged between EVs and GSO. A four-step process is implemented in the proposed model: 1) authentication and authentication; 2) request and option selection; 3) booking and confirmation; and 4) charging and completion of payment. These steps are described as follows:

1) Authentication and Authorization: The main purpose of this step is to both identify the user and verify that it is authorized to use the GSO's itinerary planning and charging slots reservation service.
2) Request and option selection: At this step, EV sends a request (SchedulingToDest) to GSO. This request comprises information about the EV SoC, current location, and final destination. Once the requests sent by EVs are processed by GSO the later responds by delivering to EVs their corresponding optimal itinerary options (represented in Fig. 2 by (Option {?}).

Note that an optimal itinerary option comprises information both about the road itinerary, the different CSs where the EV needs to stop for charging on that itinerary, the waiting time at each of these CSs, the total estimated duration of the charging operation, and the cost of energy consumption to reach destination through the itinerary. The EV chooses an itinerary option, by sending a corresponding message to GSO (PreferedOption {?} in Fig. 2). Next, the EV receives the acceptance notification from GSO (represented in Fig. 2 by (REP {accept}).

1) *Booking and confirmation:* In this step, the EV makes a final booking request (BookingREQ in Fig. 2). After a successful booking of the corresponding charging time slots at the CSs, GSO sends back an approval to EV (SuccessBook in Fig. 2).
2) *Charging and payment:* After a successful booking, the EV can move to the first CS and proceed with the charging operation.

Three possibilities may occur:

1) EV reaches the CS on the scheduled time. The EV proceeds to charging. The payment is completed before the user unplugs the charger. A message (SuccessPayment) of successful payment is sent to EV.
2) EV will not reach the CS on the desired time, for example, because the EV diverges from its planned itinerary; EV will cancel its booking. A penalty fee may be applied if the user does not cancel the booking at a specified time before the scheduled start of the charging operation.

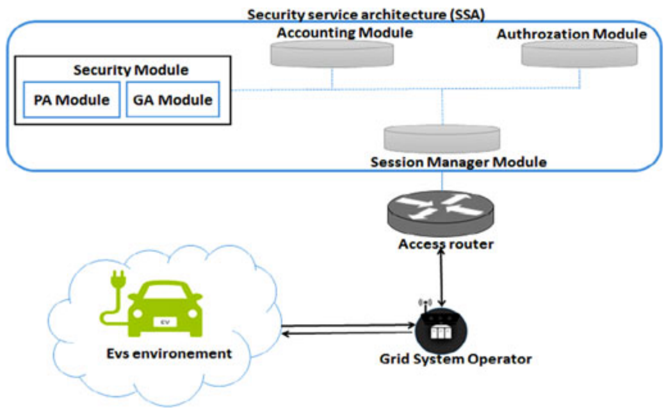

Fig. 3. Security service architecture.

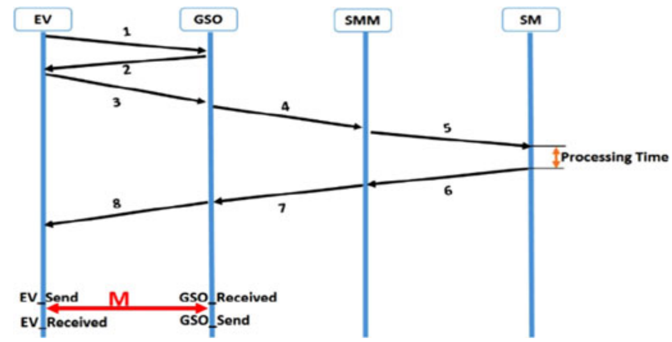

Fig. 4. Security attributes verification, generation and dispatching.

3) EV will not reach the CS on time and wants to reschedule a new charging operation based on its current status (remaining SoC, location, destination). Therefore, GSO starts a new search for available charging options

We note that the EV should remain connected to GSO during the booking process. In case of any incident (e.g., power failure at the CS, EVSE maintenance service, etc.) which may cause a delay at CSs or a change in scheduling, the GSO will deliver a notification message to the EV informing it of any changes in the initial itinerary and charging plan, and presenting it with new options for charging according to the current EV status and trajectory.

IV. Security Service Architecture

In this section, we present the proposed architecture to secure data exchange between EVs and GSO. We assume that EVs can exchange messages directly with GSO. These messages comprise information on EVs, such SoC, destination, and current position. Thus, malicious attackers can use these data to perform unlawful actions such as tracking EVs, disturbing the planning process for EVs, or steal payment information. To protect the wireless interactions of EVs with GSO we use SSA, a SSA which takes charge of securing communications between EVs and GSO. SSA also allows preserving the privacy of EVs. Here, the term "service" refers to the itinerary planning and charging slot booking at CS.

We define a Service Domain as a logical zone that corresponds to a geographical area where the itinerary planning and charging slot booking service is offered by GSO. Fig. 3 shows the elements that fall within the SSA control and that are in charge of processing and validating incoming requests for service from potential users in a Service Domain. In the following, we describe the SSA architecture and its components.

Security module (SM): This module is composed of two submodules: Governmental Authorities (GA) and Private Authorities (PA). The GA module depends on an official authority, such as a governmental entity or a car manufacturer.

We suppose that an official authority carries out control and registration procedures for all EVs to be participating in wireless exchanges with GSO or other entities. The official authority is considered to be responsible of assigning cryptographic material to EVs. This material is to be preloaded in a tamperproof device within EVs to be able, if necessary, to know its real identity. A certified key pairs (public keys and private keys) provided by the official authority allows us to secure EVs communications. Authentication is possible by verifying the validity (nonrevocation) of the public key certificates transmitted by EVs against certificate revocation lists. The public certificates of EVs include their digital signature; thus, allowing their verification. It is worth noting that the security credentials given by the GA can be the same as those intended for securing vehicle–vehicle and vehicle–infrastructure communications [5]. The PA module is in charge of securing service sessions between EVs and GSO. Once the verification of EV public certificate at the GA level is successful, the PA is able to generate shared session keys between the EV and the GSO. Additionally, the PA can create temporary identifiers or pseudonyms for the distribution of session parameters. Exchanges are secured by encrypting the information with EV's public key and GSO public key.

The PA assigns new session keys to an EV each time the EV starts a new session for accessing the service of itinerary planning and charging slot booking. These session keys are temporary for a single session.

Session manager module (SMM): This module is in charge of recovering information from GSO and sending it to the security module. The SMM creates a session ID aggregating all EV session parameters before dispatching the information to the GSO.

Accounting module (ACM): In this module, EV session parameters are recorded for accounting purposes. The ACM may follow specific policies for maintaining and updating records of sessions. We assume that there must be a preestablished relationship between the user and the GSO for accounting purposes.

Authorization module: This module grants access to the service of itinerary planning and charging slot reservation at CS. Authorization is granted after validation from the previous modules.

Fig. 4 illustrates the exchanges between EV, GSO, and the SSA modules for security attributes verification, generation, and dispatching.

First, EVs send an initial request to GSO notifying them about their presence (arrow 1). In the second stage (arrows 2 and 3), GSO asks EV about its security attributes (public key certificate). Then, GSO collects this information and sends it to the session manager (arrow 4) where a session ID is generated

Communication	Exchange of data
$EV \xrightarrow[3]{} GSO$	$Cert_{EV}$, Seq_{EV}
$GSO \xrightarrow[4]{} SMM$	$Cert_{EV}$, Seq_{EV}, $Cert_{GSO}$, Seq_{GSO}
$SMM \xrightarrow[5]{} SM$	$Cert_{EV}$, Seq_{EV}, $Cert_{GSO}$, Seq_{GSO}, SS_{id}
$SM \xrightarrow[6]{} SMM1 \xrightarrow[7]{} GSO$	$Enc\{ID^P_{EV}, SS_{id}, Kss, T, Seq_{EV},\}K_{EV-SM}$
$SM \xrightarrow[6]{} SMM2 \xrightarrow[7]{} GSO$	$Enc\{ID^P_{GSO}, SS_{id}, Kss, T, Seq_{GSO},\}K_{GSO-SM}$
$GSO \xrightarrow[8]{} EV$	$Enc\left\{\begin{matrix} ID^P_{EV}, SS_{id}, Kss, T, \\ Seq_{EV}, \end{matrix}\right\} K_{EV-SM}, Cert_{GSO}$
EV	*Decryption of message with Kss*
GSO	*Decryption of message with Kss*

Fig. 5. Security attributes used.

TABLE I
SYMBOLS

Symbol	Definition
$\mathrm{ID}^P_{\mathrm{GSO}}$	GSO pseudonym
$\mathrm{ID}^P_{\mathrm{EV}}$	EV pseudonym
k_{ss}	Session key
$\mathrm{Cert}_{\mathrm{GSO}}$	GSO certificate
$\mathrm{Cert}_{\mathrm{EV}}$	EV certificate
$\mathrm{Seq}_{\mathrm{EV}}$	EV sequence number
$\mathrm{Seq}_{\mathrm{GSO}}$	GSO sequence number
SS_{id}	Session ID
$K_{\mathrm{EV-SM}}$	Shared key EV-SM
$K_{\mathrm{GSO-SM}}$	Shared key EV-SM
T	Timestamp
A_C	Vehicle front area
C_D	Aerodynamic drag coefficient
ρ_a	Air density
M	Vehicle mass
g	Gravity acceleration
a	Acceleration
V	limit Velocity
K_{roll}	Rolling coefficient
$\mathrm{List}^{\mathrm{Slot}}$	List of occupied slots within CSs
NEVSE	Number of EVSE at CS
N_C	Total number of EVs under charging
W_Q	Total time of EVs (Queue)
W_C	EVSE that has a minimum charging time
R_{Charging}	Charging power at CS
N_q	Total number of EVs Physical queue

(arrow 5). The SM receives the processed data from the session manager where the key certificate of EV and GSO need to be verified. Next, the SM generates session keys and pseudonyms for EV and GSO. The data exchanges between EV and SM on the one hand, and GSO and SM on the other hand, are encrypted by their shared private key $\mathrm{K}_{\mathrm{EV-SM}}$, and $\mathrm{K}_{\mathrm{GSO-SM}}$, respectively (arrows 6, 7, 8). It is worth noting that the exchanges in arrows 1–8 correspond to the authentication and authorization part of Fig. 4.

Finally, GSO and EV will have the same Session Key (K_{ss}) so that all the messages can be encrypted and decrypted using K_{ss} (arrow M illustrated in Fig. 4). Fig. 5 gives the detailed content of messages exchanged and the security attributes used. Table I summarizes the notations.

It is worth noting that the proposed architecture guarantees security and privacy for the itinerary planning and charging reservation service without generating excessive wireless communication overhead between the EV and the GSO. For the generation of digital signatures, one can consider, for example, the packet size of the RSA cryptographic scheme with a fixed length of 128 bytes [5].

Temporary user pseudonyms of 32 bits can also be considered by using SHA-1 operations. Indeed, the introduction of these security attributes involves a packet overhead that will be reflected on spending additional processing resources with a subsequent increase in the overall end-to-end communication delay. Nevertheless, this extra overhead, securing EV-GSO communications requires some desired level of robustness of the system to face network threats, and to ensure the confidentiality of communications and privacy of EVs, which are effectively addressed by the SSA.

In terms of additional messaging, as illustrated in Fig. 4, the communication exchange between EV and GSO for security credentials verification, generation, and dispatching involves only four wireless messages (arrows 1, 2, 3, and 8) whose content is explained in Fig. 5. This number of message is linear with the number of EVs.

V. Itinerary Planning and Charging Slots Reservation

A. System Description

Let us consider an EV, which sends a request to GSO asking for itinerary planning to attain its destination. The plan should also comprise information regarding when to stop for charging at which CSs along the itinerary. We consider that the EV is interested in the itineraries that are the most economical in terms of energy consumption while minimizing the waiting time at CSs. Of course, energy consumption is highly correlated with the distance travelled, so often the most energy cost-effective itineraries will be the shortest.

Minimizing the waiting time also means arriving to destination sooner should the considered itineraries be the same length. GSO interacts with the EV and neighboring CSs in order to determine the optimal itinerary based on the current status of EVs (i.e., SoC, current location, and destination), the status of CSs, the road network layout and road segments' speeds, and current traffic. The GSO manages different constraints and limitations imposed by EVs and CSs to deliver optimal charging options and economic paths for EVs. The constraints imposed by EVs regard the remaining battery charge (SoC) allowing the EV to attain a maximum distance (range) without recharging its battery; and the destination, which promotes choices of CS close to the shortest itinerary. The EV can also add constraints regarding the duration of charging.

For CSs, the constraints regard their number, geographical distribution, and capacity of charge (i.e., number of charging point EVSE). Consequently, the GSO needs to run multiple analyses in order to determine the optimal solutions for EVs.

Optimal solutions should minimize the waiting time of EVs, and energy consumption from the current location to destination.

Before detailing how optimal routes are computed by GSO, let us define the different parameters used for such computation:

Layout of road network: we define $H(N, E)$ as a graph combining a set of nodes $N = \{N_1, N_2, N_3, \ldots, N_n\}$, where N_j is the intersection of edges, and $E = \{E_1, E_2, E_3, E_4, E_5, \ldots, E_m\}$, where E_e denotes the edge *e* in the graph $H(N, E)$. Nodes can be the intersection of road segments or can be the locations of CSs. The number of edges and nodes are denoted, respectively, by $|E|$ and $|N|$. GSO determines the graph $H(N, E)$ that contains all roads in a Service Domain.

CSs infrastructure: we denote by CS = {CS1, CS2 .....CSk} the location of CSs. |CS| represents the number of CSs; each station contains a number of EVSE characterized each by some fixed power. It is worth noting that CS is a subset of *N*.EV*s*: the positions of EVs are represented by the set $\mathrm{O} = \{\mathrm{O}_1, \mathrm{O}_2, \mathrm{O}_3 \ldots .. \mathrm{O}_\mathrm{X}\}$. $|O|$ denotes the number of EVs; each EV has a specific final destination D.

B. Energy Consumption

We model the EV itinerary planning through graph theory and linear programming LP. The leftmost part of Fig. 8 illustrates a graph with the direct path, where an EV can reach the destination without looking for a CS during its trip. We use the principals of vehicles' dynamics to compute the energy consumption of EVs. First, we calculate the summation of forces, which is the traction force, needed by the EV to move at a given speed

$$\sum F = F_{\text{roll}} + F_{\text{grade}} + F_{\text{air}} + F_{\text{acc}} \tag{1}$$

where

F_{roll} is the rolling resistance force between pneumatic tires and the road

$$F_{\text{roll}} = K_{\text{roll}} \cdot M \cdot g \cdot \cos(\theta) \tag{2}$$

where is θ is the road grade or slope.

F_{grade} represents the force of the gravity

$$F_{\text{grade}} = M \cdot g \cdot \sin(\theta). \tag{3}$$

F_{air} is the aerodynamics force of the EV against the air. It depends on the speed of the vehicle.

The speed is, however, not constant along an edge; indeed, an edge can be composed of several successive subedges, each having different speed limits. At each subedge, we use the speed limit established by the TA to calculate the energy consumption of EV. Therefore, each edge will be composed of several subedges. Let each subedge be denoted by $[S_{ij}, \ V_{ij}]$, where S_{ij} is the distance and V_{ij} is the speed limit of the edge, and *i* and *j* are the points of the road delimiting the subedge.

This is illustrated in the rightmost part of Fig. 6. Then,

$$F_{\text{air}_{ij}} = \frac{1}{2} \cdot \rho_a \cdot C_D \cdot A_C \cdot {V_{ij}}^2 (S_{ij}) \tag{4}$$

where $F_{\text{acc}_{ij}}$ represents the inertia of the vehicle

$$F_{\text{acc}_{ij}} = M \cdot a(S_{ij}). \tag{5}$$

From (1), the power needed to move EV at the speed limit is given by

$$P = v \sum F. \tag{6}$$

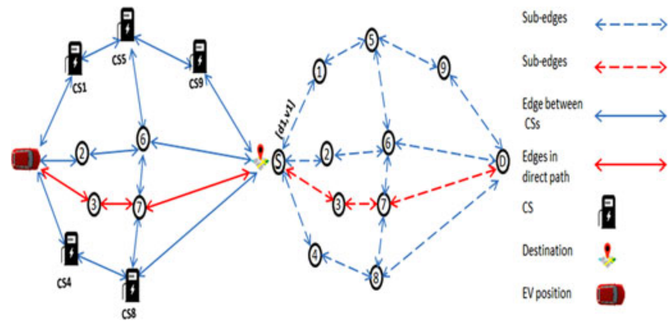

Fig. 6. Graph illustrating the road network with velocity limits and distance weight of each sub-edge.

Let η_m be the efficiency of the electric engine motor. Then

$$\text{Cons}_{ij} = S_{ij} * \sum \text{F} * \eta_m \tag{7}$$

where Cons_{ij} is the consumption of the subedge. Using the energy consumption of a subedge, we can compute the edge energy consumption by summing up the energy consumptions over all the edge

$$\text{Cons}_e = \sum_{i,j} \text{Cons}_{ij} \tag{8}$$

where i, j are the points delimiting the successive subedges of edge E_e.

Subsequently, the information about the consumption in each edge is appended to graph $H(N, E)$.

Finally, to calculate the energy consumption needed by an EV to travel from its initial position to final destination, we can sum up the total power consumption of each edge along a route as

$$\text{Cons}_{\text{route}} = \sum_{e=1}^{m} \sum_{i,j} \text{Cons}_{ij}. \tag{9}$$

We define as first objective to minimize the energy consumption for each EV to reach its final destination without consideration to recharging operations during the trip. An integer-programming model is introduced to minimize the total energy cost of travelling from source to destination. We formulate the objective as follows:

Input:

$\mathbf{B_c}$:	is the battery capacity of EV.
$\mathbf{SoC^a_{des}}$:	is the minimum SoC that is acceptable when arriving at destination. This is the minimum SoC that needs to remain at the EV, so that it can reach some CS in future, and not be trapped at destination.
$\mathbf{Cons_{ij}}$:	Energy consumption between i and j.
$\mathbf{SoC_i}$:	Initial state of charge of EV.

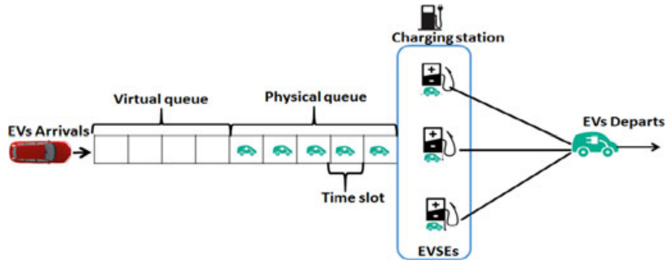

Fig. 7. Schematic view of CS model.

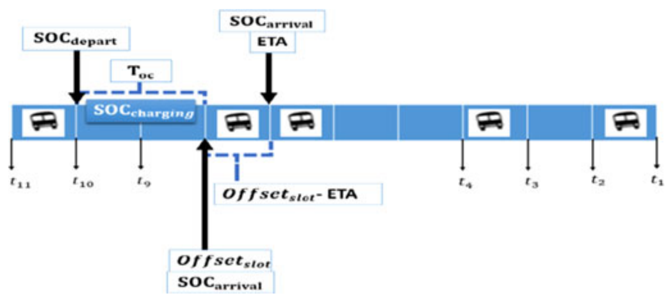

Fig. 8. Illustration of the parameters used for waiting time minimization.

SMART-EV-Slots

Input: EV_vector, CS_vector.
Output : $\text{List}^{\text{slot}}$ /*List of CS slots occupied*/

```
1.  Initialization W_Q,W_C,slot_min;
2.  For(each CS) do
3.     if(N_c<NEVSE) then
4.        W_c <— 0;
5.     else
6.        for(each EV in EVSEs) do
7.           if((EV^target − EV^Current)/R_charging ≤ slot_min)then
8.
9.              W_c <— (EV^target − EV^Current)/R_charging;
10.
11.          endif
12.       Endfor
13.    endif
14.    For(each EV in physical queue) do
15.       W_Q <— W_Q+ (EV^target − EV^Current)/R_charging;
16.
17.   Endfor
18.     W <— W_Q+W_C; /*Waiting time at each CS*/
19.    For(each slot in virtual queue) do
20.    /*Check all slots occupied in virtual queue */
21.       if(slot is booked) then
22.          Add slot to the List^slot
23.          Add W(N_q) to the List^slot
24.       endif
25.    Endfor
26. Endfor
27. Update List^slot
```

Variables:

$\mathbf{X_{ij}}$: Binary variable takes value 1 or 0.

Objective:

$$\text{Min} \sum_{e=1}^{m} \sum_{i,j} \text{Cons}_{ij} . X_{ij} \tag{10}$$

Subject to:

$$\text{SoC}_i \ \leq B_c \tag{11}$$

$$\text{SoC}_i - \frac{\text{Cons}_{\text{route}}}{B_c} \geq \text{SoC}^{a}_{\text{des}} \tag{12}$$

$$X_{ij} \begin{cases} 1, & \text{if there exsite a path between node } i \text{ and node } j \\ 0, & \text{otherwise} \end{cases} \tag{13}$$

In the case that the EV cannot reach its destination through a direct path (i.e., without recharging), because the energy is not sufficient, the GSO needs to return to the EV a list of public CSs where it needs to stop, along with specific information such as the waiting time at stations.

C. Algorithm

In this section, we consider the case where the EV needs to stop and recharge at one or several reCSs during its trip, in order to reach destination. At this stage, the nodes which are not CSs (not part of CS) are discarded from the graph, and the edges parting from each one of these nodes are joined. The resulting graph comprises only CSs as nodes.

We propose a smart algorithm based on the modeling of CS, as comprising two kinds of queues as illustrated in Fig. 7: virtual queues which correspond to reservations of time slots made by the GSO at CS, and physical queues corresponding to real queues at a CS.

Algorithm I , named SMART-EV-slots, illustrates the operations of both physical and virtual EV queuing at CSs.

To analyze the complexity of our algorithm, we consider worst-case scenario. We note $\text{n} =$ number of CS, $\text{m} =$ number of EVSEs, $\text{Lq} =$ queue length of the physical queue, and $\text{Ns} =$ number of slots in the virtual queue. In this algorithm, nested loops between line 2–26 consume $\text{O}\,(\text{n} * \text{m}) + \text{O}\,(\text{n} * \text{Lq}) + \text{O}\,(\text{n} * \text{Ns})$. Line 17 takes linear time O(n) in the worst case. The rest of the algorithm (e.g., initialization, assignment, etc.) takes O(1). Hence, we can see that our complexity is in order O (n∗(m+Lq+Ns)).

To verify the reachability of the next CS, or destination by EV, starting from a charging station CS_i, we need to compare the state of charge of the EV after charging at CS_i, with the expected consumption to reach the next CS. We have

$$\text{SoC}_{\text{depart}}\,(\text{CS}_i) \ = \begin{cases} \text{EV}_c^{\text{after}}\,(\text{CS}_i) - \text{EV}_c^{\text{before}}\,(\text{CS}_i) \\ \underline{\text{slot}_{\text{time}}(\text{CS}_i) * R_{\text{recharge}}} \\ \quad B_c \end{cases} \tag{14}$$

$$\text{SoC}_{\text{Cons}}\,(\text{e}) \ = \frac{\text{Cons}_e}{\text{Battery}_{\text{Capacity}}} \tag{15}$$

where

$\text{SoC}_{\text{Cons}}(\text{e})$:	is the energy consumption of the EV on edge Ee.
$\text{EV}_c^{\text{after}}(\text{CS}_i)$:	SoC of EV after charging at station CS_i.
$\text{EV}_c^{\text{before}}(\text{CS}_i)$:	SoC of EV before charging at station CS_i.
Cons_e:	Energy consumption of the edge(e).
Ee:	The edge between CS_i and the next CS.
$\text{slot}_{\text{time}}(\text{CS}_i)$:	The free charging slots at station CS_i.
R_{recharge}:	Charging power at the CS. This value is supposed constant as we consider all stations to be of the same level.

The next CS reachable by EV in the following condition is satisfied:

$$\mathrm{SoC}_{\mathrm{depart}}\,(i) \geq \mathrm{SoC}_{\mathrm{Cons}}\,(i)\,. \tag{16}$$

We verify that the sum of energy demand $E_d^t\,(\mathrm{CS}_i)$ at station CS_i is smaller than the CS capacity W_{CS_i} as follows:

$$E_d^t\,(\mathrm{CS}_i) \leq W_{\mathrm{CS}_i}\,. \tag{17}$$

All nodes where that inequality is not true are discarded. Next, we build a new graph using Yen's *k*-Shortest Path algorithm [36]. We calculate the *K*-shortest path in terms of energy consumption; for each shortest path, we calculate the waiting time and add it to the *K*-shortest path in terms of consumption. The value of *K* is defined by the EV. For each path, the optimal waiting time is computed as follows:

The booking algorithm selects the suitable slots of CSs based on the minimization of T_w detailed below.

Input:

$\mathbf{Offset}_{\mathbf{slot_{ij}}}$:	is the recharging start time in station j of the EV arriving from station i.
$\mathbf{ETA_{ij}}$:	denotes the arrival time at station j of the EV arriving from station i.
$\mathbf{Cons_{ij}}$:	is the estimated consumption between stations i and j.
$\mathbf{SoC}_{\mathbf{depart_{ij}}}$:	is the state of charge of the EV after charging in j arriving from station i.
B_c:	Battery capacity of EV
$\mathbf{SoC_i}$:	Initial state of charge of EV.

Variables:

$\mathbf{X_{ij}}$:	Binary variable takes value 1 or 0.

$$\mathrm{Min}\left\{T_w = \sum\nolimits_{j=1}^{n}\sum\nolimits_{i=1}^{n}\left(\mathrm{Offset}_{\mathrm{slot}_{ij}} - \mathrm{ETA}_{ij}\right) * X_{ij}\right\} \tag{18}$$

Subject to:

$$\mathrm{SoC}_{\boldsymbol{des}}^{\boldsymbol{a}} \leq \left\{\mathrm{SoC}_{\mathbf{destination}} = \left(\sum_{\boldsymbol{j=1}}^{\boldsymbol{n}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}}\mathrm{SoC}_{\mathbf{depart}_{\boldsymbol{ij}}} - \frac{\mathrm{Cons}_{\boldsymbol{ij}}}{\boldsymbol{B_c}}\right) * \boldsymbol{X_{ij}}\right\} \tag{19}$$

$$\left\{\mathrm{SoC}_{\mathbf{destination}} = \left(\sum_{\boldsymbol{j=1}}^{\boldsymbol{n}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}}\mathrm{SoC}_{\mathbf{depart}_{\boldsymbol{ij}}} - \frac{\mathrm{Cons}_{\boldsymbol{ij}}}{\boldsymbol{B_c}}\right) * \boldsymbol{X_{ij}}\right\} \leq \boldsymbol{\varepsilon} + \mathrm{SoC}_{\mathbf{des}}^{\boldsymbol{a}} \tag{20}$$

$$\mathrm{SoC}_{\boldsymbol{i}} \leq \boldsymbol{B_c} \tag{21}$$

$$\boldsymbol{X_{ij}} = \begin{cases} 1, & \text{if the vehicle leaves station } i \text{ to station } j \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

The input parameters are illustrated in Fig. 8. Using the driving time for each subedge delimited by points *m* and *n*, we can calculate the estimated time of arrival ETA_{mn}.

The driving time is given as follows:

$$T_{mn} = \frac{D_{mn}}{V_{ij}\ (1 - Tr_{mn})}. \tag{23}$$

The traffic density factor of each subedge is defined by Tr_{mn} which is varied from 0 (no traffic) to 1(blocking of the subedge), therefore Tr_{mn} has a major effect on travel speed

$$Tr_{mn} = \frac{{K_d}^{mn}}{k_{jam}^{mn}} \tag{24}$$

where ${K_d}^{mn}$ is the vehicle density (expressed by vehicles/km) on the subedge delimited by i and j between the current EV position and next destination.

k_{jam}^{mn} represents the traffic density on the subedge.

The travel time T_{ij}^{Travel} of each edge delimited by *i* and *j* is calculated from the current position of EV to CS. This is computed by summing up the driving time of each sub-edge as

$$T_{ij}^{\mathrm{Travel}} = \sum T_{\mathrm{mn}}. \tag{25}$$

Using the travel time, we can estimate the arrival time at each station by summing up the current time of departure and travel time on the edge

$$\mathrm{ETA}_{ij} = T_j^{\mathrm{arrival}} = \mathrm{T}_i^{\mathrm{current}} + \mathrm{T}_{\mathrm{ij}}^{\mathrm{Travel}} \tag{26}$$

where T_j^{arrival} is the time for an EV to arrive to station *j* to recharge its battery, from station i, where it is at time T_i^{current}.

An EV can choose the best CSs in terms of consumption energy and waiting time based on

$$\mathrm{Z} = \alpha\mathrm{C} + (1 - \alpha)\,\mathrm{W} \tag{27}$$

$$0 \leq \alpha \leq 1 \tag{28}$$

where

C:	is the energy consumed by the EV to reach the destination.
W:	denotes the sum of waiting times of all CSs to reach the destination by the EV.
α:	represents the weight given to energy consumption and waiting time. During the trip, when the EV choses a big value of α, this means that the EV prefers to select the path with less energy consumption, and conversely.

We define specific cases of α as follows:

Case1: the EV prefers to book charging slots based on the shortest path, in terms of energy consumption, to reach the destination; $\alpha = 1$.

Case2: the EV prefers to book charging slots based equally on minimizing energy consumption and minimizing waiting time; $\alpha = 0.5$.

Case3: the EV prefers to book charging slots based the shortest path, in terms of minimum waiting time; $\alpha = 0$.

VI. Simulation Results

In this section, we present the simulation results of the itinerary planning and charge slot reservation scheme.

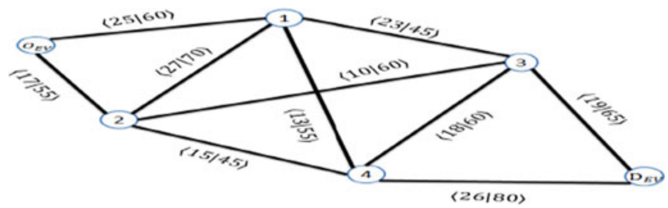

Fig. 9. Simulated graph.

TABLE II
VEHICLE SPECIFICATIONS USED IN THE MODEL

Symbol	Value	Unit
A_C	2.4	m^2
C_D	0.35	–
ρ_a	1.223	kg·m
M	1000	kg
g	9.81	m/s^2
K_{roll}	0.02	–

TABLE III
DATASET FOR THE SIMULATION

Node i	Node j	Predecessor	$Cons_{ij}$/ $Battery_{capacity}$ [%]	Waiting time [min]	SoC_{depart} [%]
O_{EV}	2	–	45	–	70
2	D	O	90	17	80
2	3	O	40	17	75
3	D_{EV}	O-2	50	15	90
		O	50	12	70
O_{EV}	2	–	45	–	75
2	D	O	90	10	90
2	4	O	50	10	80
4	D_{EV}	O-2	55	7	75
		O	55	20	85
O_{EV}	1	–	65	–	70
1	D	O	80	10	91
1	4	O	40	10	70
4	D_{EV}	O-1	55	20	75
		O	55	14.5	60

To simplify the simulation of the itinerary planning strategy, we assume a speed limit at each edge to be constant as shown in Fig. 9. We consider a geographic area where the CSs are randomly deployed. The locations of EVs and destination are also randomly chosen. The parameters of the simulation illustrated in Table II were taken from the EV prototypes which were build by Université de Sherbrooke based on eVUE vehicles [35].

These values allow us to estimate the energy consumption of the EV according to (9). First, we assume that the simulated scenario verifies the reachability and energy demand conditions in (16) and (17). Then, we use MATLAB to calculate the K-shortest path [34] with $K = 3$.

The simulation of the proposed scenario illustrated in Fig. 9 gives three best routes, from the current location of EV to the destination (chosen randomly), in terms of energy consumption. The three best routes are

Route1: O-2-3-D.
Route2: O-2-4-D.
Route 3: O-1-4-D.

Depending on the SoC of the EV, it may require to be recharged to reach the destination. The waiting time in the whole trip should be minimized as in (18). The problem is linear and can be solved using IBM ILOG CPLEX Optimization Studio. To solve the linear problem, we present an example for finding the best route in terms of waiting time for the EV from its current location to the final destination. As parameters values used in the scenario, we consider that the initial EV SoC is uniformly distributed between 45% and 90%, the EV SoC is sufficient to arrive to the first CS, the waiting time in each station is uniformly distributed between 7 and 90 mn, the percentage of energy consumption is uniformly distributed between 45% and 90%, and $\mathrm{SoC}_{\mathrm{destination}}^{\mathrm{alarm}} = 30\%$.

Using the data in Table III as a dataset, the IBM ILOG CPLEX Optimization Studio finds out the optimal solution, where

$$\mathrm{Waitingtime}_{\mathrm{Route3}} < \mathrm{Waitingtime}_{\mathrm{Route2}} < \mathrm{Waitingtime}_{\mathrm{Route1}}.$$

The optimal solution includes the following paths:

Route1: includes one charging station (CS3).
Route2: includes two charging stations (CS2, CS4).
Route3: includes one charging station (CS4).

After having computed the minimum waiting time of each path, (27) with different cases will be used. The GSO then advertises the optimal choice options to EVs. The service includes optimal paths to reach destination in terms of energy consumption along with the waiting time for each path. The EV can make its choice and notify the GSO with the chosen option. For example, if the EV (driver) wants just to minimize energy consumption and has no concern for the waiting time, the GSO will use the best solution in terms of energy consumption when making reservations at CSs.

Indeed, depending on the choice made by the EV, a set of time slots are reserved in the corresponding CSs.

VII. CONCLUSION AND FUTURE WORK

In this paper, we presented a secure architecture of EVs charge planning. The architecture aims at minimizing the waiting time of charging and/or power consumption of EVs during their journey to attain a destination. Simulations proved that our model is able to provide optimal paths in terms of energy consumption and waiting time. To ensure secure bidirectional communications between GSO and EVs, we further introduced a Security Service Architecture (SSA), which deals with the authentication and authorization of EVs to access the charge scheduling and itinerary planning service.

In our future work, we will take into account additional parameters in the optimization process such as the minimization of charging cost. In addition, we will consider various charging levels in the CSs.

REFERENCES

[1] EV World, “There are now half-a-million electric cars on the planet,” Jul. 2014. [Online]. Available: http://www.evworld.com/news.cfm?newsid=33579

[2] A. Ipakchi and F. Albuyeh, “Grid of the future,” *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar./Apr. 2009.

[3] C. Caruso, "Why range anxiety for electric cars is overblown," *MIT Technol. Rev.*, Aug. 2016. [Online]. Available: www.technologyreview.com
[4] Whitepaper, "How the smart grid enables utilities to integrate electric vehicles," [Online]. Available: http://www.silverspringnet.com/wp-content/uploads/SilverSpring-Whitepaper-ElectricVehicles.pdf. [Accessed: 27 Sep. 2017].
[5] E. S. Coronado and S. Cherkaoui, "Performance analysis of secure on demand services for wireless vehicular networks," *Secur. Commun. Netw.*, pp. 114–129, 2010.
[6] S. Dhaou, S. Cherkaoui, and L. Khoukhi, "Queuing model for EVs charging at public supply stations," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf.*, 2013, pp. 65–70.
[7] S. Dhaou, S. Cherkaoui, and L. Khoukhi, "Guidance model for EV charging service," in *Proc. Int. Conf. Commun.*, 2015, pp. 5765–5770.
[8] R. Abousleiman and O. Rawashdeh, "A bellman-ford approach to energy efficient routing of electric vehicles," in *Proc. Transp. Electrification Conf. Expo.*, 2015, pp. 1–4.
[9] R. Abousleiman and O. Rawashdeh, "Tabu search based solution to the electric vehicle energy efficient routing problem," in *Proc. Transp. Electrification Conf. Expo.*, 2014, pp. 1–6.
[10] M. Faraj and O. Basir, "Optimal energy/time routing in battery-powered vehicles," in *Proc. Transp. Electrification Conf. Expo.*, 2016, pp. 1–6.
[11] J. Rezgui, S. Cherkaoui, and S. Dhaou, "A two-way communication scheme for vehicles charging control in the smart grid," in *Proc. 8th Int. Wireless Commun. Mobile Comput. Conf.*, 2012, pp. 883–888.
[12] J. D. Adler, P. B. Mirchandani, G. Xue, and M. Xia, "The electric vehicle shortest-walk problem with battery exchanges," *Netw. Spatial Econ.*, vol. 16, no 1, pp. 155–173, 2016.
[13] A. Ruzmetov, A. Nait-sidi-moh, M. Bakhouya, and J. Gaber, "Towards an optimal assignment and scheduling for charging electric vehicles," in *Proc. Renewable Sustain. Energy Conf.*, 2013, pp. 537–541.
[14] H. G. Chale-gongora, O. D. Weck, A. Doufene, T. Ishimatsu, and D. Krob, "Planning an itinerary for an electric vehicle," in *Proc. Energy Conf.*, 2014, pp. 1385–1391.
[15] S. Mehar, S. M. Senouci, and G. Remy, "EV-planning: Electric vehicle itinerary planning," in *Proc. Smart Commun. Netw. Technol.*, 2013, pp. 1–5.
[16] H. Akbari and X. Fernando, "Modeling and optimization of PHEV charging queues," in *Proc. Elect. Comput. Eng.*, 2015, pp. 81–86.
[17] U.S. NIST, "Guidelines for smart grid cyber security, " vol. 1 to 3), NISTIR-7628, Aug. 2010.
[18] P. Chen, S. Cheng, and K. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, Aug. 2012.
[19] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grid," *IEEE Commun. Surveys Tuts*. vol. 14, no. 4, pp. 981–997, Oct.–Dec. 2012.
[20] Z. Fan *et al.*, "Smartgrid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts*., vol. 15, no. 1, pp. 21–38, Oct.–Dec. 2013.
[21] X. Fang, S. Misra, G. Xue, and D.Yang, "Smart grid the new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, Oct.–Dec. 2012.
[22] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli,, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[23] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no 10, pp. 11883–11915, 2015.
[24] M. Mustafa, N. Zhang, and Z. Fan, "Smart electric vehicle charging: Security analysis," in *Proc. IEEE PES Innovative Smart Grid Technol.*, Feb. 2013, pp. 1–6.
[25] R. Falk and S. Fries, "Securely connecting electric vehicles to the smart grid," *Int. J. Adv. Internet Technol.*, vol. 6, no 1-2, pp. 57–67, 2013.
[26] M. Stegelmann and D. Kesdogan, "Location privacy for vehicle-to-grid interaction through battery management," in *Proc. IEEE 9th Int. Conf. Inf. Technol. New Gener.*, 2012, pp. 373–378.
[27] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. Yang, and M. Guizani, "Securing vehicle-to-grid communications in the smart grid," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 66–73, Mar. 2013.
[28] 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 *Proc. Symp. Des. Anal. Intell. Veh. Netw. Appl.*, New York, NY, USA, 2013, pp. 45–54.
[29] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, and V. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations," in *Proc. Comput. Commun. Workshops*, 2013, pp. 55–60.
[30] H. Liu, H. Ning, Y. Zhang, L. T. Yang, and M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 99–110, Mar. 2013.
[31] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Security and privacy-preserving mechanism for aggregator based vehicle-to-grid network," in *Proc. Int. Conf. Ad Hoc Netw.*, 2014, pp. 75–85.
[32] H. Guo, Y. Wu, H. Chen, and M. Ma, "A batch authentication protocol for V2G communications," in *Pro. 4th IFIP Int. Conf. New Technol. Mobility Secur.*, 2011, pp. 1–5.
[33] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, "Aggregated proofs based privacy-preserving authentication for V2G networks in the smart grid," *IEEE Trans. Smart Grid,*, vol. 3, no. 4, pp. 1722–1733, Dec. 2012.
[34] J. Y. Yen, "Finding the k shortest loopless paths in a network management science," *Manage. Sci.,* vol. 17, no. 11, pp. 712–716, 1971.
[35] ATEUS. [Online]. Available: http://mecano.gme.usherbrooke.ca/∼vue/, Accessed on: Nov. 1, 2016.

Achraf Bourass received the B.S. (Hons.) degree in mechatronics from the National Schools of Applied Science, Tetouan, Morocco, in 2014. He is currently working toward the M.Sc. degree in electrical engineering at Interlab, Université de Sherbrooke, QC, Canada.

He was a Mechatronics Engineer with Amaynotech, Morocco. He has worked on the "Optimal integration of rechargeable vehicles into the grid" project, supported by Quebec's Ministry of International Relations and La Francophonie (MRIF), within the Franco-Quebec cooperation. His research interests include electric vehicles, smart grid, autonomous connected electric, hybrid vehicles, robotics and UAV control.

Soumaya Cherkaoui (M'99–SM'15) received a Bachelor degree in computer engineering, from EMI engineering school, Rabat, Morocco in 1992, and a Ph.D degree in electrical engineering from université de Sherbrooke, Sherbrooke (QC), Canada in 1998. She is currently a Professor in the Department of Electrical and Computer Engineering, Université de Sherbrooke, QC, Canada. Since 2000, she has been the Director of Interlab, a research laboratory that conducts research funded by both government and industry. Before joining U. Sherbrooke as a faculty member, she worked for the industry as a project leader on projects for the aerospace industry. She coauthored of more than 200 publications in reputable journals and conferences.

She is a Professional Engineer in Quebec, Canada.

Lyes Khoukhi (M'08) received the Ph.D. degree in electrical and computer engineering from the University of Sherbrooke, Sherbrooke, QC, Canada, in 2006.

In 2008, he was a Researcher with the Department of Computer Science and Operations Research, University of Montreal, QC, Canada, Since 2009, he has been an Assistant Professor with the University of Technology of Troyes, Troyes, France. His research interests include vehicular networks, M2M & IoT, cloud, performance evaluation, and security.