ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
Your ulti-MATE Research Paper !!!

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018.

Optimization and Authentication of Itinerary Scheduling Service for Electric Vehicles

K. Muthukumar[1], P. Suganthi[2], M. Reshma[3]
Assistant Professor, EEE, Sri Krishna College of Engineering & Technology, Coimbatore, India[1]
II Year Student, EEE, Sri Krishna College of Engineering & Technology, Coimbatore, India[2]
II Year Student, EEE, Sri Krishna College of Engineering & Technology, Coimbatore, India[3]

***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 — EV, itinerary planning, waiting time, smart grid.

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 tons in terms of equivalent CO2 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 over 500 000 registered EVs around the world and 2.7 million more EVs are expected to join the roads by 2018 [1].

Despite the increasing popularity of EVs, some of the important issues that restrain a mass adoption of EVs are the limited range 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 charging stations), 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 charging stations 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 charging station choices.

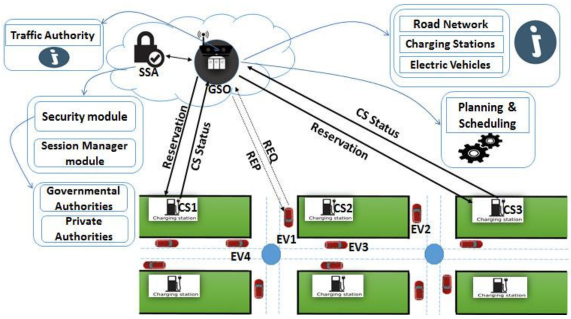


Fig.1. Itinerary Planning Architecture

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 charging stations 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 charging station by choosing the charging station 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 charging stations 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], the authors proposed a new communication protocol for the reservation process between EVs and the charging stations. However, in [10] and [11], issues related to traffic and overall EV energy consumption was 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], the authors proposed a scheduling algorithm of EVs at charging stations based on the SoC, the travel distance to the stations and road traffic. However, this work does not minimize the queuing time in the stations nor does it consider the destination location. In [14], a generalized multi commodity network flow (GMCNF) was used in a multi-criteria EV routing problem to minimize the cost and/or the time to reach the final destination. In [15], the authors 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 charging stations, EV position, destination, EV SoC, road conditions). The problem of waiting time at charging stations was not addressed in [14] and [15] even though charging stations may have significant queueing time. In [16] authors focused on queuing time and the shortest path to assign an EV to a single charging station; however, the work does not consider traffic, overall EV energy consumption, and destination position.

Battery exchange nor the waiting time at stations in their model. In [13], the authors proposed a scheduling algorithm of EVs at charging stations based on the SoC, the travel distance to the stations and road traffic. However, this work does not minimize the queuing time in the stations nor does it consider the destination location. In [14], a generalized multi commodity network flow (GMCNF) was used in a multi-criteria EV routing problem to minimize the cost and/or the time to reach the final destination. In [15], the authors 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 charging stations, EV position, destination, EV SoC, road conditions). The problem of waiting time at charging stations was not addressed in [14] and [15] even though charging stations may have significant queueing time. In [16] authors focused on queuing time and the shortest path to assign an EV to a single charging station; 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 (DoS), 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. The authors 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], the authors proposed an authentication scheme between EVs and charging stations. This scheme aims at securing EV sensitive information based on EV pseudonyms to impede third parties from monitoring EV movements. In [30], the authors 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], [32] various schemes were presented which aim at ensuring the confidentiality of EV data. In [33], the authors 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 work, we propose a secure architecture, which ensures confidentiality of information, privacy for authentication and authorization mechanisms for reserving charging slots at charging stations.

III. SYSTEM ARCHTICETURE

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 charging stations 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 charging stations (CS) along the road network. CS can exchange information with the 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 charging stations, 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 i) their remaining SoC allowing them to attain a maximum distance without recharging their battery; and

The EVs destination, which poses a particular constraint about the trajectory to be travelled. Indeed, the suggested charging stations should be as near as possible to the shortest path trajectory. For public charging stations, the limitations are related mainly to their number, geographic distribution, and their charging capability (i.e., number of charging points or electric vehicle 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) the 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:

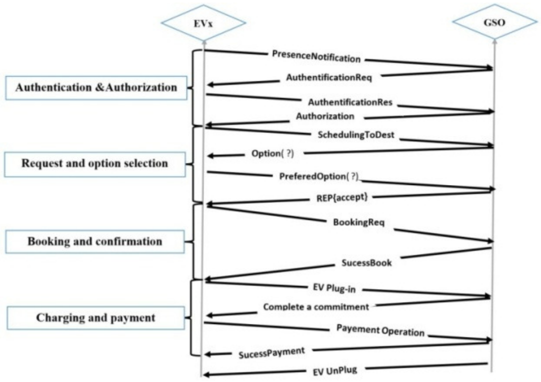


Fig.2 Sequence diagram of the booking process.

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 (Scheduling To Dest) 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 charging stations where the EV needs to stop for charging on that itinerary, the waiting time at each of these charging stations, 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 (Prefered Option {?} in Fig.2). Next, the EV receives the acceptance notification from GSO (represented in Fig.2 by (REP {accept}).

3. Booking and confirmation:

In this step, the EV makes a final booking request (Booking REQ in Fig. 2). After a successful booking of the corresponding charging time slots at the charging stations, GSO sends back an approval to EV (Success Book in Fig.2).

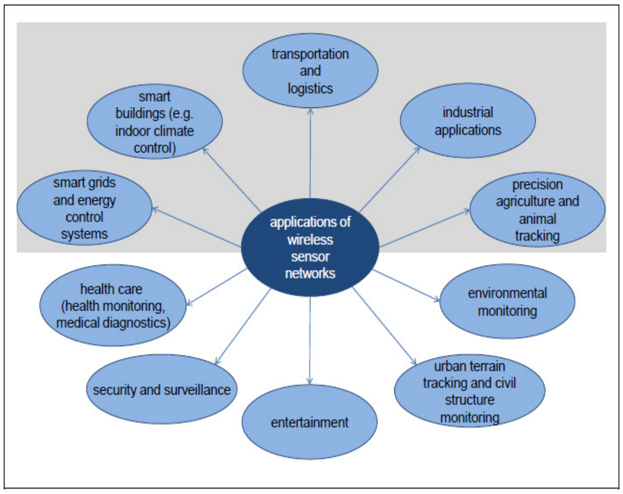
4. Charging and payment:

After a successful booking, the EV can move to the first charging station and proceed with the charging operation. Three possibilities may occur: EV reaches the charging station on the scheduled time. The EV proceeds to charging. The payment is completed before the user unplugs the charger. A message (Success Payment) of successful payment is sent to EV. EV will not reach the charging station 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. EV will not reach the charging station 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 charging station, EVSE maintenance service, etc.) which may cause a delay at charging stations 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

Fields of application of wireless sensor networks


transportation and logistics
smart buildings (e.g. indoor climate control)
industrial applications
smart grids and energy control systems
applications of wireless sensor networks
precision agriculture and animal tracking
health care (health monitoring, medical diagnostics)
environmental monitoring
security and surveillance
entertainment
urban terrain tracking and civil structure monitoring

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 secure service architecture 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 sub-modules: 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 to secure EVs communications. Authentication is possible by verifying the validity (non-revocation) 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 session manager module creates a

accounting module may follow specific policies for maintaining and updating records of sessions. We assume that there must be a pre-established relationship between the user and the GSO for accounting purposes.

Authorization module (ATM). 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.

session ID aggregating all EV session parameters before dispatching the information to the GSO.

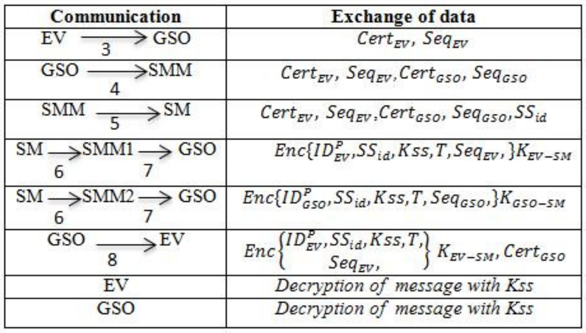
Accounting module (ACM): In this module, EV session parameters are recorded for accounting purposes. The

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 (arrow 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 (arrow 5). The security module 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 $K_{EV\text{-}SM,}$ and $K_{GSO\text{-}SM}$ 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 so that all the messages can be encrypted and decrypted 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 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. This number of message is linear with the number of EVs.



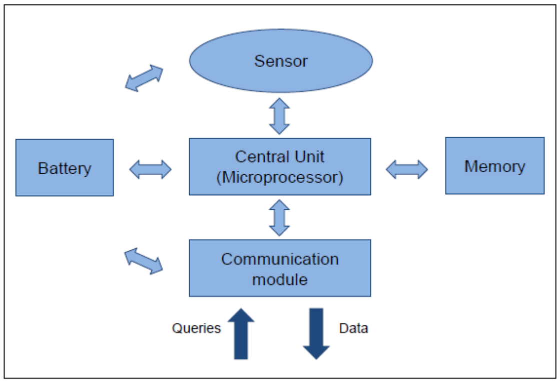
Communication	Exchange of data
$EV \xrightarrow[3]{} GSO$	$Cert_{EV}, Seq_{EV}$
$GSO \xrightarrow[4]{} SMM$	$Cert_{EV}, Seq_{EV}, Cert_{GSO}, Seq_{GSO}$
$SMM \xrightarrow[5]{} SM$	$Cert_{EV}, Seq_{EV}, Cert_{GSO}, Seq_{GSO}, SS_{id}$
$SM \xrightarrow[6]{} SMM1 \xrightarrow[7]{} GSO$	$Enc\{ID^{P}_{EV},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

Fig.3. Security Service Architecture

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 with 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.

Architecture of a sensor node



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 charging stations 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 charging stations. 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 neighbouring charging stations in order to determine the optimal itinerary based on the current status of EVs (i.e., SoC, current location and destination), the status of charging stations, the road network layout and road segments' speeds, and current traffic. The GSO manages different constraints and limitations imposed by EVs and charging stations, 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 analysis 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 34(,)6 as combining a set of nodes (= $\{(_7,(_8,(_9,..,(_1\}$ where $(_:$ is the intersection of edges, and *E*= {)7,)8,)9,);,)<,..,)=} where $)_>$ denotes the edge *e* in the graph 34(,)6. Nodes can be the intersection of road segments or can be the locations of charging stations. The number of edges and nodes are denoted, respectively, by |)|and |(|. GSO determines the graph 34(,)6 that contains all roads in a Service Domaine.

Where is J is the road grade, or slope.

B$_{/!}$: is the aerodynamics force of the EV against the air. It depends on the speed of the vehicle.

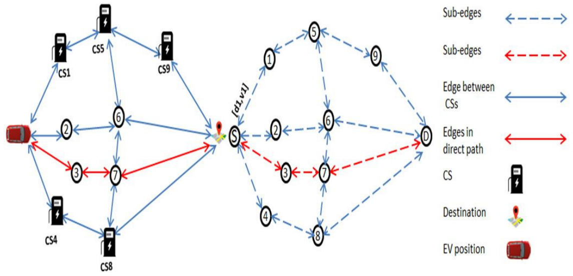
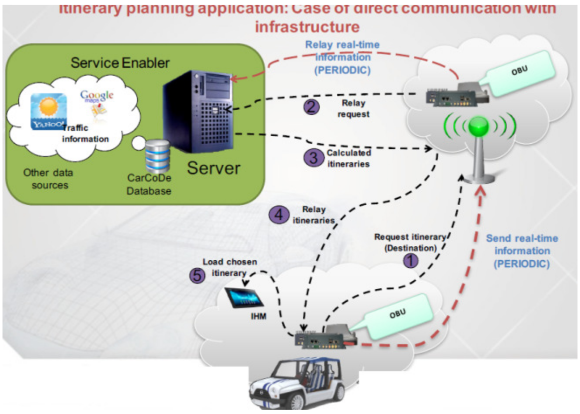


Fig.. Graph illustrating the road network with velocity limits and distance weight of each sub-edge.

The speed is, however, not constant along an edge; indeed, an edge can be composed of several successive sub-edges, each having different speed limits. At each sub-edge we use the speed limit established by the traffic authority to calculate the energy consumption of EV. Therefore, each edge will be composed of several sub-edges. Let each sub-edge, be denoted by [,] where is the distance and is the speed limit of the edge, and i and j are the points of the road delimiting the sub-edge.


Itinerary planning application: Case of direct communication with infrastructure
Service Enabler
Google maps
YAHOO!
Traffic information
Other data sources
CarCoDe Database
Server
Relay real-time information (PERIODIC)
OBU
2 Relay request
3 Calculated itineraries
4 Relay itineraries
Request itinerary (Destination)
1
Send real-time information (PERIODIC)
5 Load chosen itinerary
IHM
OBU

VI. SIMULATION RESULTS

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

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 charging stations are randomly deployed. The locations of EVs and destination are also randomly chosen. The parameters of the simulation illustrated in Table II, where taken from the EV prototypes.

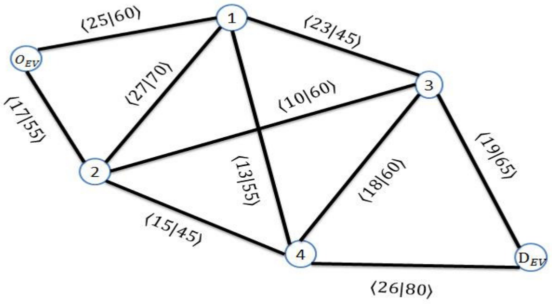


Fig.. Simulated graph.

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

The simulation of the proposed scenario illustrated in Fig. 12 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, the may require to be recharged to reach the destination. The waiting time in the whole trip should be minimized as in Eq. 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 charging station, the waiting time in each station is uniformly distributed between 7mn and 90 mn, the percentage of energy consumption

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, Eq. 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 charging stations.

VII. CONCLUSION

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 charging stations.

REFERENCES

[1] EV World. (2014,Jul.) “There Are Now Half-A-Million Electric Cars OnthePlanet,”[Online].Available:http://www.evworld.com/news.cfm?new sid =33579.

[2] A. Ipakchi and F. Albuyeh, “Grid of the Future,” IEEE power & energy magazine.

[3] C.Caruso. (2016,Aug.),“Why Range Anxiety for Electric Cars Is Overblown,”MITtechnologyreview[Online].Available:www.technologyreview.com.

[4] Whitepaper, “How the Smart Grid Enables Utilities to Integrate ElectricVehicles,”[Online]. Available: http://www.silverspringnet.com/wp-content/uploads/SilverSpring-Whitepaper-ElectricVehicles.pdf .

[5] E.S. Coronado and S. Cherkaoui “Performance analysis of secure on demand services for wireless vehicular networks,” Security and Communication Networks, 2010, pp.114-129.

[6] S. Dhaou, S. Cherkaoui and L. Khoukhi, “Queuing model for EVs charging at public supply stations,” In 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013, pp. 65-70.

[7] S. Dhaou, S. Cherkaoui, and L. Khoukhi, “Guidance model for EV charging service,” In International Conference on Communications (ICC), 2015, pp. 5765-5770.

[8] R. Abousleiman and O. Rawashdeh, “A Bellman-Ford approach to energy efficient routing of electric vehicles,” In: Transportation Electrification Conference and Expo (ITEC), 2015,pp. 1-4.

[9] R.Abousleiman and O.Rawashdeh, “Tabu search based solution to the electric vehicle energy efficient routing problem,” In: Transportation Electrification Conference and Expo (ITEC), 2014, pp. 1-6.

[10] M. Faraj and O. Basir, “Optimal energy/time routing in battery-powered vehicles,” In: Transportation Electrification Conference and Expo (ITEC), 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 8th International Wireless Communications and Mobile Computing Conference (IWCMC),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”, Networks and Spatial Economics, vol. 16, no 1 ,2016, pp. 155-173.

[13] A. Ruzmetov, A. Nait-sidi-moh, M. Bakhouya, and J. Gaber, “Towards an optimal assignment and scheduling for charging electric vehicles,” In: Renewable and Sustainable Energy Conference (IRSEC), 2013. pp. 537-541.

[14] and D.Krob, “Planning an itinerary for an electric vehicle,” In: Energy Conference (ENERGYCON), 2014. pp. 1385-1391.

[15] S. Mehar, S.M. Senouci, and G. Remy, “EV-planning: Electric vehicle itinerary planning,” In: Smart Communications in Network Technologies (SaCoNeT), 2013, pp. 1-5.

[16] H. Akbari and X. Fernando, “Modeling and optimization of PHEV charging queues,” in Electrical and Computer Engineering (CCECE), 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, “Smart attacks in smart grid communication networks,” in IEEE Communications Magazine, August 2012, pp. 24 – 29.

Muthukumar K. obtained a B.E. degree in Electronics & Instrumentation engineering from RVSCET, Anna University, Dindigul, India, in 2007, M.Tech. Degree in the Department of Embedded Systems Technology at Veltech University of Chennai, India in 2012. Currently pursuing Ph.D in the Department of Electrical at Karpagam University of Coimbatore, India. He is current research interests are in the field of developing nanodevices based and image processing using different sensors.

Suganthi P. Currently pursuing a B.E. degree in Electrical and Electronics Engineering from Sri Krishna College of Engineering and Technology, Anna University, Coimbatore, India,. He is current research interests are in the field of various instrument sensors.

Reshma M. Currently pursuing a B.E. degree in Electrical and Electronics Engineering from Sri Krishna College of Engineering and Technology, Anna University, Coimbatore, India,. He is current research interests are in the field of various instrument sensors.