Secure Communication Scheme for Electric Vehicles in the Smart Grid

Achraf Bourass, Soumaya Cherkaoui and Lyes Khoukhi†
INTERLAB Research Laboratory, University of Sherbrooke, Canada
Email: {achraf.bourass, soumaya.cherkaoui}@usherbrooke.ca
† ERA Environnements de Réseaux Autonomes, Institut Charles Delaunay (ICD), UTT,France
Email: Lyes.Khoukhi@utt.fr

Abstract— The increasing number of intelligent electric vehicles (EVs) has stimulated challengeable problems (i.e., confidentiality, privacy) for the smart grid in the last few years. These challenges impact the exchange of sensitive information between EVs and smart grid which offer different sort of services (i.e., planning itineraries, booking charging stations (CSs)). In this paper, we propose a new architecture to secure communication exchange between EVs and the smart grid. The proposed architecture ensures both confidentiality of communications and privacy of EVs, and includes authentication and authorization in order to secure service access for EVs. Simulations were performed under different scenarios to show the performance of our proposed scheme. The results have shown the proposed architecture ensures good response time when implementing the security modules.

Keywords— EV, smart grid, authentication, authorization.

I. INTRODUCTION

The number of electric vehicles (EVs) has been dramatically in many countries in the last few years, offering many environmental and economic benefits to the transportation sector. Nowadays, there are over 500 000 EVs circulating around the world (i.e., two fifth are in the US). This number is expected to reach 2 million by the end of 2018 [37].Yet, unsecure communications between EVs and the Smart grid as well as the limited number of charging stations (i.e., and the overall charging process) are key challenges for EVs rapid deployment.

Smart grid is deployed all over the world [41] in parallel with the increase of the number of EVs in roads, offering various benefits through bidirectional communications with all relevant entities. It ensures the reliability and the quality of energy as well as the safety of its connected entities in the grid network. These profits can offer the two-way communications with all entities connected in the grid network. A new architecture is proposed in this paper where the EVs can communicate and exchange the extensive data with GSO, for the sake of ensuring the privacy and confidentiality of EVs user. The malicious attacker can easily have access to sensitive data both about GSO (e.g. suitable time-slots at CSs) and EVs (e.g.ID, SoC, Current location, designated destination, type of battery), security mechanism are required. However, to ensure the confidentiality and the privacy of EVs communication. We propose an architecture, which combines a secure service architecture (SSA). This new architecture merges authorization and authentication mechanisms to permit EVs to access to a desired service, such reservation charging time-slots, EVs planning and charge scheduling. Several works (e.g., [3], [4] [5], [6]) have been proposed to study the problems of itinerary planning and charge scheduling for EVs. However, it is worth noting that none of these works considers security mechanisms. In our work, we propose a secure architecture that ensures confidentiality of information, privacy for EVs, and authentication and authorization mechanisms in order to secure service access for EVs.

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

II. RELATED WORK

In the literature, only few works (e.g., [7]-[14]) have addressed the security and privacy issues of interactions between EVs and smart grids in the recent years. However, almost existing works did not address extensively some issues related to preserving the exchanged information confidentiality, privacy for the EVs profile (e.g. ID, state of charge, position, battery capacity, time of charging) and the smart grid (e.g. available charging time-slots at charging stations). Other works have proposed complex authentication and authorization mechanisms to allow EVs to access to a preferred service.

In what follows, we explain some of existing work in this area. In [7], various attacks against EVs communication have been presented, such as impersonation attack, eavesdropping, man-in-the-middle attack. The authors in [8] have analyzed some strategies that can be used by an attacker, and proposed a solution based on Game Theory approach. In [9], the authors focused on security services by proposing a solution, which permits user to create his own keys for communication. The authors of [10] studied the anonymity of vehicles and addressed the battery effect information on V2G location privacy.

In [11], the authors proposed a secure wireless communication platform for V2G communication. The authors focused on the

978-1-5090-5019-2/17/$31.00 ©2017 IEEE

development of an authentication protocol for secure communications between EVs and smart grid. In [12], a mechanism of EV privacy which ensures safe communication between different grid entities is addressed. This mechanism aims to prevent attackers to execute Sybil attacks. An authentication scheme for securing communications between EVs and charging stations is proposed in [13]. This scheme aims to secure EV information based on EV pseudonym and avoids the third party to follow the EV trace while an EV moves to another charging station.

In [14], a battery status-aware authentication scheme is proposed to ensure the security and privacy of the smart grid in V2G networks. This scheme aims to hide the vehicles battery identity and brings the security protection and privacy preservation**.** Even the objective of all mentioned works is to ensure safe communications between EVs and smart grid; however, they did not consider extensively some issues related to the confidentiality of exchanged information of EVs profile and smart grid.

III. SYSTEM ARCHTICETURE

Let us consider an EV travelling in city, form a departure position to a destination, in this trip, EV will need many services that are offered by GSO. Indeed, in our model we allow EVs to exchange information with GSO through wireless communications technology (e.g. WiFi, DSRC, LTE, etc.).

The exchanged information (e.g., EV ID, state of charge, destination position and EV current position) depends on the service requested by EV, as GSO can offer many services intended for EVs environments. GSO has global view on the status of occupancy of public charging stations (CS) along the road network. CS can exchange information with GSO through wireless (mesh networks, LTE, etc.) or wired network technologies.

The GSO is a service provider that offers many services to EVs. For example, GSO can inform EVs about their optimal planning itineraries, the appropriate CSs where EV users need to stop for charging in the case of SoC critical power. Once an EV chooses the suitable planning itinerary and confirms its selected choice to GSO, this latter can proceed to reserve suitable slots for EVs at CS. Communication between GSO and EVs are protected with the integration of our proposed architecture, illustrated in Fig.1.The SSA, its security modules and mechanisms are detailed in Section III.

IV. SECURITY SERVICE ARCHITECTURE

To secure the data exchange between EVs and GSO, a new architecture is proposed in this section. Assuming that EVs can communicate messages with GSO, these messages enclose EVs' sensitive information such as ID, SoC, designated destination and current location. Therefore, without appropriate security measures, third parties can easily exploit this information to track EVs' movement, disturb the scheduling process for EVs, or steal billing information. To mitigate this problem, we propose secure service architecture (SSA), responsible for protecting: 1) the privacy of EVs; and 2) the data exchange of EVs with GSO. In SSA, we define the term "service" as all possible services that can be offered by GSO.

Service Domain is defined as a logical zone which is mapped to a geographical area where many services are offered by

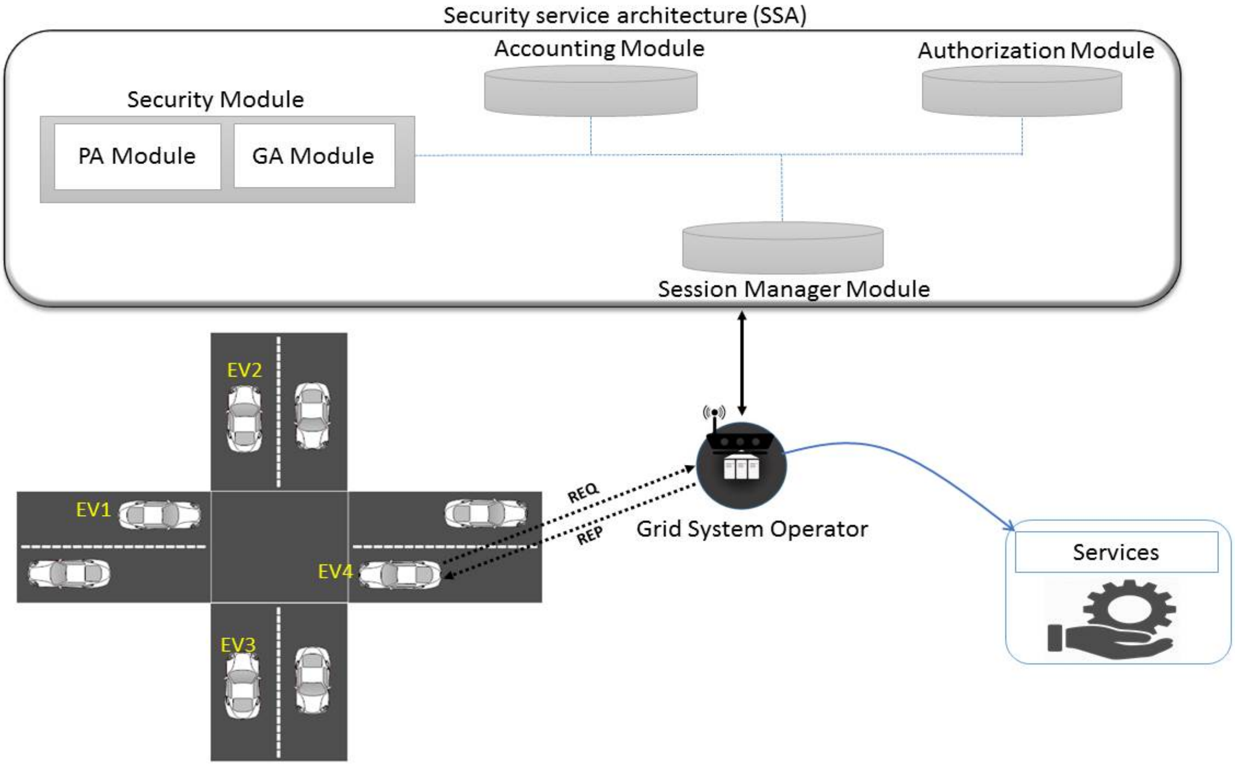


Fig.1. Proposed Architecture

service provider GSO. Fig.1 illustrates the components forming SSA, in charge of processing and validating incoming service requests from EVs in a logical zone. Hereafter, we describe the different components of SSA.

Security module (SM): As shown in Fig.1, SM is constituted of two sub-modules: Private Authorities (PA) and Governmental Authorities (GA). GA is a government entity or a vehicle manufacturer of an official authority, which applies the registration and control procedures for all EVs to participate in wireless communication with GSO. The official authority is responsible of assigning cryptographic material to all EVs. This material is originally preloaded in a tamperproof device within EVs for knowing its real identity. The official authority provides a certified key pairs (public keys, private keys) for the sake of securing EVs communication. The verification of the validity of the public key issued by EVs against certificate revocation lists is used to enable the authentication. It should be noted that the security credentials given by GA could be identical to [50] to secure vehicle to infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. PA is responsible for securing the service sessions between GSO and EV. Indeed, when the verification of EV public certificate is done at GA level, PA would generate the shared session keys between the set (EV and GSO) and creates pseudonyms or temporary identifiers for the distribution of session keys by encrypting the sensitive exchange data with public keys of both EV and GSO.

Each time an EV wants a new access to the services offered by GSO, A new session keys is assigned to the EV by PA.

Session manager module (SMM): SMM can recover information from GSO and transmit it to SM. It does so by generating a session ID and collecting all EVs session parameters before distributing the sensitive information to the GSO.

Accounting module (ACM): For the sake of accounting purposes, this module is in charge of recording EV session parameters. To maintain and update records of sessions, ACM follows specific policies. For proper functioning of ACM, we can assume that a relationship must be pre-established between the EVs and the GSO .

Authorization module (ATM): This module is in charge of granting EVs accessibility to GSO offered service .Authorization can be possible after validation from the previous modules.

Fig.2 illustrates the communication between EV, GSO and the SSA modules for security attributes verification, generation and dispatching.

As shown in Fig.2, EVs send the first notification to GSO for the presence purpose (arrow 1). Then, GSO inquiries (arrow 2 and 3) EVs about their security attributes (public key certificates). Once GSO receives them, it aggregates this information and transmits it to SM (arrow 4), where session IDs are created (arrow 5). When SM obtains the treated data from SMM, the key certificate of GSO and EVs must be verified. Afterward, SM can generate pseudonyms and session keys for GSO and all EVs. After validation from the previous modules (arrow 6), temporary registers for EVs and GSO are created for accounting purposes while it is authorized for that defined session service. The shared private key KEV-SEC and KGSO-SM are used to encrypt the data exchange between EV and SM, and between GSO and SM, respectively (arrows 7, 8, 9, 10). The extensive data exchange (arrows 1-8) illustrates the authorization and authentication of figure.3.

After that, the GSO and EVs can communicate easily because they will have similar Session Key 5 (Kss) which can be used for encryption and decryption of all messages (arrow (request –data) illustrated in Fig. 2). figure.3 shows the used security attributes and the content of data exchanged. Table I lists the notations used.

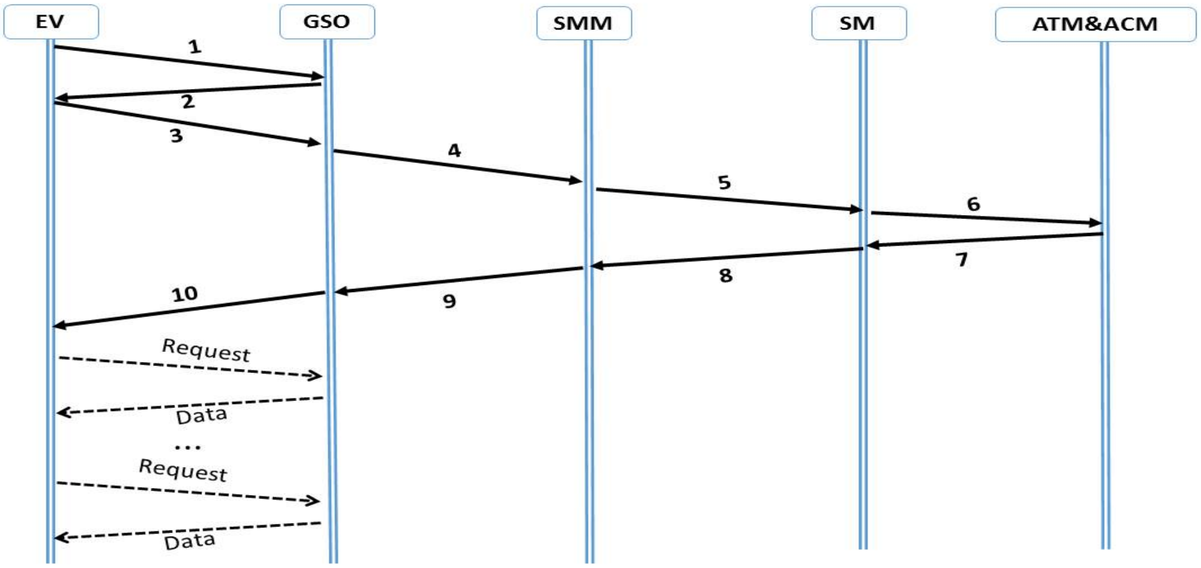
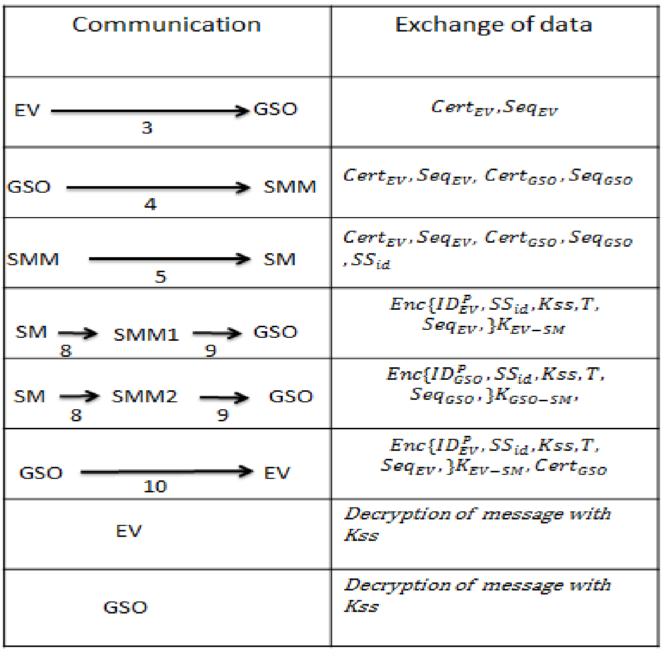


Fig.2. Security attributes verification, generation and dispatching

TABLE I: SSA PARAMETERS

Symbol	Definition
ID_{GSO}^{P}	GSO pseudonym
ID_{EV}^{P}	EV pseudonym
k_{ss}	Session key
$Cert_{GSO}$	GSO certificate
$Cert_{EV}$	EV certificate
Seq_{EV}	EV sequence number
Seq_{GSO}	GSO sequence number
SS_{id}	Session ID
K_{EV-SEC}	Shared key EV-SEC
$K_{GSO-SEC}$	Shared key EV-SEC
T	Timestamp



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 $\xrightarrow[8]{}$ SMM1 $\xrightarrow[9]{}$ GSO	$Enc\{ID_{EV}^{P}, SS_{id}, Kss, T, Seq_{EV}, \}K_{EV-SM}$
SM $\xrightarrow[8]{}$ SMM2 $\xrightarrow[9]{}$ GSO	$Enc\{ID_{GSO}^{P}, SS_{id}, Kss, T, Seq_{GSO}, \}K_{GSO-SM},$
GSO $\xrightarrow[10]{}$ EV	$Enc\{ID_{EV}^{P}, SS_{id}, Kss, T, Seq_{EV}, \}K_{EV-SM}, Cert_{GSO}$
EV	*Decryption of message with Kss*
GSO	*Decryption of message with Kss*

Fig.3. Security attributes use

V. SIMULATION RESULTS

In this section, we present the simulation results of our proposed model. We assume that an EV sends its charging request to GSO asking for some services.

Where GSO is responsible to offer services to EVs. We simulate small to medium size city; we consider a geographical area where the charging stations are randomly deployed. The first simulation focuses on the evaluation of the proposed security protocol by considering the average response time of authentication. Three scenarios are implemented and compared. The second simulation presents the CPU utilization in percentage at SM. The authentication protocol of EVs is simulated using Riverbed Molder Academic Edition 17.5software (Fig.4).

To this end, we consider the processing time at each tier involving execution of data and cryptographic processing time operations, which are based on the benchmark speeds given in crypto++ [16]. The digital signatures implemented in our simulation are based on RSA-128bytes. The signature verification processes executed at each tier and HMAC (SHA1) operations are necessary when generating pseudonyms (32bits).The objective of the first simulation is to estimate the total response time when implementing the security architecture; we define the processing time of each security operation. We assume that each stage of data processing takes 20ms besides decryption/encryption processing. We aim to estimate the response time when executing the multitier process. The simulation is executed within systems service architecture (SSA). The results of this simulation are shown in Fig.5, where the total simulation time is one hour. The graph in Fig. 5 illustrates the estimation of the response time when authenticating EV requests. After a successful authentication, EV can send its requests to GSO, in

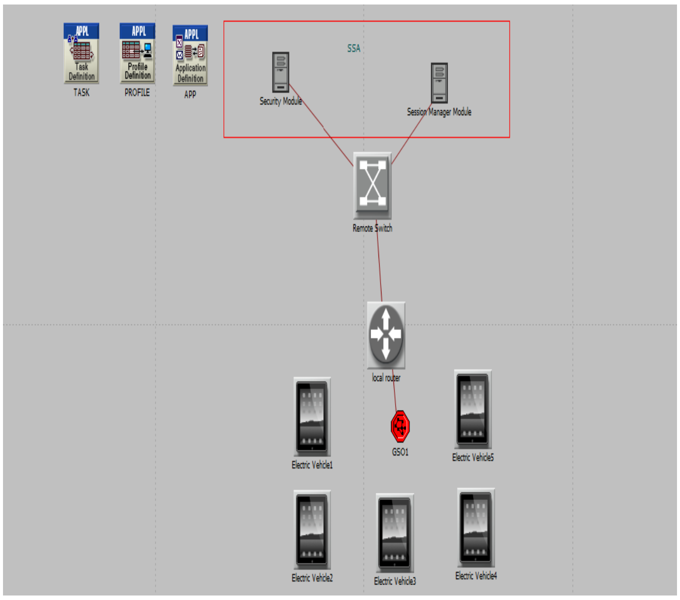


Fig.4. Network topology using Riverbed Molder Academic Edition 17.5.

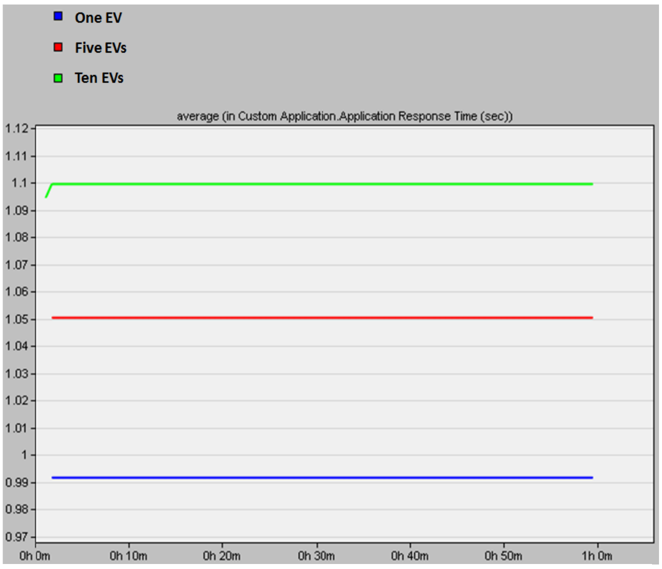


Fig.5. Average response time for three scenarios.

order to obtain the required services.

As shown in the Fig.5, three scenarios are simulated. The blue curve corresponds to the first scenario which represents the estimation of average response time required to execute all message exchanges associated with one EV. The red curve represents the average response time for the second scenario which considers five EVs. The last scenario corresponds to the average response time of ten EVs.

We observe that the response time of the three scenarios varies in a reasonable manner when the total number of vehicles is increased. This means that the number of EVs does not impact on the average response time.

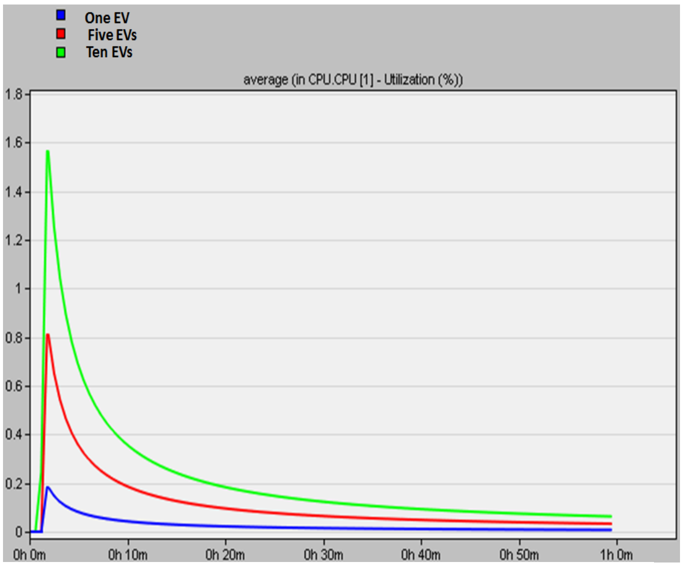


Fig.6. CPU utilization at security module.

Fig.6 shows the CPU utilization in percentage at SM. The blue curve corresponds to one EV while the red and green ones are for five EVs and ten EVs, respectively. We observe that by increasing the number of EVs, the CPU utilization also increases. We also notice that CPU utilization does not exceed two percent even though there are ten EVs requesting security services.

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented a secure architecture of EVs which ensures both confidentiality of communications and privacy of EVs. This architecture is meant to facilitate the use of service which offered by GSO. To ensure secure bidirectional communications between GSO and EVs, the introduced scheme, named a Security Service Architecture (SSA), deals with the authentication and authorization of EVs. The time taken to complete this task was simulated and the results show that the total number of vehicles has no significant effect on the average response time. Furthermore, the simulation of CPU utilization at SM proved that that the number of EVs does impact on percentage of utilization of Server SM.

As future work, we will take into account in our architecture some new parameters related to reservation payment operations and pricing.

REFERENCES

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

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

[3] 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.

[4] 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.

[5] H.G.Chale-gongora, O.D.Weck, A.Doufene, T.Ishimatsu and D.Krob, “Planning an itinerary for an electric vehicle,” In: Energy Conference (ENERGYCON), , 2014. pp. 1385-1391.

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

[7] R. Falk, S. Fries Securely connecting electric vehicles to the smart grid Int. J. Adv. Internet Technol., 6 (2013), pp. 57–67

[8] D. Zheng, F. R. Yu, and A. Boukerche, “Security and quality of service (QoS) co-design using game theory in cooperative wireless ad hoc networks,” in Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications. ACM, 2012, pp. 139–146.

[9] F. Armknecht, A. Festag, D. Westhoff and K. Zang, Cross-layer privacy enhancement and non-repudiation in vehicular communication, In 4th Workshop on Mobile Ad hoc networks, WMAN 07, February 26 - March 02, 2007, Bern, Switzerland.

[10] M. Stegelmann and D. Kesdogan, “Location privacy for vehicle-to-grid interaction through battery management,” in Ninth International Conference on Information Technology: New Generations (ITNG). IEEE, 2012, pp. 373–378.

[11] H. Q. Guo, F. Yu, W. C. Wong, V. Suhendra, and Y. D. Wu, “Secure wireless communication platform for EV-to-grid research,” in Proc. 6th Int. Wirel. Commun. Mobile Com.

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

[13] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, andV. Leung, “Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations,” in *Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on*. IEEE, 2013, pp. 55–60.

[14] Liu H, Ning H, Zhang Y, Yang LT, Guizani M. Battery status-aware authentication scheme for V2G networks in smart grid. IEEE Trans Smart Grid 2013;4(1):99–110.

[15] E.S.Coronado and S.Cherkaoui “Performance analysis of secure on demand services for wireless vehicular networks,” Security and Communication Networks, 3(23), 2010, pp.114-129.

[16]Crypto++,Crypto++ 5.6.0,Benchmarks,[Online]https://www.cryptopp.combenchmarks.html , (visited on /2016).