A Lightweight Authentication Protocol for V2G Networks in Smart Grid

Luis Fernando Arias Roman[1], Paulo R. L. Gondim[1] and Jaime Lloret[2]
[1]*Departamento de Engenharia Elétrica, Universidade de Brasília (UnB), Brasília, Brazil*
[2]*Integrated Management Coastal Research Institute, Universitat Politecnica de Valencia (UPV), Valencia, Spain*

Keywords: Authentication, Security, Electric Vehicles, Aggregator, Vehicle-to-Grid, V2G, Smart Grid.

Abstract: In a Smart Grid, a Vehicle to Grid (V2G) network aims to provide mobile distributed capacity of battery storage, helping to minimize the dependency of non-renewable energy sources. In this network, the privacy and anonymity of users' identity, confidentiality of the transmitted data and location of the Electric Vehicle (EV) must be guaranteed. This article proposes a lightweight authentication protocol devoted to the protection of EV identities, prevention against the tracking of the vehicle and confidentiality of transmitted data. In a performance comparison with other protocols, the results from computing and communications performance analyses are better. The lower consumption of resources allows contributing for reducing signalling congestion and saving bandwidth. The protocol protects from various known attacks and security analysis shows that the protocol achieves the security goals.

1 INTRODUCTION

Smart grid (SG) is based on the overlaying of communications and control system onto the power delivery infrastructure. The integration of electric vehicles (EVs) into electricity load is based on a Vehicle-to-Grid (V2G) network, able to provide mobile distributed capacity of battery storage.

There are several security holes in V2G communications. Among the several security needs to be attended, it is necessary to guarantee the privacy and confidentiality of the user's sensitive information (user identity, loading and unloading schedules, location, etc.) that can be acquired by an attacker using various attack techniques such as: spoofing / sniffing, Denial of Service (DoS) and Man-in-the-Middle attacks.

An authentication protocol is one of the most important parts in V2G networks to ensure the confidentiality and privacy of data (Jie et al. 2015; Saxena et al. 2015; Yaqoob and Shon, 2016; J. Lloret et al, 2012), in order to efficiently protect identities and control access to resources. These protocols need to be resistant to attacks and efficient, so some authors use different techniques to lower costs; among these techniques, group authentication has been used (Wang et al., 2015; Li, 2016; Shao et al. 2016) in order to offer optimum performance. Group based systems are widely used to improve the performance of the network (Lloret, 2011).

This paper proposes a group authentication protocol for the administration and distribution of keys in a V2G architecture. The protocol is based on groups to manage secret keys, Elliptic Curve - Diffie Hellman (ECDH) to share secrets and bilinear pairing to provide simultaneous and efficient session key generation and authentication for EVs grouped in aggregators. The protocol achieves very good performance in terms of computing and communication costs, and provides protection against various attacks.

The remainder of the manuscript is organized as follows: Section 2 describes some works related to the authentication of EV in the V2G network; Section 3 introduces the proposed protocol; Section 4 reports on a performance analysis of the protocol and describes the characteristics of the security properties; Section 5 provides the conclusions and suggests some future work.

2 RELATED WORK

Several protocols have been proposed for authenticating EVs in a V2G network (e.g., (Jie et al. 2015; Saxena et al. 2015; Braeken et al. 2017; Guo et al, 2011; Liu et al, 2013; Liu et al. 2014; Menezes,

Arias Roman, L., Gondim, P. and Lloret Mauri, J.
A Lightweight Authentication Protocol for V2G Networks in Smart Grid.
DOI: 10.5220/0007231702050212
In *Proceedings of the 8th International Joint Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2018)*, pages 205-212
ISBN: 978-989-758-322-3

2005). We selected two proposals for the sake of comparison, as presented below.

(Jie et al. 2015) designed an authentication protocol that preserves the privacy of users´ data in the connection of their electric vehicles for the charging or discharging of batteries in the V2G network. It also optimizes communications through aggregators and dynamically manages the system. It uses group signatures and a partially blind signature restrictive technique based on identity. The architecture comprises five entities, namely Central Aggregator (CAG), LAG, Charging/discharging station (ST), Plug-in electric vehicle (PEV) and a trusted authority (TA). The protocol consists three phases: a) Initial Configuration; b) Generation of group blind certificate for each PEV; c) Access of PEV to the V2G network through ST.

(Saxena et al. 2015) proposed authentication protocols for the access of EVs in the Smart Grid and the recharge and discharge of their batteries considering five entities: EVs, Charging Station (CS), LAG, Certification/Registration Authority (CA/RA) and Control Center (CC). The protocol consists of four parts: Initial configuration, where all entities generate a pair of public and private keys; Registration of EVs: each EV sends information to CA/RA and returns a temporary identity to the EV; LAG - CA/RA communication: all LAG must have the register of the temporary identities of all EVs registered in CA/RA, therefore, the communication between LAG - CA/RA occurs for updating the register of such entities; Protocol execution: when an EV must charge or discharge (sell) part of its energy, it approaches a CS, establishes communication with LAG and generates a session key that guarantees a mutual authentication between EV and LAG. The EV calculates an identity verification parameter and sends an encrypted message to the LAG with the session key. The LAG decrypts the researched message, adds information for the verification of the EV identity, and sends all parameters to the CA/RA in a message encrypted with the CA / RA digital signature generated by the LAG. Finally, CA/RA checks the EV identity and returns a message of commands to the EV. The remaining messages exchanged between the EV and CA/RA are encrypted under asymmetrical encryption based on blind digital firms.

3 PROTOCOL PROPOSAL

For the proposal of the protocol, a V2G network architecture is considered, involving EVs recharging/discharging their batteries; Charge/Discharge Stations (CDS); Aggregators (AGs) --- Local AG's, and a Central AG; Authentication Servers (AS), including a Central Authentication Server (CAS) and several Substation Authentication Servers (SAS), used in large SG networks; Control Center (CC).

Three phases are considered:

1st. phase: **Initialization of the System**

Two cyclic groups G and G_T of order q and *P,* and a generator element of group G are chosen. G and G_T are supposedly related to a non-degenerative pairing and a bilinear map that can be efficiently computed: $\hat{e}$: G × G → G_T such that $\hat{e}(P, P) \neq 1G_T$ and $\hat{e}(aP_1,bQ_1) = \hat{e}(b\ P_1,a\ Q_1) = \hat{e}(P_1,\ Q_1)^{ab} \in G_T$ for every $a,\ b \in Z_q^*$ and every $P_1,\ Q_1 \in$ G (Menezes, 2005). Moreover, the hash functions of the system are defined: $H_1\colon \{0,1\}^* \to G$, $H_2\colon G \to \mathbb{Z}_q^*$ and $H_3\colon \{0,1\}^* \to \mathbb{Z}_q^*$.

Finally, the central authentication server (AS) and all aggregators (AG) define an elliptical curve on a finite field E (Fq) and parameters {G, G_T, $\hat{e}$, P, H_1, H_2, H_3} are published. AS then chooses a private key $x_{AS}, \in Z_q^*$ and calcultates its public key $Y_{AS} = x_{AS} * P$ to be published.

2nd. phase: **Registration**

All EVs and AGs must register on-site in the energy supplier´s system. An identity (ID_{AG}) must be chosen for the registration of AG*s*. The aggregator then chooses a random number $x_{AG} \in \mathrm{Z}_q^*$ to be its private key and calculates a public key $y_{AG} = x_{AG} * P$. AG sends AS a message containing the public key and the identity of the device $\{ y_{AG}, \mathrm{ID_{AG}}\}$. CAS stores the data received y_{AG} and $\mathrm{ID_{AG}}$, and calculates group private key

$$KG_{AG_i} = H_1(ID_{AG}||y_{AG}||LAI_{AG}) * x_{CAS} \qquad (1)$$

and temporary group identity

$$TID_{AG_i} = H_1(ID_{AG_i}) * H_3(\ \beta_i) \qquad (2)$$

where *LAI (local area identifier)* identifies the area where the aggregator is located and $\beta_i \,\epsilon\, Z_q^*$ are random numbers.

The registration of an EV is initialized when it chooses an ID_{EV} identity and an $x_{EV} \in Z_q^*$ private key. It calculates $y_{EV} = x_{EV} * P$ public key. The user sends a message containing the public key and the user´s identity { $\mathrm{y_{EV}}, \mathrm{ID_{EV}}$} to AS through a safe channel. CAS saves the data received, i.e., $\mathrm{y_{EV}}$ and ID_{EV}, associates the EV attributes, as model, make, owner, chassis number and telephone numbers related to the vehicle and choose random numbers $\beta_{i-j}\ and\ V_{i-j}\ \epsilon\ Z_q^*$. It then calculates group private key

$$KG_{EV_{i-j}} = H_1(ID_{EV}||\ model||\ make||chassis\ number) * x_{CAS} \quad (3)$$

a temporary identity

$$TID_{EV_{i-j}} = H_1\left(ID_{EV_{i-j}}\right) * H_3(\ \beta_{i-j}) \quad (4)$$

and temporal visitor Identity

$$TVID_{EV_{i-j}} = H_1(ID_{EV}) * H_3(\ V_{i-j}) \quad (5)$$

The system creates a user account for a web service in the cloud for the sending of data necessary for the authentication phase. The web service will store the hash of the user's identity $h_{EV} = H_3(ID_{EV})$, and require the user to change the password on the first access.

CAS initializes the group by: defining the EVs and AG that will be part of the group and its identity D_{G_i} ; generating a binary tree where leaves are the private group keys $(KG_{EV_{i-j}}, KG_{AG_i})$ of each entity in the group; computes group key KG_i.

Finally the CAS sends the group private key $(KG_{EV_{i-j}}, KG_{AG_i})$ and a list of the blinded keys of its siblings $(LS = K_a, K_b, \ldots, K_z)$ to calculate the group key KG_i, the random numbers β_{i-j} and V_{i-j} for each of the EVs and the random number β_i for the AG in order to calculate the temporary identifications. In the sequence, CAS sends all necessary data $(TIDs, KG\_EV, KG_{AG}, KG_i, Y_{EV_{i-j}}, Y_{AG_i})$ for SAS for authenticating group members.

3rd. phase: **Authentication of EV and AG**

In this phase, 4 messages are exchanged:

A) When an EV is going to charge / discharge energy into a CDS, it generates a temporary identity

$$TID_{EV_{i-j}} = H_1\left(ID_{EV_{i-j}}\right) * H_3(\beta_{i-j}) \quad (6)$$

a verification message

$$M_{EV_{i-j}} = \{KG_i\ ||LAI_{i-j}\}_{\mathrm{KG_{EV_{i-j}}}} \quad (7)$$

where LAI is the location area identifier of EV, and together with a message authentication code (MAC), generates the message 1 ($\{M_{EV_{i-j}}||TID_{EV_{i-j}}||MAC_{i-j}\}$), and sends it to the aggregator AG_i.

B) After receiving message 1 the AG_i checks the $MAC_{EV_{i-j}}$ of message. If the comparison is satisfactory, AG_i adds message $M_{EV_{i-j}}$ and $TID_{EV_{i-j}}$ to a group message M_{G_i}, Otherwise, if comparison isn't satisfactory, the connection with EV is terminated. The aggregator chooses value $v_{G_i} \in Z_q^*$, calculates a temporary identity

$$TID_{AG_i} = H_1(ID_{AG_i}) * H_3(\beta_i) \quad (8)$$

a verification message

$$M_{AG_i} = \{ID_{AG_i}||LAI_{AG}\}_{KG_{AG_i}} \quad (9)$$

a temporary group identity

$$TID_{G_i} = H_1(ID_{G_i}) * v_{G_i} \quad (10)$$

and a message authentication code of the aggregate authentication information

$$MAC_{AG_i} = h_2(M_{AG_i}||TID_{AG_i}\ ) \quad (11)$$

The M_{AG_i} and v_{G_i} are added to the M_{G_i}, then the M_{G_i} message is encrypted with the group key KG_i. last message 3: $\{(\{M_{G_i}\}_{KG_i}||TID_{AG_i}||MAC_{G_i}\ \}$ is sent to SAS, where the

$$MAC_{G_i} = \left(MAC_{AG_i} \oplus MAC_{EV_{i-1}} \oplus \ldots \oplus MAC_{EV_{i-n}}\right) \quad (12)$$

C) AS decrypt the message with the group key and calculates MAC'_{AG_i} and all $MAC'_{EV_{i-j}}$ and the total MAC of the message

$$MAC'_{G_i} = \left(MAC'_{AG_i} \oplus MAC'_{EV_{i-1}} \oplus \ldots \oplus MAC'_{EV_{i-j}}\right) \quad (13)$$

and compares with the MAC_{G_i} of the received message, If the verification fails, SAS sends a MAC failure message to the group. Otherwise, decrypts the messages with the group private keys of each of the EVs and AG, and verifies the identities and location. After, it chooses as random numbers $v_{AS1}, v_{AS2}, r \in Z_p^*$ and calculates a temporary identity

$$TID_{G_i} = H_1(ID_{G_i}) * v_{G_i} \tag{14}$$

and a temporary key for the group

$$TKG_i = h_2(KG_i||v_{AS1}) \tag{15}$$

The TID_{G_i} is sent to the cloud web service with an account associated with the user. The user can join the cloud service through an application on the cell phone, computer, or with a user interface installed in the CDS; this latter feature is important to ensure that the EV owner could join their account to acquire TID_{G_i}, in a situation where, for some reason, he does not have a device with Internet access to join the cloud service in the cloud.

Then, once the TID_{G_i} were obtained, the AS sends a broadcast message 3: $\{\mathrm{\varphi}, \mathrm{X}_1, \mathrm{X}_2, \mathrm{t}_4\}$, where

$$X_1 = r * TID_{G_i} \tag{16}$$

$$X_2 = r * y_{SAS} \tag{17}$$

$$\varphi = H_2(w_1||w_2) \oplus (z \left|\left|ID_{G_i}\right|\right| v_{AS1}||F); z = H_2(h + TKG_i + w_1) \tag{18}$$

$$h = H_1(X_1\left|\left|X_2\right|\right|TKG_i) \tag{19}$$

$$F = v_{AS2} * TKG_i * y_{AS} \tag{20}$$

$$w_1 = r * H_2(TID_{G_i}) * y_{SAS} \tag{21}$$

$$w_2 = r * KG_i * TID_{Gi} \tag{22}$$

and t_4 is a timestamp. in parallel the SAS does the calculation the session keys and the hash of each EV_{i-j}:

$$Ks'_{i-j} = \hat{e}\left(TID_{EV_{i-j}}, F\right) \hat{e}\left(x_{SAS}, v_{sp2} * TKG_i * y_{EV_{i-j}}\right) \tag{23}$$

and AG_i:

$$Ks'_i = \hat{e}(TID_{AG_i}, F) \hat{e}(x_{SAS}, v_{sp2} * TKG_i * y_{AG_i}) \tag{24}$$

D) When EVs and AG_i receive the message from SAS, they calculate: $w'_1 = H_1(TID_{G_i}) * X_2$; $w'_2 = X_1 * KG_i$. Then the EVs and the AG perform an Xor operation to extract the parameters:

$$\mathrm{\varphi} \oplus \mathrm{H}_2(\mathrm{w'}_1||\mathrm{w'}_2) = (z\left|\left|ID_{G_i}\right|\right| v_{SAS1}||F) \tag{25}$$

With z, ID_{G_i}, v_{AS1} and F values found in the message, EV and AG do the following actions:

- Verification of the message:

To check the message sent by SAS, the EVs and the AG must calculate

$$TKG_i' = H_2(TID_{G_i}||v_{AS1}) \tag{26}$$

and

$$h' = H_1(X_1\left|\left|X_2\right|\right|TKG_i) \tag{27}$$

where X_1 and X_2 are the values received in the message and TKG_i is the group key found in the message. EV must then verify $z' = H_2(h' + TKG_i' + w_1)$. If the verification succeeds, EV_s and AG_i calculate the session key; otherwise, they close communication.

- Session key

The EVs and the AG must use the following calculations to obtain a session key: private keys; EV:

$$Ks_{i-j} = \hat{e}\left(\left(TID_{EV_{i-j}} + x_{EV_{i-j}}\right), F\right) \tag{28}$$

and AG:

$$Ks_i = \hat{e}\left(\left(TID_{AG_i} + x_{AG_i}\right), F\right) \tag{29}$$

Once the session key is generated, the EVs and AG calculate a hash of that key ($Hks_{i-j} = H_1(Ks_{i-j}) and\, Hks_i = H_1(Ks_i)$) and form a message that contains the temporal identity (EVs or AG) and the session key hash. This message is encrypted by an XOR operation with the group key ($Mk_{i-j} = (Hks_{i-j}||\mathrm{TID}_{\mathrm{EV_{i-j}}}) \oplus TKG_i$ and $Mk_i = (Hks_i||\mathrm{TID}_{\mathrm{AG_i}}) \oplus TKG_i$) and are sent to the SAS for verification.

In the sequence, SAS immediately receives the messages from each EV_{i-j} and AG_i, groups them and calculates their MAC'_{Mk_i}, groups them and calculates MAC_{Mk_i} of the keys and temporal identity's calculated by SAS:

$$MAC_{Mk_i} = MAC'_{Mk_i}$$
$$= H_2\left(\left(Hks'_i||Hks'_{i-1}||Hks'_{i-2}||\ldots||\ Mks'_{i-j}\right)\oplus TKG'_i\right) \tag{30}$$

If $\mathrm{M}AC'_{Mk_i} = \mathrm{M}AC_{Mk_i}$are the same, all group members have the correct session key, therefore, communication is established. On the other hand, if the verification fails, SAS checks, one by one, the Hash of the keys sent.

4 SECURITY AND PERFORMANCE ANALYSES

This section reports on an analysis of the security and performance of the proposed protocol and a comparison with the other protocols used for authentication of a V2G system.

4.1 Security Analysis

Below is a description of the processes related to authentication, preservation of privacy and integrity and resistance of the proposed protocol to attacks.

Mutual Authentication: Mutual Authentication is established among EVs, AG and AS. AS authenticates AG and EVs through the use in the authentication phase of the pre-shared keys (KG_i, KG_{AG_i}, $KG_{EV_{i-j}}$) in the registration phase. EVs authenticate AG and AS by means of *token* TID_{G_i} in the calculation phase of the group´s temporal key through a pairing operation of the message sent by AS.

Preservation of privacy: The identity of the EV is kept confidential by the authentication servers; the other entities of the V2G network know only the temporary identity of EV ($TID_{EV_{i-j}}$). The location privacy is also guaranteed in both residential and guest modes. The use of encrypted messages in the residential mode ensures only SAS can decipher the location of the vehicle. Such a location is important for the tracking and establishment of responsibilities in case of security incidents.

Protection to integrity: The integrity of the messages exchanged is maintained with the MAC generation. An adversary cannot make changes to an intercepted message without the MAC value changing, so the system would identify if a message was manipulated.

Prevention against attacks: we will describe the different types of attacks that can affect the V2G network and how the proposed protocol can resist them:

- Impersonating: an attacker that aims at impersonating a valid EV must know its the identity and secret key. However, parameter $\mathrm{TID}_{\mathrm{EV}_{\mathrm{i-j}}}$ or $\mathrm{TID}_{\mathrm{AG}_{\mathrm{i}}}$ cannot be obtained without the secret keys of the involved entities. A session key is generated whenever an EV_s is authenticated for the avoidance of use of old parameters in other devices;

- MITM: after receiving a message from AG, AS sends to EVs an One Time Password (OTP) through another channel to check the identity of EVs towards protecting the system from such an attack. EV_{s} must perform operations with both the values contained in the message received and the OTP (TID_i) sent by the server for obtaining the session key and validating the identity of AG_{AG_i} and AS;

- Replay and Injection: an attacker can intercept a message to carry out a repetition attack and inject data in the message. Therefore, random numbers chosen for each session, as TKG,v, TID_i, ks are implemented and *hash* functions check the integrity of the message;

- -Redirectioning: whenever a new EV tries to access the system, it is associated with a group attended by an AG_i. If the same user tries a second access to either the same group, or a different one, AS rejects the second connection;

- Known key: the proposed protocol generates temporary identities and sends an OTP (TID_{G_i}) to the EV to calculate a key for each session, so that an attacker cannot use old keys or data to establish a communication.

- DoS: The Server will enable a valid EV to access the V2G network by calculating the $\mathrm{TID}_{\mathrm{EV}_{\mathrm{i-j}}}$. If more than one session is requested, the server checks the location of the request and if differences between AG_i of the requests sent by the same user are detected, the system rejects the communication of this user to avoid even DDoS attacks

Table 1: Communication Costs in bits per message.

	M1	M2	M3	M4	M5	M6	M7	M8	TOTAL
(Jie et al., 2015)	257n	64n	128n	256n	128n	128n	128n	192n	**1281n**
(Saxena et al., 2015)	384n	704n	320n	128n+320	-	-	-	-	**1536n+320**
Proposed Protocol	376n	312n+376	704	192n+192	-	-	-	-	**880n+1272**

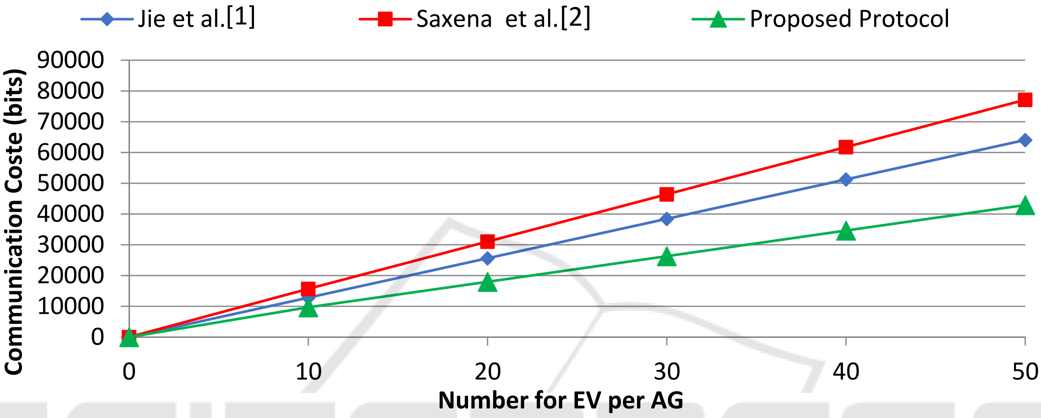

Figure 1: Communication Costs of the Protocols.

Analysis of Communication and Computational Costs

Communication Costs

Due to severe resource limitations, especially those related to bandwidth (spectrum scarcity), it is very important to evaluate the communication cost imposed by a protocol. This evaluation is commonly based on the number of bits transmitted by a network during the execution of the protocol, thus allowing inferring about bandwidth consumption.

Table 1 shows a comparison of the communication costs by entities for a group of n EVs connected to an AG.

According to Table 1, the protocol achieves better communication performance than the protocol designed by (Jie et al., 2015) for a number of EVs higher than 4, and better performance than the protocol of (Saxena et al., 2015) for a number of EVs higher than or equal to 1.45.

Figure 1 shows graphs of the communication costs of the proposed protocol and the protocols proposed by (Jie et al. 2015; Saxena et al. 2015). The communication costs of all protocols increase linearly according to the number of EVs. The superior performance of our protocol in aggregators with medium or high number of EVs is clearly demonstrated.

Computing Costs

In terms of computational costs, the run-time values of the Multiplication (T_{mul}), Exponentiation (T_{exp}) and Bilinear Pairing (T_{pair}) functions are based on (Tao et al., 2017). Other operations, as XOR and hashing, have negligible computational cost (Roman, 2018).

Figure 2 shows a comparison of the total computational cost of the authentication phase of the proposed protocol and the protocols of (Jie et al. 2015; Saxena et al. 2015). Our protocol also provides better computational performance than the protocols designed by (Jie et al. 2015; Saxena et al. 2015).

It is possible to verify (as in (Roman, 2018)) that the largest number of operations of the proposed protocol is concentrated on the entity of best computational properties, i.e., *AS*. Such a characteristic offers better performance and flexibility to the V2G network and avoids the overload of operations in elements of limited resources.

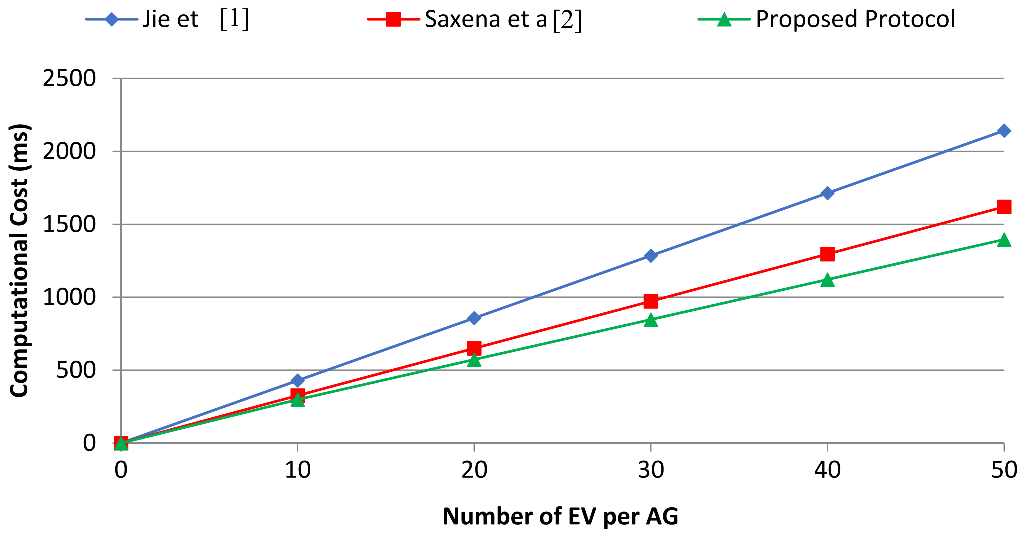

Figure 2: Comparison of Computational Costs among Protocols.

5 CONCLUSIONS

Due to the worldwide interest in reducing air pollution, research in the field of green technologies is very necessary to create alternatives that help reduce air contamination. Part of the research has been related to the integration of EVs into V2G networks, and the different functions that can be developed by EVs to assist the power plants in the demand / supply of energy.

Among the several security challenges, it has been treated the need for secure and efficient authentication of the EVs to enter and use the V2G network.

In the literature, several authentication protocols have been proposed, but their performance and security analyzes should be improved.

In this paper, we proposed a group-based protocol that considers a distributed architecture for authentication services, thus avoiding problems related to centralization; it allows a better distribution of the computational processing of the operations in the devices.

The protocol is based on techniques which include ECDH and bilinear pairing, which shows better computational and communication costs than the proposals of (Jie et al. 2015; Saxena et al. 2015), and provides better results in relation to security analysis.

Future work has considered the simulation of the protocol and its adaptation for the integration in a V2G network based on cloud. The inclusion of access control functions based on RBAC / ABAC / RABAC models has also been scheduled for future work.

REFERENCES

Braeken, A.; Touhafi, A., “AAA □ autonomous anonymous user authentication and its application in V2G” *Special Issue Paper Wiley, 2017*.

Guo, H., Wu, Y., H. Chen, Ma, M., “A batch authentication protocol for V2G communications”, *2011 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, France, February 2011*.

Jie, C.; Yueyu1, Z.; Wencong, S., “An anonymous authentication scheme for plug-in electric vehicles joining to charging-discharging station in *V2G networks” China Communication, v.12, pp. 9-19, 2015*.

Li, H., “privacy-preserving authentication and billing for dynamic charging of electric vehicles”, Doctor Dissertation, *University of Illinois at Urbana-Champaign, 2016*.

Liu, H.; Ning, H.; Zhang, Y.; Guizani, M.; “Battery Status-aware Authentication Scheme for V2G Networks in Smart Grid”, *IEEE Transactions on Smart Grid, v.4, p.p 99-110, 2013*.

Liu H., et al., "Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid", IEEE *Trans. Inf. Forensics Security, vol. 9, no. 2, pp. 208-20, Feb. 2014*.

Lloret, J.; Gilg, M.; Garcia, M.; Lorenz, P., “A group-based protocol for improving energy distribution in smart grids”, Communications (ICC), *2011 IEEE*

International Conference on, pp. 1-6, Paris, France, May 2011.

Lloret, J.; Lorenz, P.; Jamalipour, A.; "Communication protocols and algorithms for the smart grid", IEEE Communications Magazine 50 (5). 2012.

Menezes, A. (2005) "An Introduction to Pairing-Based Cryptography", Recent Trends in Cryptography, v. 477, p. 47-65.

Roman, L.F.A., "Proposal and Evaluation of Authentication Protocols for Smart Grid Networks", Master's Degree Dissertation*, Universidade de Brasilia, UnB, 2018*.

Saxena, N.; Choi, B. J.; Cho, S., "Lightweight Privacy-Preserving Authentication Scheme for V2G Networks in the Smart Grid*" IEEE Trustcom/BigDataSE/ISPA, v.1, pp. 604-611, 2015*.

Shao, J.; Lin, X.; Lu, R.; Zuo, C.; "A Threshold Anonymous Authentication Protocol for VANETs", *IEEE Transactions on Vehicular Technology, v.65*, pp. 1711-1721, 2016.

Tao, M.; Ota, K.; Dong, M.; Qian, Z., "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks", *Journal of Parallel and Distributed Computing, Vol. 118, Part 1*, August 2018, Pages 107-117.

Wang, F.; Chang, C.; Chou, Y. "Group Authentication and Group Key Distribution for Ad Hoc Networks", *International Journal of Network Security*, v.17, pp. 199-207, 2015.

Yaqoob S., and Shon, T., "A Hybrid EV Authentication Approach in Smart Grid Based Distributed Network", *Ad Hoc and Sensor Wireless Networks, Vol. 31, Number 1-4,* pp. 89-99, 2016.