Security and Privacy-Preserving Mechanism for Aggregator Based Vehicle-to-Grid Network

Binod Vaidya, Dimitrios Makrakis(✉), and Hussein T. Mouftah

School of Electrical Engineering and Computer Science,
University of Ottawa, Ottawa, Canada
{bvaidya,dimitris,mouftah}@eecs.uottawa.ca

Abstract. Electrification is foremost actor in superseding internal combustion engine vehicles with electric vehicles (EV). The EV technology will lead to fundamental shift in existing power grid as well as transportation systems. In Smart grid, EVs play vital roles to reduce dependence on fossil fuel, in turn, minimize green house gas emissions. In Vehicle-to-Grid (V2G) network, EVs communicate with power grid operators to trade demand response services by delivering stored electricity into the electric power grid. Communication between aggregator and EVs is central for such an approach. Viewing security and privacy requirements for V2G communications, privacy-preserving technique is central for efficacious V2G network implementation. In this paper, we have proposed effective security and privacy-preserving mechanism for aggregator based V2G network, which is built on ECC-based restrictive partially blind signature. We have provided security analysis and shown that the proposed mechanism is efficient than existing ones in terms of computational overheads.

1 Introduction

Rising escalations in fossil fuel prices and mounting environmental concerns are fundamental drivers in the growing interest in "green" electric-powered vehicles alternatives to internal combustion engine vehicles. For the emerging Smart grid environment, electric vehicles (EVs) play vital roles to reduce dependence on fossil fuel energy, in turn, minimize green house gas (GHG) emissions. Another noteworthy benefit of EVs is that, with large deployment of such vehicles can be used to store energy and deliver this energy back to the power grid when needed. This concept is typically referred to as Vehicle-to-grid (V2G) [1].

By allowing EVs discharge during peak hours and charge during off-peak hours could bring several benefits to the V2G network such as providing ancillary services (i.e. regulation and spinning reserve) as well as faster response time and optimized schedules for recharging. Thus, the V2G network is vital component of emerging Smart grid, which has capability of providing better ancillary services [2, 3].

However, recharging numerous EVs yields a substantial load for the power grid. In order to tackle this issue, a common monitoring entity, so-called aggregator, is deployed that could communicate directly with each EV to continuously monitor its up-to-date status and to manage charging process. Basically, the status information

N. Mitton et al. (Eds.): ADHOCNETS 2014, LNICST 140, pp. 75–85, 2014.
DOI: 10.1007/978-3-319-13329-4_7

includes the EV's location, battery's capacity, battery's state-of-charge (SoC), expected time to leave, etc. Furthermore, energy is delivered back from EVs to the power grid in a controlled way such that connected EVs could constitute a distributed grid resource [3]. The aggregator could sell services that support power grid operators with balancing out energy supply and demand [1-3]. EV owners, in turn, could be compensated for providing their energy resource.

It can be perceived that the monitoring process should be continuous due to the fact that not only presence of EVs in the V2G network are dynamic but also EVs' batteries may be damaged with fluctuating SoC. While communicating with the aggregator, the EVs have to provide information such as identity, location, duration of charging etc. to the aggregator, thus, privacy of the EV owners may be at risk [1]. For instance, by scrutinizing the monitoring data of individual EV, such as the location of parking lots it visited and duration of parking, a malicious entity could reveal sensitive details, e.g., a person's habits, social network, and other activities.

Yang *et al.* [10] proposed a privacy-preserving communication and precise reward architecture for V2G networks, in which, two-tier aggregators having single central aggregator (CAG) and multiple local aggregators (LAGs) to lessen communication burden on the CAG. Their protocol is based on identity-based public key cryptography (PKC) and also utilizes the ID-based restrictive partially blind signature for protecting the privacy of EVs. Subsequently, Tseng [11] modified Yang et al.'s protocol and presented a secure and privacy-preserving communication protocol for V2G Networks using certificate-less public key settings. Basic aim of this protocol is to overcome key escrow problem as in ID-based PKC. The problem with these systems is local aggregators have to be fully trustworthy.

Stegelmann and Kesdogan [12] presented design and evaluation of privacy-preserving architecture for V2G interaction, in which Identity Mixer (Idemix) anonymous credential technique is used. And Y. Zhang, *et al.* proposed context-based and role-based authentication mechanisms for V2G communications [14].

In this paper, we have proposed robust and effective security and privacy-preserving mechanism for aggregator based V2G network in Smart grid environment that utilizes ECC-based restrictive partially blind signature (RPBS) [4, 5].

The remainder of this paper is structured as follows. Section 2 discusses design model and security requirements, while Section 3 presents proposed security mechanism for V2G network. And Section 4 describes system analysis. Finally, in Section 5, we provide concluding remarks.

2 Network Architecture

In this section, we have presented network model for an aggregator based V2G network well as security and privacy requirements.

2.1 Network Model

A network model of the V2G network has similar architecture as in [10], hence we follow similar concept of business model for EV energy exchange as mentioned in [10]. Figure 1 shows a network model of the aggregator based V2G network.

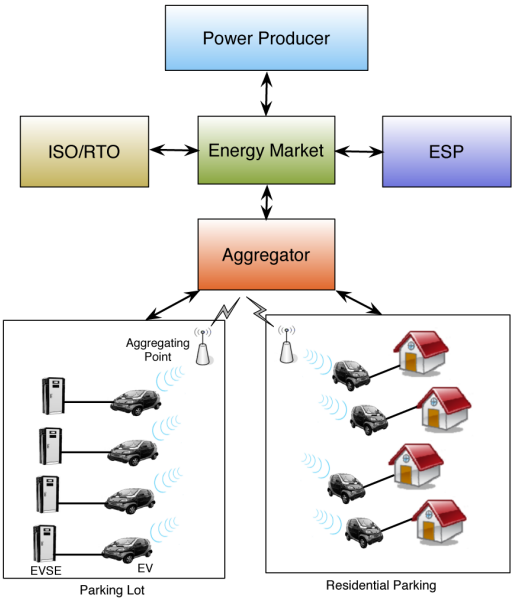

Fig. 1. Network model for Aggregator-based V2G Network

Fundamentally, there are following principal parties, incorporating trusted authority (TA), aggregator (AG), electric vehicle charging station (EVCS), aggregating points (APs) and electric vehicles (EVs). In this network model, a loosely bound two-tier aggregation technique with single AG and multiple APs is deployed. Having direct communication with individual EV, APs provide distributed local authentication and assist AG by collecting information from EVs. The TA is usually an offline authority that executes system initialization including generating system parameters and allotting partial-private-key parameter to all entities in the particular V2G network. The single TA can serve to more than one V2G network.

Electric vehicle charging station, also called electric charging point or electric vehicle supply equipment (EVSE), is an element in an EV infrastructure that supplies electric energy for the charging/recharging of plug-in electric vehicles. EVSEs may belong to a commercial parking lot or a private residence, through which the EV can connect to the electric power grid.

Each parking lot (either private or public) has at least one aggregating point (AP) to serve numerous EVSEs. The AP is particularly being positioned in every local access network such that the entire geographically outsized V2G network is covered. The main objective of the AP is to provide distributed local authentication for the EVs and mediate between the EVs and the AG. Furthermore, the AP collects secured monitoring data from each EV and sends aggregated such data to the AG. In this architecture, even gateway router of the charging station may act as AP.

Communication between the EV and the AP in the local access network is realized with various wired and wireless technologies whereas communication between APs and AG could be possible using various wide-area network (WAN) technologies.

The AG is the entity that is able to have direct communication with the energy market including Power Producer (PP), Electric Service Providers (ESPs), Independent System Operators (ISO) and Regional Transmission Organizations (RTO) [6, 7].

Every partaking EV connected to the electric power grid periodically yields its recent status to the aggregator (AG). Furthermore, the power grid announces service requests in the electricity market. With the obtained EV status updates, the aggregator can evaluate current total electricity storage capacity of each EV in the V2G network. Hence, based on the total capacity and service requests from the power grid, the aggregator can make bids in the electricity market for providing some of the V2G services. In this paper, the interaction among EVs, APs and the AG is considered, while the interaction between the aggregator and other players is neglected.

2.2 Security and Privacy Requirements

In the context of wireless access in the V2G network, the key security considerations may be as follows: authentication, integrity, access control, confidentiality, and non-repudiation. Essentially, communication between an EV and the aggregators in the V2G network should be mutually authenticated, and its confidentiality and integrity protected. Furthermore, subsequent aspects of privacy should be considered in V2G environments: anonymity, context privacy, untraceability and unlinkability.

3 Proposed Security and Privacy-Preserving Mechanism

In this section, we have proposed efficient and robust security and privacy-preserving mechanism for aggregator based V2G system. In this mechanism, we have used ECC-based RPBS along with collective group-oriented signcryption technique to offer efficient V2G-enabled service. Considering above-mentioned requirements, the proposed mechanism is divided into four phases, namely, initialization phase, license generation phase, license verification phase and EV status monitoring phase. A combination of license generation phase and license verification phase is categorized as an ECC-based access control mechanism.

In initialization phase, every entity (EV, AP, AG) in the V2G system needs to contact the trusted authority (TA) to obtain partial-secret parameter in order to construct key pair using ECC-based self-certified public key cryptosystem. Furthermore, the EVs have to open their accounts at the AG.

The key generation phase is grounded on ECC-based self-certified public key cryptosystem (SC-PKC). Initially, an entity (i.e. EV, AP, and AG) submits identification information such as unique identity (ID_A) to the trusted authority (TA). The TA derives a partial-private key using the user's identity and its master key. The entity then combines the partial-private key with a secret value to generate an actual private key. Then it can create its public key as well. It can be seen that the TA in

SC-PKC does not have access to the user's private key. The system is not ID-based, because the public key is no longer computable from a user's identity.

Prior to participating the V2G network, every EV has to undertake the registration at the registration authority (RA) at the AG. Registration phase begins when the EV wants to create user account at the AG, the AG requests the EV to provide his legal identification. The AG stores its real identity (ID_{EV}) of the particular EV along with unique account information ($\Lambda_E = \iota_E.P$) in the database. The AG also sends a group secret $\langle \varpi_S \rangle$ to all the group members (i.e. AP, EV). Figure 2 depicts ECC-based self-certified public key generation process as well as the entity registration process with RA/AG.

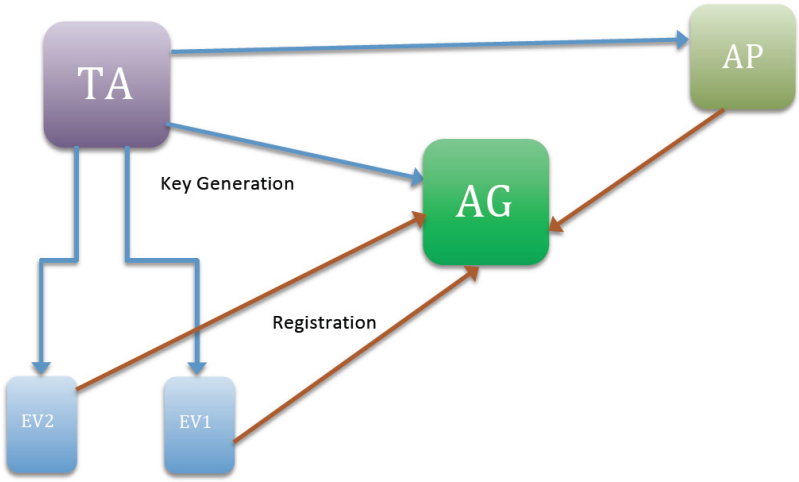

Fig. 2. Key generation and Registration Processes

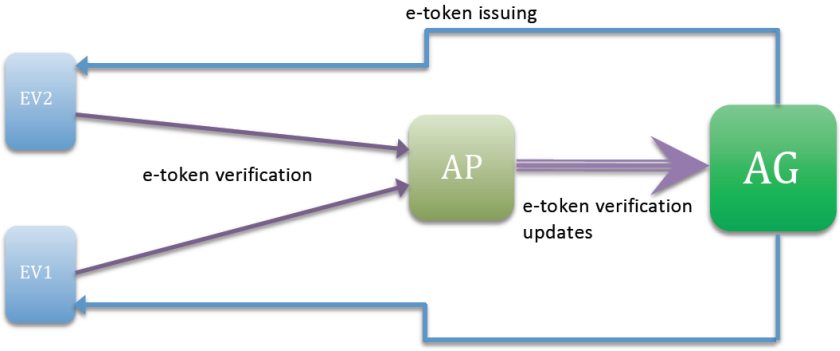

Fig. 3. E-token issuing, e-token verification and updating processes

Figure 3 illustrates e-token issuing process as well as e-token verification process and e-token verification updating process. In order to allow only the authorized EVs to access the V2G network, accredited e-tokens (TOK_{EV}) are issued to the eligible EVs after the legitimate registration. For this purpose, we have proposed ECC-based access control mechanism. This access control mechanism includes e-token issuing phase and e-token verification phase. So the ECC-based restrictive partially blind signature scheme is proposed, which has applied same concept as stated in the scheme mentioned in [10].

In e-token issuing phase, an EV has sent a request with its real-identity to obtain dynamic pseudo-identity (PID_{EV}) and an e-token (TOK_{EV}) from the AG. And ECC-based restrictive partially blind signature technique is deployed such that the AG would not be able to link EV's real identity after this phase. In the e-token issuing phase, the proposed ECC-based restrictive partially blind signature scheme is similar to the scheme mentioned in [10].

EV	Compute $\kappa_1 = (\kappa_{1x}, \kappa_{1y}) = \varpi_S.x_{EV}.X_{AG}$; and $e_1 = H(m, \Sigma_{EV}, \kappa_{1x}, t_1)$	
EV→AG	$\{ID_{EV}, \Sigma_{EV}, m, e_1, t_1\}$	
AG	Check t_1 and verify Σ_{EV}	
	Compute $\kappa_1 = (\kappa_{1x}, \kappa_{1y}) = \varpi_S.x_{AG}.X_{EV}$ and verify $e_1 = ? H(m, \Sigma_{EV}, \kappa_{2x}, t_1)$	
	Generate $w, \delta, k_1, k_2 \in Z_n^*$	
	Compute $PID_{EV} = H(ID_{EV}, \delta)$; $z = x_{AG}.m$; $a = w.P$; $b = w.m$;	
	$u = k_1.P + k_2.X_{AG}$; and $e_2 = H(PID_{EV}, z, a, b, u, \kappa_{1x}, t_2)$	
AG→EV	$\{PID_{EV}, z, a, b, u, e_2, t_2\}$	
EV	Check t_2 and verify $e_2 = ? H(PID_{EV}, z, a, b, u, \kappa_{1x}, t_2)$	
	Generate $\alpha, \beta, \gamma, \lambda, \mu, \xi \in Z_n^*$	
	Compute $m' = \alpha.m$; $z' = \alpha.z$; $a' = \gamma.a + \lambda.P$; $b' = \alpha.\gamma.b + \lambda.m'$;	
	$B = (\beta + \gamma).P$; $u' = \mu.\xi.X_{AG} + H(\Delta)(\mu.u - X_{TA})$; $c' = H(m', u', z', a', b', B)$;	
	$c_1 = \gamma^{-1}(c')$; $c_2 = \mu^{-1}(c') + \xi$; and $e_3 = H(c_1, c_2, \kappa_{1x}, t_3)$	
EV→AG	$\{c_1, c_2, s_3, e_3, t_3\}$	
AG	Check t_3 and verify $e_3 = ? H(c_1, c_2, \kappa_{1x}, t_3)$	
	Compute $\sigma_1 = w + c_1.x_{AG}$; $\sigma_2 = c_2.x_{AG} + (k_1 + k_2 x_{AG}).H(\Delta)$; and	
	$e_4 = H(\sigma_1, \sigma_2, \kappa_{1x}, t_4)$	
AG→EV	$\{\sigma_1, \sigma_2, e_4, t_4\}$	
EV	Check t_4 and verify $e_4 = ? H(\sigma_1, \sigma_2, \kappa_{1x}, t_4)$	
	Verify $\sigma_1.P = c_1.X_{AG} + a$	(1)
	Verify $\sigma_1.m = c_1 z + b$	(2)
	Compute $\sigma_1' = \gamma\sigma_1 + \lambda$; and $\sigma_2' = \mu\sigma_2$	

Fig. 4. Details of E-token issuing protocol

Let's assume $m = \Lambda_E + X_{EV}$ is a message from the EV that needs to be signed by the AG. Prior to accessing a local access network of the V2G network, a particular EV primarily computes its shared secret key (κ_{1x}, κ_{1y}) with AG. Next, the EV sends a request message including its certificate. After proper confirmation, the AG computes dynamic pseudo-identity (PID_{EV}) as well as commitments and sends to the EV.

The EV chooses some random numbers called blind factors to jumble message such that the signer (i.e. AG) will be blind to the prior message. Upon receiving the blinded message, the AG produces the blind signatures and then sends them to the EV, which in turn, creates a number of e-token (TOK_{EV}). Figure 4 shows the details of e-token issuing protocol.

The proposed ECC-based restrictive partially blind signature on (m', Δ) is (u', z', c', σ_1', σ_2'). And an e-token is given as $TOK_{EV} = \{(m', \Delta)\ (u', z', c', \sigma_1', \sigma_2'), B\}$.

In e-token verification phase, any legitimate entities (i.e. AP) can verify whether the e-token (TOK_{EV}) is genuine or not. For diverse V2G services, the EV may need to access the V2G network at different locations, thus APs can provide distributed local authentication.

Before validating e-token (TOK_{EV}), the mutual authentication between the EV and the AP takes place. The AP also checks expiration time of the TOK_{EV}. If they are valid, the AP checks legitimacy of the blind signature of the given TOK_{EV} by validating following equations (Eq. 2 & 3). If these equations meet, then the AP temporarily stores information of the particular EV. A detail explanation of the e-token verification protocol is depicted in Figure 5.

EV→AP	$\{PID_{EV}, TOK_{EV}\}$	
AP	Derive $\varepsilon = (PID_{EV} \| \varpi_S \| m' \| B)$	
	Compute $\kappa_E = (\kappa_{E_x}, \kappa_{E_y}) = x_{AP}.\ \varpi_S.P$; $d = \mathrm{H}(\varepsilon, X_{AP}, spec)$; and $AUTH_1 = \mathrm{HMAC}_{\kappa_{Ex}}(ID_{AP}, \varepsilon, d)$	
AP→EV	$\{ID_{AP}, d, AUTH_1\}$	
EV	Derive $\varepsilon = (PID_{EV} \| \varpi_S \| m' \| B)$	
	Compute $\kappa_E = (\kappa_{E_x}, \kappa_{E_y}) = \varpi_S.X_{AP}$	
	Verify $\mathrm{HMAC}_{\kappa_{Ex}}(ID_{AP}, \varepsilon, d) = ? AUTH_1$	
	Compute $q_1 = d\alpha t_E + \beta\varepsilon$; and $q_2 = d\alpha x_{EV} + \gamma\varepsilon$	
EV→AP	$\{Resp, q_1, q_2\}$	
AP	Compute $a' = (\sigma_1'.P - c'.X_{AG})$; and $b' = (m'.\sigma_1' - c'.z')$	
	Verify $c' = ?\ \mathrm{H}(m', u', z', a', b', B)$	(2)
	Verify $\sigma_2'.P = ?\ u' + c'.X_{AG} + H(\Delta).X_{TA}$	(3)
	Verify $(q_1 + q_2).P = ?\ d.m' + \varepsilon.B$	(4)

Fig. 5. Details of E-token Verification protocol

Then the AP will batch the e-token verification updates for certain time interval and send it to the AG by using Schnorr-like digital signature. The AG verifies such digital signature and stores the e-token information of all received EVs. In case the e-token is used more than once for particular PID_{EV} of the given EV, then the AG can check the exculpability of the e-token for such EV. Figure 6 shows the details of e-token verification updating protocol.

After authentic e-token validation, the AP continuously obtains secured EV status in its neighborhood and sends aggregated data to the AG. Due to space limits, the details of EV status monitoring protocol are excluded in this paper.

AP	Generate $\nu \in Z_n^*$	
	Compute $W = \nu.P$ and $\kappa_2 = (\kappa_{2x}, \kappa_{2y}) = \varpi_S.x_{AP}.X_{AG}$	
	Concatenate $\Theta = \{(PID_{EV1}, TOK_{EV1}, q_{11}, q_{21}, spec_1), .., (PID_{EVi}, TOK_{EVi}, q_{1i}, q_{2i}, spec_i)\}$	
	Encrypt $\Theta_{EN} = \Theta \oplus \kappa_{2x}$	
	Compute $h_1 = H(\Theta, \kappa_2)$; and $g_1 = \nu + x_{AP}h_1$	
AP→AG	$\{ID_{AP}, W, \Theta_{EN}, g_1\}$	
AG	Compute $\kappa_2 = (\kappa_{2x}, \kappa_{2y}) = \varpi_S.x_{AG}.X_{AP}$	
	Decrypt $\Theta = \Theta_{EN} \oplus \kappa_{2x}$	
	Verify $g_1.P =? W - H(\Theta, \kappa_2).X_{AP}$	(5)
	Keep $\{(PID_{EV1}, TOK_{EV1}, q_{11}, q_{21}, spec_1),..., (PID_{EVi}, TOK_{EVi}, q_{1i}, q_{2i}, spec_i)\}$	

Fig. 6. Details of E-token Verification updating protocol

4 System Analysis

In this section, we provide security analysis, efficiency analysis and performance analysis of the proposed mechanism.

4.1 Security Analysis

We have postulated security analysis of the proposed security and privacy-preserving mechanism.

Proposition 1: The proposed ECC-based restrictive partially blind signature scheme fulfills the property of restrictiveness.

The restrictiveness property of the protocol can be apprehended by the following assumption. The recipient acquires a signature on a message that can only be the form *m'*. During e-token issuing protocol, α is randomly selected and $m' = \alpha.m$ is computed by the EV. Thus the proposed mechanism achieves the restrictiveness.

Proposition 2: If the underlying primitives (i.e. RPBS) are secure, then the proposed mechanism satiates the requirements of anonymity and untraceability.

Since the e-token issuing protocol is based on restrictive partially blind signature technique, the AP cannot deduce the EV's real identity from dynamic pseudonym (PID_{EV}) while verifying the e-token (TOK_{EV}). Anonymity is the distinguishing property of our e-token. The privacy of the EV is guaranteed even against collaboration of the involved parties (i.e., AG and AP), unless the EV tries to use same e-token twice in the process.

Proposition 3: If the underlying primitives (i.e. RPBS) are secure, then the proposed mechanism gratifies the unlinkability.

The EV exploits dynamic pseudonym (PID_{EV}) as well as fresh RPBS-based e-token (TOK_{EV}) for every parking session, hence APs or the AG would not be able to link the specific EV's manifold parking sessions with the same EV and construct its user profile.

4.2 Efficiency Analysis

We have shown efficiency analysis of the proposed mechanism in terms of computational costs. Table 1 show the efficiency comparison for issuing protocols, whereas Table 2 shows the efficiency comparison for verification protocol of the proposed mechanism with those of the existing schemes.

Table 1. Efficiency Comparison for Issuing Protocols

	EV	**AG or CAG**
Yang et al.'s scheme [10]	8 t_P (5 offline), 9 t_{ECM}, 3 t_{ECA}, 9 t_{EXP}	4 t_P, 5 t_{ECM}, 1 t_{ECA}
Tseng's scheme [11]	8 t_P (5 offline), 7 t_{ECM}, 5 t_{ECA}, 9 t_{EXP}	4 t_P, 3 t_{ECM}, 1 t_{ECA}
Proposed scheme	15 t_{ECM}, 5 t_{ECA}	6 t_{ECM}, 1 t_{ECA}

Table 2. Efficiency Comparison for Verification Protocols

	EV	**AP or LAG**
Yang et al.'s scheme [10]	1 t_P, 1 t_{ECM}	6 t_P, 1 t_{ECM}, 1 t_{ECA}, 6 t_{EXP}
Tseng's scheme [11]	1 t_P, 1 t_{ECM}	6 t_P, 1 t_{ECM}, 1 t_{ECA}, 2 t_{EXP}
Proposed scheme	1 t_{ECM}	10 t_{ECM}, 5 t_{ECA}

In Table 1 and Table 2, notations used are as follows: t_P is time required for computing pairing operation; t_{ECM} is time required for computing Elliptic curve (EC) scalar multiplication operation; t_{ECA} is time required for computing EC addition operation; and t_{EXP} is time required for computing exponentiation operation. For sake of convenience, we have omitted computational overheads of hash functions and HMAC since their contribution to overall computational cost will be insignificant.

It can be seen that the existing representative schemes [10,11] use pairing operations, whereas the proposed mechanism uses EC scalar multiplication operations, which is much more efficient than pairing operation and consumes much less time. According to [13], time to perform EC scalar multiplication (t_{ECM}) and pairing operation (t_P) are 0.6 ms and 4.5 ms respectively, thus our protocols are more effectual than the existing protocols [10, 11].

4.3 Security Proof

In this sub-section, we have shown security proof of the proposed mechanism.

Lemma 1. If the prover is honest (i.e. he knows a representation and follows a protocol), the verifier will accept it such that the protocol will satisfy the property of completeness.

Proof. The legitimacy of the blind signature of the given TOK_{EV} can be proved by validating Equations 2 and 3.

$$\begin{aligned} c' &= \mathrm{H}(m', u', z', a', b', B) \\ &= \mathrm{H}(m', u', z', (\sigma_1^{'}.P - c'.X_{AG}), (m'.\sigma_1^{'} - c'.z'), B) \end{aligned}$$

$$\begin{aligned} \sigma_2^{'}.P &= u' + c'.X_{AG} + H(\Delta).X_{TA} \\ &= \mu\xi.X_{AG} + H(\Delta)(\mu.u - X_{TA}) + c'.X_{AG} + H(\Delta).X_{TA} \\ &= \mu\xi.X_{AG} + \mu H(\Delta)(k_1.P + k_2.X_{AG}) - H(\Delta).X_{TA} + c'.X_{AG} + H(\Delta).X_{TA} \\ &= \mu\xi.X_{AG} + \mu H(\Delta)(k_1.P + k_2.X_{AG}) + c'.X_{AG} \\ &= c'x_{AG}.P + \mu\xi.x_{AG}.P + \mu H(\Delta)(k_1.P + k_2.X_{AG}) \\ &= \mu x_{AG}(\mu^{-1}c' + \xi).P + \mu H(\Delta)\,(k_1.P + k_2x_{AG}.P) \\ &= \mu(x_{AG}c_2 + (k_1 + k_2.x_{AG})H(\Delta)).P \\ &= \mu\sigma_2.P \\ &= \sigma_2^{'}.P \end{aligned}$$

5 Conclusions and Future Works

In this paper, we have proposed security and privacy preserving mechanism for aggregator based V2G network that utilizes ECC-based RPBS. For this purpose, we have proposed ECC-based access control mechanism. We have provided security analysis, efficiency analysis and security proof of the proposed mechanism. The proposed mechanism provides privacy aspects such as anonymity, privacy, untraceability, and unlinkability that would be desirable for V2G communication. Furthermore, it can be seen that our proposed mechanism is superior to the existing ones while conducting the efficiency analysis of respective issuing and verification protocols.

In future, we will incorporate EV status monitoring process and investigate the performance of the proposed mechanism. And other future works will be secure financial transaction and other services involved in the aggregator based V2G networks.

Acknowledgement. This work was supported by the Government of Ontario under the ORF-RE WISENSE project.

References

1. Guille, C., Gross, G.: A conceptual framework for the vehicle-to-grid (V2G) implementation. Energy Policy **37**(11), 4379–4390 (2009)
2. Kempton, W., Tomic, J.: Vehicle-to-grid power implementation: From stabilizing the grid to supporting large-scale renewable energy. Journal of Power Sources **144**(1), 280–294 (2005)
3. Brooks, A.N.: Vehicle-to-Grid Demonstration Project: Grid Regulation Ancillary Service with a Battery Electric Vehicle Tech. Rep. Contract no. 01-313, AC Propulsion, Inc. (December 2002)
4. Chaum, D.: Blind signatures for untraceable payments. In: Proc. of CRYPTO 1982, pp. 199–203 (1982)
5. Maitl, G., Boyd, C.: A Provably Secure Restrictive Partially Blind Signature Scheme. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, p. 99. Springer, Heidelberg (2002)
6. Jansen, B., et al.: Architecture and Communication of an Electric Vehicle Virtual Power Plant. Proc. of IEEE SmartGridComm 2010, 149–154 (2010)
7. Marra, F., et al.: Electric vehicle requirements for operation in smart grids. In: Proc. of IEEE PES ISGT Europe (2011)
8. Tuttle, D.P., Baldick, R.: The Evolution of Plug-In Electric Vehicle-Grid Interactions. IEEE Transactions on Smart Grid **3**(1), 500–505 (2012)
9. Markel, T., et al.: Communication and control of electric drive vehicles supporting renewables. Proc. of IEEE VPPC 2009, 27–34 (2009)
10. Yang, Z., et al.: P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid. IEEE Transactions on Smart Grid **2**(4), 697–706 (2011)
11. Tseng, H.R.: A Secure and Privacy-Preserving Communication Protocol for V2G Networks. In: Proc. of 2012 IEEE WCNC, pp. 2706–2711 (2012)
12. Stegelmann, M., Kesdogan, D.: Design and Evaluation of a Privacy-Preserving Architecture for Vehicle-to-Grid Interaction. In: Petkova-Nikova, S., Pashalidis, A., Pernul, G. (eds.) EuroPKI 2011. LNCS, vol. 7163, pp. 75–90. Springer, Heidelberg (2012)
13. Zhang, C., et al.: On batch verification with group testing for vehicular communications. Wireless Network **17**(8), 1851–1865 (2011)
14. Zhang, Y., et al.: Securing Vehicle-to-Grid Communications in the Smart Grid, In: IEEE Wireless Communications (2013)