An Efficient and Secure Anonymous Authentication Scheme for V2G Networks

[1]PINNAMRAJU T.S PRIYA, [2]ALAMANDA NAVEEN

Assistant Professor, Department Of MCA, 2MCA Final Semester, Master of Computer Applications,

Sanketika Vidya Parishad Engineering College, Vishakhapatnam, Andra Pradesh, India

Abstract:

The vehicle-to-grid (V2G) network involves intelligent charge and discharge decisions are made based on user operational energy requirements. It is economically beneficial, and it has attracted the interest of power system and electric vehicle (EV) users. The vehicle can temporarily serve as a distributed energy storage system to reduce the peak load on the power grid by utilizing its battery capacity. There are many continues transactions between EV's and grid, the security problems in these transactions block its progress. Information management capabilities enabled by a secured network, such as a reliable privacy-preserving payment systems are also supported by V2G. Many present V2G techniques such as bilinear pairing or elliptical curve to execute the authentication protocol, which results in significant computational costs. Moreover, in the existing V2G technique, the system master key is generated independently by a trusted third party, subjecting the system master key to leakage if the third party is compromised by the attacker. This approach uses the anti-super singular elliptic curve to create a lightweight authentication system for electric vehicles and smart grids.

Introduction:

Non-renewable resources are not available once they are used continuously, so by using Renewable resources such as solar energy, wind energy, In the coming years, fuel automobiles will be gradually replaced by new hybrid vehicles, such as electric vehicles (EVs). To put it another way, Electric vehicles are more expected to play a major role in the automotive industry. In vehicle-to-grid (V2G) network, information and energy is exchanged between the grid and the EVs via a dedicated network. Moreover, the connectivity between the electric grid with transportation networks is exemplified in V2G network. In this work EV will be connected to the electric grid for charging purpose and also it can feed power in to grid. By doing this we can achieve services such as demand (load) balance, frequency regulation, and backup power etc. The EV users in this get profited by buying power from the grid at a reduced rate during the minimal time, they can sell the same power to the grid for a greater price during peak hours.

So, illustrate the importance V2G systems in future, authentication protocol between all EVs and their associated servers or LAGs servers will be used to make sure that only real elements in the system communicate. Typical architecture of V2G network includes Third- party authorities (TPAs) which has local aggregators, dispatching centres (DCs) the DCs can devise an optimal schedule control method for achieving the required EV charge/discharge operations and also it is responsible to Calculate the overall amount and pricing of transaction power based on EV charging and discharging requirements, and schedule complete V2G networks. The storage and trading of power is handled through electricity markets (EMs). During the minimal time, they can sell the same power to the grid for a greater price. Electric vehicles should be equipped with a tamper-proof on-board device that facilitates communication in addition, the EV can charge and discharge only after mutual authentication between EVs and grid is done. Local aggregators (LAs) are in charge of tracking and relaying data Verification messages, request messages, battery level, and other data are shared between EVs and DCs. Some of the advantages of V2G network includes Increase grid stability and dependability while lowering power system operating expenses, Increase EV users' income while still improving environmental preservation etc., Moreover, the batteries in electric vehicles are employed as a buffer to provide auxiliary grid services such as reactive power correction and peak correction

However, V2G networks face significant obstacles in terms of security and privacy, which are mostly observed in two areas: service and authentication. The Electric vehicles and grid are to be authorized with each other before the grid can provide services to them. Malicious attackers can imitate unauthorised CSs to acquire the location information and identity of EVs if mutual authentication is not implemented. The previous schemes do not address some potential strikes in V2G network, like impersonation, replay, man in the middle (MITM), repudiation attacks, redirection known key, and flood-based denial of service (DoS).

In response to the above-mentioned difficulties, a unique way i.e Authentication while maintaining privacy for V2G networks is presented in this research. This technique can provide Authentication with minimal overhead while maintaining privacy which is resistant to internal attacks.

The suggested technique is also better effective than the present V2G scheme in view of delay in communication and the Cost of computation, according to the performance evaluation.

Research contributions:

The main objective of the project work include as follows:
1. To mutually check the legitimacy of the vehicle users and charging stations during the time of charging and discharging process without the intervention of third parties.
2. To provide conditional privacy to revoke the malicious vehicles from misbehaving during the time of charging/s discharging process in the V2G network.

The leftover parts of the proposed framework are as per the following. In area 2, Applicable writings are assessed. The general framework model and fundamental discoveries of this review Section 3 characterizes them. The review that is being proposed is Section 4 clarifies everything. This has been exposed to a thorough security assessment Section 5 contains the exploration work. The estimation and the exploration work's correspondence intricacy are surveyed in section 6. At long last, area 7 wraps the proposed work up.

Literature Survey:

W. Han *et.al* [1] proposed Privacy Protection Technique for V2G networks in the smart grid. This work deals with the approach that privacy preservation can fulfil a variety of privacy aims. In this work, Group signature, third party anonymity are used to deal with the issue of Location privacy and identity privacy. Hasen Nicanfar *et.al* [2] proposed Robust Privacy Preserving Authentication Scheme for Communication Between Electric Vehicles and Power Stations. This work deals with the possible privacy concerns and advocate a sophisticated privacy preserving information security measures for the connection between electric vehicles and power stations, to avoid the customers data leakage. Matthias *et.al* [3] proposed Integrating Power Systems, Vehicle Technology and Transport Systems for Electric Mobility Impact Assessment and Efficient Control. This work deals with the Electric transport in which it is seen as a possible alternative in terms of future individual transport with lesser -emissions, as well as a lower reliance on fossil fuels. To properly deal with the effects, an agent-based paradigm is developed to assess it. Yan Zhang *et.al* [4] proposed Role Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid which is about the V2G network that includes charging and discharging of the vehicles that significantly improves the smart grid layout by reducing the energy consumption peaks. The interactions among EVs and the electric grid in a V2G setup may be vulnerable to cyber security threats. Aldar CF.Chan *et.al* [5] proposed Cyber Physical Device Authentication for Smart Grid Electric Vehicle Ecosystem This work deals with a two-computer equipment verification system to protect from coordinated computer assaults in the electric grid. In the widely used task technique is used to combine a unique environmental feature related to power grid physical links with a traditional authentication factor. The resulting procedure ensures not just a device's digital identity, but also its physical controllability. We offer a computer equipment authentication scheme and CAN cyber security is the practice to build a tight connection in between Improvised explosive device and the EV to prevent the substitution

attack. A concrete evidence model is developed to demonstrate the capabilities of the combined computer technique to counter combined computer threats in the power system. Santiago Grinjalva *et.al* [6] proposed Network security and privacy challenges in smart vehicle -to-grid. This work deals with the guideline objective of the power association is to pass on strong capacity to consumers as well as moving electricity from the vehicle to the organisation during the delivery process. To use it, the power supplier makes sure that the different electrical amounts (such as polarities and energy streams) in the networks are tracked inside practical cut-off locations. Chi Cheng *et.al* [7] proposed Security Analysis and Modification on Two Homomorphic Authentication Scheme for Network Coding. This work deals that a multigeneration pollution attack on the homomorphic subspace signature (HSS) and a key pre-distribution-based tag encryption process is possible (KEPTE). This proposed key distribution schemes can prevent multigenerational pollution threats. Huei Ru Tseng [8] proposed The Security of a Unique Batch Authentication Protocol for V2G Communications. This work deals that a collection of forged signatures that meets the batch verification requirement may be generated by either the vehicle or the aggregator. A. Mustafa Ning *et.al* [9] proposed Smart Electric Vehicle Charging Security Analysis. This work delivers a full security analysis of the electric vehicles service in a Smart Grid system. Security issues and possible safety risks are investigated, leading to the development of safety and privacy criteria. These specifications are used to promote the process of further solutions for a safe advanced EV charging systems, as well as a risk analysis of these systems. João Soares *et.al*
[10] proposed An Optimal Scheduling Problem in Distribution Networks Considering V2G.This work deals mainly with the issue of energy resource allocation. All distributed assets connected to a distribution system will be managed by an aggregator, including distributed energy resources on the renewable energies, storage solutions, demand response and electric grid able cars. Asmaa Abdallah *et.al* [11] proposed Lightweight Authentication and Privacy Preserving Scheme for V2G Connections. This work deals a compact safe and secure V2G connection architecture where the electric grid ensures the authenticity and privacy of shared information during discharging energy sessions and solves the authentication challenge faced by electric vehicles. Huaqun Wang *et.al* [12] proposed Traceable Privacy-preserving Communication (TPP) and Precise Reward for V2G Networks in Smart Grids. This work deals with traceable a novel privacy preserving communication system and an appropriate reward scheme by a cryptographic primitive that are currently accessible.

System Overview:

Electricity Market: An electricity market is a system in which electricity sellers and consumers interact to decide the quantity and price of electrical energy or power. From the dispatching center the information regarding both the charging and discharging of vehicles is provided in the electricity market.so whenever there is a need of electricity for the vehicles then the charge required for the vehicles is taken from the power plant and through the electricity market it is supplied to the vehicles by charge stations. Whenever there is an excess power then the vehicles can also discharge the power back to the electricity market for an affordable price.

Charge Stations: The charge station is in charge of exchanging information and power between EVs and the grid. A power source, also referred as an EV station or an EVSE, is a device which enables plug-in electric vehicles to be charged. Charging stations have a variety of connectors that meet a variety of standards. Charging stations generally include many ports, allowing them to power a variety of vehicles.

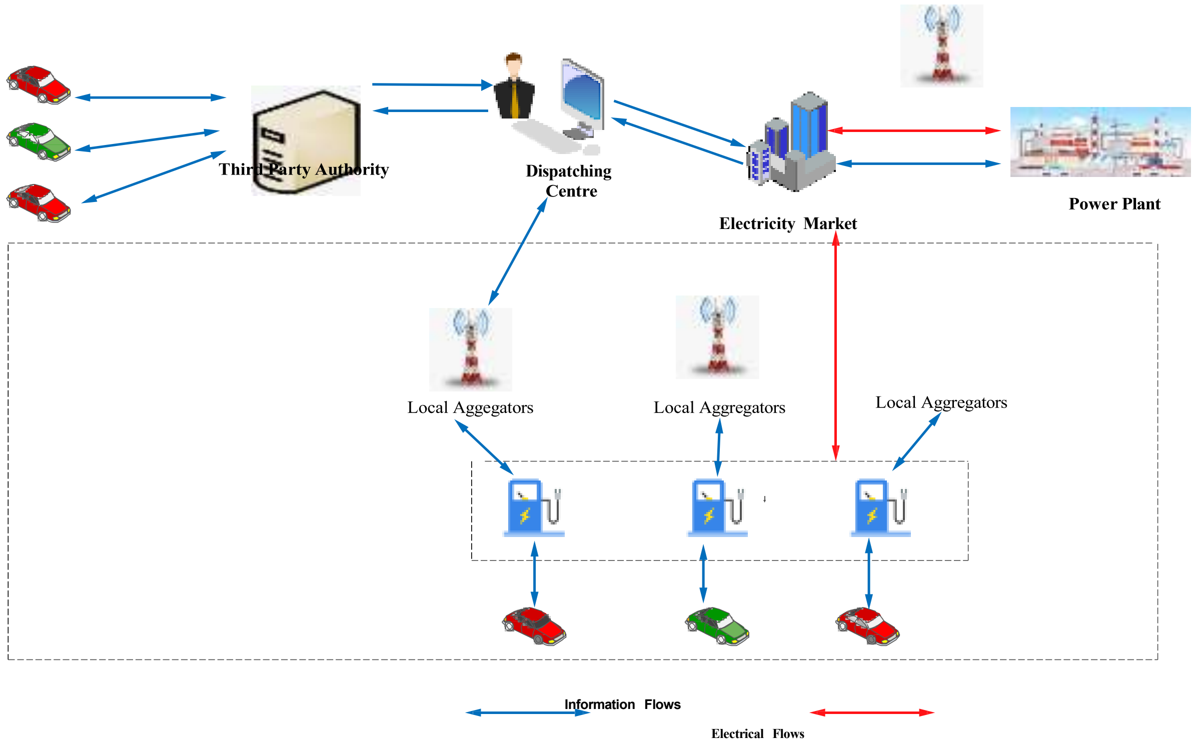
Local Aggregators: Clusters of electric vehicles (EVs) are connected to aggregators in the V2G connection structure. Aggregators are in charge of sending information such as authentication messages, request commands, and battery state between the grid and electric vehicles. A hierarchy's structure is widely utilized in the aggregation method of a V2G network to avoid the communication load produced by manually data transmission between the dispatching center (DC) and each electric vehicle (EV). In V2G, a hierarchical architecture is used to avoid putting too much strain on one aggregator.

Third Party Authorities: Third party authorities are responsible for privacy and security issues in V2G networks. There are so many challenges facing in the field of Authentication and services, so this third-party authorities and dispatching centers together will implement mutual authentication between the dispatching center and electric vehicles. If mutual authentication is not completed between the electric vehicle es and dispatching center (OR) If mutual authentication is not implemented in this two cases, the malignant foes can mimic the illicit charging stations to take the identity and location data of electric vehicles and also there is a chance for illegal benefits by unregistered electric vehicles .So, the third party authorities have the registered data of the electric vehicles to avoid this type of illegal issues and to provide more security and privacy to the users.

Dispatching Centre: The dispatching center focus on developing an ideal planning control technique to accomplish the activity of required electric vehicles charge/discharge. It is also responsible for request services between electric vehicles and grid i.e., Both charging and discharging can only performed after the mutual authentication has completed. Generally, electric vehicles interact with grid through charging stations.

Power Plant: A power system, sometimes known as a generating station, is an economic structure that produces power. It is also known as power station or power plant. The bulk of power plants are linked to the power grid. A power plant is an economic facility that generates electricity from energy production. Most generating stations are employing one or more engines to convert heat into electricity in order to offer power to the electrical grid for society's electrical demands.

Electric Vehicles: Exchanging of information and energy between grid and electric vehicles through a V2G network. This V2G network uses a multiple number of EVs and this EVs are used to store power. When the grid load is extremely high, EVs will provide electricity to the grid, and because the framework power is low, EVs will hold the framework's abundance energy in this way staying away from the misuse of the energy of the V2G organizations. Thusly, EV clients can buy power from framework during the low value time frame, and they can likewise offer capacity to matrix to acquire a few advantages



Proposed work:

In this work, we consider one CS and group of EV’s for easy understanding, the energy and information sharing take place in 5 steps. They are:

1. System Initialization
2. Registration of EV users
3. Registration of Charge Station
4. Mutual authentication

5. Key generation and message integrity preservation

Initialization:

TA chooses the master key on $x \in Z_q^*$ where q is the large prime number. The private key for the TA is chosen as $y \in Z_q^*$. Based on the private key, the public key is calculated as $Y_{ta} = g_1^{x+y}$. G_1, G_2, G_n are the multiplicative cyclic groups. g_1 be the generator of G_1 and g_2 be the generator of G_2. H:$(0,1)^*$ be the severe hash function. Moreover, TA compute $A = e(g_1, g_2)$and publisher. $(G_1, G_2, g_1, g_2, e, H, q, Y_{ta})$ →open medium.

Registration of EV users:

Once the required credentials are verified by TA. TA chooses the random number $v_i \in Z_q^*$ and calculates the public key Y_{ev}=$g_2^{1/(x+y+vi)}$ and dummy identity DID_{ev}=$g_1^{1/(x+y)+vi}$ and for both batch authentication calculates VBK_i=g_2^{x+y+vi}.

Registration of charge station (CS):

After successful verification of credentials of CS, TA chooses a random number $C_i \in Z_q^*$ as its private key and calculate the public key as Y_{cs}=$g_2^{1/(x+y+Ci)}$, the dummy identity of CS is calculated as DID_{cs} $=\frac{(x+y)^2}{C_i}$. Moreover, CS batch key is calculated as $CBK_i = g_2^{x+y}$.

Mutual authentication:

In order to transfer the information effectively between the CS and EV, both of them should be mutually authenticated. For this EV calculates α=$g_1^{vi}$and sends (α.Y_{ev},DID_{ev}) to CS. CS checks $e(Y_{ta}.\alpha, Y_{ev}) = A$. Moreover, CS calculates α'=g_1^{ci} and sends $(\alpha', Y_{cs}, DID_{cs})$ to EV.

EV checks $e(Y_{ta}.\alpha', Y_{cs}) = A$.

Proof of correctness

$$e\,(Y_{ta}.\alpha, Y_{ev}) = e\,(g_1^{x+y}.g_1^{vi}, g_2^{\frac{1}{x+y+vi}})$$

$$= e\,(g_1^{x+y+v_i}, g_2^{\frac{1}{x+y+v_i}})$$

$$= e\,(g1, g2)^{\frac{x\pm y\pm v_i}{x+y+v_i}}$$

$$\Rightarrow \; e(g_1\, g_2) = A$$

$$e(Y_{ta}.\alpha', Y_{cs}) = e(g_1^{x+y}.g_1^{ci}, g_2^{\frac{1}{x+y+ci}})$$

$$= e(g_1^{x+y+c_i}, g_2^{\frac{1}{x+y+c_i}})$$

$$\Rightarrow \; e(g_1\, g_2) = A$$

Key generation and message integrity preservation:

EV chooses a random number $a \in Z_q^*$ and computes $K_0 = g_1^{(x+y)v_i}, K_1 = DID_{cs} \oplus a$, $K_2 = H\ (k_0||k_1||a)$ and K_3=a$\oplus K_2$ and sends $(k_0, k_{2,}a.m)$ to CS. CS checks K_0, K_2 by the following way:

CS checks $e(k_0, DID_{ev}) = e(g_1\ g_2)$

Proof of correctness:

$$e(k_0, DID_{ev}) = e\ (g_1^{(x+y)v_i}, g_1^{\overline{(x+y)v_i}^{\,1}})$$

$$= e(g_1\ g_1)$$

Using a and DID_{cs}, CS calculate k_1
Now CS calculates K'_2 = H (K₀||K₁ ||a) if $K' = K_2$ then integrity of message is preserved.

CS generates the final transfer key as $k_{cs} = (DID_{ev})^{c_i}$ and sends $k_{cs}\ to\ EV.$
EV checks $(k_{cs})^{DID_{CS}\ .v_i} = Y_{ta}$. If the condition satisfied; then final transfer key is accepted for exchange of messages.
Proof:

$$(H_{cs})^{DID_{cs}}.\,v_i = (DID_{evi})^{ci\ .DID_{cs}.v_i}$$

$$= (g1^{1/(x+y)vi})^{ci.\frac{((x+y)^2)}{ci}\cancel{.vi}}$$

$$= g_1^{x+y} = y_{ta}$$

Batch authentication:

In order to authenticate a batch (group) of EV, Choose the following procedure is adopted. EV chooses a random b_i from Z_q^* where($b_i = b_1, b_2 \ldots\ldots b_i$) as its short life private key and calculate the short life public key as f_i=g_2^{bi}. More over the parameters B_i=$g_2^{-\ Vi+bi}$,
D_i=B_i. VBK_i and E_i=H (f_i||D_i) to pressure integrity. The parameters, (D_i, f_i, E_i) are given to CS. CS checks H (f_i||D_i)= E_i. If the condition is satisfied then integrity is preserved. CS checks $\frac{D}{F} = \overline{(CBK_i)^i}$
For verifying group of EV, where

$$D = \Pi_{u=1}^{i} D_i,$$

$$F = \Pi^{i} f_{i_{u=1}}$$

Proof:

$$D = \Pi_{n=1}^{i} D_i$$

$$= B_i\ .\text{VB}K_i$$

$$= B_1.\text{VB}K_1 \,.\, B_2.\text{VB}K_2 \ldots\ldots\ldots\ldots B_i.\text{VB}K_i$$

$$= g_2^{-v_1+b_1}.\,g_2^{x+y+v_1}\,.\,g_2^{-v_2+b_2}.\,g_2^{x+y+v_2}\,\ldots\ldots..$$

$$= g_2^{b_1+b_2+\cdots b_i+x+y}$$

$$F = \Pi_{n=1}^{i} f_i$$

$$= \Pi_{n=1}^{i} g_2^{b_i}$$

$$= {g_2}^{b_1} \cdot {g_2}^{b_2} \cdot {g_2}^{b_3} \cdots {g_2}^{b_i}$$

$$= {g_2}^{b_1+b_2+b_3 \ldots}$$

$$\frac{D}{F} = g_{\overline{2}}^{b_1+x+y+b_2+x+y+b_3+x+y+\ldots c_i+x+y-(b_1+b_2+\ldots b_i)}$$

$$= g^{i(x+y)}$$

$$= (CBK_i)^{i^2}$$

Thus, group of EV are authenticated

Conclusion:

In this work, we have proposed An Efficient and Secure Anonymous Authentication Scheme for V2G Networks, in which it makes use of 2PC protocol between TPA and DC as well as an elliptic curve is used to construct a light weight authentication for Smart Grid and EV using bilinear pairing. The proposed scheme not only preserve the EV’s user information privacy, but also enables low-computational cost and anonymous authentication. Furthermore, this scheme can also survive with internal attacks within the system, it is efficient and convenient scheme when compared to other existing schemes in terms of Security and Simulation Results.

Acknowledgement:

Pinnamraju T S Priya working as a HOD, Assistant Professor in Master of Computer Applications at Sanketika Vidya Parishad Engineering college, Visakhapatnam, Andhra Pradesh with 13 years of experience in Master of Computer Applications (MCA), accredited by NAAC. Her area of interest is in Computer Programming Using C, Computer Organization, Software Engineering, Artificial Intelligence, Internet of Things (IoT) and Distributed Systems.

Alamanda Naveen is pursuing his final semester MCA in Sanketika Vidya Parishad Engineering College, accredited with A grade by NAAC, affiliated by Andhra University and approved by AICTE With interest in Machine learning A. Naveen has taken up his PG project on An Efficient and secure anonymous authentication for V2G Networks and published the paper in connection to the project under the guidance of P.T.S. Priya, Assistant Professor, Master of Computer Applications, SVPEC

References:

1. W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," Computer Communications, vol. 91-92, pp. 17–28, 2016.

2. H. Nicanfar, S. Hosseininezhad, P. Talebifard, and V. C. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations," 2013 Proceedings IEEE INFOCOM, 2013.

3. M. D. Galus, R. A. Waraich, F. Noembrini, K. Steurs, G. Georges, K. Boulouchos, K. W. Axhausen, and G. Andersson, "Integrating Power Systems, Transport Systems and Vehicle Technology for Electric Mobility Impact Assessment and Efficient Control," IEEE Transactions on Smart Grid, vol. 3, no. 2, pp. 934–949, 2012.

4. H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 9, no. 2, pp. 208–220, 2014.

5. A. C.-F. Chan and J. Zhou, "Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," IEEE Journal on Selected Areas in Communications, vol. 32, no. 7, pp. 1509–1517, 2014**.**

6. N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network Security and Privacy Challenges in Smart Vehicle-to-Grid," IEEE Wireless Communications, vol. 24, no. 4, pp. 88–98, 2017.

7. C. Cheng, J. Lee, T. Jiang, and T. Takagi, "Security Analysis and Improvements on Two Homomorphic Authentication Schemes for Network Coding," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 993–1002, 2016.

8. H.-R. Tseng, "On the security of a unique batch authentication protocol for vehicle-to-grid communications," 2012 12th International Conference on ITS Telecommunications, 2012.

9. M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Smart electric vehicle charging: Security analysis," 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), 2013.

10. J. Soares, T. Sousa, H. Morais, Z. Vale, and P. Faria, "An optimal scheduling problem in distribution networks considering V2G," 2011 IEEE Symposium on Computational Intelligence Applications In Smart Grid (CIASG), 2011.

11. A. Abdallah and X. S. Shen, "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections," IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2615–2629, 2017.

12. H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable Privacy-Preserving Communication and Precise Reward for Vehicle-to-Grid Networks in Smart Grids," IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2 340–2351, 2015.