Computer Science and Application 计算机科学与应用, 2024, 14(6), 25-31
Published Online June 2024 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2024.146138

Hans汉斯

面向雾辅助V2G网络的匿名认证方案

毕　雪，岳笑含

沈阳工业大学信息科学与工程学院，辽宁 沈阳

收稿日期：2024年5月14日；录用日期：2024年6月14日；发布日期：2024年6月21日

摘　要

车辆到电网(Vehicle-to-grid, V2G)作为一种新的智能电网模式，可以与可再生能源相结合，提供电力服务，管理电力需求，并建立双向互动的服务模式。电动汽车在请求充放电服务时，需要先向充电站发送带有可识别信息的身份认证信息，从而引起一些安全与隐私方面的威胁。因此，针对此类问题，本文结合密码学匿名凭证思想，提出了一种面向雾辅助V2G网络的匿名认证方案，满足匿名性、不可伪造性、可追踪性、可撤销性等安全需求。在性能方面，给出了方案的功能性分析和性能测试结果，对不同阶段各实体的计算代价进行分析，结果表明所提出的方案在功能性和性能两个方面都具有实际意义。综上，提出的方案可为V2G网络提供一种高效、隐私且安全的认证方案。

关键词

V2G网络，匿名认证，隐私保护

Anonymous Authentication Scheme for Fog-Assisted V2G Networks

Xue Bi, Xiaohan Yue

School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: May 14th, 2024; accepted: Jun. 14th, 2024; published: Jun. 21st, 2024

Abstract

Vehicle-to-grid (V2G), as a new smart grid model, can be combined with renewable energy sources to provide electricity services, manage electricity demand, and establish a two-way interactive service model. When electric vehicles request charging and discharging services, they need to send identification information with identifiable information to the charging station, which causes some security and privacy threats. Therefore, in order to solve such problems, this paper proposes an anonymous authentication scheme for fog-assisted V2G network based on the idea of anonym-

文章引用: 毕雪, 岳笑含. 面向雾辅助 V2G 网络的匿名认证方案[J]. 计算机科学与应用, 2024, 14(6): 25-31.
DOI: 10.12677/csa.2024.146138

ous credential in cryptography, which meets the security requirements of anonymity, unforgeability, traceability, revocation and so on. In terms of performance, the functional analysis and performance test results of the scheme are given, and the computational cost of each entity in different stages is analyzed. The results show that the proposed scheme has practical significance in both functionality and performance. In summary, the proposed scheme can provide an efficient, private and secure authentication scheme for V2G networks.

Keywords

V2G Networks, Anonymous Authentication, Privacy-Preserving

1. 引言

随着电力供应需求的不断增加，部署高效环保的智能电网已成为当前重要的发展目标。V2G 网络作为智能电网[1]的关键技术，在平衡能源负载和跟踪电力需求方面发挥着重要作用，可以提供电能和信息的双向流动。在图 1 所示的 V2G 网络架构中，智能电网从电动汽车收集身份信息、荷电状态(State of Charge, SoC)、期望 SoC、充放电偏好[2]等信息进行数据分析，从而使其更容易调节电压和设定电价。V2G 实体之间的通信通过标准的专用短程通信(Dedicated Short Range Communication, DSRC)协议实现，包括 IEEE 802.11 p 和 IEEE 1609 [3]。总的来说，电网和电动汽车可以以近乎实时的方式监测和控制电力生产和消费，从而改善能源运营。

在 2024 年发布的《关于加强新能源汽车与电网融合互动的实施意见》[4]中明确说明：新能源汽车通过充换电设施与供电网络相连与供电网络相连，构建新能源汽车与供电网络的信息流、能量流双向互动体系，可有效发挥动力电池作为可控负荷或移动储能的灵活性调节能力，为新型电力系统高效经济运行提供重要支撑。车网互动主要包括智能有序充电、双向充放电等形式，可参与削峰填谷、虚拟电厂、聚合交易等应用场景。换句话说，在 V2G 中，EV 不仅是能源的消耗者，也是能源的提供者。当电网负荷过高时，由 EV 储能源向电网馈电；而当电网负荷低时，用来存储电网过剩的发电量，避免造成浪费。通过这种方式，EV 用户可以在电价低时，从电网买电，电网电价高时向电网售电，从而获得一定的收益。

V2G 技术的应用领域广泛，涵盖了电动汽车、能源管理、智能交通、物联网和智能家居等多个方面。在电动汽车领域，V2G 技术为电动汽车提供了更为智能、高效的充电解决方案，同时充分利用电动汽车的储能资源为电网提供有力支持。在能源管理领域，V2G 技术有助于实现能源的优化管理，提升电力系统的稳定性和可靠性。在智能交通领域，V2G 技术为智能交通系统提供了有力支撑，实现车与车、车与充电桩之间的智能通信和便捷充电服务。在物联网和智能家居领域，V2G 技术促进了设备之间的能量交换和数据交互，提升了生活的便捷性和舒适性。

V2G 网络虽然可以提供充放电服务，但其服务过程存在各种安全与隐私挑战[5]。电动汽车用户与其他 V2G 实体传输的消息中包含电动汽车的身份、位置、充放电时间等敏感数据，因此其用电量可能被攻击者伪造和篡改，导致网络中实体缺乏安全性和隐私性。针对上述问题，本文提出了一种面向雾辅助 V2G 网络的隐私保护认证方案。该方案允许雾服务器签发基于属性的证书，充电站通过验证电动汽车发送的匿名证书来判断电动汽车是否具有访问服务的权限。

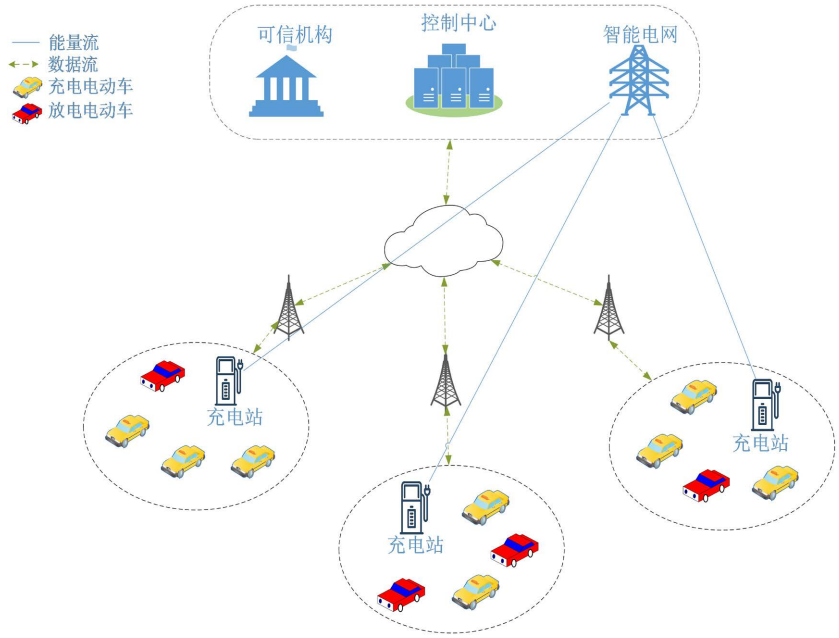

Figure 1. The V2G network architecture
图 1. V2G 网络架构

2. 技术背景

2.1. 双线性配对

双线性配对[6]是当下构建密码学方案的主流方法，因其具有满足密码学方案需要的一些特殊要求而对被广泛地应用在一些密码学方案的构造中。

假设 G_1， G_2， G_T 是三个素数 p 阶乘法循环群，其中 g_1， g_2 分别是 G_1， G_1 的生成元。双线性配对 $e: G_1 \times G_2 \to G_T$ 满足如下性质：

1) 双线性：对于任意的 $a,b \in Z_p$， $g_1 \in G_1$， $g_2 \in G_2$，存在 $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$。

2) 非退化性：满足 $e(g_1, g_2) \neq 1_T$。

3) 可计算性：对于任意的 $g_1 \in G_1$， $g_2 \in G_2$，配对 $e(g_1, g_2)$ 都可以被有效计算。

2.2. 难题假设

1) 离散对数难题[7] (Discrete Logarithm, DL)：假设 G_1 是素数 p 阶乘法循环群， $g_1 \in G_1$ 是它的生成元。给定 (g_1, g_1^x)，在概率多项式时间内很难计算的到 x 的值。

2) 判定 Diffie-Hellman 假设[8] (Decisional Diffie-Hellman, DDH)：假设 G_1 是素数 p 阶乘法循环群，$g_1 \in G_1$ 是它的生成元。给定 $(g_1, g_1^x, g_1^y, g_1^z)$，在概率多项式时间内很难判定 $z = x \cdot y$ 或 z 是随机元素。

3) Pointcheval-Sanders (PS)假设[9]：假设 (G_1, G_2, G_T, p, e) 是一组双线性配对，其中 g_1， g_2 分别是 G_1， G_2 的生成元。给定 (g_2, g_2^x, g_2^y)， $x, y \in Z_p$ 以及对以 $m \in Z_p$ 为输入的谕言机的无限访问权，随机选取 $a \in G_1$ 生成 (a, a^{x+my})，在概率多项式时间内没有敌手可以根据未被质询的 m^* 生成一个新的有效的 (a, a^{x+m^*y})。

3. 方案构建

3.1. 方案系统模型

本文方案涉及四类实体，包括注册中心(Registration Center, RC)、雾服务器(Fog Server, FS)、充电站

(Charging Station, CS)和电动汽车(Electric Vehicles, EV)。本文构建方案模型如图 2 所示。各实体责任定义如下：

注册中心：是云端可信权威机构，负责生成全局公共参数，处理系统内全部实体的注册申请。

雾服务器：部署在云网络边缘的 FS，负责发放电动汽车电网访问凭证，作为云实体和终端实体之间的通信中介，包括向上层云服务器上传信息和向终端实体发送信息。

充电站：由电动汽车制造商提供的充电站，可以验证车辆是否有权限访问充放电服务。验证通过后，CS 提供充电接口供电动汽车充电。

电动汽车：电动汽车配备了名为车载单元(On-board Unit, OBU)的防篡改装置，可以与附近的 CS 或 EV 通信，并执行充放电任务。

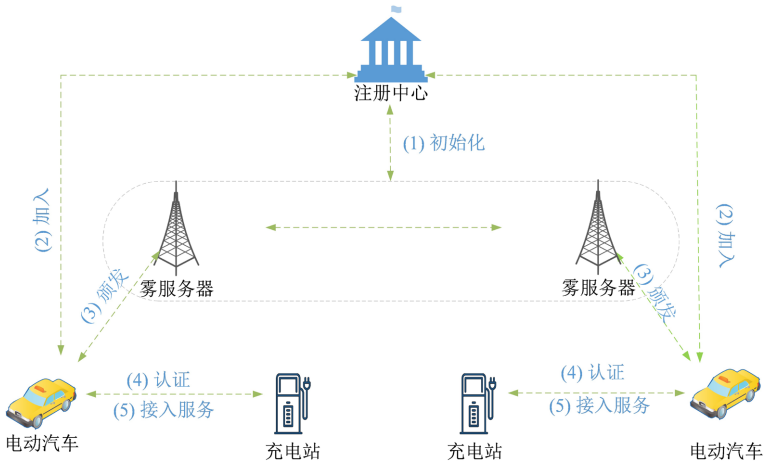

Figure 2. The system model
图 2. 系统模型

3.2. 方案形式化定义

1) 初始化阶段

该步骤主要是生成系统中所使用的一些基本参数，然后利用公共参数生成注册中心、电网控制中心、雾服务器、充电站和电动汽车用户的公私钥以及相关参数，以便在后续的系统功能实现中使用。

$\text{Setup}\left(1^{\lambda}\right)\rightarrow param$：此算法主要用于生成方案中的全局公共参数。注册中心输入一个安全参数 λ，然后输出一个全局的参数 $param$。

$\text{GenRKey}\left(param\right)\rightarrow\left(rpk,rsk\right)$：此算法将全局参数 $param$ 作为输入，并输出注册可信中心的密钥对 $\left(rpk,rsk\right)$。

$\text{GenFKey}\left(param\right)\rightarrow\left(fpk,fsk\right)$：此算法将全局参数 $param$ 作为输入，并输出雾服务器的密钥对 $\left(fpk,fsk\right)$。

$\text{GenVKey}\left(param\right)\rightarrow\left(upk,usk\right)$：此算法将全局参数 $param$ 作为输入，并输出电动汽车的密钥对 $\left(upk,usk\right)$。

2) 加入阶段

每一个加入 V2G 网络的电动汽车都要向 RC 发出加入申请，RC 审核通过后为其颁发身份令牌用于后续身份认证。

$\text{TokenObtain}\left(param,usk\right)\rightarrow\pi_{tok}$：此算法将全局参数 $param$ 和电动汽车私钥 usk 作为输入，输出电

动汽车用户的私钥持有性证明 π_{tok}。

$\text{TokenIssue}(param,uvk,rsk,t)\rightarrow Token$：收到来自电动汽车侧的持有性证明后，注册中心 RC 首先验证证明的有效性，如果有效，则为其颁发与身份相关的令牌，并存储在本地数据库。

$\text{TVerify}(param,rpk,upk,Token,t)\rightarrow 0/1$：此算法由 EV 执行，用来验证令牌的有效性，若有效，则输出 1；反之，输出 0。

3) 颁发阶段

在此阶段，每个 EV 与 FS 进行交互，以获取认证凭证。

$\text{CredObtain}(param,usk,fvk)\rightarrow \pi_{cred}$：此算法由电动汽车 EV 侧执行，用于生成其私钥持有性证明以证明其身份合法性。即，以公共参数 $param$，用户私钥 usk 和雾服务器公钥 fvk 为输入，输出私钥持有性证明 π_{cred}。

$\text{CredIssue}(param,uvk,fsk,\{\alpha_i\}_{i=1}^{n})\rightarrow cred$：在验证持有性证明 π_{cred} 的有效性之后，雾服务器通过自己的私钥 fsk，根据 PS 假设为其颁发基于属性 $\{\alpha_i\}_{i=1}^{n}$ 的凭证 $cred$，其中，n 代表该 FS 能够签署的属性数量。

$\text{CredVerify}(param,fvk,usk,cred)\rightarrow 0/1$：此算法由 EV 执行，用来验证凭证 $cred$ 的有效性，若有效，则输出 1；反之，输出 0。

4) 认证阶段

在认证阶段，EV 需要向 CS 证明自己有权访问服务，即 EV 根据 CS 发布的服务访问策略，出示相应的属性凭证来进行权限验证。同时，EV 还需向 CS 证明自己的身份是合法的，没有处于撤销状态。

$\text{Show}(param,usk,rvk,cred,\{\alpha_i\}_{i=1}^{n},\Gamma,Token)\rightarrow \pi_{auth}$：此算法由 EV 侧执行，通过私钥 usk，注册中心公钥 rvk，凭证 $cred$，令牌 $Token$，根据当前 CS 的访问策略 Γ，生成相应的身份认证信息 π_{auth} 并发送给 CS。

$\text{Verify}(param,rpk,fvk,\pi_{auth},\{\alpha_i\}_{i=1}^{n})\rightarrow 0/1$：此算法由 CS 侧执行，通过雾服务器 FS 的公钥 fvk，注册中心公钥 rpk，验证来自 EV 的身份认证信息 π_{auth} 的有效性，若有效则输出 1，并为其提供相应服务；反之，输出 0，并拒绝提供服务。

3.3. 安全及隐私需求

匿名性：在身份认证阶段，应该保持 EV 身份信息的机密性，使攻击者无法根据提供的身份认证信息确定其真实身份。必要时，只有 RC 能恢复真实身份。

不可伪造性：攻击者不能伪造有效的匿名凭证或未被撤销的令牌。只有持有 FS 颁发的有效凭证的 EV 才能通过 CS 的验证。

双向认证：为防止网络中存在恶意攻击者，通信双方在接入充放电业务前必须实现相互身份认证。在该方案中，EV 发送请求时使用 FS 颁发的匿名验证凭据，从而抵抗伪造攻击。

4. 性能分析

本节进行了仿真实验来测试实际性能。使用的测试平台参数如下：1.5 GHz 的 i.MX6DL (Cortex-A9) CPU，2GB 内存，Android 6.0 操作系统，JPBC 密码库[10]。令 T_{G_1}，T_{G_2}，T_{G_T} 表示在 G_1，G_2，G_T 中完成指数运算的时间，分别为 0.155 ms、0.5 ms、0.75 ms。T_e 表示完成一次配对操作的时间，为 7.85 ms，n 为属性数量，k 表示认证阶段 EV 呈现的属性数量。各阶段的时间代价如表 1 所示。

在图 3 中，根据本文所模拟的实体环境，给出了不同阶段的时间代价情况。方案的认证过程包括 Show 阶段和 Verify 阶段。假设凭证只包含一个属性，每个 EV 在显示阶段的计算开销为 24.25 ms，CS 在验证

阶段的计算开销为 71.98 ms。

Table 1. Computational cost of our scheme
表 1. 方案计算代价

实体	初始化	加入	颁发	认证
RC	$T_{G_1}+4T_{G_2}$	$5T_{G_1}+2T_{G_2}$	-	-
FS	$(n^2+1)T_{G_1}+nT_{G_2}$	-	$(3+n)T_{G_2}$	-
EV	$T_{G_1}+T_{G_2}$	$2T_{G_1}+5T_{G_2}+4T_e$	$(n+1)T_{G_2}+2T_e$	$(2(n-k)+8)T_{G_1}+2T_{G_2}+8T_{G_T}+2T_e$
CS	-	-	-	$(k+5)T_{G_1}+11T_{G_T}+8T_e$

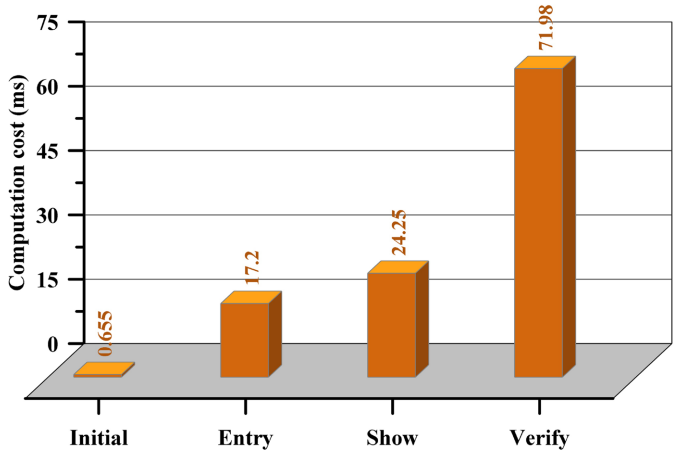

Figure 3. Computation overheads in different phases
图 3. 不同阶段的计算代价

在通信代价方面，通过实验基准测试，可以得出基于 Type F 曲线生成的 G_1 群和 G_2 群的元素长度分别为 40 字节和 80 字节，而 Z_p 群中的元素长度为 20 字节。在本实验的认证阶段中，车辆 OBU 向服务提供商发送一个随机化后的凭证，即一个 G_1 群元素，其实验值为 40 字节。而出示凭证需要 4 个 G_1 群元素和 7 个标量，即理论值为 $4G_1+7Z_p$。因此，本实验中车辆 OBU 出示一个匿名凭证需要发送 300 字节。

总而言之，本文提出了一种适用于雾辅助下 V2G 网络的匿名凭证方案，为解决 V2G 网络的隐私和安全问题提供了一种匿名认证方案。从性能角度出发，根据不同阶段的理论时间代价和通信代价可以看出，各阶段均在各实体的计算能力范围内。

致　谢

感谢全部参与本文章撰写工作的作者。

参考文献

[1] 王睿涛. 基于区块链的 V2G 安全认证技术研究[D]: [硕士学位论文]. 北京: 华北电力大学, 2023.

[2] Guille, C. and Gross, G. (2009) A Conceptual Framework for the Vehicle-to-Grid (V2G) Implementation. *Energy Policy*, **37**, 4379-4390. https://doi.org/10.1016/j.enpol.2009.05.053

[3] Hussain, S.M.S., Ustun, T.S., Nsonga, P. and Ali, I. (2018) IEEE 1609 WAVE and IEC 61850 Standard Communication Based Integrated EV Charging Management in Smart Grids. *IEEE Transactions on Vehicular Technology*, **67**, 7690-7697. https://doi.org/10.1109/tvt.2018.2838018

[4] 中华人民共和国国家发展和改革委员会. 国家发展改革委等部门关于加强新能源汽车与电网融合互动的实施意见[EB/OL]. https://www.ndrc.gov.cn/xxgk/zcfb/tz/202401/t20240104_1363096_ext.html, 2023-12-23.

[5] Saxena, N., Grijalva, S., Chukwuka, V. and Vasilakos, A.V. (2017) Network Security and Privacy Challenges in Smart Vehicle-to-Grid. *IEEE Wireless Communications*, **24**, 88-98. https://doi.org/10.1109/mwc.2016.1600039wc

[6] Galbraith, S.D., Paterson, K.G. and Smart, N.P. (2008) Pairings for Cryptographers. *Discrete Applied Mathematics*, **156**, 3113-3121. https://doi.org/10.1016/j.dam.2007.12.010

[7] Menezes, A. and Menezes, A. (1993) The Discrete Logarithm Problem. *Elliptic Curve Public Key Cryptosystems*, 49-59.

[8] Boneh, D. (1998) The Decision Diffie-Hellman Problem. *Algorithmic Number Theory*: *Third International Symposium*, Oregon, 48-63. https://doi.org/10.1007/BFb0054851

[9] Pointcheval, D. and Sanders, O. (2016) Short Randomizable Signatures. CT-RSA. *Cryptographers' Track at the RSA Conference*, Springer, Berlin, 111-126. https://doi.org/10.1007/978-3-319-29485-8_7

[10] Angelo, D. and Vincenzo, C. (2011) Java Pairing Based Cryptography. 16*th IEEE Symposium on Computers and Communications* (*ISCC*), Kerkyra, 850-855.