基于动态密钥与分片加密的超快充 V2G 数据安全传输方法研究

刘彤[1]，许朋举[2]，吴蔚[1]，谢慧勤[1]，姜伟[2]
1.国网武汉供电公司营销运营中心，湖北 武汉 430000
2.河南许继仪表有限公司，河南 许昌 461100
DOI:10.61369/EPTSM.2026010011

摘　　要： 【目的】针对超快充 V2G交互中设备身份易篡改仿冒、密钥静态化、数据防护及传输完整性不足等问题，提出一种动态密钥与分片加密的数据安全传输方法。【方法】围绕“身份可信—密钥动态—数据分级—传输完整”的总体思路，提出基于唯一硬件标识与物理特征参数的双向认证机制，引入实时充电工况参与椭圆曲线密钥协商，构建与工况状态耦合的动态会话密钥；同时对 V2G交互数据进行核心 /辅助分级处理，分别采用“强加密 +完整性认证”和轻量化加密策略，并结合哈希校验与重传机制实现端到端完整性防护。【结果】研究表明，所提方法可显著提高设备身份认证的唯一性与不可伪造性，增强会话密钥的随机性与时效性，降低密钥泄露导致的大范围安全风险；核心计量与调度指令获得更高强度的保密与抗篡改能力，辅助运行数据在较低计算开销下亦能实现基本防护，整体适配超快充站侧有限算力条件。【结论】该方法显著提升了设备身份可信度、密钥动态安全性及数据传输完整性，适配超快充高功率场景的安全需求。

关 键 词： 超快充；V2G；数据安全；双向认证；动态密钥；分片加密

Research on the Secure Data Transmission Method of Ultra-Fast Charging V2G Based on Dynamic Key and Fragment Encryption

Liu Tong[1], Xu Pengju [2], Wu Wei[1], Xie Huiqin [1], Jiang Wei [2]
1.Marketing and Operation Center of State Grid Wuhan Power Supply Company, Wuhan, Hubei 430000
2. Henan Xuji Instrument Co., LTD., Xuchang, Henan 461100

Abstract: [Objective] Aiming at the problems such as easy tampering and counterfeiting of device identities, static keys, insufficient data protection and transmission integrity in the interaction of ultra-fast charging V2G, a data security transmission method based on dynamic keys and fragment encryption is proposed. [Method] Centering on the overall idea of "trusted identity – dynamic key – hierarchical data – complete transmission", a two-way authentication mechanism based on unique hardware identifiers and physical characteristic parameters is proposed. Real-time charging conditions are introduced to participate in elliptic curve key negotiation, and a dynamic session key coupled with the condition status is constructed. At the same time, core/auxiliary hierarchical processing is carried out on V2G interaction data. The "strong encryption + integrity authentication" and lightweight encryption strategies are respectively adopted, and end-to-end integrity protection is achieved by combining hash check and retransmission mechanisms. [Results] The research shows that the proposed method can significantly improve the uniqueness and unforgeability of device identity authentication, enhance the randomness and timeliness of session keys, and reduce the large-scale security risks caused by key leakage. The core metering and dispatching instructions have gained higher levels of confidentiality and tamper-resistance capabilities. The auxiliary operation data can also achieve basic protection with relatively low computing overhead, and the overall performance is adapted to the limited computing power conditions on the side of ultra-fast charging stations.[Conclusion] This method significantly enhances the credibility of device identity, the dynamic security of keys, and the integrity of data transmission, meeting the security requirements of ultra-fast charging high-power scenarios.

Keywords: **ultra-fast charging; V2G; data security; two-way authentication; dynamic key; shard encryption**

作者简介：刘彤（1972.12），男，武汉黄陂人，大专，工程师，研究方向：电力计量。

引言

随着电动汽车保有量的快速增长和超快充技术的持续演进，大功率、短时、高频次的充电需求日益凸显[1]。超快充车桩与电网软件系统之间通过专用通信通道进行充电功率调节、电量计量、电网调度指令等数据交互，已成为支撑大规模充电设施集中管理、负荷调节与电价结算的关键基础设施，也是构建车网互动（V2G）与柔性配电网的重要支撑[2]。然而，在超快充高功率场景下，一旦 V2G 数据链路遭受攻击，不仅可能导致计量与结算纠纷，还可能引发错误调度、功率越限乃至配电网局部失稳，对电网安全和用户权益带来严重影响，因此对数据保密性、完整性和身份可信度的要求显著提升。

目前的车网互动通信安全方案普遍存在以下不足：（1）认证机制多依赖固定设备编号与静态访问密码，缺乏对设备固有物理特征的绑定，存在设备仿冒、伪装接入等风险[3]；（2）会话密钥生成往往与电网实时负荷、车桩充电工况脱钩，密钥生命周期长且更新策略粗糙，一旦泄露可能危及整个会话周期[4]；（3）数据加密未充分区分计量数据、调度指令等高敏感业务与运行监测等低敏感业务，安全性与计算负载难以兼顾[5]；（4）部分系统缺乏系统化的传输完整性校验与异常重传机制，难以及时发现链路篡改、丢包或重放攻击。

针对上述问题，本文提出一种基于动态密钥与分片加密的超快充 V2G 数据安全传输方法。方法从设备身份本征特征建模、双向认证、工况感知密钥协商、数据分级加密与传输完整性校验到密钥动态更新，构建起贯穿“起始认证 - 安全传输 - 密钥演化”的完整安全链路。通过将唯一硬件标识与物理特征参数深度绑定，引入实时充电工况参与密钥生成与更新，区分核心 / 辅助数据采用不同强度加密策略，并结合哈希校验与过渡密钥机制，在不显著增加车桩侧算力开销的前提下，全面提升了超快充 V2G 数据传输的安全性与可用性。文中对关键步骤给出形式化描述与工程实现要点，并从安全性与工程适配性角度进行分析，为超快充 V2G 系统的安全通信设计提供参考。

一、超快充车网互动数据安全加密识别方法设计

（一）总体方案与安全设计思路

提出的超快充设施车网互动重要数据安全加密识别方法整体流程如图 1 所示，主要包括六个核心步骤：

（1）设备身份初始化：为车桩与电网软件系统分配唯一硬件标识，采集并固化双方的物理特征参数，构建初始特征库；

（2）双向身份认证：基于设备标识、时间戳、随机数与特征参数哈希值，完成车桩与电网系统之间的双向身份互验；

（3）动态会话密钥生成：结合随机数异或结果与实时充电工况参数 C，利用椭圆曲线 ECDH 算法生成动态会话密钥 K；

（4）数据分片加密：根据业务敏感度将数据划分为核心数据 M_1 和辅助数据 M_2，分别采用 AES+HMAC 与哈希 +XOR 轻量化加密；

（5）传输完整性校验：发送端预先计算接收哈希值，接收端对加密数据与接收时间戳进行哈希运算并比对，以判定数据完整性；

（6）密钥动态更新：根据充电功率 P 与电网负荷变化幅度动态调整密钥更新间隔 ΔT，周期性生成新密钥并安全销毁旧密钥，更新期间通过临时过渡密钥保障传输不中断。

通过上述六个子过程，方法在设备可信身份、会话密钥安全、数据保密性与完整性、密钥生命周期管理等方面形成闭环防护体系。

（二）设备身份初始化与特征库构建

1. 唯一硬件标识分配

在设备部署阶段，为超快充车桩与电网软件系统分别分配唯一硬件标识 ID_1、ID_2：

车桩侧：通过编程工具将 ID_1 固化于车桩主控芯片只读存储区，不可在线修改；

电网系统侧：将 ID_2 写入服务器安全芯片的安全存储分区，并启用访问控制机制防止非法读取与篡改。

唯一标识是后续认证与密钥生成过程的基础，也是识别伪造设备的第一道防线。

2. 物理特征参数采集与建模

为增强身份唯一性与不可伪造性，在初始化阶段采集车桩与电网系统各自的固有物理特征参数。

（1）车桩物理特征参数集 F：充电接口阻抗、通信模块频率偏移值、充电电缆阻抗基准值、通信模块 MAC 地址硬件指纹。其中 MAC 硬件指纹可通过提取 MAC 地址前、后各 6 字节并进行 SHA-256 哈希运算生成。

（2）电网软件系统特征参数集 V：服务器硬件指纹、系统固件版本哈希值、电网负荷基准参数、数据库服务器硬盘序列号哈希值。

（3）初始特征库构建与访问控制

将 ID_1 与 F 关联存储于车桩主控芯片内，将 ID_2 与 V 关联存储于电网系统安全芯片内，分别形成本地初始特征库。特征库访问权限严格限定为管理员级读写，外部程序仅可通过特定安全接口调用哈希值，不可直接读取原始特征参数，从而降低特征信息泄露风险。

（三）基于物理特征的双向身份认证机制

1. 认证请求与时间戳有效性校验

认证阶段由车桩发起：

（1）车桩生成 32 位随机数 R_1，并获取当前时间戳 T_1；

（2）将 ID_1、T_1、R_1 封装为认证请求数据包，通过车网互动专用通信通道发送至电网系统；

（3）电网系统接收后解析 ID_1、T_1、R_1，比较 T_1 与当前系统

时间差值是否在预设有效窗口内，以过滤重放或过期请求。

2.电网系统端认证码计算与反馈

当时间戳校验通过后，电网系统执行以下操作：

（1）生成32位随机数 R_2；

（2）调用安全芯片中存储的特征参数 V，计算哈希值 H(V)；

（3）按式（1）拼接 ID_2、T_1、R_1、R_2、H(V)计算认证码 Auth_1；

（4）将 Auth_1 与 R_2 一并返回车桩。

$$\text{Auth}_1 = H(ID_2 \| T_1 \| R_1 \| R_2 \| H(V)) \quad (1)$$

3.车桩端认证与反向验证

车桩接收 Auth_1 与 R_2 后：

（1）调用本地存储的 ID_2、H(V)以及已发送的 T_1、R_1，按式（1）重新计算 Auth_1；

（2）将计算结果与接收的 Auth_1 比对，一致则判定电网系统身份合法；

（3）随后生成车桩响应时间戳 T_2，依据车桩特征参数 F 计算 H(F)；

（4）按式（2）拼接 ID_1、T_2、R_2、H(F)计算认证码 Auth_2，并发送至电网系统：

$$\text{Auth}_2 = H(ID_1 \| T_2 \| R_2 \| H(F)) \quad (2)$$

电网系统端接收后使用本地存储的 ID_1、H(F)、R_2、T_2 进行验证，一致则完成双向身份认证。该双向认证过程将设备标识、时间戳、随机数与物理特征参数哈希值同时纳入认证计算，攻击者即使窃取部分身份信息，也难以在缺失特征参数与时间随机性的条件下实现有效伪造。

（四）基于实时工况的动态会话密钥生成

1.实时充电工况参数采集与同步

双向身份认证通过后，进入会话密钥协商阶段。为增强密钥与工况的绑定性，车桩与电网系统需同步采集充电与电网状态信息。

车桩侧：以不低于100Hz的频率采集充电电压 U、电流 I、温度 θ 及充电电缆阻抗；

电网侧：实时采集区域电网负荷 P、电压波动值 ΔU 等。

双方通过时间同步协议将采集时间差控制在1ms以内，并将上述参数汇总成实时充电工况参数集合 C，确保车桩和电网系统对 C 的认识一致。

2.ECDH会话密钥计算

在获得 C 后，车桩与电网系统分别执行：

（1）对 R_1 与 R_2 进行异或运算得到 $R_1 \oplus R_2$；

（2）获取密钥生成时间戳 T_3；

（3）按式（3）将 $R_1 \oplus R_2$、C、T_3 进行字节拼接并计算哈希值；

（4）以 ID_1、ID_2 为椭圆曲线 ECDH 算法的公私钥生成基础，将所得哈希值作为附加验证参数，计算会话密钥 K：

$$K = \text{ECDH}(ID_1, ID_2, H(R_1 \oplus R_2 \| C \| T_3)) \quad (3)$$

通过引入工况参数 C 和时间戳 T_3，每一轮密钥协商的输入熵与运行状态深度耦合，使得相同设备对在不同工况下生成的密钥彼此独立，大幅提高了攻击者通过离线分析推导密钥的难度。

（五）数据分片加密与传输完整性校验

1.数据分级与核心数据加密

在完成密钥协商后，对待传输数据进行敏感度划分：

核心数据 M_1：包括充电功率调节指令、电量计量数据、电网调度信号等，对电网安全与计量结算高度敏感；

辅助数据 M_2：包括车桩散热状态、设备心跳信号、电网电压监测值等，对安全与计量影响相对较小。

对核心数据 M_1 的加密按式（4）进行：

$$E_1 = \text{AES}_K(M_1 \| \text{HMAC}_K(M_1 \| T_4)) \quad (4)$$

其中，T_4 为加密时间戳，HMAC-K 为基于会话密钥 K 的哈希消息认证码。该设计将保密性（AES加密）与完整性（HMAC）合并在一个封装中，可抵御篡改和伪造。

2.轻量化辅助数据加密

为降低对车桩侧计算资源的占用，对辅助数据 M_2 采用轻量加密策略。先计算数据长度 Len(M_2)，然后按式（5）生成密钥流并进行异或：

$$E_2 = \text{XOR}(M_2, H(K \| T_4 \| \text{Len}(M_2))) \quad (5)$$

其中，H 为 SHA 系列哈希函数，取其128位输出作为异或掩码。该方式在不引入高级分组密码运算的前提下，为低敏感度数据提供基础保密性保护。

3.传输完整性校验与重传机制

发送端在封装数据包时，预先按照式（6）计算接收哈希值[6]：

$$\text{Verify} = H(E_1 \| E_2 \| T_5) \quad (6)$$

其中，T_5 为接收方记录的接收时间戳字段（或发送方预估接收时间窗口标识）。

接收方在收到 E_1、E_2 与包头中的接收哈希值后，记录实际接收时间戳 T_5，重新计算 Verify 并与包头中的哈希值比对。若一致，则认为数据在传输过程中未被篡改或丢失，进入解密流程；若不一致，则拒绝数据并向发送方发起重传请求。

该机制在链路层加密的基础上，提供了应用层完整性校验，有助于及时发现链路异常与中间人攻击行为。

（六）基于工况的密钥动态更新策略

1.充电功率驱动的更新间隔自适应

为兼顾安全性与计算开销，本方法根据实时充电功率 P 自适应调整密钥更新间隔 ΔT：当 P>50kW 时，ΔT =5s；当 20kW ≤ P ≤ 50kW 时，ΔT =15s；当 P<20kW 时，ΔT =30s。

在高功率场景下密钥轮换更为频繁，可有效缩短单一密钥的有效时长，降低其一旦泄露造成的风险范围；在低功率场景下适度延长更新周期，减少冗余计算。

2.电网负荷扰动触发的更新调整

考虑电网负荷波动对整体风险水平的影响，当监测到电网负

荷 P 的变化幅度超过 ±5kW 时，即认为系统处于负载变化较剧烈的状态，立即重新评估ΔT 取值并可触发新一轮会话密钥协商，以提升在负荷扰动时期的通信安全等级。

3.密钥轮换与过渡密钥机制

在每个ΔT 周期到达后，车桩与电网系统重新执行动态会话密钥生成环节：采集当前实时充电工况参数 C，生成新的随机数对，计算新会话密钥 K'。当双方完成新密钥的生成与校验后，立即在各自安全芯片中删除旧密钥 K，不保留任何缓存记录，避免旧密钥因软件漏洞或调试接口被导出。

为避免在密钥轮换期间出现短暂的“无密钥”状态，核心数据 M_1 采用临时过渡密钥进行加密传输。过渡密钥可由旧密钥 K 与新密钥 K' 合成，并仅在极短更新窗口内有效，从而保障业务连续性与安全性。

二、安全性与工程应用分析

（一）安全性分析

从攻击者视角出发，本文方法在以下方面显著提高了攻击门槛：

（1）抗设备伪造：双向认证同时依赖唯一硬件标识与物理特征参数哈希值，攻击者不仅需窃取标识，还需复制或模拟多源物理特征，难度大幅提高。

（2）抗重放与中间人攻击：引入时间戳有效窗口与随机数参与认证与密钥生成，旧报文即便被重放也无法通过时间戳校验与哈希码比对，中间人难以构造合法认证码。

（3）密钥动态绑定工况：会话密钥与实时充电工况参数 C 与随机数异或结果耦合，同一设备在不同时间、不同工况下的密钥高度去相关，减少了通过长期流量分析破解密钥的可能性。

（4）分级加密与完整性保障：对核心数据采用 AES+HMAC 组合加密与认证，确保保密性与抗篡改性；对辅助数据采用轻量化加密，在一定程度上降低信息泄露风险。

（5）全生命周期密钥管理：基于功率与负荷扰动的更新策略缩短高风险时段的密钥生命周期，配合旧密钥彻底删除与过渡密钥机制，减少密钥泄露后可利用的攻击窗口。

（二）工程实现与性能考虑

在工程实现层面，本方法充分考虑了车桩侧算力与实时性约束：

（1）关键密码运算可依托主控芯片或外置安全芯片的硬件加速模块实现，减轻 CPU 负担；

（2）对辅助数据采用基于哈希的 XOR 轻量化加密，避免对所有数据统一采用重型加密算法，兼顾能耗与延时；

（3）通过合理配置采样频率、时间同步与缓存机制，可在不影响充电控制实时性的前提下，完成工况采集与密钥协商过程。

三、结论

本文针对超快充车桩与电网系统车网互动过程中存在的身份伪造风险、密钥管理薄弱以及数据传输安全隐患等问题，提出了一种超快充设施车网互动重要数据安全加密识别方法。主要工作与结论如下：

（1）构建了基于唯一硬件标识与多源物理特征参数的初始特征库，设计了融入时间戳与随机数的双向身份认证机制，实现车桩与电网系统的高可信互认；

（2）提出结合实时充电工况参数 C 与随机数异或结果的 ECDH 动态会话密钥生成方法，使密钥与车网运行状态紧密绑定，显著提高了密钥破解难度；

（3）设计数据分片与分级加密策略，对核心数据采用 AES+HMAC 强加密，对辅助数据采用哈希 +XOR 轻量化加密，并通过接收哈希值比对实现传输完整性校验；

（4）构建以充电功率与电网负荷变化为驱动的密钥动态更新机制，结合临时过渡密钥保障密钥轮换过程中的业务连续性，从而实现密钥全生命周期安全管理。

总体来看，该方法在不显著增加车桩侧算力压力的前提下，系统性提升了超快充车网互动的数据保密性、完整性与身份可信度，适合在面向大规模超快充站群与车网协同控制场景中推广应用。

参考文献

[1] 刘书琪，唐啸，吴滨，等 . 基于用户需求与充电站用能特征的插电式电动汽车充电需求预测研究 [J]. 微型电脑应用，2025,41(10):20-23+28.

[2] 沈润，程晴，陈业策，等 . 含 V2G 充电桩和储能的台区重过载风险评估与治理 [J]. 供用电，2025,42(06):22-30.

[3] 魏志超 . 网络通信中的信息安全保障措施探究 [J]. 中国宽带，2025,21(01):46-48.

[4] 李森森，黄一才，黄美根，等 . 面向移动边缘计算的高效条件隐私保护认证密钥协商方案 [J]. 通信学报，2025,46(09):195-212.

[5] 张欣 . 基于云计算环境的计算机安全防护策略研究 [J]. 信息记录材料，2025,26(11):191-193.

[6] 王艳玲 . 基于哈希值计算的数据爬取策略 [J]. 昆明冶金高等专科学校学报，2024,40(06):73-77.

