电子不停车收费系统数据安全传输与加密技术

欧阳拉丁

湖北交投科技发展有限公司 湖北 武汉 430000

【摘　要】：电子不停车收费系统在提高通行效率的同时，面临数据传输过程中潜在的安全风险，包括信息泄露和篡改。为了确保系统的安全性与可靠性，采用先进的加密算法和安全传输协议，对收费数据进行实时加密和验证，实现数据完整性保护和防篡改措施。实验结果显示，基于改进的加密与传输方案，系统在高速通信环境下保持高效运行，同时有效防止信息泄露，提高了通行安全性与用户数据保护水平，为智能交通系统的数据安全提供可行方案。

【关键词】：电子不停车收费；数据安全；加密技术；传输协议；信息保护

DOI:10.12417/2705-0998.26.08.075

引言

电子不停车收费系统在现代交通管理中广泛应用，其高效便捷的特点依赖于实时数据传输。高速数据交换环境下的安全威胁日益增加，存在信息泄露、篡改和非法攻击风险。保障系统数据安全不仅关系收费准确性，也影响用户信任度。通过对加密技术和安全传输机制的优化，可在保证高速通行效率的同时，提升系统数据完整性和抗攻击能力。深入分析和设计高效的加密传输方案，将为智能交通系统提供稳定可靠的安全保障，并在实际应用中展现可行性和有效性。

1 电子不停车收费系统的数据传输问题

1.1 高速通信环境下的数据泄露风险

电子不停车收费系统依赖高速无线通信进行车辆识别和支付信息传输，数据在短时间内跨多个节点传递。高速传输增加了信息在无线信道中被截获的可能性，未加密或弱加密的数据存在被窃取的风险。同时，网络拓扑复杂，信号覆盖区域广，易形成潜在攻击面，数据包在不同网络层被嗅探和分析的概率提升。在 ETC 系统中，数据泄露不仅涉及账户信息，还包括车辆身份和通行记录，这类信息敏感性高，对系统整体安全和用户隐私保护提出了严格要求。在高速通信环境下，必须采取高强度加密和多层防护措施，以确保传输链路中的数据机密性和防止非授权访问。

1.2 信息篡改对收费准确性的影响

在电子不停车收费系统中，数据传输环节的完整性直接决定收费计算的准确性。信息在传输过程中可能被恶意篡改或出现非恶意误传，导致账单错误、交易冲突和系统异常。篡改行为包括数据字段替换、金额修改、时间戳伪造等，这些问题不仅破坏收费记录的准确性，也会引发系统结算的不一致性[1]。现有传输链路若缺乏有效的完整性校验机制，攻击者或网络干扰可在不被检测的情况下改变关键数据。建立多层验证机制、消息摘要和数字签名技术可增强数据不可篡改性，保证在高速传输条件下系统收费的精确和可靠性。

1.3 现有传输协议的安全缺陷

现行电子不停车收费系统采用的传输协议多为标准化通信协议，设计重点在于效率和兼容性，而安全防护功能不足。协议在身份认证、密钥管理、加密算法适配性方面存在漏洞，易受到中间人攻击、重放攻击和会话劫持。部分协议缺乏动态密钥更新和实时验证机制，使长期使用的静态密钥成为攻击目标。高速数据传输对协议的抗攻击能力提出更高要求，单纯依赖传统协议容易导致数据泄露和信息篡改。优化传输协议、引入端到端加密和多因素认证策略，可以在保证通信效率的基础上提升安全性，适应现代智能交通系统对数据安全的高标准需求。

2 数据加密技术选择与实现

2.1 对称加密算法的应用与优化

对称加密算法在电子不停车收费系统中承担着实时数据加密的核心角色，其特性是加密和解密使用相同密钥，计算速度高、适合处理大量快速生成的交易数据。在高速通信环境下，通过优化密钥管理和分段加密机制，可显著降低数据泄露风险，并满足低延迟的传输要求。优化策略包括采用动态密钥生成和周期性更新机制，使攻击者难以获取长期有效密钥，同时结合高效的分组加密模式，对数据流进行实时分段处理，保障密文在传输链路中保持一致性和完整性。对称算法的实现应兼顾系统计算能力与安全强度，通过硬件加速或并行计算优化数据处理效率，以支撑大规模车辆通行的实时需求，同时提高系统整体抗攻击能力，形成高速且安全的数据加密环境。

2.2 非对称加密算法的集成方案

非对称加密算法在 ETC 系统中主要用于密钥交换、身份验证和数据签名，其公私钥结构能够保证通信双方的身份可验证性和数据完整性。集成方案需在系统通信框架中设计端到端密钥传递和数字签名验证流程，以防止中间人攻击和重放攻击。公钥基础设施（PKI）管理机制能够实现密钥的动态分发和权限控制，提高系统在大规模网络环境下的适应性[2]。算法优化包括采用高效的椭圆曲线加密和基于短密钥长度的快速

签名技术，在降低计算负荷的同时保持高安全强度。通过与传输协议的深度结合，非对称加密可在保证数据机密性与完整性的同时，支持系统实时认证需求，使 ETC 系统在面对复杂通信环境和潜在攻击时保持可靠性和安全性。

2.3 混合加密模式在 ETC 系统中的应用

混合加密模式将对称加密与非对称加密优势结合，实现数据传输的高效性和安全性双重保障。在 ETC 系统中，交易数据通过对称算法快速加密，而密钥则使用非对称算法进行安全传输，从而兼顾数据处理速度和密钥安全性。该模式设计需考虑数据流量、传输延迟和系统资源限制，通过分层加密策略和动态密钥更新机制增强抗攻击能力，同时引入消息认证码和签名验证确保数据完整性。混合加密还可以支持安全会话建立和端到端加密，提升整个收费系统的防护水平。结合现代智能交通系统对高速数据处理和实时安全性的要求，混合模式能够在大规模车辆通行场景中保持数据机密性和完整性，并提高系统对异常行为和攻击尝试的自适应能力，实现安全与效率的有机统一。

3 安全传输协议设计与改进

3.1 基于 TLS/SSL 的传输安全方案

基于 TLS/SSL 的传输安全方案在电子不停车收费系统中实现了端到端的数据加密和身份认证，确保收费信息在高速通信链路上的机密性和完整性。该方案通过握手协议建立安全会话，动态生成会话密钥，实现数据加密和解密的实时转换，减少数据在传输过程中被截获的风险。协议支持分层加密和会话分离，可在高速数据流中有效管理不同类型的数据包，提高系统处理效率。同时，TLS/SSL 能够与现有网络架构无缝集成，支持证书验证和加密算法协商，使数据传输在不同网络节点间保持一致的安全等级。优化实施包括启用高强度加密套件和实时密钥更新机制，使 ETC 系统在面对高速通信、海量交易和潜在攻击时保持稳定性和安全性，保障收费数据的可信性。

3.2 消息认证与完整性验证机制

消息认证与完整性验证机制是保证电子不停车收费系统数据可靠性的重要环节。通过使用消息认证码（MAC）、数字签名和哈希函数对传输数据进行验证，能够即时检测数据是否在传输过程中被篡改。机制设计包括数据块划分、散列算法运算和签名附加，实现对每条数据的完整性检查，同时支持高速处理和并行计算，降低验证延迟[3]。动态密钥与散列算法结合可以提升抗攻击能力，使数据即便在多跳网络传输中也保持一致性和防篡改特性。系统可实时比对发送和接收的数据摘要，检测异常变化并触发安全响应，有效保障收费数据在无线通信环境中的准确性和可靠性，为 ETC 系统在高速运行条件下提供稳定的安全保障基础。

3.3 抗攻击策略在高速数据传输中的实践

抗攻击策略在高速数据传输中通过多层防护和异常检测实现对电子不停车收费系统的安全增强。策略包括对中间人攻击、重放攻击和拒绝服务攻击的防御，结合加密传输、动态密钥管理和行为异常检测算法，形成主动防御体系。系统通过实时监测数据流量和通信特征，对异常传输行为进行识别和隔离，同时结合速率限制和分段传输机制减少攻击影响范围。策略还包括端到端加密与分级权限控制，确保敏感数据仅在授权节点间传输，降低潜在泄露风险。在实际应用中，通过策略集成和算法优化，能够在高速数据传输环境中保持系统稳定性和数据安全性，确保收费信息的完整性和可追溯性，同时提升系统对未知攻击的自适应响应能力。

4 系统集成与实验验证

4.1 加密与传输模块的集成方法

加密与传输模块集成需实现数据加密、解密和安全传输的高效协同。系统通过模块化设计，将对称加密、非对称加密及混合加密策略嵌入通信链路，实现密钥管理、数据加密及完整性验证的统一接口。集成过程中对网络拓扑进行优化，确保不同节点间数据交换延迟最小化，同时保持加密处理的实时性。模块间采用统一的数据格式和协议适配层，保证加密数据与传输协议的兼容性和可扩展性。通过分层处理和异步通信机制，减少加密操作对传输速度的影响，同时实现加密算法的动态选择和安全策略的快速更新，提高系统在多车辆并发通信条件下的整体可靠性和数据保护水平。

4.2 系统性能测试与安全性评估

系统性能测试与安全性评估包括通信效率、数据加密开销和安全防护能力的综合考核[4]。测试内容覆盖高并发数据传输场景下的吞吐量、延迟及加密解密响应时间，通过量化指标分析加密算法和传输协议在实际运行环境中的性能表现。安全性评估针对信息泄露、数据篡改和潜在攻击风险，验证消息认证、密钥更新及异常检测机制的有效性。评估过程中引入多维指标体系，包括密文完整性、会话安全性和节点身份验证强度，为优化系统结构和加密方案提供数据支撑。性能测试与安全评估紧密结合，为电子不停车收费系统在高速数据传输环境下提供可靠的技术保障依据。

4.3 实验结果分析与优化策略

实验结果显示，通过模块化加密集成和优化传输协议，系统在高密度车辆通行环境中保持低延迟、高吞吐量的数据处理能力，同时有效防止数据泄露和篡改。对不同加密算法组合及密钥长度进行性能对比，分析加密负荷对传输效率的影响，识别系统瓶颈。优化策略包括动态调整加密模式、密钥周期性更新及数据分段传输，以降低加密计算开销并增强数据完整性保障。实验数据支持安全策略的迭代更新，使系统能够在复杂网

络环境中维持稳定运行和高安全等级，同时满足智能交通对实时性和可靠性的双重要求，为电子不停车收费系统的安全传输提供实证基础。

5 数据安全保障效果评估

5.1 信息泄露防护效果分析

信息泄露防护效果通过对数据传输链路和存储节点的多层加密策略进行验证。数据在传输过程中采用动态密钥和混合加密方式，密文在不同网络节点间保持不可解读性，显著降低信息被截获的概率。防护机制涵盖端到端加密、密钥管理、身份认证及异常流量监控，实现对潜在攻击和非授权访问的实时阻断。对网络数据包进行加密处理和完整性校验，提高敏感信息在无线通信环境中的保密性。同时，系统支持密钥自动更新和会话隔离，确保短周期密钥更新可降低长期使用密钥带来的泄露风险。实验数据表明，多重防护机制能够有效封锁外部威胁，维持收费系统信息安全水平，确保用户身份和交易数据的高度机密性。

5.2 数据完整性与准确性验证

数据完整性与准确性验证通过对交易信息的实时校验、消息认证码以及数字签名进行实施，确保数据在传输和存储过程中不被篡改。每条交易数据在加密前生成唯一摘要，接收端通过摘要比对和签名验证检测异常变化，实现对信息篡改的即时识别[5]。高频交易和大规模并发访问环境下，采用分段验证与并行校验机制，提高数据处理效率与安全可靠性。密钥管理和动态验证策略保证验证过程对数据完整性和准确性无延迟影响，同时降低系统误报率。验证结果显示，通过多层认证机制，可有效防止数据损坏、丢失或误写问题，保证电子不停车收费系统在高速通信条件下的交易精度和账单一致性，为收费过程的可靠性提供技术支撑。

5.3 系统稳定性和用户信任度提升

系统稳定性与用户信任度通过安全传输和加密机制的整体性能优化得以提升。多层加密和动态密钥管理保障通信链路在高并发车辆通行条件下保持低延迟和高吞吐量，减少数据丢包和传输错误，维持系统持续运行的可靠性。异常检测与防护机制增强系统对潜在攻击的自适应处理能力，确保数据处理过程连续性和操作安全性。稳定运行与高安全性共同构建用户信任基础，使收费信息和车辆通行数据保持高度一致和透明性。实验和性能监测表明，优化后的系统在应对高速数据传输和网络波动时仍能维持安全和高效运行，为智能交通环境下的电子不停车收费提供可信赖的数据安全保障。

6 结语

电子不停车收费系统的数据安全传输与加密技术在保障交易信息完整性、预防信息泄露以及提高系统稳定性方面发挥关键作用。优化的加密策略、动态密钥管理和安全传输协议实现了高效通信与安全防护的结合，为智能交通环境下的收费系统提供可靠的数据保护基础，支持系统在高速数据传输和复杂网络环境中稳定运行，并增强用户信任度。

参考文献：

[1] 卜骁男.电子信息数据加密技术在计算机网络安全中的应用[J].中国自动识别技术,2025(4):67-69.

[2] 李解焕.电子工程中的数据安全与加密技术研究[J].电子元器件与信息技术,2025,9(7):143-145+149.

[3] 洪焕江.基于数据加密技术的电子商务计算机网络安全管理研究[J].中国电子商务,2025,26(22):33-36.

[4] 陈磊.电子信息工程数据传输领域的安全性与加密技术研究[J].移动信息,2025,47(5):199-201.

[5] 裴雅,李亚珂.数据加密技术在计算机网络通信安全中的应用探究[J].信息记录材料,2025,26(4):87-89.