doi: 10.3969/j.issn.1672-6073.2025.04.016

基于超级SIM卡与盲化ECDSA的轨道交通无人机智能检测与认证方案

孔令南[1]，冯国栋[1]，钱振东[1]，孙彭轩[2]
（1. 中国移动通信集团云南有限公司，昆明 650228；2. 北京工业大学，北京 100124）

摘　要：为满足轨道交通设备安全监测与维护过程中高效、低功耗且安全的认证机制需求，本文对跨域身份认证的实现展开系统研究。设计一种以超级 SIM 卡为身份载体、结合低功耗蓝牙技术实现设备间快速数据交互的系统架构，在此基础上提出一种融合盲化椭圆曲线数字签名算法(elliptic curve digital signature algorithm，ECDSA)的高效匿名身份认证方案，并将该方案与可监管匿名认证方案等现有方法在计算和通信开销方面进行对比。研究结果表明：与基于 NIST 标准的 ECDSA 和传统椭圆曲线密码(elliptic curve cryptography，ECC)算法相比，本文方案在签名生成阶段表现更优，综合运行时间最短；相比可监管匿名认证方案，在认证效率方面提升 43.8%，验证了本文方案的有效性和可行性。研究结果可为低空经济与轨道交通领域设备的智能化安全监测与维护提供参考。

关键词：低空经济；轨道交通；超级 SIM 卡；盲化 ECDSA；无人机；安全监测；身份认证
中图分类号：TN925；U231　　**文献标志码：**A　　**文章编号：**1672-6073(2025)04-0117-08

Drone Authentication and Intelligent Monitoring Solutions for Rail Transit Equipment Based on Super SIM Card and Blinded ECDSA Technology

KONG Lingnan[1], FENG Guodong[1], QIAN Zhendong[1], SUN Pengxuan[2]
(1. China Mobile Group Yunnan Co., Ltd., Kunming 650228;
2. Beijing University of Technology, Beijing 100124)

Abstract: To meet the demand for efficient, low-power, and secure authentication mechanisms in the safety monitoring and maintenance of rail transit equipment, this study systematically investigates the implementation of cross-domain identity authentication. First, a system architecture is designed using a super SIM card as the identity carrier, combined with Bluetooth Low Energy (BLE) technology for rapid data exchange between devices. Second, a high-efficiency anonymous identity authentication scheme integrating a blinded ECDSA algorithm is proposed. Finally, the proposed scheme is compared with supervised anonymous authentication schemes and other traditional authentication algorithms regarding computation and communication overheads. The results indicate that, compared to NIST-standard-based ECDSA and traditional ECC algorithms,

收稿日期：2025-02-08　修回日期：2025-03-01
第一作者：孔令南，男，硕士，主要从事轨道交通设备通信研究工作，KongL1ngNan@163.com
基金项目：北京市科委(2024YFB3108202)
引用格式：孔令南，冯国栋，钱振东，等. 基于超级 SIM 卡与盲化 ECDSA 的轨道交通无人机智能检测与认证方案[J]. 都市快轨交通，2025，38(4)：117–124.
KONG Lingnan, FENG Guodong, QIAN Zhendong, et al. Drone authentication and intelligent monitoring solutions for rail transit equipment based on super SIM card and blinded ECDSA technology[J]. Urban rapid rail transit, 2025, 38(4): 117–124.

the proposed scheme demonstrates superior performance in signature generation with the shortest overall runtime. Additionally, authentication efficiency is improved by 43.8% compared to supervised anonymous authentication schemes, verifying the effectiveness and feasibility of the proposed approach. These findings provide a valuable reference for intelligent security monitoring and maintenance of equipment in low-altitude economic sectors and the rail transit field.
Keywords: low-altitude economy; rail transit; super SIM card; blinded ECDSA; drone; security monitoring; authentication

低空经济指在低空飞行空间(一般指地面至约1000 m 高度之间)进行商业运营和资源开发的经济活动。低空经济的发展得益于无人机、低空飞行器以及相关技术的快速进步，这些技术在农业、物流、环境监测、基础设施建设和维护等多个领域得到了广泛应用[1]。轨道交通作为现代城市化的重要支撑系统，其设备的运行状态和维护需求对交通安全与效率至关重要。轨道交通设备通常分布广泛、环境复杂，传统的监测和维护方式在效率和实时性方面存在一定局限[2]。无人机搭载低功耗蓝牙技术，为轨道交通设备的监测和维护提供了一种创新的解决方案。然而，随着无人机数量的激增和应用场景的多样化，如何保障无人机的安全性、稳定性和高效性，有效完成对轨道交通设备的监测任务，已成为低空经济发展的关键挑战之一[3]。传统的身份认证方式，如密码、加密算法等，往往在执行过程中面临性能瓶颈，无法满足无人机在复杂环境下快速、安全的身份认证需求。

目前，市场上的无人机身份认证方案主要依赖于传统的加密技术和无线通信协议[4]。无人机在空中飞行时需要与地面控制系统进行频繁通信，这要求身份认证过程能够实现低延迟、高效率，同时保障通信过程中的数据安全[5]。传统的加密算法，如高级加密标准(advanced encryption standard，AES)，虽然能够提供较强的安全性，但在进行高频次、大规模的身份认证时，其计算负担较重，难以满足实时性要求[6]。

在此背景下，超级 SIM 卡(super SIM card)作为一种高安全性身份认证技术，逐渐在无人机领域获得关注。超级 SIM 卡是运营商为用户提供高安全级别认证的硬件载体，能够为无人机提供快速且可靠的身份验证机制。无人机能够快速覆盖轨道交通沿线广泛分布的设备区域。相比传统人工巡检，无人机搭载高清摄像头和多种传感器，可以实现对设备的实时监控和异常检测，提高了监测效率[7]。利用无人机监测轨道交通设备的主要优势在于无人机方案可以通过预设飞行路径和自动监测功能降低成本与减少人力投入；无人机可以利用高分辨率成像设备和先进的传感技术提升监测精度与安全性；灵活性与多样化应用使无人机能够适应复杂的轨道交通环境，快速响应突发事件。

超级 SIM 卡所使用的蓝牙无线技术因其成本低廉、安全性高、可靠性好等优势而获得消费者和市场的青睐，在短距离无线通信领域占据重要位置，被广泛应用于轨道交通电子设备、低空无人机设备、可穿戴设备以及各种移动设备[8]。采用蓝牙低功耗技术可以使超级 SIM 卡的效率提高 17 倍，而且让它拥有更远的传输距离和更快的传输速度。随着制造工艺技术的不断提高，低功耗蓝牙的成本也会变得更加低廉[9]。

现在市场上的无人机基本都配备了低功耗蓝牙设备，通过应用软件可轻松实现无人机认证无卡化[10-12]。但是，低功耗蓝牙采用 128 位的 AES 算法来对数据进行加密，通过基础的配对协议来对密钥进行管理，使用户身份认证过程的安全性较低。增加该算法的运算位数能够增强安全性但是与低功耗蓝牙的计算能力不匹配。

在低空轨道设备通信认证方面，许多研究者们提出了高效安全的认证机制。黄婉悦等[13]以先进的 RISC 机器(advanced RISC machines，ARM)处理器 STM32 芯片作为控制核心，使蓝牙模块将采集到的信息发送到 STM32F103 处理器，对信息进行处理和比对，实现对低空移动系统的控制；弓皓臣等[14]针对无人机自组网设备算力有限的问题，设计了一种轻量化区块链的无人机蜂群身份认证系统，利用一种轻量化可信的区块链共识算法(practical byzantine fault tolerance，PBFT)，降低了通信复杂度，实现了更高的效率和稳定性；KIRSAL 等[15]提出了一个基于椭圆曲线的无人机网络环境认证框架，无人机被视为无线感知网络(wireless sensor networks，WSNs)物联网应用的移动接收器，能够提高传感器节点的生命周期和连通性，抵抗和密钥泄露假冒攻击和密码猜测攻击；LEI 等[16]针对无人机互联网络，提出了一种基于优化身份协议的轻量级身份安全认证协议，该协议针对 IoD 网络面临的安全风险，提出了由 3 个阶段和 7 个认证过程组成的安全认证机制，确保协议兼具前向和后向安全性；

JAN 等[17]针对飞行自组网的信息传输完整性和真实性问题，设计了一个基于可验证安全椭圆曲线密码(elliptic curve cryptography，ECC)的飞行自组网认证方案。然而，ECC 算法虽然对于密钥的分发和管理实现较简单，但运算速度相对较慢，只适合加密很短的数据。

现有研究均没有充分解决无人机认证方案中传统蓝牙通信功耗、安全性不足和用户身份认证可靠性不高的问题，因此，本文对更加安全可靠且高效的无人机身份认证与监测方案进行研究，基于超级 SIM 芯片的可信身份认证能力与盲化 ECDSA 算法，设计了一种通过 SPI 接口扩展低功耗蓝牙协议的无人机通信系统，提出了一种基于盲化 ECDSA 改进的高效匿名身份认证机制，有效提升了认证的安全性与效率，整体效率较同类方案提高了 43.8%。

1 相关概念

1.1 超级 SIM 卡

超级 SIM 卡相比传统 SIM 卡在存储、安全性、计算能力和应用扩展方面进行了提升。传统 SIM 卡存储空间有限，仅用于基本身份认证，而超级 SIM 卡采用大容量芯片，可存储加密证书和私钥，支持更高级的加密算法，如 ECC、RSA、SM2/SM4 等，提供更强的安全防护[18]。其内置独立计算单元，支持复杂密码运算，如零知识证明和多方安全计算，使身份认证更加高效安全[19]。同时，超级 SIM 卡具备开放式应用程序编程接口(application programming interface，API)，支持加载第三方应用，可用于移动支付、区块链钱包和物联网设备认证。此外，它兼容 5G、NB-IoT 等多种通信协议，适用于更多智能设备。相比传统 SIM 卡仅限于网络接入，超级 SIM 卡已成为集存储、安全计算和身份认证于一体的智能终端，适用于高安全性应用场景。

1.2 数字签名

数字签名算法(digital signature algorithm，DSA)是一种基于公钥密码学的加密技术，用于确认数字信息的身份并验证其完整性[20]，它涉及签名和验证两个主要过程。在签名过程中，使用私钥对数字信息进行加密，以证明其身份和完整性，并生成数字签名。在验证过程中，使用公钥解密签名以验证数字信息的身份。

数字签名算法的定义中涉及两种密码学技术：公钥密码学和哈希函数。公钥密码学是一种非对称加密技术，使用两个不同的密钥。哈希函数是一种密码学算法，将任意长度的消息映射为固定长度的哈希值。数字签名算法通常使用哈希函数来计算数字信息的摘要，再利用私钥将其加密生成数字签名。

1.3 ECDSA 数字签名

椭圆曲线数字签名算法(elliptic curve digital signature algorithm，ECDSA)是一种非常流行的算法之一。它是基于椭圆曲线密码学的一个变种，能够在相对较短的密钥长度下提供比其他算法更高的安全性[19]。ECDSA 涉及 4 种具体算法。

1) 初始化算法 Initial(1^{μ})：输入安全常数 μ，生成椭圆期限群 $Q=(q, G, g, \boldsymbol{Z}_{\mathrm{r}})$，其中 q 表示 Q 的阶，G 是基于椭圆曲线上的加法运算构成的群集合，g 表示 G 的基点，$\boldsymbol{Z}_{\mathrm{r}}$ 表示整数模群，用于表示哈希函数的输出空间。选择扛碰撞哈希函数 H：$\{0, 1\}^{*} \rightarrow \boldsymbol{Z}_{\mathrm{r}}$，输出 ECDSA 数字签名的公开参数 parameters=(Q，H)。

2) 密钥生成算法 KeyGeneration(parameters)：输入公开参数 parameters，生成密钥对(pubKey，scrKey)。在整数群 $\boldsymbol{Z}_{\mathrm{r}}$ 上随机选择整数 ranNum，计算 $p=g^{\mathrm{ranNum}}$，最后输出生成的密钥对 scrKey 设为 x，pubKey 设为 p。

3) 签名算法 Sign(parameters，scrKey，message)：输入公开参数 parameters、用于签名的私钥 scrKey、消息 message，输出关于消息 message 的签名 l。在整数群 $\boldsymbol{Z}_{\mathrm{r}}$ 上随机选一个整数 z，计算 $J=g^{z}$，令 $j=J_x(\mathrm{mod}\ q)$，若 $j=0$，则重新选择 z，计算 signature=$z^{-1}(H(m)+J_x)(\mathrm{mod}\ q)$，输出签名 l=(signature，j)。

4) 验证算法 VerifySignature：(parameters，message，l，pubkey)：输入公开参数 parameters、消息 message、消息 message 的签名 l 及对应公钥 pubKey，针对签名进行验证是否有效，若 $j=0$ 且 signature=0，返回 0；否则计算 $h=H(\mathrm{message})$，$w=\mathrm{signature}^{-1}(\mathrm{mod}\ q)$，$y_1=h\cdot w(\mathrm{mod}\ q)$，$y_2=j\cdot w(\mathrm{mod}\ q)$。最后根据 y_1 和 y_2 的计算数据，算出 $J=g^{y_1}\mathrm{pubKey}^{y_2}$，如果 $J_x=j(\mathrm{mod}\ q)$，则输出 1；反之，输出 0。

1.4 基于盲化 ECDSA 改进的高效匿名算法

基于盲化 ECDSA 改进的高效匿名身份认证方案主要包含 7 种算法。

1) 初始化算法 Initial：输入安全常数 μ，输出系统公共参数 parameters = $\{G, G_{\mathrm{T}}, e, g, H, \boldsymbol{Z}_p\}$。其中 G_T 是乘法循环群，e 为双线性映射函数，$\boldsymbol{Z}_p$ 是模 p 的整数群。

2) 密钥生成算法 KeyGeneration(params)：输入系统公开参数 parameters，输出密钥对(pubKey，scrKey)。

3) 用户注册算法 UserIndentity：输入个人信息 m，公钥 pubKey、私钥 r，生成身份摘要 CH(message)，记为 ChameleonHash(pubKey，message，scrKey)→CH(message)。

4) 认证密钥生成算法 GenerateKey：输入公共参数值 parameters，输出密钥对(pk_{ca}，sk_{ca})，用于生成和验证用户身份证明。

5) 身份证明生成算法 CertificationGen：输入 CH(message)、pk_{ca}，输出身份证明 certification。

6) 出示身份证明 ShowCertification：输入系统公开参数 parameters、pk_{ca}，输出对应身份证明 certification。

7) 验证身份证明 CertificationVertify：验证者验证用户身份证明，输入公开参数 parameters，用户给出的证明 certification 及 pk_{ca}，若 certification 有效且验证通过输出 1，否则输出 0。

2 无人机监测轨道设备任务下达方案

通过无线蓝牙技术和超级 SIM 卡的认证技术，用户通过终端的 APP 就能安全地发起无人机对轨道交通设备的安全监测任务。任务下达流程如下。

1) 任务分配：服务端生成轨道交通设备监测任务信息，包括设备位置、监测类型等，并通过蓝牙发送至无人机。用户在 APP 里点击发起信息传输，终端即通过蓝牙模块向从机发送身份证明 certificate、身份证明公钥 pk_{ca}、盲化因子等数据，无人机控制器对传送来的身份证明 certificate 进行盲化之后跟证明中心中存储的盲化身份证明 blind_certificate 进行比较验证，若通过则表示用户身份属实，开启信息传输流程，并向中央控制器发送该任务记录，不通过则不予执行。

2) 监测执行：无人机启用搭载的传感器(如摄像头、振动传感器、温湿度传感器等)对轨道交通设备进行全面扫描和数据采集。检测轨道交通设备的运行状态(如轨道磨损情况、信号灯工作情况、设备表面温度等)，并记录异常数据。

3) 数据分析与反馈：无人机将采集到的原始数据通过蓝牙传输至移动终端，由终端上传至服务端。服务端对数据进行处理与分析，生成监测报告，并将结果推送至相关维护人员。

4) 任务记录与状态更新：服务端记录监测任务的执行情况，包括任务分配时间、数据上传时间以及异常检测结果。无人机任务完成后进入低功耗待机模式，等待后续指令。

监测任务下发流程如图 1 所示，通过高效的任务分配与执行机制，系统能够实时保障轨道交通设备的安全运行，为低空经济与轨道交通的深度融合提供可靠支持。

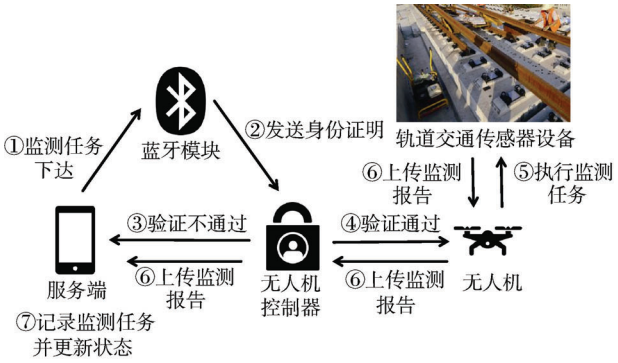


图 1 轨道交通设备监测任务下发流程

Figure 1 Task deployment process for rail transit equipment monitoring

3 无人机安全身份认证方案设计

3.1 总体框架

由于轨道设备通常分布广泛，且环境复杂，传统的人工巡检方式面临效率和安全性的挑战。无人机提供了一种高效、智能的解决方案，但与此同时，如何确保无人机的任务下达与数据传输的安全性，也成为确保监测任务顺利执行的关键问题。因此，确保无人机的身份认证和任务执行的安全性，是实现精确监控和高效管理的基础。

无人机安全身份认证方案由服务端、蓝牙通信、无人机控制器 3 个模块组成。服务端模块作为中央控制器，负责管理用户身份的注册、认证密钥的分发，以及无人机与轨道交通设备之间的任务协作。蓝牙通信模块通过低功耗蓝牙技术，实现无人机与轨道交通设备、用户移动终端的高效数据交互。无人机控制模块控制无人机的飞行任务和设备交互，包括身份认证、轨道交通设备监测任务的执行与反馈。无人机安全身份认证方案的总体框架如图 2 所示。

3.2 设计细节

3.2.1 用户注册

用户在首次使用时，需要先进行注册，用户需在 APP 内填写基本信息，包括姓名、电话号码、无人机设备 ID，无人机通信模块信息等，作为用户信息 $message_1$。中央控制器中要进行以下操作。

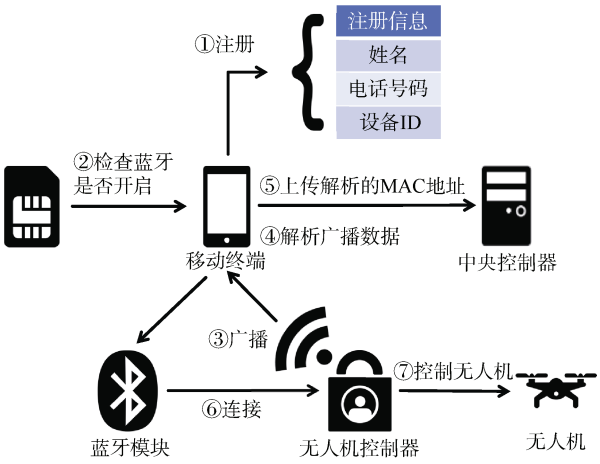


图 2　无人机安全身份认证方案的总体框架

Figure 2　Framework of drone security authentication

1) 初始化参数列表：输入安全常数 μ，选择两个阶为素数 p 的循环群 G 和 G_T，并选择 G 群的生成元 g，设置双线性对映射 e：$G\times G\to G_T$，设 H：$\{0,1\}^*\to G$ 为加密散列函数。输出公共参数值 parameters = $\{G,G_T,e,g,H,\boldsymbol{Z}_p\}$。

2) 生成初始身份摘要：输入公共参数值 parameters 及用户信息 message_1，在 $\boldsymbol{Z}_p$ 整数群上选择一个随机数 x，并计算出 $\text{h}=g^{x\cdot H(\text{message}_1)}$，其中 x 作为用户私钥 scrKey，用户公钥 pubKey=(g，h)。然后计算生成初始身份摘要 $\text{CHash}=e\left(g^{\text{message}_1},\ \text{h}^x\right)$。选择唯一值用户手机号 UID，获取当前用户生成证明的时间戳 t_{cur}，并设置证明的有效期 t_{valid}。输出用户参数组 $\text{param}_{\text{UID}}=\left\langle \text{UID},t_{\text{cur}},t_{\text{valid}},\text{CHash},g,H\left(\text{message}_1\right),\text{message}_1\right\rangle$。

3) 存储参数：将生成的哈希值 CHash 通过智能合约写入区块链中。

4) 初始化身份证明密钥对 $(\text{pk}_{\text{ca}},\text{sk}_{\text{ca}})\leftarrow$ getGeneratekey()：输入公共参数值 parameters，并初始化椭圆曲线函数 E，在曲线上随机选取一点 g_E 作为基点，在 $\mathbf{Z}_p$ 整数群上选择一个随机数 γ，使得私钥 $\text{sk}_{\text{ca}}=\gamma$，公钥 $\text{pk}_{\text{ca}}=g_E^{\gamma}\left(\text{mod}\ p\right)$；该密钥用于后续生成和验证身份证明。

5) 生成身份证明：输入用户参数组 $\text{param}_{\text{UID}}$，利用 SHA256 算法生成身份证明 certificate，并将生成的身份证明 certificate 交给用户，然后通过智能合约将 CHash 及 certificate 进行链上存储证据。

6) 盲化身份证明：输入用户参数组 $\text{param}_{\text{UID}}$，在整数群 $\boldsymbol{Z}_p$ 上随机选择两个整数 α，β，获取用户真实身份证明 certificate，计算 $r=(g^{\text{pk}_{\text{ca}}-\alpha}\ \text{mod}\ p)\text{mod}\ p$，$s=\text{pk}_{\text{ca}}\times\text{certificate}+\beta\times r\ \text{mod}\ p$，生成 $\text{blind_certificate}=\{r,s\}$，将盲化因子交与用户。

7) 存储证明：证明中心存储盲化身份证明 blind_certificate。

注册成功即中央控制器将相关私钥及身份摘要交与用户自行保存后，还需将身份摘要上传区块链；然后初始化认证密钥对并将其公钥通过智能合约上传到区块链中；接着通过算法生成用户身份证明将其交与用户及上传区块链；最后将身份证明通过进一步盲化之后存储到证明中心并将盲化因子告知用户。

3.2.2　连接流程

打开 APP 后，APP 首先会检查手机端的蓝牙是否开启，若没有开启，会提醒用户打开手机蓝牙。蓝牙设备一般分为两种角色，即主设备和从设备，在连接过程中，无人机控制器充当从设备的角色，向周围一定范围内进行广播，广播的数据主要包含无人机控制器自身的 MAC 地址。手机会充当主设备的角色，打开 APP 后手机端会自动扫描周围的无人机控制硬件广播，获取从设备广播的数据并进行解析。若扫描到授权设备，则手机端从其广播的数据中破解从机的 MAC 地址，上传给中央控制器后，中央控制器检索数据库，验证用户的手机号是否与该设备的 MAC 地址相对应。若对应，则证明用户拥有连接权限，此时主机就可向该从机发起连接，连接成功后，即可进行无人机验证流程。连接流程如图 3 所示。

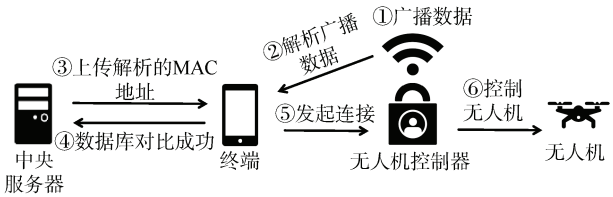


图 3　连接流程

Figure 3　Connection process

3.3　无人机安全监测轨道交通设备方案

在经过无人机身份认证和轨道交通的安全认证后，无人机才能开始执行对轨道交通各种设备的安全监测任务。无人机需配备高清摄像头、红外热成像仪、激光雷达、蓝牙模块和 GPS 定位系统。集成飞行控制系统、实时监测系统和数据处理模块，支持任务规划和自动飞行。通信方式采用低功耗蓝牙，实现无人机与中

央控制系统的数据传输。监测任务执行流程如下。

1) 任务规划：根据轨道分布和设备位置，制定无人机飞行任务，包括飞行路径、高度和监测区域。设置监测频率和特定巡检任务，例如高温区域的热成像检查。

2) 监测实施：无人机起飞后根据预定路径飞行，实时监控轨道设备并采集图像和数据，对重点设备(如轨道扣件、电气系统)进行细致检测，记录设备状态。

3) 数据传输：无人机将采集的数据通过蓝牙或蜂窝网络实时上传至中央系统。数据传输采用本文提出的加密方式，确保敏感信息安全。

4) 数据处理与分析：中央系统对数据进行实时处理，识别异常情况，如设备磨损、过热或电气故障，生成设备状态报告，并推送至运维团队。

无人机监测轨道设备流程如图 4 所示，利用无人机的设备监测结果对轨道交通系统进行状态分析，有效预防物理安全问题。



图 4 轨道交通设备监测流程

Figure 4 Rail transit equipment monitoring process

4 安全性与抗攻击性分析

4.1 威胁定义

本文允许恶意攻击者在无人机认证方案的任意阶段对信息传输进行攻击以达成篡改或破解的结果。对于安全威胁，定义身份认证和数据传输两种。

假设恶意攻击者具备较强的信息截获能力，允许其篡改消息以干扰正常的认证流程，但无法控制或破坏用户手机、无人机控制器以及无人机硬件设备，从而不会阻碍无人机认证过程的正常进行。

4.2 安全性

本文从 3 个方面对所提出认证方案的安全性能进行分析。

1) 认证过程安全。当涉及身份认证时，认证安全是至关重要的。本文所提出的身份认证方案基于离散对数难题，建立在用户拥有各自身份证明和私钥的基础上。在认证消息计算的过程中，双方的私钥都被用到，但由于离散对数难题的特性，攻击者无法获取这些私钥，因此攻击者也不可能伪造有效的认证消息。这种高度的认证安全性保证了该方案在实际应用中的可靠性。

2) 用户匿名。在相互认证的过程中，用户的真实身份和匿名身份都没有以明文的形式进行传送，攻击者无法获取得到这些信息，因此本方案可以保证用户的匿名性。

3) 不可跟踪性。在生成身份证明时，本文方案加入了随机数和时间戳，每个认证消息都互不相同，攻击者无法从这些消息中找到身份和认证信息之间的关系，因此无法跟踪用户行为。

4.3 抗攻击性

本文方案能够抵御以下攻击。

1) 中间人攻击。在身份认证的过程中，假设攻击者处于两个相互认证的用户之间，攻击者要想生成有效的身份证明，需要知道用户私钥。在缺少密钥的情况下，无法进行正确通信，因此可以抵御中间人攻击。

2) 伪装攻击。在进行身份认证时，用户必须使用其私钥进行认证，攻击者无法获取到这些私钥，也就无法通过认证。因此，本方案可以有效地防御伪装攻击。

3) 分布式拒绝服务攻击。由于用户之间经由双方共享会话密钥进行安全通信，所有以错误方式加密的信息都会被拒绝掉。

4) 重放攻击。本文方案中使用了时间戳，可以通过查验时间戳排除过期消息，免于重放攻击。

4.4 黑名单机制

本文方案采用的黑名单机制为：如某个移动智能终端未通过系统身份认证，即提交的 MAC 地址与自身手机号不匹配或是开锁码不正确，则断开连接，并将其加入系统通信黑名单，以此来防止其恶意占用蓝牙通信接口，导致其他用户无法正常使用系统蓝牙通信。加入系统通信黑名单的设备短时间内将不能与系统建立连接。此时系统恢复广播状态，重新向四周进行广播，等待与其他终端设备建立连接。

5 试验结果分析

本文首先实现了基于盲化 ECDSA 改进的高效匿名身份认证方案中的核心算法，主要包括密钥生成、身份证明生成及身份证明验证等步骤。

使用 Java 语言实现了无人机安全身份认证方案中

核心算法部分，实验运行环境为：Intel Core i5、内存 8GB 的笔记本电脑，macOS Monterey 操作系统、IntelliJ IDEA 平台。图 5 为本方案中算法的运行结果。

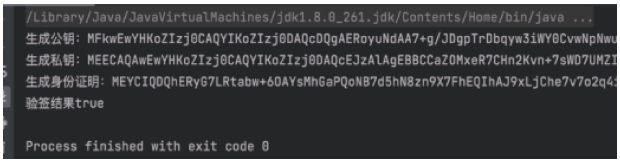


图 5　核心算法实现结果

Figure 5　Results of core algorithm implementation

针对本文所提的基于盲化 ECDSA 改进的高效匿名身份认证方案，分别从功能和效率两方面与其他方案进行比较和分析。

5.1　抗攻击性分析

本文方案基于盲化 ECDSA 改进身份认证，结合随机时间戳、用户唯一标识符和盲化签名，增强匿名性与安全性。用户身份证明盲化存储于证明中心，验证时先进行盲化匹配，减少区块链交互，降低通信成本。盲化签名确保即使证明中心泄露，攻击者也无法关联真实身份，从而抵御中间人攻击和伪装攻击。随机时间戳防止重放攻击，使历史数据无法复用。智能合约辅助验证可筛选合法请求，缓解 DDoS 攻击风险。整体方案通过去中心化存证、盲化处理和智能合约机制，实现高效、安全的身份认证。

5.2　效率分析

采用计算和通信开销两种常用指标来对比本文提出的匿名身份认证方案与其他认证方案。由于本文方案中用户注册的过程仅需要执行一次，该过程对于整个方案性能的影响几乎可以忽略不计，因此在后续的分析过程当中，主要针对匿名身份认证过程中的计算和通信开销。

图 6 对比了 ECC 和基于 NIST 标准的 ECDSA 在密钥生成、签名生成和签名验证阶段的运行时间。由图 6 可知，两者在密钥生成阶段的效率不同；在签名生成阶段，ECDSA 因采用安全哈希算法(secure hash algorithms，SHA)而表现更优；而在签名验证阶段稍慢，这是由于 ECDSA 签名一般由两个整数组成，使得其长度大约是曲线安全位数的两倍，导致签名验证阶段计算量有所增加。总体而言，ECDSA 在签名生成阶段的表现更加突出，综合性能较为优越。

图 7 展示了本文方案与可监管匿名认证方案及其预计算方案的计算效率对比。由图 7 可知，本文方案在用户密钥生成阶段耗时较长，原因是需初始化系统参数，但在生成证明密钥、身份证明、出示和验证阶段耗时更短，整体认证过程中运行时间最短。主要得益于 ECC 短密钥低成本特性及优化后的数据复用机制，整体效率更优。综合考虑计算和通信开销，本文的方案相比可监管匿名认证方案在认证效率方面提升了 43.8%。

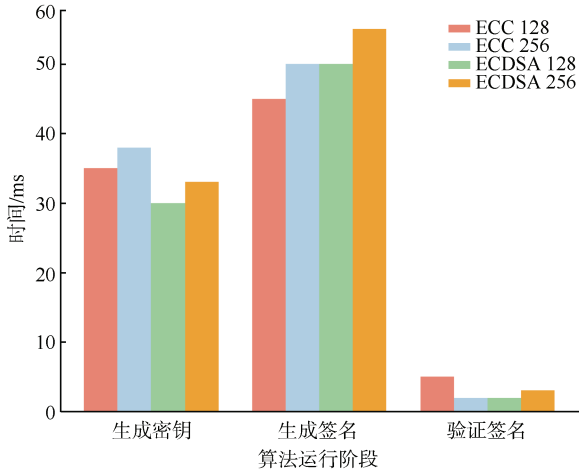


图 6　不同算法运行时间对比

Figure 6　Runtime comparison of different algorithms

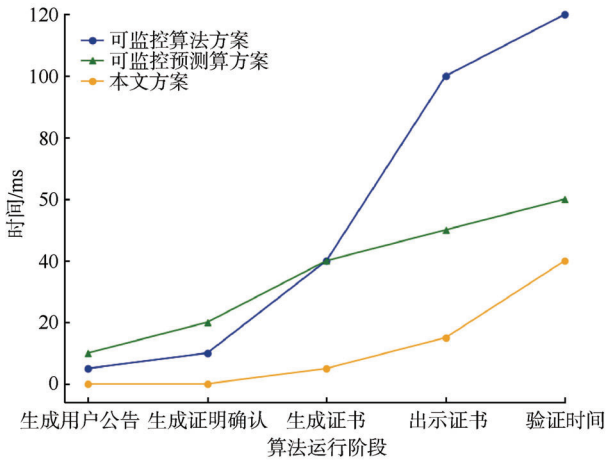


图 7　不同阶段的计算效率对比

Figure 7　Computational efficiency comparison across stages

综上，从抗攻击性和效率两方面的分析与对比验证了本文所提出的基于盲化 ECDSA 改进的匿名身份认证方案在实际应用中的可行性与有效性。该方案不仅有效抵御了常见的中间人攻击、伪装攻击、重放攻击以及 DDoS 攻击，同时还显著提高了整体计算效率和通信性能，表现出明显的综合优势。

6　结论

1) 提出一种基于超级 SIM 卡的无人机与轨道交通设备的认证方案，设计了利用超级 SIM 卡支持物理防

克隆模式，在运营商协助下完成用户注册的身份认证架构，保障了用户身份的安全性与唯一性。

2) 与传统的低功耗蓝牙系统采用 AES 算法的方案相比，本文提出的基于盲化 ECDSA 改进的高效匿名身份认证方案在认证效率方面提升了 43.8%。与基于 NIST 标准的 ECDSA 和传统 ECC 算法相比，本文方案在签名生成阶段表现更优，综合运行时间最短，本文在身份认证方案的安全性和效率方面做了研究，但只考虑了实验室环境下的计算和通信开销，与真实复杂环境可能存在一定误差。未来将进一步优化认证效率并在实际场景中评估方案的性能与可靠性。

参考文献

[1] 裘德馨. 低空经济中无人机产业发展概述[J]. 商业全球化, 2024, 12(3): 117-122.
QIU Dexin. Overview of UAV industry development in low-altitude economy[J]. Business and Globalization, 2024, 12(3): 117-122.

[2] 罗海风, 詹显军, 陈博. 轨道交通监测信息化管理系统研发与运用[J]. 铁路计算机应用, 2018, 27(3): 58-62.
LUO Haifeng, ZHAN Xianjun, CHEN Bo. Monitoring information management system for urban rail transit[J]. Railway computer application, 2018, 27(3): 58-62.

[3] 夏泳, 田洛. 面向低空经济的空联网络组网关键技术研究综述[J]. 重庆邮电大学学报(自然科学版), 2024, 36(4): 619-632.
XIA Yong, TIAN Luo. Survey of key networking technologies for air-space networks in low-altitude economy[J]. Journal of Chongqing University of Posts & Telecommunications (Natural Science Edition), 2024, 36(4): 619-632.

[4] 刘军, 袁霖, 冯志尚. 面向无人机群组的轻量动态密钥管理方案[J]. 计算机应用研究, 2023, 40(5): 1515-1521.
LIU Jun, YUAN Lin, FENG Zhishang. Lightweight dynamic key management scheme for UAV group[J]. Application research of computers, 2023, 40(5): 1515-1521.

[5] 何道敬, 杜晓, 乔银荣, 等. 无人机信息安全研究综述[J]. 计算机学报, 2019, 42(5): 1076-1094.
HE Daojing, DU Xiao, QIAO Yinrong, et al. A survey on cyber security of unmanned aerial vehicles[J]. Chinese journal of computers, 2019, 42(5): 1076-1094.

[6] 李蕊, 亢保元, 麦凯强. 面向智慧城市监控的无人机网络身份认证方案的分析与改进[J]. 计算机科学与应用, 2021, 11(9): 2387-2395.
LI Rui, KANG Baoyuan, MAI Kaiqiang. Analysis and improvement of UAV network identity authentication scheme for smart city monitoring[J]. Computer science and application, 2021, 11(9): 2387-2395.

[7] 李旻翰, 白浩, 蒋周良, 等. 基于超级 SIM 卡的网络安全访问控制解决方案[C]//2023 年网络安全优秀创新成果大赛论文集.武汉, 2023: 71-74.

[8] 贾博奇, 刘晓华, 许锋, 等. 基于低功耗蓝牙技术的智慧输液系统设计和应用[J]. 中国医疗设备, 2022, 37(2): 121-124.
JIA Boqi, LIU Xiaohua, XU Feng, et al. Design and application of the smart infusion monitoring based on the bluetooth of low energy[J]. China medical devices, 2022, 37(2): 121-124.

[9] 张瑞吟. 低功耗蓝牙技术市场应用前景广阔[J]. 集成电路应用, 2012(10): 32-33.

[10] 张鹏富. 浅谈蓝牙技术的发展现状和前景[J]. 计算机光盘软件与应用, 2014, 17(16): 36.

[11] 崔超, 赵云, 肖勇, 等. 一种高吞吐率低功耗的 AES-CCM 硬件实现[J]. 密码学报, 2021, 8(3): 365-375.
CUI Chao, ZHAO Yun, XIAO Yong, et al. A high-throughput and low-power hardware implementation of AES-CCM[J]. Journal of cryptologic research, 2021, 8(3): 365-375.

[12] 闫实. 蓝牙技术在现代化高校中的应用与实现[J]. 农业网络信息, 2011(5): 152-154.
YAN Shi. Application and achievement of bluetooth in modern medical colleges[J]. Agriculture network information, 2011(5): 152-154.

[13] 黄婉悦, 张席克, 黄毅, 等. 基于蓝牙技术的智能灯控制系统设计[J]. 黄河科技学院学报, 2019, 21(5): 62-64.
HUANG Wanyue, ZHANG Xike, HUANG Yi, et al. A design of intelligent lighting control system based on bluetooth technology[J]. Journal of Huanghe S&T College, 2019, 21(5): 62-64.

[14] 弓皓臣, 胡涛, 吴迪, 等. 基于轻量化区块链的无人机蜂群身份认证设计[J]. 指挥控制与仿真, 2024, 46(5): 29-36.
GONG Haochen, HU Tao, WU Di, et al. Design of UAV swarm identity authentication based on lightweight blockchain[J]. Command control & simulation, 2024, 46(5): 29-36.

[15] KIRSAL EVER Y. A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications[J]. Computer communications, 2020, 155: 143-149.

[16] LEI Y, ZENG L N, LI Y X, et al. A lightweight authentication protocol for UAV networks based on security and computational resource optimization[J]. IEEE access, 2021, 9: 53769-53785.

[17] JAN S U, ABBASI I A, ALGARNI F, et al. A verifiably secure ECC based authentication scheme for securing IoD using FANET[J]. IEEE access, 2022, 10: 95321-95343.

[18] 谢宇威, 朱设峰. 基于超级 SIM 卡技术的 NFC 校园卡应用探索[J]. 电脑知识与技术, 2023, 19(9): 98-100.

[19] 范建伟. 基于 SIM 卡的数字身份实现与应用[J]. 科学技术创新, 2022(35): 91-94.
FAN Jianwei. Design and implementation of the digital identity based on SIM card[J]. Scientific and technological innovation, 2022(35): 91-94.

[20] SAEPULROHMAN A, ISMANGIL A. Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA)[J]. International journal of electronics and communications systems, 2021, 1(1): 11-15.

[21] KIM M, CHO S, CHOI S, et al. A key recovery protocol for multiparty threshold ECDSA schemes[J]. IEEE access, 2022, 10: 133206-133218.

（编辑：王艳菊）