移动应用终端网络数据加密传输方法研究

王 斌[1] 郑渭渭[1]
WANG Bin ZHENG Weiwei

摘 要 为了提高移动应用终端网络数据传输的安全性与可靠性，优化其抵抗攻击的能力，开展了移动应用终端网络数据加密传输方法研究。首先，线性加密预处理移动应用终端网络数据，形成对数据的限制和加密；其次，计算移动应用终端网络数据加密核心节点的细粒度，布设加密节点；然后利用公钥密码体制，设计数据加密算法，对数据进行加密与解密处理；最后，在此基础上，设计数据传输程序，将加密处理完毕的数据安全传输给接收方，实现加密传输目标。实验结果表明，在加密传输数据量持续增加的情况下，提出方法的抵抗攻击能力始终较高，均达到了 98% 以上，能够有效抵抗各种攻击手段，保护数据的安全性和机密性。

关键词 移动应用终端；网络；数据；加密；传输

doi：10.3969/j.issn.1672-9528.2024.02.031

0 引言

随着移动设备的广泛普及和互联网技术的飞速发展，移动应用终端已经成为人们日常生活和工作中不可或缺的一部分。然而，与此同时，网络安全问题也变得日益严峻。如何保障移动应用终端网络数据的安全，防止数据泄露和非法获取，成为一个亟待解决的问题。移动应用终端网络数据传输面临的安全威胁主要来自以下几个方面。（1）网络攻击：黑客可以通过网络监听、截获、篡改等方式，获取移动应用终端的网络数据，造成用户信息的泄露和财产的损失[1]。（2）恶意软件：恶意软件可以感染移动应用终端，记录用户的输入信息、窃取用户的账号密码等敏感数据，或者通过发送垃圾信息、恶意扣费等方式侵犯用户的权益[2]。（3）内部人员泄露：由于内部人员的不当操作或者恶意行为，可能导致移动应用终端网络数据的泄露[3]。为了应对以上安全威胁，对移动应用终端网络数据进行加密传输显得尤为重要。

当前，传统的网络数据加密传输方法多数采用文献 [4] 提出的方法原理，该方法在实际移动应用终端网络应用中仍然存在不足。主要体现在安全性不足，该方法往往只针对单个因素或场景进行加密，难以全面保障数据的安全性，且加密后的数据传输速度变慢，效率降低，影响用户体验[4]。

为了改善传统网络数据加密传输方法存在的不足，更好地保护移动应用终端网络数据的安全性和用户隐私，本文提出了移动应用终端网络数据加密传输方法研究，为用户提供

1. 甘肃同兴智能科技发展有限责任公司 甘肃兰州 730050

[12] CHEN J R, KAO S H, HE H, et al. Run, don't walk: chasing higher flops for faster neural networks[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.Piscataway:IEEE, 2023: 12021-12031.

[13] WANG Q L, WU B G, ZHU P F, et al. ECA-Net: Efficient channel attention for deep convolutional neural networks[C]// Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. Piscataway:IEEE,2020:11534-11542.

【作者简介】

杨坚（1983—），通信作者（email: jianyang@yzu.edu.cn），男，江苏南京人，博士，讲师，研究方向：深度学习、智能制造技术。

秦宇（1996—），男，江苏扬州人，硕士，研究方向：深度学习、智能制造技术。

竺志大（1965—），男，江苏扬州人，本科，正高级工程师，研究方向：装备自动化、智能制造技术。

陈爱军（1996—），男，江苏常州人，硕士，研究方向：深度学习、智能制造技术。

（收稿日期：2023-11-28）

更加安全、可靠的网络服务。

1 移动应用终端网络数据的特性及其加密的意义

移动应用终端上包含用户的大量敏感信息，如个人隐私、金融交易和商业机密等，这些信息往往需要进行加密保护。移动应用终端网络数据具有时效性和实时性。用户对于移动应用的使用侧重于即时交互和信息获取，因此移动应用终端网络数据通常需要在瞬息之间传输和处理，这要求加密方法在不影响速度的情况下能够高效地进行加密和解密操作。移动应用终端网络数据面临着各种网络环境的挑战。用户在使用移动应用时可能处于不同的网络环境中，如 4G、5G、Wi-Fi 等，这些网络环境的不确定性会导致数据传输受到干扰甚至遭受恶意攻击，因此数据加密需要具备强大的适应性和抗干扰能力。移动应用终端网络数据具有跨平台传输的特点。由于移动应用终端存在多种操作系统和设备类型，数据在不同终端之间的传输也需要考虑到跨平台的兼容性和稳定性。移动应用终端网络数据涉及用户隐私和个人信息的保护。随着信息安全意识的增强，用户对于个人隐私的保护要求越来越高，因此移动应用终端网络数据的传输过程必须得到有效的加密保护，以防止用户隐私泄露和个人信息被窃取。

针对以上特性，数据加密在移动应用终端网络数据传输中具有重要的意义。加密可以保障数据传输的安全性和隐私性。通过加密算法对数据进行加密，即使在数据传输过程中被第三方恶意获取，也无法解读其中的内容，从而有效保护了用户的隐私和个人信息。加密可以确保数据传输的完整性。利用加密技术对数据进行加密签名，在数据传输过程中验证数据的完整性，防止数据在传输过程中被篡改或损坏。加密可以防范网络攻击和窃听风险。移动应用终端网络数据容易受到黑客攻击或窃听，通过加密对数据进行保护，可以最大程度上防止数据泄露和被窃取的风险。加密可以提升用户信任和应用安全。作为移动应用的基本功能之一，加密可以提高用户对应用的信任度，增强应用的安全性，从而提升用户体验和满意度。

2 移动应用终端网络数据加密传输方法

2.1 移动应用终端网络数据线性加密预处理

收集需要加密传输的网络数据，这些数据可能来自不同的移动设备和应用，需要进行分类和整理。对收集到的数据进行清洗，去除无关的数据和重复的数据，确保数据的准确性和完整性 [5]。对清洗后的数据进行标准化处理，即对数据进行归一化、去量纲、统一数据格式等操作，使得数据具有更好的可读性和可操作性 [6]。在此基础上，为了提升移动应用终端网络数据整体的加密安全性，对上述处理完毕的网络数据进行线性加密预处理。首先，根据移动应用终端网络数据类型与应用区域，将数据划分为不同的加密层级，生成对应层级的文字编码，对其进行序列重组处理，形成灰度混淆帧结构 [7]。然后将该结构作为线性加密的标准，调整编码生成序列与对应的编码长度，基于不确定的网络环境，形成对终端网络数据的限制和加密，完成加密预处理。

2.2 布设加密节点

移动应用终端网络数据线性加密预处理完毕后，根据终端网络数据的特征结构，布设加密节点。首先需要确定需要布设的加密节点数量，加密节点数量需要根据网络规模、数据传输量、安全性要求等因素进行综合考虑 [8]，在确定加密节点数量后，需要选择合适的位置进行布设，一般来说，加密节点需要放置在网络的关键位置，如网络中心、数据中心、服务器等，以便对整个网络进行监控和保护 [9]。其次，计算移动应用终端网络数据加密核心节点的细粒度，计算公式为：

$$Q=\frac{r+1}{2}-(t+1.5) \tag{1}$$

式中：r 表示网络数据加密核心节点重组距离；t 表示网络数据传输过程中应变加密极限值。通过计算，得出移动应用终端网络数据加密核心节点的细粒度，将细粒度设定在数据内部的加密结构中，进而设定加密目标，在核心加密节点周围布设辅助节点，形成移动应用终端网络数据加密覆盖范围。在该范围内，通过控制节点细粒度，调整动态加密目标，完成网络数据加密基础性布设。

2.3 移动应用终端网络数据非对称加密算法设计

加密节点布设完毕后，设计加密算法，对移动应用终端网络数据进行加密处理。综合考虑加密算法的性能后，本文选用公钥密码体制，即非对称加密算法。该算法使用两种不同的密钥，其中一个作为公钥公开使用，另一个作为私钥自己拥有。需要注意的是，两个密钥之一必须是保密的。根据具体的应用场景和安全性要求，设计加密流程。通常包括数据明文的输入、公钥加密、输出密文等步骤。公钥加密原理示意图，如图 1 所示。

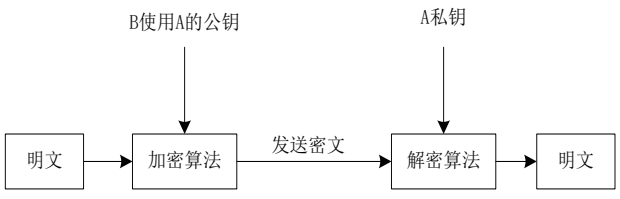

图 1 公钥加密原理示意图

图 1 中，B 向 A 发送移动应用终端网络数据，B 和 A 分

别产生各自的一对密钥，将自己其中一个密钥存放在公开寄存设备中，另一个密钥由自己私下保存[10]。具体的加密流程为：消息源 B 产生明文消息，用公式表示为：

$$X=\{X_1,X_2,...,X_M\} \tag{2}$$

式中：M 表示明文消息元素个数。A 产生公钥 PU_b 和私钥 PR_b，私钥 PR_b 只有 B 知道，B 用 A 的公钥对待发送的网络数据进行加密处理，生成密文：

$$Y=\{Y_1,Y_2,...,Y_M\}=E(PU_b,X) \tag{3}$$

将密文发送给 A，A 在接收到消息后，用自己的私钥对接收到的数据信息进行逆变换解密处理。

$$X=D(PR_b,Y) \tag{4}$$

其他接收者由于没有 A 的私钥，因此即便接收到 B 发送的消息，也无法对数据进行解密。

2.4 数据传输程序设计

移动应用终端网络数据非对称加密算法设计完毕后，在此基础上，设计数据传输程序，将上述加密处理完毕的数据安全传输给接收方。数据加密传输程序设计流程如下文所示。

（1）确定传输协议：选择适合的传输协议，如 TCP/IP、UDP、HTTP 等。根据具体需求，确定是采用可靠的连接还是无连接的传输方式。

（2）设计数据封装格式：本文采用 JSON 数据封装格式，封装数据，以便于数据的传输和解析。

（3）建立连接：在发送端和接收端建立网络连接。根据所选择的传输协议，建立相应的连接方式。

（4）发送数据：在连接建立完成后，发送端使用数字信封，将加密后的数据发送给接收端。

（5）接收端接收到数据后，进行解封装操作，获取到原始数据。

（6）验证数据完整性：接收端使用校验盒，对数据进行完整性验证，以确保数据的完整性和一致性。

（7）测试和验证：对设计的程序进行测试和验证，以确保其正确性和安全性。测试包括模拟各种场景下的数据传输，以验证程序的可靠性和性能。

使用均方误差作为数据加密过后传输的结果与初始数据输入结果的差异程度的度量指标，计算公式为：

$$MSE\left(X,\hat{X}\right)=\frac{1}{n}\sum_{i=1}^{n}\left(\hat{x}^i-x^i\right)^2 \tag{5}$$

式中：X 表示初始数据输入结果；$\hat{X}$ 表示数据加密过后传输的结果；n 表示数据的类型数量；$\hat{x}^i$ 表示第 i 个加密后的数据传输结果；x^i 表示第 i 个初始数据输入结果。

当公式 5 获得的结果比设定的指标数值大时，可以判定加密数据的传输出现过多的误差，数据传输失效；反之，当 MSE 小于或等于设定的指标数值时，则认定加密数据的加密过程和传输过程具有完整性和一致性，数据的传输是正确并安全的，具有有效性。

在此基础上，将上述设计的程序部署到实际运行环境中，并进行长期运行和维护。根据实际运行情况，及时处理异常情况并进行必要的更新和优化。

3 实验分析

3.1 实验准备

综上所述，本文提出的移动应用终端网络数据加密传输方法的全部设计流程，在该方法投入实际应用前，进行了如下文所示的实验。通过实验验证所设计的加密算法和协议是否能够有效地保护移动应用终端网络数据的安全性和隐私性，进而验证其在实际应用中的可行性。为了全面评估移动应用终端网络数据加密传输方法的性能和安全性，本文设计了一个包含多种数据类型和场景的实验数据集。实验数据集类型如表 1 所示。

表 1 实验数据集类型

序号	数据类型	具体说明
（1）	HTTP 请求和响应	包含不同类型和格式的 HTTP 请求和响应数据，如 GET、POST 请求，以及 JSON、XML 和 HTML 响应。
（2）	图片	选取不同大小和格式的图片数据，如 JPEG、PNG 和 GIF 等。
（3）	视频和音频	选取不同格式和分辨率的视频和音频数据，如 MP4、AVI 和 MP3 等。
（4）	用户隐私数据	包含姓名、邮箱地址、手机号码等用户个人信息。

如表 1 所示，为此次实验选用数据集中数据的具体类型。首先根据特定场景和需求生成模拟数据，用于测试加密算法和协议在异常情况下的表现。然后，利用 MATLAB 模拟软件，模拟实验中的安全威胁场景，包括三个场景，如下文所示。

（1）恶意软件攻击：模拟恶意软件对移动应用终端的攻击，包括截获、篡改和重放网络数据等操作。

（2）黑客攻击：模拟黑客对移动应用终端的网络攻击，如中间人攻击、SQL 注入等。

（3）竞争条件攻击：模拟多个用户同时访问同一资源的情况，测试加密算法和协议在竞争条件下的表现。

在此基础上，搭建不同网络环境和网络条件，包括 Wi-Fi、4G、5G 等，应用上述本文提出的移动应用终端网络数据加密传输方法，评估加密算法在实际应用中的表现。

3.2 结果分析

选取移动应用终端网络数据加密传输过程中抵抗攻击能力作为性能评价指标，能够有效地评估加密算法面对各种攻

击手段时的抵抗能力。抵抗攻击能力计算公式为：

$$R=\left(P_a / P\right)\times 100\% \quad (5)$$

式中：P_a 表示成功破解的攻击次数；P 表示总攻击次数。抵抗攻击能力越强，说明加密算法越能有效地保护数据安全，反之同理。为了使实验测试结果更加清晰直观，采用对比实验的方法原理，将上述本文提出的移动应用终端网络数据加密传输方法设置为实验组，将文献 [3]、文献 [4] 提出的方法分别设置为对照组 1 与对照组 2，对比三种方法应用后，移动应用终端网络数据加密传输的抵抗攻击能力。设定移动应用终端网络数据量分别为 200 GB、400 GB、600 GB、800 GB、1000 GB、1200 GB，在数据量增加的情况下，测定加密传输抵抗攻击能力，并作出对比，结果如图 2 所示。

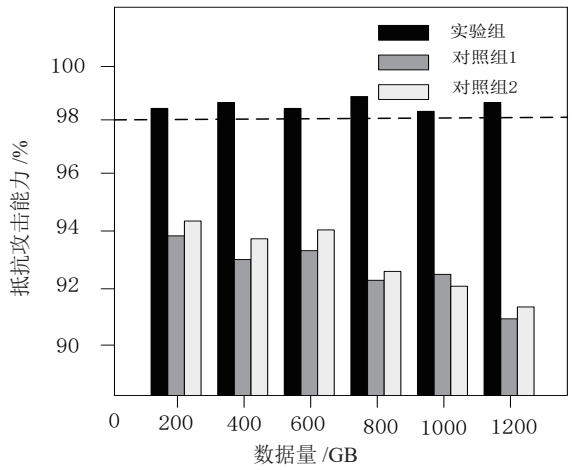

图 2 网络数据加密传输抵抗攻击能力对比结果

通过图 2 的对比结果可知，本文提出的移动应用终端网络数据加密传输方法应用后，在加密传输数据量持续增加的情况下，抵抗攻击能力始终高于另外两个对照组，均达到了 98% 以上。抵抗攻击能力高，说明加密方法能够有效地抵抗各种攻击手段，可以保护数据的安全性和机密性。同时，抵抗攻击能力越高，数据传输过程中遭受攻击和篡改的可能性就越小，从而能够提高数据传输的可靠性和完整性。

4 结语

为了提高移动应用终端网络数据传输过程中的安全性与可靠性，本文提出了一种新型的加密传输方法，以提高移动应用终端网络数据的安全性和隐私保护。一方面，通过加密技术，可以将原始数据转化为不易被他人理解的密文，只有持有正确密钥的人才能解密并获取原始数据。这样使得数据在传输过程中不会被窃取或篡改。即使数据被截获，也无法被恶意利用，从而保障了用户信息的安全，为用户提供更加安全、可靠的网络服务。另一方面，不同的移动设备和操作系统可能采用不同的网络协议和数据格式，而本文提出的加密传输方法可以适应不同的协议和格式，使得数据可以在不同设备之间进行传输和交换，兼容性、适应性和灵活性较强。总之，移动应用终端网络数据加密传输方法具有高安全性、完整性保障，对于保护用户的数据安全和隐私、提高数据传输可信度具有重要的作用。

参考文献：

[1] 田如意，顾风军，彭坤，等．基于一维 Logistic 映射和二维 Tent 映射双混沌思路的网络信息加密 [J]. 计算机测量与控制，2023, 31 (6): 280-286.

[2] 邓欣，杨波，于超，等．基于 DES 算法的海上油气生产设备数据海陆加密传输方法的研究 [J]. 自动化应用，2023, 64 (11): 45-47.

[3] 蒋鸣东．安全约束下嵌入式终端数据分层传输同步加密算法 [J]. 湖北理工学院学报，2023, 39 (2): 25-29.

[4] 奠石镁，何蓉．“互联网 +”环境下局域通信网络数据安全传输方法 [J]. 中国新通信，2023, 25 (3): 16-18.

[5] 秦武韬，王鹏，李玉峰．基于周期耦合处理的 CAN 总线数据组合加密方法 [J]. 通信学报，2023, 44 (1): 29-38.

[6] 仝军，田洪生，吴翠红．考虑节点能量特征的无线传感数据加密传输方法 [J]. 传感技术学报，2022, 35 (9): 1277-1281.

[7] 杨娜．基于分组密码算法的网络传输数据信息加密方法研究 [J]. 信息与电脑 (理论版), 2022, 34 (17): 210-212.

[8] 陈明亮，李鑫，谢国强．基于嵌入式技术的电力监控网络数据安全传输方法 [J]. 单片机与嵌入式系统应用，2022, 22 (6): 33-37.

[9] 杨帅航，何进荣．数据加密技术在计算机网络数据安全中的应用 [J]. 延安大学学报（自然科学版），2021, 40 (1): 78-82.

[10] 王鹏，王福新，李来杰，等．基于电力行业的智能移动应用网络安全技术综述 [J]. 通信电源技术，2021, 38 (2): 127-130.

【作者简介】

王斌（1995—），男，甘肃武威人，本科，工程师，研究方向：数字化应用。

郑渭渭（1991—），男，甘肃兰州人，本科，工程师，研究方向：数字化应用。

（收稿日期：2023-12-07）