 DOI: https://doi.org/10.12349/iser.v6i3.5195

Discussion on information security encryption technology in wireless network

Jianwei lv

Shanghai Maoyuan Shengyou Information Technology Co., Ltd., Shanghai, 200002, China

Abstract

With the rapid development of wireless communication technology, wireless network has become an important carrier of modern information transmission. However, the open transmission environment makes it face many security threats such as data theft, middleman attack and illegal intrusion. In this context, information security encryption technology, as the core means to ensure the confidentiality, integrity and attack resistance of wireless network data, has attracted wide attention. The applicability of traditional encryption technology in the wireless network environment is restricted by computing resources, energy consumption, communication delay and other factors, and the rise of emerging security technologies such as quantum computing and zero-trust architecture also poses new challenges to the wireless network security system. Therefore, this paper discusses the main encryption technology in the wireless network, and analyzes its challenges in ensuring information security, and proposes its optimization countermeasures for reference.

Keywords

wireless network; information security encryption technology; challenges; countermeasures

无线网络中信息安全加密技术的探讨

吕建伟

上海茂源盛悠信息技术有限公司，中国 · 上海 200002

摘　要

随着无线通信技术的快速发展，无线网络已成为现代信息传输的重要载体。然而，开放性的传输环境使其面临数据窃取、中间人攻击、非法入侵等诸多安全威胁。在此背景下，信息安全加密技术作为保障无线网络数据机密性、完整性及抗攻击能力的核心手段，受到广泛关注。传统加密技术在无线网络环境下的适用性受到计算资源、能耗、通信延迟等因素的制约，而量子计算、零信任架构等新兴安全技术的兴起，也对无线网络安全体系提出了新的挑战。因此，本文探讨无线网络中的主要加密技术，并分析其在保障信息安全方面的挑战，并提出其优化对策，以供参考。

关键词

无线网络；信息安全加密技术；挑战；对策

1 引言

随着无线通信技术的飞速发展，无线网络已广泛应用于个人、企业及政府机构。然而，由于无线信号的开放性和传播特性，无线网络面临着窃听、中间人攻击、数据篡改等安全威胁。为了保障数据的机密性、完整性和可用性，加密技术在无线网络安全防护中发挥着关键作用。

2 无线网络中的主要加密技术

2.1 对称加密技术

对称加密是密码学机制，利用单一 Key 进行加解密操作。在无线网络环境中，由于具有较高的计算效率和较快的资料处理速度，对称加密算法在安全通讯协议和资料加密存储中得到了广泛的应用。这项技术的重点是使用相同密钥来进行加密与解密，所以安全管理与分发对称加密算法是一项重要步骤 [1]。在无线通信领域，常用的对称加密算法有国际数据加密算法 (IDEA)，高级加密标准 (AES, DES)。其中，AES 是目前主流的对称加密方案，支持 128 位、192 位和 256 位密钥的长度，采用分组加密模式，通过多轮替换、扩展和混淆操作，提高数据安全性。

2.2 非对称加密技术

非对称加密基于公钥密码体系，通过不同密钥分别执行加密与解密操作。该体系由公钥和私钥构成，其中公钥用于数据加密，私钥用于解密，确保密钥分离特性，提高密钥管理的安全性。在无线通信系统中，非对称加密广泛应用于身份认证、密钥交换及数字签名等安全机制。无线网络环境下，常见的非对称加密算法包括 RSA、ECC 及 DSA。RSA

【作者简介】吕建伟（1986–），男，中国甘肃人，本科，工程师，从事系统集成、信息安全与网络架构研究。

基于大整数分解问题，采用 1024 位、2048 位及更长密钥进行加密运算，安全性随密钥长度增加而提高。ECC 基于椭圆曲线离散对数问题，在较短密钥长度（如 256 位）下提供与 RSA 2048 位相当的安全性，适用于低计算资源的无线设备。DSA 采用离散对数问题构建数字签名体系，结合 SHA 实现数据完整性校验 [2]。

2.3 哈希算法与完整性保护

无线网络环境下的数据传输易受中间人攻击、篡改等安全威胁，为保证数据完整性，通常采用哈希算法进行校验。哈希函数将任意长度的输入映射为固定长度的散列值，该散列值具备不可逆性和雪崩效应，即微小变动的输入将导致哈希值发生较大变化。无线网络协议中，哈希算法主要用于生成消息摘要，确保数据未被恶意篡改。

常见哈希算法有 MD5，SHA 系列等。MD5 算法采用了多轮迭代压缩输入数据并最终输出 128 位哈希值的分块处理方式。但它的抗碰撞性较弱，碰撞漏洞被广泛证明是存在的。SHA 系列算法包括 SHA-1、SHA-256、SHA-512 等，其中 SHA-1 产生了比 MD5 抗碰撞性更强的 160 位哈希值，但仍存在安全隐患。SHA-256 和 SHA-512 采用了更复杂的位运算和提供更高强度完整性保护的逻辑运算，在无线通信安全领域得到了广泛的应用。

3 无线网络中信息安全加密技术面临的挑战

3.1 计算资源受限与能耗问题

无线网络中的信息安全需求随着信息通信技术的不断发展而逐步提高。但在计算资源受限和能源消耗问题上，信息加密技术的应用面临双重挑战。计算能力和存储能力在许多网络设备中受到严格限制，尤其是边缘设备和物联网终端，导致在执行过程中可能出现加密算法性能瓶颈。如 AES、RSA 等高强度加密算法，

其对于计算资源需求量较大，尤其是数据量大的时候，计算负担愈加明显，以致于网络通信效率下降。此外，移动装置和电池驱动装置中，能耗问题也格外凸显。很多加密技术在加密、解密过程中，为了确保信息安全，需要消耗较高的电能，不仅对设备的使用时间造成影响，而且还可能导致设备出现过热等问题，这对系统的稳定性、安全性都会产生影响。特别是在 5G 等高带宽网络环境下，大规模的数据传输对计算更为复杂的加密强度要求更高，这就使得如何在优化能耗的同时保证数据的安全性，成为当前迫切需要解决的问题。

3.2 量子计算威胁

快速发展的量子计算使传统加密技术面临空前挑战。基于量子力学原理，量子计算采用量子比特 (QuantumBit) 进行计算，其并行处理能力远远超过经典电脑。在此背景下，由于对大数分解和离散对数问题的依赖，许多现有的基于公钥密码学的加密算法，如 RSA 和 ECC，都极有可能在短时间内被量子计算机破解。具体地说，量子算法中的 Shor 算法可以在多项式时间内对这些加密算法进行高效破解，也就是说，即使是强度更高的加密方式，在量子计算的攻击中也无法抵挡。

在量子计算威胁的环境下，传统的对称加密算法，如 AES，虽然在理论上不易被量子计算直接破解，但量子计算能够通过 Grover 算法将其安全性降低至平方根级别，这使得原本需要 256 位密钥的 AES 算法，其实际安全性相当于经典计算中的 128 位密钥。这种安全性的大幅下降，使得量子计算对现有加密系统的威胁进一步加剧。

3.3 端到端加密与零信任架构

作为保证资料保密的核心技术，端到端加密要求资料必须加密在发送端，且只在接收端解密，以免在传输过程中被第三方截取或篡改数据。但在密钥管理、计算开销和系统兼容等方面，广泛部署端到端加密面临着不小的挑战。首先，密钥分配机制的安全性直接影响到数据的保护效果，特别是在分布式环境下，密钥同步与更新的复杂度明显提高。另外，高强度的端到端加密算法会占用更多的计算资源，导致运行效率受到影响，从而导致低功耗设备的操作负担增加。

零信任架构强调默认不信任任何网络实体，需要严格的身份验证和访问控制，即使是用户和内部网络的设备也不信任任何网络实体。该架构依赖于减少攻击面暴露的动态授权、多因子认证和细粒度访问权限管理。但实施零信任依赖于对计算资源、存储能力和数据流量处理能力提出更高要求。同时，身份识别管理策略在不同业务场景下复杂多变，为满足安全需求变化，要求能够实时调整动态访问控制机制，运维管理难度加大。

4 无线网络中信息安全加密技术的发展策略

4.1 优化计算资源利用与降低加密能耗策略

在无线网络环境下，计算资源受限与能耗问题对信息安全加密技术的实施形成制约。为应对这一问题，可采用多种优化策略，包括算法简化、计算架构调整、硬件加速与动态资源管理等方法，以提高运算效率并降低能耗。

首先，在算法层面，为了减少计算复杂度，选择了轻量级的加密算法，适用于低功耗环境。如嵌入式设备中流口令 ChaCha20 和块口令 Present 的适配性较高，在降低存储资源占用的同时，能有效减少计算量。并且采取对密钥调度机制与子密钥生成方式进行优化的方式来实现设计路径的改良，减少计算冗余，实现数据加密效率的提升 [3]。其次，在计算架构上，引入边缘计算技术，向边缘节点分散一些密集的计算任务，减少终端设备的运算压力。同时采用分层加密策略，将对称加密与 Hash 校验结合起来，在数据传输过程中实现最优化的计算任务分配，增强系统整体反应能力。再者，依靠硬体加速能力，在确保资料安全的前提下，可借由安全晶片 (如 TPM)、可信执行环境 (TEE) 或专用加密协

处理器来降低中央处理单元的运算负担。此外，针对特定加密算法的执行效率提升，并进一步降低功耗，采用可重构计算架构，结合 FPGA 或 ASIC 加速模块。

4.2 构建抗量子加密体系与增强安全防护机制

构建抗量子加密系统成为信息安全防护在量子计算技术发展背景下的关键举措。一是要采用格密码、多变量公钥密码等基于数学难题的抗量子密码技术。格密码主要是凭借高维格问题的计算复杂性，能够形成强大的抗量子能力。基于纠错码理论的码码密码，其解码复杂度足以抵御量子计算攻击。其次，在对称式加密等级中，为了加强安全性，密钥长度应该有所提高。对称性加密算法如 AES 受 Grover 算法影响后安全性下降，因此为了抵消量子计算的运算能力提升，应优先考虑 512 位或以上的密钥长度。此外，可以合理应用变密钥加密机制，在传送数据时对密钥进行动态调整，以增强其抵抗功能的能力。再者，在哈希算法方面，为了减少量子搜索算法的影响，可以应用哈希族中的 SHA-3 等具有极高安全系数的算法，且将输出长度延长，提高其对量子计算的，减少量子搜索算法的影响。同时将基于哈希链的认证协议组合起来，数据完整的保护能力就可以得到增强，而且量子计算所要造成的篡改风险也会随之降低。最后，在网络安全架构层次上，可使用量子密钥分发（QKD）技术，根据量子态的特征来形成无法破解的密钥，让整体通信链路安全系数得以提高。同时，结合后量子密码学与传统密码技术，构建混合加密体系，在量子计算尚未成熟前，保障数据传输的长期安全性。

4.3 优化端到端加密机制与强化零信任安全体系

优化密钥管理体系是改善端到端加密可行性的重要措施。可采用基于公钥基础设施（PKI）的自动化密钥分发机制，结合密钥轮换与分片存储策略，以达到降低密钥外泄危险性的目的。为了降低计算负担，提高执行效率，低功耗设备中，可以采用椭圆曲线密码学（ECC）和哈希链技术之类的轻量级的加密算法。而且为了在计算过程中保证数据上的隐私性，为了避免加解密操作而暴露敏感的信息，应采用同态加密和安全多方计算。

通过建设起人工智能的动态信任评估体系来有效应对零信任架构的实施挑战。将用户行为分析（UBA）与威胁检测技术相融合，对访问权限进行动态调整，增强系统适应性。此外还可采取结合基于属性的访问控制（ABAC）与基于策略的访问控制（PBAC）的方式来将细粒度权限管理强度加大，将讲台策略维护成本费用降低。在计算和存储资源优化方面，要实现去中心化身份认证，应用分布式身份管理（DID）体系，避免身份管理的集中化而产生的单点故障几率。同时，结合安全访问服务边缘（SASE）架构，将零信任策略扩展至云环境，提高跨设备、跨网络环境的适应性，增强数据安全防护能力。

5 结语

无线网络的信息安全加密技术在保障通信数据安全方面发挥着至关重要的作用。面对计算资源受限、能耗管理难题及量子计算威胁等挑战，传统加密算法需结合轻量级加密、后量子密码学与零信任架构等创新技术进行优化。未来，随着人工智能、区块链及安全多方计算等技术的深度融合，无线网络的加密体系将在安全性与性能之间寻求平衡，以满足高速、低延迟、多终端接入的需求。通过不断优化加密机制与安全架构，可有效提升无线网络环境下的数据安全保障能力，推动信息通信技术的健康发展。

参考文献

[1] 袁国朝.数据加密技术在计算机网络信息安全中的应用分析[J].大众科学, 2024, 45(1):1-3.

[2] 霍兰兰.计算机网络信息安全及加密技术研究[J].计算机应用文摘, 2023, 39(8):105-107.

[3] 吴玉洁.数据加密技术在计算机网络通信工程中的应用[J].计算机与自主智能研究进展, 2023, 1(1):10-12.