 DOI: https://doi.org/10.12349/iser.v5i11.3612

Application and Optimization of Encryption Technology in Network Data Transmission

Lin Wang

Guizhou West Electric Power Co., Ltd. Qianbei Power Plant, Bijie, Guizhou, 551800, China

Abstract

With the popularization of the Internet and the continuous development of communication technology, the security problem of network data transmission has become increasingly prominent. This paper first introduces the classification and basic principles of encryption technology, and then discusses the application of encryption technology in network data transmission, including chain encryption, end-to-end encryption, node encryption and common encryption algorithms such as AES, RSA, etc. Finally, this paper proposes optimization strategies for encryption technology in network data transmission, including selecting appropriate encryption algorithms, using security protocols, strengthening key management, and real-time monitoring and response. Through these measures, the security of network data transmission can be effectively improved, and user privacy and data integrity are protected.

Keywords

encryption technology; network data transmission; data security

加密技术在网络数据传输中的应用与优化

王林

贵州西电电力股份有限公司黔北发电厂，中国 · 贵州 毕节 551800

摘　要

随着互联网的普及和通信技术的不断发展，网络数据传输的安全性问题日益凸显。论文首先介绍了加密技术的分类与基本原理，然后详细探讨了加密技术在网络数据传输中的应用，包括链条加密、端对端加密、节点加密以及常见的加密算法，如AES、RSA等。最后，论文提出了加密技术在网络数据传输中的优化策略，包括选择合适的加密算法、使用安全协议、加强密钥管理以及实时监控和响应等。通过这些措施，可以有效地提高网络数据传输的安全性，保护用户的隐私和数据完整。

关键词

加密技术；网络数据传输；数据安全

1 加密技术的分类与原理

1.1 对称加密

对称加密是一种采用相同密钥进行加密和解密的加密方式，其显著特点是加密速度快、效率高。然而，这种加密方式在密钥的分发和管理上存在一定的挑战。在常见的对称加密算法中，DES（Data Encryption Standard）是一种历史悠久的算法，它使用 56 位密钥对 64 位的数据块进行加密，尽管已被证明存在安全漏洞，但在某些特定情境下仍具有一定的应用价值。相比之下，AES（Advanced Encryption Standard）作为当前广泛使用的对称加密算法，提供了 128 位、192 位和 256 位三种密钥长度，以其卓越的安全性和加密效率，成为保护敏感数据的首选方案，广泛应用于各种需要确保数据安全性的场景中。

1.2 非对称加密

非对称加密是一种采用不同密钥进行加密和解密的加密方式，分为公钥和私钥。公钥可以公开发布，用于加密数据；而私钥则需妥善保管，用于解密数据。这种加密方式的安全性较高，但加密速度相对较慢。在常见的非对称加密算法中，RSA（Rivest-Shamir-Adleman）算法基于大数分解的困难性，使用一对密钥进行加密和解密，目前尚未找到有效的破解方法，因此具有较高的安全性。而 ECC（Elliptic Curve Cryptography）算法则基于椭圆曲线数学，相比 RSA 算法，在相同的安全性下可以使用更短的密钥长度，从而提高了加密和解密的速度，特别适用于物联网等需要低功耗、高效率加密的场景，具有广泛的应用前景。

1.3 不可逆加密

不可逆加密是一种无需密钥、直接将明文通过加密算法转换为无法解密的密文的加密方式。MD5 和 SHA 是两种常见的不可逆加密算法。MD5 算法广泛被应用，能将任意

【作者简介】王林（1977–），男，彝族，中国贵州贵阳人，本科，工程师，从事网络安全、数字化转型、智慧化建设研究。

长度的数据映射为 128 位的哈希值，尽管存在碰撞攻击等安全漏洞，但在特定场合下仍有一定价值。而 SHA 算法由美国国家安全局设计，包括 SHA-1 及 SHA-2（含 SHA-224、SHA-256、SHA-384、SHA-512）等多个版本，提供了更高的安全性和更长的哈希值，适用于保护数据完整性的各种场景，确保了数据在传输或存储过程中的不可篡改性。

2 加密技术在网络数据传输中的应用

2.1 链条加密

链条加密是一种先进的加密技术，它在信息传输过程中确保了数据的安全性。具体而言，在信息被传送之前，首先会对其进行严格的加密处理。随后，在数据经过链路的各个节点时，每个节点都会对接收到的数据进行解密操作。但这一过程并非仅仅为了读取数据，而是为了对数据进行进一步的处理或验证。完成必要的处理后，节点会利用下一个链条的密钥对消息进行充分的加密，然后再将其继续传送出去。这样的加密和解密过程在链路的每个节点都会重复进行，形成了一个紧密的加密链条 [1]。链条加密的主要作用是掩盖信息的传输源点和终点，从而有效地防止通信信息被恶意分析或窃取。通过不断地变换密钥和加密方式，链条加密能够确保数据在传输过程中的完整性和机密性，为信息的安全传输提供了有力的保障 [2]。因此，在需要高安全性数据传输的场景中，链条加密技术得到了广泛的应用。

2.2 端对端加密

端对端加密是一种先进的数据加密技术，其核心原理在于确保数据在发送端被加密后，仅在接收端才能被解密，从而有效地防止数据在传输过程中的任何环节被非法窃取或恶意篡改。这种加密方式极大地提升了数据传输的安全性。端对端加密的实现离不开加密算法和安全协议的有力支持 [3]。通过采用复杂的加密算法，数据在发送前被转化为难以解读的密文形式，只有在接收端利用相应的密钥和解密算法才能还原为原始明文。这一过程中，即使数据在传输途中被截获，也无法被轻易解读。此外，安全协议如 HTTPS 中的 SSL/TLS 加密技术，为端对端加密提供了坚实的保障。在 HTTPS 协议下，数据在客户端与服务器之间传输时，会经过 SSL/TLS 加密技术的处理，确保通信的双方能够安全地交换信息，防止数据泄露和篡改的风险 [4]。因此，端对端加密技术在保障互联网通信安全方面发挥着至关重要的作用。

2.3 节点加密

节点加密是一种在数据传输过程中保障数据安全的重要技术。它采用密文形式进行数据传送，确保所有传输的数据都经过加密处理，这一过程对用户而言是明确且可知的。与链路加密相比，节点加密在网络节点的处理方式有所不同。具体来说，当数据到达网络节点时，并不会直接进行加密操作 [5]。相反，节点会首先对接收到的数据进行解密处理，以便在节点内部进行必要的操作或验证。完成这些操作后，节点会使用另一个不同的密钥对数据进行再次加密，以确保数据在后续传输过程中的安全性。这一过程需要在节点之上的安全模块中进行实践操作，以确保加密和解密操作的准确性和安全性。通过这种方式，节点加密能够有效地防止数据在传输过程中被非法窃取或篡改，为数据传输提供了更加可靠的保障 [6]。因此，在需要高安全性数据传输的场景中，节点加密技术得到了广泛的应用和认可。

2.4 使用安全协议和加密算法

在网络数据传输领域，确保数据安全至关重要，而使用安全协议和加密算法正是实现这一目标的关键手段。常见的安全协议如 SSL/TLS 和 IPSec，以及加密算法如 AES 和 RSA，共同构成了数据传输的安全基石。SSL/TLS 协议，作为网络通信中的保密性和数据完整性保障，广泛应用于 HTTPS、FTPS 等场景。它们通过加密数据传输通道，确保数据在传输过程中不被窃取或篡改，从而维护了数据的机密性和完整性。而 IPSec 协议则是一组专为 IP 数据包提供安全性的协议，它在 IP 层提供认证、完整性和加密服务，有效防止了数据在网络通信中受到未经授权的访问和篡改。

3 加密技术在网络数据传输中的优化

3.1 选择合适的加密算法

在选择加密算法时，我们需细致考虑应用场景及实际需求。对于涉及敏感数据传输的场合，对称加密算法无疑是理想之选，其中 AES（高级加密标准）凭借其卓越的加密效率和坚实的安全性，成为众多领域中的佼佼者。AES 算法不仅能够快速处理大量数据，同时提供了 128 位、192 位及 256 位等多种密钥长度，以满足不同安全级别的需求，确保数据在传输过程中的机密性。然而，在需要确保数据完整性及来源可信性的场景下，非对称加密算法则展现出了其独特的优势。RSA（Rivest-Shamir-Adleman 算法）作为非对称加密领域的经典之作，通过公钥与私钥的巧妙配合，既实现了数据的加密传输，又确保了数据的完整性和发送者的身份认证 [7]。此外，数字签名技术也是保护数据完整性和来源可信性的有力工具，广泛应用于电子合同、软件分发等领域。

3.2 使用安全协议

在数据传输过程中，确保数据的机密性和完整性是至关重要的。为此，使用安全协议成为一种行之有效的解决方案。TLS/SSL 协议是其中最为常见的安全协议之一。它通过在数据传输通道上建立加密连接，有效地防止了数据在传输过程中被窃听或篡改。无论是进行网页浏览、在线购物，还是进行敏感信息的传输，TLS/SSL 协议都能提供坚实的保护。它利用复杂的加密算法和密钥管理机制，确保数据在客户端与服务器之间的传输过程中始终保持机密性和完整性。此外，IPSec 协议也是保护数据传输安全的重要手段 [8]。它专注于为 IP 数据包提供全面的安全性保障。通过 IPSec 协议，

可以对 IP 数据包进行加密、认证和完整性校验，从而确保数据在传输过程中不会受到未经授权的访问和篡改。这一协议广泛应用于企业网络、远程访问和虚拟专用网络（VPN）等场景，为数据传输提供了可靠的安全保障。

3.3 加强密钥管理

密钥管理在加密技术中扮演着举足轻重的角色，它直接关系到加密系统的安全性和可靠性。为了筑牢密钥的安全防线，我们必须对密钥的生成、存储、分发及更新等各个环节实施精细化的管理。在密钥生成阶段，应确保算法的随机性和不可预测性，以产生高强度、难破解的密钥。随后，密钥的存储也需格外谨慎，防止被未经授权的人员获取。此时，硬件安全模块（HSM）便成为我们的得力助手。HSM 通过提供物理隔离和高级别的安全机制，能够确保密钥在存储过程中的安全性和完整性。在密钥分发环节，需要建立安全的分发渠道，确保密钥能够准确无误地送达指定的接收方 [9]。同时，密钥的更新也至关重要，它有助于我们应对潜在的安全威胁，保持加密系统的持续强健。

3.4 实时监控和响应

构建一个实时的数据传输安全监控系统，是提升系统安全性的重要举措。该系统能够即时监测数据传输过程中的各类异常行为，如数据泄露、篡改等潜在安全威胁，从而迅速采取应对措施，确保数据传输的安全无虞。在这一监控系统中，先进的检测技术和算法发挥着至关重要的作用。它们能够精准识别数据传输中的异常模式，及时发出警报，为安全团队提供宝贵的时间窗口，以便迅速定位问题源头并启动应急响应机制。同时，实时的响应措施也是监控系统不可或缺的一环。一旦检测到异常行为，系统应立即触发预设的应急预案，包括但不限于隔离受感染区域、阻断恶意数据传输、启动数据恢复程序等，以最大限度地减少安全事件对系统的影响。

3.5 定期更新加密算法和协议

随着计算技术的飞速进步和算法研究的不断深入，传统的加密算法与协议正逐渐面临被破解的风险，这对数据传输的安全性构成了潜在威胁。为了确保数据传输的持续安全，定期更新加密算法和协议显得尤为重要。加密算法和协议的更新不仅是为了应对已知的破解方法，更是为了预防未来可能出现的安全漏洞。通过引入新的、更强大的加密算法，可以有效提升数据传输的保密性和完整性，使得潜在的攻击者难以突破安全防线。同时，密切关注新的安全威胁和技术发展动态也是确保数据传输安全的关键。随着技术的不断进步，新的安全漏洞和攻击手段层出不穷。因此，需要定期评估当前加密技术的应用策略，及时调整和优化，以适应不断变化的安全环境。此外，更新加密算法和协议还可以提升系统的兼容性和互操作性。随着技术的发展，一些旧的加密算法和协议可能逐渐被淘汰，而新的算法和协议则可能成为新的标准 [10]。通过及时更新，可以确保系统能够与其他系统无缝对接，实现数据的顺畅传输。

4 结论

加密技术在网络数据传输中发挥着至关重要的作用。通过选择合适的加密算法、使用安全协议、加强密钥管理以及实时监控和响应等优化策略，可以有效地提高数据传输的安全性和效率。随着互联网的不断发展和通信技术的不断进步，加密技术将继续在网络数据传输中发挥着越来越重要的作用。未来，需要继续关注新的安全威胁和技术发展动态，不断探索和创新加密技术的应用策略和方法，以更好地保障用户的数据安全和隐私。

参考文献

[1] 姜森.数据加密技术在计算机网络安全中的应用研究[J].网络安全技术与应用,2024(4):31-32.

[2] 祖晓明.数据加密技术在计算机网络通信安全中的应用策略[J].信息记录材料,2024,25(2):30-32.

[3] 程光德.数据加密技术在计算机网络安全中的应用研究[J].信息记录材料,2024,25(2):84-86.

[4] 曹剑锋.数据加密技术在计算机网络通信安全中的应用实践[J].数字技术与应用,2024,42(2):103-105.

[5] 李荣,夏天勇,张琪,等.论数据加密技术在计算机网络安全中的应用[J].网络安全技术与应用,2024(1):24-25.

[6] 乔中辉.数据加密技术在计算机网络安全中的应用[J].中国宽带,2023,19(11):91-93.

[7] 张洲.数据加密技术在网络通信安全中的应用[J].中国宽带,2023,19(11):28-30.

[8] 陈克通.浅析数据加密技术在计算机网络安全中的应用[J].电子元器件与信息技术,2023,7(10):193-196+202.

[9] 吕维宗.数据加密技术在计算机网络中的应用[J].电子技术,2023,52(9):152-153.

[10] 闫军.数据加密技术在计算机网络信息安全中的应用研究[J].信息记录材料,2023,24(9):152-154.