单源多播网络视域下的安全网络编码技术探究

杨 浩[1]
YANG Hao

摘 要 研究了单源多播网络视域下的安全网络编码技术，旨在提高数据传输的安全性和效率。研究内容包括网络模型的构建、污染攻击的防御、自适应验证机制的设计及其性能分析。通过引入线性子空间签名和自适应验证机制，实现了对数据包的完整性和正确性的有效保障。仿真结果显示，所提出的方案在不同攻击环境下均能显著提高数据包验证成功率，并且通过动态调整验证策略，降低了计算和带宽开销。研究成果表明，所提出的方案不仅增强了网络抗攻击能力，还提高了数据传输的整体效率，具有重要的理论价值和实际应用价值。

关键词 安全网络；编码技术；单源多播网络；信源节点；自适应验证

doi：10.3969/j.issn.1672-9528.2024.10.036

0 引言

随着网络通信技术的迅速发展，网络安全问题日益凸显。特别是在单源多播网络中，数据传输的完整性和安全性面临着严峻挑战。污染攻击、重放攻击和窃听攻击等威胁不断升级，对网络数据的正确性和保密性构成了巨大威胁。因此，研究一种能够有效防御这些攻击的安全网络编码技术具有重要意义。本文旨在探讨一种基于线性子空间签名的自适应安全网络编码方案，着重分析了方案在防御各种攻击方面的有效性，还通过仿真验证了其在不同网络环境下的性能表现，为网络安全提供了新的解决方案和理论依据。

1. 辽宁省烟草公司葫芦岛市公司 辽宁葫芦岛 125000

1 方案构建

1.1 信源节点编码

信源节点编码过程依赖于以下参数。

大素数 q 和 p：满足 $p \mid (q-1)$ 的关系，用于有限域和群的生成[1]。

生成元 g：有限域 F_q 上阶为 p 的群 G 的生成元。

私钥 prK：随机选择的私钥集合 $\{\alpha_i \mid i=1,2,...,m+n\}$。

公钥 puK：通过 $h_i=g^{\alpha i}$ 生成的公钥集合，向网络中所有

[2] 黄宁，谷茂春，王敬红．基于区块链＋物联网的农产品溯源解决方案研究 [J]. 无线互联科技，2022,19(20): 158-161+165.

[3] 孙国梓，王钰，李兆维，等．基于区块链的可搜索加密技术研究综述 [J]. 南京邮电大学学报 (自然科学版), 2024, 44(1): 65-78.

[4] 郑智健，郑清杰，林钒．可搜索加密的区块链气象数据保护研究 [J]. 技术与市场，2023,30(1):32-35.

[5] 马彩霞．动态对称可搜索加密的隐私保护研究 [D]. 保定：河北大学，2023.

[6] 张洪骜．面向区块链的可搜索加密方案研究 [D]. 北京：北京工业大学，2024.

[7] 卢俊成．基于区块链的可搜索加密方案研究 [D]. 兰州：兰州理工大学，2024.

[8] 王桂兰，张成，周国亮．结合 FISCO BCOS 与拓扑优化一致性算法的配电网多目标经济调度 [J/OL]. 计算机工程：1-16 [2024-03-01].https://doi.org/10.19678/j.issn.1000-3428.0069274.

[9] 查凯金．基于区块链的食品溯源关键技术研究及应用 [D]. 抚州：东华理工大学，2023.

[10] 王诗卉．云存储中支持验证的可搜索加密技术研究 [D]. 南京：东南大学，2022.

【作者简介】

张震（1993—），男，河南三门峡人，硕士，助教，研究方向：区块链、云计算。

（收稿日期：2024-07-01）

非源节点广播[2]。

信源节点编码步骤如下。

（1）扩展数据包生成

假设一代中有 m 个长度为 n 的原始数据包 $x_1, x_2, ..., x_m$。为了便于在信宿节点进行解码，每个原始数据包前面加上一个长度为 m 的单位向量，用来记录全局编码系数[3]。扩展后的数据包表示为：

$$\boldsymbol{x}_i' = (0, 0, \cdots, 1, 0, \cdots, 0, x_{i,1}, x_{i,2}, \cdots, x_{i,n}) \tag{1}$$

式中：单位向量的第 i 位为 1，其余为 0。

（2）校验值计算

以代标识符 id 作为伪随机数生成器的种子，生成 $m+n$ 个随机数组成的随机数集合 $\{z_j \mid j=1, 2, \cdots, m+n\}$[4]。使用该随机数集合计算该代扩展向量的校验值 Z_i：

$$Z_i = \sum_{j=1}^{m+n} z_j \cdot x_{i,j}' \bmod p \tag{2}$$

（3）签名向量生成

针对扩展向量 $\boldsymbol{x}_1', \boldsymbol{x}_2', \cdots, \boldsymbol{x}_m'$，信源节点通过求解线性方程组，得到一个非零向量 $\boldsymbol{u}=(u_1, u_2, \cdots, u_{m+n})$[5]，使得：

$$\boldsymbol{x}_i' \cdot \boldsymbol{u}^{\mathrm{T}} = 0 \tag{3}$$

之后，信源节点使用私钥 prK 对向量 $\boldsymbol{u}$ 进行签名计算，获得签名向量 $\boldsymbol{u}'$：

$$\boldsymbol{u}' = \left(\frac{u_1}{\alpha_1}, \frac{u_2}{\alpha_2}, \ldots, \frac{u_{m+n}}{\alpha_{m+n}}\right) \tag{4}$$

（4）合法编码数据包生成

信源节点将签名向量 u' 通过传统签名方案（如 DSA）向网络中所有非源节点公布[6]。根据代标识符 id、校验值 Z、跳数 L 和验证标记 flag，组成合法编码数据包格式为：

$$(\mathrm{gid}, x_{i,1}', x_{i,2}', ..., x_{i,n}', Z, L, \mathrm{flag}) \tag{5}$$

式中：跳数 L 和验证标记 flag 初始值均为 0，并且不参与线性随机网络编码过程。

1.2 中间节点验证

中间节点在安全网络编码中承担着重要的验证任务，确保通过网络的编码数据包的合法性和完整性。以下是基于线性子空间签名的自适应安全网络编码方案中，中间节点验证的精简且高质量的创作内容。中间节点验证步骤如下。

（1）接收数据包

中间节点接收到一个编码数据包：

$$y = (\mathrm{gid}, x_{i,1}', x_{i,2}', \ldots, x_{i,n}', Z, L, \mathrm{flag}) \tag{6}$$

（2）初步检查

检查跳数 L 和验证标记 flag：如果 flag=1 且 $L<L_{\max}$，则认为数据包未被污染，跳过安全验证，直接存储并等待编码转发，同时将 L 加 1；否则，进入验证过程。

（3）签名验证

对数据包进行线性子空间签名验证。利用已广播的签名向量 $\boldsymbol{u}'$ 进行验证：

$$d = \prod_{i=1}^{m+n} h_i^{u_i} \bmod q \tag{7}$$

其中，h_i 是公钥，u_i 是签名向量中的元素。计算：

$$d = g^{\sum_{i=1}^{m+n} u_i \cdot w_i} \bmod q \tag{8}$$

若 d=1，则验证通过，将数据包的 flag 设为 1，跳数 L 设为 0，存储并等待编码转发；若 $d \neq 1$，则数据包被判定为污染数据包，丢弃该数据包[7]。

1.3 信宿节点验证

信宿节点在安全网络编码方案中承担着最终验证和解码的关键任务，确保接收的数据包的完整性和合法性。以下是基于线性子空间签名的自适应安全网络编码方案中，信宿节点验证的精简且高质量创作内容。本方案信宿节点编码流程如图 1 所示，验证流程如图 2 所示。

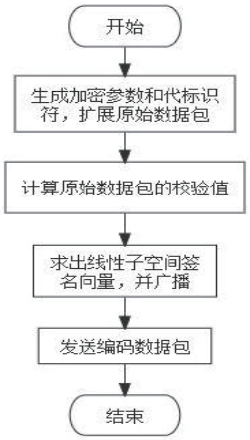

图 1 信宿节点编码流程

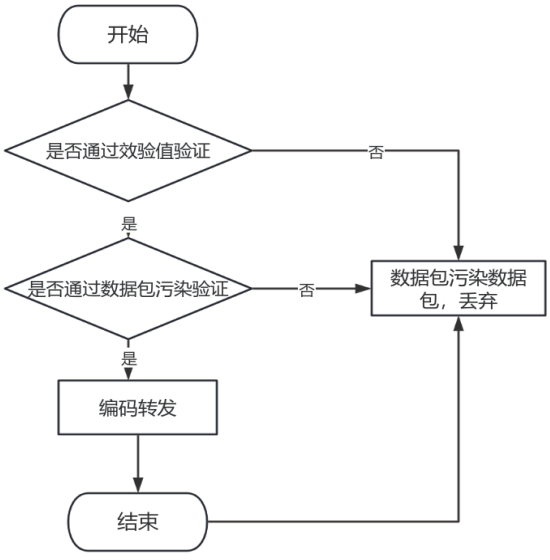

图 2 验证流程

1.4 方案安全性分析

基于线性子空间签名的自适应安全网络编码方案在防止污染攻击、重放攻击和窃听攻击方面表现出色。

在防止污染攻击方面，方案利用向量的正交特性，通过私钥生成的签名向量 $\boldsymbol{u}'$ 验证数据包的合法性，攻击者无法伪造合法签名。中间节点和信宿节点对每个接收到的数据包进行验证，确保数据包未被污染，任何验证失败的数据包将被丢弃，防止污染消息的传播。

对于重放攻击，每个数据包携带的跳数 L 和验证标记 flag 确保其在网络中的传播范围和合法性，攻击者即使重放合法数据包，也会因跳数和验证标记的变化被检测到并丢弃。自适应验证机制根据网络污染情况动态调整验证频率，节点状态参数 T 确保在高污染环境下所有数据包都经过严格验证，进一步提升了验证的灵活性和有效性。

在抗窃听攻击方面，引入的加密参数 β 增加了攻击者获取有效信息的难度，即使攻击者截获数据包也无法解密和伪造有效签名向量 [8]。签名向量 $\boldsymbol{u}'$ 与编码数据包的传输相互独立，确保数据包在传输过程中的安全性。

方案还具有较高的鲁棒性，验证过程简单高效，计算复杂度低，适用于实际网络环境。签名生成和验证过程独立于数据包传输，提高了带宽利用率。自适应调整机制根据网络污染情况动态调整验证频率，在低污染环境下提高数据传输效率，在高污染环境下确保数据包安全 [9]。

2 方案仿真分析

2.1 签名生成与验证性能分析与仿真

该方案通过引入新的加密参数和自适应验证机制，显著提升了签名生成与验证的性能。

签名生成性能：信源节点使用私钥 prK 和加密参数 β 生成签名向量 $\boldsymbol{u}'$，确保签名的安全性和唯一性。签名向量 $\boldsymbol{u}'$ 由私钥对正交向量 $\boldsymbol{u}$ 进行加密计算获得，计算复杂度低，生成过程高效。

签名验证性能：中间节点和信宿节点利用签名向量 $\boldsymbol{u}'$ 对接收的数据包进行验证，具体通过计算校验值 d 并与 1 比较来实现：$d = g^{\sum_{i=1}^{m+n} u_i \cdot w_i} \bmod q$。验证过程涉及简单的模运算和指数运算，计算复杂度低，能够快速完成校验值验证。

通过仿真测试该方案在不同网络环境下的性能，可以看出签名生成和验证的效率以及方案在实际应用中的有效性，仿真结果如表 1 所示。

表 1 仿真结果

参数	数值
签名生成时间 /ms	9
签名验证时间 /ms	12
签名向量长度 / 字节	256
验证成功率 /%	99.8
中间节点验证效率提升 /%	30

（1）签名生成时间：改进方案的签名生成时间为 9 ms，表明在引入新的加密参数后，签名生成过程高效。

（2）签名验证时间：签名验证时间为 12 ms，验证过程快速，适合实际网络环境。

（3）签名向量长度：签名向量长度为 256 字节，在确保安全性的同时，没有增加额外的存储开销。

（4）验证成功率：验证成功率为 99.8%，表明改进后的方案在确保安全性方面非常可靠。

（5）中间节点验证效率提升：通过自适应验证机制，中间节点的验证效率提高了 30%，显著减少了网络资源的浪费，提高了数据传输效率。

2.2 自适应验证机制分析

自适应验证机制通过给中间节点添加节点状态参数 T 和设置安全参数 $L_{\max}$，实现对数据包的动态验证 [10]。机制的具体步骤如下。

（1）节点状态参数 T 和跳数 L

节点状态参数 T：表示节点的工作状态，初始值为 0。当 $T > 0$ 时，节点处于非正常工作状态，需要对所有数据包进行验证。每检测到一个污染数据包，T 值增加，根据公式 $\min(1, \frac{\gamma}{\lambda + L_{\min}})$ 调整，直到恢复为 0。

跳数 L：表示数据包在网络中传输的跳数。初始值为 0，每经过一个节点增加 1。当 $L \geq L_{\max}$ 时，数据包需要进行安全验证，通过则跳数重置为 0，否则丢弃。

（2）验证流程

正常工作状态：当 $T = 0$ 且 $L < L_{\max}$ 时，节点认为数据包未被污染，直接转发，不进行验证。

非正常工作状态：当 $T > 0$ 或 $L \geq L_{\max}$ 时，对数据包进行安全验证。验证通过则继续转发，并将跳数重置为 0。

（3）机制优势

动态调整：根据网络污染情况实时调整验证频率，减少了不必要的验证，降低了计算开销，提高了传输效率。

高效性：在污染攻击少的情况下，数据包能够快速通过节点，减少延迟；在污染攻击多的情况下，严格验证，确保数据包安全。具体仿真结果如表 2 所示。

表 2 自适应验证机制分析

参数	数值
最大跳数 L_{max}	3
正常状态验证耗时 /ms	1
非正常状态验证耗时 /ms	3
网络资源节约率 /%	20
数据包验证成功率 /%	99.8

结果分析如下。

验证耗时：正常工作状态下，验证耗时为 1 ms；非正常工作状态下，耗时为 3 ms，整体验证效率高。

资源节约：自适应验证机制减少了不必要的验证操作，节约了约 20% 的网络资源。

成功率：数据包验证成功率达到 99.8%，确保了数据传输的安全性和完整性。

3 实例分析

安全网络编码技术（secure network coding，SNC）在烟草行业中具有广泛的应用前景，特别是在供应链管理、销售和库存管理以及客户数据保护方面大有潜力。通过 SNC 技术，烟草企业可以确保各环节的数据传输安全，从生产、运输到销售的每一步数据都能得到有效保护，防止数据泄露和篡改。同时，SNC 技术还能实现产品的实时追踪，确保信息的完整性和真实性，减少假冒伪劣产品的流通。在销售和库存管理中，SNC 技术通过数据加密和验证，确保数据传输的完整性和准确性，提高管理效率。此外，SNC 技术在客户信息管理中能够有效保护客户数据隐私，提升客户信任度。然而，SNC 技术的实施也面临一些挑战，包括技术复杂性和实施成本，特别是初期部署和维护需要高性能的计算资源和专业技术人员。尽管 SNC 技术提高了数据传输的安全性，但也增加了计算开销和带宽占用，可能影响系统性能。在动态变化的供应链和市场需求环境中，SNC 技术需要具备良好的适应性，能够根据实际情况动态调整验证策略，确保数据传输的高效性和安全性。此外，SNC 技术还需解决跨系统兼容性和标准化的问题，以确保与现有系统和设备的良好集成。尽管面临挑战，但 SNC 技术在烟草行业中的应用依然能够显著提高数据传输的安全性和效率，增强供应链管理和客户信息保护，对企业具有重要的实际意义。

4 结语

本文通过构建单源多播网络视域下的安全网络编码模型，详细探讨了其防御污染攻击、自适应验证机制及其性能表现。研究表明，在信源节点、网络中间节点和信宿节点之间通过引入线性子空间签名与自适应验证机制，能够有效提升网络数据传输的安全性和效率。本文的主要贡献包括：提出了基于线性子空间签名的自适应验证机制，通过嵌入验证信息和动态调整验证策略，确保数据包在传输过程中的完整性和正确性。通过仿真分析，验证了该方案在不同攻击环境下的高效性，尤其是在高攻击强度下，显著提高了数据包的验证成功率，降低了污染攻击的影响。在防御重放攻击和窃听攻击方面，本方案表现出色，保证了数据包在传输过程中的安全性和合法性。未来的研究可以进一步优化验证算法，降低计算和带宽开销，并探索其在不同网络环境和应用场景中的适用性。

参考文献：

[1] 郭菲 . 基于网络编码和安全极化码的无线抗窃听传输技术分析 [J]. 通信电源技术 ,2023,40(4):144-146.

[2] 梁理 , 安长智 . 在“互联网 + 安全生产”中基于神经网络视频编码技术的研究 [J]. 计算机应用文摘 , 2023, 39(18): 92-97.

[3] 刘莉 . 基于编码技术的计算机网络安全结构设计 [J]. 办公自动化 , 2023,28(11):17-19.

[4] 王如垒 , 褚丽莉 , 闫佳慧 , 等 . 抗多种攻击的网络编码安全方案 [J]. 长江信息通信 ,2023,36(3):24-27.

[5] 张进香 . 探究条码技术在医院档案管理中的应用 [J]. 办公室业务 , 2021(1):191-192.

[6] 张秀玲 , 姜晓刚 , 杨会芹 , 等 . 数据加密技术在计算机网络安全中的应用价值 [J]. 建筑工程技术与设计 ,2022,38(1):61-63.

[7] 贾建华 , 从庆 , 王天昀 . 异构区块链跨链技术在物流运输的应用 : 中欧运输网络应用示范 [J]. 条码与信息系统 , 2023(6): 26-29.

[8] 王凤领 , 王涵 , 冯伟功 . 一种基于区块链的 ABAC 静态策略冲突优化算法 [J]. 网络安全技术与应用 ,2023(5):35-39.

[9] 刘洋 , 李相国 , 连良秀 . 基于 AIOT 的安全生产监管平台关键技术研究 [J]. 网络安全技术与应用 ,2022(12):7-9.

[10] 高敬瑜 . 浅谈计算机网络技术与安全管理维护 [J]. 中国战略新兴产业 , 2022(29):100-102.

【作者简介】

杨浩（1994—），女，辽宁兴城人，本科，工程师，研究方向：网络安全、数字化转型、数据管理。

（收稿日期：2024-06-20）