混合加密机制下网络在线检测数据多链路安全传输方法

孙思雨 [1]
SUN Siyu

摘 要 网络在线检测的数据来源广泛，多链路传输环境复杂多变，数据传输多呈单向特性，极易遭受外部恶意攻击与内部安全威胁。单一的对称加密算法虽加解密速度较快，但存在密钥分发与管理困难、易被破解等问题，而单一的非对称加密算法安全性较高，但加解密速度慢，在处理海量数据时效率低下，易造成数据传输过程中解码失败或传输延迟。为此，文章提出一种基于混合加密机制的网络在线检测数据多链路安全传输方法。利用哈希算法对分割后的数据块计算生成摘要值，结合数据元组密度、初始化标识符等关键特征挖掘强关联数据，提取核心数据；采用 DES 对称加密与 RSA 非对称加密相结合的混合加密机制，设计安全传输协议，使用 DES 加密核心数据，并通过 RSA 对 DES 密钥进行二次加密。同时，借助 PCA 方法对加密数据进行降维处理，构建低维特征阵列，通过多维部署完成身份验证，验证通过后按照协议进行数据传输。对于通过身份验证的合法重要数据，采用 OFDM 技术进行多链路资源分配：通过划分链路资源并计算链路总带宽，设定融合链路特性与数据接入时序的多链路通信接入权重，进而计算各链路资源分配量，最终实现多链路安全传输。实验结果表明，所提方法可实现终端数据包的实时加密传输，在显著降低解码失败率的同时，有效提升数据传输效率。

关键词 混合加密机制；核心信息提取；安全传输；多链路；在线检测数据

doi：10.3969/j.issn.1672-9528.2026.02.038

0 引言

互联网技术的发展，推动了其在社会中多个行业的应用。随着网络规模的增加，网络在线测试数据量也越来越大。网络测试数据是实现终端信息交互、资源共享的主要载体，如何实现此部分数据的安全传输，有效防御多种手段的攻击，成为技术部与相关部门的关注重点。

针对这一问题，相关学者开展了多项深入研究。例如，张伟等 [1] 以过程工业为研究对象，设计了面向过程工业的安全生产数据多层次、多路径传递的无线传感器网络模型。实践证明，设计方案能有效地提升系统的实时性与精度，减少系统的误报率，为工业过程的安全运行提供强有力的保证。在网络在线检测数据易受攻击的背景下，该模型缺乏对数据加密、身份验证等关键安全环节的设计，数据在传输过程中可能面临被窃取、篡改等风险，无法有效保障数据的保密性、完整性和可用性。蔺海荣等 [2] 以人脑为基础，构建双忆阻类脑型混沌神经网络模型，将其用于 IoMT 数据的隐私保护，以提高数据的保密性。实践证明，所设计的网络可以有效地抵抗外界的攻击，并能保证数据的保密性。该模型主要用于 IoMT 数据的隐私保护，以提高数据保密性，但仅构建了一个用于隐私保护的网络模型，未形成完整的数据安全传输体系，导致数据在传输前或传输后可能被窃取或篡改。

为解决上述方法存在的问题，优化数据传输，保证多链路通信的安全性，本文将以网络在线检测数据为研究对象，基于混合加密机制设计一种多链路安全传输方法。

1 网络在线检测数据核心信息提取

在网络在线检测数据的多链路安全传输过程中，数据量极为庞大且来源复杂多样，其中夹杂着大量冗余、无关或价值较低的信息。若直接传输所有数据，不仅会大量占用网络带宽，显著降低数据传输效率，还会大幅增加数据安全防护工作的复杂程度与难度。因此，需要提取网络在线检测数据的核心信息，以此聚焦关键数据，提升数据传输效率以及安全防护的整体效能。通过提取核心信息，能够深入掌握数据集合的特征，进而明确数据安全防护的重点方向 [3]。

在提取核心信息的过程中，运用哈希算法。该算法通过对输入的原始数据进行特定的计算，从而生成一个固定长度的摘要值，且该摘要值与原始数据存在一一对应的关系。任何细微改动都会导致哈希结果变化。通过比对接收数据的摘

1. 大庆油田第二采油厂数字化运维中心数控管理室
黑龙江大庆 163414

要与原始摘要，可以验证数据在传输和存储过程中是否被篡改，从而确保接收端数据的完整性和可靠性 [4-5]。在提取核心信息前，需先将原始数据进行分割处理，使其成为由若干个数据块构成的集合。每个数据块经哈希算法计算后，都会生成一个对应的数据摘要 [6]。在数据传输或存储环节，若某个数据块的摘要在传输或存储前后不一致，即可判定该数据块已被篡改；若部分数据块缺失对应摘要或摘要信息出现异常，则表明数据出现了损毁情况 [7]。在此过程中，依据网络在线检测数据的元组密度与初始化标识符，结合数据的其他关键特征挖掘强关联数据，以提取核心信息：

$$A=\frac{l\times m}{\rho\times c} \tag{1}$$

$$g=\frac{A\times\|\boldsymbol{z}\|}{x} \tag{2}$$

式中：A 表示数据集合调制系数；l 表示数据均衡处理系数；m 表示数据初始化标识符；ρ 表示数据元组密度；c 表示数据时序特征；g 表示网络在线检测数据集合中的核心数据；$\boldsymbol{z}$ 表示数据关联矩阵；x 表示哈希编码常数 [8]。

通过对数据源中的强关联数据进行深度挖掘、统计分析以及聚类操作，可实现对网络在线检测数据中核心数据的提取。

2 基于混合加密的数据安全传输协议设计

在网络在线检测数据多链路安全传输中，完成核心信息提取后，虽明确了关键数据，但这些数据在传输过程中仍面临诸多安全风险。常规通信网络中，数据传输多呈单向性，极易受到外部恶意攻击和内部安全威胁。一旦数据在传输中被破坏，接收端接收到的将是错误或残缺信息，严重影响后续基于数据的检测、分析和决策工作。因此，为保障核心数据在复杂网络环境下的安全传输，引入混合加密机制，设计数据安全传输协议。该混合加密机制由 DES 对称与 RSA 非对称加密算法构成，综合考虑 DES 的高效性与 RSA 的安全性，确保数据在传输中的隐私性与完整性 [9]。RSA 算法是一种利用公共密钥加密数据、用私有密钥解密数据的不对称密码算法 [10]。在这种加密方式下，发送端能够安全地向接收端传递 DES 密钥，而不用考虑在传送时密钥被截取或篡改。接收端接收到 RSA 加密的 DES 密钥后，可使用自身的 RSA 私有密钥对其进行解密，从而还原出密钥。在此过程中，发送端和接收端可利用公钥对原始数据进行加密和解密操作 [11]。

为确保所设计的安全传输协议符合规范性与安全性要求，采用 64 位的 DES 数据块密码体制，数据块经 16 轮循环加密，得到的传输协议子密钥用公式表示为：

$$M(t)=L\sqrt{\frac{\chi}{\gamma}} \tag{3}$$

式中：M 表示传输协议子密钥；t 表示时序点；L 表示加密处理轮次；χ 表示数据块数量；γ 表示 DES 数据块位数。

在此基础上，利用 DES 对称私钥进行传输协议中关键信息的解密操作。通过解密过程，还原出传输协议覆盖的明文更新信息，此过程可通过公式计算为：

$$\varphi=M(t)\exp\left(-\frac{K_1}{K_2}\right) \tag{4}$$

式中：φ 表示传输协议覆盖的明文更新信息；K_1 表示密钥签名；K_2 表示更新次数。

完成解密后，为进一步保障 DES 加密密钥的安全性，使用非对称加密算法对 DES 加密密钥进行双重加密处理。通过这种双重加密方式，结合 DES 与 RSA 加密算法的优势，确保应用该传输协议可实现对网络在线检测数据的混合加密，此过程用公式表示为：

$$Q=\varphi\sqrt{\frac{\delta}{\|\boldsymbol{S}\|}} \tag{5}$$

式中：Q 表示混合加密后的结果；δ 表示有效签名文件数量；$\boldsymbol{S}$ 表示随机矢量。

完成上述安全传输协议设计后，需明确常规通信网络中数据传输方式大多呈现单向性，正因如此，数据在受到外部和内部的攻击时，接收端接收到的数据会遭到破坏。针对此问题，利用混合加密后的安全传输协议，采用 PCA 方法对网络在线检测数据进行降维处理。通过 PCA 方法，提取数据中的主要特征，去除冗余信息，得到具有较低维数的特征阵列，具体计算公式为：

$$\boldsymbol{W}=Q\cdot g\cdot\sum_{n=1}^{k}\frac{\lambda_n}{\|\boldsymbol{P}_n\|} \tag{6}$$

式中：$\boldsymbol{W}$ 表示低维数的特征阵列；k 表示网络在线测试数据中的主成分数量；λ_n 表示主成分分析中的特征值；$\boldsymbol{P}_n$ 表示数据的权值向量。

采用多维部署的方式，对降维处理后的信息进行身份验证。多维部署可综合利用多种身份验证手段，从不同维度验证数据的合法性与完整性。若身份验证通过，则可按照上述设计的混合加密安全传输协议进行数据传输，确保数据在多链路安全传输过程中的隐私性、完整性和可用性。

3 基于资源分配的数据多链路传输

在网络在线检测数据多链路安全传输过程中，完成数据安全传输协议设计后，仅保障了数据在传输过程中的隐私性与完整性，但实际通信环境复杂多变。常规通信网络中数据传输单向性易受外部恶意攻击和内部安全威胁，且不同链路的带宽、时延、丢包率等特性存在差异，单一链路传输易因链路故障或拥塞导致数据传输中断或延迟，影响数据传输的可靠性和效率。因此，需进一步开展数据多链路传输设计，

以充分利用多条链路的资源，提升数据传输的稳定性与效率。具体采用对多链路进行资源分配的方式，在此过程中引入OFDM技术，其凭借正交子载波特性，能够有效对抗多径干扰，进而优化通信链路中的带宽资源分配。

设定通信链路由若干个子信道和子时隙构成[12]。通信网络的总带宽容量，是指每个无线接入网被指派最初带宽的总和，即该网络上所有已连接用户所分配带宽与整个网络可用带宽的总和。通过这种对链路资源细致划分的方式，可计算网络在线检测数据通信链路带宽总和，计算公式为：

$$E = W\sum_{j>1}^{i}\eta_{ij} \tag{7}$$

式中：E 表示网络在线检测数据通信链路带宽的总和；η 表示多链路通信接入的权重；i 表示子信道；j 表示子时隙。在掌握网络链路可调用与分配的带宽总和基础上，考虑到在线数据传输并非同一时刻接入混合无线网络（HWNs），而是按照一定时序进行数据接入，不同时序下各链路的传输需求和状态可能不同。针对此情况，设定多链路通信接入的权重，该权重不仅与链路本身的特性相关，还与数据接入的时序有关。计算公式为：

$$\eta = \psi \times \frac{E}{\lambda_{ij}} \tag{8}$$

式中：ψ 表示信道叠加系数；λ 表示状态变量。

根据多链路的接入权重，进一步计算对应链路通信传输中的资源分配量。此过程通过公式计算为：

$$\max R = \max\sum_{i>1}^{m} r_i(\eta) \tag{9}$$

式中：R 表示带宽资源分配量；m 表示传输节点；r 表示分配决策状态。

通过上述方式，在混合加密机制保障数据安全传输的基础上，进一步实现对网络在线检测数据的多链路安全传输，不仅能够确保数据传输的隐私性与完整性，还能够显著提高数据传输的稳定性、可靠性和效率。

4 对比实验

4.1 实验准备

完成上述设计后，为实现对网络在线检测数据多链路安全传输方法的测试，准备多链路传输测试计算平台，在平台上建立由3台PC机构成的数据传输硬件环境。在此基础上，将两台PC机分别用作网络在线检测数据的接收终端和用于传输数据服务器，在两者之间进行数据传输，另外一台PC机则作为云计算实体主机，负责建立虚拟技术。完成测试环境的构建后，为排除外部环境中相关因素的干扰，保证实验结果的真实性与可靠性，可按照表1所示的内容，进行测试环境技术参数的设计。

表1 测试环境技术参数

序号	项目	参数
1	计算机节点	Name-Node节点（1个） Data-Node节点（8个）
2	实验的软件环境系统	Linux系统
3	数据处理引擎软件	Spark
4	数据传输与下载软件	FileZila

在此基础上，对两个测试终端的技术参数进行分析，如表2~3所示。

表2 发送端PC机技术参数

序号	项目	参数
1	带宽/MHz	5
2	子载波	200
3	发射功率/dBm	46
4	半帧下行符号数	35
5	路径损耗模型	Cost-231

表3 接收端PC机技术参数

序号	项目	参数
1	通信传输标准	80211a
2	带宽/MHz	20
3	接收覆盖半径/m	50
4	帧长/ms	5

在上述准备工作完成后，按照设计的方法，进行网络在线检测数据的安全传输，为确保实验结果的真实性与可比性，引进文献[1-2]提出的方法，将其作为对照，参与本次数据安全传输等相关测试工作。

4.2 网络在线检测数据传输实时加密量

将网络在线检测数据传输的实时加密量作为检验指标，可综合评估在数据传输中的安全性。理想状态下，期望输出的实时加密量与输入终端的数据包数量完全一致，以此确保所有数据均得到安全加密处理。若实时加密量小于输入终端的数据包数量，则表明存在部分数据未被加密，这些未加密数据在传输过程中极易出现丢失、泄露等异常状况；反之，若实时加密量大于输入终端的数据包数量，则说明数据包在录入后可能遭到被篡改，导致数据中携带大量冗余数据，不仅浪费带宽资源，还可能干扰正常数据传输与处理。对该指标进行检验，其结果如图1所示。从图1所示的实验结果可以看出，本文方法采用RSA非对称加密算法进行网络在线检测数据传输时，其安全密钥管理机制确保了加密密钥的保密性和完整性。只有合法收发双方能够使用正确密钥进行加解密操作，有效防止了密钥泄漏导致的非法数据注入或篡改。数据在传输过程中保持原始状态，实时加密量与输入数据包数量一致，符合预期输出标准。

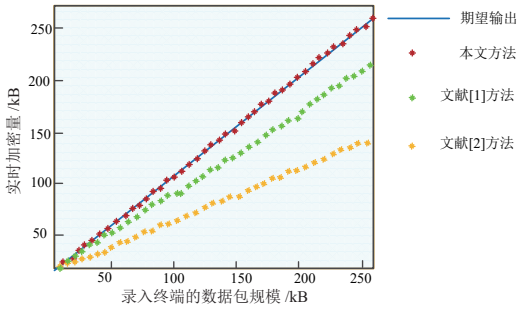
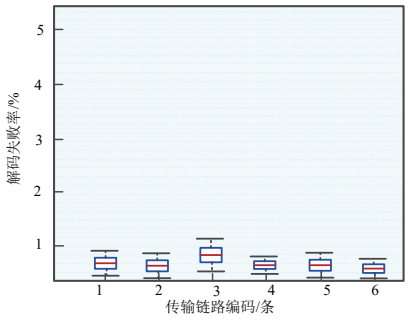


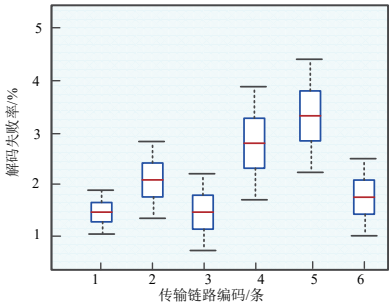
图 1 网络在线检测数据传输实时加密量检验结果

4.3 多链路数据安全传输解码失败率检验

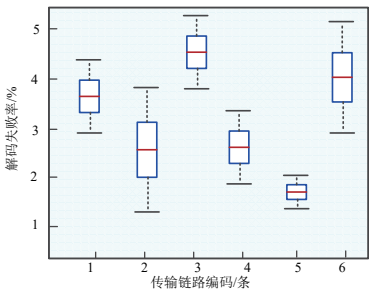
在此基础上，将多链路数据安全传输解码失败率作为检验指标。该指标用于衡量数据在到达传输终端后，终端对数据进行解码时未能按照规范完成解码的数据占比情况。解码失败率越高，表明数据安全传输效果越差，数据在传输过程中可能遭受更多干扰或加密机制未能有效保障数据正确性；反之，解码失败率越低，说明加密机制的应用效果越好，即终端所使用的密钥能够满足解码数据的需求。采用箱型图对多链路的网络在线检测数据传输解码失败率进行检验，结果如图 2 所示。从图 2 可以看出，在多链路数据安全传输场景下，本文方法所采用的混合加密协议结合了 DES 对称加密算法的高效性和 RSA 非对称加密算法的密钥管理优势。DES 算法可快速加密大量数据，确保传输过程中的数据保密性；RSA 算法则保障密钥的安全交换，只有合法接收方才能获取解密密钥。这种双重加密机制既保证了数据加密的准确性，又确保接收端能正确解密，显著降低了加解密过程中的解码失败率。相比之下，文献 [1]~[2] 方法的解码失败率明显较高。



（1）本文方法



（2）文献 [1] 方法



（3）文献 [2] 方法

图 2 多链路数据安全传输解码失败率检验结果

4.4 传输效率检验

将单位时间内网络在线检测数据的吞吐量设定为检验传输效率的关键指标。吞吐量越高，表示在单位时间内成功传输的数据量越大，即数据传输效率越高；反之，吞吐量越低，则表明数据传输效率越低。检验结果如图 3 所示。

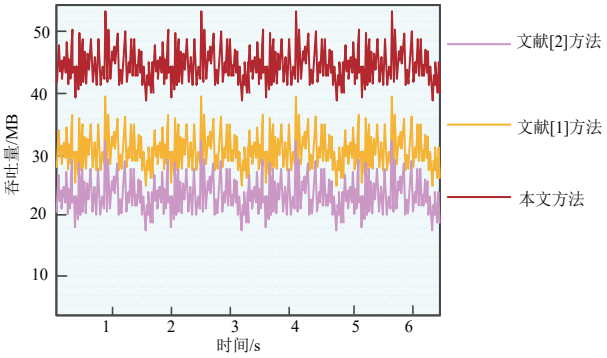


图 3 数据传输效率检验

从图 3 可以看出，在相同的测试环境下，本文方法展现出了最高的数据传输效率，具体表现为单位时间内的数据吞吐量显著高于其他情况，能够充分满足实际应用中对高效数据传输的需求。本文方法中动态调整带宽和时序权重，不仅有助于提高数据传输效率，还能增强数据传输的稳定性和可靠性。当某条链路出现突发故障或干扰时，采用 OFDM 技术能够迅速调整带宽和时序权重，将数据传输任务转移到其他正常链路上，保证数据传输的连续性。这种动态适应能力使得数据在复杂多变的网络环境中能够稳定、高效地传输，从而提高了单位时间内的数据吞吐量。

5 结语

多链路数据传输环境复杂且具有单向性特征，使其面临严重的安全威胁。对称加密算法密钥管理困难，非对称加密算法处理效率低下，均难以满足实时安全传输需求。本研究提出一种基于混合加密的多链路安全传输方法。数据预处理阶段采用哈希算法生成数据块摘要，基于关键特征提取核心数据；混合加密机制采用 RSA 算法保障密钥安全传输，DES

算法实现高效数据加密，双重加密确保传输安全；传输优化处理通过 PCA 降维减少数据量，多维身份验证确保合法性；资源动态分配采用 OFDM 技术实现多链路调度，基于带宽计算与权重分配。实验结果表明，该方法实现了终端数据包的实时加密传输，在降低解码失败率的同时提升了传输效率。随着网络技术发展，需持续优化加密技术以应对日益复杂的安全挑战。

参考文献：

[1] 张伟 , 李泽亚 , 张充 , 等 . 基于 WSN 的流程行业安全生产数据多优先级多路径传输方法 [J]. 中国安全生产科学技术 , 2023, 19(9):5-11.

[2] 蔺海荣 , 段晨星 , 邓晓衡 , 等 . 双忆阻类脑混沌神经网络及其在 IoMT 数据隐私保护中应用 [J]. 电子与信息学报 , 2025, 47:1-17.

[3] 张杰 , 杜金华 , 刘立 , 等 . 水下通信网络中基于公钥加密体制的安全数据传输方法 [J]. 小型微型计算机系统 , 2023, 44(8): 1805-1811.

[4] 涂剑峰 , 李芳丽 . 冒充性攻击下无线传感节点信息数据安全推荐算法 [J]. 传感技术学报 , 2024, 37(8):1434-1440.

[5] 欧家祥 , 胡厚鹏 , 何沛林 , 等 . 基于国密算法的电网 AMI 数据安全防护技术 [J]. 西南师范大学学报 : 自然科学版 , 2023, 48(3):17-24.

[6] 陈佟 , 黄文雯 , 夏小萌 , 等 . 基于 RSA 算法的电力通信工程环境安全监测方法 [J]. 微电子学与计算机 , 2023, 40(4):63-71.

[7] 王惠明 , 刘志明 , 何娜 , 等 . 复杂环境山地灾害监测智能感知与数据传输关键技术 [J]. 科学技术与工程 ,2025, 25(2):640-648.

[8] 张晓烁 , 倪唯一 , 肖海林 . 基于 RIS-UAV 协作的车载通信系统安全传输研究 [J]. 电子科技大学学报 , 2023, 52(4): 539-548.

[9] 王怀乐 , 刘然 , 马明 , 等 . 基于云资源的青藏高原科考数据收集与传输平台设计与实现 [J]. 气象科技 , 2023, 51(5): 648-657.

[10] 许子恒 , 李王睿 , 张立东 , 等 . 基于信息备份技术提升城市轨道交通数据单向传输可靠性的设计方法 [J]. 城市轨道交通研究 , 2024, 27(9):227-230.

[11] 覃润楠 , 彭晓东 , 谢文明 , 等 . 面向航天器大数据安全传输的发布 / 订阅系统设计 [J]. 系统工程与电子技术 , 2024, 46(3): 963-971.

[12] 刘炜 , 郭灵贝 , 夏玉洁 , 等 . 基于门限聚合签名的区块链预言机数据传输模型 [J]. 郑州大学学报 : 理学版 ,2023, 55(4): 23-29.

【作者简介】

孙思雨（1991—），女，黑龙江大庆人，本科，助理工程师，研究方向：数字运维。

（收稿日期：2025-05-14　修回日期：2026-02-12）

（上接第 156 页）

参考文献：

[1] 吴小凤 . 基于数据挖掘的智慧图书馆信息自动化检索系统设计 [J]. 自动化技术与应用 ,2024,43(4):155-158.

[2] 杨月 . 数字图书馆交互式信息分类检索模型设计 [J]. 科技通报 , 2021,37(12):112-116.

[3] 康丽丽 , 钱婧 . 网络信息资源分类检索方法的应用 [J]. 集成电路应用 , 2023,40(5):158-159.

[4] 王欣玥 . 信息检索领域 IPC 分类号与 CPC 分类号的对比分析 [J]. 海峡科技与产业 ,2022,35(12):77-83.

[5] 孟怡悦 , 彭蓉 , 吕其标 . 一种结合标签分类和语义查询扩展的文本素材推荐方法 [J]. 计算机科学 ,2023,50(1):76-86.

[6] 代佳洋 , 周栋 . 基于多任务学习的跨语言信息检索方法研究 [J]. 广西师范大学学报 (自然科学版),2022,40(6):69-81.

[7] 江雪姣 . 基于大数据技术的网络信息资源分类检索方法 [J]. 信息与电脑 (理论版),2022,34(13):10-12.

[8] 林广朋 . 基于贝叶斯算法的网络信息安全过滤系统设计 [J]. 长江信息通信 , 2022,35(6):54-56.

[9]ZHANG J .Data-driven development of entrepreneurial ecosystem based on the apriori algorithm[J].Journal of computational methods in sciences and engineering,2025,25(4):3224-3238.

[10]LI T T, LIU F, CHEN X B, et al.Publisher correction: web log mining techniques to optimize apriori association rule algorithm in sports data information management[J].Scientific reports, 2024,14(1):30568.

【作者简介】

黄海涛（1992—），男，安徽霍邱人，本科，高级工程师，研究方向：大数据、人工智能、智慧图书馆。

（收稿日期：2025-07-08　修回日期：2026-01-14）