文章编号:1671-4598(2025)10-0266-07 DOI:10.16526/j.cnki.11-4762/tp.2025.10.034 中图分类号:TP13 文献标识码:A

基于非对称加密的云网 5G 通信下行信道传输安全控制

龚险峰[1]，徐胜超[2]
(1. 广州华商学院 数字传播学院，广州 511300；
2. 广州华商学院 人工智能学院，广州 511300)

摘要：为了降低云网 5G 通信环境串行干扰下的信道传输译码错误率，设计基于非对称加密技术的云网第五代移动通信技术通信下行信道传输安全控制方法；根据通信信道最优控制值、最优平衡指标、最优控制节点，建立 5G 通信下行信道传输衰减平衡优化方程；基于非对称加密生成信道传输控制节点安全公钥，并结合衰减平衡优化方程，解密公钥加密数据；创新性地动态生成云网 5G 通信节点，离网传输控制素数，更新私钥，使一个公钥能够在不同传输控制节点上对应不同的私钥，实现串行干扰中的下行信道传输安全控制；实验结果表明，该方法应用后，边缘服务器译码错误率达到 10^{-8} 以下，降低了译码错误概率，保证了数据在传输过程中不被篡改或损坏，数据传输安全控制效果较佳，有助于解决边缘服务器在数据传输过程中面临的挑战，推动边缘计算生态的完善和发展。

关键词：非对称加密技术；云网；5G 通信；下行信道；传输安全；控制方法

Transmission Security Control for Cloud Network 5G Communication Downlink Channels Based on Asymmetric Encryption

GONG Xianfeng[1], XU Shengchao[2]
(1. School of Digital Communication, Guangzhou Huashang College, Guangzhou 511300, China;
2. School of Artificial Intelligence, Guangzhou Huashang College, Guangzhou 511300, China)

Abstract: In order to reduce the decoding error rate of channel transmission under serial interference in cloud network 5G communication environment, a security control method for downlink channel transmission of cloud network 5G mobile communication technology based on the asymmetric encryption technology is designed. Establish an optimization equation for 5G communication downlink channel transmission attenuation balance based on optimal control value, optimal balance index, and optimal control node of the communication channel. Generate secure public keys for channel transmission control nodes based on the asymmetric encryption, decrypt the public key, and encrypt the encrypted data by combining with the attenuation balance optimization equation. Innovatively and dynamically generate cloud network 5G communication nodes and off network transmission control prime number, update a private key, enable a public key correspond to different private keys on different transmission control nodes, and realize the downlink channel transmission security control under serial interference. Experimental results show that by using this method, the decoding error rate of the edge server reaches below 10^{-8}, reducing the decoding error probability, ensuring that the data will not be tampered or damaged during the transmission process, and the data transmission security control effect is better, which helps to solve the challenges faced by the edge server during the data transmission process, and promote the improvement and development of the edge computing ecology.

Keywords: asymmetric encryption technology; cloud network; 5G communication; downlink channel; transmission security; control methods

收稿日期:2025-03-28； **修回日期**:2025-05-11。
基金项目:广东省教育科学规划课题“新文科背景下艺术类本科生‘LAAA’课程建设—以广州华商学院为例”(2022GXJK377)；2024 年度广东省重点建设学科科研能力提升项目(2024ZDJS108)。
作者简介:龚险峰 1978-),男,博士,副教授。
徐胜超(1980-),男,硕士,副教授。
引用格式:龚险峰,徐胜超.基于非对称加密的云网 5G 通信下行信道传输安全控制[J].计算机测量与控制,2025,33(10):266-272.

0　引 言

云网整合了云计算与网络技术，能够根据动态分配需求，计算并存储资源，实现资源的高效利用。通过分布式架构，能够备份 5G（5G，5th generation mobile communication technology）通信数据，使其在故障时快速恢复，提高通信服务质量[1]。5G 通信是一种高效率、低时延的通信技术，是实现人机交互的重要设施。5G 下行信道是从基站向用户发送信号与数据的通道，能够实现呼叫、短信、数据互传等服务。在 5G 通信网络中，开放性、高速性虽然提高了通信效率，但是也增加了分布式拒绝服务攻击、木马病毒的攻击概率，导致通信数据被恶意窃取。由此目前国内外学者研发了多种传输安全控制方法。

文献［2］提出了基于散射下轨道角动量（OAM，orbital angular momentum）位调制的信道传输安全控制方法，利用 OAM 模式对通信数据进行编码，能够抵抗多模自由基的多重散射效应，实现通信信道的精确数据的安全传输。但该方法受到散射环境的影响，译码时可能出现数据缺失的问题，译码错误概率较高。文献［3］提出了基于 5G 通信的有源配电网线路差动保护实用化整体解决方案，研制出保护装置；但该装置在通信环境中对抗强干扰的能力欠佳，在干扰下出现传输译码错误。文献［4］提出了一种差动保护方法能够适用于 5G 通信，通过优化差动保护逻辑，降低通信延时对动作速度的影响。但多波束通信信道中的重要信号受传播距离影响，存在串行干扰和噪声，增加了信道传输过程中的译码错误概率。文献［5］提出了基于扩频和加密正交频分复用（OFDM，orthogonal frequency division multiplexing）调制的信道传输安全控制方法，在没有背景噪声干扰时，采用空间移位编码正交频分复用（SSE-OFDM，space shift encoding orthogonal frequency division multiplexing）调制提高接收机灵敏度。在不漏电的情况下，抑制窃听者的信噪比，从而实现信道传输控制。但是该方法接收的通信数据众多且分布广泛，密钥管理难度较大，经常出现译码后数据错误。文献［6］研究了基于云计算的 5G 通信信道传输安全控制系统。系统硬件上改装了交换机合路器、均衡器等元件。提取信道传输时频域特征，基于匹配度和信道占用率判断通信信道传输状态，结合云计算技术实现 5G 通信信道传输安全控制。但该方法仅从占用率上优化信道状态，未考虑到串行干扰下的信道衰减情况，导致安全控制后无法降低译码错误。文献［7］提出了基于轻量级密码学和水印与压缩技术的传输信道安全控制方法。估计安全认证协议共享私密信道状态进行。将预编码更新密钥为序列密码，并根据三角顶点变换将彩色图像转换至不同颜色空间，融合 2 级离散小波变换（DWT，discrete wavelet transform）与离散余弦变换（DCT，discrete cosine transform）技术，实现水印的巧妙嵌入，最后通过密钥交换完成信道传输安全控制。但该方法虽然通过水印嵌入更新了密钥提升了信道安全性，但无法使一个公钥在不同传输控制节点上对应不同的私钥，仍造成较高的译码错误率。文献［8］通过实时数字签名提高 5G 无线通信数据传输安全性。定义信道数据实时数字签名完成通信对象的安全认证，重同步密钥，实现 5G 无线通信多层实时网络安全认证，确定加密传输方案。但该方法重同步密钥时，未考虑密钥的动态更新必要性，无法保证信道传输通信数据的安全性。

为了解决现有研究进行信道控制后存在的译码错误率较高，无法保证传输安全性的问题，本文结合非对称加密技术，设计了云网 5G 通信下行信道传输安全控制方法。考虑到散射环境出现串行干扰使得信道出现衰减，影响传输安全性，建立了信道传输衰减平衡方程，动态调整信道传输参数，减少信号衰减，提高信号传输的稳定性和可靠性；并利用非对称加密技术，确保传输数据在信道中的保密性和完整性，为信道传输控制节点生成安全公钥，用于加密传输数据。创新性地动态生成云网 5G 通信节点离网传输控制素数，用于更新私钥，使得一个公钥能够在不同传输控制节点上对应不同的私钥，即使公钥被截获，攻击者也无法轻易解密数据，有效抵抗干扰和攻击，同时减少了因密钥固定或泄露导致的译码错误，提高了数据传输的准确性，确保信道传输通信数据的安全性。

1　5G 通信下行信道非对称加密传输安全控制方法设计

本文设计的 5G 通信下行信道非对称加密传输安全控制方法，控制流程如图 1 所示。

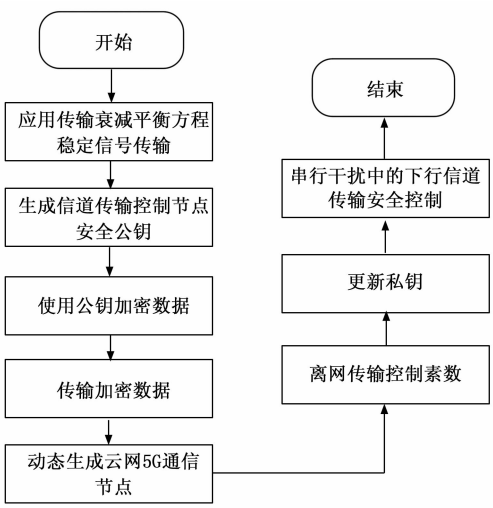


图 1　本文方法的控制流程图

由图 1 可知，本文应用传输衰减平衡方程优化物理层下行信道的信号传输，确保信号在复杂环境中稳定传输，减少信号衰减和干扰传输；利用非对称加密技术生成信道传输控制节点安全公钥，保护应用层数据完整性，使用公钥加密数据并传输；之后动态生成云网 5G 通信节点，适应不同的通信需求或优化网络性能。并在离网环境下更新传输控制素数，更新私钥，实现串行干扰中的下行信道传输安全控制，既解决信道传输的稳定性问题，又解决数据传输的安全性问题，满足 5G 通信的多维度需求。

1.1 5G 通信下行信道传输衰减平衡方程建立

在 5G 通信云网中，下行信道的传输衰减是影响通信信道传输数据安全、可靠的关键因素[9-10]。因此为了优化 5G 通信下行信道传输安全性能，构建一个能够控制信道传输衰减的平衡优化方程，通过该方程动态调整发射功率、调制编码方式等参数，以应对不同的信道条件，从而确保传输的可靠性和效率。这个方程包括通信信道最优控制值、最优控制器的解析解、最优平衡指标等内容。将 5G 通信某下行衰减信道 $x(k)$ 作为控制对象 k，在下行信道的通信状态，u 作为执行器的控制输入，y 为最优控制器。由此构建通信衰减信道结构，如图 2 所示。

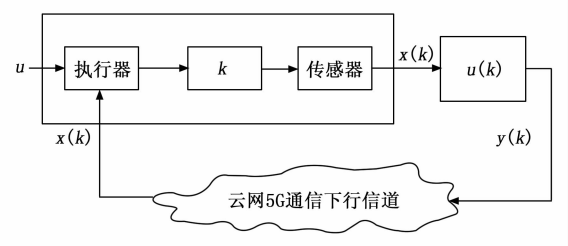


图 2 通信衰减信道结构图

由图 2 可知，云网 5G 通信下行信道存在复杂性与相邻时间之间的跳变相关性[11-12]。在控制对象 k 与控制器中，建立一个可许控制，对任何的 $x(k)$ 均能够最小化处理，能够解决通信信道衰减的问题。在考虑信道的多模态跳变、伴随状态、平衡有限时域以及最优控制器变量等因素的综合作用下，使得某种与信道衰减相关的量的期望为 0，以达到最小化处理通信信道衰减问题的目标，则在最优控制器 y 中的通信下行信道传输数据衰减情况如下：

$$\boldsymbol{E}\left[\boldsymbol{G}_{\theta}\eta(k)\eta y \mid \zeta_{k}\right]=0 \tag{1}$$

$$\eta_{r}=p(T+1)x(k+1) \tag{2}$$

由式（1）、（2）可知，$\boldsymbol{E}$ 为通信状态转移概率矩阵；θ 为通信信道多模态跳变参数，反映信道在不同模态（如不同的通信状态、传输条件）之间跳变特征的参数集合；$\boldsymbol{G}_{\theta}$ 为正半正定矩阵；$\eta(k)$ 为伴随状态；ζ_{k} 为随机变量生成的代数；η 为平衡有限时域；$p(T+1)$ 为通信信道终端状态的惩罚函数；$x(k+1)$ 为 k 相邻对象 $k+1$ 在下行信道的通信状态。

最优平衡方程公式如下：

$$u=\boldsymbol{E}\left[\boldsymbol{G}_{\theta}M_{\theta}x(k)\upsilon\right] \tag{3}$$

$$J_{T}=y=x^{2}M_{\theta} \tag{4}$$

由式（3）、（4）可知，M_{θ} 为 y 的解析解；J_{T} 为最优平衡指标，利用拉格朗日乘数法求解使得性能指标最小化的系统参数和控制策略；υ 为最优控制节点，利用最优控制理论求解使得控制目标最优的控制策略；$x(0)$、M_{θ} 为 $k=0$ 情况下的通信状态、解析解[13]。通过多次 $k=0\sim k=T$ 的叠加，将 0 替换成 $0\sim T$ 任意一个值，得到的 J_{T} 越小，信道传输衰减越弱，能够达到控制下行信道传输衰减的目的。

1.2 基于非对称加密的信道传输控制节点安全公钥生成

5G 通信网络中，受到病毒攻击、数据被恶意窃取的概率不断增加，非对称加密技术的私钥严格保密，仅为密钥拥有者持有，且公钥对应唯一私钥，能够提高通信数据传输的安全性。因此，本文基于非对称加密生成信道传输控制节点安全公钥。非对称加密技术通过特定规则的公钥、私钥，完成云网 5G 通信信息加密任务，公钥与私钥对应，满足下行信道传输安全控制需求[14-16]。

在信道达到理想状态时，生成一对用于加密、解密的公钥、私钥。公钥安全目标博弈如图 3 所示。

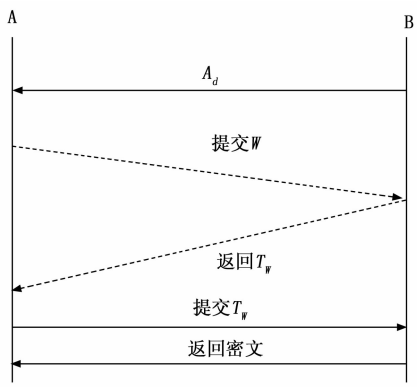


图 3 公钥安全目标博弈示意图

由图 3 可知，返回的 T_{w} 为合适状态，能够输出公钥 A_{d} 的私钥，否则无法获取私钥[17-18]。

基于公钥安全目标博弈流程，采用非对称加密技术进行非对称加密，其中公钥用于加密和验证签名，私钥用于解密和生成签名，共同保障了数据传输的安全性、保密性、完整性和不可抵赖性。非对称加密密钥生成与更新流程如图 4 所示。

由图 4 可知，通过 A 和 B 各自生成一对密钥，包括公钥和私钥。A 使用自己的私钥 $E1$ 对消息 $M1$ 进行

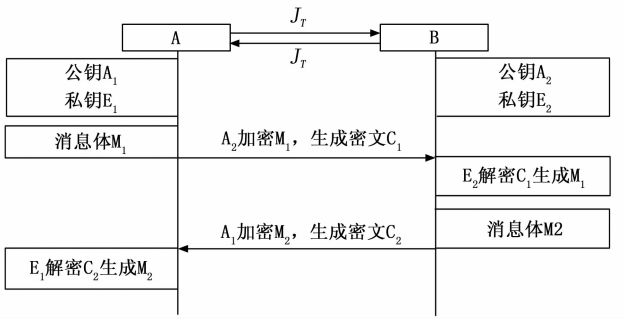


图 4　非对称加密密钥生成与更新流程图

加密，生成密文 $C1$ 的一部分。A 再使用 B 的公钥 $A2$ 对另一部分进行加密，生成完整的密文 $C1$。由于私钥是接收方独有的，其他方无法使用正确的私钥进行解密，这就确保了只有合法的接收方能够获取原始消息，保障了数据的保密性。B 使用自己的私钥 $E2$ 对消息 $M2$ 进行加密，生成密文 $C2$ 的一部分。然后发送方 A 使用自己的私钥对消息 $M1$ 进行签名，生成签名信息。这个签名信息可以随消息一起发送给接收方。由于私钥只有发送方自己拥有，所以签名具有唯一性和不可抵赖性。接收方可以使用发送方的公钥验证签名，从而确认消息的发送者身份以及消息在传输过程中是否被篡改。B 再使用 A 的公钥 $A1$ 对另一部分进行加密，生成完整的密文 $C2$。由于只有 B 拥有与之匹配的私钥，其他任何截获密文 $C1$ 的第三方都无法解密获取原始消息 $M1$，从而保证了数据在传输过程中的机密性。虽然公钥本身不能用于签名，但可以用于验证数字签名。当发送方使用自己的私钥对消息进行签名后，接收方可以使用发送方的公钥来验证签名的有效性。如果验证通过，说明消息确实是由拥有对应私钥的发送方发出的，保证了消息的来源可信和完整性。

在 A 向 B 发送通信数据时，采用 J_T 对发送、接收双方的信道进行衰减平衡控制。随机选择两个大素数 A_q 和 A_m，以增加攻击者通过猜测或分析找到素数的难度，生成安全公钥，计算公式如下：

$$A_d^{'}=\frac{\left|2J_T\left[Exp_p{}^I\Rightarrow A_v(M1,W)\right]-1\right|}{A_m\times A_q} \tag{5}$$

由式（5）可知，W 为关键词；$M1$ 为关于 W 的消息体。$A_d^{'}$ 为下行信道中，传输控制节点向 A 传输的安全控制公钥；A_v 为私钥；Exp_p^I 为安全协议。

1.3　云网 5G 通信节点离网信道传输控制素数更新

公钥与私钥非对称加密时，长时间使用同一个私钥，容易增加私钥被破解的风险，从而影响下行信道传输安全性[19-21]。因此，本文采用离网传输控制素数更新的方式，将密钥信息存储在云端，通过两个素数，更新通信节点离网传输私钥，进一步确保下行信道传输安全性。通信信道素数更新[22-24]公式如下：

$$n=A_q\times A_m \tag{6}$$

$$\kappa(n)=A_d^{'}(A_m-1)\times A_m(A_q-1) \tag{7}$$

由式（6）可知，n 为素数乘积；$A_d^{'}$（A_m）、$A_m(A_q)$ 为对应安全公钥 $A_d^{'}$ 的素数对；$\kappa(n)$ 为加密系数；$A_d^{'}(A_m-1)$、$A_m(A_q-1)$ 为更新后的素数对。在云网网关中，每完成 T 次通信轮次或检测到信道异常时触发更新，根据云网安全认证中心监测的密钥使用周期，从 5G 通信节点数量中找出最大对应的素数对进行自动替换，完成离网传输控制素数的更新任务[25-26]。素数更新完成之后，在云网中进行安全认证，如图 5 所示。

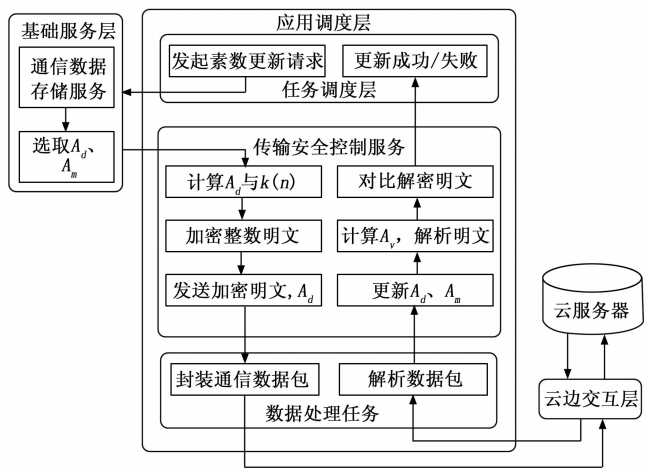


图 5　云网安全认证示意图

由图 5 可知，在非对称加密素数更新完成之后，输入到云网安全认证中心（即云服务器）得到新的 A_v，利用其获得加密、解密后的 5G 通信数据，在云网 5G 通信下行信道传输云边交互层中导出。输出在云边交互层的数据，满足云网 5G 通信下行信道传输数据译码完整性需求。

2　实验验证与性能分析

2.1　实验环境的构造

本次实验主要将安全传输速率、安全等级、译码错误概率等控制结果作为云网 5G 通信下行信道传输安全控制方法进行安全性测试指标。在不同信噪比（SNR，signal-to-noise ratio）环境下，对不同控制方案进行联合对比分析，判断非对称加密技术对信道传输安全的影响。

为实验搭建硬件环境，5G 基站设备采用华为 AAU5613（支持 Sub-6 GHz 频段，Massive MIMO 技术），5G 终端设备为华为 Mate 40 Pro（支持 5G NSA/SA 双模）模拟用户终端，接收下行信道数据。服务器设备采用 Dell PowerEdge R740（2x Intel Xeon Silver 4210，64 GB RAM，1TB SSD）；交换机采用华为 S5735S-L24T4S-A（千兆交换机）；采用 FortiGate 100E

作为防火墙，支持 5G 协议的安全策略。

实验软件操作系统为 Window 10，网络运行采用 Open5GS v2.4.5 模拟 5G 核心网，支持下行信道传输。采用 Wireshark v3.6.5 监控和分析下行信道数据传输，检测译码错误。

将基站通过光纤连接到核心网服务器。核心网服务器通过交换机连接到防火墙和终端。在服务器上安装 Open5GS，配置 AMF、SMF 和 UPF。在服务器上安装 Wireshark，配置网络监控。数据集采用的合法流量来自 Modbus TCP 协议封装（占比 60%）的工业物联网数据和 H.265 编码的 4K 视频切片（占比 40%）的视频流数据，攻击流量采用通过 USRP 捕获的 I/Q 信号（含 30%中间人恶意攻击数据）和伪造的 RRC 连接请求消息，按照 8∶1∶1 的；比例划分训练集，验证集和测试集，其中验证集/测试集中含 20%恶意样本。

通过数据清洗去除 RTP 序列号不连续的数据包，过滤 RSSI＞－30 dBm 的非法信号。提取数据包头信息，如源地址作为加密密钥生成的辅助特征。选择数据包负载的熵值，衡量数据随机性，作为加密强度调整的依据。通过加性高斯白噪声拟不同信噪比环境，高 SNR（20 dB）模拟近基站用户，信道质量良好。中 SNR（15 dB）模拟中距离用户，存在一定干扰。低 SNR（0 dB）模拟边缘用户，信号较弱。

在上述实验环境中输入 QiFang Mini Digital Pickup Camera 的视频通信数据，输出格式为 PAL。采用基于散射下 OAM 相位调制的安全控制方法（文献［2］方法）和基于轻量级密码学和水印与压缩技术的传输安全控制方法（文献［7］方法）为对比方法，其中轻量级密码学控制方法的密钥长度设置为 256 位，认证标签为 128 位，数字水印采用 DCT 域低频系数调制的嵌入方式，水印容量为每数据包 16 比特，可抵抗 3%以下的随机丢包。采用 LZMA 压缩算法，压缩率为平均 1∶1.8（文本数据）；OAM 相位调制控制方法的轨道角动量采用拓扑荷数 $l=\pm 3$ 的涡旋波束，调制深度为 $\pi/2$ 弧度，符号速率为 1 Gbaud，反射面数量为 3 个，信道相关性为 0.35。

在 Window 下串口波特率为 115 200 bit/s 时，下行信道总发送量为 3 012 987 bit，持续时间为 322 s，发送速率为 9.12 k/s，能够满足本次实验需求。实验相关参数，如表 1 所示。

由表 1 可知，下行信道发送分组总数为 1 000，分组发送量为 275 B，发送速率为 7.61 kbps，接收分组总数为 789，接收耗时为 36 735 ms，到达速率为 5.12 m/s。由此可见，下行信道传输丢失了部分数据，影响后续使用。因此，通过非对称加密技术，对下行信道发送数据进行安全加密传输控制，使其达到理想接收量上限。

表 1 实验参数列表

参数	取值
载频	2.0 GHz
带宽	10 MHz
DCI format	0/1A(29 bits,不含 CRC)，2C(45 bits,不含 CRC)
聚合等级	1 PRB
天线配置	8＊2,±45°双极化,间距 0.5λ
信道模型	ITU Uma LOS/NLOS
信道估计	真实信道估计
传输资源	PRB 集合{＃0,＃6,＃12,＃18,＃24,＃30,＃36,＃42}的子集
下行信道噪声功率	$\sigma_1^2=5;\sigma_2^2=9$
云端服务器发送功率	P=8

2.2 信道传输安全等级实验

在不同信噪比条件下，通过安全系数分析下行信道传输安全等级，并分析安全系数随通信轮次变化的曲线，其中，安全系数的计算公式如下：

$$S=\frac{C_e}{C_a} \tag{8}$$

由式（8）可知，S 为安全系数，表示通信系统在安全传输方面的保障程度。其值介于 0～1 之间，值越接近 1 说明通信的安全性越高；C_e 为安全通信容量，信道能够可靠传输的信息速率；C_a 为总通信容量，是信道在不考虑安全因素时理论上能够传输的最大信息速率。

信噪比为 10 dB 与 15 dB 的安全系数如图 6 所示。

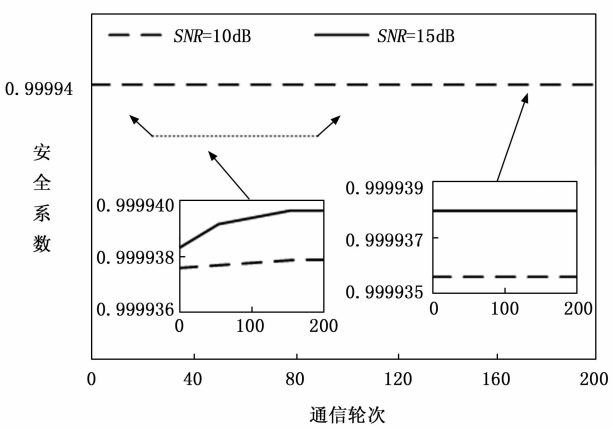


图 6 信道传输安全等级曲线变化图

由图 6 可知，在云网 5G 通信下行信道传输安全控制过程中，安全系数几乎恒定，无限接近于“1”，并未出现随着通信轮次增加而降低的情况，结合非对称加密技术，通过定期更新密钥对（公钥和私钥）确保传输的安全性。能够得到这样的结果原因是每隔一定的通信轮次则重新生成新密钥对，攻击者即使获取旧密钥，也无法解密后续的通信数据。此时，安全系数在通信轮次增加的过程中能够保持通信信道的环境较为稳定且波动较

小，能够更好的保证传输的安全。

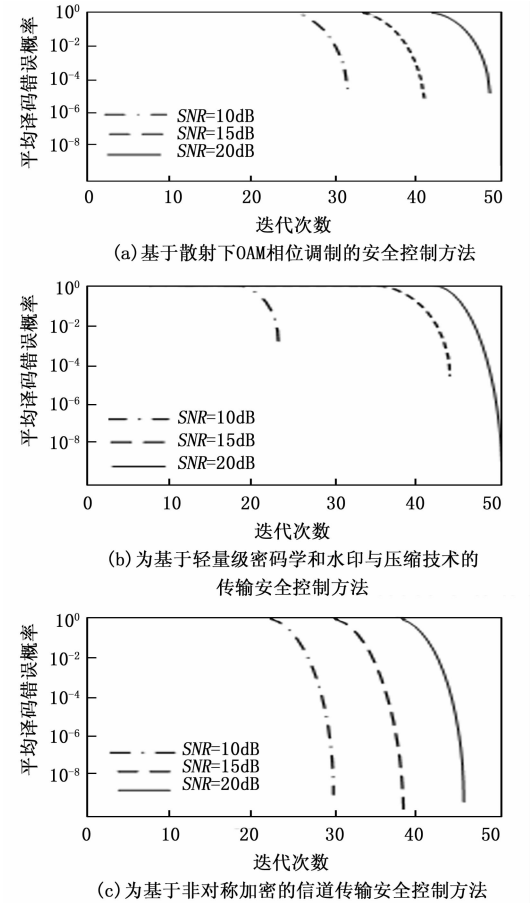
2.3　信道传输译码错误实验

在不同信噪比环境下（*SRN* 为 10 dB、15 dB、20 dB）进行信道传输后，采用公式（9）计算译码错误率，计算公式如下：

$$B_{ER}=\frac{N_e}{N_a} \tag{9}$$

由式（9）可知，N_e 为错误比特数，即经过译码后，接收端判断为错误的比特数量；N_a 为传输的总比特数。

应用公式（9）计算 3 种方法的译码错误率情况，每组信噪比条件下重复 10 次实验，得到 3 种方法的平均译码错误率如图 7 所示。



(a)基于散射下OAM相位调制的安全控制方法

(b)为基于轻量级密码学和水印与压缩技术的传输安全控制方法

(c)为基于非对称加密的信道传输安全控制方法

图 7　译码错误概率变化曲线图

本次实验在使用非对称加密技术对数据进行加密处理后，数据会以密文的形式传输。相对于原始数据密文具有更强的抗干扰性，即使传输过程中有误，由于密钥的保密性，攻击者很难通过错误获取信息及篡改。接收数据后使用正确的私钥进行解密，仍能正确还原出原始数据。在最终的控制结果中，边缘服务器译码错误概率在迭代 50 次之内，均能够达到 10^{-8} 以下，错误概率较低，传输过程中数据仍能保持原始状态，未被篡改或损坏。由此可见，使用基于非对称加密技术的信道传输安全控制方法，能够减少数据被损坏的次数，确保数据传输前后，均能够保持原始状态，对于提高通信信道传输安全性具有重要作用。

然而非对称加密依赖公钥基础设施（PKI）体系，基站需为每个终端动态分配临时公钥时，在 5G 海量终端接入场景下，公钥证书的生成、分发和验证过程需要消耗大量网络资源，可能导致信令风暴，增加计算延迟。未来研究将在保证密钥安全性基础上，构建分层密钥管理架构，在核心网部署轻量化 PKI 服务，采用国密 SM2/9 算法降低计算开销，同时结合区块链技术实现公钥证书的分布式存证与验证。在基站侧引入密钥缓存机制，预生成短期公钥池以减少实时生成资源压力，降低延迟。

3　结束语

本文设计了基于非对称加密技术的云网 5G 通信下行信道传输安全控制方法。通过抑制下行信道传输衰减情况，估计传输路径的损耗，在云网 5G 通信下行信道传输安全控制过程中，安全系数无限接近于 1 时，能够确保通信信道传输安全性；引入非对称加密技术，将公钥对应唯一的私钥，并以实时更新素数的形式，更新下行信道传输安全私钥，最终边缘服务器译码错误概率在迭代 50 次之内，均能够达到 10^{-8} 以下，数据在传输过程中仍能保持原始状态，安全传输数据的效果较好。

但是本文方法仍具有一定的局限性，如未考虑在不同通信场景，如城市密集区、农村开阔区下的信道特性、干扰源和信号衰减的各异情况，可能会影响衰减平衡优化方程的有效性和加密密钥的适应性，导致通信性能变差；未来的研究可以针对不同通信场景，研究自适应的衰减平衡优化方程和加密密钥生成策略，提高方法的泛化能力。结合机器学习和人工智能技术，对信道特性进行预测和建模，优化加密和解密过程，提高 5G 通信网络的整体性能。

参考文献：

[1] WANG C M，XU W，PANG C，et al. Wearable full-textile spoof surface Plasmon polariton transmission line for secured communication in wireless body area network [J]. Plasmonics，2024，19 (5)：2705－2713.

[2] LIU Z，ZHANG B，HENG K，et al. Multi-channel data transmission through a multimode fiber based on OAM phase encoding [J]. Optics Letters，2023，48 (21)：5615－5618.

[3] PU H F，WU T H，YAO G，et al. Practical scheme of line differential protection for active distribution network based on 5G communication [J]. Automation of Electric Power Systems，2022，46 (23)：117－124

[4] ZOU X F，SHEN B，JIANG X W. A quick action scheme

of differential protection for a distribution network with 5G communication [J]. Power System Protection and Control, 2022, 50 (16): 163 - 169.

[5] ZHANG J, GAO G, ZHANG J, et al. Secure and noise-resistant underwater wireless optical communication based on spectrum spread and encrypted OFDM modulation [J]. Optics Express, 2022, 30 (10): 17140 - 17155.

[6] ZHOU L. Design of 5G Communication channel transmission control system based on cloud computing [J]. Computer Measurement & Control, 2024, 32 (10): 125 - 131.

[7] NAZARI H, BIDGOLI M M, GHASVARI H. Integration of lightweight cryptography and watermarking with compression for high speed and reliable communication of digital images in IoT [J]. IET Image Processing, 2023, 17 (10): 2984 - 3001.

[8] NAN S, ZHONG Z G, CHEN R X, et al. Multi-layer real-time network data encryption transmission method based on 5G wireless communication [J]. Electronic Design Engineering, 2024, 32 (23): 57 - 60.

[9] ANASTASOV J, CVETKOVI A, PANAJOTOVI A, et al. Physical layer security of ground-to-UAV communication in the presence of an aerial eavesdropper outside the guard zone [J]. Wireless Personal Communications, 2024, 138 (3): 1597 - 1614.

[10] SHEBA M A A, MANSOUR D E A, ABBASY N H H. A new low-cost and low-power industrial internet of things infrastructure for effective integration of distributed and isolated systems with smart grids [J]. IET Generation, Transmission & Distribution, 2023, 17 (20): 4554 - 4573.

[11] JEBRANE J, LAZAAR S. An enhanced and verifiable lightweight authentication protocol for securing the Internet of medical things (IoMT) based on CP-ABE encryption [J]. International Journal of Information Security, 2024, 23 (6): 3691 - 3710.

[12] PULLIGILLA M K, VANMATHI C. An energy efficient access control for secured intelligent transportation system for 6G networking in VANET [J]. Peer-to-Peer Networking and Applications, 2024, 17 (6): 3618 - 3633.

[13] ZHENG X, LIU Y, ZHAN S, et al. A novel low-latency scheduling approach of TSN for multi-link rate networking [J]. Computer Networks, 2024, 240 (2): 1 - 10.

[14] LIU S, TANG P, ZHANG J, et al. Statistical channel modeling for indoor VLC communications based on channel measurements [J]. China Communications, 2024, 21 (1): 131 - 147.

[15] FREITAS M B J M D, FREITAS J M D, JOLYON M, et al. Shannon-hartley channel capacity for underwater wireless optical communications [J]. ACS Photonics, 2024, 11 (3): 866 - 873.

[16] LIU Y, LI M, HAN L T X. Information-theoretic limits of integrated sensing and communication with correlated sensing and channel states for vehicular networks [J]. IEEE Transactions on Vehicular Technology, 2022, 71 (9): 10161 - 10166.

[17] ANDRIANOV M N, KORBAKOV D A, POZIDAEV V N. Error probabilities in the millimeter-wave channel in the spacecraft-ground tracking station communication line taking into account arctic climatic conditions [J]. Bulletin of the Lebedev Physics Institute, 2022, 49 (8): 266 - 270.

[18] CHENG Y X, YANG M, LU Z J, et al. Time transfer over 113 km free space laser communication channel [J]. Optics Express, 2024, 32 (7): 12645 - 12655.

[19] KOU L, ZHANG J, ZHANG Y H F. Composite channel modeling for underwater optical wireless communication and analysis of multiple scattering characteristics [J]. Optics Express, 2023, 31 (7): 11320 - 11334.

[20] LI X, LU T, SONG P. Transmission characteristics of the rough surface scattering channel for wireless ultraviolet communication in a cemented ground scenario [J]. Applied Optics, 2023, 62 (17): 4591 - 4599.

[21] ANDRIANOV M N. Efficiency of relay communication in the millimeter wave channel in the spacecraft-ground tracking station data transmission line [J]. Bulletin of the Lebedev Physics Institute, 2023, 50 (7): 274 - 278.

[22] ISMAIL A, MOHAMEDPOUR K. Performance study of HF communication using NOMA over narrowband HF channel [J]. IET Communications, 2023, 17 (14): 1683 - 1690.

[23] PICALLO I, ITURRI P L, FALCONE A F. Deterministic wireless channel characterization towards the integration of communication capabilities to enable context aware industrial internet of thing environments [J]. Mobile Networks & Applications, 2023, 28 (1): 4 - 18.

[24] ALMUSTAFA K M, EISA T A E, AMANI A, etal.. qos aware multicast routing protocol for video transmission in smart cities [J]. Computers, Materials & Continua, 2022, 72 (1): 2483 - 2499.

[25] VIJAYA M T, RAVISHANKAR K C, RAGHU M E. Selective encryption of video frames using the one-time random key algorithm and permutation techniques for secure transmission over the content delivery network [J]. Multimedia Tools and Applications, 2024, 83 (35): 82303 - 82342.

[26] CHEN Z, LIU F, LI D, et al. Video security in logistics monitoring systems: a blockchain based secure storage and access control scheme [J]. Cluster Computing, 2024, 27 (8): 10245 - 10264.