Hans Journal of Wireless Communications 无线通信, 2026, 16(3), 48-58
Published Online June 2026 in Hans. https://www.hanspub.org/journal/hjwc
https://doi.org/10.12677/hjwc.2026.163005

Hans汉斯

基于协作NOMA系统的物理层安全性能研究

刘家康，王俊利，马卓凡，任　薇，张文博，徐元丰，朱大磊

郑州师范学院物理与电子工程学院，河南　郑州

收稿日期：2026年5月26日；录用日期：2026年6月19日；发布日期：2026年6月29日

摘　要

针对协作非正交多址接入(Non-Orthogonal Multiple Access, NOMA)系统的物理层安全传输需求，本文提出一种基于解码转发(DF)与修改转发(MF)的自适应中继安全传输算法。首先构建包含发射端、中继节点、合法强弱用户及窃听者的协作NOMA系统模型，并推导信干噪比、保密容量及保密中断概率等关键性能指标的解析表达式。在此基础上，设计可根据实时信道状态动态切换转发模式的自适应策略，最终实现系统安全传输概率的最大化。仿真结果表明，相比传统正交多址接入系统与单一DF协议NOMA系统，所提自适应算法在全功率范围内实现了更低的保密中断概率；特别是在高发射功率(>25 dBm)阶段，该算法成功突破传统DF协议的安全容量瓶颈，使得安全传输概率持续攀升，有效提升了协作NOMA系统的物理层安全性能。

关键词

非正交多址接入，物理层安全，协作中继，自适应转发，保密中断概率

Research on Physical Layer Security Performance of Cooperative NOMA Systems

Jiakang Liu, Junli Wang, Zhuofan Ma, Wei Ren, Wenbo Zhang, Yuanfeng Xu, Dalei Zhu

School of Physics and Electronic Engineering, Zhengzhou Normal University, Zhengzhou Henan

Received: May 26, 2026; accepted: June 19, 2026; published: June 29, 2026

Abstract

To address the physical layer secure transmission requirements of cooperative non-orthogonal multiple access (NOMA) systems, this paper proposes an adaptive relay secure transmission algorithm based on decode-and-forward (DF) and modify-and-forward (MF) protocols. First, a cooperative

文章引用: 刘家康, 王俊利, 马卓凡, 任薇, 张文博, 徐元丰, 朱大磊. 基于协作 NOMA 系统的物理层安全性能研究[J]. 无线通信, 2026, 16(3): 48-58. DOI: 10.12677/hjwc.2026.163005

NOMA system model comprising a transmitter, a relay node, legitimate strong and weak users, and an eavesdropper is established. Subsequently, analytical expressions for key performance metrics, including the signal-to-interference-plus-noise ratio, secrecy capacity, and secrecy outage probability, are derived. Building upon this, an adaptive strategy is designed to dynamically switch forwarding modes according to real-time channel state information, ultimately maximizing the secure transmission probability of the system. Simulation results demonstrate that, compared to traditional orthogonal multiple access systems and single DF-protocol NOMA systems, the proposed adaptive algorithm achieves a lower secrecy outage probability across the entire transmit power range. Particularly in the high transmit power regime (> 25 dBm), the algorithm successfully overcomes the secrecy capacity bottleneck inherent in traditional DF protocols, enabling a continuous increase in secure transmission probability and effectively enhancing the physical layer security performance of cooperative NOMA systems.

Keywords

Non-Orthogonal Multiple Access, Physical Layer Security, Cooperative Relaying, Adaptive Forwarding, Secrecy Outage Probability

Copyright © 2026 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

第五代移动通信技术规模化商用已全面落地，但海量物联网设备的爆发式接入，让本就稀缺的无线频谱资源陷入了严重的供需缺口。非正交多址接入[1] (Non-Orthogonal Multiple Access, NOMA)作为 5G 的关键技术之一，在提升频谱效率方面展现出显著优势。然而，NOMA 的共享机制也带来了新的安全隐患，信号在空口中广播传输，窃听者可以利用多用户检测手段截获机密信息。传统的加密方法依赖复杂的密钥分发与管理，但大量低功耗物联网终端计算能力弱、电池寿命有限，难以承载这类高开销的安全机制[2]。物理层安全(Physical Layer Security, PLS)技术[3]不依赖传统加密，而是利用无线信道的衰落、噪声和干扰等固有物理特性来保障合法通信，天然适配资源受限的物联网设备。协作中继技术则可以有效对抗信道衰落、延伸网络覆盖范围。将协作中继引入 NOMA 系统，不仅能够改善边缘用户的通信质量，也为物理层安全创造了额外的设计自由度。

近年来，学术界围绕协作 NOMA 系统的物理层安全展开广泛研究，其核心技术路线可归结为传输协议改进与辅助增强策略两类。在传输协议层面，除了对传统的解码转发(Decode and Forward, DF) [4]和放大转发(Amplify and Forward, AF) [5]协议进行保密性能分析外，修改转发(Modify and Forward, MF) [6]协议作为一种进阶方案被提出。该协议通过在中继节点主动修改信号特征，有效扩大合法用户与窃听者之间的信道差异，提升基础防御能力。在辅助增强策略层面，现有方案多利用空间自由度或外部干扰来进一步压制窃听能力，例如，通过中继发送人工干扰配合接收端 SIC 技术降低保密中断概率[7]，或者利用多候选中继选择[8]、机会调度与功率分配等系统级优化手段[9]，最大化合法传输链路的优势。

综上，为提升协作 NOMA 系统的安全传输性能，本文提出一种基于信道状态自适应切换解码转发(DF)与修改转发(MF)模式的中继算法[10]。研究过程中，首先建立由发射端、中继、多用户(强/弱)及窃听方构成的物理层安全模型，并严格推导保密容量、中断概率等关键性能的闭合表达式。最终，通过引入基于实时信道状态的动态决策机制，有效实现系统整体安全传输概率的最大化。

2. NOMA 系统物理层安全理论与技术基础

2.1. 非正交多址接入技术

非正交多址接入技术是第五代移动通信系统的核心多址接入技术之一，能够显著提升系统频谱效率并降低传输时延。传统正交多址接入[11]技术通过正交的时频资源块为不同用户分配专属通信资源，保证用户间无正交域内的相互干扰，但该机制会导致频谱资源利用率受限。与之不同，NOMA 技术采用非正交的资源分配方式[12]，允许多个用户在同一时频资源块上同时传输数据，通过功率域的信号叠加实现多用户区分。其设计原则为，信道条件[13]越差，分配功率越高，通过差异化功率分配保障弱信道用户的通信质量，实现系统整体性能与用户公平性的平衡。

考虑典型的双用户下行 NOMA 传输场景，包含一个信道条件较好的近端用户(强用户)和一个信道条件较差的远端用户(弱用户)。设基站总发射功率为 P，分配给近端用户的功率因子为 a_1，分配给远端用户的功率因子为 a_2，满足归一化约束 $a_1 + a_2 = 1$。为保障远端用户的可靠通信，功率分配需满足 $a_2 > a_1$。

基站采用叠加编码(SC)技术[14]生成发送信号，其表达式为：

$$x = \sqrt{a_1 P}x_1 + \sqrt{a_2 P}x_2 \tag{1}$$

其中，x_1 为近端用户的发送符号，x_2 为远端用户的发送符号。如图 1 所示，接收端在收到这个混合信号后，需要使用连续干扰消除(SIC)技术[15]来分出正确的信号。

接收端通过连续干扰消除(SIC)技术实现多用户信号的分离：首先解码功率较高的远端用户信号，将其从接收叠加信号中完全剔除后，再解码功率较低的近端用户信号。SIC 技术不仅能够有效解决多用户共享时频资源带来的同频干扰问题[16]，大幅提升系统频谱效率与接入容量，同时也为物理层安全性能的增强提供了技术基础。

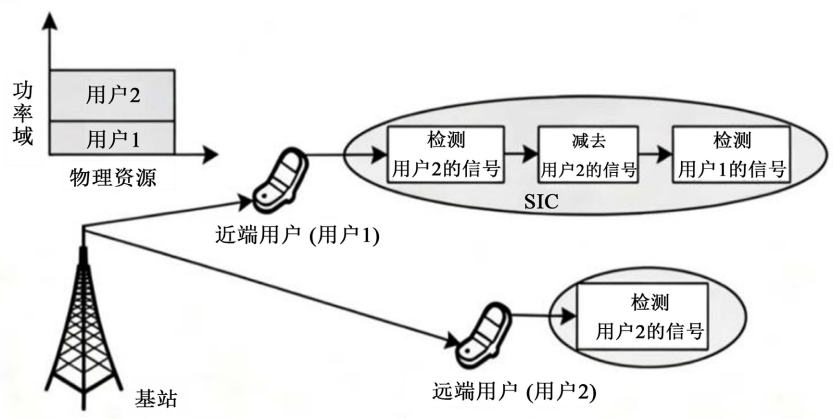

Figure 1. Schematic diagram of the basic principle of power-domain NOMA
图 1. 功率域 NOMA 基本原理示意图

2.2. 物理层安全传输原理

物理层安全(PLS)是一种新兴的无线通信安全防护机制，能够有效缓解无线网络面临的安全威胁，且无需依赖传统复杂的密码学算法。当前物联网终端普遍存在计算能力有限、电池容量低的硬件约束，传统加密技术的高计算开销和能耗需求难以适配这类资源受限设备，而物理层安全技术恰好能够解决这一矛盾。

该技术的核心思想是充分利用无线信道的固有物理特性实现安全传输[17]。无线信号在传播过程中

不可避免地会经历衰落、干扰和噪声，合法接收端与窃听端所处的无线信道环境存在天然差异。系统通过利用这种信道差异性，在保证合法用户可靠接收信号的同时，使窃听者因接收信号质量严重下降而无法正确解调信息。例如，系统可通过自适应功率分配策略，针对性地降低窃听端的接收信噪比，从而实现信息的安全传输。

物理层安全性能通常由两个指标进行量化评估：

一是保密中断概率，表示系统发生信息泄露事件的概率，其数值越小，系统的安全可靠性越高：

$$P_{out} = Pr\left(\log_2 \frac{1+\gamma_b}{1+\gamma_e} < R_s\right) \tag{2}$$

其中，γ_b 表示合法接收端信噪比，γ_e 表示窃听者信噪比；

二是安全吞吐量，指系统在保证绝对安全传输的前提下，能够实现的最大有效数据传输速率：

$$ST = R_S \cdot (1 - P_{out}) \tag{3}$$

其中，R_s 表示系统预设的目标保密传输速率。

2.3. 协作中继安全工作原理

协作中继技术是提升无线通信系统传输性能的关键技术。无线信号在远距离传输或穿越障碍物时，会遭受严重的路径损耗和多径衰落，导致接收端信号质量显著下降。协作中继技术[18]的基本思想是在源节点与目的节点之间引入中继节点，源节点首先将信号发送至中继节点，中继节点对信号进行相应处理后，再将其转发至目的节点。该机制能够有效补偿无线信道的传输损耗，显著扩展通信覆盖范围并提升系统可靠性。近年来的研究表明，结合缓存机制的协作非正交多址接入(NOMA)方案，能够进一步改善系统的物理层安全性能。

根据信号处理方式的不同，中继节点主要分为三类：第一类是放大转发(AF)中继，中继节点对接收到的信号仅进行线性放大处理后直接转发，其实现复杂度低、处理时延小(图 2)。

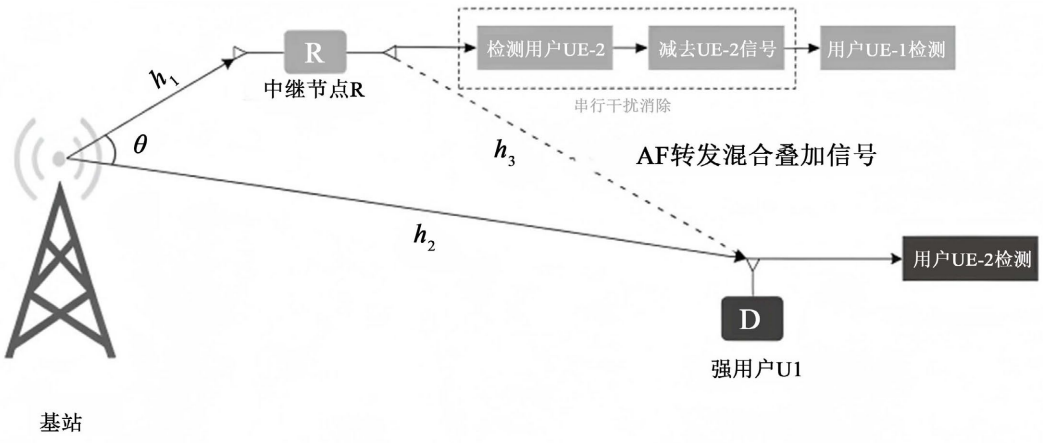

Figure 2. NOMA-based AF relay cooperative system model
图 2. 基于 NOMA 的 AF 中继协作系统模型

第二类是解码转发(DF)中继，中继节点首先对接收信号进行解码和纠错，去除噪声干扰后，再重新编码并转发至目的节点。该方案能够有效抑制噪声累积，提升传输可靠性，但计算复杂度较高，处理时延相对较大(图 3)。

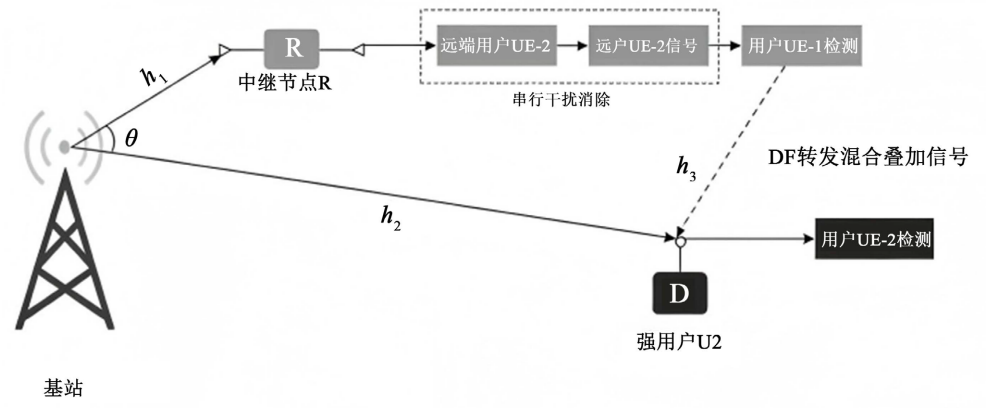

Figure 3. NOMA-Based DF relay cooperative system model
图 3. 基于 NOMA 的 DF 中继协作系统模型

第三类是修改转发(MF)中继，作为解码转发方案的进阶型，其核心思想是中继节点在完成解码重编后，并不直接转发原信号，而是将总发射功率按照特定比例划分为两部分：一部分用于发送有用的机密信号，另一部分用于发送人工噪声。通过信道状态信息，中继可将人工噪声精准投射到窃听信道方向，或利用预共享密钥使合法用户消除该噪声，从而在物理层面人为拉大合法信道与窃听信道的容量差，实现对窃听者的强力压制(图 4)。

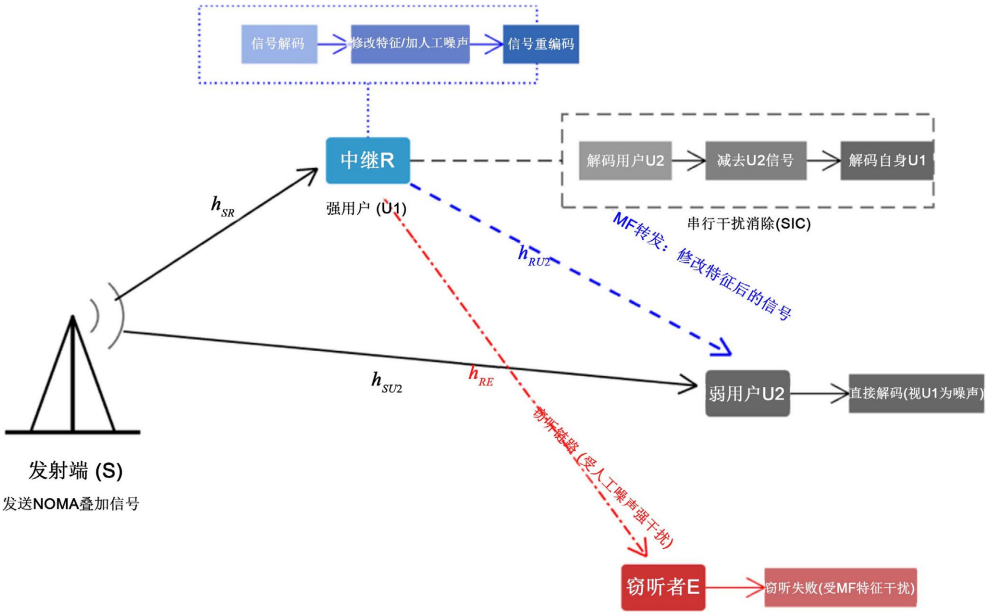

Figure 4. NOMA-Based MF relay cooperative system model
图 4. 基于 NOMA 的 MF 中继协作系统模型

3. 基于自适应转发的协作 NOMA 安全传输算法

3.1. 系统模型建立

协作 NOMA 系统物理层安全传输模型如图 5 所示，该网络拓扑结构包含一个发射端(S)、一个半双工中继节点(R)、两个合法接收用户以及一个窃听者(E)，在两个合法用户中，定义距离发射端较近、信道

条件较好的为强用户(U_1)，距离发射端较远、信道条件较差的为弱用户(U_2)。

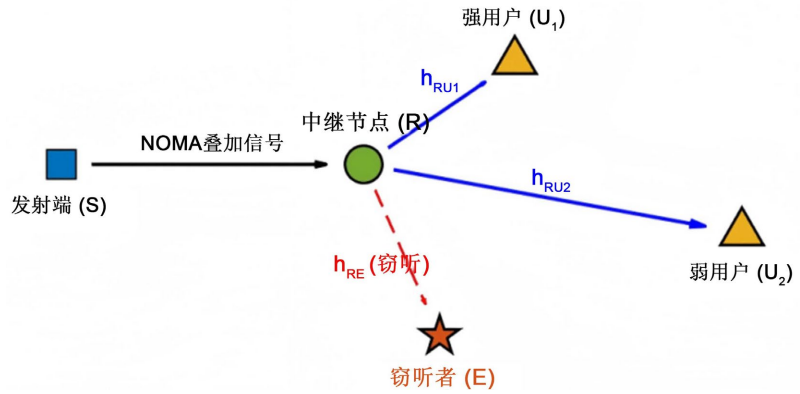

Figure 5. Physical layer secure transmission model of cooperative NOMA system
图 5. 协作 NOMA 系统物理层安全传输模型

假设网络中的所有通信节点均只配置单根天线，且系统运行在半双工模式下，系统中的所有无线通信链路均经历相互独立的瑞利(Rayleigh)平坦衰落，且环境背景中持续存在均值为零、方差为 N_0 的加性高斯白噪声(AWGN)干扰。

发射端采用 NOMA 技术将发往两个用户的信号在功率域进行叠加编码。设基站的总发射功率为 P_S，分配给强用户 U_1 的功率占比为 a_1，分配给弱用户 U_2 的功率占比为 a_2。为了保障远端弱用户的可靠通信质量，功率分配因子需满足 $a_1 + a_2 = 1$ 且 $a_2 > a_1$ 的约束条件。发射端 S 广播的叠加信号 x_S 可表示为：

$$x_S = \sqrt{a_1 P_S}\, x_1 + \sqrt{a_2 P_S}\, x_2 \tag{4}$$

其中，x_1 和 x_2 分别代表需要发送给强用户和弱用户的有用信息符号，且假定均为单位能量信号。

信号经过无线空间传播后，中继节点 R 接收到的信号为：

$$y_R = h_{SR} x_S + n_R \tag{5}$$

h_{SR} 代表从发射端 S 到中继节点 R 链路的信道衰落系数，包含大尺度路径损耗与小尺度瑞利衰落；n_R 代表中继节点处接收机的加性高斯白噪声。中继节点在接收到该信号后，将进行后续的算法处理并准备转发，而在此过程中，窃听者 E 始终尝试拦截并破译在空间中传输的无线信号。

3.2. 自适应中继安全传输算法分析

为了在存在非法窃听者的复杂环境中达到较优的安全性，本节设计一种自适应中继传输算法。该算法允许中继节点根据当前的信道环境状态，自动在解码转发(DF)和修改转发(MF)协议之间进行动态切换。

在使用 DF 协议时，中继节点先对接收到的混合信号进行解码，去除信号中的噪声干扰后，直接重新编码并进行广播转发。然而，这种清晰的重构信号也极易被窃听者截获。MF 协议作为 DF 协议的进阶升级版，其主导思想是中继节点在重新编码之前，结合信道状态信息特意改变信号的相位或附加特征。这种修改能够人为拉大合法信道和窃听信道的接收差异，从而强力干扰窃听者的解码过程，提升物理层安全。

在本文所提的自适应算法中，当系统判定需切换至 MF 模式时，中继节点 R 的发送信号不再是纯净的叠加信号，而是叠加了人工噪声的复合信号。设中继总发射功率为 P_R，功率分配比例因子为 $\phi\,(0 < \phi \le 1)$，则中继在 MF 模式下的发送信号 $x_{R,MF}$ 的数学模型可表示为：

$$x_{R,MF}=\sqrt{\phi P_R}x_S+\sqrt{(1-\phi)P_R}\omega \tag{6}$$

其中，x_S为解码重编后的 NOMA 有用信号；ω为中继产生的人工噪声信号，满足$E\left[|\omega|^2\right]=1$。本文假设中继节点与合法接收端之间存在安全的伪随机种子共享机制，使得强、弱用户在接收端能够凭借先验信息将人工噪声ω完全对消；而窃听者 E 缺乏该伪随机序列，只能将其视作不可消除的同频干扰。

在中继节点处理并转发信号(进入第二传输阶段)后，合法用户端开始进行解码。强用户 U_1 采用连续干扰消除(SIC)技术，首先解码分配功率较高的弱用户信号 x_2 并将其从混合信号中减去，随后再解码自身的信号 x_1。在理想 SIC 条件下，强用户解码自身信号的信干噪比为：

$$\gamma_{U1}=\frac{P_R|h_{RU1}|^2a_1}{N_0} \tag{7}$$

P_R代表中继节点的发射功率，h_{RU1}代表中继节点到强用户 U_1 的信道衰落系数。

对于弱用户 U_2，由于分配给强用户 x_1 的功率较低，它无法消除这部分干扰，只能将其视作底噪的一部分直接进行解码。因此，弱用户的信干噪比为：

$$\gamma_{U2}=\frac{P_R|h_{RU2}|^2a_2}{P_R|h_{RU2}|^2a_1+N_0} \tag{8}$$

h_{RU2}为中继到弱用户 U_2 的信道衰落系数。

窃听者 E 在同一时隙内尝试拦截中继转发的叠加信号。假设窃听者具备与强用户类似的多用户检测与解码能力，其尝试破译信息的信干噪比上限可表示为：

$$\gamma_E=\frac{P_R|h_{RE}|^2}{N_0} \tag{9}$$

h_{RE}为中继节点到窃听者 E 之间的信道衰落系数。

由于合法用户可完全消除人工噪声，其在 MF 模式下的信干噪比与 DF 模式结构类似，仅等效发送功率由 P_R 缩减为 ϕP_R。然而，对于窃听者 E，其在拦截 MF 转发信号时，不仅面临强用户信号的干扰，还必须承受人工噪声带来的毁灭性压制。其在 MF 模式下尝试破译弱用户信息的信干噪比上限被极大地限制为：

$$\gamma_{E,MF}=\frac{\phi P_R|h_{RE}|^2a_2}{\phi P_R|h_{RE}|^2a_1+(1-\phi)P_R|h_{RE}|^2+N_0} \tag{10}$$

上式分母中的$(1-\phi)P_R|h_{RE}|^2$，即为人工噪声干扰项。正是该项的存在，使得无论发射功率如何增加，窃听者的信干噪比都会受到严重制约，从而从数学机理上打破了传统 NOMA 系统的安全容量瓶颈。

根据香农定理，合法多用户系统的等效信道容量 C_m 受限于瓶颈用户的传输速率，即$C_m=\log_2\left(1+\min\left(\gamma_{U1},\gamma_{U2}\right)\right)$，而窃听者的信道容量为$C_e=\log_2\left(1+\gamma_E\right)$。

系统的总体保密容量 C_s 定义为合法用户的信道容量减去窃听者的信道容量，若差值小于零则记作零。保密容量的闭合表示如下，其中，$[x]^+$表示 $\max(x, 0)$：

$$C_s=\left[C_m-C_e\right]^+ \tag{11}$$

保密中断概率(SOP)是衡量系统安全可靠性的最关键指标，它是指系统的实际保密容量 C_s 低于预先设定的目标安全速率 R_s 的概率，该数字越小，系统抵御窃听的能力越强、越安全。保密中断概率的理论定义式为：

$$P_{out} = P\left(C_s < R_s\right) \tag{12}$$

同时，与之对应的安全传输概率(SPS)表示系统能够安全、成功完成数据传输的概率，可推导为：

$$P_{sps} = 1 - P_{out} \tag{13}$$

基于前文构建的系统数学模型与保密性能分析框架，本文所提 DF/MF 智能切换自适应中继算法的执行逻辑与实现流程如下：在数据传输的相干时间块内，中继节点首先获取合法信道(h_{RU1}, h_{RU2})与窃听信道(h_{RE})的状态信息估计。随后，将状态代入公式计算采用普通 DF 协议时的预期保密容量 $C_{s,DF}$ 以及引入相位特征修改后采用 MF 协议的预期保密容量 $C_{s,MF}$ 中继系统最终以最大化安全传输概率为目标，自适应输出决策指令，选择 max($C_{s,DF}$, $C_{s,MF}$)对应的中继模式进行信号转发。

4. 仿真验证与结果分析

4.1. 仿真环境搭建与参数设定

仿真模型考虑一个典型的下行协作 NOMA 通信场景，其中包含发射端、中继节点、强弱用户及一个不可信的窃听者。设定无线链路均遵循瑞利衰落分布，并伴随加性高斯白噪声。为了量化评估系统的安全性能，设定表 1 所示的基准参数。

Table 1. Collaborative NOMA system simulation parameter setting table
表 1. 协作 NOMA 系统仿真参数设置表

参数名称	符号表示	数值设定	备注
仿真迭代次数	N	105	蒙特卡洛实验规模
发射功率范围	P_S	0~30 dBm	系统主自变量
目标安全速率	R_s	1.0 bit/s/Hz	业务需求门限
功率分配因子	a_1，a_2	0.25，0.75	遵循 $a_2 > a_1$ 原则
路径损耗指数	α	3.0	典型城市场景
噪声功率谱密度	N_0	−90 dBm	环境底噪

4.2. 系统安全性能的多维度仿真分析

4.2.1. 发射功率对保密中断概率(SOP)的动态影响

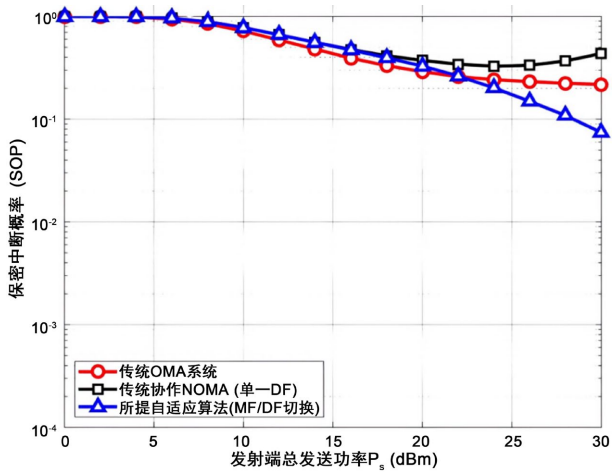

Figure 6. Comparison of SOP performance under different multiple access modes
图 6. 不同多址接入模式下的 SOP 性能对比

如图 6 所示，随着发射功率从 0 dBm 增加到 30 dBm，所有系统的保密中断概率(SOP)均在一定范围呈现单调下降趋势。这表明提升发射功率可以有效增强合法用户的信号强度，降低信息被截获的风险。对比发现，协作 NOMA 系统的曲线始终低于传统 OMA 系统。这证明了 NOMA 技术在功率域复用方面的优势，能够提供比 OMA 更高的安全容量冗余。

4.2.2. 窃听者位置对系统安全性影响的 3D 建模分析

为更全面地展示空间几何分布对物理层安全的影响，引入三维仿真分析。

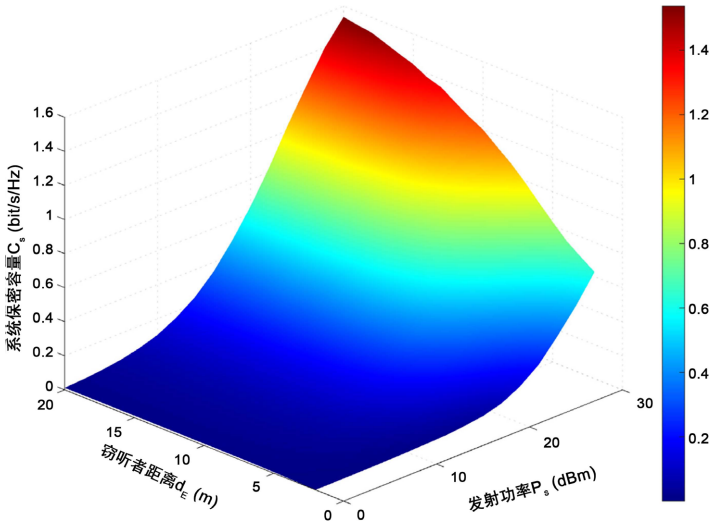

Figure 7. 3D surface plot of secrecy capacity varying with eavesdropper distance (d_E) and transmit power (P_S)
图 7. 保密容量随窃听者距离(d_E)与发射功率(P_S)变化的 3D 曲面图

如图 7 所示，系统保密容量呈现出一个向上的曲面形态。当窃听者逐渐远离中继节点时，窃听链路的路径损耗急剧增加，其截获信号的能力迅速削弱，导致系统的 SOP 显著降低。仿真结果印证了物理层安全技术利用信道差异性保障通信的理论核心：即当窃听信道劣于合法信道时，系统安全性会得到质的提升。

4.2.3. 功率分配比例的全局最优化分析

仿真曲线呈现明显的抛物线特征，当 a_2 过小时，弱用户通信中断；当 a_2 过大时，强用户由于剩余功率不足导致解码失败，且窃听者更容易从高功率信号中提取信息。图 8 标出的峰值(约在 $a_2 = 0.75$ 处)证明系统存在一个最优的功率分配平衡点，这是提升物理层安全性能的重要参数。

4.3. 所提自适应算法与先进调度机制的性能验证

本节验证本研究所提出的“自适应 MF/DF 切换算法”在复杂环境下的表现(图 9)。

在高功率阶段(>25 dBm)，传统的单一解码转发(DF)协议由于无法有效抑制窃听者，其安全传输概率增长趋于停滞甚至出现回落。而本研究提出的自适应算法在检测到安全风险时，会自动切换至修改转发(MF)模式，通过相位修正人为拉大信道差异。

此外，在自适应算法中引入机会调度机制(即从多个候选节点中选择最优中继)后，系统的安全传输概率得到了进一步的显著提升。这不仅证明了动态切换策略的灵活性，也体现了引入调度机制后系统在抵御多节点窃听方面的卓越性能。

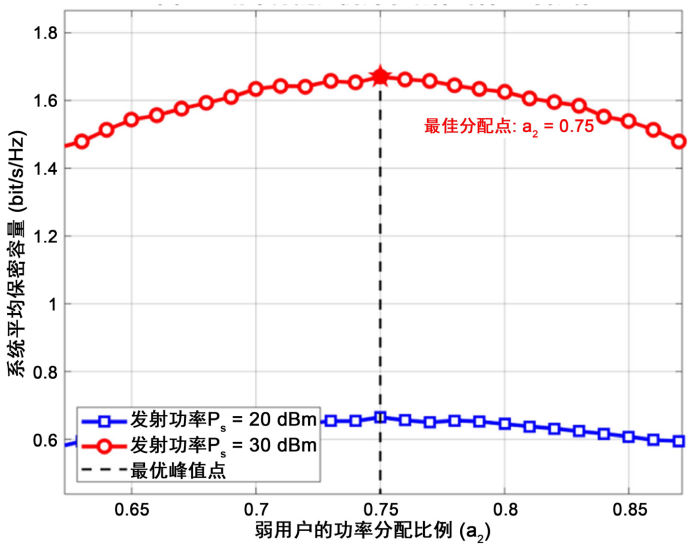

Figure 8. Curve of the effect of power allocation factor a_2 on average secrecy capacity
图 8. 功率分配因子 a_2 对平均保密容量的影响曲线

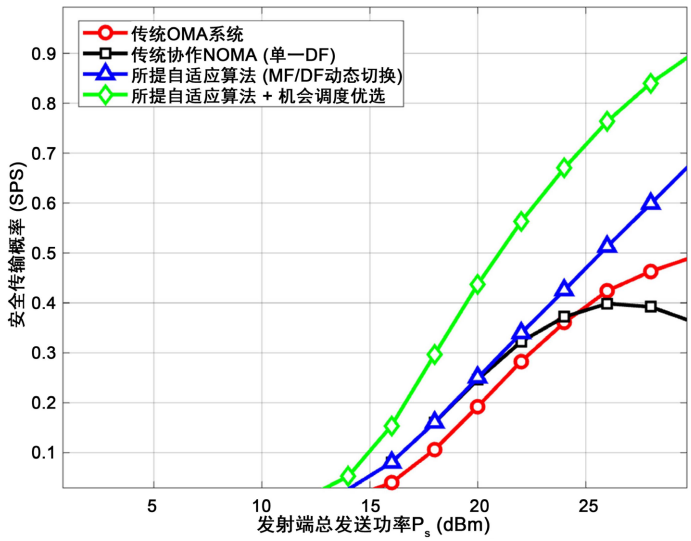

Figure 9. Comparison of the secure transmission probability (SPS) of the proposed adaptive algorithm and the traditional single protocol
图 9. 所提自适应算法与传统单一协议的安全传输概率(SPS)对比图

5. 总结与展望

本文针对物联网海量设备接入的频谱紧缺与安全隐患问题，开展协作 NOMA 系统的物理层安全性能研究。通过构建含强弱用户与窃听者的协作传输模型，推导了信干噪比、保密容量及保密中断概率等关键指标的闭合表达式，提出可在解码转发(DF)与修改转发(MF)协议间动态切换的自适应中继安全传输算法，并引入机会调度机制。多维度仿真验证：增大发射功率、拉远窃听者距离能有效降低保密中断概率；系统存在最优的功率分配比例以达到安全性能峰值；所提算法结合调度机制，突破了传统单一 DF 协议在高信噪比下的安全容量瓶颈，显著提升了系统的安全传输概率。

本文相关研究仍存在可拓展空间：一是现有模型基于单天线节点、单一窃听者假设，后续可拓展至

多天线、多窃听者协同攻击的复杂网络场景；二是算法依赖理想信道状态信息(CSI)，可针对非理想 CSI、硬件损伤等实际场景研究高鲁棒性方案，提升工程实用性；三是可引入机器学习技术实现多节点调度与功率分配的联合优化，进一步提升系统智能化水平与安全性能。

参考文献

[1] 张延良, 田月华, 李兴旺, 等. 基于 MF 协议的协作 NOMA 系统物理层安全性能研究[J]. 电子与信息学报, 2023, 45(4): 1211-1218.

[2] 王文学. 基于协作 NOMA 系统的中继选择及保密性能分析[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2021.

[3] 黄开枝, 金梁, 钟州. 5G 物理层安全技术——以通信促安全[J]. 中兴通讯技术, 2019, 25(4): 43-49.

[4] 陈书平, 王文博, 张兴. 解码转发协同中继网络多用户分集[J]. 北京邮电大学学报, 2009, 32(1): 95-98+107.

[5] 王东, 李永成, 白铂, 等. 放大转发中继网络中绿色的物理层安全通信技术[J]. 电子与信息学报, 2016, 38(4): 841-847.

[6] 叶明珠, 李光球, 张旭, 等. 基于硬件损伤的修改转发协作 NOMA 系统的物理层安全[J]. 电信科学, 2025, 31(10): 123-132.

[7] 王浩, 李娟, 张敏. 非正交多址全双工中继网络中的人工干扰保密性分析[J]. 通信技术, 2025, 58(12): 2890-2898.

[8] 罗延翠, 李光球, 叶明珠, 高辉, 张亚娟. 中继选择 NOMA 无线系统的物理层安全[J]. 电信科学, 2024, 40(3): 116-127.

[9] Ali, K., Chafii, M. and Al-Dweik, A. (2024) Opportunistic Scheduling Scheme to Improve Physical-Layer Security in Cooperative NOMA System. *IEEE Transactions on Communications*, **72**, 5845-5858.

[10] 张贞凯, 许姣, 田雨波. 多目标跟踪时的自适应功率分配算法[J]. 信号处理, 2017, 33(S1): 22-26.

[11] 王夕予, 许晓明, 陈亚军. 非理想连续干扰消除下非正交多址接入上行传输系统性能分析[J]. 电子与信息学报, 2019, 41(12): 2795-2801.

[12] 毕奇, 梁林, 杨姗, 等. 面向 5G 的非正交多址接入技术[J]. 电信科学, 2024, 31(5): 14-21.

[13] 吴宣利, 许智聪, 王禹辰, 等. 基于信道相关性的物理层安全性能分析[J]. 通信学报, 2024, 42(3): 65-74.

[14] 丁青锋, 刘梦霞, 连义罘. 基于非理想 CSI 的全双工双向中继系统保密中断概率性能研究[J]. 计算机应用研究, 2020, 37(9): 2819-2821+2826.

[15] 孙立悦, 赵晓晖, 虢明. 基于中断概率的协作通信中继选择与功率分配算法[J]. 通信学报, 2013, 34(10): 84-91.

[16] 谭立新, 何艳丽. 多径衰落信道的统计特性与仿真研究[J]. 计算机仿真, 2010, 27(7): 96-98+129.

[17] 李伟, 严康, 耿静茹, 等. NGSO 通信星座系统间同频干扰场景与建模研究[J]. 天地一体化信息网络, 2024, 2(1): 20-27.

[18] 芮雄丽, 曹雪虹. 一种基于叠加编码的协作传输协议[J]. 计算机应用研究, 2020, 37(12): 3736-3738.