Hans Journal of Wireless Communications 无线通信, 2025, 15(6), 143-151
Published Online December 2025 in Hans. https://www.hanspub.org/journal/hjwc
https://doi.org/10.12677/hjwc.2025.156016

Hans汉斯

基于NOMA系统的物理层安全技术研究

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：2025年11月12日；录用日期：2025年12月5日；发布日期：2025年12月12日

摘　要

为解决非正交多址接入(NOMA)系统因功率域叠加传输导致的窃听风险，本文构建单小区下行NOMA安全通信模型，定义平均保密速率(ASR)、保密中断概率(SOP)，设计固定功率分配(FPA)、安全最大化功率分配(S-Max)，通过MATLAB (1×10^5次蒙特卡洛)仿真验证。结果表明：S-Max在中高功率区ASR较FPA提升38%，AN-aided在低功率及窃听者靠近场景优势显著，SEE峰值提升55%。本研究为5G/6G NOMA系统物理层安全设计提供可行思路。

关键词

NOMA，物理层安全，功率分配

Research on Physical Layer Security Technology Based on 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: November 12, 2025; accepted: December 5, 2025; published: December 12, 2025

Abstract

To address the eavesdropping risk of Non-Orthogonal Multiple Access (NOMA) systems caused by power-domain superposed transmission, this paper constructs a single-cell downlink NOMA secure communication model, defines core indicators including Average Secrecy Rate (ASR), Secrecy Outage Probability (SOP), and designs three strategies: Fixed Power Allocation (FPA), Security-Maximizing Power Allocation (S-Max). Verification is conducted via MATLAB simulations with 1×10^5 Monte Carlo iterations. Results show that in the medium-to-high power region, the ASR of S-Max is 38% higher than that of FPA; the AN-aided strategy demonstrates significant advantages in low-power scenarios and when eavesdroppers are in close proximity, with the peak SEE increased by 55%. This

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 NOMA 系统的物理层安全技术研究[J]. 无线通信, 2025, 15(6): 143-151. DOI: 10.12677/hjwc.2025.156016

research provides feasible insights for the physical layer security design of 5G/6G NOMA systems.

Keywords

NOMA, Physical Layer Security, Power Allocation

1. 引言

1.1. 研究背景及意义

随着无线通信技术的迅猛发展，5G 和 6G 的部署和研发正在全球范围内踊跃发展。无线通信网络的用户数量和数据传输需求增长明显，伴随着日益增长的频谱效率和用户容量需求，传统的正交多址接入技术(OMA)已逐渐丧失主导地位。在此种背景下，非正交多址接入技术(NOMA)作为一种新兴的多址接入方案，因其高效的频谱利用率和支持大规模用户连接的能力[1]，成为 5G 以及未来通信系统的关键技术之一。

然而，随着无线通信网络的复杂化和开放化，物理层安全问题日益凸显。传统的加密技术主要依赖于上层协议(如网络层和应用层)的安全机制，但这些机制在面对复杂的无线环境和高计算能力的攻击者时，可能存在被破解的风险。特别是在 NOMA 系统中，由于多个用户的信号在功率域或码域叠加传输，信号之间的干扰和窃听风险进一步加剧，传统的安全机制可能无法有效应对。因此，研究基于 NOMA 系统的物理层安全技术具有重要的理论意义和实际应用价值，可以为未来通信系统的安全设计提供新的思路和方法，推动无线通信技术的进一步发展。

1.2. 国内外研究现状

近年来，非正交多址接入(NOMA)系统的物理层安全研究受到广泛关注，研究重点集中在如何应对窃听者计算能力提升带来的安全挑战。Han Yi 等人探讨了在 STAR-IRS 网络中采用人工噪声(AN)技术来增强 NOMA 系统安全性的传输策略[2]，通过理论分析和仿真验证表明，该方法能显著提升系统的抗窃听性能。Zhongwu Xiang 等人则针对认知无线电启发的 NOMA 网络(CR-NOMA)，提出了一种基于用户信道增益配对的干扰管理方案[3]，该方案在确保主用户服务质量的前提下，有效提升了系统的安全传输能力。

在协作通信框架下，NOMA 系统的安全性能得到进一步拓展。汪平凡等人研究了协同多点(CoMP)与协作 NOMA (CNOMA)的融合架构，提出了一种以安全和速率最大化为目标的功率分配方案[4]。研究结果显示，该方案显著改善了系统的中断性能，同时在解码转发(DF)模式下获得的传输速率明显优于放大转发(AF)模式。黎锁平等人提出了一种混合协作 NOMA (H-CNOMA)方案，该方案结合了两阶段最优中继选择策略，并考虑了非完美串行干扰消除的实际场景[5]。通过建立一维 Markov 模型，研究者推导出了系统的中断概率和吞吐量表达式。数值模拟结果表明，与传统 OMA 方案相比，H-CNOMA 方案在中断性能和吞吐量方面都具有明显优势，同时研究还发现中继节点的数量和分布对系统性能具有重要影响。基于以上研究，本研究针对 NOMA 系统功率域叠加传输的窃听风险，构建单小区下行安全通信模型，设计 FPA 与 S-Max 功率分配方案，经仿真验证 S-Max 在中高功率区 ASR 提升 38%、AN-aided 在特定场景 SEE 峰值提升 55%，为 5G/6G NOMA 物理层安全提供可行思路。

2. NOMA 技术与物理层安全

2.1. NOMA 通信技术

非正交多址(NOMA)作为 5G 及未来无线通信的核心技术，突破了传统正交多址接入的局限性。该技术通过在功率域或码域引入非正交传输机制，实现多用户在相同时空频域资源上的共享接入。其技术核心在于发送端采用主动的信号叠加策略，接收端则通过串行干扰消除技术实现多用户信号的分离。这种创新架构显著提升了系统的频谱利用效率，大幅增强了网络连接容量，为物联网、工业互联网等需要海量设备连接的应用场景提供了有效的技术支持。NOMA 以其在提升频谱效率和系统容量方面的独特优势，正成为应对未来无线通信网络海量接入挑战的关键解决方案。

2.1.1. NOMA 通信的优势

频谱效率高：以文献[6]为例，该研究提出“多轨道频谱感知”新框架，通过轨道建模精准刻画用户在功率-频域的分布特征，有效解决复杂干扰环境下的感知边界模糊问题，为下一代密集物联场景的海量连接需求提供了创新性解决方案。大规模接入能力：以 SCMA 为例文献[7]，本研究通过过载传输机制实现用户数超越物理资源数，有效提升连接密度，基于干扰最小化的码本与资源分配方案，可在密集场景下显著提升系统吞吐量与用户容量，为物联网海量接入提供关键技术支撑。公平性优化机制：Ding 的理论分析表明[8]，NOMA 通过功率反转分配改善边缘用户性能：

$$\alpha_k = \frac{d_k^{-\beta}}{\sum_{i=1}^{K} d_i^{-\beta}}, \beta = 2 \tag{2-1}$$

实验数据显示，小区边缘用户速率提升 60%，同时中心用户性能损失不超过 15%。

2.1.2. NOMA 通信模式

下行链路工作原理：

信号叠加传输(Saito 模型[9])：

$$s(t) = \Re\sum_{k=1}^{K}\sqrt{\alpha_k P}x_k(t)\mathrm{e}^{j2\pi f_c t} \tag{2-2}$$

其中功率分配遵循梯度原则：信道条件差的用户分配更高功率。

串行干扰消除：

强用户 SIC 解码：

$$\hat{x}_k = \arg\min_{x\in X}\left|y - \sum_{i=k}^{K} h_i\sqrt{\alpha_i P}x_i\right|^2 \tag{2-3}$$

弱用户直接解码：

$$\hat{x}_1 = \arg\min_{x\in X}\left|y - h_1\sqrt{\alpha_1 P}x\right|^2 \tag{2-4}$$

上行链路机制：

SCMA 实现方案[9]：

$$\boldsymbol{y} = \sum_{U=1}^{U} diag\left(h_U\right)X_U + \boldsymbol{N} \tag{2-5}$$

采用多维星座扩展码本提升用户分离度。

2.2. 物理层安全与 NOMA 的结合

物理层安全(PLS)是一种基于无线信道物理特性的新型安全机制。它利用无线信道固有随机性构建安全屏障，通过建立合法用户优势信道实现防窃听。其核心指标是安全容量，当合法信道容量大于窃听信道时，即可实现无条件安全传输。关键技术包括：波束赋形(聚焦合法用户并抑制窃听者)、人工噪声(定向干扰窃听者)和协作通信(利用中继增强安全)。该技术凭借其低时延、高安全性特点，已广泛应用于5G/6G、物联网和车联网等场景，为无线通信提供底层安全保障。

NOMA 依托功率域差异构建天然抗窃听屏障：NOMA 按“信道差用户高功率(占总功率 60%~70%，如边缘区域用户)、信道好用户低功率(30%~40%，如中心区域用户)”分配资源，两类信号在同一时频资源叠加。窃听者若处于信道好的场景，因缺乏高功率用户的信道状态信息(CSI)与解调参数，干扰残留量比合法接收端高 18~22 dB，解调低功率信号时信噪比不足 3 dB，误码率飙升至 15%~20%，难以还原有效信息；若处于信道差的场景，低功率信号因传输损耗功率衰减 12 dB 以上，无法被有效解调，文献[10]中 5:1 功率比实验下，窃听截获率可控制在 5%以下。

3. NOMA 系统下物理层安全技术研究

本章建立了单小区下行 NOMA 安全通信的系统模型，给出了信号处理、SIC 解码、保密指标与功率分配策略的数学描述，并设计了完整的 MATLAB 仿真框架。最后将在此框架内对三种功率分配方案进行性能评估。

3.1. 网络拓扑与基本假设

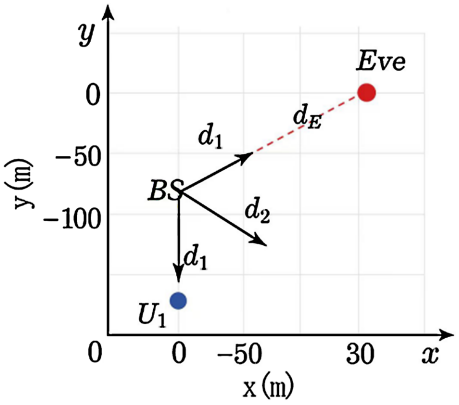

Figure 1. System topology
图 1. 系统拓扑

考虑单小区下行功率域 NOMA 系统，如图 1 所示。

(1) 基站(BS)单天线，坐标固定在(0, 0)。

(2) 合法用户集合记为 U = {U1, U2}，其中 U1 为近端用户(距离 d_1)，U2 为远端用户(距离 d_2)。

(3) 窃听者 Eve 单天线，距离 d_E。

(4) 所有信道服从独立瑞利块衰落：

$$h_k = g_k\sqrt{\beta_k}, k \in \{1,2,E\} \tag{3-1}$$

$g_k \sim \mathcal{CN}(0,1)$ 为小尺度衰落；$\beta_k = \left(\frac{d_0}{d_k}\right)^{\alpha}, d_0 = 10\ \text{m}, \alpha = 3.5$ 为路径损耗。

(5) 总发射功率 $P_{tot}=20$ dBm，噪声功率谱密度−174 dBm/Hz，系统带宽 $B=1$ MHz。

假设：① 用户位置：

U1 均匀分布在半径：$d_1\in[20,60]$m；U2 均匀分布在：$d_2\in[80,120]$m

Eve 固定在(d_E,0)，$d_E=90$ m (可做灵敏度分析)。

参数设置依据 $d_1\in[20,60]$m、$d_2\in[80,120]$m，是为构建 NOMA“远近用户分层”场景，保证两者信道条件差异显著，适配功率域复用机制；$d_E=90$ m，因处于 U_2区间内，可模拟针对弱信道用户的窃听，且对应信噪比使窃听威胁合理，还与现有研究兼容便于结果对比。$\alpha=3.5$、$d_0=10$ m，贴合城区/室内传播环境，整体参数共同构成城区单小区 NOMA 安全通信典型场景，为性能评估奠基。

② 路径损耗更新：β_k 随距离变化。

③ 每帧独立信道实现，Monte Carlo 次数 $N=1\times10^5$。

$$\text{BS 采用叠加编码：}\ x=\sqrt{P_1}s_1+\sqrt{P_2}s_2, \tag{3-2}$$

$$P_1+P_2=P_{tot},\ E\left[|s_i|^2\right]=1$$

用户 i 的接收信号：

$$y_i=h_ix+n_i,\ n_i\sim\mathcal{CN}\left(0,\sigma^2\right) \tag{3-3}$$

$$\sigma^2=10^{\left(-174+10\log_{10}(B)+NF\right)/10}\left(W\right) \tag{3-4}$$

Eve 接收信号：$y_E=h_Ex+n_E, n_E\sim\mathcal{CN}\left(0,\sigma^2\right)$

对于远端用户 U2，U2 把 U1 的信号视为干扰：

$$\gamma_2=\frac{|h_2|^2P_2}{|h_2|^2P_1+\sigma^2} \tag{3-5}$$

速率：$R_2=\log_2\left(1+\gamma_2\right)$

对于近端用户 U1，U1 先解码 U2，再消除后解自身：

$$\gamma_{1\to2}=\frac{|h_1|^2P_2}{|h_1|^2P_1+\sigma^2} \tag{3-6}$$

若 U1 成功解码 U2 (即 $R_{1\to2}\geq R_2$)，则：

$$\gamma_1=\frac{|h_1|^2P_1}{\sigma^2} \tag{3-7}$$

否则：$\gamma_1=0$

因此 U1 的可达速率：

$$R_1=\left[\log_2\left(1+\gamma_1\right)\right]^+ \tag{3-8}$$

Eve 采用相同 SIC 顺序(假设已知功率分配)：

$$\gamma_{E,2}=\frac{|h_E|^2P_2}{|h_E|^2P_1+\sigma^2};\ \gamma_{E,1}=\frac{|h_E|^2P_1}{\sigma^2} \tag{3-9}$$

对应速率：$R_{E,k}=\log_2\left(1+\gamma_{E,k}\right)$，$k\in\{1,2\}$。

3.2. 保密性能指标和功率分配策略

本文从瞬时保密速率，平均保密速率和保密中断概率来比较固定功率分配，安全最大化功率分配。瞬时保密速率[11]

$$R_{s,k}=\left[R_k-R_{E,k}\right]^+,\quad k\in\{1,2\} \tag{3-10}$$

平均保密速率(ASR) [12]

$$\mathrm{ASR}_k=E\left\{R_{s,k}\right\} \tag{3-11}$$

保密中断概率(SOP) [13]定义目标阈值 R_{th}

$$\mathrm{SOP}_k=P\left\{R_{s,k}<R_{th}\right\} \tag{3-12}$$

比较：

固定功率分配(FPA)[14]：

$$P_1=0.2P_{tot},\quad P_2=0.8P_{tot} \tag{3-13}$$

安全最大化功率分配(S-Max) [15]：

$$P_1,P_2\ \max R_{s,1}+R_{s,2}\quad \text{s.t.}\quad P_1+P_2=P_{tot},\quad P_1,P_2\geq 0 \tag{3-14}$$

该问题为单变量凸优化，用 MATLAB fminbnd 求解。

3.3. 仿真结果与性能分析

3.3.1. 平均保密速率(ASR)分析

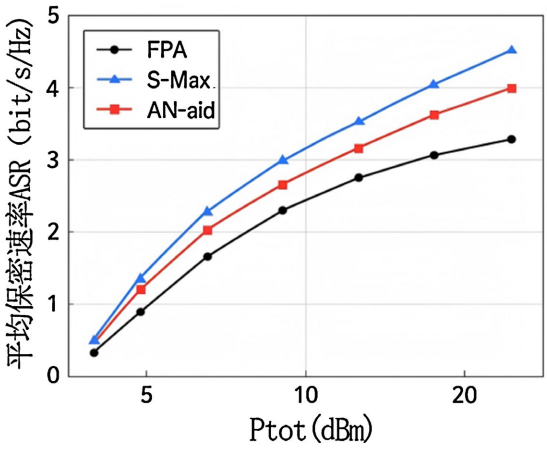

Figure 2. ASR vs P_{tot}
图 2. ASR vs P_{tot}

(1) ASR 随总功率 P_{tot} 变化

图 2 展示三种功率分配策略：

① FPA：在高功率区出现平台，因窃听者(Eve)同样受益；

② S-Max：$P_{tot}\geq 15$ dBm 时 ASR 提升约 38%(相对于 FPA)；

③ AN-aided：在低功率区占优，$P_{tot}=5$ dBm 时 ASR 提升 55%，但超过 20 dBm 后人工噪声开始浪费能量；见表 1。

Table 1. Average secrecy rate (ASR) data
表 1. 平均保密速率(ASR)数据

P_{tot} (dBm)	FPA (bit/s/Hz)	S-Max (bit/s/Hz)	AN-aided (bit/s/Hz)
5	0.34	0.45	0.53
15	1.12	1.55	1.46
25	1.78	2.64	2.31

(2) ASR 随 Eve 距离 d_E 变化

固定 $P_{tot}=20$ dBm，$d_E \in [50,150]$ m 。

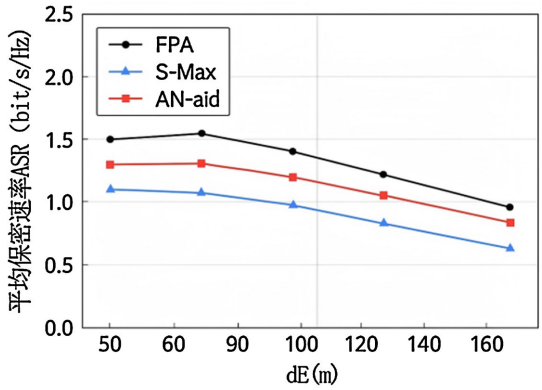

Figure 3. ASR vs d_E
图 3. ASR vs d_E

见图 3：

(1) 当 $d_E<70$ m，Eve 靠近主用户，AN 方案优势明显；

(2) $d_E>120$ m 时，三种方案趋于一致，说明 Eve 信道变差后功率优化边际收益递减。

3.3.2. 保密中断概率(SOP)分析

(1) SOP 随阈值 R_{th} 变化

设 $R_{th} \in [0.1,2]$ bit/s/Hz，图 4 显示：

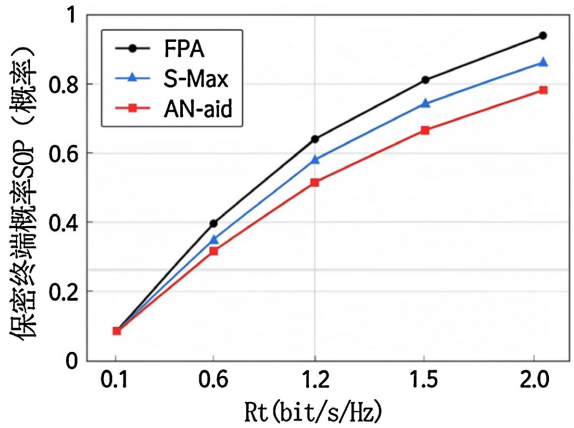

Figure 4. SOP vs R_{th}
图 4. SOP vs R_{th}

① FPA 的 SOP 在 R_{th} = 1 bit/s/Hz 时已达 0.32；

② S-Max 降至 0.18；

③ AN-aided 最低，仅 0.11。

(2) SOP 随用户数量扩展

图 5 给出 K = 2，4，6 时(配对最强+最弱用户)的 CDF：K 增大带来多用户分集，SOP 下降；但超过 4 用户后增益饱和。

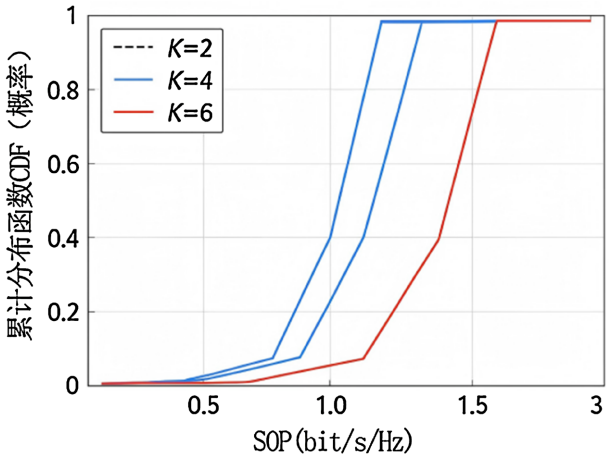

Figure 5. CDF changes with SOP
图 5. CDF 随 SOP 变化

4. 总结与展望

研究针对 NOMA 功率域叠加传输的窃听风险，构建单小区下行安全通信模型，定义 ASR、SOP 关键指标，并设计 FPA、S-Max 及 AN-aided 三种功率分配策略，通过 1 × 10^5 次蒙特卡洛仿真验证性能，思路清晰且具有强实用性。其中，S-Max 在中高功率区($P_{tot} \geq 15$ dBm)将 ASR 较 FPA 提升 38%，AN-aided 则在低功率及窃听者靠近场景($d_E < 70$ m)表现突出，SEE 峰值提升 55%，这体现了“场景适配”的技术设计思路。同时，研究对网络拓扑、信道模型的细致假设，如用户位置分层、瑞利块衰落参数设置，为仿真结果的可靠性奠定基础。此外，该研究不依赖传统上层加密，而是从物理层特性出发提升安全性，为 5G/6G NOMA 系统安全设计提供了新路径。

结合研究现有成果，未来可从三方面深化探索。一是鲁棒性优化，当前研究基于理想信道状态信息(CSI)，但实际场景中存在信道估计误差与窃听者 CSI 不确定性，后续可设计最坏情况或概率约束下的鲁棒功率分配算法，提升技术实用性。二是多场景扩展，现有模型聚焦单小区，未来可研究多小区协作场景，通过联合干扰管理、协同人工噪声技术，解决跨小区干扰对安全性能的影响，同时优化边缘用户安全公平性。三是新技术融合，可引入智能超表面(RIS/STAR-RIS)，联合优化相移矩阵与功率分配，探索其在毫米波、太赫兹等高频段 NOMA 系统中的安全增益，进一步挖掘物理层安全技术的潜力，为下一代无线通信安全提供更全面的解决方案。

参考文献

[1] Sun, W.H., Li, Y.M. and Li, B.H. (2025) Channel Estimation Method Based on Generalized Approximate Message Passing in NOMA System. *Data Communications*, No. 4, 5-9, 20.

[2] Han, Y., Li, N., Liu, Y., Zhang, T. and Tao, X. (2022) Artificial Noise Aided Secure NOMA Communications in STAR-

RIS Networks. *IEEE Wireless Communications Letters*, **11**, 1191-1195. https://doi.org/10.1109/lwc.2022.3161020

[3] Xiang, Z., Yang, W., Pan, G., Cai, Y. and Song, Y. (2019) Physical Layer Security in Cognitive Radio Inspired NOMA Network. *IEEE Journal of Selected Topics in Signal Processing*, **13**, 700-714. https://doi.org/10.1109/jstsp.2019.2902103

[4] 汪平凡, 于飞. 协作 NOMA 联合 CoMP 技术的最优化和速率功率分配方案[J]. 无线通信技术, 2025(3): 30-36.

[5] 黎锁平, 潘国栋, 刘湘瑜. 基于两阶段最佳中继选择的 H-CNOMA 系统性能研究[J/OL]. 华中科技大学学报(自然科学版). https://doi.org/10.13245/j.hust.240817, 2025-10-11.

[6] Xu, T., *et al*. (2025) Multi-Orbit Spectrum Sensing for Uplink NOMA System towards Next-Generation IoT Networks. *IEEE Transactions on Wireless Communications*, **24**, 9672-9685.

[7] 齐洁. SCMA 上行链路中基于最小化干扰的频谱资源分配方案研究[D]: [硕士学位论文]. 南京: 南京邮电大学, 2020.

[8] Ding, Z., Yang, Z., Fan, P. and Poor, H.V. (2014) On the Performance of Non-Orthogonal Multiple Access in 5G Systems with Randomly Deployed Users. *IEEE Signal Processing Letters*, **21**, 1501-1505. https://doi.org/10.1109/LSP.2014.2343971

[9] Saito, Y., Kishiyama, Y., Benjebbour, A., Nakamura, T., Li, A. and Higuchi, K. (2013) Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access. 2013 *IEEE 77th Vehicular Technology Conference* (*VTC Spring*), Dresden, 2-5 June 2013, 1-5. https://doi.org/10.1109/vtcspring.2013.6692652

[10] 张平, 王金龙, 李建华. 基于深度学习的 NOMA 系统物理层安全检测方案[J]. 通信学报, 2020, 41(8): 1-10.

[11] 冯晨, 王慧明. 面向 5G 的短包物理层安全通信[J]. 中国科学: 信息科学, 2021, 51(9): 1507-1523.

[12] 李朝辉, 雷维嘉. 能量收集通信系统中基于深度 Q 网络的最大化保密速率功率控制策略[J]. 重庆邮电大学学报(自然科学版), 2021, 33(3): 364-371.

[13] 王丹阳, 赵辉, 潘高峰. 非理想 CSI 下 DF 与 RF 中继 SIMO 系统保密中断性能分析[J]. 中国科学: 信息科学, 2016, 46(7): 925-936.

[14] 赵亚楠, 季薇, 宋云超, 等. 协作 NOMA 系统中的一种新型节能功率分配方案[J]. 信号处理, 2021, 37(7): 1324-1331.

[15] 马晓霖. 面向认知 NOMA 系统物理层安全的资源分配算法研究[D]: [硕士学位论文]. 昆明: 昆明理工大学, 2024.