

有关 NOMA 与 CR 技术的通信系统物理层安全问题研究

韩振华

新疆师范大学 新疆乌鲁木齐

【摘要】 无线通信使用电磁波代替了传统线缆传输信息的方式，使得信息传输的效率得到了更进一步的提升。使用无线通信信息传输载体，展现出光速自由、开放传播等特性。无线通信最显著的优势在于仅需借助电磁波就可以在短时间内传输信息，但与此同时也为窃听攻击创造了条件。无线通信的高速率、高容量、低时延的确带来了极大的便利，但与此同时更要考虑通信系统的安全性。物理层安全技术可以运用无线信道的自身衰落、噪声等特性，通过功率控制等技术阻隔窃听共计无法正确解码，进而使系统安全容量得到提升，更不需要设计复杂的加密、解密算法，因此使用物理层安全技术成为现阶段解决无线通信安全问题的关键手段与方式。非正交多址接入技术和认知无线电技术的功率控制均属于核心技术，在此基础上实现物理层安全技术是现阶段的重点研究内容之一。

【关键词】 无线通信；物理层安全；非正交多址接入；认知无线电

Research on Physical Layer Security of Communication System with NOMA and CR Technology

huahan Zhen

Xinjiang Normal University, Urumqi China

【Abstract】 Wireless communication uses electromagnetic wave instead of the traditional cable transmission of information, so that the efficiency of information transmission has been further improved. Using wireless information transmission carrier, it shows the characteristics of free and open transmission at the speed of light. The most obvious advantage of wireless communication is that it can transmit information in a short time using only electromagnetic waves, but it also creates the conditions for eavesdropping attacks. The high rate, high capacity and low delay of wireless communication do bring great convenience, but at the same time, the security of communication system should be considered more. The physical security technology can use wireless channel fading and noise of features, through the power control technology such as blocking hacking total can't decode correctly, and then make the system safe capacity improved, more do not need to design complex encryption and decryption algorithm, therefore using the physical security technology become the key means and ways to solve the problem of wireless communication security. Non-orthogonal multiple access technology and power control of cognitive radio technology are both core technologies. The realization of physical layer security technology on this basis is one of the key research contents at present.

【Keywords】 Wireless communication; Physical layer security; Non-orthogonal multiple access; Cognitive radio

引言：无线通信伴随着需求的增长，相应的基础设施与服务也呈现不断上升趋势，为了更好的满足无线通信的需求，现阶段急需提升无线通信系统的安全性与系统容量，同时降低时延、改善频谱效率，这对于发展 5G 至关重要。

非正交多址接入技术（NOMA, Non-orthogonal Multiple Access）、认知无线电技术（CR, Cognitive Radio）对于提升频谱效率具有至关重要的作用，充分运用信道特性与功率控制技术提升频谱效率，NOMA 技术的实现方式多种多样，包括功率域、

码域等。截至目前为止目前大部分研究根据不同用户信道响应存在的差异,运用功率域 NOMA 技术真正能够做到同时、同频功率域复用,从而实现对用户信号传输的控制,这种方式有助于提升用户的信息对称性和与通信性能。而 CR 技术运用机会方式、协作方式使未授权用户,以功率控制技术与访问授权频谱相接。

无论是 NOMA 技术还是 CR 技术对于提升无线通信效率都具有积极意义,因此将二者结合可以实现系统频谱效率的进一步提升。但是相比有线网络,无线网络受到攻击的风险更大,鉴于此可以选择在移动通信技术快速发展的前提下,进一步提升移动通信技术的安全通信性能。

本次研究中对基于 NOMA 技术和 CR 技术的无线通信系统中的物理层安全 (PLS, Physical Layer Security) 问题进行分析,目的在于降低信息传输安全中断概率,对通信系统的安全性能与用户间最优功率分配的问题进行研究分析,尝试使用物理层安全技术提升系统安全性能。

1 NOMA 与 CR 通信系统的物理层安全技术理论

1.1 物理层安全技术的作用

相比于 CR-NOMA 技术,普通 NOMA 当中的资源块与用户之间存在着——对应关系,如果窃听的话也只能获得一个用户的信息。CR-NOMA 因为每个资源块都拥有多个用户,这使得信息泄露的风险显著增加。除了外部窃听以外,NOMA 中近端用户企图开展窃听时,只需使用 SIC 解码 (Serial Interference Cancellation, 串行干扰消除) 就可以获得来自远端用户的信息。

鉴于此,保护无线 NOMA 通信系统免受窃听攻击是目前急需解决的问题。与普通 NOMA 技术相比,CR-NOMA 技术为授权频谱中争取获得了主网络合法用户活动,同时对于次网络合法用户而言同样可以开展通信,这是对于窃听攻击依然可以获得主、次网络的信息,依然会导致信息泄露^[1]。

为了充分运用 CR-OMA 技术的优势以及防止信息泄露,本次研究中借助防信息泄露安全手段——物理层安全,物理层安全具有信道特性,与单纯使用 CR-OMA 技术相比,物理层安全实现了对合法用户功率的分配、在信道基础上选择最佳中继;与

单纯使用 NOMA 相比,CR 功率控制、主用户对次用户的干扰都增加了 CR-NOMA 信道特性的复杂性。

NOMA 技术通过功率控制实现多址接入,进一步实现资源复用,相比传统的移动网络技术的正交复用具有更高的使用效率。NOMA 技术可以帮助每个用户都可以访问全部子载波信道,由此实现为信道条件较差的用户分配到足够的带宽资源,信道条件较强的用户同样可以访该带宽资源问,这使得频谱效率得到显著提升。

相比单纯为强信道条件用户服务的传统机会用户调度,NOMA 技术凭借充足的系统吞吐量以及用户公平性获得了理想的平衡效果^[2]。NOMA 技术可以同时满足不同信道条件的用户需求,这对于满足无线通信超低延迟、实现超高连通性具有积极意义。

1.2 串行干扰消除技术

串行干扰消除 (SIC) 是一种多用户检测技术,在第三代移动通信技术 (CDMA) 中就已经被使用。相比传统检测器,SCI 的性能得到了卓越提升,同时硬件差距并不显著,正因如此 SIC 技术很快在通信行业被广泛应用。

SIC 基本原理在于实现输入端信号重叠编码,进而将最大信号功率对用户造成的干扰逐渐去除。SIC 在接收信号时可以时间对多个用户逐个数据进行判决,当判决出一个用户就意味着可以减去该用户的信号导致的多址干扰,依据信号功率大小进行顺序以此生成操作顺序,功率较大信号优先执行操作,直至所有多址干扰全部被消除为止。

SIC 接收器每一级对应检测一个信号,由此推断出判决数量最终由用户数量决定。按照功率值排列对用户操作顺序进行排列,功率越大的信号处理顺序就越靠前,信号捕获的原则也是按照输出功率的实际大小。每级输出功率最大的用户对应的数据判决以及去除该用户导致多址干扰后接收的信号,通过这种方式将多址干扰控制在最低水平,信号越弱对应的获益也就越大,使得检测的可靠性得到有效提升。

2 NOMA 系统物理层安全性分析

次网络 SN (secondary network) 感知到主用户 PU (primary user) 占用频谱的情况下,此时对应的次发射机 ST (secondary transmitter) 可以用作主网

络 PN (primary network) 中继, 收到主发射机 PT (primary transmitter) 的信息后进一步放大后再转发给主用户 PU, 这样可以实现 PN 网络性能的提升^[3]。次网络 SN 感知频谱处于空穴状态, 此时次发射机 ST 向次用户 (SU₁、SU₂) 发送所需信号。这种方式充分运用了 CR 技术的网络感知特性, 充分运用授权频段频谱空穴, 防止频谱资源浪费的现象发生。

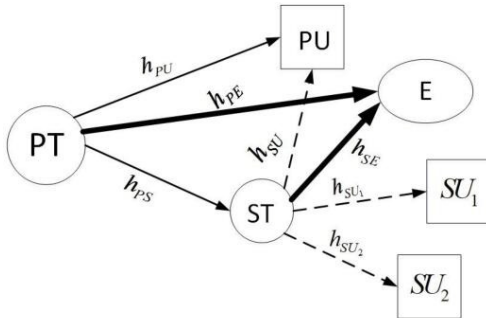


图 1 CR-NOMA 协作中继模型

2.1 SN 第一种工作模式

在主发射机 PT 的作用下混合叠加主用户 PU 所需信号, 随后再发送至 PU。占用频谱被次网络 SN 检测出来以后, 次发射机 ST 辅助主发射机 PT 信息, 将主网络 PN 作为中继。

此时 PN 发送的信号为 $\sqrt{a_1 p_p} x_1 + \sqrt{a_2 p_p} x_2$, 其中 x_1 为向 PU 发送的机密信号, x_2 为抵御窃听的干扰信号

假设干扰信号是预设存储在 PU 的随机信号, 作用是为了抵御干扰。则 P_p 为 PT 总发送功率、 a_1 为 x_1 功率分配系数、 a_2 为 x_2 功率分配系数, 此时 $a_1 + a_2 = 1$

假设信号同时遭遇窃听攻击, 此时对应的主用户 PU、次发射机 ST、窃听用户 E (eavesdropper) 接收到的信号:

$$y_{pu}^1 = h_{pu}(\sqrt{a_1 p_p} x_1 + \sqrt{a_2 p_p} x_2) + n_{pu} \quad (1)$$

$$y_{st} = h_{ps}(\sqrt{a_1 p_p} x_1 + \sqrt{a_2 p_p} x_2) + n_{st} \quad (2)$$

$$y_E^1 = h_{pE}(\sqrt{a_1 p_p} x_1 + \sqrt{a_2 p_p} x_2) + n_E \quad (3)$$

PU 可以实现干扰信号分辨、去除, 窃听攻击 E 只能对背景噪声进行处理, 此时 PU、E 对 x_1 解码对应的接收 SNR、SINR 分别对应:

$$\gamma_{pu}^1 = |h_{pu}|^2 a_1 \rho_p \quad (4)$$

$$\gamma_E^1 = \frac{|h_{pE}|^2 a_1 \rho_p}{|h_{pE}|^2 a_2 \rho_p + 1} \quad (5)$$

3 安全性验证

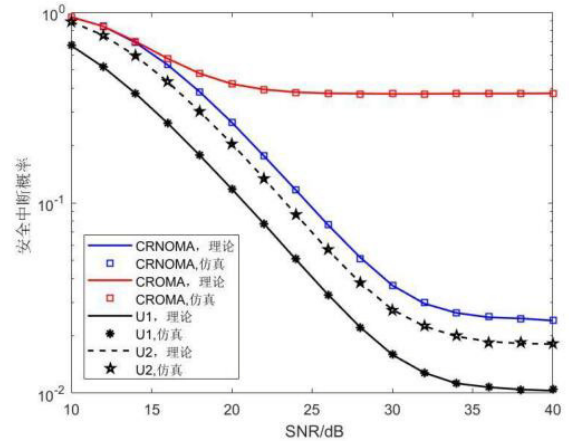


图 2 安全中断概率随传输 SNR 变化的曲线

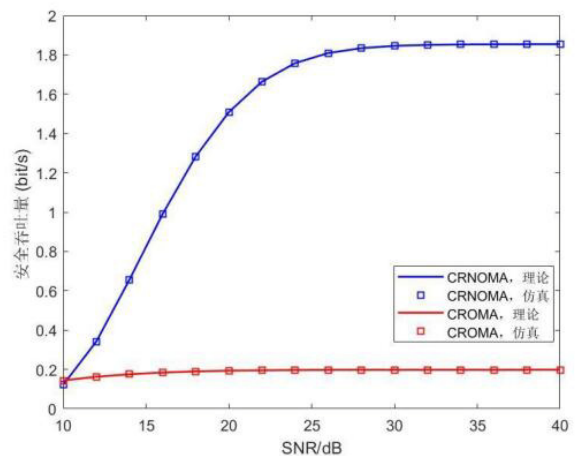


图 3 安全吞吐量随传输 SNR 变化的曲线

图 2 所示为 CR-NOMA 系统安全中断概率伴随传输信噪比 SNR 变化的趋势。由图可见, 理论值曲线与蒙特卡洛仿真曲线在信噪比全部范围内具有良好的匹配性。图中进一步展示了 CR-NOMA 的系统安全性能显著优于 CR-OMA 的系统安全性能, 由此验证了本次研究设想的有效性^[4]。

信噪比在中低范围内 (<35dB) 增加时, CR-NOMA 系统安全中断概率呈现持续下降趋势, 安全性能随之被逐渐优化; 当信噪比增加到较高的范围时 (>35dB 时), 安全中断概率与极限下界值逐渐接近。

图 3 所示为安全吞吐量随传输 SNR 变化的曲线，由此可以直观的看出 CR-NOMA 系统安全吞吐量与传统 NOMA 系统安全吞吐量伴随传输信噪比变化的对比。图中可以直接看出，每一种系统的安全吞吐量与信噪比成正比关系，同时 CR-NOMA 系统安全吞吐量显著高于传统 NOMA 系统。同时 CR-NOMA 系统安全中断概率与一个下界无限趋近，安全吞吐量也与上限无限趋近。

图 4 所示为不同系统参数下安全中断概率变化的曲线，由此可见不同干扰温度约束 ($I=20\text{dB}$, $I=30\text{dB}$, $I=40\text{dB}$) 与目标速率 ($R=0.5$, $R=1$) 条件下，从 CR-NOMA 系统安全中断概率变化的对比中可以发现，不同的参数条件下对应的系统的安全中断概率与下界值无限接近。通过纵向对比得知：

(1) 目标速率在不断变化的过程中，对应的系统安全中断概率也不断增加，系统要进行实现高速传输要建立在安全性能的基础上；系统设计工作中，进一步导致充分考虑到通信速率与安全性之间平衡；

(2) 如图所示可以清晰发现，伴随干扰温度约束的增加，相应的安全中断概率下界值会越来越低；对应的次基站、中继端发射功率约束变化与干扰温度存在密切相关，随着干扰温度约束的不断变化，相应的次基站、中继端获得的发射功率就越大，证明系统的安全中断性能就越强^[5]。

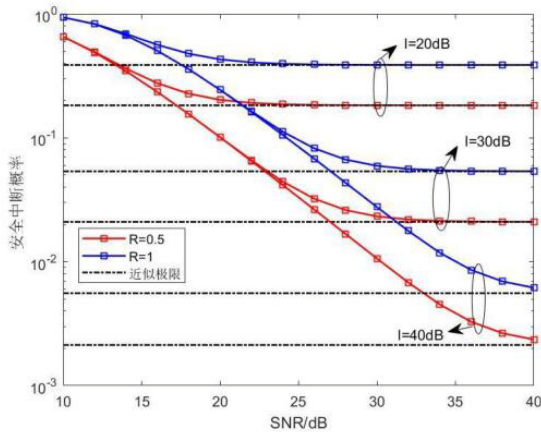


图 4 不同系统参数下安全中断概率变化的曲线

图 5 所示为系统的安全中断概率随中继数变化的曲线，由图可见系统安全中断概率伴随中继数量变化而变化。中继处于基站与合法用户之间，在多个中继中筛选出瞬时信道 CSI 最大辅助转发信号。

伴随中继数量的增加，相应的安全中断概率随

之降低，由此展现出中继数量的增加，抵御窃听攻击的水平也就随着增加。由此证明了人工噪声辅助与中继结合的方式相比使用单一中继协作传输的方案更加有效，因此在信道条件的基础上选择中继可以获得解码能力最强的中继。

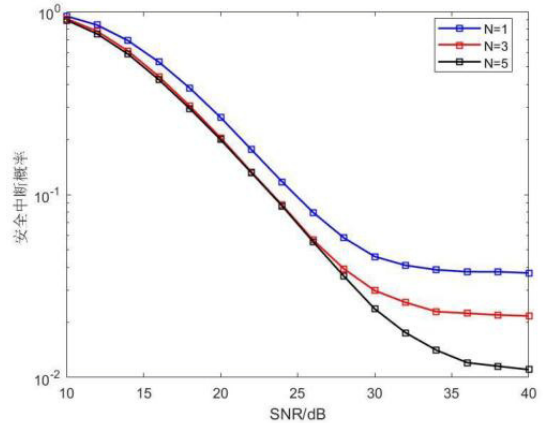


图 5 系统的安全中断概率随中继数变化的曲线

结论

未来的移动通信在发展过程中会将信息传输速率不断提升，预计会大规模使用天线、密集组网、超密集组网、同时同频全双工等技术，并且会更进一步的挖掘新频谱资源，包括高频段、毫米波等，这对于提升信道空间分辨率、信息容量而言具有积极意义。

伴随无线频段提升、波长的缩短，相应的不同位置用户与基站之间存在的信道差异性会逐渐增加，由此导致无线信道凭借自身特性，配合物理层安全技术提升通信安全性的目的更加切合实际。

当物理层安全技术被成熟运用在无线通信技术中以后，5G 可以够达到容量、传输速率、接入性、可靠性成倍增加。物理层安全可以创造一种低复杂度、多场景、一体化的安全环境，与 5G 可以具备相对理想的兼容性，有效解决了未来无线通信发展过程中面临的一系列问题。

参考文献

[1] 顾兆伟,江凌云.基于 NOMA 异构云无线接入网的联合子信道和功率分配算法[J/OL].计算机应用研究:1-9[2022-04-21].DOI:10.19734/j.issn.1001-3695.2022.02.0050.
 [2] 李小双,欧阳玉玲,徐天衡,周婷,胡宏林.非正交多址接入异构网络中基于公平性的模运算算法[J].现代电子技术:

- 65-69[2022,45(07)].DOI:10.16652/j.issn.1004-373x.2022.07.012.
- [3] 陈扬钊,袁伟娜.深度学习辅助上行免调度 NOMA 多用户检测方法[J/OL].浙江大学学报(工学版):1-7[2022-04-21].<http://kns.cnki.net/kcms/detail/33.1245.T.20220321.1718.006.html>
- [4] 杨艺.面向认知无线电适变能力提升的决策机制研究[D].哈尔滨工业大学,2019.DOI:10.27061/d.cnki.ghgdu.2019.000033.
- [5] 李婷.认知无线电系统中资源分配算法研究[D].宁波大学,2017.

收稿日期: 2022 年 3 月 9 日

出刊日期: 2022 年 6 月 14 日

引用本文: 韩振华, 有关 NOMA 与 CR 技术的通信系统物理层安全问题研究[J]. 科学发展研究, 2022, 2(1):37-41

DOI: 10.12208/j.sdr.20220010

检索信息: 中国知网 (CNKI Scholar)、万方数据 (WANFANG DATA)、Google Scholar 等数据库收录期刊

版权声明: ©2022 作者与开放获取期刊研究中心 (OAJRC) 所有。本文章按照知识共享署名许可条款发表。<http://creativecommons.org/licenses/by/4.0/>



OPEN ACCESS