

非理想硬件条件下协作NOMA系统安全中断性能研究

李美玲¹, 陈 琴¹, 杨晓霞¹, 王安红¹, 董增寿¹, Sami Muhaidat²

(1. 太原科技大学电子信息工程学院, 山西太原 030024; 2. Khalifa大学, 阿联酋阿布扎比 127788)

摘 要: 实际收发设备的非理想硬件(RHI, Residual Hardware Impairment)特性会对协作非正交多址接入(NOMA, Non-Orthogonal Multiple Access)系统性能产生重要影响. 因此, 本文提出了基于RHI的下行链路单窃听多中继协作NOMA系统模型, 推导了联合考虑合法链路和窃听链路使目标信噪比最大化(M-LaE-SNR, Maximized SNR for Legitimate and Eavesdropping link)中继传输方案下的安全中断概率闭合表达式和渐近表达式. 分析和仿真结果表明, 所提M-LaE-SNR方案相比其他方案可有效提高用户的安全中断性能, 且中继数越多所提方案性能优势越明显; 同时RHI使得系统安全传输性能降低, 且RHI对性能的影响程度主要与主链路信噪比以及协作中继个数有关; 且不同节点处的RHI对系统安全性能造成的影响程度不同. 研究结果还证明了用户的安全分集阶数等于中继数量 K .

关键词: 非正交多址接入; 物理层安全; 非理想硬件; 中继选择方案; 安全中断概率; 安全分集阶数

中图分类号: TN911.1

文献标识码: A

文章编号: 0372-2112 (2021) 07-1354-09

电子学报 URL: <http://www.ejournal.org.cn>

DOI: 10.12263/DZXB.20201101

Research on Secrecy Outage Performance of Cooperative NOMA System with Residual Hardware Impairment

LI Mei-ling¹, CHEN Qin¹, YANG Xiao-xia¹, WANG An-hong¹, DONG Zeng-shou¹, Muhaidat Sami²

(1. School of Electronic and Information Engineering, Taiyuan University of Science and Technology, Taiyuan, Shanxi 030024, China;

2. University of Khalifa, Abu Dhabi 127788, The United Arab Emirates)

Abstract: Residual hardware impairment (RHI) characteristics exist in actual transceiver which will have an important impact on the cooperative non-orthogonal multiple access (NOMA) system performance. In this paper, downlink single eavesdropper and multi relay cooperative non-orthogonal multiple access system with RHI is proposed, and the closed expression and asymptotic expression of secrecy outage probability performance is derived under the relay transmission scheme by maximizing SNR for joint legitimate and eavesdropping link (M-LaE-SNR); The analytical and simulation results show that the secrecy outage performance of RHI-D-E-MR-NOMA system using M-LaE-SNR scheme is better than the other schemes, and the more the number of relays, and the performance advantage of the proposed scheme is more obvious with more relay numbers; Meanwhile, RHI can reduce the secrecy transmission performance of the system, and the influence of RHI on the performance is mainly related to the signal-to-noise ratio (SNR) of the main link and the number of cooperative relays; And RHI at different nodes have different influences on system secure performance. It is also proved that the order of user's secrecy diversity order is equal to the number of relays K .

Key words: non-orthogonal multiple access; physical layer security; residual hardware impairment; relay selection scheme; secrecy outage probability; secrecy diversity order

1 引言

非正交多址接入(NOMA, Non-Orthogonal Multiple

Access)技术作为5G关键技术之一,通过利用功率域在相同的资源块上(时域、频域或码域)为多个用户服务,可以有效提高频谱效率,受到学术界广泛青睐,关于NOMA频

收稿日期:2020-10-08;修回日期:2021-01-10;责任编辑:覃怀银

基金项目:国家自然科学基金(No.62001320);山西省重点研发计划项目(No.201903D121117);山西省高等学校科技创新项目(No.201802090);山西省回国留学人员科研资助项目(No.2020-126, No.2021-133);山西省研究生教育创新项目(No.2020SY419)

谱有效性和传输可靠性的研究已经有了大量文献^[1].

中继协作技术作为一种可有效提高传输可靠性的方式在无线系统中得到了广泛应用,在 NOMA 系统中的应用也受到广泛关注. 代表性文献[2, 3]分别基于单中继协作 NOMA 传输方案和多中继协作 NOMA 传输方案,对系统中断性能进行了研究,结果表明,中继协作可有效抵抗无线信道衰落从而提高 NOMA 系统传输可靠性. 然而从另一个角度,物理层安全(PLS, Physical Layer Security)技术从信息论角度出发,利用无线信道的不确定性和时变性特征可以实现安全的通信链路,而不需要使用密钥加密技术^[4]. 最近学者们也纷纷展开了基于 NOMA 系统的 PLS 性能研究.

文献[5]比较了存在窃听者的协作 NOMA 系统中,中继分别采用放大转发(AF, Amplify-and-Forward)协议和解码转发(DF, Decode-and-Forward)协议时的系统安全中断性能,结果表明在高信噪比下二者性能几乎相同. 文献[6]则研究了基于双跳 DF 中继协作 NOMA 网络的安全中断性能,从 PLS 角度提出了有效提高网络安全性能的方法. 最近,文献[7]考虑多中继协作 NOMA 传输网络,分析了不同的中继选择方案对网络安全中断性能的影响. 我们在文献[8]对基于全双工中继协作 NOMA 的物理层安全传输性能进行了研究. 文献[9]提出了一种混合自动重发请求(HARQ, Hybrid Automatic Repeat Request)辅助认知 NOMA 网络传输方案,以减轻连续干扰删除(SIC, Successive Interference Cancellation)错误并提高安全要求用户(SRU, Security-Required User)的安全性能.

以上文献均考虑收发信机理想的情况,然而在实际通信系统中,无线节点的收发器硬件总会受到 RHI 特性的影响,例如 I/Q 不平衡、放大器振幅非线性和相位噪声^[10]. 文献[11]分别对基于 AF 和 DF 的中继传输网络受 RHI 的影响情况进行了研究,结果表明,RHI 对两种中继传输网络性能均有影响,且对 AF 的影响更大. 最近,一些文献研究了 RHI 对协作 NOMA 系统的影响^[12-14]. 文献[12]考虑基于 AF 的单中继协作 NOMA 网络,分析了 RHI 对系统中断性能的影响. 文献[13]进一步针对基于 AF 的单中继协作 NOMA 传输网络,考虑复杂衰落信道模型,分析了 RHI 和非理想 SIC 对中继协作 NOMA 网络的影响,结果表明,在高信噪比情况下,协作 NOMA 方案的中断性能优于非协作 NOMA 方案. 文献[14]中考虑了存在窃听者的单 AF 中继协作 NOMA 系统,从 PLS 角度分析了 RHI 对系统中断概率和截获概率的影响情况. 研究发现,中继的选择将会对考虑 RHI 的协作 NOMA 系统物理层安全性能有重要影响.

由于在实际通信系统中,收发器硬件总会不可避免

地受到各种类型的硬件损伤. 虽然可以通过采用一些补偿和校正算法来减轻硬件损伤带来的影响,但是这种损伤并不能完全消除^[14]. 文献[14]通过合法用户的中断概率和窃听者的截获概率对存在 RHI 的物理层安全性能进行了分析. 研究发现,RHI 对各节点的中断性能和截获性能影响不同. 然而,单独考虑合法用户的中断性能和窃听者的截获性能不能有效衡量系统的物理层安全传输性能,尤其是在非理想信道条件下,需要联合考虑合法链路和窃听链路. 基于这一动机,本文考虑了基于 RHI 的下行链路单窃听多中继协作 NOMA 系统模型(RHI-D-E-MR-NOMA, Downlink single Eavesdropper and Multi Relay cooperative Non-Orthogonal Multiple Access system with RHI),对中继选择方案进行了研究,提出了 M-LaE-SNR (Maximized SNR for Legitimate and Eavesdropping link)中继传输方案,并推导了该方案下的安全中断概率(SOP, Secrecy Outage Probability)闭合表达式. 为了直观的衡量安全中断性能,推导了该方案下安全中断概率的渐近表达式,分析了用户的安全分集增益. 为了与所提出的 M-LaE-SNR 比较,论文还分别分析了基于 RR 和 MRC 方案下 RHI-D-E-MR-NOMA 的安全中断性能. 结果表明,采用 M-LaE-SNR 方案下系统的安全中断性能优于其它两种方案. 通过仿真结果发现,RHI 的存在会显著降低系统的安全性能,且影响程度主要与主链路信噪比 ρ 以及协作中继个数有关. 此外,我们还研究了不同节点处的 RHI 对系统安全性能造成的影响程度. 研究表明,当 RHI 仅存在源端或中继处时,对系统安全性能造成的影响较小;而当 RHI 仅存在目的端或窃听用户处时,对系统安全性能造成的影响更为显著;例如,取安全中断概率为 10^{-2} ,与理想硬件情况相比,当 RHI 仅发生在窃听用户节点时可以得到约 2dB 的性能提升;而当 RHI 仅发生在目的节点时,会造成约 3dB 的性能损失. 因此我们在实际系统安全传输过程中,应该更加注重目的端与窃听用户处的硬件损耗情况,进行精确建模.

2 系统模型

本文考虑的 RHI-D-E-MR-NOMA 系统模型如图 1 所示,包括一个基站(BS, Base Station)、 K 个 AF 中继 $\{R_k\}_{k=1}^K$, N 个 NOMA 用户 $\{D_n\}_{n=1}^N$ 和 1 个外部窃听者(E). 实线和虚线分别表示主链路和窃听链路. 假设系统中所有节点均为单天线设备,且 BS 和 D_n 由于距离较长或其它阴影衰落存在,BS 与 D_n 和 E 之间不存在直传链路,即: D_n 和 E 只能接收到中继转发的信号. h_{R_k} 、 $h_{R_k D_n}$ 和 $h_{R_k E}$ 分别表示 $S \rightarrow R_k$ 链路、 $R_k \rightarrow D_n$ 链路与 $R_k \rightarrow E$ 链路的信道衰落系数,考虑任意两节点间的信道均为瑞利衰落信道,且 h_{R_k} 、 $h_{R_k D_n}$ 和 $h_{R_k E}$ 的瑞利衰落参数分别

为 λ_{R_k} 、 $\lambda_{R_k D_n}$ 和 $\lambda_{R_k E}$. 本文考虑实际硬件损耗限制, 系统中所有发送设备和接收设备均存在非理想特性, 用 RHI 表示^[12]. 下面先给出每个节点的信号模型.

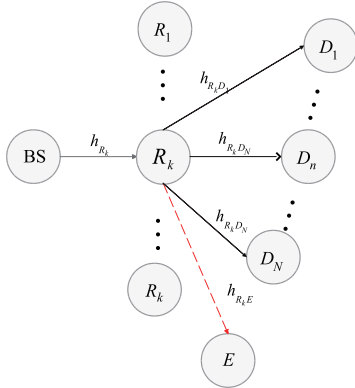


图1 RHI-D-E-MR-NOMA系统

2.1 信号模型

在 RHI-D-E-MR-NOMA 系统中, 信号传输分为两个阶段. 在第一阶段, BS 根据 NOMA 准则发送混合叠加信号 $x_s = \sum_{n=1}^N \sqrt{\alpha_n P_S} x_n$ 到 K 个中继 $\{R_k\}_{k=1}^K$. P_S 是 BS 的发射功率, x_n 是 D_n 的消息, $E[x_n^2] = 1$. α_n 是 D_n 的功率分配系数, 根据 NOMA 原理, 为了保证用户之间的公平性, N 个用户根据其信道质量进行排序 $|h_{R_k D_1}|^2 \leq \dots \leq |h_{R_k D_N}|^2$, 考虑 $\alpha_1 > \dots > \alpha_N$, 且 $\sum_{n=1}^N \alpha_n = 1$ ^[12]. 本文考虑系统中每个节点都存在 RHI, 根据文献[14, 15], RHI 产生的影响可以建模为额外的噪声源, 从而可以得到受 RHI 影响下 R_k 接收到的信号为:

$$y_{R_k} = h_{R_k} \left(\sum_{n=1}^N \sqrt{\alpha_n P_S} x_n + \mu_{SR_k} \right) + n_{R_k} \quad (1)$$

其中, $\mu_{SR_k} \sim \text{CN}(0, \rho_{SR_k}^2 P_S)$ 为 BS 到 R_k 链路的硬件损耗, $\rho_{SR_k} = \sqrt{(\rho_s^t)^2 + (\rho_{R_k}^r)^2}$ 表示 $S \rightarrow R_k$ 链路的总体 RHI 水平, ρ_s^t 和 $\rho_{R_k}^r$ 分别表示 BS 发送信号和 R_k 接收信号时受 RHI 影响系数. $n_{R_k} \sim \text{CN}(0, \sigma_{R_k}^2)$ 为 R_k 处的加性高斯白噪声.

在第二阶段, 本文考虑多中继转发方案和单中继转发方案, 在多中继转发方案中, 系统中所有接收到源信号的中继都将采用 AF 方式转发数据. 而在单中继转发方案中, 选择其中一个中继采用 AF 方式转发数据. 需要注意的是, 中继的选择将会直接影响系统性能. 在文献[7]中, 作者考虑基于理想的硬件条件下, 给出了综合主信道条件与窃听信道条件时基于 DF 的最佳中继选择方案. 而文献[14]的研究表明, RHI 对合法用户

和窃听者的中断性能均会产生影响, RHI 将会影响中继的选择, 而且 AF 中继方式相比 DF 中继方式实现简单, 但抗噪声性能较差, 为此, 本文考虑非理想条件下基于 AF 的多中继协作 NOMA 系统模型, 对中继选择方案进行了研究, 给出了所提系统模型中联合考虑主信道和窃听信道且存在 RHI 影响的最佳中继选择方案. 该方案将在后面 3.2 小节具体说明.

当第 k 个中继 R_k 将接收到的信号采用 AF 方式转发数据到 D_n 时, 放大增益为 $G_k = \sqrt{\frac{P_R}{(1 + \rho_{SR_k}^2) P_S |h_{R_k}|^2 + \sigma_{R_k}^2}}$, P_R 表示发射功率. D_n 接收到来自中继 R_k 的信号为:

$$y_{D_n}^k = h_{R_k D_n} (G y_{R_k} + \mu_{R_k D_n}) + n_{D_n} \quad (2)$$

其中, $\mu_{R_k D_n} \sim \text{CN}(0, \rho_{R_k D_n}^2 P_R)$ 表示 R_k 到 D_n 链路的硬件损耗, $\rho_{R_k D_n} = \sqrt{(\rho_{R_k}^t)^2 + (\rho_{D_n}^r)^2}$ 表示 $R_k \rightarrow D_n$ 链路的总体 RHI 水平, $\rho_{R_k}^t$ 和 $\rho_{D_n}^r$ 分别描述了 R_k 发送信号和 D_n 接收信号时受 RHI 影响系数. $n_{D_n} \sim \text{CN}(0, \sigma_{D_n}^2)$ 为 D_n 处的加性高斯白噪声.

另一方面, 在第二阶段中继转发信号到目的用户的同时, E 也会截获相应信息, 此阶段 E 接收到的信号为:

$$y_E^k = h_{R_k E} G \left[h_{R_k} \left(\sum_{n=1}^N \sqrt{\alpha_n P_S} x_n + \mu_{SR_k} \right) + n_{R_k} \right] + h_{R_k E} \mu_{R_k E} + n_E \quad (3)$$

其中, $\mu_{R_k E} \sim \text{CN}(0, \rho_{R_k E}^2 P_R)$ 表示 R_k 和 E 之间的硬件损耗, $\rho_{R_k E} = \sqrt{(\rho_{R_k}^t)^2 + (\rho_E^r)^2}$ 表示 $R_k \rightarrow E$ 链路的总体 RHI 水平, $\rho_{R_k}^t$ 和 ρ_E^r 分别描述了 R_k 发送信号和 E 接收信号时受 RHI 影响系数. 为了方便分析, 后面我们假设主链路噪声方差为 $\sigma_{R_k}^2 = \sigma_{D_n}^2 = \sigma^2$, 窃听链路噪声方差为 σ_e^2 .

2.2 基于 SIC 的 SIDNR 分析

根据 SIC 技术原理, D_n 首先解码较弱的用户 $D_l (l < n)$, 而强用户信号 $D_j (j > n)$ 在 D_n 处被视为噪声, 因此, 当选择第 k 个中继转发信号时, 结合式(1)和式(2)可得在 D_n 处解码 D_l 信号时可获得的信号干扰失真噪声比 (SIDNR, Signal-to-Interference-plus-Distortion-and-Noise Ratio) 为:

$$\gamma_{l \rightarrow n}^k = \alpha_l G^2 P_S |h_{R_k}|^2 |h_{R_k D_n}|^2 / \left[G^2 |h_{R_k D_n}|^2 \left(P_S |h_{R_k}|^2 \left(\sum_{j=l+1}^N \alpha_j + \rho_{SR_k}^2 \right) + \sigma^2 \right) + \rho_{R_k D_n}^2 P_R |h_{R_k D_n}|^2 + \sigma^2 \right] \quad (4)$$

令 $\rho_{0,k} = \rho_{SR_k}^2 + \rho_{R_k D_n}^2 + \rho_{SR_k}^2 \rho_{R_k D_n}^2$, $\rho_{1,k} = 1 + \rho_{SR_k}^2$, $\rho_{2,k} = 1 + \rho_{R_k D_n}^2$. 将 G^2 代入式(4), 并令 $X_{R_k} = \rho_S |h_{R_k}|^2$, $Y_{D_n,k} = \rho_R |h_{R_k D_n}|^2$, $\rho_S = \frac{P_S}{\sigma^2}$ 和 $\rho_R = \frac{P_R}{\sigma^2}$. 则式(4)可改写成:

$$\gamma_{l \rightarrow n}^k = \frac{\alpha_l \Delta_n^k}{\left(\sum_{j=l+1}^N \alpha_j + \rho_{0,k} \right) \Delta_n^k + 1} \quad (5)$$

其中, $\Delta_n^k = \frac{X_{R_k} Y_{D_n,k}}{\rho_{1,k} X_{R_k} + \rho_{2,k} Y_{D_n,k} + 1}$, $1 \leq n \leq N$. 进一步, 根据式(5), 令 $\varepsilon_n = \sum_{j=n+1}^N \alpha_j + \rho_{0,k}$, 当 R_k 转发信号到 D_n 时, D_n 解码自身信号时的 SIDNR 为:

$$\gamma_{n \rightarrow n}^k = \gamma_n^k = \frac{\alpha_n \Delta_n^k}{\varepsilon_n \Delta_n^k + 1} \quad (6)$$

本文考虑 E 具有强大的信号处理能力, 可以执行理想 SIC 操作. 类似式(6)的获得过程, 根据式(3)可得, 当 R_k 转发信号到 D_n 时, 通过令 $\Delta_E^k = \frac{X_{R_k} Z_{E,k}}{\rho_{e,1,k} X_{R_k} + \rho_{e,2,k} Z_{E,k} + 1}$, $Z_{E,k} = \rho_e |h_{R_k E}|^2$, $\rho_e = \frac{P_R}{\sigma_e^2}$, $\eta_n = \sum_{j=n+1}^N \alpha_j + \rho_{e,0,k}$, $\rho_{e,0,k} = \rho_{SR_k}^2 + \rho_{R_k E}^2 + \rho_{SR_k}^2 \rho_{R_k E}^2$, $\rho_{e,1,k} = 1 + \rho_{SR_k}^2$, $\rho_{e,2,k} = 1 + \rho_{R_k E}^2$, E 截获 D_n 信号时的 SIDNR 为:

$$\gamma_{E,n}^k = \frac{\alpha_n \Delta_E^k}{\eta_n \Delta_E^k + 1} \quad (7)$$

3 性能分析

基于图 1 中所提出的 RHI-D-E-MR-NOMA 系统模型, 本小节首先给出所涉及复合变量的信道统计特性, 作为后面分析安全中断性能的基础.

3.1 信道统计特性

定理 1 式(5)中 $\Delta_n^k = \frac{X_{R_k} Y_{D_n,k}}{\rho_{1,k} X_{R_k} + \rho_{2,k} Y_{D_n,k} + 1}$ 的累积

分布函数(CDF, Cumulative Distribution Function):

$$F_{\Delta_n^k}(x) = 1 - 2Q_n \Omega(i, j) e^{-\beta_k x} \sqrt{\frac{(1 + \tau_k x)x}{\delta_k \delta_n (j+1)}} \times K_1 \left(2 \sqrt{\frac{(j+1)(1 + \tau_k x)x}{\delta_k \delta_n}} \right) \quad (8)$$

其中, $\Omega(i, j) = \sum_{i=0}^{N-n} \binom{N-n}{i} (-1)^i \sum_{j=0}^{n+i-1} \binom{n+i-1}{j} (-1)^j$,

$$Q_n = \frac{N!}{(N-n)!(n-1)!}, \quad \beta_k = \frac{(j+1)\rho_{1,k}}{\delta_n} + \frac{\rho_{2,k}}{\delta_k}, \quad \delta_k =$$

$\rho_S \lambda_{R_k}, \delta_n = \rho_R \lambda_{R_k D_n}, \tau_k = \rho_{1,k} \rho_{2,k}, K_v(\cdot)$ 表示为第二类 v 阶修正贝塞尔函数.

证明 根据式(5)可得:

$$F_{\Delta_n^k}(x) = \Pr \left\{ (Y_{D_n,k} - \rho_{1,k} x) X_{R_k} \leq \rho_{2,k} Y_{D_n,k} x + x \right\} \\ = 1 - \int_{\rho_{1,k} x}^{\infty} \left[1 - F_{Y_{R_k}} \left(\frac{(\rho_{2,k} y + 1)x}{y - \rho_{1,k} x} \right) \right] f_{Y_{D_n,k}}(y) dy \quad (9)$$

令 $y - \rho_{1,k} x = t$, 并将 X_{R_k} 的 CDF 与 $Y_{D_n,k}$ 的 PDF^[16] 代入式(9), 则:

$$F_{\Delta_n^k}(x) = 1 - \frac{Q_n}{\rho_R \lambda_{R_k D_n}} \Omega(i, j) e^{-\frac{\rho_{2,k} x}{\rho_S \lambda_{R_k}} - \frac{(j+1)\rho_{1,k} x}{\rho_R \lambda_{R_k D_n}}} \\ \times \int_0^{\infty} e^{-\frac{x}{\rho_S \lambda_{R_k}} - \frac{\rho_{1,k} \rho_{12,k} x + 1}{t}} e^{-\frac{(j+1)t}{\rho_R \lambda_{R_k D_n}}} dt \quad (10)$$

根据文献[17]对式(10)进行代数运算, 可得式(8).

定理 2 式(7)中 $\Delta_E^k = \frac{X_{R_k} Z_{E,k}}{\rho_{e,1,k} X_{R_k} + \rho_{e,2,k} Z_{E,k} + 1}$ 的 CDF:

$$F_{\Delta_E^k}(y) = 1 - 2e^{-\beta_{E,k} y} \sqrt{\frac{(1 + \tau_{E,k} y)y}{\delta_k \delta_E}} K_1 \left(2 \sqrt{\frac{(1 + \tau_{E,k} y)y}{\delta_k \delta_E}} \right) \quad (11)$$

其中, $\beta_{E,k} = \frac{\rho_{e,1,k}}{\delta_E} + \frac{\rho_{e,2,k}}{\delta_k}$, $\delta_E = \rho_e \lambda_{R_k E}$, $\tau_{E,k} = \rho_{e,1,k} \rho_{e,2,k}$.

3.2 基于 M-LaE-SNR 的 RHI-D-E-MR-NOMA 系统安全中断性能

本文提出的 M-LaE-SNR 最优中继选择方案中, 联合考虑 RHI 对合法用户和窃听者的影响以及合法链路信道状态信息和窃听链路信道状态信息, 以目标用户获得的 SIDNR 和窃听者截获目标用户时的 SIDNR 比最大化为原则选择最优协作中继, 所提模型用户 D_n 的最优中继选择方案可表示为:

$$\text{BestRelay}_{D_n} = \arg \max_{R_k} \left(\frac{\gamma_n^k}{\gamma_{E,n}^k} \right) \quad (12)$$

本文在文献[14]的基础上, 考虑系统信道状态信息已知的情况, 通过安全中断概率来衡量系统的安全可靠性, 相比[14], 可以更好地从物理层安全角度定性分析系统的安全可靠性. 安全中断事件定义为当用户主信道的信道容量小于窃听信道的信道容量时, 用户发生安全中断. 当选择任意中继 R_k 转发数据时 D_n 的主信道容量为 $C_n^k = \frac{1}{2} \log_2(1 + \gamma_n^k)$, E 截获 D_n 时的信道容量为 $C_{E,n}^k = \frac{1}{2} \log_2(1 + \gamma_{E,n}^k)$, 可以得到此时 D_n 的安全中断概率的表达式:

$$\begin{aligned} \text{SOP}_n^k &= \Pr\left\{\frac{1}{2}\log_2(1+\gamma_n^k) < \frac{1}{2}\log_2(1+\gamma_{E,n}^k)\right\} \\ &= 1 - \int_0^\infty (1 - F_{\gamma_n^k}(y)) f_{\gamma_{E,n}^k}(y) dy \end{aligned} \quad (13)$$

可以看出,为了得到式(13)的结果,需要分析信噪比 γ_n^k 的 CDF 和 $\gamma_{E,n}^k$ 的概率密度函数(PDF, Probability Density Function).

引理 1 γ_n^k 的 CDF 为:

$$\begin{aligned} F_{\gamma_n^k}(x) &= 1 - 2Q_n \Omega(i, j) e^{-\beta_k z_x} \sqrt{\frac{(1+\tau_k z_x) z_x}{\delta_k \delta_n (j+1)}} \\ &\quad \times K_1 \left(2 \sqrt{\frac{(j+1)(1+\tau_k z_x) z_x}{\delta_k \delta_n}} \right) \end{aligned} \quad (14)$$

其中, $z_x = \frac{x}{\alpha_n - \varepsilon_n x}$, 条件 a 为: $0 < x < \frac{\alpha_n}{\varepsilon_n}$.

证明 根据式(6)可得:

$$F_{\gamma_n^k}(x) = \Pr\left((\alpha_n - \varepsilon_n x) \Delta_n^k \leq x\right) \quad (15)$$

对于式(15), 当 $x \leq 0$ 时, $F_{\gamma_n^k}(x) = 0$; 当 $x \geq \frac{\alpha_n}{\varepsilon_n}$ 时,

$F_{\gamma_n^k}(x) = 1$; 当 $0 < x < \frac{\alpha_n}{\varepsilon_n}$ 时, 令 $z_x = \frac{x}{\alpha_n - \varepsilon_n x}$, 可以得到:

$$F_{\gamma_n^k}(x) = \Pr(\Delta_n^k \leq z_x) = F_{\Delta_n^k}(z_x) \quad (16)$$

将式(8)代入式(16)可以得到如式(14)所示 γ_n^k 的 CDF 表达式.

$$\begin{aligned} f_{\gamma_{E,n}^k}(y) &= 2e^{-\beta_{E,k} w_y} \sqrt{\frac{(1+\tau_{E,k} w_y) w_y}{\delta_k \delta_E}} w_y' \\ &\quad \times \left[\left(\beta_{E,k} - \frac{(1+2\tau_{E,k} w_y)}{2(1+\tau_{E,k} w_y) w_y} \right) K_1 \left(2 \sqrt{\frac{(1+\tau_{E,k} w_y) w_y}{\delta_k \delta_E}} \right) \right. \\ &\quad \left. + \frac{(1+2\tau_{E,k} w_y) \left(K_0 \left(2 \sqrt{\frac{(1+\tau_{E,k} w_y) w_y}{\delta_k \delta_E}} \right) + K_2 \left(2 \sqrt{\frac{(1+\tau_{E,k} w_y) w_y}{\delta_k \delta_E}} \right) \right)}{2\sqrt{\delta_k \delta_E} (1+\tau_{E,k} w_y) w_y} \right] \end{aligned} \quad (17)$$

引理 2 $\gamma_{E,n}^k$ 的 PDF 如本页底部式(17)所示. 其中,

$w_y = \frac{y}{\alpha_n - \eta_n y}$, $w_y' = \frac{\alpha_n}{(\alpha_n - \eta_n y)^2}$, 条件 b 为: $0 < y < \frac{\alpha_n}{\eta_n}$.

证明 根据式(7)可得:

$$F_{\gamma_{E,n}^k}(y) = \Pr\left((\alpha_n - \eta_n y) \Delta_E^k \leq y\right) \quad (18)$$

当 $0 < y < \frac{\alpha_n}{\eta_n}$ 时, 结合式(9)、式(18)可进一步表

示为:

$$\begin{aligned} F_{\gamma_{E,n}^k}(y) &= 1 - \\ &\quad 2e^{-\beta_{E,k} w_y} \sqrt{\frac{(1+\tau_{E,k} w_y) w_y}{\delta_k \delta_E}} K_1 \left(2 \sqrt{\frac{(1+\tau_{E,k} w_y) w_y}{\delta_k \delta_E}} \right) \end{aligned} \quad (19)$$

对式(19)求导可得如式(17)所示 $\gamma_{E,n}^k$ 的 PDF. 结合引理 1 与引理 2 中对 $F_{\gamma_n^k}(x)$ 与 $f_{\gamma_{E,n}^k}(y)$ 的讨论, 可以得到:

$$\text{SOP}_n^k = \underbrace{\int_0^{\theta^*} F_{\gamma_n^k}(y) f_{\gamma_{E,n}^k}(y) dy}_{\Lambda_1} + \underbrace{1 - F_{\gamma_{E,n}^k}(\theta^*)}_{\Lambda_2} \quad (20)$$

其中, $\theta^* = \min\left(\frac{\alpha_n}{\varepsilon_n}, \frac{\alpha_n}{\eta_n}\right)$.

将式(14)与式(17)代入式(20)可以看出, 很难求得 Λ_1 的积分结果, 因此, 通过利用 Gaussian-Chebyshev Quadrature 定理^[18], 令 $G_1(y) = F_{\gamma_n^k}(y) f_{\gamma_{E,n}^k}(y)$, 解得 Λ_1 :

$$\Lambda_1 = \sum_{v=1}^V \frac{\theta^* \pi}{2V} \sqrt{1 - \varphi_v^2} G_1\left(\frac{\theta^*}{2} \varphi_v + \frac{\theta^*}{2}\right) \quad (21)$$

其中, $\varphi_v = \cos\left(\frac{2v-1}{2V} \pi\right)$.

将 Λ_1 和 Λ_2 代入式(20)中, 可进一步获得 D_n 的安全中断概率表达式:

$$\text{SOP}_n^k = \begin{cases} \Lambda_1 + \Lambda_2, & \frac{\alpha_n}{\varepsilon_n} < \frac{\alpha_n}{\eta_n} \\ \Lambda_1, & \frac{\alpha_n}{\varepsilon_n} \geq \frac{\alpha_n}{\eta_n} \end{cases} \quad (22)$$

进一步, 根据式(12)所描述的最佳中继选择方案, M-LaE-SNR 方案下 D_n 的安全中断概率为:

$$\text{SOP}_n^{\text{M-LaE-SNR}} = \Pr\left\{\max_{R_k} \frac{\gamma_n^k}{\gamma_{E,n}^k} < 1\right\} = \prod_{k=1}^K \text{SOP}_n^k \quad (23)$$

将式(22)代入上式可得 M-LaE-SNR 方案下 D_n 的安全中断概率表达式.

3.3 安全分集阶数分析

我们假设 $P_S = P_R = P$, 则 $\rho = \frac{P}{\sigma^2}$ 表示主链路的信噪比(SNR, Signal-to-Noise-Ratio). 为了直观的描述系统安全中断性能, 本节选择了安全分集阶数来评估所提 M-LaE-SNR 方案下系统的安全性能, 该性能能够描述 SOP 随着 SNR 降低的速度. 因此, 安全分集阶数定义为^[19]:

$$d = -\lim_{\rho \rightarrow \infty} \frac{\log(\text{SOP}_n^{\text{M-LaE-SNR}, \infty})}{\log \rho} = K \quad (24)$$

在高信噪比范围($\rho \rightarrow \infty$), M-LaE-SNR 方案下 D_n 的渐近 SOP 如式(25)所示:

$$\text{SOP}_n^{\text{M-LaE-SNR}, \infty} = \prod_{k=1}^K \left[\frac{\rho_{2,k}}{\rho \lambda_{R_k} \lambda_{R_k E} (\eta_n - \varepsilon_n)} J_1 + \frac{Q_n}{\lambda_{R_k} n} \left(\frac{\rho_{1,k}}{\rho \lambda_{R_k D_n} (\eta_n - \varepsilon_n)} \right)^n J_2 \right] \frac{\rho_{2,k}}{\rho \lambda_{R_k} \lambda_{R_k E} (\eta_n - \varepsilon_n)} \cdot \frac{Q_n}{\lambda_{R_k} n} \left(\frac{\rho_{1,k}}{\rho \lambda_{R_k D_n} (\eta_n - \varepsilon_n)} \right)^n J_1 J_2 \quad (25)$$

其中, $J_1 = \int_0^\infty \frac{y e^{-\frac{y}{\lambda_{R_k E}}}}{\left(y + \frac{\rho_{e,1,k}}{(\eta_n - \varepsilon_n) \rho_e} \right)} dy, J_2 = \int_0^\infty \frac{y^n e^{-\frac{y}{\lambda_{R_k E}}}}{\left(y + \frac{\rho_{e,1,k}}{(\eta_n - \varepsilon_n) \rho_e} \right)^n} dy$

均为与 ρ 无关的常数, 可通过 Matlab 数值积分得到.

证明 不失一般性, 我们令 $\rho_s = \rho_R = \rho$, 则在高信噪比区域($\rho \rightarrow \infty$), 式(6)中的 Δ_n^k 与式(7)中的 Δ_E^k 可简化成:

$$\Delta_n^k = \frac{X_{R_k} Y_{D_n, k}}{\rho_{1,k} X_{R_k} + \rho_{2,k} Y_{D_n, k} + 1} \approx \frac{\rho |h_{R_k}|^2 |h_{R_k D_n}|^2}{\rho_{1,k} |h_{R_k}|^2 + \rho_{2,k} |h_{R_k D_n}|^2} \approx \rho \min \left(\frac{|h_{R_k}|^2}{\rho_{2,k}}, \frac{|h_{R_k D_n}|^2}{\rho_{1,k}} \right) \quad (26)$$

$$\Delta_E^k = \frac{X_{R_k} Z_{E, k}}{\rho_{e,1,k} X_{R_k} + \rho_{e,2,k} Z_{E, k} + 1} \approx \frac{\rho_e |h_{R_k}|^2 |h_{R_k E}|^2}{\rho_{e,1,k} |h_{R_k}|^2} = \frac{\rho_e |h_{R_k E}|^2}{\rho_{e,1,k}} \quad (27)$$

因此, 基于式(13), RHI-D-E-MR-NOMA 系统的安全中断概率可以渐近表示为:

$$\text{SOP}_n^{k, \infty} = \Pr \left(\frac{\alpha_n \Delta_n^k}{\varepsilon_n \Delta_n^k + 1} < \frac{\alpha_n \Delta_E^k}{\eta_n \Delta_E^k + 1} \right) \approx 1 - \underbrace{\int_0^\infty F_{|h_{R_k}|^2} \left(\frac{\rho_e \rho_{2,k} \gamma}{\rho ((\eta_n - \varepsilon_n) \rho_e \gamma + \rho_{e,1,k})} \right) f_{|h_{R_k E}|^2}(\gamma) d\gamma}_{J_1} \times \underbrace{\left(1 - \int_0^\infty F_{|h_{R_k D_n}|^2} \left(\frac{\rho_e \rho_{1,k} \gamma}{\rho ((\eta_n - \varepsilon_n) \rho_e \gamma + \rho_{e,1,k})} \right) f_{|h_{R_k E}|^2}(\gamma) d\gamma \right)}_{J_2} \quad (28)$$

当 $\rho \rightarrow \infty$ 时, $\frac{y}{\rho} \rightarrow 0$, 因此 $|h_{R_k}|^2, |h_{R_k D_n}|^2$ 的 CDF 为:

$$F_{|h_{R_k}|^2} \left(\frac{\rho_e \rho_{2,k} \gamma}{\rho ((\eta_n - \varepsilon_n) \rho_e \gamma + \rho_{e,1,k})} \right) \approx \frac{\rho_e \rho_{2,k} \gamma}{\rho \lambda_{R_k} ((\eta_n - \varepsilon_n) \rho_e \gamma + \rho_{e,1,k})} \quad (29)$$

$$F_{|h_{R_k D_n}|^2} \left(\frac{\rho_e \rho_{1,k} \gamma}{\rho ((\eta_n - \varepsilon_n) \rho_e \gamma + \rho_{e,1,k})} \right) \approx \frac{Q_n}{n} \left(\frac{\rho_e \rho_{1,k} \gamma}{\rho ((\eta_n - \varepsilon_n) \rho_e \gamma + \rho_{e,1,k})} \right)^n \quad (30)$$

将式(29)、(30)代入 J_1, J_2 中并根据 $\text{SOP}_n^{\text{M-LaE-SNR}} = \prod_{k=1}^K \text{SOP}_n^k$ 可以得到式(25).

将式(25)代入式(24)中可以看到, $d = K$. 可以看出, 当 K 足够大时, 提出的 M-LaE-SNR 方案下 SOP 曲线的斜率在几何意义上趋于无穷, 也就是说, 所提出的中继选择方案的安全中断概率的斜率随着中继数目的增加而降低得更快.

4 仿真结果

在本小节中, 针对所提出的 RHI-D-E-MR-NOMA 系统模型, 分析了 RHI 对存在窃听者的多中继协作 NOMA 系统性能的影响, 通过搭建 Matlab 仿真平台进行性能分析和验证, 给出了 M-LaE-SNR 方案、RR 方案和 MRC 方案在安全性能方面的对比. 仿真中, 除非特别说明, 假设用户数 $N=3, \rho_s = \rho_R = \rho, \rho_e = 10\text{dB}$, 功率分配系数 $\alpha_1 = \frac{1}{2}, \alpha_2 = \frac{1}{3}, \alpha_3 = \frac{1}{6}$ [14], 中继数目 $K=2$. 同时, 假设所有节点都受到 RHI 的影响且 $\rho^i = \rho_s^i = \rho_R^i, \rho^r = \rho_R^r = \rho_{D_n}^r$. 在本节中, 数值结果用线条表示, 标记表示数值仿真结果.

图 2 给出了采用 M-LaE-SNR 中继选择方案时, RHI-D-E-MR-NOMA 系统三个用户的安全中断概率与

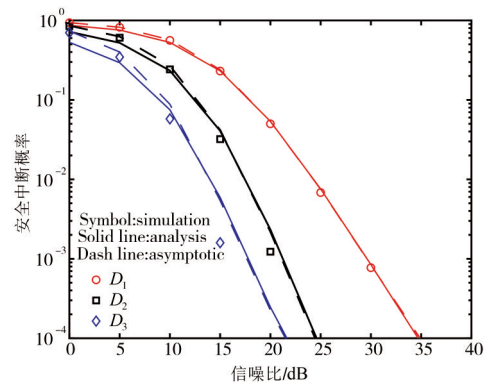


图2 联合 RHI 下安全中断概率随 ρ 的变化情况

主链路信噪比 ρ 的变化关系, 设置参数 $\rho' = \rho'' = \rho_E^r = 0.1$. 从图中我们可以看出, 在高信噪比下, 渐近结果与推导出的精确结果相吻合.

图3比较了在不同中继选择方案下, 理想和非理想情况下的 NOMA 系统的安全性能. 从图中我们可以看出 RHI 会导致系统性能显著降低. 例如, 在 M-LaE-SNR 方案下, 安全中断概率为 10^{-3} 时, 非理想硬件下对接收机 SNR 的要求相比理想条件下对接收机 SNR 的要求约高 3dB, 而且恶化程度随着 ρ 的增加而增强. 此外, 我们还观察到, 在相同信噪比条件下, 相较于另外两种中继选择方案, M-LaE-SNR 方案能够得到更高的安全性能.

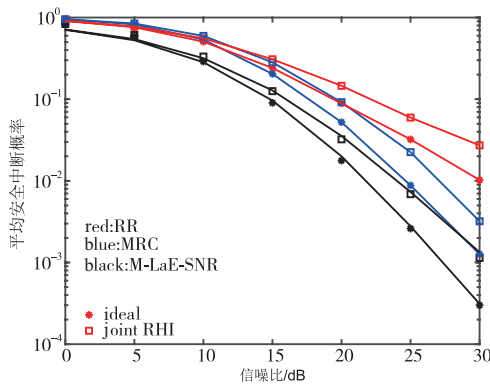
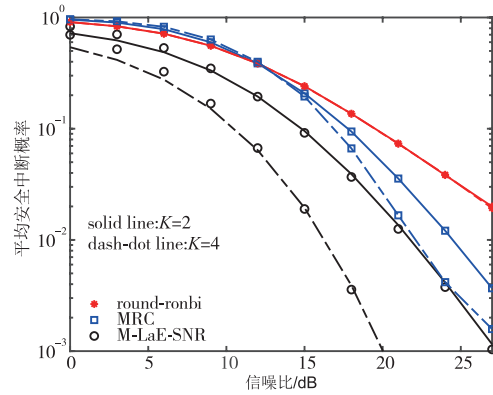


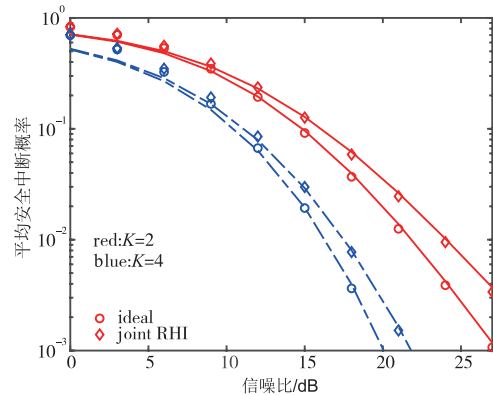
图3 三种中继选择方案下平均安全中断概率随 ρ 的变化情况

图4所示为在 RHI-D-E-MR-NOMA 系统中, 中继数目和 RHI 对安全性能分别产生的影响. 从图4(a)中可以观察到, 随着中继数目的增加, M-LaE-SNR 和 MRC 方案下的安全性能都得到了-定的改善. 然而对于 RR 方案来说, 增加中继数目对安全性能无任何变化, 这是因为 RR 方案下的安全中断概率定义为 K 个中继的平均安全中断概率. 此外, 从图4(a)我们还可以看出, 增大中继数目时, 相比于 MRC 方案, 本文所提出的方案对于安全性能的提升更加显著. 例如, 取 $\rho=18$ dB 时, 在 M-LaE-SNR 方案下, 当 K 从 2 增加到 4, 相应的平均安全中断概率从 3.68×10^{-2} 降低到 3.89×10^{-3} , 而在 MRC 方案下, 平均安全中断概率从 9.43×10^{-2} 降低到 6.65×10^{-2} . 从图4(b)中我们观察到, 在 M-LaE-SNR 方案下, 对于固定中继数目和 ρ , RHI 会导致安全中断概率显著增加. 对于 M-LaE-SNR 方案, 当系统在低信噪比范围内, 例如在 15dB 以下, 当中继个数 K 从 2 增加到 4, 在非理想硬件与理想硬件条件下, 安全中断概率下降程度几乎相同, 说明此时 RHI 对安全性能的影响程度主要与信噪比有关, 而与中继个数无关. 在中高信噪比范围内, RHI 对安全性能的影响程度随着中继个数的增加更加显著.

RHI 对不同节点的影响如图5所示. 我们观察到, 在 RHI-D-E-MR-NOMA 系统中, 当 RHI 仅发生在源节点



(a) 不同中继数目对不同中继选择方案下平均安全中断概率的影响



(b) M-LaE-SNR 方案下中继数目和 RHI 对平均安全中断概率的影响

图4 平均安全中断概率随 ρ 的变化情况

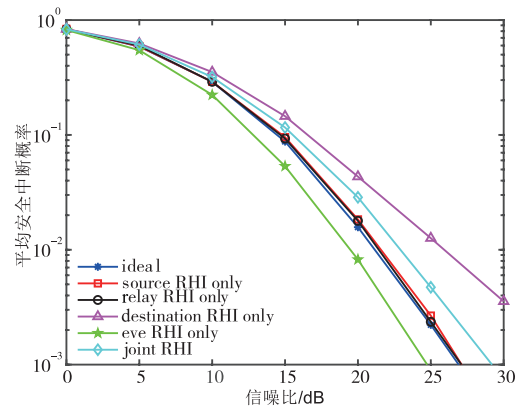


图5 RHI 在不同节点时平均安全中断概率随 ρ 的变化情况, $\rho' = \rho'' = 0.15$

与中继节点时, 对平均安全中断概率的影响较小. 而当 RHI 仅发生在目的节点或者窃听用户节点时, 则会对安全性能造成较大的影响. 例如, 当采用 M-LaE-SNR 方案时, 当安全中断概率为 10^{-2} , 与理想硬件情况相比, 当 RHI 仅发生在窃听用户节点时可以得到约 2dB 的性能提升; 而当 RHI 仅发生在目的节点时, 会造成约 3dB 的

性能损失. 此外研究结果还发现, 由于联合 RHI 不仅对合法用户造成影响, 同时也恶化了窃听用户的性能, 因此造成的总的安全性能损失略小于 RHI 仅发生在目的节点的情况.

图 6 所示为 RHI-D-E-MR-NOMA 系统中, 采用所提 M-LaE-SNR 方案下窃听信道信噪比 ρ_e 取不同值时, 用户平均安全中断概率随信噪比的变化情况. 从图 6 中可以看出, 随着 ρ_e 减小时, 能够有效提高用户的安全中断性能.

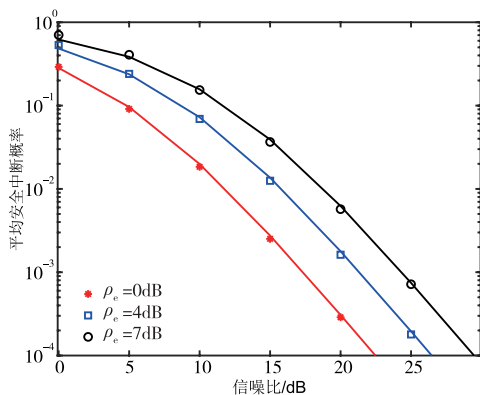


图 6 不同 ρ_e 取值下平均安全中断概率随 ρ 的变化情况

5 结论

本文针对所提出的 RHI-D-E-MR-NOMA 系统模型, 研究了在瑞利衰落条件下, RHI 对系统用户安全中断性能的影响; 为了提高系统的安全中断性能, 给出了联合考虑合法链路和窃听链路信号信息, 从而使系统目标信噪比最大化 (M-LaE-SNR) 的中继传输方案, 并分析了所提方案下的用户安全中断概率, 给出了其闭合表达式. 相对于 RR 与 MRC 方案, 所提出的 M-LaE-SNR 方案提高了用户的安全性能. 并且仿真结果表明, RHI 的存在会降低系统安全性能, 且影响程度主要与主链路信噪比 ρ 以及协作中继个数有关. 并且不同节点处的 RHI 对系统安全性能造成的影响程度也不同.

参考文献

- [1] Wu W, Zhou F H, Hu Q Y, et al. Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks[J]. IEEE Transactions on Communications, 2020, 68(1): 493 – 505.
- [2] Ding Z G, Peng M, Poor H V. Cooperative non-orthogonal multiple access in 5G systems[J]. IEEE Communications Letters, 2015, 19(8): 1462 – 1465.
- [3] Ding Z G, Dai H Y, Poor H V. Relay selection for cooperative NOMA[J]. IEEE Wireless Communications Letters, 2016, 5(4): 416 – 419.
- [4] Mukherjee A, Fakoorian S A A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1550 – 1573.
- [5] Chen J, Yang L, Alouini M. Physical layer security for cooperative NOMA systems[J]. IEEE Transactions on Vehicular Technology, 2018, 67(5): 4645 – 4649.
- [6] Zheng B, Wen M, Wang C, et al. Secure NOMA based two-way relay networks using artificial noise and full duplex[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(7): 1426 – 1440.
- [7] Lei H J, Yang Z X, Park K, et al. Secrecy outage analysis for cooperative NOMA systems with relay selection schemes[J]. IEEE Transactions on Communications, 2019, 67(9): 6282 – 6298.
- [8] 李美玲, 田莉莉, 杨晓霞, 等. 基于 STBC 的无线认知 NOMA 系统物理层安全性能研究[J]. 电子学报, 2020, 48(3): 463 – 469.
Li Mei-ling, Tian Li-li, Yang Xiao-xia, et al. On the secrecy performance of NOMA cognitive radio networks with STBC[J]. Acta Electronica Sinica, 2020, 48(3): 463 – 469. (in Chinese)
- [9] Xiang Z W, Yang W W, Cai Y M, et al. Secure transmission design in HARQ assisted cognitive NOMA networks[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 2528 – 2541.
- [10] Burg A, Studer C, Wenk M. MIMO transmission with residual transmit-RF impairments[A]. 2010 International ITG Workshop on Smart Antennas[C]. Bremen, Germany: IEEE, 2010. 189 – 196.
- [11] Bjornson E, Matthaiou M, Debbah M. A new look at dual-hop relaying: Performance limits with hardware impairments[J]. IEEE Transactions on Communications, 2013, 61(11): 4512 – 4525.
- [12] Ding F, Wang H, Zhang S L, et al. Impact of residual hardware impairments on non-orthogonal multiple access based amplify-and-forward relaying networks[J]. IEEE Access, 2018, 6: 15117 – 15131.
- [13] Makarfi A U, Rabie K M, Kaiwartya O, et al. Physical layer security in vehicular networks with reconfigurable intelligent surfaces[A]. 2020 IEEE 91st Vehicular Technology Conference[C]. Antwerp, Belgium: IEEE, 2020. 1 – 6.
- [14] Li M L, Selim B, Muhaidat S, et al. Effects of residual hardware impairments on secure NOMA-based cooperative systems[J]. IEEE Access, 2020, 8: 2524 – 2536.

- [15] Matthaiou M, Papadogiannis A, Bjornson E, et al. Two-way relaying under the presence of relay transceiver hardware impairments [J]. IEEE Communications Letters, 2013, 17(6): 1136 – 1139.
- [16] Men J J, Ge J H, Zhang C S. Performance analysis of non-orthogonal multiple access for relaying networks over Nakagami-m fading channels [J]. IEEE Transactions on Vehicular Technology, 2017, 66(2): 1200 – 1208.
- [17] Gradshteyn I S, Ryzhik I M. Table of Integrals, Series and Products (7th ed) [M]. San Diego, CA, USA: Academic, 2007.
- [18] Hildebrand F B. Introduction to Numerical Analysis [M]. London: McGraw-Hill, 1974.
- [19] Yue X W, Liu Y W, Yao Y Y, et al. Secure communications in a unified non-orthogonal multiple access framework [J]. IEEE Transactions on Wireless Communications, 2020, 19(3): 2163 – 2178.

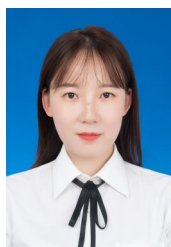
作者简介



李美玲 女, 1982年生于山西宁武. 2012年毕业于北京邮电大学获博士学位. 现为太原科技大学教授. 主要研究方向为认知无线电、协作通信、NOMA和物理层安全技术.
E-mail: meiling_li@126.com



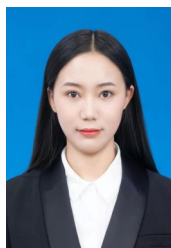
王安红 女, 1972年生于山西闻喜. 2009年毕业于北京交通大学获博士学位. 现为太原科技大学教授. 主要研究方向为图像视频编码与传输、压缩感知、秘密图像共享.
E-mail: ahwang@tyust.edu.cn



陈 琴(通信作者) 女, 1994年生于安徽池州. 现为太原科技大学电子信息工程学院硕士研究生, 主要研究方向为基于非正交多址接入系统的物理层安全性能.
E-mail: 773574827@qq.com



董增寿 男, 1970年生于山西寿阳. 2009年毕业于太原科技大学获博士学位. 现为太原科技大学教授. 主要研究方向为故障诊断、图像处理与模式识别、专网通信技术等.
E-mail: dongzs@tyust.edu.cn



杨晓霞 女, 1995年生于山西阳曲. 现为太原科技大学电子信息工程学院硕士研究生, 主要研究方向为无线网络的物理层安全性能.
E-mail: 2509085887@qq.com



Sami Muhaidat 男, Khalifa大学教授. 主要研究方向为无线通信关键技术、物理层安全、物联网技术等.
E-mail: muhaidat@ieee.org