

6-1-2020

Performance Analysis on Multiuser Untrusted Amplify-and-Forward Relay Networks

Deng Dan

1. *Guangzhou Panyu Polytechnic, Guangzhou 511483, China;*

Zhou Wen

2. *Nanjing Forestry University, Nanjing 210037, China;*

Follow this and additional works at: <https://dc-china-simulation.researchcommons.org/journal>



Part of the [Artificial Intelligence and Robotics Commons](#), [Computer Engineering Commons](#), [Numerical Analysis and Scientific Computing Commons](#), [Operations Research, Systems Engineering and Industrial Engineering Commons](#), and the [Systems Science Commons](#)

This Paper is brought to you for free and open access by Journal of System Simulation. It has been accepted for inclusion in Journal of System Simulation by an authorized editor of Journal of System Simulation.

Performance Analysis on Multiuser Untrusted Amplify-and-Forward Relay Networks

Abstract

Abstract: The effect of the untrusted relaying node was investigated on the secrecy outage probability (SOP) of amplify-and-forward (AF) relay networks in the presence of direct links and multiple users. In the considered system, the best user was selected according a certain criterion. It transmitted signals to the destination node with the aid of the untrusted relaying node. *To reduce the useful information leakage, three selection criteria were proposed based on the channel state information of the direct and/or relaying link. The closed-form analytical SOP and the corresponding asymptotic expressions were derived.* Computer simulation was conducted to validate the theoretical analysis. The SOP performance with the proposed three criteria was compared and their respective diversity orders were proposed.

Keywords

secrecy outage probability, amplify-and-forward, relay networks, user selection

Recommended Citation

Deng Dan, Zhou Wen. Performance Analysis on Multiuser Untrusted Amplify-and-Forward Relay Networks[J]. Journal of System Simulation, 2017, 29(8): 1822-1828.

多用户不可信放大转发无线中继网络安全性能分析

邓单¹, 周雯²

(1. 广州番禺职业技术学院, 广东 广州 511483; 2. 南京林业大学, 江苏 南京 210037)

摘要: 针对放大转发无线中继网络, 对直接链路和中继链路进行联合设计, 研究不可信中继节点对系统安全截断概率(SOP, secrecy outage probability)性能的影响。根据不同的选择准则, 最佳用户被选中, 在不可信中继节点的协助下, 最佳用户向目标用户发送信号。为减少信息泄漏, 基于直接链路和中继链路的信道状态信息条件, 我们提出三种不同的选择准则, 并且推导了不同准则下 SOP 的解析式及其渐近表达式。数值仿真对比了三种准则下系统的 SOP 性能, 给出了各自的分集增益阶数, 验证了理论分析。

关键词: 安全截断概率; 放大转发; 中继网络; 用户选择

中图分类号: TN 802

文献标识码: A

文章编号: 1004-731X (2017) 08-1822-07

DOI: 10.16182/j.issn1004731x.joss.201708024

Performance Analysis on Multiuser Untrusted Amplify-and-Forward Relay Networks

Deng Dan¹, Zhou Wen²

(1. Guangzhou Panyu Polytechnic, Guangzhou 511483, China; 2. Nanjing Forestry University, Nanjing 210037, China)

Abstract: The effect of the untrusted relaying node was investigated on the secrecy outage probability (SOP) of amplify-and-forward (AF) relay networks in the presence of direct links and multiple users. In the considered system, the best user was selected according a certain criterion. It transmitted signals to the destination node with the aid of the untrusted relaying node. To reduce the useful information leakage, three selection criteria were proposed based on the channel state information of the direct and/or relaying link. The closed-form analytical SOP and the corresponding asymptotic expressions were derived. Computer simulation was conducted to validate the theoretical analysis. The SOP performance with the proposed three criterions was compared and their respective diversity orders were proposed.

Keywords: secrecy outage probability; amplify-and-forward; relay networks; user selection

引言

无线信道天然的广播特性使协作中继网络的物理层安全问题吸引了广泛的关注。Wyners 及其

后续研究者建立了基于窃听信道的研究框架, 并逐步深入到多天线系统^[1-3]。为进一步防止信息泄漏, 相关研究提出基于人工噪声^[4-6]和天线选择^[7]的发射策略, 并进行了深入分析。文献[8]研究了安全中继系统中的波束成形问题, 并证明了在非理想信道状态信息(Channel State Information, CSI)下, 秩为 1 的波束成形策略是全局最优算法。文献[9]则关注理想信道状态信息条件下最优成形算法。文献[10-11]研究反馈延迟对安全截断概率(SOP)的影响作用。

收稿日期: 2016-10-21 修回日期: 2016-12-16;
基金项目: 国家青年自然科学基金(61601275), 广州市科技计划(201707010389), 广州番禺职业技术学院“青山湖青年学者”科研项目(2016Q001), 广州市教育局 2016 年市属高校科研项目(1201620439), 京信通信研究基金(H2017007);

作者简介: 邓单(1981-), 男, 湖北京山, 博士, 副教授, 研究方向为无线通信, 物理层安全; 周雯(通讯作者 1981-), 男, 安徽, 博士, 副教授, 研究方向为无线通信与优化。



<http://www.china-simulation.com>

• 1822 •

此外, 用户选择算法能有效发掘无线通信系统中的多用户分集增益, 也被广泛应用于增强系统的安全性能。文献[12]中提出三种选择准则, 并推导了相应的 SOP 解析表达式。类似地, 基于 SOP 最小化, 文献[13]提出中继节点与干扰节点的最优选择准则。基于统计位置分布架构, 文献[14]详细分析了窃听者随机分布条件上的安全通信机制。然而, 此类文献并没有考虑当中继节点存在信息泄露情况下的安全通信方法。

更进一步, 在一些应用场合中, 合法链路用户需要利用中继节点协作传输, 同时还需要防止不可信中继节点的窃听。基于不可信中继, 文献[15]提出联合用户与中继节点的迭代式波束成形算法; 针对不可信中继节点阵列, 文献[16]利用极值理论推导了遍历安全速率(ergodic secrecy rate, ESR)的解析式和下界。文献[17]从容量角度分析在不可信中继条件下的安全通信问题; 基于单用户不可信中继网络, 文献提出基于机会通信的安全传输机制, 推导了严格的 SOP 表达式, 并设计了基于直接链路或者中继链路的传输模式。上述文献大多关注于中继链路的优化问题, 没有充分考虑直接链路对多用户安全通信的积极作用。本文将单用户不可信中继网络扩展到多用户网络, 并同时考虑直接链路和中继链路对安全通信的性能影响, 推导不同准则下严格的 SOP 表达式及其渐近分析式。

本文针对 AF 无线中继网络, 对直接链路和中继链路进行联合设计, 研究不可信中继节点对系统 SOP 性能的影响。根据不同的选择准则, 最佳用户被选中; 在不可信中继节点的协助下, 最佳用户向目标用户发送信号。为减少信息泄露, 基于直接链路和中继链路的信道状态信息条件, 我们提出三种不同的选择准则。为深入理解不可信中继链路对系统 SOP 性能的影响, 我们推导了不同准则下 SOP 的解析式及其渐近表达式。数值仿真结果也进一步验证了理论分析。

1 系统模型与假设

图 1 给出了不可信 AF 无线中继网络的系统模型。系统模型中包括 N 个用户节点 (S_1, S_2, \dots, S_N), 一个不可信 AF 中继节点(Relay node, R)以及目标节点(Destination Node, D)。在用户节点与目标节点之间同时存在直接链路和中继链路。所有节点假设为单天线配置且只能工作于时分半双工模式。

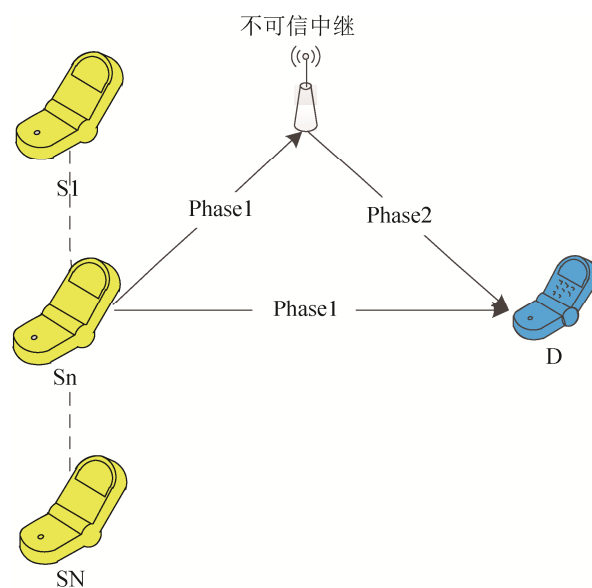


图 1 基于用户选择的不可信 AF 无线中继网络的系统模型
Fig. 1 System model of untrusted AF wireless relay network with user selection

中继网络以两阶段为基本周期进行信息传输。第一阶段, 从 N 个用户节点中选择一个最佳用户, 其他用户保持静默。此时, 目标节点与中继节点同时对选中用户的发射信号进行接收。此时, 中继节点还可以对用户节点进行窃听。多用户选择算法的目标是保证合法链路容量最大化同时尽量减少对不可信中继节点的信息泄露。在第二阶段中, 中继节点对第一阶段中的接收信号进行放大转发, 并向目标节点进行发射。为恢复出原始信息, 目标节点通过对直接链路和中继链路接收到的信号进行最大比合并。每个链路的接收信号的噪声均建模为加性高斯白噪声, 且均值为 0, 方差为 N_0 。我们使用符号 $h_{S_n R} \sim \mathcal{CN}(0, \alpha)$, $h_{S_n D} \sim \mathcal{CN}(0, \beta)$, $h_{RD} \sim \mathcal{CN}(0, \varepsilon)$ 分别表示 $S_n - R$, $S_n - D$ 以及 $R - D$ 链

路之间的瞬时信道衰落系数。假设所有链路衰落模型均为准静态瑞利块衰落，且彼此统计独立。信道衰落系数在每次发射周期中保持恒定。

假设用户节点 S_n 在第一阶段被选择为最佳用户，则中继节点的接收信号可表示为

$$r_{S_nR} = \sqrt{P_S} x_n h_{S_nR} + n_{R}, \quad (1)$$

式中： P_S 表示用户节点的发射功率； x_n 表示用户节点 S_n 的发射信号； $n_R \sim \mathcal{CN}(0, N_0)$ 表示中继节点所接收到的噪声分量。第一阶段中，中继节点的信噪比可表示为：

$$\text{SNR}_R^{(n)} = \rho_S \gamma_{S_nR} \quad (2)$$

式中： $\rho_S \triangleq P_S / N_0$ ， $\gamma_{S_nR} \triangleq |h_{S_nR}|^2$ 表示 $S_n - R$ 链路的瞬时信道衰落系数之功率。不可信中继节点可从上述链路中窃听到用户节点的信息，此时非法链路的容量可表示为：

$$C_R^{(n)} = \frac{1}{2} \log_2(1 + \text{SNR}_R^{(n)}) \quad (3)$$

同理，目标节点的接收信号可表示为：

$$r_{S_nD} = \sqrt{P_S} x_n h_{S_nD} + n_{D,1} \quad (4)$$

式中： $n_{D,1} \sim \mathcal{CN}(0, N_0)$ 表示目标节点的在第一阶段的接收端噪声。此时目标节点的 SNR 可表示为：

$$\text{SNR}_{D,1}^{(n)} = \rho_S \gamma_{S_nD} \quad (5)$$

式中： $\gamma_{S_nD} \triangleq |h_{S_nD}|^2$ 表示 $S_n - D$ 链路的瞬时信道衰落系数功率。

在第二阶段中，中继节点对第一阶段的接收信号进行放大转发，并保持发射功率为 P_R 。对应的第二阶段的功率放大因子为

$$\kappa_n = \sqrt{\frac{P_R}{P_S \gamma_{S_nR} + N_0}} \quad (6)$$

考虑到总发射功率的限制，我们假设两阶段的总发射功率为 P_T ，且两阶段之间的功率满足如下约束关系：

$$P_R = \eta P_T, P_S = (1 - \eta) P_T \quad (7)$$

式中： η 表示第二阶段的归一化功率因子。此时目标节点在第二阶段的接收信号可表示为：

$$r_{RD} = \kappa_n r_{S_nR} h_{RD} + n_{D,2} \quad (8)$$

式中： $n_{D,2} \sim \mathcal{CN}(0, N_0)$ 表示目标节点的在第二阶

段的接收端噪声。相应地，第二阶段目标节点的信噪比可表示为：

$$\text{SNR}_{D,2}^{(n)} = \frac{\rho_S \gamma_{S_nR} \cdot \rho_R \gamma_{RD}}{\rho_S \gamma_{S_nR} + \rho_R \gamma_{RD} + 1} \quad (9)$$

式中： $\rho_R \triangleq \frac{P_R}{N_0}$ ， $\gamma_{RD} \triangleq |h_{RD}|^2$ 。目标节点使用最大比

合并接收机对两个阶段的接收信号进行合并处理，其等效的信噪比为两次独立接收信噪比之和，即：

$$\text{SNR}_D^{(n)} = \text{SNR}_{D,1}^{(n)} + \text{SNR}_{D,2}^{(n)} \quad (10)$$

合法链路的信道容量可表示为：

$$C_M^{(n)} = \frac{1}{2} \log_2(1 + \text{SNR}_D^{(n)}) \quad (11)$$

系统的安全容量为合法链路容量与窃听信道容量之差，即

$$R_S^{(n)} = [C_M^{(n)} - C_R^{(n)}]^+ = \frac{1}{2} \left[\log_2 \frac{1 + \rho_S \gamma_{S_nD} + \frac{\rho_S \gamma_{S_nR} \cdot \rho_R \gamma_{RD}}{\rho_S \gamma_{S_nR} + \rho_R \gamma_{RD} + 1}}{1 + \rho_S \gamma_{S_nR}} \right]^+ \quad (12)$$

式中： $[x]^+ \triangleq \max(x, 0)$ 。

为简化分析复杂度，我们采用文献[18]中的不等式(22)，即

$$\frac{1}{2} \min(X, Y) \leq \frac{XY}{X+Y} \leq \min(X, Y) \quad (13)$$

瞬时的安全截断概率可表示为：

$$P_{out}^{(n)} = \Pr[R_S^{(n)} \leq R_0] = \Pr[z_n \leq \gamma_0] \quad (14)$$

式中： $z_n \triangleq \frac{\frac{1}{\rho_S} + \gamma_{S_nD} + \zeta \min(\gamma_{S_nR}, \frac{\rho_R}{\rho_S} \gamma_{RD})}{\frac{1}{\rho_S} + \gamma_{S_nR}}$ ，且

$\gamma_0 \triangleq 2^{2R_0}$ 。 R_0 表示安全容量门限值。 $\zeta = 1$ 和 $\zeta = 0.5$ 分别对应于截断概率的上界与上界。

2 用户选择准则

考虑公式(14)中的 SOP 表达式，最优的用户选择准则可表示为：

$$n_1^* = \arg \max_{1 \leq n \leq N} \{z_n\} \quad (15)$$

从式(15)易知，最优选择准则需要同时获取直接链路和中继链路的信道状态信息(CSI)，从而会给系统实现增加额外的负担。然而，在一些通信场

景下, 系统可能只能获得直接链路或者中继链路的 CSI。在这些场景下, 我们需要考虑更为简化的选择准则。

首先考虑系统只能获取直接链路 CSI 的场景, 其对应的次优选择准则可表示为:

$$n_2^* = \arg \max_{1 \leq n \leq N} \{\gamma_{S_n D}\} \quad (16)$$

此准则选择直接链路的最大信道增益。当系统只能获取直接链路 CSI 条件下, 能保证安全速率的最大化。

当系统只能获得中继链路 CSI 条件下, 其对应的次优选择准则为:

$$n_3^* = \operatorname{argmin}_{1 \leq n \leq N} \{\gamma_{S_n R}\} \quad (17)$$

由上式易知, 此准则选择中继链路增益最小的用户。当只能获取中继链路 CSI 条件下, 通过最小化窃听信道容量, 可使得安全速率最大化。

为表述方便, 我们分别使用准则 I, II 与 III 分别代表公式(15), (16)和(17)。在下面的章节中, 我们将分析三种准则对应的 SOP 解析表达式及对应的渐近分析式。特别地, 准则 I 以最大的复杂度达到最优性能。

3 安全截断概率分析

3.1 选择准则 I

对于最优选择准则 I, 我们首先分析其 SOP 解析表达式, 有如下定理。

定理 I: 对于选择准则 I, 其安全截断概率(SOP)可表示为:

$$P_{\text{out}}^{(n_1^*)} = \Pr[z_{n_1^*} \leq \gamma_0] = \sum_{n=1}^N \binom{N}{n} m_3^{N-n} m_4^n \frac{1}{1 + \frac{m_2 \varepsilon \rho_R}{\alpha \rho_S} n} \quad (18)$$

式中:

$$\begin{aligned} m_1 &\triangleq \frac{(\gamma_0 - 1)}{\beta \rho_S}, m_2 \triangleq 1 + \frac{\alpha(\gamma_0 - \xi)}{\beta}, \\ m_3 &\triangleq 1 - \frac{e^{-m_1}}{m_2}, m_4 \triangleq \xi \frac{e^{-m_1}}{m_2} \frac{\alpha}{\beta} \frac{1}{m_2 + \frac{\alpha}{\beta}} \end{aligned} \quad (19)$$

证明: 首先, 当 γ_{RD} 固定时, 考虑 z_n 的累积分布函数

$$F_{z_n | \gamma_{RD}}(\gamma_0) = \Pr[z_n \leq \gamma_0 | \gamma_{RD}] \quad (20)$$

根据文献[19]中的全概率展开公式, 式(20)可展开为

$$\begin{aligned} F_{z_n | \gamma_{RD}}(\gamma_0) &= \Pr\left[\frac{1}{\rho_S} + \gamma_{S_n D} + \xi \gamma_{S_n R} \leq \gamma_0 \left(\frac{1}{\rho_S} + \gamma_{S_n R}\right), \right. \\ &\left. \gamma_{S_n R} \leq \frac{\rho_R}{\rho_S} \gamma_{RD} | \gamma_{RD}\right] + \Pr\left[\frac{1}{\rho_S} + \gamma_{S_n D} + \xi \frac{\rho_R}{\rho_S} \gamma_{RD} \leq \right. \\ &\left. \gamma_0 \left(\frac{1}{\rho_S} + \gamma_{S_n R}\right), \gamma_{S_n R} > \frac{\rho_R}{\rho_S} \gamma_{RD} | \gamma_{RD}\right] \end{aligned} \quad (21)$$

式(21)经过必要的数学推导, 可得

$$F_{z_n | \gamma_{RD}}(\gamma_0) = 1 - \frac{e^{-m_1}}{m_2} + \frac{\alpha}{\beta} e^{-\frac{m_2 \rho_R}{\alpha \rho_S} \gamma_{RD}} \frac{\xi e^{-m_1}}{(m_2 + \frac{\alpha}{\beta}) m_2} \quad (22)$$

根据排序统计理论^[20], 选择准则 I 对应的 $z_{n_1^*}$ 的累积分布函数可表示为:

$$F_{z_{n_1^*} | \gamma_{RD}}(\gamma_0) = [F_{z_n | \gamma_{RD}}(\gamma_0)]^N \quad (23)$$

使用条件概率公式, 有

$$F_{z_{n_1^*} | \gamma_{RD}}(\gamma_0) = \int_0^{+\infty} F_{z_{n_1^*} | (\gamma_{RD}=w)}(\gamma_0) f_{\gamma_{RD}}(w) dw = \sum_{n=0}^N \binom{N}{n} m_3^{N-n} m_4^n \frac{1}{1 + \frac{m_2 \varepsilon \rho_R}{\alpha \rho_S} n} \quad (24)$$

定理 I 证毕。

3.2 选择准则 II

考虑公式(16)中的选择准则 II, $\gamma_{S_{n_2^*} D}$ 的累积分布函数可表示为

$$F_{\gamma_{S_{n_2^*} D}}(u) = (1 - e^{-\frac{u}{\beta}})^N = \sum_{n=0}^N \binom{N}{n} (-1)^n e^{-\frac{nu}{\beta}} \quad (25)$$

对应的概率分布函数为

$$f_{\gamma_{S_{n_2^*} D}}(u) = \sum_{n=1}^N \binom{N}{n} (-1)^{n-1} \frac{n}{\beta} e^{-\frac{nu}{\beta}} \quad (26)$$

则选择准则 II 对应的安全截断概率可表示为:

$$P_{\text{out}}^{(n_2^*)} = \Pr[z_{n_2^*} \leq \gamma_0] = F_{z_{n_2^*}}(\gamma_0) = \Pr\left[\frac{1}{\rho_S} + \gamma_{S_{n_2^*} D} + \xi \min(\gamma_{S_{n_2^*} R}, \frac{\rho_R}{\rho_S} \gamma_{RD}) \leq \gamma_0\right] \quad (27)$$

考虑到 $\gamma_{S_n^*D}$ 与 $\gamma_{S_n^*R}$ 的统计独立性, 上式可简化为:

$$F_{z_{n_2}^*}(\gamma_0) = \Pr\left[\frac{1 + \gamma_{S_n^*D} + \xi \min(\gamma_{S_n^*R}, \frac{\rho_R}{\rho_S} \gamma_{RD})}{\rho_S + \gamma_{S_n^*R}} \leq \gamma_0\right] \quad (28)$$

再根据全概率公式上式进行展开, 并将公式(25)和(26)代入展开式, 选择准则 II 对应的安全截断概率可表示为:

$$P_{out}^{(n_2^*)} = 1 - \sum_{n=1}^N \frac{c_{1,n}}{\alpha n} \left[1 - \frac{\alpha}{\beta} \frac{\xi}{c_{2,n}} \frac{n}{1 + \frac{\alpha n}{\beta} \gamma_0}\right] \quad (29)$$

$$c_{1,n} \triangleq \binom{N}{n} (-1)^{n-1} e^{-\frac{n(\gamma_0-1)}{\beta \rho_S}}, \quad (30)$$

$$c_{2,n} \triangleq \frac{\varepsilon \rho_R}{\alpha \rho_S} + n \frac{\varepsilon \rho_R}{\alpha \rho_S} (\gamma_0 - \xi) + 1$$

3.3 选择准则 III

考虑公式(17)中的选择准则 III, $\gamma_{S_n^*D}$ 的累积分布函数可表示为

$$F_{\gamma_{S_n^*D}}(u) = 1 - e^{-\frac{Nu}{\alpha}} \quad (31)$$

对应的概率分布函数为

$$f_{\gamma_{S_n^*D}}(u) = \frac{N}{\alpha} e^{-\frac{Nu}{\alpha}} \quad (32)$$

类似地, 考虑到 $\gamma_{S_n^*D}$ 与 $\gamma_{S_n^*R}$ 的统计独立性, 选择准则 III 对应的安全截断概率可表示为

$$P_{out}^{(n_3^*)} = F_{z_{n_3}^*}(\gamma_0) = \Pr\left[\frac{1 + \gamma_{S_n^*D} + \xi \min(\gamma_{S_n^*R}, \frac{\rho_R}{\rho_S} \gamma_{RD})}{\rho_S + \gamma_{S_n^*R}} \leq \gamma_0\right] \quad (33)$$

根据全概率展开公式, 将式(32)代入式(33), 得

$$P_{out}^{(n_3^*)} = 1 - \frac{e^{-\frac{\gamma_0-1}{\beta \rho_S}}}{1 + \frac{\alpha(\gamma_0-\xi)}{N\beta}} + \frac{e^{-\frac{\gamma_0-1}{\beta \rho_S}}}{1 + \frac{\alpha(\gamma_0-\xi)}{N\beta}} \times \frac{\frac{\xi \alpha}{N\beta}}{1 + \frac{\varepsilon N \rho_R}{\alpha \rho_S} + \frac{\varepsilon \rho_R}{\beta \rho_S} (\gamma_0 - \xi)} \quad (34)$$

3.4 渐近性能分析

为了更深入地了解不同选择准则下 SOP 性能, 我们通过渐近性能进行对比。渐近条件下, 系统的总发射功率和直接链路的信道增益均假设为足够大。

首先考虑公式(18)中选择准则 I 对应的 SOP 解析式, 渐近条件下的 SOP 可表示为:

$$P_1^{asy} \triangleq \lim_{\beta \rightarrow \infty, P_T \rightarrow \infty} P_{out}^{(n_1^*)} = \left(\frac{\alpha}{\beta}\right)^N \sum_{n=0}^N \binom{N}{n} (\gamma_0 - 1)^{N-n} \frac{1}{1 + \frac{n\varepsilon \rho_R}{\alpha \rho_S}} \quad (35)$$

从式(35)可看出, 渐近条件下, 选择准则 I 的分集增益阶数与用户节点数目 N 相等。

同样, 考虑公式(29)中选择准则 II 对应的 SOP 解析式, 通过分析可知, 其渐近 SOP 分集增益阶数也为 N 。类似地, 考虑公式(34)中选择准则 III 对应的 SOP 解析式, 其相应的渐近 SOP 可表示为

$$P_3^{asy} \triangleq \lim_{\beta \rightarrow \infty, P_T \rightarrow \infty} P_{out}^{(n_3^*)} = \frac{\alpha}{N\beta} \left[\frac{1}{1 + \frac{\varepsilon N \rho_R}{\alpha \rho_S}} + (\gamma_0 - \xi)\right] \quad (36)$$

从式(36)可知, 对应选择准则 III, 其对应的分集增益阶数为 1, 与用户节点数目无关。

4 数值仿真与分析

为验证以上理论分析的正确性, 我们采用计算机数值仿真进行对比分析。在仿真系统中, 我们主要关注直接链路平均信道增益(β)及用户节点数目(N) 对系统安全截断概率及其渐近曲线的影响。

不失一般性, 我们假设 $h_{S_n^*R}$ 及 h_{RD} 的平均信道增益均固定为 1, 即 $\alpha = \varepsilon = 1$ 。同时, 假设所有节点的接收噪声功率均为 1, 即 $N_0 = 0$ dBmW。并且在所有仿真环境中, 系统的总发射功率为 $P_T = 20$ dBmW。

图 2 中给出了选择准则 I 对应的 SOP 解析式及其渐近式性能仿真曲线。我们还对选择准则 I 与现有单用户网络性能进行了对比, 其中标注 no selection 的曲线对应于现有的单用户算法性能曲

线。从图中易知, 基于用户选择的安全通信机制性能远优于现有算法。我们同时给出了当 $\xi = 0.5$ 及 $\xi = 1$ 对应的 SOP 上界与下界的曲线对比图。在仿真系统中, 用户节点数目 N 从 2 增长到 5。从图中我们可看到, 在所有仿真场景中, SOP 上界曲线与仿真曲线及渐近曲线吻合较好。此外, 当 N 变大时, SOP 曲线随之不断变小。这是因为当 N 变大时, 更多的用户可产生更强的多用户分集增益, 使得合法链路的容量增大。考虑到 SOP 下界曲线与数值仿真曲线吻合较松, 在下面讨论中我们只关注 SOP 上界, 即 $\xi = 0.5$ 。

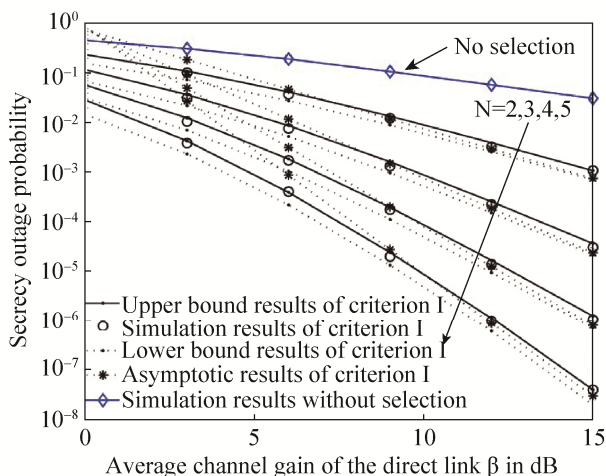


图 2 选择准则 I 对应的安全截断概率曲线

Fig. 2 Secrecy outage probability curves for Criterion I

对于选择准则 II 与选择准则 III, 同样的结论依然成立。

图 3 给出了三种选择准则下 SOP 性能的对比曲线, 仿真系统中设置参数如下: $N = 3, \beta = 12$ dB。从图中易知, 选择准则 I 明显优于选择准则 II 和 III。原因在于选择准则 I 同时考虑直接链路和中继链路的信道容量, 其选择算法为最优算法。而选择准则 II 和 III 分别只考虑直接链路和中继链路的 CSI, 两者均为次优算法。此外, 三种准则下的解析 SOP 与数值仿真曲线吻合均较好。数值仿真结果也进一步验证了理论分析的正确性。

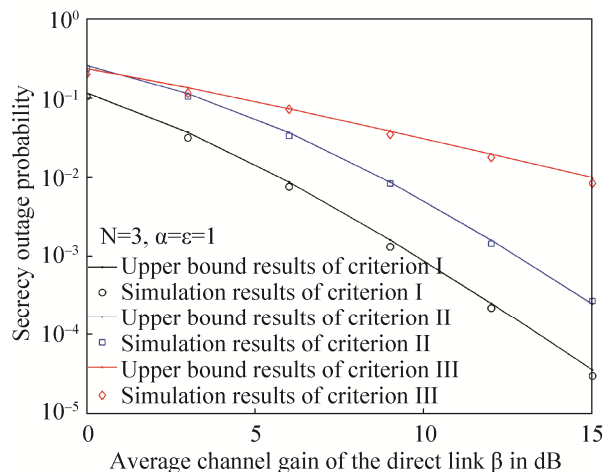


图 3 三种选择准则下的安全截断概率曲线

Fig. 3 Secrecy outage probability curves for 3 criteria

图 4 显示了用户节点数目对系统安全性能的影响。仿真系统中设置 $\beta = 12$ dB, 用户节点数目从 2 增长到 6。从图中可看到, 系统安全性能随着 N 的增长而快速增强。特别地, 选择准则 I 相比于其他两种准则表现出明显的性能增益。同样, 数值仿真的 SOP 曲线与 SOP 理论分析解析式几乎完全重合。

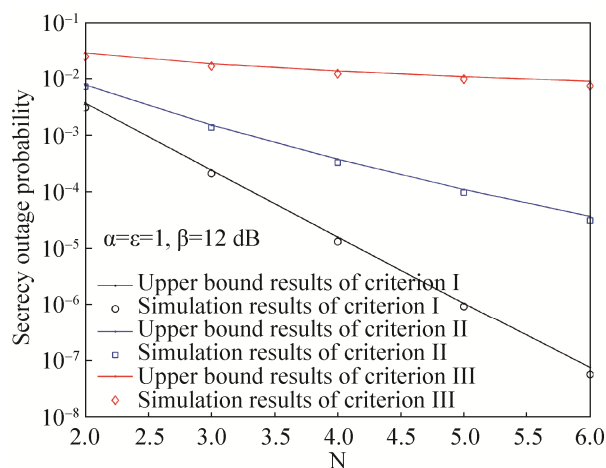
图 4 用户节点数目 N 对系统安全性能的影响

Fig. 4 Effect of number of users on secrecy performance

5 结论

本文同时考虑直接链路与中继链路的作用, 分析在不可信中继节点对系统安全截断概率的影响。在系统模型中, 最佳用户节点被选中, 并向中继节点和目标节点发射信号。为减少系统实现的复杂

度, 并基于直接链路和中继链路的信道状态信息, 我们分析了最优选择准则及两种次优选择准则。论文推导了三种选择准则下的安全截断概率的理论分析式及其渐近表达式, 并通过数值仿真结果对理论分析进行了验证。从渐近分析式可看出, 最优选择准则及基于直接链路选择的次优选择准则的分集增益阶数与用户节点数目相同, 而基于中继链路的次优选择准则其分集阶数为 1。

参考文献:

- [1] A Khisti, G W Wornell. Secure transmission with multiple antennas Part I: The MISOME wiretap channel [J]. *Information Theory, IEEE Transactions on* (S0018-9448), 2010, 56(7): 3088-3104.
- [2] A Khisti, G W Wornell. Secure transmission with multiple antennas Part II: The MIMOME wiretap channel [J]. *Information Theory, IEEE Transactions on* (S0018-9448), 2010, 56(11): 5515-5532.
- [3] A D Wyner. The wiretap channel [J]. *Bell System Technology Journal* (S0005-8580), 1975, 54(7): 1355-1387.
- [4] S Goel, R Negi. Guaranteeing secrecy using artificial noise [J]. *Wireless Communications, IEEE Transactions on* (S1536-1276), 2008, 7(6): 2180-2189.
- [5] H-M Wang, T Zheng, X-G Xia. Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading [J]. *Wireless Communications, IEEE Transactions on* (S1536-1276), 2015, 14(1): 94-106.
- [6] N Romero-Zurita, D McLernon, M Ghogho. Physical layer security by robust masked beamforming and protected zone optimization [J]. *IET Communications* (S1751-8628), 2014, 8(8): 1248-1257.
- [7] Z Ding, Z Ma, P Fan. Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise [J]. *Wireless Communications, IEEE Transactions on* (S1536-1276), 2014, 13(4): 2189-2203.
- [8] X Wang, K Wang, X-D Zhang. Secure relay beamforming with imperfect channel side information [J]. *IEEE Transactions on Vehicular Technology* (S0018-9545), 2013, 62(5): 2140-2155.
- [9] X Wang, Z Zhang, K Long. Secure beamforming for multiple antenna amplify-and-forward relay networks [J]. *Signal Processing, IEEE Transactions on* (S1053-587X), 2015, 64(6): 1477-1492.
- [10] D Deng, L Fan, R Zhao, et al. Secure communications in multiple amplify-and-forward relay networks with outdated channel state information [J]. *Transactions on Emerging Telecommunications Technologies* (S2161-3915), 2016, 33(4): 457-464.
- [11] L Fan, X Lei, R Q Hu, et al. Outdated relay selection in two-way relay network [J]. *IEEE Transactions on Vehicular Technology* (S0018-9545), 2013, 62(8): 4051-4057.
- [12] L Fan, X Lei, T Q Duong, et al. Karagiannidis, Secure multiuser communications in multiple amplify-and-forward relay networks [J]. *IEEE Transactions on Communications* (S0090-6778), 2014, 62(9): 3299-3310.
- [13] H Hui, A Swindlehurst, G Li, et al. Secure relay and jammer selection for physical layer security [J]. *Signal Processing Letters, IEEE* (S1070-9908), 2015, 22(8): 1147-1151.
- [14] T-X Zheng, H-M Wang, J Yuan, et al. Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers [J]. *IEEE Transactions on Communications* (S1536-1276), 2015, 63(11): 4347-4362.
- [15] J Mo, M Tao, Y Liu, et al. Secure beamforming for MIMO two-way communications with an untrusted relay [J]. *Signal Processing, IEEE Transactions on* (S1053-587X), 2014, 62(9): 2185-2199.
- [16] L Sun, P Ren, Q Du, et al. Security-aware relaying scheme for cooperative networks with untrusted relay nodes [J]. *Communications Letters, IEEE* (S0163-6804), 2015, 19(3): 463-466.
- [17] X He, A Yener. Cooperation with an untrusted relay: a secrecy perspective [J]. *IEEE Transactions on Information Theory* (S0018-9448), 2010, 56(8): 3807-3827.
- [18] M Seyfi, S Muhaidat, J Liang. Amplify-and-forward selection cooperation over rayleigh fading channels with imperfect CSI [J]. *Wireless Communications IEEE Transactions on* (S1536-1276), 2012, 11(1): 199-209.
- [19] B V Nguyen, K Kim. Secrecy outage probability of optimal relay selection for secure AnF cooperative networks [J]. *Communications Letters, IEEE* (S0163-6804), 2015, 19(12): 2086-2089.
- [20] H A David, H N Nagaraja. *Order Statistics* [M]. 3rd. USA: Wiley Online Library, 2003: 223-224.