不可信无线中继网络中基于用户选择的安全通信研究

邓 单[1],周 雯[2]
(1. 广州番禺职业技术学院信息工程学院,广东广州 511483 ;2. 南京林业大学信息科学技术学院,江苏南京 210037)

摘 要: 该文研究在不可信解码转发无线中继网络中,基于用户选择的安全通信策略与性能分析. 根据直接链路与中继链路的信道增益,本文提出三种不同的选择准则以提升系统的安全性;文章推导了三种选择准则下安全截断概率的闭式解析表达式及渐近表达式. 根据渐近表达式和数值仿真结果可知,次优准则可以达到与最优准则几乎相同的系统安全性能. 同时部分选择准则也能达到全分集增益性能.

关键词: 不可信中继; 用户选择; 物理层安全; 中继网络; 安全截断概率
中图分类号: TN801 **文献标识码:** A **文章编号:** 0372-2112 (2017)07-1593-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.07.007

Secure Selection for Decode-and-Forward Cooperative Networks with Untrusted Relay

DENG Dan[1], ZHOU Wen[2]
(1. *School of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou, Guangdong* 511483, *China*;
2. *College of Information Science and Technology, Nanjing Forestry University, Nanjing, Jiangsu* 210037, *China*)

Abstract: Secure communication in decode-and-forward cooperative networks with untrusted relay in the presence of direct links is investigated in this paper. In the considered system, one base-station is selected for secure transmission to the destination node with the aid of an untrusted relay node. Three selection criteria are proposed to improve the secrecy capacity based on both the direct links and the relaying links. The exact close-form expressions and corresponding asymptotic expressions on secrecy outage probability are derived. From the asymptotic expressions and simulation results, the sub-optimal criterion has the same performance with the optimal criterion. Furthermore, the partial selection criterion achieves the full diversity gain.

Key words: untrusted relay; user selection; physical-layer security; relay networks; secrecy outage probability

1 引言

无线中继技术能有效提升网络覆盖和链路质量. 由于无线信道的广播特性,使得无线中继网络中的物理层安全问题吸引了学术界和工业界的广泛关注[1~10]. 文献[4,11~13]在使用非理想信道状态信息条件下,推导了安全截断概率的闭式表达及上下界. 考虑到实际通信系统中的信道估计误差,文献[14,15]提出基于开关发射策略的安全通信方法,当合法链路信噪比大于预设门限时才进行发射,可有效提高系统安全容量. 基于中继节点业务量模型,文献[16]分析了中继节点数目随机变化情况下的安全截断概率. 基于加权选择算法,文献[17]推导了最优加权因子条件下,使用过时信道状态信息时双向中继系统安全截断概率的上下界及其渐近表达式. 考虑到实际通信系统中,信道估计的滞后效应,文献[18~23]详细分析不同的选择准则下的系统安全性能及其分集增益特点. 更进一步,中继节点也可能对合法链路进行窃听. 文献[24~27]分析了不可信中继信

收稿日期:2016-05-23;修回日期:2016-09-06;责任编辑:蓝红杰
基金项目:广州市科技计划项目(No. 201707010389);广州市教育局市属高校科研项目(No. 1201620439);广州市教育科学“十二五”规划课题(No. 1201431075);广州番禺职业技术学院“青山湖青年学者”科研项目(No. 2016Q001);京信通信研究基金(No. JX-PYP-201501, No. H2017007)广东省自然科学基金(No. 2016A030313068);国家青年自然科学基金(No. 61601275)

道对系统安全性能的影响. 然而,在不可信解码转发无线中继网络中,如何同时利用直接链路和中继链路,并通过用户选择来提升系统安全性能,目前仍少有文献关注.

本文将研究在不可信解码转发无线中继网络中,设计基于用户选择的安全通信策略,并分析直接链路和中继链路对安全截断概率的影响. 文章推导了最优选择准则和部分选择准则下安全截断概率的准确解析表达式及渐近表达式;针对次优选择准则,我们则给出安全截断概率的上下界及其渐近表达式. 从数值仿真和理论推导可以看出,使用复杂度较低的次优选择准则,可以获得与最优选择准则几乎相同的安全性能.

本文中所使用的数学符号如下:对于随机变量 X,$f_X(x)$ 表示其概率密度函数(probability density function,PDF);$F_X(x)$ 表示其概率分布函数(Cumulant Distribution Function,CDF);$x\sim\mathcal{CN}(\mu,\sigma^2)$ 表示 x 为循环对称复高斯随机变量,且其均值为 μ,方差为 σ^2;$[x]^+$ 表示截断函数,即 $[x]^+=\begin{cases}x,x\geqslant 0\\0,\text{else}\end{cases}$.

2 系统模型与假设

如图 1 所示,不可信解码转发(Decode-and-Forward,DF)无线中继网络系统模型由 M 个基站节点(S_1,S_2,$\cdots S_M$)、不可信 DF 中继节点(R)以及目标节点(D)组成. 所有节点均配置为单天线并且只能以半双工模式进行通信. 基站节点与目标节点之间存在两条通信链路:直接链路和中继链路. 直接链路由基站与目标节点之间的无线链路构成;中继链路经由中继节点进行解码后再重新发送给目标节点. 目标节点可以对两种链路的接收信号进行最大比合并,以提升通信容量. 同时假设各节点之间的链路衰落均相互独立,且为瑞利准静态块衰落,即在每个发射周期内保持恒定,且不同周期之间相互独立.

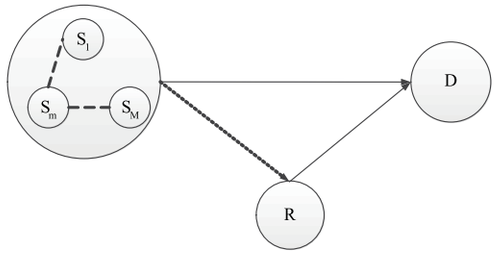

图1 基于用户选择的不可信无线中继网络安全通信系统模型

我们使用 h_{S_mR},h_{RD},h_{S_mD} 分别表示基站节点 S_m 到中继节点 R、中继节点 R 到目标节点 D 以及基站节点 S_m 到目标节点 D,其分布分别满足 $h_{S_mR}\sim\mathcal{CN}(0,\alpha)$,$h_{S_mD}\sim\mathcal{CN}(0,\beta)$ 和 $h_{S_mD}\sim\mathcal{CN}(0,\varepsilon)$.

无线中继网络的通信过程分为两阶段进行. 第一阶段,假设 M 个基站节点中的第 m 个基站 S_m 被选中,以功率 P 用于进行信号发射. 此时中继节点与目标节点的接收信号分别为:

$$r_m^R=h_{S_mR}\sqrt{P}x_m+n_R \tag{1}$$

$$r_m^{D,1}=h_{S_mD}\sqrt{P}x_m+n_{D,1} \tag{2}$$

式中 $n_R,n_{D,1}\sim\mathcal{CN}(0,N_0)$ 分别表示中继节点与目标节点接收机的高斯白噪声.

此时,中继节点 R 可以对接收信号进行窃听,窃听信道的容量可表示为:

$$C_E=\frac{1}{2}\log_2(1+\gamma u_m) \tag{3}$$

式中 u_m 为 S_m 到中继节点 R 的信道增益,即 $u_m\triangleq|h_{S_mR}|^2$;$\gamma$ 定义为系统发射端信噪比,即 $\gamma\triangleq\frac{P}{N_0}$.

此阶段中,目标节点经直接链路的有效信噪比可表示为:

$$\gamma_m^{D,1}=\gamma w_m \tag{4}$$

式中,w_m 为 S_m 到目标节点 D 的信道增益,即 $w_m\triangleq|h_{S_mD}|^2$.

第二阶段,中继节点同时还需要对接收信号进行解码并恢复出原始信息,再以相同功率 P 对目标节点进行转发. 此时目标节点经中继链路的有效信噪比可表示为:

$$\gamma_m^{D,2}=\min(\gamma u_m,\gamma v) \tag{5}$$

式中,v 为中继节点 R 到目标节点 D 的信道增益,即 $v\triangleq|h_{RD}|^2$. 目标节点最后对中继链路与直接链路进行最大比合并,其最终的信噪比为:

$$\gamma_m^D=\gamma_m^{D,1}+\gamma_m^{D,2}=\gamma w_m+\min(\gamma u_m,\gamma v) \tag{6}$$

相应地,合法链路的系统容量可表示为:

$$\begin{aligned}C_M&=\frac{1}{2}\log_2(1+\gamma_m^D)\\&=\frac{1}{2}\log_2[1+\gamma w_m+\min(\gamma u_m,\gamma v)]\end{aligned} \tag{7}$$

不可信无线中继网络系统的安全容量为合法链路容量与窃听链路容量之差,即

$$\begin{aligned}C_S&=[C_M-C_E]^+\\&=\left[\frac{1}{2}\log_2\left[\frac{1+\gamma w_m+\min(\gamma u_m,\gamma v)}{1+\gamma u_m}\right]\right]^+\end{aligned} \tag{8}$$

对应的安全截断概率(SOP)可表示为:

$$\begin{aligned}P_{\text{out}}&=\Pr[C_S<R_S]\\&=\Pr\left[\frac{1+\gamma w_m+\min(\gamma u_m,\gamma v)}{1+\gamma u_m}<\gamma_S\right]\end{aligned} \tag{9}$$

式中,R_S 表示安全容量门限,且 $\gamma_S\triangleq 2^{2R_S}$. 为简化理论分析的复杂度,当发射功率 P 足够大时,安全截断概率可近似表达为:

$$P_{\text{out}} \approx Pr\left[\frac{w_m + \min(u_m, v)}{u_m} < \gamma_S\right] \tag{10}$$

3　用户选择准则

根据安全截断概率表达式,通过一定的选择准则可有效降低截断概率. 定义 $z_m \triangleq \dfrac{w_m + \min(u_m, v)}{u_m}$,根据公式易知,其最优选择准则可表示为:

$$m_1^* = \arg\max_{m \in [1,M]}(z_m) \tag{11}$$

由上式可以看出,最优选择准则需要同时连续监测直接链路和中继链路的增益,直接加重了系统的负担和复杂性. 实际的无线通信场景中,系统可能只能获得相邻链路的信道增益,而难于获得其他链路的信道增益. 基于以上考虑,我们还需要设计复杂度更低且更为实用的选择准则.

考虑安全截断概率表达式中的存在着以下的上下界关系:

$$\frac{w_m}{u_m} < z_m \leqslant \frac{w_m + u_m}{u_m} \tag{12}$$

当系统只能获取与基站节点相邻的信道增益时,次优选择准则可表示为

$$m_2^* = \arg\max_{m \in [1,M]}\left(\frac{w_m}{u_m}\right) \tag{13}$$

上述选择准则,通过选取直接链路与窃听链路信道增益之比最大值对应的基站节点,可使得在极限情况下 z_m 取得最大值,从而提高系统安全容量.

更进一步,当系统只能获得直接链路的信道增益时,其对应的部分选择准则可表示为:

$$m_3^* = \arg\max_{m \in [1,M]}(w_m) \tag{14}$$

显然,部分选择准则只需要监测直接链路的信道增益,复杂度最低. 由于只关注直接链路的信道增益,部分选择准则无法对中继链路的信道增益进行选择,故而不能直接保证安全容量最大化,其性能会劣于最优选择准则.

4　安全截断概率分析

本节中我们将分别对三种选择准则下的安全截断概率进行详细分析.

4.1　最优选择准则

对于最优选择准则(11),首先考虑当 m 固定时,分析其安全截断概率,即

$$P_{\text{out},m} \triangleq \Pr\left[\frac{\min(u_m, v) + w_m}{u_m} < \gamma_S\right] \tag{15}$$

根据全概率公式,我们将上式进行概率展开,可得

$$\begin{aligned} P_{\text{out},m} &= \Pr[w_m < \gamma_S u_m - \min(u_m, v)] \\ &= \Pr[w_m < (\gamma_S - 1)u_m, u_m < v] \\ &\quad + \Pr[w_m < \gamma_S u_m - v, u_m \geqslant v] \end{aligned} \tag{16}$$

根据瑞利衰落特性,其信道衰落增益满足指数分布,即

$$\begin{aligned} f_{u_m}(u) &= \frac{1}{\alpha}\mathrm{e}^{-\frac{u}{\alpha}}, u > 0 \\ f_v(v) &= \frac{1}{\beta}\mathrm{e}^{-\frac{v}{\beta}}, v > 0 \\ f_{w_m}(w) &= \frac{1}{\varepsilon}\mathrm{e}^{-\frac{w}{\varepsilon}}, w > 0 \end{aligned} \tag{17}$$

将上式代入到式(16),并进行相关积分运算,可得:

$$\begin{aligned} P_{\text{out},m} &= \Pr[w_m < (\gamma_S - 1)u_m, u_m < v] \\ &\quad + \Pr[w_m < \gamma_S u_m - v, u_m \geqslant v] \\ &= \boldsymbol{E}_v\Big[\int_0^v \frac{1}{\alpha}\mathrm{e}^{-\frac{u}{\alpha}}\left(1 - \mathrm{e}^{-\frac{(\gamma_S - 1)}{\varepsilon}u}\right)\mathrm{d}u \\ &\quad + \int_v^\infty \frac{1}{\alpha}\mathrm{e}^{-\frac{u}{\alpha}}\left(1 - \mathrm{e}^{-\frac{\gamma_S u - v}{\varepsilon}}\right)\mathrm{d}u\Big] \end{aligned} \tag{18}$$

将式(17)代入上式,并经过必要的数学推导,可得 $P_{\text{out},m}$ 的闭式表达式:

$$\begin{aligned} P_{\text{out},m} &= \frac{\dfrac{\alpha(\gamma_S - 1)}{\varepsilon}}{1 + \dfrac{\alpha(\gamma_S - 1)}{\varepsilon}} \\ &\quad + \frac{\dfrac{\alpha}{\varepsilon}}{\left[1 + \dfrac{\alpha(\gamma_S - 1)}{\varepsilon}\right](1 + \dfrac{\alpha\gamma_S}{\varepsilon})\left[\dfrac{\beta}{\alpha} + 1 + \dfrac{\beta(\gamma_S - 1)}{\varepsilon}\right]} \end{aligned} \tag{19}$$

考虑到 u_m 与 w_m 的独立性,则最优选择准则下的安全截断概率可表示为

$$\begin{aligned} P_{\text{out},m_1^*} &= \Pr[z_{m_1^*} < \gamma_S] \\ &= \prod_{m=1}^{M} \Pr[z_m < \gamma_S] = (P_{\text{out},m})^M \end{aligned} \tag{20}$$

根据上式易知:最优选择准则下安全截断概率是 M 的单调减函数,且其分集增益与基站数目 M 相等. 类似地可证明,当窃听信道为莱斯衰落时,上述分集增益结论依然成立.

为更加深入地分析直接链路对系统安全性能的影响,我们还将分析渐近条件下安全截断概率的分集特性. 利用一阶近似,式(19)的渐近表达式可化简为

$$P_{\text{out},m} \simeq \frac{\alpha(\gamma_S - 1)}{\varepsilon} + \frac{\dfrac{\alpha}{\varepsilon}}{(\dfrac{\beta}{\alpha} + 1)} = \frac{\alpha}{\varepsilon}\left[(\gamma_S - 1) + \frac{1}{(\dfrac{\beta}{\alpha} + 1)}\right] \tag{21}$$

相应地,渐近条件下最优选择准则下的安全截断概率可表示为

$$P_{\text{out},m_1^*} \simeq \left(\frac{\alpha}{\varepsilon}\right)^M\left[(\gamma_S - 1) + \frac{1}{(\dfrac{\beta}{\alpha} + 1)}\right]^M \tag{22}$$

由上述渐近分析式易知,最优选择准则下的安全截断概率是关于直接链路平均信道衰落增益的单调减函数,且其分集增益阶数等于基站节点数目 M.

4.2 次优选择准则

考虑到次优选择准则的准确解析式难于推导,我们转而寻求推导安全截断概率紧密的上下界解析式.根据最优选择准则的上下界关系式并结合安全截断概率的表达式易知,安全截断概率的上界与下界可分别表示为:

$$P_{\text{out},m}^{UB} \triangleq \Pr\left[\frac{w_m}{u_m} < \gamma_S\right] \tag{23}$$

$$P_{\text{out},m}^{LB} \triangleq \Pr\left[\frac{w_m}{u_m} + 1 < \gamma_S\right] = \Pr\left[\frac{w_m}{u_m} < \gamma_S - 1\right] \tag{24}$$

由上述两公式易知,当 γ_S 足够大时,其上下界曲线必定非常接近.特别地,当 $R_S = 2\text{bps/Hz}$ 时,次优选择的上下界几乎完全重叠.

首先分析 m 固定条件下的安全截断概率.将式(17)代入上界表达式中,并进行必要的积分推导,可得

$$\begin{aligned} P_{\text{out},m}^{UB} &= \Pr[w_m < \gamma_S u_m] \\ &= \int_0^{\infty} \frac{1}{\alpha} e^{-\frac{u}{\alpha}} (1 - e^{-\frac{\gamma_S u}{\varepsilon}}) du = \frac{\frac{\alpha}{\varepsilon}\gamma_S}{1 + \frac{\alpha}{\varepsilon}\gamma_S} \end{aligned} \tag{25}$$

类似地,考虑到 u_m 与 w_m 的独立性,则次优选择准则下的安全截断概率上界可表示为

$$P_{\text{out},m_2^*}^{UB} = [P_{\text{out},m}^{UB}]^M = \left[\frac{\frac{\alpha}{\varepsilon}\gamma_S}{1 + \frac{\alpha}{\varepsilon}\gamma_S}\right]^M \tag{26}$$

同理易知,次优选择准则下的安全截断概率下界可表示为

$$P_{\text{out},m_2^*}^{LB} = \left[\frac{\frac{\alpha}{\varepsilon}(\gamma_S - 1)}{1 + \frac{\alpha}{\varepsilon}(\gamma_S - 1)}\right]^M \tag{27}$$

由上式易知,次优选择准则下安全截断概率是 M 的单调减函数,且其分集增益与基站数目 M 相等.

渐近条件下,当 $\varepsilon \to \infty$ 时,再次利用公式 $\frac{1}{1+x} \simeq (1 - x)$,$x \to 0$,次优选择准则下的安全截断概率上下界可表示为:

$$P_{\text{out},m_2^*}^{UB} \simeq \left[\frac{\alpha}{\varepsilon}\gamma_S\right]^M, P_{\text{out},m_2^*}^{LB} \simeq \left[\frac{\alpha}{\varepsilon}(\gamma_S - 1)\right]^M \tag{28}$$

根据上述渐近表达式易知,次优选择准则降低了选择算法的实现复杂度,但仍能达到最优选择准则的分集增益阶数,即全分集增益.值得指出的是:当 γ_S 足够大,即 R_S 足够大时,上述上下界性能曲线将趋于吻合.

4.3 部分选择准则

根据部分选择准则(14),我们首先可推导出 $w_{m_3^*}$ 的概率分布函数,根据排序统计理论可知

$$\begin{aligned} F_{w_{m_3^*}}(x) &= \Pr[w_{m_3^*} < x] = [\Pr(w_m < x)]^M \\ &= [1 - e^{-\frac{x}{\varepsilon}}]^M \end{aligned} \tag{29}$$

再由二项式定理[28]对上式展开,可得

$$\begin{aligned} F_{w_{m_3^*}}(x) &= [1 - e^{-\frac{x}{\varepsilon}}]^M \\ &= \left[1 - \sum_{m=1}^{M} \binom{M}{m} (-1)^{m+1} e^{-\frac{mx}{\varepsilon}}\right] \end{aligned} \tag{30}$$

根据公式(16),可得部分选择准则下的安全截断概率为:

$$\begin{aligned} P_{\text{out},m_3^*} &= \Pr[w_{m_3^*} < (\gamma_S - 1)u_{m_3^*}, u_{m_3^*} < v] \\ &\quad + \Pr[w_{m_3^*} < \gamma_S u_{m_3^*} - v, u_{m_3^*} \geqslant v] \end{aligned} \tag{31}$$

由于部分选择准则只对直接链路进行了优选,故 $u_{m_3^*}$ 与 u_m 为同概率分布的随机变量,上式可简化为:

$$\begin{aligned} P_{\text{out},m_3^*} &= \Pr[w_{m_3^*} < (\gamma_S - 1)u_m, u_m < v] \\ &\quad + \Pr[w_{m_3^*} < \gamma_S u_m - v, u_m \geqslant v] \end{aligned} \tag{32}$$

再将式(17)代入上式,并进行必要的积分运算,可得安全截断概率的准确表达式:

$$\begin{aligned} P_{\text{out},m_3^*} &= \Pr[w_{m_3^*} < (\gamma_S - 1)u_m, u_m < v] \\ &\quad + \Pr[w_{m_3^*} < \gamma_S u_m - v, u_m \geqslant v] \\ &= \mathbb{E}_v\left\{\int_0^v \frac{1}{\alpha} e^{-\frac{u}{\alpha}} \left[1 - \sum_{m=1}^{M} \binom{M}{m} (-1)^{m+1} e^{-\frac{m(\gamma_S - 1)u}{\varepsilon}}\right] du \right. \\ &\quad \left. + \int_v^{\infty} \frac{1}{\alpha} e^{-\frac{u}{\alpha}} \left[1 - \sum_{m=1}^{M} \binom{M}{m} (-1)^{m+1} e^{-\frac{m(\gamma_S u - v)}{\varepsilon}}\right] du \right\} \\ &= \mathbb{E}_v\left\{1 - \int_0^v \frac{1}{\alpha} e^{-\frac{u}{\alpha}} \sum_{m=1}^{M} \binom{M}{m} (-1)^{m+1} e^{-\frac{m(\gamma_S - 1)u}{\varepsilon}} du \right. \\ &\quad \left. - \int_v^{\infty} \frac{1}{\alpha} e^{-\frac{u}{\alpha}} \sum_{m=1}^{M} \binom{M}{m} (-1)^{m+1} e^{-\frac{m\gamma_S u}{\varepsilon}} e^{\frac{mv}{\varepsilon}} du \right\} \\ &= 1 + \underbrace{\sum_{m=1}^{M} \binom{M}{m} (-1)^m \frac{1 - \frac{1}{\frac{\beta}{\alpha} + 1 + \frac{\beta m(\gamma_S - 1)}{\varepsilon}}}{[1 + \frac{\alpha m(\gamma_S - 1)}{\varepsilon}]}}_{P_1} \\ &\quad + \underbrace{\sum_{m=1}^{M} \binom{M}{m} (-1)^m \frac{\frac{1}{\frac{\beta}{\alpha} + 1 + \frac{\beta m(\gamma_S - 1)}{\varepsilon}}}{[1 + \frac{\alpha m \gamma_S}{\varepsilon}]}}_{P_2} \end{aligned} \tag{33}$$

根据式(32)易知,当基站数目 M 越大时,安全截断概率必然越小.即部分选择准则下,安全截断概率是 M 的单调减函数.

下面我们将分析当 $\varepsilon \to \infty$ 时,上式的分集增益.

引理 1　定义函数 $G(M,k)=\sum_{m=1}^{M}\binom{M}{m}(-1)^m m^k$，则有以下关系式成立：

$$G(M,k)=0,\forall k=1,2,\cdots,M-1 \tag{34}$$

证明：根据 $G(M,k)$ 的定义式，并利用二项式展开公式，易知 $G(M,0)=-1$. 考察 $G(M,1)$，对其进行变量代换，并再次利用二项式展开公式可得：

$$\begin{aligned}G(M,1)&=\sum_{m=1}^{M}\binom{M}{m}(-1)^m m\\&=\sum_{m=1}^{M}\frac{M!}{(M-m)!m!}(-1)^m m\\&=\sum_{m=1}^{M}\frac{M(M-1)!}{(M-m)!(m-1)!}(-1)^m\\&=-M\sum_{m=1}^{M}\binom{M-1}{m-1}(-1)^{m-1}\\&=-M\sum_{k=0}^{M-1}\binom{M-1}{k}(-1)^k=0\end{aligned} \tag{35}$$

类似地，可证明 $G(M,2)=0$.

一般地，考察 $G(M,k)$，并对其进行二项式展开如下：

$$\begin{aligned}G(M,k)&=\sum_{m=1}^{M}\binom{M}{m}(-1)^m m^k\\&=\sum_{m=1}^{M}\frac{M(M-1)!}{(M-m)!(m-1)!}(-1)^m m^{k-1}\\&=-M\sum_{m=1}^{M}\binom{M-1}{m-1}(-1)^{m-1}[m-1+1]^{k-1}\\&=-M\sum_{m=1}^{M}\binom{M-1}{m-1}\\&\quad(-1)^{m-1}\left[1+\sum_{j=1}^{k-1}\binom{k-1}{j}(m-1)^j\right]\\&=-M\sum_{m=0}^{M-1}\binom{M-1}{m}\\&\quad(-1)^m\left[1+\sum_{j=1}^{k-1}\binom{k-1}{j}(m)^j\right]\end{aligned} \tag{36}$$

利用二项式展开定理，上式可简化为

$$\begin{aligned}G(M,k)&=-M\sum_{m=0}^{M-1}\binom{M-1}{m}\sum_{j=1}^{k-1}\binom{k-1}{j}m^j(-1)^m\\&=-M\sum_{j=1}^{k-1}\binom{k-1}{j}\sum_{m=1}^{M-1}\binom{M-1}{m}m^j(-1)^m\\&=-M\sum_{j=1}^{k-1}\binom{k-1}{j}G(M-1,j)\end{aligned} \tag{37}$$

将 $G(M,1)=G(M,2)=0$ 代入上式，易知 $G(M,3)=0$. 再根据公式的递推关系，易证引理 1 成立.

定理 1　部分选择准则下的安全截断概率函数的分集增益阶数等于基站数目 M.

证明：根据部分选择准则下的安全截断概率的准确表达式，当 $\varepsilon\to\infty$，采用级数展开[28]公式 $\frac{1}{1+x}=\sum_{k=1}^{\infty}(-1)^{k-1}x^{k-1}$，分别对中的 P_1 和 P_2 部分进行近似处理如下：

$$\begin{aligned}P_1&=\sum_{m=1}^{M}\binom{M}{m}(-1)^m\frac{1-\dfrac{1}{\dfrac{\beta}{\alpha}+1+\dfrac{\beta m(\gamma_S-1)}{\varepsilon}}}{\left[1+\dfrac{\alpha m(\gamma_S-1)}{\varepsilon}\right]}\\&=\sum_{m=1}^{M}\binom{M}{m}\\&\quad\cdot(-1)^m\frac{1-\dfrac{1}{\left(\dfrac{\beta}{\alpha}+1\right)}\dfrac{1}{1+\dfrac{1}{\left(\dfrac{1}{\alpha}+\dfrac{1}{\beta}\right)}\dfrac{m(\gamma_S-1)}{\varepsilon}}}{\left[1+\dfrac{\alpha m(\gamma_S-1)}{\varepsilon}\right]}\\&=\sum_{m=1}^{M}\binom{M}{m}(-1)^m\left\{1-\frac{1}{\left(\frac{\beta}{\alpha}+1\right)}\right.\\&\quad\left.\left[1+\sum_{k=1}^{\infty}(-1)^k\left[\frac{1}{\left(\frac{1}{\alpha}+\frac{1}{\beta}\right)}\frac{m(\gamma_S-1)}{\varepsilon}\right]^k\right]\right\}\\&\quad\cdot\left\{1+\sum_{j=1}^{\infty}(-1)^j\left[\frac{\alpha m(\gamma_S-1)}{\varepsilon}\right]^j\right\}\end{aligned} \tag{38}$$

考虑到引理 1 的约束关系，上式中只需要考虑常数部分以及变量 m 阶数大于或等于 M 的部分分量即可. 同时由于 $\varepsilon\to\infty$，阶数大于 M 的部分可视为高阶小量进行删除. 故渐近条件下，上式可简化为

$$\begin{aligned}P_1&\simeq\frac{1}{c_2}-1+\left\{1-\frac{1}{c_2}\left[\frac{1-\dfrac{1}{(c_1)^{M+1}}}{1-\dfrac{1}{c_1}}\right]\right\}\\&\quad\cdot\left[\frac{-\alpha(\gamma_S-1)}{\varepsilon}\right]^M G(M,M)\end{aligned} \tag{39}$$

上式中，

$$c_1\triangleq 1+\frac{\alpha}{\beta},c_2\triangleq 1+\frac{\beta}{\alpha} \tag{40}$$

类似地，对于公式(33)中的 P_2 部分，当 $\varepsilon\to\infty$ 时，

$$\begin{aligned}P_2&\simeq\frac{1}{c_2}\frac{1-\left[\dfrac{(\gamma_S-1)}{\gamma_S c_1}\right]^{M+1}}{1-\dfrac{(\gamma_S-1)}{\gamma_S c_1}}\left(\frac{-\alpha\gamma_S}{\varepsilon}\right)^M\\&\quad\cdot\sum_{m=1}^{M}\binom{M}{m}(-1)^m m^M-\frac{1}{c_2}\end{aligned} \tag{41}$$

将公式(39)和(41)代入式(33)，可得部分选择准则下安全截断概率的渐近表达式：

$$P_{\text{out},m_3^*} \simeq \left(\frac{\alpha}{\varepsilon}\right)^M (-1)^M G(M,M) \cdot \left\{\left\{1-\frac{1}{c_2}\left[\frac{1-\frac{1}{c_1^{M+1}}}{1-\frac{1}{c_1}}\right]\right\}(\gamma_S-1)^M + \frac{1}{c_2}\frac{1-\left[\frac{(\gamma_S-1)}{c_1\gamma_S}\right]^{M+1}}{1-\frac{(\gamma_S-1)}{c_1\gamma_S}}(\gamma_S)^M\right\} \tag{42}$$

由上式易知,部分选择准则下安全截断概率是关于$\frac{\alpha}{\varepsilon}$的 M 阶函数.

定理 1 证毕.

5 数值仿真与分析

数值仿真验证系统采用图 1 中的网络拓扑结构. 我们使用 Criterion I,Criterion II 以及 Criterion III 分别表示最优选择准则,次优选择准则和部分选择准则. 在所有仿真系统中,我们设置发射端信噪比 $\gamma=20$dB,系统安全容量门限为 $R_S=2$bps/Hz. 不失一般性,我们将中继链路的两跳 $h_{S,R}$ 与 h_{RD} 的平均信道增益均设置为 1,即 $\alpha=\beta=1$.

图 2 给出了当基站节点数 $M=2$ 时,三种准则下安全截断概率的理论分析结果的对比,并使用仿真数据进行了验证. 图中横坐标为直接链路的平均信道增益 ε,纵坐标为系统安全截断概率. 最优选择准则(Criterion I)和部分选择准则(Criterion III)分别使用了理论分析的精确表达式和式;次优选择准则(Criterion II)则使用了理论分析的上界式与下界式. 从图中易知,最优选择准则与次优选择准则性能几乎完全接近,而部分选择准则相比于最优选择准则的性能损失约 1.5dB. 这是由于部分选择准则只使用了直接链路的信道状态信息,而没有考虑中继链路的影响,不能有效抑制窃听信道的信息泄露,故其性能略差. 从图中还可知,当 ε 足够大时,三种准则下的安全截断概率的分集增益相同,且等于基站节点数目 M.

此外,对于次优选择准则(Criterion II),我们给出的上下界分析结果也几乎完全接近,即为紧密的上下界分析式. 当安全容量门限足够大时,本文给出的上下界结果也作为准确分析式. 我们注意到次优选择准则的上下界几乎重合,下文中我们只对次优选择准则的上界进行分析. 三种准则下的仿真分析数据与理论分析数据都十分吻合,也进一步验证了理论分析结果.

图 3 给出不同基站节点数目 M 条件下,最优选择准则与次优选择准则的安全截断概率曲线. 其中次优选择准则理论分析使用理论上界进行分析. 图中我们设置基站节点数目由 2 逐步增加到 5. 由图中可以看出,两种选择准则的安全截断概率性能随着 M 的增加

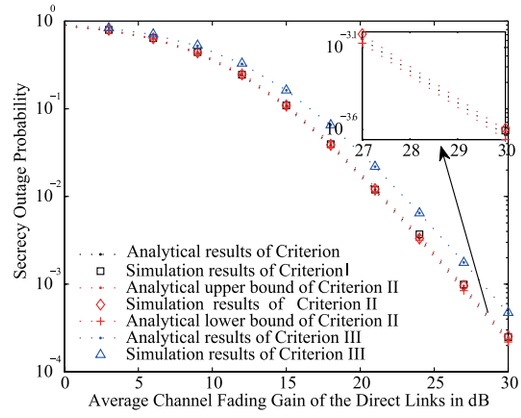

图2 三种准则下安全截断概率性能曲线

而变优;准确地说,安全截断概率的分集增益阶数随着基站节点数目增加而增加. 同时,仿真分析数据也再次验证了理论分析结果的正确性:对不同的 ε 及 M 的设置条件下,理论分析与仿真结果都很好地吻合.

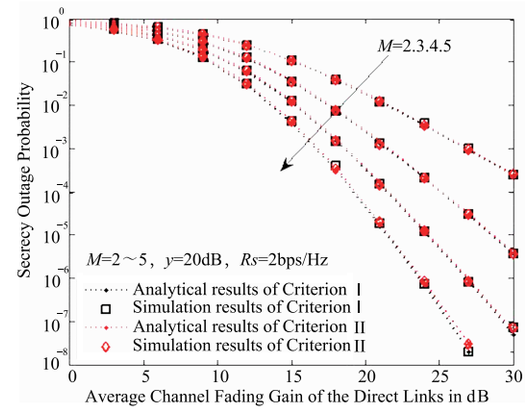

图3 不同基站节点数下安全截断概率性能曲线(Criterion I & II)

图 4 给出了不同基站节点数下,最优选择准则与次优选择准则的安全截断概率性能的渐近曲线. 基站节点的数目设置为 2 到 5. 由图中易知,对于最优选择准则与次优选择准则,当基站节点数目 M 变化时,其性能仍然几乎完全相同. 进一步地,由渐近分析可知,两种准则下的安全截断概率性能均能达到全分集增益. 仿真结果验证了渐近分析式的正确性.

类似地,我们对部分选择准则(Criterion III)也进行了渐近分析对比. 图 5 给出了在不同基站节点数目下部分选择准则的安全截断概率性能曲线. 我们分别使用理论分析的准确表达式、仿真分析数据以及理论分析渐近表达式进行对比. 由图中可以看出,当 M 的取值越大时,部分选择准则的性能越好. 准确地说,部分选择准则的安全截断概率性能曲线也可以达到全分集增益,即其分集增益阶数与基站节点数目相等. 从图中也可以发现,当 M 取值不同时,理论分析的准确表达式与仿

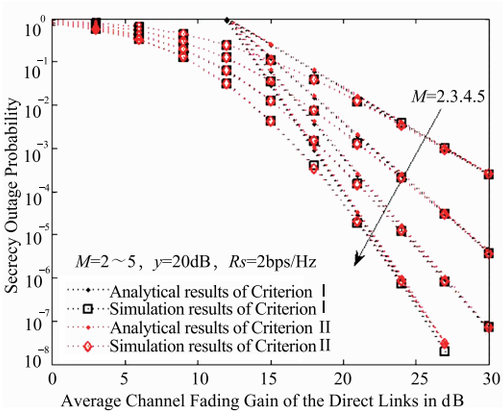

图4　不同基站节点数下安全截断概率的渐近性能曲线（Criterion I & II）

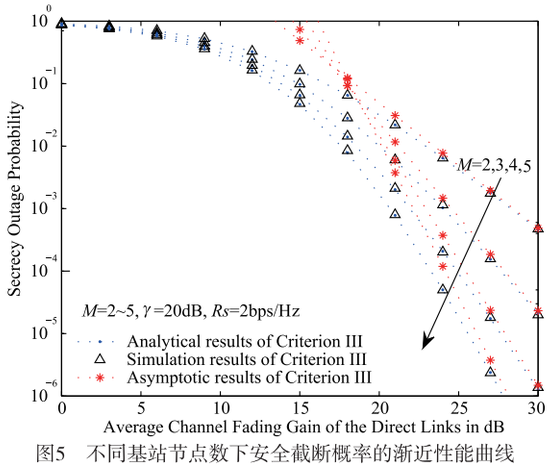

图5　不同基站节点数下安全截断概率的渐近性能曲线

真分析数据十分吻合;当 ε 足够大,仿真数据与渐近分析式的性能曲线也非常吻合. 从而,仿真数据验证了部分选择准则理论分析结果的正确性.

更进一步地,当窃听信道为莱斯衰落模型时,我们通过数值仿真深入分析了莱斯因子 K[9] 对系统安全容量的影响. 针对最优选择准则,图 6 给出了不同莱斯因子条件下系统安全容量 C_s 的性能曲线. 系统参数中基站节点数 $M=4$. 特别地,当莱斯因子 $K=0$ 时,信道模型退化为瑞利衰落. 由图中易知,系统安全容量随着莱斯因子的增加而恶化. 其原因是当莱斯因子增加时,窃听信道中主径能量变强,窃听信道对应的信道容量增加,故而导致系统的安全容量相对降低.

6　结束语

本文研究在不可信解码转发无线中继网络中,直接链路及基站节点数目对系统安全性能的影响. 针对不同的信道状态信息条件,本文提出三种不同的选择准则,即最优选择准则、次优选择准则和部分选择准则. 针对复杂度最高的最优选择准则,我们推导了安全截断概率的准

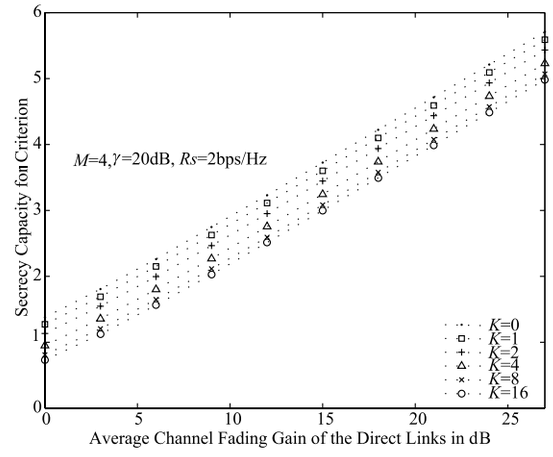

图6　不同莱斯因子下系统安全容量曲线

确闭式表达式及渐近分析式;针对次优选择准则,推导了紧密的上下界分析式,并通过上下界间接分析了其分集增益;针对复杂度最低的部分选择准则,同样给出了准确闭式表达式及渐近分析式,并证明了其全分集增益特性.

参考文献

[1] Fan Lisheng, Lei Xianfu, Duong T Q, Elkashlan M. Secure multiuser communications in multiple amplify-and-forward relay networks[J]. IEEE Transactions on Communications, 2014, 62(9): 3299 – 3310.

[2] Huang Xiaobin, He Jing, et al. Optimal power allocation for multicarrier secure communications in full-duplex decode-and-forward relay networks[J]. IEEE Communications Letters, 2014, 18(12): 2169 – 2172.

[3] Fan L, Zhang S, et al. Secure switch-and-stay combining (SSSC) for cognitive relay networks[J]. IEEE Transactions on Communications, 2016, 64(1): 70 – 82.

[4] Krikidis I, Thompson J, Mclaughlin S, Goertz N. Amplify-and-forward with partial relay selection[J]. IEEE Communications Letters, 2008, 12(4): 235 – 237.

[5] Lee Jong Ho. Full-duplex relay for enhancing physical layer security in multi-hop relaying systems[J]. IEEE Communications Letters, 2015, 19(4): 525 – 528.

[6] Maletic N, Cabarkapa M, Neskovic N, Budimir D. Hardware impairments impact on fixed-gain AF relaying performance in Nakagami-m fading[J]. Electronics Letters, 2015, 52(2): 121 – 122.

[7] Wang Dong, Bai Bo, et al. Energy efficient secure communication over decode-and-forward relay channels[J]. IEEE Transactions on Communications, 2015, 63(3): 892 – 905.

[8] Zhao Mingxiong, Wang Xiangfeng, Feng Suili. Joint power splitting and secure beamforming design in the multiple non-regenerative wireless-powered relay networks [J]. IEEE Communications Letters, 2015, 19(9): 1540 – 1543.

[9] Zhou Siyuan, Alfano Giuseppa, Nordio Alessandro, Chiasserini Carla Fabiana. Ergodic capacity analysis of mimo relay network over rayleigh-rician channels[J]. Communications Letters IEEE, 2015, 19(4): 601 – 604.
[10] Maleki Sadr M, Mahboobi B, Mehrizi S, Ahmadian-Attari M. Stochastic robust collaborative beamforming: non-regenerative relay[J]. IEEE Transactions on Communications, 2016, 64(3): 947 – 958.
[11] Wu Nien En, Li Hsueh Jyh. Effect of feedback delay on secure cooperative networks with joint relay and jammer selection[J]. IEEE Wireless Communication Letters, 2013, 2(4): 415 – 418.
[12] Suraweera, H A, Michalopoulos, D S, Karagiannidis, G K Semi-blind amplify-and-forward with partial relay selection[J]. Electronics Letters, 2009, 45(6): 317 – 319.
[13] Zhou Yameng, Pan Gaofeng, Li Tingting, Liu Hequn. Secrecy outage performance for partial relay selection schemes in cooperative systems[J]. IET Communications, 2015, 9(16): 1980 – 1987.
[14] He Biao, et al. Secure on-off transmission design with channel estimation errors[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(12): 1923 – 1936.
[15] Dai Mingjun, Chi Sung. A distributed on-off amplify-and-forward protocol for the fading parallel relay channel[J]. Communications Letters IEEE, 2009, 13(9): 643 – 645.
[16] Long Min, Chen Yunfei, Renzo M Di. Performance analysis of relay selection in the presence of on-off relay traffic[J]. IEEE Transactions on Vehicular Technology, 2014, 63(6): 2959 – 2964.
[17] Cui Hongyu, Song Lingyang, Jiao Bingli. Weighted bidirectional relay selection for outdated channel state information[J]. IEEE Transactions on Communications, 2014, 62(62): 500 – 509.
[18] Deng Dan, Fan Lisheng, Zhao Rui, Hu Rose Qingyang. Secure communications in multiple amplify-and-forward relay networks with outdated channel state information[J]. Transactions on Emerging Telecommunications Technologies, 2016, 33(4): 457 – 464.
[19] Khan F A, Tourki K, Alouini M S, Qaraqe K A. Opportunistic fixed gain bidirectional relaying with outdated CSI[A]. IEEE Vehicular Technology Conference[C]. Boston, USA: IEEE Press, 2015. 1 – 5.
[20] Lei Xianfu, Fan Lisheng, Hu Rose Qingyang, Michalopoulos Diomidis S, Fan Pingzhi. Secure multiuser communications in multiple decode-and-forward relay networks with direct links[A]. Global Communications Conference[C]. Austin, USA: IEEE, 2014. 3180 – 3185.
[21] Fan Lisheng, Yang Nan, Duong Trung, Elkashlan Maged. Exploiting direct links for physical layer security in multi-user multi-relay networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(6): 3856 – 3867.
[22] 杨斌, 王文杰, 等. 基于混合信号的放大转发中继系统的物理层安全传输[J]. 电子学报, 2016, 44(2): 268 – 274.
YANG Bin, WANG Wen-jie, et al. Secure wireless communication for af relay system with hybrid signals[J]. Acta Electrica Sinica, 2016, 44(2): 268 – 274. (in Chinese)
[23] Ferdinand Nuwan S, Costa Daniel Benevides da, Latva-aho Matti. Physical layer security in mimo ostbc line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation[J]. IEEE Wireless Communications Letters, 2013, 2(5): 467 – 470.
[24] Sun L, Ren P, et al. Security-aware relaying scheme for cooperative networks with untrusted relay nodes[J]. IEEE Communications Letters, 2015, 19(3): 463 – 466.
[25] Zhang S, Fan L, et al. Near-optimal modulo-and-forward scheme for the untrusted relay channel[J]. IEEE Transactions on Information Theory, 2016, 62(5): 2545 – 2556.
[26] Ju Min Chu, Kim Do Hoon, Hwang Kyu Sung. Opportunistic transmission of nonregenerative network with untrusted relay[J]. IEEE Transactions on Vehicular Technology, 2015, 64(6): 2703 – 2709.
[27] 吴亚峰, 赵睿, 贺玉成, 谢维波. 基于有限反馈的非可信中继系统的物理层安全性能分析[J]. 电子学报, 2015, 43(11): 2247 – 2254.
WU Ya-feng, ZHAO Rui, HE Yu-cheng, XIE Wei-bo. Performance analysis of physical layer security of untrusted relay system based on limited feedback[J]. Acta Electrica Sinica, 2015, 43(11): 2247 – 2254. (in Chinese)
[28] Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, and Products[M]. San Diego, USA: Academic Press, Elsevier Inc, 2007. 372 – 374.

作者简介

邓 单 男, 1981 年生于湖北京山. 工学博士, 广州番禺职业技术学院副教授. 研究方向为无线通信、物理层安全.
E-mail: dengdan@ustc.edu

周 雯 男, 1981 年生于安徽宿州. 工学博士, 南京林业大学副教授. 研究方向为移动通信的信号处理等.
E-mail: wenzhou@ustc.edu