



研究与开发

Nakagami- m 衰落信道下存在窃听攻击的 认知中继网络安全性与可靠性折中方案

王兴鹏, 许晓荣, 胡安迪, 冯维

(杭州电子科技大学通信工程学院, 浙江 杭州 310018)

摘要: 研究了由源节点、目的节点和多个中继节点组成的认知解码转发 (DF) 中继网络中物理层安全与可靠性折中方案。该方案以保障最大安全主链路信道容量为目标, 提出了存在窃听攻击情况下的最佳中继选择方案。以传统直接传输方案作为基准, 给出了安全性与可靠性折中性能 (SRT)。数值仿真结果表明, 所提方案的 SRT 性能优于传统直接传输方案的 SRT, 并且其性能随着中继数量和在一定中继数下 Nakagami 信道衰落因子 m 的增加而显著改善。

关键词: 认知中继网络; Nakagami- m 衰落信道; 窃听攻击; 安全性与可靠性折中; 最佳中继选择

中图分类号: TP393

文献标识码: A

doi:10.11959/j.issn.1000-0801.2018247

Security-reliability tradeoff scheme for cognitive relay networks with eavesdropping attack over Nakagami- m fading channels

WANG Xingpeng, XU Xiaorong, HU Andi, FENG Wei

School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: Physical layer security (PLS) and reliability tradeoff scheme in a cognitive decode-and-forward (DF) relay network consisting of one source, one destination and multiple relays was investigated. A best relay selection scheme (BRS) against eavesdropping attack was proposed, in order to guarantee the maximum secure main link channel capacity. Traditional direct transmission scheme was taken into consideration as a benchmark. In addition, security-reliability tradeoff (SRT) performance was presented. Numerical results show that the proposed SRT scheme strictly outperforms traditional direct transmissions in terms of SRT performance. SRT performance can be enhanced obviously with the increasing of relays and Nakagami channel fading factor m for a given numbers of relays.

Key words: cognitive relay network, Nakagami- m fading channel, eavesdropping attack, security-reliability tradeoff, best relay selection

收稿日期: 2018-04-25; 修回日期: 2018-09-07

通信作者: 许晓荣, xuxr@hdu.edu.cn

基金项目: 浙江省自然科学基金一般项目“绿色无线携能网络中继选择与资源调度策略研究”; 2017 年度杭州电子科技大学“优秀骨干教师支持计划”人才项目; 杭州电子科技大学“电子科学与技术”浙江省一流学科 A 类开放基金项目 (No.GK178800207001/024); 浙江省科协青年科技人才培育工程资助项目 (No.2016YCGC009)

Foundation Items: Zhejiang Provincial Natural Science Foundation of China “Research on Relay Selection and Resource Scheduling Strategies in Green Wireless SWIPT Networks”, Excellent Backbone Teacher Support Program in Hangzhou Dianzi University in 2017, The Open Project of “Electronic Science and Technology” Zhejiang First Class Discipline(Class A) (No.GK178800207001/024), Young Talent Cultivation Project of Zhejiang Association for Science and Technology (No.2016YCGC009)

1 引言

在无线通信中,由于无线介质的广播性质,信号很容易被窃听者窃听,为了实现安全传输,已经研究了许多技术。传统的保密通信主要基于密码相关的加密技术^[1],即便窃听者和合法用户获得相同的信息,窃听者也不能解密原始信息,因为他们不知道密钥。但是,由于密钥有限,这种加密技术实际上可以进行破解。因此,传统的安全传输主要是基于加密和解密的。随着计算机技术的发展,这种加密技术变得不太安全。

近年来,物理层安全(PLS)技术引起了很多关注^[2-3],它利用无线信道的物理特性而不是复杂的加密算法^[4]。参考文献[5]中,香农最早证明了存在一个最佳的安全通信系统。随后,参考文献[6]指出如果窃听信道的质量比合法接收者差,那么总是可以找到一种信道编码,如果合法用户能够正确解调信号,窃听者就不能从接收信号中获得任何信息。该文献还提出了保密(安全)容量的概念,它表示主链路(从源节点(S)到目的节点(D))的容量与窃听链路(从源节点(S)到窃听者(E))之间的容量差异。参考文献[7]证明了如果主链路容量小于窃听链路的容量,那么窃听者可以成功截获信号的传输。为了提高传输的安全性以防止窃听攻击,通过提高安全容量来减少截获事件非常重要。然而,在多径衰落信道中,无线安全容量下降。

为了克服信道衰落特性,人们提出了一些安全传输技术,如多输入多输出(MIMO)电力通信^[8]技术、波束成形技术^[9]以及协作无线网络中的最优中继选择技术^[10]。参考文献[8]主要集中于MIMO电力线通信(PLC)的安全容量研究。参考文献[9]给出了面向安全的波束成形技术。该技术允许信源在特定的方向上将其信息发送给合法接收机,而窃听者接收具有破坏性干扰的信号。因此,合法接收机的信号强度远高于窃听接收机

的信号强度。在波束成形技术的帮助下,也可以在保密性方面得到加强。另外,中继可以用来抵御窃听攻击。参考文献[10]提出了在放大转发(AF)和解码转发(DF)中继协议下的一些中继选择方案,用于增强无线安全容量。

上述参考文献主要集中于系统安全性能的提高,但未考虑通信可靠性。因此,邹教授等学者^[11-13]研究了无线通信中的安全性与可靠性折中(SRT)策略。根据窃听者是否成功截获原信号对安全性进行量化,而可靠性表示在目的地是否发生通信中断事件及其中断概率。它们分别由截获概率(IP)和中断概率(OP)来表示。通过增加S的发射功率降低OP,但是,增加的功率也提高了S-E窃听信道容量并且提高了IP。根据参考文献[11-12],IP的增加将导致OP的减少,反之亦然,即安全性和可靠性之间存在折中关系。此外,提出了一种单个最佳中继选择方案来实现增强SRT。结果表明,中继协作传输优于直接传输。在参考文献[13]中,随着中继数量的提高,SRT性能显著提高。此外,在参考文献[14]中,分别研究了Nakagami-*m*衰落信道上,移动通信网络中的单中继选择和多中继选择的SRT方案。

在参考文献[11-13]中,研究了在瑞利信道下存在一个窃听者的DF无线网络最佳中继选择方案。本文将瑞利信道模型扩展到Nakagami-*m*衰落信道模型^[15]。首先对存在窃听干扰的多中继认知DF中继网络最佳中继选择方案(BRS)进行了研究,并以直接传输作为对比方案,推导了Nakagami-*m*衰落信道下采用直接传输与BRS方案的OP和IP闭合解析表达式,并给出了所提方案的仿真与性能分析。

2 系统模型

2.1 直接传输

首先研究信源S和目的节点D之间存在窃听者E情况下的直接传输模型。假设直接传输模型



中的各个节点服从均匀分布, 该模型如图 1 所示。 h_{sd} 和 h_{se} 分别表示 S-D 和 S-E 信道衰落系数。这两个信道参数分别服从信道衰落因子为 m_{sd} 和 m_{se} 的独立同分布 Nakagami- m 衰落。首先, S 向 D 发送信号, 同时窃听者 E 窃听该信号。根据参考文献[11-13], 假设 E 已知 S-D 直接传输的密钥并尝试解密 S 信号。S 以功率 P 和传输速率 R_s 传输信号 x , 那么在 D 处接收到的信号可以表示为:

$$y_d = h_{sd}\sqrt{P}x + n_d \quad (1)$$

其中, n_d 表示方差为 N_0 的零均值加性高斯噪声。根据以上假设, E 接收到的信号可写成:

$$y_e = h_{se}\sqrt{P}x + n_e \quad (2)$$

其中, n_e 同样表示方差为 N_0 的零均值加性高斯噪声。由式 (1) 可以得到 S-D 的主信道容量为:

$$C_{sd} = \text{lb}\left(1 + |h_{sd}|^2 \frac{P}{N_0}\right) \quad (3)$$

S-E 的窃听信道容量表示为:

$$C_{se} = \text{lb}\left(1 + |h_{se}|^2 \frac{P}{N_0}\right) \quad (4)$$

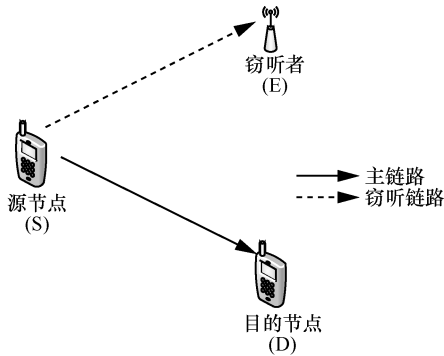


图 1 信源 S 和目的节点 D 之间存在窃听者 E 情况下的直接传输模型

2.2 最佳中继选择传输

在如图 2 所示的协作无线网络中, 假设选择 N 个中继中的最佳中继进行辅助传输, 单窃听者随机位于 S 和中继节点周围。同样, 假设该网络中的各节点服从均匀分布。假设 E 不仅窃听 S 传

输, 还窃听中继转发信号。 h_{si} 、 h_{id} 、 h_{se} 和 h_{ie} 分别表示 S- R_i 、 R_i -D、S-E、 R_i -E 的信道衰落系数。同样, 这些信道参数分别服从信道衰落因子为 m_{si} 、 m_{id} 、 m_{se} 和 m_{ie} 的独立同分布的 Nakagami- m 衰落。采用 $\mathbf{R} = \{R_i | i=1,2,\dots,N\}$ 表示 N 个中继, 这些中继采用解码转发 (DF) 协议转发信号。

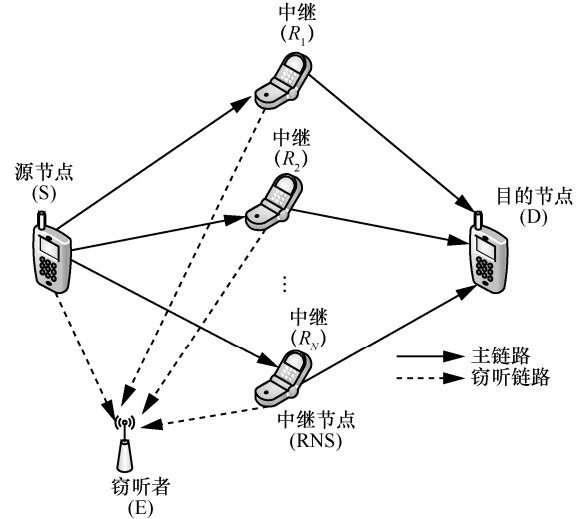


图 2 存在窃听攻击的协作中继网络模型

S 首先将信号广播给中继, 这些中继会解码原始信号。采用集合 Φ 表示成功解码信号的中继, N 个中继就有 2^N 种可能的子集。因此, 解码样本集可以表示为:

$$\Phi = \{\phi, D_1, D_2, \dots, D_{2^N-1}\} \quad (5)$$

其中, ϕ 表示空集, D_n 代表第 n 个非空子集。如果 Φ 为空, 表示所有的中继都无法解码原始信号; 如果 Φ 不为空, 选择一个最佳中继来解码原信号并转发给 D。同样, 假设 S 以功率 P 、传输速率 R_s 向中继传输信号 x , 中继 R_i 处收到的信号可以表示为:

$$y_i = h_{si}\sqrt{P}x + n_i \quad (6)$$

其中, n_i 表示方差为 N_0 的零均值加性高斯噪声。根据式 (6) 可以得到 S- R_i 的信道容量为:

$$C_{si}^{\text{BRS}} = \frac{1}{2} \text{lb}\left(1 + |h_{si}|^2 \frac{P}{N_0}\right) \quad (7)$$

其中, 系数 1/2 表示需要两个时隙完成从 S 到 D

的传输。与此同时, E 可以窃听 S 的传输信号, E 接收信号表示为:

$$y_{se} = h_{se}\sqrt{P}x + n_e \quad (8)$$

S-E 信道容量表示为:

$$C_{se}^{BRS} = \frac{1}{2} \text{lb} \left(1 + |h_{se}|^2 \frac{P}{N_0} \right) \quad (9)$$

根据香农定理, 当信道容量低于数据速率时, 即 $C_{si}^{BRS} < R_s$, 则中继无法解码原始信号。因此, $\Phi = \emptyset$ 的情况可以表示为:

$$\frac{1}{2} \text{lb} \left(1 + |h_{si}|^2 \frac{P}{N_0} \right) < R_s, R_i \in R \quad (10)$$

同理, $\Phi = D_n$ 的情况可以由式 (11) 给出:

$$\begin{aligned} \frac{1}{2} \text{lb} \left(1 + |h_{si}|^2 \frac{P}{N_0} \right) &> R_s, R_i \in D_n \\ \frac{1}{2} \text{lb} \left(1 + |h_{sr}|^2 \frac{P}{N_0} \right) &< R_s, R_r \in \overline{D_n} \end{aligned} \quad (11)$$

其中, $\overline{D_n}$ 是 D_n 的补集, $\overline{D_n} = R - D_n$ 。当 $\Phi = D_n$ 时, 从 D_n 中选择一个最佳中继以功率 P 、传输速率 R_s 来转发它解码的原始信号, 目的节点 D 处接收到的信号为:

$$y_d = h_{id}\sqrt{P}x + n_d \quad (12)$$

由式 (12) 可以得到 R_i -D 的信道容量为:

$$C_{id}^{BRS} = \frac{1}{2} \text{lb} \left(1 + |h_{id}|^2 \frac{P}{N_0} \right) \quad (13)$$

选择具有最高信道容量 C_{id}^{BRS} 的中继为最佳中继。根据式 (13), 最佳中继选择 (BRS) 准则为:

$$\text{Best relay} = \arg \max_{R_i \in D_n} C_{id}^{BRS} = \arg \max_{R_i \in D_n} |h_{id}|^2 \quad (14)$$

即最佳中继选择准则只需知道信道信息 $|h_{id}|^2$, 而无需知道窃听者信息。结合式 (13) 和式 (14), 最佳中继到 D 的信道容量为:

$$C_{bd}^{BRS} = \frac{1}{2} \max_{R_i \in D_n} \text{lb} \left(1 + |h_{id}|^2 \frac{P}{N_0} \right) \quad (15)$$

其中, b 表示最佳中继。然而, 窃听者同样可以窃

听最佳中继转发信号。将 E 窃听到的信号表示为:

$$y_{be} = h_{be}\sqrt{P}x + n_e \quad (16)$$

则最佳中继到 E 的窃听信道容量为:

$$C_{be}^{BRS} = \frac{1}{2} \text{lb} \left(1 + |h_{be}|^2 \frac{P}{N_0} \right) \quad (17)$$

3 Nakagami- m 衰落信道下的认知中继网络安全性与可靠性

本节对 Nakagami- m 衰落信道下直接传输和 BRS 策略的安全性 with 可靠性进行分析。信道衰落系数 $|h_{sd}|^2$ 、 $|h_{se}|^2$ 、 $|h_{si}|^2$ 、 $|h_{ie}|^2$ 、 $|h_{id}|^2$ 、 $|h_{be}|^2$ 、 $|h_{bd}|^2$ 分别服从平均功率为 Ω_{sd} 、 Ω_{se} 、 Ω_{si} 、 Ω_{ie} 、 Ω_{id} 、 Ω_{be} 、 Ω_{bd} 的伽马分布。根据参考文献[15], 信道衰落系数的概率密度函数为 Nakagami- m 分布, 即:

$$f_z(z) = \frac{z^{m_z-1}}{\Gamma(m_z)} \left(\frac{m_z}{\Omega_z} \right)^{m_z} e^{-\frac{z m_z}{\Omega_z}} \quad (18)$$

其中, 当 $m=1$ 时为瑞利分布。采用中断概率 (OP) 和截获概率 (IP) 分别表征系统可靠性和安全性。如果主链路的信道容量低于信号传输速率, 则发生中断事件; 当窃听链路的信道容量高于信号传输速率, 则发生截获事件。分别研究在直接传输和 BRS 策略下的 OP、IP 及安全性—可靠性折中性能 (SRT)。

3.1 直接传输

由式 (3) 中所示的直接传输信道容量, 直接传输的 OP 可写为:

$$\text{Pr}_{\text{out}}^{\text{direct}} = \Pr(C_{sd} < R_s) = \Pr(|h_{sd}|^2 < \alpha) \quad (19)$$

其中, $\alpha = (2^{R_s} - 1)/\gamma$, $\gamma = \frac{P}{N_0}$ 。因为 $|h_{sd}|^2$ 遵循概率密度函数为式 (18) 的伽马分布, 则式 (19) 可表示为:

$$\text{Pr}_{\text{out}}^{\text{direct}} = 1 - \frac{\Gamma\left(m_{sd}, \frac{m_{sd}}{\Omega_{sd}} \alpha\right)}{\Gamma(m_{sd})} \quad (20)$$



其中, $\Gamma(a, b)$ 是不完全伽马函数, $\Gamma(a)$ 是伽马函数。另外, 由式 (4) 的窃听信道容量, 可以得到直接传输时的 IP 为:

$$\begin{aligned} \Pr_{\text{int}}^{\text{direct}} &= \Pr(C_{\text{se}} > R_s) \\ &= \Pr(|h_{\text{se}}|^2 > \alpha) \\ &= \frac{\Gamma\left(m_{\text{se}}, \frac{m_{\text{se}}}{\Omega_{\text{se}}} \alpha\right)}{\Gamma(m_{\text{se}})} \end{aligned} \quad (21)$$

在不失一般性的前提下, 假设 $m_{\text{sd}} = m_m$, $m_{\text{se}} = m_e$, $\Omega_{\text{sd}} = \Omega_m$, $\Omega_{\text{se}} = \Omega_e$ 。式 (20) 和式 (21) 可以简化为:

$$\Pr_{\text{out}}^{\text{direct}} = 1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \alpha\right)}{\Gamma(m_m)} \quad (22)$$

$$\Pr_{\text{int}}^{\text{direct}} = \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e} \alpha\right)}{\Gamma(m_e)} \quad (23)$$

3.2 最佳中继选择传输

当 $\Phi = \phi$ 时, 没有中继可以解码原信号, 那么 D 就无法接收信号, 因此中断事件发生; 当 $\Phi = D_n$ 时, 一些中继可以成功解码原信号, 选择最佳的中继向 D 传输信号, 但如果 $C_{\text{bd}}^{\text{BRS}}$ 低于信号传输速率, 中断事件同样发生。因此, 根据全概率公式, 得到最佳中继选择方案下的 OP 为:

$$\Pr_{\text{out}}^{\text{BRS}} = \Pr(\Phi = \phi) + \sum_{n=1}^{2^N-1} \Pr(\Phi = D_n) \Pr(C_{\text{bd}}^{\text{BRS}} < R_s) \quad (24)$$

由式 (10) 可以得到 $\Phi = \phi$ 的概率为:

$$\begin{aligned} \Pr(\Phi = \phi) &= \prod_{i=1}^N \Pr\left(\frac{1}{2} \text{lb}\left(1 + |h_{\text{si}}|^2 \frac{P}{N_0}\right) < R_s\right) \\ &= \prod_{i=1}^N \left[1 - \frac{\Gamma\left(m_{\text{si}}, \frac{m_{\text{si}}}{\Omega_{\text{si}}} \beta\right)}{\Gamma(m_{\text{si}})}\right] \end{aligned} \quad (25)$$

其中, $\beta = (2^{2R_s} - 1)/\gamma$ 。同样, 由式 (11) 可以得到 $\Phi = D_n$ 的概率为:

$$\begin{aligned} \Pr(\Phi = D_n) &= \prod_{R_i \in D_n} \Pr\left(\frac{1}{2} \text{lb}\left(1 + |h_{\text{si}}|^2 \frac{P}{N_0}\right) > R_s\right) \times \\ &\quad \prod_{R_r \in \bar{D}_n} \Pr\left(\frac{1}{2} \text{lb}\left(1 + |h_{\text{sr}}|^2 \frac{P}{N_0}\right) < R_s\right) \\ &= \prod_{R_i \in D_n} \frac{\Gamma\left(m_{\text{si}}, \frac{m_{\text{si}}}{\Omega_{\text{si}}} \beta\right)}{\Gamma(m_{\text{si}})} \times \prod_{R_r \in \bar{D}_n} \left[1 - \frac{\Gamma\left(m_{\text{sr}}, \frac{m_{\text{sr}}}{\Omega_{\text{sr}}} \beta\right)}{\Gamma(m_{\text{sr}})}\right] \end{aligned} \quad (26)$$

在式 (24) 中, $\Pr(C_{\text{bd}}^{\text{BRS}} < R_s)$ 可以由式 (15) 得到:

$$\begin{aligned} \Pr(C_{\text{bd}}^{\text{BRS}} < R_s) &= \Pr\left(\frac{1}{2} \max_{R_i \in D_n} \text{lb}\left(1 + |h_{\text{id}}|^2 \frac{P}{N_0}\right) < R_s\right) \\ &= \prod_{R_i \in D_n} \left[1 - \frac{\Gamma\left(m_{\text{id}}, \frac{m_{\text{id}}}{\Omega_{\text{id}}} \beta\right)}{\Gamma(m_{\text{id}})}\right] \end{aligned} \quad (27)$$

假设 $m_{\text{si}} = m_{\text{id}} = m_{\text{rd}} = m_m$, $\Omega_{\text{si}} = \Omega_{\text{id}} = \Omega_{\text{rd}} = \Omega_m$, 简化式 (25) ~ 式 (27) 为:

$$\Pr(\Phi = \phi) = \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)}\right]^N \quad (28)$$

$$\Pr(\Phi = D_n) = \left[\frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)}\right]^{|D_n|} \times \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)}\right]^{\overline{|D_n|}} \quad (29)$$

$$\Pr(C_{\text{bd}}^{\text{BRS}} < R_s) = \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)}\right]^{|D_n|} \quad (30)$$

其中, $|D_n|$ 和 $|\overline{D_n}|$ 分别为集合 $|D_n|$ 和 $|\overline{D_n}|$ 的基数。

将式 (28) ~ 式 (30) 代入式 (24), 可以得到最佳中继选择方案下的中断概率闭式表达式为:

$$\begin{aligned} \Pr_{\text{out}}^{\text{BRS}} &= \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)} \right]^N \times \left[1 + \sum_{n=1}^{2^N-1} \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)} \right]^{|D_n|} \\ &= \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)} \right]^N \times \left[1 + \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)} \right]^N \\ &= \left[1 - \frac{\Gamma\left(m_m, \frac{m_m}{\Omega_m} \beta\right)}{\Gamma(m_m)} \right]^{2^N} \end{aligned} \quad (31)$$

对于截获概率, 当 $\Phi=\phi$ 时, 没有中继能够解码原信号, 也就没有中继进行协作信号转发, 则 $C_{\text{be}}^{\text{BRS}}=0$ 。这时, 窃听者只能窃听 S 处的信号传输。当 $\Phi=D_n$ 时, 最佳中继转发信号, 窃听者不仅能够窃听 S 到最佳中继之间的信号传输, 而且可以窃听最佳中继到 D 之间的信号传输。此时引入 $C_e = \max(C_{\text{se}}^{\text{BRS}}, C_{\text{be}}^{\text{BRS}})$ 。如果 $C_{\text{se}}^{\text{BRS}} > R_s$ 或者 $C_e > R_s$, 那么截获事件发生。BRS 策略下的 IP 可以表示为:

$$\Pr_{\text{int}}^{\text{BRS}} = \Pr(\Phi=\phi) \Pr(C_{\text{se}}^{\text{BRS}} > R_s) + \sum_{n=1}^{2^N-1} \Pr(\Phi=D_n) \Pr(C_e > R_s) \quad (32)$$

根据式 (9), 得到 $\Pr(C_{\text{se}}^{\text{BRS}} > R_s)$ 的表达式为:

$$\begin{aligned} \Pr(C_{\text{se}}^{\text{BRS}} > R_s) &= \Pr(|h_{\text{se}}|^2 > \beta) \\ &= \frac{\Gamma\left(m_{\text{se}}, \frac{m_{\text{se}}}{\Omega_{\text{se}}} \beta\right)}{\Gamma(m_{\text{se}})} \end{aligned} \quad (33)$$

根据一系列推导, 得到 $\Pr(C_e > R_s)$ 为:

$$\begin{aligned} \Pr(C_e > R_s) &= \sum_{R_i \in D_n} \left[1 + \sum_{q=1}^{2^{|D_n|-1}} \sum_{p=0}^{(m_m-1)|A_q|} (-1)^{|A_q|} \frac{\Gamma(p+m_m)}{\Gamma(m_m)} \frac{a_p^{|A_q|, m_m}}{(|A_q|+1)^{p+m_m}} \right] \times \\ &\quad \left[\frac{\Gamma\left(m_{\text{ie}}, \frac{m_{\text{ie}}}{\Omega_{\text{ie}}} \beta\right)}{\Gamma(m_{\text{ie}})} + \frac{\Gamma\left(m_{\text{se}}, \frac{m_{\text{se}}}{\Omega_{\text{e}}} \beta\right)}{\Gamma(m_{\text{se}})} - \frac{\Gamma\left(m_{\text{ie}}, \frac{m_{\text{ie}}}{\Omega_{\text{e}}} \beta\right) \Gamma\left(m_{\text{se}}, \frac{m_{\text{se}}}{\Omega_{\text{e}}} \beta\right)}{\Gamma(m_{\text{ie}}) \Gamma(m_{\text{se}})} \right] \end{aligned} \quad (34)$$

其中, A_q 是集合 $\{D_n - i\}$ 的第 q 个非空子集, $|A_q|$ 是集合 A_q 的基数。根据参考文献 [15],

$a_w^{c,d}$ ($0 \leq w \leq c(d-1)$) 可以通过计算得到, 即:

$$\begin{aligned} a_0^{c,d} &= 1, a_1^{c,d} = c \\ a_w^{c,d} &= \frac{1}{w} \sum_{i=1}^{\min(w, d-1)} \frac{i(c+1)-w}{i!} a_{w-i}^{c,d}, 2 \leq w < c(d-1) \\ a_w^{c,d} &= \frac{1}{[(d-1)!]^c}, w = c(d-1) \end{aligned} \quad (35)$$

将式 (28)、式 (29)、式 (33)、式 (34) 分别代入式 (32), 可以得到 IP 的闭合表达式。假设 $m_{\text{se}} = m_{\text{ie}} = m_e, \Omega_{\text{se}} = \Omega_{\text{ie}} = \Omega_e$ 。当 $N \rightarrow \infty$ 时, $\Phi=\phi$ 的情况发生的概率趋向于 0, 因此, IP 的闭式表达式为:

$$\Pr_{\text{int}}^{\text{BRS}} = 2 \frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e} \beta\right)}{\Gamma(m_e)} - \left[\frac{\Gamma\left(m_e, \frac{m_e}{\Omega_e} \beta\right)}{\Gamma(m_e)} \right]^2 \quad (36)$$

4 数值结果与性能分析

本节首先给出了直接传输和 BRS 策略的 SRT 性能数值结果。直接传输和 BRS 方案的 OP 和 IP 分别通过式 (22)、式 (23)、式 (31)、式 (36)



给出。根据以上解析表达式,通过数值计算进行性能仿真。假设信道平均功率 $\Omega_m=1$ 、 $\Omega_e=0.1$,另外,假设传输信号采用 BPSK 调制,其频带利用率为 $R_b=1$ bit/(s·Hz)。

图 3 给出了在不同 Nakagami 信道衰落因子 m 的情况下直接传输和 BRS 方案的 OP 性能。假设中继数 $N=6$ 。由图 3 可知,随着信噪比的增加,无论是直接传输还是 BRS,中断概率均降低。在相同衰落因子 m 的前提下,所提 BRS 方案的中断概率在较大 SNR 情况下较直接传输中断概率显著降低,即可靠性显著提升。当 $m=1$ 时,为瑞利衰落信道,仿真结果与参考文献[11]中给出的中断性能一致。当 m 增加时,直接传输和 BRS 的中断性能都得以提升。因此,增加信道衰落因子 m 可以提升信号传输可靠性。

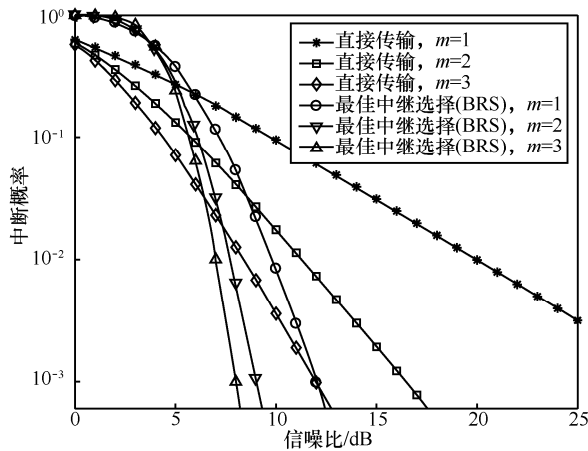


图 3 不同 Nakagami 信道衰落因子下直接传输与 BRS 方案的中断性能

图 4 给出了在不同 Nakagami 信道衰落因子 m 情况下,直接传输和 BRS 方案的 IP 性能。中继数为 6。由图 4 可知,随着窃听信道信噪比的增加,直接传输和 BRS 方案的截获概率增加。在相同衰落因子情况下,所提 BRS 方案的截获概率始终小于直接传输,即 BRS 方案的安全性优于直接传输。另外,随着信道衰落因子的增加,在稍小 SNR 情况下截获概率均降低。因此,增加信道衰落因子 m 可以提升信号传输的安全性。

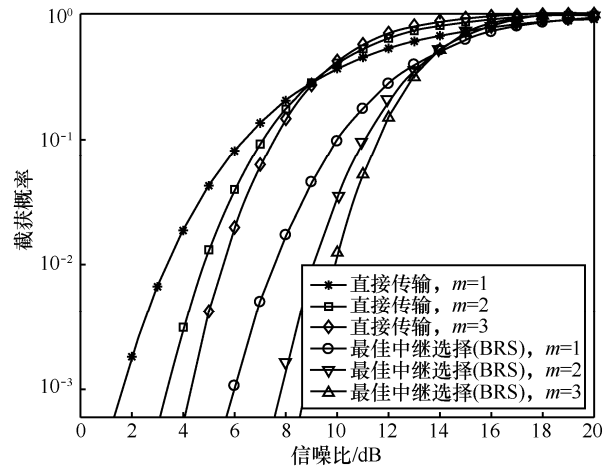


图 4 不同 Nakagami 信道衰落因子下直接传输与 BRS 方案的截获性能

图 5 给出了在不同 Nakagami 信道衰落因子 m 情况下,直接传输和 BRS 方案的 SRT 性能。假设中继数为 6。由图 5 可知,当 OP 增加时,IP 降低,即 OP 与 IP 存在折中。在衰落因子相同的情况下,所提 BRS 方案的 SRT 性能优于直接传输。另外,当 $m=1$ 时为瑞利衰落,其 SRT 性能与参考文献[11]中的 SRT 性能一致。当衰落因子增加时,不论直接传输还是 BRS 方案,其 SRT 性能都得以提升。因此,增加信道衰落因子 m 可以提升 SRT 性能。

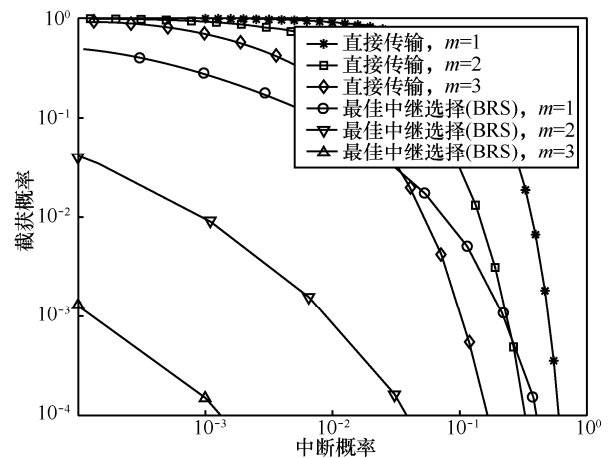


图 5 不同 Nakagami 信道衰落因子下直接传输与 BRS 方案的 SRT 性能

图 6 给出了不同中继数对直接传输和 BRS 方案 SRT 性能的影响。分别取中继数为 2、4、6。

图6中虚线表示在参考文献[12]中ORS方案的SRT性能,且瑞利衰落 $m=1$ 。实线表示本文所提BRS方案的SRT性能,此时 $m=2$ 。由图6可知,OP增加的同时IP在减小,即OP与IP之间存在折中。随着中继数的增加,SRT性能均提高,这说明了中继对协作传输的优势。另外,在相同中继数时,所提BRS方案的SRT性能要优于ORS方案的SRT性能。

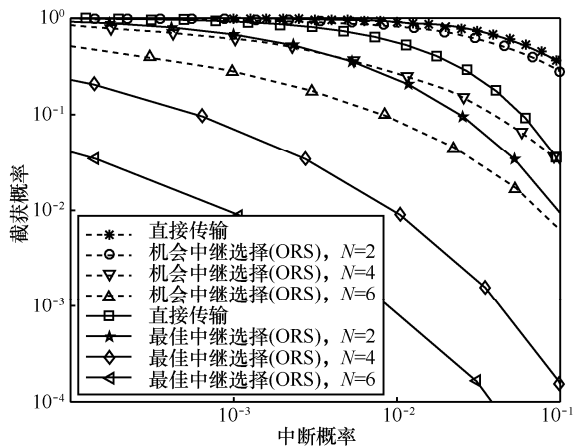


图6 不同中继数对直接传输与BRS方案SRT性能的影响

5 结束语

本文提出了在 Nakagami- m 衰落信道下针对单窃听用户攻击的多中继认知 DF 中继网络中实现安全性与可靠性折中的最佳中继选择(BRS)策略。以直接传输和参考文献[12]中的ORS方案作为对比,进行SRT性能分析,所提BRS方案优于直接传输,且在相同中继数时,所提方案的SRT性能优于ORS方案的SRT性能。所提方案的SRT性能随着中继数和在一定中继数下 Nakagami 信道衰落因子 m 的增加而显著改善。

参考文献:

- [1] KARALOPOULOS S V. A primer on cryptography in communications [J]. IEEE Communications Magazine, 2006, 44(4): 146-151.
- [2] 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.
- [3] ZOU Y, ZHU J, WANG X, et al. Improving physical-layer security in wireless communications using diversity techniques[J]. IEEE Network, 2015, 29(1): 42-48.
- [4] MANU, GOEL A. Encryption algorithm using dual modulus[C]//2017 IEEE the 3rd International Conference on Computational Intelligence & Communication Technology (CICIT), February 9-10, 2017, Ghaziabad, India. Piscataway: IEEE Press, 2017: 1-4.
- [5] SHANNON C E. Communication theory of secrecy systems [J]. The Bell System Technical Journal, 1949, 28(4): 656-715.
- [6] WYNER A D. The wire-tap channel[J]. The Bell System Technical Journal, 1975, 54(8): 1355-1387.
- [7] LEUNG-YAN-CHENG S K, HELLMAN M E. The Gaussian wire-tap channel [J]. IEEE Transactions on Information Theory, 1978, 24(4): 451-456.
- [8] ZHUANG Y, LAMPE L. Physical layer security in MIMO power line communication networks [C]//2011 the 18th IEEE International Symposium on Power Line Communications and its Applications, March 30-April 2, 2014, Glasgow, UK. Piscataway: IEEE Press, 2014: 272-277.
- [9] ZOU Y, ZHU J, WANG X, et al. A survey on wireless security: technical challenges, recent advances, and future trends [J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.
- [10] ZOU Y, WANG X, SHEN W. Optimal relay selection for physical-layer security in cooperative wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2013, 31(10): 2099-2111.
- [11] ZHU J, ZOU Y, CHAMPAGNE B, et al. Security-reliability tradeoff analysis of multi-relay-aided decode-and-forward cooperation systems [J]. IEEE Transactions on Vehicular Technology, 2016, 65(7): 5825-5831.
- [12] ZOU Y, WANG X, SHEN W, et al. Security versus reliability analysis of opportunistic relaying [J]. IEEE Transactions on Vehicular Technology, 2014, 63(6): 2653-2661.
- [13] ZOU Y, ZHU J, LI X, et al. Relay selection for wireless communications against eavesdropping: a security reliability tradeoff perspective [J]. IEEE Network, 2016, 30(9): 74-79.
- [14] HUANG H, SUN W, YANG J, et al. Relay selections for security and reliability in mobile communication networks over Nakagami- m fading channels [J]. Security and Communication Networks, 2017: 1-8.
- [15] YUAN Y, ZHAO R, LIN, et al. Secrecy outage probability of



cognitive decode-and-forward relay networks[C]//2016 IEEE International Conference on Communications Workshops (ICCW), May 23-27, 2016, Kuala Lumpur, Malaysia. Piscataway: IEEE Press, 2016: 260-265.

[作者简介]



王兴鹏（1993-），男，杭州电子科技大学硕士生，主要研究方向为认知无线网络协作传输中的物理层安全策略。



许晓荣（1982-），男，博士后，杭州电子科技大学副教授、硕士生导师，主要研究方向为能效优先认知无线网络的物理层安全策略与资源分配方法等。

胡安迪（1994-），男，杭州电子科技大学硕士生，主要研究方向为认知携能通信网络中的物理层安全策略。

冯维（1984-），女，博士，杭州电子科技大学讲师，主要研究方向为无线多跳网络中的物理层安全策略等。