

## 不完美时间同步下物理层安全协同干扰功率分配

郭文博<sup>1</sup>, 宋长庆<sup>1</sup>, 文荣<sup>2</sup>, 赵宏志<sup>1</sup>, 唐友喜<sup>1</sup>

(1. 电子科技大学通信抗干扰技术国家级重点实验室, 四川 成都 611731;

2. 成都工业学院网络与通信工程学院, 四川 成都 611730)

**摘要:** 物理层安全中, 考虑不完美时间同步, 提出了一种使通信系统保密容量最大化的协同干扰功率分配方法。通过分析授权接收机处由不完美时间同步引入的残余干扰功率, 给出了最优功率分配方法, 并讨论了最优干扰功率与相对信道质量之间的关系。理论和仿真分析表明, 当同步误差较小时, 需要消耗额外功率来达到预设的保密容量, 且干扰功率随误差增大而增大; 随着误差进一步增大, 系统保密容量渐渐无法达到预设目标, 甚至可能降至0。

**关键词:** 物理层安全; 不完美时间同步; 保密容量; 协同干扰; 功率分配

**中图分类号:** TN975

**文献标识码:** A

**doi:** 10.11959/j.issn.1000-436x.2019214

## Cooperative interference power allocation in physical layer security under imperfect time synchronization

GUO Wenbo<sup>1</sup>, SONG Changqing<sup>1</sup>, WEN Rong<sup>2</sup>, ZHAO Hongzhi<sup>1</sup>, TANG Youxi<sup>1</sup>

1. National Key Lab of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

2. School of Network and Communication Engineering, Chengdu Technological University, Chengdu 611730, China

**Abstract:** In physical layer security, considering imperfect time synchronization, a power allocation scheme was proposed to maximize the system secrecy capacity. By analyzing the residual interference power at the authorized receiver caused by imperfect time synchronization, the optimal power distribution method was given, and the relationship between the optimal interference power and the relative channel quality was discussed. Theory and simulation analysis show that when the synchronization error is small, the synchronization error consumes extra power to reach the preset secrecy capacity, and the interference power increases with its increase. As the synchronization error increases, the secrecy capacity of the system gradually fails to reach the preset target, and may even drop to zero.

**Key words:** physical layer security, imperfect time synchronization, secrecy capacity, cooperative interference, power allocation

### 1 引言

物理层安全技术可以降低通信信息被非法窃听的风险, 并可以应用于下一代无线通信<sup>[1]</sup>。但

Wyner<sup>[2]</sup>表明, 只有当窃听信道弱于合法信道时, 通信安全才能够得到保证, 这限制了通信系统的安全性能。为了打破这一限制, 文献[3]提出利用协同干扰来主动降低窃听信道的质量。协同干扰的先验

收稿日期: 2019-06-27; 修回日期: 2019-08-05

通信作者: 赵宏志, lyn@uestc.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2018YFB1801903); 国家自然科学基金资助项目 (No.61771115, No.61771107, No.61701075, No.61531009); 国家重大科技专项基金资助项目 (No.2016ZX03001009); 四川科技基金资助项目 (No.2019JDRC0006)

**Foundation Items:** The National Key Research and Development Program of China (No.2018YFB1801903), The National Natural Science Foundation of China (No.61771115, No.61771107, No.61701075, No.61531009), The National Science and Technology Major Project (No. 2016ZX03001009), Sichuan Science and Technology Program (No.2019JDRC0006)

信息对授权接收机已知、对窃听装置未知，因此在授权接收机处进行时频同步和信道估计可以消除协同干扰，而窃听装置处无法做到这一点<sup>[4]</sup>，这提高了合法信道的安全性。

现有文献<sup>[5-13]</sup>假设协同干扰在授权接收机处被完美消除。例如，在上述完美消除干扰的假设下，文献[5-6]研究了单跳通信网络的安全性能；文献[7-9]研究了两跳通信网络的安全性能；文献[10]中使用了全双工中继器，研究了多跳网络情形。近年来，随着基于射频技术的无线功率传输技术的发展，文献[11-12]中的能量采集型协同干扰技术成为可能。此外，文献[13]利用协同干扰来阻塞窃听装置的模数转换器，提出了一种强保密方案。

但是，上述文献未曾考虑实际系统中的非理想因素，由于精确的时间同步难以实现，授权接收机很难彻底消除协同干扰的影响<sup>[14]</sup>。并且协同干扰功率大于信号功率，干扰消除后即使微弱的同步误差也会造成相当大的干扰泄露，很大程度地降低了通信和安全性能。

为了解决这一问题，本文针对基于协同干扰保护的点对点通信系统，考虑不完美时间同步在授权接收机处引入的残余干扰，提出了一种使通信系统保密容量最大化的物理层安全协同干扰功率分配方案。本文首先分析了授权接收机处的残余干扰功率，随后给出了最优功率分配方法，然后讨论了最佳干扰功率与相对信道质量之间的关系，并在仿真部分针对同步误差对保密容量和总功耗的影响进行了验证。

## 2 通信系统模型

基于协同干扰的点对点通信系统模型如图 1 所示。通信发射机（节点 s）以功率  $P_s$  向授权接收机

（节点 r）发送通信信号  $\tilde{x}_s(t)$ ，同时协同干扰机（节点 c）以功率  $P_c$  发送协同干扰信号  $\tilde{x}_c(t)$  来干扰窃听装置（节点 e）。协同干扰信息对授权接收机已知，但对窃听装置未知。

### 2.1 通信发射机

假设通信发射机处数字基带信号为  $s(n)$ ，经过数模转换器（DAC, digital-to-analog converter）转换为连续基带信号  $s(t)$ 。将  $s(t)$  上变频到射频域，变为

$$\tilde{x}_s(t) = s(t)e^{j(2\pi f_s t + \varphi_s)} \quad (1)$$

其中， $f_s$  和  $\varphi_s$  分别表示通信信号  $\tilde{x}_s(t)$  的载波频率和初始相位。

### 2.2 协同干扰机

假设协同干扰机处协同干扰的数字基带信号为  $c(n)$ ，且服从均值为 0 的高斯分布<sup>[15]</sup>，经过数模转换器后转换为连续基带信号  $c(t)$ 。将  $c(t)$  上变频到射频域，变为

$$\tilde{x}_c(t) = c(t)e^{j(2\pi f_c t + \varphi_c)} \quad (2)$$

其中， $f_c$  和  $\varphi_c$  分别表示协同干扰信号  $\tilde{x}_c(t)$  的载波频率和初始相位。协同干扰信息  $c(n)$  对授权接收机是已知的，但对窃听装置未知。

### 2.3 信道

假设通信信号  $\tilde{x}_s(t)$  和协同干扰信号  $\tilde{x}_c(t)$  互不相关，且在传播过程中经历平坦慢衰落。授权接收机和窃听装置处的接收射频信号分别为

$$\tilde{y}_r(t) = h_{cr}\tilde{x}_c(t - \tau_{cr}) + h_{sr}\tilde{x}_s(t - \tau_{sr}) + \tilde{n}_r(t) \quad (3)$$

$$\tilde{y}_e(t) = h_{ce}\tilde{x}_c(t - \tau_{ce}) + h_{se}\tilde{x}_s(t - \tau_{se}) + \tilde{n}_e(t) \quad (4)$$

其中， $h_{cr}$ 、 $h_{ce}$ 、 $h_{sr}$ 、 $h_{se}$  分别表示节点 c 和 r、节点 c 和 e、节点 s 和 r、节点 s 和 e 间信号的复信道衰落， $\tau_{cr}$ 、 $\tau_{ce}$ 、 $\tau_{sr}$ 、 $\tau_{se}$  分别表示节点 c 和 r、节

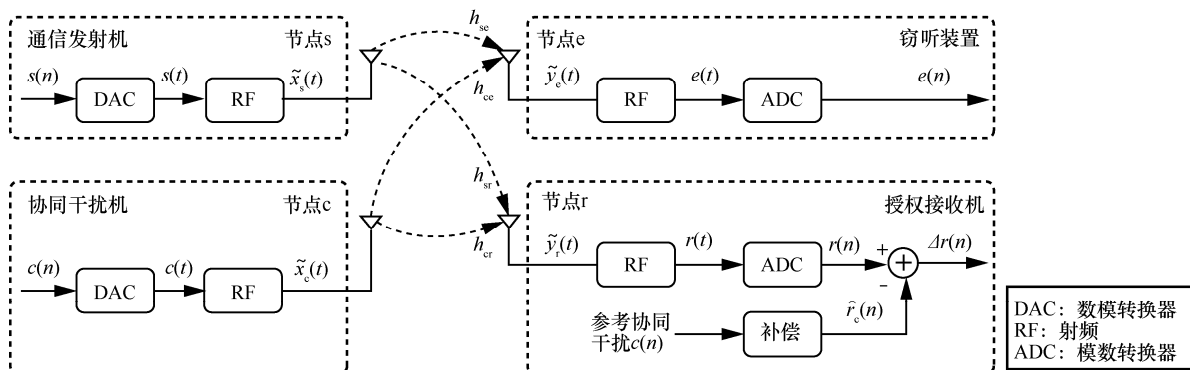


图 1 基于协同干扰的点对点通信系统模型

点 c 和 e、节点 s 和 r、节点 s 和 e 间的传播时延， $\tilde{n}_r(t)$ 、 $\tilde{n}_c(t)$  分别为授权接收机和窃听装置处的热噪声，且与  $\tilde{x}_s(t)$  和  $\tilde{x}_c(t)$  不相关。

### 2.4 授权接收机

实际系统中，授权接收机的振荡器并不总能与通信发射机和协同干扰机的振荡器完美匹配，三者之间可能存在频率和相位偏移。假设授权接收机的载波频率和初始相位分别为  $f_r$  和  $\varphi_r$ ，接收信号  $\tilde{y}_r(t)$  经下变频之后变为基带信号，即

$$r(t) = \tilde{y}_r(t)e^{-j(2\pi f_r t + \varphi_r)} = h_{cr}c(t - \tau_{cr})e^{j(2\pi\Delta f_{cr}t + \Delta\varphi_{cr})} + h_{sr}s(t - \tau_{sr})e^{j(2\pi\Delta f_{sr}t + \Delta\varphi_{sr})} + n_r(t) \quad (5)$$

其中， $\Delta f_{cr} = f_c - f_r$ 、 $\Delta f_{sr} = f_s - f_r$  分别表示节点 c 和 r、节点 s 和 r 间的载波频率偏移， $\Delta\varphi_{cr} = \varphi_c - \varphi_r - 2\pi f_c \tau_{cr}$ 、 $\Delta\varphi_{sr} = \varphi_s - \varphi_r - 2\pi f_s \tau_{sr}$  分别表示节点 c 和 r、节点 s 和 r 间的载波相位偏移。节点 r 处的等效基带噪声为  $n_r(t) = \tilde{n}_r(t)e^{-j(2\pi f_r t + \varphi_r)}$ 。

记模数转换器的采样周期为  $T$ 。经模数转换器后，授权接收机处离散时间基带信号序列可以表示为

$$r(n) = r_c(n) + r_s(n) + w_r(n) \quad (6)$$

其中， $r_c(n) = h_{cr}c(n - D_{cr})e^{j(2\pi F_{cr}n + \Delta\varphi_{cr})}$  表示协同干扰部分， $r_s(n) = h_{sr}s(n - D_{sr})e^{j(2\pi F_{sr}n + \Delta\varphi_{sr})}$  表示通信信号部分， $w_r(n)$  表示噪声部分， $D_{cr} = \frac{\tau_{cr}}{T}$ 、 $D_{sr} = \frac{\tau_{sr}}{T}$  分别表示节点 c 和 r、节点 s 和 r 间的归一化传播时延， $F_{cr} = \Delta f_{cr}T$ 、 $F_{sr} = \Delta f_{sr}T$  分别表示节点 c 和 r、节点 s 和 r 间的归一化频率偏移， $\Delta\varphi_{cr}$ 、 $\Delta\varphi_{sr}$  分别表示节点 c 和 r、节点 s 和 r 间的相位偏移。

### 2.5 窃听装置

类似于授权接收机，经模数转换器后窃听装置处接收信号为

$$e(n) = e_c(n) + e_s(n) + w_e(n) \quad (7)$$

其中， $e_c(n) = h_{ce}c(n - D_{ce})e^{j(2\pi F_{ce}n + \Delta\varphi_{ce})}$  表示协同干扰部分， $e_s(n) = h_{se}s(n - D_{se})e^{j(2\pi F_{se}n + \Delta\varphi_{se})}$  表示通信信号部分， $w_e(n)$  为噪声部分， $D_{ce} = \frac{\tau_{ce}}{T}$ 、 $D_{se} = \frac{\tau_{se}}{T}$  分别表示节点 c 和 e、节点 s 和 e 间的归一化传播时延， $F_{ce} = \Delta f_{ce}T$ 、 $F_{se} = \Delta f_{se}T$  分别表示节点 c 和 e、节点 s 和 e 间的归一化频率偏移， $\Delta\varphi_{ce}$ 、 $\Delta\varphi_{se}$  分别表示节点 c 和 e、节点 s 和 e 间的相位偏移。

## 3 不完美时间同步的功率分配方案

### 3.1 信干噪比分析

假设归一化传播时延的估计值为  $\hat{D}_{cr}$ ，且协同干扰机与授权接收机间的频偏  $\Delta f_{cr}$  和等效信道衰落  $h_{cr}e^{j\Delta\varphi_{cr}}$  已经得到精确估计。经过信道补偿和时频对齐后，本地协同干扰数字基带参考信号  $c(n)$  变为

$$\hat{r}_c(n) = h_{cr}c(n - \hat{D}_{cr})e^{j(2\pi F_{cr}n + \Delta\varphi_{cr})} = h_{cr}c_0(n)e^{j(2\pi F_{cr}n + \Delta\varphi_{cr})} \quad (8)$$

令  $D = D_{cr} - \hat{D}_{cr}$  表示归一化同步误差，则有  $c(n - D_{cr}) = c_0(n - D)$ 。 $c_0(n - D)$  可以看作  $c_0(n)$  的一个延迟重复，可展开成

$$c_0(n - D) = c_0(n) * \text{sinc}(n - D) = c_0(n)\text{sinc}(D) + \sum_{\substack{i=-\infty \\ i \neq 0}}^{+\infty} [c_0(n - i)\text{sinc}(i - D)] = A_D c_0(n) + c_D(n) \quad (9)$$

其中， $*$  表示卷积运算， $c_D(n) = \sum_{\substack{i=-\infty \\ i \neq 0}}^{+\infty} [c_0(n - i)\text{sinc}(i - D)]$ ， $A_D = \text{sinc}(D)$  表示  $c_0(n)$  中由归一化同步误差引起的衰减系数。

$c_0(n)$  服从均值为 0 的高斯分布，因此  $c_0(n)$  与其延迟重复线性组合的  $c_D(n)$  不相关。则授权接收机处离散时间基带信号中协同干扰部分  $r_c(n)$  可以表示为

$$r_c(n) = h_{cr}c_0(n - D)e^{j(2\pi F_{cr}n + \Delta\varphi_{cr})} = A_D \hat{r}_c(n) + \hat{c}_D(n) \quad (10)$$

其中， $\hat{c}_D(n) = h_{cr}c_D(n)e^{j(2\pi F_{cr}n + \Delta\varphi_{cr})}$  为来自其他符号的干扰成分，即符号间串扰 (ISI, inter-symbol interference)，且  $\hat{r}_c(n)$  与  $\hat{c}_D(n)$  互不相关。

$r_c(n)$  和  $\hat{c}_D(n)$  的功率分别为

$$P\{r_c(n)\} = P\{\hat{r}_c(n)\}, \\ P\{\hat{c}_D(n)\} = P\{r_c(n)\} - P\{A_D \hat{r}_c(n)\} = (1 - A_D^2)P\{\hat{r}_c(n)\} \quad (11)$$

协同干扰重建完成之后，进行协同干扰抵消。考虑同步误差的影响，授权接收机处残余协同干扰  $\Delta r_c(n)$  可以表示为

$$\Delta r_c(n) = r_c(n) - \hat{r}_c(n) = (A_D - 1)\hat{r}_c(n) + \hat{c}_D(n) \quad (12)$$

$\Delta r_c(n)$  的功率为

$$P\{\Delta r_c(n)\} = (2 - 2A_D)|h_{cr}|^2 P_c \quad (13)$$

协同干扰消除后，授权接收机处的信干噪比为

$$\gamma_r = \frac{|h_{sr}|^2 P_s}{[2 - 2A_D]|h_{cr}|^2 P_c + \sigma_r^2} \quad (14)$$

其中,  $\sigma_r^2$  表示授权接收机处噪声的功率。

另一方面, 窃听装置处的信干噪比为

$$\gamma_e = \frac{|h_{se}|^2 P_s}{|h_{ce}|^2 P_c + \sigma_e^2} \quad (15)$$

其中,  $\sigma_e^2$  表示窃听装置处的噪声功率。简单起见, 假设  $\sigma_r^2 = \sigma_e^2 = \sigma^2$ 。此外, 功率约束关系为  $P_s + P_c = P$ ,  $P$  为发送通信信号和协同干扰的总功率预算。为了进一步简化节点  $r$  和节点  $e$  处的信干噪比, 引入比例因子  $\alpha \geq 0$ , 满足  $P_c = \alpha P_s$ , 则式(14)和式(15)可以表示为

$$\gamma_r = \frac{|h_{sr}|^2 \eta}{[2 - 2A_D] |h_{cr}|^2 \eta \alpha + \alpha + 1} \quad (16)$$

$$\gamma_e = \frac{|h_{se}|^2 \eta}{|h_{ce}|^2 \eta \alpha + \alpha + 1} \quad (17)$$

其中,  $\eta = \frac{P}{\sigma^2}$  表示归一化功率预算。通信系统中的信道衰落  $h_{sr}$ 、 $h_{cr}$ 、 $h_{se}$  和  $h_{ce}$  的值是可获得的: 在节点  $r$  处进行信道估计可得到  $h_{sr}$  和  $h_{cr}$  的值, 通过监测活跃的窃听装置并预测其可能的活动可以得到  $h_{se}$  和  $h_{ce}$  的值<sup>[15]</sup>。

### 3.2 协同干扰功率分配方案

考虑授权接收机处由于不完美时间同步引起的协同干扰泄露, 本文提出一种功率分配方案, 该方案可最大化保密容量。对于平坦慢衰落信道, 保密容量  $C_s$  为<sup>[16]</sup>

$$C_s = \begin{cases} \frac{1}{2} \text{lb}(1 + \gamma_r) - \frac{1}{2} \text{lb}(1 + \gamma_e), & \gamma_r > \gamma_e \\ 0, & \gamma_r \leq \gamma_e \end{cases} \quad (18)$$

由式(18)可知, 只有当授权接收机处的信干噪比高于窃听装置处, 即  $\gamma_r > \gamma_e$  时, 才能保证保密容量为正值。于是最大化保密容量问题可以数学表征为

$$\begin{aligned} \max_{\alpha} \quad & C_s = \frac{1}{2} \text{lb}(1 + \gamma_r) - \frac{1}{2} \text{lb}(1 + \gamma_e) \\ \text{s.t.} \quad & \begin{cases} \gamma_r > \gamma_e \\ \alpha \geq 0 \end{cases} \end{aligned} \quad (19)$$

**命题** 最优功率分配因子  $\alpha^*$  可由式(20)计算。

$$\alpha^* = \begin{cases} 0, & a \geq c \text{ 且 } b > d \\ \alpha_1, & a < c \text{ 且 } b > \frac{ad + c - a}{c} \\ \phi, & \text{其他} \end{cases} \quad (20)$$

其中,  $a = [2 - 2A_D] |h_{cr}|^2 \eta + 1$ ,  $b = |h_{sr}|^2 \eta + 1$ ,  $c = |h_{ce}|^2 \eta + 1$ ,  $d = |h_{se}|^2 \eta + 1$ 。  $\alpha_1$  可以表示为

$$\alpha_1 = \frac{ac(b-d) - \sqrt{ac(a-c)(ad-bc)(b-1)(d-1)}}{ac[(ad-bc) - (a-c)]} \quad (21)$$

当  $\alpha^* = 0$  时, 意味着通信系统的保密性能很好, 不需要发送协同干扰; 当  $\alpha^* = \phi$  时, 意味着系统最好停止发送通信信号和协同干扰, 因为此时加密能力恒为非正值。

**证明**

式(19)可以表示为

$$\begin{aligned} \max_{\alpha} \quad & C_s = \frac{1}{2} \text{lb} \left[ \frac{(a\alpha + b)(c\alpha + 1)}{(a\alpha + 1)(c\alpha + d)} \right] \\ \text{s.t.} \quad & \begin{cases} [(ad-bc) - (a-c)]\alpha < b-d \\ \alpha \geq 0 \end{cases} \end{aligned} \quad (22)$$

对  $C_s$  关于  $\alpha$  进行一阶求导, 可得

$$\frac{dC_s}{d\alpha} = \frac{A\alpha^2 + B\alpha + C}{2\beta(\alpha)\ln 2} \quad (23)$$

其中, 有

$$\begin{cases} A = ac[(ad-bc) - (a-c)] \\ B = 2ac(d-b) \\ C = (ad-bc) - bd(a-c) \\ \beta(\alpha) = (a\alpha + b)(c\alpha + 1)(a\alpha + 1)(c\alpha + d) \end{cases} \quad (24)$$

因为  $a \geq 1$ ,  $b > 1$ ,  $c > 1$ ,  $d > 1$ ,  $\alpha \geq 0$ , 故  $\beta(\alpha) > 0$ 。令  $\frac{dC_s}{d\alpha} = 0$ , 则有

$$A\alpha^2 + B\alpha + C = 0 \quad (25)$$

通过式(23)观察  $C_s$  的单调性, 本文给出了以下 4 种情形的最佳功率分配因子。

**情形 1** 对于  $A = 0$ , 即  $a - c = ad - bc$ , 约束条件等价于  $b > d$ , 可得  $B < 0$ , 式(25)的解为

$$\alpha_0 = \frac{(a-c)(bd-1)}{2ac(d-b)} \quad (26)$$

当  $\alpha < \alpha_0$  时,  $\frac{dC_s}{d\alpha} > 0$ ; 当  $\alpha > \alpha_0$  时,  $\frac{dC_s}{d\alpha} < 0$ ; 因此随着  $\alpha$  的增大,  $C_s$  先增大后减小, 最大保密容量在  $\alpha^* = \max\{0, \alpha_0\}$  处取得。由  $b > d$  可得  $a = \frac{(b-1)c}{d-1} > c$ , 故  $\alpha_0 < 0$ , 此时的最佳功率分配因子为

$$\alpha^* = \begin{cases} 0, & a > c \text{ 且 } b = \frac{ad+c-a}{c} \\ \phi, & a < c \text{ 且 } b = \frac{ad+c-a}{c} \end{cases} \quad (27)$$

**情形 2** 对于  $A \neq 0$  且  $B^2 = 4AC$ , 即  $a-c \neq ad-bc$  且  $(a-c)(ad-bc) = 0$ , 约束条件等价于  $b > d$ , 可得  $A < 0$ , 对于任意的  $\alpha$  恒有  $\frac{dC_s}{d\alpha} \leq 0$ , 即  $C_s$  是关于  $\alpha$  的非增函数。最佳功率分配因子为

$$\alpha^* = \begin{cases} 0, & a > c \text{ 且 } b = \frac{ad}{c} \text{ 或 } a = c \text{ 且 } b > d \\ \phi, & a < c \text{ 且 } b = \frac{ad}{c} \text{ 或 } a = c \text{ 且 } b < d \end{cases} \quad (28)$$

**情形 3** 对于  $A \neq 0$  且  $B^2 < 4AC$ , 即  $(a-c) \cdot (ad-bc) < 0$ , 最佳功率分配因子为

$$\alpha^* = \begin{cases} 0, & a > c \text{ 且 } b > \frac{ad}{c} \\ \phi, & a < c \text{ 且 } b < \frac{ad}{c} \end{cases} \quad (29)$$

情形 3 证明如下。

1) 当  $a > c$ ,  $ad < bc$  时,  $A < 0$ , 约束条件等价于  $\alpha \geq 0$ , 此时对于任意的  $\alpha$  恒有  $\frac{dC_s}{d\alpha} < 0$ , 即  $C_s$  关于  $\alpha$  单调递减, 最佳功率分配因子为  $\alpha^* = 0$ 。

2) 当  $a < c$ ,  $ad > bc$  时, 约束条件等价于  $\phi$ 。证毕。

**情形 4** 对于  $A \neq 0$  且  $B^2 > 4AC$ , 即  $a-c \neq ad-bc$  且  $(a-c)(ad-bc) > 0$ , 式(25)的解为

$$\alpha_1 = \frac{ac(b-d) - \sqrt{ac(a-c)(ad-bc)(b-1)(d-1)}}{ac[(ad-bc) - (a-c)]} \quad (30)$$

$$\alpha_2 = \frac{ac(b-d) + \sqrt{ac(a-c)(ad-bc)(b-1)(d-1)}}{ac[(ad-bc) - (a-c)]} \quad (31)$$

最佳功率分配因子为

$$\alpha^* = \begin{cases} 0, & a > c \text{ 且 } d < b < \frac{ad}{c} \text{ 且 } b \neq \frac{ad+c-a}{c} \\ \alpha_1, & a < c \text{ 且 } b > \frac{ad+c-a}{c} \\ \phi, & a > c \text{ 且 } b \leq d \text{ 或 } a < c \text{ 且 } \frac{ad}{c} < b < \frac{ad+c-a}{c} \end{cases} \quad (32)$$

情形 4 证明如下。

1) 当  $a-c > ad-bc$  且  $b > d$  时,  $A < 0$ , 此时  $\alpha \geq 0$ 。当  $\alpha < \alpha_2$  或  $\alpha > \alpha_1$  时,  $\frac{dC_s}{d\alpha} < 0$ ; 当

$\alpha_2 < \alpha < \alpha_1$  时,  $\frac{dC_s}{d\alpha} > 0$ ; 因此  $C_s$  随着  $\alpha$  的递增先递减再递增再递减, 最佳功率分配因子在  $\alpha^* = \max\{0, \alpha_1\}$  处获得。

若  $a-c > ad-bc > 0$ , 则由式(33)可得  $\alpha_1 < 0$ , 此时  $\alpha^* = 0$ 。

$$\begin{aligned} & ac(a-c)(ad-bc)(b-1)(d-1) < \\ & ac(a-c)(b-1)(a-c)(d-1) = \\ & ac[ab + (-bc - a + c)][(ad - a + c) - cd] < \\ & ac(ab - ad)(bc - cd) = [ac(b-d)]^2 \end{aligned} \quad (33)$$

若  $0 > a-c > ad-bc$ , 类似式(33), 可证得  $\alpha_1 > 0$ , 此时  $\alpha^* = \alpha_1$ 。

2) 当  $a-c > ad-bc$  且  $b \leq d$  时,  $A < 0$ , 此时  $\alpha > \frac{b-d}{(ad-bc) - (a-c)}$ 。当  $\alpha < \alpha_2$  或  $\alpha > \alpha_1$  时,

$\frac{dC_s}{d\alpha} < 0$ ; 当  $\alpha_2 < \alpha < \alpha_1$  时,  $\frac{dC_s}{d\alpha} > 0$ 。因此  $C_s$  随着  $\alpha$  的递增先递减再递增再递减, 最佳功率分配因子在  $\alpha^* = \alpha_1$  处获得。

3) 当  $a-c < ad-bc$  且  $b > d$  时,  $A > 0$ , 此时  $0 \leq \alpha < \frac{b-d}{(ad-bc) - (a-c)}$ 。当  $\alpha < \alpha_1$  或  $\alpha > \alpha_2$  时,

$\frac{dC_s}{d\alpha} > 0$ ; 当  $\alpha_1 < \alpha < \alpha_2$  时,  $\frac{dC_s}{d\alpha} < 0$ 。因此  $C_s$  随着  $\alpha$  的增大先递增再递减再递增, 最佳功率分配因子在  $\alpha^* = \max\{0, \alpha_1\}$  处获得。

类似式(33), 若  $0 < a-c < ad-bc$ ,  $\alpha^* = 0$ ; 若  $a-c < ad-bc < 0$ ,  $\alpha^* = \alpha_1$ 。

4) 当  $a-c < ad-bc$  且  $b \leq d$  时,  $\alpha^*$  取值为  $\phi$ 。由式(27)~式(32), 可得式(20)和式(21)中的结论。证毕。

由式(20)可得出以下结论。

1) 系统可实现的最大保密容量为

$$C_s^* = \frac{1}{2} \text{lb} \left[ \frac{(a\alpha^* + b)(c\alpha^* + 1)}{(a\alpha^* + 1)(c\alpha^* + d)} \right] \quad (34)$$

2) 当  $a \geq c$  时, 授权接收机处消除部分协同干扰后, 其协同干扰功率仍强于窃听装置处。此时, 最优功率分配因子  $\alpha^*$  可表示为

$$\alpha^* = \begin{cases} 0, & b > d \\ \phi, & b \leq d \end{cases} \quad (35)$$

式(35)表明, 当  $a \geq c$  时, 发送协同干扰并没有发挥作用。如果授权接收机处的通信信号功率强于

窃听装置处，通信系统的保密性能很好，不需要发送协同干扰；如果授权接收机处的通信信号功率弱于窃听装置处，系统应停止工作，因为此时无论协同干扰机是否发送协同干扰，窃听装置总能窃听到通信信息。

3) 当  $a < c$  时，即使消除了部分协同干扰，授权接收机处的协同干扰功率仍弱于窃听装置处。此时，最优功率分配因子  $\alpha^*$  可以表示为

$$\alpha^* = \begin{cases} \alpha_1, & b > \frac{ad+c-a}{c} \\ \phi, & b \leq \frac{ad+c-a}{c} \end{cases} \quad (36)$$

式(36)表明，当  $b > \frac{ad+c-a}{c}$  时，发送协同干扰有助于提升系统的保密容量；当  $b \leq \frac{ad+c-a}{c}$  时，发送的协同干扰失去作用。

4) 若协同干扰被完美消除，即  $a=1$  时，最优功率分配因子  $\alpha^*$  可以表示为

$$\alpha^* = \begin{cases} \alpha_\infty, & b > \frac{c+d-1}{c} \\ \phi, & b \leq \frac{c+d-1}{c} \end{cases} \quad (37)$$

其中，有

$$\alpha_\infty = \frac{c(d-b) + \sqrt{c(bc-d)(b-1)(c-1)(d-1)}}{c[(bc-d)-(c-1)]} \quad (38)$$

5) 若合法信道远强于窃听信道，即  $b \gg d$  时，最优功率分配因子  $\alpha^* = 0$ ，此时没有必要发送协同干扰，因为即使协同干扰机不工作，窃听装置也无法窃听到通信信息。

6) 若合法信道远弱于窃听信道，即  $b \ll d$  时，最优功率分配因子  $\alpha^*$  为

$$\alpha^* = \begin{cases} \infty, & \frac{ad+c-a}{c} < b \ll d \\ \phi, & b \leq \frac{ad+c-a}{c}, b \ll d \end{cases} \quad (39)$$

式(39)表明，当  $\frac{ad+c-a}{c} < b \ll d$  时，协同干扰机应该尽可能地发送协同干扰以干扰窃听装置；当  $b \leq \frac{ad+c-a}{c}$  且  $b \ll d$  时，协同干扰机和通信发射机均应停止工作，因为此时系统的保密容量恒为非正值。

7) 若合法信道质量与窃听信道质量相当，协同干扰的发射功率应根据信道衰落情况和协同干扰消除能力而定，具体分析将在第 4 节中通过系统仿真与性能分析给出。

### 4 系统仿真与性能分析

本节对提出的最优功率分配方案进行了仿真验证。仿真中，通信信号和协同干扰均为独立同分布的高斯信号<sup>[17]</sup>。 $h_{cr}$ 、 $h_{ce}$ 、 $h_{sr}$ 、 $h_{se}$  分别表示节点 c 和 r、节点 c 和 e、节点 s 和 r、节点 s 和 e 间信号的复信道衰落， $d_{sr}$ 、 $d_{se}$ 、 $d_{cr}$ 、 $d_{ce}$  分别为节点 s 与 r、节点 s 与 e、节点 c 与 r、节点 c 与 e 间的距离。仿真参数如表 1 所示，并与文献[17]中未考虑不完美时间同步的功率分配方法进行了性能对比。

| 表 1      | 实施例参数设置   |
|----------|---|
| 参数       | 取值  |
| 载波频率/GHz | 2.4   |
| 工作带宽/MHz | 10  |
| 归一化同步误差  | $0 \leq D_{cr} \leq 1$  |
| 信道衰落/dB  | $ h_{sr} ^2 =  h_{se} ^2 = -66$ , $ h_{cr} ^2 =  h_{ce} ^2 = -60$ |
| 节点间距离/m  | $d_{sr} = d_{se} = 20$ , $d_{cr} = d_{ce} = 10$                   |

图 2 给出了考虑不完美时间同步、未考虑不完美时间同步、协同干扰被完美消除 3 种功率分配方案中通信系统可以达到的保密容量，其中归一化的功率预算分别为 90 dB、100 dB 和 110 dB。由图 2 可知，功率预算越大，保密容量越大。因为随着协同干扰功率的增加，窃听装置处的信噪比比授权接收机处降低得更严重。

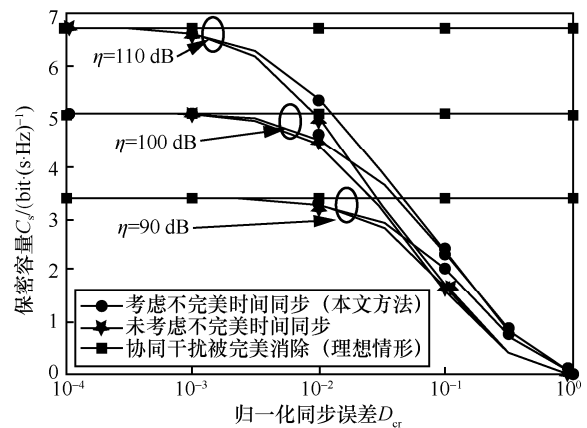


图 2 不同方案的通信系统保密容量对比

通过仿真结果观察可知，当归一化同步误差小于  $\frac{1}{10\sqrt{\eta}}$  时，同步误差的影响可以忽略不计，且功率预算越低，对同步误差的容忍度越大，因为此时协同干扰功率较小，授权接收机处由同步误差引起的残余干扰较弱；当归一化同步误差大于  $\frac{1}{10\sqrt{\eta}}$  时，

保密容量随着误差的增加而降低，且当时间同步误差超过 1 个符号时，经过协同干扰消除后授权接收机处的协同干扰功率仍强于窃听装置处，这将导致保密容量降至 0，即窃听装置总能窃听到通信信息。进一步地，当同步误差较大时，与未考虑同步误差的功率分配方案相比，本文提出的功率分配方案的保密容量提升了约 0.5 bit/(s·Hz)。

图 3 给出了在满足保密容量的要求下，归一化最小功耗与归一化同步误差的关系，其中保密容量阈值分别为 3 bit/(s·Hz)、5 bit/(s·Hz)、7 bit/(s·Hz)。通过仿真结果观察可知，当归一化同步误差小于  $\frac{1}{10\sqrt{\eta}}$  时，同步误差的影响可以忽略不计；当归一化同步误差大于  $\frac{1}{10\sqrt{\eta}}$  时，为了满足保密容量的要求，归一化功耗应随着同步误差的增加而增大。

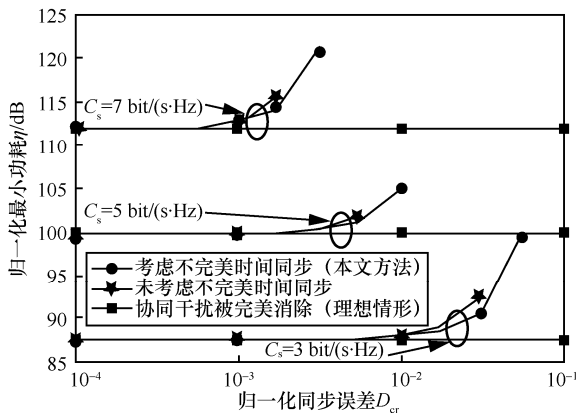


图 3 归一化最小功耗与归一化同步误差的关系

对于较小的同步误差，可以通过增大总功率预算来达到保密容量要求，表明同步误差的存在会导致功耗的增加；当同步误差增大时，为了达到预设的保密容量要求，本文功率分配方案比未考虑同步误差的功率分配方案需要更少的功耗；当同步误差进一步增大时，即使提高功率预算可能也达不到预设的保密容量要求。例如当保密容量要求不低于 5 bit/(s·Hz) 时，归一化同步误差应小于  $1 \times 10^{-2}$ 。

当归一化同步误差为  $1 \times 10^{-2}$  时，图 4 和图 5 分别展示了窃听信道与合法信道间的相对信道质量对归一化协同干扰功率和相应的保密容量的影响。下面的仿真中，信道衰落  $|h_{cr}|^2$ 、 $|h_{ce}|^2$ 、 $|h_{sr}|^2$  分别设置为 -60 dB、-60 dB、-66 dB。

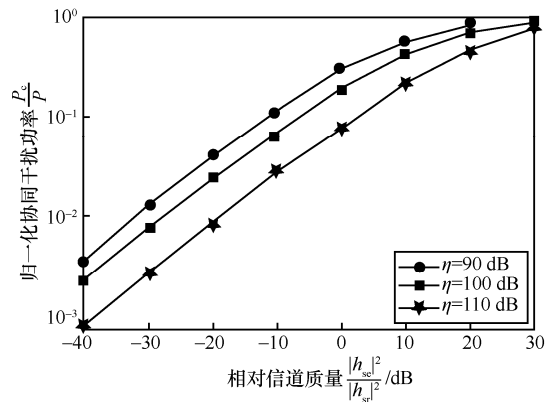


图 4 窃听信道质量对最优协同干扰功率的影响

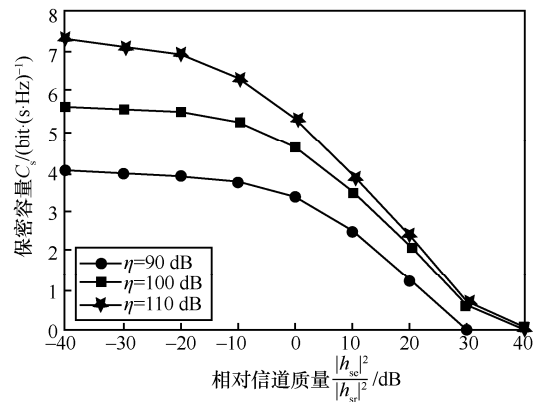


图 5 主信道质量对系统保密容量的影响

由图 4 和图 5 可知，当窃听信道质量增强时，通信系统将需要更大的功率来发送协同干扰，以进一步降低窃听节点处的信干噪比。特别地，当窃听信道远弱于合法信道时，系统不发送协同干扰也具有很好的保密容量；当其强于合法信道时，协同干扰发射机应全功率发送协同干扰；但当其远强于合法信道时，如  $\eta < 90$  dB、 $\frac{|h_{sc}|^2}{|h_{sr}|^2} > 20$  dB 时，通信发送机和协同干扰机均应停止工作，因为此时的保密容量恒为非正值。而且随着窃听信道的增强，系统的保密容量会降低，即使增大协同干扰的发射功率也无法改变保密容量下降的趋势。

### 5 结束语

本文研究了不完美时间同步下协同干扰功率

的分配问题，提出了一种可以使通信系统保密容量最大化的功率分配方法，给出了精确的闭式解，并分析了最佳协同干扰功率与相对信道质量之间的关系。仿真结果表明，同步误差对保密容量和总功耗有影响，并验证了所提出的功率分配方案优于未考虑时间不完美同步的功率分配方案。本文的研究成果对下一代无线通信系统的安全传输具有一定的参考意义。

### 参考文献：

- [1] 钟州, 张波, 戚晓慧, 等. 多天线全双工中继辅助的异构蜂窝网物理层安全性能分析[J]. 通信学报, 2019, 40(5): 24-31.  
ZHONG Z, ZHANG B, QI X H, et al. Physical layer security performance analysis of multi-antenna full-duplex relay aided heterogeneous cellular network[J]. Journal on Communications, 2019, 40(5): 24-31.
- [2] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8):1355-1387.
- [3] 张丽娟, 刘志宏, 张洪波, 等. 协作干扰下的无线安全增强[J]. 通信学报, 2017, 38(2):183-195.  
ZHANG L J, LIU Z H, ZHANG H B, et al. Wireless secure enhancement with cooperative jamming[J]. Journal on Communications, 2017, 38(2):183-195.
- [4] HONGLIANG H, QINGHE D, PINYI R, et al. Joint feedback and artificial noise design for secure communications over fading channels without eavesdropper's CSI[J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 11414-11418.
- [5] CHAKRABORTY P, PRAKRIYA S. Secrecy performance of an idle receiver assisted underlay secondary network[J]. IEEE Transactions on Vehicular Technology, 2017, 66(10):9555-9560.
- [6] ANJOS G, CASTANHEIRA D, SILVA A, et al. Exploiting reciprocal channel estimations for jamming to secure wireless communications[C]// 2017 Wireless Days. IEEE, 2017: 136-142.
- [7] CHOI Y, LEE J H. Power allocation for cooperative jamming in amplify-and-forward relaying network with eavesdropper[C]// 2015 IEEE 81st Vehicular Technology Conference. IEEE, 2015: 1-5.
- [8] KUHESTANI A, MOHAMMADI A, MOHAMMADI M. Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(2):341-355.
- [9] HE B, NI Q, CHEN J, et al. User-pair selection in multiuser cooperative networks with an untrusted relay[J]. IEEE Transactions on Vehicular Technology, 2019, 68(1):869-882.
- [10] LEE J H. Full-duplex relay for enhancing physical layer security in multi-hop relaying systems[J]. IEEE Communications Letters, 2015, 19(4):525-528.
- [11] ZHANG M, LIU Y, ZHANG R. Artificial noise aided secrecy information and power transfer in OFDMA systems[J]. IEEE Transactions on Wireless Communications, 2016, 15(4):3085-3096.
- [12] 王伟, 李鑫睿, 殷柳国, 等. 联合能量收集中继与全双工目的节点的安全资源分配方案[J]. 通信学报, 2019, 40(1):114-122.  
WANG W, LI X R, YIN L G, et al. Secure resource allocation in hybrid energy-harvesting relay and full-duplex receiver[J]. Journal on Communications, 2019, 40(1):114-122.
- [13] SHEIKHOLESAMI A, GOECKEL D, PISHRO-NIK H. Jamming based on an ephemeral key to obtain everlasting security in wireless environments[J]. IEEE Transactions on Wireless Communications, 2015, 14(11):6072-6081.
- [14] SICHITIU M L, VEERARITTIPHAN C. Simple, accurate time synchronization for wireless sensor networks[C]// Wireless Communications & Networking. IEEE, 2003: 1266-1273.
- [15] DONG L, HAN Z, PETROPULU A P, et al. Cooperative jamming for wireless physical layer security[C]// IEEE/SP Workshop on Statistical Signal Processing. IEEE, 2009: 417-420.
- [16] PARK K H, WANG T, ALOUINI M S. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9):1741-1750.
- [17] ZHENG G, CHOO L C, WONG K K. Optimal cooperative jamming to enhance physical layer security using relays[J]. IEEE Transactions on Signal Processing, 2011, 59(3):1317-1322.

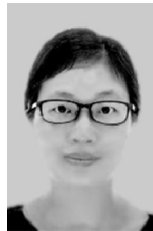
### [作者简介]



郭文博（1994-），男，四川南充人，电子科技大学博士生，主要研究方向为协同干扰抑制、物理层安全和全双工通信等。



宋长庆（1996-），男，江苏徐州人，电子科技大学硕士生，主要研究方向为无线通信信号处理、全双工通信自干扰抑制技术等。



文荣（1987-），女，广西桂林人，成都工业学院助教，主要研究方向为多天线信号处理、通信抗干扰技术。

赵宏志（1978-），男，河北石家庄人，博士，电子科技大学教授、博士生导师，主要研究方向为无线通信信号处理、通信抗干扰技术、同时同频全双工技术、并行化通信信号处理等。

唐友喜（1964-），男，河南潢川人，博士，电子科技大学教授、博士生导师，主要研究方向为无线通信抗干扰技术、同时同频全双工技术、高效固态射频功率放大器技术以及软件无线电技术等。