中国科学: 信息科学 2023 年 第 53 卷 第 3 期: 550–565
SCIENTIA SINICA Informationis
论文

人工噪声掩护下跳频安全通信

宋长庆, 张译丹, 赵宏志*, 邵士海*

电子科技大学通信抗干扰技术国家级重点实验室, 成都 611731
* 通信作者. E-mail: lyn@uestc.edu.cn, ssh@uestc.edu.cn

收稿日期: 2021–10–12; 修回日期: 2021–12–22; 接受日期: 2022–02–17; 网络出版日期: 2023–03–13

国家重点研发计划基金 (批准号: 2018YFB1801903) 和国家自然科学基金 (批准号: U19B2014, 62071094, 61901396) 资助项目

摘要 为了对抗电磁干扰与敌方窃听, 提出了人工噪声掩护下的跳频通信架构. 其中, 人工噪声对消是提升系统安全的关键步骤, 但实际接收节点处的时间同步误差会降低人工噪声对消效果与系统保密性能. 鉴于此, 分析了同步误差下人工噪声对消后的残余人工噪声成分和系统保密性能, 并提出了具有同步误差鲁棒性的人工噪声最优功率分配方法. 理论分析和仿真结果表明, 时间同步误差会在人工噪声对消时引入符号间干扰与跳间干扰, 进而降低系统的保密性能. 此外, 当接收节点可以实现完美时间同步时, 人工噪声与通信信号应等功率发射. 随着时间同步误差的增加, 人工噪声与通信信号的功率比应当逐渐减小, 以降低时间同步误差引起的保密性能损失.

关键词 人工噪声, 跳频, 时间同步误差, 噪声对消, 功率分配

1 引言

由于无线信道的开放特性, 无线通信信号容易遭受电磁干扰与敌方窃听 [1,2], 使得收发节点间通信的安全性受到了愈加广泛的关注 [3,4]. 在对抗电磁干扰方面, 跳频技术可以通过改变载波频率躲避电磁干扰 [5], 但在强窃听场景中, 部分窃听节点可以精准地估计出跳频图案、速率、带宽等信息, 进而能够窃听到通信信息 [6,7], 即跳频通信存在被窃听的风险. 在对抗敌方窃听方面, 人工噪声技术可以有效地降低窃听节点的接收信干噪比性能, 进而降低窃听信道质量、保护己方通信信号免受敌方窃听 [8]. 但人工噪声不具备干扰躲避能力, 当遭受电磁攻击时己方通信会被恶意阻塞, 影响收发双方的正常通信 [9,10].

当同时存在电磁干扰与敌方窃听时, 为了保证无线通信的安全性, 本文提出了人工噪声掩护下的跳频通信架构. 其中, 发射节点同时发送人工噪声和通信信号以阻塞敌方窃听, 同时收发节点均采用跳频技术躲避电磁干扰. 理想情况下, 授权接收节点可以利用先验信息将接收到的人工噪声信号抑制

引用格式: 宋长庆, 张译丹, 赵宏志, 等. 人工噪声掩护下跳频安全通信. 中国科学: 信息科学, 2023, 53: 550–565, doi: 10.1360/SSI-2021-0347
Song C Q, Zhang Y D, Zhao H Z, et al. Artificial noise shielded frequency hopping secure communication (in Chinese). Sci Sin Inform, 2023, 53: 550–565, doi: 10.1360/SSI-2021-0347

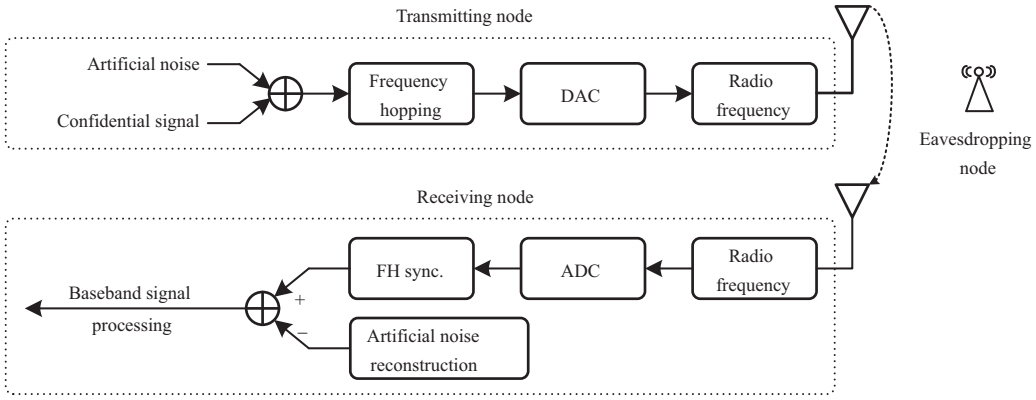

图 1 人工噪声掩护下跳频安全通信架构

Figure 1 Transceiver architecture of artificial noise shielded frequency-hopping communication

到底噪水平, 进而提取出通信信号. 但实际收发节点之间存在时间同步误差 [11], 会降低系统的人工噪声对消效果和保密性能 [12].

针对上述问题, 本文基于所提的安全通信架构, 度量并分析了时间同步误差对人工噪声对消效果和保密性能的影响, 并提出了具有时间同步误差鲁棒性的人工噪声最优功率分配方案. 本文的主要贡献总结如下.

(1) 提出了人工噪声掩护下的跳频通信架构. 该架构中收发节点采用跳频技术躲避电磁干扰, 并采用人工噪声技术降低窃听节点的信干噪比性能, 进而降低窃听信道质量、阻塞敌方窃听.

(2) 度量并分析了时间同步误差对所提系统性能的影响. 研究发现, 时间同步误差会在人工噪声对消操作中同时引入符号间干扰与跳间干扰, 进而降低系统的保密性能.

(3) 提出了具有时间同步误差鲁棒性的人工噪声最优功率分配方案, 根据收发节点的信号处理能力与信道传播特性优化了人工噪声和通信信号的发射功率, 进而降低同步误差带来的保密性能损失. 研究发现, 随着时间同步误差的增大, 人工噪声与通信信号的功率比应逐渐减小, 以降低同步误差引起的保密性能损失. 特别地, 当接收节点可以实现完美时间同步时, 人工噪声与通信信号应等功率发射.

本文其余部分安排如下: 第 2 节给出人工噪声掩护下的跳频通信架构; 第 3 节分析了时间同步误差下的系统保密性能; 第 4 节提出了具有时间同步误差鲁棒性的人工噪声最优功率分配方案; 第 5 节对理论分析结果进行了数值仿真; 第 6 节对全文进行总结.

2 系统模型

人工噪声掩护下的跳频通信架构如图 1 所示. 收发节点间的通信采用了跳频技术, 通过不断跳变发射载波频率躲避电磁干扰. 但在强窃听场景中, 部分窃听节点可以精准地估计出跳频图案、速率、带宽等信息, 进而能够窃听到通信信息 [6,7], 即跳频通信存在被窃听的风险. 因此, 发射节点在发送通信信号时掺入人工噪声, 进而降低窃听节点处的信干噪比性能, 阻塞非法窃听. 假设发射信号在传播过程中经历了平坦慢衰落. 在接收端, 授权接收节点依次执行跳频同步、人工噪声重构与对消操作, 分别移除频率跳变和人工噪声的影响, 然后执行基带信号处理等操作.

2.1 发射节点

在发射节点处, 通信信号与人工噪声的和信号依次经过跳频调制、模数转换、射频调制后发射,

第 k 跳发射信号可以表示为

$$\tilde{x}(t) = [s(t) + c(t)]\,\mathrm{e}^{\mathrm{j}[2\pi(f_c+f_k)t+\varphi_0]} g\left(t - kT\right), \tag{1}$$

其中, $s(t)$ 与 $c(t)$ 分别表示通信信号与人工噪声成分, f_c 表示载波频率, f_k 表示第 k 跳信号的跳频频率, φ_0 表示信号的初始相位, $T = N \cdot T_b$ 表示跳频周期, T_b 表示每比特信息的持续时间, N 表示每跳信号所包含的比特数, $g(t)$ 表示每跳信号的持续时间且满足

$$g(t) = \begin{cases} 1, & 0 < t \leqslant T, \\ 0, & \text{其他}. \end{cases} \tag{2}$$

收发节点处人工噪声的产生与工作机制如下 [13,14]. 发射节点与接收节点预先存储大量的随机干扰序列集, 并且收发节点的干扰序列信息一致. 这些序列服从零均值高斯分布, 且干扰序列在序列集中的索引值用作收发节点的通信密钥. 通信过程中, 发射节点利用信道独立与互易性等机密方式 [14~16] 将密钥发送给授权接收节点, 从而保证收发双方采用了同一组干扰序列.

2.2 窃听节点

在窃听节点处, 接收到的射频信号可以表示为

$$\tilde{e}(t) = \tilde{h}_e\,[s(t-\tau_e) + c(t-\tau_e)]\,\mathrm{e}^{\mathrm{j}2\pi(f_c+f_k+f_e)t} g\left(t - \tau_e - kN\right) + \tilde{w}_e(t), \tag{3}$$

其中, $\tilde{h}_e$ 表示复信道衰落, τ_e 表示发射节点与窃听节点间的传播时延, f_e 表示频率偏移, $\tilde{w}_e(t)$ 表示窃听节点处的高斯白噪声.

考虑强窃听情形, 即窃听节点可以准确地估计出跳频参数, 进而可以将接收信号解跳到基带. 此时, 窃听节点处的基带接收信号可以表示为

$$\begin{aligned} e[n] &= \mathcal{LPF}\{\tilde{e}[n] m^*[n - \hat{D}_e] \mathrm{e}^{-\mathrm{j}(2\pi f_c n T_b + \varphi_p)}\} \\ &= e_s[n] + e_c[n] + w_e[n], \end{aligned} \tag{4}$$

其中, $\mathcal{LPF}\{\cdot\}$ 表示低通滤波操作, $\tilde{e}[n]$ 表示 $\tilde{e}(t)$ 的离散形式, $m[n] = \mathrm{e}^{\mathrm{j}2\pi f_k n T_b} g[n - kN]$ 表示本地跳频载波信号, $(\cdot)^*$ 表示共轭操作, $\hat{D}_e$ 表示归一化后的传播时延估计值, $g[n-kN]$ 表示 $g(t-kT)$ 的离散形式, φ_p 表示本地射频载波的初始相位. 此外, $w_e[n]$ 表示高斯白噪声成分, $e_s[n]$ 和 $e_c[n]$ 分别表示通信信号和人工噪声成分, 且满足

$$e_s[n] = h_e s[n - D_e] \mathrm{e}^{\mathrm{j}2\pi f_e n T_b} g_e[n], \tag{5}$$

$$e_c[n] = h_e c[n - D_e] \mathrm{e}^{\mathrm{j}2\pi f_e n T_b} g_e[n], \tag{6}$$

其中, h_e 表示窃听节点处的等效信道增益, $g_e[n]$ 是 $g_e(t)$ 的离散形式. $g_e(t)$ 在 $t \in H_e$ 时取值为 1, 否则为 0, 且 H_e 满足

$$H_e = \begin{cases} \left(\hat{\tau}_e + kT, \tau_e + (k+1)T\right], & \hat{\tau}_e > \tau_e, \\ \left(\tau_e + kT, \hat{\tau}_e + (k+1)T\right], & \hat{\tau}_e \leqslant \tau_e, \end{cases} \tag{7}$$

其中 $\hat{\tau}_e = \hat{D}_e T_b$ 表示窃听节点处的传播时延估计值. 从式 (4) 可以看出, 即使窃听节点可以解除接收信号的频率跳变特性, 解跳后得到的基带接收信号中仍掺杂着人工噪声成分. 因此在强窃听场景中, 即当窃听节点可以获得跳频参数信息时, 窃听节点仍无法窃听到通信信息.

2.3 授权接收节点

在授权接收节点处, 首先执行跳频同步操作将接收的跳频信号变到基带. 接着执行人工噪声的重构与对消操作, 消除基带接收信号中的人工噪声分量.

2.3.1 跳频同步

与式 (4) 类似, 授权接收节点执行跳频同步操作后, 所得到的基带接收信号可以表示为

$$r[n] = r_s[n] + r_c[n] + w_r[n], \tag{8}$$

其中,

$$r_s[n] = h_r s[n - D_r]\mathrm{e}^{\mathrm{j}2\pi f_r n T_b} g_{r_1}[n], \tag{9}$$

$$r_c[n] = h_r c[n - D_r]\mathrm{e}^{\mathrm{j}2\pi f_r n T_b} g_{r_1}[n], \tag{10}$$

和 $w_r[n]$ 分别表示授权接收节点处的通信信号、人工噪声和高斯白噪声分量. h_r 表示等效信道增益, $D_r = \tau_r/T_b$ 表示归一化后的传播时延值, τ_r 表示传播时延, $g_{r_1}[n]$ 是 $g_{r_1}(t)$ 的离散形式. $g_{r_1}(t)$ 在 $t \in H_{r_1}$ 时取值为 1, 否则为 0, 且 H_{r_1} 满足

$$H_{r_1} = \begin{cases} (\hat{\tau}_r + kT, \tau_r + (k+1)T], & \hat{\tau}_r > \tau_r, \\ (\tau_r + kT, \hat{\tau}_r + (k+1)T], & \hat{\tau}_r \leqslant \tau_r, \end{cases} \tag{11}$$

其中, $\hat{\tau}_r$ 表示授权接收节点处的传播时延估计值.

2.3.2 人工噪声重构与对消

人工噪声重构与对消主要包含 3 个步骤 [17,18]. (1) 接收节点从本地干扰序列集中选取与发射节点一致的人工噪声序列, 并利用接收信号与本地人工噪声序列信息估计出人工噪声传播信道参数, 参数包括信道衰减、时间延迟、频率偏移; (2) 将估计出的信道信息补偿给本地人工噪声序列, 完成人工噪声重构; (3) 将接收信号减去本地重构的人工噪声, 完成人工噪声对消.

为了分离出时间同步误差对系统性能的影响, 本文假设授权接收节点处可以完美地估计出频率偏移和信道增益 [12,19]. 利用所得的参数估计值进行人工噪声重构, 重构后所得信号可以表示为

$$\begin{aligned} \hat{r}_c[n] &= h_r c[n - \hat{D}_r]\mathrm{e}^{\mathrm{j}2\pi f_r n T_b} g[n - \hat{D}_r - kN] \\ &= h_r c[n - \hat{D}_r]\mathrm{e}^{\mathrm{j}2\pi f_r n T_b}(g_{r_1}[n] + g_{r_2}[n]), \end{aligned} \tag{12}$$

其中, $\hat{D}_r = \hat{\tau}_r/T_b$ 表示归一化后的时延估计值, $g_{r_2}[n]$ 是 $g_{r_2}(t)$ 的离散形式. $g_{r_2}(t)$ 在 $t \in H_{r_2}$ 时取值为 1, 否则为 0, 且 H_{r_2} 满足

$$H_{r_2} = \begin{cases} (\tau_r + (k+1)\,T, \hat{\tau}_r + (k+1)\,T], & \hat{\tau}_r > \tau_r, \\ (\hat{\tau}_r + kT, \tau_r + kT], & \hat{\tau}_r \leqslant \tau_r. \end{cases} \tag{13}$$

接着, 将基带接收信号 $r[n]$ 与人工噪声重构信号 $\hat{r}_c[n]$ 相减, 进而抑制授权接收节点处的人工噪声分量. 对消操作后残余的人工噪声分量可以表示为

$$\Delta r[n] = r[n] - \hat{r}_c[n] = r_s[n] + \Delta r_c[n] + w_r[n], \tag{14}$$

其中 $\Delta r_c[n] = r_c[n] - \hat{r}_c[n]$ 表示对消操作后残余的人工噪声分量. 可以发现, 时间同步误差会引入残余的人工噪声分量 $\Delta r_c[n]$, 进而造成系统性能损失. 在接下来的部分, 我们将进一步地分析时间同步误差对系统性能的影响, 并提出相应的解决方案.

3 性能分析

时间同步误差会在人工噪声对消时引入残余人工噪声, 进而降低系统性能. 鉴于此, 本节首先分析了时间同步误差引起的残余人工噪声成分, 并在此基础上衡量了同步误差下系统的保密性能.

3.1 残余人工噪声成分分析

窃听节点无法执行人工噪声对消操作, 因此本部分仅分析授权接收节点处的人工噪声对消性能. 考虑到可以将 $c[n-D_r]$ 看作 $c[n-\hat{D}_r]$ 的延迟重复 [12], 我们有

$$c[n-D_r] = c[n-\hat{D}_r+\Delta D_r] = c[n-\hat{D}_r]\mathrm{sinc}[\Delta D_r] + c_{\Delta D_r}[n], \tag{15}$$

其中, $\Delta D_r = \hat{D}_r - D_r$ 表示归一化时间同步误差, $c_{\Delta D_r}[n] = \sum_{i=-\infty, i\neq 0}^{+\infty} (c[n-\hat{D}_r-i]\mathrm{sinc}[i+\Delta D_r])$. 用符号 $\mathcal{P}\{\cdot\}$ 表示求功率操作, 则 $c[n-\hat{D}_r]$ 和 $c_{\Delta D_r}[n]$ 的功率可以表示为

$$\mathcal{P}\{c[n-\hat{D}_r]\} = \mathcal{P}\left\{c[n-D_r]\right\} = P_c, \tag{16}$$

$$\mathcal{P}\left\{c_{\Delta D_r}[n]\right\} = \left(1-\mathrm{sinc}^2\left[\Delta D_r\right]\right)P_c. \tag{17}$$

在人工噪声对消操作中, 时间同步误差一方面会引起接收信号与本地重构的人工噪声符号间的时间不对齐, 进而引入符号间干扰 [12]; 另一方面会引起接收信号与重构人工噪声之间的频率不对齐, 进而引入跳间干扰. 因此对消操作后残余的人工噪声可以分为符号间干扰 $\Delta r_{\mathrm{ISI}}[n]$ 和跳间干扰 $\Delta r_{\mathrm{IHI}}[n]$ 两部分, 即

$$\Delta r_c[n] = r_c[n] - \hat{r}_c[n] = \Delta r_{\mathrm{ISI}}[n] + \Delta r_{\mathrm{IHI}}[n], \tag{18}$$

其中, $\Delta r_{\mathrm{ISI}}[n]$ 与 $\Delta r_{\mathrm{IHI}}[n]$ 互不相关, 且满足

$$\Delta r_{\mathrm{ISI}}[n] = h_r\left(\mathrm{sinc}[\Delta D_r]-1\right)c[n-\hat{D}_r]\mathrm{e}^{\mathrm{j}2\pi f_r n T_b}g_{r_1}[n] + h_r c_{\Delta D_r}[n]\mathrm{e}^{\mathrm{j}2\pi f_r n T_b}g_{r_1}[n], \tag{19}$$

$$\Delta r_{\mathrm{IHI}}[n] = -h_r c[n-\hat{D}_r]\mathrm{e}^{\mathrm{j}2\pi n f_r n T_b}g_{r_2}[n], \tag{20}$$

并且两者的功率可以表示为

$$\mathcal{P}\left\{\Delta r_{\mathrm{ISI}}[n]\right\} = |h_r|^2 P_c\left(2-2\mathrm{sinc}[\Delta D_r]\right)\frac{N-|\Delta D_r|}{N}, \tag{21}$$

$$\mathcal{P}\left\{\Delta r_{\mathrm{IHI}}[n]\right\} = |h_r|^2 P_c\frac{|\Delta D_r|}{N}. \tag{22}$$

由式 (19) 和 (20) 可知, 符号间干扰与跳间干扰均可以由人工噪声信号经过线性变换得到. 已知人工噪声服从高斯分布, 可得残余人工噪声 $\Delta r_c[n]$ 也服从高斯分布 [20]. 记符号间干扰与跳间干扰的功率比为 Γ, 我们可以得到下述结论.

命题1 在人工噪声掩护下的跳频通信系统中, 时间同步误差会在人工噪声对消时引入残余人工噪声, 且残余人工噪声中各成分间的功率关系可以由 Γ 衡量. 其中 Γ 定义为符号间干扰与跳间干扰的功率比, 且满足

$$\Gamma \triangleq \frac{\mathcal{P}\left\{\Delta r_{\mathrm{ISI}}[n]\right\}}{\mathcal{P}\left\{\Delta r_{\mathrm{IHI}}[n]\right\}} = \frac{2-2\mathrm{sinc}[\Delta D_r]}{|\Delta D_r|}(N-|\Delta D_r|). \tag{23}$$

由式 (23) 可知, Γ 是关于同步误差 ΔD_r 的偶函数, 且当 $|\Delta D_r|$ 趋于 0 时 Γ 收敛到 0. 这表明当授权接收节点处的时间同步误差相对较小时, 符号间干扰的功率与跳间干扰的功率相比可以忽略不计. 相似地, $N=|\Delta D_r|$ 也是 Γ 的一个零点, 即

$$\lim_{|\Delta D_r|\to N}\Gamma=\lim_{|\Delta D_r|\to 0}\Gamma=0, \tag{24}$$

表明当 $N=|\Delta D_r|$ 时, 残余人工噪声中只包含跳间干扰分量.

3.2 保密性能

在残余人工噪声成分分析的基础上, 本小节先给出了授权接收节点和窃听节点处的信干噪比, 然后衡量了时间同步误差下系统的保密性能.

窃听节点处的信干噪比可以表示为

$$\gamma_e=\frac{|h_e|^2P_s\frac{N-|\Delta D_e|}{N}}{|h_e|^2P_c\frac{N-|\Delta D_e|}{N}+w_e[n]}=\frac{|h_e|^2\eta_e(N-|\Delta D_e|)}{|h_e|^2\alpha\eta_e(N-|\Delta D_e|)+N(\alpha+1)}, \tag{25}$$

其中, $\eta_e=\frac{P}{\mathcal{P}\{\tilde{w}_e(t)\}}$ 表示窃听节点处的归一化功率预算.

授权接收节点处的信干噪比可以表示为

$$\begin{aligned}\gamma_r&=\frac{|h_r|^2P_s\frac{N-|\Delta D_r|}{N}}{|h_r|^2P_c\left(2-2\mathrm{sinc}[\Delta D_r]\right)\frac{N-|\Delta D_r|}{N}+|h_r|^2P_c\frac{|\Delta D_r|}{N}+\mathcal{P}\{w_r[n]\}}\\&=\frac{|h_r|^2\eta_r(N-|\Delta D_r|)}{|h_r|^2\alpha\eta_r\left(2-2\mathrm{sinc}[\Delta D_r]\right)(N-|\Delta D_r|)+|h_r|^2\alpha\eta_r|\Delta D_r|+N(\alpha+1)},\end{aligned} \tag{26}$$

其中, $\eta_r=\frac{P}{\mathcal{P}\{w_r[n]\}}$ 表示授权节点处的归一化功率预算.

命题2 在人工噪声掩护下的跳频安全通信中, 系统的保密性能可以用保密容量来衡量 [21, 22]. 当存在时间同步误差时, 其表达式为

$$C_s\triangleq\begin{cases}\frac{1}{2}\log_2\left(1+\gamma_r\right)-\frac{1}{2}\log_2\left(1+\gamma_e\right), & \gamma_r\geqslant\gamma_e,\\ 0, & \gamma_r<\gamma_e.\end{cases} \tag{27}$$

当窃听节点与授权接收节点均可以实现完美时间同步, 即 $\Delta D_r=\Delta D_e=0$ 时, 相应的系统保密容量可以表示为

$$C_{s\max}=\max\left\{\frac{1}{2}\log_2\frac{\left(|h_r|^2\eta_r+\alpha+1\right)\left(|h_e|^2\alpha\eta_e+\alpha+1\right)}{\left(|h_e|^2\eta_e+1\right)(\alpha+1)^2},0\right\}. \tag{28}$$

可以发现, $C_{s\max}$ 是仅关于相对信道质量和功率分配因子的函数, 与跳频周期的取值无关.

当窃听节点与授权接收节点处的时间同步性能较差, 即 $\min\{\Delta D_r,\Delta D_e\}\gg 0$ 时, 相应的系统保密容量可以表示为

$$\begin{aligned}C_{s\min}&=\left\{\frac{1}{2}\log_2\frac{|h_r|^2\eta_r\left(N-\Delta D_r\right)(\alpha+1)+N\left(|h_r|^2\alpha\eta_r+\alpha+1\right)}{\left[|h_r|^2\alpha\eta_r\left(2N-\Delta D_r\right)+N\left(\alpha+1\right)\right]\left(1+\gamma_e\right)},0\right\}\\&\overset{\text{(a)}}{\approx}\left\{\frac{1}{2}\log_2\frac{\left[|h_r|^2\eta_r\left(2\alpha+1\right)+\alpha+1\right]\left(|h_e|^2\alpha\eta_e+\alpha+1\right)}{\left[2|h_r|^2\alpha\eta_r+\alpha+1\right]\left(|h_e|^2\eta_e+1\right)(\alpha+1)},0\right\},\end{aligned} \tag{29}$$

其中近似 (a) 成立的条件为 $N\gg\max\{\Delta D_r,\Delta D_e\}$. 可以发现 $C_{s\min}$ 是关于相对信道质量、跳频周期和功率分配因子的函数, 且当 $N\gg\max\{\Delta D_r,\Delta D_e\}$ 时, 跳频周期对保密容量 $C_{s\min}$ 的影响可以忽略.

4 人工噪声最优功率分配及简化方案

本节首先给出了具有时间同步误差鲁棒性的人工噪声最优功率分配方案. 该方案以最大化系统保密容量为目标, 根据收发节点的信号处理能力和信道传播特性优化人工噪声与通信信号的发射功率, 进而降低时间同步误差带来的系统保密性能损失. 接着, 考虑到各系统中具有不同的时间同步性能和相对信道质量, 我们对最优功率分配方案进行了简化.

4.1 人工噪声最优功率分配方案

在发射节点处, 最优功率分配方案的准则是通过调整人工噪声与通信信号的功率分配因子使得系统保密容量最大化, 即

$$\begin{aligned}&\max_{\alpha} C_s = \frac{1}{2}\log_2\left(1+\gamma_r\right) - \frac{1}{2}\log_2\left(1+\gamma_e\right)\\ &\text{s.t.}\begin{cases}\gamma_r \geqslant \gamma_e,\\ \alpha \geqslant 0\,.\end{cases}\end{aligned} \tag{30}$$

命题3 在人工噪声掩护下的跳频通信系统中, 当存在时间同步误差时人工噪声和通信信号的最优发射功率分配方案为

$$\alpha^* = \begin{cases}\alpha_1, \text{ 当 } aN+bc > bN+ab \text{ 且 } aN+bc > cN+ac,\\ 0, \text{ 当 } aN+bc \leqslant bN+ab \text{ 且 } b \geqslant c,\\ \phi, \text{ 当 } aN+bc \leqslant cN+ac \text{ 且 } b < c,\end{cases} \tag{31}$$

其中 α^* 表示人工噪声与通信信号的最优发射功率分配因子, $\alpha^*=0$ 表示发射节点只发送通信信号而不发送人工噪声, $\alpha^*=\phi$ 表示发射节点应停止发送任何信号, 因为此时系统的保密容量恒为负. 此外, 式 (31) 中 α_1 的表达式为

$$\alpha_1 = \frac{aN\left(b-c\right) - \sqrt{aN\left(a-b\right)\left(a-c\right)\left(b-N\right)\left(c-N\right)}}{a\left(ac+cN-bc-aN\right)}, \tag{32}$$

并且 $\{a,b,c\}$ 满足

$$\begin{cases}a = |h_r|^2\eta_r\left\{\left[2-2\mathrm{sinc}\left(\Delta D_r\right)\right]\left(N-|\Delta D_r|\right)+|\Delta D_r|\right\}+N,\\ b = |h_r|^2\eta_r\left(N-|\Delta D_r|\right)+N,\\ c = |h_e|^2\eta_e\left(N-|\Delta D_e|\right)+N.\end{cases} \tag{33}$$

当 $\alpha=\alpha^*$ 时系统保密容量取得最大值 C_s^*, 其可以表示为

$$C_s^* = \frac{1}{2}\log_2\left[\frac{\left(a\alpha^*+b\right)\left(c\alpha^*+N\right)}{\left(a\alpha^*+N\right)\left(c\alpha^*+c\right)}\right]. \tag{34}$$

证明 见附录 A.

为了衡量所提方案的计算复杂度, 表 1 给出了本文所提方案中使用的加法器与乘法器数量. 为了对比分析, 表 1 还给出了文献 [23] 中所提人工噪声功率分配方案的计算复杂度, 并在仿真部分给出了两种方案的性能对比. 为了简便而不失一般性, 平方根运算可以等效为 1 个复数乘法运算, 实数除法

表 1 计算复杂度

Table 1 Computational complexity

Power allocation scheme	Number of real adders	Number of real multipliers	Number of complex multipliers
Our scheme	20	26	1
Scheme in [23]	16	26	1

运算可以等效为一个实数乘法运算, 实数比较和实数减法运算均可以等效为一个实数加法运算 [24]. 此外, sinc(∗) 运算可以通过本地查表方式获得, 因此不消耗计算资源.

鉴于浮点运算数 (flops) 指标可以有效地衡量计算复杂度, 并且该指标不依赖于具体的实验平台 [25,26], 因此本文采用该指标来衡量算法的整体复杂度. 一个 flop 定义为两个浮点数间的一次加法、减法、乘法, 或者除法运算 [27], 并且一个复数乘法运算消耗 6 flops. 因此, 本文所提方案的计算复杂度为 52 flops, 文献 [23] 的计算复杂度为 48 flops, 可以发现两种方案的整体计算复杂度相当. 在仿真部分, 将给出两种方案的性能对比.

4.2 基于时间同步性能的人工噪声功率分配方案

不同的通信系统具有不同的时间同步性能. 鉴于此, 我们对最优功率分配方案进行了拓展, 可以得到如下结论.

4.2.1 完美时间同步

当授权接收节点和窃听节点可以完美地实现时间同步, 即 $\Delta D_r = \Delta D_e = 0$ 时, 根据式 (33) 可得 $a = N$, $b = |h_r|^2\eta_r N + N$, $c = |h_e|^2\eta_e N + N$. 将 $\{a, b, c\}$ 的值代入式 (32), 可以得到完美时间同步下系统的功率分配方案为

$$\alpha^* = \begin{cases} \dfrac{N^2 + bc - 2bN}{N^2 + bc - 2cN}, & \text{当 } N^2 + bc > 2bN \text{ 且 } N^2 + bc > 2cN, \\ 0, & \text{当 } N^2 + bc \leqslant 2bN \text{ 且 } b \geqslant c, \\ \phi, & \text{当 } N^2 + bc \leqslant 2cN \text{ 且 } b < c. \end{cases} \tag{35}$$

在完美时间同步情形下, b 和 c 一般满足

$$\begin{cases} b = |h_r|^2\eta_r N + N \gg 2N, \\ c = |h_e|^2\eta_e N + N \gg 2N, \end{cases} \tag{36}$$

可得 $N^2 + bc > 2bN$ 和 $N^2 + bc > 2cN$. 代入式 (35), 可得

$$\alpha^* = \frac{N^2 + bc - 2bN}{N^2 + bc - 2cN} \approx 1, \tag{37}$$

表明对于完美时间同步情形, 最优的功率分配方案通常为 $P_c \approx P_s$, 此时系统的最大保密容量为

$$C_s^* \approx \frac{1}{2}\log_2 \frac{(b+N)(c+N)}{4cN}. \tag{38}$$

值得注意的是, 式 (35) 也可以表示未考虑时间同步误差的功率分配方案. 与考虑同步误差的方案相比, 未考虑同步误差的功率分配方案对同步误差不具备鲁棒性. 在仿真部分, 我们将给出这两种方案的性能对比.

4.2.2 时间同步性能良好

当授权接收节点和窃听节点都具有良好的时间同步性能时, 此时假设系统的同步误差较小且满足 $a<\frac{c(b-N)}{c-N}$. 将 $N-|\Delta D_r|\approx N$ 与泰勒展开式 $\sin(x)\approx 1-\frac{\pi^2}{x^2}(|x|\ll 1)$ 代入式 (33), 可得

$$\begin{aligned} a &= |h_r|^2\eta_r\left\{\left[2-2\mathrm{sinc}\left(\Delta D_r\right)\right]\left(N-|\Delta D_r|\right)+|\Delta D_r|\right\}+N \\ &\approx \frac{\pi^2|h_r|^2\eta_r N\Delta D_r^2}{3}+|h_r|^2\eta_r|\Delta D_r|+N. \end{aligned} \tag{39}$$

此时 $a<\frac{c(b-N)}{c-N}$ 可以等效为 $a=|\Delta D_r|<\varepsilon$, 其中

$$\varepsilon\approx\sqrt{\frac{3(|h_rh_e|^2\eta_r\eta_e+|h_r|^2\eta_r-|h_e|^2\eta_e)}{\pi^2|h_rh_e|^2\eta_r\eta_e}+\frac{9}{4N^2\pi^4}}-\frac{3}{2N\pi^2}, \tag{40}$$

进而可得在时间同步性能良好的情形下, 系统的最优功率分配方案为

$$\alpha^*=\begin{cases}\alpha_1, & \text{当 } aN+bc>bN+ab,\\ 0, & \text{当 } aN+bc\leqslant bN+ab.\end{cases} \tag{41}$$

当系统的时间同步性能良好时, $\{a,b,c\}$ 一般满足 $\min\{b,c\}\gg a>N$, 进而有 $aN+bc>ab+bN$. 由式 (41) 可知, 此时 $\alpha^*=\alpha_1$.

4.2.3 时间同步性能较差

当系统的时间同步性能较差, 即 $|\Delta D_r|\geqslant\varepsilon$ 时, 式 (31) 中的最优功率分配方案可以简化为

$$\alpha^*=\begin{cases}\phi, & \text{当 } b<c,\\ 0, & \text{当 } b\geqslant c.\end{cases} \tag{42}$$

表明当时间同步误差较大但相对信道质量较好, 即 $|\Delta D_r|\geqslant\varepsilon$ 且 $b\geqslant c$ 时, 发射节点应当只发送通信信号; 当时间同步误差较大且相关信道质量较差, 即 $|\Delta D_r|\geqslant\varepsilon$ 且 $b<c$ 时, 发射节点应当停止发送人工噪声和通信信号以避免信息泄露, 因为此时系统的保密容量恒为零.

4.3 基于相对信道质量的人工噪声功率分配方案

不同的通信系统在不同的通信环境中具有不同的相对信道质量. 鉴于此, 我们对式 (31) 中的最优功率分配方案进一步拓展, 可得如下结论.

4.3.1 相关信道质量良好

当相对信道质量良好, 即 $b\geqslant c$ 时, 式 (31) 中的最优功率分配方案可以简化为

$$\alpha^*=\begin{cases}\alpha_1, & \text{当 } aN+bc>bN+ab,\\ 0, & \text{当 } aN+bc\leqslant bN+ab.\end{cases} \tag{43}$$

特别地, 当 $\alpha^*=0$ 时最大信道容量 C_s^* 满足

$$C_s^*|_{\alpha^*=0}=\frac{1}{2}\log_2\frac{b}{c}\geqslant 0 \quad \text{当 } b\geqslant c, \tag{44}$$

表明当系统的相对信道质量良好时, 本文提出的功率分配方案即使在不发送人工噪声时仍能够保证保密容量为非负值, 验证了方案的有效性.

4.3.2 相关信道质量较差

当相对信道质量较差, 即 $b<c$ 时, 式 (31) 中的最优功率分配方案可以简化为

$$\alpha^*=\begin{cases}\alpha_1, & \text{当 } aN+bc>cN+ac,\\ \phi, & \text{当 } aN+bc\leqslant cN+ac.\end{cases}\tag{45}$$

特别地, 当 $aN+bc>cN+ac$ 且二者取值相近时, α_1 满足

$$\lim_{(aN+bc)-(cN+ac)\to 0^+}\alpha_1=\begin{cases}-\dfrac{N}{a}, & \text{当 } b>c,\\ \sqrt{\dfrac{N}{a}}, & \text{当 } b=c,\\ +\infty, & \text{当 } b<c.\end{cases}\tag{46}$$

由于 $aN+bc>cN+ac$, 我们有 $a<\frac{c(b-N)}{c-N}$, 表明此时的时间同步性能良好. 当 $b>c$, 即 $aN+bc\approx cN+ac\leqslant bN+ab$ 时, 由式 (42) 可知此时最优功率分配因子为 $\alpha^*=0$. 当 $b\leqslant c$, 即 $aN+bc>bN+ab$ 时, 由式 (45) 可知此时最优功率分配因子为 $\alpha^*=\alpha_1$. 将上述结论带入式 (46), 可得

$$\lim_{(aN+bc)-(cN+ac)\to 0^+}\alpha^*=\begin{cases}0, & \text{当 } b>c,\\ \sqrt{\dfrac{N}{a}}, & \text{当 } b=c,\\ +\infty, & \text{当 } b<c.\end{cases}\tag{47}$$

5 仿真分析

5.1 仿真条件

基于图 1 所示的通信系统结构, 本节利用 MATLAB 工具进行了数值仿真验证, 仿真参数如表 2 所示. 本节包含两部分内容: 第 1 部分对人工噪声掩护下的跳频安全通信系统性能进行了仿真, 包含人工噪声对消后的残余人工噪声成分和系统保密性能; 第 2 部分对最优功率分配方案进行了数值仿真, 以验证其有效性. 在下述仿真中, 假设授权接收节点和窃听节点处的时间同步能力相当, 即 $\Delta D_r=\Delta D_e=\Delta D_{re}$.

5.2 时间同步误差下系统性能仿真

在授权接收节点处, 时间同步误差会引入残余人工噪声. 鉴于此, 图 2 分析了不同同步误差下残余人工噪声成分间的功率关系, 其中图 2(a) 仿真了符号间干扰与跳间干扰的功率比与时间同步误差的关系, 图 2(b) 仿真了两者的功率比与跳频周期的关系. 可以发现对于一个给定的跳频周期, 当同步误差远小于跳长, 即 $\Delta D_r\ll N$ 时, 符号间干扰与跳间干扰的功率比会随着同步误差的增加而增加; 当同步误差与跳频周期相近, 即 $\Delta D_r\approx N$ 时, 两者的功率比趋于零. 这一现象符合式 (24) 中的结论, 即 $\Delta D_r=N$ 是符号间干扰与跳间干扰功率比的零点, 且当 $\Delta D_r\approx N$ 时码间干扰的功率与跳间干扰的功率相比可以忽略不计. 另一方面, 对于一个给定的时间同步误差, 两者的功率比会随着跳频周期的增加而增加, 且当 N 趋于 $+\infty$ 时, 两者的功率比会随着跳频周期的增加而线性增大. 由此可知, 残余人工噪声中的符号间干扰与跳间干扰的功率比随着跳频周期的增加而增加, 且当 N 趋于 $+\infty$ 时, 跳间干扰的功率与码间干扰的功率相比可以忽略不计.

表 2　数值仿真参数设置

Table 2　Parameters of numerical simulations

Parameter	Value
Confidential signal type	BPSK signal
Artificial noise type	Gaussian signal with zero mean [23]
Frequency-hopping bandwidth	30 MHz
Baseband bandwidth	50 kHz
Hopping period	1∼1000 symbols
Cycle of the FH pattern	1000 hops
Radio frequency	2 GHz
Range of the power allocation factor	0∼1
Sampling interval	5 ns
Normalized time synchronization error	$10^{-6} \sim 10^{0}$
Thermal noise power at the eavesdropping node	−100 dBm
Thermal noise power at the authorized receiving node	−100 dBm

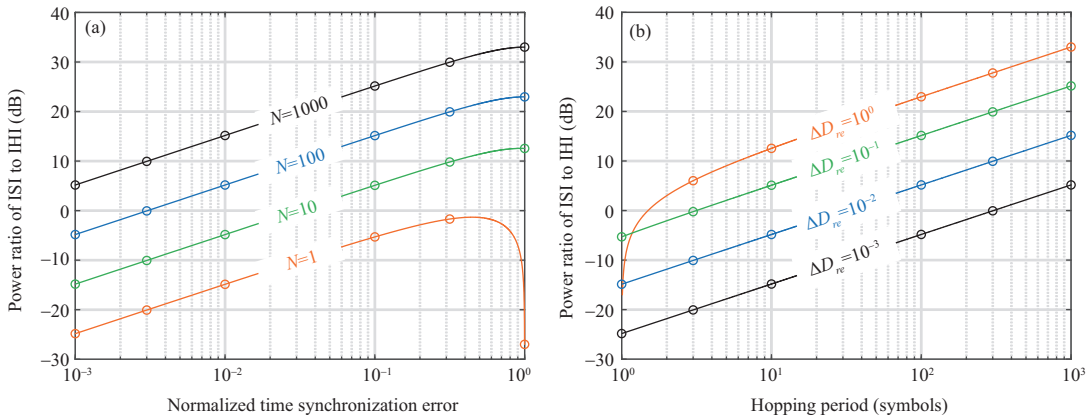

图 2　(网络版彩图) 残余人工噪声成分分析

Figure 2　(Color online) Component analysis of the residual artificial noise after cancellation. (a) The relationship between the power ratio of ISI to IHI and the time synchronization error; (b) the relationship between the power ratio of ISI to IHI and the hopping period

图 3 描绘了系统保密容量随时间同步误差的变化关系. 可以发现, 保密容量会随着同步误差的增加而降低, 表明时间同步误差会降低系统的保密性能. 当同步误差比较小时, 系统的保密容量近似等于式 (28) 中 C_{smax} 的值, 该值仅与相对信道质量和功率分配因子有关、而与跳频周期无关. 此外, 仿真曲线 ① 和 ③ 表明授权接收节点处的相对信道质量优势有利于提升系统的保密性能, 同时仿真曲线 ③-④-⑤ 表明在给定的仿真条件下, 系统保密容量会随着跳频周期的增加而增大. 进一步地, 由仿真曲线 ①-②-⑥ 可知不同的功率分配因子对应着不同的系统保密性能, 优化发射节点处的功率分配方案可以有效地提升系统的保密性能.

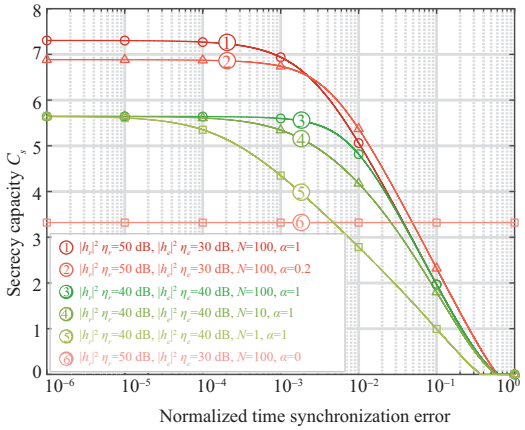

图 3　(网络版彩图) 保密容量随时间同步误差的变化趋势

Figure 3　(Color online) Variation tendency of the secrecy capacity under various time synchronization errors

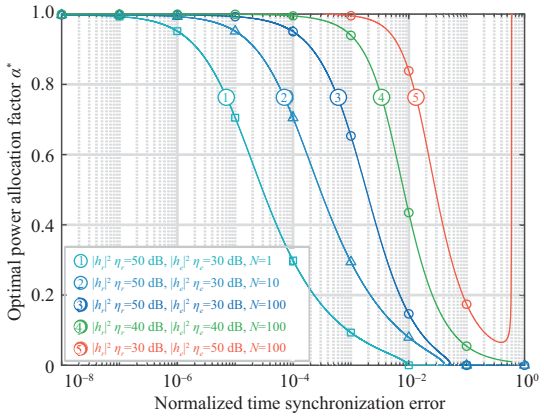

图 4　(网络版彩图) 最优功率分配因子随时间同步误差的变化趋势

Figure 4　(Color online) Variation tendency of the optimal power allocation factor under various time synchronization errors

5.3　人工噪声最优功率分配方案的性能仿真

图 4 展示了最优功率分配因子随时间同步误差的变化趋势. 可以发现, 最优功率分配因子随着同步误差的增大而逐渐减小, 表明人工噪声的发射功率应随着时间同步误差的增大而减小; 当同步误差趋于 0 时, 最优功率分配因子收敛到常数 1 附近, 表明完美时间同步时的最优功率分配方案为 $P_c = P_s$. 仿真曲线 ①-②-③ 表明功率分配因子应随着跳频周期的增加而增大, 并且仿真曲线 ③-④-⑤ 表明功率分配因子应随着相对信道质量的降低而增大. 此外, 曲线 ③, ④, ⑤ 分别仿真了 $b < c$, $b = c$ 和 $b > c$ 3 种不同的情况, 可以发现最优功率分配因子在 $aN + bc$ 趋于 $ac + cN$ 时分别收敛于 0, $\frac{1}{\sqrt{a}}$ 和 $+\infty$, 验证了式 (47) 中的结论. 还可以发现, 当同步误差较大时, 曲线 ①-②-③ 中最优功率分配因子的取值为 0, 曲线 ④ 和 ⑤ 中的最优功率分配因子的取值为 ϕ, 表明当时间同步误差较大而相对信道质量较好时, 发射节点应只发射通信信号, 利用相对信道质量优势即可保证保密容量恒为正值; 当时间同步误差较大并且相对信道质量较差时, 发射节点应停止发送人工噪声和通信信号, 以避免通信信号被敌方窃听.

图 5 绘制了最大保密容量随着时间同步误差的变化趋势. 可以发现, 随着时间同步误差的增加, 最大保密容量总体呈下降趋势, 表明时间同步误差会降低系统的最大保密容量性能. 当时间同步误差较小时, 最大保密容量的取值近似等于式 (28) 中 C_{smax} 的值, 该值仅与相对信道质量有关. 仿真曲线 ①-②-③ 表明优化相对信道质量可以有效地提升系统的保密性能, 并且仿真曲线 ③-④-⑤ 表明较长的跳频周期有利于增大系统的保密容量. 此外, 曲线 ⑤ 中包含了 3 组曲线, 分别仿真对比了本文提出的人工噪声最优发射功率分配方案, 文献 [23] 提出的人工噪声最优发射功率分配方案, 未考虑同步误差的功率分配

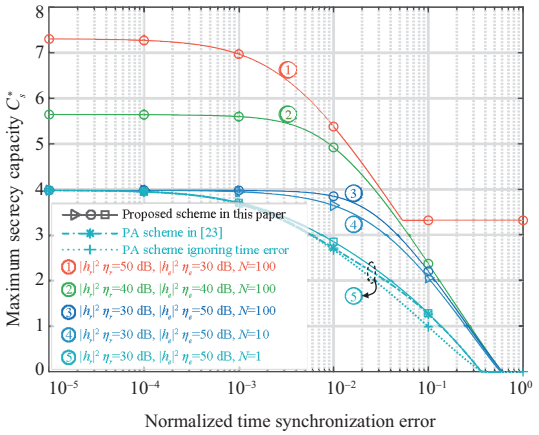

图 5 (网络版彩图) 最大保密容量随时间同步误差的变化趋势

Figure 5 (Color online) Variation tendency of the maximum secrecy capacity performance under various time synchronization errors

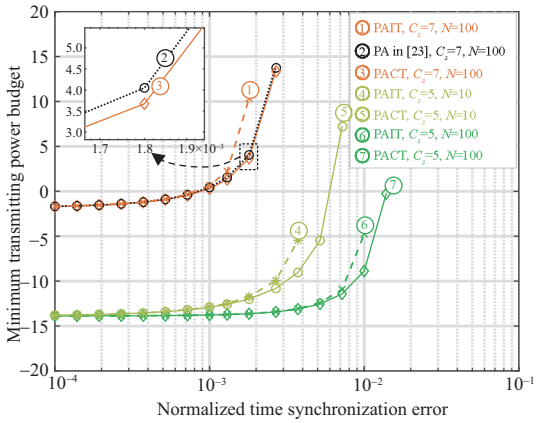

图 6 (网络版彩图) 给定保密容量下的最小发射功率预算与时间同步误差的关系

Figure 6 (Color online) Relationship between the time synchronization error and the minimum transmitting power budget under a given secrecy capacity

方案之间的性能. 曲线 ⑤ 仿真结果表明, 与其余两种人工噪声功率分配方案相比, 本文提出的方案具有明显的保密性能优势, 进而可以更好地对抗非法窃听.

在给定的保密容量下, 图 6 给出了最小发射功率预算与时间同步误差之间的关系, 其中授权接收节点与窃听节点处的噪声功率均为 -100 dBm, 且 $|h_r|^2 = -50$ dB, $|h_e|^2 = -60$ dB. 可以发现最小的发射功率预算会随着保密容量门限的增大而增大, 并且会随着时间同步误差的增加而增大. 当时间同步误差趋于 0 时, 最小发射功率预算收敛为常数, 该常数表示完美时间同步下的功率预算值. 仿真曲线 ①-③, ④-⑤, ⑥-⑦ 分别仿真对比了功率分配时是否考虑了时间同步误差对功率预算的影响. 可以发现, 与未考虑同步误差的功率分配方案相比, 本文提出的考虑时间同步误差的功率分配方案具有更低的功耗, 并且在给定的保密容量下本方案可以容忍更大的时间同步误差. 接着, 曲线 ②-③ 仿真对比了文献 [23] 所提方案与本文方案的能耗对比情况. 从图 6 的放大区域可以发现, 两种方案的能耗情况相当, 本文的人工噪声最优功率分配方案的能耗略低于文献 [23] 提出的方案. 此外, 仿真曲线 ④-⑥ 和 ⑤-⑦ 均表明在给定的保密容量门限下, 较长的跳频周期可以有效地降低发射功率预算.

6 结论

本文提出了人工噪声掩护下的跳频安全通信架构, 该架构可以有效地对抗电磁干扰与敌方窃听. 在此基础上, 建模并分析了时间同步误差下的系统性能, 发现时间同步误差会在人工噪声对消操作中引入符号间干扰与跳间干扰, 进而降低人工噪声对消效果和系统保密性能. 此外, 提出了具有同步误差鲁棒性的人工噪声最优功率分配方案. 当接收节

点可以实现完美时间同步时, 人工噪声与通信信号应等功率发射. 随着时间同步误差的增加, 人工噪声与通信信号之间的发射功率比应当逐渐减小, 以降低同步误差引起的保密性能损失.

参考文献

1 Wu F L, Wang W J, Wang H M, et al. A unified mathematical model for spatial acrambling based secure wireless communication and its wiretap method. Sci Sin Inform, 2012, 42: 483–492 [吴飞龙, 王文杰, 王慧明, 等. 基于空域加扰的保密无线通信统一数学模型及其窃密方法. 中国科学: 信息科学, 2012, 42: 483–492]

2 Xu J, Duan L J, Zhang R. Proactive eavesdropping via cognitive jamming in fading channels. IEEE Trans Wireless Commun, 2017, 16: 2790–2806

3 Huang K Z, Jin L, Chen Y J, et al. Development of wireless physical layer key generation technology and new challenges. J Electron J Electron Inf Technol, 2020, 42: 2330–2341 [黄开枝, 金梁, 陈亚军, 等. 无线物理层密钥生成技术发展及新的挑战. 电子与信息学报, 2020, 42: 2330–2341]

4 Yang Y Y, Zhou W, Zhao S R, et al. Survey of IoT security research: threats, detection and defense. J Commun, 2021, 42: 188–205 [杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述: 威胁、检测与防御. 通信学报, 2021, 42: 188–205]

5 Wang Y B, Quan H D, Sun H X, et al. Multi-sequence frequency hopping communication method combined with pseudo-random feature codes. Syst Eng Electron, 2020, 42: 711–718 [王耀北, 全厚德, 孙慧贤, 等. 结合伪随机特征码的多序列跳频通信方法. 系统工程与电子技术, 2020, 42: 711–718]

6 Zhao L F, Wang L, Bi G, et al. Robust frequency-hopping spectrum estimation based on sparse Bayesian method. IEEE Trans Wireless Commun, 2015, 14: 781–793

7 Liu X Q, Li J L, Ma X L. An EM algorithm for blind hop timing estimation of multiple FH signals using an array system with bandwidth mismatch. IEEE Trans Veh Technol, 2007, 56: 2545–2554

8 Luo M, Wang H M, Yin Q Y. Hybrid relaying and jamming for wireless physical layer security based on cooperative beamforming. Sci Sin Inform, 2013, 43: 445–458 [罗苗, 王慧明, 殷勤业. 基于协作波束形成的中继阻塞混合无线物理层安全传输. 中国科学: 信息科学, 2013, 43: 445–458]

9 Tang Y X, Xu L, Wu F, et al. Electromagnetic spectrum umbrella. Sci Sin Inform, 2019, 49: 911–931 [唐友喜, 许林, 吴飞, 等. 电磁频谱伞罩. 中国科学: 信息科学, 2019, 49: 911–931]

10 Hong S, Pan C H, Ren H, et al. Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans Commun, 2020, 68: 7851–7866

11 Elsharief M, El-Gawad M A, Kim H W. Low-power scheduling for time synchronization protocols in a wireless sensor networks. IEEE Sens Lett, 2019, 3: 1–4

12 Guo W B, Song C Q, Xia X J, et al. Analysis of cooperative jamming cancellation with imperfect time synchronization in physical layer security. IEEE Wireless Commun Lett, 2021, 10: 335–338

13 Zhang M, Liu Y, Zhang R. Artificial noise aided secrecy information and power transfer in OFDMA systems. IEEE Trans Wireless Commun, 2016, 15: 3085–3096

14 Liu M Y, Liu Y. Power allocation for secure SWIPT systems with wireless-powered cooperative jamming. IEEE Commun Lett, 2017, 21: 1353–1356

15 Harrison W K, Almeida J, McLaughlin S W, et al. Coding for cryptographic security enhancement using stopping sets. IEEE Trans Inform Forensic Secur, 2011, 6: 575–584

16 Harrison W K, McLaughlin S W. Tandem coding and cryptography on wiretap channels: EXIT chart analysis. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), 2009. 1939–1943

17 Quan X, Liu Y, Shao S H, et al. Impacts of phase noise on digital self-interference cancellation in full-duplex communications. IEEE Trans Signal Process, 2017, 65: 1881–1893

18 Jain M, Choi J, Kim T, et al. Practical, real-time, full duplex wireless. In: Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MOBICOM), 2011. 301–312

19 Zhong Y, Guo W B, Zhao H Z, et al. Cooperative jamming cancellation analysis based on RC shaping filter in physical layer security. In: Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops), 2021. 1–5

20 Zlatanov N, Sippel E, Jamali V, et al. Capacity of the Gaussian two-hop full-duplex relay channel with residual self-interference. IEEE Trans Commun, 2017, 65: 1005–1021
21 Pan G F, Tang C Q, Li T T, et al. Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems. IEEE Trans Commun, 2015, 63: 3423–3433
22 Huang Y, Al-Qahtani F S, Duong T Q, et al. Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. IEEE Trans Commun, 2015, 63: 2959–2971
23 Gou W B. Key technologies of co-frequency interference cancellation in spectrum symbiosis systems. Dissertation for Ph.D. Degree. Chengdu: University of Electronic Science and Technology of China, 2021 [郭文博. 频谱共生系统中的同频干扰抑制关键技术. 博士学位论文. 成都: 电子科技大学, 2021]
24 Ku S J, Wang C L, Chen C H. A reduced-complexity PTS-based PAPR reduction scheme for OFDM systems. IEEE Trans Wireless Commun, 2010, 9: 2455–2460
25 Aziz M, Rawat M, Ghannouchi F M. Low complexity distributed model for the compensation of direct conversion transmitter's imperfections. IEEE Trans Broadcast, 2014, 60: 568–574
26 Benesty J, Huang Y T, Chen J D. A fast recursive algorithm for optimum sequential signal detection in a BLAST system. IEEE Trans Signal Process, 2003, 51: 1722–1730
27 Luo Z D, Gao H, Liu Y N. Adaptive transmission with linear computational complexity in MIMO-OFDM systems. IEEE Trans Commun, 2007, 55: 1873–1877

附录 A　命题 3 中人工噪声最优功率分配方案推导证明

式 (30) 中最优功率分配的优化问题可以重新表述为

$$\max_{\alpha} C_s = \frac{1}{2}\log_2\left[\frac{(a\alpha+b)(c\alpha+N)}{(a\alpha+N)(c\alpha+c)}\right] \tag{A1}$$

$$\text{s.t.} \begin{cases} (aN+bc-cN-ac)\alpha \geqslant (c-b)N, & ① \\ \alpha \geqslant 0. & ② \end{cases} \tag{A2}$$

首先计算 C_s 对 α 的一阶偏导数, 得到

$$\frac{\partial C_s}{\partial \alpha} = \frac{A\alpha^2+B\alpha+C}{2\ln 2\times\beta(\alpha)}, \tag{A3}$$

其中 $\beta(\alpha)=(a\alpha+b)(c\alpha+N)(a\alpha+N)(c\alpha+c)$, $A=ac(cN+ac-aN-bc)$, $B=2acN(c-b)$, $C=Nc(aN+bc)-Nb(cN+ac)$.

进而可以得到 $\frac{\partial C_s}{\partial \alpha}=0$ 等价于

$$A\alpha^2+B\alpha+C=0. \tag{A4}$$

情形一. 当 $A=0$, 即 $aN+bc=cN+ac$ 时, 若 $b<c$, 可行条件 ① 和 ② 等价于 $\alpha\in\phi$; 若 $b\geqslant c$, 可行条件 ① 和 ② 等价于 $\alpha\in[0,+\infty)$. 则在 $A=0$ 的情形下, 我们可以得到以下结论:

• 当 $b<c$ 时, 最优功率分配因子满足 $\alpha^*=\phi$.

• 当 $b\geqslant c$, 即 $B\leqslant 0$, $C\leqslant 0$ 时, 由 $\alpha\geqslant 0$ 可得 $\frac{\partial C_s}{\partial \alpha}\leqslant 0$, 表明 C_s 随着 α 的增加而减小. 因此, 此时的最优功率分配因子满足 $\alpha^*=0$.

情形二. 当 $A>0$, 即 $aN+bc<cN+ac$ 时, 若 $b<c$, 可行条件 ① 和 ② 等价于 $\alpha\in\phi$; 若 $b\geqslant c$, 可行条件 ① 和 ② 等价于 $\alpha\in[0,\alpha_0]$, 其中 $\alpha_0=\frac{N(b-c)}{cN+ac-aN-bc}$. 则在 $A>0$ 的情形下, 我们可以得出以下结论:

• 当 $b<c$ 时, 最优功率分配因子满足 $\alpha^*=\phi$.

• 当 $b\geqslant c$, 即 $C<0$ 时, 由式 (A5) 可得 $\frac{\partial C_s}{\partial \alpha}|_{\alpha=\alpha_0}<0$. 定义 $\frac{\partial C_s}{\partial \alpha}=0$ 的解为 α_1 和 α_2, 表达式分别如式 (32) 和 (A6) 所示, 则有 $\alpha_1<0<\alpha_0<\alpha_2$. 因此当 $\alpha\in[0,\alpha_0]$ 时, 我们有 $\frac{\partial C_s}{\partial \alpha}<0$, 表明当 $A>0$ 和 $b\geqslant c$ 时 C_s 随着的 α 增加而减小, 此时的最优功率分配因子满足 $\alpha^*=0$.

$$\left.\frac{\partial C_s}{\partial \alpha}\right|_{\alpha=\alpha_0} = \frac{acN^2(b-c)^2}{2\ln 2\cdot\beta(\alpha_0)\cdot(aN+bc-ac-cN)} + \frac{Nc(aN+bc)-Nb(ac+cN)}{2\ln 2\cdot\beta(\alpha_0)}, \tag{A5}$$

$$\alpha_2 = \frac{aN(b-c)+\sqrt{aN(a-b)(a-c)(b-N)(c-N)}}{a(ac+cN-bc-aN)}. \tag{A6}$$

情形三. 当 $A<0$, 即 $aN+bc>cN+ac$ 时, 若 $b<c$, 可行条件 ① 和 ② 等价于 $\alpha\in[\alpha_0,+\infty)$; 若 $b\geqslant c$, 可行条件 ① 和 ② 等价于 $\alpha\in[0,+\infty)$. 则在 $A<0$ 的情形下, 我们可以得到以下结论:

• 当 $b<c$ 时, 我们有 $C>0$, $\frac{\partial C_s}{\partial\alpha}|_{\alpha=\alpha_0}>0$, 且 $\alpha_2<0<\alpha_0<\alpha_1$. 因此当 $\alpha\in[\alpha_0,\alpha_1)$ 时满足 $\frac{\partial C_s}{\partial\alpha}>0$, 当 $\alpha\in(\alpha_1,+\infty)$ 时满足 $\frac{\partial C_s}{\partial\alpha}<0$, 此时最优功率分配因子满足 $\alpha^*=\alpha_1$.

• 当 $b\geqslant c$ 且 $c(aN+bc)\leqslant b(cN+ac)$ 时, 我们有 $B\leqslant 0$, $-\frac{B}{2A}\leqslant 0$, 且 $C\leqslant 0$. 因此在 $\alpha\in(0,+\infty)$ 时满足 $\frac{\partial C_s}{\partial\alpha}<0$, 此时的最优功率分配因子满足 $\alpha^*=0$.

• 当 $b\geqslant c$ 且 $c(aN+bc)>b(cN+ac)$ 时, 我们有 $C>0$, $\alpha_2<0<\alpha_1$. 因此当 $\alpha\in[0,\alpha_1)$ 时满足 $\frac{\partial C_s}{\partial\alpha}>0$, 当 $\alpha\in(\alpha_1,+\infty)$ 时满足 $\frac{\partial C_s}{\partial\alpha}<0$, 此时最优功率分配因子满足 $\alpha^*=\alpha_1$.

整合上述分析, 可得命题 3 中的最优功率分配结论.

Artificial noise shielded frequency hopping secure communication

Changqing SONG, Yidan ZHANG, Hongzhi ZHAO* & Shihai SHAO*

National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731*, China*

* Corresponding author. E-mail: lyn@uestc.edu.cn, ssh@uestc.edu.cn

Abstract To counteract electromagnetic interference and hostile wiretapping, an artificial noise-shielded frequency hopping (ANS-FH) architecture is proposed in this paper. In this regard, AN cancellation is a key procedure for secrecy enhancement, but the time-synchronization error between a received signal and the locally reconstructed AN degrades the AN cancellation and system secrecy performance. Given this circumstance, the residual AN components after the cancellation and secrecy performance under the time-synchronization error are analyzed. Based on this analysis, a closed-form optimal transmitting power-allocation (PA) scheme for AN and a confidential signal (CS) is provided to reduce the secrecy loss by synchronization errors. Theoretical and simulation results show that the time-synchronization error in the proposed ANS-FH systems increases the inter-symbol and inter-hop interference during AN cancellation and, thus, degrades the AN cancellation and secrecy performance. Meanwhile, simulations on the proposed PA scheme show that the power ratio of AN to CS should be equivalent when perfect time synchronization is performed and should decrease gradually when the synchronization error increases to counteract the performance degradation by the time-synchronization error.

Keywords artificial noise, frequency hopping, time synchronization error, noise cancellation, power allocation