物理层安全保密电话的实现

Realization of Wireline Telephone Based on Physical Layer Security

林立峰/LIN Lifeng，周子健/ZHOU Zijian，焦秉立/JIAO Bingli
（北京大学，中国 北京 800718）
（Peking University， Beijing 800718， China）

DOI：10.12142/ZTETJ.202502011
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20240814.1036.002.html
网络出版日期：2024-08-15
收稿日期：2024-07-10

摘要：提出一种基于物理层安全的安全保密电话的实现方法。该方法通过在双向通信的每个信道上释放人工噪声，使得线路任意窃听点检测到的信号功率远低于噪声功率，从而无法识别通信信息。合法用户采用同频同时全双工技术消除人工噪声，恢复正常通信。理论分析与实验结果表明，该系统能有效抑制自干扰，使合法用户的信干噪比显著优于窃听者。硬件原型的成功研制验证了系统的实用性和有效性，为高安全性通信场景提供了可行的技术解决方案。

关键词：物理层安全；同频同时全双工；保密电话；人工噪声

Abstract: An implementation method for a secure telephone system based on physical layer security is proposed. The security principle involves injecting artificial noise into each bidirectional communication channel, ensuring that the signal power detected by any illegal eavesdropper at any probing point on the line is far lower than the artificial noise power, thereby preventing information extraction. Legitimate users employ co-frequency co-time full-duplex technology to cancel the artificial noise and recover the original communication signal. Theoretical analysis and experimental results demonstrate that this system can effectively eliminate self-interference, allowing the legitimate user's signal-to-interference-plus-noise ratio to significantly outperform that of an eavesdropper, thereby ensuring communication security. The successful implementation of a hardware prototype further validates the system's practicality and effectiveness, offering a feasible technical solution for high-security communication scenarios.

Keywords: physical layer security; co-frequency co-time full-duplex; secure telephone; artificial noise

引用格式：林立峰, 周子健, 焦秉立. 物理层安全保密电话的实现 [J]. 中兴通讯技术, 2025, 31(2): 77-82. DOI: 10.12142/ZTETJ.202502011
Citation: LIN L F, ZHOU Z J, JIAO B L. Realization of the wireline telephone based on physical layer security [J]. ZTE technology journal, 2025, 31(2): 77-82. DOI: 10.12142/ZTETJ.202502011

随着通信业务种类和规模的快速发展，信息安全作为隐私保护的核心需求，已成为现代通信领域的重要组成部分[1-6]。在点对点保密通信研究中，学术界通常采用包含合法用户（Alice和Bob）与窃听者（Eve）的典型模型。相关研究主要围绕两个关键问题展开：一是确保合法用户之间的安全信息传输；二是有效防止窃听者的信息截获。

为阐明本文物理层安全方法的特性，我们先对传统密码学方法进行介绍。该方法起源于两次世界大战期间的密码通信，其核心机制是将明文转换为密文，使窃听者Eve在无密钥条件下难以还原信息。然而，此方法存在两点局限性：1）Alice需将解码密钥告知Bob；2）即便Eve不知晓密钥，仍可能借助高性能计算设备破解密文。

另一种方法为物理层安全方法，其理论根基源于SHANNON信道容量理论，后经WYNER于1975年完善。该方法以信息比特作为基本单元，通过数学方法描述信息比特与噪声的关联特性，从而构建安全容量模型[7]。物理层安全的核心目标在于当通信信噪比低于特定阈值时，即便Eve采用任何方法也无法恢复被噪声或干扰所隐匿的信息比特。通常只要Bob的信噪比高于Eve，即可实现安全通信，这一结论在安全容量框架下具备坚实的信息论理论支撑。

然而在实际通信环境中，合法用户难以始终维持对窃听者的信噪比优势。为此，研究者提出了人工噪声（AN）技术来抑制Eve的窃听能力。文献[8]指出，通过在接收机端发射AN，利用Eve对噪声信息的未知性，可将其信噪比降低至安全阈值以下。例如，文献[9]、[10]提出通过部署AN成功实现Alice与Bob间的秘密通信。由于AN在接收机（即Bob）处释放，对于Bob而言，该噪声属于已知干扰，理论上可完全消除，从而保障其与Alice间的合法通信。近年来，文献[11]、[12]提出采用无人机搭载干扰器的方案，旨在借助空间维度拓展，提升保密通信的灵活性与覆盖范围。

基金项目：国家自然科学基金项目（62171006）

同频同时全双工（CCFD）技术被应用于合法用户的AN的消除处理[13-16]。该技术利用CCFD的自干扰消除机制，在实现大功率AN发射的同时，可在接收端有效消除AN干扰，从而保障Alice通信信号的接收质量。

早期AN方法在无线通信应用中取得了一定的效果，但其存在局限性：由于无线信号在空中传播时会随距离急剧衰减，当窃听者Eve与合法接收方Bob的距离较远时，Eve接收到的AN功率会显著降低，甚至导致该方法失效。此外，该方法无法满足信息双向传输场景下的保密通信需求。

针对现有AN方法的不足，本研究基于文献[17]将无线通信场景拓展至有线电话系统。该方法通过电话线注入AN，具有两大优势：首先，有效克服了路径损耗导致的噪声衰减，确保所有潜在窃听点的信噪比均低于安全阈值；其次，完整保留了电话线路的双向通信功能。下文将详细论述该方法的实现原理、系统架构及实验验证结果。

1 工作原理和系统构成

本文中我们提出的物理层安全电话，其核心思路在于由接收机（Bob）向线路发送干扰信号，使线路上传输的信号被干扰所覆盖。鉴于电话系统具备双向信号传输特性，为便于阐述基本原理，我们先对单向信号传输接收的工作机制进行说明，后续将进一步介绍完整的双向通信保密原理。

1）保密电话工作原理

图1（a）展示了Alice向Bob发射信号的单向通信保密模型，两者通过长度为L的导线进行通信，窃听者Eve在链路中间采用搭线方式进行窃听。将Alice发射的通信信号记为$s_1(t)$，Bob在接收该信号的同时发射人工噪声$n_1(t)$，经噪声消除处理后，Bob可获取$s_1(t)$携带的信息；而Eve接收到的电信号则为$s_1(t)$与人工噪声的叠加。

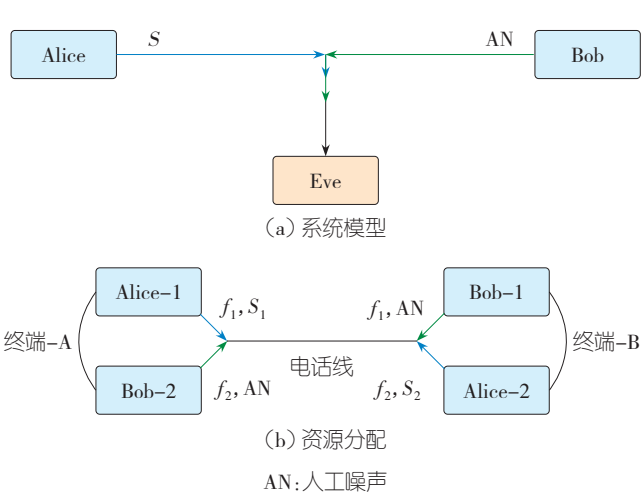


图1 有线安全通信的理论模型

当Eve在距离Alice点x处时，其接收电磁为：

$$r_{\mathrm{Eve}}(x,t)=\sqrt{\alpha(x)}\,s_1\left(t-\frac{x}{c}\right)+\sqrt{\alpha(L-x)}\,n_1\left(t-\frac{L-x}{c}\right)+n_e(t) \quad (1)。$$

在公式（1）中$s_1(t)$、$n_1(t)$和$n_e(t)$分别表示Alice发射的信号、AN和热噪声；c表示光速，$\alpha(x)$描述了电磁波功率沿着导线传播距离的衰减因子。

此时，Bob在消除AN后的接收电磁波可以表达为：

$$r_{\mathrm{Bob}}(t)=\sqrt{\alpha(L)}\,s_1\left(t-\frac{L}{c}\right)+\beta n_1(t)+n_b(t) \quad (2)。$$

在公式（2）中，β、$n_b(t)$分别表示Bob处AN消除因子和热噪声。强大的消除能力保证了$\beta \ll 1$。

从公式（1）和（2）可以看出：一方面，我们希望Bob能够彻底消除AN，即满足$\beta=0$；另一方面，需要保证Eve处的AN功率足够大，以发挥有效干扰作用。上述约束条件共同构成了本文所提出的AN环境下物理安全模型。

2）保密电话系统

我们提出的物理层安全电话为双向通信保密系统，在电话线两端均配置发射机与接收机，分别记为通信终端–A和通信终端–B。其中，将终端–A的发射机定义为Alice–1，终端–B的接收机定义为Bob–1，对应上述单向保密通信模型；在反向通信中，将终端–B的发射机定义为Alice–2，终端–A的接收机定义为Bob–2，由此构建双向通信的两条链路。为避免Alice–1与Bob–1、Alice–2与Bob–2两条通信链路间的相互干扰，系统采用频率分离技术，其中Alice–1与Bob–1链路采用频率f_1，Alice–2与Bob–2链路采用频率f_2，Bob–1和Bob–2释放的AN亦分别对应f_1和f_2。此外，通过滤波器实现两个频率信号的隔离。系统结构如图1（b）所示。

因此，我们仅需对通信链路Alice–1与Bob–1的物理安全问题展开分析，Alice–2与Bob–2链路的情况与之类似。

3） 安全性能分析

安全通信的绝对安全性需在时空维度上同时满足。对于窃听者Eve所拦截的信号，其最大能量可通过对整个信息符号持续时间T进行积分运算来确定。实际通信中，Eve可能进行多次拦截，并在特定时刻实现与ID符号同步，达到最佳检测状态。此外，还需考虑拦截者在干扰效率最大化时的极端情况。

我们采用矩形波形模型分别表征通信符号与AN的相关性。以持续时间T的首个通信符号为例，在该时段内，窃听

者Eve的拦截信号可综合表示为：

$$\hat{r}_{\text{Eve}}^{x}=\frac{1}{T}\int_0^T r_{\text{Eve}}(x,t)\mathrm{d}t=\sqrt{\alpha(x)}\,s_1(0)+\sqrt{\alpha(L-x)}\,\hat{n}_1+\hat{n}_e \quad (3),$$

其中，$\hat{n}_1=\frac{1}{T}\int_0^T n_1(t)\mathrm{d}t$ 和 $\hat{n}_e=\frac{1}{T}\int_0^T n_e(t)\mathrm{d}t$。同样，Bob在第一个符号持续时间内收到的信号可表示为：

$$\hat{r}_{\text{Bob}}=\frac{1}{T}\int_0^T r_{\text{Bob}}(t)\mathrm{d}t=\sqrt{\alpha(L)}\,s_1(0)+\sqrt{\beta}\,\hat{n}_1+\hat{n}_b \quad (4),$$

其中，$\hat{n}_1=\frac{1}{T}\int_0^T n_1(t)\mathrm{d}t$ 和 $\hat{n}_b=\frac{1}{T}\int_0^T n_b(t)\mathrm{d}t$。

为获取最大信干噪比（SINR），需综合考虑多次拦截的叠加效应。据此，Eve拦截信号SINR计算方法如下：

$$\gamma_{\text{Eve}}^{x}=\frac{\alpha(x)\mathbb{E}\left[\left|s_1(0)\right|^2\right]}{\alpha(L-x)\mathbb{E}\left[\left|\hat{n}_1\right|^2\right]+\sigma_n^2}=\frac{\alpha(x)P_s}{\alpha(L-x)P_n+\sigma_n^2} \quad (5)。$$

安全通信的最不利情况出现在窃听者Eve处于距Alice最近且距Bob最远的位置。此时，Alice信号的传播距离达到最大L，Eve可获得的SINR为：

$$\gamma_{\text{Eve}}^{\max}=\frac{P_s}{\alpha(L)P_n+\sigma_n^2} \quad (6)。$$

相应地，Bob的SINR计算为：

$$\gamma_{\text{Bob}}=\frac{\alpha(L)P_s}{\beta P_n+\sigma_n^2} \quad (7)。$$

我们提出的有线通信系统的容量可以表示为：

$$C_s=\left[\log_2\left(1+\gamma_{\text{Bob}}\right)-\log_2\left(1+\gamma_{\text{Eve}}^{\max}\right)\right]^+ \quad (8)。$$

容量C_s表示在窃听者（Eve）存在的条件下，发送方（Alice）向接收方（Bob）发送可靠且安全信息的最大速率。为了确保绝对安全，需要满足$\gamma_{\text{Bob}}>\gamma_{\text{Eve}}^{\max}$，即：

$$P_n>\frac{1-\alpha(L)}{\alpha^2(L)-\beta-\alpha(L)}\sigma_n^2 \quad (9),$$

$$\alpha^2(L)-\beta-\alpha(L)>0 \quad (10)。$$

由于AN消除系数β<<1，且远小于导线衰减因子$\alpha(L)$，因此公式（10）在实际应用中通常能够得到满足。需要注意的是，公式（9）和（10）构成了保障有线通信系统绝对安全传输的必要条件。导线长度的增加会显著提高系统对AN消除能力的要求。

2 一种基于2/4线电路的AN消除方法

我们提出一种基于经典的2/4线电路的AN消除方法。AN消除的原理如图2（a）所示，其中V_s表示等效电压源，Z_1—Z_6是输入端的电阻，Z_0为输出端的等效阻抗。从Alice端看，Bob作为其负载，Z_0即为Bob电路的等效输入阻抗，反之亦然。在通信过程中，一个合法用户向另一个发送V_3-V_4，而其接收到的信号是V_1-V_2。通过合理设计阻抗参数，可有效抑制AN干扰。由于合法链路的性能主要取决于AN的消除能力β，我们将推导出该系统的自我取消能力β。

当Alice处于信息数据与AN发送状态而Bob处于空闲状态时（其电压源未启动），根据前节分析可知，Alice接收的信号为V_1-V_2。由于Bob处于空闲状态且未向Alice发送任何信号，此时Alice接收的信号本质上是自身发送的AN，因此，Alice发送的AN可通过差分电压信号V_1-V_2来表示。同理，Bob发送的AN亦可采用相同方法分析，在此不再重复讨论。

如图2（b）所示，基于网格电流法，我们对每个回路应用Kirchhoff电压定律，可得到以下线性方程组：

$$\begin{aligned}&(Z_1+Z_2+Z_3+Z_0)I_1-Z_0I_2-Z_3I_3=0\\&-Z_0I_1+(Z_4+Z_5+Z_6+Z_0)I_2-(Z_5+Z_6)I_3=0\\&-Z_3I_1-(Z_5+Z_6)I_2+(Z_3+Z_5+Z_6)I_3=-V_s\end{aligned} \quad (11)。$$

上述线性方程组可转化为如下矩阵形式：

$$\boldsymbol{ZI}=\boldsymbol{V} \quad (12),$$

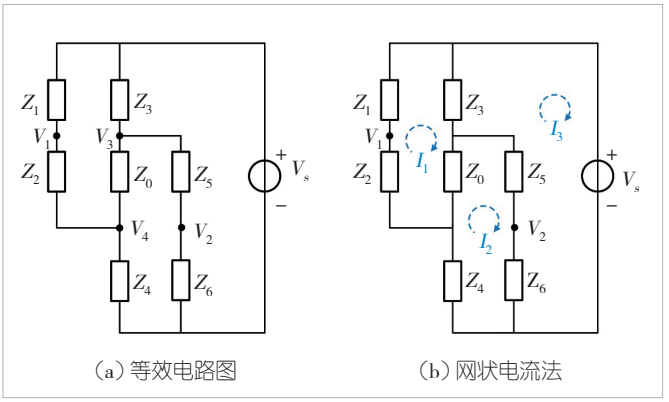
其中，$\boldsymbol{Z}$、$\boldsymbol{I}$和$\boldsymbol{V}$分别表示系数矩阵、未知数和常数项的列向量。

$$\begin{bmatrix}Z_1+Z_2+Z_3+Z_0 & -Z_0 & -Z_3\\ -Z_0 & Z_4+Z_5+Z_6+Z_0 & -(Z_5+Z_6)\\ -Z_3 & -(Z_5+Z_6) & Z_3+Z_5+Z_6\end{bmatrix}\begin{bmatrix}I_1\\I_2\\I_3\end{bmatrix}=\begin{bmatrix}0\\0\\-V_s\end{bmatrix} \quad (13)。$$

利用Cramer法则，网格电流可以通过公式（14）解出：

$$I_i=\frac{\det(\boldsymbol{Z}_i)}{\det(\boldsymbol{Z})}(i=1,2,3) \quad (14),$$

其中，$\boldsymbol{Z}_i$表示将$\boldsymbol{Z}$的第i列替换为$\boldsymbol{V}$后形成的矩阵。矩阵$\boldsymbol{Z}_1$、



（a）等效电路图　（b）网状电流法

图2　2/4线人工噪声消除电路等效电路图

Z_2、Z_3和Z的行列式可以按照方程（15）计算。

$$
\begin{aligned}
&det(Z_1) = -V_s \cdot \left[Z_0(Z_5 + Z_6) + Z_3(Z_4 + Z_5 + Z_6 + Z_0) \right] \\
&det(Z_2) = -V_s \cdot \left[(Z_1 + Z_2 + Z_3 + Z_0)(Z_5 + Z_6) + Z_0 Z_3 \right] \\
&det(Z_3) = -V_s \cdot \left[(Z_1 + Z_2 + Z_3 + Z_0)(Z_4 + Z_5 + Z_6 + Z_0) + Z_0^2 \right] \\
&det(Z) = Z_3 Z_4 (Z_1 + Z_2 + Z_5 + Z_6) + (Z_3 + Z_4)(Z_1 + Z_2)(Z_5 + Z_6) + \\
&Z_0 \left[(Z_1 + Z_2 + Z_4) Z_3 + Z_4 (Z_5 + Z_6) + (Z_5 + Z_6)(Z_1 + Z_2) \right]
\end{aligned}
\tag{15}
$$

根据方程$V_{SI} = V_1 - V_2$可知，残余AN过于复杂难以处理。然而，在实际系统中，我们可对残余AN进行近似与简化。具体来说，将电阻值设计为$Z_1, Z_2, Z_5, Z_6 \gg Z_3, Z_4$，可使输出阻抗$Z_0$近似等于$Z_3 + Z_4$，即$Z_0 \approx Z_3 + Z_4$。基于此，可通过舍弃方程中包含小阻值乘积的项，进一步简化全双工系统中的残余AN信号表达式，最终得到公式（16）：

$$
V_{SI} = V_1 - V_2 \approx V_s \left[\frac{Z_4 Z_5 - Z_0 Z_6}{(Z_3 + Z_4 + Z_0)(Z_5 + Z_6)} + \frac{Z_2 Z_3 + Z_0 Z_2}{(Z_3 + Z_4 + Z_0)(Z_1 + Z_2)} \right] \tag{16}
$$

实际电阻值被设计为$Z_1 = Z_6$，$Z_2 = Z_5$和$Z_3 = Z_4$。因$Z_1, Z_2, Z_5, Z_6 \gg Z_3, Z_4$，我们可以进一步假设$Z_3 = Z_4 \triangleq Z_S$，$Z_2 = Z_5 \triangleq Z_L$和$Z_1 = Z_6 \triangleq \alpha Z_L$。利用上述符号，则有$Z_0 \approx Z_3 + Z_4 = 2Z_S$。全双工残余AN可以被简化为公式（17）：

$$
V_{SI} \approx V_s \left[\frac{Z_S Z_L - 2\alpha Z_S Z_L}{4(1+\alpha) Z_S Z_L} + \frac{Z_S Z_L + 2Z_S Z_L}{4(1+\alpha) Z_S Z_L} \right] = \frac{2 - \alpha}{2 + 2\alpha} V_s \tag{17}
$$

最终，我们得到AN抑制能力β：

$$
\beta = \frac{V_{SI}}{V_s} = \frac{2 - \alpha}{2 + 2\alpha} \tag{18}
$$

图3展示了残余AN信号幅度与公式（18）中参数α之间的关系。可以看出，当$\alpha = 2$时，系统达到AN抑制效果。然而，受硬件非理想特性影响，α的实际取值往往存在微小误差，从而降低AN抑制性能。因此，采用高精度电子元件对优化系统性能具有关键作用。

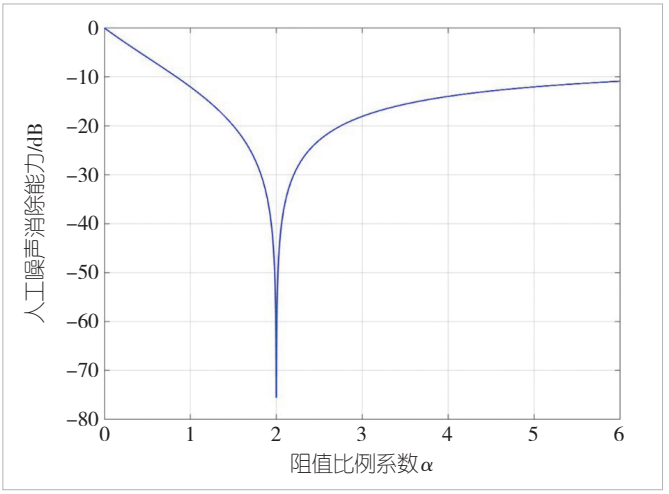


图3　残余人工噪声对应α值

3 性能分析

本章节我们介绍硬件原型的实现方案和实测性能。实验结果表明，本文所提的保密电话方案具有实用性和有效性。根据文献[17]，信号强度按每100 m距离衰减2 dB的规律递减[17]。同时，设置P_s = 10 dBm，$\sigma_n^2 = -100$ dBm，那么发射的AN功率为$P_n = -60$ dBm。

硬件系统的实现架构和实物展示分别如图4和图5所示。图4展示了包含Alice和Bob两个通信节点的通信系统架构，各节点通过电话机与现场可编程门阵列（FPGA）相连，由FPGA承担信号的发送与接收处理任务。在发送路径中，FPGA将通信信号与AN传输至数模转换器（DAC），经转换后的模拟信号依次通过放大器与滤波器处理，再输入至2/4线AN消除器；接收路径中，信号经模数转换器（ADC）采样后，回传至FPGA进行处理。该架构在收发路径均部署放大器与滤波器，以保障信号质量与传输性能。音频信号的输入和输出由WM8731执行。基带音频信号处理依托搭载Intel Cyclone V SE 5CSXFC6D6F31C6N芯片的DE10-Standard开发板实现，基带信号上变频与射频信号下变频分别由AD9767和AD9226芯片执行。系统选用AD8065作为功率放大器，AD8138作为滤波器件，2/4线电路则基于THS6022与THS6062芯片搭建。

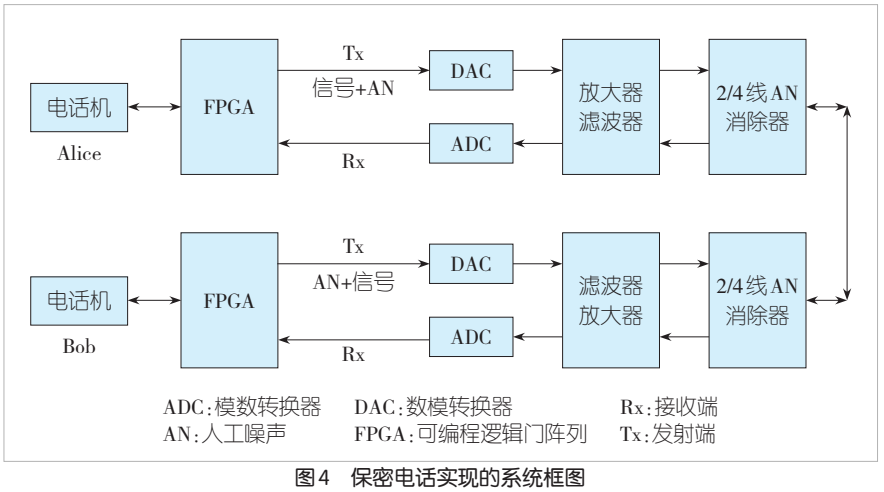


图4　保密电话实现的系统框图

(a)内部电路图

(b)保密电话产品图

图5 保密电话实物展示

图6展示了信息信号与残余AN的实际频率响应。实验步骤如下：首先，在Alice端生成基带单频正弦波信号；随后，该信号经上变频处理后通过有线信道传输至Bob端。在Alice端，我们通过导线前端采集传输信号，同时在Bob端的导线后端同步接收信号。此外，实验还采集了经2/4线转换处理后的Alice端残余AN信号。通过对接收信号、残余AN信号及传输信号的功率比进行计算，结果表明：该硬件原型具有优异的AN消除性能，可实现至少26 dB的残余AN抑制，同时保持可忽略的信号损耗。

图7对比了合法链路与窃听链路的SINR。实验步骤如下：首先，将1 s时长的音频信号输入合法用户链路，经ADC采样后与AN叠加；随后，叠加信号通过脉冲整形滤波器与功率放大器处理，并经由有线信道传输至另一合法用户。实验结果表明，在所有测试场景中，合法链路的SINR均优于窃听链路约27 dB，与理论值（30 dB）的3 dB偏差验证了所提全双工通信物理层安全方案的有效性与合理性。

图8展示了在26 dB AN消除能力下，系统安全容量与AN功率的关系曲线。安全容量通过公式（8）计算获得，实验测试了100 m、200 m和300 m 3种线缆长度下的性能表现。结果表明：线缆长度的增加会导致安全容量降低；而提升AN功率则能显著改善系统性能，这源于增强的AN干扰有效抑制了潜在窃听者的信号截获能力。

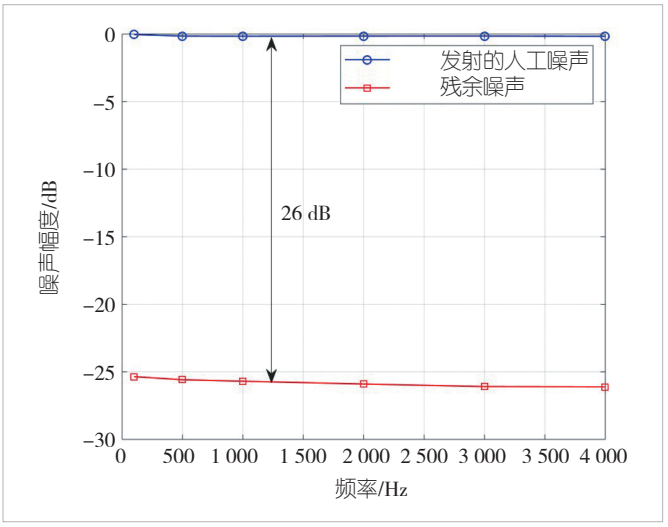


图6 信号和人工噪声消除后的频率响应(L = 100 m)

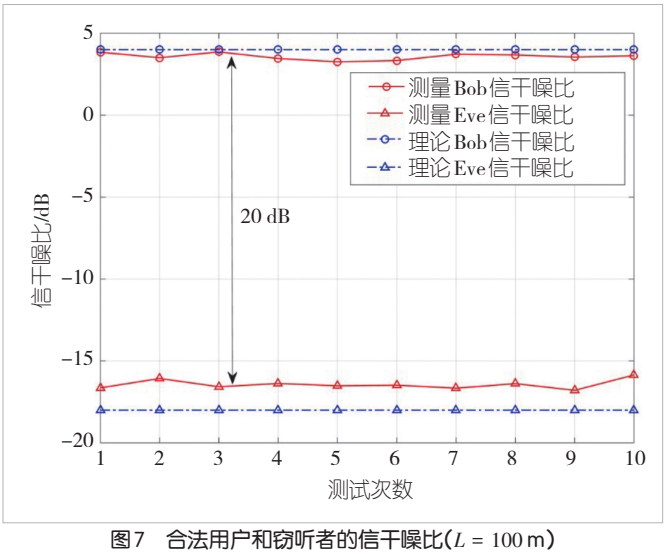


图7 合法用户和窃听者的信干噪比(L = 100 m)

4 结束语

本文中，我们提出并实现了一种基于全双工技术的新型安全有线通信方案及配套硬件系统。首先，详细阐述了系统设计原理与架构模型，通过信息数据与AN的叠加保障合法用户的通信安全。其次，创新性地提出了一种基于简易电阻网络的AN消除方法，实现了高效的噪声抑制性能。紧接着，重点分析了合法链路的传输性能，其关键性能指标取决于AN消除效果。其中，残余AN水平通过差分信号计算方法精确量化。通过理论仿真与实物实验相结合的方式，充分验证了所提方案的技术可行性与实用价值。

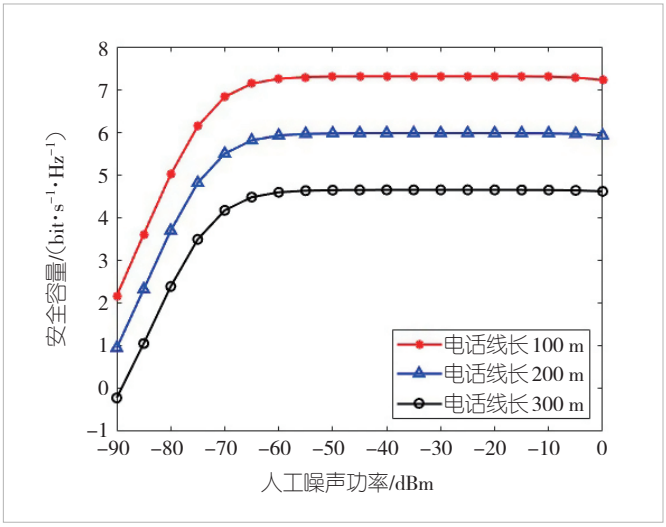


图8 不同电话线长下的安全容量性能对比

致谢

烟台大学的姜佩贺老师、湖北民族大学的刘三军老师，以及北京大学的魏来博士对本文的研究做出了贡献，专此致谢！

参考文献

[1] WYNER A D. The wire-tap channel [J]. Bell system technical journal, 1975, 54(8): 1355-1387. DOI: 10.1002/j. 1538-7305.1975.tb02040.x
[2] LIU F, CUI Y H, MASOUROS C, et al. Integrated sensing and communications: toward dual-functional wireless networks for 6G and beyond [J]. IEEE journal on selected areas in communications, 2022, 40(6): 1728-1767
[3] NGUYEN D C, DING M, PATHIRANA P N, et al. 6G Internet of Things: a comprehensive survey [J]. IEEE Internet of Things journal, 2021, 9(1): 359-383. DOI: 10.1109/jiot.2021.3103320
[4] CHETTRI L, BERA R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems [J]. IEEE Internet of Things journal, 2019, 7(1): 16-32. DOI: 10.1109/jiot.2019.2948888
[5] SHAFIQUE K, KHAWAJA B A, SABIR F, et al. Internet of Things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios [J]. IEEE access, 2020, 8: 23022-23040
[6] QIAO X Q, REN P, NAN G S, et al. Mobile web augmented reality in 5G and beyond: challenges, opportunities, and future directions [J]. China communications, 2019, 16(9): 141-154
[7] SHANNON C E. Communication theory of secrecy systems [J]. Bell system technical journal, 1949, 28(4): 656-715. DOI: 10.1002/j.1538-7305.1949.tb00928.x
[8] LI W, GHOGHO M, CHEN B, et al. Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis [J]. IEEE communications letters, 2012, 16(10): 1628-1631. DOI: 10.1109/LCOMM.2012.081612.121344
[9] SOBERS T V, BASH B A, GUHA S, et al. Covert communication in the presence of an uninformed jammer [J]. IEEE transactions on wireless communications, 2017, 16(9): 6193-6206. DOI: 10.1109/TWC.2017.2720736
[10] LI K, SOBERS T V, TOWSLEY D, et al. Covert communication in continuous-time systems in the presence of a jammer [J]. IEEE transactions on wireless communications, 2022, 21(7): 4883-4897. DOI: 10.1109/TWC.2021.3134179
[11] ZHOU Y, YEOH P L, CHEN H, et al. Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location [J]. IEEE transactions on vehicular technology, 2018, 67(11): 11280-11284. DOI: 10.1109/tvt.2018.2868944
[12] ZHOU Y, YEOH P L, PAN C H, et al. Caching and UAV friendly jamming for secure communications with active eavesdropping attacks [J]. IEEE transactions on vehicular technology, 2022, 71(10): 11251-11256. DOI: 10.1109/TVT.2022.3186730
[13] DING J Z, ZHOU Z J, LI W Y, et al. Movable antenna-enabled co-frequency co-time full-duplex wireless communication [EB/OL]. [2025-03-16]. https://arxiv.org/abs/2401.17049v3
[14] DING J Z, ZHOU Z J, WANG C B, et al. Secure full-duplex communication via movable antennas [EB/OL]. [2025-03-15]. https://arxiv.org/abs/2403.20025v2
[15] DING J, ZHOU Z, JIAO B L. New paradigm for secure full-duplex transmission: movable antenna-aided multi-user systems [EB/OL]. [2025-03-15]. https://arxiv.org/pdf/2407.10393v1
[16] MA M, TIAN S Y, CHEN Y Y, et al. A prototype of co-frequency co-time full duplex networking [J]. IEEE wireless communications, 2020, 27(1): 132-139. DOI: 10.1109/mwc.001.1800565
[17] LIU S J, MA M, LI Y Z, et al. An absolute secure wire-line communication method against wiretapper [J]. IEEE communications letters, 2017, 21(3): 536-539. DOI: 10.1109/LCOMM.2016.2636836

作 者 简 介

林立峰，北京大学电子学院在读博士研究生，正高级工程师；主要从事同频同时全双工技术的研究工作以及无线收发机研究设计，研究方向为无线通信、卫星通信、物理层安全；参与省部级科研项目2项；已发表论文11篇。

周子健，北京大学电子学院科研助理；主要从事同频同时全双工技术的研究与相关原理样机的开发工作，研究方向为无线通信中的信号处理、极化天线系统，以及软件无线电应用；已发表论文12篇。

焦秉立，北京大学电子学院教授、中国通信学会智慧医疗专家委员会常务副主任、国家重大专项无限医疗物联网总体规划课题组组长、IEEE高级会员、北大-时空道宇先进通信联合实验室主任；主要从事同频同时全双工技术、通信中的信号处理以及移动医疗物联网的研究工作；先后主持新一代宽带无线通信重大专项、国家“863”课题、国家自然科学基金重点项目等；已发表论文180余篇。