恶意导频干扰对采用人工噪声方案系统的安全性能影响分析

沈利华[1],林胜斌[2],黄开枝[3]
(1. 浙江工业大学之江学院,浙江绍兴 312000;2. 重庆通信学院,重庆 400000;
3. 国家数字交换系统工程技术研究中心,河南郑州 450001)

摘 要: 针对窃听方发送恶意导频干扰破坏系统安全性能的问题,本文将研究场景扩展到三节点MIMO(Multple-Input Multiple-Output)网络,首先分析存在恶意导频干扰时最小二乘和最小均方误差准则下的信道估计结果,并推导基于人工噪声的系统安全速率公式,得出当窃听方到达发送方的导频干扰功率大于合法接收方达到的功率时,安全速率值只能为零.然后,进一步分别研究半双工窃听方和全双工窃听方场景下的最优功率分配方案.最后,通过数值仿真分析窃听者位置、窃听者类型和干扰功率等因素对安全性能的影响.

关键词: 物理层安全;恶意导频干扰;安全速率;功率分配
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2017)03-0650-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.03.022

Analysis of the Artificial Noise Based System Security Performance Under Malicious Pilot Contamination

SHEN Li-hua[1], LIN Sheng-bin[2], HUANG Kai-zhi[3]
(1. *Zhijiang College of Zhejiang University of Technology, Shaoxing, Zhejiang* 312000, *China*;
2. *Chongqing Communication Institute, Chongqing* 400000, *China*;
3. *National Digital Switching System Engineering & Technological Research Center, Zhengzhou, Henan* 450001, *China*)

Abstract: According to the security problem caused by the malicious pilot contamination, this paper considers a three-node MIMO(Multple-Input Multiple-Output) network. First, the channel estimation results based on the least square criterion and the minimum mean square error criterion under the malicious pilot contamination are analyzed. Then by deducing the secrecy rate, we conclude that when the power of the pilot contamination from the eavesdropper is larger than that from the legitimate receiver, the secrecy rate is zero. Finally, the optimal power allocation schemes for the half-duplex and full-duplex eavesdropper are further studied, respectively. Simulation results show the effects of eavesdropping position, eavesdropping type, jamming power and other factors on the security performance.

Key words: physical layer security; malicious pilot contamination; secrecy rate; power allocation

1 引言

无线网络具有广播特性,这给非法用户窃听、干扰、甚至攻击网络带来了便利条件,从而引发了一系列安全问题.针对这些安全威胁,传统的解决方法是在高层对信息进行加密.但密钥的频繁更新增加了加密算法的复杂度,且密钥的分发和管理也面临着挑战.近年来提出的物理层安全方法从无线信道的本质和特点出发,利用编码、调制等通信传输手段,在保证期望用户通信质量的同时,增加窃听者截获信号与还原信息的难度,实现无线信号的安全传输[1,2].

针对存在发送方,合法接收方和窃听方的三节点窃听场景,物理层安全方法主要分为三类,(1)基于无线信道特征的信号处理技术,如人工噪声[3];(2)利用

收稿日期:2015-06-01;修回日期:2016-01-04;责任编辑:梅志强
基金项目:国家863高技术研究发展计划(No. SS2015AA011306);国家自然科学基金(No. 61379006);科技部科技支撑计划(No. 2014BAH30B01)

无线信道的互易性,合法通信双方生成一致性密钥[4];(3)利用无线信道质量的差异性进行安全编码,如 LDPC 编码[5]. 其中,人工噪声技术是指发送方根据其到合法接收方的信道状态信息(Channel State Information, CSI),同时发送经过预编码的信号和噪声,从而使该噪声只对窃听方产生干扰,提高合法通信的安全性能[6]. 它需要事先获取合法通信之间的 CSI,于是在数据信号传输之前,存在一个反向训练阶段,合法接收方发送导频信号,发送方根据接收的导频信号进行信道估计. 然而,在存在窃听方的网络中,被多次传输的导频很可能被窃听方获取,当合法接收方发送导频信号时,窃听方同时发射导频信号,干扰发送方的信道估计. 文献[7]针对多小区大规模 MIMO 系统,分析了小区间的导频干扰对信道估计的影响,同时给出信道估计的优化方案,然而该文献仅考虑同频被动干扰的影响. 文献[8]研究了 MISO 场景下一个窃听方在反向训练阶段主动发送导频信号,干扰合法发送方的信道估计结果,从而破坏了发送方的随机波束成型技术,提高窃听性能. 随着 MIMO 和人工噪声的广泛应用,研究 MIMO 场景下导频干扰对采用人工噪声方案系统的安全性能影响,用于指导设计有效的抗导频干扰方案,具有理论指导意义.

针对现有文献缺乏导频干扰对采用人工噪声方案系统的安全性能影响分析,在存在一个发送方,合法接收方和窃听方的三节点 MIMO 网络中,与传统窃听方只窃听[9]或发送噪声干扰[10]不同,假设该窃听方已知导频信号[8],并在反向训练阶段同时发送导频信号实现恶意导频干扰. 本文首先给出存在恶意导频干扰时基于最小二乘准则和最小均方误差准则的信道估计结果. 接着在数据信号传输阶段,根据获取的信道状态信息设计信号和人工噪声预编码矩阵,并推导基于人工噪声的系统安全速率公式. 然后,进一步研究半双工窃听方场景下基于数值分析和全双工场景下基于零和博弈的最优功率分配方案. 最后,用数值仿真具体分析窃听者位置、类型和干扰功率等因素对安全性能的影响,同时证明本文所提结论的正确性.

2　网络模型和问题提出

在一个三节点多天线复高斯网络中,存在一个发送方,一个合法接收方和一个窃听方,它们的天线数分别是 N_A,N_B 和 N_E,如图 1 所示.

当窃听方只窃听时,合法接收方和窃听方接收的信号分别为:

$$\boldsymbol{y}_B = \sqrt{\beta_{AB}}\boldsymbol{H}_{AB}\boldsymbol{x}_A + \boldsymbol{n}_B \tag{1}$$

$$\boldsymbol{y}_E = \sqrt{\beta_{AE}}\boldsymbol{H}_{AE}\boldsymbol{x}_A + \boldsymbol{n}_E \tag{2}$$

其中,假设各节点间的信道有大尺度路径损耗衰减和小尺度块衰落,用 $\sqrt{\beta_{kl}}\boldsymbol{H}_{kl}, k = A, B, E, l = A, B, E, k \neq l$ 表示节点 k 到节点 l 的信道状态信息,$\sqrt{\beta_{kl}} = \kappa(d_0/d_{kl})^{\alpha}$ 表示大尺度路径损耗衰减系数,d_0 是参考距离,d_{kl} 是两个节点间的距离,α 和 κ 为路劲损耗常数. $\boldsymbol{H}_{kl}$ 表示小尺度块衰落矩阵,假设它的每个参数是服从 $CN(0,1)$ 的复数,并且在一个传输块的时间内保持不变. 由于信道互易性,易得 $\boldsymbol{H}_{kl} = \boldsymbol{H}_{lk}^{\mathrm{T}}$. $\boldsymbol{n}_B$ 和 $\boldsymbol{n}_E$ 是合法接收方和窃听方的零均值、方差分别为 σ_B^2 和 σ_E^2 的独立加性复高斯噪声矩阵.

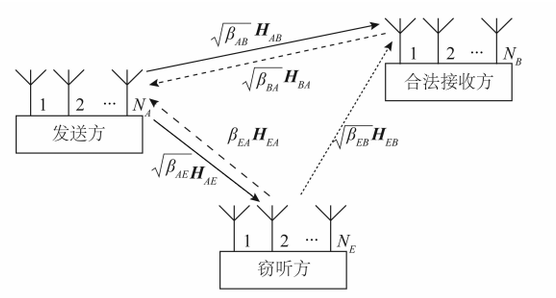


图 1　三节点窃听模型 A: 发送方, B: 合法接收方, E: 窃听方

当发送方同时发送信号和人工噪声来提高系统安全性能,通常假设发送方已知其到合法接收方的 CSI,并根据该 CSI 设计合适的信号和噪声预编码矩阵. $\boldsymbol{x}_A$ 是经过预编码后的信号和噪声,它可以表示为:

$$\boldsymbol{x}_A = \boldsymbol{T}\boldsymbol{z} + \boldsymbol{T}'\boldsymbol{z}' \tag{3}$$

其中,$\boldsymbol{T} \in \mathbb{C}^{N_A \times d}$ 是数据信号 $\boldsymbol{z}$ 预编码矩阵,$\boldsymbol{T}' \in \mathbb{C}^{N_A \times (N_A - d)}$ 是噪声 $\boldsymbol{z}'$ 预编码矩阵. d 是用于发送数据信号的维数,剩余的 $N_A - d$ 维用于发送人工噪声,P_A 是发送方的总发送功率.

为了实现人工噪声只对窃听方产生干扰,取 $\boldsymbol{T}$ 和 $\boldsymbol{T}'$ 分别为 $\boldsymbol{H}_{AB}$ 的子空间和零空间向量组,从而达到 $\boldsymbol{H}_{AB}\boldsymbol{T}' = 0$ 且 $\boldsymbol{H}_{AE}\boldsymbol{T}' \neq 0$.

然而在现实场景中,通常存在一个反向训练阶段信道,通过信道估计获取 CSI. 在信道估计的过程中,当存在一个主动干扰的窃听方时,假设该窃听方已知导频信号,且能实现与合法通信节点之间的同步. 于是在反向训练阶段,窃听方发送的导频干扰会显著影响信道估计结果,从而对系统安全性能造成影响. 针对该问题,本文将深入研究导频干扰对采用人工噪声方案系统的安全性能影响.

3　导频干扰对采用人工噪声方案系统的安全性能影响

本节主要分析导频干扰对采用人工噪声方案系统的安全性能影响. 在反向训练阶段,我们先分析窃听方发送恶意导频干扰时的信道估计结果;然后在数据传输阶段推导基于人工噪声的系统安全速率公式;最后研究半双工窃听方和全双工窃听方场景下的最优功率

分配方案.

3.1 反向训练阶段的信道估计

在反向训练阶段,合法接收方和窃听方用相同的天线数发送导频信号,发送方的接收信号可以表示为

$$\boldsymbol{y}_A = \sqrt{P_B\beta_{BA}}\boldsymbol{H}_{BA}\boldsymbol{x}_p + \sqrt{P_{Ep}\beta_{EA}}\boldsymbol{H}_{EA}\boldsymbol{x}_p + \boldsymbol{n}_A \tag{4}$$

其中,P_B 和 P_{Ep} 分别是合法接收方和窃听方发送导频信号的功率,$\boldsymbol{x}_p \in \mathbb{C}^{N_B\times 1}$ 是归一化的导频信号,即 $\boldsymbol{x}_p^{\mathrm{H}}\boldsymbol{x}_p = \boldsymbol{I}$. $\boldsymbol{n}_A \in \mathbb{C}^{N_A\times 1}$ 是加性高斯噪声矩阵.

当采用最小二乘信道估计[11]时,发送方以接收信号和估计结果间误差的二范数为代价函数,它只需要知道发送信号与接收信号,其估计值为

$$\hat{\boldsymbol{H}}_{BA} = \frac{\boldsymbol{y}_A\boldsymbol{x}_p^{\mathrm{H}}(\boldsymbol{x}_p\boldsymbol{x}_p^{\mathrm{H}})^{-1}}{\sqrt{P_B\beta_{BA}}} \tag{5}$$

由于最小二乘估计忽略了噪声的影响,信道估计结果对噪声干扰十分敏感. 假设发送方知道合法接收方的发送功率和接收信号的总功率,在线性最小均方误差准则[11]下的信道估计为

$$\begin{aligned}\hat{\boldsymbol{H}}_{BA} &= (\boldsymbol{R}_{\boldsymbol{H}_{BA}^{\mathrm{H}}\boldsymbol{y}_A^{\mathrm{H}}}\boldsymbol{R}_{\boldsymbol{y}_A^{\mathrm{H}}\boldsymbol{y}_A^{\mathrm{H}}}^{-1}\boldsymbol{y}_A^{\mathrm{H}})^{\mathrm{H}}\\ &= \frac{\sqrt{P_B\beta_{BA}}}{P_B\beta_{BA}+P_{Ep}\beta_{EA}+\sigma_A^2}\boldsymbol{y}_A\boldsymbol{x}_p^{\mathrm{H}}\\ &= \frac{P_B\beta_{BA}\boldsymbol{H}_{BA}}{P_B\beta_{BA}+P_{Ep}\beta_{EA}+\sigma_A^2} + \frac{\sqrt{P_B\beta_{BA}P_{Ep}\beta_{EA}}\boldsymbol{H}_{EA}}{P_B\beta_{BA}+P_{Ep}\beta_{EA}+\sigma_A^2}\\ &\quad + \frac{\sqrt{P_B\beta_{BA}}\boldsymbol{n}_A\boldsymbol{x}_p^{\mathrm{H}}}{P_B\beta_{BA}+P_{Ep}\beta_{EA}+\sigma_A^2}\end{aligned} \tag{6}$$

由上述分析可知,发送方到合法接收方之间的信道估计结果受到窃听方导频干扰的显著影响,该估计值是主信道 $\boldsymbol{H}_{BA}$ 和窃听信道 $\boldsymbol{H}_{EA}$ 的线性相加,且加权系数与发送功率成正相关. 当窃听方的导频干扰功率足够大,即满足 $P_B\beta_{BA} \ll P_{Ep}\beta_{EA}$,信道估计的结果 $\hat{\boldsymbol{H}}_{BA}$ 近似为窃听信道的线性加权,那么在下面的数据传输阶段,窃听方会对系统安全性能造成严重威胁.

3.2 基于人工噪声的数据信号传输

发送方在反向训练阶段获取合法节点间的 CSI 后,根据该 CSI 设计预编码矩阵. 此时,对反向训练阶段获取的 $\hat{\boldsymbol{H}}_{AB}$ 进行奇异值分解,取信号的预编码矩阵 $\hat{\boldsymbol{T}}$ 为 $\hat{\boldsymbol{H}}_{AB}$ 的右奇异向量组,取噪声的预编码矩阵 $\hat{\boldsymbol{T}}'$ 为 $\hat{\boldsymbol{H}}_{AB}$ 的零空间向量组[12].

为了推导安全速率公式,我们令 $\boldsymbol{T}_{AB}$ 和 $\boldsymbol{T}'_{AB}$ 分别为 $\boldsymbol{H}_{AB}$ 的子空间和零空间向量,$\boldsymbol{T}_{AE}$ 和 $\boldsymbol{T}'_{AE}$ 分别为 $\boldsymbol{H}_{AE}$ 的子空间和零空间向量组. 由于 $[\hat{\boldsymbol{T}}\quad\hat{\boldsymbol{T}}']$、$[\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]$ 和 $[\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]$ 是三个的基矩阵,则存在基变换矩阵 $\boldsymbol{C}_{AB}$,$\boldsymbol{C}_{AE} \in \mathbb{C}^{N_A\times N_A}$ 满足

$$[\hat{\boldsymbol{T}}\quad\hat{\boldsymbol{T}}'] = [\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]\boldsymbol{C}_{AB} = [\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]\boldsymbol{C}_{AE} \tag{7}$$

其中,矩阵 $\boldsymbol{C}_{AB}$ 和 $\boldsymbol{C}_{AE}$ 的差异由 $\hat{\boldsymbol{H}}_{BA}$ 中 $\boldsymbol{H}_{AB}$ 和 $\boldsymbol{H}_{AE}$ 的加权系数决定. 当 $P_B\beta_{BA} \ll P_{Ep}\beta_{EA}$,即 $\boldsymbol{H}_{AE}$ 的加权系数远大于 $\boldsymbol{H}_{AB}$ 的加权系数,则 $\boldsymbol{C}_{AE} \approx \boldsymbol{I}$,表示估计的信道 $\hat{\boldsymbol{H}}_{BA}$ 与窃听信道 $\boldsymbol{H}_{AE}$ 近似,他们右奇异矩阵也相近. 反之,则 $\boldsymbol{C}_{AB} \approx \boldsymbol{I}$. 当不满足上述情况,那么 $[\hat{\boldsymbol{T}}\quad\hat{\boldsymbol{T}}']$ 这个基矩阵在 $[\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]$ 和 $[\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]$ 这两个基矩阵上的映射主要取决于 $\boldsymbol{H}_{AB}$ 和 $\boldsymbol{H}_{AE}$ 的加权系数.

将 $\boldsymbol{C}_{AB}$ 分块为 $\boldsymbol{C}_{AB} = [\boldsymbol{C}_{AB}^1\quad\boldsymbol{C}_{AB}^2]$,$\boldsymbol{C}_{AB}^1 \in \mathbb{C}_d^{N_A\times d}$,$\boldsymbol{C}_{AB}^2 \in \mathbb{C}_{N_A-d}^{N_A\times(N_A-d)}$,同理将 $\boldsymbol{C}_{AE}$ 分块为 $\boldsymbol{C}_{AE} = [\boldsymbol{C}_{AE}^1\quad\boldsymbol{C}_{AE}^2]$,$\boldsymbol{C}_{AE}^1 \in \mathbb{C}_d^{N_A\times d}$,$\boldsymbol{C}_{AE}^2 \in \mathbb{C}_{N_A-d}^{N_A\times(N_A-d)}$,则 $\hat{\boldsymbol{T}}$ 和 $\hat{\boldsymbol{T}}'$ 可以表示为

$$\begin{aligned}\hat{\boldsymbol{T}} &= [\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]\boldsymbol{C}_{AB}^1 = [\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]\boldsymbol{C}_{AE}^1\\ \boldsymbol{T}' &= [\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]\boldsymbol{C}_{AB}^2 = [\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]\boldsymbol{C}_{AE}^2\end{aligned} \tag{8}$$

结合式(3)和(7),式(1)和(2)可变为

$$\begin{aligned}\boldsymbol{y}_B &= \sqrt{\beta_{AB}}\boldsymbol{H}_{AB}(\hat{\boldsymbol{T}}\boldsymbol{z}+\boldsymbol{T}'\boldsymbol{z}') + \boldsymbol{n}_B\\ &= \sqrt{\beta_{AB}}\boldsymbol{H}_{AB}([\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]\boldsymbol{C}_{AB}^1\boldsymbol{z} + [\boldsymbol{T}_{AB}\quad\boldsymbol{T}'_{AB}]\boldsymbol{C}_{AB}^2\boldsymbol{z}') + \boldsymbol{n}_B\\ &= \sqrt{\beta_{AB}}\boldsymbol{H}_{AB}\boldsymbol{T}_{AB}(\boldsymbol{C}_{AB}^{11}\boldsymbol{z} + \boldsymbol{C}_{AB}^{22}\boldsymbol{z}') + \boldsymbol{n}_B\end{aligned} \tag{9}$$

$$\begin{aligned}\boldsymbol{y}_E &= \sqrt{\beta_{AE}}\boldsymbol{H}_{AE}(\hat{\boldsymbol{T}}\boldsymbol{z}+\boldsymbol{T}'\boldsymbol{z}') + \boldsymbol{n}_E\\ &= \sqrt{\beta_{AE}}\boldsymbol{H}_{AE}([\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]\boldsymbol{C}_{AE}^1\boldsymbol{z} + [\boldsymbol{T}_{AE}\quad\boldsymbol{T}'_{AE}]\boldsymbol{C}_{AE}^2\boldsymbol{z}') + \boldsymbol{n}_E\\ &= \sqrt{\beta_{AE}}\boldsymbol{H}_{AE}\boldsymbol{T}_{AE}(\boldsymbol{C}_{AE}^{11}\boldsymbol{z} + \boldsymbol{C}_{AE}^{22}\boldsymbol{z}') + \boldsymbol{n}_E\end{aligned} \tag{10}$$

其中,$\boldsymbol{C}_{AB}^{11} \in \mathbb{C}^{d\times d}$ 为 $\boldsymbol{C}_{AB}^1$ 的上分块方阵,$\boldsymbol{C}_{AB}^{22} \in \mathbb{C}^{d\times(N_A-d)}$ 为 $\boldsymbol{C}_{AB}^2$ 的上分块矩阵,$\boldsymbol{C}_{AE}^{11}$ 和 $\boldsymbol{C}_{AE}^{22}$ 也类似.

为了简化研究,假设用于发送信号的功率为 P_{sig},而用于发送噪声的功率为 $P_S - P_{\mathrm{sig}}$,P_S 是发送方的总功率,且节点在所有维度上均匀分配功率. 于是窃听方仅仅窃听时,安全速率的公式为[13]

$$\begin{aligned}R_S = \varepsilon_h\{&\log_2|\boldsymbol{I} + P_{\mathrm{sig}}\beta_{AB}\boldsymbol{H}_{AB}\boldsymbol{T}_{AB}\boldsymbol{C}_{AB}^{11}\boldsymbol{C}_{AB}^{11\,\mathrm{H}}\boldsymbol{T}_{AB}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}}\boldsymbol{K}_B^{-1}/d|\\ &-\log_2|\boldsymbol{I} + P_{\mathrm{sig}}\beta_{AE}\boldsymbol{H}_{AE}\boldsymbol{T}_{AE}\boldsymbol{C}_{AE}\boldsymbol{C}_{AE}^{H}\boldsymbol{T}_{AE}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}}\boldsymbol{K}_E^{-1}/d|\}\end{aligned} \tag{11}$$

其中,$\boldsymbol{K}_B$ 和 $\boldsymbol{K}_E$ 为合法接收方和窃听方的干扰噪声协方差矩阵,可以表示为

$$\begin{aligned}\boldsymbol{K}_B &= P_{\mathrm{sig}}\beta_{AB}\boldsymbol{H}_{AB}\boldsymbol{T}_{AB}\boldsymbol{C}_{AB}^{22}\boldsymbol{C}_{AB}^{22\,\mathrm{H}}\boldsymbol{T}_{AB}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}}/d + \sigma_B^2\boldsymbol{I}\\ \boldsymbol{K}_E &= P_{\mathrm{sig}}\beta_{AE}\boldsymbol{H}_{AE}\boldsymbol{T}_{AE}\boldsymbol{C}_{AE}^{22}\boldsymbol{C}_{AE}^{22\,\mathrm{H}}\boldsymbol{T}_{AE}^{\mathrm{H}}\boldsymbol{H}_{AE}^{\mathrm{H}}/d + \sigma_E^2\boldsymbol{I}\end{aligned} \tag{12}$$

当面临的是全双工窃听方时,在数据传输阶段,窃听方同样也能发送噪声干扰,假设窃听方在接收信号中能消除该噪声干扰[14]. 在一个传输块中,窃听方的总功率受限,即窃听方在反向训练阶段用于发送导频干扰功率 P_{Ep} 和在数据传输阶段用于发送噪声干扰的功率 P_{Ed} 满足 $P_{Ep} + P_{Ed} \leqslant P_E$. 由于导频干扰和噪声干扰都能实现提高窃听性能,窃听方会完全分配总功率 P_E,实现 $P_{Ep} + P_{Ed} = P_E$.

当窃听方同时发送导频干扰和噪声干扰,在数据传输阶段,合法接收方的接收信号变为

$$\boldsymbol{y}_B = \sqrt{\beta_{AB}}\boldsymbol{H}_{AB}\boldsymbol{x}_A + \sqrt{\beta_{EB}}\boldsymbol{H}_{EB}\boldsymbol{x}_E + \boldsymbol{n}_B \tag{13}$$

其中,$\boldsymbol{x}_E$ 是窃听方发送的高斯噪声干扰. 则合法接收方的干扰噪声协方差矩阵变为

$$\boldsymbol{K}_B = P_{\mathrm{sig}}\beta_{AB}\boldsymbol{H}_{AB}\boldsymbol{T}_{AB}\boldsymbol{C}_{AB}^{22}\boldsymbol{C}_{AB}^{22\,\mathrm{H}}\boldsymbol{T}_{AB}^{\mathrm{H}}\boldsymbol{H}_{AB}^{\mathrm{H}}/d$$

$$+P_{Ed}\boldsymbol{\beta}_{EB}\boldsymbol{H}_{BE}\boldsymbol{H}_{BE}^{\mathrm{H}}/N_B+\sigma_B^2\boldsymbol{I} \tag{14}$$

3.3 发送方和半双工窃听方的功率分配

当窃听方是半双工窃听方,它在反向训练阶段发送导频干扰,在正向传输阶段仅窃听时,所有的干扰功率被用于发送导频干扰. 发送方在功率约束条件下,通过分配合适的信号功率和噪声功率来增大系统安全速率. 于是,该功率分配方案变为解决以下最优化问题

$$\begin{aligned} &R_S=\max_{P_{\mathrm{sig}}}R_S(P_{\mathrm{sig}})\\ &\text{s.t. } 0\leqslant P_{\mathrm{sig}}\leqslant P_S \end{aligned} \tag{15}$$

针对该最优化问题,由于窃听方的导频干扰使信道估计结果为主信道和窃听信号的线性相加. 当 $P_B\beta_{BA}\leqslant P_{Ep}\beta_{EA}$ 时,即窃听信道的加权系数大于主信道的加权系数,那么发送方发送的信号和人工噪声都对窃听方更有利,此时对任意的 $P_{\mathrm{sig}}\leqslant P_S$,安全速率值都为零.

当满足 $P_B\beta_{BA}\geqslant P_{Ep}\beta_{EA}$ 时,即信道估计结果中的主信道权值更大,人工噪声可以发挥其原来的作用. 我们首先通过对 $R_S(P_{\mathrm{sig}})$ 求 P_{sig} 的二阶导得出,在约束条件下二阶导数不是恒小于零,所以这不是一个凸优化问题,不能得到最优分配功率的解析表达式. 于是,用数值分析的方法令 $P_{\mathrm{sig}}=[0,\Delta_{P_{\mathrm{sig}}},\cdots,P_S-\Delta_{P_{\mathrm{sig}}},P_S]$,得到对应功率分配下的系统安全速率,然后遍历寻找最大值从而获取最优的功率分配值及其对应的安全速率值. 本文将在数值仿真中分析半双工窃听方对系统安全性能的影响.

3.4 发送方和全双工窃听方的功率分配

由于全双工窃听方通过分配导频功率和噪声功率降低安全速率,而发送方发送的信号和人工噪声提高安全速率如式(12)所示,针对这种存在竞争关系的物理层安全问题,本小节用博弈的方法进行分析. 先将发送方和窃听方建立成一个以安全速率为目标函数的零和博弈,然后通过求解纳什均衡解,得到发送方和全双工窃听方各自最优的功率分配值及其对应的安全速率值.

$$\begin{aligned} &R_S(P_{\mathrm{sig}},P_{Ep})=\max_{P_{\mathrm{sig}}}\min_{P_{Ep}}R_S(P_{\mathrm{sig}},P_{Ep})\\ &\text{s.t. } 0\leqslant P_{\mathrm{sig}}\leqslant P_S,0\leqslant P_{Ep}\leqslant P_E \end{aligned} \tag{16}$$

首先根据功率约束,确定发送方和窃听方的混合策略空间 $\boldsymbol{\Psi}$ 和 $\boldsymbol{\Phi}$

$$\begin{aligned} \boldsymbol{\Psi}&=\{0,\Delta_S,2\Delta_S,\cdots,P_S-\Delta_S,P_S\}\\ \boldsymbol{\Phi}&=\{0,\Delta_E,2\Delta_E,\cdots,P_E-\Delta_E,P_E\} \end{aligned} \tag{17}$$

针对该有限离散博弈,每个策略空间中的值(P_{sig},P_{Ep})对应一个非负的安全速率 $R_S(P_{\mathrm{sig}},P_{Ep})$,于是得到一个二维非负收益矩阵 A. 其中,$A(i,j)=R_S(P_{\mathrm{sig}},P_{Ep})$.

令发送方以概率 $\boldsymbol{p}=(p_1,p_2,\cdots,p_{n_S})$ 取策略集 $\boldsymbol{\Psi}$ 中的功率值,n_S 是 P_{sig} 的离散值个数,窃听方以概率 $\boldsymbol{q}=(q_1,q_2,\cdots,q_{n_\rho})$ 取策略集 $\boldsymbol{\Phi}$ 中的离散值,n_E 为 P_{Ep} 的离散值个数. 当 n_S 和 n_E 的值越大,混合策略均衡的分析和求解过程越精确,但是复杂度也会越高.

于是,混合策略下的安全速率为

$$\begin{aligned} &R_S(p_1,\cdots,p_{n_S},q_1,\cdots,q_{n_\rho})=\boldsymbol{p}^{\mathrm{T}}R_S(P_{\mathrm{sig}_i},\boldsymbol{\rho}_j)\boldsymbol{q}\\ &\text{s.t. }\sum_{i=1}^{n_S}p_i=1,\sum_{j=1}^{n_\rho}q_j=1 \end{aligned} \tag{18}$$

针对该收益矩阵,发送方通过确定 $\boldsymbol{p}=(p_1,p_2,\cdots,p_{n_S})$ 来增大系统安全速率,窃听方通过 $\boldsymbol{q}=(q_1,q_2,\cdots,q_{n_\rho})$ 降低系统安全速率. 由文献[15]的极大极小定理可知,如果存在一个非负数 v,使得对任意的 j 有 $\sum_{i=1}^{n_S}A_{ij}p_i\geqslant v$,对任意的 i 有 $\sum_{j=1}^{n_\rho}A_{ij}q_j\leqslant v$,那么($\boldsymbol{p}^*$,$\boldsymbol{q}^*$)是该博弈的混合策略均衡.

由于 $\boldsymbol{A}$ 是一个非负的收益矩阵,那么 v 是非负数,令 $a_i=p_i/v,i=1,\cdots,n_S;b_j=q_j/v,j=1,\cdots,n_\rho$,根据文献[15]的定理,该零和博弈的混合策略纳什均衡可以通过以下对偶线性规划问题的求解.

$$\begin{aligned} &\min\sum_{i=1}^{n_S}a_i\\ &\text{s.t. }\sum_{i=1}^{m}\boldsymbol{A}_{ij}a_i\geqslant 1,j=1,\cdots,n_E;\\ &\qquad 0\leqslant a_i;i=1,\cdots,n_S \end{aligned} \tag{19}$$

该最优化解得出 $\boldsymbol{p}=(va_1,va_2,\cdots,va_{n_S})$ 为发送方发送源信号功率的概率分布.

$$\begin{aligned} &\max\sum_{j=1}^{n_E}b_j\\ &\text{s.t. }\sum_{j=1}^{n_\rho}A_{ij}b_j\leqslant 1,i=1,\cdots,n_S;\\ &\qquad 0\leqslant b_j;j=1,\cdots,n_E \end{aligned} \tag{20}$$

该最优化解得出 $\boldsymbol{q}=(vb_1,vb_2,\cdots,vb_{n_E})$ 为均衡时恶意干扰者线性系数的概率分布,而最终的混合策略均衡值为

$$R_S=v=\frac{1}{\sum_{i=1}^{n_S}a_i}=\frac{1}{\sum_{j=1}^{n_E}b_j} \tag{21}$$

4 数值仿真与安全性能分析

本章用数值仿真分析导频干扰对系统安全性能的影响. 在此次仿真在一个 1km × 1km 的区域中,发送方和合法接收方的位置坐标为(-250m,0)和(250m,0),窃听方的位置是(0,500m),参考距离 $d_0=1$m,路径衰减常数 $\alpha=2,\kappa=1$. 令节点的天线数和功率分别为 $N_A=7,N_B=N_E=4,P_A=P_B=P_E=100$mW,噪声功率 -40dBm,离散个数 $n_S=n_E=20$.

图 2 分析了系统安全速率随窃听方位置的变化. 当固定发送方和合法接收方的位置,横坐标表示的是窃听方从(-250m,500m)到(250m,500m)直线移动的过程. 当窃听方只窃听或发送导频干扰时,由于窃听方远离发送方,所以窃听效果或导频干扰效果变差而安全速率逐渐增加. 当窃听方不发送导频干扰,在数据传输阶段发送噪声干扰并窃听时,安全速率较纯窃听时明显降低. 该曲线先降低后慢慢提高的趋势是窃听方噪声干扰和窃听效果的叠加. 在从(-250m,500m)到(0m,500m)的过程中,发送噪声产生的干扰性能要优于窃听方由于距离增加而降低的窃听性能,所以安全速率随之减小. 而从(0m,500m)到(250m,500m)的过程,则相反,于是安全速率随之增加. 另外,当窃听方的位置是(0m,500m)时,窃听方离发送方和合法接收方的距离相等,可以看出在相同的干扰功率下,导频干扰达到的安全速率比噪声干扰的要小.

图 3 和图 4 描绘了半双工窃听方对系统安全性能的影响. 此时,为了适当增大窃听方的能力,横坐标表示的是窃听方从(-250m,400m)到(250m,400m)直线移动的过程. 图 3 分析了安全速率随窃听位置的变化,可以看出当窃听方的位置在(50m,400m)之后,安全速率的值从零开始逐渐增大. 在仿真条件下,这个位置对应的是 $P_B\beta_{BA} = P_{Ep}\beta_{EA}$ 的条件,所以当存在导频干扰时,只有保证合法接收方的到达的导频功率大于窃听方到达的功率,系统才能有非负的安全速率值. 图 4 给出最优信号功率随窃听位置的影响,最优的信号功率一开始保持为零,其原因是当 $P_B\beta_{BA} \leqslant P_{Ep}\beta_{EA}$ 时,发送方无法实现安全速率大于零. 从(50m,400m)这个位置开始,发送方的信号功率在短距离内快速增大,并趋于用全功率发送信号,这是因为存在导频干扰后,发送方发送的人工噪声不足以有效干扰窃听方,发送方发送信号对系统性能的提升更有效.

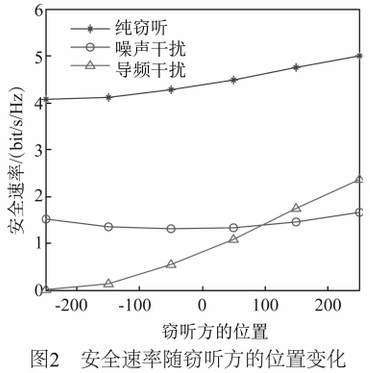


图2 安全速率随窃听方的位置变化

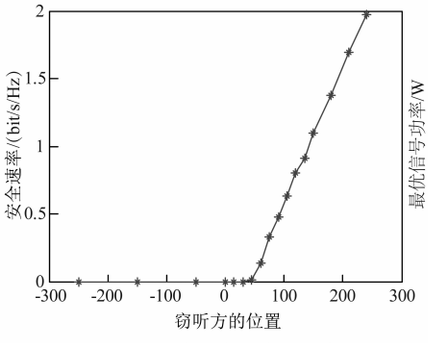


图3 半双工窃听方下安全速率随窃听位置的变化

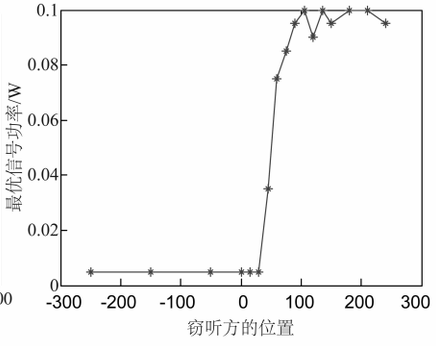


图4 半双工窃听方下最优信号功率随窃听位置的变化

图 5 和图 6 描绘了全双工窃听方对安全性能的影响. 图 5 分析了安全速率随窃听位置和干扰总功率的影响. 当窃听方的干扰功率固定,安全速率随着窃听方远离发送方而增加,主要是因为导频干扰性能随着窃听方远离发送方的降低程度比噪声干扰提高的程度要大. 值得注意的是,当窃听方的干扰功率为 0. 1W 时,有

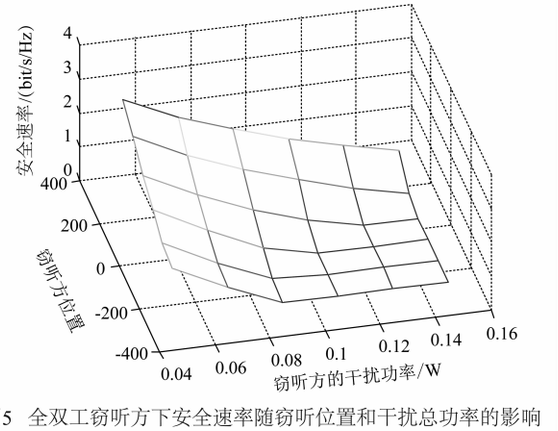


图5 全双工窃听方下安全速率随窃听位置和干扰总功率的影响

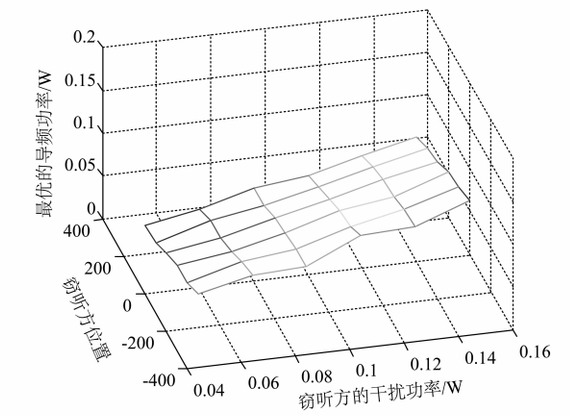


图6 全双工窃听方下最优的导频功率随窃听位置和干扰总功率的变化

部分安全速率的值已经为零,而相同条件下图 2 中导频干扰对应的安全速率值都大于零,这说明全双工窃听方比半双工窃听方的干扰能力更强. 图 6 给出最优的导频功率随窃听位置和干扰总功率的变化. 当固定

窃听方的位置为(0m,500m)时,无论干扰功率如何变化,窃听方会用大于一半的功率发送导频干扰.

5 结论

针对存在一个发送方,一个合法接收方和一个窃听方的三节点 MIMO 网络,发送方通过发送信号和人工噪声提高系统安全性能,然而具有主动干扰能力的窃听方在反向训练阶段同时发送导频,干扰发送方的信道估计结果,从而达到降低系统安全性能. 本文首先研究 MIMO 场景下导频干扰对信道估计的影响,发现信道估计结果是主信道和窃听信道的线性相加,且增大导频干扰功率能同时降低合法接收质量和提高窃听性能. 接着进一步推导系统安全速率公式,同时研究半双工窃听方和全双工窃听方场景下的最优功率分配方案,得出只有满足窃听方到达发送方的导频干扰功率大于合法接收方达到的功率时,安全速率值才能是非负值. 最后,用数值仿真分析导频干扰对系统安全速率的影响.

参考文献

[1] A D Wyner. The wire-tap channel[J]. Bell System Technical Journal,1975,54(8):1355 – 1387.

[2] M Bloch,M Debbah. Special issue on physical-layer security[J]. Journal of Communications and Networks,2012,14(4):349 – 351.

[3] P H Lin,S H Lai. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels [J]. IEEE Journal on Selected Areas in Communications, 2013,31(9):1728 – 1740.

[4] T H Chou,S C Draper. Secret key generation from sparse wireless channels:ergodic capacity and secrecy outage[J]. IEEE Journal on Selected Areas in Communications,2013, 31(9):1751 – 1764.

[5] G Dziwoki,W Sulek. Subchannel ordering scheme for LDPC-coded OFDM transmission over selective channels [A]. International Conference on Telecommunications and Signal Processing[C]. Rome:IEEE,2013. 66 – 70.

[6] S Goel,R Negi. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008,7(6):2180 – 2189.

[7] Xiangyun Zhou, Behrouz Maham. Pilot contamination for active eavesdropping[J]. IEEE Transactions on Wireless Communications,2012,11(3):903 – 907.

[8] M Yuksel,E Erkip. Analysis and design of channel estimation in multi-cell multi-user MIMO OFDM systems[J]. IEEE Transactions on Vehicular Technology,2014,64(2): 610 – 620.

[9] Hao Li, Xianbin Wang. Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems [J]. IEEE Communications Letters, 2014, 18(6): 1059 – 1062.

[10] H Paik, N Sastry. Effectiveness of noise jamming with white Gaussian noise and phase noise in amplitude comparison monopulse radar receivers[A]. IEEE International Conference on Electronics, Computing and Communication Technologies[C]. Bangalore:IEEE,2014. 1 – 5.

[11] S M Kay. Fundamentals of Statistical Signal Processing: Estimation Theory[M]. New jersery:Prentice Hall,1993.

[12] A Mukherjee, A L Swindlehurst. Jamming games in the MIMO wiretap channel with an active eavesdropper[J]. IEEE Transactions on Signal Processing,2013,61(1):82 – 91.

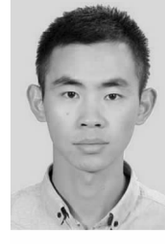
[13] A Mukherjee, A L Swindlehurst. Optimal strategies for countering dual-threat jamming/eavesdropping capable adversaries in MIMO channels[A]. IEEE Military Communication[C]. San Jose:IEEE,2010. 476 – 481.

[14] Gan Zheng, Ioannis Krikidis, Jiangyuan Li. Improving physical layer secrecy using full-duplex jamming receivers[J]. IEEE Transactions on Signal Processing,2013,61 (20):4962 – 4974.

[15] Tamer Basar,Geert Jan Olsder. Dynamic Non-cooperative Game Theory[M]. Second Edition. New York:Academic Press,1995.

作者简介

沈利华　女,1978 年生,浙江绍兴人,现为浙江工业大学之江学院副教授,硕士,主要研究领域为网络安全、算法设计和无线通信技术.
E-mail:shenlihua777@tom.com



林胜斌　男,1990 年生,浙江温州人,硕士生,研究方向为移动通信、物理层安全.
E-mail:realbinforever@163.com

黄开枝　女,1973 年生,安徽来安人,现为国家数字交换系统工程技术研究中心教授,博士生导师,主要研究领域为无线与移动通信、无线物理层安全技术、异构无线网络安全等.
E-mail:huangkaizhi@tsinghua.org.cn