计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(11):217−223 [doi: 10.15888/j.cnki.csa.008171]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

以用户为中心的超密集网络中窃听用户检测技术①

王国栋, 潘　鹏, 胡　松

(杭州电子科技大学 通信工程学院, 杭州 310018)
通讯作者: 潘　鹏, E-mail: panpeng@hdu.edu.cn

摘　要: 在以用户为中心的超密集网络 (User-centric Ultra-Dense Networking, UUDN) 中, 由于进行信道估计的导频序列长度有限, 导致传统的基于信息论准则的窃听检测技术效果不理想甚至完全失效. 针对这种情况, 提出了一种基于 LS-FDC 准则的多节点联合检测算法. 首先, 该方法利用统计学中的线性收缩 (Linear Shrinkage, LS) 理论, 对各节点接收到的样本协方差矩阵进行收缩优化, 使其特征分解后更好的拟合总体特征值的分布情况; 然后, 接入节点组 (Access Points Group, APG) 中的各节点利用灵活检测准则 (Flexible Detection Criterion, FDC) 算法进行联合判定是否存在窃听用户; 最后, 仿真实验与理论分析表明: 相较于其他的信源估计检测算法, 该算法在较低信噪比和导频序列长度有限时的检测概率显著提高, 甚至在导频序列长度小于节点天线数的情况下都能达到很好的检测效果.

关键词: 以用户为中心的超密集网络; 大规模 MIMO; 主动窃听; 线性收缩; 时分双工

引用格式: 王国栋,潘鹏,胡松.以用户为中心的超密集网络中窃听用户检测技术.计算机系统应用,2021,30(11):217–223. http://www.c-s-a.org.cn/1003-3254/8171.html

Eavesdropper Detection Technology in User-Centric Ultra-Dense Network

WANG Guo-Dong, PAN Peng, HU Song

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

Abstract: In the User-centric Ultra-Dense Network (UUDN), due to the limited length of the pilot sequence for channel estimation, the traditional eavesdropping detection technology based on information theoretic criteria cannot function ideally or is even completely invalid. In view of this, this study proposes a multi-node joint detection algorithm based on the LS-FDC criterion. This method uses the Linear Shrinkage (LS) theory in statistics to shrink and optimize the sample covariance matrix received by each node so that it can better fit the distribution of the overall eigenvalues after eigen-decomposition. The nodes in the Access Point Group (APG) jointly determine whether there are eavesdroppers with the Flexible Detection Criterion (FDC) algorithm. The simulation experiments and theoretical analysis show that compared with other algorithms for signal source estimation and detection, this algorithm has a significantly improved detection probability when the signal-to-noise ratio is low and the pilot sequence length is limited. A good detection effect can still be achieved even when the pilot sequence length is shorter than the number of node antennas.

Key words: User-centric Ultra Dense Network (UUDN); massive MIMO; active eavesdropping; linear contraction; time division duplex

近几年随着流量密集型应用的普及, 如物联网、自动驾驶、高清视频播放等, 大大增加了现有通信网络的负担. 因此, 为了满足用户的巨大流量需求, 在 5G 中提出了以用户为中心的超密集网络 (User-centric Ultra-

① 基金项目: 国家自然科学基金 (61372093, 61401130)
Foundation item: National Natural Science Foundation of China (61372093, 61401130)
收稿时间: 2021-01-30; 修改时间: 2021-02-26; 采用时间: 2021-03-11; csa 在线出版时间: 2021-10-22

Dense Networking, UUDN) 架构. UUDN 通过灵活地组织所需网络资源, 构建以用户为中心的动态网络资源池, 形成了“智能的网络感知用户、动态的网络服务用户、安全的网络保障用户”新特性, 实现了“网随人动”的服务效果, 从而满足更高的网络容量和更好的用户体验[1,2]. 但是, UUDN 架构中, 接入节点 (Access Point, AP) 变得更加小型化, 部署更加灵活, 甚至允许用户自行部署, 从而导致信道的物理环境复杂多变, 存在非法或恶意窃听的可能性更高, 信息传输受到严重的威胁.

非法用户的窃听方式灵活多变, 根据有无干扰信号发送, 主要可以分为被动窃听和主动窃听两种方式. 在被动窃听模式下, 窃听者不对外发送任何干扰信号, 只是被动接收发送节点传输的数据, 然后通过自身强大的处理能力对接收数据进行解析, 以非法获取有用信息. UUDN 系统架构中, 由于大规模 MIMO 天线技术的使用, 节点天线的波束赋形能力大大提高, 可以使无线信号的传播路径精确对准合法用户, 从而显著提高被动窃听的难度, 保障无线通信的数据安全[3]; 但是, 随着第三方窃听设备功能的增强, 窃听者可以通过主动窃听的方式对合法用户的信息进行窃取. 在时分双工 (Time Division Duplex, TDD) 模式下, 合法用户发送导频序列到节点端, 节点根据信道的互异性来估计下行信道状态信息 (Channel State Information, CSI). 此时, 主动窃听者可以通过窃取合法用户的导频序列, 随合法用户向节点同步发送, 以干扰节点与合法用户之间的信道估计, 进而在下行数据传输中获取偏向自身的信号分量, 达到窃取合法信息的目标[4].

1 UUDN 系统的主动窃听模型

目前针对主动窃听场景, 传统蜂窝网络中, 一般采用上层加密技术保证传输数据的安全, 即通过编码技术或密钥将有用信息隐藏, 增加窃听者的破解难度. 但是随着移动终端等设备处理能力的增强, 以及大数据技术的不断发展, 窃听者破解信息的难度逐渐降低, 加密技术已经不能满足数据传输的安全需求. 所以, 利用无线信道广播特性的物理层安全技术逐渐兴起, 吸引了大量学者对此进行研究, 并取得了一定的研究成果. 后者直接在物理层层面进行保密研究, 既不涉及复杂的密码计算, 也不过分要求通信实体的处理能力, 大大降低了 UUDN 中低功耗、低成本小型节点和移动终端的负担[5,6]. 因此, 物理层安全技术在 UUDN 中具有广阔的前景.

针对主动窃听者的检测, 近年来, 学者们提出了许多种方法. 文献 [7] 中, 作者利用 PSK 信号代替公共导频序列, 接收节点通过分析两次接收信号叠加的相位信息来判断是否存在主动窃听现象; 文献 [8] 中, 作者提出一种能量比检测方案, 即节点接收到导频序列后, 再以与用户相同功率将接收信号的功率信息发送给合法用户, 合法用户利用两者的接收信号功率之比作为检测统计量进行分析, 进而判断是否存在主动窃听现象. 文献 [9] 中, 作者提出了基于接收功率与噪声功率比的检测方法, 但是该方法需要提前获知噪声信息. 以上这些方法均需要经过两次传输才能够进行检测, 不仅浪费资源, 而且非常耗时, 不适合在 UUND 系统中采用. 最近的研究大多是基于信息论准则进行展开, 它的优点是可以在参数变化环境中自适应地检测窃听用户. 文献 [10–12] 给出了一种最小描述长度 (Minimum Description Length criterion, MDL) 的信源估计算法, 该算法的核心思想是通过推断接收信号协方差矩阵中噪声特征值的个数来估计出信源数目, 进而判断有无主动窃听者的存在. 但是, MDL 算法在信噪比相对较低时会产生欠估计的问题. 文献 [13,14] 中提出了一种灵活检测准则 (Flexible Detection Criterion, FDC) 算法, 该算法是在贝叶斯理论 (Bayesian Information Criterion, BIC) 基础上引入了一个可以灵活调整的参数, 通过寻找参数的最佳值来减少信源数目低估和高估的风险, 相较于 MDL 算法有了明显的提高. 通过信源估计算法进行窃听用户检测的前提是导频序列长度趋于无穷大, 而在实际中, 导频的样本数目有限, 导致最终的检测效果不理想, 所以在 UUDN 系统中进行窃听用户检测时, 需要对该方法进行改进.

基于以上的研究, 本文借鉴统计学中的线性收缩 (Linear Shrinkage, LS) 理论[15], 对 FDC 信源估计算法进行了优化, 并且利用 APG 中的多个 AP 进行联合检测, 进一步提高了检测概率. 仿真结果证明较传统的 MDL、FDC 等算法, 本文方法的性能具有明显的提升, 尤其是在导频样本数小于 AP 天线数的极限情况下, 具有明显的优势.

1.1 UUDN 系统模型

本文参考的 UUDN 系统模型如图 1 所示, 主要由以下几部分组成: 在一定的区域范围内, N 个配备了 M 根天线的小型接入节点 (APs) 采用泊松点过程 (PPP)

的方式分布在该区域内; 配备了单根天线的合法用户 (Bob) 以及窃听用户 (Eve) 采用随机的方式分布在该区域内; 节点与用户之间的信道采用时分双工模式.

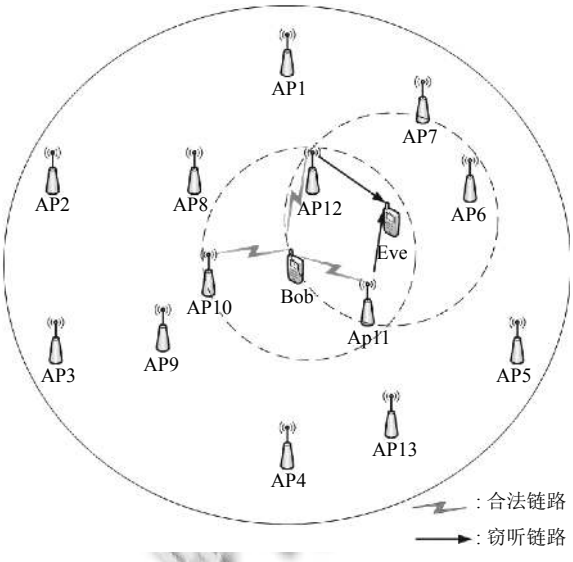

图 1 UUDN 系统模型

该系统模型下, Bob 首先根据信号传输范围的大小, 确定能够连接到的接入节点, 然后这些节点组成 APG 共同服务于 Bob. 根据主动窃听原理, Bob 向 APG 中的所有节点发送一段公共导频序列, 此时的 Eve 通过窃取 Bob 的导频序列, 与 Bob 同步向所有连接节点发送, 进而干扰 Bob 与 APs 之间的信道估计.

本文采用均值为零且独立同分布的归一化 BPSK 随机序列作为公共导频, 则 Bob 到 APG 中第i个节点AP_i的信道系数矩阵为$H_{BA_i}=\sqrt{d_{BA_i}}\tilde{h}_{BA_i}\in C^{M\times 1}$; 附近的 Eve 如果同样能够连接到该节点, 那么 Eve 到节点AP_i的信道系数矩阵为$H_{EA_i}=\sqrt{d_{EA_i}}\tilde{h}_{EA_i}\in C^{M\times 1}$. 其中, d_{BA_i}、d_{EA_i}分别表示 Bob、Eve 到AP_i的大规模路径损耗; $\tilde{h}_{BA_i}\sim CN(0,I_M)$、$\tilde{h}_{EA_i}\sim CN(0,I_M)$分别表示 Bob、Eve 到$AP_i$信道的小尺度衰落矢量[12], 它们都服从均值为 0, 方差为I_M的循环对称复高斯分布.

假设H_0表示没有主动窃听时的情况, H_1表示存在主动窃听时的情况, 则AP_i接收到的信号矩阵为:

$$H_0: y_i(n)=H_{BA_i}\left(\sqrt{P_B(1-\beta)}x_B(n)+\sqrt{P_B\beta}x_t(n)\right)+v_i(n) \tag{1}$$

$$H_1: y_i(n)=H_{BA_i}\left(\sqrt{P_B(1-\beta)}x_B(n)+\sqrt{P_B\beta}x_t(n)\right)+\sqrt{P_E}H_{EA_i}x_E(n)+v_i(n) \tag{2}$$

其中, P_B、P_E分别为 Bob 和 Eve 的发送功率, $v(n)\sim CN\left(0,\sigma^2 I_M\right)$表示均值为 0, 方差为$\sigma^2$的循环对称复高斯分布的随机噪声矢量, $x_B(n)=x_E(n)\in C^{N\times 1}$分别为 Bob 和 Eve 发送的长度为 N 的公共导频序列, $x_t(n)\in C^{N\times 1}(0<\beta<1, 1\le n\le N)$ 是 Bob 端叠加的随机导频序列, 由于是随机生成的, 所以对于 Eve 来说是未知的[10].

1.2 问题描述

为了简化公式, 下面对 APG 中所有服务 AP 的接收矩阵进行统一表述. 当 AP 的天线数 M 固定, 导频长度$N\to\infty$时, 每个 AP 接收信号的总体协方差矩阵为$R_{y,j}(j=0,1)$:

$$R_{y,j}=\frac{1}{N}E\left\{y(n)y^H(n)|H_j\right\} \tag{3}$$

然后, 对协方差矩阵$R_{y,j}$进行特征值求解, 得到总体特征值分布λ_i, $i=1,2,\cdots,M$, 降序排列, 满足如下关系:

$$\lambda_1\ge\lambda_2\ge\cdots\ge\lambda_k>\lambda_{k+1}=\cdots=\lambda_M=\sigma^2 \tag{4}$$

其中, 前 k 个特征值是信号和噪声共同作用的结果, 称为信号特征值, 剩余的$M-k$个特征值只与噪声有关, 称为噪声特征值. 但是, 实际中由于导频长度 N 受限的影响, 往往只能以样本协方差矩阵去估计总体协方差矩阵, 样本协方差矩阵为:

$$\hat{R}_{y,j}=\frac{1}{N}\sum_{n=1}^{N}y(n)y^H(n)(j=0,1) \tag{5}$$

对上式进行特征分解, 可以得到样本特征值分布$\lambda_1\ge\lambda_2\ge\cdots\ge\lambda_M>0$, $i=1,2,\cdots,M$.

得到样本特征值之后, 就可以使用 MDL、FDC 等信源估计算法来估计是否存在主动窃听.

另外, 相对于传统的单节点-单用户的系统模型, 在 UUDN 系统中, 多个 AP 可以组成 APG 共同服务于用户, 因此这些 AP 可以进行联合检测, 即只要有一个 AP 端检测到了导频攻击, 就可认为该用户附近存在窃听者. 所以相对于单节点检测模型, UUDN 分布式天线系统本身就能明显提高检测效率.

2 LS-FDC 检测方法

由于信号分量与噪声分量是相互独立的, 所以可以将$\hat{R}_{y,j}$分为信号子空间分量和噪声子空间分量[14]:

$$\hat{R}_{y,j}=\hat{R}_{s,j}+\hat{R}_{n,j}(j=0,1) \tag{6a}$$

$$\text{s.t. } \hat{R}_{s,j}=AE\left[y(n)y(n)^H\right]A \tag{6b}$$

$$\hat{R}_{n,j}=\sigma^2 I_M \tag{6c}$$

其中, 对角矩阵A的对角元素由特征值$\{\lambda_1,\lambda_2,\cdots,\lambda_M\}$组成, $\hat{R}_{s,j}$为信号分量, $\hat{R}_{n,j}$为噪声分量.

传统的 MDL、FDC 等算法的思想是通过估计噪声特征值的个数来检测信源数目, 当$N\gg M$时, 这些检测方法都能够达到一致估计性. 但是, 在 UUDN 系统中, 由于导频长度受限的影响以及大规模 MIMO 技术的应用, 节点天线数和导频长度将处于同一数量级$(M,N\to\infty,\ M/N\to c\in(0,\infty))$, 甚至还会出现节点天线数大于导频长度这种极端情况, 导致样本协方差矩阵不再是总体协方差矩阵的极大似然估计, 造成基于信源估计算法的性能剧烈下降.

针对这种情况, 本文将线性收缩算法与 FDC 算法进行结合, 设计出了新的窃听用户检测方法: LS-FDC 算法. 具体做法: 首先利用 LS 算法对噪声协方差矩阵进行线性优化, 使其特征分解后更好地拟合总体特征值的分布情况; 然后通过 FDC 方法检测是否存在窃听用户. 关键步骤分为以下两点.

2.1 利用线性收缩算法优化噪声子空间分量

首先假设当前合法用户的数目为 k, 然后利用线性收缩算法来优化样本的噪声协方差矩阵$\hat{R}_{n,j}(j=0,1)$. 具体做法为: 通过最小化优化矩阵$R_{LS,j}$与总体噪声协方差矩阵$R_{n,j}$之间的均方误差 (Mean Squared Error, MSE) 来计算总体噪声协方差矩阵的最佳估计. 根据文献 [15] 的线性收缩推导可知, 具体的优化矩阵设计如下:

$$\min_{\rho} E\left[\left\|R_{LS,j}-R_{n,j}\right\|_F^2\right] \tag{7}$$

$$\text{s.t. } R_{LS,j}=\alpha^{(k)}\hat{\lambda}I_{M-k}+\left(1-\alpha^{(k)}\right)\hat{R}_{n,j} \tag{8}$$

其中, $\|\cdot\|_F$是 Frobenius 范数, $\alpha\in[0,1]$表示收缩系数, $\hat{\lambda}=(1/M-k)\sum_{i=k+1}^{M}\lambda_i$为噪声方差$\sigma^2$的估计值, 其中线性收缩系数$\alpha$由以下公式求得:

$$\alpha=\frac{\sum_{i=k+1}^{M}\lambda_i^2+\left(\sum_{i=k+1}^{M}\lambda_i\right)^2}{(N+1)\left\{\sum_{i=k+1}^{M}\lambda_i^2-\frac{\left(\sum_{i=k+1}^{M}\lambda_i\right)^2}{M-k}\right\}} \tag{9}$$

因为α可能大于 1, 故取$\rho=\min(\alpha,1)$作为噪声协方差矩阵的有效收缩系数. 因此, 最终优化矩阵为:

$$R_{LS,j}=\rho\hat{\lambda}I_{M-k}+(1-\rho)\hat{R}_{n,j}=diag(l_{k+1},\cdots,l_M) \tag{10}$$

经过收缩优化后, 噪声特征值为$l_i=\rho\hat{\lambda}+(1-\rho)\lambda_i(i=k+1,\cdots,M)$.

如图 2 所示, 当节点天线数$M=30$, 导频长度$N=100$, 噪声方差$\sigma^2=1$ dB 时, 原始的噪声特征值分布偏离总体噪声方差的程度较大. 经过线性收缩后, 如图 3 所示, 噪声特征值分布很好的拟合了总体的分布情况.

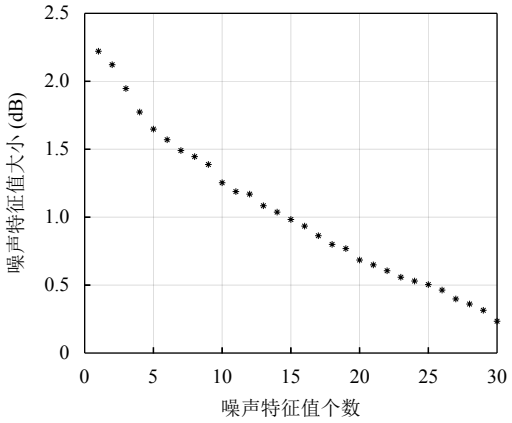

图 2 噪声协方差矩阵的特征值分布

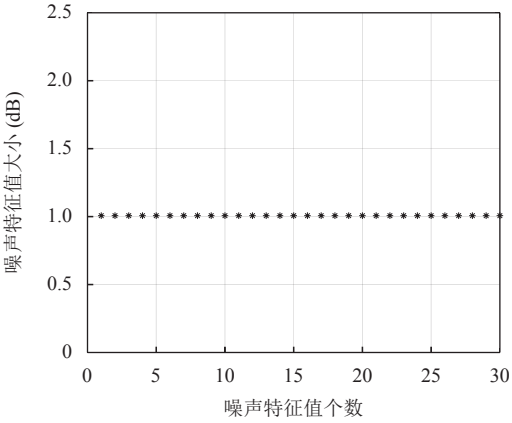

图 3 线性收缩后的噪声协方差矩阵的特征值分布

2.2 利用 FDC 信源估计算法进行窃听检测

通过线性收缩优化噪声特征值分布, 解决了样本有限情况下噪声特征值与信号特征值出现交叉模糊的问题. 之后, 再将噪声特征值带入 FDC 算法表达式中, 得到了重新定义后的 FDC 算法:

$$LS\text{-}FDC(k)=N(M-k)\log_2\frac{\frac{1}{M-k}\sum_{i=k+1}^{M}l_i^r}{\left(\prod_{i=k+1}^{M}l_i\right)^{\frac{r}{M-k}}}+\frac{1}{2}k(2M-k)\log_2 N \tag{11}$$

利用上式可以计算出合法用户为 k 时的 FDC 结果值, 然后, 再将假设的合法用户数k+1, 进行反复循环上面的步骤, 直到得到使上式计算结果最小的 k 值, 即为信源数目的真实估计值:

$$\hat{k} = \arg \min_{1\le k\le \bar{M}-1} LS\text{-}FDC(k) \tag{12}$$

其中, $\bar{M} = \min(M,N) - 1$, 并且根据文献 [13] 的验证可知, 当灵活参数$r = 1.5$时的估计效果最好.

当只有一个合法用户时, 根据假设检验:

$$\begin{cases} H_0 : k = 1 \\ H_1 : k \ne 1 \end{cases} \tag{13}$$

其中, k 为合法用户的数目, 如果$k = 1$, 则判定系统中不存在主动窃听者; 如果$k \ne 1$, 判定系统中存在主动窃听者.

传统 MDL、FDC 算法的时间复杂度主要由样本协方差矩阵和特征值分解两部分决定. 其中, 样本协方差矩阵的复杂度为$\mathrm{O}\left(NM^2\right)$, 特征值分解的复杂度为$\mathrm{O}\left(M^3\right)$. 本文方法在此基础上又加入了线性收缩步骤, 其复杂度为$\mathrm{O}(M-k)$, 因此, 本文算法与传统算法的复杂度处于同一数量级内, 并不会额外增加算法的计算复杂度.

基于上述的理论分析, 该算法的具体实施步骤如算法 1.

算法 1. LS-FDC 检测方法

(1) 分别对各 AP 端接收到的信号矩阵进行自相关运算, 得到样本协方差矩阵, 然后进行特征值分解并降序排列$\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_M > 0$, i=1,2,⋯,M.

(2) 假设有$1 \le k \le \bar{M}-1$个合法用户, 利用$\hat{\lambda} = (1/M-k)\sum_{i=k+1}^{M}\lambda_i$估计出噪声方差$\hat{\lambda}$, 并计算出线性收缩系数$\rho$.

(3) 将线性收缩系数ρ带入式 (10), 计算收缩后的噪声协方差矩阵, 并对它进行特征值分解, 然后将噪声特征值带入式 (11) 求得结果.

(4) 循环步骤 (2) 和步骤 (3), 得到使得式 (12) 最小的 k 值, 即为估计的合法用户数 k.

(5) 对步骤 (4) 的结果进行假设检验, 只要有一个 AP 端检测出结果$k \ne 1$, 则代表合法用户附近存在窃听者, 反之, 判定不存在窃听者.

3 仿真实践及结果分析

本节中, 通过仿真实验将本文方法与传统的 MDL[11]、FDC[13] 以及采用随机矩阵进行优化的 RMT-MDL 方法[16] 进行比较, 来验证 LS-FDC 方法的优越性. 具体的仿真模型为: 在直径为 100 m 的小区范围内, 小型 AP 采用泊松点过程, 动态分布在该小区范围内, 密度为λ_{AP}; Bob 设置于该小区中心, 并且规定 Bob 信号发射范围极限值为 30 m; Eve 随机分布在该小区内. 信道模型采用瑞利平坦衰落信道, 信道的大规模衰落系数设为$d = (d_r/d_o)^v$, 其中d_o, d_r = 10 m 和v = 3分别表示 Bob 端到 AP 端的实际地理距离、参考距离和路径损失指数[12]; 噪声方差$\sigma^2 = 1$; Bob 信噪比P_B/σ^2 = 10 dB; 功率系数β=0.9; 导频序列采用归一化的 BPSK 调制信号.

后文的每个实验数据都进行 500 次蒙特卡洛仿真获得.

3.1 各检测方法之间的性能比较

图 4 为节点天线数$M = 100$, 样本导频长度N = 150条件下的各方法检测概率随 Eve 信噪比的变化曲线. 由仿真结果可知, 在样本导频长度相对有限下的情况下, 本文的 LS-FDC 检测算法较 MDL、FDC 以及最近基于随机矩阵进行优化的 RMT-MDL 算法相比, 在低信噪比和导频长度有限情况下的检测概率更高, 更加适合 UUDN 系统.

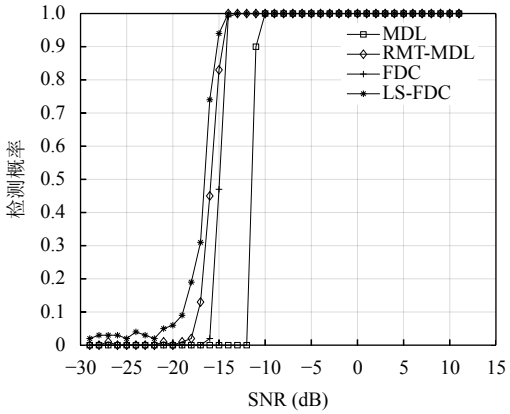

图 4 $M = 100, N = 150$时各方法检测概率变化曲线图

图 5 为节点天线数$M = 200$, 样本导频长度$N = 100$条件下的各方法检测概率随 Eve 信噪比的变化曲线. 由仿真结果可知, 在样本导频长度小于节点天线数目的极限情况下, MDL、FDC、RMT-MDL 等信源估计算法均失效, 而本文的 LS-FDC 检测算法, 当 Eve 信噪比达到−14 dB 左右时依然能够有接近 1 的检测概率. 由此可知, LS-FDC 检测算法在样本导频长度小于节点天线数目的情况下具有明显的优势.

3.2 各参数对 LS-FDC 检测方法性能的影响

图 6 为不同天线数目下 LS-FDC 算法检测概率随 Eve 信噪比的变化曲线. 其中, 导频长度$N = 200$, 节点的天线数目分别取$M = 30, 60, 120$. 由仿真结果可知, 当$M = 120$时, LS-FDC 检测算法在 Eve 信噪比增加到−14 dB 时检测概率达到 1, 比$M = 60$情况下提高了约

2 dB、$M = 30$情况下提高了约 4 dB. 由此可以看出, 通过增加节点的天线数目能明显提高主动窃听的检测性能.

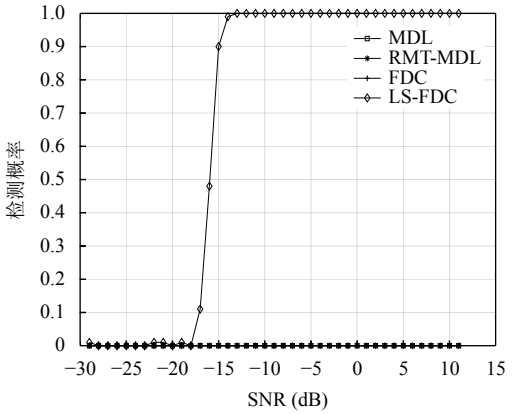

图 5 $M = 200, N = 100$时各方法检测概率变化曲线图

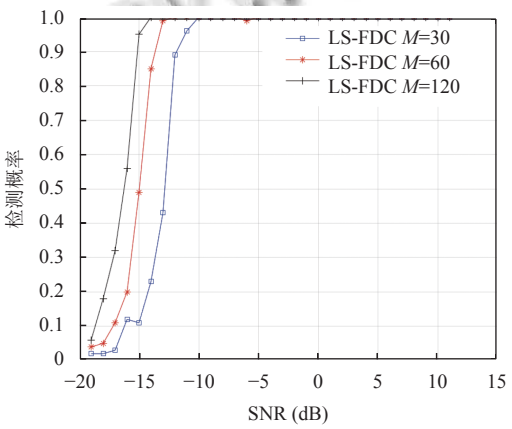

图 6 不同天线数目下的检测概率变化曲线图

图 7 为不同导频长度下的 FDC 与 LS-FDC 算法检测概率随导频长度的变化曲线. 其中, 节点天线数 $M = 120$, Bob 信噪比$P_B/\sigma^2 = 0$ dB, Eve 信噪比$P_E/\sigma^2 = -15$ dB, 导频长度从 100 逐渐增加到 200. 由仿真结果可知, LS-FDC 检测算法在导频长度$N = 120$时就能达到接近 1 的检测概率, 而 FDC 方法, 在导频长度小于天线数时, 检测概率基本为 0, 直到增加到 160 时才达到接近 1 的检测概率. 由此可以证明, 相比较原始的 FDC 方法, 本文方法在导频长度受限的情况下具有更好的检测性能.

4 总结

本文提出了一种 LS-FDC 多节点联合检测算法. 该算法首先通过统计学中的线性收缩理论, 对噪声子空间分量的样本协方差矩阵进行优化, 使其接近总体的分布情况, 从而解决了导频长度受限情况下噪声特征值与信号特征值产生交叉模糊的情况. 随后将线性收缩后计算出的噪声特征值代入 FDC 算法中进行主动窃听检测. 仿真结果表明该算法与其他导频攻击检测算法相比, 在各种环境中都具有显著优势, 特别是在导频长度小于节点天线数时依旧能够保持良好的性能, 为在 UUDN 中更好的检测出主动窃听用户提供了可能.

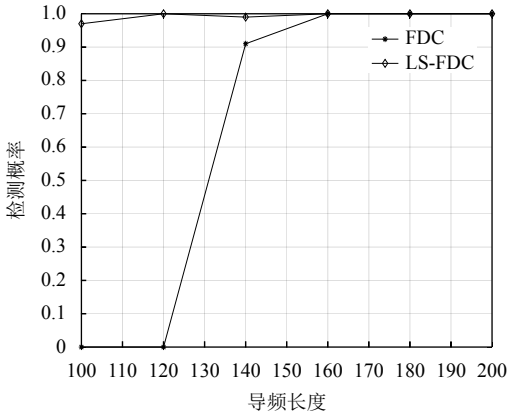

图 7 不同导频长度下的检测概率变化曲线图

参考文献

1 Chen SZ, Qin F, Hu B, *et al*. User-centric ultra-dense networks for 5G: Challenges, methodologies, and directions. IEEE Wireless Communications, 2016, 23(2): 78–85. [doi: 10.1109/MWC.2016.7462488]

2 Kamel M, Hamouda W, Youssef A. Ultra-dense networks: A survey. IEEE Communications Surveys & Tutorials, 2016, 18(4): 2522–2545. [doi: 10.1109/COMST.2016.2571730]

3 Zhang W, Chen J, Kuo YH, *et al*. Artificial-noise-aided optimal beamforming in layered physical layer security. IEEE Communications Letters, 2019, 23(1): 72–75. [doi: 10.1109/LCOMM.2018.2881182]

4 Darsena D, Gelli G, Iudice I, *et al*. Design and performance analysis of channel estimators under pilot spoofing attacks in multiple-antenna systems. IEEE Transactions on Information Forensics and Security, 2020, 15: 3255–3269. [doi: 10.1109/TIFS.2020.2985548]

5 Kamel M, Hamouda W, Youssef A. Physical layer security in ultra-dense networks. IEEE Wireless Communications Letters, 2017, 6(5): 690–693. [doi: 10.1109/LWC.2017.2731840]

6 Wu YP, Khisti A, Xiao CS, *et al*. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 2018, 36(4): 679–695. [doi: 10.1109/JSAC.2018.2825560]

7 Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. IEEE Communications Magazine, 2015, 53(6): 21–27. [doi: 10.1109/MCOM.2015.7120012]

8 Xiong Q, Liang YC, Li KH, *et al*. An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems. IEEE Transactions on Information Forensics and Security, 2015, 10(5): 932–940. [doi: 10.1109/TIFS.2015.2392564]

9 Gao N, Qin ZJ, Jing XJ. Pilot contamination attack detection and defense strategy in wireless communications. IEEE Signal Processing Letters, 2019, 26(6): 938–942. [doi: 10.1109/LSP.2019.2913085]

10 Tugnait JK. Detection of active eavesdropping attack by spoofing relay in multiple antenna systems. IEEE Wireless Communications Letters, 2016, 5(5): 460–463. [doi: 10.1109/LWC.2016.2585549]

11 Zhang WL, Lin H, Zhang RN. Detection of pilot contamination attack based on uncoordinated frequency shifts. IEEE Transactions on Communications, 2018, 66(6): 2658–2670. [doi: 10.1109/TCOMM.2018.2791535]

12 Zhang XY, Guo DX, An K, *et al*. Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems. IEEE Access, 2019, 7: 57332–57340. [doi: 10.1109/ACCESS.2019.2914028]

13 Lu ZH, Zoubir AM. Flexible detection criterion for source enumeration in array processing. IEEE Transactions on Signal Processing, 2013, 61(6): 1303–1314. [doi: 10.1109/TSP.2012.2234747]

14 Nie XZ, Jiang H, Zhang MH. Secure transmission against pilot spoofing attack: A random matrix theory based scheme. 2018 IEEE International Conference on Communications Workshops (ICC Workshops). Kansas City: IEEE, 2018. 1–5.

15 Huang L, So HC. Source enumeration via MDL criterion based on linear shrinkage estimation of noise subspace covariance matrix. IEEE Transactions on Signal Processing, 2013, 61(19): 4806–4821. [doi: 10.1109/TSP.2013.2273198]

16 Xu L, Chen JQ, Liu M, *et al*. Active eavesdropping detection based on large-dimensional random matrix theory for massive MIMO-enabled IoT. Electronics, 2019, 8(2): 146. [doi: 10.3390/electronics8020146]