基于异构导频能量估计的边缘节点导频攻击检测算法

王仕果[1]，田淑娟[2]，邓清勇[3]

（1. 长沙理工大学计算机与通信工程学院，湖南 长沙 410076；
2. 湘潭大学计算机学院，湖南 湘潭 411105；3. 广西师范大学计算机学院，广西 桂林 541001）

摘 要：针对边端协同联邦学习中边缘服务器与设备终端频繁交互更新模型和梯度参数时，窃听者容易通过导频攻击干扰信道估计，从而达到降低模型更新效率和窃取模型参数的问题，基于异构导频能量估计提出一种导频攻击检测算法。首先，通过深入分析导频攻击对系统安全速率的影响，构建联邦学习导频攻击系统模型。进而，基于随机分割和加密方法提出一种信号平均能量差的导频攻击检测方法，能够准确地检测出潜在的导频攻击并进行污染信道的恢复。实验结果表明，与其他已有算法相比，所提算法适用于检测发射功率小、隐蔽性强的导频攻击，基于恢复的信道状态信息进行预编码可以大幅度提高边缘服务器的数据传输速率。

关键词：导频攻击检测；能量估计；攻击对抗；边缘计算

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023231

Pilot spoofing detection algorithm for edge nodes based on heterogeneous pilot energy estimation

WANG Shiguo[1], TIAN Shujuan[2], DENG Qingyong[3]

1. School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410076, China
2. College of Computer, Xiangtan University, Xiangtan 411105, China
3. School of Computer, Guangxi Normal University, Guilin 541001, China

Abstract: For the federated learning scenarios with edge-end cooperation, edge servers and device terminals update their models and exchange gradient parameters frequently, and hence eavesdroppers can manipulate channel estimation through pilot spoofing to intercept the transmitted information and reduce the update efficiency of federated learning model. Therefore, a pilot attack detection algorithm with heterogeneous pilot energy estimation was proposed. Firstly, a federated learning pilot attack system model was constructed after the security of pilot attacks on data transmission had been analyzed. Then, a pilot attack detection method based on random segmentation and encryption methods was proposed to detect the pilot spoofing accurately and the contaminated channel could be recovered as well. Experimental results show that the proposed algorithm is more suitable for detecting pilot attacks with low transmit power and strong concealment compared to other existing algorithms. Furthermore, the data transmission rate of edge servers is improved significantly through the precoding based on the recovered channel state information.

Keywords: pilot spoofing detection, energy estimation, attack combating, edge computing

---

收稿日期：2023−08−02；**修回日期：**2023−11−14

通信作者：田淑娟，sjtianwork@xtu.edu.cn

基金项目：国家自然科学基金资助项目（No.62372065，No.62172349，No.62076214）；湖南省自然科学基金项目（No.2023JJ30597，No.2021JJ30737）；湖南省教育厅基金资助项目（No.21B0139）；中国科学院计算科学国家重点实验室开放基金资助项目（No.SYSKF2101）

Foundation Items: The National Natural Science Foundation of China (No.62372065, No.62172349, No.62076214), The Natural Science Foundation of Hunan Province (No.2023JJ30597, No.2021JJ30737), The Research Foundation of Education Bureau of Hunan Province (No.21B0139), The Open Project of the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences (No.SYSKF2101)

0　引言

随着无线通信和人工智能技术的广泛应用，物联网用户和业务数据量呈指数级增长，集中式云计算服务模式已很难满足智能业务对数据处理低时延的要求，移动边缘计算与缓存成为解决带宽资源受限和业务低时延要求的可行范式[1-2]。边缘计算将计算、网络、存储等能力扩展到物联网终端附近的网络边缘侧，适用于基于集成的算法模型进行本地小规模智能分析与预处理，实现分布式、低时延、高可靠的边缘智能服务。由于 AI 模型训练和推理需要消耗大量的计算资源，而当前大多数移动设备资源受限，边缘用户可以从边缘服务器下载训练好的模型进行本地推理，也可以将任务卸载到边缘服务器，从而提高系统的吞吐量和实时性。联邦学习能在保证用户隐私的前提下通过多用户联合弥补计算资源不足的缺陷，但需要参与设备与服务器之间来回交互更新后的梯度参数，频繁通信和传输数据量都会产生大量的通信开销；其次，大量异构设备有限的网络带宽，会造成通信拥塞，导致通信时延增长；边缘用户所处的环境复杂，系统很容易受到非法用户的恶意攻击，窃听者可能通过信道估计阶段的导频攻击使信息泄露和系统性能下降，从而影响联邦学习系统的稳定性和鲁棒性。因此，如何保证数据的高效和安全传输成为移动边缘计算和边缘智能的关键[3-4]。

导频攻击是非法用户主要使用的一种主动窃听手段。窃听者在通信节点进行信道估计阶段发起攻击，通过发送与合法用户相同的导频序列污染信道估计，误导信号发送端在进行预编码处理时使发射信号偏向窃听者，从而窃取到更大功率的信号进行解码，并降低合法接收端的可达速率。对于边缘系统，当节点受到导频攻击时，边缘节点发送的信号功率将主要被窃听者所接收，严重威胁信息的传输安全；与此同时，还会导致边缘服务器接收的信号功率变小，任务卸载速率下降，系统的实时性变差[5]。因此，导频攻击严重威胁边缘系统的信息传输安全并降低数据传输效率，而对导频攻击的有效检测是进行攻击对抗策略设计的前提。所以，本文对导频攻击检测展开研究，提出一种基于能量估计的导频攻击检测算法，并对污染的估计信道进行恢复，增大节点任务卸载的安全性和数据卸载效率。

目前，针对如何快速有效检测出无线通信系统中可能存在的导频攻击，研究者已提出了一些相关算法。Tugnait[6]最先采用随机导频来进行物理层主动攻击检测，使合法用户端添加一段随机导频序列，然后利用最小描述长度（MDL，minimum description length）来分析上行训练阶段接入点接收信号自相关矩阵的秩，从而判断系统中是否存在导频攻击。但是，添加随机导频序列会增大系统的资源消耗和导频算法实现的复杂度。文献[7]将导频序列分成等长的几段，每段随机引入导频频偏，对接收信号进行自相关，通过 MDL 分析每段导频接收信号子空间的维数，若有一个或一个以上的维数大于 1，则存在导频攻击。Xu 等[8]在上行训练阶段将合法用户端的上行导频伪随机地分成了两段，基站端通过分析这两段接收信号差值的二范数分布进行导频攻击检测。

可信节点的参与，有利于分析接收端信号的成分，因此通过节点辅助有望检测出系统中存在的导频攻击。Liu 等[9]针对基站为多天线、用户和窃听者为单天线的场景，通过引入一个可信任的单天线中继，提出一种三阶段上行链路训练（TPUP, three-phase uplink training）检测方法，并获得了用户和窃听者的信道状态信息。利用智能反射面（RIS，reconfigurable intelligent surface）可以控制反射信号的相位和幅度的特点，Wu 等[10]利用可重构 RIS 来限制信息泄露给主动窃听者；文献[11]分析了 RIS 在提高去蜂窝大规模多输入多输出系统的保密容量方面的潜力，并提出了一种新的下行链路传输方案，以最小化信息泄露。Akbar 等[12]基于小区之间协作提出了一种导频攻击检测方法。

由于信号的相干和多径传播特性，在受到导频攻击时，导频接收信号的功率会出现细微差别，而且收发双方接收信号的功率电平存在不对称性。因此，Xiong 等[13]提出了一种基于能量比的检测（ERD, energy ratio detector）方法。Xu 等[14]利用接收信号的相关性进行导频攻击检测，并且有效区分了导频攻击信号和信道噪声。文献[15]通过分析接收信号功率、相位和幅度等特征的差异进行导频攻击检测，提出了一种基于深度学习的检测方法。Ahmed 等[16]利用导频接收信号在时域和频域上自相关和互相关的频率选择性特征进行攻击检测。对于 5G 免授权物联网，Wang 等[17]基于等效虚拟信道提出了一种导频攻击检测和信道估计策略。对于只有上行链路受到攻击的情况，可以采取双向训练检测

（TWTD, two-way training detector）方法，通过比较收发双方信道估计的差异可以有效检测出导频攻击[18]，但是系统需要双向信道进行训练。

对于特定的网络场景，上述导频攻击检测算法都能较准确地检测出系统中存在的导频攻击。然而，它们大多需要修改导频协议，增加了系统的复杂度，适用性不强；而且不能有效捕获到窃听信道的状态信息，为后续的攻击对抗设计提供基础。因此，本文基于随机分割和加密方法提出一种信号平均能量差的导频攻击检测算法，该算法不仅可以对导频攻击进行准确检测，而且能够估计出用户的真实信道状态信息和窃听信道的状态信息，为导频攻击对抗提供了基础和依据。

1 系统模型

对于一个边端协同联邦学习网络，边缘节点 Bob 需要将本地参数上传给边缘服务器 Alice 进行处理，并需要从 Alice 处获得更新后的模型参数。假设有一个恶意节点 Eve 为了窃听 Bob 从 Alice 处下载的模型或数据，在信道估计阶段发起导频攻击，系统模型如图 1 所示。

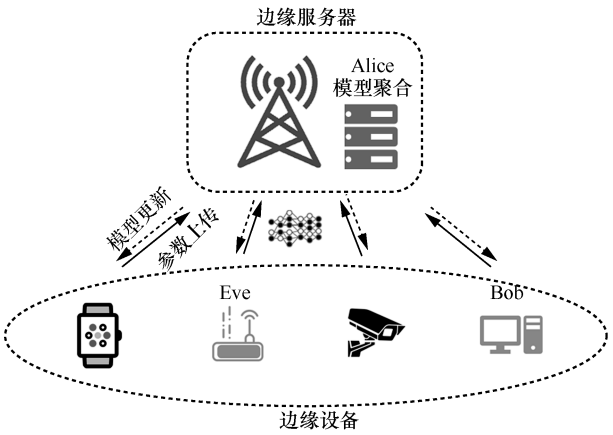


图 1 联邦学习系统中导频攻击系统模型

服务器 Alice 在向边缘节点发送数据之前，需要获得其与 Bob 之间的信道状态信息。因此，在导频阶段，边缘节点 Bob 向边缘服务器 Alice 发送导频序列，Alice 基于接收到的信号进行信道估计。设 Alice 到 Bob 的信道为 $\sqrt{\beta_{\mathrm{AB}}}\boldsymbol{h}_{\mathrm{AB}}$，Bob 到 Alice 的信道为 $\sqrt{\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}$，其中 $\sqrt{\beta_{\mathrm{AB}}}\left(\sqrt{\beta_{\mathrm{BA}}}\right)$ 表示大尺度路径衰落，$\boldsymbol{h}_{\mathrm{AB}}$（$\boldsymbol{h}_{\mathrm{BA}}$）表示小尺度衰落。根据 TDD 系统的信道互易性可知，$\sqrt{\beta_{\mathrm{AB}}}=\sqrt{\beta_{\mathrm{BA}}}$，$\boldsymbol{h}_{\mathrm{BA}}=\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{T}}$。对于块衰落信道模型，在一个相干时间 T 内，信道状态信息保持不变。

当此边缘节点受到恶意节点 Eve 主动窃听时，Eve 发送与 Bob 同频同相的导频序列 $\boldsymbol{x}_p$。记 Eve 到 Alice 的路径衰落和小尺度衰落分别为 $\sqrt{\beta_{\mathrm{EA}}}$ 和 $\boldsymbol{h}_{\mathrm{EA}}$，并假设 $\boldsymbol{h}_{\mathrm{BA}}$ 和 $\boldsymbol{h}_{\mathrm{EA}}$ 彼此相互独立，则在上行导频训练阶段，边缘服务器 Alice 接收的信号为

$$\boldsymbol{y}_{\mathrm{A}}=\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\boldsymbol{x}_p+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_p+\boldsymbol{n}_{\mathrm{A}} \tag{1}$$

其中，P_{B} 和 P_{E} 为 Bob 和 Eve 的导频信号发射功率，$\boldsymbol{n}_{\mathrm{A}}$ 为在 Alice 处的加性噪声，设其服从高斯分布 $N\sim(0,\sigma_{\mathrm{A}}^2)$。

边缘服务器 Alice 根据导频接收信号式(1)进行信道估计。由于 Alice 已知该上行训练导频序列，基于最小二乘法，可得到[19]上行链路信道 $\boldsymbol{h}_{\mathrm{BA}}$ 的估计值，即

$$\hat{\boldsymbol{h}}_{\mathrm{BA}}=\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\boldsymbol{x}_p\boldsymbol{A}+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_p\boldsymbol{A}+\boldsymbol{n}_{\mathrm{A}}\boldsymbol{A} \tag{2}$$

其中，$\boldsymbol{A}=\dfrac{\boldsymbol{x}_p^{\mathrm{H}}(\boldsymbol{x}_p\boldsymbol{x}_p^{\mathrm{H}})^{-1}}{\sqrt{P_{\mathrm{B}}}}$。根据导频序列的特点，式(2)可以进一步表示为

$$\hat{\boldsymbol{h}}_{\mathrm{BA}}=\hat{\boldsymbol{h}}'_{\mathrm{BA}}+\boldsymbol{h}'_{\mathrm{EA}}=\boldsymbol{h}_{\mathrm{BA}}+\boldsymbol{h}'_{\mathrm{EA}}+\boldsymbol{\varepsilon}_u \tag{3}$$

其中，$\boldsymbol{h}'_{\mathrm{EA}}=\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_p\boldsymbol{A}$，$\boldsymbol{\varepsilon}_u$ 是一个由高斯白噪声引起的估计误差，其均值为 0、方差为 $\sigma_{\boldsymbol{\varepsilon}_u}^2\boldsymbol{I}_M$。显然，$\hat{\boldsymbol{h}}'_{\mathrm{BA}}$ 和 $\boldsymbol{\varepsilon}_u$ 与 $\boldsymbol{h}'_{\mathrm{EA}}$ 互不相关。由于信道 $\boldsymbol{h}_{\mathrm{BA}}$ 和 $\boldsymbol{\varepsilon}_u$ 是相互独立的，因此可得 $\mathrm{E}\left\{\left\|\boldsymbol{h}_{\mathrm{BA}}\right\|^2\right\}=\mathrm{E}\left\{\left\|\hat{\boldsymbol{h}}'_{\mathrm{BA}}\right\|^2\right\}+\mathrm{E}\left\{\left\|\boldsymbol{\varepsilon}_u\right\|^2\right\}$。对于一个给定的时间帧，$\sigma_{\boldsymbol{\varepsilon}_u}^2$ 可以根据矩阵反引理论计算得出[19]

$$\sigma_{\boldsymbol{\varepsilon}_u}^2=\frac{\beta_{\mathrm{BA}}\sigma_{\mathrm{A}}^2}{\sigma_{\mathrm{A}}^2+P_{\mathrm{B}}\beta_{\mathrm{BA}}\tau} \tag{4}$$

其中，τ 为导频序列的长度。由式(3)可知，边缘服务器 Alice 估计出的上行估计信道信息 $\hat{\boldsymbol{h}}_{\mathrm{BA}}$ 受到了攻击信道 $\boldsymbol{h}'_{\mathrm{EA}}$ 的污染。在数据发送阶段，如果没有对该污染采取恢复措施，那么服务器 Alice 将基于 $\hat{\boldsymbol{h}}_{\mathrm{BA}}$ 进行波束成形。若采用最大比波束成形，记成形向量为 $\boldsymbol{w}$，则在下行数据传输阶段，合法边缘节点 Bob 和恶意节点 Eve 接收信号的信噪比分别为

$$\mathrm{SNR}_{\mathrm{B}}=\frac{P_{\mathrm{A}}\left\|\boldsymbol{h}_{\mathrm{BA}}^{\mathrm{H}}\boldsymbol{w}\right\|^2}{\sigma_{\mathrm{A}}^2} \tag{5}$$

$$\mathrm{SNR_E}=\frac{P_{\mathrm{A}}\left\|\boldsymbol{h}_{\mathrm{EA}}^{\mathrm{H}}\boldsymbol{w}\right\|^2}{\sigma_{\mathrm{A}}^2} \tag{6}$$

因此，得到边缘节点下载数据的安全速率为 $R_s=\mathrm{lb}(1+\mathrm{SNR_B})-\mathrm{lb}(1+\mathrm{SNR_E})$。

由式(2)可知，当系统中不存在导频攻击，即 $P_{\mathrm{E}}=0$ 时，$\boldsymbol{w}$ 将指向合法边缘节点的方向；相反，当通信系统中存在主动导频攻击时，$\boldsymbol{w}$ 则会偏离合法节点方向，转向恶意节点 Eve 所在的方向。偏离的程度由两者导频信号发射功率决定。当 $P_{\mathrm{B}}>P_{\mathrm{E}}$ 时，$\boldsymbol{h}_{\mathrm{EA}}$ 在 $\hat{\boldsymbol{h}}_{\mathrm{BA}}$ 中占的比重大于 $\boldsymbol{h}_{\mathrm{BA}}$，这会使波束成形向量基本指向窃听节点。同时，从式(5)和式(6)可知，如果窃听节点 Eve 增大导频攻击的发射功率，可以窃听到更多信息速率。随着 P_{E} 的增加，合法节点 Bob 的可达信道速率随之减小，当 P_{E} 达到与 P_{B} 同样的水平，保密速率将会变成 0，即边缘服务器发送给节点 Bob 的所有信息都将被 Eve 窃听。

因此，导频攻击严重威胁到边缘节点数据传输安全和数据传输效率，有必要对其进行准确检测和有效对抗。针对该系统模型，本文基于异构导频能量估计提出一种新的导频攻击检测算法，并对污染信道进行了恢复。

2　导频序列设计

为了能够根据导频接收信号的能量差异进行攻击检测，本文首先提出了一种新的导频序列构建方法。

由于导频序列是公开的，假设恶意节点 Eve 知道边缘节点 Bob 将利用导频序列 $\boldsymbol{x}_p$ 进行信道估计，它将发送 $\boldsymbol{x}_p$ 进行信道污染。为了有利于边缘服务器进行导频攻击检测，Bob 将发送的导频序列随机分成两部分（为保证子序列与该其他用户使用的导频序列之间的正交性，子导频序列长度均大于或等于系统所能承受的最大用户数），并乘以一个随机数以避免恶意节点的检测，如图 2 所示。

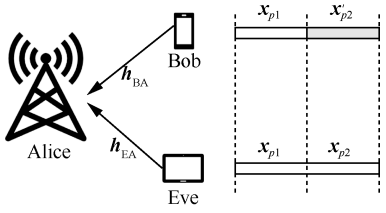


图 2　导频过程与导频序列

具体地，首先将 $\boldsymbol{x}_p$ 随机分为两段，记为 $\boldsymbol{x}_p=[\boldsymbol{x}_{p1},\boldsymbol{x}_{p2}]$。设 $\boldsymbol{x}_{p1}$ 和 $\boldsymbol{x}_{p2}$ 的长度分别为 Δ_1 和 Δ_2，$\Delta_1+\Delta_2=\tau$，按式(7)对导频序列 $\boldsymbol{x}_p$ 进行变换

$$\tilde{\boldsymbol{x}}_p=\zeta\boldsymbol{x}_p\boldsymbol{\Psi} \tag{7}$$

其中，$\boldsymbol{\Psi}=\begin{bmatrix}\begin{bmatrix}r_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & r_1\end{bmatrix} & \begin{matrix}0 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 0\end{matrix}\\ \begin{matrix}0 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 0\end{matrix} & \begin{bmatrix}r_2 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & r_2\end{bmatrix}\end{bmatrix}$，$\boldsymbol{\Psi}\in R^{\tau\times\tau}$，$r_1=1$，$r_2$ 为一个(0,1)区间的随机数；ζ 为功率正则化因子，其目的在于保证总导频序列满足 $\tilde{\boldsymbol{x}}_p\tilde{\boldsymbol{x}}_p^{\mathrm{H}}=\tau$，故有 $\zeta=\sqrt{\dfrac{1}{r_1^2\dfrac{\Delta_1}{\tau}+r_2^2\dfrac{\Delta_2}{\tau}}}$。因此，边缘服务器 Alice 接收到的导频信号为

$$\boldsymbol{y}_{\mathrm{A}}=\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\tilde{\boldsymbol{x}}_P+I\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_P+\boldsymbol{n}_{\mathrm{A}} \tag{8}$$

其中，$I=\{0,1\}$ 为指示系数，$I=0$ 表示不受导频攻击，$I=1$ 表示受到导频攻击。为了表示两段导频序列对应的接收信号，记 $\boldsymbol{y}_{\mathrm{A}}=[\boldsymbol{y}_{\mathrm{A1}},\boldsymbol{y}_{\mathrm{A2}}]$，其中，$\boldsymbol{y}_{\mathrm{A1}}\in C^{M\times\Delta_1}$，$\boldsymbol{y}_{\mathrm{A2}}\in C^{M\times\Delta_2}$。

由于节点 Bob 对导频序列 $\boldsymbol{x}_p$ 进行了上述随机操作，服务器 Alice 在基于接收信号进行信道估计之前，必须估计出每段导频序列的长度和每段的随机放大系数。下面分别对 2 个导频序列子段的长度和放大系数进行估计。

2.1　子导频序列的长度估计

边缘服务器 Alice 根据接收信号 $\boldsymbol{y}_{\mathrm{A}}$，计算标准化协方差矩阵 $\dfrac{\boldsymbol{y}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{y}_{\mathrm{A}}}{M}$，取出其对应的对角元素，记为 $\boldsymbol{e}=[e_{\mathrm{A1},1},e_{\mathrm{A1},2},\cdots,e_{\mathrm{A1},\Delta1},e_{\mathrm{A2},1},e_{\mathrm{A2},2},\cdots,e_{\mathrm{A2},\Delta2}]$。根据中心极限定理可知，对角序列 $\boldsymbol{e}$ 中的每一个元素都可看作一个高斯分布变量。因此，在不受导频攻击（简记为 H_0）和受到导频攻击（简记为 H_1）情况下，$e_{\mathrm{A}i}$ 的数学期望分别为

$$H_0:\mathrm{E}\{e_{\mathrm{A}i}\}=P_{\mathrm{B}}\beta_{\mathrm{BA}}\left|\zeta r_i\right|^2+\sigma_{\mathrm{A}}^2 \tag{9}$$

$$H_1:\mathrm{E}\{e_{\mathrm{A}i}\}=P_{\mathrm{B}}\beta_{\mathrm{BA}}\left|\zeta r_i\right|^2+\mathrm{P_E}\beta_{\mathrm{EA}}+\sigma_{\mathrm{A}}^2 \tag{10}$$

由式(9)和式(10)可知，无论边缘节点是否受到导频攻击，$\mathrm{E}\{e_{\mathrm{A2}}\}-\mathrm{E}\{e_{\mathrm{A1}}\}=P_{\mathrm{B}}\beta_{\mathrm{BA}}\zeta^2(r_2^2-r_1^2)$ 总是

成立，即在两段导频序列 $\boldsymbol{x}_{p1}$ 与 $\boldsymbol{x}_{p2}$ 分界处，标准化协方差矩阵的对角元素期望存在一个阶跃。因此，可以根据导频接收信号的标准化协方差矩阵对角元素的阶跃间隔来确定这 2 个子导频序列的长度。由上述分析可知，边缘服务器 Alice 可以获得 2 个导频段的接收信号，即

$$H_0:\boldsymbol{y}_{\mathrm{A}i}=\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\tilde{\boldsymbol{x}}_{pi}+\boldsymbol{n}_i \tag{11}$$

$$H_1:\boldsymbol{y}_{\mathrm{A}i}=\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\tilde{\boldsymbol{x}}_{pi}+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_{pi}+\boldsymbol{n}_i \tag{12}$$

其中，$i=\{1,2\}$，$\boldsymbol{n}_i\in C^{M\times\Delta i}$ 为接收子导频序列 $\boldsymbol{x}_{pi}$ 时的高斯白噪声。

2.2 子导频序列的放大系数

在边缘服务器 Alice 估计出合法节点随机分割的两段导频序列的长度后，还需要对第二段子导频序列乘上的随机系数进行估计，即估计 r_2 的值。由于此时已知 $\boldsymbol{x}_{pi}$，则当系统不受导频攻击时，可以得到

$$H_0:\boldsymbol{z}_i=\frac{\boldsymbol{y}_{\mathrm{A}i}\boldsymbol{x}_{pi}^{\mathrm{H}}}{\Delta i\sqrt{P_{\mathrm{B}}}}=\zeta r_i\boldsymbol{h}_{\mathrm{BA}}+\frac{\boldsymbol{n}_i\boldsymbol{x}_{pi}^{\mathrm{H}}}{\Delta i\sqrt{P_{\mathrm{B}}}} \tag{13}$$

当存在导频攻击时，可以得到

$$H_1:\boldsymbol{z}_i=\frac{\boldsymbol{y}_{\mathrm{A}i}\boldsymbol{x}_{pi}^{\mathrm{H}}}{\Delta i\sqrt{P_{\mathrm{B}}}}=\zeta r_i\boldsymbol{h}_{\mathrm{BA}}+\sqrt{\frac{P_{\mathrm{E}}}{P_{\mathrm{B}}}}\boldsymbol{h}_{\mathrm{EA}}\frac{\boldsymbol{n}_i\boldsymbol{x}_{pi}^{\mathrm{H}}}{\Delta i\sqrt{P_{\mathrm{B}}}} \tag{14}$$

其中，$\boldsymbol{z}_i\in C^{M\times1}$。可以发现，无论是否受到导频攻击，$\boldsymbol{\mu}=\boldsymbol{z}_2-\boldsymbol{z}_1$ 的值始终保持不变，即

$$\boldsymbol{\mu}=\zeta(r_2-r_1)\boldsymbol{h}_{\mathrm{BA}}+\frac{1}{\sqrt{P_{\mathrm{B}}}}\left(\frac{\boldsymbol{n}_2\boldsymbol{x}_{p2}^{\mathrm{H}}}{\Delta2}-\frac{\boldsymbol{n}_1\boldsymbol{x}_{p1}^{\mathrm{H}}}{\Delta1}\right) \tag{15}$$

因此，Eve 的存在与否并不影响对 r_2 的估计。

为了求出第二段导频序列随机放大系数 r_2，令 $\delta=\boldsymbol{\mu}^{\mathrm{H}}\boldsymbol{\mu}$，则有

$$\begin{aligned}\delta=&\zeta^2(r_2-r_1)^2\boldsymbol{h}_{\mathrm{BA}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{BA}}+\\&\frac{1}{P_B}\left(\frac{\boldsymbol{x}_{p2}\boldsymbol{n}_2^{\mathrm{H}}}{\Delta2}-\frac{\boldsymbol{x}_{p1}\boldsymbol{n}_1^{\mathrm{H}}}{\Delta1}\right)\left(\frac{\boldsymbol{n}_2\boldsymbol{x}_{p2}^{\mathrm{H}}}{\Delta2}-\frac{\boldsymbol{n}_1\boldsymbol{x}_{p1}^{\mathrm{H}}}{\Delta1}\right)+\\&\frac{\zeta(r_2-r_1)}{\sqrt{P_B}}\boldsymbol{h}_{\mathrm{BA}}^{\mathrm{H}}\left(\frac{\boldsymbol{n}_2\boldsymbol{x}_{p2}^{\mathrm{H}}}{\Delta2}-\frac{\boldsymbol{n}_1\boldsymbol{x}_{p1}^{\mathrm{H}}}{\Delta1}\right)+\\&\frac{\zeta(r_2-r_1)}{\sqrt{P_B}}\left(\frac{\boldsymbol{x}_{p2}\boldsymbol{n}_2^{\mathrm{H}}}{\Delta2}-\frac{\boldsymbol{x}_{p1}\boldsymbol{n}_1^{\mathrm{H}}}{\Delta1}\right)\boldsymbol{h}_{\mathrm{BA}}\end{aligned} \tag{16}$$

当序列长度足够大时，根据中心极限定理可得

$$\boldsymbol{\delta}=\zeta^2(r_2-r_1)^2M\beta_{\mathrm{BA}}+\left(\frac{1}{\Delta2}+\frac{1}{\Delta1}\right)\frac{M\sigma_{\mathrm{A}}^2}{\sqrt{P_{\mathrm{B}}}} \tag{17}$$

联立式(17)和 $r_1=1$，边缘服务器 Alice 可以求解出 r_2。至此，边缘服务器 Alice 可以还原出边缘节点发送的导频序列。

3 导频攻击检测

假定边缘服务器节点对每根天线接收到的信号采用最大比合并技术，则对于发送的第 n 个导频符号，接收到的导频信号可以表示为

$$H_0:\boldsymbol{y}_{\mathrm{A}}(n)=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA}}^{\mathrm{H}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA}}\right\|}\left[\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\tilde{\boldsymbol{x}}_p(n)+\boldsymbol{n}(n)\right] \tag{18}$$

$$H_1:\boldsymbol{y}_{\mathrm{A}}(n)=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA}}^{\mathrm{H}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA}}\right\|}\left[\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\tilde{\boldsymbol{x}}_p(n)+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_p(n)+\boldsymbol{n}(n)\right] \tag{19}$$

其中，$\boldsymbol{x}_p(n)$ 为原始导频序列的第 n 个导频符号，$\boldsymbol{n}(n)$ 为高斯白噪声向量，$\boldsymbol{y}_{\mathrm{A}}(n)$ 为 Alice 接收第 n 个上行导频符号合并后的信号，$\hat{\boldsymbol{h}}_{\mathrm{BA}}$ 为 Alice 采用最小二乘法估计得到的信道矩阵。

在边缘服务器 Alice 处，分别统计发送两段导频序列时接收信号的平均能量，分别记为 Q_1 和 Q_2，即

$$Q_i=\frac{1}{\Delta i}\sum_{n=1}^{\Delta i}\left|\boldsymbol{y}_{\mathrm{A}}(n)\right|^2,i=1,2 \tag{20}$$

根据中心极限定理可知，当两段导频序列长度都足够大时，则接收信号的平均能量 Q_1 和 Q_2 都近似于服从不同均值和方差的高斯分布[20]，即 $Q_1\sim N(\mu_1,\sigma_1^2)$，$Q_2\sim N(\mu_2,\sigma_2^2)$。令 $Z=Q_1-Q_2$，则 $Z\sim N(\mu_1-\mu_2,\sigma_1^2+\sigma_2^2)$。

因此，当 $1\leqslant n\leqslant\Delta1$ 时，有

$$H_0:\boldsymbol{y}_{\mathrm{A}}(n)=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA1}}^{\mathrm{H}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA}}\right\|}\left[\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\zeta r_1\boldsymbol{x}_p(n)+\boldsymbol{n}(n)\right] \tag{21}$$

$$H_1:\boldsymbol{y}_{\mathrm{A}}(n)=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA1}}^{\mathrm{H}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA1}}\right\|}\left[\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\zeta r_1\boldsymbol{x}_p(n)+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_p(n)+\boldsymbol{n}(n)\right] \tag{22}$$

其中，$\hat{\boldsymbol{h}}_{\mathrm{BA1}}$ 为信道估计矩阵，在不受导频攻击和受到导频攻击时分别为 $\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\zeta r_1\boldsymbol{h}_{\mathrm{BA}}+\tilde{\boldsymbol{e}}_1$ 和 $\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\zeta r_1\boldsymbol{h}_{\mathrm{BA}}+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}+\tilde{\boldsymbol{e}}_1$，$\tilde{\boldsymbol{e}}_1$ 为高斯白噪声引起的估计误差。根据式(21)和式(22)以及中心极限定理，接收信号平均能量 Q_1 的均值为

$$\mu_1=\begin{cases}\left|\dfrac{\hat{\boldsymbol{h}}_{\mathrm{BA1}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{BA1}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA1}}\right\|}\right|^2\xi^2r_1^2P_{\mathrm{B}}+\sigma_{\mathrm{A}}^2\to H_0\\ \left|\dfrac{\hat{\boldsymbol{h}}_{\mathrm{BA1}}^{\mathrm{H}}\left(\sqrt{P_{\mathrm{B}}}\boldsymbol{h}_{\mathrm{BA}}r_1\xi+\sqrt{P_{\mathrm{E}}}\boldsymbol{h}_{\mathrm{EA}}\right)}{\hat{\boldsymbol{h}}_{\mathrm{BA1}}}\right|+\sigma_{\mathrm{A}}^2\to H_1\end{cases}\tag{23}$$

且 $\sigma_1^2=\dfrac{1}{\Delta 1}\mu_1^2$。

同理，当 $\Delta 1<n\leqslant\tau$ 时，有

$$H_0:\boldsymbol{y}_{\mathrm{A}}(n)=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA2}}^{\mathrm{H}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA2}}\right\|}\left[\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\zeta r_2\boldsymbol{x}_p(n)+\boldsymbol{n}(n)\right]\tag{24}$$

$$H_1:\boldsymbol{y}_{\mathrm{A}}(n)=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA2}}^{\mathrm{H}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA2}}\right\|}\left[\sqrt{P_{\mathrm{B}}\beta_{\mathrm{BA}}}\boldsymbol{h}_{\mathrm{BA}}\zeta r_2\boldsymbol{x}_p(n)+\sqrt{P_{\mathrm{E}}\beta_{\mathrm{EA}}}\boldsymbol{h}_{\mathrm{EA}}\boldsymbol{x}_p(n)+\boldsymbol{n}(n)\right]\tag{25}$$

对应的接收信号平均能量 Q_2 的均值为

$$\mu_2=\begin{cases}\left|\dfrac{\hat{\boldsymbol{h}}_{\mathrm{BA}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{BA}}}{\left\|\hat{\boldsymbol{h}}_{\mathrm{BA}}\right\|}\right|^2\xi^2r_2^2P_{\mathrm{B}}+\sigma_{\mathrm{A}}^2\to H_0\\ \left|\dfrac{\hat{\boldsymbol{h}}_{\mathrm{BA}}^{\mathrm{H}}\left(\sqrt{P_{\mathrm{B}}}\boldsymbol{h}_{\mathrm{BA}}r_2\xi+\sqrt{P_{\mathrm{E}}}\boldsymbol{h}_{\mathrm{EA}}\right)}{\hat{\boldsymbol{h}}_{\mathrm{BA}}}\right|+\sigma_{\mathrm{A}}^2\to H_1\end{cases}\tag{26}$$

且 $\sigma_2^2=\dfrac{1}{\Delta 2}\mu_2^2$。

显然，在受到导频攻击和不受攻击情况下，两段导频平均能量差值 Z 不同。当系统没有受到导频攻击时，平均能量差值只受到合法节点导频信号发射功率和高斯白噪声的影响；当系统中存在主动攻击时，平均能量差值由窃听者信号发射功率、合法用户导频信号发射功率和高斯白噪声三部分组成。因此，可以根据式(27)进行导频攻击检测

$$\begin{matrix}H_0\\ Z\lessgtr\gamma\\ H_1\end{matrix}\tag{27}$$

其中，γ 为设定的检测阈值。

检测阈值 γ 可以根据系统允许的虚警概率进行设置。根据虚警概率 P_{fa} 的定义可知

$$P_{\mathrm{fa}}=P\{Z>\gamma\mid H_0\}=\int_{\gamma}^{+\infty}f_0(x)\mathrm{d}x=1-F_0(\gamma)\tag{28}$$

其中，$f_0(x)$ 为系统不受导频攻击情况下接收平均能量差 Z 的概率密度函数，$F_0(x)$ 为 $f_0(x)$ 对应的累积分布函数。因此，给定 P_{fa} 可反推出检测阈值 γ，即

$$\gamma=F_0^{-1}(1-P_{\mathrm{fa}})\tag{29}$$

根据设定的检测阈值，可求得所提检测算法的检测概率为

$$P_d=P\{Z>\gamma\mid H_1\}=\int_{\gamma}^{+\infty}f_1(x)\mathrm{d}x=1-F_1(\gamma)\tag{30}$$

其中，$f_1(x)$ 为系统受到导频攻击时平均能量差 Z 的概率密度函数，$F_1(x)$ 为 $f_1(x)$ 对应的累积分布函数。

由上述的检测算法分析可知，相较于经典检测算法，本文算法只需要利用上行链路，不需要收发双方之间的信息交互。因此，本文算法不需要额外开销，实现的复杂度较低。

4　污染信道的信息恢复

由上述导频攻击检测方法可知，边缘服务器通过统计两段导频接收信号的平均能量差，根据式(27)判断边缘节点是否受到导频攻击。如果存在导频攻击，则由式(15)可以估计出边缘节点 Bob 到边缘服务器 Alice 不受污染的真实信道信息，即

$$\hat{\boldsymbol{h}}_{\mathrm{BA}}=\frac{\boldsymbol{z}_2-\boldsymbol{z}_1}{\zeta(r_2-r_1)}=\boldsymbol{h}_{\mathrm{BA}}+\boldsymbol{e}\tag{31}$$

其中，$\boldsymbol{e}=\dfrac{\dfrac{\boldsymbol{n}_2\boldsymbol{x}_{p2}^{\mathrm{H}}}{\Delta 2}-\dfrac{\boldsymbol{n}_1\boldsymbol{x}_{p1}^{\mathrm{H}}}{\Delta 1}}{\zeta(r_2-r_1)\sqrt{P_{\mathrm{B}}}}$。

因此，在边缘服务器向边缘节点发送数据阶段，可以基于式(31)估计所得的信道状态信息进行预编码设计，从而防止信号发射功率偏向窃听者，增强数据传输的安全性和数据传输效率。当然，由于估计所得的信道状态信息中包含高斯白噪声，下行保密速率不一定达到理想情况下的最大值。根据时分双工系统的信道互易性，从边缘服务器 Alice 到 Bob 的估计信道为 $\hat{\boldsymbol{h}}_{\mathrm{BA}}{}^{\mathrm{T}}$，因此波束成形向量为

$$\boldsymbol{w}=\frac{\hat{\boldsymbol{h}}_{\mathrm{BA}}{}^{\mathrm{T}}}{\sqrt{\mathbf{Tr}(\hat{\boldsymbol{h}}_{\mathrm{BA}}{}^{\mathrm{H}}\hat{\boldsymbol{h}}_{\mathrm{BA}})}}\tag{32}$$

其中，$\mathbf{Tr}(\boldsymbol{A})$ 为矩阵 $\boldsymbol{A}$ 的迹，$\hat{\boldsymbol{h}}_{\mathrm{BA}}{}^{\mathrm{T}}$ 为的 $\hat{\boldsymbol{h}}_{\mathrm{BA}}$ 转置，$\hat{\boldsymbol{h}}_{\mathrm{BA}}{}^{\mathrm{H}}$ 为 $\hat{\boldsymbol{h}}_{\mathrm{BA}}$ 的共轭转置。

5　仿真结果

为了验证本文所提导频攻击检测算法的性能，本节从以下几个方面对所提算法进行了计算机仿真。在仿真过程中，假设导频序列的总长度为

$\tau = 256$，Bob 和 Eve 离边缘服务器的距离相同，即大尺度衰落 $\beta_{\mathrm{BA}} = \beta_{\mathrm{EA}} = 1$。

首先，为了展示恶意节点导频攻击信号发射功率对检测概率的影响，在导频攻击信号发射功率从−15 dBW 变化到 15 dBW 时，对 $P_{\mathrm{fa}} = 0.001$ 和 $P_{\mathrm{fa}} = 0.01$ 这 2 种虚警概率下的检测概率进行了数值仿真，并与理论值进行了比较，仿真结果如图 3 所示。在仿真实验中，边缘服务器的天线数量设置为 M=4，第一段导频序列长度为 96，第二段子导频序列长度为 160，第二段导频的随机放大系数取 $r_2 = 0.5$。边缘节点 Bob 的导频信号发射功率 $P_{\mathrm{B}} = 10$ dBW，边缘服务器 Alice 处接收信号加性噪声方差为 $\sigma_{\mathrm{A}}^2 = 1$。从仿真结果可以看出，随着导频攻击信号发射信号功率的增大，被检测出的概率也不断增大。当 $P_{\mathrm{E}} = 10$ dBW 时，检测概率接近 100%，即当窃听者以与合法节点相同的发射功率进行导频攻击时，攻击都能被服务器节点成功检测。因此，所提导频攻击检测算法的灵敏度比较高。同时，还可以看出，系统要求的虚警概率越大，导频攻击被检测出的概率也越大，而且检测概率的仿真结果与理论分析非常吻合。

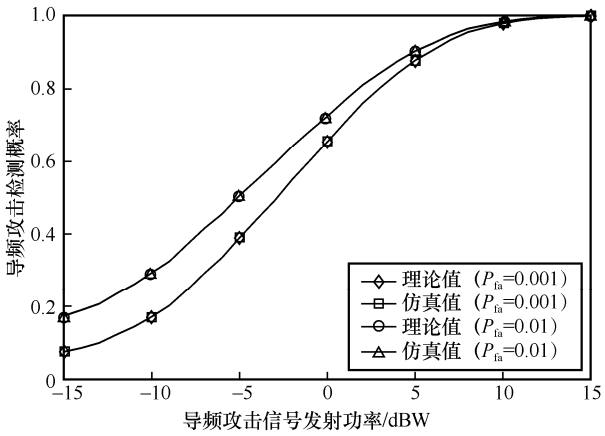


图 3　本文算法检测概率与导频攻击信号发射功率关系

在 $P_{\mathrm{B}} = P_{\mathrm{E}} = 10$ dBW，虚警概率分别为 $P_{\mathrm{fa}} = 0.001$ 和 $P_{\mathrm{fa}} = 0.01$ 的情况下，对检测概率随边缘服务器 Alice 天线数量变化进行了仿真，实验结果如图 4 所示。从仿真结果可知，随着服务器天线数量的不断增加，相同功率的导频攻击被检测出的概率不断增大。当接收天线数量大于 12 时，几乎所有导频攻击都能检测到。直观来看，天线数量越多，服务器接收到的攻击信号的样本数就越多，对接收信号合并之后的信号能量的差异就更大，也就更容易判断是否受到导频攻击。随着毫米波无线通信技术的不断发展，大规模天线阵列将不断应用于移动通信系统中。因此，本文所提的导频检测算法将在未来大规模多输入多输出毫米波和太赫兹通信系统中展现优越性能。

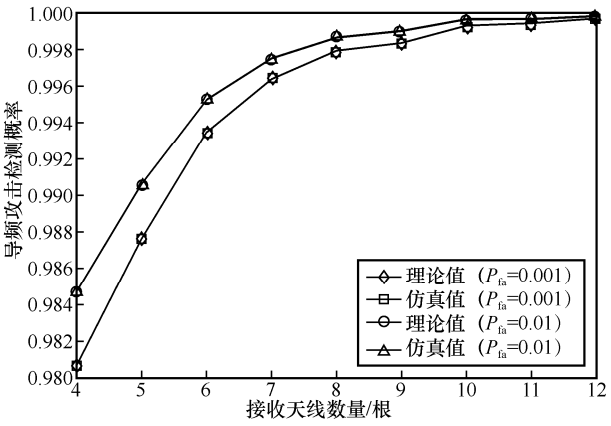


图 4　本文算法检测概率与接收天线数量关系

为了验证本文算法的优越性，将本文算法与 MDL[6]、ERD[13]、TPUT[9]和 TWTD[18]这 4 种经典算法进行了仿真对比，仿真结果如图 5 所示。不失不一般性，在仿真比较实验中的设置如下：在 MDL 算法中，外加导频序列上的发射功率分配比设置为 0.9；在 ERD 算法中，下行训练阶段的导频长度和上行导频长度设置为相同；在 TPUT 算法中，辅助节点导频发射功率设置为10 dBW；在 TWTD 算法中，下行训练长度等于上行训练长度乘以基站天线数；在本文算法中，假设第一段导频长度为 96，第二段子导频序列长度为 160，对应的变换系数 $r_2 = 0.5$；所有算法均不考虑大尺度衰落。从仿真结果可知，在相同的条件下本文算法的检测概率低于 MDL、TPUT 和 TWTD 算法，而高于 ERD 算法。但是 MDL 额外增加了导频序列长度，TPUT 算法需要第三方信任节点的辅助，TWTD 算法需要双向导频和收发端的信息交互。与此同时，在导频攻击信号发射功率 $P_{\mathrm{E}} < -10$ dBW 时，本文算法的检测概率高于 MDL、TWTD 和 ERD 算法。因此，本文算法更有利于检测出发射功率小、隐蔽性强的导频攻击。

为了展示恢复污染信道后边缘节点下载时可达速率的改善，将本文算法与不进行信道恢复时的情况进行了比较，仿真结果如图 6 所示。在仿真过程中，M=4，$P_{\mathrm{B}} = P_{\mathrm{E}} = 10$ dBW；边缘服务器在向边缘节点发射信号时采用最大比方式进行波束成

形。由仿真结果可知，基于恢复后的信道进行波束成形的可达速率不受导频攻击信号发射功率的影响，因此信道恢复的准确度很高。而不采取信道恢复措施时的可达速率随导频攻击发射功率的增大快速下降，即随着 P_{E} 的增大，越来越多的信号功率被窃听者接收，而合法边缘节点接收到的信号功率越来越小。通过本文算法的导频攻击检测和污染信道恢复后，下载速率能够保持恒定，既能保证正常的下载速率，又有效防止了交互信息被恶意节点窃听。

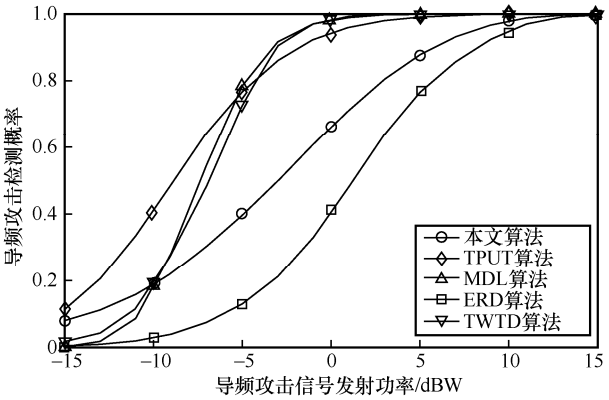


图 5　不同算法检测概率与导频攻击信号发射功率关系

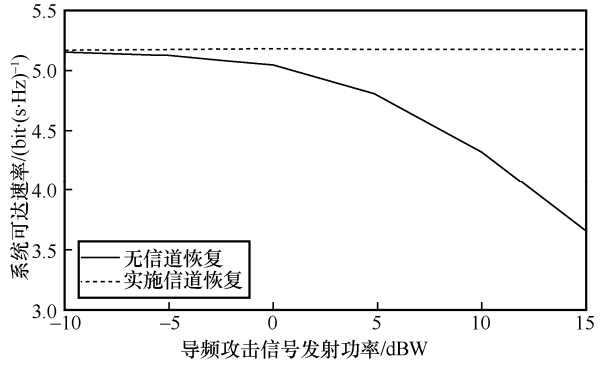


图 6　污染信道恢复后的可达速率

6　结束语

针对边端协同联邦学习中边缘节点容易受到导频攻击而导致下载速率降低和信号泄露的问题，本文提出了一种随机分割和加密方法的导频构建算法，并基于此提出一种信号平均能量差的导频攻击检测算法。利用本文所提算法，不仅能提高导频攻击的检测精度，而且可以恢复污染信道，提高边缘节点数据下载的速率和数据传输的安全性。随着毫米波技术的不断发展，移动终端配备多天线阵列成为未来发展趋势。因此，下一步笔者将对多天线和大规模阵列天线用户场景下的导频攻击检测与对抗展开研究。同时，在复杂的通信环境下，边缘节点如何准确检测出下行链路的导频攻击，并采取相应的对抗措施，以提高边缘节点任务卸载的速率和卸载数据的传输安全，这将为实现边缘智能提供保障。

参考文献：

[1] WANG J, CAO C M, WANG J P, et al. Optimal task allocation and coding design for secure edge computing with heterogeneous edge devices[J]. IEEE Transactions on Cloud Computing, 2022, 10(4): 2817-2833.

[2] 龙隆, 刘子辰, 陆在旺, 等. 移动边缘网络下服务缓存与资源分配联合优化策略[J]. 通信学报, 2023, 44(1): 64-74.
LONG L, LIU Z C, LU Z W, et al. Joint optimization strategy of service cache and resource allocation in mobile edge network[J]. Journal on Communications, 2023, 44(1): 64-74.

[3] MAO B M, LIU JJ, WU YY, et al. Security and privacy on 6G network edge: a survey[J]. IEEE Communications Surveys&Tutorials, 2023, 25(2): 1095-1127.

[4] 余雪勇, 邱礼翔, 宋家宁, 等. 无人机辅助边缘计算中安全通信与能效优化策略[J]. 通信学报, 2023, 44(3): 45-54.
YU X Y, QIU L X, SONG J N, et al. Security communication and energy efficiency optimization strategy in UAV-aided edge computing[J]. Journal on Communications, 2023, 44(3): 45-54.

[5] CSISZAR I, KORNER J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[6] TUGNAIT J K. Self-contamination for detection of pilot contamination attack in multiple antenna systems[J]. IEEE Wireless Communications Letters, 2015, 4(5): 525-528.

[7] ZHANG W L, LIN H, ZHANG R N. Detection of pilot contamination attack based on uncoordinated frequency shifts[J]. IEEE Transactions on Communications, 2018, 66(6): 2658-2670.

[8] XU W Y, YUAN C, XU S B, et al. On pilot spoofing attack in massive MIMO systems: detection and countermeasure[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 1396-1409.

[9] LIU X M, LI B, CHEN H B, et al. Detecting pilot spoofing attack in MISO systems with trusted user[J]. IEEE Communications Letters, 2019, 23(2): 314-317.

[10] WU Q Q, ZHANG R. Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming[J]. IEEE Transactions on Wireless Communications, 2019, 18(11): 5394-5409.

[11] ELHOUSHY S, IBRAHIM M, HAMOUDA W. Exploiting RIS for limiting information leakage to active eavesdropper in cell-free massive MIMO[J]. IEEE Wireless Communications Letters, 2022, 11(3): 443-447.

[12] AKBAR N, YAN S H, KHATTAK A M, et al. On the pilot contamination attack in multi-cell multiuser massive MIMO networks[J]. IEEE Transactions on Communications, 2020, 68(4): 2264-2276.

[13] XIONG Q, LIANG Y C, LI K H, et al. An energy-ratio-based ap-

proach for detecting pilot spoofing attack in multiple-antenna systems[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(5): 932-940.

[14] XU S B, XU W Y, PAN C H, et al. Detection of jamming attack in non-coherent massive SIMO systems[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(9): 2387-2399.

[15] GAO N, QIN Z J, JING X J. Pilot contamination attack detection and defense strategy in wireless communications[J]. IEEE Signal Processing Letters, 2019, 26(6): 938-942.

[16] AHMED A, ZIA M, HAQ I U, et al. Detection of pilot contamination attack for frequency selective channels[J]. IEEE Access, 2020, 8: 123966-123978.

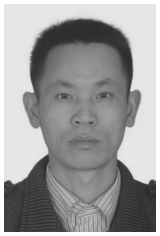
[17] WANG N, LI W W, ALIPOUR-FANID A, et al. Pilot contamination attack detection for 5G mmWave grant-free IoT networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 658-670.

[18] XIONG Q, LIANG Y C, LI K H, et al. Secure transmission against pilot spoofing attack: a two-way training-based scheme[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 1017-1026.

[19] TYLAVSKY D J, SOHIE G R L. Generalization of the matrix inversion lemma[J]. Proceedings of the IEEE, 1986, 74(7): 1050-1052.

[20] LIANG Y C, ZENG Y H, PEH E C Y, et al. Sensing-throughput tradeoff for cognitive radio networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(4): 1326-1337.

[作者简介]



王仕果（1975− ），男，湖南隆回人，博士，长沙理工大学教授，主要研究方向为通信系统物理层安全、无人机协同通信、毫米波通信、物联网等。

田淑娟（1982− ），女，湖南攸县人，博士，湘潭大学教授，主要研究方向为通信系统安全、边缘计算、物联网、隐私保护等。

邓清勇（1981− ），男，湖南武冈人，博士，广西师范大学特聘教授，主要研究方向为宽带无线通信、边缘计算、物联网、隐私保护、深度学习等。