基于信道指纹的毫米波MIMO系统身份欺骗攻击检测方案

杨立君[①] 李明航[①] 陆海涛[②③] 郭 林[*④]

[①](南京邮电大学物联网学院 南京 210003)

[②](中兴通讯股份有限公司 深圳 518057)

[③](深圳市5G接入网安全技术研究及应用重点实验室 深圳 518055)

[④](南京邮电大学现代邮政学院 南京 210003)

摘 要：针对毫米波多输入输出系统(MIMO)中的身份欺骗攻击问题，该文提出一种基于信道指纹的攻击检测方案。在波束域中，毫米波信道图样呈现波束的稀疏性和高方向特性，且这种波束域特性与终端位置有极高的相关性。该文将该波束域信道图样作为一种信道指纹，提出了一种基于信道指纹的身份欺骗攻击检测方案，将欺骗攻击中的终端身份认证问题建模成对其信道指纹的二分类问题，并使用基于监督学习的支持向量机算法求解该分类问题。为获得好的分类效果，基于对信道指纹的数值分析，比较了皮尔逊相关系数、余弦相似度、相关矩阵距离、欧氏距离等相似度指标。根据比较结果，选择最优的指标作为分类特征训练分类模型。仿真结果表明，即使在低信噪比条件下，该方案仍具有高认证准确性和鲁棒性。与现有相关机制相比，攻击检测精度显著提高。

关键词：信道指纹；身份欺骗攻击；毫米波；多输入输出；支持向量机

中图分类号：TN928 **文献标识码**：A **文章编号**：1009-5896(2023)12-4228-08

DOI: 10.11999/JEIT220934

Spoofing Attack Detection Scheme Based on Channel Fingerprint for Millimeter Wave MIMO System

YANG Lijun[①] LI Minghang[①] LU Haitao[②③] GUO Lin[④]

[①](*School of Internet of Things*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)

[②](*ZTE Corporation*, *Shenzhen* 518057, *China*)

[③](*Shenzhen Key Laboratory of 5G RAN Security Technology Research and Application*, *Shenzhen* 518055, *China*)

[④](*School of Modern Posts*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)

Abstract: Millimeter wave Multiple Input and Multiple Output (MIMO) channel exhibits beam sparsity and high directivity in the beam domain, and the beam domain channel pattern is highly correlated with the terminal position. In this paper, the beam domain channel pattern is regarded as a channel fingerprint. A channel fingerprint-based identity spoofing attacks detection scheme is proposed for millimeter-wave MIMO systems. The identity authentication problem is modeled as a binary classification problem of the corresponding channel fingerprint. Then, the supervised learning Support Vector Machine (SVM) algorithm is employed to solve the classification problem. In order to achieve good classification effect, different similarity indexes on channel fingerprint are compared based on the numerical analysis of the beam domain, and the one with the best classification effect is selected as the final classification feature to train the classifier model. The simulation results show that the proposed scheme has good authentication performance even under low signal-to-noise ratio conditions. Compared with the existing relative schemes, the detection accuracy is significantly improved.

Key words: Channel fingerprint; Identify spoofing Attacks; Millimeter-wave; Multiple Input and Multiple Output (MIMO); Support Vector Machine (SVM)

收稿日期：2022-07-08；改回日期：2023-03-30；网络出版：2023-03-31

*通信作者： 郭林 guolin@njupt.edu.com

基金项目：中兴通讯产学研(2023ZTE08-02)，南京邮电大学校级自然科学基金(NY222132)，中国博士后基金(2017M621798)，江苏省高等学校自然科学研究项目(19KJB510048)，江苏省研究生科研与实践创新计划项目(SJCX21_0300)

Foundation Items: ZTE Industry-University-Research Fund (2023ZTE08-02), The Natural Science Foundation of Nanjing University of Posts and Telecommunications (NY222132), The National Post-doctoral Fundation (2017M621798), The Universities Natural Science Research Project of Jiangsu Province (19KJB510048), The Postgraduate Research & Practice Innovation Program of Jiangsu Province (SJCX21_0300)

1　引言

由于使用了多种新兴物理层通信技术如毫米波(millimeter-Wave, mmWave)[1]，多输入输出(Multiple Input and Multiple Output, MIMO)[2]等，第五代通信技术(Fifth Generation, 5G)有望提供更快速更可靠的通信服务。但是，由于无线通信的广播特性，5G通信网络更易遭到攻击[3]，如身份欺骗攻击[4]等。已有的基于密码学的安全方案[5]面临安全强度不足的挑战，而基于信道的物理层认证技术是一项很有研究前景的网络安全技术，有望对当前基于密码学的安全方案进行补充和增强。目前大多数基于信道的认证方案主要利用信道状态信息(Channel State Information, CSI)[6]，接收信号强度(Received Signal Strength, RSS)[7]，功率谱密度(Power Spectral Density, PSD)[8]，信道冲激响应(Channel Impulse Response, CIR)[9]等传统信道特性。

在已有的基于信道的物理层认证技术中，具体的代表性工作包括：文献[10]分析了MIMO信道的波束表示，通过对原始信道矩阵进行2维离散傅里叶变换(Two Dimensional-Discrete Fourier Transform, 2D-DFT)可得到对应的波束域表示。文献[10]认为波束域本质上是对信号不同空间角度的采样。基于此项研究，许多研究者将信道的波束域表示应用在物理层认证技术中。文献[11]提出一种将波束域中主要路径分量的坐标作为认证特征的检测方案。为了统一认证特征的维度，该方案对主要路径的数目进行了固定处理。但是，主要路径的数目由于环境等因素的影响为不定值，会随着环境变化而改变，因此该方案不具备实际可行性。文献[12]提出一种利用波束域之间的矩阵二范数值作为认证特征的方案。但该方案仅在信道相关系数和信噪比(Signal-to-Noise Ratio, SNR)条件较高的情况下达到较高的认证准确度，且没有比较其他的指标，如皮尔逊系数和余弦相似度等。文献[13]提出在IEEE 802.11 ad网络中，利用波束搜索过程中扇区级扫描(Sector Level Sweep, SLS)所获得关于设备的信噪比轨迹作为认证特征，这种特征与设备内部构造及位置有关。但受限于IEEE 802.11 ad网络，此方法仅适用于该网络标准和室内办公室环境。文献[14]将毫米波设备本身天线阵列因固有缺陷而导致设备拥有的唯一的波束方向图作为认证特征，并使用了实际的60GHz软件无线电设备证实了该特征良好的分类性能。但波束方向图的获取需要较为精细的设备，该方法不适用于低功耗系统。

此外，以上方案中所使用的信道模型都仅适用于频率低于6GHz(sub-6 GHz)的通信系统。而恰恰相反，毫米波信号具备与sub-6 GHz信号完全不同的传播规律和信道特性[13]，较高的频率使得毫米波信号变化更快，信道相干时间更短，同时受多普勒效应的影响更明显[14]。由于这些因素的影响，以上方案均无法直接适用于5G mmWave MIMO系统。此外，以上方案均假设实验中终端始终处在静止状态，而这样的实验设置限制了对移动状态下终端的认证技术研究。

为解决以上不足，本文基于对mmWave MIMO信道的特性分析，将波束域特性与终端位置之间的高度相关性认作为一种信道指纹，提出一种基于此信道指纹的身份欺骗攻击检测方案。为了对移动状态下的终端进行身份认证技术研究，本文建立了具有空间一致性的信道模型，该模型可对移动终端进行建模。为更好地解决信道指纹分类问题，本文使用基于监督学习的支持向量机(Support Vector Machine, SVM)算法，并基于对波束域数值的分析，比较了不同的相似度指标，选择具有最佳分类效果的相似度指标作为分类特征。仿真结果表明，与其他方案相比，本文所提方案具备更好的认证性能。

2　系统模型

考虑如图1所示的5G mmWave MIMO时分双工(Time Division Duplexing, TDD)或频分双工(Frequency Division Duplexing, FDD)通信系统，其中Alice和Bob为合法通信终端，Bob提供通信服务，Eve为非法终端。假设Eve可通过修改自身的网络协议(Internet Protocol, IP)或媒体访问控制(Media Access Control, MAC)地址发起身份欺骗攻击以试图获取Bob的通信服务。在信道相干时间内，上下链路信道具有互易性。此外，Bob处在静止状态，Alice与Eve处在慢速移动状态，二者的移动轨迹如图1所示。

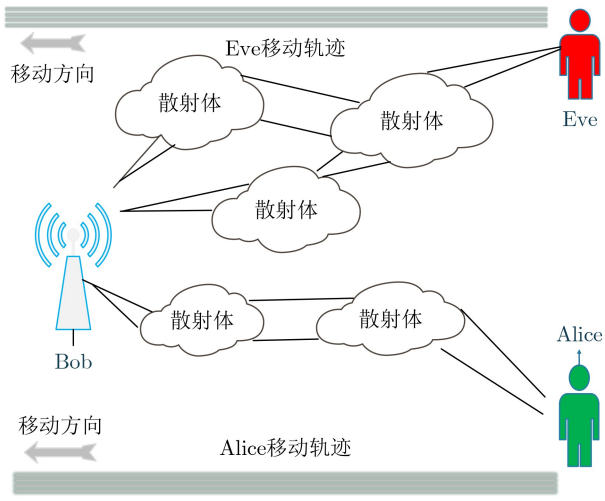


图 1 系统模型

本文中的物理层认证方案为辅助认证，即通信过程中的首次认证仍需由基于密码学的安全方案[15]来完成。在首次认证通过后，使用基于信道指纹的检测方案来保证后续通信过程中没有非法终端的入侵。模型中Alice处在移动状态，因此，在Alice与Bob基于密码学方案建立合法通信后Bob每隔一段时间发送一次导频信号，从而通过信道估计获取Alice的信道指纹信息。

3 基于信道指纹的身份欺骗攻击检测方案

3.1 mmWave MIMO 信道模型

统计空间信道模型(Statistical Spatial Channel Model, SSCM)[16]是一种面向毫米波信号建模且得到国际认可的信道模型，属于基于几何与基于地图的混合信道模型[17]。该模型以时间簇(Time Cluster, TC)和空间波瓣(Spatial Lobe, SL)为建模框架来生成对应的信道响应，具体形式可表示为

$$\boldsymbol{H}(t,\Theta_d,\Phi_d)=\sum_{n=1}^{N}\sum_{m=1}^{M_n}a_{m,n}\mathrm{e}^{\mathrm{j}\varphi_{m,n}}\cdot\delta(t-\tau_{m,n})\cdot\boldsymbol{g}_{\mathrm{TX}}(\Theta_d-\Theta_{m,n})\cdot\boldsymbol{g}_{\mathrm{RX}}(\Phi_d-\Phi_{m,n}) \tag{1}$$

其中，t是传播时间，Θ_d和Φ_d分别是来自发射方(Transmitter, TX)和接收方(Receiver, RX)的天线指向角，N和M_n分别是TC和TC中子路径的数量，$a_{m,n}$是从属于第n^{th}个TC的第m^{th}个子路径的路径增益，$\varphi_{m,n}$和$\tau_{m,n}$分别是从属于第n^{th}个TC的第m^{th}个子路径的相位和传播时延，$\boldsymbol{g}_{\mathrm{TX}}(\Theta)$和$\boldsymbol{g}_{\mathrm{RX}}(\Phi)$分别是多元天线阵列收发端的阵列响应矢量，$\Theta_{m,n}$和$\Phi_{m,n}$是每一个多径分量到达角(Angel of Arrival, AoA)和离开角(Angel of Departure, AoD)方位角/仰角的度数。

3.2 mmWave MIMO 信道指纹分析

式(1)中的$\boldsymbol{g}_{\mathrm{TX}}(\Theta)$和$\boldsymbol{g}_{\mathrm{RX}}(\Phi)$具体表达形式由天线类型和天线数量决定。对均匀线性阵列(Uniform Linear Array, ULA)而言，对应的阵列响应矢量表示为

$$\boldsymbol{g}(\theta)=\frac{1}{\sqrt{N}}\left[1,\ \mathrm{e}^{-\mathrm{j}\frac{2\pi}{\lambda}d\sin\theta},\ \mathrm{e}^{-\mathrm{j}2\cdot\frac{2\pi}{\lambda}d\sin\theta},\cdots,\ \mathrm{e}^{-\mathrm{j}(N-1)\frac{2\pi}{\lambda}d\sin\theta}\right]^{\mathrm{T}} \tag{2}$$

其中，d表示天线阵元间隔，λ为载波波长，N表示收发端阵列的阵元数量，典型的阵元间隔$d=\lambda/2$，$\boldsymbol{a}(\theta)\in\mathbb{C}^{N\times1}$。

通过对mmWave MIMO原始信道矩阵$\boldsymbol{H}$进行2D-DFT可得到对应的波束域表示$\boldsymbol{H}_{\mathrm{b}}$，对应关系为

$$\boldsymbol{H}_{\mathrm{b}}=\boldsymbol{U}_{\mathrm{r}}^{\mathrm{H}}\boldsymbol{H}\boldsymbol{U}_{\mathrm{t}} \tag{3}$$

其中，$\boldsymbol{U}_{\mathrm{r}}$和$\boldsymbol{U}_{\mathrm{t}}$分别是收、发端的阵列响应矩阵，由各个采样角的阵列响应矢量组成。$\boldsymbol{U}$正好是一个DFT酉矩阵，满足$\boldsymbol{U}^{\mathrm{H}}\boldsymbol{U}=\boldsymbol{U}\boldsymbol{U}^{\mathrm{H}}=\boldsymbol{I}$，具体表达式为

$$U(i,j)=\sqrt{\frac{1}{N}}\exp(-\mathrm{j}2\pi(i-1)(j-N/2)/N) \tag{4}$$

因此，式(1)可对应的改写为式(5)形式

$$H_{\mathrm{b}}=\frac{1}{\sqrt{N_{\mathrm{r}}N_{\mathrm{t}}}}\sum_{i=1}^{N_{\mathrm{r}}}\sum_{j=1}^{N_{\mathrm{t}}}H(i,j)a_{\mathrm{RX}}(\theta_i)a_{\mathrm{TX}}^{\mathrm{H}}(\phi_j) \tag{5}$$

其中，θ_i和ϕ_j分别是2D-DFT对应的虚拟采样角，满足$\theta_i=\dfrac{i}{N_{\mathrm{r}}-1}$，$\theta_j=\dfrac{j}{N_{\mathrm{t}}-1}$。

在波束域中可将mmWave MIMO信道的波束稀疏性和高度方向性表现出来，如图2所示。图2(a)和图2(b)分别表示天线数64×64和128×128时的原始信道矩阵(基于CSI)。可观察出对应信道的整体数据毫无分布规律且难以区分，这也是其认证性能下降的主要原因。图2(c)和图2(d)表示对应的波束域，其中大多数路径分量的功率都接近于零，仅有少数几条路径具有较高的功率，且波束域的空间精度与天线数量呈正相关。这种波束域信道图样与终端位置有极高的相关性。如果终端处在不同的位置(大于1个波长)，那么对应的波束域特性也不同，如图3所示，图3表示同一时刻Alice与Eve的波束域对比，可明显看出二者具有很大的差异。因此，本文将这种波束域信道图样作为一种信道指纹。

3.3 基于信道指纹的身份欺骗攻击检测方案

基于3.2节的分析，本文将欺骗攻击的身份检测问题建模成对其信道指纹的二分类问题。在n时刻，Alice发送请求服务消息，Bob通过基于密码学的安全方案与Alice建立通信。检测目标是确认第$n+1$时刻的通信终端是否仍为Alice。在检测之前，由于无法确认第$n+1$时刻通信终端的真实身份，因此我们使用$\boldsymbol{H}^{?}(n+1)$表示第$n+1$时刻终端的信道，？代表其身份尚未确认，接着Bob使用基于信道指纹的检测方案对终端进行识别，分为两种情况

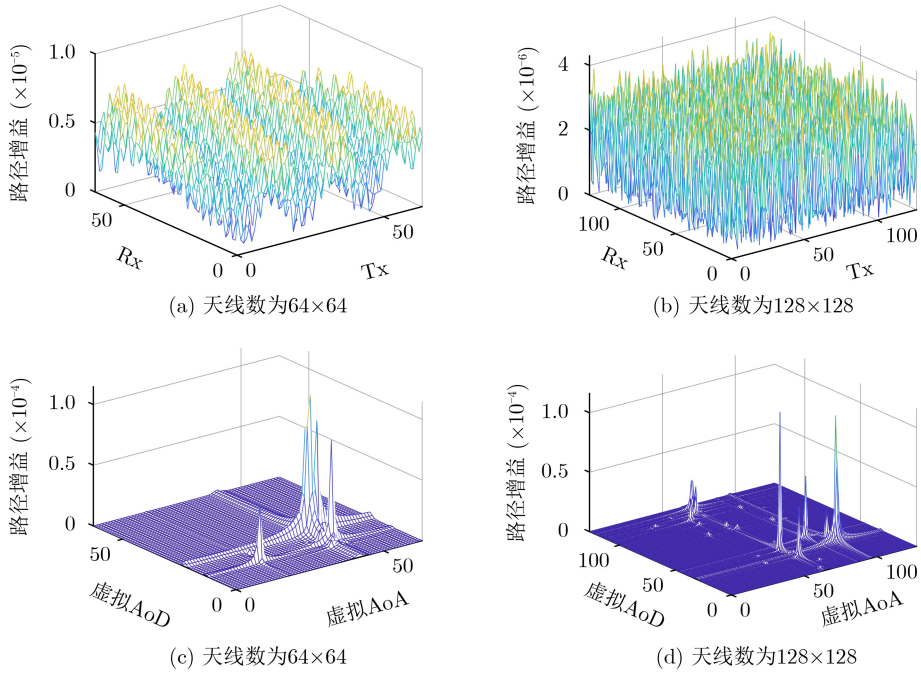
$$\left.\begin{aligned}&\mathrm{Cond}_0:\boldsymbol{H}^{?}(n+1)=\boldsymbol{H}^{\mathrm{A}}(n+1),\mathrm{Alice}\\&\mathrm{Cond}_1:\boldsymbol{H}^{?}(n+1)=\boldsymbol{H}^{\mathrm{E}}(n+1),\mathrm{Eve}\end{aligned}\right\} \tag{6}$$

在对信道进行波束域表示后，式(6)可改写为

$$\left.\begin{aligned}&\mathrm{Cond}_0:\boldsymbol{H}_{\mathrm{b}}{}^{?}(n+1)=\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n+1),\mathrm{Alice}\\&\mathrm{Cond}_1:\boldsymbol{H}_{\mathrm{b}}{}^{?}(n+1)=\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{E}}(n+1),\mathrm{Eve}\end{aligned}\right\} \tag{7}$$

Bob可通过式(8)来判断终端身份

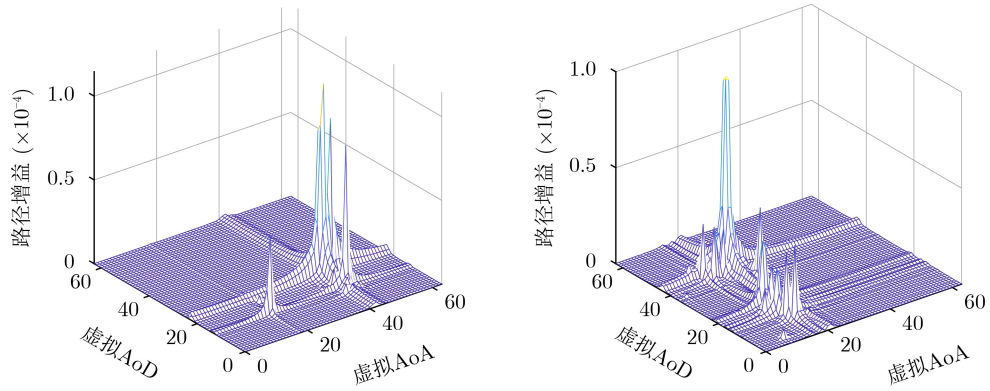
$$\left.\begin{aligned}&\mathrm{Cond}_0:\eta_0=\left\|\boldsymbol{H}_{\mathrm{b}}^{?}(n+1)-\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n)\right\|\le\eta_{\mathrm{th}}\\&\mathrm{Cond}_1:\eta_1=\left\|\boldsymbol{H}_{\mathrm{b}}^{?}(n+1)-\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n)\right\|\ge\eta_{\mathrm{th}}\end{aligned}\right\} \tag{8}$$



(a) 天线数为64×64　(b) 天线数为128×128

(c) 天线数为64×64　(d) 天线数为128×128

图 2 原始矩阵与波束域表示对比



(a) Alice的波束域表示　(b) Eve的波束域表示

图 3 Alice与Eve波束域对比(不同位置处)

其中，$\|\cdot\|$表示使用某种相似度指标计算$\boldsymbol{H}_{\mathrm{b}}^{?}(n+1)$和$\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n)$之间的相似度值的操作，$\eta$表示对应的相似度值。

基于信道指纹的身份欺骗攻击检测方案主要步骤如下：

步骤1　数据初始化：在n时刻，获取Alice的初始信道指纹$\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n)$；在$n$+1时刻，获取未知身份终端的信道指纹$\boldsymbol{H}_{\mathrm{b}}{}^{?}(n+1)$；

步骤2　输入：$\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n)$, $\boldsymbol{H}_{\mathrm{b}}{}^{?}(n+1)$；

步骤3　计算$\boldsymbol{H}_{\mathrm{b}}{}^{\mathrm{A}}(n)$与$\boldsymbol{H}_{\mathrm{b}}{}^{?}(n+1)$之间的相似度值$\eta$；

步骤4　根据η判断终端身份：如果$\eta < \eta_{\mathrm{th}}$，则判定为$\mathrm{Cond}_0$，终端身份为Alice；若$\eta > \eta_{\mathrm{th}}$，则判定为$\mathrm{Cond}_1$，终端身份为Eve；

步骤5　输出判定结果：Cond_0或Cond_1。

3.4 相似度指标的选择

为了获得好的分类效果，本文基于对信道指纹的数值分析比较了不同的相似度指标，并选择分类效果最好的一种指标作为本文方案所用的分类特征。

首先为缩小相似度指标的选择范围，从数值角度对二者的信道指纹进行分析。当天线数为64×64时，对400个采样点对应的Alice与Eve波束域的数值进行取平均值的操作，结果如图4所示。如图4所示，两个链路波束域数值均分布在1×10^{-9}～1×10^{-5}，且接近一半的数据分布在1×10^{-9}～1×10^{-8}，数值极小。另一方面，两个链路数据所处的分布区间也极为相似，接近80%的数据分布在1×10^{-9}～1×10^{-7}。因此，如果从矩阵之间元素距离的角度选择对应的相似度指标，如用向量空间中两

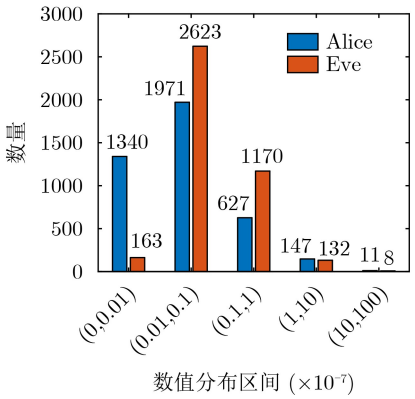


图 4 Alice与Eve波束域数值对比

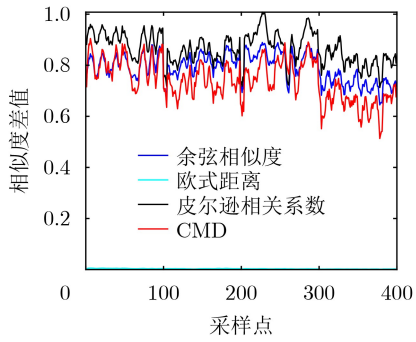


图 5 相似度差值

个矩阵之间直线距离作为衡量二者之间差异大小的欧氏距离[18]，分类效果会欠佳。

而从图3可以观察到，两个链路峰值之间的相对位置存在极大的差异性，并且其余次峰值之间的相对位置也存在一定的差异性，因此相比较侧重于距离上绝对差异的欧氏距离，如果考虑方向差异性，选择侧重于方向上相对差异的余弦相似度[19]，分类效果应该会极佳；或者考虑峰值之间的相对位置差异性，选择皮尔逊系数[20]和相关矩阵距离(Correlation Matrix Distance, CMD)[21]，分类效果也会较好。经过以上分析，最终选择余弦相似度，皮尔逊相关系数和相关矩阵距离作为备选指标。同时为了验证对信道指纹数值分析结果的正确性，选择欧氏距离作为实验对比指标。

本文根据相似度值的大小与稳定性选择最佳相似度指标。为得到最佳分类指标，首先计算Alice和Eve链路与上一时刻合法终端信道指纹之间的相似度值，接着相减取相似度差值，差值越大说明该指标的分类效果更好；为便于分辨，将差值归一化处理到0到1之间，越接近1，说明链路之间差异越大，分类效果更优。如图5所示，当相似度指标为皮尔逊相关系数时，两个链路的差异极其明显，几乎接近于1；也正如先前的分析，当指标为欧氏距离时，两个链路几乎没有差异，接近于0。因此，选择皮尔逊相关系数作为本文方案所使用的相似度指标。

3.5 基于机器学习的分类算法

3.3节将身份欺骗攻击的检测问题建模成对其信道指纹的二分类问题，可通过比较未知身份终端与前一时刻合法终端信道指纹之间的相似度值η判断其身份，3.4节经对比选出最佳相似度指标-皮尔逊相关系数。本小节，为了优化分类算法的性能，使用基于监督学习的SVM算法来解决信道指纹的二分类问题。将皮尔逊相关系数作为分类特征，利用SVM算法训练分类模型，并用该分类模型对终端身份进行判定，可有效提高方案性能。基于SVM的信道指纹分类算法主要步骤如下：

步骤1 初始化：根据3.1节的信道模型生成合法链路Alice-Bob的N个连续信道矩阵$\boldsymbol{H}^{\mathrm{Alice}}$、非法链路Eve-Bob的$N$个连续信道矩阵$\boldsymbol{H}^{\mathrm{Eve}}$；

步骤2 提取信道指纹：对信道采样数据进行2D-DFT，得到对应的信道指纹$\boldsymbol{H}_{\mathrm{b}}^{\mathrm{Alice}}$和$\boldsymbol{H}_{\mathrm{b}}^{\mathrm{Eve}}$；

步骤3 计算分类特征：在皮尔逊相关系数的衡量下，分别计算n+1时刻信道指纹$\boldsymbol{H}_{\mathrm{b}}^{\mathrm{Alice}}(n+1)$和$\boldsymbol{H}_{\mathrm{b}}^{\mathrm{Eve}}(n+1)$与$n$时刻$\boldsymbol{H}_{\mathrm{b}}^{\mathrm{Alice}}(n)$之间的相似度值$\eta_{n+1,n}^{\mathrm{Alice}}$和$\eta_{n+1,n}^{\mathrm{Eve}}$作为分类特征；

步骤4 数据预处理：对数据标签化，将$\eta_{n+1,n}^{\mathrm{Alice}}$定为正类$\mathrm{Y}_0$，标签为“合法”，$\eta_{n+1,n}^{\mathrm{Eve}}$定为负类$\mathrm{Y}_1$，标签为“非法”；

步骤5 输入：Y_0和Y_1；

步骤6 划分数据集：70%为训练集，30%为测试集；

步骤7 通过对训练集进行学习，得到分类模型，使用测试集测试分类模型；

步骤8 输出：“合法”或“非法”，拒真率，认假率，认证成功率。

4 仿真结果与分析

为验证本文方案的性能，本节首先在不同的SNR条件下，对基于CSI的传统方案[22]，文献[11]给出的物理层认证方案，文献[12]给出的欺骗攻击检测方案以及本文方案进行了性能对比；然后在不同的终端移动速度、天线数量条件下对所提方案的检测性能进行了进一步的验证。

4.1 仿真参数设置

除图6对应的仿真实验参数与表1、表2部分不同之外，其余仿真实验参数设置均按照表1、表2，且其余未列出的与实验相关的环境参数均按照文献[16]。

4.2 实验结果及分析

本小节从认证准确率和受试者工作特征(Re-

ceiver Operating Characteristic, ROC)曲线的角度出发分析所提方案的认证性能。

为对比说明本文所提方案的有效性，当信道相关系数为0.2时，在不同的SNR条件下，比较传统方案[22](基于CSI方案)，文献[11]认证方案，文献[12]检测方案以及本文方案的认证成功率，结果如图6所示。从图6可以看出，传统方案的认证性能较差，无法保障安全通信。而与其他同类方案相比，本文方法具有良好的认证性能，即使在SNR较低的情况下，整体认证准确率基本保持在96%以上，具有较好的鲁棒性。图7为SNR为5 dB时，基于SVM的检测方案的ROC曲线。从图7可以看出，此时的曲线下面积(Area Under Curve, AUC)为1，接近于完全识别，此时认证成功率为99.3%。图7表明本文所提基于信道指纹的检测方案具有良好的认证性能。

另外，为了研究移动速度、天线数量对所提方案检测性能的影响，本文进行了相应的仿真实验，实验结果如图8所示。除天线数量与移动速度设置不同之外，其余仿真实验参数均参照表1、表2。从图8可以看出，所提方案的认证准确率与天线数量呈正相关，这是因为随着天线数量的增加，其波束域的空间精度也会提高，更加利于识别；而随着移动速度的增加，准确率也会下降，这是因为移动速度的增加会导致与终端位置有关的信道指纹特性变化得更快，增加了识别的难度，但即使当终端移动速度为5 m/s时，所提方案仍可以保持95%的认证准确率，表明所提方案具备较强的鲁棒性，能够在时变环境下保障安全通信。

表 1　信号仿真参数设置

信号参数	频率	带宽	天线类型	天线数目
数值	73 GHz	800 MHz	ULA	64×64

表 2　用户仿真参数设置

用户参数	移动距离	速度	轨迹	采样间隔
数值	40 m	1 m/s	图1	0.1 次/s

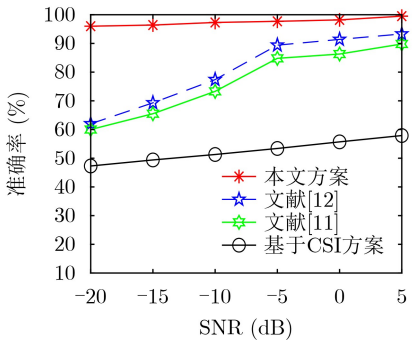


图 6 准确率对比

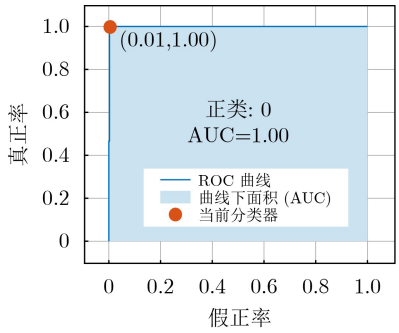


图 7 ROC曲线

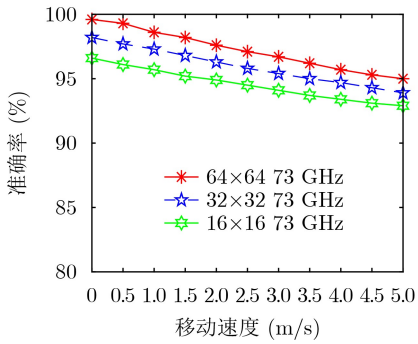


图 8 不同天线数量以及移动速度下的认证准确率

5　结论

本文提出了一种mmWave MIMO系统中基于信道指纹的身份欺骗攻击检测方案。本方案将波束域特性认作为一种信道指纹，并将欺骗攻击中的身份检测问题建模成对其信道指纹的二分类问题。选用基于监督学习的SVM算法，对比分析了不同的相似度指标，选用具有最佳分类性能的指标皮尔逊相关系数作为SVM算法的分类特征。仿真结果表明，与其它方案相比，即使在低SNR条件下，本文所提方案仍具有较高的认证准确率，对于不同频率、天线数量、移动速度(低速)具有较好的鲁棒性。本文方案所基于的信道指纹与终端位置强相关，因此本文方案的局限性在于无法检测共址攻击，这也是目前信道指纹类认证方案所共有的局限性。

参 考 文 献

[1] SEKER C, GÜNESER M T, and OZTURK T. A review of millimeter wave communication for 5G[C]. The 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2018: 1–5. doi: 10.1109/ISMSIT.2018.8567053.

[2] HEATH R W, GONZÁLEZ-PRELCIC N, RANGAN S, *et al*. An overview of signal processing techniques for millimeter wave MIMO systems[J]. *IEEE Journal of*

Selected Topics in Signal Processing, 2016, 10(3): 436–453. doi: 10.1109/JSTSP.2016.2523924.

[3] WANG Ning, LI Weiwei, WANG Pu, *et al*. Physical layer authentication for 5G communications: Opportunities and road ahead[J]. *IEEE Network*, 2020, 34(6): 198–204. doi: 10.1109/MNET.011.2000122.

[4] YILMAZ M H and ARSLAN H. A survey: Spoofing attacks in physical layer security[C]. The IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), Clearwater Beach, USA, 2015: 812–817. doi: 10.1109/LCNW.2015.7365932.

[5] MENEZES A J, VAN OORSCHOT P C, and VANSTONE S A. Handbook of Applied Cryptography[M]. Boca Raton: CRC Press, 1996.

[6] PAN Fei, WEN Hong, LIAO Runfa, *et al*. Physical layer authentication based on channel information and machine learning[C]. The 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, USA, 2017: 364–365. doi: 10.1109/CNS.2017.8228660.

[7] AHMADPOUR D and KABIRI P. Detecting forged management frames with spoofed addresses in IEEE 802.11 networks using received signal strength indicator[J]. *Iran Journal of Computer Science*, 2020, 3(3): 137–143. doi: 10.1007/s42044-020-00053-3.

[8] GALTIER F, CAYRE R, AURIOL G, *et al*. A PSD-based fingerprinting approach to detect IoT device spoofing[C]. The IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC), Perth, Australia, 2020: 40–49. doi: 10.1109/PRDC50213.2020.00015.

[9] ALAM J and KENNY P. Spoofing detection employing infinite impulse response—constant Q transform-based feature representations[C]. The 25th European Signal Processing Conference (EUSIPCO), Kos, Greece, 2017: 101–105. doi: 10.23919/EUSIPCO.2017.8081177.

[10] SAYEED A M. Deconstructing multiantenna fading channels[J]. *IEEE Transactions on Signal Processing*, 2002, 50(10): 2563–2579. doi: 10.1109/TSP.2002.803324.

[11] TANG Jie, XU Aidong, JIANG Yixin, *et al*. MmWave MIMO physical layer authentication by using channel sparsity[C]. The 2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS), Dalian, China, 2020: 221–224. doi: 10.1109/ICAIIS49377.2020.9194916.

[12] LI Weiwei, WANG Ning, JIAO Long, *et al*. Physical layer spoofing attack detection in MmWave massive MIMO 5G networks[J]. *IEEE Access*, 2021, 9: 60419–60432. doi: 10.1109/ACCESS.2021.3073115.

[13] WANG Ning, JIAO Long, WANG Pu, *et al*. Exploiting beam features for spoofing attack detection in mmWave 60-GHz IEEE 802.11ad networks[J]. *IEEE Transactions on Wireless Communications*, 2021, 20(5): 3321–3335. doi: 10.1109/TWC.2021.3049160.

[14] BALAKRISHNAN S, GUPTA S, BHUYAN A, *et al*. Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 1831–1845. doi: 10.1109/TIFS.2019.2948283.

[15] HEMADEH I A, SATYANARAYANA K, EL-HAJJAR M, *et al*. Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(2): 870–913. doi: 10.1109/COMST.2017.2783541.

[16] JU Shihao and RAPPAPORT T S. Millimeter-wave extended NYUSIM channel model for spatial consistency[C]. The 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018: 1–6. doi: 10.1109/GLOCOM.2018.8647188.

[17] LIM Y G, CHO Y J, SIM M S, *et al*. Map-based millimeter-wave channel models: An overview, guidelines, and data[EB/OL]. http://arxiv.org/abs/1711.09052, 2017.

[18] GOWER J C and LEGENDRE P. Metric and Euclidean properties of dissimilarity coefficients[J]. *Journal of Classification*, 1986, 3(1): 5–48. doi: 10.1007/BF01896809.

[19] 卜凡鹏, 陈俊艺, 张琪祁, 等. 一种基于双层迭代聚类分析的负荷模式可控精细化识别方法[J]. 电网技术, 2018, 42(3): 903–910. doi: 10.13335/j.1000-3673.pst.2017.1397.
BU Fanpeng, CHEN Junyi, ZHANG Qiqi, *et al*. A controllable refined recognition method of electrical load pattern based on bilayer iterative clustering analysis[J]. *Power System Technology*, 2018, 42(3): 903–910. doi: 10.13335/j.1000-3673.pst.2017.1397.

[20] YOU Yang, DEMMEL J, CZECHOWSKI K, *et al*. CA-SVM: Communication-avoiding support vector machines on distributed systems[C]. The 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, 2015: 847–859. doi: 10.1109/IPDPS.2015.117.

[21] SINHASHTHITA W and JEARANAITANAKIJ K. Improving KNN algorithm based on weighted attributes by Pearson correlation coefficient and PSO fine tuning[C]. The 5th International Conference on Information Technology (InCIT), Chonburi, Thailand, 2020: 27–32. doi: 10.1109/InCIT50588.2020.9310938.

[22] XIAO L, GREENSTEIN L, MANDAYAM N, *et al*. Fingerprints in the ether: Using the physical layer for wireless authentication[C]. The 2007 IEEE International Conference on Communications, Glasgow, UK, 2007: 4646–4651. doi: 10.1109/ICC.2007.767.

杨立君：女，讲师，研究方向为无线网络与信息安全.

李明航：男，硕士生，研究方向为物理层身份认证.

陆海涛：男，高级工程师，研究方向为5G/B5G/6G通信安全技术.

郭 林：男，讲师，研究方向为MIMO天线系统及安全技术.

责任编辑：陈 倩