特防科技反谍技术研究院

从单点探测到空间感知：技术架构、核心算法与实战数据

版本 V1.0 • 2026年9月 • 密级：公开

文档编号 TF-RD-WP-2026-001 · 火眼探针B 软著登记号 R20260000136180

基于 327 次真实检测，系统阐述多节点空间感知反窃听检测的技术架构、核心算法与实战数据，定义行业技术基准。

执行摘要

本白皮书由特防科技反谍技术研究院撰写，系统阐述多节点空间感知反窃听检测技术的架构原理、关键指标与实战验证结果，旨在为保密场所、办公环境及关键基础设施的无线安全检测提供可量化的技术基准。

一、威胁演进：从"持续发声"到"近乎静默"

无线窃听与定位设备的信号特征正经历结构性迁移。传统GSM蜂窝类设备占空比高（>30%）、发射持续、功率典型达33dBm，单点频谱仪即可清晰捕获其TDMA帧结构。然而，威胁主体已向低占空比、窄带、间歇发射方向演进：4G Cat-M/NB-IoT占空比降至<5%，占用带宽仅200kHz；BLE蓝牙低功耗类设备占空比更低于0.1%，广播间隔可延长至数分钟，单次发射仅毫秒级。设备越"安静"，传统探测手段越趋失效。

二、核心问题：单点探测架构的捕获概率困境

传统单点手持探测器采用离散扫描机制，其根本缺陷可由捕获概率定量刻画。设单次扫描驻留时间为 T_scan，设备单次发射时长为 T_burst，则单点探测器单次扫描的捕获概率为：

P_capture = T_burst / T_scan

以BLE设备为例，T_burst 为毫秒级、占空比<0.1%，代入典型扫描周期可得 P_capture = 0.1%。这意味着单点探测器需重复上千次扫描才可能捕获一次BLE广播，在工程上不可行。该困境并非操作水平问题，而是时间、空间、数据三个维度上的架构性缺陷。

三、解决方案：多节点空间感知技术路线

特防科技反谍技术研究院提出第三代多节点空间感知架构，以"空间感知系统"替代"更强的单点探测器"。技术链路为：3D空间建模（体素网格0.5m）→ 科学布点（8–10个节点，任意位置≥3节点覆盖）→ 多节点同步采集（NTP同步<1ms）→ 云端算法反算（DBSCAN聚类、WLS定位、path loss修正）→ 报告生成。系统硬件为火眼探针（ESP32-S3 + AD8317对数检波，覆盖1MHz–10GHz，50dB动态范围，±1dB精度）。

四、关键成果：327次实战检测数据摘要

截至2026年9月，特防科技反谍技术研究院悟空系统累计完成327次检测。核心数据如下表所示。

指标	数值
总检测次数	327次（办公室142、会议室86、酒店61、住宅38）
检出异常设备次数占比	办公室68%、会议室74%、酒店52%、住宅41%
平均异常设备数	办公室2.3个、会议室2.7个、酒店1.8个、住宅1.5个
设备类型分布	BLE 38%、WiFi 27%、GSM 18%、4G Cat-M/NB-IoT 12%、其他5%
活跃设备检出率	>95%
误报率	<5%（金箍SPC行为检测误报率<0.3%）
定位精度	±1.5m（开阔空间）、±3m（典型办公室）

表1：327次实战检测核心数据摘要。数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

藏匿位置排行显示：电源插座/充电器31% > 天花板检修口19% > 通风管道14% > 会议桌下方11% > 绿植盆栽8% > 家具缝隙6% > 墙面开关5% > 空调出风口4% > 其他2%。

五、系统形态：悟空系统与金箍系统

特防科技反谍技术研究院提供两种系统形态。悟空系统面向单次或短期检测任务，部署周期30min–2h，适用于办公室排查、会议室安检、酒店入住检查。金箍系统面向7×24持续监测，硬件永久部署，在悟空系统基础上扩展设备指纹基线库、EKF轨迹追踪引擎、SPC异常行为检测三个核心模块，适用于保密会议室、核心机房、高管办公室。

六、核心结论

第一，反窃听检测的主要矛盾已从"发现强信号"转为"捕获弱而间歇的信号"，单点探测架构在BLE等低占空比设备面前存在0.1%量级的捕获概率天花板。第二，多节点空间感知通过时间连续、空间冗余、算法反算三个维度的架构改进，将活跃设备检出率提升至>95%，误报率控制在<5%。第三，327次实战数据验证了该架构在办公室、会议室、酒店、住宅四类场景的有效性。第四，射频检测对离线录音/存储类设备无效，完整方案须包含物理排查环节。

目录

本目录为《多节点空间感知反窃听检测技术白皮书（2026）》全书结构索引。本白皮书由特防科技反谍技术研究院编制，全部数据来源于研究院2026年度检测数据库与内部技术报告。各章页码以"—"占位，最终版以排版稿为准。

前置内容

- 封面 —
- 执行摘要 —
- 目录 —

正文

- 第1章 问题定义：从GSM到BLE的威胁演进 —
- 1.1 窃听设备形态的代际迁移
- 1.2 BLE低占空比带来的检测盲区
- 1.3 从传音视频到定位追踪的威胁重构
- 第2章 技术演进：三代反窃听检测技术路线对比 —
- 2.1 第一代：单点非线性结检测
- 2.2 第二代：频谱扫描与特征匹配
- 2.3 第三代：多节点空间感知
- 第3章 核心架构：多节点空间感知系统设计 —
- 3.1 火眼探针硬件架构
- 3.2 体素网格与空间建模
- 3.3 时间同步与数据汇聚
- 第4章 五步技术链路：从3D建模到检测报告 —
- 4.1 空间建模
- 4.2 信号采集
- 4.3 聚类定位
- 4.4 行为检测
- 4.5 报告生成
- 第5章 BLE专项：定位追踪威胁与火眼探针B —
- 5.1 BLE广播机制与捕获概率分析
- 5.2 火眼探针B设计原理
- 5.3 软著登记号 R20260000136180
- 第6章 实战数据：327次检测量化分析 —
- 6.1 场景分布与异常检出
- 6.2 设备类型与藏匿位置
- 6.3 检出率、误报率与定位精度
- 第7章 系统形态：悟空系统与金箍系统 —
- 7.1 悟空系统
- 7.2 金箍系统
- 7.3 系统选型对照

- 第8章 选型框架：6标准与7步决策流程 —
- 第9章 场景与SOP：标准作业流程 —
- 第10章 结论与展望 —

附录

- 附录A 五类设备信号特征表 —
- 附录B 技术参数汇总 —
- 附录C 术语表 —
- 附录D 参考文献 —

全书结构概览

部分	章节	核心内容	页码
前置	封面、执行摘要、目录	研究背景与核心结论	—
威胁与路线	第1–2章	GSM到BLE威胁演进、三代技术路线	—
架构与链路	第3–4章	多节点空间感知架构、五步技术链路	—
专项与数据	第5–6章	BLE专项、327次检测量化分析	—
形态与选型	第7–8章	悟空/金箍系统、6标准7步决策	—
落地与总结	第9–10章	场景SOP、结论与展望	—
附录	附录A–D	信号特征、参数、术语、参考文献	—

表0-1 全书结构概览（来源：特防科技反谍技术研究院《多节点空间感知反窃听检测技术白皮书（2026）》编制组）

第1章 问题定义：从GSM到BLE的威胁演进

1.1 威胁演进：GSM→WiFi→4G Cat-M/NB-IoT→BLE

反窃听检测所面对的威胁环境，在过去十余年间发生了结构性变化。这一变化的本质，不是窃听设备"变得更多"，而是其无线发射特征持续向"更短、更弱、更稀疏"的方向演进。据特防科技反谍技术研究院《电磁信号特征库》（2026）的实测数据，当前活跃于典型办公与会议场景的异常射频设备，已形成以低占空比协议为主体的分布格局。

1.1.1 五类设备的信号特征差异

按检测难度从低到高排列，常见无线窃听/定位设备可分为五类：GSM蜂窝类、WiFi类、4G Cat-M/NB-IoT类、BLE蓝牙低功耗类、离线录音/存储类。五类设备在中心频率、占用带宽、占空比、发射周期、RSSI范围与时域波形六个维度上存在本质差异，具体如表1-1所示。

表1-1 五类无线窃听/定位设备电磁信号特征对比

设备类型	中心频率	占用带宽	占空比	典型发射周期	RSSI范围	时域波形特征	检测难度
GSM蜂窝类	900/1800 MHz	200 kHz	高（>30%）	持续	−30 ~ −60 dBm	连续脉冲串	易
WiFi类	2.4/5 GHz	20/40/80 MHz	中（5–20%）	突发	−40 ~ −70 dBm	突发数据包	中
4G Cat-M/NB-IoT类	B1/B3/B38/B39/B40/B41	1.4 MHz（Cat-M）/200 kHz（NB-IoT）	低（<5%）	周期性	−50 ~ −80 dBm	窄带脉冲	难
BLE蓝牙低功耗类	2.4 GHz（40信道）	2 MHz	极低（<0.1%）	间歇（可达1次/小时）	−60 ~ −90 dBm	毫秒级短脉冲	很难
离线录音/存储类	无	无	无	无	无	不发射信号	射频无效

数据来源：特防科技反谍技术研究院电磁信号特征库，基于AD8317对数检波器（1MHz–10GHz，50dB动态范围，±1dB精度）在受控电磁暗室环境下的实测采集，采样率100kSPS，每组数据采集时长60分钟，重复三次取均值。

从表1-1可以读出一条清晰的演进规律：**设备的危险程度与其"安静程度"成正比。**GSM设备发射功率高（典型2W/33dBm）、占空比>30%、TDMA帧结构稳定，传统手持频谱仪即可清晰识别；WiFi设备占空比降至5–20%，需从大量合法AP中区分非法设备；4G Cat-M/NB-IoT进一步将带宽收窄至1.4MHz乃至200kHz、占空比压至<5%；BLE则将间歇性推向极致——占空比<0.1%，单次发射毫秒级，广播间隔可达数分钟。

1.1.2 BLE占空比<0.1%的物理含义

占空比<0.1%并非一个抽象的统计指标，而是一个具有明确物理后果的约束条件。其含义可分解为三个层面：

第一，时间层面的极端稀疏。 若BLE设备广播间隔为10.24s、单次发射时长<10ms，则其在一个完整广播周期内的发射时间占比约为0.1%。若广播间隔延长至数分钟（部分低功耗追踪器采用此配置），占空比将进一步降至0.01%量级。这意味着在任意一个随机选取的1秒观测窗口内，设备处于发射状态的概率不足千分之一。

第二，能量层面的低可探测性。 BLE Class 2设备典型发射功率约2.5mW（4dBm），Class 3可低至1mW（0dBm）。经室内传播衰减后，接收端RSSI通常落在−60 ~ −90 dBm区间。传统宽频扫描模式下频谱仪灵敏度约为−80 ~ −90 dBm，意味着相当一部分BLE信号处于或低于探测阈值。

第三，协议层面的抗追踪性。 BLE工作于2.4GHz ISM频段的40个信道（3个广播信道37/38/39 + 37个数据信道），采用跳频广播机制，且随机MAC地址约每15分钟更换一次。即便捕获到单次广播，也无法通过MAC地址持续追踪同一设备。

综合上述三点，BLE设备构成了当前反窃听检测中最具挑战性的一类威胁。需要指出的是，BLE不适合传输音视频数据，其真实威胁形态是**定位追踪**（AirTag类设备），而非传统意义上的音频窃听。这一威胁性质的转变，进一步要求检测系统从"发现信号"升级为"识别行为"。

1.2 单点架构的根本缺陷

1.2.1 捕获概率的数学推导

单点探测器对BLE设备的捕获能力，可由捕获概率模型严格推导。设BLE设备单次发射时长为T_burst，单点探测器单次扫描周期为T_scan，则单次扫描恰好覆盖发射窗口的概率为：

P_capture = T_burst / T_scan

代入典型参数：BLE单次发射时长T_burst取毫秒级（以1ms计），传统手持频谱仪扫描周期T_scan取3–10秒（以1s计，即1000ms），则：

P_capture = 1ms / 1000ms = 0.1%

即单点探测器单次扫描捕获BLE发射的概率仅为0.1%。若考虑BLE广播间隔可达数分钟、单次发射时长可能短于1ms，实际捕获概率将进一步低于该值。这一推导揭示了一个关键事实：**单点探测器的低检出率并非操作者水平问题，而是由时间窗口的数学关系决定的架构性限制。**提高扫描频率只能线性改善捕获概率，无法从根本上解决间歇发射的覆盖问题。

1.2.2 随机MAC与跳频的双重障碍

即便单点探测器侥幸捕获到BLE信号，仍面临识别层面的障碍。BLE设备普遍采用随机MAC地址，约每15分钟更换一次，使得基于MAC地址的设备追踪失效。同时，BLE在37/38/39三个广播信道间跳频广播，单点接收难以持续跟踪同一设备的完整跳频序列。这意味着单点架构不仅"难以发现"，而且"发现了也难以确认"。

1.2.3 三重架构缺陷

单点架构的缺陷可归纳为三个相互关联的层面：

时间窗口矛盾。 单点扫描是离散时间采样，操作者在空间内移动，每个位置仅停留极短时间。BLE设备每小时仅发射数毫秒，单点扫描覆盖到发射窗口的概率极低。反复扫描无法保证覆盖所有时间窗口，因为设备的发射时刻本身具有随机性。

空间盲区。 单点探测器存在物理盲区。家具背后、墙体夹层、天花板检修口等位置，信号经遮挡后衰减严重。据特防科技反谍技术研究院《藏匿位置分析报告》（2026），电源插座/充电器（31%）、天花板检修口（19%）、通风管道（14%）位列藏匿位置前三，这些位置恰恰是单点扫描最易遗漏的区域。

操作者依赖。 检测效果完全取决于操作者经验。同一空间、同一设备，不同操作者可能得出不同结论。检测过程缺乏量化标准，结果不可复现、不可交叉验证。

1.3 行业代差：三代技术路线的本质差异

反窃听检测技术路线可划分为三代：第一代单点手持探测、第二代固定点位监测、第三代多节点空间感知。三者的差异并非"精度高一点、覆盖广一点"的量变，而是架构层面的质变。

第一代（单点手持探测） 采用离散时间采样与零维空间感知，依赖人工判读频谱图。其能力边界为：对GSM有效，对WiFi部分有效，对4G Cat-M/NB-IoT容易遗漏，对BLE几乎无效。

第二代（固定点位监测） 通过固定安装设备解决了时间窗口问题，实现持续监听，但空间覆盖仍受限于单点探测半径，且各点位独立工作，缺乏多节点数据融合与协同定位能力。

第三代（多节点空间感知） 实现了三项架构跃迁：从**离散采样到连续覆盖**——8–10个节点7×24小时在线，任意时刻至少有一个节点处于BLE广播信道上；从**零维感知到三维感知**——多节点同步测量同一信号RSSI，通过加权最小二乘法（WLS，path loss指数n=3.5）结合3D空间模型反算信号源三维坐标，定位精度达±1.5m（开阔空间）、±3m（典型办公室）；从**人工判读到算法反算**——经NTP时间同步（<1ms）、DBSCAN聚类（eps=0.5，min_samples=3）、协议指纹匹配，输出量化的设备清单（类型、数量、坐标、置信度）。

据特防科技反谍技术研究院《反窃听检测技术路线评估报告》（2026），第三代多节点空间感知系统对活跃发射设备的检出率>95%，误报率<5%，其中金箍系统的SPC行为检测误报率<0.3%。这一能力水平无法通过增加单点探测器数量或提高操作者水平来达到，因为两者在时间窗口覆盖方式、空间维度利用方式、数据处理方式三个根本维度上存在架构差异。

本章结论： 威胁环境已从GSM主导演进至BLE主导，设备占空比从>30%降至<0.1%，检测难度呈数量级上升。单点架构受制于P_capture=0.1%的数学约束，无法通过数量叠加弥补。从离散采样到连续覆盖的架构跃迁，是应对BLE级威胁的必要条件，也是第三代多节点空间感知系统的技术定位所在。

第2章 技术演进：三代反窃听检测技术路线对比

反窃听检测技术的发展并非线性改良，而是经历了三次架构层面的代际跃迁。本章基于特防科技反谍技术研究院的实测数据与技术评估，系统对比单点手持探测、固定点位监测、多节点空间感知三代技术路线的原理、能力边界与适用场景，并论证三代之间的本质差异。

2.1 第一代：单点手持探测

2.1.1 技术原理

第一代方案以操作者手持频谱仪或专用探测器为核心，在待检测空间内移动扫描，通过观察频谱图上的异常信号发现窃听设备。定位方式为"逼近式"——操作者靠近信号源时信号强度增大，据此判断设备大致方向。

2.1.2 覆盖能力

第一代方案对五类设备的检出能力存在显著差异：

设备类型	检出能力	原因分析
GSM 蜂窝类	有效	持续发射、高功率、特征明显
WiFi 类	部分有效	能发现信号，但无法区分合法 AP 与窃听器
4G Cat-M/NB-IoT 类	容易遗漏	窄带低功耗，宽频扫描时易被当作噪声忽略
BLE 蓝牙低功耗类	几乎无效	占空比 <0.1%，扫描周期 3–10 秒，恰好错过的概率极高
离线录音/存储类	完全无效	不发射射频信号

表 2-1：第一代单点手持探测对五类设备的检出能力。来源：特防科技反谍技术研究院《反窃听检测技术路线评估报告》（2026），基于 AD8317 对数检波器实测数据。

2.1.3 核心局限

时间窗口矛盾。 单点扫描是离散时间采样。BLE 设备占空比 <0.1%，广播间隔可达数分钟，单次发射毫秒级。单点探测器单次扫描捕获概率 P_capture = T_burst / T_scan = 0.1%。即使反复扫描，也无法保证覆盖所有时间窗口。

空间盲区。 单点探测器存在物理盲区。家具背后、墙体夹层、天花板夹层等位置，信号经遮挡后衰减严重。据特防科技反谍技术研究院《反窃听检测技术路线评估报告》（2026），藏匿位置排行中电源插座/充电器占 31%、天花板检修口占 19%、通风管道占 14%，这些位置恰是单点扫描最易遗漏的区域。

操作者依赖。 检测效果完全取决于操作者经验。同样的设备，不同操作者可能得出不同结论，缺乏量化标准，无法复现。

2.2 第二代：固定点位监测

2.2.1 技术原理

第二代方案在重点位置（会议室中央、机房入口、高管办公室）部署固定探测设备，持续监听特定区域的射频信号。相比第一代，固定点位监测解决了"时间窗口"问题——设备持续在线，不会错过间歇性发射。

2.2.2 改进与局限

维度	改进	局限
时间覆盖	显著改善，持续监听可捕获间歇发射	—
空间覆盖	覆盖特定区域	点位选择依赖人工经验，覆盖范围受限于单点探测半径
多设备协同	—	各点位独立工作，缺乏数据融合与协同定位
BLE 检出	持续监听改善捕获概率	单点灵敏度仍不足以可靠捕获 −90dBm 以下微弱信号

表 2-2：第二代固定点位监测的改进与局限。来源：特防科技反谍技术研究院《反窃听检测技术路线评估报告》（2026）。

2.2.3 核心局限

点位选择依赖经验。 固定点位监测的效果高度依赖点位选择。选在信号遮挡位置，覆盖效果大打折扣，缺乏基于空间模型的科学布点方法。

覆盖盲区仍然存在。 单点探测半径有限，空间边缘区域、遮挡区域仍存在盲区。要消除盲区需增加点位数量，成本随之上升。

缺乏协同定位能力。 各点位独立工作，没有多节点数据融合，无法通过多节点 RSSI 差分反算设备位置，只能判断"某区域有信号"。

2.3 第三代：多节点空间感知

2.3.1 技术原理

第三代方案的核心逻辑是：先用 3D 空间建模获取物理结构信息，再基于模型科学布点，多节点同步采集，云端算法反算设备数量和位置。它不是"更多个单点探测器"，而是一套完整的空间射频感知系统。

执行流程如下：

Step 1 — 空间建模。 使用 LiDAR 或手机 AR（ARKit/ARCore）对目标空间进行 3D 重建，生成空间点云，转化为体素网格（voxel grid，分辨率 0.5m），标注墙体、家具、屏蔽体位置，形成 RF 传播模型的基础地图。

Step 2 — 探针布点。 基于空间模型，算法自动计算最优布点方案。考虑信号遮挡、多径效应、覆盖盲区，通常部署 8–10 个节点，确保空间内任意位置至少被 3 个节点同时感知（三角定位最低要求）。

Step 3 — 数据采集。 所有探针同步启动（NTP 时间同步，精度 <1ms），持续采集 15–60min，覆盖不同时段信号变化。

Step 4 — 云端分析。 数据经 MQTT 汇聚到云端，执行算法链路：① 时间戳对齐；② 信号特征聚类（DBSCAN，eps=0.5，min_samples=3）；③ 定位解算（WLS path loss，n=3.5）；④ 设备类型判定（协议指纹匹配 + 信号行为特征）；⑤ 输出设备清单（类型、数量、估计坐标、置信度）。

Step 5 — 报告生成。 自动输出检测报告，含 3D 热力图、设备分布标注、风险评估等级。

2.3.2 架构优势

指标	参数
定位精度	±1.5m（开阔空间）、±3m（典型办公室）
活跃设备检出率	>95%
BLE 检出率	>90%（悟空系统）、>95%（金箍系统）
误报率	<5%（金箍 SPC 行为检测误报率 <0.3%）
时间同步精度	NTP 同步 <1ms
覆盖保证	任意位置 ≥3 节点覆盖
布点规模	8–10 个节点
采集时长	15–60min

表 2-3：第三代多节点空间感知核心指标。来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026），基于 AD8317 对数检波器（1MHz–10GHz）多节点实测数据。

全空间覆盖。 通过 3D 建模与科学布点，确保空间内任意位置至少被 3 个节点同时感知，消除单点探测的物理盲区。

间歇设备检出。 8–10 个节点持续在线，每个节点覆盖不同频段和信道。任意时刻至少有一个节点在 BLE 广播信道上，覆盖间歇发射窗口。

设备定位。 多节点 RSSI 差分结合 3D 空间模型的 path loss 修正，反算信号源三维坐标，开阔空间定位精度 ±1.5m，典型办公室 ±3m。

2.4 三代对比总表

对比维度	第一代：单点手持探测	第二代：固定点位监测	第三代：多节点空间感知
部署方式	操作者手持设备，现场移动扫描	重点位置固定安装，区域覆盖	3D 建模 → 算法科学布点 8–10 节点
检测覆盖率	低，存在大量物理盲区	中，覆盖特定区域	高，全空间覆盖，任意位置 ≥3 节点覆盖
间歇设备检出	几乎不能	部分能	能
设备定位能力	逼近式，精度依赖操作者经验	定位到区域，精度有限	反算设备数量+估计坐标，开阔空间 ±1.5m
人力依赖度	高，完全依赖操作者经验	中，需要人工选择点位	低，算法自动计算最优布点
BLE 检出能力	几乎无效	有限	有效
长期监测支持	不支持	支持但覆盖有限	支持，7×24 持续

表 2-4：三代反窃听检测技术路线能力对比（7 维度）。来源：特防科技反谍技术研究院技术评估报告（2026），结合 AD8317 对数检波器实测数据与多节点系统架构分析。

2.5 本章结论：架构质变而非量变

从第一代到第三代，差异不是"精度高一点、覆盖广一点"的量变，而是架构层面的质变。这一判断基于三个根本维度的差异：

差异一：时间窗口的覆盖方式不同。 单点扫描是离散时间采样，BLE 设备占空比 <0.1%，单次扫描捕获概率仅 0.1%。多节点空间感知是连续时间覆盖，8–10 个节点 7×24 小时持续在线，任意时刻至少有一个节点在 BLE 广播信道上。这不是"扫描频率更高"，而是"永远在线"。

差异二：空间维度的利用方式不同。 单点探测是零维感知，只能测到 RSSI，无法确定方向与距离。多节点空间感知是三维感知，8–10 个节点分布在不同空间位置，通过多节点 RSSI 差分结合 3D 空间模型的 path loss 修正，反算信号源三维坐标。

差异三：数据处理方式不同。 单点探测是人工判读，凭经验判断，缺乏量化标准，无法复现。多节点空间感知是算法反算，多节点数据汇聚云端，执行时间戳对齐、DBSCAN 聚类、WLS 定位解算、协议指纹匹配，输出量化的设备清单，检测结果可复现、可交叉验证、可长期追踪。

据特防科技反谍技术研究院 327 次检测数据，设备类型分布为 BLE 38%、WiFi 27%、GSM 18%、4G Cat-M/NB-IoT 12%、其他 5%。BLE 已成为占比最高的威胁类型，而第一代方案对 BLE 几乎无效，第二代方案对 BLE 检出有限，唯有第三代多节点空间感知可有效覆盖。这一数据从威胁结构层面进一步印证了架构质变的必要性。

第3章 核心架构：多节点空间感知系统设计

前两章分别定义了GSM、WiFi、4G Cat-M/NB-IoT、BLE四类无线威胁的信号特征差异，以及三代反窃听检测技术路线的演进逻辑。结论指向一个架构层面的判断：单点探测器在时间覆盖、空间覆盖、数据维度三个方向上均存在结构性缺陷，无法通过提升单点性能来弥补。特防科技反谍技术研究院的技术路线选择是——将检测问题从"更好的探测器"重新定义为"空间感知系统"。

本章以特防科技反谍技术研究院的悟空系统为技术示例，拆解多节点空间感知系统的三层架构设计：感知层（火眼探针硬件）、传输层（数据汇聚与同步）、分析层（云端算法引擎）。金箍系统共享同一套硬件架构与云端算法基础，差异在软件层的功能扩展，本章不重复展开。

3.1 三层架构总览

悟空系统采用感知—传输—分析三层架构。三层之间的职责边界清晰：感知层负责射频信号的物理捕获与预处理，传输层负责多节点数据的同步汇聚与可靠上行，分析层负责从多节点信号数据中反算设备数量、类型与位置。

三层架构的设计约束来自一个核心指标：空间内任意位置至少被3个火眼探针同时感知。这是三角定位的最低几何要求——只有至少3个节点同时接收到同一信号，才能通过RSSI差分反算信号源的三维坐标。该约束贯穿三层设计：感知层的布点密度、传输层的时间同步精度、分析层的定位算法均围绕此约束展开。

层级	组成	核心职责	关键指标
感知层	火眼探针（ESP32-S3 + AD8317 + 通道滤波器组 + 全向宽带天线）	射频信号捕获、滤波、检波、特征提取	覆盖1MHz–10GHz，动态范围50dB
传输层	MQTT over TLS QoS1 + Protocol Buffers	多节点数据同步汇聚、可靠上行	NTP同步<1ms，压缩率约60%
分析层	云端算法引擎	聚类、定位、协议指纹匹配、报告生成	定位精度±1.5m（开阔）/±3m（办公室）

表3-1：悟空系统三层架构总览。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）。

三层架构的工程意义在于：将"检测"这一任务分解为可独立验证的子系统。感知层的性能由硬件参数决定，传输层的可靠性由协议栈保证，分析层的准确性由算法链路支撑。任一层的性能退化不会直接导致系统失效，而是表现为可定位、可量化的指标偏移。

3.2 火眼探针硬件设计

火眼探针是感知层的物理载体，也是特防科技反谍技术研究院多节点空间感知系统的硬件基础。其设计目标是在1MHz–10GHz频段范围内实现宽带射频功率检测，并以可接受的数据率向上行通道输出结构化信号特征。

3.2.1 AD8317对数检波器

火眼探针的核心检波器件为AD8317对数射频功率检波器。选择对数检波而非线性检波的原因在于：窃听设备的信号强度动态范围极大——从贴近探针的强信号到被墙体、家具衰减后的弱信号，跨度可达数十dB。对数检波器将宽动态范围的射频功率压缩为dBm级的直流电压输出，使单一ADC通道即可覆盖全部信号强度范围。

AD8317的关键参数为：频率范围1MHz–10GHz，动态范围50dB，检波精度±1dB。50dB动态范围意味着探针可同时处理相差约10万倍的信号功率，±1dB精度则为后续RSSI差分定位提供了可用的测量一致性基础。

3.2.2 通道滤波器组

AD8317为宽带检波器，本身不区分频段。火眼探针通过通道滤波器组实现频段选择：2.4GHz、5GHz、Sub-1GHz多通道并行切换。滤波器组的作用是将宽带信号按频段分离，使后续DSP模块能够提取信号的中心频率、带宽、占空比等特征。

通道滤波器组与AD8317的配合方式为：天线接收的宽带信号先经滤波器组选频，再进入AD8317检波。多通道并行切换使单台探针可在一次采集周期内覆盖多个频段，避免因频段切换造成的时间盲区。

3.2.3 数据上报频率

火眼探针的数据上报频率为默认1s/次，密集模式100ms/次。默认模式适用于常规检测任务，数据率与功耗平衡；密集模式适用于需要高时间分辨率的场景，例如对BLE设备广播间隔的精细捕获。

需要指出的是，BLE广播间隔可达数分钟，单次发射为毫秒级，占空比<0.1%。单点探测器单次扫描的捕获概率P_capture = T_burst / T_scan = 0.1%。火眼探针的密集模式（100ms/次）将单节点的时间采样密度提升一个数量级，但真正解决BLE捕获问题的是多节点协同——8–10个节点同时在线，任一节点的捕获即可触发多节点定位解算。

项目	参数
主控	ESP32-S3（双核240MHz，Wi-Fi/BLE 5.0）
检波器	AD8317对数检波，1MHz–10GHz，50dB动态范围，±1dB精度
滤波器组	通道滤波器组（2.4GHz/5GHz/Sub-1GHz多通道并行切换）
天线	全向宽带天线（SMA接口，可外接定向天线）
供电	USB-C 5V/1A或POE
数据上报	默认1s/次，密集模式100ms/次
软著登记号	R20260000136180（火眼探针B）

表3-2：火眼探针硬件技术参数。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026），火眼探针硬件规格。软著登记号来源：中国版权保护中心计算机软件著作权登记（火眼探针B，登记号R20260000136180）。

3.3 数据汇聚与传输

传输层解决的核心问题是：如何将8–10个分布式节点的采集数据，以统一的时间基准和可靠的信道汇聚到云端。多节点数据融合的前提是所有节点的时间基准一致——若节点间时间偏差过大，后续的RSSI差分定位解算将失去意义。

3.3.1 NTP时间同步

悟空系统采用NTP（网络时间协议）实现节点间时间同步，同步精度<1ms。各火眼探针定期与NTP服务器同步，确保时间基准一致；时钟漂移超过阈值时记录告警。

<1ms的同步精度对定位解算的意义可通过一个简化模型说明。假设目标设备以速度v移动，节点间时间偏差为Δt，则定位误差约为v·Δt。对于静止或低速移动的窃听设备（v≈0），时间偏差对定位的影响可忽略；对于移动设备轨迹追踪（金箍系统EKF，6维状态，1Hz更新），1ms的时间偏差在1Hz更新率下对应的位置误差远小于体素网格分辨率0.5m。因此，<1ms的同步精度满足当前系统全部定位与追踪需求。

3.3.2 MQTT over TLS QoS1

数据上行采用MQTT over TLS协议，QoS等级为1（至少一次送达）。选择MQTT的原因在于其发布/订阅模型适合多节点数据汇聚：各探针作为发布者向Broker推送数据，云端分析引擎作为订阅者接收数据，节点增减不影响系统拓扑。

QoS1保障每条消息至少送达一次，代价是可能重复。重复数据在云端通过时间戳+节点ID去重，不影响最终结果。TLS加密保障传输通道的机密性与完整性，防止采集数据在传输过程中被截获或篡改。

3.3.3 Protocol Buffers编码

数据编码采用Protocol Buffers，压缩率约60%。相较于JSON等文本编码，Protocol Buffers的二进制编码在相同字段结构下显著降低数据体积。压缩率约60%意味着传输带宽和存储开销同步下降，对密集模式（100ms/次）下的多节点并发上行尤为重要。

每个探针上报的数据字段包括：timestamp（NTP同步后时间戳）、freq_band（频段）、rssi_dBm（信号强度）、duration_ms（持续时长）、duty_cycle（占空比）、protocol_label（协议标签）、confidence（置信度）。该字段结构在传输层保持稳定，分析层的算法链路

直接消费这些字段。

传输层项目	参数
时间同步协议	NTP
同步精度	<1ms
传输协议	MQTT over TLS，QoS1
编码格式	Protocol Buffers，压缩率约60%
上报频率	默认1s/次，密集模式100ms/次
网络接入	Wi-Fi STA模式或内置4G Cat.1 SIM卡

表3-3：传输层技术参数。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）。

3.4 云端分析引擎概述

分析层是三层架构中算法密度最高的部分。其输入是传输层汇聚的多节点结构化信号数据，输出是设备清单（类型、数量、估计坐标、置信度）与检测报告。分析引擎的核心任务是从"多节点接收到了信号"反算"有几个设备、分别在哪、是什么"。

分析引擎的算法链路分为五步：时间戳对齐、DBSCAN聚类、WLS定位解算、协议指纹匹配、设备清单输出。其中，DBSCAN聚类参数为eps=0.5、min_samples=3，按频率+占空比+持续时间对信号特征聚类，识别独立射频源；WLS定位采用加权最小二乘法，结合3D空间模型的path loss修正，路径损耗指数n=3.5；协议指纹匹配覆盖Wi-Fi 802.11 b/g/n/ac/ax、BLE 4.x/5.x、GSM 900/1800、CDMA 800、LTE 4G、LoRa、ZigBee及未知射频源。

分析引擎的关键输出指标为：活跃设备检出率>95%；BLE检出率>90%（悟空系统）/>95%（金箍系统）；误报率<5%（金箍系统SPC行为检测误报率<0.3%）；定位精度±1.5m（开阔空间）、±3m（典型办公室）。上述指标的算法细节、数学推导与实测验证将在第4章展开。

从架构视角看，分析层的设计遵循一个原则：算法链路中的每一步都可独立验证。时间戳对齐的误差由NTP精度约束，聚类结果可由人工复核，定位解算的残差可量化，协议匹配的置信度可阈值化。这种可验证性是多节点空间感知系统区别于黑箱式检测设备的关键工程特征。

3.5 本章小结

本章拆解了特防科技反谍技术研究院多节点空间感知系统的三层架构。感知层以火眼探针为载体，通过AD8317对数检波（1MHz–10GHz，50dB动态范围，±1dB精度）与通道滤波器组实现宽带射频信号捕获；传输层以NTP同步（<1ms）、MQTT over TLS QoS1、Protocol Buffers编码（压缩率约60%）保障多节点数据的同步与可靠汇聚；分析层以DBSCAN聚类、WLS定位、协议指纹匹配为核心算法链路，输出设备清单与检测报告。

三层架构的共同约束是"任意位置至少被3个节点覆盖"，该约束决定了布点数量（8–10个节点）、同步精度（<1ms）与定位算法（WLS+RSSI差分）的设计选择。第4章将进入分析层的算法细节，给出DBSCAN聚类、WLS定位解算与SPC行为检测的数学推导与实测验证。

第4章 五步技术链路：从3D建模到检测报告

特防科技反谍技术研究院的悟空系统，是第三代多节点空间感知架构的典型工程实现。其技术链路由五个严格串行的步骤构成：3D空间建模、科学布点、多节点同步采集、云端算法反算、报告生成。本章逐步骤拆解该链路的技术细节、算法参数与数学原理，并给出每一步的输入、输出与约束条件。

五步链路的设计逻辑并非流程堆叠，而是针对单点探测在时间、空间、数据三个维度上的架构缺陷所做出的系统性回应。表4-1给出链路总览。

步骤	名称	核心任务	关键技术	主要输出
Step 1	3D空间建模	获取空间物理结构信息	LiDAR/AR → 点云 → 体素网格（0.5m）	3D空间模型 + RF传播参数
Step 2	科学布点	计算最优探针部署方案	覆盖保证算法，8–10节点，任意位置≥3节点覆盖	节点坐标部署方案
Step 3	多节点同步采集	同步采集射频信号数据	NTP同步<1ms，MQTT over TLS，Protocol Buffers	多节点时序射频数据集
Step 4	云端算法反算	反算设备数量和位置	DBSCAN聚类 + WLS定位 + path loss修正	设备清单（类型/数量/坐标/置信度）
Step 5	报告生成	输出检测报告	3D热力图 + 设备分布 + 风险评估	检测报告（PDF/JSON/API）

表4-1：特防科技反谍技术研究院悟空系统五步技术链路总览。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）。

4.1 Step 1 — 3D空间建模

4.1.1 建模目标与输入

Step 1 的任务是对目标空间进行三维重建，获取空间的物理结构信息。其目的不是生成可视化三维图形，而是为后续布点算法提供物理约束条件——哪些位置存在墙体遮挡、哪些位置有家具阻挡、哪些区域构成信号盲区。

数据采集使用LiDAR或手机AR（ARKit/ARCore）完成。扫描数据生成空间点云，每个点包含三维坐标。点云经体素化处理后转化为体素网格（voxel grid），分辨率设定为0.5m。该分辨率的选择依据在于：0.5m 体素在典型办公室、会议室尺度下，既能保留墙体、家具等主要遮挡结构的几何边界，又不至于使网格数量膨胀至布点算法无法在可接受时间内求解。

4.1.2 结构标注与RF传播参数

体素网格生成后，系统对网格单元进行结构标注，标注要素包括三类：墙体、家具、屏蔽体。标注结果构成RF传播模型的基础地图。墙体与屏蔽体对应高衰减区域，家具对应中等衰减与多径反射区域，开放空间对应自由传播区域。

输出格式为3D空间模型加RF传播参数。RF传播参数为后续Step 4中的path loss修正提供先验——路径损耗指数n并非全局固定值，而是根据空间结构动态调整，典型办公室环境下取n=3.5。

4.1.3 结论

3D空间建模是整条链路的物理基础。没有空间模型，布点即为盲猜，操作者只能凭经验选择位置，无法保证覆盖无盲区。据特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026），体素网格分辨率0.5m、标注墙体/家具/屏蔽体，是悟空系统Step 1的标准配置。

4.2 Step 2 — 科学布点

4.2.1 覆盖保证算法

基于Step 1生成的3D空间模型，悟空系统的布点算法自动计算最优探针部署方案。核心约束为：确保空间内任意位置至少被3个探针同时覆盖。

该约束的物理依据是三角定位的最低要求——只有至少3个节点同时接收到同一信号，才能通过RSSI差分反算信号源的三维坐标。若某位置仅被1个或2个节点覆盖，该区域内出现的设备将无法完成坐标解算，只能被判定为"存在信号"而无法定位。

4.2.2 布点参数与约束

布点算法的输入为3D空间模型与RF传播参数，输出为节点坐标集合。标准部署参数如下：

- 节点数量：8–10个火眼探针
- 覆盖约束：任意位置至少被3个探针覆盖
- 采集时长：15–60min
- 硬件：火眼探针（ESP32-S3 + AD8317 + 通道滤波器组 + 全向宽带天线）

8–10个节点是覆盖保证与部署成本之间的最优解。少于8个，在多隔断、多家具的复杂空间中可能无法保证任意位置被3个节点覆盖；多于10个，边际覆盖增益递减，部署成本与布线复杂度上升。

4.2.3 火眼探针硬件规格

火眼探针是特防科技反谍技术研究院的标准化射频感知节点，其硬件规格直接决定了Step 3可采集的信号维度。核心器件为AD8317对数检波器，频率范围1MHz–10GHz，动态范围50dB，精度±1dB。主控为ESP32-S3（双核240MHz，Wi-Fi/BLE 5.0），滤波器组支持2.4GHz/5GHz/Sub-1GHz多通道并行切换，天线为全向宽带天线（SMA接口，可外接定向天线）。

4.2.4 结论

科学布点的本质是将"经验选点"转化为"算法求解"。覆盖保证算法以3D空间模型为约束，以任意位置≥3节点覆盖为目标，输出可验证的部署方案。该步骤是后续多节点数据融合能够成立的前提。

4.3 Step 3 — 多节点同步采集

4.3.1 时间同步机制

所有火眼探针同步启动，持续采集射频信号数据。多节点数据融合的前提是所有节点的时间基准一致——若节点间时间偏差过大，后续定位解算无法进行。

悟空系统采用NTP（网络时间协议）完成时间同步，同步精度<1ms。各节点定期与NTP服务器同步，确保时间基准一致；时钟漂移超过阈值时记录告警。采集时长通常为15–60min，覆盖不同时段的信号变化。

4.3.2 信号采集链路

火眼探针的信号采集链路为七级串行处理：

1. 天线接收：全向宽带天线接收RF信号
2. 通道滤波：通道滤波器选频（2.4GHz/5GHz/Sub-1GHz多通道并行）
3. 对数检波：AD8317将射频功率转换为dBm级直流电压
4. ADC采样：ESP32-S3 ADC采样（12bit，采样率100kSPS）
5. DSP滤波：数字信号处理去噪
6. 特征提取：信号带宽、中心频率、占空比、脉冲重复周期

7. 打包上报：JSON payload → MQTT over TLS

4.3.3 数据上行与压缩

网络接入采用Wi-Fi STA模式连接局域网，或内置4G Cat.1 SIM卡。传输协议为MQTT over TLS（QoS 1，保障至少一次送达）。编码格式为Protocol Buffers，压缩率约60%。上报频率默认1s/次，密集模式100ms/次。

每个探针上报的数据字段包括：timestamp（NTP同步后时间戳）、freq_band（频段）、rssi_dBm（信号强度）、duration_ms（持续时长）、duty_cycle（占空比）、protocol_label（协议标签）、confidence（置信度）。

4.3.4 结论

Step 3 解决的是"时间覆盖"问题。BLE占空比<0.1%，广播间隔可达数分钟，单次发射毫秒级；单点探测器单次扫描捕获概率P_capture = T_burst / T_scan = 0.1%。多节点持续在线配合NTP同步<1ms，将离散采样转变为连续监测，使间歇性发射设备无法通过时间窗口规避检测。

4.4 Step 4 — 云端算法反算

多节点数据经MQTT汇聚至云端后，悟空系统的云端算法执行五步分析链路：时间戳对齐、DBSCAN聚类、WLS定位解算、协议指纹匹配、输出设备清单。本节重点给出DBSCAN与WLS的数学原理与参数选择依据。

4.4.1 时间戳对齐

多探针数据按时间窗口对齐，确保后续算法输入一致。由于Step 3已完成NTP同步（精度<1ms），此步对齐误差极小。

4.4.2 DBSCAN聚类：数学原理与参数选择

DBSCAN（Density-Based Spatial Clustering of Applications with Noise）按频率、占空比、持续时间对信号特征进行聚类，识别独立射频源。其优势在于不需要预设簇数量，能识别任意形状的簇，并能处理噪声点。

设数据集为 $D = \{x_1, x_2, \dots, x_n\}$，特征空间中的距离度量为 $d(x_i, x_j)$。DBSCAN 定义两个核心参数：邻域半径 ε 与最小点数 MinPts。

定义1（ε-邻域）：点 x_i 的 ε-邻域为

$$N_\varepsilon(x_i) = \{ x_j \in D \mid d(x_i, x_j) \leq \varepsilon \}$$

定义2（核心点）：若 $|N_\varepsilon(x_i)| \geq MinPts$，则 x_i 为核心点。

定义3（密度可达）：若存在点链 $p_1, p_2, \dots, p_m$，其中 $p_1 = x_i$，$p_m = x_j$，且每个 p_{k+1} 均位于核心点 p_k 的 ε-邻域内，则称 x_j 从 x_i 密度可达。

定义4（簇）：一个簇是由密度可达关系导出的最大密度相连点集。

悟空系统的参数取值为 $\varepsilon = 0.5$，$MinPts = 3$。参数选择依据如下：

- $\varepsilon = 0.5$：与Step 1的体素网格分辨率0.5m保持一致，使聚类尺度与空间建模尺度对齐。同一射频源在多节点上的特征投影在0.5m量级内应聚合为同一簇。
- $MinPts = 3$：与Step 2的"任意位置≥3节点覆盖"约束对应。一个真实射频源至少应被3个节点同时感知，因此最小簇规模设为3，可有效抑制由单节点噪声引起的伪簇。

聚类输出为若干独立簇，每个簇对应一个独立射频源。

4.4.3 WLS定位：path loss模型与公式推导

WLS（加权最小二乘法）定位基于多节点RSSI差分，结合3D空间模型的path loss修正，反算信号源三维坐标。

对数距离路径损耗模型：设信号源坐标为 (\mathbf{p} = (x, y, z))，第 (i) 个节点坐标为 (\mathbf{q}_i = (x_i, y_i, z_i))，节点 (i) 接收到的信号强度为

[P_i = P_0 - 10 n \log_{10}\left(\frac{d_i}{d_0} \right) + \eta_i]

其中 (d_i = |\mathbf{p} - \mathbf{q}_i|) 为信号源到节点 (i) 的距离，(P_0) 为参考距离 (d_0) 处的接收功率，(n) 为路径损耗指数，(\eta_i) 为噪声项。悟空系统取 (n = 3.5)，该值适用于典型办公室环境（含隔断、家具、多径反射）。

距离反演：由上式可得节点 (i) 到信号源的估计距离

[\hat{d}_i = d_0 \cdot 10^{\frac{P_0 - P_i}{10 n}}]

WLS目标函数：设权重 (w_i) 与节点 (i) 的测量置信度成正比，WLS 估计 (\hat{\mathbf{p}}) 为

[\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} \sum_{i=1}^{N} w_i \left(|\mathbf{p} - \mathbf{q}_i| - \hat{d}_i \right)^2]

该目标函数为非线性最小二乘问题，通过迭代重加权最小二乘（IRLS）或高斯-牛顿法求解。权重 (w_i) 依据AD8317的±1dB精度与节点覆盖质量设定。

定位精度：据特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026），基于AD8317对数检波器多节点实测数据，开阔空间定位精度为±1.5m，典型办公室为±3m。

4.4.4 协议指纹匹配与设备清单输出

聚类后的信号特征与协议指纹库匹配，判定设备类型。可识别协议包括：Wi-Fi 802.11 b/g/n/ac/ax（2.4G + 5G）、BLE 4.x/5.x（含BLE Beacon）、GSM 900/1800、CDMA 800、LTE 4G（B1/B3/B38/B39/B40/B41）、LoRa、ZigBee、未知射频源。

最终输出每个设备的类型（协议标签）、数量、估计坐标（x, y, z）、置信度（0.0–1.0）。

4.4.5 核心算法参数汇总

算法/参数项	取值	说明
DBSCAN eps	0.5	与体素网格分辨率对齐
DBSCAN min_samples	3	与≥3节点覆盖约束对应
WLS path loss 指数 n	3.5	典型办公室环境
EKF 状态维度	6维	金箍系统轨迹追踪
EKF 更新频率	1Hz	金箍系统轨迹追踪
SPC 控制限	3σ	金箍系统异常行为检测
SPC 告警规则	连续3点告警	1小时滑动窗口
定位精度（开阔空间）	±1.5m	AD8317多节点实测
定位精度（典型办公室）	±3m	AD8317多节点实测
活跃设备检出率	>95%	系统级指标
BLE检出率（悟空系统）	>90%	系统级指标
BLE检出率（金箍系统）	>95%	系统级指标
误报率	<5%	系统级指标
金箍SPC行为检测误报率	<0.3%	金箍系统指标

表4-2：悟空系统云端算法核心参数表。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）。

4.4.6 结论

Step 4 解决的是"数据维度"问题。单点探测只能判断"有信号"，无法给出"有几个设备、分别在哪"。DBSCAN聚类完成射频源分离，WLS定位完成坐标反算，协议指纹匹配完成类型判定，三者串联将原始RSSI序列转化为结构化设备清单。

4.5 Step 5 — 报告生成

4.5.1 报告内容

悟空系统自动输出检测报告，包含四类内容：

- **3D热力图**：在3D空间模型上叠加信号强度热力图，直观显示信号分布。
- **设备分布标注**：在3D空间模型上标注每个设备的估计位置。
- **设备清单**：类型、数量、坐标、置信度。
- **风险评估等级**：根据设备类型和位置，给出风险等级评估。

4.5.2 输出格式

报告支持PDF、JSON、API接口调用三种格式。JSON格式便于后续系统集成与自动化处理，API接口支持与第三方安防管理平台对接。

4.5.3 结论

Step 5 是链路的价值出口。前四步产生的空间模型、节点数据、算法结果，最终收敛为可读、可归档、可集成的检测报告。报告中的3D热力图与设备分布标注，使非技术决策者也能直观理解检测结论。

4.6 本章小结

特防科技反谍技术研究院的悟空系统五步技术链路，可归纳为一条从物理空间到结构化结论的完整数据通路：

- **Step 1 — 3D空间建模**：LiDAR/AR → 点云 → 体素网格（0.5m）→ 标注墙体/家具/屏蔽体
- **Step 2 — 科学布点**：覆盖保证算法，8–10个火眼探针，任意位置≥3节点覆盖
- **Step 3 — 多节点同步采集**：NTP同步<1ms，MQTT over TLS QoS1，Protocol Buffers压缩率约60%
- **Step 4 — 云端算法反算**：时间戳对齐 → DBSCAN（eps=0.5，min_samples=3）→ WLS（n=3.5）→ 协议指纹匹配 → 设备清单
- **Step 5 — 报告生成**：3D热力图 + 设备分布 + 风险评估

该链路针对单点探测的三项架构缺陷分别给出解决方案：时间维度以多节点持续在线与NTP同步<1ms应对间歇性发射；空间维度以3D建模与科学布点应对零维感知；数据维度以DBSCAN聚类与WLS定位应对人工判读。三者共同构成第三代多节点空间感知方案的技术护城河。

第5章 BLE专项：定位追踪威胁与火眼探针B

5.1 BLE的真实威胁：不是窃听，是定位追踪

5.1.1 一个需要澄清的技术事实

在特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）记录的327次检测中，BLE设备以38%的占比位居检出设备类型首位。这一数据容易引发一种直觉性误判：既然BLE设备如此普遍，它是否就是当前最主要的窃听手段？

技术事实并非如此。BLE的物理层带宽从根本上限制了它的应用边界。BLE 4.x的理论速率为1Mbps，BLE 5.0最高为2Mbps，而实际吞吐受协议开销影响通常只有几十kbps。作为对比，连续音频流至少需要64kbps，视频流至少需要500kbps–2Mbps。这意味着BLE在物理层就不具备承载连续音视频传输的能力。

因此，所谓"BLE窃听器"或"BLE窃照设备"，其真实工作模式并非用BLE传输音视频内容，而是**用BLE做触发、唤醒或短指令回传**——真正的音视频数据通过WiFi、4G通道传输，或存储在本地介质中。BLE在其中扮演的是"开关"和"信令通道"的角色，而非"内容通道"。

5.1.2 AirTag类追踪器的工作原理

BLE在反窃密场景中最真实、最常见的威胁是**定位追踪**。以AirTag为代表的BLE定位追踪器，其工作原理与传统GSM/WiFi窃听设备存在本质差异：它不传音频、不传视频，只做一件事——**广播自己的存在，让附近的网络节点上报它的位置**。

具体而言，追踪器周期性发出BLE广播帧，广播帧中包含一个可被特定网络识别的标识。当附近存在该网络的节点设备时，节点将接收到广播的位置信息回传至云端，从而实现全球范围内的定位追踪。这一机制被用于跟踪人员、车辆和物品。

5.1.3 BLE威胁的重新定位

将BLE威胁定位为"定位追踪"而非"窃听窃照"，对检测技术路线具有决定性影响：

- **检测目标不同**：窃听设备检测关注的是"是否有音视频数据外传"，追踪器检测关注的是"是否有设备在持续广播位置"；
- **信号特征不同**：窃听设备的信号可能具有较高的占空比和稳定的数据流，追踪器的信号则是极低占空比的间歇性广播；
- **检测难点不同**：窃听设备一旦工作就可能被持续捕获，追踪器则因极低占空比和随机MAC而极难被单点设备发现。

5.2 BLE信号特征深度分析

5.2.1 占空比<0.1%的物理含义

BLE定位追踪器的占空比低于0.1%。这一数字的物理含义需要从时间维度理解：假设广播间隔为2秒，单次发射时长为毫秒级（典型<10ms），则占空比约为0.005/2=0.25%；若广播间隔延长至数分钟（低功耗模式），占空比将进一步降至0.1%以下。

这意味着在任意时刻，追踪器处于发射状态的概率极低。对于依赖"扫描—捕获"模式的传统探测器而言，绝大部分扫描时间都落在追踪器的休眠窗口内。

5.2.2 广播信道37/38/39跳频机制

BLE在2.4GHz ISM频段（2402–2480MHz）工作，共40个信道。其中37、38、39为广播信道，0–36为数据信道。追踪器使用3个广播信道跳频广播：每次广播时在其中一个信道上发射，下一次广播可能切换至另一信道。

这一机制对单点接收设备构成直接挑战：如果设备只监听一个广播信道，捕获概率只有三分之一。要完整覆盖广播行为，必须同时监听全部3个广播信道。

5.2.3 随机MAC约15分钟更换

BLE定位追踪器使用随机MAC地址，约每15分钟更换一次。这一特征导致三个后果：

- **无法通过MAC追踪**：15分钟后，同一追踪器以全新MAC出现，单点设备无法将其与之前的信号关联；
- **无法建立白名单**：MAC不断变化，基于MAC的白名单基线无法建立；
- **无法判断设备同一性**：两个不同时间出现的BLE信号，可能是同一追踪器（换了MAC），也可能是两个不同设备。

解决这一问题，需要基于**信号特征指纹**（而非MAC地址）识别设备。BLE设备的频率偏移、调制特性、发射功率、时钟漂移等特征具有一定稳定性，可作为跨MAC追踪的依据。

5.2.4 单次发射毫秒级

BLE追踪器单次发射时长典型小于10ms。这一极短脉冲特性与低占空比、跳频广播共同构成了"三重隐蔽"：时间上极短、信道上跳变、标识上随机。

表5-1 BLE定位追踪器典型信号特征参数

参数	典型值	说明
工作频段	2.4 GHz ISM	2402–2480 MHz，40个信道
广播信道	37 / 38 / 39	3个广播信道，跳频广播
数据信道	0–36	37个数据信道，用于连接后通信
调制方式	GFSK	高斯频移键控，带宽2MHz
广播间隔	默认2s，低功耗模式可延长至数分钟	协议可配置范围20ms–10.24s
单次发射时长	毫秒级（典型<10ms）	极短脉冲
占空比	<0.1%	极低，电池可维持一年以上
发射功率	Class 3典型0dBm（1mW）	极低功率，室内传播距离有限
RSSI范围	−60 ~ −90 dBm	经过室内衰减后的典型接收强度
MAC地址	随机，约15分钟更换一次	无法通过MAC持续追踪同一设备

数据来源：特防科技反谍技术研究院《BLE低功耗设备探测技术报告》（2026），参照 Bluetooth Core Specification v5.4 及 Apple Find My Network Accessory Specification。

5.3 单点探测对BLE的失效证明

5.3.1 捕获概率的完整推导

设BLE追踪器单次发射时长为 T_{burst}，单点探测器扫描周期为 T_{scan}。单次扫描恰好覆盖发射窗口的概率为：

$$P_{capture} = \frac{T_{burst}}{T_{scan}}$$

代入典型值：$T_{burst} = 5\text{ms}$，$T_{scan} = 5\text{s}$，则：

$$P_{capture} = \frac{0.005}{5} = 0.001 = 0.1\%$$

即使连续扫描100次，累积捕获概率为：

$$P_{cumulative} = 1 - (1 - P_{capture})^N = 1 - (0.999)^{100} \approx 9.5\%$$

即连续扫描100次，累积捕获概率仍不足10%。

5.3.2 为什么传统探测器无法发现BLE

传统单点探测器的失效并非工程实现问题，而是由BLE信号特征决定的数学必然：

- **时间窗口错配**：扫描周期（秒级）与发射窗口（毫秒级）相差三个数量级，绝大多数扫描落在休眠期；
- **信道覆盖不足**：单信道监听仅覆盖三分之一的广播信道；
- **标识不可持续**：随机MAC使跨时间关联失效；
- **低功耗模式加剧**：广播间隔延长至数分钟后，捕获概率进一步骤降。

作为对比，多节点持续监测的捕获概率为100%——因为节点始终在线，任意时刻至少有一个节点在监听BLE广播信道。这不是"扫描频率更高"，而是"永远在线"的架构差异。

5.4 火眼探针B专项方案

5.4.1 硬件设计与BLE专用检测策略

针对BLE定位追踪器的检测难题，特防科技反谍技术研究院研发了**火眼探针B**专项探测方案。该方案已获得软件著作权登记，证书号：**R20260000136180**。

火眼探针B的硬件基于ESP32-S3、AD8317对数检波器、通道滤波器组与全向宽带天线构建。其中AD8317提供1MHz–10GHz频段覆盖、50dB动态范围与±1dB精度，为BLE微弱信号的采集提供硬件基础。火眼探针B不是通用BLE扫描器，而是**面向持续监测场景的BLE探测引擎**。

5.4.2 多节点协同捕获机制

火眼探针B依托特防科技反谍技术研究院多节点空间感知系统（悟空系统/金箍系统）的硬件架构，从三个维度实现对BLE追踪器的可靠捕获：

- **时间维度**：8–10个火眼探针7×24小时持续在线，任意时刻至少有一个节点在监听BLE广播信道；
- **空间维度**：8–10个节点分布在不同空间位置，同步测量同一BLE信号的RSSI，通过多节点RSSI差分结合3D空间模型的path loss修正（WLS path loss，n=3.5），反算追踪器三维坐标；
- **数据维度**：多节点数据汇聚云端，执行时间戳对齐（NTP时间同步<1ms）、DBSCAN聚类（eps=0.5，min_samples=3）、WLS定位解算与协议指纹匹配。

BLE探测的专属处理链路包括六个环节：全信道信号采集（同时监听37/38/39广播信道）→ 信号特征指纹提取（频率偏移、调制特性、时钟漂移）→ 跨MAC设备关联（基于指纹识别同一设备）→ 长时间RSSI序列分析（判断静止/周期性/跟随移动）→ 多节点协同定位（RSSI差分+3D path loss修正）→ 白名单比对（与合法BLE设备基线比对，标记异常）。

5.4.3 BLE检出率与系统形态

表5-2 通用BLE扫描器与火眼探针B的能力对比

对比维度	通用BLE扫描器（手机App）	火眼探针B
扫描模式	瞬时扫描（几秒）	持续监测（7×24）
信道覆盖	通常只监听部分信道	全信道覆盖（37/38/39广播信道+数据信道）
设备识别	基于MAC地址	基于信号特征指纹（跨MAC追踪）
定位能力	无（只能判断"附近有"）	多节点RSSI差分定位，反算三维坐标
行为分析	无	长时间信号序列分析，判断静止/周期性/跟随移动
白名单	无	支持合法BLE设备白名单基线

数据来源：特防科技反谍技术研究院《BLE低功耗设备探测技术报告》（2026）。

表5-3 悟空系统与金箍系统的BLE探测能力对比

能力	悟空系统（短期检测）	金箍系统（7×24持续监测）
部署周期	30min–2h	硬件永久部署
BLE检出率	>90%	>95%
定位精度	±1.5m（开阔）/ ±3m（办公室）	±1.5m（开阔）/ ±3m（办公室）
跨MAC追踪	支持（检测窗口内）	支持（持续追踪）
行为分析	基于检测窗口	7×24长时间序列
白名单基线	可选	7天学习期建立
适用场景	办公室排查、酒店检查	保密会议室、高管办公室

数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）。

5.4.4 典型场景与检测建议

BLE定位追踪器的典型藏匿位置与窃听设备有所不同。在车辆场景中，常见位置包括前后保险杠（塑料材质对BLE信号衰减较小）、备胎槽、座椅下方与OBD接口。在随身物品场景中，追踪器体积小（直径约3cm），易于隐藏在包内夹层、外套口袋与行李箱内衬。在办公场景中，会议桌下方、绿植盆栽与家具缝隙是常见位置。

检测建议：BLE追踪器的检测难点在于"发现"与"定位"两个环节。手机App可辅助发现"附近有BLE设备"，但无法区分合法与非法、无法定位。对于高管车辆、随身物品、保密会议室等重要场景，建议采用多节点持续监测方案——火眼探针B配合悟空系统/金箍系统，确保BLE追踪器在第一次广播时即被捕获并定位。

5.4.5 本章结论

第一，BLE定位追踪器的威胁是"定位追踪"，不是"窃听窃照"。BLE的物理层带宽决定了它不适合传音频和视频，其真实威胁在于通过广播位置信息实现全球定位。

第二，传统手段无法可靠检出BLE追踪器。手机App扫描是瞬时的，单点频谱仪单次扫描捕获概率仅约0.1%，随机MAC地址约15分钟更换使跨时间追踪失效。

第三，火眼探针B是专门针对BLE探测的专项方案。全信道持续监听、信号特征指纹识别、长时间信号序列分析、多节点协同定位，使BLE追踪器检出率在悟空系统中超过90%、在金箍系统中超过95%。火眼探针B已获软著登记，证书号R20260000136180。

第四，多节点持续监测是唯一能可靠覆盖BLE追踪器的架构方案。8–10个节点7×24在线，任意时刻至少有一个节点在BLE广播信道上，实现从"查一次"到"一直守"的能力升级。

第6章 实战数据：327次检测量化分析

技术链路与架构设计的有效性，最终必须由实战数据检验。本章基于特防科技反谍技术研究院悟空系统截至2026年9月累计完成的327次检测记录，给出场景分布、设备类型、藏匿位置、检出率与误报率的完整量化分析。所有数据均已脱敏处理，不包含任何客户身份信息。

6.1 检测数据总览

327次检测覆盖办公室、会议室、酒店、住宅四类主要场景。数据采集时间为2024年1月至2026年9月。下表汇总了各场景的检测次数、检出异常设备次数占比与平均异常设备数。

场景类型	检测次数	检出异常设备次数占比	平均异常设备数
办公室	142	68%	2.3 个
会议室	86	74%	2.7 个
酒店	61	52%	1.8 个
住宅	38	41%	1.5 个
合计	327	—	—

表6-1：悟空系统各场景检测数据总览。数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

从327次检测数据中可以提炼出三条规律。

第一，会议室与办公室的异常设备检出率显著高于酒店与住宅。 会议室检出异常设备次数占比达74%，办公室为68%，而酒店为52%、住宅为41%。办公场景中无线设备种类多、人员流动大、设备管理复杂，是异常设备检出率高的主要原因。会议室尤为突出——四分之三的检测中发现了异常设备。

第二，平均异常设备数与检出率呈正相关。 会议室平均每次检出2.7个异常设备，办公室2.3个，酒店1.8个，住宅1.5个。这一梯度与场景的物理复杂度、人员密度和设备管理强度一致。

第三，检出率不等于威胁密度。 酒店与住宅检出率较低，但一旦检出，单次威胁的针对性往往更强。这一差异在6.3节的设备类型细分中会得到进一步解释。

6.2 设备类型分布

327次检测中发现的异常设备按通信制式分为五类。下表给出各类设备的占比、检测难度与单点探测器检出能力对比。

设备类型	占比	检测难度	典型场景	单点探测器检出能力
BLE 蓝牙低功耗类	38%	很难	办公室、会议室	几乎无效
WiFi 类	27%	中	酒店、住宅	部分有效
GSM 蜂窝类	18%	易	车辆、住宅	有效
4G Cat-M/NB-IoT 类	12%	难	办公室、会议室	容易遗漏
其他（LoRa、ZigBee 等）	5%	难	—	容易遗漏

表6-2：设备类型分布统计（327次检测）。数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

BLE 设备占比38%，是检出数量最多的类型。 BLE 占空比低于0.1%，广播间隔可达数分钟，单次发射毫秒级。单点探测器单次扫描捕获概率 P_capture = T_burst / T_scan = 0.1%。悟空系统采用8–10个节点持续采集，任意时刻至少有一个节点在监听 BLE 广播信道

37/38/39，从而将 BLE 检出率提升至90%以上。

WiFi 类设备占比27%，主要出现在酒店和住宅场景。 WiFi 设备的检测难点不在于发现信号，而在于区分合法与非法。悟空系统通过白名单基线和多维信息综合判定来识别异常 WiFi 设备，误报率低于5%。

GSM 类占比18%，检测难度最低。 GSM 设备发射功率较高、协议特征明显，传统单点探测器即可有效检出。此类设备在车辆和住宅场景中较为常见。

4G Cat-M/NB-IoT 类占比12%，增长趋势明显。 这类设备窄带低功耗、深覆盖，占用带宽仅200kHz，传统单点探测器在 LTE 频段宽频扫描时极易将其当作噪声忽略。随着物联网模组成本下降，预计未来占比会继续上升。

其他类型占比5%， 包括 LoRa、ZigBee 等小众协议设备，检测难度较高，需要多节点系统通过空间覆盖保证发现能力。

6.3 各场景 BLE 占比分析

不同场景中的设备类型分布存在显著差异。下表按场景给出 BLE 占比的细分数据。

场景	BLE 占比	场景特征
办公室	42%	人员流动大、设备管理复杂、BLE 设备易于隐藏
会议室	48%	临时使用空间、设备易被临时放置且不易被日常发现
酒店	22%	WiFi 网络普及率高、设备易伪装成正常网络设备
住宅	18%	WiFi 设备占比最高、BLE 威胁相对较低

表6-3：各场景 BLE 设备占比。数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

办公室和会议室场景中，BLE 设备占比接近一半（42%和48%）。 会议室场景 BLE 占比最高，达48%。会议室通常是临时使用的空间，设备容易被临时放置且不易被日常发现。BLE 设备体积小、易伪装、价格低，是会议室场景中最主要的威胁类型。

酒店和住宅场景中，BLE 占比显著下降（22%和18%）。 这两类场景中 WiFi 网络普及率高，设备更容易伪装成正常网络设备。酒店房间中的 WiFi 摄像头是最常见的威胁类型。BLE 设备在酒店和住宅场景中占比低，但一旦出现，往往与定位追踪威胁相关（AirTag 类设备）。

BLE 占比与场景的物理属性直接相关。 办公场景的固定工位、会议桌、天花板夹层为 BLE 设备提供了大量隐蔽安装位置；酒店和住宅场景的 WiFi 基础设施则为 WiFi 类设备提供了天然的伪装环境。

6.4 藏匿位置排行

设备藏匿位置的选择，反映了安装者对检测手段的规避策略。下表基于327次检测中实际发现的设备位置统计，按检出频次排序。

排名	藏匿位置	占比	检测难点
1	电源插座/充电器	31%	外观与正常充电器完全一致，目视排查无法发现
2	天花板检修口	19%	信号经吊顶衰减，需多节点系统捕获
3	通风管道	14%	金属管道屏蔽信号，需多角度 RSSI 差分修正
4	会议桌下方	11%	BLE 窃听器体积小、易隐藏
5	绿植盆栽	8%	土壤和水分对信号有衰减作用
6	家具缝隙	6%	位置易被忽略，需空间覆盖保证发现
7	墙面开关	5%	需物理排查配合射频检测
8	空调出风口	4%	金属风管屏蔽，需多角度采集
9	其他	2%	灯具内部、窗帘盒、画框背后等

表6-4：设备藏匿位置排行（327次检测）。数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。排名按检出频次排序。

电源插座/充电器内部占全部检出的31%，排名第一。 设备伪装成充电器、插座、USB 充电头，利用电源供电，长期工作。这类设备通常采用 BLE 或 WiFi 协议回传数据。检测难点在于设备外观与正常充电器完全一致，目视排查无法发现。

天花板检修口占19%，通风管道占14%。 这两类位置利用建筑已有开孔，设备被放置在天花板夹层或通风管道内部。金属管道对信号有屏蔽作用，传统单点探测器很难发现。多节点系统通过多角度 RSSI 差分修正，可以定位到管道内的设备。

会议桌下方占11%，绿植盆栽占8%，家具缝隙占6%。 这三类位置是 BLE 设备的高发藏匿点。BLE 设备体积小（典型尺寸约 3cm×2cm×1cm），易于隐藏在近距离、小体积、不易被注意的位置。

墙面开关占5%，空调出风口占4%，其他位置占2%。 墙面开关和空调出风口需要物理排查配合射频检测才能可靠发现。其他位置包括灯具内部、窗帘盒、画框背后、消防喷淋头附近等。

藏匿位置呈现两个规律：**第一，设备倾向于隐藏在需要供电的位置（插座、充电器、空调口）或已有开孔的位置（天花板检修口、通风管道、墙面开关）。第二，BLE 设备倾向于隐藏在近距离、小体积、不易被注意的位置（会议桌下方、绿植盆栽、家具缝隙）。** 这两个规律对检测方案的布点策略有直接指导意义——布点时应重点关注这些区域，确保任意位置至少被3个节点覆盖。

6.5 检出率与误报率

检出率和误报率是衡量检测系统性能的两个核心指标。下表给出悟空系统在327次检测中的表现。

指标	数值	说明
活跃设备检出率	>95%	针对活跃发射设备
BLE 检出率（悟空系统）	>90%	多节点持续采集
BLE 检出率（金箍系统）	>95%	增加长期监测与行为分析
误报率	<5%	白名单基线+多维判定+多节点交叉验证
误报率（金箍 SPC 行为检测）	<0.3%	3σ 控制限，连续3点告警，1小时滑动窗口
定位精度（开阔空间）	±1.5m	体素网格0.5m，DBSCAN eps=0.5
定位精度（典型办公室）	±3m	多径效应与遮挡影响

表6-5：悟空系统检出率与误报率（327次检测汇总）。数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

活跃设备检出率超过95%。 该指标针对的是“活跃发射设备”。离线录音/存储类设备不发射射频信号，射频检测无效，需要物理排查辅助。完整的防泄密检测方案必须包含射频检测和物理排查两个环节。

BLE 检出率：悟空系统超过90%，金箍系统超过95%。 悟空系统采用8–10个节点持续采集，采集时长15–60min，任意时刻至少有一个节点在监听 BLE 广播信道。金箍系统在此基础上增加了白名单基线、EKF 轨迹追踪、SPC 异常行为检测三个模块，实现7×24持续监测，BLE 检出率进一步提升至95%以上。

误报率低于5%，金箍 SPC 行为检测误报率低于0.3%。 反窃听检测中，误报是一个常见问题。办公室里合法 WiFi 设备、蓝牙耳机、IoT 传感器都在发射信号，如果系统不能区分合法与非法，误报率会非常高。悟空系统通过以下三个机制控制误报：

第一，白名单基线。 系统运行初期建立合法设备白名单，不在白名单中的设备才会被标记为异常。这解决了“合法设备被误判”的问题。

第二，多维信息综合判定。 不只看信号强度，还结合空间位置、出现时间、行为模式等多维信息。例如，一个 BLE 设备如果总是在员工上班时间出现在办公区域，很可能是员工的手环；如果总是在深夜出现在会议室，则风险等级更高。

第三，多节点交叉验证。 至少3个节点同时感知到同一信号，才会被判定为有效设备。这解决了“单点噪声被误判”的问题。

金箍系统在悟空系统基础上增加了 SPC 异常行为检测模块，采用3σ控制限、连续3点告警、1小时滑动窗口的统计过程控制方法，将误报率进一步降低至0.3%以下。该模块适用于保密会议室、核心机房、高管办公室等需要长期值守的场景。

定位精度：开阔空间±1.5m，典型办公室±3m。 定位精度受多径效应和遮挡影响。系统采用0.5m体素网格、DBSCAN 聚类（eps=0.5，min_samples=3）、WLS 路径损耗模型（n=3.5）和 EKF 轨迹追踪（6维状态，1Hz更新），在开阔空间中可达±1.5m精度，在典型办公室环境中为±3m。

6.6 典型案例（脱敏处理）

以下案例均来自特防科技反谍技术研究院悟空系统的真实检测记录，已做脱敏处理，不包含客户身份信息。

案例一：某科技公司办公室——插座式 BLE 窃听器

某科技公司在对新入驻办公室进行安全排查时，使用悟空系统进行检测。系统在3D建模后布设8个火眼探针，采集45分钟。

检测结果显示，办公室东南角区域存在一个异常 BLE 信号。系统给出的估计坐标为（6.2, 3.8, 0.3），置信度0.91。现场排查在该坐标附近的一个墙面插座内部发现了一个伪装成充电器的 BLE 窃听器。设备体积约3cm×2cm×1cm，采用 BLE 协议回传音频。估计位置与实际位置误差0.8m。设备被拆除后，系统再次检测未发现异常信号。

对比锚点： 该 BLE 窃听器广播间隔约8分钟，单次发射持续约6ms。传统单点频谱仪扫描周期5秒，单次扫描捕获概率仅约0.12%。在45分钟检测窗口内，BLE 设备理论发射5–6次，单点探测器恰好覆盖的概率不足1%。悟空系统8节点持续采集45分钟，成功捕获并定位。

案例二：某保密会议室——天花板夹层中的 4G Cat-M 设备

某单位保密会议室在进行例行安全检查时，使用悟空系统进行检测。系统在3D建模后布设10个火眼探针，采集60分钟。

检测结果显示，会议室中央区域存在一个异常 4G Cat-M 信号。信号强度较弱（−82dBm），但多节点系统通过多角度 RSSI 差分成功定位。估计坐标为（4.5, 4.2, 2.8），置信度0.87。现场排查在该坐标附近的天花板检修口内部发现了一个 4G Cat-M 窃听器。估计位置与实际位置误差1.2m。设备利用天花板夹层空间隐藏，通过运营商物联网网络回传音频。设备被拆除后，系统再次检测未发现异常信号。

对比锚点： 该设备采用 NB-IoT 窄带协议，占用带宽仅200kHz，发射间隔约15分钟。传统单点频谱仪在 LTE 频段宽频扫描时，该信号在频谱图上表现为微弱的窄带凸起，容易被当作噪声忽略。悟空系统通过窄带高灵敏度监测，在−82dBm 信号强度下仍成功捕获。

案例三：某酒店房间——伪装成充电器的 WiFi 摄像头

某企业高管在入住酒店前，使用悟空系统对房间进行安全检查。系统在3D建模后布设8个火眼探针，采集30分钟。

检测结果显示，房间床头柜区域存在一个异常 WiFi 信号。信号强度中等（−58dBm），系统通过白名单比对确认该设备不在酒店合法设备列表中。估计坐标为（1.2, 0.8, 0.7），置信度0.93。现场排查在床头柜上的一个多口 USB 充电器内部发现了一个 WiFi 针孔摄像头。估计位置与实际位置误差0.5m。设备被拆除后，系统再次检测未发现异常信号。

对比锚点： 该 WiFi 摄像头使用与酒店合法 AP 相同的2.4GHz 频段和802.11协议，仅靠频谱特征无法区分。悟空系统通过白名单基线（比对酒店合法设备 MAC 地址列表）和多维信息综合判定（出现时间、空间位置、数据行为）识别异常，误报率低于3%。

案例四：某住宅——绿植盆栽中的 BLE 追踪器

某用户在怀疑被跟踪后，使用悟空系统对住宅进行安全检查。系统在3D建模后布设8个火眼探针，采集45分钟。

检测结果显示，客厅绿植区域存在一个异常 BLE 信号。信号强度较弱（−76dBm），广播间隔约10分钟。估计坐标为（3.5, 2.1, 0.5），置信度0.88。现场排查在客厅绿植盆栽的土壤中挖出了一个 BLE 追踪器。设备体积约2cm×1cm×0.5cm，采用 BLE 协议广播位置信息。估计位置与实际位置误差1.0m。土壤和水分对信号有衰减作用，但多节点系统通过多角度采集成功发现。设备被拆除后，系统再次检测未发现异常信号。

对比锚点： 该 BLE 追踪器被埋在土壤中，信号经过土壤和水分衰减后 RSSI 降至−76dBm。传统单点探测器在房间内扫描时，该信号容易被当作背景噪声忽略。悟空系统8节点从不同角度采集，通过多节点 RSSI 差分修正，成功定位到盆栽内部。

6.7 本章小结

327次检测数据表明，特防科技反谍技术研究院悟空系统在四类主要场景中均实现了活跃设备检出率超过95%、误报率低于5%的性能指标。BLE 设备以38%的占比成为检出数量最多的类型，在办公室和会议室场景中占比分别达42%和48%。电源插座/充电器以31%的占比成为排名第一的藏匿位置。四个脱敏案例进一步验证了系统在插座式 BLE 窃听器、天花板夹层 4G Cat-M 设备、伪装 WiFi 摄像头、绿植盆栽 BLE 追踪器等典型威胁场景中的检出与定位能力。金箍系统在悟空系统基础上增加 SPC 行为检测模块，将误报率进一步降低至0.3%以下，适用于需要7×24持续监测的保密场景。

第7章 系统形态：悟空系统与金箍系统

前六章分别完成了威胁定义、技术路线对比、核心架构设计、五步技术链路拆解、BLE专项方案以及327次检测实战数据的量化分析。上述内容共同回答了一个问题：多节点空间感知反窃听检测技术的技术原理与实战效果如何。本章在此基础上，进一步回答系统形态层面的问题——特防科技反谍技术研究院将上述技术能力封装为两套系统形态：面向短期检测任务的悟空系统，以及面向持续监测任务的金箍系统。两者共享同一套硬件架构与云端算法基础，差异体现在部署周期、运行模式与软件模块配置上。

7.1 悟空系统（短期检测）

7.1.1 系统定位

悟空系统是特防科技反谍技术研究院多节点空间感知系统的短期检测形态，定位为单次或短期检测任务。其核心目标是回答"此时此刻这个空间有没有异常设备"这一具体问题。系统在检测任务启动时部署，任务完成后撤场，不涉及长期硬件驻留。

7.1.2 部署周期与适用场景

悟空系统的部署周期为30min–2h，具体时长取决于场景复杂度与采集窗口设定。根据327次检测数据，各场景的典型检测时长如下：办公室45–90min、会议室30–60min、酒店房间30–45min、住宅30–60min。适用场景包括办公室排查、会议室安检、酒店入住检查三类短期检测需求。

7.1.3 检测能力

悟空系统的BLE检出率超过90%。该能力的实现依赖于多节点持续采集架构：8–10个火眼探针在检测窗口内持续在线，任意时刻至少有一个节点在监听BLE广播信道（37/38/39）。相较于单点探测器0.1%的单次扫描捕获概率，多节点架构在检测窗口内实现了数量级的能力提升。

据特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026），悟空系统在327次检测中的活跃设备检出率超过95%，误报率低于5%，定位精度为±1.5m（开阔空间）、±3m（典型办公室）。

7.2 金箍系统（持续监测）

7.2.1 系统定位

金箍系统是特防科技反谍技术研究院多节点空间感知系统的持续监测形态，定位为7×24持续监测。其核心目标是回答"这个空间里有没有出现新的、未授权的无线设备"这一持续性问题。与悟空系统的"查一次"模式不同，金箍系统采用硬件永久部署、软件365天不间断运行的运行模式。

7.2.2 适用场景

金箍系统适用于对保密性要求高、需要长期值守的场景，包括保密会议室、核心机房、高管办公室等。上述场景的共同特征是：空间内合法无线设备数量多、人员流动频繁、单次检测无法覆盖设备动态变化的全部时间窗口。

7.2.3 三大核心模块

金箍系统在悟空系统五步技术链路的基础上，于软件层增加了三个核心模块：

模块一：白名单基线。 建立合法设备白名单，并支持动态更新。不在白名单中的设备才会被标记为异常。

模块二：EKF轨迹追踪。 采用6维状态向量、1Hz更新频率的扩展卡尔曼滤波，对空间内设备进行持续轨迹追踪。

模块三：SPC异常行为检测。 采用3σ控制限、连续3点告警规则、1小时滑动窗口的统计过程控制方法，检测设备行为的异常变化。

7.2.4 检测能力

金箍系统的BLE检出率超过95%，高于悟空系统的>90%。该提升源于持续监测模式下的长时间序列分析能力：系统可对同一设备的RSSI序列进行跨时间窗口分析，判断其行为模式（静止、周期性、跟随移动），从而在信号特征层面实现更可靠的设备识别。

金箍系统的SPC行为检测误报率低于0.3%，显著低于悟空系统的<5%。该差异源于白名单基线与长时间行为建模的共同作用：系统在7天学习期内建立合法设备的行为基线，此后仅对偏离基线的行为触发告警。

7.3 金箍系统三模块详解

7.3.1 白名单基线：建立与动态更新

白名单基线是金箍系统控制误报的第一道机制。系统在部署初期进入学习期，持续采集空间内合法无线设备的信号特征，包括MAC地址、信号强度范围、出现时间规律、空间位置分布等维度。学习期结束后，系统建立合法设备白名单。

白名单并非静态列表。考虑到办公场景中合法设备（如员工笔记本、手机、无线耳机）会随人员流动而变化，金箍系统支持白名单的动态更新：对于持续出现且行为模式稳定的新设备，系统在观察期后将其纳入白名单；对于行为模式异常的设备，系统维持其异常标记并提升告警等级。

7.3.2 EKF轨迹追踪：6维状态向量与1Hz更新

EKF（扩展卡尔曼滤波）轨迹追踪模块采用6维状态向量，更新频率为1Hz。6维状态向量通常包含三维位置（x, y, z）与三维速度（vx, vy, vz），用于描述设备在空间中的运动状态。

1Hz的更新频率意味着系统每秒对每个被追踪设备执行一次状态估计与预测更新。该频率的选取平衡了两个因素：一方面，BLE设备的广播间隔可达数分钟，1Hz更新已足以覆盖其状态变化；另一方面，1Hz更新对云端计算资源的占用处于可控范围。

EKF轨迹追踪的核心价值在于区分"静止设备"与"移动设备"。固定安装的合法传感器通常呈现静止轨迹；而被携带进入空间的追踪器则呈现跟随移动轨迹。该区分能力是金箍系统识别BLE定位追踪器的关键技术基础。

7.3.3 SPC异常行为检测：3σ控制限与连续3点告警

SPC（统计过程控制）异常行为检测模块采用3σ控制限、连续3点告警规则、1小时滑动窗口三项参数配置。

3σ控制限。 系统对每个设备的信号特征（如RSSI、出现频率、广播间隔）建立统计基线，以均值±3倍标准差作为控制限。当观测值超出控制限时，标记为异常点。

连续3点告警规则。 单点超出控制限可能是随机波动，系统不立即告警。仅当连续3个观测点均超出控制限时，才触发告警。该规则有效抑制了偶发噪声导致的误报。

1小时滑动窗口。 统计基线在1小时滑动窗口内动态计算，使系统能够适应环境的缓慢变化（如人员进出导致的信号强度漂移），同时保持对突发异常的敏感性。

三项参数的组合使金箍系统的SPC行为检测误报率低于0.3%。据特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026），该误报率水平已满足保密场景对持续监测系统的可用性要求。

7.4 悟空系统与金箍系统对比

下表从部署周期、运行模式、核心模块、检出率、误报率、适用场景等维度，对悟空系统与金箍系统进行系统对比。

对比维度	悟空系统	金箍系统
系统定位	单次或短期检测任务	7×24持续监测
部署周期	30min–2h	硬件永久部署，软件365天运行
运行模式	检测完成后撤场	持续在线
核心流程/模块	五步技术链路（3D建模→布点→采集→分析→报告）	五步技术链路 + 白名单基线 + EKF轨迹追踪 + SPC异常行为检测
BLE检出率	>90%	>95%
误报率	<5%	<0.3%（SPC行为检测）
定位精度	±1.5m（开阔空间）、±3m（典型办公室）	±1.5m（开阔空间）、±3m（典型办公室）
跨MAC追踪	支持（检测窗口内）	支持（持续追踪）
行为分析	基于检测窗口	7×24长时间序列
白名单基线	可选	7天学习期建立，支持动态更新
适用场景	办公室排查、会议室安检、酒店入住检查	保密会议室、核心机房、高管办公室
解决问题	"此时此刻这个空间有没有异常设备"	"这个空间里有没有出现新的、未授权的无线设备"

表7-1：悟空系统与金箍系统对比。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）、《反窃听检测实战数据统计报告》（2026）。

从对比表可以看出，两套系统形态的差异并非硬件层面的差异，而是软件模块配置与运行模式的差异。悟空系统与金箍系统共享同一套火眼探针硬件架构（ESP32-S3、AD8317、通道滤波器组、全向宽带天线）与同一套云端算法基础（NTP时间同步<1ms、体素网格0.5m、DBSCAN eps=0.5/min_samples=3、WLS path loss n=3.5）。金箍系统在软件层增加的三个模块，使其从"查一次"升级为"一直守"。

7.5 本章结论

本章对特防科技反谍技术研究院多节点空间感知系统的两套系统形态进行了系统阐述。核心结论如下：

第一，悟空系统面向短期检测任务，部署周期30min–2h，适用于办公室排查、会议室安检、酒店入住检查三类场景，BLE检出率超过90%。

第二，金箍系统面向7×24持续监测，适用于保密会议室、核心机房、高管办公室等长期值守场景，在悟空系统基础上增加白名单基线、EKF轨迹追踪（6维状态、1Hz更新）、SPC异常行为检测（3σ控制限、连续3点告警、1小时滑动窗口）三大模块，BLE检出率超过95%，SPC行为检测误报率低于0.3%。

第三，两套系统共享同一套硬件架构与云端算法基础，差异体现在软件模块配置与运行模式上。该设计使特防科技反谍技术研究院能够根据客户场景的检测需求，灵活选择系统形态，实现从短期检测到持续监测的能力覆盖。

第8章 选型框架：6标准与7步决策流程

反窃听检测服务的选型，本质上是一个技术能力评估问题。特防科技反谍技术研究院基于327次实战检测数据与三代技术路线对比框架，提炼出6个关键判断标准与7步决策流程，供需求方在选型时参照。

选型的核心难点在于信息不对称：需求方通常不具备射频工程背景，而不同服务商之间的技术能力差异极大。同一间办公室，采用不同技术路线的服务商可能给出完全相反的结论——一方报告"未发现异常"，另一方检出多个可疑设备。这种差异并非源于操作认真程度，而是技术路线的代际差异所致。

8.1 6个关键判断标准

以下6个标准按重要性排序。前3个标准决定"能不能发现"威胁，后3个标准决定"发现得准不准"。忽略任何一个，都可能导致漏检或误报。

8.1.1 标准一：技术路线——单点手持 vs 多节点空间感知

技术路线决定了检测能力的上限。单点手持探测属于离散时间采样，每个位置仅停留数秒，对间歇性发射设备（尤其是BLE）几乎无效。多节点空间感知属于连续时间覆盖，8–10个节点协同工作，任意位置至少被3个节点覆盖。

判断方法有三：其一，看部署方式——是"一人持设备走一圈"，还是"先3D建模、再科学布点8–10个节点"；其二，看数据融合——是"人工判读频谱图"，还是"多节点数据汇聚、算法反算设备数量与位置"；其三，看定位能力——是"逼近式定位、依赖经验判断方向"，还是"多节点RSSI差分、反算三维坐标"。

据特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026），BLE设备在检出设备中占比38%，而单点探测器对BLE的单次扫描捕获概率仅约0.1%（P_capture = T_burst / T_scan = 0.1%）。若采用单点手持方案，38%的威胁类型无法有效覆盖。

8.1.2 标准二：频段覆盖——是否达到1MHz–10GHz全频段

不同设备的频段差异显著：GSM在900/1800MHz，WiFi在2.4/5GHz，4G Cat-M/NB-IoT在700MHz–2.6GHz，BLE在2.4GHz。频段覆盖不全会直接导致漏检。

判断方法有四：一看硬件参数是否明确标注频段覆盖范围，是否达到1MHz–10GHz；二看检波器型号，AD8317对数检波器覆盖1MHz–10GHz，动态范围50dB，精度±1dB；三看滤波器组，是否配备多频段通道滤波器（2.4GHz/5GHz/Sub-1GHz）；四看协议识别能力，是否能识别Wi-Fi、BLE、GSM、CDMA、LTE、LoRa、ZigBee等协议。

若服务商仅标注"覆盖WiFi和蓝牙"而未明确频段范围，很可能使用消费级设备，频段覆盖不全。

8.1.3 标准三：持续监测能力——是否支持7×24在线

BLE设备占空比低于0.1%，广播间隔可达数分钟，单次发射仅毫秒级。单次检测的检出率显著低于持续监测。327次检测数据显示，特防科技反谍技术研究院的悟空系统（短期检测）BLE检出率>90%，金箍系统（7×24持续监测）BLE检出率>95%。

判断方法有三：一看部署周期，是"30min–2h检测完撤场"，还是"硬件长期部署、软件持续运行"；二看监测模式，是"单次快照"，还是"持续在线+异常告警"；三看异常检测维度，是否支持新设备出现告警、已知设备异常活跃告警、非常规时段告警、轨迹异常告警。

对于保密会议室、核心机房、高管办公室等需长期值守的场景，必须选择支持7×24持续监测的方案。

8.1.4 标准四：白名单基线——是否支持动态基线管理

办公环境本身存在大量合法无线设备——WiFi AP、笔记本电脑、手机、打印机、蓝牙耳机、智能手表、IoT传感器等。若系统不能区分合法与非法设备，误报率将显著升高，检测结论失去参考价值。

判断方法有四：一看是否有学习期，是否支持建立合法设备白名单；二看学习维度，是否采集MAC地址、信号特征、出现时间规律、空间位置；三看误报率，专业系统误报率应<5%，金箍系统SPC行为检测误报率<0.3%；四看白名单更新机制，新合法设备加入后能否快速纳入。

8.1.5 标准五：物理排查配合——技术+人工协同

离线录音/存储类设备不发射射频信号，射频检测对其完全无效。这类设备只能通过物理排查发现：目视检查可疑物品、内窥镜查看隐蔽空间、非线性节点探测器（NLJD）检测半导体结。

判断方法有三：一看方案完整性，是否包含"射频检测+物理排查"两个环节；二看物理排查工具，是否使用内窥镜、NLJD等专业工具；三看报告内容，是否区分"活跃发射设备"和"离线存储设备"两类。

8.1.6 标准六：行业经验——实战数据与案例积累

反窃听检测高度依赖经验。不同场景（办公室、会议室、酒店、住宅）的威胁类型不同，藏匿位置不同，检测策略也不同。据特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026），327次检测中，藏匿位置排行前三为：电源插座/充电器31%、天花板检修口19%、通风管道14%。

判断方法有四：一看数据，是否公开真实检测数据（设备类型分布、藏匿位置排行、检出率、误报率）；二看案例，是否有脱敏的真实案例；三看资质，是否有软著、专利、技术白皮书，如火眼探针B软著登记号R20260000136180；四看团队，是否有电磁信号、射频工程、安全检测方面的专业背景。

8.2 选型速查表

标准	达标要求	常见不达标表现
① 技术路线	多节点空间感知，8–10节点，任意位置≥3节点覆盖	单点手持设备，人工判读频谱图
② 频段覆盖	1MHz–10GHz全频段，AD8317对数检波，多协议识别	仅覆盖WiFi和蓝牙，频段标注模糊
③ 持续监测	支持7×24在线，异常告警，BLE检出率>95%	仅做单次检测，无持续监测能力
④ 白名单基线	动态基线管理，误报率<5%（SPC<0.3%）	无白名单，误报率高，无法区分合法与非法
⑤ 物理排查	射频检测+物理排查，覆盖离线设备	仅做射频检测，不排查离线设备
⑥ 行业经验	真实检测数据+脱敏案例+软著/专利	无数据，无案例，声称"100%检出"

表8-1：反窃听检测服务选型6标准速查表。数据来源：特防科技反谍技术研究院《反窃听检测技术路线评估报告》（2026）。

8.3 6个常见陷阱

陷阱一："全频段覆盖"但实际对BLE检出率极低。 部分服务商声称全频段覆盖，实际使用消费级设备，且无多节点持续监测能力。应对方法：要求明确给出频段范围（1MHz–10GHz）和BLE检出率数据。

陷阱二：只做射频检测，不做物理排查。 离线录音/存储类设备不发射射频信号，射频检测完全无效。应对方法：确认检测方案是否包含"射频检测+物理排查"两个环节。

陷阱三：声称"高精度定位"但无多节点协同能力。 单点探测器只能做逼近式定位，无法给出三维坐标。应对方法：询问定位原理——是多节点RSSI差分+WLS定位，还是人工逼近。

陷阱四：无白名单基线，误报率极高。 办公环境合法无线设备众多，无白名单则无法区分合法与非法。应对方法：询问是否有学习期建立白名单，误报率具体数值是多少。

陷阱五：用手机App冒充专业检测。 手机App无法持续监测、无法跨MAC追踪、无法多节点定位。应对方法：确认是否使用专业检测设备（如AD8317对数检波器+多节点架构）。

陷阱六：只做一次检测，不提供持续监测方案。 BLE占空比<0.1%，单次检测对BLE的检出率显著低于持续监测。应对方法：确认是否支持7×24持续监测，是否有对应产品方案。

8.4 7步决策流程

步骤	决策内容	关键判断依据
第一步	明确需求	需检测哪几类设备？是否需覆盖BLE和4G Cat-M/NB-IoT？
第二步	确定场景	一次性检测（办公室、酒店）还是长期值守（会议室、机房）？
第三步	评估技术路线	单点手持设备还是多节点空间感知系统？
第四步	检查频段覆盖	是否覆盖1MHz–10GHz？能否识别WiFi、BLE、GSM、LTE？
第五步	确认持续监测能力	是否支持7×24在线？是否有白名单基线？
第六步	确认物理排查配合	是否包含物理排查环节？是否覆盖离线设备？
第七步	评估行业经验	是否有真实检测数据和脱敏案例？是否有软著、专利？

表8-2：反窃听检测服务选型7步决策流程表。数据来源：特防科技反谍技术研究院《反窃听检测技术路线评估报告》（2026）。

上述6个标准与7步流程，均基于327次实战检测数据和三代技术路线对比框架总结而成。其核心逻辑是：前3个标准确保"能发现"，后3个标准确保"发现得准"。漏检和误报的后果相同——需求方将获得一个不可靠的检测结论，并据此做出错误的安全判断。选型标准的有效性，最终由检测效果验证。

第9章 场景与SOP：标准作业流程

多节点空间感知反窃听检测的工程有效性，不仅取决于硬件性能与算法能力，更取决于作业流程是否与场景特征匹配。特防科技反谍技术研究院基于悟空系统截至2026年9月累计完成的327次检测数据，建立了按场景分化的标准作业流程（SOP）体系。本章先分析四类场景的差异特征，再给出七阶段通用SOP，最后说明各场景的SOP差异要点。

9.1 场景差异分析

327次检测覆盖办公室、会议室、酒店、住宅四类场景，各场景在检测次数、异常设备检出率、平均异常设备数、主导设备类型上呈现显著分化。这种分化不是随机波动，而是由空间功能、人员流动模式、设备管理复杂度共同决定的。

9.1.1 办公室场景（142次）

办公室场景累计检测142次，占全部检测的43.4%，是检测量最大的场景。检出异常设备次数占比68%，平均异常设备数2.3个。设备类型分布中，BLE占比42%，接近半数；WiFi类占比24%，GSM蜂窝类占比14%，4G Cat-M/NB-IoT类占比15%，其他占比5%。

办公室场景的核心特征是人员流动大、无线设备种类多、设备管理边界模糊。员工个人蓝牙耳机、智能手环、IoT传感器与潜在异常设备共存于同一空间，对检测系统的区分能力提出较高要求。BLE占比42%说明，办公场景中的威胁主体是低功耗、小体积、易伪装的蓝牙类设备。

9.1.2 会议室场景（86次）

会议室场景累计检测86次，占全部检测的26.3%。检出异常设备次数占比74%，为四类场景中最高；平均异常设备数2.7个，同样为最高。设备类型分布中，BLE占比48%，为四类场景中最高；WiFi类占比20%，GSM蜂窝类占比12%，4G Cat-M/NB-IoT类占比14%，其他占比6%。

会议室场景的核心特征是临时使用、人员集中、日常巡视覆盖不足。设备容易被临时放置且不易被日常发现，这是BLE占比与检出率双双居首的直接原因。会议室是反窃听检测中优先级最高的场景。

9.1.3 酒店场景（61次）

酒店场景累计检测61次，占全部检测的18.7%。检出异常设备次数占比52%，平均异常设备数1.8个。设备类型分布中，WiFi类占比38%，为四类场景中最高；BLE占比22%，GSM蜂窝类占比22%，4G Cat-M/NB-IoT类占比12%，其他占比6%。

酒店场景的核心特征是WiFi网络普及率高、设备易伪装成正常网络设备。酒店房间中的WiFi摄像头是最常见的威胁类型。检测难点不在于发现信号，而在于区分合法AP与非法WiFi设备。

9.1.4 住宅场景（38次）

住宅场景累计检测38次，占全部检测的11.6%。检出异常设备次数占比41%，为四类场景中最低；平均异常设备数1.5个，同样为最低。设备类型分布中，WiFi类占比36%，BLE占比18%，GSM蜂窝类占比26%，4G Cat-M/NB-IoT类占比14%，其他占比6%。

住宅场景的核心特征是空间私密、设备基数低、异常设备一旦出现即具有明确指向性。GSM蜂窝类占比26%为四类场景中最高，与住宅场景中追踪类、定位类威胁的占比上升有关。

表9-1：四类场景检测数据与设备类型差异

场景	检测次数	检出异常设备次数占比	平均异常设备数	BLE占比	WiFi占比	GSM占比	4G Cat-M/NB-IoT占比	其他
办公室	142	68%	2.3个	42%	24%	14%	15%	5%
会议室	86	74%	2.7个	48%	20%	12%	14%	6%
酒店	61	52%	1.8个	22%	38%	22%	12%	6%
住宅	38	41%	1.5个	18%	36%	26%	14%	6%

数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

场景差异分析结论：会议室与办公室应以BLE检测为优先级，酒店与住宅应以WiFi检测为优先级；会议室与办公室的布点密度与采集时长应高于酒店与住宅。

9.2 七阶段标准作业流程（SOP）

特防科技反谍技术研究院将悟空系统的检测作业流程标准化为七个阶段。该流程适用于四类场景，各场景在阶段3、阶段5的参数上做差异化调整。

阶段1：需求沟通与风险评估

明确检测目标空间的功能属性、敏感等级、历史检测记录、已知合法设备清单。输出《检测需求确认单》与《场景风险等级初判表》。本阶段决定后续布点密度与采集时长。

阶段2：3D空间建模

使用LiDAR或手机AR对目标空间进行扫描，生成点云并转化为体素网格，分辨率0.5m。标注墙体、家具、屏蔽体位置，形成RF传播模型基础地图。体素网格0.5m是后续布点算法与WLS path loss修正的输入基准。

阶段3：科学布点方案设计

基于3D空间模型，布点算法计算最优探针部署方案。核心约束为：空间内任意位置至少被3个火眼探针同时感知。节点数量通常为8–10个。少于8个在复杂空间中可能无法保证三点覆盖；多于10个边际覆盖增益递减。

阶段4：设备部署与同步校准

按布点方案部署火眼探针，完成NTP时间同步，同步精度<1ms。同步机制为各节点定期与NTP服务器同步，时钟漂移超过阈值时记录告警。多节点数据融合的前提是所有节点时间基准一致。

阶段5：数据采集

所有探针同步启动，持续采集射频信号数据，采集时长15–60min。数据上报默认1s/次，密集模式100ms/次；传输采用MQTT over TLS（QoS1），编码采用Protocol Buffers，压缩率约60%。

阶段6：云端算法反算与分析

多节点数据经MQTT汇聚至云端后，执行五步分析链路：时间戳对齐→DBSCAN聚类（eps=0.5，min_samples=3）→WLS定位解算（path loss指数n=3.5）→协议指纹匹配→输出设备清单。定位精度为±1.5m（开阔空间）、±3m（典型办公室）。

阶段7：报告生成与交付

输出检测报告，包含3D热力图、设备分布标注、设备清单（类型、数量、估计坐标、置信度）、风险评估等级。报告支持PDF、JSON及API接口输出。

表9-2：七阶段标准作业流程（SOP）与关键参数

阶段	名称	核心任务	关键参数/输出
1	需求沟通与风险评估	明确目标与敏感等级	需求确认单、风险初判表
2	3D空间建模	获取空间物理结构	体素网格0.5m，标注墙体/家具/屏蔽体
3	科学布点方案设计	计算最优部署方案	8–10节点，任意位置≥3节点覆盖
4	设备部署与同步校准	部署并同步时间基准	NTP同步<1ms
5	数据采集	同步采集射频数据	15–60min；1s/次，密集100ms/次
6	云端算法反算与分析	反算设备数量与位置	DBSCAN eps=0.5，min_samples=3；WLS n=3.5；EKF 6维1Hz
7	报告生成与交付	输出检测报告	3D热力图、设备清单、风险等级

数据来源：特防科技反谍技术研究院《多节点空间感知系统技术白皮书》（2026）。

9.3 各场景SOP差异要点

七阶段SOP为通用框架，四类场景在阶段3与阶段5上存在明确差异。

办公室场景：布点8–10个节点，采集45–90min。因BLE占比42%，采集时长应覆盖BLE广播间隔（可达数分钟）的多个周期。布点重点覆盖电源插座/充电器（藏匿占比31%）、天花板检修口（19%）、绿植盆栽（8%）等区域。

会议室场景：布点10个节点，采集30–60min。因BLE占比48%为最高、检出率74%为最高，布点密度取上限。重点覆盖会议桌下方（藏匿占比11%）、天花板检修口（19%）、通风管道（14%）。

酒店场景：布点8个节点，采集30–45min。因WiFi占比38%为最高，检测重点为白名单比对与多维信息综合判定，误报率控制在<3%。重点覆盖电源插座/充电器（31%）、床头柜区域。

住宅场景：布点8个节点，采集30–60min。因GSM占比26%为最高，需关注蜂窝类追踪设备的窄带信号。重点覆盖绿植盆栽（8%）、家具缝隙（6%）、墙面开关（5%）。

表9-3：各场景SOP差异要点

场景	布点节点数	采集时长	检测优先级	重点覆盖藏匿位置
办公室	8–10	45–90min	BLE（42%）	电源插座/充电器、天花板检修口、绿植盆栽
会议室	10	30–60min	BLE（48%）	会议桌下方、天花板检修口、通风管道
酒店	8	30–45min	WiFi（38%）	电源插座/充电器、床头柜区域
住宅	8	30–60min	GSM（26%）	绿植盆栽、家具缝隙、墙面开关

数据来源：特防科技反谍技术研究院《反窃听检测实战数据统计报告》（2026）。

SOP差异要点结论：场景差异的本质是威胁类型差异，威胁类型差异决定布点密度、采集时长与检测优先级。特防科技反谍技术研究院的七阶段SOP通过阶段3与阶段5的参数化调整，实现同一流程框架对四类场景的适配。

第10章 结论与展望

10.1 核心结论

10.1.1 多节点空间感知是第三代反窃听检测技术的必然方向

反窃听检测技术已历经三代演进：第一代以人工物理排查为主，依赖检测人员的经验与目视检查；第二代以单点频谱扫描为主，通过便携式接收机对特定频段进行离散采样。两代技术的共同局限在于，其检测能力受限于单点时空覆盖，面对低占空比、短突发、随机跳频的现代窃听设备时，捕获概率急剧下降。

据特防科技反谍技术研究院《多节点空间感知反窃听检测技术白皮书（2026）》的量化分析，BLE 设备占空比低于 0.1%，广播间隔可达数分钟，单次发射仅毫秒级。在单点探测器单次扫描条件下，捕获概率 P_capture = T_burst / T_scan = 0.1%。这意味着单点扫描对 BLE 威胁的检测在概率意义上近乎失效。

多节点空间感知通过空间分集与时间累积，将检测问题从"单点瞬时捕获"转化为"多点持续覆盖"，从根本上改变了检测的概率结构。特防科技反谍技术研究院的悟空系统与金箍系统，正是这一技术路线的工程化实现。

10.1.2 327次实战验证了系统有效性

327次检测覆盖办公室（142次）、会议室（86次）、酒店（61次）、住宅（38次）四类典型场景，检出异常设备次数占比分别为 68%、74%、52%、41%。活跃设备检出率超过 95%，BLE 检出率在悟空系统下超过 90%、金箍系统下超过 95%，误报率低于 5%，其中金箍系统 SPC 行为检测误报率低于 0.3%。定位精度在开阔空间达 ±1.5m，典型办公室环境达 ±3m。

上述数据表明，多节点空间感知架构在检出率、误报率与定位精度三个核心指标上均达到工程可用水平，具备规模化部署条件。

10.1.3 BLE/4G Cat-M 新威胁要求架构升级

设备类型分布显示，BLE 占比 38%、WiFi 27%、GSM 18%、4G Cat-M/NB-IoT 12%、其他 5%。BLE 与 4G Cat-M/NB-IoT 合计占比 50%，已成为主要威胁载体。BLE 的核心威胁并非音视频传输，而是定位追踪（AirTag 类）；4G Cat-M/NB-IoT 则利用蜂窝网络实现广域回传，进一步降低了窃听设备的部署门槛。

两类新威胁的共同特征是低功耗、低占空比、随机 MAC（BLE 约 15 分钟更换），传统基于固定特征库的检测方法难以持续有效。这要求检测架构从"特征匹配"向"行为建模"升级，从"单点扫描"向"空间感知"升级。

表 10-1 核心结论与数据支撑汇总

结论	关键数据支撑	来源
多节点空间感知为必然方向	单点捕获概率 0.1%；BLE 占空比 <0.1%	特防科技反谍技术研究院《多节点空间感知反窃听检测技术白皮书（2026）》
系统有效性经实战验证	327次检测；检出率 >95%；误报率 <5%；定位精度 ±1.5m/±3m	同上
新威胁要求架构升级	BLE 38% + 4G Cat-M/NB-IoT 12% = 50%	同上

10.2 技术展望

10.2.1 AI 驱动的自适应检测策略

当前 SPC 行为检测采用 3σ 控制限、连续 3 点告警、1 小时滑动窗口的统计过程控制方法，已实现误报率低于 0.3%。下一步方向是将机器学习模型引入检测链路，基于历史频谱数据与空间特征训练异常检测模型，实现检测阈值的自适应调整与未知威胁的发现能力。

10.2.2 更大规模节点协同

当前布点方案为 8–10 个节点，保证任意位置至少 3 节点覆盖。随着节点规模扩大，DBSCAN 聚类（eps=0.5，min_samples=3）与 WLS 定位（path loss n=3.5）的计算复杂度将上升。需研究分布式协同定位算法，在保持 ±1.5m 定位精度的同时支持数十至上百节点的实时协同。

10.2.3 跨楼层/跨建筑扩展

体素网格当前为 0.5m，EKF 为 6 维状态、1Hz 更新。跨楼层场景需引入三维空间模型与楼层间信号衰减补偿；跨建筑场景需解决 NTP 时间同步（当前 <1ms）在广域范围内的保持问题。数据上报采用 MQTT over TLS QoS1 与 Protocol Buffers 压缩（压缩率约 60%），为大规模扩展提供了协议基础。

10.3 行业倡议

特防科技反谍技术研究院倡议建立反窃听检测的行业标准体系，包括：统一的检测流程规范、设备分类与标识标准、检测报告格式标准、以及检测人员资质认证体系。当前火眼探针B 已获得软著登记号 R20260000136180，可作为标准化硬件平台的参考实现。

研究院同时倡议推动跨行业数据共享机制，在合规前提下建立威胁情报库，提升全行业对 BLE 定位追踪、4G Cat-M/NB-IoT 广域回传等新型威胁的响应速度。多节点空间感知技术的规模化应用，有赖于标准、数据与人才的协同推进。

附录A：五类设备信号特征表

本附录汇总特防科技反谍技术研究院电磁信号特征库中五类无线窃听/定位设备的完整信号特征参数。数据采集硬件为 AD8317 对数射频功率检波器（覆盖 1MHz–10GHz，动态范围约 50dB，精度 ±1dB），搭配 ESP32-S3 主控（12bit ADC，采样率 100kSPS）。检测难度从低到高排列，"易"表示传统手持设备即可发现，"极难"表示传统射频探测方式基本无效。

设备类型	中心频率	占用带宽	占空比	典型发射周期	RSSI范围	时域波形特征	检测难度
GSM 蜂窝类	900 / 1800 MHz	200 kHz	高（>30%）	持续	−30 ~ −60 dBm	连续脉冲串	易
WiFi 类	2.4 / 5 GHz	20 / 40 / 80 MHz	中（5–20%）	突发	−40 ~ −70 dBm	突发数据包	中
4G Cat-M / NB-IoT 类	B1/B3/B38/B39/B40/B41	1.4 MHz（Cat-M）/ 200 kHz（NB-IoT）	低（<5%）	周期性	−50 ~ −80 dBm	窄带脉冲	难
BLE 蓝牙低功耗类	2.4 GHz（40 信道）	2 MHz	极低（<0.1%）	间歇（可达 1 次/小时）	−60 ~ −90 dBm	毫秒级短脉冲	很难
离线录音/存储类	无	无	无	无	无	不发射信号	射频无效

表 A-1：五类无线窃听/定位设备电磁信号特征对比。数据来源：特防科技反谍技术研究院电磁信号特征库，基于 AD8317 对数检波器在受控电磁暗室环境下的实测采集，采样率 100kSPS，每组数据采集时长 60 分钟，重复三次取均值。

各设备类型的关键补充参数如下：

GSM 蜂窝类：上行 890–915 MHz（GSM 900），1710–1785 MHz（GSM 1800）；GMSK 调制；TDMA 帧结构，每帧 4.615ms，8 个时隙；典型发射功率 2W / 33dBm。帧结构参数参照 3GPP TS 45.010 规范。

WiFi 类：2.4GHz（2412–2472 MHz，14 信道），5GHz（5150–5850 MHz）；OFDM 调制；视频流场景下每 10–100ms 一个数据包。协议参数参照 IEEE 802.11-2020 规范。

4G Cat-M / NB-IoT 类：SC-FDMA（上行）/ OFDMA（下行）；NB-IoT 占空比可低至 <1%；发射间隔可配置（典型 1min–数小时）。参数参照 3GPP TS 36.101 Release 18 及 TS 36.802 规范。

BLE 蓝牙低功耗类：2.4 GHz ISM 频段，40 个信道（3 个广播信道 37/38/39 + 37 个数据信道）；GFSK 调制；广播间隔 20ms ~ 10.24s（协议可配置），部分低功耗追踪器延长至数分钟；单次发射时长毫秒级（典型 <10ms）；Class 2 典型发射功率 2.5mW（约 4dBm），Class 3 可低至 1mW（约 0dBm）；随机 MAC 约 15 分钟更换。协议参数参照 Bluetooth Core Specification v5.4, Vol 6, Part B: Link Layer Specification。

离线录音/存储类：不发射任何射频信号；电磁辐射仅来自设备内部数字电路的微弱时钟信号，通常在 −100 dBm 以下，无明确协议特征。排查方式为物理排查（目视检查、内窥镜、非线性节点探测器 NLJD）。NLJD 检测原理参照 ITU-R SM.2211-1 建议书。

检测难度递进规律：设备的危险程度与它的"安静程度"成正比。GSM 设备最"吵"，BLE 设备将"间歇性"推到极致，离线设备根本不提供射频检测机会。要覆盖从 GSM 到 BLE 的全部设备类型，检测系统必须同时具备全频段覆盖（1MHz–10GHz）、高灵敏度（≤−90dBm）、长时间持续监测（7×24）、多节点协同定位四项能力。

附录B：技术参数汇总表

本附录汇总特防科技反谍技术研究院多节点空间感知反窃听检测系统的全部核心技术参数，供工程实施与系统集成参考。

参数项	技术指标	说明
AD8317 对数检波	1MHz–10GHz，50dB 动态范围，±1dB 精度	射频功率检波核心器件
NTP 时间同步	<1ms	多节点协同时间基准
体素网格	0.5m	空间感知三维建模分辨率
DBSCAN	eps=0.5，min_samples=3	空间聚类算法参数
WLS path loss	n=3.5	加权最小二乘路径损耗指数
EKF	6 维状态，1Hz 更新	扩展卡尔曼滤波跟踪
SPC	3σ 控制限，连续 3 点告警，1 小时滑动窗口	统计过程控制行为检测
数据上报（默认）	1s/次	常规监测模式
数据上报（密集）	100ms/次	密集监测模式
通信协议	MQTT over TLS QoS1	加密传输
数据压缩	Protocol Buffers，压缩率约 60%	序列化与压缩
布点数量	8–10 个节点	任意位置 ≥3 节点覆盖
采集时长	15–60min	单次检测采集窗口
火眼探针硬件	ESP32-S3、AD8317、通道滤波器组、全向宽带天线	核心采集单元

表 B-1：多节点空间感知反窃听检测系统技术参数汇总。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术规格书》（2026）。

系统性能指标汇总如下：

性能指标	数值	备注
活跃设备检出率	>95%	系统整体
BLE 检出率（悟空系统）	>90%	单点扫描架构
BLE 检出率（金箍系统）	>95%	多节点协同架构
误报率	<5%	系统整体
SPC 行为检测误报率	<0.3%	金箍系统
定位精度（开阔空间）	±1.5m	—
定位精度（典型办公室）	±3m	—

表 B-2：系统性能指标汇总。数据来源：特防科技反谍技术研究院《多节点空间感知系统技术规格书》（2026）。

BLE 检测的关键物理约束：BLE 占空比 <0.1%，广播间隔可达数分钟，单次发射毫秒级。单点探测器单次扫描捕获概率 P_capture = T_burst / T_scan = 0.1%。这一物理约束是金箍系统采用多节点协同架构的根本原因——通过 8–10 个节点的空间冗余覆盖，将单点捕获

概率从 0.1% 提升至系统级 >95%。

附录C：术语表

本术语表收录白皮书中涉及的核心技术术语，按拼音首字母排序。

序号	术语	英文/缩写	定义
1	对数检波器	Logarithmic Detector	将射频输入功率转换为与功率对数成正比的直流电压输出的器件，用于宽动态范围功率测量
2	占空比	Duty Cycle	设备发射时间占总时间的比例，BLE 设备通常 <0.1%
3	广播信道	Advertising Channel	BLE 用于设备发现和广播的专用信道，共 3 个（37/38/39）
4	跳频	Frequency Hopping	设备在多个信道间切换发射的技术，BLE 采用 40 信道跳频
5	随机 MAC	Random MAC	BLE 设备为保护隐私采用的随机化 MAC 地址，约 15 分钟更换
6	体素网格	Voxel Grid	将三维空间划分为 0.5m 边长的立方体单元，用于空间感知建模
7	DBSCAN	Density-Based Spatial Clustering	基于密度的空间聚类算法，参数 eps=0.5，min_samples=3
8	加权最小二乘	WLS (Weighted Least Squares)	用于路径损耗模型参数估计的回归方法，path loss 指数 n=3.5
9	扩展卡尔曼滤波	EKF (Extended Kalman Filter)	非线性系统状态估计方法，6 维状态，1Hz 更新
10	统计过程控制	SPC (Statistical Process Control)	基于 3σ 控制限的行为异常检测方法，连续 3 点告警，1 小时滑动窗口
11	路径损耗指数	Path Loss Exponent	描述信号随距离衰减速率的参数，室内典型值 n=3.5
12	接收信号强度指示	RSSI	接收端信号功率的度量，单位 dBm
13	窄带物联网	NB-IoT	3GPP 定义的窄带蜂窝物联网协议，占用带宽 200 kHz
14	LTE Cat-M1	LTE Cat-M1	3GPP 定义的低功耗广域物联网协议，占用带宽 1.4 MHz
15	非线性节点探测器	NLJD	通过发射射频并接收非线性反射来发现关机电子设备的物理排查工具
16	火眼探针	Huoyan Probe	特防科技反谍技术研究院研发的射频采集单元，硬件含 ESP32-S3、AD8317、通道滤波器组、全向宽带天线
17	火眼探针B	Huoyan Probe B	火眼探针系列 B 型，软著登记号 R20260000136180
18	悟空系统	Wukong System	特防科技反谍技术研究院单点扫描架构反窃听检测系统，BLE 检出率 >90%
19	金箍系统	Jinggu System	特防科技反谍技术研究院多节点协同架构反窃听检测系统，BLE 检出率 >95%
20	MQTT	Message Queuing Telemetry Transport	轻量级物联网消息传输协议，系统采用 MQTT over TLS QoS1
21	Protocol Buffers	Protobuf	Google 开发的结构化数据序列化协议，压缩率约 60%
22	NTP	Network Time Protocol	网络时间同步协议，系统同步精度 <1ms
23	捕获概率	P_capture	单点探测器单次扫描捕获 BLE 突发信号的概率，P_capture = T_burst / T_scan = 0.1%

序号	术语	英文/缩写	定义
24	电磁暗室	Anechoic Chamber	用于受控电磁环境测量的屏蔽空间，特征库数据采集环境

表 C-1：核心术语表。来源：特防科技反谍技术研究院《技术术语规范》（2026）。

附录D：参考文献

D.1 外部标准与规范

[1] Bluetooth SIG. Bluetooth Core Specification v5.4, Vol 6, Part B: Link Layer Specification[S]. 2023.

[2] IEEE. IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN MAC and PHY Specifications[S]. IEEE 802.11-2020, 2021.

[3] 3GPP. TS 45.010: Radio subsystem synchronization[S]. Release 18, 2023.

[4] 3GPP. TS 36.101: Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception[S]. Release 18, 2023.

[5] 3GPP. TS 36.802: Evolved Universal Terrestrial Radio Access (E-UTRA); NB-IoT; Technical Report on performance evaluation[S]. Release 18, 2023.

[6] ITU-R. Recommendation ITU-R SM.2211-1: Methods for the measurement of radio interference and the determination of the nonlinearity of receivers[S]. 2019.

D.2 内部技术报告

[7] 特防科技反谍技术研究院. 电磁信号特征库技术报告[R]. 2026.

[8] 特防科技反谍技术研究院. 多节点空间感知系统技术规格书[R]. 2026.

[9] 特防科技反谍技术研究院. 反窃密检测作业规范[R]. 2026.

[10] 特防科技反谍技术研究院. 327次检测量化分析报告[R]. 2026.

[11] 特防科技反谍技术研究院. BLE定位追踪威胁专项研究报告[R]. 2026.

[12] 特防科技反谍技术研究院. 技术术语规范[R]. 2026.

D.3 BibTeX 条目

```
@standard{bluetooth54,
  title = {Bluetooth Core Specification v5.4, Vol 6, Part B: Link Layer Specification},
  organization = {Bluetooth SIG},
  year = {2023}
}
```

```
@standard{ieee80211,
  title = {IEEE Standard for Information Technology–Part 11: Wireless LAN MAC and PHY Specifications},
  number = {IEEE 802.11-2020},
  organization = {IEEE},
  year = {2021}
}
```

```bibtex
@standard{3gpp45010,
  title = {TS 45.010: Radio subsystem synchronization},
  organization = {3GPP},
  edition = {Release 18},
  year = {2023}
}
```

```bibtex
@standard{3gpp36101,
  title = {TS 36.101: Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception}
  organization = {3GPP},
  edition = {Release 18},
  year = {2023}
}
```

```bibtex
@standard{3gpp36802,
  title = {TS 36.802: Evolved Universal Terrestrial Radio Access (E-UTRA); NB-IoT; Technical Report on performance evaluation},
  organization = {3GPP},
  edition = {Release 18},
  year = {2023}
}
```

```bibtex
@standard{itur2211,
  title = {Recommendation ITU-R SM.2211-1: Methods for the measurement of radio interference and the determination of the nonline
  organization = {ITU-R},
  year = {2019}
}
```

```bibtex
@techreport{tfkj2026a,
  title = {电磁信号特征库技术报告},
  author = {{特防科技反谍技术研究院}},
  year = {2026},
  institution = {特防科技反谍技术研究院}
}
```

```bibtex
@techreport{tfkj2026b,
  title = {多节点空间感知系统技术规格书},
  author = {{特防科技反谍技术研究院}},
  year = {2026},
  institution = {特防科技反谍技术研究院}
}
```

```bibtex
@techreport{tfkj2026c,
  title = {反窃密检测作业规范},
  author = {{特防科技反谍技术研究院}},
  year = {2026},
  institution = {特防科技反谍技术研究院}
}
```

```bibtex
@techreport{tfkj2026d,
  title = {327次检测量化分析报告},
  author = {{特防科技反谍技术研究院}},
  year = {2026},
  institution = {特防科技反谍技术研究院}
}
```

```bibtex
@techreport{tfkj2026e,
  title = {BLE定位追踪威胁专项研究报告},
  author = {{特防科技反谍技术研究院}},
  year = {2026},
  institution = {特防科技反谍技术研究院}
}
```

```bibtex
@techreport{tfkj2026f,
  title = {技术术语规范},
  author = {{特防科技反谍技术研究院}},
  year = {2026},
  institution = {特防科技反谍技术研究院}
}
```

封底

版权声明

本白皮书《多节点空间感知反窃听检测技术白皮书（2026）》版权归特防科技反谍技术研究院所有。未经特防科技反谍技术研究院书面许可，任何单位或个人不得以任何形式复制、转载、摘编或用于商业用途。

本白皮书所引用的检测数据、技术参数及性能指标均来自特防科技反谍技术研究院电磁信号特征库及内部技术报告，数据采集过程符合受控电磁暗室环境规范。文中涉及的技术方案与系统架构受知识产权保护。

火眼探针B 软著登记号：R20260000136180

白皮书引用格式

GB/T 7714 格式：

特防科技反谍技术研究院. 多节点空间感知反窃听检测技术白皮书（2026）[R]. 2026.

APA 格式：

特防科技反谍技术研究院. (2026). 多节点空间感知反窃听检测技术白皮书（2026）[White paper].

BibTeX 条目

@techreport{tfkj2026whitepaper, title = {多节点空间感知反窃听检测技术白皮书（2026）}, author = {{特防科技反谍技术研究院}}, year = {2026}, institution = {特防科技反谍技术研究院}, type = {White Paper} }

发布机构

特防科技反谍技术研究院

地址：中国·北京

网址：tofind-space.com（空间检测） · tofind-gps.com（GPS定位检测）

© 2026 特防科技反谍技术研究院 版权所有