# 无线内生安全技术2.0

（2024年）

紫金山实验室

2024年11月

# 撰写组名单

## 主编

金　梁　国家数字交换系统工程技术研究中心

## 校稿

胡晓言　国家数字交换系统工程技术研究中心

孙小丽　国家数字交换系统工程技术研究中心

王飞虎　国家数字交换系统工程技术研究中心

李　凯　紫金山实验室

## 贡献单位

国家数字交换系统工程技术研究中心

紫金山实验室

# 前 言

无线通信摆脱了有线通信的束缚，使人们能够在任何时间、任何地点享受无线服务，极大地提高了生活便利性。然而，无线通信中电磁波开放式传播同时造成了无线链路的脆弱性，为攻击者实施恶意攻击提供了天然条件，是引发无线网络安全问题的根源所在。

目前无线通信安全基本上依靠两类方法：一类是直接移植传统有线通信系统中的方法，没有考虑具体的物理层安全传输技术，回避了无线信号本身易被截获的问题；另一类是采用序列扩频/跳频、超宽带等所谓低截获概率传输技术，依赖设计特殊的信号体制提高信息还原的复杂度，仍然没有考虑无线信道传输等因素，一旦信号体制被破解则失去作用，因此没有根本解决信号辐射泄露带来的问题。

无线内生安全技术基于无线环境内生安全属性——“各点异性”的利用和改造，构建高自由度的无线内生安全架构，对抗无线环境中自然与人为的广义不确定扰动，提供抵御“未知威胁”的能力，是内生安全理论与传统无线通信信息安全与功能安全技术的相互融合、相互渗透，能够为开发新的无线通信可靠性、安全性方法提供指导，有望成为未来无线通信安全发展的趋势，具有重要的理论研究与应用价值。

本蓝皮书首先回顾无线通信发展范式，在梳理无线内生安全问题的基础上，提出无线内生安全基础理论；然后，总结了支撑无线内生安全的关键技术，以及目前研究的无线内生安全原型验证系统；最后，结合 6G 愿景，展望了无线内生安全在 6G 中的应用。

本蓝皮书受国家自然科学基金区域创新发展联合基金重点项目

“无线通信‘一次一密’的内生安全理论与基于信息超材料的实现方法”（基金编号：U22A2001）、国家重点研发计划课题“6G 安全内生及隐私保护总体架构和试验验证”（课题编号：2022YFB2902201）、“融合无线空口使能新技术的 6G 内生安全”（课题编号：2022YFB2902202）、“6G 安全内生及隐私保护关键技术评估”（课题编号：2022YFB2902205）、国家自然科学基金青年基金项目“逼近“一次一密”的 RIS 辅助物理层密钥生成关键技术研究”（基金编号：6230012880）的资助。

# 目 录


前 言 ..... III
图目录 ..... VI
缩略语说明 ..... VII
一、 无线内生安全概述 ..... 1
（一）无线内生安全需求 ..... 1
（二）无线内生安全研究现状 ..... 3
1. 无线内生信息安全 ..... 4
2. 无线内生功能安全 ..... 6
二、 无线内生安全基础理论 ..... 11
（一）内生安全的信息论诠释 ..... 11
1.网络空间内生安全问题 ..... 11
2.基于香农完美保密的完美安全猜想 ..... 13
3.内生安全属性——结构的差异性 ..... 14
（二）无线内生安全属性——各点异性 ..... 15
（三）无线内生安全构造 ..... 17
（四）实现完美安全的高自由度构造 ..... 18
1. 无线内生安全的自由度 ..... 18
2. 实现完美安全的自由度条件 ..... 19
3. 信息超材料赋能内生安全自由度 ..... 21
三、 无线内生安全新技术 ..... 23
（一）信息安全 ..... 23
1. 抗截获 ..... 23
1.1 信息超材料辅助的密钥生成 ..... 24
1.2 信息超材料辅助的安全传输 ..... 25
2. 认证 ..... 26
（二）功能安全 ..... 28
1. 隐蔽通信 ..... 28
2. 抗干扰 ..... 30
3. 抗衰落 ..... 31
四、 无线内生安全原型系统与原理验证 ..... 33
（一） 基于 RIS 的无线高速密钥生成与加密系统 ..... 33
（二） 基于 RIS 的 5G 内生安全小基站认证系统 ..... 38
（三） 基于 RIS 的信号隐写与安全传输系统 ..... 41
（四） 基于 RIS 天线的射频前端抗干扰系统 ..... 44
（五） 基于 RIS 的无线内生抗衰落通信系统 ..... 48
五、 无线内生安全的应用展望 ..... 52
（一） 6G ..... 52
（二） 高弹性和强韧性军事无线通信 ..... 54
参考文献 ..... 56

# 图目录

图 1 移动通信与安全演进历程.....1
图 2 基于超材料的 DHR 天线阵列.....8
图 3 信息物理系统广义功能安全问题域.....11
图 4 无线内生安全架构.....18
图 5 信息超材料辅助的物理层密钥生成典型模型示意图.....24
图 6 信息超材料辅助的物理层安全传输典型模型示意图.....26
图 7 通信-无条件认证方案原理图.....27
图 8 基于信息超材料的动态异构阵列精细化匹配多径.....29
图 9 空域抗干扰原理图.....31
图 10 天线匹配接收多径信号.....33
图 11 RIS 辅助的无线高速密钥生成与加密系统总体架构.....34
图 12 系统流程图.....35
图 13 测试场景.....36
图 14 抗攻击测试场景.....37
图 15 物理层密钥测试效果.....37
图 16 基于超材料智能表面的无线内生安全原型系统.....38
图 17 整体测试环境.....38
图 18 基站告警界面.....39
图 19 终端 B 无法驻留网络并访问网页界面.....40
图 20 终端间隔 2m.....41
图 21 终端间隔 0m.....41
图 22 基于 RIS 的信号隐写与安全传输系统架构.....42
图 23 基于 RIS 的信号隐写与安全传输系统工作流程.....43
图 24 隐写信息帧格式.....43
图 25 信号隐写功能测试.....44
图 26 安全传输功能测试.....44
图 27 基于 RIS 天线的射频前端抗干扰系统总体架构.....45
图 28 基于 RIS 天线的射频前端抗干扰系统软硬件组成.....46
图 29 基于 RIS 天线的射频前端抗干扰系统工作流程.....47
图 30 基于 RIS 天线的射频前端抗干扰系统外场测试.....48
图 31 基于 RIS 天线的射频前端抗干扰系统测试效果.....48
图 32 无线内生抗衰落通信系统总体架构.....49
图 33 无线内生抗衰落通信系统硬件图.....49
图 34 无线内生抗衰落通信系统工作流程.....51
图 35 无线内生抗衰落通信系统测试.....51
图 36 无线内生抗衰落通信系统测试.....52

# 缩略语说明

| 缩写 | 英文全称 | 中文解释 |
| --- | --- | --- |
| 1G | 1st Generation Mobile Communication System | 第一代移动通信系统 |
| 2G | 2th Generation Mobile Communication System | 第二代移动通信系统 |
| 3G | 3th Generation Mobile Communication System | 第三代移动通信系统 |
| 4G | 4th Generation Mobile Communication System | 第四代移动通信系统 |
| 5G | 5th Generation Mobile Communication System | 第五代移动通信系统 |
| 6G | 6th Generation Mobile Communication System | 第六代移动通信系统 |
| AES | Advanced Encryption Standard | 高级加密标准 |
| CDMA | Code Division Multiple Access | 码分多址 |
| CSI | Channel State Information | 信道状态信息 |
| DDoS | Distributed Denial of Service | 分布式拒绝服务 |
| DHR | Dynamic Heterogeneous Redundancy | 动态、异构、冗余性 |
| DOA | Direction Of Arrival | 波达方向 |
| EF | Expected Function | 期望功能 |
| eMBB | Enhanced Mobile Broadband | 增强型移动宽带 |
| ESS | Endogenous Safety and Security | 内生安全 |
| FDMA | Frequency Division Multiple Access | 频分多址 |
| FFT | Fast Fourier Transformation | 快速傅里叶变换 |
| FPGA | Field Programmable Gate Array | 现场可编辑门阵列 |

| 缩写 | 英文全称 | 中文解释 |
| --- | --- | --- |
| IDF | Invisible Dark Function | 隐式的暗功能 |
| IFFT | Inverse Fast Fourier Transform | 快速傅里叶逆变换 |
| ITU | International Telecommunication Union | 国际电信联盟 |
| MIMO | Multiple-Input Multiple-Output | 多输入多输出 |
| mMTC | Massive Machine Type Communication | 大规模机器类型通信 |
| NR | New Radio | 新空口 |
| PKI | Public Key Infrastructure | 公钥基础设施 |
| RIS | Reconfigurable Intelligent Surface | 可重构智能超材料表面 |
| RSS | Received Signal Strength | 接收信号强度 |
| SS7 | Signaling System Number 7 | 七号信令系统 |
| SUPI | Subscription Permanent Identifier | 用户永久身份标识 |
| TDD | Time Division Duplexing | 时分双工 |
| TDMA | Time Division Multiple Access | 时分多址 |
| uRLLC | Ultra-reliable and Low Latency Communications | 超可靠和低延迟通信 |
| VSEF | Visible Side-Effect Function | 显式的副作用功能 |
| WESU | Wireless Endogenous Security Unit | 无线内生安全单元 |
| ZUC | ZU Chongzhi | 祖冲之密码算法 |

# 一、无线内生安全概述

## （一）无线内生安全需求

无线通信的发展，以地面蜂窝移动通信系统为例，从只支持语音通信的 1G 时代，短信业务风靡一时的 2G 时期，支持高速数据传输的 3G 时期，智能手机与移动互联网蓬勃发展的 4G 时期，发展到如今万物互联的 5G 时代，移动通信在市场需求、技术进步的驱动下日新月异，其演进过程具有明显的代际效应。反观无线通信安全的发展，以已知的安全问题为导向，采用“亡羊补牢”、“围堵修补”的打补丁方式予以应对。例如，2G 中采用 A51/A52 加密算法实现单向认证机制，存在无法抵抗伪基站攻击的问题。为了弥补这一漏洞，3G 中改为基于 Kasumi 算法的双向鉴权机制，然而 SS7 信令自身的缺陷导致无法抵御信令劫持攻击。4G 中基于 Diameter 协议，采用基于 Snow3G/AES/ZUC 分级密钥的方法应对这一安全威胁，但又出现了跨网攻击问题，在 5G 中通过增加网元认证、元数据防护等技术予以解决。

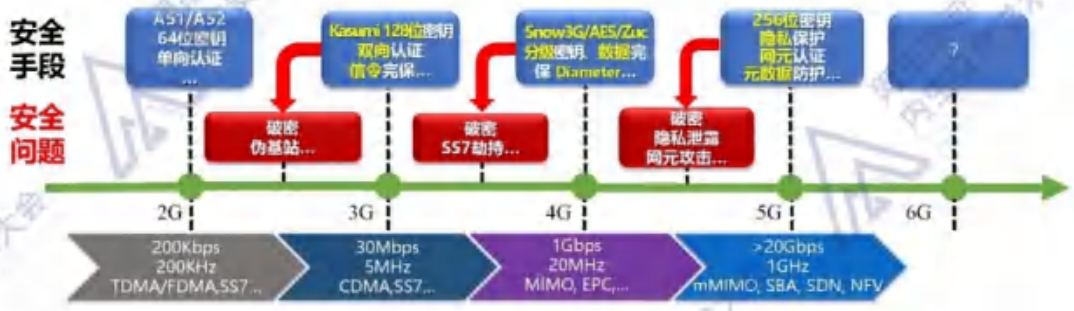


图 1 移动通信与安全演进历程

不难发现在上述演进历程中，安全通常被视作通信的伴随技术，相对滞后于通信技术的变革，呈现出伴随式发展、渐进式增强的特点。

这主要是因为当前无线通信系统大多沿用了传统有线通信中“外挂式”的安全机制，采用的各类加密算法、安全协议与通信过程相对独立，难以针对无线安全问题精准施策，只能依靠新补丁解决旧问题，而无法预防当前系统中的未知风险和漏洞。除此之外，随着未来的无线接入设备日趋多样，无线网络愈发开放融合，无线通信系统面临着更多无法预估的安全威胁和更加严峻的安全形势。在此背景下，如果沿用传统安全策略，势必重蹈覆辙，不断陷入找漏洞、打补丁的死循环，致使无线通信系统一直延续被动挨打、疲于奔命的态势。

此外，近年来安全的内涵在 6G 的研究中得以拓展和丰富，ITU 发布的 6G 纲领性文件中，提出 6G 系统设计原则包括但不限于可持续性、安全性/隐私性/弹性等，且安全性、隐私性和弹性被确定为 6G 的七大目标之一，同时被列为 6G 的能力指标。安全、隐私和弹性成为 6G 的安全属性，既包含了信息安全，也涵盖功能安全。2011 年，美国研究机构 MITRE 提出网络弹性/韧性（Cyber Resiliency）概念，后被美国政府和标准化组织采纳，强调从任务视角去保障系统，重点考虑如何在防护失效的情况下也能确保任务达成，即功能安全。2019 年，美国 NIST 正式发布《开发网络弹性系统—一种系统安全工程方法》，标志着全球第一部权威性的网络弹性技术文件正式出台。2021 年，美国国家科学基金会发布面向 NextG 网络（美国 6G）RINGS（Resilient & Intelligent NextG Systems）计划，强调网络弹性，安全性、适应性、自主性和可靠性。2022 年，北美 6G 联盟发布 6G 路线图，确定了信任、安全及弹性等六个目标。可见，功能安全正受到越

来越多的重视。因此，6G 安全需在充分考虑信息安全需求的同时，需深入规划和实现功能安全，从而为未来社会打造坚强可靠的数字化连接底座。

内生安全理论是解决上述问题的理想途径之一。内生安全理论是利用具有动态、异构、冗余属性（Dynamic Heterogeneous Redundancy, DHR）的内生安全架构（DHR 架构）来实现内生安全功能。相较于现有的“捆绑”、“拼盘”式的安全机制，内生安全理论旨在探索系统自身构造或运行机理中的安全属性，构建内生安全架构，使系统自身具备敌方难以认知的“测不准”效应，从而实现抵御未知威胁，以及安全与通信的技术共用、资源复用、均衡发展的内生安全功能。这一内生安全机制不仅保证了系统的可靠性，也使攻击者对系统结构、运行机制产生认知困境，从而难以开展有效攻击。因此，内生安全理论能够用于抵御已知和未知的安全威胁及攻击。近些年来，该理论在原理探索、技术突破、系统研制等方面均取得了重要成果。

在内生安全理念的启发下，无线内生安全的相关研究也在深入开展。在无线内生安全 1.0 的基础上，可以进一步认识到，与传统内生安全的研究有所不同，无线信道天然就具有“各点异性”的内生安全属性。利用这些属性，可以设计无线通信系统特有的内生安全架构，保障发射机到接收机之间信息传输的安全与可靠。

### （二）无线内生安全研究现状

无线内生安全的目标是保证无线通信中信息传输的安全与可靠，包括无线内生信息安全和无线内生功能安全。

## 1. 无线内生信息安全

无线内生信息安全是利用无线信道的内生安全属性来保护信息的机密性、可信性和完整性。核心安全机理来源于无线信道的时变性、互易性、随机性、唯一性。利用无线信道内生安全属性搭建安全通信的“专属信道”。既可以实现对信号随机加扰的物理层安全传输技术[1]，也可以实现基于“一次一密”的物理层密钥生成技术[2]，以及基于信道指纹和射频指纹的物理层安全认证技术。

其中，物理层安全传输技术本质是利用无线信道的唯一性，设计与无线信道强相关的信号传输和处理机制，使得只有特定信道上的用户可以正确解调信号，而在其它信道上的信号是经过随机加扰且无法恢复的。文献[3]研究了异构携能通信网络中 CSI 存在随机误差时，顽健能量与信息安全传输问题，给出一种人工噪声辅助的安全传输方案。通过联合设计下行波束矩阵及人工噪声矩阵，使网络中其他用户信号及人工噪声能够干扰窃听者，同时提升系统能量的接收性能，并验证了其方案有效性和顽健性。新兴技术的发展也为安全传输提供新的助力。文献[4]针对窃听节点随机分布的 MISO 系统通信场景，分析了智能超表面（Reconfigurable Intelligent Surface，RIS）辅助下的安全通信性能。给出了传输安全中断概率的闭式表达式，分析了反射单元数量、发射天线数量等参数对中断概率的影响，并证明了部署反射面可以在低能耗下提升安全性能。文献[5]指出在 ISAC 场景中，ISAC 发射机需要将功率集中到目标方向以获得良好的估计效果，这导致目标对传感波形中嵌入的保密信号具有较高的 SINR，使得目标容易截

获其中携带的机密信号，即ISAC系统中存在需要将功率集中到目标方向和限制目标处的有用信号功率之间的权衡。文献[6]研究了感知功能辅助ISAC系统安全传输，利用ISAC信号接收机获得的感知信息来辅助安全通信，建立了感知精度与保密速率联合最大化的优化问题，并提出了一种利用感知信息实现保密速率迭代提升的迭代算法，仿真结果表明所提方案的安全性能相较于ISAC接收机完美知道CSI的AN方案安全性能提升了约28%.

文献[7]指出，利用无线信道的唯一性、时变性和随机性等内生安全属性，能够从信道中提取随机密钥，生成第三方无法测量、无法重构、无法复制的密钥。通过无线内生属性与RIS等新兴使能技术的结合，充分挖掘RIS的电磁环境定制能力和电磁可重构特性，从增强无线信道熵与精细化感知无线信道两个角度双管齐下，同时提高无线通信容量和无线密钥生成速率。作为动态异构冗余构造框架下的具体实现之一，可以基于RIS的电磁性态柔性可重构和操控电磁波的特性，通过材料科学与信息科学交叉融合赋能无线内生安全，为实现可控的异构执行体构造提供了技术途径[8]。文献[9]利用RIS辅助，提出了一种基于多径信道分集的物理层密钥生成方案，通过多径分离和参数估计，利用多维独立路径增益生成密钥。文献[10]提出猜想，在快速衰落环境中，必然存在内生密钥速率能够与用户数据速率相匹配的无线系统，并进行了理论分析和仿真实验，提出在无线通信系统中，通过内生密钥实现一次一密是可能的。2023年12月8日，紫金山实验室发布了全球首款支持无线内生安全加密算法的芯片，可提供一次一密

的信道密钥协商功能，即将信号密码与时空坐标结合，除非攻击方与合法用户的时空坐标完全一致，否则合法信道不可测量、不可复制[11]。

物理层安全认证技术从物理层的视角出发，利用与位置相关的信道特征硬件和固有的设备特征来保障无线网络安全。文献[7]指出，在无线通信系统中，无线环境通过自然信道起作用。信道具有随机性和时变性，是自然界中一种天然的随机源。同时，无线信道还具“各点异性”，不同位置对应的无线信道所表现出的特征属性不同,即无线信道具有天然的内生安全属性。典型的无线通信系统可看成是一种天然和人工的 DHR 构造。文献[12]利用 RIS 增强无线信道系统的内生安全属性，生成更加健壮的认证标签。文献[7]表明，无线信号中还蕴含着另一典型的内生安全属性——射频指纹。射频指纹源于发射机中部件容差和工艺条件等造成的系统不一致性，其产生机理决定了射频指纹具有唯一性和第三方不可仿冒性。因此，射频指纹可用于识别接收信号来源从而实现信息保护和设备的快速认证。文献[7]指出，得益于无线内生安全理念，使物理层加密和认证天然具有密不可分的内在联系。例如，在收发双方完成初始认证后，发送方利用信道指纹生成密钥对消息进行加密，若接收方可正确解密便是认证了合法信道，从而实现了对发送方身份的认证。文献[7]提出了一种 PHYLOCK 结构，为无条件认证提供一次性密钥。利用信道指纹生成密钥不仅在加密方面具备轻量级、动态更新、逼近“一次一密”的优势，在认证方面也具备低时延、安全、高效的特点。

## 2. 无线内生功能安全

无线内生安全不仅能提供高可信的信息安全，也能提供高可靠、高可用的功能安全，实现通信、安全和抗干扰的一体化内生安全功能。功能安全是指无线传输的可靠性[8]，许多传统无线通信技术的目的都属于保障通信的功能安全，它们主要是对抗包含自然信道的不确定干扰和人为扰动在内的广义不确定扰动，属于基于非典型 DHR 架构的内生安全技术。例如无线通信抗干扰技术，大致可分为时域[13]、频域[14]和空域[14]抗干扰。时域抗干扰和频域抗干扰主要通过信号传统带宽的扩展来提高信息传输的可靠性，包括跳时通信、猝发通信、交织纠错编码、跳频扩谱、直接序列扩频等。空域抗干扰利用无线信号在空间的传播特性，通过调整天线极化方式、主瓣方向实现空域内的抗干扰，主要包括自适应天线调零技术和分集技术。可以看出，传统抗干扰技术是在有限的信号空间内与干扰进行对抗与博弈。随着干扰功率的增加和干扰变化规律的日益复杂，现有抗干扰方法能够获得的性能增益将会显著下降。未来抗干扰技术的发展演进，其基础核心能力的生成必然遵循电磁空间体系自由度对抗的规则，通过主动构造自由度优势，发现并利用干扰与目标信号的差异性达到抑制干扰提取信号的效果。传统抗干扰“轻采集、重处理”、“轻模拟、重数字”的体系架构发展路线过分强调后端数字处理带来的自由度增益，没有充分意识到射频前端在电磁空间自由度构造方面的潜力和能力，忽视了干扰与目标信号在电磁波域的物理差异性。

当前无线内生功能安全研究主要包括基于无线环境差异的隐蔽通信、抗干扰、抗衰落等技术。RIS 是一种通过数字化手段重构电磁

特性模拟参数的新型技术，可以部署在传输过程对信号传输环境进行实时重构。图 2 所示为基于超材料的 DHR 天线阵列，通过空域多样性构造，可使得不同位置的阵元具有异构、不相关的方向图。该阵列能够使空域资源摆脱空谱墙的限制，在天线孔径受限条件下提升效能。

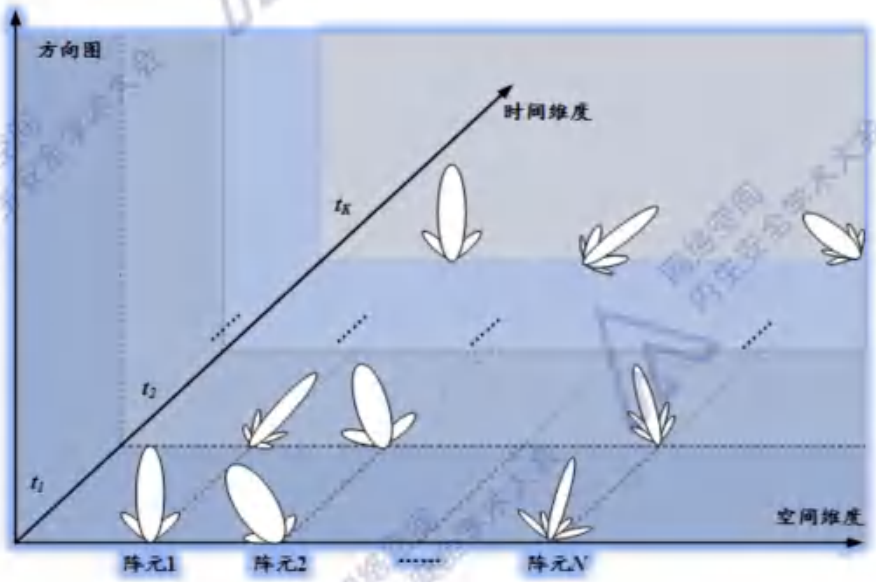


图 2 基于超材料的 DHR 天线阵列

针对隐蔽通信问题，通过将信号能量按既定规则或码本分别在时间或频率上打散，以增加敌方信号检测难度。尽管以扩频通信为代表的隐蔽通信应用已经较为成熟，但事实上，实现的隐蔽性能从未得到理论证明，隐蔽传输能力也难以有效衡量，且盲解扩[15]、盲检测等技术使其具备的隐蔽性和安全性不断受到质疑。直到 2013 年 Bash 等人发现并证明了隐蔽通信的平方根律，直截了当地回答了隐蔽通信的信息理论限制[16]。文献[16]开展了基于无线环境差异的多天线隐蔽通信技术研究，为隐蔽通信的实现、评估和改进提供新思路。该文献首先针对目前缺乏有效方案对抗敌方能量趋势检测手段的问题，在丰富散射无线环境下提出一种基于公开通信掩体的多天线隐蔽通信方案，具

体通过非理想ZF预编码、导频及数据发射功率的联合最优设计，对最大隐蔽容量目标进行优化。而后针对目前缺乏面向上下行联合隐蔽的发射功率和通信块长最优设计问题，在丰富散射无线环境下，分别基于无线环境固有的噪声不确性场景和源自有限块长的噪声不确定性场景，进行了多天线隐蔽通信方案设计，具体分别通过最优发射功率设计、以及导频和数据长度最优分配，对最大隐蔽吞吐量目标进行优化。接着针对目前隐蔽通信评价指标难以衡量系统抵御未知检测威胁能力的问题，构建了隐蔽威胁区域这一新的评价指标。最后针对面向隐蔽通信需求的信号能量在空域上精细化打散问题，在有限散射无线环境下，设计了一种基于随机跳径方案的空域打散机制，并提出一种DHA构造，显著提高了打散效率。

针对无线通信抗衰落问题，现有技术较少考虑天线前端抗衰落，而是衰落已经在天线前端发生的情况下在后端采取补救办法，或者通过多天线分集等方法降低多径衰落的影响[17]。文献[17]中提出一种基于 RIS 天线的抗衰落方案，具体介绍了 RIS 天线接收多径信号的基本模型，给出了相应数学表达关系，然后提出了以最大化接收信号的信噪比为目标的 RIS 天线相位响应系数的设计优化问题，并给出了两种解决方案，仿真结果表明，RIS 的引入可以降低硬件成本和能耗，在单天线前端实现多径环境下的抗衰落。文献[18]在 RIS 辅助的宽带 MISO-OFDM 系统抗干扰通信方案中考虑了由于频率选择性衰落效应导致不同频率子载波信号有不同的衰落的问题，在抗干扰设计过程中考虑到 RIS 反射系数需满足具有不同信道增益的子载波信号

的构造性叠加的问题，结果表明RIS的赋能可以提高系统的抗干扰和抗衰落能力。

针对无线通信抗干扰问题，采用RIS可以主动构造自由度，在前端发现并利用干扰与目标信号的差异性达到抑制干扰、提取信号的效果。文献[19]设计了一种基于RIS空频联合的抗干扰方案，利用RIS在不同频率上的响应差异对干扰信号进行空间与频率联合滤波。文献[20]考虑了无线传感网络中的抗干扰问题，设计了一种基于深度神经网络的RIS相移调控方案，在保证低功耗的同时最大化传输速率。为应对智能干扰器导致干扰模型和干扰行为未知问题，文献[21]设计了一种强化学习策略，在考虑合法用户服务质量的同时，对基站的功率分配和RIS的反射波束成形进行联合优化，提高抗智能干扰能力。文献[22]则针对智能干扰，在RIS辅助条件下建立了合法用户与干扰机之间的博弈模型，并考虑了信道信息不完美的情况，提出了一种鲁棒的抗干扰算法。针对干扰存在的突发性与不确定性，文献[23]利用RIS轻量化的特点，搭建了无人机空中RIS平台，最大程度上发挥其灵活性，对空中RIS的部署位置和无源波束成形进行联合优化，保证传输性能。文献[24]基于RIS捷变的特点提出了一种空时异构天线阵列，以及前后端联合盲抗干扰方案。其中每一个异构天线快速扫描、分辨多径，实现对无线环境的精细化感知和操纵，利用超表面天线方向图快速可重构能力提升阵列自由度；在未知干扰信道条件下分离期望信号，并根据信道盲估计结果，优化设计超表面天线参数；所提方案在保证单天线信干比的条件下实现阵列接收信干噪比的最大

化，降低射频前端大功率干扰与期望信号叠加导致的信息损失。

## 二、无线内生安全基础理论

本章首先从香农信息论视角剖析了网络空间内生安全问题，提出了基于香农完美保密的完美安全猜想，总结了内生安全的本质和内生安全属性——结构的差异性；接着，类比网络空间内生安全，归纳并提出了无线内生安全属性——“各点异性”，以及基于各点异性的无线内生安全构造；最后，探讨了无线内生安全自由度和实现完美安全的自由度条件，提出了利用信息超材料提升内生安全自由度、逼近完美安全的新思路。

### （一）内生安全的信息论诠释

#### 1.网络空间内生安全问题


图 3 信息物理系统广义功能安全问题域

当前的开放式产业生态环境使得网络空间的内生安全问题数量正比于软硬件产品规模，内生安全问题呈弥漫的态势遍布整个网络空间。这一方面导致网络系统软硬件物理失效等等的功能安全威胁难以规避，另一方面也导致人为注入的安全漏洞、蓄意后门无法杜绝。如

图 3 所示，如果信息物理系统内部既存在某些传统类型的不确定扰动（例如随机性错误、失效、故障等可靠性问题），也存在人为的针对目标系统漏洞、后门等“暗功能”的未知网络攻击扰动，则它们也可称之为广义功能安全问题（Generalized Safety and Security Problems, GSSP）。这类问题大多由人为攻击这个外因，通过目标对象自身存在的内生安全个性或共性问题这个内因的相互作用而形成[25]。在这一背景下，如何在不依赖先验知识的条件下，解决基于目标对象未知内生安全问题的网络攻击问题，是网络内生安全关注的重点[26]。

一个显而易见的结论是，攻击者攻击的前提，是先要认清目标系统的构造。也就是说，目标对象的视在多样性表达会给攻击者造成很大的认知障碍。这说明，如果能够使信息物理系统内部构造及运行环境对外呈现出多样性和随机性，就有可能在面对“未知的未知”安全威胁时逆转攻击者的单向透明优势。在无任何先验知识的条件下，这能使攻击者陷入由于无法认知“系统构造”而无法发起有效攻击的困境。显然，如果一个系统能够通过系统的内源性构造属性（即，内生安全属性）使得“历史攻击结果”与“下一次攻击结果”无关，那么无论获得多少关于“历史攻击结果”的信息，对于攻击者认知系统构造进而控制“下一次攻击结果”都是没有帮助的。这是内生安全所期望获得的安全效应，即：

$$\Pr(\text{下一次攻击结果} \mid \text{历史攻击结果}) = \Pr(\text{下一次攻击结果}) \quad (1)$$

其中，$\Pr(\ )$为概率。上式蕴含了无法通过分析“历史攻击结果”推导出“下一次攻击结果”，也就是知晓“历史攻击结果”之后的后验概

率等于未知“历史攻击结果”时的先验概率[27]。

**2.基于香农完美保密的完美安全猜想**

不难发现，内生安全机制所期望的“无法认知系统构造”与密码学中定义的完美保密十分相似。两者都具有“A 与 B 相互独立”以及“无需先验知识”等相同的内涵。这说明内生安全机制的某些特性可能与经典密码学是相通的，内生安全机制可能在满足一定的条件下获得与经典密码学相似的安全效果。为了探讨这一问题，首先给出完美保密的定义。

定义 1　完美保密性（Perfect Secrecy）：对于明文空间为$\mathcal{M}$的加密方案，当以任意分布从$\mathcal{M}$中选择明文，并且选出的任意明文$m\in\mathcal{M}$和得到的任意密文$c\in\mathcal{C}$（$\Pr(C=c)>0$）都满足下式时，该加密方案是完美保密方案[28]，

$$\Pr(M=m|C=c)=\Pr(M=m) \tag{2}$$

该定义与式(1)在形式和概念上是一致的。明显的启示是：构造一个“下一次攻击结果与历史攻击结果无关的系统”与构造一个“明文与密文无关的加密方案”在原理上很可能是相通的。

上述分析表明，完美保密与内生安全两者存在相同的前提假设，如“不依赖先验知识”、“无需考虑攻击者的能力、攻击方式”；也存在相同的期望目标，如式(1)和式(2)都蕴含了“无法从攻击目标（密文）中获得任何关于系统构造（明文）的信息”的安全效果，使攻击者陷入认知迷雾（拟态迷雾）。这说明不依赖先验知识的内生安全与不依赖先验知识的完美加密之间存在某些相同或相似的性质。

猜想的证明过程见[29]。

**3.内生安全属性——结构的差异性**

上述猜想和证明过程初步说明了网络空间完美安全的存在性和可实现性，也揭示了内生安全的本质是基于构造的安全，其安全基因源于内生安全属性——结构的差异性。结构差异使得攻击者难以获得攻击所需的完全信息量，等价地，能够在攻击方产生相对于防御者永远更不确定的信息（随机性）。因此，内生安全属性可定义为：防御者与攻击者之间由先天的自然结构或/和后天的人工构造带来的差异性。该属性源于构造的差异性，除非攻击者能改变自身或/和防御者的构造，否则永远无法彻底消除。

内生安全的“完美”效应如下。

**基于构造的安全：**完美安全可以用“物理构造加密”来实现，攻击者要有破译“一次一重构”的结构密码的能力才能有效攻击，这说明内生安全的本质是基于构造的安全。

**无需攻击者先验信息：**能在不依赖（但不排斥）攻击者先验信息的条件下，有效避免已知的未知或未知的未知等广义功能安全问题导致的安全事件。

**结构赋能：**基于物理结构加密的赋能机制，能够阻断广义功能安全问题之内因和人为或非人为扰动之外因间的相互作用，架构内即使存在内生安全问题也难以演变为安全故障。

**安全是可度量设计的：**不论是已知的未知概率问题，或者未知的未知不确定性问题所造成的广义不确定扰动都能变换为广义可靠性

量纲呈现的可量化设计与可验证度量指标。

### （二）无线内生安全属性——各点异性

对于当今无线通信技术，已很难说清楚环境中是否存在被第三方恶意控制、部署的无线传感器在进行窃听、干扰、电磁环境测量等行为。因此，不能再将希望寄托于窃听信道条件恶劣于合法者信道、窃听信道难以获知合法者信道等理想条件。需将整个无线通信过程、无线电磁环境等先验知识，以白盒方式、无约束地提供给第三方攻击者，并在此条件下探讨无线内生安全的属性、构造等问题。

首先，给出内生安全属性定义，并由此提出无线内生安全属性——各点异性。

**内生安全属性：**防御者与攻击者之间由生来固有的自然结构或/和人工构造带来的差异性。攻击者由于这些差异性难以精确获得攻击所需的完全信息量。等价地，使攻击者相对于防御者永远更随机的那部分信息。

由内生安全属性定义可知，防御者应当利用某种天然/人工的差异属性来摆脱攻击。对于无线通信来说，环境中不同位置处的无线信道，天然具有差异性，这是原始的、空间位置结构造成的差异。攻击者能否克服差异的影响只取决于它的相对物理位置。从无线通信“第一性原理”麦克斯韦方程分析，各点异性和边界条件相异等价，会导致方程解的差异性。**因此，各点异性可定义为：攻防双方由先天的自然结构或/和后天的人工构造带来的无线环境差异性。**各点异性作为属性的原因和价值是具有本源性和基础性，可以把其它约束放得很宽：

可容忍超强攻击者假定，即精确已知无线环境，可知自己信道和对方信道，可确知差异的大小。但只要差异存在就能被防御者利用以提高安全增益，产生安全效应。

下面给出具体例子，无线通信的一般表达式为 $Y = HWX + N = GX + N$。其中，$X$、$Y$ 分别表示发送、接收信号，$N$ 表示噪声。$H$ 表示物理环境映射的自然信道，令 $H_A$ 表示合法者信道、$H_E$ 表示攻击者信道，由于物理位置差异，$H_A$ 和 $H_E$ 存在差异。$W$ 表示预编码系数，亦将其视为人工信道，其物理对应形式，包括但不限于多天线阵列、多载波传输等多维信号空间。$G = HW$ 表示人工+自然的广义无线信道，令 $G_A$、$G_E$ 分别表示广义合法者、攻击者的无线信道。

根据前文所述，攻击者可已知 $H_A$、$H_E$，并确切了解二者间差异。对于基于无线内生安全的防御者，其根据具体需要实现的无线内生安全功能（信息安全、功能安全），通过设计防御方的 $W$，利用/构建各点异性环境，来决定保持/放大差异。

在无线内生安全下，合法方公开一切通信协议、边界条件（等价为密码学的加密算法、协议等），并利用物理位置差异构建各点异性环境（对环境加密，等价为密码学的密钥），进而实现无线内生安全功能。而各点异性使得攻击方无法通过无线环境感知、地理与位置信息获取、数学解算等方式抵消信道差异，只能通过物理位置抵近、阵列等效自由度提升等物理手段来缩小信道差异、完成攻击。因此可认为无线内生安全实现了一种基于物理复杂度的安全通信方式。

这样，游戏规则及其博弈方式变成了阵列自由度、位置抵近等物

理条件下信道差异分辨率的比拼。在这场博弈中各向异性是天生的且始终存在的，防御者相对于攻击者具有先天不对称信息优势，如果这种不对称优势能以某种（人工）机制保持甚至放大，则可以定义为“在信道分辨率 ε 下的完美安全”。

在白皮书 1.0 版本提出的无线信道的其它性质中，唯一性、多样性、测不准性都可看作源于各点异性，时变性在假定环境变化且攻击者未知无线环境时产生随机性，可以用于安全，但比各向异性的前提约束强。目前看，**无线内生安全属性有且仅有各点异性**。

### （三）无线内生安全构造

以基于构造差异的内生安全视角审视无线通信系统，可以发现：无线内生安全以无线信道作为执行体，通过重构无线信道实现构造加密，获得各点异性的差异性信道环境。

基于上述推论，无线内生安全架构可以归纳为如图 4 所示，与典型网络空间内生安全架构对应的异构执行体是无线信道，输入代理为发信机，输出裁决为接收机。以上三者所包含的区域称为拟态界，也就是无线内生安全架构所要保护的范围。此外，输出裁决进行的分集技术(如最大比合并等)，可以减小随机噪声带来的影响，类似于拟态系统纠错输出中的策略裁决机制。发信机利用接收机发送的导频估计信道后，进行的波束形成技术可类比于拟态系统的输入分发、策略调度和反馈控制。

无线内生安全架构的工作原理是利用无线信道作为执行体，在执行体上传输信息的同时，也将执行体构造与信息绑定。它的好处是合

法者可以借助执行体具有 DHR 特点和相对于第三方的“测不准”属性，使攻击者无法获得执行体构造的信息，也就无法针对该机制发起主动攻击或实施被动窃听。由此可见，无线内生安全架构虽然没有消除电磁波广播特性导致的暗功能，但是规避了其带来的不利影响。因此，无线内生安全架构与经典内生安全架构一样，可以用来对抗未知安全威胁。

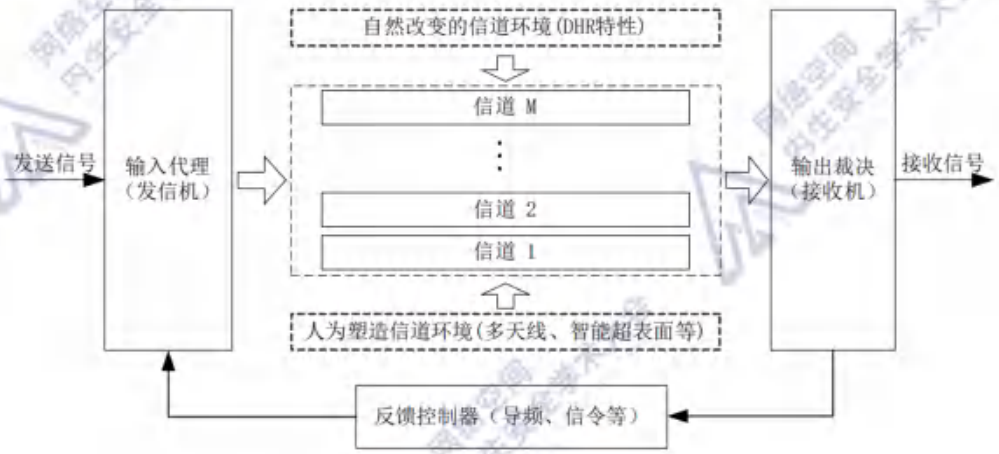


图 4 无线内生安全架构

以“构造加密”内生安全视角审视电磁空间，可以发现，电磁空间内生安全以无线信道作为执行体，通过重构无线信道实现构造加密，获得各点异性的差异性信道环境，也即，电磁空间与网络空间的执行体构造具有同态性。由此不难得出，网络空间通过“一次一重构”可实现完美安全，因此电磁空间也可能存在同样的方式以实现内生的完美安全。

### （四）实现完美安全的高自由度构造

#### 1. 无线内生安全的自由度

在物理学与工程学中，自由度是指能够独立对物理状态产生影响的变量的数量。这一概念在无线通信领域得到了进一步的深化和拓展，

形成了无线内生安全自由度的独特视角。**无线内生安全的自由度指的是内生安全构造的物理空间的维度，即内生安全系统可重构空间的大小。**它反映了无线通信系统可以主动调整的通信空间的独立参数个数，包括其分别对时域、频域、码域、空域等独立感知与操控的维度。通过在这些维度上的灵活调整与优化，内生安全系统能够实现对电磁空间的独立感知与操控，从而在物理层面构建出难以被攻破的安全屏障。内生安全自由度的大小直接决定了内生安全指标 $\varepsilon$，这一指标是衡量无线通信系统内生安全性能的重要量化标准。从自由度的角度来看，无线内生安全的本质在于通过提升物理空间的维度实现最优的构造加密，从而创设出一种基于物理复杂度而不限于计算复杂度的安全机制。

在众多自由度维度中，空域自由度以其独特的个性化特征和内生安全属性而备受瞩目。受通信环境与通信位置的影响，无线环境边界条件的不断变化会导致麦克斯韦方程解空间的改变，进而影响到系统的空域自由度。因此，与传统的时域、频域等公共资源不同，空域自由度直接关联于通信方的位置与无线环境的边界条件，这使得它成为了一种具有显著差异性和安全性的资源，成为决定通信系统内生安全能力的关键因素。无线通信系统的空域自由度由发送端自由度、环境自由度和接收端自由度共同组成，并最终取决于三者的最小值。从电磁环境和收发系统两个方向开展对无线内生安全空域自由度的重新挖掘、利用与塑造成为了提升无线通信系统内生安全能力的关键所在。

**2. 实现完美安全的自由度条件**

电磁空间对抗的第一性原理是系统自由度的比拼。在内生安全系统中，合法方想要利用自由度，构造自身与攻击方的差异性，从而产生内生安全效应。而对于攻击方而言，则是想要利用自由度，抵消自身与合法方的差异性，从而实现攻击。因此可以说，内生安全的强度取决于合法方与攻击方的自由度大小。在此背景下，无线攻防的范式本质上就是合法方与攻击方自由度的博弈，有效自由度较大的一方将占据优势地位，从而更有可能实现信息的安全传输。因此，对于内生安全系统而言，实现完美安全的条件就在于确保合法方自由度大于攻击方自由度。反之，当攻击方自由度大于合法方自由度时，则无法实现信息论意义上的完美安全。在这种情况下，合法方仅能设法提高攻击方攻击代价，实现基于计算复杂度的安全而非基于物理复杂度的安全。

然而，在实际应用中要实现完美安全的自由度条件并非易事。随着攻击技术的不断演进和升级，攻击方往往能够利用更为复杂的手段来抵消合法方的自由度优势。此时，合法方需要采取更为积极的应对策略来提升自身的自由度水平。例如，通过引入超大规模 MIMO 技术等先进技术手段来提升空域和空时频域的自由度；或者通过应用高频段大宽带等新型频谱资源来进一步增加系统的自由度资源。此外，还可以利用 RIS 来实现对无线环境的实时重构与动态可编程，从而在物理层面构建出更为复杂多变的通信链路以抵御攻击。

提高自由度是实现内生安全的关键，而利用高自由度实现高弹性和强韧性的通信系统则是内生安全的核心理念。其中强韧性指的是高

自由度张成的高维信号空间总能抵消低维干扰空间，保证系统即使在自由度降低的情况下，仍存在可用自由度以保持底线通信；高弹性指的是当干扰空间变化时，系统能够对可用的自由度进行动态重构，以逼近当前可达的最优性能，即当干扰消失时恢复到初始最优通信性能，当干扰存在时优化通信资源分配于可用自由度上，自由度利用率最高。面对恶性人为干扰、恶劣自然信道等外部因素压迫时，只有高自由度的无线通信系统才能具备强韧性和高弹性能力。当干扰方自由度大于等于通信自由度时，系统则失去了韧性和弹性。

此外，提高自由度不仅是实现内生安全的关键所在，更是推动通信与安全一体化发展的重要驱动力。高自由度的无线通信系统不仅能够具备更强的抗干扰能力和更高的数据传输速率，还能够通过动态重构自由度来应对各种复杂多变的安全威胁。这使得无线通信系统能够在保证通信效率的同时实现更高层次的安全保障。因此，自由度是通信与安全设计的公因子，高自由度既是通信的目标，也是安全的刚需。从自由度的角度实现内生于通信的安全，有可能实现真正意义下的通信安全一体化。

### 3. 信息超材料赋能内生安全自由度

在 6G 及未来通信技术的发展进程中，信息超材料以其独特的优势成为了提升内生安全自由度的创新利器，其能够通过智能调控电磁波的传播路径和相位分布来实现对无线环境的实时重构与动态编程，为内生安全系统逼近“一次一密”的完美安全理论目标提供了新的可能。

在传统无线通信系统中，无线信道通常被认为是不可控的。多种无线通信技术都是将无线信道作为不可改变的客观存在，通过调整收发信机来适应无线信道。因此，信息超材料技术对于无线信道的动态重构能力正是打破了无线环境与自然信道对于系统自由度的制约。此外，相比于传统天线系统而言，信息超材料天线或智能反射面能够逼近天线系统物理自由度的理论极限，并突破传统天线系统在工作频段、工作带宽、天线增益以及孔径效率等方面的瓶颈。它不仅能够提升系统的空域自由度水平，还能够通过优化射频前端的性能来提升对环境自由度的利用能力。这些优势使得信息超材料技术在提升无线通信系统内生安全自由度方面展现出了巨大的潜力与价值。

信息超材料辅助的无线内生安全系统的目标是充分利用电磁波域自由度差异对信息传输链路物理构造加密的效果，实现完美安全，或者说基于物理复杂度的安全，而不仅仅是基于计算复杂度的安全。无线通信系统自由度的物理极限取决于电磁环境和收发系统，因此提高自由度的核心在于改造电磁环境以提升自由度的操控能力，以及改造射频前端以优化对提升后自由度的利用能力。信息超材料可从电磁环境和收发系统两方面入手实现全域自由度的提升，表现为构建高自由度环境和高自由度天线两种形式，通过提高电磁环境和收发系统的自由度从而有效提升无线通信系统整体自由度。

由于信息超材料能够提供“无线环境可重构、无线信道可编程”的新质能力，可首先利用可重构智能表面弹性改变无线环境的约束条件，提升原有无线环境条件下自由度；其次，可利用敏捷可重构智能天线，

提升自由度的物理极限，逼近上述环境优化定制产生的自由度上限，构造人工信道拉大合法方与攻击方差异，实现基于“自然+人工”复合信道的构造，提升原有信道的动态性和随机性。此外，利用可操控的自由度，动态重构使期望位置与其它任意位置统计独立的人工信道，将自然信道的“有差异”放大到“全独立”，将无线内生安全属性——各点异性尽可能利用到极致，其最终达到的效应就是ε完美安全。因此，基于对传播条件的弹性改变，信息超材料技术能够提高原有无线环境条件下的自由度，使得无线通信系统在面对各种复杂多变的安全威胁时都能够保持高度的安全性和稳定性。

除了构建高自由度环境外，信息超材料技术还可以在收发系统中构建敏捷可重构智能天线以提升系统的自由度水平，利用智能超表面的“数字孪生”特性，可以实现电磁环境到天线编码空间信息熵的保熵映射，从而提高信道熵的物理极限。

综上所述，无线内生安全自由度作为衡量无线通信系统内生安全能力的重要指标之一，其重要性不言而喻。通过深入挖掘和利用空域自由度等关键资源以及引入RIS等先进技术手段，可以有效提升无线通信系统的内生安全自由度水平，从而实现更高层次的安全保障。

## 三、无线内生安全新技术

### （一）信息安全

#### 1. 抗截获

无线内生安全抗截获的技术研究目前可以分为两类，分别是无线内生密钥生成技术和无线内生安全传输技术。信息超材料用其特有的

定制和改造信道的能力，为传统的信息安全带来了新的技术突破，下面将简要介绍信息超材料辅助的两种抗截获模型。

### 1.1 信息超材料辅助的密钥生成

密钥生成技术将无线信道作为随机源提取密钥，其原理上利用了各点异性，使得攻击方无法通过无线环境感知、地理位置信息获取等方式抵消攻击信道与合法信道之间的差异，确保了合法方密钥的私密性。在此基础上，可通过信息超材料提升收、发或环境自由度，进一步放大信道差异性，同时提高无线通信容量和无线密钥生成速率，逼近“一次一密”完美保密的理论目标。

信息超材料相移优化一般以密钥生成速率最大化为目标，目前关于信息超材料辅助的物理层密钥生成技术的研究可以根据通信环境的不同分为两个方面：随机相移提升信道熵和优化相移提升信道相关性。信息超材料辅助的物理层密钥生成典型模型如图 5 所示。

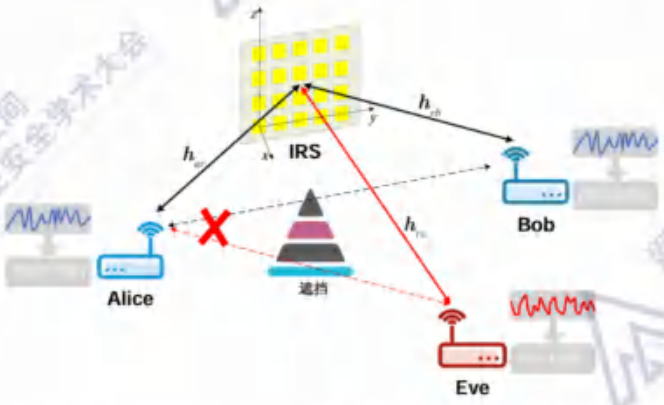


图 5 信息超材料辅助的物理层密钥生成典型模型示意图

随机相移提升信道熵：当通信环境处于静态和稀疏多径环境中，利用信息超材料在相干时间内快速切换相移扰动无线环境，从而引入人工随机性增大信道熵。该技术一般包含 3 个步骤：首先，信息超材

料根据某种概率分布随机选择反射系数。接着，合法双方互相发送导频，依次探测信道。在一次双向探测过程中，信息超材料反射系数保持不变。在下一次双向探测时，信息超材料切换反射系数。最后，合法双方根据获得的信道估计样本，从中提取密钥。

优化相移提升信道相关性：当通信环境在富散射或移动场中，可优化信息超材料系数提升信道相关性，从而增大密钥单次提取量。与随机信息超材料相移方案每探测一次信道切换一次信息超材料相移的方法不同，优化信息超材料相移辅助的密钥生成基于信道统计信息，如信道协方差矩阵。该协议一般包含 3 个步骤：基站首先探测获取统计信道信息。接着，基站以密钥速率最大化为目标配置信息超材料相移，并且在密钥提取过程中信息超材料相移不再改变，除非信道统计特征发生变化。最后，合法双方发送导频双向探测信道，从信道探测值中提取密钥。

### 1.2 信息超材料辅助的安全传输

安全传输技术可以利用信号的不可预测性和自由度（时域、频域、空域）设计复杂的信号传输方式，同时加入噪声干扰非法接收者。通过这项技术，合法用户能顺利接收信号，而攻击者难以窃听或解码信息，从而保障通信的隐私性和安全性。在此基础上，信息超材料辅助的安全传输技术通信系统能够主动调控多维空间自由度，使得攻击者更加难以预测或控制信号的传播，进一步强化安全保障。

信息超材料辅助的物理层安全传输典型模型如图 6 所示，具体而言，信息超材料辅助的物理层安全传输技术能够利用信息超材料对

波束的灵活操控性，实现信号传播方向调控及增强或消除，从而给目标接收机构造增强波束而对未知接收机构建抑制波束，构造出合法信道质量与窃听信道质量的差异构造私密信道，省去了复杂的加解密步骤，避免了密钥分发与管理环节。该技术具有轻量化、易实现和方案灵活等优点，尤其适用于物理资源受限设备的通信安全。

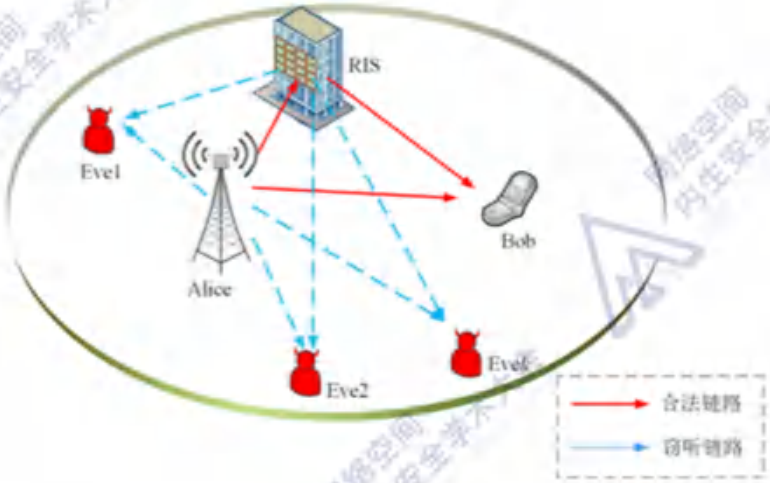


图 6 信息超材料辅助的物理层安全传输典型模型示意图

该技术旨在针对不同通信和窃听场景，可通过设计基站与 RIS 的联合波束赋形，建立并求解优化问题，对无线资源进行合理配置。相关优化问题主要涉及信号处理、资源分配和路径规划等方面。优化目标通常是安全速率、安全能量效率（Secure Energy Efficiency，SEE）、发射功率等性能指标。同时需要满足各种约束条件，例如发射功率约束、RIS 相移约束和用户 QoS 约束等。

**2. 认证**

认证的本质是通过可信根的对比鉴别用户身份的合法性和信息的完整性。目前应用最广泛的认证技术是基于现代密码学的高层认证技术。高层认证技术依赖于预先植入身份信息索引的根密钥作为可信

根和计算复杂度，通过认证算法完成可信根的对比。无线信道指纹的物理层安全认证利用无线信道的随机性、时空不一致性和各点异性实现认证。这种方法具有第三方无法重构的特点，安全性高，并且在认证复杂度及开销方面具有优势。通过提升信道的观测自由度，物理层安全认证能够进一步放大信道间差异性，从而增强认证的可靠性和效率，迅速成为信息安全领域的研究热点之一。

事实上，提取与物理位置强耦合的无线信道特征可以生成天然的认证可信根，实现基于无线信道密钥的无条件认证。无条件认证与计算安全认证相对应，建立在信息论基础之上，假设合法通信双方的认证可信根总是共享一部分私密熵，攻击者无法通过试错和计算能力消除这部分不确定度，因此可以实现一定强度的无条件认证安全。即使攻击者拥有无穷的计算能力，也可以实现一定强度的认证安全。进一步，为了减少共享私密熵产生的额外通信开销，利用无线信道密钥加密传统信道编码（如 CRC 校验码），实现通信-无条件认证一体化。

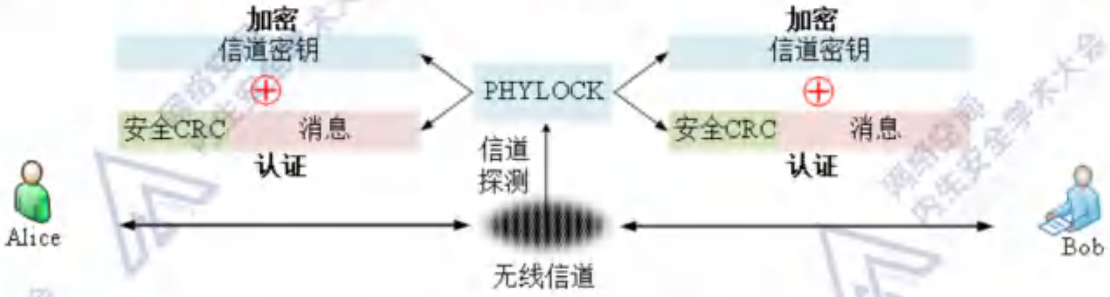


图 7 通信-无条件认证方案原理图

同时，无线信道指纹认证通过对通信双方的无线信道特征进行估计和提取，从无线信道的波形和信号层面实现认证功能，无需密钥分发和管理，协议交互简单，复杂度低。近年来，随着 RIS 赋能无线通信相关研究的兴起，进一步推进了物理层安全认证的发展。RIS 辅助

的物理层安全认证原理在于，利用 RIS 增强对电磁波传播特性的调控能力，从而在无线信道天然内生安全的基础上进行人为可控的优化与改造，以实现增强合法链路通信质量及安全保密容量，增加信道复杂冗余细粒度以定制利于认证检测的期望合法及非法信道特征的概率密度分布。具体来说，使用 RIS 减少或消除来自其他方向的干扰，增强合法用户之间的通信质量，结合认证方接收信号与混合 RIS 接收信号进行联合认证以实现对认证信道特征更精准的估计；同时，通过随机控制部分可控信道配置 RIS 相位分布来设计基于物理层安全的挑战-响应认证机制，以 RIS 相位随机配置作为挑战，预测信道作为预期响应，可以在非法者获取合法者完美信道分布的极端假设下依旧保证认证安全。

## （二）功能安全

### 1. 隐蔽通信

基于无线内生安全理论的隐蔽无线通信技术，从合法信道与非法信道天然存在的空域差异入手，研究面向隐蔽通信需求的能量空域打散机制，其原理上是利用无线环境的各点异性实现信号在私有空域资源上的传输。此外，可通过信息超材料精细化匹配多径信道，进一步放大合法方与窃听方之间的空域差异，在满足隐蔽性需求的条件下保证隐蔽通信的传输速率。

隐蔽无线通信是指通过信号处理技术、通信系统设计等在物理层降低无线信号的检测概率，实现信息的低检测概率或低拦截概率传输。传统的隐蔽通信实现方式包含猝发通信、扩频及跳频通信，其基本原

理是将信号能量在时间或频率上打散，增加非法用户的信号检测难度。然而，时频域资源都属于公共资源，当非法用户具备同等或强大能力时，比如获知跳时、扩频及跳频序列，或者采用盲检测技术手段，这些传统隐蔽通信方案的隐蔽效果将大打折扣。

本质上隐蔽无线通信所面临的无线安全问题是由电磁波的广播特性这一内生属性生成，因此，由其产生的一系列已知或未知的安全威胁均属于无线通信的内生安全问题。基于无线内生安全理论，无线信道天然具备各点异性，是通信双方与生俱来的私有空域资源，也是敌我双方始终具有的非对称性资源。通过利用合法信道与非法信道之间的天然空域差异，将信号能量在私有空域资源上打散，并基于信息超材料设计能够精细化利用多径信息的动态异构阵列，通过设计其多径预编码，对其感知的多径信道进行差异化的发送，实现精细化的多径匹配，不仅能够在敌方位置未知的情况下保证系统的隐蔽性能，还能确保隐蔽通信需求下的传输速率，实现高效的空域能量打散。

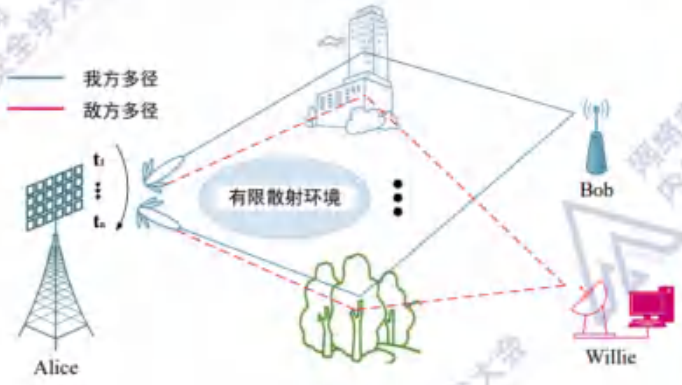


图 8 基于信息超材料的动态异构阵列精细化匹配多径

除了基于信息超材料设计动态异构阵列精细化匹配多径信道，挖掘无线信道内生安全属性，其具备的强大电磁调控特性也为隐蔽通信

开辟了新的实现思路。例如，利用 RIS 作为发送方将需要传递的信息映射为 RIS 阵面时变的相位响应，通过反射调制环境中已有无线信号相位的方式将信息加载在反射信号上，接收端通过检测反射信号相位的变化还原出信息，可以在不主动发射信号、不改变载体信息结构的情况下，以信号隐写的方式实现隐蔽通信。

**2. 抗干扰**

基于无线内生安全理论的空域抗干扰安全技术利用无线信道在空域中的各点异性，从干扰和信号在信道中天然存在的空域差异入手有利于实现针对性的干扰消除，挖掘新的抗干扰维度。此外，信息超材料可以通过其对无线环境重构能力提升有效自由度，为空域抗干扰安全技术注入无线内生安全特色方案。

无线通信中由于电磁波传播环境的开放性导致其面临着复杂且丰富的干扰因素、来源、样式，例如在趋于对抗的战场无线通信，各种压制式、欺骗式干扰攻击手段层出不穷，最终使得通信质量下降甚至产生通信中断，严重影响了系统的稳定正常运行。与此同时，来自系统内或系统外发送端的非恶意干扰信号以及环境干扰也会给通信系统带来无法预料的外部扰动，导致通信系统产生异常甚至瘫痪，给信息的安全传输带来严峻挑战。因此，抗干扰技术也随着无线通信系统的发展而愈发受到重视。由于信号和干扰的差异在不同的变换域中都有体现，所以当前的无线通信抗干扰技术在时、频、码域都有相应技术，但基于时、频、码域的抗干扰技术往往都需要消耗相应的资源，因此会一定程度上影响通信的性能，导致抗干扰技术的发展空间非常

有限。

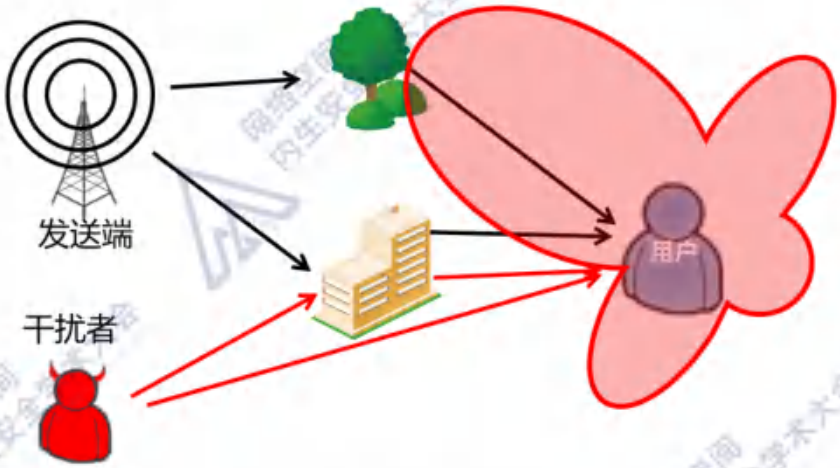


图 9 空域抗干扰原理图

实际上，无线信道的产生机理决定了其在空域具有异构性，因此可以利用各方空域信道的这种内生差异性进一步挖掘新的抗干扰维度。由于无线信道的独立性，不同位置发送的信号经过不同的传输路径，最终呈现出不同的信道特征，有利于对干扰进行针对性地解决。如上图所示，利用信号传输固有的空间差异性和信息超材料的接收天线可重构特性，形成接收方向图零陷和主瓣分别对准干扰和信号来削弱干扰信号、增强合法信号，为收发双方通信建立最优通路，在增强合法用户通信质量的同时阻断干扰信号注入，划定无线环境中的“干扰禁区”。另外，利用信息超材料的无线信道可编程特性实现信道的精细化管理与利用，通过空域信道的选择与重构打造具有内生专属特性的私有传输管道，探索新一代抗干扰通信的技术机理和工程实现方法，开辟一个从本源上就利于合法方抗干扰强鲁棒通信的“新战场”。

### 3. 抗衰落

基于无线内生安全理论的抗衰落安全技术，从多径在空域中的差

异性入手，通过提高观测的自由度来对不同多径进行差异化感知接收，最大程度地保真恢复获取多径信道，充分利用无线信道的内生安全属性，恢复系统的本征安全能力。

由于无线通信开放的电磁传播环境通常较为复杂，各种障碍物、散射体等的存在会产生多径效应，每条路径在传播过程中经历的无线信道环境不同，产生的信道复增益与到达角不同，天然存在内生差异性。但现有典型接收阵列中采用的均为同构天线，即天线的方向图形状、指向均相同，这使得在阵列的任一天线上，多径信号均以相同的方式进行观测感知，使得本质上差异化的多径信号通过射频前端阵列天线的加权叠加处理，丧失了信道特征中的多径信息，从而产生了多径衰落，这给无线通信的功能安全带来了严峻挑战。

基于无线信道的内生安全属性，研究探索无线内生抗衰落通信技术为高可靠强鲁棒的无线通信提供了新的技术思路。其中，最大程度地保真恢复获取多径信道的天然差异化特征是实现无线内生抗衰落通信的关键，这就要求必须在射频模拟前端天线处完成信号处理，如下图所示，可通过动态改变天线观测函数（即异构天线方向图）对多径信道进行多维度感知，在进入射频通道前使得每个阵元上采用差异化的加权叠加方式，从而利用多维度观测方式恢复出多径信道的方向、相位等信息，实现对多径信息的精细化辨识。在此基础上，通过调整不同径的相位实现多径信号的同相匹配接收，从而抵消多径衰落，提升无线通信的可靠性和鲁棒性。

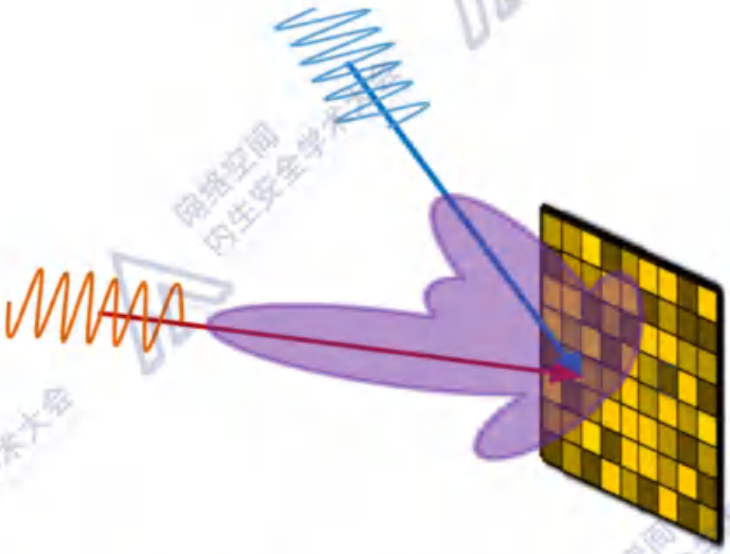

图 10 天线匹配接收多径信号

信息超材料赋能的空时异构阵列与传统的微带线馈电阵列天线相比，将多个超材料阵元集成在一个天线上，并且共同使用一个波导作为馈源，使得阵列结构更加紧凑，更好的满足复杂系统和多任务的工作需求。与经典 MIMO 系统相比，针对多径信道，能够利用空域、时域二维异构，调控天线的口面分布，进而提高有效自由度。此外，空间异构增大了不同天线处多径信道和的差异，令有效自由度始终与阵列自由度相同，而时间异构令每根天线等效为多天线阵列，进一步增大有效自由度。

## 四、无线内生安全原型系统与原理验证

本章介绍了 5 个典型的无线内生安全原型系统，在利用 RIS 提升空域自由度、挖掘无线信道各点异性的基础上，开展了对无线内生安全抗截获、抗干扰等多个关键技术的原理验证并探讨了安全效果。

### （一） 基于 RIS 的无线高速密钥生成与加密系统

RIS 辅助的无线高速密钥生成与加密系统面向战场环境等高等

级安全需求场景，针对根密钥安全的生成、分发与更新难等问题，利用无线密钥生成技术，为无线网络提供物理层安全防线。系统总体架构如图 11 所示。


图 11 RIS 辅助的无线高速密钥生成与加密系统总体架构

系统包含车载式电台、单兵电台以及 RIS 单元，其中车载式电台包含 NI 机箱（NI PXIe-1092）、USRP 无线收发机及上位机软件；单兵电台包含 PC 主机、USRP 无线收发机及上位机软件；RIS 单元包含 RIS 模块、RIS 控制模块。系统工作流程如图 12 所示。军用电台利用提出的 RIS 赋能的高速密钥生成算法，计算接收信噪比最大时 RIS 码字，将该码字用于后续密钥提取算法；根据相移随机化算法，RIS 单元随机切换 RIS 码字，在最大比合并接收的同时，对多径信道的相位进行随机化加扰，增大密钥源随机性，实现密钥速率的提升；合法通信双方在相干时间内发送导频信号，探测无线信道，获取信道特征观测值；合法通信双方采用多比特差分量化方法对无线信道特征值进行量化，获得初始密钥；合法通信双方通过公共通道上的信息交

换完成不一致密钥位的验证，获得一致的密钥位；合法双方使用通用哈希函数从较长的输入流中获得固定大小的长度输出，确保 Eve 无法获得有关密钥的任何信息；利用跨层动态链式密钥加密算法对需要传递的信息进行加密，确保实现无差错的安全传输。


图 12 系统流程图

RIS 辅助的无线高速密钥生成与加密系统通过外场测试，验证密钥生成技术带来的增益，以及面对各种窃听攻击时系统的安全性。如图 13 所示，系统包含了 1 个单兵电台，1 个窃听电台，1 个车载式电台以及一块 RIS 单元。采用喇叭天线、USRP 和上位机软件搭建了单兵电台和窃听电台。利用喇叭天线，NI 机箱、USRP 无线收发机和

上位机软件模拟了车载式电台，RIS 部署在天线附近。


图 13 测试场景

为解决根密钥失效后的信息泄露问题，采用物理层密钥来替换根密钥，分析启用物理层密钥前后的安全效果。合法者可以通过实时切换 RIS，解决传统加密方式存在的安全问题，增加密钥破解难度。在测试中，两合法者 Alice、Bob 间距离大约 10 米。在距离 Bob 的 5 米处放置被动窃听者 Eve，其不会主动发送无线信号。Eve 在测试中仅被动接收 Alice 和 Bob 间交互的密钥生成信令，并以测量 Bob 处的无线信道作为其物理层密钥生成的基准，如图 14 所示。


图 14 抗攻击测试场景

由图 15 可知，合法者 Alice 和 Bob 处的信道曲线十分相似，而窃听者 Eve 处的信道曲线与二者相差较大，因此 Alice 与 Bob 具有一致密钥、Eve 与二者具有不同密钥，从而实现基于空间位置差异的安全隔离。本系统通过融合物理层安全技术和密码学方法，利用 RIS 对无线环境实时重构的调控能力实现信道密钥的高速分发和动态更新，在传统信息层面安全防护手段的基础上，增加了无线网络的物理层安全防线，提高信息安全防护等级，消除无线军事无线通信网络等高安全等级网络的安全痼疾。

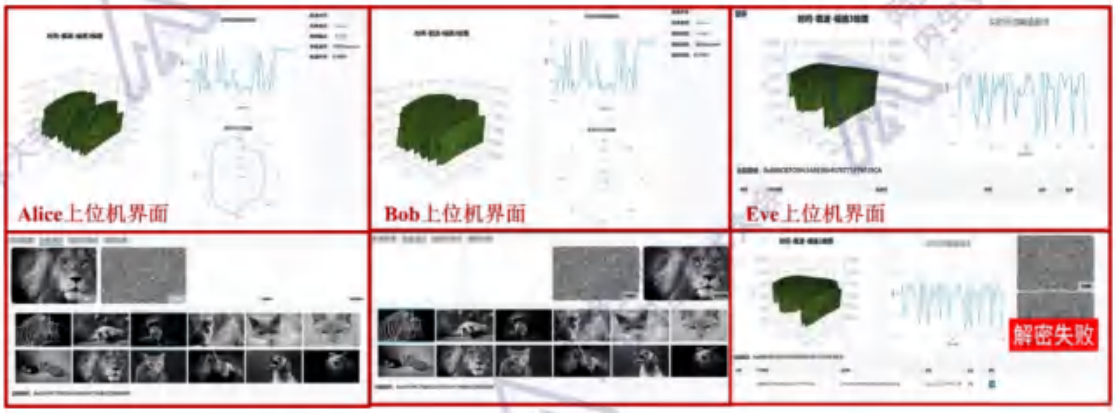


图 15 物理层密钥测试效果

## （二） 基于 RIS 的 5G 内生安全小基站认证系统

基于 RIS 的 5G 内生安全小基站认证系统，利用商用核心网、商用终端和 5G 内生安全小基站搭建环境进行测试，可在 5G 空中接口的信号层面对终端身份认证，抵御攻击者实施身份假冒、信息篡改等典型无线接入攻击，在 3GPP 安全标准技术上实现了不依赖但可融合于传统密码认证体制的内生安全功能。本原型系统对系统的认证功能、认证成功率和认证安全间隔进行测试，原型系统如图 16 所示。

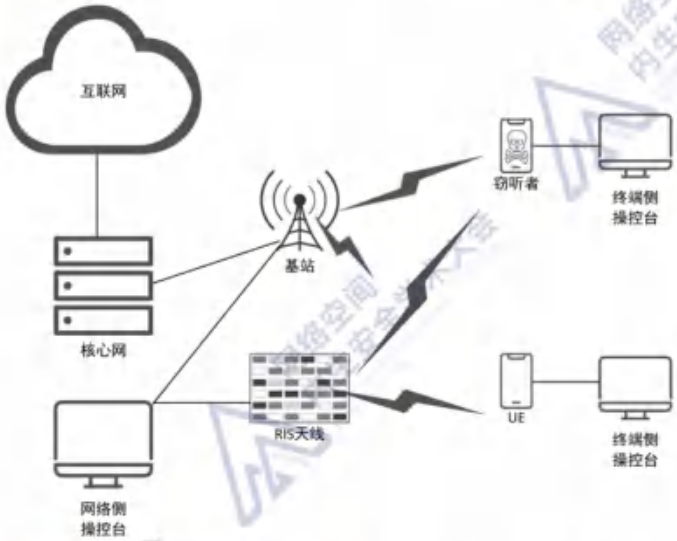


图 16 基于超材料智能表面的无线内生安全原型系统

图 17 整体测试环境

按照图 17 搭建测试环境，将核心网、基站、终端与对应的操控台连接，保持连接状态正常，将 2 个相同型号的 5G 终端标记为 A

和 B。认证成功率测试是统计基站侧能够正确识别非法终端身份的成功率。测试流程如下：（1）启动核心网、基站及网络侧操控软件，确保核心网和基站处于正常工作的状态；（2）在基站端的操控软件上打开终端侧认证功能；（3）启动终端 A 和终端侧操控软件，确保终端完成开机附着流程，然后在终端操控台上进行上网拨号，确保操控台可通过终端连接网络；（4）在终端侧操控台上通过浏览网页等方式，触发终端与基站不断地进行无线通信；（5）启动终端 B 和终端侧操控软件，确保终端完成开机附着流程，然后在终端操控台上进行上网拨号，确保操控台可通过终端连接网络；（6）观察在基站侧的操控台上是否对终端 B 的驻留发出告警，同时终端 B 无法驻留于网络中;（7）重复步骤 3~6 20 次；（8）统计基站侧操控台发出告警且终端 B 无法驻留于网络中的次数为 s，计算认证成功率 s/20 * 100%，确认认证成功率是否不小于 90%。测试结果表明，测试认证成功率可达 100%。

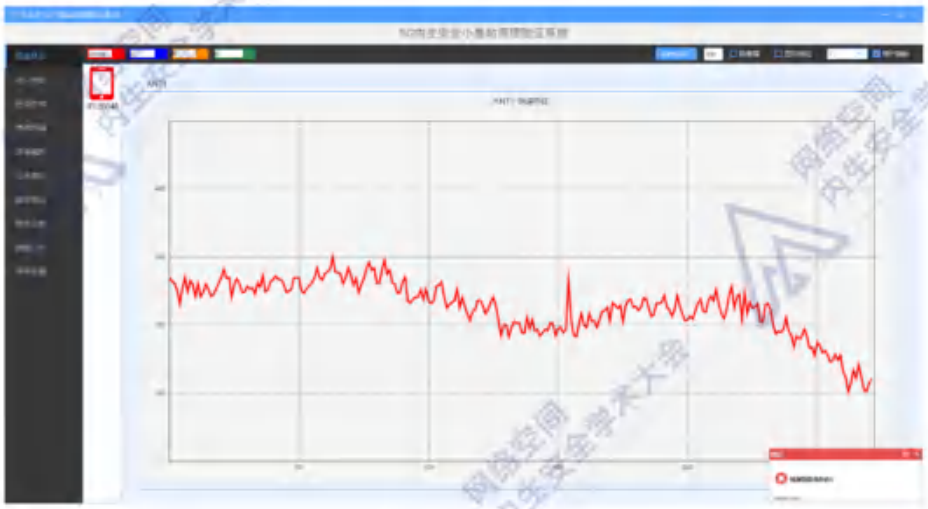

图 18 基站告警界面

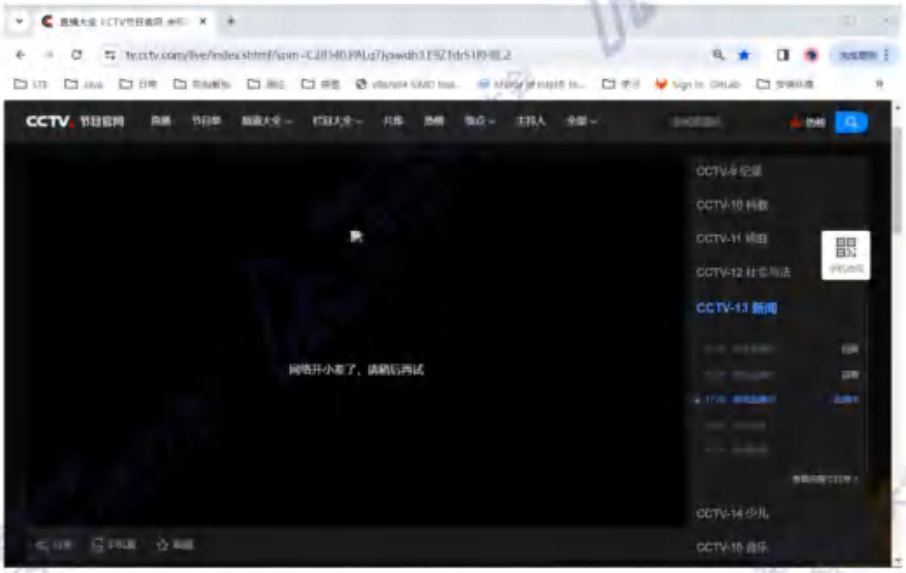


图 19 终端 B 无法驻留网络并访问网页界面

认证安全间隔测试是在合法终端与非法终端之间的距离小于 10 米的条件下，测试基站是否能够正确识别非法终端的身份。测试流程如下：（1）启动核心网、基站及网络侧操控软件，确保核心网和基站处于正常工作的状态；（2）在基站端的操控软件上打开终端侧认证功能；（3）选择终端 B 在终端 A 距离 2 米的任意位置；（4）启动终端 A 和终端侧操控软件，确保终端完成开机附着流程，然后在终端操控台上进行上网拨号，确保操控台可通过终端连接网络；（5）在终端侧操控台上通过浏览网页等方式，触发终端与基站不断地进行无线通信；（6）启动终端 B 和终端侧操控软件，确保终端完成开机附着流程，然后在终端操控台上进行上网拨号，确保操控台可通过终端连接网络；（7）观察在基站侧的操控台上是否对终端 B 的驻留发出告警，同时终端 B 无法驻留于网络中；（8）重复步骤（3）~（6）20 次；（9）统计基站侧操控台发出告警且终端 B 无法驻留于网络中的次数为 s，计算认证成功率 s/20 * 100%，确认认证成功率是否

不小于 90%。（10）逐步递减终端 B 与终端 A 之间的距离，每次减小 0.5 米（距离 0 的模拟方式是通过功分器将终端 A 和终端 B 连接至同一根天线），重复步骤 （4）~（9），直至认证成功率小于 90%为止，将前一次满足成功率要求的终端 A 和终端 B 之间的距离记为认证安全间隔，确认认证安全间隔是否优于 10 米。测试结果表示终端间隔 2m、1.5m、1m、0.5m 时认证成功率都是 100%，终端间隔 0m 时认证成功率是 25%。

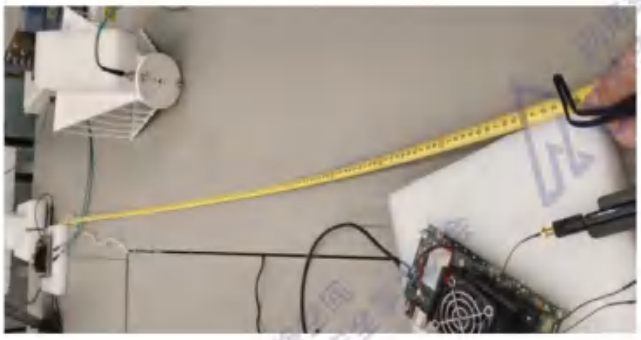

图 20 终端间隔 2m

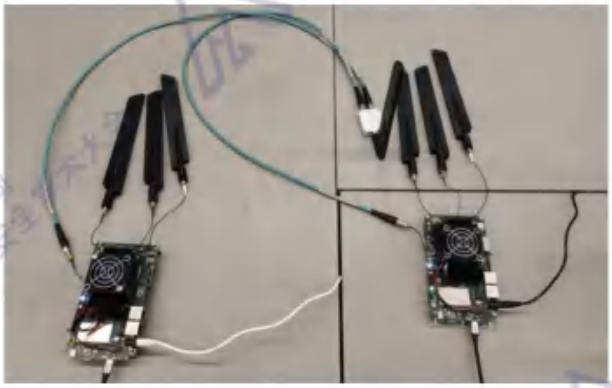

图 21 终端间隔 0m

5G 小基站从无线信道中提取终端信道指纹，用户身份与信道绑定，可感知并抵御其它时空坐标上发起的无线接入攻击。与密码算法融合，可实现低开销、高吞吐量的数据完整性保护。

## （三） 基于 RIS 的信号隐写与安全传输系统

基于 RIS 的信号隐写与安全传输系统，通过利用 RIS 的反向散射与方向调制技术，实现了在不主动发射无线信号的前提下，私密信息的隐蔽与安全传输。系统总体架构如图 22 所示。

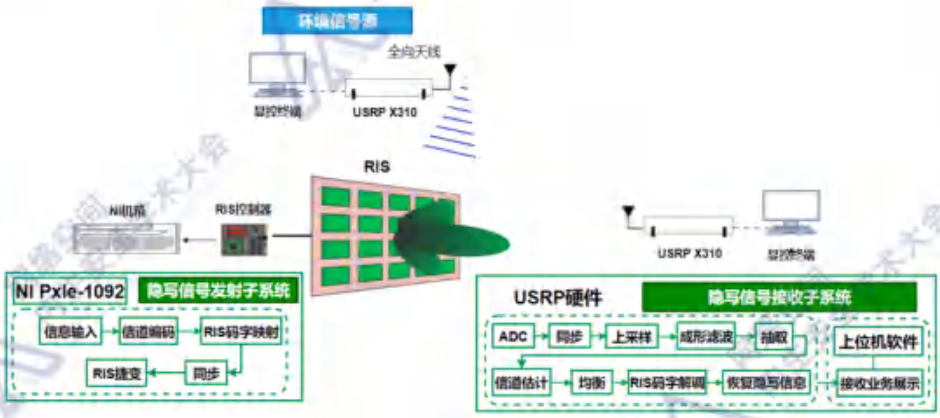


图 22 基于 RIS 的信号隐写与安全传输系统架构

系统中主要包含隐写信号发射子系统与接收子系统。其中隐写信号发射子系统由 RIS 及其控制设备共同构成，主要实现了有用信息的信息编码以及 RIS 阵面码字映射，同时控制 RIS 捷变使得信息比特流得以依次发送。隐写信号接收子系统用于解调接收隐写信号，恢复被隐写在环境信号中的私密信息。

系统的工作流程如图 23 所示。隐写发射子系统首先将待传输的数据信息嵌入如图 24 所示的隐写信息帧中。随后发端依据方向调制原理，选择适当的 RIS 相位码字，以确保反射信号仅可被合法接收端正确解调。进一步，发端将帧比特流映射为 RIS 相位码字，并控制 RIS 按照码字时序依次捷变。当环境中的无线信号到达 RIS 阵面时，该信号被 RIS 反射的同时将叠加此时刻阵面上加载的相位。当反射信号抵达隐写接收子系统后，接收设备首先进行信号解调，随后通过捕捉信号的相位变化，恢复出由 RIS 隐写的数据比特流，最后经处理后解码

出隐写信息。

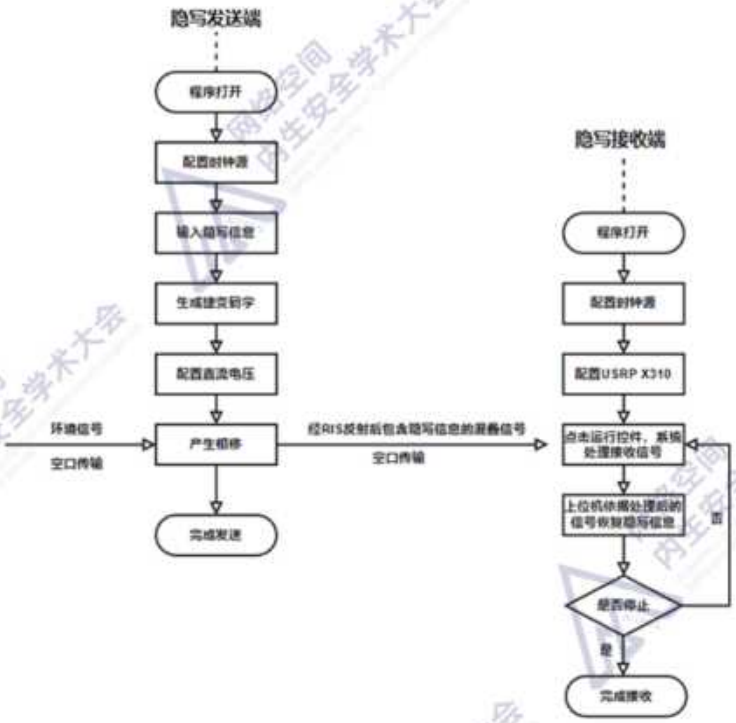


图 23 基于 RIS 的信号隐写与安全传输系统工作流程

| 同步帧头 (62bit) | 特征信息 (10bit) | 数据信息(256bit) | CRC校验值 (64bit) |
|---|---|---|---|

图 24 隐写信息帧格式

基于 RIS 的信号隐写与安全传输系统通过外场测试（如图 25，图 26 所示），验证了其在信号层面实现信息隐蔽、安全传输的能力，拓展了信息隐写的新维度，具有强隐蔽，易部署，低能耗的特点，能够切实满足情报回传，战场指挥等场景下的无线通信功能安全需求。


图 25 信号隐写功能测试

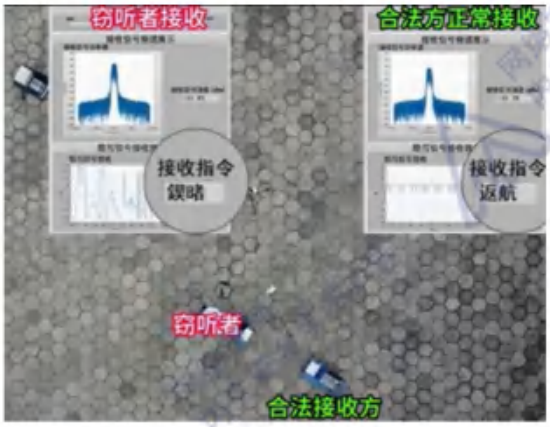


图 26 安全传输功能测试

## （四） 基于 RIS 天线的射频前端抗干扰系统

基于 RIS 天线的射频前端抗干扰系统利用超材料的敏捷可重构特性制备实时可重构 RIS 天线，解决复杂电磁环境下天线口面域模拟处理能力的有无问题，在无线最前端实现抗干扰和匹配滤波。基于 RIS 天线的射频前端抗干扰系统总体架构如图 27 所示。

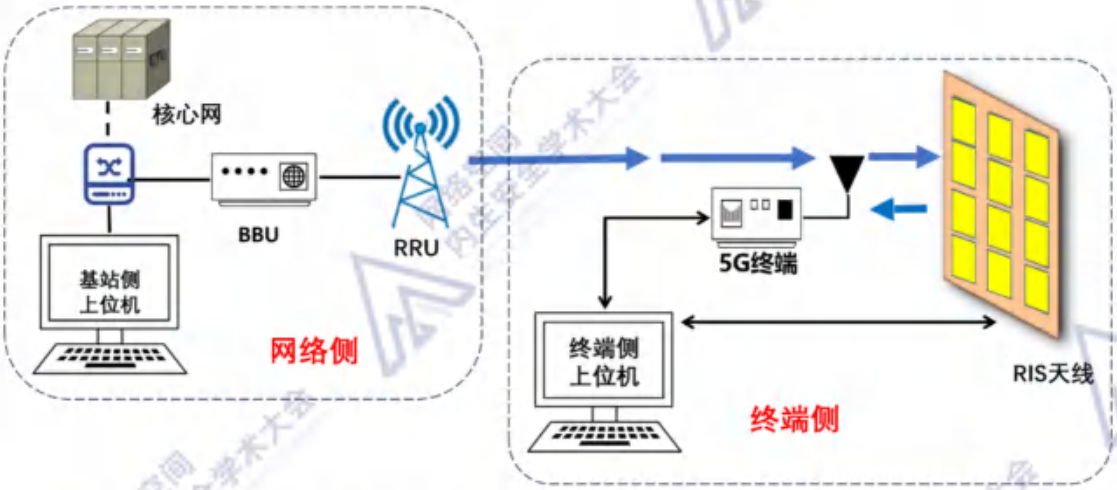


图 27 基于 RIS 天线的射频前端抗干扰系统总体架构

系统包含网络侧和终端侧两个部分，网络侧包括 5G 小基站远端射频单元（Remote Radio Unit, RRU）、基带处理单元（Building Baseband Unit, BBU）、上位机和核心网等，完成 5G 基站侧信号处理、空口协议处理以及核心网各网元功能。终端侧包括商用 5G 终端、RIS 天线和上位机等，完成 5G 终端侧信号处理以及空口和高层协议处理，5G 终端接收来自 RIS 天线的反射信号并测量信号质量，终端侧上位机通过 5G 终端接入 5G 网络从而访问互联网。网络侧和终端侧的软硬件组成如图 28 所示。

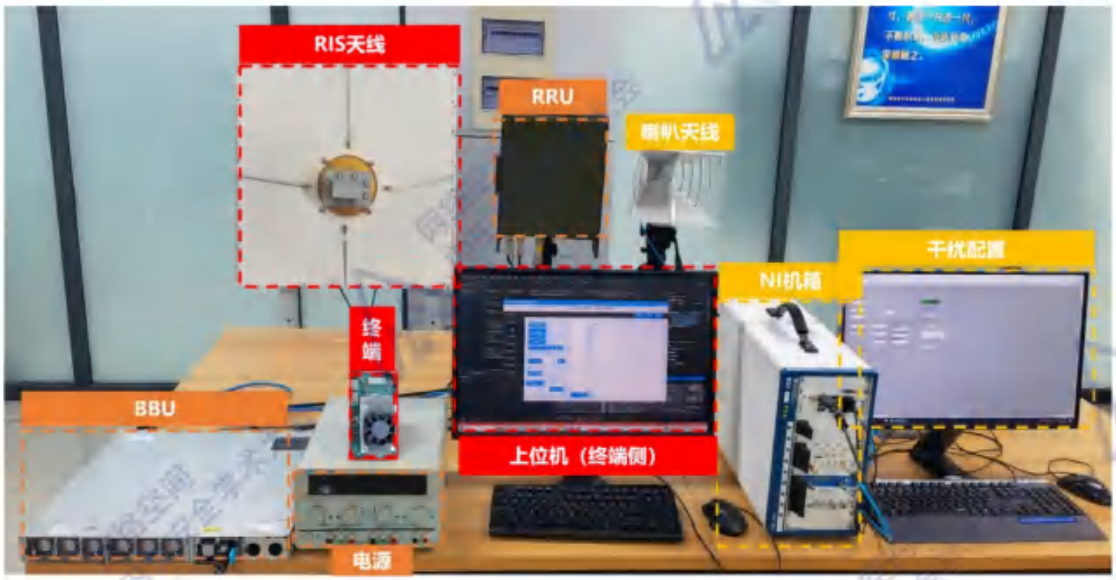


图 28 基于 RIS 天线的射频前端抗干扰系统软硬件组成

系统工作时，网络侧的所有网元始终处于正常工作状态。终端侧的所有设备上电正常工作后，5G 终端首先扫描环境中的 5G 信号并尝试接入 5G 网络，同时实时计算接收参考信号接收质量（SS Reference Signal Receiving Quality, SS-RSRQ），之后终端侧 SS-RSRQ 值通过 AT 指令接口传输到上位机，上位机通过反馈值迭代粒子群，快速优化 RIS 天线的编码状态，并通过网口回传至 RIS 天线口面。整个流程基于动态反馈迭代编码机制，拟合到达天线口面的电磁场，从而在射频前端实现实时抗干扰。以最大化 SS-RSRQ 值为目标，不断重复这个过程直到判断信道质量指标满足终端正常上网需求。具体工作流程如图 29 所示。

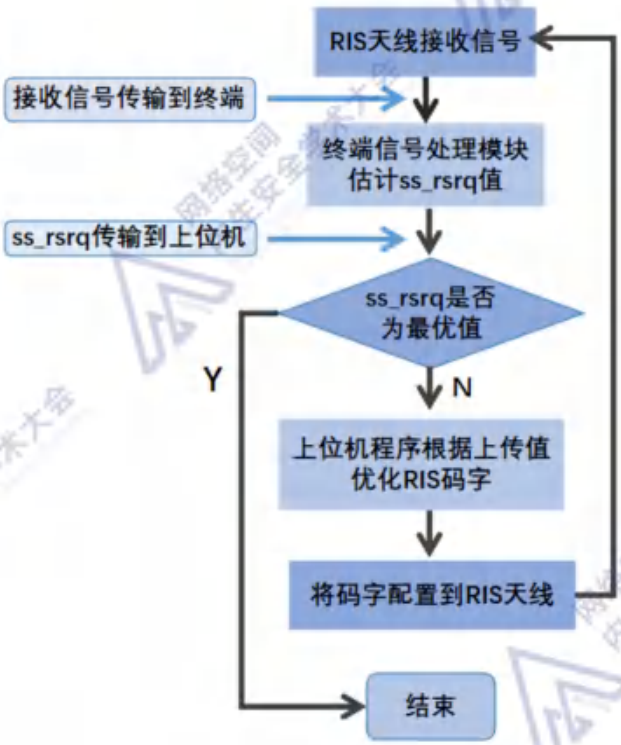


图 29 基于 RIS 天线的射频前端抗干扰系统工作流程

基于 RIS 天线的射频前端抗干扰系统（如图 30 所示）通过在室内散射多径条件下搭建测试环境，引入的干扰源产生干扰信号，其发射频率、带宽以及干扰信号方向与基站信号完全一致，也就是干扰信号与有用信号“三同”，即同时同频同向。实验在同时同频同向干扰的环境中也能保证 5G 通信质量，直播视频可以流畅播放，测试效果如图 31 所示，可以看出一旦 RIS 重新加电并加载优化码字，SS-RSRQ 值迅速回升，随着 SS-RSRQ 值上升到一定水平，网络传输效率得到恢复，终端侧的网页直播播放恢复正常，无卡顿现象，直观反映了终端侧通信体验的显著提升，验证了在恶劣干扰情况存在时抗干扰的可靠性。


图 30 基于 RIS 天线的射频前端抗干扰系统外场测试

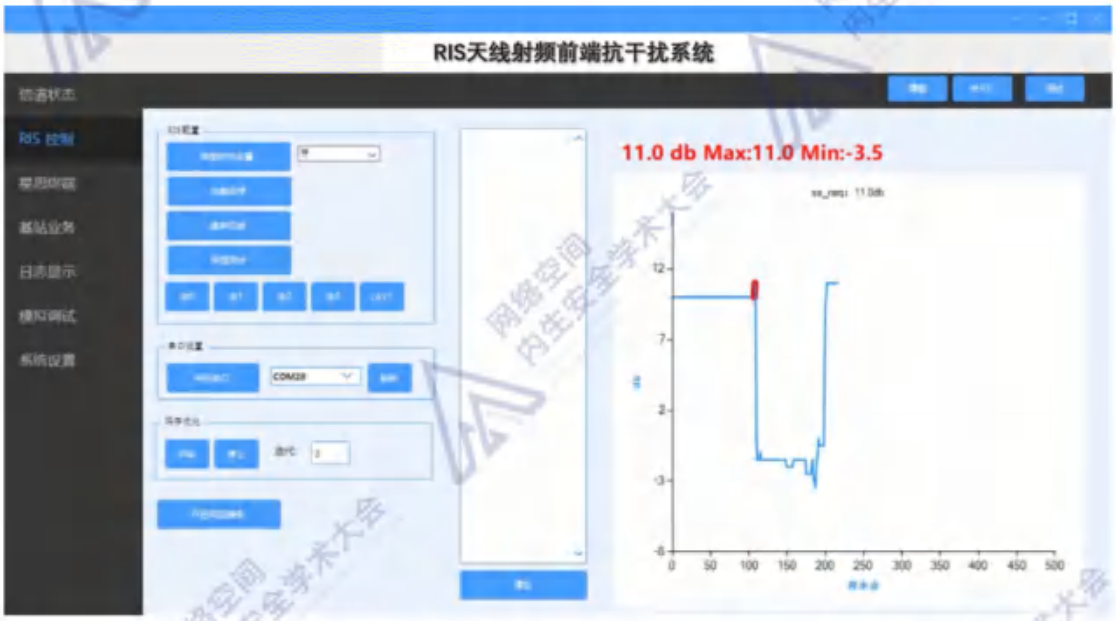


图 31 基于 RIS 天线的射频前端抗干扰系统测试效果

本系统为无线通信抗干扰提供了一套基于新材料、新技术、新理念的高性能、高可用、自主可控的创新解决方案，在军事和民用领域具有广阔应用前景。

## （五） 基于 RIS 的无线内生抗衰落通信系统

无线内生抗衰落通信系统在多径深衰落测试环境中成功验证了其有效性。无线内生抗衰落通信系统主要包括：视频信号产生、调制

与发送设备、视频信号接收、解调与测算设备和可重构智能反射面控制设备。总体架构如图 32 所示。

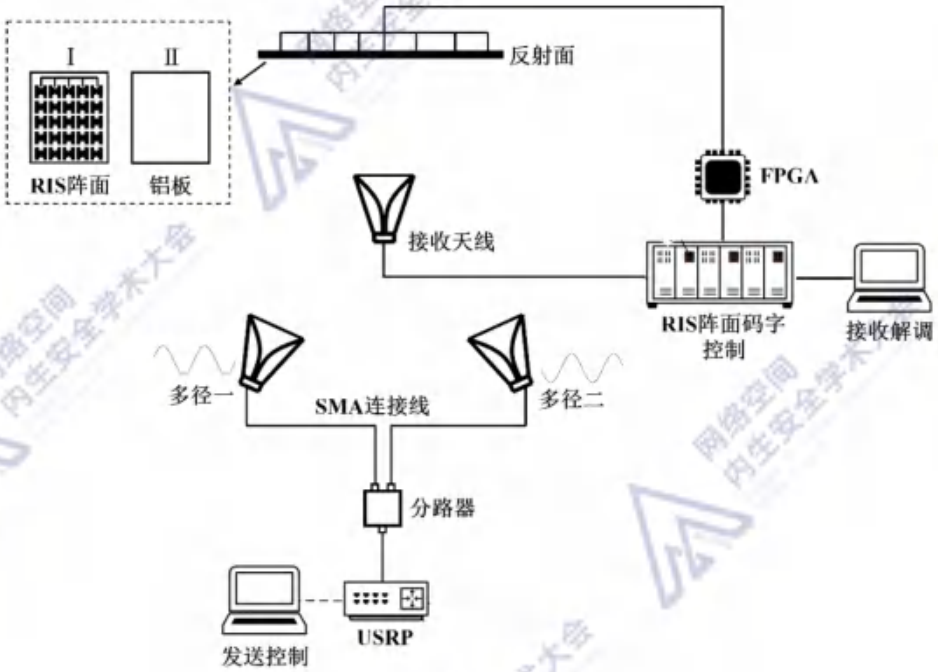


图 32 无线内生抗衰落通信系统总体架构

为便于减少设备复杂度，缩小运算时间，将视频信号接收解调与测算设备和可重构智能反射面控制设备集成在同一设备中。系统的各个模块如图 33 所示。


图 33 无线内生抗衰落通信系统硬件图

系统工作流程如图 34 所示。基于可重构智能反射面的无线内生抗衰落通信系统可以分为两个部分，分别为信号产生与发送控制部分和信号接收解调与 RIS 阵面码字控制部分。

在信号产生与发送控制端部分，PC 设备将视频信号编码，并利用 USRP 产生发送信号输出至分路器和衰减器，然后将两路信号传输至辐射天线，模拟一路用户视频信号产生两路多径干扰信号的通信过程。通过调整两个辐射天线的位置和角度确保两路多径干扰信号到达接收天线时的强度相等且相位相反，模拟深度衰落通信环境，对 RIS 阵面效能进行验证评估。

在信号接收解调与 RIS 阵面码字控制部分，通过接收天线对两径衰落信号进行接收解调并测定接收信号信噪比，然后通过 RIS 阵面码字控制程序修改 RIS 阵面码字配置，传输至 FPGA 电路产生控制信号，对 RIS 阵面状态进行实时调控，重新测定接收信号信噪比。重复迭代上述“码字配置—接收与信噪比测量—更新阵面码字配置”的循环过程，直至所有 RIS 阵面码字状态遍历完成，自适应选择当前通信环境下的最佳码字组合对 RIS 阵面进行配置，动态感知信道状态，提升接收信号强度，实现深度衰落信号的最佳接收。

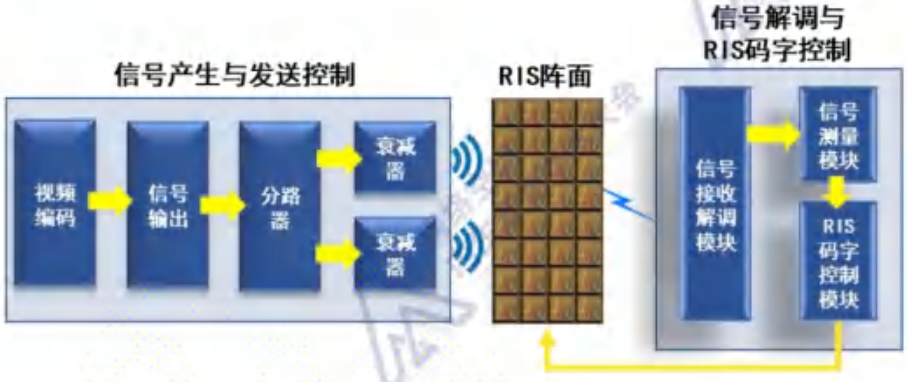

图 34 无线内生抗衰落通信系统工作流程

无线内生抗衰落通信系统总体架构通过实验场景测试（如图 35 所示），验证了抗衰落的能力。通过搭建微波暗室并在低环境噪声干扰条件下，采用无线通信链路的方式发送两路相位相反信号以模拟多径深衰落通信环境，通过接收天线观察接收信号强度和星座图情况。

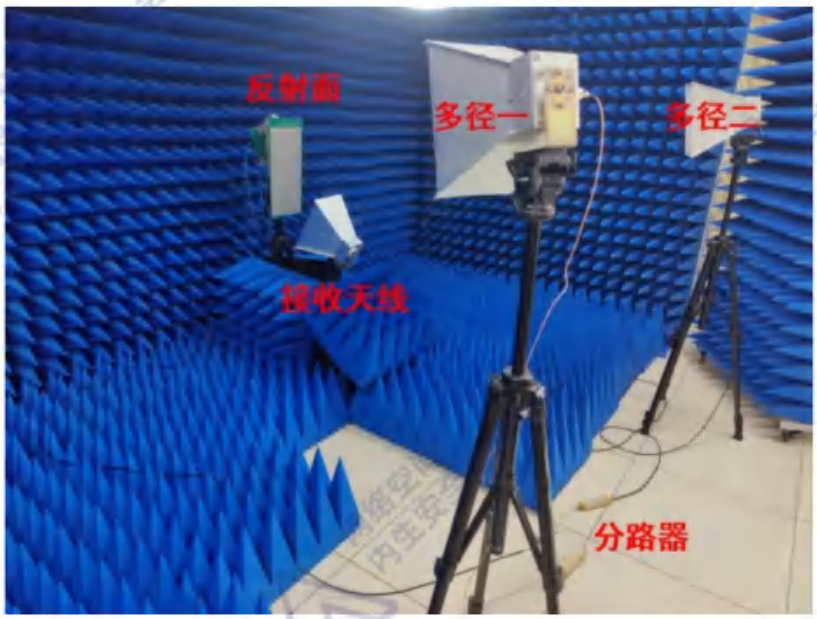


图 35 无线内生抗衰落通信系统测试

相较于一般反射面的情况下，基于可重构智能反射面的无线内生抗衰落通信系统能够将接收信号强度提升 20dB 左右，同时提升星座图质量与视频业务接收解调质量，系统测试效果如图 36 所示。

| 试验次数 | 普通反射面 | | | | 可重构智能反射面 | |
|---|---|---|---|---|---|---|
| | 多径I<br>信号强度（dBm） | 多径II<br>信号强度（dBm） | 无遮挡接收<br>信号强度（dBm） | 视频解调情况 | 无遮挡接收<br>信号强度（dBm） | 视频解调情况 |
| 第一次 | -79.62 | -79.09 | -94.50 | 卡顿 | -73.35 | 流畅 |
| 第二次 | -78.85 | -78.01 | -93.32 | 卡顿 | -72.94 | 流畅 |
| 第三次 | -76.53 | -76.44 | -92.58 | 卡顿 | -71.90 | 流畅 |
| 第四次 | -77.92 | -76.75 | -90.44 | 卡顿 | -72.32 | 流畅 |
| 第五次 | -79.58 | -79.93 | -94.63 | 卡顿 | -74.17 | 流畅 |

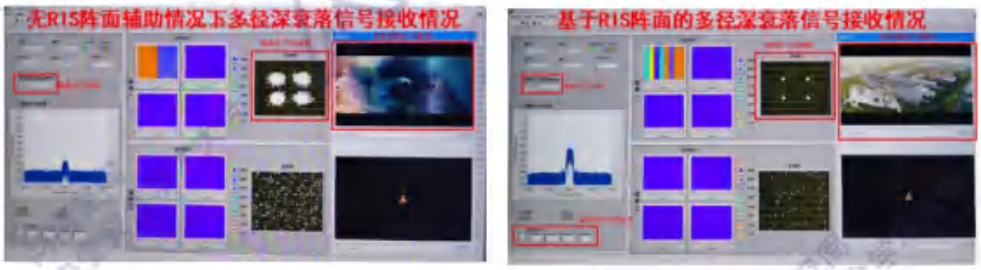


图 36 无线内生抗衰落通信系统测试

## 五、无线内生安全的应用展望

2023 年 6 月 ITU 发布的建议书中提出了 6G 的典型场景，并认为安全、隐私和弹性是适用于 6G 所有应用场景的四个设计原则之一。军事无线通信系统具有抗截获、高弹性和强韧性能力需求，面对战场强干扰阻塞/拒止攻击手段，保证基本的通信生存能力，即在电磁空间对抗中具备无线通信的高弹性和强韧性至关重要。无线内生安全是实现 6G 安全性和军事无线通信高弹性和强韧性的关键技术。下面给出无线内生安全在 6G 和军事无线通信中的应用展望。

### （一）6G

6G 的典型场景包含沉浸式通信、超大规模连接、极高可靠低时延、通感一体化、泛在连接等，其中，沉浸式通信、超大规模连接、极高可靠低时延分别是对 5G 的增强型移动宽带（eMBB）、大规模机器类型通信（mMTC）、超可靠和低延迟通信（uRLLC）的扩展。超高吞吐量是实现沉浸式通信的关键，空天地一体化是实现泛在连接

场景无缝覆盖的关键。

针对超高吞吐量场景中存在信息被假冒、篡改以及通信信号被截获等典型无线主被动攻击问题，需要设计可融合但不依赖于传统密码的安全机制，有效应对传统加密和完整性保护机制中计算资源开销大、能效低的问题。基于无线内生安全理念，利用无线信道的内生属性，无需占用大量通信资源，能够实现超高速数据加密、认证和信号安全传输。另外，可利用 6G 潜在关键技术具有的内生安全属性来进一步提升无线内生安全性能，同时满足 6G 宽带通信场景高吞吐量和安全需求，从而实现通信安全一体化设计，在信号层面增强高速数据流的加密和完整性保护能力。

在 6G 超大规模连接场景中，海量资源受限的终端需接入网络，为大规模恶意终端提供了巨大攻击入口，采用传统安全手段将面临巨大挑战。具体而言，传统加密、认证协议在网络侧存在伪造仿冒/DDoS 攻击、海量密钥分发管理难、以及大量设备并发请求产生巨大安全开销等问题，在终端侧存在复杂度高、安全强度不足等问题，对安全防御提出更大挑战。基于无线内生安全理念，采用基于信道特征的密钥生成/分发方案，可大大降低密钥分发管理开销，实现轻量级加密和认证。对于资源受限的终端，采用不依赖于计算复杂度的内生安全机制可降低对于终端能耗和处理能力的要求，同时获得安全性和轻量级。

针对 6G 车联网、远程医疗等要求接近零时延和极高可靠通信场景，这些应用的安全性需求也同样严苛。传统安全手段在终端和网络侧均需要经过高层协议，这种跨协议层跨物理域的实现方式使得信息

安全传输/处理时延大、传输效率低。同时，现有认证机制依赖外挂式安全字段，降低了传输效率，增加了传输时延，使得时延敏感场景下低时延与高安全的矛盾更加突出。针对以上问题，基于无线内生安全理念，可通过在无线链路侧物理层直接处理，且采用无外挂字段的加密或认证方式实现极高可靠低时延安全通信。

通信感知一体化网络中存在大量的通信和感知节点，恶意节点可能冒充这些合法节点进行恶意活动，对控制信号、导频信号、通信信号和感知信息等发起攻击，导致操作失控、信道估计错误、通信异常、感知错误等后果，同时也可能存在恶意窃听等行为，感知波形的强方向性使得私密信息传输面临更大安全挑战。针对以上问题，基于无线内生安全理念，可在物理层实现基于位置的安全，利用系统的感知功能获取窃听者的位置、CSI 等信息，赋能物理层安全方案的设计。

空天地一体化网络中，服务链路、星间链路、馈线链路都使用无线通信，无线链路具有开放性，更容易受到人为干扰、窃听、重放和无线资源占用等威胁。针对以上问题，在认证方面，采用融合星地链路物理指纹的双向认证机制，有效降低认证时延和开销；在加密方面，采用基于多星随机源的密钥生成技术，利用星地复合信道特征生成随机源，在无需密钥推送的情况下增强用户链路和馈电链路安全性。

### （二） 高弹性和强韧性军事无线通信

电磁频谱制胜背景下，战场无线通信与信号战、网络战、电子战等如影随形，电磁空间环境呈现出高度复杂化、强对抗性的特征。高动态、强对抗战场条件下无线通信系统的抗干扰与安全通信能力显得

至关重要。电磁空间对抗的博弈范式是敌我双方体系自由度之间的比拼，只有通过高自由度体系对抗低自由度体系，才能实现电磁空间高效利用和自由行动。提高系统自由度的意义在于面对恶性人为干扰、恶劣自然信道等外部因素压迫时，还有足够的自由度保证底线通信实现强韧性；通过牺牲部分自由度抑制干扰，动态利用剩余自由度恢复通信性能实现高弹性。

电子战的发展推动了电子防御技术的发展，近年来美军推出大量抗干扰安全通信项目，以强调战场无线通信韧性和弹性能力的关键性，充分反映了未来军事通信发展重点所在。高压迫的电磁空间对抗态势下，只有高自由度的战场无线通信系统才能具备靠自由度抵消强干扰阻塞/拒止攻击的强韧性能力，以及利用自由度重构内部与外部条件以恢复性能的高弹性能力。如何构建高自由度无线通信体系架构，是面向未来作战必须回答的重大现实问题。

复杂电磁环境中，敌方一旦采用饱和式攻击发送强干扰信号，使得干扰信号远大于期望信号强度，将会大幅压缩期望信号的接收电平，甚至造成接收机阻塞，无法恢复出目标信号。此外，当目标信号多径反向叠加时，将导致信号深衰落，使得接收信号能力大幅降低，影响通信可靠性。这对于强对抗条件下的抗干扰能力提出了更高要求，由于后端数字处理能力依赖高性能核心器件，面对核心器件/芯片的卡脖子问题和非对称代际劣势，需通过机理机制与体系架构创新获取新质增益。

经典无线通信体系架构下，阵列模拟处理前端采用功效同构化、

构造固定化、位置异构化排布的阵元感知信号，再靠后端的数字计算获取处理增益，导致通信系统关键指标的提升依赖于前端阵列的大规模和后端数字处理的大算力。模拟处理最前端（天线端）手段的缺失产生的信息缺失（获取信号差异性的缺失），难以通过后端“大算力、大数据”的数字处理来恢复。

以阵元和阵列构造为突破口，变革传统刚性同构天线阵列系统架构，构造基于 RIS 的空时异构阵列，增大等效阵列孔径，增强空域分辨率和动态适应性，由“规模决定论”向“构造决定论”发展，可实现系统模拟计算前端能力的增强。在此基础上，突破“先采样后处理”的传统阵列信号处理体系架构，创新构建以“数控模拟计算”为核心的模数混合智能计算的新型无线系统体系架构，利用 RIS 天线提供的敏捷重构模拟计算能力减轻后端计算负荷，从而降低对高性能核心器件/芯片的依赖度，用国产化器件/芯片有可能达到高性能器件/芯片同样的功能和性能，满足军事无线系统高弹性、强韧性通信的刚需。

## 参考文献


[1] 钟智豪, 罗文宇, 彭建华, 等. 多层异构蜂窝网协作传输和协作干扰机制的安全性能分析[J]. 中国科学:信息科学, 2016, 46(01): 33-48.

[2] 楼洋明, 金梁, 钟州, 等. 基于 MIMO 接收信号空间的密钥生成方案[J]. 中国科学:信息科学, 2017, 47(03): 362-373.

[3] 张波, 黄开枝, 钟州, 等. 异构携能通信网络中人工噪声辅助的顽健能量与信息安全传输方案[J]. 通信学报, 2019, 40(03): 60-72.

[4] 杨杰, 季新生, 王飞虎, 等. 窃听者随机分布下智能反射面辅助的MISO系统物理层安全性能分析[J]. 电子与信息学报, 2022, 44(05): 1809-1818.

[5] Z. WEI, F. LIU, C. MASOUROS, et al. Toward Multi-Functional 6G Wireless Networks: Integrating Sensing, Communication, and Security[J]. IEEE Communications Magazine, 2022, 60(4): 65-71.

[6] SU N, LIU F, MASOUROS C. Sensing-Assisted Eavesdropper Estimation: An ISAC Breakthrough in Physical Layer Security[J]. IEEE Transactions on Wireless

Communications, 2024, 23(4): 3162-3174.
[7] 金梁, 楼洋明, 孙小丽, 等. 6G 无线内生安全理念与构想[J]. 中国科学:信息科学, 2023, 53(02): 344-364.
[8] 季新生, 邬江兴, 黄开枝. 6G 内生安全可信技术白皮书[R]. 网络通信与安全紫金山实验室, 2023.
[9] WAN Z, LOU Y, XU X, et al. Physical-Layer Key Generation Based on Multipath Channel Diversity Using Dynamic Metasurface Antennas[J]. China Communications, 2023, 20(04): 153-166.
[10] JIN L, WANG X, LOU Y, et al. Achieving one-time pad via endogenous secret keys in wireless communication[C]. 2020 IEEE/CIC International Conference on Communications in China (ICCC). 2020: 1092-1097.
[11] 紫金山新闻. 全球首款+全国产化！两款芯片在南京发布[J/OL]. 2023. https://m.zjsnews.cn/news/6233901969382146759.
[12] ZHANG P, TENG Y, SHEN Y, et al. Tag-Based PHY-Layer Authentication for RIS-Assisted Communication Systems[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20: 4778-4792.
[13] ADEM N, HAMDAOUI B, YAVUZ A A. Pseudorandom Time-Hopping Anti-Jamming Technique for Mobile Cognitive Users[C]. 2015 IEEE Globecom Workshops (GC Wkshps), 2015: 1-6.
[14] HANAWAL M K, ABDEL-RAHMAN M J, KRUNZ M. Joint Adaptation of Frequency Hopping and Transmission Rate for Anti-Jamming Wireless Systems[J]. IEEE Transactions on Mobile Computing, 2016, 15: 2247-2259.
[15] 赵晓艳. 直接序列扩频信号的盲检测和参数估计方法[D]. 北京邮电大学, 2008.
[16] 林钰达. 基于无线环境差异的多天线隐蔽通信技术研究[D].信息工程大学, 2022.
[17] 操文政. 基于可重构智能表面天线的信息调制与多用户收发技术研究[D]. 战略支援部队信息工程大学, 2023.
[18] 任章搏. 基于智能超表面的无线通信抗干扰技术研究[D].信息工程大学, 2023.
[19] JIANG W, REN Z, HUANG K, et al. A Joint Space-Frequency Anti-jamming Scheme Based on Reconfigurable Intelligent Surface[C]. GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 2022: 6408-6414.
[20] THANH P D, GIANG H T H, HONG I P. Anti-Jamming RIS Communications Using DQN-Based Algorithm[J]. IEEE Access, 2022, 10: 28422-28433.
[21] YANG H. Intelligent Reflecting Surface Assisted Anti-Jamming Communications: A Fast Reinforcement Learning Approach[J]. IEEE Transactions on Wireless Communications, 2020, 20: 1963-1974.
[22] SUN Y, ZHU Y, AN K, et al. Robust Design for RIS-Assisted Anti-Jamming Communications With Imperfect Angular Information: A Game-Theoretic Perspective[J]. IEEE Transactions on Vehicular Technology, 2022, 71: 7967-7972.
[23] TANG X, WANG D, ZHANG R, et al. Jamming Mitigation via Aerial Reconfigurable Intelligent Surface: Passive Beamforming and Deployment Optimization[J]. IEEE Transactions on Vehicular Technology, 2021, 70: 6232-6237.

[24] JIN L, LOU Y, XU X, et al. Separating Multi-Stream Signals Based on Space-Time Isomerism[C]. 2020 International Conference on Wireless Communications and Signal Processing (WCSP), 2020: 418-423.
[25] 邬江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(02): 189-204.
[26] 邬江兴. 网络空间内生安全——拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020.
[27] SHANNON C E. A mathematical theory of communication[J]. The Bell system technical journal, 1948, 27(3): 379-423.
[28] KATZ J, LINDELL Y. Introduction to modern cryptography[M]. CRC press, 2020.
[29] JIN L, HU XY, WU JX. From perfect secrecy to perfect safety & security: cryptography-based analysis of endogenous security[J]. Security and Safety, 2023; 2: 2023004. https://doi.org/10.1051/sands/2023004.
[30] JIN L, HU X Y, LOU Y M, et al. Introduction to Wireless Endogenous Security and Safety: Problems, Attributes, Structures and Functions[J]. China Communications, 2021, 18(4): 99-114.

THE 4th
ACADEMIC CONFERENCE
ON **CYBERSPACE**
**ENDOGENOUS**
Safety & Security

THE 7th
**"QIANGWANG"**
**INTERNATIONAL** ELITE
CHALLENGE
ON **CYBER MIMIC**
**DEFENSE**