文章编号：2095-4980(2023)03-0301-10

太赫兹通信物理层安全技术发展研究

吴振东[1,2]，马建军*[3,4]，张玉萍[1,2]，李德华[1,2]

(1.山东科技大学 电子信息工程学院，山东 青岛 266590；2.青岛市太赫兹技术重点实验室，山东 青岛 266590；
3.北京理工大学 集成电路与电子学院，北京 100081；4.北京市毫米波与太赫兹技术重点实验室，北京 100081)

摘　要：在太赫兹通信技术快速发展的背景下，建筑遮挡、恶劣天气等原因导致的复杂、弥散信道对通信安全性、可靠性提出新的挑战。太赫兹通信的保密属性在通信网络的广域性下隐含泄露、窃听等风险，研究现有的加密和防窃听手段在太赫兹通信中的可行性，推动物理层安全技术的创新与应用，实现信息的稳定安全传输，成为具备研究价值的热点问题。本文从安全通信角度出发，分析部分现有物理层加密与防窃听方法，总结其在太赫兹通信领域中的融合应用与效果，并对其未来发展趋势进行展望。

关键词：太赫兹通信；物理层安全；加密；防窃听

中图分类号：TN918.91　　**文献标志码：**A　　**doi：**10.11805/TKYDA2022052

Development of physical layer security communication in terahertz band

WU Zhendong[1,2]，MA Jianjun*[3,4]，ZHANG Yuping[1,2]，LI Dehua[1,2]

(1.College of Electronic Information Engineering，Shandong University of Science and Technology，Qingdao Shandong 266590，China；
2.Qingdao Key Laboratory of Terahertz Technology，Qingdao Shandong 266590，China；
3.School of Integrated Circuits and Electronics，Beijing Institute of Technology，Beijing 100081，China；
4.Beijing Key Laboratory of Millimeter Wave and Terahertz Technology，Beijing 100081，China)

Abstract：In the context of rapid development of terahertz communication technology, the complex scattering property of wireless channel caused by building occlusion, bad weather and other reasons poses new challenges on secure and reliable data transmission. The confidentiality property of terahertz communication contains risks such as leakage and eavesdropping under the wide area of the communication network. Investigations on the feasibility of existing encryption and anti-eavesdropping methods in terahertz communication systems, promoting the innovation and application of physical layer security technology, and achieving stable and secure data transmission have become a valuably urgent topic. In this paper, from the perspective of secure communication, some of the existing physical layer encryption and anti-eavesdropping methods are presented and analyzed; their fusion applications and efficiencies in terahertz communication are summarized; and the trends on future development are expected.

Keywords：terahertz communication；physical layer security；encryption；anti-eavesdropping

在太赫兹通信技术快速发展的趋势下，凭借高速通信优势所兴起的各项技术成为研究热点。太赫兹通信带来极高的信息传输速率和信道容量，但也使得信道弥散特性更复杂，引发针对安全、窃听、保密等问题的审视。无线信道本身具有的开放性与随机性，叠加环境因素引起的多径散射效应[1]，以及人为的窃听和恶意攻击，导致太赫兹通信技术仍存在泄漏风险。但同时，这些特性使得信道内生安全元素更丰富、更便于提取。物理层安全技术可充分利用信道的差异性设计，提升信息传输的安全性，使物理层安全可以和下一代无线通信新空口技术同步演进、融合发展，实现安全与通信一体化发展。

目前，物理层安全主要面临缺少高效加密手段、现有加密手段在新系统环境中适应性差、应用成本高等问

收稿日期：2022-02-28；**修回日期：**2022-04-18

基金项目：国家自然科学基金面上资助项目(62071046)；北京理工大学“特立青年学者”人才支持计划资助项目(3050011182153)

*通信作者：马建军　email:jianjun_ma@bit.edu.cn

题。如常用的通信密钥在如今设备计算能力不断增强的背景下，有被破译的风险；复杂信道环境降低了有效保密率、提高了信息传输成本等。现有的加密手段已无法满足太赫兹通信技术的安全需求，成为制约物理层安全技术在新一代无线网络中发展和应用的因素之一。

物理层安全技术包括了基于通信密钥、信道特性、多技术融合等多种保密方法，但实际应用环境、配套技术、成本等问题会给这些方法的使用带来各种各样的困难，如5G基站覆盖范围小，以及复杂的城市传播环境导致基站建设成本增加；基础设施与加密技术发展的非同步性导致保密手段落后于智能设备的进步。在开展对新的调制方式、天线阵列研究，实现陆地、海洋、空中的多维度通信，探讨区块链、可见光通信等潜在技术发展基础上，研究如何实现物理层安全技术在这些领域的有效应用[2-4]，是近年来学者们的主要研究方向。新技术的提出应用往往需要多领域的共同进步、软硬件的结合发展才可实现。太赫兹通信物理层安全技术的实现，可以借鉴现有技术进行创新，或相近领域的技术移植，在现有加密方案的基础上进一步发展。如，移植人工噪声、协作干扰、多重物理认证、认证机制创新等手段应用在毫米波、太赫兹通信。又如引入物理层认证，对场景应用、信息传输机制、通信设备设计等问题进行技术创新，实现认证机制在可见光通信系统中的应用。太赫兹波濒临毫米波和光波，可充分发展、利用两者的优势技术。微波、毫米波中基于信道特性和信号处理的加密手段，有望通过移植创新，实现在太赫兹通信中的使用。太赫兹通信网络中信号识别算法、认证策略、传输机制等技术的实现，可以借鉴毫米波网络中的认真策略、算法等成果进行发展研究。

本文分析了当前的主要物理层安全保密手段，对物理层安全通信领域的部分技术研究进行概括总结。探讨了太赫兹通信中，通信密钥、信道内生特性等物理层安全技术的研究现状、主要问题等，最后对太赫兹通信物理层通信技术的发展趋势进行展望。

1 物理层安全技术

无线信道天然的开放性和随机性，使其容易受到复杂天气条件的影响，并面临人为窃听等安全威胁。物理层安全技术的本质是利用无线信道特性的内生安全机制，为“一次一密”提供可行思路[5]。此前，通信密钥的广泛使用为加密通信提供了可靠支撑，但随着计算机科学的不断进步，智能设备的计算能力迅速增强，密钥的安全性已不能被完全保证。

另一方面，智能网络中设备数量的不断增加，也对密钥的分发和有效性提出了挑战[6]。超可靠低延迟通信(Ultra-Reliable and Low-Latency Communication，URLLC)技术的广泛研究发展也为其他保密手段提供了无限可能[7]。5G网络下，分散式组网为大量设备的运行提供支撑，窃听者利用设备工作方式造成的漏洞对通信真实性、保密性造成威胁，设备通信连接的往复性、随机性给密钥的有效性带来挑战[8]。计算机数据处理能力的增强也给暴力破解密钥提供可能，穷举法、逆向法等密钥破解方式层出不穷。利用脱离密钥算法的无线信道特征，进行人工噪声的引入和协作干扰，是实现通信安全性的提升可行方案之一。通过借鉴物理层安全技术在毫米波波段的应用方法，如最优传输预编码设计、基站空间复用、混合多输入多输出系统(Multiple Input Multiple Output，MIMO)相控阵或借助无人机等外部设备实现的中继通信等[9-12]，实现方案设计调整和研究思路创新，达到物理层安全技术在太赫兹信道中有效应用的目的。如，借助发射和接收端的设备优化，在通信过程中除了发送信息内容外，同时作为人工噪声的产生源用于干扰窃听，或采用无人机作为通信中继，在复杂地形中实现信号转发并进行协作干扰。

尽管作为加密技术之一的密钥，在新一代技术产业革命下，已不再具备“绝对安全”。重新考虑专注于无线信道特性而发展的物理层安全技术，实现信道特征与密钥之间的高效结合，可以探索出新的安全通信方案。

2 主要研究问题

2.1 通信密钥性能研究

安全性是伪随机码的一个重要性质，特别对于卫星通信，安全性更是至关重要。现代通信系统中，应用的常用短码如m序列、Gold码，具有序列平衡、相关性好的特点，但它们的线性复杂度不高，安全性较差。通信密钥通常由系统自动生成或人工生成，且一组密钥分为加密和解密2部分。使用时，通信双方按照协定各自留存一份密码，用于信息的加解密传输。密钥是将一组无序校验码通过与明文中的二进制编码进行有限次的逻辑运算而得到，因此在窃听设备计算能力足够强大的前提下，其安全性将不会得到完全保证。

常见的通信双方通过公钥和私钥组成一对密钥对，实现身份验证和保证安全性，图1为通信密钥的工作过程。通过公钥基础设施(Public Key Infrastructure，PKI)实现身份核验的过程计算较为复杂，往往会造成设备的运

行负担，产生较高延迟或牺牲掉一定的匿名性[13-14]。这对实时性要求高的工作提出了挑战，尤其在无人驾驶这些对时延要求较高的应用场景中。在提高通信密钥性能方面，将通信延迟性、算法复杂性、设备响应时间等因素纳入研究范畴，针对不同应用场景制定适合的认证策略是有效的研究手段。

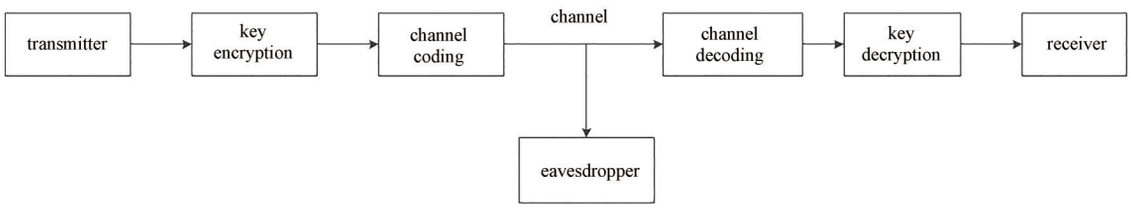
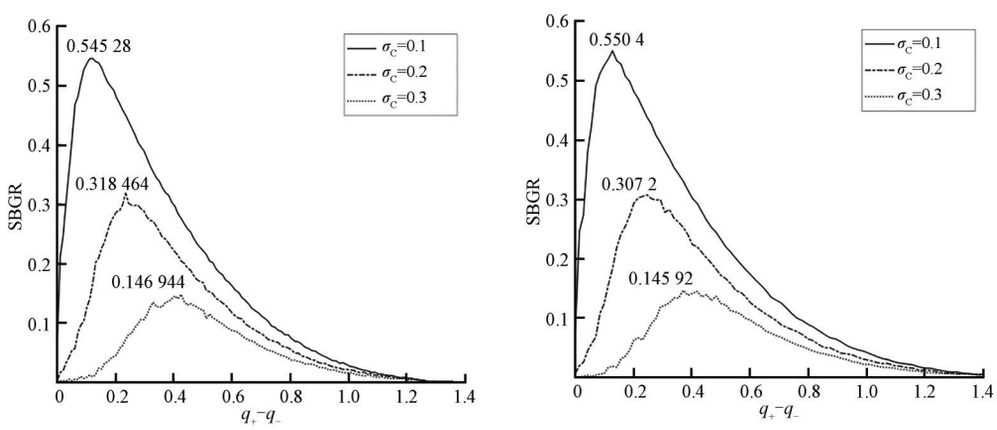


Fig.1 Working process of key encryption and decryption
图1 密钥加解密工作流程

Bottarelli 等[15]针对车辆 V2V 通信环境下产生的通信密钥延迟性和有效性问题，提出了基于累积分布函数(Cumulative Distribution Function，CDF)和平均衰落持续时间(Average Fade Duration，AFD)的阈值分割技术，用来增大密钥的熵，提升密钥性能，并引入了密钥比特产生率(Secret-Bit Generation Rate，SBGR)进行效果评估。他们将 SBGR 定义为单位信道在单位时间内可以提取的密钥比特数，将 CDF 和 AFD 同阈值相关联，通过改变阈值的大小和信道非互易性参数 σ_c，实现不同环境的模拟。图 2 为基于 CDF 和 AFD 策略的阈值分割对 SBGR 的影响[14]。图中 q_+和 q_-分别为阈值的上下限，σ_c的大小代表了信道的非互易性程度。通过对不同阈值和 σ_c的测试，发现 AFD 策略在互易性高的情况下优于 CDF 策略。



(a) CDF threshold segmentation strategy　　(b) AFD threshold segmentation strategy

Fig.2 Influence of channel non-reciprocity factors under different threshold segmentation strategies
图2 不同阈值分割策略下的信道非互易性因素影响

Holenstein 等[16]在单向通信的条件下，推导了减低公钥加密方案中解密错误率、提升密钥安全性的有关公式，给出了单向密钥协商下接收双方有效生成密钥的准确速率以及有关参数，给出了应用极化法提高密钥性能的具体推导并证明了单比特密钥条件下，极化法与密钥协议的联系。Holenstein 等认为在单行密钥传输条件下，有效密钥速率可被描述为：

$$S(X;Y|Z)=\sup_{(V\leftarrow U\leftarrow X)} H(U|ZV)-H(U|YV) \tag{1}$$

式中：V←U←X是指 V,U,X 三者构成一条马尔科夫链，只从 X经单一方向传达至 V而不考虑其他可能情况。基于此条件，可得出发送方到接收方的有效密钥速率为 $H(U|ZV)$-$H(U|YV)$。

另一方面，通信环境具有随机性。恶劣天气或复杂城市环境导致的衰落和多径效应使信号传播条件恶化，影响传输效率[17]，这在一定程度上成为制约密钥安全性能的因素。此外，5G 混合网络架构、传感器网络、AI、高清视频、VR 等技术的发展推动了网络方案的升级[18]，促使通信网络朝多元化方向前进，为密钥产生和传播提供新的环境和可能。在这一背景下，产生多种新型的密钥算法以及在原有基础上增强安全性的方案被逐渐发掘出来，如智能电网中的轻量级加密算法[19]、结合脑电设备的脑电波(Electroencephalogram，EEG)增强型密钥[20]等。

为了适应在复杂天气或城市条件下的通信环境，Y Kong 等[21]提出了多径传播条件下的联合密钥生成方法，省略了密钥交换过程。将发送方、中继、接收方之间的密钥分别用 k_A, k_B, k_{AB} 等表示，h 作为信道估计量用于联合

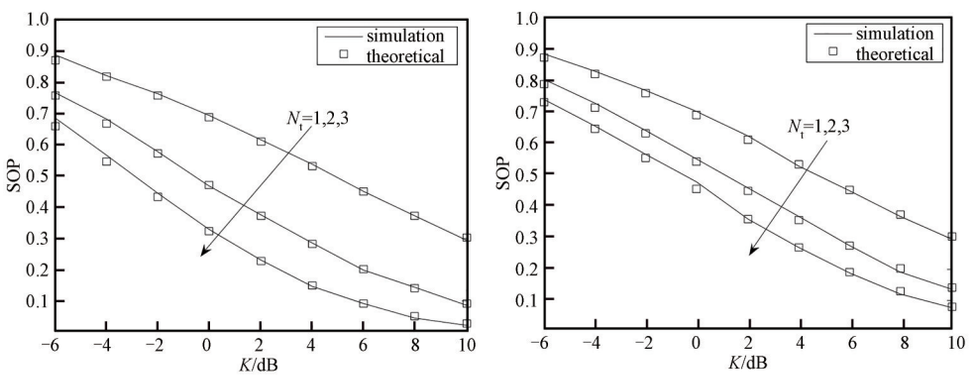
密钥的有关表示，最后通过仿真给出了在直接网络编码(Straight Forward Network Coding，SFNC)和物理层网络编码(Physical Layer Network Coding，PLNC)系统中联合密钥生成(Joint Key Generation，JKG)的密钥生成方法的误比特率。结果表明2种系统下，随着信噪比(Signal to Noise Ratio，SNR)从0增大至30 dB，误比特率(Bit Error Rate，BER)从$10^{-0.25}$下降至10^{-6}左右，从而证明了JKG方法的有效性。图3为传统密钥生成与联合密钥生成的过图[20]。

(a) traditional key generation (b) JKG

Fig.3 Key generation process

图3 密钥生成过程

J Zhang等[22]在多径环境下开展了大量实验测试，证实了信号的多径传输规律，并认为其随机性利于密钥产生，但部分研究忽略了设备对不同密钥算法的兼容性和成本问题。探索多径条件下密钥生成算法与基础设施的有效结合、保证安全性能是当前研究迫切需要解决的问题。H Wang等[23]在Wyner窃听模型的基础上，证明通过发射天线类型和规模的设计，可以增强在城市衰落模型下的密钥保密性能。通过设置最优和次优2种天线选择方案，比较不同的天线设计对密钥保密性能的影响。在环境衰落模型方面，引入相较于Rayleigh和Rician衰落模型更为优秀的Nakagami模型，使模拟结果更贴近于复杂的城市环境。H Wang等将安全中断概率(Security Outage Probability，SOP)作为评估指标，模拟了2种天线选择方案随SNR变化对SOP的影响[23]。图4为最优和次优方案对安全中断概率的影响表现。



(a) SOP performance of optimal TAS scheme (b) SOP performance of suboptimal TAS scheme

Fig.4 Influence of antenna optimization scheme on SOP

图4 天线优化方案对SOP的影响

在城市化不断加深、通信速率不断加快、网络覆盖率不断扩大的情况下，通过改善天线方向性、网络拓扑结构、信号传播链路和机制等强化通信安全性、延展通信距离和克服高路径损耗是可行的[24]。

在太赫兹通信技术的快速发展下，数据传输的高速率和强安全性之间的结合也在逐步迈进。S Ju等[25]提出了办公室环境下的室内模型，建立的模拟器可以模拟室内环境下约150 GHz载波频率的信号，提出的室内统计信道模型对未来6G网络下的发射接收器设计具备参考价值。作者考虑了近距离自由空间的路径损耗(Path Loss，PL)模型，并将PL通过解析表达：

$$PL(f,d)=FSPL(f,d)+10n\lg\frac{d}{d_0}+x_\sigma \tag{2}$$

式中：$FSPL(f,d)=20\lg 4\pi d_0 f/c$；$d_0$为参考距离，默认为1 m；$x_\sigma$是期望为0，方差为$\sigma^2$的对数正态分布。

此外，作者将视距传输(Line of Sight，LOS)和非视距传输(Non-Line of Sight，NLOS)纳入研究范围，将PL作为太赫兹通信链路性能的评估指标，通过调整发射单元和接收单元数量、发射机与接收机的距离以及时间集群值，在测试中得到了对应的PL和延时扩展(Delay Spread，DS)等结果。在28 GHz，3个发射单位、16个接收单位，距离为5.3 m时，LOS可实现最小延迟和路径损耗，分别为4.9 ns和68.0 dB；在距离为5.5 m，发射单元为3个、接收单元为26个时，NLOS可达到最优效果，得到3.4 ns延迟和72.9 dB的损耗。当频率扩大至140 GHz时，LOS和NLOS两种情况均显示为无规律的结果，任何变量都有可能对PL和DS产生影响。

总的来看，虽然已能建立较小范围内同种设备间的太赫兹通信，但在太赫兹波段下保证种类不同的设备间的密钥有效性，仍需进一步研究。

2.2 基于信道特性的安全通信

利用信道内生特性实现的加密通信，作为实现物理层安全通信的方向之一，其通过改变信号传播特性的工作方式，在通信设施的用户容纳能力、通信运营商的合作组网力度不断提高的情况下，成为研究热点。其在一定程度上脱离了构建密钥所需的复杂算法，更注重通信设施的规划、信号传播方式的优化等，如，天线阵列的设计、信号协作干扰等。

D P M Osorioel等[26]指出，在6G网络概念逐渐成熟的今天，太赫兹链路、物理层认证、大规模MIMO系统是6G重要的组成部分。在普及5G网络并发展6G网络的很长一段时间内，智能设备的计算能力会伴随着通信技术的不断进步而逐渐增强，给密钥安全性造成风险，使密钥的破解成为可能。在这背景下，借助信道内生特性实现安全通信是可行的方案。在太赫兹波段内，支持高速率通信下大信道容量的实现，可以从设施上进行改变。大规模MIMO和通信中继作为增加频谱利用率和扩展通信范围的方式，两者结合可以解决频谱资源匮乏、覆盖范围小的问题。尽管付出了使发送和接收端的设备更复杂化的代价，但实现了频谱的高利用率，并为其他设备在信号处理方面实现保密性能的增强，提供了解决空间[27−28]。特别的，文献[27]将干扰信号搭载到MIMO系统上，有效实现了高频谱利用率下通信的安全性，并引入了误信率(Mdr)作为参量之一，用以指代接收端收到错误消息的概率。

$$Mdr=P_{\mathrm{r}}\left(H_{\mathrm{r}}|H_{\mathrm{r}}+H_{1}\right) \tag{3}$$

此外，引入了far作为假报警率(指接收端正确接收了信息，但将其作为错误信息处理的概率)：

$$far=P_{\mathrm{r}}\left(H_{\mathrm{r}}|H_{\mathrm{r}}+H_{\mathrm{r}-1}\right) \tag{4}$$

借助人工噪声，实现协作干扰，在最大化窃听方干扰的同时，确保通信双方的保密率是研究的方案之一。赵伟等[29]利用发送人工噪声的方式，并借助天线方向调整、MIMO技术实现了多波束下的安全通信，模拟的窃听方未能解密出有效信息。Z Xie等[30]基于全双工接收机发送人工噪声，并提出新的传输方案，用以消除人工噪声对发射机的影响以及提高保密性能。全双工接收机工作时，利用功分器实现自身能量供应和噪声信号产生。发射端通过中继或直射链路进行信息传递，最终由接收端接收。接收端工作的同时，产生人工噪声用于干扰窃听者，实现保密功能。图5为全双工接收机的工作场景[29]。

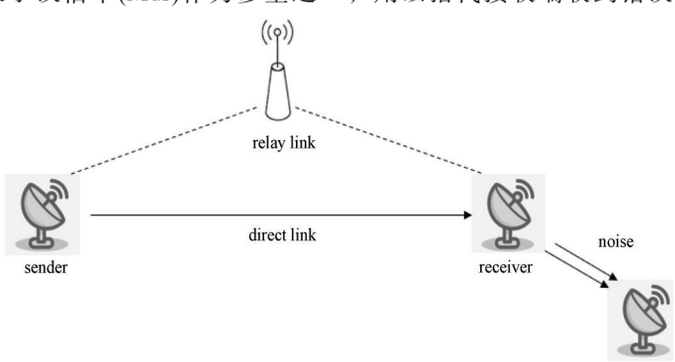


Fig.5 Working scenario of full duplex receiver
图5 全双工接收机工作场景

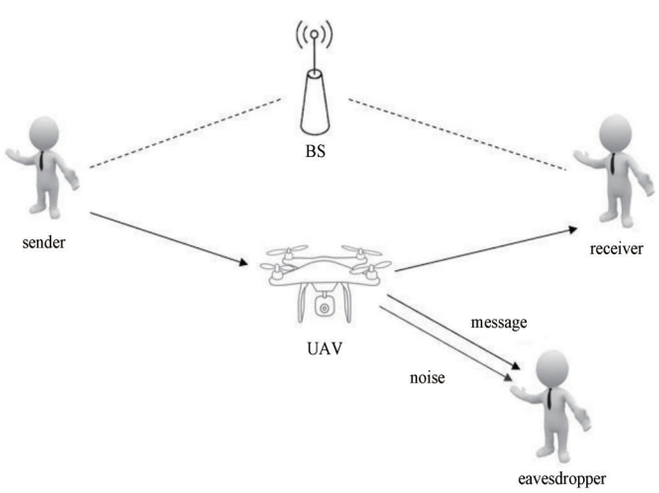


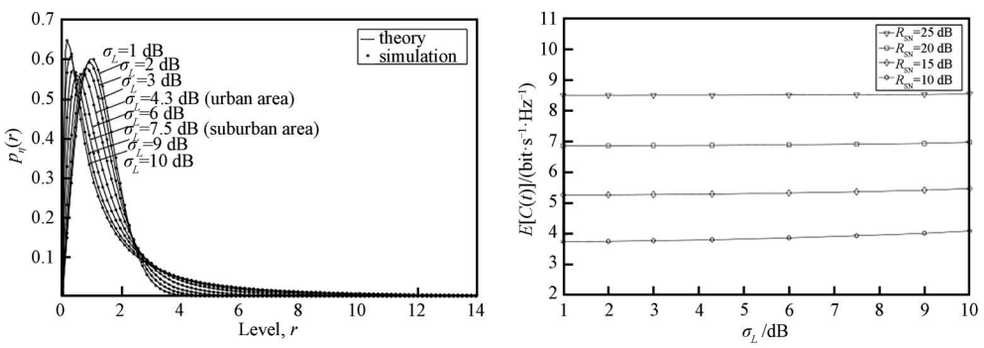
Fig.6 UAV relay and cooperative jamming
图6 无人机中继与协作干扰

实际通信过程中，窃听者信道的信息往往未知[31]，这给人工噪声的参数、协作干扰的有关参数设置造成了困难。如何在未知窃听者的设备数量、地理位置等条件下实现通信的保密，需要联合使用人工噪声、协作干扰等多种手段。文献[31–32]中提出利用多个能量收集节点或无人机设备作为辅助干扰器，结合人工噪声实现协作干扰，达到打击主动窃听，提高信道安全容量的目的。另一方面，无人机作为新一代技术产业革命的产物，有学者将其作为通信中继设备的一种，用于信号的中继转发，或作为加密设备用作干扰信号的发射源，这种方案具有增强通信保密性能的作用[32−33]。但作为独立的设备，因能量供应导致无法持续工作是无人机设备普遍具有的缺点，致使无人机不能作为固定设备工作，无法长期投入使用。图6为无人机在信号中继与协作干扰中的工作场景[32]。

S I Alnagar 等[34]提出了基于Q学习的优化算法，用于无人机网络下的功率分配调整，对无人机信号转发的功率和噪声产生的功率进行了划分，并最小化通信网络的通信中断概率。Alnagar 将无人机的数量 N、无人机传输功率 P_{u}、通信者数量 L 等指标同通信中断概率 P_{out} 结合，测试在 SNR 临界值为 9 dBm、莱斯参数为 2、基站传输功率为 20 dBm 条件下，P_{u} 对 P_{out} 以及截获概率的影响。得出随着无人机传输功率的增加以及无人机数量的增多，通信中断概率得到有效降低；随着干扰功率的增加，截获概率也降低。最后通过优化算法得到了传输功率与干扰功率的最佳分配策略。

此外，复杂的传播环境也是需要考虑的问题。研究大气环境的多变性影响对于保证协作干扰过程中人工噪声的有效性、稳定性是必要的。大气湍流、降雨、降雪、大雾等天气条件，都会在信号的传播过程中产生恶劣的多径效应和阴影衰落[35-36]。

G Rafiq 等[37]研究了阴影衰落条件对移动设备通信性能的影响，特别引入了 Suzuki 城市模型进行分析。作者探讨了不同瑞利衰落(σ_L)条件下，传输信号在 Suzuki 模型下的传输效果；仿真了 1,2,3,…,10 dB 瑞利衰落效果下的包络曲线，得到随着城市中瑞利衰落的逐步加剧，传输信号幅值衰减越趋严重，高电平分量被完全抑制的结果，并给出了不同 SNR 下，Suzuki 信道的平均容量，如图 7 所示。



(a) influence of Suzuki city model on signal envelope (b) Suzuki channel average capacity under different SNRs

Fig.7 Suzuki city model

图7 Suzuki城市模型

为了保证通信链路的稳定性、信号传播的有效性，Seyedi 等[38]将城市环境转化为具体参数，引入阴影矩的估计模型中。Seyedi 设置一对球面角(θ,ϕ)用以表示 2 座建筑物之间的连接方向，给出了 BER 的表达式，将位错误概率(Bit Error Outage，BEO)作为评估服务质量的指标。研究了多种相移键控(Phase Shift Keying，PSK)调制方式下平均噪声功率与 BEO 的关系，给出了正交相移键控(Quadrature Phase Shift Keying，QPSK)调制方式下，方位角 θ、仰角 ϕ 对信号中断概率的具体影响，为城市环境内通信链路优化、信号传播有效性的提高提供了具体成果，对城域太赫兹通信网络的搭建和引入物理层安全技术的可行性提供了参考。O S Badarneh 等[39]使用了 Nakagami 城市模型，描述了城市环境下的多径衰落和阴影效应，通过引入主信道和窃听信道的衰落参数 m_{D},m_{E}、阴影参数 m_{sD},m_{sE} 以及噪声差异 σ^2，推导验证了 SOP 和平均保密容量(Average Secrecy Capacity，ASC)的关系。Badarneh 通过探索主信道和窃听者信道下信噪比和衰落对 ASC 和 SOP 的影响，得出在 Nakagami 模型下 ASC 和 SOP 同有关影响因素之间的联系，并以 $C_{\mathrm{s}}^{\mathrm{ASC}}$ 和 $C_{\mathrm{s}}^{\mathrm{SOP}}$ 2 个指标进行评估，最终得出以下结论：

1) 随着主信道的衰落系数和 SNR 的增大，SOP 降低，ASC 增大。

2) 窃听者信道中，随着衰落系数和 SNR 的增大，SOP 增大，ASC 降低。

3) 随着主、窃听信道中阴影效应的增强，ASC 显著提高。

总之，已有研究学者利用信道自身特性，通过人工噪声加扰、多方协作干扰，或采用第三方设备协作干扰实现通信安全，但将这些成果转化为太赫兹应用条件下的具体实物，还需多方的联合发展，并经历理论创新、实验验证、系统优化等过程。

2.3 不同领域的结合

与相近的科研领域联合研究或跨学科研究是物理层安全通信的一种发展方向。结合其他学科领域的工作大多是将自身的信息交换功能同其他知识结合，需要利用物理层安全技术的研究目前仍较少，除了在通信领域应用，如光通信一类的其他通信类型上。结合太赫兹技术实现在医学领域中的应用，也存在对物理层安全技术的引入，如医疗纳米网络、远程医疗等。

通过太赫兹通信与物理层安全技术的结合，实现太赫兹通信物理层的安全，并将这种研究应用到医学领域

中的纳米通信是当前的成果之一。利用太赫兹通信与物理层认证的双重优点，实现对患者病症的精准判断，是医疗诊断和治疗的重要发展课题[40−41]。由于太赫兹波的波长同生物体内的大分子直径相近，因此利用反射显示的电磁波图像，可以精准判断患者体内的病变部位。进一步地，物理层认证为这一过程提供了可靠的链路安全保证。Rahman 等[40]设想了纳米网络中的纳米机器人在人体内与外界的实时通信的工作场景：医疗人员通过外部通信设备与患者体内纳米设备无线连接，定期实现血压、心跳、血糖等指标的实时监测或药物定点投放。作者将恶意窃听方引入到工作场景中，设想第三方人员假装医疗工作者向纳米设备传递错误指令的情况，具体工作场景如图 8 所示[39]。为此作者引入了基于距离的路径认证，以保证通信的稳定性，这一思想也被发展到医院内药物递送和办公室智能建设中。

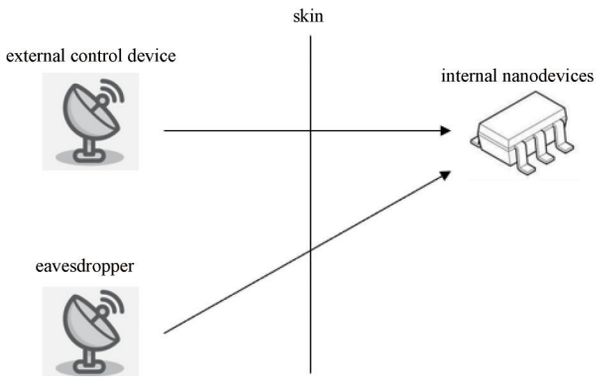


Fig.8 Working scenario of nanomedical network
图 8　纳米医疗网络工作场景

在与可见光通信系统融合研究上，将可见光通信高带宽、稳定性好等优点与太赫兹通信高穿透、抗干扰等特性结合，引入物理层安全技术。将具体的物理层安全技术在可见光通信系统中进行效果验证，为实现太赫兹通信中的物理层安全提供参考。另一方面，对发展自由空间中可见光通信安全手段也具有推动作用。将光频段高速信息传输的通信技术与物理层安全技术结合[42]，引入平均保密容量等参数进行评估，实现光通信与物理层认证联合使用，可有效解决光通信中的安全性问题。Y Ai 等[43]研究了卫星通信与自由空间光通信的混合系统。他们推导了中继后的具体的平均保密容量和保密中断概率的表达式，并根据推导分析了系统的物理层保密性能。Y Ai 将 SOP 性能作为评估指标，模拟了混合卫星自由空间光通信(Free−Space Optical，FSO)系统在解码转发(Decode and Forward，DF)中继和放大转发(Amplify and Forward，AF)中继 2 种情况下，SOP 随平均信噪比 γ_{R} 的变化情况。作者引入平均信噪比为 $\overline{\gamma_{\mathrm{E}}}$ 的窃听信道情形，得出随 γ_{R} 增大或 $\overline{\gamma_{\mathrm{E}}}$ 减小，混合系统的 SOP 性能显著提高的结果。

X Zhao 等[44]分析研究了在单窃听者和多窃听者 2 种情况下，可见光通信系统与物理层安全技术的结合。其模拟了在固定空间内的通信场景，如图 9 所示[43]。作者引入了 SOP 作为评估指标，将窃听者在空间中的极坐标 $(r_{\mathrm{e}},\theta_{\mathrm{e}})$ 和用户极坐标 (r_k,θ_k) 等作为变量，模拟出 LED 照射半角在 15°~60°之间时，系统 SOP 稳定在 0.2 左右。研究发现多窃听者情况下，降低窃听者分布密度或缩减 LED 照射半角，对提高系统 SOP 性能有积极作用。Y Ai[43]和 X Zhao[44]的成果表明太赫兹通信下的物理层安全技术具备较高的研究价值，在卫星通信、可见光通信等系统中的有关应用，证明其可移植至其他高速率、宽频带的通信网络中形成专用的系统。

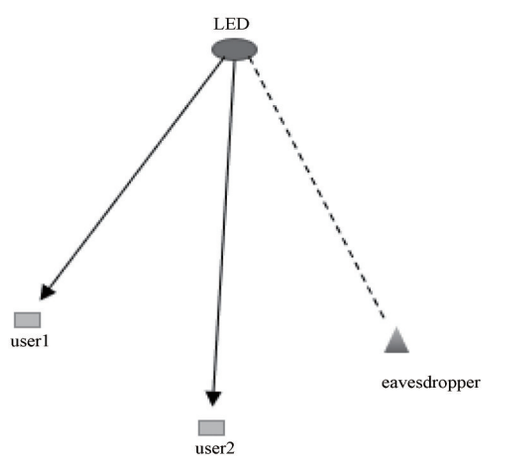


Fig.9 Working scenario of visible light communication system[43]
图 9　可见光通信系统工作场景[43]

3　分析总结

表 1 总结了已发表的通信密钥和基于信道特性保密方式的具体研究工作，以及其他领域中物理层安全技术的应用研究成果。目前，物理层安全通信手段主要包括通信密钥和信道特性 2 种。依据密钥实现的保密手段倾向算法的突破以及设施利用率的优化；基于信道特性的保密方式注重收发双方的合作干扰或第三方设备的协作干扰，在保证信道容量的同时，可降低窃听者的有效解密率。通信密钥与信道特性的研究侧重不同，但均受限于信号传播环境的影响，引入包含恶劣天气情况在内的 Suzuki 和 Nakagami 等城市阴影衰落模型进行仿真研究是常用手段。当前太赫兹通信物理层安全研究成果主要局限于实验室中，将这些成果转化到基础设施创新、软硬件设计上，实现在太赫兹技术下的物理层安全通信是亟待解决的重要课题。

综上，通信密钥和基于信道内生特性的保密手段作为物理层安全技术的 2 个主要分支，通信密钥可适应种类复杂的通信设备，减少了因软硬件不适配导致的资源浪费，使用场景灵活。但随着各类智能设备的逐渐发展，密钥安全性能受到设备强大计算能力的威胁。本文中引用的研究成果也偏向于密钥生成算法的复杂性与保密性

能的联系，以产生在太赫兹通信网络下通信密钥的工作思路。基于信道特性的保密手段脱离了复杂算法，避免了单凭计算能力破解的风险，但受到硬件设施复杂度及部署规划的制约。文中引用的研究成果集中在人工噪声及多方协作的干扰系统，此类系统与硬件设施联系密切，可为太赫兹通信网络下依靠基础设施实现的物理层安全技术提供借鉴方案。

表1 主要研究问题汇总

Table1 Summary of main research questions

main research questions	specific direction	research work
research on security of communication key	research on security of V2V communication environment	key performance research based on two threshold segmentation techniques of CDF and AFD[15]
	one-way communication key agreement	derivation of effective key rate in one-way communication[16]
	joint key generation	joint key generation method under multipath conditions[21]
	antenna design and key performance research	relationship between different TAS schemes and key performance[23]
security method based on channel characteristics	research on communication security of MIMO system	research on interfering signal performance in MIMO system[27]
	full duplex receiver cooperative jamming	combination of full-duplex receiver and artificial noise[30]
	UAV jamming network performance optimization	power allocation problems in cooperative jamming process of UAV[34]
	mobile communication performance under shadow fading	research on mobile communication performance under fading conditions[37]
performance and system integration application of physical layer security technology	research on performance of physical layer security technology in different scenarios	research on BER and BEO of channel in urban model[38]
		performance of main and eavesdropping channels in urban model[29]
		research on ultra-high speed communication performance of indoor model[25]
	multi-domain physical layer encryption technology	physical layer authentication of nano medical network[40]
		research on security performance of hybrid satellite and FSO system[43]
		ommunication security performance of visible light communication system[44]

4 研究展望

在智能设备计算能力的快速进步下，基于通信密钥的保密手段需要更新加密算法。多重加密的算法是可行的途径，利用外貌、生物电磁波等个人生物特征的独特性将脑电技术或AI用于生成密钥，可在一定程度上提高安全性。另一方面，V Raghavan等[45]提到，在后5G时代，有限的带宽以及设备复杂度扩展无法满足无线通信长期的发展需要，对基于信道内生特性的安全手段存在限制。扩充硬件设备的支撑，提高频谱利用率，促进设备进步，换取更多高效算法和证书的开发，具备研究价值。

当前，基础设施的覆盖率不断增大，硬件条件不断改善，考虑防止因计算能力导致的密钥泄露、弥补安全技术与设施发展不同步导致的短板、优化频谱利用等因素，发展基于信道内生特性的物理层保密手段较密钥具有更广阔的研究空间。T S Rappaport等[46]认为，频宽的增加，将会带来电路系统、软件、信号处理等多种元素的快速发展。伴随通信密钥、信道内生特性等安全手段的成果进步，太赫兹通信物理层安全技术将朝算法复杂化、机制完备化、工作协同化的趋势进行发展。一方面，基站、移动台设备的处理能力越来越强，为通信密钥更复杂、更安全的产生算法提供了支撑；另一方面，随着终端设备普及率的增加，中继设备架设手段的成熟，多方协作干扰是可行的发展方向。人工噪声的加扰、天线设施的支撑以及协作干扰手段的应用，给通信加密提供了多种可行方案。尽管太赫兹通信物理层安全技术正向密钥算法、协同系统2个分支稳步迈进，但就当前的发展情况来看，实现未来太赫兹通信条件下的信息保密传输被硬件设施、软件算法等问题限制，存在理论与技术亟待完善，硬件设施与算法策略发展不同步等问题，仍需投入大量科研来推动理论技术的发展及软硬件研究的突破。

参考文献：

[1] MEI Y,MA Y,MA J,et al. Eavesdropping risk evaluation on terahertz wireless channels in atmospheric turbulencee[J]. IEEE Access, 2021(9):101916-101923.

[2] AKYILDIZ I F,KAK A,NIE S. 6G and beyond:the future of wireless communications systems[J]. IEEE Access, 2020(8):133995-134030.

[3] TATARIA H, SHAFI M, MOLISCH A F, et al. 6G wireless systems: vision, requirements, challenges, insights, and opportunities[J]. Proceedings of the IEEE, 2021,109(7):1166-1199.

[4] HUANG T, YANG W, WU J, et al. A survey on green 6G network: architecture and technologies[J]. IEEE Access, 2019(7): 175758-175768.

[5] 黄开枝,金梁,钟州. 5G物理层安全技术—以通信促安全[J]. 中兴通讯技术, 2019,25(4):43-49. (HUANG Kaizhi,JIN Liang, ZHONG Zhou. 5G physical layer security technology:enhancing security by communication[J]. ZTE Technology Journal, 2019,25 (4):43-49.)

[6] NICANFAR H, JOKAR P, BEZNOSOV K, et al. Efficient authentication and key management mechanisms for smart grid communications[J]. IEEE Systems Journal, 2014,8(2):629-640.

[7] CHEN R, LI C, YAN S, et al. Physical layer security for ultra-reliable and low-latency communications[J]. IEEE Wireless Communications, 2019,26(5):6-11.

[8] PATTANAYAK D R,DWIVEDI V K,KARWAL V,et al. Secure transmission for energy efficient parallel mixed FSO/RF system in presence of independent eavesdroppers[J]. IEEE Photonics Journal, 2022,14(1):1-14.

[9] VUPPALA S,TOLOSSA Y J,KADDOUM G,et al. On the physical layer security analysis of hybrid millimeter wave networks[J]. IEEE Transactions on Communications, 2018,66(3):1139-1152.

[10] WANG W,ZHENG Z. Hybrid MIMO and phased-array directional modulation for physical layer security in mm wave wireless communication[J]. IEEE Journal on Selected Areas in Communications, 2018,36(7):1383-1396.

[11] ZHANG Y, SHEN Y, JIANG X, et al. Secure millimeter-wave ad hoc communications using physical layer security[J]. IEEE Transactions on Information Forensics and Security, 2022(17):99-114.

[12] SUN X,YANG W,CAI Y,et al. Physical layer security in millimeter wave SWIPT UAV-based relay networks[J]. IEEE Access, 2019(7):35851-35862.

[13] EAE E C,ZHANG S J,LIU E J,et al. Advances in vehicular ad-hoc networks:challenges and road-map for future development[J]. International Journal of Automation and Computing, 2016,13(1):1-18.

[14] EMURA K, KANAOKA A, OHATA S, et al. Secure and anonymous communication technique: formal model and its prototype implementation[J]. IEEE Transactions on Emerging Topics in Computing, 2016,4(1):88-101.

[15] BOTTARELLI M,KARADIMAS P,EPIPHANIOU G,et al. Adaptive and optimum secret key establishment for secure vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2021,70(3):2310-2321.

[16] HOLENSTEIN T, RENNER R. One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption[C]// 25th Annual International Cryptology Conference. Berlin,Heidelberg:[s.n.], 2005:478-493.

[17] WENG Z,KANNO A,DAT P T,et al. Millimeter-wave and terahertz fixed wireless link budget evaluation for extreme weather conditions[J]. IEEE Access, 2021(9):163476-163491.

[18] SUOMALAINEN J, JULKU J, VEHKAPER M, et al. Securing public safety communications on commercial and tactical 5G networks:a survey and future research directions[J]. IEEE Open Journal of the Communications Society, 2021,2(1):1590-1615.

[19] 马李翠,黎妹红,吴倩倩,等. 智能电网通信中动态密钥加密方法的研究与改进[J]. 北京邮电大学学报, 2017,40(4):74-79. (MA Licui, LI Meihong, WU Qianqian, et al. Research of dynamic key encryption algorithm in smart grid communication[J]. Journal of Beijing University of Posts and Telecommunications, 2017,40(4):74-79.)

[20] ŠVOGOR I, KiŠASONDI T. Two-factor authentication using EEG augmented passwords[C]// Proceedings of the 34th International Conference on Information Technology Interfaces. Cavtat,Dubrovnik:[s.n.], 2012:373-378.

[21] KONG Y, LYU B, CHEN F, et al. The security network coding system with physical layer key generation in two-way relay networks[J]. IEEE Access, 2018(6):40673-40681.

[22] ZHANG J, WOODS R, DUONG T Q, et al. Experimental study on key generation for physical layer security in wireless communications[J]. IEEE Access, 2016(4):4464-4477.

[23] WANG H, XU L, LIN W, et al. Physical layer security performance of wireless mobile sensor networks in smart city[J]. IEEE Access, 2019(7):15436-15443.

[24] GHAFOOR S, BOUJNAH N, REHMANI M H, et al. MAC protocols for terahertz communication: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020,22(4):2236-2282.

[25] JU S, XING Y, KANHERE O, et al. Millimeter wave and sub-terahertz spatial statistical channel model for an indoor office building[J]. IEEE Journal on Selected Areas in Communications, 2021,39(6):1561-1575.

[26] OSORIOEL D P M, AHMAD L, SANCHEZ J D, et al. Towards 6G-enabled internet of vehicles: security and privacy[J]. IEEE Open Journal of the Communications Society, 2022(3):82-105.

[27] HAO Y,QIU X. MIMO cross-layer secure communication algorithm for cyber physical systems based on interference strategies[J]. IEEE Access, 2020(8):226797-226810.

[28] MA R,YANG W,SUN X,et al. Secure communication in millimeter wave relaying networks[J]. IEEE Access, 2019(7):31218-31232.

[29] 赵伟,宋茂忠. 一种基于多波束与人工噪声的物理层安全通信方法[J]. 电讯技术, 2011,51(7):30-33. (ZHAO Wei,SONG Maozhong. A secure method of physical layer transmission based on multi-beam and artificial noise[J]. Telecommunications Technology, 2011,51(7):30-33.)

[30] XIE Z, GENG X, CHEN Y, et al. Secured green communication scheme for interference alignment based networks[J]. Communications and Networks, 2020,22(1):23-36.

[31] SHARMA K K,BOSE R. Secure communication with energy-harvesting buffer-aided jammer[J]. IEEE Open Journal of the Communications Society, 2021(2):1799-1808.

[32] 胡实,熊俊,马东堂,等. 一种面向无人机通信的协作干扰安全传输技术[J]. 信号处理, 2022,38(7):1525-1534. (HU Shi, XIONG Jun,MA Dongtang,et al. Cooperative interference secure transmission in UAV communication system[J]. Journal of Signal Processing, 2022,38(7):1525-1534.)

[33] FOTOUHI Azade,QIANG Haoran,DING Ming,et al. Survey on UAV cellular communications:practical aspects,standardization advancements, regulation,and security challenges[J]. IEEE Communications Surveys & Tutorials, 2019,21(4):3417-3442.

[34] ALNAGAR S I,SALHAB A M,ZUMMO S A. Q-learning-based power allocation for secure wireless communication in UAV-aided relay network[J]. IEEE Access, 2021(9):33169-33180.

[35] CANG L,ZHAO H,ZHENG G. The impact of atmospheric turbulence on terahertz communication[J]. IEEE Access, 2019(7):88685-88692.

[36] HUANG J,GAO Y,RAIMUNDO X,et al. Rain statistics investigation and rain attenuation modeling for millimeter wave short-range fixed links[J]. IEEE Access, 2019(7):156110-156120.

[37] RAFIQ G, PATZOLD M. The impact of shadowing on the capacity of mobile fading channels[C]// The 4th International Symposium on Wireless Communication Systems. Trondheim:IEEE, 2007:209-214.

[38] SEYEDI Y,SHIRAZI M,MOHARRER A,et al. Use of shadowing moments to statistically model mobile satellite channels in urban environments[J]. IEEE Transactions on Wireless Communications, 2013,12(8):3760-3769.

[39] BADARNEH O S,SOFOTASIOS P C,MUHAIDAT S,et al. Achievable physical-layer security over composite fading channels[J]. IEEE Access, 2020(8):195772-195787.

[40] RAHMAN M M U,ABBASI Q H,CHOPRA N,et al. Physical layer authentication in nano networks at terahertz frequencies for biomedical applications[J]. IEEE Access, 2017(5):7808-7815.

[41] ABBASI Q H,YANG K,CHOPRA N,et al. Nano-communication for biomedical applications:a review on the state-of-the-art from physical layers to novel networking concepts[J]. IEEE Access, 2016(4):3920-3935.

[42] SUN X,DJORDJEVIC I B. Physical-layer security in orbital angular momentum multiplexing free-space optical communications[J]. IEEE Photonics Journal, 2016,8(1):1-10.

[43] AI Y,MATHUR A,CHEFFENA M,et al. Physical layer security of hybrid satellite-FSO cooperative systems[J]. IEEE Photonics Journal, 2019,11(1):1-14.

[44] ZHAO X,CHEN H,SUN J. On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access[J]. IEEE Access, 2018(6):34004-34017.

[45] RAGHAVAN V,LI J. Evolution of physical-layer communications research in the Post-5G era[J]. IEEE Access, 2019(7):10392-10401.

[46] RAPPAPORT T S,XING Y,KANHRE O,et al. Wireless communications and applications above 100 GHz:opportunities and challenges for 6G and beyond[J]. IEEE Access, 2019(7):78729-78757.

作者简介:

吴振东(2000-),男,在读硕士研究生,主要研究方向为太赫兹物理层通信、信号调制识别.mail:wzd187695@163.com.

马建军(1986-),男,博士,教授,博士生导师,主要研究方向为太赫兹信道测量与建模、无线物理层安全.

张玉萍(1976-),女,博士,教授,博士生导师,主要研究方向为太赫兹与激光技术超材料理论与器件.

李德华(1963-),男,博士,教授,主要研究方向为太赫兹科学与技术.