文章编号:1007-5321(2018)05-0069-09 **DOI**:10.13190/j.jbupt.2018-205

面向 5G 的物理层安全技术综述

任品毅, 唐 晓

(1. 西安交通大学 电子与信息工程学院, 西安 710049; 2. 陕西省智慧网络与泛在互联工程技术研究中心, 西安 710049)

摘要: 从 3 个方面对第 5 代移动通信系统(5G)中物理层安全技术的研究和应用进行了回顾,包括 5G 中的新型传输技术与物理层安全技术的结合、5G 新型网络场景下的安全保障以及 5G 中新型安全威胁的应对. 综述了最新的研究成果,指出了尚待解决的问题和未来的研究方向.

关 键 词: 第 5 代移动通信系统; 物理层安全; 毫米波

中图分类号: TN92 **文献标志码**: A

A Review on Physical Layer Security Techniques for 5G

REN Pin-yi, TANG Xiao

(1. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;
2. Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China)

Abstract: Physical layer security techniques exploit the inherent randomness of wireless medium for information security, but which has been significantly challenged by the rapid development and evolvement of the fifth generation of mobile communications system (5G). The research and application of physical layer security techniques in 5G wireless networks was reviewed from three aspects: the joint investigation of physical layer security techniques and the new transmission techniques, the security enhancement schemes under emerging network scenarios, and the countermeasure design against the new threats in 5G wireless networks. Based on the survey of the latest researches in these areas, the open issues and future research directions were discussed.

Key words: the fifth generation of mobile communications system; physical layer security; mmWave

未来第 5 代移动通信系统(5G)将综合利用多种新型无线技术,基于复杂异构的网络构架,为海量数目的连接、多种多样的无线业务和呈指数增长的数据流量提供支持[1-2]. 信息安全作为通信的基础和前提,正凸显出前所未有的重要性. 物理层安全技术基于无线信道的随机特性,无需密钥即可保证信息论意义上的完美安全,并且能够在实际系统中便捷地实现[3]. 目前,相关研究已取得了丰硕的成果,极大地促进了理论的发展和技术的进步. 近年来,基于 5G 的新特点和新需求,针对物理层安全技术进行了进一步研究,产生了新的研究成果[4-5]. 笔者首先回顾了物理层安全的基本原理,其次从 3 个方面对 5G 中物理层安全的研究进行了调研,包括新型传输技术与物理层安全技术的结合、新型网络场景下的安全策略和针对新型安全威胁的安全方案. 总结了最新的研究成果,指出了未来的研究方向.

收稿日期: 2018-08-20

基金项目: 陕西省重点研发计划重点项目(2017ZDXM-GY-012); 国家自然科学基金重点项目(61431011)

作者简介: 任品毅(1971—), 男, 教授, 博士生导师; 唐 晓(1988—), 男, 博士生, E-mail: xiaotang@stu.xjtu.edu.cn.

1 物理层安全的基本原理

1.1 物理层安全的基本概念

物理层安全的核心思想是利用无线信道的随机性,如干扰、衰落和噪声等以实现安全传输. 相关理论研究起始于 Claude Shannon[6] 的先驱工作,建立了完美私密的概念. 完美私密定义如下

$$I(M;C)=0 \tag{1}$$

其中:M 为发送端消息,C 为加密后的信息也即窃听者的观察,完美私密要求 M 和 C 之间的互信息为零. 如果完美私密条件成立,那么对窃听者而言,从加密后的信息恢复原始信息的最好方法即随机猜测. Wyner[7] 提出了窃听信道模型,考虑窃听者接收到的信息是合法接收信息的退化版本. 具体来说,合法用户发射机将消息 M 以速率 R 和长度 n 进行编码形成码字 X^n,合法接收机和窃听者的接收码字分别为 Y^n 和 Z^n. 如果以下条件成立,则可以实现私密速率 R

$$\lim_{n\to\infty}\Pr(\hat{M}\neq M)=0 \tag{2}$$

$$\lim_{n\to\infty}I(M;Z^n)=0 \tag{3}$$

其中 $\hat{M}$ 代表合法接收机对于 M 的估计. 在以上条件中,式(2)表示可靠性条件,即合法用户可以恢复原始信息;式(3)表示安全性条件,即窃听者无法获取关于原始消息的任何信息. 从 Wyner 模型的角度,当且仅当窃听信道条件比合法传输主信道条件差时,可以实现物理层安全. 无信通信中的各种随机因素,包括干扰、衰落和噪声等,可以被充分利用以建立起合法传输的相对优势进而实现安全. 这一思想催生了多种多样的物理层安全技术,以下对经典的安全机制进行回顾.

1.2 人工噪声设计

人工噪声注入是指在传输的同时生成一个额外的干扰信号,该干扰信号只对窃听端有影响而不会影响合法接收端,通过降低窃听链路的容量来提升私密容量[8-9]. 在实际中,合法用户可以合理利用自身的部分功率以发射人工噪声. 相关研究表明,只要合法发射机的天线数多于窃听端天线数,即在使窃听端相比合法接收端距离合法发射机更近的情况下,也能实现非负的私密速率. 容易看到,在基于人工噪声的方法中,由于发射人工噪声需要消耗部分功率,故而会对安全传输造成负面影响. 因此,相关工作以私密速率为导向,研究了针对有用信息和人工噪声的最优功率问题[10].

1.3 安全波束赋形设计

多天线传输可以利用空间自由度进行波束赋形以使得合法发射机的信号只在特定的方向上被合法接收机有效地接收,以减少甚至完全避免被窃听端所接收,进而提升安全传输性能[11]. 在部分信息的情况下,可以相应地引入稳健波束赋形设计. 此外,还可以利用基于多天线技术的波束赋形和人工噪声联合设计以提升安全传输性能[12-13].

1.4 协作安全策略

合法用户还可以借助于外界的辅助节点利用协作分集以提升合法传输的安全性[14-15]. 例如,来自中继节点(如放大转发或者解码转发等)的协作传输可以提升合法传输的性能,但同时也有提升窃听性能的风险. 在此,协作中继节点(和合法发射端)可以进行分布式的波束赋形,使合法传输具有更好的方向性,进而提升安全性能. 同样地,协作也可以来自协作干扰源,通过这些额外的干扰源,对窃听者进行干扰,降低窃听链路的性能进而提升安全性. 在相关的研究工作中,也有很多是基于对协作中继和干扰源的联合安全机制设计,即同时由协作中继提升合法链路传输性能而利用干扰源降低窃听链路性能,以更好地利用协作分集来保障合法用户的安全传输[16-17].

1.5 物理层密钥生成

在实际无线通信中,可能缺乏合适的条件来建立合法传输链路的优势或者因窃听者位置不可知导致无法评估合法传输的链路优势,此时可以利用密钥以提升安全性[18-19]. 物理层密钥生成技术基于无线信道的互易性,合法用户的收发端可以基于对收发链路的观察生成相应的密钥. 密钥基于无线信道的随机性建立,而无需中心节点的密钥分发. 无线信道的随机性保证了合法传输双方可以动态地生成密钥. 与此同时,只要窃听端位于合法收发端的安全距离之外,即可保证窃听端无法获得与合法链路相关的信道特征,进而无法获取密钥.

2 5G 网络中物理层安全的挑战

物理层安全的相关研究经过多年的发展,已经取得了丰硕的研究成果. 这些研究为物理层安全技术提供了很多深刻的思想和有效的方法. 但是,物理层安全的研究远未尽善尽美,尤其近年来在 5G 无线通信和网络技术快速发展的背景下,无线安全

面临着诸多亟待解决的新问题，形成了对传统物理层安全技术的新挑战. 在此主要从以下几个方面进行总结.

1）物理层安全技术与新型传输技术的联合研究. 5G 的萌芽带来了多种新型无线传输技术，如大规模 MIMO（MaMIMO，massive multiple input and multiple output）、毫米波（Millimeter Wave，mm-Wave）通信、非正交接入（NOMA，non-orthogonal multiple access）、全双工（Full-Duplex）通信等. 这些技术的应用为 5G 中高速率、大连接、低延迟的无线服务提供了有力的支持，却无法为信息的安全传输提供保护. 为此需要将这些技术与物理层安全技术进行联合研究，以在保证用户服务质量的同时，提供信息的安全保障.

2）新型无线网络场景下的安全传输机制. 5G 的发展衍生了多种新型无线场景，典型的如 5G 中所定义的增强移动宽带通信、大规模机器通信、高可靠低时延通信这三类场景，抑或 Ad Hoc 网络、异构网、车联网等特定的网络场景. 不同场景下的用户需求和无线业务大相径庭，因此物理层安全技术的相关研究需要针对不同的用户需求和业务特点设计相应的安全策略.

3）针对新型安全威胁的物理层安全技术. 5G 的发展带来了多种无线技术，其在提升合法用户性能的同时，也可能被恶意用户所利用，进而形成更为严峻的安全威胁. 为此，物理层安全技术需要应对潜在的新型安全威胁，进而形成可靠的安全防御.

3　面向 5G 网络的物理层安全研究

3.1　物理层安全技术与新型传输技术的联合研究

5G 为了满足大连接、高速率的服务需求，引入了多种新型无线传输技术，包括大规模 MIMO、毫米波、非正交接入、全双工等. 相关研究将物理层安全技术与这些新型传输技术相结合，实现了信息的安全传输.

大规模 MIMO 技术可以显著提升无线信号传输的空间自由度，在提高频谱效率的同时有效地降低功率开销[20]. Zhu 等[21]利用了大规模 MIMO 技术在多小区网络中设计了安全传输策略，其联合利用了线性预编码和人工噪声技术，针对不同的信号预编码设计了相应的人工噪声预编码器. 在考虑导频污染和非完美信道测量的条件下，研究了多小区大规模 MIMO 系统中的安全传输问题，设计了随机人工噪声方案以实现性能和复杂度的折中[22]. Asaad 等[23]以安全传输为导向研究了大规模 MIMO 系统中的天线选择机制. 研究表明，针对特定场景，安全性能并非始终随着天线数目的增加而提升. 因此，在大规模 MIMO 系统中使用天线选择够在降低射频端的复杂度的同时提升安全性能. Chen 等[24]考虑了大规模 MIMO 中继节点在解码转发协议下的安全传输问题，联合研究了合法用户发射功率、中继传输功率和两跳时间分配策略. Wang 等[25]针对基于大规模 MIMO 系统的云接入网络，研究了安全传输和能效优化问题，利用软频率复用以降低系统中的干扰，同时提升了网络的安全性能和传输的能量效率. Guo 等[26]研究了多用户大规模 MIMO 系统中的安全传输问题. 在多个大规模 MIMO 基站组成的分布式天线系统进行协作传输的条件下，研究了以安全传输为约束的功率分配策略.

毫米波通信具有波长极短而带宽极大的特点，其无线信号的波束很窄，具有很好的方向性，可以实现很高的天线增益，在视距传播条件下具有极好的性能，同时提供了大量的可用频谱资源[27-28]. 其能够在 5G 时代为用户提供极高速率的数据服务，为多媒体、移动视频、在线游戏等业务提供有力的支持. 然而，由于毫米波通信与传统的 6 GHz 以下频段的通信面临着不同的传播性能和衰落特性，其安全传输也面临着诸多亟待解决的问题. Huang 等[29]利用毫米波波长短而空间稀疏的特性设计了混合的数字-模拟域预编码，具有良好的方向性，以在多用户传输场景中实现很好的抗窃听性能. Vuppala 等[30]研究了毫米波通信和微波通信共存的无线网络中的安全性能，基于各自的衰落特性和传播模型，综合分析了混合网络下连接中断概率、安全中断概率和平均私密速率，并基于上述分析给出了用户端的网络选择策略. Ramadan 等[31]研究了部分信道状态信息条件下多输入单输出毫米波通信系统中的混合数字-模拟域安全预编码问题. 通过对窃听信干噪比的分析，推得了私密速率的下界，进一步设计而人工噪声预编码方案以最大化私密速率的下界. Eltayeb 等[32]研究了车载网中利用毫米波通信提高安全性的技术，在单天线通信保证合法接收的同时，使得非法接收端只能收到类噪声的信号，而在多天线的条件下则可以适时地发射人工噪声以降低非法接收端的性能，同时降低系统中的干扰水平. Zhu 等[33]研究了毫米波通信在 Ad hoc 网络安全通信中

的应用,考虑了毫米波通信的信道特性、随机障碍物和天线增益,在窃听者随机分布的条件下分析了网络的安全性能,进一步探讨了人工噪声的应用对安全性能的提升. Wang 等[34]针对毫米波通信中的物理层安全问题,提出一种混合 MIMO 相控和时间调制的方向性传输策略. 在 MIMO 相控的同时利用了空间分集和相控阵的相干方向增益. 通过将天线阵分为若干子阵,各子阵实现了方向性传输,同时多个子阵形成 MIMO 以实现更好的角度分辨率,由基于时间调制的方向调制实现了安全通信.

非正交接入技术允许不同的用户的信号在功率域进行叠加,通过接收端的串行干扰消除以对不同用户的信号进行区分. 非正交接入技术可以显著地提升频谱效率进而提高系统吞吐量,同时允许接入更多的用户以增强网络覆盖,为 5G 系统的大连接高速率通信提供强有力的支持[35]. Lv 等[36]针对多输入单输出非正交接入系统提出了一种安全波束赋形机制,利用人工噪声降低了窃听性能,进而保护了非正交接入的合法用户的安全传输,进一步分析了在非理想干扰消除的情况下安全中断概率. Liu 等[37]基于随机几何理论研究了大规模网络中非正交接入条件下的物理层安全问题. 提出建立保护区域以在单天线传输的条件下保障安全,在多天线传输条件下利用人工噪声以降低窃听性能,并分析了相应的安全中断概率. Lei 等[38]在单输入单输出和基于天线选择的多输入单输出场景下,针对下行非正交接入条件下的两用户传输问题进行了安全性能分析. 基于对安全中断概率的分析,给出了相应的天线选择方案,进一步基于信道增益较高条件下的渐进分析,给出了保证分集阶数非零的天线选择机制. He 等[39]联合考虑了解码阶数、传输速率和功率分配的优化提出了一种非正交接入策略, 以合法用户的安全中断概率为约束,联合考虑上述因素以实现最低功耗的传输. Chen 等[40]关注了基于协作的非正交接入系统中物理层安全问题,分析了放大转发和解码转发协议下的安全中断概率和正私密速率的概率. Xu 等[41]研究了基于非正交接入的认知无线网络中时延约束条件下的资源分配问题,联合考虑时延约束、次级用户数目、次级用户功耗和次级用户对主用户的干扰限制设计了安全传输策略.

全双工技术使得用户可以进行同时同频的通信,具有实现双倍频谱效率潜力,可以有效地提高用户的传输性能[42]. 但是受限于器件的硬件水平,全双工通信会在用户自身产生自干扰,进而影响传输性能. Zhu 等[43]针对全双工基站研究了基于自干扰抑制的安全波束赋形方案,提出了基于目标合法传输信干噪比和窃听信干噪比约束的发射功率最小化的方案. Sun 等[44]研究了全双工基站服务的多用户系统中,同时进行上下行传输情况下的安全传输问题. 以上下行用户的安全服务质量为约束,建立了多目标优化问题以在保证安全的前提下线,同时最小化上行链路和下行链路的传输功率. Mahmood 等[45]详尽地分析了全双工通信中的遍历安全容量和安全自由度. Tang 等[46]综合利用了协作干扰源和全双工接收机以增强下行传输的安全性,利用协作干扰和全双工接收机发射人工噪声以降低窃听性能. 基于对连接性和安全性的理论分析,给出了一种协作干扰源选择方案以在满足安全性约束的条件下提升连接性能. Tian 等[47]从跨层优化的角度研究了全双工多跳网络中的安全传输问题,其联合考虑了全双工传输约束、安全性能约束和安全信息流约束,进而建立了安全传输模型并给出了相应的安全传输策略. Chen 等[48]研究了全双工中继系统中的安全传输性能,研究表明在自干扰充分消除的条件下,全双工传输相比半双工传输可以显著提升安全性能,同时提出了一种利用全双工进行协作干扰的方案,并对安全中断概率进行了分析. Parsaeefard 等[49]研究了全双工中继协作传输下的安全传输问题,分别考虑了全双工中继进行同时接收和转发或者同时接收和协作干扰两种情况下的安全传输性能,并分别给出了相应的功率分配算法. Wang 等[50]研究了信能同传全双工系统中的安全传输问题,全双工基站同时进行上行和下行传输,同时空闲用户进行能量接收. 提出发射人工噪声信号以防止空闲用户进行窃听并同时提升空闲用户的能量接收水平,联合设计了合法信号相关矩阵、人工噪声相关矩阵和接收矢量以最大化上下行加权和私密速率. Bi 等[51]考虑了能量受限的全双工协作干扰节点,其需要通过无线能量收集以对协作干扰进行供能. 基于自身电池状态和能量收集的情况,协作干扰节点可以进行专一的能量收集或者机会的能量收集,以实现无线供能条件下最优的协作干扰性能.

3.2 面向新型网络场景的安全策略

无线网络的持续发展和不断演进使得网络呈现出越来越强的复杂性和异构性. 同时,由于多种多样的新型无线业务的提供,出现了多种新型网络场

景. 在 5G 中安全传输需要在针对特定的通信场景进行设计,以为无线业务的安全性和服务质量提供可靠的保障.

5G 是由多种不同的基础设施构成的异构网,为用户提供高速的数据传输和无缝的接入. 因此,安全策略需要针对网络的异构性进行有针对性的设计. Lv 等[52]研究了宏蜂窝系统和毫微微蜂窝系统共存下的安全传输波束赋形方案. 在正交频率分配和部分频率复用的条件下,给出了安全性能最优的波束赋形方案. Zhong 等[53]基于随机几何理论研究了多层异构网络场景下的物理层安全问题,在考虑跨层干扰的条件下,分析了用户的私密速率并推导了安全中断概率的上界和下界. Wang 等[54]针对多层动态异构网络,在联合考虑基站位置随机分布和用户随机到达离去的条件下,研究了安全传输问题. 在三维随机模型下,对用户的连接中断概率和安全中断概率进行了分析,并给出了私密吞吐量最优的资源分配方案. Tang 等[55]研究了安全传输用户和常规用户共存的异构网络,不同用户之间进行分布式的资源竞争,提出了一种基于优先级的安全传输策略,显著增强了高优先级的安全用户的传输性能. Wang 等[56]考虑了 6 GHz 以下微波网络和毫米波网络共存的异构超密集网络,联合考虑了物理层安全技术、缓存技术和无线能量收集技术,展示了异构网络在多方面的巨大潜力.

物联网在 5G 时代为海量节点接入提供了可能. 近期很多研究工作关注了物联网场景下的安全传输问题. Jia 等[57]针对物联网通信提出了一种双重非正交传输方案,联合利用非正交复用和非正交接入以显著提升频谱效率,其中非正交复用加入了安全性的考量以提升传输安全性. Hu 等[58]研究了存在大量窃听者的场景下的物联网安全传输问题,联合利用了发射机的人工噪声设计和协作干扰机制,在目标私密速率约束条件下最小化安全中断概率. Xu 等[59]考虑物联网中存在着数量和位置都无法确知的窃听者,合法用户在随机-转发中继协议下实现多跳安全传输,提出了一种联合的功率和码字速率分配策略以在中断概率的约束下最大化私密速率. Atat 等[60]研究了移动医疗场景中移动设备和生物传感器之间的安全通信问题,分析了安全通信范围和平均端到端时延. Xu 等[61]研究了放大转发协议下物联网通信,通过人工噪声辅助的波形设计以在多径衰落的条件下实现安全传输.

5G 中的新型传输技术也在不断驱动着新型场景的产生,典型的如全双工通信网络和无人机通信网络,其安全议题同样受到了广泛的关注. Tang 等[62]研究了全双工通信网络中的分布式资源竞争问题,提出了一种分布式的功率分配算法,具有良好收敛性,同时提升了系统的平均安全性能. Wang 等[63]提出利用无人机作为移动中继以辅助合法用户的安全传输. Lee 等[64]研究了无人机与多个地面节点之间的安全通信问题,利用其他无人机节点进行协作干扰以提升安全性. 通过联合的飞行轨迹、功率分配和用户调度优化,实现了最差私密速率的最大化. Zhao 等[65]研究了无人机和小小区基站在缓存技术的支持下为用户提供高速数据传输场景下的安全问题. 设计了干扰对齐方案以避免相互干扰,提出在无人机通信的同时由小小区基站进行协作干扰以保证安全性.

3.3　针对新型威胁的安全方案

5G 带来了多种新技术,其一方面有助于合法用户传输性能和安全性能的提升,另一方面也可能被恶意用户所利用形成新的安全威胁,对此需要设计相应的措施以保证安全传输.

对于单一窃听者而言,其在全双工技术或者多天线技术的加持下,会形成更严峻的安全威胁. Tang 等[66]针对基于全双工技术的主动窃听攻击进行了研究,主动窃听者在窃听的同时发起干扰攻击以提升自身的窃听性能. 基于博弈建模和均衡分析分别为合法用户和主动窃听者给出了最优的传输策略和干扰策略. Abedi 等[67]针对全双工主动窃听者,引入了全双工合法接收机以在合法接收的同时对窃听者进行干扰. 在考虑信道状态信息误差的条件下,提出了一种稳健的功率分配策略以最大化最差情况下的私密速率. Li 等[68]研究了相似场景下的安全问题,其以安全自由度最大化为目标设计了全双工接收端的发射/接收天线分配策略. Xu 等[69]研究了非正交接入系统中,窃听者利用全双工技术在进行串行干扰消除实施窃听的同时进行干扰攻击的安全问题. 提出利用时间信道传输以对抗干扰攻击并提升安全性能. Chen 等[70]针对大规模 MIMO 窃听者,提出了一种基于原始符号相位旋转的安全策略. 通过对原始符号的随机相位旋转,使得窃听者难以分辨真实有效的信号.

随着无线设备通信和计算能力的提升,多个窃听者之间可以进行共谋以联合对合法传输实施更为

有效的攻击. Babaei 等[71]考虑了全双工小小区网络在多个窃听者进行被动窃听和共谋窃听场景下的安全问题,共谋窃听基于合并结果对安全传输形成显著的威胁. 研究了利用保护域内的用户端串行干扰消除和在基站端自干扰消除条件下的安全传输性能. Pinto 等[72]研究了多个窃听者进行协作和合并情况下的安全传输问题,基于图论分析了网络的安全性能,明确了窃听者在共谋条件下相比独立窃听情况下的安全性能下降程度. Vuppala 等[73]研究了网络中随机分布的窃听者之间的共谋,通过对窃听者位置和信道状态的近似,对私密速率的分布和安全中断概率进行了渐进分析. Jiang 等[74]研究了上行非正交接入系统中多个窃听者独立窃听和进行共谋情况下的安全传输问题,分析了合法用户联合利用串行干扰消除和最小均方误差解码条件下的私密速率和安全中断概率.

无线设备的智能化水平近年来得到显著的提高,催生了更为灵活多样的攻击类型. Wang 等[75]考虑网络中的恶意用户可以在被动窃听和主动攻击之间进行自适应的切换以最大化攻击效果. 基于随机几何的建模,给出了攻击类型切换的条件. Xiong 等[76]研究了恶意用户在信道训练阶段进行导频污染攻击以促进其在信息传输阶段的窃听,提出了一种双向训练机制以对导频污染进行检测并降低安全性能的损失. Xu 等[77]针对导频污染攻击提出了一种基于码字-频率块分组的导频鉴定方案,导频信息被转化成为了码字-频率空间的模式. 通过对不同模式的识别和区分,可以有效地对合法用户和攻击者的导频进行鉴别. Tang 等[78]研究了反应式干扰攻击下的安全传输问题,考虑反应式干扰者基于对合法传输的监测确定干扰策略,提出利用攻击者检测的非完美特性设计了相应的安全传输策略.

4 结束语

物理层安全技术为 5G 中的信息安全提供了高效可靠的解决方案. 本文以 5G 无线网络的新特性为立足点,回顾了面向 5G 的物理层安全技术研究的最新进展和成果. 尽管现有的研究已经给出了多种有效的安全策略,但是由于 5G 的复杂性,现有研究尚难以为 5G 提供全方位的安全防护,还有大量的研究工作尚需开展. 此外,以下研究主题也是值得关注的. 一是物理层安全技术与加密技术的联合设计,旨在实现内容层面和传输层面的跨层安全体系;二是针对不同无线业务引入安全等级设计,以实现精细化的安全管理;三是智能化的安全策略,针对层出不穷的安全威胁建立起学习机制,以实现安全策略的自我进化和自适应的安全防御体系.

参考文献:

[1] Andrews J G, Buzzi S, Choi W, et al. What will 5G be? [J]. IEEE J Sel Areas Commun, 2014, 32(6): 1065-1082.

[2] Wang C X, Haider F, Gao X, et al. Cellular architecture and key technologies for 5G wireless communication networks[J]. IEEE Commun Mag, 2014, 52(2): 122-130.

[3] Mukherjee A, Fakoorian S A A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: a survey[J]. IEEE Commun Surveys & Tuts, 2014, 16(3): 1550-1573.

[4] Wu Y, Khisti A, Xiao C, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead[J]. IEEE J Sel Areas Commun, 2018, 36(4): 679-695.

[5] Sun L, Du Q. Physical layer security with its applications in 5G networks: a review[J]. China Commun, 2017, 14(12): 1-14.

[6] Shannon C E. Communication theory of secrecy systems [J]. The Bell Sys Tech J, 1949, 28(4): 656-715.

[7] Wyner A D. The wire-tap channel[J]. The Bell Sys Tech J, 1975, 54(8): 1355-1387.

[8] Zhou X, Mckay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Trans Veh Technol, 2010, 59(8): 3831-3842.

[9] Wang B, Mu P, Li Z. Artificial-noise-aided beamforming design in the MISOME wiretap channel under the secrecy outage probability constraint[J]. IEEE Trans Wireless Commun, 2017, 16(11): 7207-7220.

[10] Li N, Tao X, Xu J. Artificial noise assisted communication in the multiuser downlink: optimal power allocation [J]. IEEE Commun Lett, 2015, 19(2): 295-298.

[11] Chen X, Ng D W K, Gerstacker W, et al. A survey on multiple-antenna techniques for physical layer security [J]. IEEE Commun Surveys & Tuts, 2017, 19(2): 1027-1053.

[12] Zhang G, Li X, Cui M, et al. Signal and artificial noise beamforming for secure simultaneous wireless information and power transfer multiple-input multiple-output relaying systems[J]. IET Commun, 2016, 10(7): 796-

804.

[13] Wu Y, Chen X, Chen X. Secure beamforming for cognitive radio networks with artificial noise[C] // Proc WCSP. Nanjing China: IEEE, 2015: 1-5.

[14] Sendonaris A, Erkip E, Aazhang B. User cooperation diversity. part I. system description[J]. IEEE Trans Commun, 2003, 51(11): 1927-1938.

[15] Wang W, Teh K C, Li K H. Generalized relay selection for improved security in cooperative DF relay networks [J]. IEEE Wireless Commun Lett, 2016, 5(1): 28-31.

[16] Hui H, Swindlehurst A L, Li G, et al. Secure relay and jammer selection for physical layer security[J]. IEEE Signal Process Lett, 2015, 22(8): 1147-1151.

[17] Guo H, Yang Z, Zhang L, et al. Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks[J]. IEEE Access, 2017(5): 19620-19630.

[18] Chou T H, Draper S C, Sayeed A M. Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage[J]. IEEE J Sel Areas Commun, 2013, 31(9): 1751-1764.

[19] Im S, Choi J, Ha J. Secret key agreement for massive MIMO systems with two-way training under pilot contamination attack[C] // Proc GC Wkshps. San Diego, USA: IEEE, 2015: 1-6.

[20] Molisch A F, Ratnam V V, Han S, et al. Hybrid beamforming for massive MIMO: a survey[J]. IEEE Commun Mag, 2017, 55(9): 134-141.

[21] Zhu J, Schober R, Bhargava V K. Linear precoding of data and artificial noise in secure massive MIMO systems [J]. IEEE Transa Wireless Commun, 2016, 15(3): 2245-2261.

[22] Zhu J, Schober R, Bhargava V K. Secure transmission in multicell massive MIMO systems[J]. IEEE Transa Wireless Commun, 2014, 13(9): 4766-4781.

[23] Asaad S, Bereyhi A, Rabiei A M, et al. Optimal transmit antenna selection for massive MIMO wiretap channels[J]. IEEE J Sel Areas Commun, 2018, 36(4): 817-828.

[24] Chen J, Chen X, Gerstacker W H, et al. Resource allocation for a massive MIMO relay aided secure communication[J]. IEEE Trans Inf Forensics Sec, 2016, 11(8): 1700-1711.

[25] Wang L, Wong K, Elkashlan M, et al. Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: a new look at interference[J]. IEEE J Sel Topics Signal Process, 2016, 10(8): 1375-1389.

[26] Guo K, Guo Y, Ascheid G. Security-constrained power allocation in MU-massive-MIMO with distributed antennas[J]. IEEE Trans Wireless Commun, 2016, 15(12): 8139-8153.

[27] Zhang R, Cai L, Zhong Z, et al. Cross-polarized three-dimensional channel measurement and modeling for small-cell street canyon scenario[J]. IEEE Trans Veh Technol, 2018, 67(9): 7969-7983.

[28] Hemadeh I A, Satyanarayana K, El-Hajjar M, et al. Millimeter-wave communications: physical channel models, design considerations, antenna constructions, and link-budget[J]. IEEE Commun Surveys & Tuts, 2018, 20(2): 870-913.

[29] Huang Y, Zhang J, Xiao M. Constant envelope hybrid precoding for directional millimeter-wave communications[J]. IEEE J Sel Areas Commun, 2018, 36(4): 845-859.

[30] Vuppala S, Tolossa Y J, Kaddoum G, et al. On the physical layer security analysis of hybrid millimeter wave networks[J]. IEEE Trans Commun, 2018, 66(3): 1139-1152.

[31] Ramadan Y R, Minn H. Artificial noise aided hybrid precoding design for secure mmWave MISO systems with partial channel knowledge[J]. IEEE Signal Process Lett, 2017, 24(11): 1729-1733.

[32] Eltayeb M E, Choi J, Al-Naffouri T Y, et al. Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems[J]. IEEE Trans Veh Technol, 2017, 66(9): 8139-8151.

[33] Zhu Y, Wang L, Wong K, et al. Secure communications in millimeter wave ad hoc networks[J]. IEEE Transa Wireless Commun, 2017, 16(5): 3205-3217.

[34] Wang W, Zheng Z. Hybrid MIMO andphased-array directional modulation for physical layer security in mmWave wireless communications[J]. IEEE J Sel Areas Commun, 2018, 36(7): 1383-1396.

[35] Islam S M R, Avazov N, Dobre O A, et al. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges[J]. IEEE Commun Surveys & Tuts, 2017, 19(2): 721-742.

[36] Lv L, Ding Z, Ni Q, et al. Secure MISO-NOMA transmission with artificial noise[J]. IEEE Trans Veh Technol, 2018, 67(7): 6700-6705.

[37] Liu Y, Qin Z, Elkashlan M, et al. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks[J]. IEEE Transa Wireless Com-

mun, 2017, 16(3): 1656-1672.

[38] Lei H, Zhang J, Park K, et al. On secure NOMA systems with transmit antenna selection schemes[J]. IEEE Access, 2017(5): 17450-17464.

[39] He B, Liu A, Yang N, et al. On the design of secure non-orthogonal multiple access systems[J]. IEEE J Sel Areas Commun, 2017, 35(10): 2196-2206.

[40] Chen J, Yang L, Alouini M. Physical layer security for cooperative NOMA systems[J]. IEEE Trans Veh Technol, 2018, 67(5): 4645-4649.

[41] Xu L, Nallanathan A, Pan X, et al. Security-aware resource allocation with delay constraint for NOMA-Based cognitive radio network[J]. IEEE Trans Inf Forensics Sec, 2018, 13(2): 366-376.

[42] Kim D, Lee H, Hong D. A survey of in-band full-duplex transmission: from the perspective of PHY and MAC layers[J]. IEEE Commun Surveys & Tuts, 2015, 17(4): 2017-2046.

[43] Zhu F, Gao F, Zhang T, et al. Physical-layer security for full duplex communications with self-Interference mitigation[J]. IEEE Transa Wireless Commun, 2016, 15(1): 329-340.

[44] Sun Y, Ng D W K, Zhu J, et al. Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems[J]. IEEE Transa Wireless Commun, 2016, 15(8): 5511-5526.

[45] Mahmood N H, Ansari I S, Popovski P, et al. Physical-Layer security with full-duplex transceivers and multiuser receiver at eve[J]. IEEE Trans Commun, 2017, 65(10): 4392-4405.

[46] Tang W, Feng S, Ding Y, et al. Physical layer security in heterogeneous networks with jammer selection and full-duplex users[J]. IEEE Transa Wireless Commun, 2017, 16(12): 7982-7995.

[47] Tian F, Chen X, Liu S, et al. Secrecy rate optimization in wirelessmulti-hop full duplex networks[J]. IEEE Access, 2018(6): 5695-5704.

[48] Chen G, Gong Y, Xiao P, et al. Physical layer network security in the full-duplex relay system[J]. IEEE Trans Inf Forensics Sec, 2015, 10(3): 574-583.

[49] Parsaeefard S, Le-Ngoc T. Improving wireless secrecy rate via full-duplex relay-assisted protocols[J]. IEEE Trans Inf Forensics Sec, 2015, 10(10): 2095-2107.

[50] Wang Y, Sun R, Wang X. Transceiver design to maximize the weighted sum secrecy rate infull-duplex SWIPT systems[J]. IEEE Signal Process Lett, 2016, 23(6): 883-887.

[51] Bi Y, Chen H. Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer[J]. IEEE J Sel Topics Signal Process, 2016, 10(8): 1538-1550.

[52] Lv T, Gao H, Yang S. Secrecy transmit beamforming for heterogeneous networks[J]. IEEE J Sel Areas Commun, 2015, 33(6): 1154-1170.

[53] Zhong Z, Peng J, Luo W, et al. A tractable approach to analyzing the physical-layer security in K-tier heterogeneous cellular networks[J]. China Commun, 2015, 12(Sup): 166-173.

[54] Wang B, Huang K, Xu X, et al. Resource allocation for secure communication in K-tier heterogeneous cellular networks: a spatial-temporal perspective[J]. IEEE Access, 2018(6): 772-782.

[55] Tang X, Ren P, Han Z. Hierarchical competition as equilibrium program with equilibrium constraints towards security-enhanced wireless networks[J]. IEEE J Sel Areas Commun, 2018, 36(7): 1564-1578.

[56] Wang L, Wong K, Jin S, et al. A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks[J]. IEEE Commun Mag, 2018, 56(6): 49-55.

[57] Jia M, Li D, Yin Z, et al. High spectral efficiency secure communications with non-orthogonal physical and multiple access layers[J]. IEEE Internet Things J, 2018.

[58] Hu L, Wen H, Wu B, et al. Cooperative jamming for physical layer security enhancement in Internet of things[J]. IEEE Internet Things J, 2018, 5(1): 219-228.

[59] Xu Q, Ren P, Song H, et al. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations[J]. IEEE Access, 2016, 4: 2840-2853.

[60] Atat R, Liu L, Ashdown J, et al. A physical layer security scheme for mobile health cyber-physical systems[J]. IEEE Internet Things J, 2018, 5(1): 295-309.

[61] Xu Q, Ren P, Song H, et al. Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions[J]. IEEE Internet Things J, 2017, 4(6): 1924-1933.

[62] Tang X, Ren P, Han Z. Distributed power optimization for security-aware multi-channel full-duplex communications: a variational inequality framework[J]. IEEE Trans Commun, 2017, 65(9): 4065-4079.

[63] Wang Q, Chen Z, Mei W, et al. Improving physical layer security using UAV-enabled mobile relaying[J].

IEEE Wireless Commun Lett, 2017, 6(3): 310-313.

[64] Lee H, Eom S, Park J, et al. UAV-aided secure communications with cooperative jamming[J]. IEEE Trans Veh Technol, 2018, 67(10): 9385-9392.

[65] Zhao N, Cheng F, Yu F R, et al. Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment[J]. IEEE Trans Commun, 2018, 66(5): 2281-2294.

[66] Tang X, Ren P, Wang Y, et al. Combatingfull-duplex active eavesdropper: a hierarchical game perspective [J]. IEEE Trans Commun, 2017, 65(3): 1379-1395.

[67] Abedi M R, Mokari N, Saeedi H, et al. Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: active adversary[J]. IEEE Transa Wireless Commun, 2017, 16(2): 885-899.

[68] Li L, Petropulu A P, Chen Z. MIMO secret communications against an active eavesdropper[J]. IEEE Trans Inf Forensics Sec, 2017, 12(10): 2387-2401.

[69] Xu D, Ren P, Lin H. Combat hybrid eavesdropping inpower-domain NOMA: joint design of timing channel and symbol transformation[J]. IEEE Trans Veh Technol, 2018, 67(6): 4998-5012.

[70] Chen B, Zhu C, Li W, et al. Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper[J]. IEEE Access, 2016(4): 3016-3025.

[71] Babaei A, Aghvami A H, Shojaeifard A, et al. full-duplex small-cell networks: a physical-layer security perspective[J]. IEEE Trans Commun, 2018, 66(7): 3006-3021.

[72] Pinto P C, Barros J, Win M Z. Secure communication in stochastic wireless networks—part II: maximum rate and collusion[J]. IEEE Trans Inf Forensics Sec, 2012, 7(1): 139-147.

[73] Vuppala S, Abreu G. Asymptotic secrecy analysis of random networks with colluding eavesdroppers [J]. IEEE Systems Journal, 2018, 12(1): 871-880.

[74] Jiang K, Jing T, Huo Y, et al. SIC-based secrecy performance in uplink NOMA multi-eavesdropper wiretap channels[J]. IEEE Access, 2018, 6: 19664-19680.

[75] Wang W, Teh K C, Li K H, et al. On the impact of adaptive eavesdroppers inmulti-antenna cellular networks [J]. IEEE Trans Inf Forensics Sec, 2018, 13(2): 269-279.

[76] Xiong Q, Liang Y, Li K H, et al. Secure transmission against pilot spoofing attack: a two-way training-based scheme[J]. IEEE Trans Inf Forensics Sec, 2016, 11(5): 1017-1026.

[77] Xu D, Ren P, Ritcey J A, et al. Code-frequency block group coding for anti-spoofing pilot authentication in multi-antenna OFDM systems [J]. IEEE Trans Inf Forensics Sec, 2018, 13(7): 1778-1793.

[78] Tang X, Ren P, Han Z. Jamming mitigation via hierarchical security game for IoT communications[J]. IEEE Access, 2018(6): 5766-5779.