

6G 网络安全场景分析及安全模型研究

张成磊, 付玉龙, 李晖, 曹进

(西安电子科技大学网络与信息安全学院, 陕西 西安 710126)

摘要: 6G 网络的概念已经被提出并引起了学术界的广泛关注。整体而言, 6G 网络将对 5G 网络的性能进行优化, 并拓展 5G 技术难以实现的业务场景。然而, 这些新场景、新技术的引入势必带来新的安全隐患和威胁。首先, 针对 6G 网络的关键技术、实现手段等展开研究, 重点围绕国际上 5G/6G 的主要研究机构、公司和企业的研究进展进行详细调研。然后, 汇总 6G 网络的愿景和核心技术, 并在此基础上提出 6G 网络可能存在的安全问题和挑战。最后, 根据现有的技术情况, 总结针对这些安全问题的解决方案, 并探讨面向 6G 网络的安全模型。

关键词: 6G; 网络安全; 无线通信安全

中图分类号: TN91

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021004

Research on security scenarios and security models for 6G networking

ZHANG Chenglei, FU Yulong, LI Hui, CAO Jin

School of Cyber Engineering, Xidian University, Xi'an 710126, China

Abstract: The concept of 6G has been proposed and has attracted the wide attention of academe. Generally speaking, the 6G network will optimize the performance of 5G, and expand the network scenarios which are difficult to achieve within 5G. However, the introduction of new scenarios and technologies will also bring new security threats to cyber security. The research progress on the key technologies and implementation methods of the 6G were conducted. To summarize a vision of core technologies of 6G, the research work of major 5G/6G research institutions, companies and enterprises were focused on. On this basis, the possible security problems and security challenges in 6G network were put forward. Finally, according to the existing network techniques, the possible solutions and proposed a general security model for 6G networks were discussed.

Keywords: 6G, network security, wireless communication security

收稿日期: 2020-07-31; 修回日期: 2020-12-12

通信作者: 付玉龙, ylfu@xidian.edu.cn

基金项目: 国家自然科学基金(61772404); 陕西省重点产业创新链(群)-工业领域项目(2020ZDLGY08-08)

Foundation Items: The National Natural Science Foundation of China (61772404), Key Research and Development Program of Shaanxi (2020ZDLGY08-08)

论文引用格式: 张成磊, 付玉龙, 李晖, 等. 6G 网络安全场景分析及安全模型研究[J]. 网络与信息安全学报, 2021, 7(1): 28-45.
ZHANG C L, FU Y L, LI H, et al. Research on security scenarios and security models for 6G networking[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 28-45.

1 引言

2020年7月3日,第三代合作伙伴计划(3GPP, 3rd Generation Partnership Project)宣布5G标准R16 (Release16)冻结,至此,5G网络的架构、频谱技术和商业模式基本确定,5G进入全面部署的快车道。自移动通信系统诞生以来,移动通信以及相关技术的发展日新月异,遵循“十年周期法则”,即基本上每十年会更新下一代的无线通信系统,而且每一代通信系统从开展研究到商业化部署需要5~10年,所以,当上一代移动通信系统步入商用化后,就应该展开针对下一代移动通信的理论和技术的研究,面向6G网络的研究呼之欲出。

尽管5G的使用越来越普及,它的一些技术手段仍然不够成熟,无法满足人们最初对5G的要求和期望。例如,5G虽然提供了较4G优势明显的大带宽、低时延、广连接等性能指标,但是依然无法满足实际生活中对于虚拟现实、自动驾驶、远程医疗,以及万物互联等业务的智能化通信需求。这就激发了人们对通信系统的研究和探索,期望在6G网络中达到虚拟现实和自动驾驶等所需要的关键性能指标,也以此为出发点展开了对6G愿景、使能以及一些潜在关键技术的研究。

6G网络与5G相比将会有巨大的革新,相比之下,6G不仅要求更高的带宽、更低的时延和更高的可靠性,同时6G网络会具备更多5G所没有的数据形式,如未来6G所传输的大量人体数字信息(包含物联网、工业物联网、电子健康、人体局域网等)。此外,6G将会更广泛地渗透到工业物联网以及各种垂直行业中,网络中的大量数据将包含极其敏感的个人隐私。

首先,在6G时代,设备将与人们的感官无缝集成。虚拟现实(VR)、增强现实(AR)和混合现实(MR)技术正在合并到XR(XR=VR+AR+MR)中。在通信网络中所传输的信息除了机密文件、隐私信息,还包含人的生物特征识别信息、家庭电器控制信息甚至是车辆的自动驾驶控制信息等。人们将可以通过可穿戴移动设备随时随地与互联网相连。在这样的情况下,恶意网络

活动可能会导致人们的财产、精神甚至生命损失。因此,6G网络的安全研究和完善的安全机制建立至关重要。没有健全的安全机制,6G通信网络就无法被广泛应用和接受,也无法发挥其全部潜力。

除此之外,未来6G网络的设备形式和服务类型可能与现在有着翻天覆地的变化,相应的网络架构趋向复杂化,应用场景以及所包含的终端设备也会极大地增加,并且网络有向边缘化发展的趋势。这就意味着很多传统的安全方法难以在6G的新终端设备中实行,同时网络会存在更多可能被攻击的安全设备和安全漏洞。为了解决这些问题,需要在6G网络架构设计的同时融入安全方案和相对完整的安全体系,以保证6G网络具有更高的安全性和可信度。

2 6G 研究背景

2.1 性能指标与关键技术

6G的关键性能指标包括支持1 Gbit/s的用户体验速率,1 Tbit/s的峰值速率,10~100 μ s的时延,1 Gbit/(s·m²)的区域通信流量,10⁷台/千米²的连接密度以及至少1000 km/h的流动性。图1展示了6G与5G关键指标的对比,可以看出,6G网络的关键网络性能指标较5G具有显著提升。

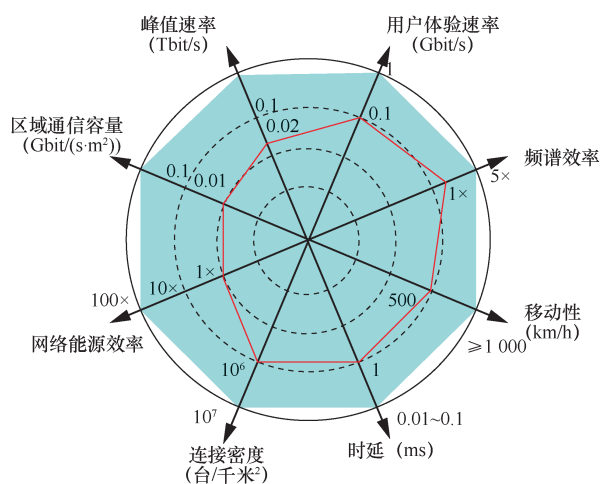


图1 5G和6G的关键指标比较
Figure 1 Comparison of 5G and 6G key indicators

为了实现上述关键性能指标要求,6G网络在频谱、编码、天线等方面需要产生革命性的创新,

而当前 6G 网络的最终技术实现方式还不明确, 其潜在技术将包括太赫兹 (THz) 通信、可见光通信 (VLC)、新一代信道编码技术、超大规模天线技术、基于人工智能 (AI) 的无线通信技术、空天地海一体化通信等关键技术^[1-10]。表 1 对介绍 6G 相关的文献进行了对比和总结, 其中, OAM 为轨道角动量; SM-MIMO 为超大型天线阵列; B5G 为后 5G。

2.2 应用场景

6G 网络性能的提升将带来全新的网络应用场景的变化, 进而促进新业务发展并出现相应的网络安全问题。文献[1]中提出了 5 种 6G 的新型应用场景, 包括进一步增强的移动宽带 (FeMBB, further enhanced mobile broadband)、超大规模机器类型通信 (umMTC, ultra-massive machine-type communications)、增强型超可靠和低时延的通信 (ERLLC, extremely reliable and low-latency communications)、长距离和高移动性通信 (LDHMC, long-distance and high-mobility communications) 以及超低功耗通信 (ELPC, extremely low-power communications)。图 2 给出了未来 6G 的潜在使用场景, 表 2 总结了 5G 与 6G 在应用场景、特性以及关键指标这些方面的区别。

2.3 网络架构

经过广泛调研, 本文发现现有的 6G 相关文献主要是提出愿景和分析讨论潜在技术。由于很多技术尚不成熟, 很难确定一个具体的框架。这里采用文献[1]中所提出的天地一体化自治网络框架来进行说明, 该模型主要是对 5G 网络架构进行天地一体化的延伸, 阐明了天地一体化自治系统的基本思路和框架。图 3 给出了空天地海一体化 4 层网络结构。

从结构上讲, 6G 将是一个 4 层大维网络, 可分为太空、空中、地面和水下 4 个网络层。

1) 太空网络层: 支持空间旅行等应用中的空间互联网服务, 并通过密集部署近地轨道、中轨道地球和地球静止轨道卫星为地面网络未覆盖、未服务和覆盖不足地区提供无线覆盖。对于大容量星地传输, 将部署毫米波通信卫星。同时激光通信可以在自由空间实现卫星间的远距离传输。

2) 空中网络层: 该系统在低频、微波和毫米波段工作, 通过密集使用飞行基站, 如无人机和浮空基站, 为紧急事件或偏远山区提供更灵活可靠的连接。浮空基站的定位特性有助于使 6G 定义的光接口连接太空网络和可到达的无人机基站。

表 1 6G 关键性能技术指标研究进展现状
Table 1 Current status of research on 6G key performance technical indicators

参考文献	6G 网络架构	潜在技术方法	主要贡献
[1]	大型自治 6G 网络架构	太赫兹通信、SM-MIMO、大型智能反射面、全息波束成形、OAM 多路复用、可见光通信、激光通信、基于区块链的频谱共享、量子通信、分子通信	提出 6G 愿景, 讨论 6G 的指标和潜在技术
[2]	舒适、安全、智能的一体化网络架构	超高频段、深度学习、智能反射面	比较 5G、B5G 和 6G 的主要业务, 从多方面分析潜在的技术方法
[3]	绿色 6G 网络架构	太赫兹通信、可见光通信、分子通信、量子通信、分布式安全区块链、柔性智能材料、能量收集与管理	提出绿色 6G 愿景的概念, 讨论潜在关键技术
[4]	未讨论	未讨论	介绍 6G 的驱动力、新场景和指标等, 并提出有待解决的问题和挑战, 为研究者奠定研究方向
[5]	智能化网络架构	6G 大数据分析、AI 闭环优化、智能无线通信	从智能化的角度分析 6G 的愿景, 介绍 AI 对 6G 的赋能
[6-9]	未讨论	微小蜂窝、集成频段收发器、大型智能反射面、边缘人工智能、地面-空中-卫星综合网络、能量转移与收集、第六感网络、极限网络、全息无线电和光电二极管耦合天线阵列、基于 AI 和光光学的认知无线电	介绍 6G 的愿景, 讨论 6G 具有的新指标和潜在关键技术, 并提出 6G 在发展中所面临的问题
[10]	未讨论	太赫兹通信、可见光通信、稀疏理论-压缩感知、全新信道编码、超大规模天线技术、灵活频谱技术、基于 AI 的无线通信技术、空天地海一体化通信、无线触觉网络	比较全面、清晰地概述了 6G 的愿景、使能以及潜在关键技术

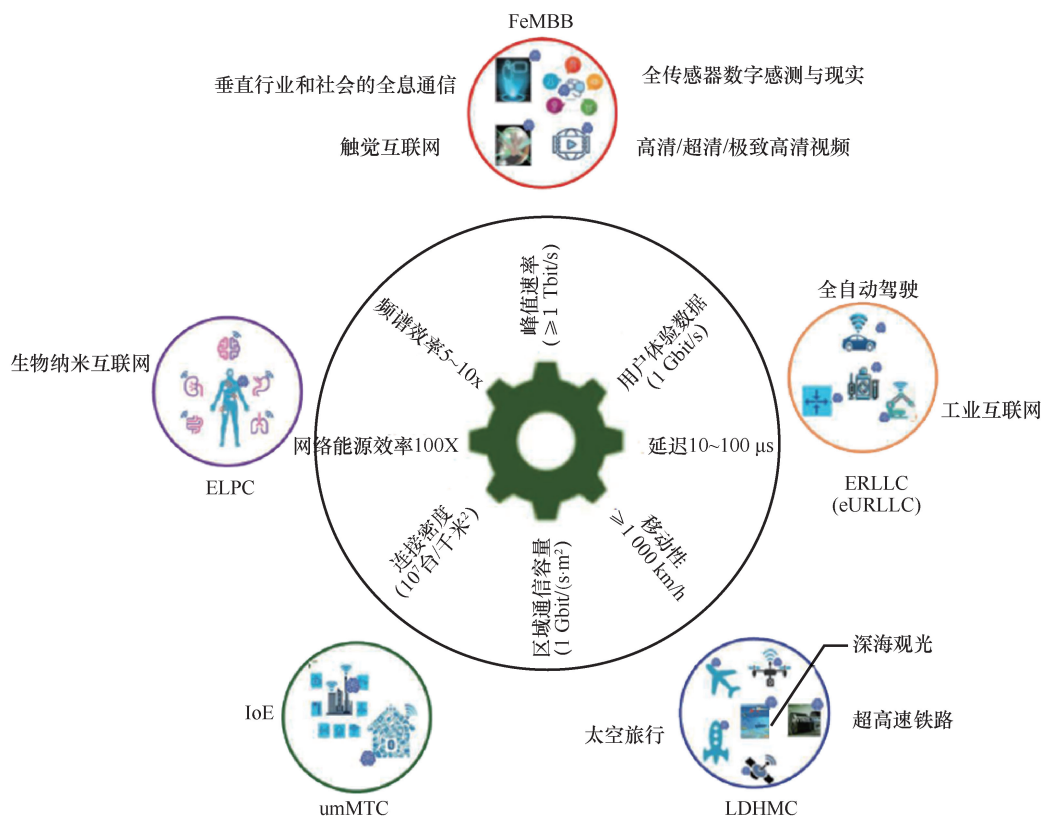


图2 6G 典型应用场景

Figure 2 The typical scenarios of 6G networks

表2 5G 与 6G 应用场景与关键指标对比

Table 2 Comparison of 5G and 6G application scenarios and key indicators

移动通信系统	应用场景	应用	特点	最高速率	用户体验速率	时延	数据区域流量	设备密度	可支持移动性
5G	- eMBB - URLLC - mMTC	- VR/AR/全景视频 - 超高清视频 - 车联网 - 物联网 - 智慧城市/工厂/家庭 - 远程医疗 - 可穿戴设备	云化、软件化、虚拟化、切片	20 Gbit/s	0.1 Gbit/s	1 ms	10 Mbit/(s·m²)	10⁶ 台/千米²	500 km/h
6G	- FeMBB - ERLLC - umMTC - LDHMC - ELPC	- 触觉互联网 - 全感官数字传输 - 全自动驾驶 - 工业互联网 - 太空旅行、深海观光 - 生物纳米物联网	智能化、云化、软件化、虚拟化、切片	≥1 Tbit/s	1 Gbit/s	10~100 μs	1 Gbit/(s·m²)	10⁷ 台/千米²	≥1 000 km/h

3) 地面网络层: 为大多数人类活动提供无线覆盖的主要解决方案。为了满足数据速率高达 1 Tbit/s 的业务需求, 则利用 THz 波段; 地面网络将支持低频、微波、毫米波和 THz 波段 (即全波段)。毫米波 (mmWave) 和 THz 通信的路径损耗非常大, 需要部署更多的小基站, 因此, 6G

地面网络将是一个超密集的异构网络, 需要部署超高容量的太赫兹传输通道。

4) 水下网络层: 将为具有军事或商业应用的远海和深海活动提供互联网覆盖服务。由于水具有不同于陆地的传播特性, 因此可以利用水声通信和激光通信来实现水下双向通信的高速数据传

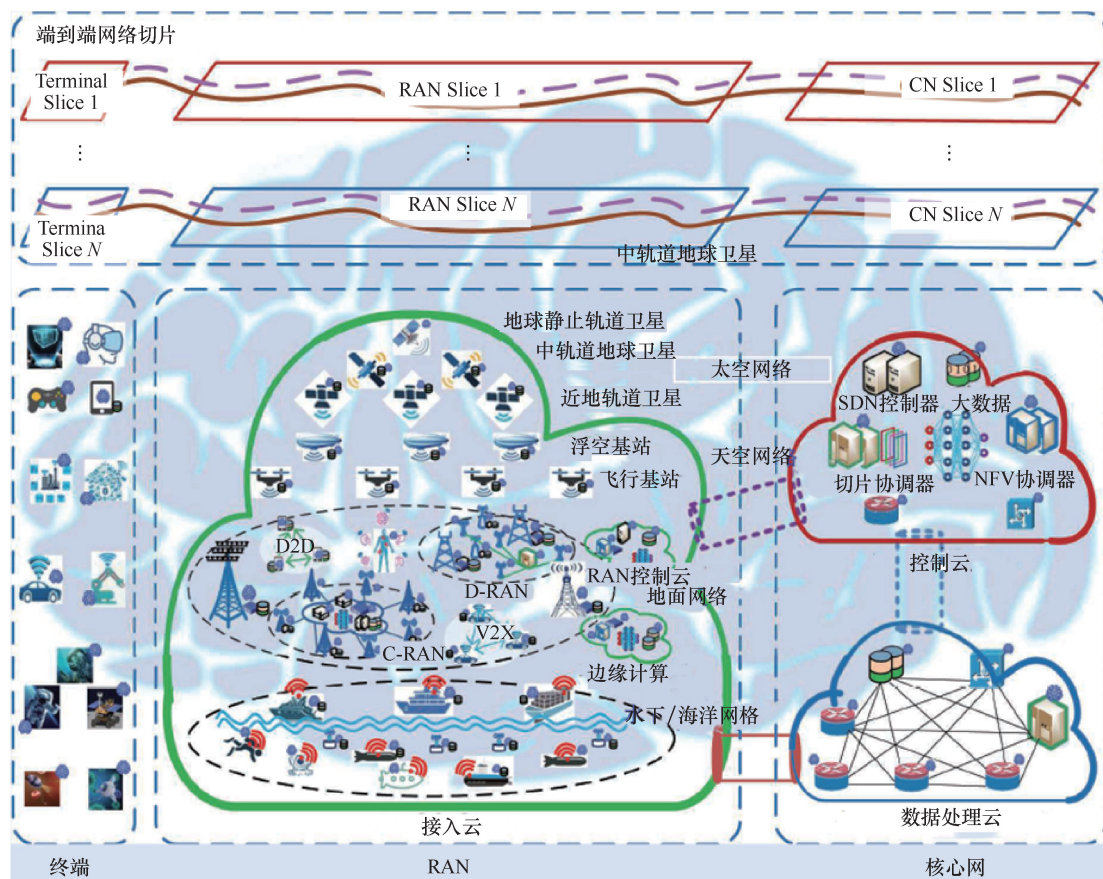


图3 6G网络体系结构

Figure 3 The network architecture of 6G

输，并可以部署更多的水下集线器。

3 6G 网络安全挑战和需求

3.1 新技术和新特征

为提高通信系统的效能、灵活性和自治能力，并降低成本，6G 网络架构将引入新的互联网技术，如人工智能和可见光通信。这些新技术的引入将为 6G 安全提供很好的赋能，同时也会存在新的安全挑战。

6G 网络与 5G 网络相比最明显的特征就是其对 AI 的支持，AI 将在设计和优化 6G 架构、协议、操作以及安全性等方面扮演关键角色^[5]。然而，人工智能所带来的安全问题也是不可避免的^[11]。未来的 6G 通信系统将依靠人工智能实现高度自治化，系统中基于人工智能的安全防护也是这样。基于自动化的人工智能安全手段，虽然大大降低了成本和人工开销，但是也存在被攻击者找到漏洞的风险。由于整个系统高度基于 AI 的运作模

式，一旦攻击者找到漏洞并植入恶意的脚本或者对系统功能进行篡改，将会对整个系统造成大面积的危害。因此，如何将 AI 安全地融合进通信系统是未来值得探讨和研究的问题。在文献[12]中，研究者发现在 B5G 网络和 6G 网络中，AI 和通信网络的集成将会引入一些新的安全威胁：1) 机器学习 (ML) 与通信系统在结合时存在新的集成点和应用程序，这为攻击者开放新的攻击媒介；2) 区块链技术会在运营商环境中引入微型运营商和微蜂窝，为恶意的实体创建了新的激励结构。可以发现，AI 与通信系统的结合就像一把双刃剑。在某种程度上，它可以限制攻击对设备和系统环境的影响。但是，AI 的学习机制需要庞大的数据量支持，如果对手攻击一个数据中心，则可能损害或控制该地理位置提供的服务。为了应对这种情况，需要采取相应的安全措施。例如，将人工智能学习处理的数据尽可能分散到边缘设备中，安全攻击的最严重后果将仅影响该特定用户，而

不影响其他设备。不仅如此,在设计与 AI 融合的通信系统时,还需要制定严格的安全模型,并基于该模型指定安全协议。

VLC 作为 6G 通信系统中光无线通信的主要部分,将会在未来有很大范围的应用。这种通信技术利用了照明时传输的方法,可以自由利用频谱资源,为低成本宽带通信创造了机会,同时可以很大程度上减轻频谱拥塞。VLC 可以作为现有射频通信技术的有力补充,如无线体域网和个人区域网、无线局域网、车辆区域网络和水下传感器网络。VLC 在传统射频通信不太有效的情况下也很有用,如飞机机舱内互联网服务、水下通信、医疗区域等^[13]。VLC 本身具有一些固定的安全性能,如可见光的物理性质决定了它的传播范围局限在一个没有遮挡物的区域内,这样在室内通过可见光进行的数据传输在理论上无法被室外或者遮挡物之后的人拦截和窃听。然而,与通信双方在同一空间下的实体,就很容易发现并窃取到信息,因此,VLC 技术需要足够可靠的物理层安全技术来对其通信的机密性进行保障。现有物理层安全体系和机制主要针对射频通信,相比之下可见光在物理层的安全机制比较薄弱,应当针对可见光设计更加全面和完善的物理层安全机制。

除了以上的技术特征,少数技术将与 6G 同时成熟,因此有可能在 6G 标准化和研究过程结束时发挥作用。例如,量子计算和通信可以提供高安全性和长距离的联网。目前,世界上主要的研究工作集中在量子领域,量子计算的技术还有待突破,暂时没有过多对其他领域(如通信领域)的渗透,在未来量子计算技术成熟时,如何用量子通信提升通信的效能和安全性将会是一个值得探讨和研究的问题。与此同时,如果量子计算机进入商用阶段,那么现代密码算法中普遍使用的公钥密码算法将不再安全,很容易被量子计算机破解,需要后量子密码算法来进行代替。

3.2 设备能源限制

6G 将能够灵活有效地连接上万亿个自治的低功耗移动设备,并且在 6G 网络的体系中,多数终端将趋向于微型化,如人体植入设备等,这些设备的能耗和安全性的权衡是个非常值得研究的问题。在这种情况下,针对用户体验而言,节

能技术变得非常重要,需要更好的电池及能源技术以及轻型的信号处理架构,才能使在 6G 网络下的移动设备拥有更强大的续航能力。为了解决这个问题,除了为通信设备设计良好的能源收集方案外,安全技术的能耗应当考虑在内。

目前,常用的物联网芯片在链路层采用固定的认证和加密方案。由于不同的认证和加密操作意味着不同的保护等级和能量消耗,固定安全策略忽略了剩余能量、动态威胁和不同的服务需求,容易导致能源效率低。此外,固定的高级安全保护虽然安全防护能力较强,但能耗太大,会导致设备工作时间缩短。

在 6G 物联网中,能量收集和移动边缘计算(MEC)^[14]技术将在一定程度上大大缓解电池和计算能力受限的限制。利用太阳能、射频等多种能源可以为物联网设备持续提供能量。一些敏感的计算任务将被卸载到边缘服务器进行实时数据处理。目前的物联网芯片通常支持多种安全规范,但是在芯片初始化过程中固定加密和认证的方式,这样做简化了网络配置,适合资源受限的物联网芯片。然而,这种固定的安全配置可能无法满足 6G 网络对网络服务质量、能量效率和消息安全的严格要求。因为网络威胁通常是动态的,这些威胁可能远远超出了所提供的固定低级保护。另外,安全保护意味着额外的能源消耗,固定的高级安全配置会很快耗尽电池,导致服务停止,这说明现有的固定安全配置存在能效低的缺陷。考虑到未来 6G 网络中广泛采用的能量手机技术和业务需求^[15],需要合理利用可用能量来应对网络威胁,从而同时提升安全保护能力和网络性能。

3.3 更高的隐私保护需求

6G 的愿景之一就是支持无所不在的互联互通服务,为无数的设备、传感器和自主应用提供可靠、安全的通信服务。这为家庭、工厂、城市和政府提供了未来智能服务的基本推动力,而这些服务又依赖于个人和组织之间或个人与政府之间共享大量的个人数据。例如,未来会普遍融入人们生活的智能家居服务,为了提供更好的服务,智能家居相关的产品会尽可能地存储有关人们生活习惯的数据信息,很多情况下还会将信息上传

至云服务器进行模型的训练等。例如智能照明系统,就需要知道用户什么时候在家、会使用哪些房间、家里有多少人等。这些未经使用者确认的数据大量包含了有关于使用者的社会关系、习惯和偏好等隐私信息。使用这些用户数据的优势是能够根据用户的个人喜好以及对更广泛的用户和提供商网络的理解,创建本地优化或个性化的服务,提高服务质量。但同时带来了巨大的隐私泄露风险,并且使服务提供双方的信任问题变得更加突出。

随着 6G 技术的到来以及生物科学、材料科学、生物电子医学等交叉学科的进一步成熟,其中无论是思维感知还是人体数字孪生,都包含着大量敏感的人体机能甚至人脑的数字信息。并且,由于 6G 业务场景的多样性,以及网络的开放性,用户隐私信息从封闭的平台转移到开放的平台上,接触状态从线下变成线上,泄露的风险也因此增加。例如,在智能医疗系统中,病人病历、处方和治疗方案等隐私性信息在采集、存储和传输过程中存在被泄露、篡改的风险,而在智能交通中,车辆的位置和行驶轨迹等隐私信息存在暴露和被非法跟踪使用的风险。如果这些数据集被连接起来,在连接的数据中就会包含大量全方位的个人信息,通过这些信息足以重新识别数据中所代表的个人。怎么对这些数据进行周密的安全防护、如何使用这些数据以及风险应该由谁来承担,是比较值得讨论和探索的问题。

B5G 智能生态系统将是一个共享的网络基础设施,多个利益相关者协同为消费者提供多种服务。因此,它也为管理隐私与建立所需信任之间的权衡展开了讨论。随着人们给予利益相关者更多的信任,隐私泄露的风险增加。因此,6G 需要新的信任模型以及更好的隐私保护方法,从而在维护消费者隐私和信任之间提供平衡。

3.4 需要支持广连接、高覆盖的设备接入

6G 网络提出了一个新的网络体系,即空天地海一体化网络,它相比 5G 具有更广的覆盖范围和更远的覆盖深度和高度。这样的网络体系不仅需要为物联网提供可靠的网络通信服务,还需要支持不同环境和空间下的各种设备实时通信。海量的设备对连接管理提出了很高要求。例如,车联网系统中的车车通信、车人通信、车路通信和

车网通信涉及上亿传感设备的连接,对于保障交通安全、提高城市交通运行效率、降低污染排放具有重要意义。大型城市的智能电表装机量过千万,每天需要从大量电表向电网数据中心上传大量的计量数据。智能制造要求持续在线、广覆盖、大连接,为连续运转的机器、数量庞大的产品和工人提供随时随地、无处不在的连接,保证生产各个环节任何位置间物的连接。物联网设备数量庞大,无人值守,对网络安全管理和安全防御带来新的挑战。因此,6G 网络需要拥有足够自主化和智能化的安全防御体系,为将来 6G 时代中趋近于无限数量的移动终端提供安全防护能力。

4 6G 网络安全模型

6G 的安全模型和技术应该为差异化的 6G 应用场景与新的网络架构提供全面且可靠的安全防护。由于 6G 应用场景下终端种类数目巨大、安全防护等级要求高、安全能耗效率要求高等特点,6G 的安全架构应该满足以下需求。

1) 分布式模型训练: 6G 网络具有高度 AI 化的特点,模型的集中训练将会存在很大的安全威胁,需要分布式的模型训练方案来改善。

2) 可见光安全: 可见光作为 6G 中一种新兴的通信技术,需要具有不同于射频通信的物理层安全机制来支持。

3) 量子密码安全: 预计 6G 时代大规模量子计算机将会得到商用,基于量子计算层面的密码体系值得研究。

4) 高效能安全: 6G 网络中除了用户的移动设备具有移动化和微型化的特性,很多小型的基站等通信基础设施也会趋向移动化,能源消耗是十分重要的问题,需要设计具有良好能耗效率的安全算法来提供安全保护。

5) 隐私保护: 6G 网络中存在大量的敏感信息,需要增加新的隐私保护手段,并对现有的隐私保护技术进行拓展和增强。

6) 智能化安全: 一方面,随着 6G 网络范围的扩大和设备的增多,网络攻击不仅越来越普遍,而且在攻击方式上也越来越复杂,单靠人工力量以及固定的防御机制很难应对数量巨大并且多变的攻击,因此需要利用 AI 对网络攻击进行预测并调

整相适应的安全能力,设计基于 AI 的安全方案。同时, AI 可以为日益复杂化的网络安全配置带来便利。另一方面, AI 的融入为 6G 网络安全带来新的安全需求,需要针对智能化系统设计新的安全规范。

6G 网络安全架构的设计需满足上述新的安全需求和挑战,包括新业务、新技术、新特征以及新的设备形态等。6G 网络安全架构的设计原则包括:对集中的数据进行分散化的处理,考虑新的通信技术和设备形式带来的安全问题,加强隐私保护能力以及安全手段需要向智能化发展。

结合针对 6G 网络安全场景的调研结果,通过扩展 3GPP 5G 安全架构模型,本文认为未来 6G 网络的安全架构将具有类似图 4 的架构。

根据 6G 网络安全设计预测,本文认为未来 6G 网络安全架构将包含以下 8 个安全域。

(1) 终端设备安全:类似于 5G 网络,如何确保海量接入设备自身的安全,将成为保障未来 6G 安全的基础。6G 网络中将会存在大量的微型/小型设备,它们形式多样、包含功能广泛,如可穿戴微型设备、电子纺织物、触觉感知设备和人体植入物等,这些设备获取并传输的数据普遍涉及重要的人体数字特征或人脑思维信息。首先,需要针对不同类型的设备制定差异化的安全策略,使每种设备根据安全需求具有自身的安全保

护能力。微型小型设备往往具有比较严格的低功耗需求,因此安全策略制定的同时需要综合考虑设备的能源收集能力以及安全算法和协议本身的能耗。

(2) 网络接入安全:保障用户接入网络的数据安全,安全需求将包含用户设备(UE)与网络之间信令的机密性和完整性安全保护,包括无线接入网和核心网信令保护;UE 和网络之间用户数据的机密性和完整性安全保护,包括 UE 与无线接入网之间的空口数据保护;以及 UE 与核心网中用户安全节点之间的数据保护。

(3) 网络域安全:保障 6G 在网络域上数据处理和传输的安全性。网络域安全涉及承载网络、核心网络上诸多安全要素的防护问题,安全需求将包括安全域切换、移动设备的无缝安全漫游,以及异构网络的安全统一认证等。

(4) 应用程序域安全:保证用户和业务提供方之间的安全通信。应用程序域安全面向用户实际使用的应用程序,涉及用户的安全体验和利益,其安全性需求较多,如病毒木马检测、脚本注入、零日漏洞等,涉及的安全防护方法可能包括代码审计、加密流量分析、模式识别等相关技术内容。

(5) 物理层信道/天线安全防护:6G 网络将会采用一些新的物理层技术,如 Cell-free 大规模 MIMO(多进多出)、智能反射面(IRS)、可见光通信等。对于新的物理层通信技术,以往的物理层

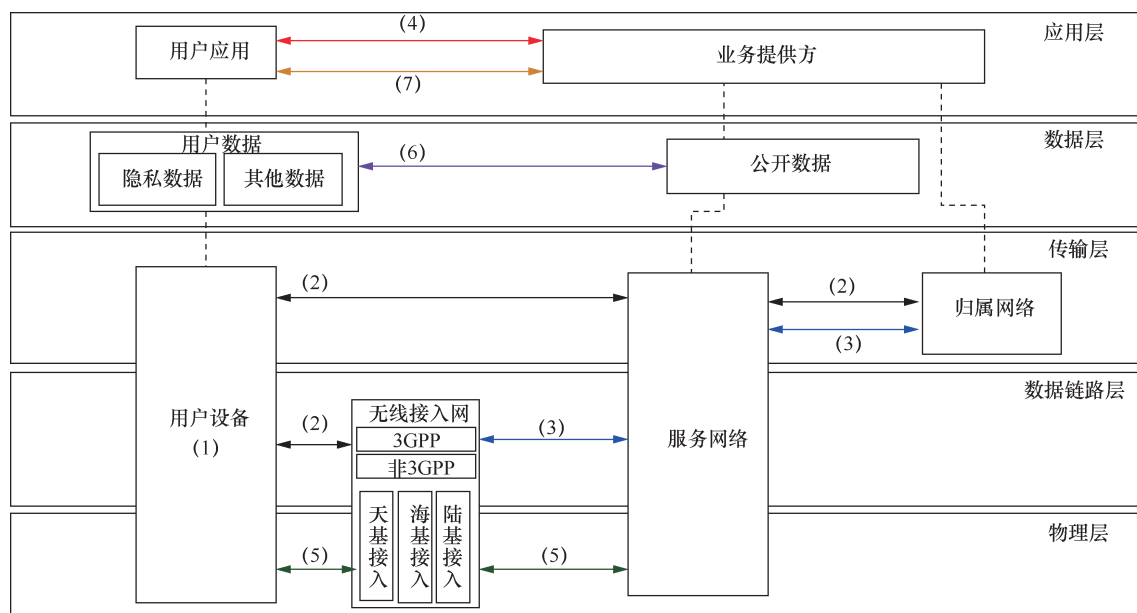


图4 6G 网络安全架构

Figure 4 The security architecture of 6G networks

安全方案已经不再适用,需要针对新的物理层技术提出相应的物理层安全方案,如 VLC,与传统的无线电通信在传输数据的媒介上有直接的区别,需要针对可见光独特的物理性质采取安全解决措施。此外,未来的 6G 将会是一个空天地海一体化的无线通信网络,除了地面的无线通信传输,还需要支持海洋、天空、太空中的实时通信,在这些空间区域的信息传输方式和传输媒介都与地面无线通信有明显的不同,在不同的空间区域需要使用不同的安全策略来满足通信的安全需求。

(6) 数据安全/隐私保护:6G 网络将会极大限度上地满足人们对日常生活的智能化需求,如智能家居、智能汽车、虚拟智能助手等,这些智能化的服务需要基于对人们生活以及生理数据的大量收集;同时,如人体植入物、人脑思维感知等应用需要收集大量与人们体征有关的数据,这些数据本身就是非常隐私并且敏感的。因此,未来 6G 的数据安全和隐私保护将会上升到新的高度。针对 6G 的新特征和应用场景,可以采取区块链、差分隐私、联邦学习、建立信任模型等方法进一步提高对用户隐私和数据的保护。

(7) 软件定义网络(SDN)及切片安全:5G 网络的一个典型特征就是通过对通信功能的软件化实现网络功能的前置化部署,从而减少业务通信的时延,提高网络的反应能力。在 6G 网络中,软件定义网络和网络切片的应用将比 5G 网络更加普遍。可以预见,6G 网络中将会根据不同的业务场景,依据软件功能虚拟化技术建立大量的网络切片,以实现 6G 网络中特殊的网络性能需求。因此,如何保证网络切片的建立、管理等过程的安全性,如 UE 接入切片的授权安全、切片隔离安全将成为 6G 网络安全需要解决的问题。

(8) 密码基础安全:量子计算机预计会在未来几年内商业化,这意味着攻击者也有使用量子计算机对现代密码算法进行破解的能力。6G 网络的密码学体系需要将攻击者具有大规模的量子计算能力列入考虑范围,需要基于大规模量子计算机的计算能力,设计全新的公钥密码算法。

5 6G 安全解决方案

上文从 6G 的背景出发,探讨了 6G 可能存在的安全问题和挑战,并设计了 6G 安全模型。根据对 5G 和 6G 相关安全文献的整理和总结,本节将 6G 网络中可行的安全解决方案分为以下 6 类进行说明。表 3 是对本节所用参考文献中关于 6G 相关安全问题情况的分类汇总。

表 3 6G 相关安全问题研究情况
Table 3 Research status of 6G related security issues

参考文献	涉及安全问题	解决方法
[16-19]	VLC 安全	VLC 物理层安全技术
[20-22]	抗量子密码安全	新的密码方案和密码体系
[23-24]	考虑能耗的安全	低能耗安全协议
[25]		动态可调的安全方案
[26]	隐私保护技术	分布式账本技术
[27]		差分隐私技术
[28-31]		联邦学习
[4,13]		信任模型
[13]	智能化安全	基于 AI 的安全框架
[32-36]		基于 AI 的主动防御和检测等
[37]		基于 AI 的安全配置优化

5.1 联邦学习对数据集集中化的改善

在 6G 网络中,各种类型的移动设备和传感器将会提供大量适合人工智能学习的数据,而数据通过模型进行学习和训练反过来可以大大改善设备上用户的体验。例如,语言模型可以改进语音识别和文本输入,图像模型可以基于个人偏好自动对图片进行筛选。然而,AI 任务是计算密集型的,并且大多数情况下是使用自定义设计的服务器在数据中心进行培训、开发和部署的。鉴于智能移动设备的快速增长,预计将在无线网络的边缘部署大量智能应用程序。未来的 6G 无线网络将利用先进的无线通信和移动计算技术来支持各种边缘移动设备上的 AI 应用程序。这些丰富的数据通常是对隐私敏感的,并且数据量巨大。如果将这些数据存储在集中的位置将会存在很大的安全隐患。为了保护隐私,很多 AI 应用程序的数据采取分散式的管理方法,这样能有效避免数据集中,尽可能减少安

全攻击造成的损失。这时需要分布式的学习技术,可以让用户从这些丰富的数据中获得共享模型的好处,同时无须集中存储这些数据,这种方法叫作联邦学习 (FL, federated learning)。与数据中心对数据的长时间训练相比,联邦学习具有明显的隐私优势。因为作为模型训练需要使用到的用户数据都保存在本地,仅抽象模型会被共享在集中的数据中心。在联邦学习中,进行传输的信息是改进特定模型所需的最小更新,更新本身是短暂的。它们永远不会包含比原始训练数据更多的信息,并且通常包含的信息会少得多。这种方法可以很大程度上提升对用户隐私数据的保护能力。

文献[28]论证了联邦学习在未来通信网络中对隐私保护的重要性,并且提出了一种基于迭代模型平均的深层网络联合学习方法,通过实验数据证明了联邦学习及其优化算法在未来移动通信中是可行的,并且通过联邦学习与差异隐私安全多方计算等内容的结合,将会给未来的安全体系提供更加强大的安全保证。

文献[29]考虑到有限的通信带宽是聚合本地计算更新的主要瓶颈,为此通过探索无线多路访问信道的叠加特性,提出了一种基于空中计算的新颖方法,用于快速全局模型聚合。文献[31]提出了联邦学习在未来通信车联网中的应用和优化方案,研究了车辆网络中超可靠低时延通信的联合功率和资源分配问题。

文献[30]主要综合考虑了联邦学习和无线通信中的度量因素,提出了一种新的框架,使联邦学习算法能够在无线网络上实现。他们提出了一个综合考虑用户选择和资源分配的优化解决方案,能够使 FL 损失函数的值最小化。仿真结果证明,与现有的 FL 算法相比,联合联邦学习与通信框架的性能有了显著的提高。同时,文献中给出了在移动通信场景下的联邦学习算法的学习过程,如图 5 所示。

文献[5]在介绍 AI 对 6G 的赋能之后,提到了未来可以利用联邦学习等技术来保障隐私和数据的安全性,设备上分布式联邦学习的无线计算结构,如图 6 所示。对于深度神经网络,可以在终端设备上提取初始特征,然后将其发送到边缘和云计算设备以进一步处理。

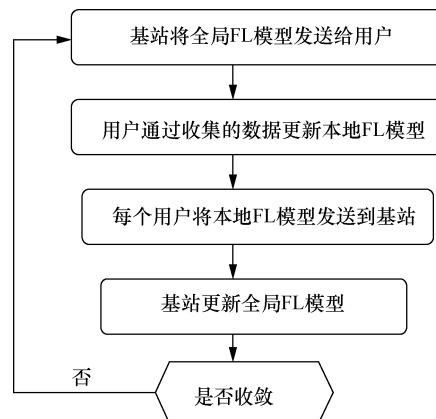


图5 联邦学习算法的学习过程
Figure 5 The learning process of FL algorithm

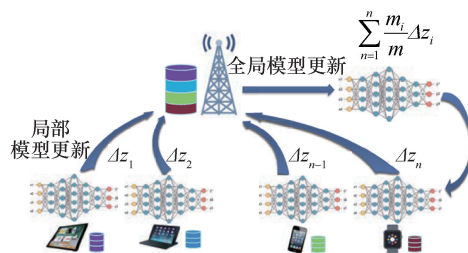


图6 设备上分布式联邦学习的无线计算
Figure 6 Over-the-air computation for on-device distributed FL

通过对相关文献的调研可以发现,已经有很多研究开始对联邦学习的算法和技术进行优化,并且存在将联邦学习与移动通信以及车联网相结合的研究。说明在未来的移动通信中将具有很大的潜力,并且具备极大的泛用性,可以有效解决 6G 移动通信系统引入 AI 而产生的数据安全性问题,为过于集中化的计算提供解决思路。

5.2 VLC 的物理层安全技术

过去几年的研究表明,物理层安全 (PLS) 已经成为解决 VLC 安全问题的相当重要的技术方法,它提供了抵御窃听攻击的第一道防线。其核心思想是利用 VLC 信道的固有特性来实现增强的物理层安全性。6G 无线通信的发展给 VLC 研究中的 PLS 带来了新的技术挑战,包括物理层安全编码、大规模多输入多输出、非正交多址接入、全双工技术等。此外,传统的 PLS 技术主要针对射频通信,不能直接嫁接到 VLC 中,本节将综合一些针对 VLC 的 PLS 增强方法给出安全防范措施。

文献[16]介绍了一种带有水印的盲物理层安全性 (WBPLSec) 协议,来解决针对机密性攻击

的问题。目前的 VLC 方案中,使用红、绿、蓝 (RGB) 发光二极管 (LED) 进行传输更为优选,因为每个颜色分量有着更高的带宽,并且 3 个不同的独立通道可以增加数据吞吐量。假定 Alice 使用 RGB LED 进行传输,而 Bob 拥有一个 RGB 色彩调谐的光电二极管 (PD) 和一个 RGB LED,对 Alice 发送的信号进行干扰并接收和处理,方案如图 7 所示。RGB LED 使用 3 个独立的通道来确保通信安全性。Alice 首先使用扩频序列调制要发送的消息,然后仅使用红光进行发送; Bob 的干扰接收器会干扰部分接收信号,并且知道哪些部分被干扰,这种干扰叫作友好干扰,接收器在接收信号之后能够将干扰后的信号重建成原始信号。这种方法使用蓝光和红光通过两条独立的路径传输信息,信息使用蓝光通过窄带幅移键控 (ASK) 信号发送。而扩频 (SS) 信号使用红灯,因为它的带宽比蓝灯宽,SS 信号实现水印的功能。窄带信号被 Bob 的蓝光部分阻塞。最后,利用 SS 信号中的水印来重新组合整个符号。

文献[17]提出使用中继辅助装置来协助 VLC 通信的安全模型。模型假设一个考虑存在外部窃听者情况下的 VLC 广播频道,发送器与两个合法接收器进行通信。在振幅约束下,为了使 LED 在

其动态范围内工作,基于具有统一信号的叠加编码,得出了可达到的保密区域。然后,引入了受信任的协作半双工中继节点,以通过多种中继方案来协助保护来自窃听者的数据,即协作干扰、解码转发和放大转发。在继电器处设计了安全的波束成形信号,以提高可达到的保密率。并且,最佳的中继方案会根据发射机和中继站到窃听者的距离而变化。

文献[18]针对室内 VLC 系统提出了一种新颖的 PLS 技术。所提出的基于 MIMO-GSSK 的技术设计空间星座图,可以借助合法用户的发送器来最大化发送符号集的最小欧几里得距离。PLS 技术采用零强制预编码来减轻信号间干扰,以使发送符号集成为合法用户的已接收符号集,而对于窃听者,该技术引入了自然干扰信号,有效地向合法用户提供了安全的信息传输,并且禁止了窃听者以可靠的方式成功接收相同的信息。

文献[19]研究了三维多用户 VLC 网络中物理层保密的性能,发现接入点 (AP) 与相邻 AP 的协作可以增强 VLC 网络的保密性能,但只能在一定限度上增强。并且,在 AP 周围建立一个保密区域可以显著提高网络的保密性能。

文献[18]汇总了具有代表性的面向 VLC 的

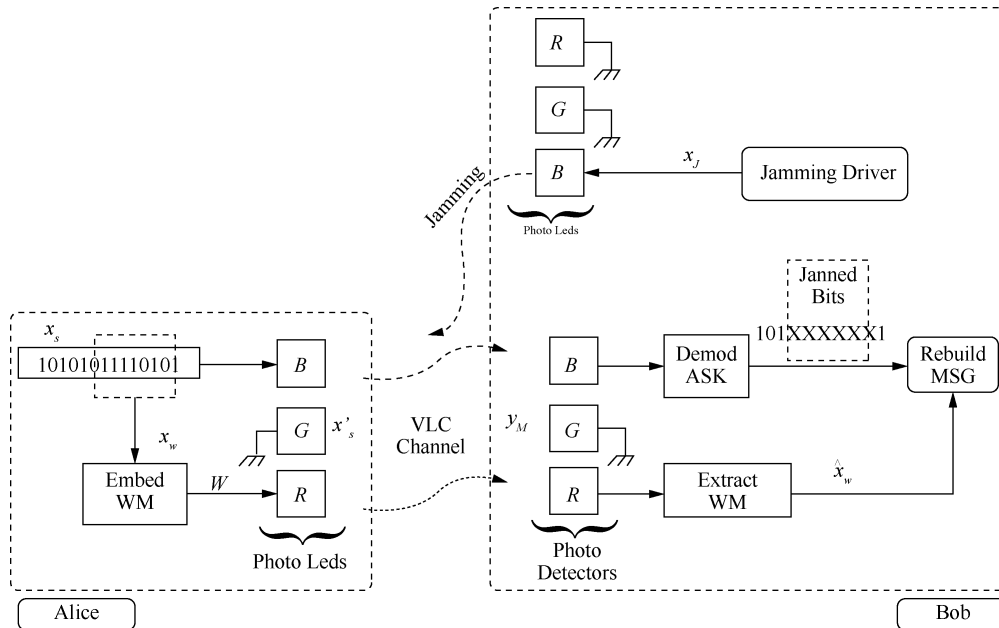


图 7 VLC 网络中的 Wbplsec 系统模型
Figure 7 The model of Wbplsec in VLC networks

PLS 安全机制, 根据其汇总的结果, 做出如图 8 所示的 PLS 安全分类。

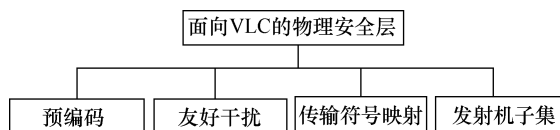


图8 VLC 系统的 PLS 分类
Figure 8 Taxonomy of the PLS for VLC systems

其中, 预编码技术通过使用合法用户的发送器 (CSIT) 和窃听者的信道状态信息 (CSI) 来设计预编码矩阵系数。因此, 当机密消息对窃听者隐藏时, 该机密消息被合法用户清楚地感知。友好干扰技术的主要目的是在合法用户的空间内创建一种人为噪声。在机密信息与发送方的干扰信号结合后, 只有窃听者会受到干扰信号的破坏性影响, 而接收者可以根据自己的噪声信息进行还原。传输符号映射技术通过给定调制的加密密钥来维护保密性, 其中在合法用户侧使用相同的密钥对机密消息进行解码。发射机子集技术是选择发射实体的特定子集, 以便调制发射单元的辐射图, 可以将机密信号集设计为最大化合法用户处的最小欧几里得距离或 SNR。因此, 窃听者可实现的性能将低于合法用户。

5.3 抗量子密码安全

量子计算与经典计算有着根本的不同。很多在当代计算机上难以解决的计算问题, 可以在量子计算机上得到有效的解决。比如, 离散对数问题是现代非对称密码学的基础。如果大规模量子计算成为现实, 这些密码原语需要被量子安全原语取代。根据最近的一项调查^[20], 量子计算可能会在几年内商业化。现有的绝大多数公钥密码算法 (RSA、Diffie-Hellman、椭圆曲线等) 能被足够大和稳定的量子计算机攻破, 虽然大规模量子计算的实现可能需要更长的时间, 但是一些基本的思路已经成型, 因此研究量子计算中安全密码体系的时机已经成熟。根据目前对量子计算的了解, 即使在量子计算出现之后, 当代对称密码在很大程度上仍然是安全的。

目前的 5G 标准并没有解决量子计算的问题, 而是依赖于椭圆曲线密码 (ECC) 等传统加密技术。然而, 椭圆曲线离散对数问题 (ECDLP) 在

量子计算机上可以在多项式时间内求解。预计 6G 网络将会继续向云化和边缘本地化基础结构发展, 与前几代通信系统相比, 6G 的安全体系结构将更加复杂, 以当前的传输层安全标准为主导, 对公钥基础设施 (PKI) 的依赖性越来越大。这一发展将使核心网络完全依赖于底层 PKI 的功能和安全性。目前已经有一些公钥原语被认为是量子安全的^[21], 但是与基于 ECDLP 的方案相比, 它们的效率很低, 密钥也很大。为了满足 6G 体系结构的预期性能和功能, 需要更多的研究来确定量子安全密码的正确应用。在相关文献中, 比较具有代表性的是文献[22], 该文详细地介绍和总结了量子计算技术的发展以及目前最新的研究成果。文献[21]提出了后量子密码学的概念, 并对其进行了详细的介绍和解析。

量子密码的标准化工作正在进行中, 美国国家标准与技术研究所 (NIST) 目前正在主持一个选择进程 NIST PQC, 用于量子密码标准化。这些新的原语有望提供量子安全密钥交换, 并增强数字签名标准 (DSS) FIPS 186-4。

5.4 考虑能耗的安全

未来 6G 网络中的终端设备将更多地趋向于轻型化和微型化, 并且这样的设备会在总的通信节点中占绝大多数。设备的微型化会不可避免地给设备造成能源储备的缩减, 要想在 6G 网络中维护用户对于这样的轻型及微型设备的体验感, 增加其续航, 需要从以下几个方面入手: 首先是对于未来先进电池的研究, 希望能在减小电池体积和重量的同时尽可能扩大其能源量; 然后是设备本身的能源收集技术需要进一步的研究, 以此来维持设备的持续运行; 同时, 如何最大限度地降低设备的运行基本能耗是一个重要问题, 其中安全机制和算法不可避免地存在能耗需求, 因此, 需要设计适用于轻型及微型移动设备有限能源的安全机制。

考虑能源的安全机制设计有两个思路方向: 一是设计具有低能耗和高安全特性的安全协议, 使设备具有的认证加密等功能在消耗较低能源的同时具备相当可观的安全能力; 二是设计一个安全方案灵活可调整的机制, 设备可以基于自身实时的能源收集能力和安全威胁等级, 调整所用的安全能力, 从而使在能源条件可接受的情况下最

大化自身的安全性。

文献[23]介绍了一种基于令牌的安全协议,该协议考虑到物联网(IoT)设备能量和网络服务质量的折中,用于物联网系统中的身份验证和授权。提议的协议基于 OAuth 2.0 框架,使其适合物联网要求的各种大型系统。所提出的协议是基于质询-响应机制,结合使用物理不可复制功能(PUF)的椭圆曲线密码学。从硬件子系统到协议,都可以实现动态的能量质量折中。该研究发现,当将密钥大小动态调整为实际所需的安全级别时,每降低 1 位密钥大小,将使能量消耗降低 0.31%~0.4%。并且在用于物联网设备的身份验证和授权时,能源最多可减少 69%,在数据传输期间,尤其是在传输短消息时,最多可减少 45%。其主要原理是由于 OAuth 框架启用了令牌重用,避免了模块化指数运算以及能源质量可伸缩性,因此,与最新的协议相比,这种协议所需的能源更少。

在文献[24]中,作者在两种不同的 IoT 系统场景下引入了提供相互身份验证、隐私保护和数据源的安全协议:1) IoT 设备直接连接到无线网关时;2) IoT 设备处于安全状态时,通过其他物联网设备间接连接到网关。所提出的协议使用物理上不可复制的功能,以及从两个通信实体之间的无线信道特征中得出的无线链路指纹。该研究发现,所提出的协议在检测数据来源攻击方面的准确性提高了 100%,并且就 CPU 和无线电能量而言,可以为 IoT 设备分别节省多达 83.8%和 73.5%的能耗。这说明协议不仅在计算复杂性和能量需求方面是有效的,而且对于各种类型的攻击(包括物理和复制攻击)也是安全的。

这几个文献主要的研究方向是安全协议的设计,从这几个实验结果中可以发现,如果以能源消耗为前提来设计安全协议,是可以通过相关技术在保证安全能力的同时大幅度地降低通信设备的能量消耗。因此,在 6G 时代的安全协议设计中,能源消耗是一个非常值得考虑的问题。

此外,在实际的通信安全场景中,网络威胁通常是未知的,移动设备应该通过可用能量来调

整安全防护策略。比如,当设备的收获能源不足或者具有很重的工作负载时,可以考虑将设备的安全能力调整为所需的最低安全保护水平,以最大限度地延长工作时间。反之,当收获功率较大时,可以改进所提供的安全保护以获得更好的消息安全性。为了解决这个问题,在文献[25]中,作者提出了一种基于 AI 的 6G 能量收集物联网服务质量和安全性联合优化方案,此方案的假设应用场景是基于 6G 网络下设备通过太赫兹和毫米波的不同频带连接到蜂窝网络的通信。在研究中,作者提出首先采用扩展卡尔曼滤波(EKF)方法来预测未来移动设备的能量捕获功率;然后,在每一个能量感知周期内,设计一个数学模型,计算不同安全策略所需的能量,选择当前设备能量捕获功率所能支持的最高级别保护,以满足服务需求,减少能量消耗。该方案不仅能为不同业务提供满意的安全保护,而且能调整安全保护以避免能量耗尽,从而显著提高移动设备的数据吞吐量和工作时间。这种方案引入了 AI,通过预测设备实时的能源收集效率,动态地对设备的安全防护等级进行调整,以达到设备可支持的最强安全防护能力。

以上介绍了在未来的 6G 移动通信网络中,在考虑能耗的基础上设计移动设备的安全性所用到的两种思路。这两种思路并不是互斥的,未来这两种思路更加成熟时,将两者结合起来设计安全方案也是一个值得思考和研究的问题。

5.5 隐私保护技术

6G 网络将会涉及更多的网络接入类型和垂直行业的应用,并且 6G 网络的特点将更加趋向于以人为中心进行服务,通过各个传感设备会获得大量的人体生理特征数据,这些数据普遍是敏感的、不可泄露的。同时,用户隐私信息会在多种网络、服务、应用及设备中存储使用。同时,随着 5G 网络的发展,6G 预计将越来越多地依赖于支持 AI 的智能应用程序,这些应用程序需要情景、上下文感知和定制的隐私解决方案。根据现有与隐私保护相关的研究,区块链、差分隐私技术、联邦学习以及信任模型可以用来作为隐私保护比较合适的潜在技术。

区块链等分布式账本技术 (DLT) 可以作为促进利益相关者之间使用无信任计算的一个技术, 同时可以提供网络中的隐私保护机制。区块链可以提供安全和隐私特性, 如不变性、透明性、可验证性、匿名性和假名等。区块链可以提供隐私保护的数据共享机制, 优化认证和访问控制, 提供数据完整性、可追溯性、监控等关键特性, 并确保高效的问责机制等。

在相关文献中, 文献[26]是比较典型且具有代表性的。文中提出了一个基于区块链的去中心化系统, 如图 9 所示。该系统 3 个实体分别是移动用户、服务提供者、节点 (受托维护区块链的实体)。系统的设计如下: 区块链接受两种新的交易类型: T_{access} (用于访问控制管理) 和 T_{data} (用于数据存储和检索)。用户可以通过 T_{access} 改变服务提供者的权限, 而服务提供者使用 T_{data} 向区块链查询需要的用户数据, 区块链可以辨别其权限并决定是否基于数据。这里的节点是维护区块链的实体, 就像是一个第三方数据中转中心, 基于其区块链的透明性和可验证性, 用户和服务提供者都是对其可信任的。这样就可以达到用户与服务提供者双方在可信的条件下进行数据传输的目的。

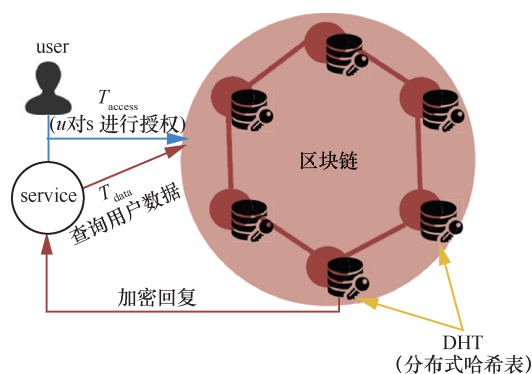


图 9 去中心化系统概述
Figure 9 Overview of the decentralized platform

差分隐私技术对解决未来智能 6G 无线应用中的隐私保护问题十分重要。由于 6G 网络中业务和应用场景的多样性和网络的开放性, 用户的隐私信息可能会从封闭安全的平台转移到开放的平台, 造成隐私的泄露, 因此需要利用差分隐私技术对用户行为相关的数据分析进行保护, 防止攻击者从公开的信息中挖掘并获取用户隐

私信息。

文献[27]提出了一种在雾计算上下文 (PCP) 中具有差分隐私的基于内容的隐私保护方案。PCP 可以确保用户的隐私、隐私保护系统的功能, 并抵御串通攻击。所提出的方案可以在维持典型隐私保护系统功能的同时, 保护用户的隐私和机密性。差分隐私在将最终输出发送到指定的服务器之前, 使用人工设计的随机噪声函数对实际数据进行扰动。这可以防止攻击者对接收到的数据进行统计分析, 并防止从用户数据推断个人信息。

与联邦学习相关的概念也是研究界为确保隐私保护而积极讨论的话题。FL 是一种分布式机器学习技术, 允许在生成数据源的本地设备上对大量数据进行模型训练, 所需的建模在联邦中的每个学习者处完成。每个学习者不发送原始训练数据集, 而是将其本地模型传输到“聚合器”以构建全局模型。FL 可以为数据隐私、数据所有权和数据局部性等重大挑战提供解决方案。FL 基于其对数据进行分布式存储和训练的特点, 可以很大程度上减少隐私泄露的风险, 因为它遵循“将代码带到数据中, 而不是将数据放入代码”的规则。

嵌入式的信任模型是 6G 白皮书中提到的比较重要的一个概念^[4]。与隐私的相关问题很多涉及通信网络中各个实体之间的信任问题, 在 6G 网络框架中嵌入信任模型将会是解决这一问题的主要方案。

6G 白皮书中提出了信任网络的概念模型, 如图 10 所示。这个模型提出了 IP/ID 拆分器, 使每个设备都拥有一个稳定的 ID, 边缘节点将根据设备的 ID 收集其所有与信任和声誉相关的信息, 可以对不良行为提出索赔。分配这些 ID 的边缘节点还将根据请求将它们转换为 IP 和其他地址。同时, 在信任网络中应使用策略管理, 以根据用例或最终用户和管理员的需要定制通用信任引擎。策略用于描述每个实体的期望以及节点行为的许多方面。每个实体 (管理员、订阅者、用户) 都有自己的策略。策略可以扩展到单个应用程序的级别。信任协商的各个方面都可能受到策略的控制。支持信任组网的节点应普遍收集所有可见

的远程网络实体的行为证据。收集到的证据可以在域中的节点之间共享。这些证据用于为远程实体产生声誉。信任网络节点将具有嵌入式信誉系统。信誉用于做出信任决策，如请求更多信息、接受通信、拒绝通信、根据负载情况为传入流分配资源等。此外，应提供激励措施，以鼓励与信任相关的数据共享以产生声誉^[13]。通过这种为每个设备和用户收集和计算信誉的方式，可以为网络形成良好的信任链，解决很多因信任而导致的安全问题。

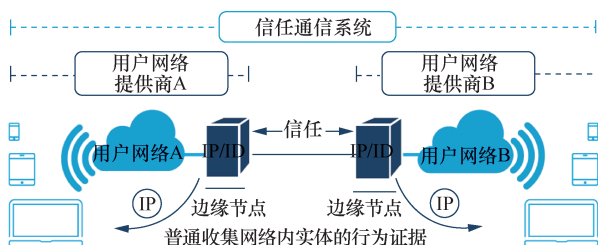


图 10 信任网络概念模型
Figure 10 Conceptual model for trust networking

通过上面的综述和分析，可以将 6G 中隐私保护会用到的技术分类如图 11 所示。其中，分布式账本技术主要通过如区块链这种有效的技术，来构建通信中各个利益相关者的信任关系，使其之间的通信透明化且可验证可溯源；差分隐私技术通过对隐私数据的查询中间值注入噪声，防止攻击者查询真正的数据，达到保护用户隐私的目的；联邦学习技术主要是让隐私数据尽可能保存在本地进行学习训练，从而减小受到攻击后用户隐私被大范围窃取和泄露的风险；网络信任模型旨在构建一个健康的网络用户之间的信任链，增强各个实体之间的信任程度和信任关系来促进隐私保护。

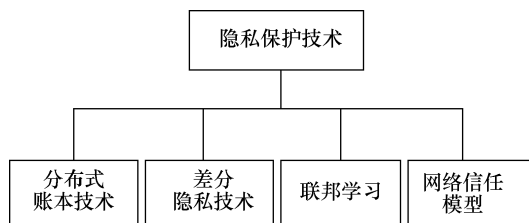


图 11 隐私保护技术分类
Figure 11 Taxonomy of the privacy protection

5.6 智能化安全

在 6G 的诸多研究和愿景中，最引人注目的是 6G 的智能化。预计未来的 6G 网络将超越传统

的移动互联网，可以支持从核心网到边缘网到终端设备的无处不在的人工智能服务。人工智能将在设计和优化 6G 体系结构、协议和操作控制方面发挥关键的作用。并且，未来的 6G 网络将会有近乎无限数量的设备和节点，在全球范围内覆盖陆地、海洋和太空，向具有更高带宽、更致密化和云化的太赫兹频谱迈进。人工智能技术可以利用安全功能软件化和虚拟化的概念实现自动化安全，将人工智能与 6G 的安全防护进行融合是未来的大势所趋。

文献[13]给出了一个基于 AI 的软件定义安全平台，如图 12 所示。为了消除现有和发展中的 5G 网络安全限制，必须进一步改进使用 SDN 和 NFV 现有概念的安全系统，并嵌入动态智能，以满足 6G 安全的需求。6G 网络将在一个集成环境中协调 SDN、NFV 和 AI 的概念，不仅提供必要的服务，而且确保端到端网络安全。在图 12 中，可编程转发平面上的可编程接口将允许在虚拟环境中的任何网络周边或实体中部署软硬件化的安全功能，不仅可以主动发现威胁，还可以在整个网络中从点到点发起安全功能转移。

随着 6G 网络范围的扩大和设备的增多，网络攻击不仅越来越普遍，而且攻击方式越来越复杂。AI 所提供的机器学习、深度学习 (DL) 等技术可以为许多安全策略提供巨大的支持。AI 可以帮助促进网络的自动化和误报检测。各个服务器和终端节点可以通过人工智能自动执行日常任务，包括分析网络流量、根据规则标准授予访问权限，以及检测系统中的异常情况。同时人工智能可以加强网络中的预测分析。

人工智能的第一个自然应用是大数据分析。可以应用于 6G 的分析有 4 种类型：描述性分析、诊断分析、预测性分析和规范性分析。描述性分析可以挖掘历史数据，获取有关网络性能、流量配置文件、通道状况和用户观点等信息。它极大地增强了网络运营商和服务提供商的态势感知能力。诊断分析可以自动检测网络故障和服务缺陷，确定网络异常的根本原因，并最终提高网络的可靠性和安全性。预测性分析使用数据来预测未来事件，如流量模式、用户位置、用户行为和偏好以及资源可用性。规范性分析利用这些预测来对

资源分配、网络切片和虚拟化、缓存放置、边缘计算等进行建议和决策。

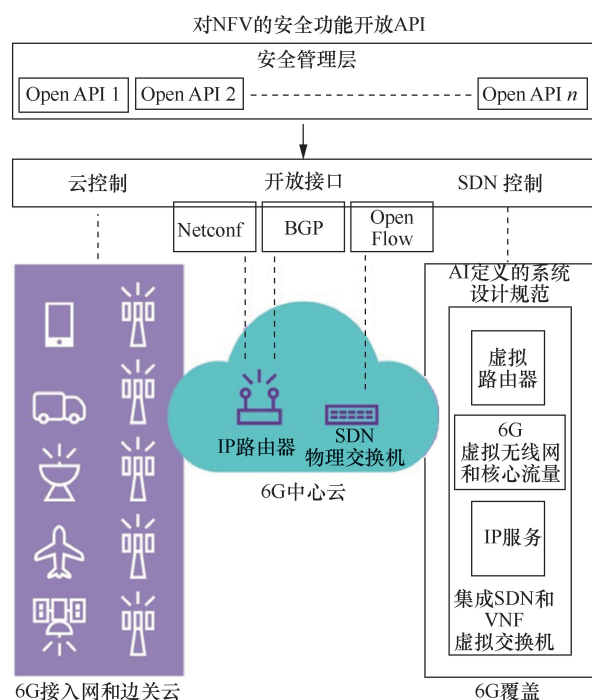


图 12 利用 AI 的软件定义安全平台

Figure 12 A holistic software defined security platform leveraging AI

人工智能在网络安全中的另一个应用是入侵检测和态势感知。如何精确有效地进行恶意行为的检测是网络安全中最普遍的问题。由于 6G 智能化的特点, 可以利用 ML 来制定主动的安全防御方案, 这将有助于鉴别网络流量中的恶意活动。为了防御拥有合法网络证书的威胁行为体, 需要使用深度学习方法来分析特定用户在一系列操作中的行为。除此之外, 网络防御方可以采用类似蜜罐的人工智能技术, 通过提供虚假信息或资源来欺骗攻击者。

相关研究方面, Husák 等^[32]2019 年对网络安全中的攻击预测进行了比较系统性的综述, 综述中涵盖了基于离散模型的方法、基于连续模型的方法和机器学习与数据挖掘方法, 分析和总结了各种机器学习在攻击预测和态势感知中的应用。文献[33]发现认知算法的最新发展可以促进人工智能在 6G 网络中应用来满足用户的时延和极其敏感的安全要求。此外, 人工智能算法和模型可用于发现配置错误、安全漏洞和威胁。文献[34]提出由新兴网络技术(如 MEC 和 SDN)提供的

计算功能可以在边缘层提供强大的计算功能, 可以与先进的 ML 和数据挖掘策略一起帮助设计有效的策略来防止分布式拒绝服务(DDoS)攻击。文献[35]提出了一种基于协作智能代理的云监控模型。位于云不同单元中的代理使用特定的监视方法了解通信环境, 彼此通信并基于 AI 做出决策, 可以用于检测系统内的异常、故障和安全威胁。文献[36]介绍了使用 AI 在车联网通信中基于滥用的检测、基于异常的检测和混合检测这几个入侵检测方面的应用。

上面这些文献主要是 AI 在安全的主动防御和检测上相关的应用。由于下一代网络中服务和设备的多样性, 在安全策略验证、策略到配置的转换以及随后的部署方面的自主决策也可以利用 AI 来实现。文献[37]提出 6G 网络中数据流量将会前所未有地庞大, 如果不使用 AI, 很难将安全攻击与合法流量区分开; 并且提出物联网设备的主要要求之一就是时延, 为了满足主要服务要求, 如从一个边缘节点到另一个边缘节点的服务迁移, 需要在时间限制内主动执行诸如身份验证和访问控制之类的安全服务。在这种情况下, 人工智能将发挥关键作用, 及时识别终端行为和要求, 以避免服务中断。

通过对相关文献的总结和综述, 可以发现 AI 对网络安全的部署和自动化都有很大的促进作用。人工智能可以通过监测更广泛的数据以及识别正常和异常活动的模式来帮助解决攻击预测的问题, 而不必寻找明显的恶意活动。在攻击的初始阶段通过人工智能识别这种活动, 将有助于减轻攻击和定位攻击者。在基于 AI 的各种安全技术的聚合下, 可以塑造一个网络安全的“免疫系统”。如果 AI 能像人体免疫系统一样训练, 那么它将能够更快更有效地定位和消除威胁, 就像白细胞和抗体一样可以中和与已知模式不符的威胁, 这个系统将会不断地学习并变得更强。

6 结束语

本文首先介绍了 6G 的研究背景、愿景以及关键指标, 通过将 5G 与 6G 关键指标进行对比, 明确 6G 网络在应用场景和架构上与 5G 的区别, 从而为后面分析 6G 应用场景和安全需求进行铺

垫;同时分析了研究 6G 安全的意义。接下来,本文对 6G 新型的应用场景和安全需求进行了探讨,方便读者能够快速理解 6G 通信系统的新特征和新技术,并了解针对 6G 的新体系结构存在的安全问题和挑战。最后,本文对这些安全挑战提出了相应的应对方法,设计出面向 6G 网络安全的模型。

本文针对现有研究中对于 5G 和 6G 网络安全模型的探讨进行总结和归纳。然而,现实中 5G 的体系以及 5G 安全方案还在不断发展和变化,且一些有望在 6G 安全中应用的技术有待深入研究。6G 的安全体系和架构将很大程度上取决于未来 10 年间 5G 网络的变化以及相关新型技术的研究和发展。5G 网络在投入更加广泛的应用过程中,也会遭遇大量不同于传统的攻击方式,这将成为 6G 制定安全策略的重要参考标准;并且许多诸如量子计算之类的技术正在萌芽,从技术特性上能极大地改善网络的安全防护能力。这些目前来说都是未知数。6G 无线通信系统的安全理论框架不是一蹴而就的,它需要千千万万的学者通过无数个日夜的辛苦耕耘和默默努力,最后将每个人的成果如河流一般汇聚成大海,形成 6G 网络坚固的安全防御体系。

参考文献:

- [1] ZHANG Z, XIAO Y, MA Z, et al. 6G Wireless networks: vision, requirements, architecture, and key technologies[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 28-41.
- [2] GUI G, LIU M, TANG F, et al. 6G: opening new horizons for integration of comfort, security and intelligence[J]. IEEE Wireless Communications, 2020: 1-7.
- [3] HUANG T, YANG W, WU J, et al. A survey on green 6G network: architecture and technologies[J]. IEEE Access, 2019, 7: 175758-175768.
- [4] LATVA-AHO M, LEPPÄNEN K. Key drivers and research challenges for 6G ubiquitous wireless intelligence [M]. White Paper. University of Oulu. 2019.
- [5] LETAIEF K B, CHEN W, SHI Y, et al. The roadmap to 6G: AI empowered wireless networks[J]. IEEE Communications Magazine, 2019, 57(8): 84-90.
- [6] SAAD W, BENNIS M, CHEN M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems[J]. IEEE Network, 2020, 34(3): 134-142.
- [7] VISWANATHAN H, MOGENSEN P E J I A. Communications in the 6G era[J]. IEEE Access, 2020, 8: 57063-57074.
- [8] YANG P, XIAO Y, XIAO M, et al. 6G wireless communications: vision and potential techniques[J]. IEEE Network, 2019, 33(4): 70-75.
- [9] ZONG B, FAN C, WANG X, et al. 6G technologies: key drivers, core requirements, system architectures, and enabling technologies[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 18-27.
- [10] 赵亚军, 郁光辉, 徐汉清. 6G 移动通信网络: 愿景、挑战与关键技术[J]. 中国科学: 信息科学 2019, 49(8): 963-987.
ZHAO Y J, YU G H, XU H Q. 6G mobile communication networks: vision, challenges, and key technologies[J]. Sci Sin Inform, 2019, 49(8): 963-987.
- [11] YAMPOLSKIY R V, SPELLCHECKER M J A P A. Artificial intelligence safety and cybersecurity: a timeline of AI failures[J]. arXiv Preprint arXiv: 1610.07997, 2016.
- [12] PORAMBAGE P, KUMAR T, LIYANAGE M, et al. Sec-Edge AI: AI for edge security VS security for edge AI[C]//The 1st 6G wireless summit. 2019.
- [13] YLIANTTILA M, KANTOLA R, GURTOV A, et al. 6G white paper: research challenges for trust, security and privacy[J]. arXiv Preprint arXiv: 2004.11665, 2020.
- [14] CHEN M, CHALLITA U, SAAD W, et al. Artificial neural networks-based machine learning for wireless networks: a tutorial[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3039-3071.
- [15] NI J, LIN X, SHEN X S J I N. Toward edge-assisted Internet of things: from security and efficiency perspectives[J]. IEEE Network, 2019, 33(2): 50-57.
- [16] SODERI S. Enhancing Security in 6G visible light communications[C]//2020 2nd 6G Wireless Summit (6G SUMMIT), 2020: 1-5.
- [17] ARAFA A, PANAYIRCI E, POOR H V J I T O C. Relay-aided secure broadcasting for visible light communications[J]. IEEE Transactions on Communications, 2019, 67(6): 4227-4239.
- [18] PANAYIRCI E, YESILKAYA A, COGALAN T, et al. Physical-layer security with optical generalized space shift keying[J]. IEEE Transactions on Communications, 2020, 68(5): 3042-3056.
- [19] YIN L, HAAS H J I J O S A I C. Physical-layer security in multiuser visible light communication networks[J]. IEEE Journal on Selected Areas in Communication, 2017, 36(1): 162-174.
- [20] AHMAD I, SHAHABUDDIN S, KUMAR T, et al. Security for 5G and beyond[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3682-3722.
- [21] BERNSTEIN D J, LANGE T J N. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.
- [22] GYONGYOSI L, IMRE S J C S R. A survey on quantum computing technology[J]. Computer Science Review, 2019, 31: 51-71.
- [23] AMAN M N, TANEJA S, SIKDAR B, et al. Token-based security for the Internet of things with dynamic energy-quality tradeoff[J]. IEEE Internet of Things Journal, 2018, 6(2): 2843-2859.
- [24] AMAN M N, BASHEER M H, SIKDAR B J I I O T J. Data provenance for IoT with light weight authentication and privacy preservation[J]. IEEE Internet of Things Journal, 2019, 6(6): 10441-10457.
- [25] MAO B, KAWAMOTO Y, KATO N. AI-based joint optimization of QoS and security for 6G energy harvesting internet of things[J]. IEEE Internet of Things Journal, 2020, 7(8): 7032-7042.
- [26] ZYSKIND G, NATHAN O. Decentralizing privacy: using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops. 2015: 180-184.
- [27] WANG Q, CHEN D, ZHANG N, et al. PCP: a privacy-preserving

content-based publish-subscribe scheme with differential privacy in fog computing[J]. IEEE Access, 2017, 5: 17962-17974.

- [28] MC-MAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial Intelligence and Statistics, 2017: 1273-1282.
- [29] YANG K, JIANG T, SHI Y, et al. Federated learning via over-the-air computation[J]. IEEE Transactions on Wireless Communications, 2020, 19(3): 2022-2035.
- [30] CHEN M, YANG Z, SAAD W, et al. A joint learning and communications framework for federated learning over wireless networks[J]. IEEE Transactions on Wireless Communications, 2019.
- [31] SAMARAKOON S, BENNIS M, SAAD W, et al. Distributed federated learning for ultra-reliable low-latency vehicular communications[J]. IEEE Transactions on Communications, 2019, 68(2): 1146-1159.
- [32] HUSÁK M, KOMÁRKOVÁ J, BOU-HARB E, et al. Survey of attack projection, prediction, and forecasting in cyber security[J]. IEEE Communications Surveys & Tutorials, 2018, 21(1): 640-660.
- [33] HENGSTLER M, ENKEL E, DUELLI S J T F, et al. Applied artificial intelligence and trust—the case of autonomous vehicles and medical assistance devices[J]. Technological Forecasting and Social Change, 2016, 105: 105-120.
- [34] PHAN T V, PARK M J I A. Efficient distributed denial-of-service attack defense in SDN-based cloud[J]. IEEE Access, 2019, 7: 18701-18714.
- [35] GRZONKA D, JAKOBIK A, KOŁODZIEJ J, et al. Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security[J]. Future Generation Computer Systems, 2018, 86: 1106-1117.
- [36] TANG F, KAWAMOTO Y, KATO N, et al. Future intelligent and secure vehicular network toward 6G: machine-learning approaches[J]. Proceedings of the IEEE, 2020, 108(2): 292-307.
- [37] SHARMA P, LIU H, WANG H, et al. Securing wireless communications of connected vehicles with artificial intelligence[C]//2017 IEEE International Symposium on Technologies for Homeland Security (HST), 2017: 1-7.

[作者简介]



张成磊（1998—），男，湖北武汉人，西安电子科技大学硕士生，主要研究方向为移动通信安全、LTE 攻防。



付玉龙（1983—），男，黑龙江齐齐哈尔人，西安电子科技大学副教授，主要研究方向为移动网络安全、大数据及人工智能安全、形式化安全。



李晖（1968—），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。



曹进（1985—），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为 4G/5G 网络、天地一体化网络安全性及认证协议设计与分析。