中国科学: 信息科学 2021 年 第 51 卷 第 3 期: 347–366
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
评述

5G 安全技术研究与标准进展

强奇[1], 武刚[1*], 黄开枝[2*], 胡苏[1], 李少谦[1]

1. 电子科技大学通信抗干扰技术国家级重点实验室, 成都 611731
2. 国家数字交换系统工程技术研究中心, 郑州 450002
* 通信作者. E-mail: wugang99@uestc.edu.cn, Huangkaizhi@tsinghua.org.cn

收稿日期: 2020–07–23; 接受日期: 2020–09–21; 网络出版日期: 2021–02–24

电子科技大学通信抗干扰技术国家级重点实验室稳定支持科研项目 (批准号: IFN2020207) 和四川省重点研发项目 (编号: 2020YFG0315) 资助

摘要 随着第五代移动通信系统 (5th generation wireless systems, 5G) 及其演进系统的商用和其在物联网、车联网等垂直领域的融合发展, 其安全问题越来越受到关注. 本文从潜在威胁、安全架构和安全技术 3 个方面阐述了相关研究进展. 首先, 根据攻击者对系统有效性、信息完整性、身份认证、隐私和机密性保护的不同安全目标, 将 5G 潜在的安全威胁进行了分类, 分析了各个层次可能面临的威胁与攻击手段. 其次, 简述了相关标准中的 5G 安全架构, 讨论了 5G 及其演进系统潜在的物理层、网络层和应用层安全技术. 最后, 本文指出了未来继续提升 5G 及 B5G 安全的潜在研究方向.

关键词 5G 安全, 5G 演进, 系统架构, 安全威胁, 物理层安全

1 背景介绍

随着 5G (5th generation wireless systems) 的逐步商用及其演进系统 (beyond 5G, B5G) 标准制订, 其安全问题越来越多地受到人们的关注. 国际标准化组织第三代合作伙伴计划 (3rd generation partnership project, 3GPP) 在技术规范中定义了 70 多种 5G 的需求, 主要可分为 3 种场景, 即增强移动宽带、海量机器类通信和超可靠低时延通信 [1]. 为满足新的应用场景和技术需求, 5G 技术标准中引入了包括大规模天线阵列、全双工技术、软件定义网络、网络功能虚拟化等关键技术 [2], 这些物理层与网络层技术一方面会导致潜在的安全威胁, 另一方面也会提升 5G 系统和终端的安全能力. 同时, 面向新业务与新应用的多形态 5G 部署, 比如 5G 物联网、5G 车联网和 5G 专网 [3,4], 以及 5G 基础设施与垂直行业的典型业务的结合[1)], 可能会导致更多的系统安全问题和用户隐私泄露 [5]. 此外, 由于并行/分布式架构和量子计算带来的计算力提升, 及基于大数据和人工智能的先进数据分析方法, 5G 已有的安全架构与安全技术面临着新的安全威胁 [6].

1) 中兴通讯. 5G 行业应用安全白皮书. https://www.zte.com.cn/china/about/news/20190919c4.

引用格式: 强奇, 武刚, 黄开枝, 等. 5G 安全技术研究与标准进展. 中国科学: 信息科学, 2021, 51: 347–366, doi: 10.1360/SSI-2020-0225
Qiang Q, Wu G, Huang K Z, et al. Survey on research and standardization of 5G security technology (in Chinese). Sci Sin Inform, 2021, 51: 347–366, doi: 10.1360/SSI-2020-0225

从 4G 长期演进 (long term evolution, LTE) 系统安全技术标准开始, 到 5G Release 15 标准被制订, 已有相当多的标准研究机构、企业、大学和学者对 5G 安全技术进行了总结. 文献 [5] 全面地分析了 5G 业务应用程序的安全要求、网络架构、空中接口和用户隐私的安全需求, 以内源性防御架构为重点, 总结了 5G 安全架构的发展趋势, 并对几种 5G 安全技术进行了调研, 包括物理层安全技术、轻量级加密、网络切片安全、用户隐私保护, 以及应用于 5G 的区块链技术. 2018 年 3 月, 3GPP 发布 5G 安全 R15 第 1 阶段标准, 文献 [7] 对该标准进行了详细全面的解读, 介绍了新的安全架构及其增强安全的新措施. 文献 [8] 总结了 5G 无线网络系统潜在的攻击和安全服务, 介绍了 5G 无线安全的最新发展和现有方案, 提出了一种新的 5G 无线安全性体系结构并进行了分析, 最后, 总结了 5G 无线安全的挑战和未来方向. 文献 [9] 从云、软件定义无线电 (software defined network, SDN) 和网络功能虚拟化 (network function virtualization, NFV) 的角度概述了 5G 安全挑战并提出了这些挑战的解决方案和 5G 安全系统的未来方向.

在上述的 5G 安全相关研究综述发布之时, 相关的安全标准还不够完善, 一些应用场景的需求还不够清晰. 2018 年以后, 随着相关标准的进一步演进以及 5G 与垂直行业的进一步融合, 关于 5G 安全技术和策略的讨论愈发热烈. 2019 年 11 月未来移动通信论坛在世界 5G 大会上发布以终端为中心的 5G 安全体系白皮书, 分析了 5G 中的终端和系统的安全威胁以及传统和新兴的安全解决方案, 讨论了 “以终端为中心的 5G 安全体系” 概念[2)]. 中国信息通信研究院和 IMT-2020(5G) 推进组 2020 年 2 月联合发布 5G 安全报告, 系统地梳理了 5G 关键技术、典型应用场景及产业生态的安全风险, 提出了安全理念和应对思路措施[3)]. 文献 [10] 重点关注了 5G 带来的新功能和新技术为移动互联网带来的巨大挑战, 包括物联网、设备到设备 (device to device, D2D)、车联网 (vehicle-to-everything, V2X) 和网络切片, 并且详细讨论 5G 安全特性、安全需求和安全漏洞, 给出了现有的解决方案, 以及有关 3GPP 5G 网络中新功能和新技术的一些开放研究问题. 文献 [11] 从安全性和隐私性的角度介绍了用于构建 5G 安全模型的核心技术和支持技术, 包括网络软件化、物理层和 5G 隐私安全, 提出了符合 5G 及更高安全要求的关键项目, 并指出了未来的研究方向.

上述的 5G 安全综述分别从 5G 新功能、新技术和隐私性的不同角度阐述了当前的研究现状, 白皮书则是针对终端、已标准化的相关技术和典型应用场景进行了全面的总结. 2020 年 7 月, 随着 3GPP R16 标准的冻结, 5G NR 中的安全相关标准也一并冻结. 本文在补充了 3GPP 等国际标准化组织已经确定和正在讨论的相关提案的基础上, 多角度地梳理了 5G 网络中的安全问题, 系统性地将这些问题分为潜在威胁、安全架构、5G 和 B5G 安全技术, 并分别从物理层、网络层, 以及应用层对这些安全技术进行了全面的总结. 根据攻击者不同的攻击目标及目的, 针对 5G 和 B5G 的安全威胁可以分为对系统有效性、信息完整性、身份认证, 以及隐私和机密性保护的安全威胁 [8]. 面对这些安全威胁, 现有的 5G 安全架构也在不断演进. 相比 LTE, 5G 网络的密钥体系、身份认证方面都更加复杂, 增强了抵抗攻击的能力, 同时增强了用户面和运营商网络间的信息交互的安全 [12]. 面对一些新的安全威胁以及现有安全架构中存在的一些漏洞, 一些新的安全技术包括物理层、网络层和应用层安全技术被提出来增强安全. 最后, 本文指出了未来继续提升 5G 及 B5G 安全的潜在研究方向.

2 5G 网络安全威胁

为实现通信系统中信息的安全传输, 首先要保证通信系统及信道的有效性或可用性. 其次需要保

2) 世界 5G 大会未来移动通信论坛. 以终端为中心的 5G 安全体系. http://www.w5gc.com.
3) 中国信息通信研究院 &IMT-2020(5G) 推进组. 5G 安全报告. http://www.caict.ac.cn/kxyj.

证信息在传递过程中不被篡改, 即信息的完整性. 由于移动通信信道的开放性, 为实现在移动通信系统中的信息传输安全, 除了有效性和完整性以外, 还需要网络对通信用户身份和设备进行合法性认证, 及用户对接入的网络设备进行认证. 此外, 随着大数据等信息处理技术的提升, 针对隐私的攻击也越来越多, 还需要增加对用户的机密数据隐私进行保护. 考虑 5G 的新应用, 及引入的新空口技术和更多部署场景, 5G 的网络协议变得较 4G 更复杂, 因此, 设计 5G 的安全机制时, 需要从系统的有效性、信息的完整性、身份认证, 及隐私保护这 4 个安全服务的需求保障角度, 考虑更多类型、更复杂的安全威胁.

2.1 系统有效性面临的威胁

系统有效性用于评估系统在面对各种攻击时的稳健性, 目前已知的系统有效性攻击手段主要是干扰和拒绝服务 (denial of service, DoS) 攻击, 此外还有恶意节点攻击 [13] 和智能干扰器 [14]. 通信网络中的恶意节点, 或第三方软件无线电设备, 也可能故意或无意地干扰和破坏合法用户之间的数据通信, 甚至阻止授权用户访问无线电资源 [13]. 目前已出现了一种根据当前的无线电环境灵活地控制器干扰策略的智能干扰器 [14], 是通过可编程软件无线电设备实现.

DoS 攻击是目前最常见的一种安全威胁, 其目的是令通信网络无法提供正常服务. DoS 实现手段包括对网络协议漏洞的利用, 或滥用大量数据等野蛮手段耗尽被攻击网络带宽、文件系统空间容量和允许连接量等资源, 使得目标计算机或网络无法提供正常服务或资源访问, 导致系统服务系统停止响应或崩溃. 移动通信系统也提供了用户设备或服务器在网络中暴露的可能, 因此也会受到 DoS 攻击的威胁. 当存在多个分布式攻击者时, 可以形成分布式拒绝服务攻击 (distributed denial of service, DDoS). DoS 和 DDoS 都是可以在不同层应用的主动攻击, 包括物理层、媒体接入控制 (media access control, MAC) 层等, 使得网络不能提供服务 [15].

5G 网络中引入的 SDN/NFV 和网络切片技术, 使得传统封闭的管理模式变得更加开放, 用户自定义、资源可视化、网络虚拟化等功能的实现增大了 5G 网络的攻击面, 攻击者可以以新技术和新应用为跳板进行 DoS 和 DDoS 攻击, 影响 5G 网络的有效性. 在核心网, 攻击者可以发动核心网组件的恶意洪泛攻击, 耗尽组件资源并导致组件提供的服务减少或完全关闭. 在接入网, 攻击者可以非法占用或者蓄意干扰特定的频谱使得合法用户无法使用对应的频谱资源, 攻击者还可以破坏接入网元素 (如基站) 以伪造配置数据造成认证失败, 导致用户无法连接网络. 在边缘节点, 攻击者可以通过特定的应用程序或设备发起定向请求从而导致边缘节点过载 [16].

2.2 信息完整性面临的威胁

信息的完整性需要通信系统保证信息在传输的过程中不被篡改或替换. 中间人 (man in the middle, MITM) 攻击是常见的破坏信息完整性的攻击方式, 它通过秘密控制两个合法通信方之间的通信通道, 拦截、修改和替换通信消息, 由于无线通信的广播特性, 其更有可能受到 MITM 攻击 [17]. 文献 [18] 描述了一种常见的 MITM 攻击方式, 国际移动用户识别码 (international mobile subscriber identity, IMSI) 捕获器. IMSI 捕获器是一种设备, 使攻击者能够捕获用户的 IMSI 信息, 以便跟踪用户的位置、窃听电话或冒充用户. 文献 [19] 讨论了 MITM 攻击者作为一个透明的中继对无线通信中的导频估计产生的影响, 当所信道中存在攻击者时, MITM 攻击者可以截获所有的信道信息.

用户面和控制面的分离是 5G 核心网的重要特征, 它使用户面更加灵活, 也给降低时延和边缘计算奠定了基础. 但中继节点和边缘节点的增加给信息的完整性带来了极大的挑战, 因为每个节点都可以成为 MITM 攻击者攻击的目标. 在核心网, 攻击者可以利用网络漏洞操纵网络配置数据, 从而影响

信息的完整性. 在边缘节点, 攻击者可以通过伪造的移动边缘计算 (mobile edge computing, MEC) 网关部署自己网关设备, 造成与中间人攻击相同的效果 [16].

2.3 身份认证面临的安全威胁

关于身份认证, 通信网络不仅要对通信网络中的实体单元进行认证, 有时也要对信息进行认证. 用户设备 (user equipment, UE) 与移动管理实体 (mobility management entity, MME) 之间的互认证是传统蜂窝安全框架中最重要的安全特性. 4G 以前的蜂窝网络中, UE 和 MME 之间的互认证是在双方通信之前实现的. 4G LTE 蜂窝网络中的认证与密钥协议是基于对称密钥的 [20]. 在 5G 网络中, 不仅需要 UE 和 MME 之间的认证, 还需要服务运营商等第三方之间的认证 [21]. 而且 5G 网络中的密钥协议是基于非对称密钥的, 这大大增强了 5G 系统的安全性. 但是由于 5G 无线网络的高速数据速率和极低的延迟要求, 5G 认证的速度将比以往任何时候都要快. 此外, 由于 5G 网络的信任模型中增加了一些层来增强安全, 5G 网络会进行非常频繁的不同层之间的切换和认证.

已公开的 5G 身份认证安全威胁研究包括网络切换漏洞 [22] 和身份认证漏洞 [23, 24] 等. 在文献 [22] 中, 作者发现了一个 5G 网络切换认证机制中的安全漏洞: 由于受到身份认证复杂性影响, 在下一代基站 (next generation NodeB, gNB) 内部切换中存在的安全漏洞. 该漏洞可以导致接入和移动性管理功能 (access and mobility management function, AMF) 中的安全信息泄露, 从而使合法的 gNB 的安全性面临严重的威胁. 在文献 [23] 中, 作者利用安全协议验证工具 Tamarin 针对 5G 安全目标对模型进行了全面、系统的评估, 一些关键的身份认证属性在密钥确认之前可以被破坏, 而标准并没有明确规定这一点. 针对目前的 5G 认证协议, 有一种可链接性攻击, 攻击者事先拦截一个合法身份认证请求消息, 他可以通过重放捕获的身份认证请求来检查 UE 是否在特定区域中的存在 [24]. 另外, 在文献 [24] 中给出了一种用户永久标识符 (subscription permanent identifier, SUPI) 猜测攻击, 攻击者可以通过多次重复 SUPI 猜测攻击, 将整个 SUPI 数据库遍历, 发动基于 SUPI 的认证攻击.

5G 认证协议面对的安全威胁不仅包括协议漏洞, 更要面对近来快速增强的量子计算能力带来的安全威胁 [25]. 由于量子力学效应的存在, 使用量子计算机来解决某些加密问题的效率比在经典计算机上解决的要高很多 [26]. 文献 [27] 分析了基于量子计算的密码分析方法产生的安全威胁, 多数对称/非对称加密及哈希算法的计算安全性受到挑战. 量子计算中的 Grover 算法对非结构化搜索问题提供了理论上的二次加速, 可以提升破解分组密钥的效率, 随着量子计算的发展, AES-128 的安全性将会降低 [27]. 量子计算中的 Shor 算法及其变体可以极大地提升整数因子分解和有限域或者椭圆曲线中的离散对数的计算效率, 对 RSA 等非对称加密算法有极大的威胁 [27]. 在身份认证过程中, 一些机密信令的传递往往会受到攻击者的窃听或者 MITM 攻击, 一般情况下系统会对这些机密信令进行必要的完整性和机密性保护.

在核心网, 攻击者可以在短时间内发送的大量身份认证请求, 使得授权设备的身份认证失败并导致连接的丢失, 攻击者还可以利用漫游场景中的安全漏洞获取目标用户的身份认证向量 [23]. 在接入网, 攻击者可以伪装成合法基站或者改变网络设备上分配的 MAC 地址, 改变基站或计算机的身份, 从而发起其他攻击 [16].

2.4 隐私和机密性保护面临的安全威胁

隐私保护在 5G 网络中是一个很大的威胁. 这是因为 5G 网络中业务和场景的多样性, 以及网络的开放性. 5G 网络中端到端的数据流包含着广泛的个人隐私信息, 如机密数据、身份、位置等. 一般情况下对用户机密数据的隐私保护也可以称为机密性保护. 由于各类终端应用程序, 及网络内容和服

务提供商的安全漏洞, 可能在某些情况下, 导致隐私泄露, 并产生严重的后果. 目前, 窃听和通信流量分析是常见的威胁隐私保护的攻击方式 [8].

窃听通常是一种被动攻击. 在不影响正常通信的前提下, 窃听者可以获取双方的通信信息. 目前, 已知一种基于 "截获 – 存储 – 转发" 过程的窃听方式 [28]. 窃听者通过截获信息发送方的信号完成对截获信息的备份, 再将截获信息转发至信息接收方. 由于窃听过程中窃听者没有发送任何除了双方通信内容外的其他信息, 因此窃听很难被发现. 而一些具有干扰辅助功能的主动窃听者往往具有更佳的窃听能力 [29~31]. 在文献 [29] 中描述了一种主动的窃听者, 这种窃听者会主动攻击时分双工系统中的导频序列, 造成导频污染, 从而使下行阶段使用的预编码器增加窃听方的波束赋形分量, 进而增加窃听方的传输信噪比, 造成信息的泄露.

通信流量分析是另一种被动攻击 [8]. 窃听者通过分析接收信号的流量来捕获通信方的位置和身份等信息, 在这个过程中不需要知道信号本身的内容. 即使信号被加密, 流量分析仍可捕获通信方的一些相关信息, 而且这个过程也不会影响合法通信. 在文献 [32] 中, 作者讨论了基于大数据的数据挖掘技术给隐私保护带来的潜在威胁.

在核心网中, 攻击者可以利用合法监听功能进行窃听或者分析接收信号的流量来捕获通信方的位置和身份等有价值的信息. 在接入网中, 攻击者可以向网络发送伪造的地址解析协议 (address resolution protocol, ARP) 消息使该 IP 地址的所有流量被发送给攻击者 [16].

5G 网络中新应用、新技术, 以及新空口的引入, 在使网络开放性, 灵活性得到保障的同时扩大了网络的攻击面, 使得 5G 网络更容易受到 DoS 等主动攻击, 用户更容易受到侧信道攻击, 从而影响系统有效性、身份认证, 以及用户隐私保护. 而边缘节点的出现在满足用户计算需求的同时增加了其受到 MITM 攻击的风险, 给信息的完整性带来挑战. 而数据挖掘技术和量子计算的迅速发展又对隐私数据保护和 5G 系统的加密算法构成了极大威胁. 因此 5G 安全架构应该增强 5G 系统的身份认证, 并且对网络中的数据提供更全面的完整性和机密性保护.

3 5G 安全架构

面对 5G 和 B5G 目前面临的系统有效性、信息完整性、身份认证和隐私和机密性保护方面的安全威胁, 5G 网络也有相应的安全架构来应对. 相比 LTE, 5G 网络的密钥体系、身份认证方面都更加复杂, 增强了抵抗攻击的能力. 同时 5G 网络的移动性和网络注册协议都更加灵活以适应 5G 网络的需求, 并且增强了用户面和运营商网络间的信息交互的安全 [12].

5G 安全架构跨越 UE、无线接入网络、核心网和应用程序等, 主体架构可以分为应用层、服务层和传输层. 根据各个层之间不同的信息传递, 又可以将 5G 安全架构划分为 6 个安全域, 如图 1 所示, 其中 (I)∼(V) 分别表示网络接入域、网络域、用户域、应用程序域和服务框架 (service-based architecture, SBA) 域, 可见性和可配置性域没有在图 1 中显示. 3GPP 标准在各个安全域中定义了不同的安全功能, 这些安全功能结合在一起构成了完整的 5G 安全架构 [12].

5G 核心网架构的变化使得 5G 安全架构也有一些相应的变化. 一方面, 5G 核心网架构为了更灵活地引入垂直行业结构, 采用了基于服务的网络架构, 以满足垂直行业灵活的需求. 因此在 5G 安全架构中新增 SBA 安全域以保障 SBA 域内的网络功能之间的安全通信. 另一方面, 5G 实现了核心网和接入网的解耦, 其主要目标就是通过核心网对其他接入技术的支持实现运营商对接入网系统的统一管理与控制. 同时, 5G 非 3GPP 接入框架还支持非可信的非 3GPP 接入架构, 并提供统一接入和鉴权服务. 因此 5G 接入域安全新增了保障非 3GPP 接入的安全通信. 本节将主要从信任模型和密钥体系、

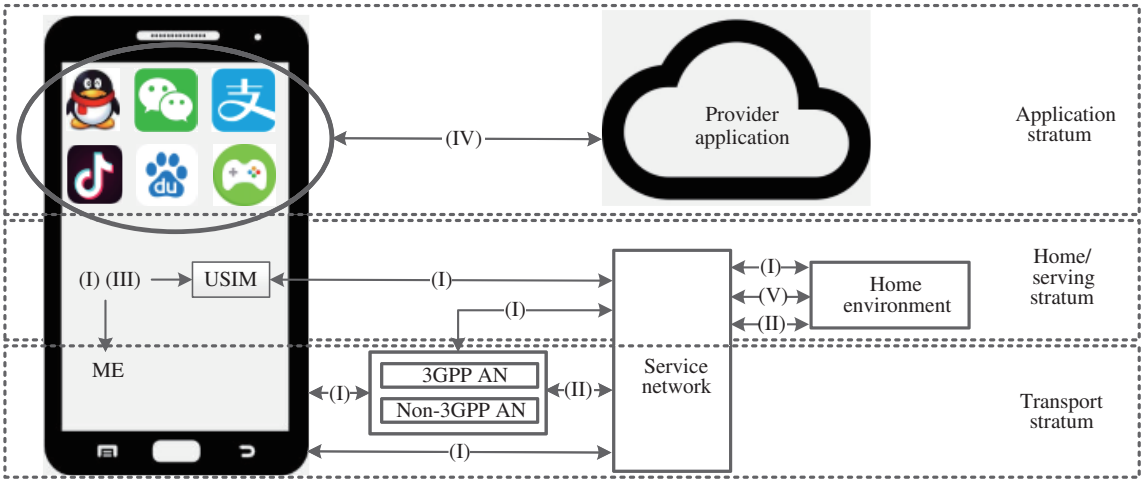

图 1　(网络版彩图) 5G 安全体系结构概述

Figure 1　(Color online) 5G security architecture overview

身份认证、安全上下文与公共陆地移动网之间的安全, 以及用户面安全 4 个方面具体阐述 5G 安全架构中的一些重要的安全功能.

3.1　信任模型和密钥体系

由于 5G 服务框架的更新, 5G 安全的信任模型也发生了相应的变化. 用户侧由 USIM 和移动设备 (mobile equipment, ME) 组成, 网络侧由有源天线基站 (active antenna unit, AAU)、分布式单元 (distributed unit, DU)、中心单元 (center unit, CU)、安全锚定功能 (security anchor function, SEAF)、认证服务功能 (authentication server function, AUSF)、身份认证凭据存储库和处理函数 (authentication credential repository and processing function, ARPF) 和统一数据管理 (unified data management, UDM) 组成. 如图 2 所示, 在新的信任模型中, 离核心网越近的层越被信任, 离核心网越远就需要越复杂的认证过程, 通用用户标识模块 (universal subscriber identity module, USIM) 离核心网最远也就需要最复杂的认证过程 [7].

5G 的密钥体系是 5G 信任模型的重要体现, 5G 的长期密钥储存在 UDM/ARPF 中, 其他派生的密钥储存在 SEAF, AUSF 和 AMF 中. UDM 可以实现身份认证凭据生成、用户标识、服务和会话连续性等功能. 5G 密钥体系中的派生密钥层次丰富, 以应对更复杂的无线环境.

3.2　身份认证

5G 中有两种认证类型, 一种是所有设备访问移动网络服务时必须执行的主认证, 另一种是在外部数据网需要的时候进行的二次认证 [12]. 在 LTE 身份认证过程中, IMSI 在 LTE 网络中不经过任何加密被清晰地发送, 因此导致了各种隐私相关的攻击. 而在 5G 网络中被发送的是经过加密的 SUCI, 需要认证的时候会在 UDM/ARPF 中返回经过解密的 SUPI 进行身份认证, 如图 3 所示. 基于 SUCI 和 SUPI 的 5G 主身份认证解决了 IMSI 暴露在无线环境中的风险, 同时还提供二次认证, 增强了身份认证安全.

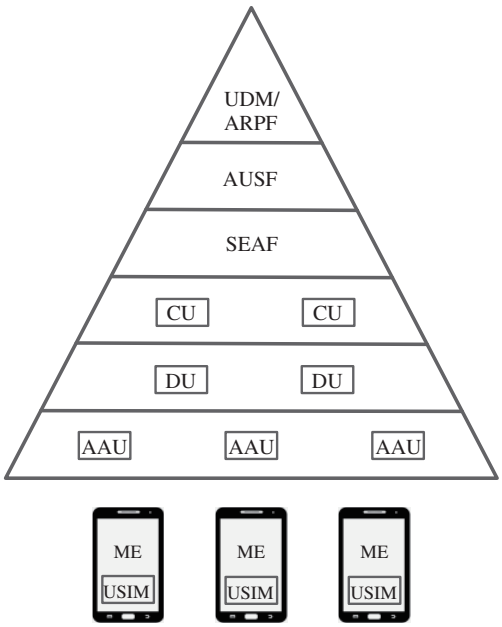

图 2　5G 信任模型

Figure 2　5G trust model

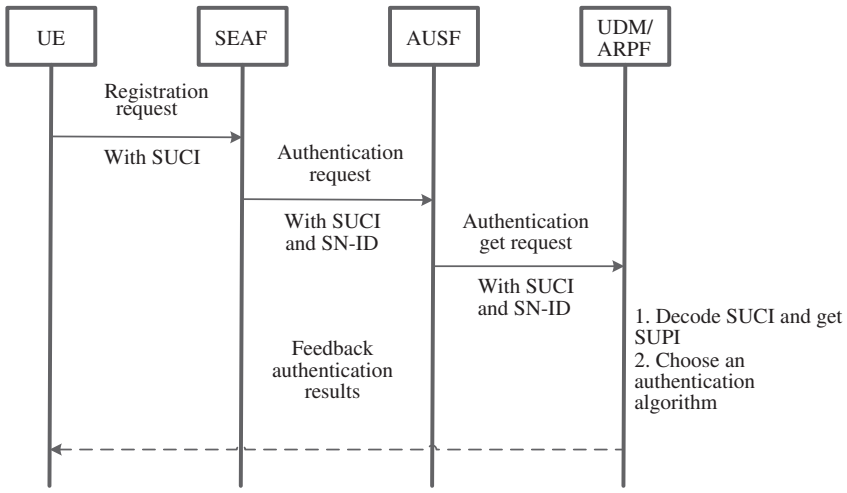

图 3　5G 主认证程序

Figure 3　5G primary authentication procedure

3.3　安全上下文与公共陆地移动网之间的安全

由于 5G 网络允许非 3GPP 网络的接入, 并且可以支持用户分别通过 3GPP 和非 3GPP 网络在 5G 网络中注册 [12]. 因此 5G 支持多注册网络的安全上下文管理, 而 LTE 不支持多注册安全上下文管理.

在 5G 网络中, 为了确保跨网互连, 即用户在不同公共陆地移动网 (public land mobile network, PLMN) 之间漫游的安全性, 5G 安全架构引入安全边缘保护代理 (security edge protection proxy, SEPP)

表 1　5G 相对 LTE 的安全增强

Table 1　5G security enhancements over LTE

Security aspects	5G	LTE
Trust model	Composed of AMF, SEAF, AUSF, UMD, and ARPF.	Composed of MME, HSS, and AuC.
Authentication	Using SUCI and SUPI for authentication, EAP-AKA and 5G AKA are necessary authentication methods. Secondary authentication can be carried out if the external data network required.	Using IMSI and TMSI for authentication, the authentication method is EPS AKA and does not support secondary authentication.
Security context	Additional security context management in the case of multiple registrations.	Does not support multiple registration security contexts.
Security between PLMNs	Ensure security between PLMNs through SEPP and N32 interface.	No SEPP.
Mobility	With more flexible mobility management, operators can decide whether to perform Xn or N2 handover for a specific gNB according to the security features of a specific gNB. Xn handover is only switched through the Xn interface without involving AMF.	Mobility management must be done through AMF.
User plane security	Additional optional integrity and confidentiality protection.	No integrity and confidentiality protection.

作为驻留在 PLMN 周边的实体, 为跨两个不同 PLMN 之间交换的所有服务层信息实现应用层安全[12]. SEPP 提供完整性保护, 部分消息和重放保护的机密性保护, 相互认证, 授权和密钥管理. 这也是新增的接口来增强 5G 网络的安全, 以满足用户在不同 PLMN 之间频繁切换过程中的安全需求.

3.4　用户面安全

用户面和控制面的分离是 5G 核心网的重要特征, 因此需要新的安全措施来保护用户面安全. 在 PDU 会话建立过程中, SMF 需要向 gNB 提供 PDU 会话的用户平面 (user plane, UP) 安全策略. UP 安全策略用于为属于 PDU 会话的所有无线数据承载 (data radio bearers, DRP) 提供 UP 机密性和完整性保护, 增强了用户面安全.

5G 安全架构中新增的 SEAF 等安全功能单元和新的密钥体系以及基于 SUCI 和 SUPI 的 5G 认证程序有效地保护了身份认证的安全, 防止了 IMSI 等信息在空口中的暴露的风险. 新增的 SEPP 安全功能增强了 PLMN 之间的信息完整性和机密性, 同时也增强了用户在 PLMN 间通信的身份认证安全, 保护了用户在漫游环境下的通信安全. 用户面安全则是在 5G 系统用户面和控制面分离的情况下增强了用户面信息的完整性和机密性保护. 总的来说, 5G 安全架构有效地防止了针对 5G 系统的安全威胁, 保护了用户和网络的通信安全, 其相对于 LTE 的安全增强如表 1 所示.

4　5G 和 B5G 的安全技术研究进展

在现有 5G 安全架构的基础上, 为了提升 5G 安全能力, 可从物理层、网络层及应用层分别进行设计和优化. 5G 物理层安全增强技术主要从提升信道抗截获能力与提升信号安全保密容量角度, 增强通信系统的安全性能. 已知的可用于增强物理层安全的技术包括波束赋形、预编码、全双工技术、智能抗干扰优化算法、毫米波通信和大规模多输入多输出 (multiple input and multiple output, MIMO)

等. 网络层安全增强技术通过设计或改进交互协议, 解决现有通信协议中可能存在的安全漏洞, 实现网络层安全. 应用层安全是以用户终端为中心, 针对 5G 多元应用场景所表现出的一些特征, 在不同的应用场景下设计不同的抵抗攻击方案达到增强系统安全的目的. 这些方案可以是多个物理层安全技术的组合, 或是多个网络层安全策略的组合, 也可是物理层安全技术与网络层安全策略的组合. 从应用场景角度区分, 相对于 4G 网络, 需要引入安全增强技术的 5G 和 B5G 的场景包括设备到 D2D, V2X 和物联网等.

4.1 物理层安全

现在的移动通信安全主要依靠加密和解密技术以及一些相关安全协议. 基于加密的安全技术存在计算复杂度高、密钥管理成本高等缺点. 物理层安全技术以信息论框架为基础, 利用物理介质固有的随机性和合法信道与窃听信道的差异性, 保证信息安全传输. 与加密方法相比, 物理层安全不依赖于通信设备的计算能力, 可以降低复杂度和资源节约, 同时, 窃听者即使有强大的计算能力, 依然可以实现安全可靠的通信 [33]. 此外, 通过利用物理层特性, 物理层安全技术还可以根据信道的变化和不同的安全需求灵活地调整传输策略和参数 [34]. 因此, 物理层安全吸引了越来越多的研究人员, 是过去 20 年来非常活跃的研究领域. 目前物理层安全技术主要包括波束赋形和预编码、全双工技术、智能抗干扰优化算法、毫米波通信和大规模 MIMO.

4.1.1 波束赋形和预编码

新一代的 5G 基站支持 64 发 64 收的天线阵列, 这极大地满足了波束赋形和预编码的需求. 目前的天线阵列主要用于初始随机接入、寻呼、数据和控制信息, 以及移动性处理 [35]. 由于多天线阵列对波束赋形的支持, 使其成为实现物理层安全的有效途径 [36]. 安全波束赋形通常是指在多个天线或节点上只传输一个数据流的单级传输. 波束赋形可以将在合法接收方方向的信号功率增强而减少其他方向的信号功率, 这样在增强合法信道信噪比的同时降低了窃听信道的信噪比, 从而实现安全传输 [37], 如图 4 所示. 在文献 [38] 中, 作者提出了一种混合的合作波束赋形和干扰方案, 以提高具有窃听者的单天线双向中继网络的物理层安全性能. 利用人工噪声也是波束赋形中一种很好的物理层安全方法. 在文献 [39] 中, 作者提出了一种人工噪声辅助的最优波束赋形方案, 这种方案可在满足低层信息保密速率约束的前提下, 降低窃听者接收到的信号的质量, 从而最大限度地提高更高级别的信息安全性能.

保密速率是评估物理层安全策略传输效率的基本指标. 在物理层安全中, 保密率被定义为每秒在给定信道上传输的秘密比特数, 通常假设信源输入服从高斯分布. 保密容量是保密速率的上限, 即源节点的机密消息能够安全可靠地传输到目标节点的最大保密速率. 对于高斯信道, 其保密容量为

$$C_{\mathrm{s}} = C_{\mathrm{d}} - C_{\mathrm{e}} = \log\left(1 + \frac{S_{\mathrm{d}}}{N_{\mathrm{d}}}\right) - \log\left(1 + \frac{S_{\mathrm{e}}}{N_{\mathrm{e}}}\right), \tag{1}$$

其中 C_{s} 表示非退化窃听信道的保密容量, C_{d} 和 C_{e} 分别表示目标用户信道和窃听信道的 Shannon 容量, S_{d} 和 S_{e} 分别表示目标用户和窃听者的接收信号功率, N_{d} 和 N_{e} 分别表示目标用户和窃听者的噪声功率 [40]. 图 5 中, 假设窃听者和目标用户都可以得到完美的信道状态信息 (channel state information, CSI), 窃听者和目标用户有同等水平的接收机噪声. 由于有波束赋形的存在, 窃听者的接收信号功率会小于目标用户的接收信号功率. 从图中可以看出, 随着 $S_{\mathrm{e}}/S_{\mathrm{d}}$ 的逐渐减小, 窃听信道容量逐渐减小, 可达保密容量逐渐增大, 表示保密性能越好.

预编码技术在多节点协作网络中有着广泛的应用, 也是实现物理层安全的有效途径 [36]. 安全预编码是指同时传输多个数据流的多级传输. 一般来说, 波束赋形是预编码的一种特殊情况. 预编码是

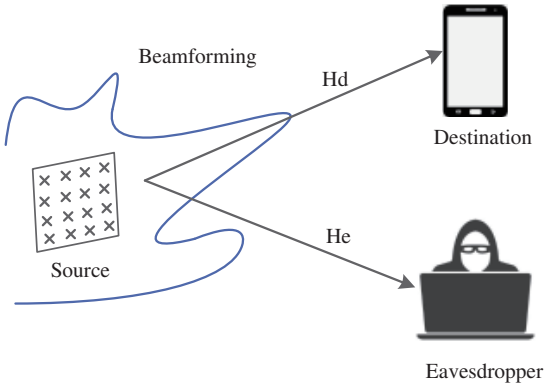

图 4 (网络版彩图) 波束赋形安全传输示意图

Figure 4 (Color online) Beamforming secure transmission

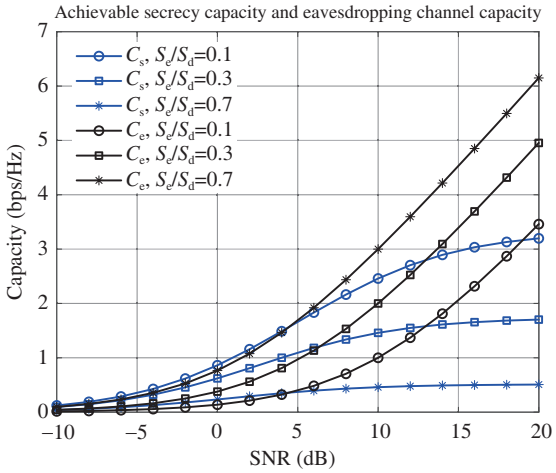

图 5 (网络版彩图) 波束赋形可达保密容量和窃听容量

Figure 5 (Color online) Beamforming for confidential and eavesdropping capacity

实现物理层安全中不同设计目标的另一项重要技术, 尤其适用于多流数据传输或多用户访问. 当所设计的收发器装有多个天线时, 一个或多个用户的信息可以通过预编码在空间上复用到多个独立的子信道. 通过对预编码器的优化, 可以定向地将信息发送给多个合法的接收方, 而窃听方的信道质量将变得很差 [41]. 文献 [42] 研究了多小区大规模 MIMO 系统在无源多天线窃听器存在的情况下, 采用结合匹配滤波器预编码和人工噪声的安全下行链路传输方案的可行性.

目前关于波束赋形和预编码技术的研究重点在于如何分别在完美 CSI 和非完美 CSI 的情况下高效准确地构造一个预编码矩阵. Liu 和 Poor [43] 提出的保密脏纸编码 (secret dirty-paper coding, S-DPC) 可以达到最大的保密速率. 然而, 由于 S-DPC 的复杂性, 在计算上难以实现, 因此很难将这种预编码方案应用于实际. 为了降低计算复杂度并促进其实际应用, 已经开发了较为简单的线性预编码技术, 其中广义奇异值分解和正则化信道反转被广泛应用于物理层安全传输中 [44, 45].

4.1.2 全双工技术

全双工技术是指交换机在发送数据的同时也能够接收数据, 两者同步进行. 信息的接收方可以在接收信息的同时发出干扰信号, 这个干扰信号可以是基于窃听信道的人工噪声, 这样可以有效降低窃听信道的质量, 从而有效保护物理层安全 [46]. 在多跳中继系统中, 全双工中继在接收信息的同时将干扰信号发送给窃听者可以增强无线物理层安全性 [47]. 在物联网网络中, 文献 [48] 提出了一种主从全双工技术, 每个物联网节点生成一个相位调制的随机密钥传输给主节点, 同时主节点使用全向天线广播高功率信号, 这样既可以掩盖物联网节点生成的密钥还可以降低窃听者接收信噪比. 全双工接收机下新的信道训练方案也可以增强物理层安全性, 接收机传输有限数量的导频符号用于估计信道, 秘密的信道训练方案可以防止窃听者估计接收机到窃听者的干扰信道 [49].

4.1.3 智能抗干扰优化算法

智能抗干扰优化算法指的是针对无线环境中可预测和不可预测的干扰攻击, 利用深度学习的优化算法合理分配功率、频率、信道等资源以抵抗干扰攻击. 目前的智能抗干扰算法主要包括 Q 学习 [50]、

强化学习 [14] 和生成对抗网络算法 [51]. 文献 [50] 针对认知无线网络中的竞争性移动网络博弈, 将通信节点与干扰节点融合在一起, 利用 Q 学习算法给出最佳的信道访问策略. 文献 [14] 针对下行非正交多址系统中存在的智能干扰器, 提出了一种在无需了解干扰和无线电信道参数的情况下基于强化学习的功率控制方案. 文献 [51] 为干扰器开发了一个生成对抗网络, 以通过使用合成样本扩充训练数据集来减少收集训练数据集的时间, 同时开发了一种在频谱访问中可靠的干扰分类器. 除了利用深度学习算法, 基于 Markov 博弈框架的抗干扰防御模型也是一个研究方向 [52].

4.1.4 毫米波通信和大规模 MIMO

毫米波通信作为 5G 中的一个重要技术, 它能有效提高系统带宽, 极窄的波束有利于增强系统的安全性 [53]. 已有的研究主要包括: 随机几何框架下毫米波蜂窝网络的物理层安全性能 [54]、毫米波自组织网络中的物理层安全 [55], 以及毫米波蜂窝网络安全性能的数学框架分析 [56].

由于毫米波的频率特性, 其天线一般用阵列的形式来体现, 可以与大规模 MIMO 技术相结合实现更好的通信性能 [57]. 通过在基站使用大量天线, 大规模 MIMO 可以提供高频谱效率和能量效率, 以同时支持更多用户, 并将大部分信号处理和计算从用户终端转移到基站, 而且, 大规模 MIMO 可以提高通信的安全性 [58]. 已有的研究包括:

(1) 不完美 CSI 的多用户 MIMO 物理层安全 [59];

(2) 匹配滤波器预编码和基站人工噪声的多小区安全大规模 MIMO 传输方案 [42];

(3) 大规模 MIMO 中继系统中安全通信的功率和时间分配 [60];

(4) FDD 大规模 MIMO 系统的下行信道训练抵抗多天线干扰 [61];

(5) TDD 导频污染攻击下的数据辅助安全大规模 MIMO 传输 [62].

物理层安全是利用物理介质固有的随机性和合法信道与窃听信道的差异性来保证通信的安全, 这是它的优点, 也是它的缺点. 优点是它不依赖于通信设备的计算能力, 可以降低复杂度和资源节约, 缺点是密钥生成和协商的成功依赖于信道估计的准确性. 波束赋形、预编码、全双工技术, 以及大规模 MIMO 技术都是利用对信道信息的估计实现通信安全, 智能抗干扰技术则是利用足够多的先验信息以及 Q 学习, 强化学习等深度学习算法生成物理层抗干扰策略来抵御干扰攻击. 随着深度学习算法的逐步优化, 人工智能算法与大规模 MIMO, 全双工技术等物理层技术的联合抗干扰策略将是物理层安全研究的重要方向.

4.2 网络层安全

网络层安全通过加密解密技术以及协议栈来增强通信安全, 一直以来都是 5G 安全的重点关注领域. 5G 网络层安全研究主要关注网络切片 [63]、SDN/NFV [64,65]、隐私保护 [66]、密钥体系和认证增强等方面 [67].

4.2.1 SDN/NFV 与网络切片安全

SDN 与 NFV 是 5G 网络的重要技术, SDN 通过将控制平面与数据平面解耦, 实现了对网络的集中控制, 带来了更简单、更可编程、更灵活的网络管理 [68]. NFV 可以通过软硬件解耦及功能抽象, 使网络设备功能不再依赖于专用硬件, 资源可以充分灵活共享, 实现新业务的快速开发和部署等 [69]. 5G 网络切片可以根据用户需求, 通过动态切割、调度、多个独立虚拟网络的组合而成为多个虚拟网络功能 (virtual network functions, VNF), 这些 VNF 可以基于虚拟化技术为用户提供定制的需求服务 [70]. 网络切片提供者向用户提供定制的网络切片服务时, 不仅满足用户性能要求, 还满足用户安全要求. 网

络切片技术的引入, 使得网络边界变得十分模糊, 目前关于网络切片安全的讨论聚焦于网络切片特定的身份认证以及信令数据的机密性保护和归属控制问题 [63].

文献 [64] 对 SDN 安全方面的研究进行了全面的综述, 讨论了使用 SDN 框架带来的安全性增强和框架带来的安全性挑战. 已有相关研究提出利用网络流量的拓扑特性 [71] 和区块链技术 [72] 解决 SDN 安全问题.

针对 NFV 安全, 文献 [65] 介绍了 NFV 中存在的关键安全威胁, 并提出了防范这些威胁的最佳安全策略. 文献 [73] 介绍了一种基于策略安全管理和监控的多用户 NFV/SDN 5G 接入网整体安全架构的智能分析以应对 NFV 中的安全威胁. 3GPP TR 33.818 [74] 和 TR 33.848 [75] 定义了针对网络功能虚拟化产品的安全保障方法和安全保障规范, 考虑了虚拟化对 3GPP 架构的影响, 以便识别威胁和应对后续的安全要求. 目前关于虚拟化的安全问题主要聚焦于为 3GPP 虚拟网络产品执行安全保障方法的参与者也应该得到安全保障机构的认证, 虚拟网络产品的安全保障过程与 3GPP 物理网络产品评估过程相同, 同时每个网络产品类别只考虑一个安全保障方法 (security assurance methodology, SECAM) 级别, 可以降低网络产品评估的复杂性 [74].

针对 5G 网络切片中的网络安全差异问题, 文献 [76] 提出了网络切片安全信任度的概念, 并建立了一个信任模型来衡量所提供的网络切片服务能够满足的期望. 文献 [77] 提出了一个基于按需切片隔离的模型在保证 5G 核心网端到端延迟的情况下用来来防御 DDoS 攻击. 3GPP TR 33.813 [63] 研究了网络切片特定访问身份认证和授权解决方案相关的安全和隐私问题、网络切片与 EPC 互通安全问题, 以及其他与网络切片相关的开放性安全问题, 包括切片间安全隔离、漫游方案中切片的安全性、切片管理安全等.

4.2.2 隐私保护

隐私保护在 5G 网络中是一个很大的威胁 [21]. 根据隐私信息的类型, 可以将 5G 网络中的隐私分为数据隐私、位置隐私, 以及身份隐私 [66]. 利用冗余机制的数据私有保护算法 [78] 和大数据隐私保护算法 [79] 可保护数据隐私. 位置隐私保护方法包括基于差分隐私约束的位置隐私保护方法 [80]、位置隐私保护机制的量化框架 [81] 和隐私需求和服务质量需求之间平衡的隐藏技术 [82]. 技术报告 3GPP TS 33.814 研究了 5G 系统中增强位置服务的潜在安全问题, 包括授权和隐私保护等安全关键问题, 详细说明了解决方案 [83]. 为保护身份隐私, 文献 [84] 提出了一种在移动边缘计算中基于零知识证明和令牌验证的安全身份管理方法来减轻统一身份管理中的攻击.

4.2.3 密钥体系和认证增强

随着计算机结算能力的提高, 特别是量子计算的发展, 关于密钥体系增强的讨论越来越多. 技术报告 3GPP TR 33.834 对 USIM 中保存的 3GPP 长期密钥的远程更新进行了研究, 目前 5G 中的长期密钥 K 是 128 或 256 位, 且用于 UE 和 gNB 之间的数据机密性和完整性保护的加密算法是 SNOW 3G, 基于 128 位的 AES 和基于 128 位的 ZUC 算法. 面对长期密钥泄露的风险, 该报告提出了密钥更新, 预设多组密钥, 建立基于证书的相互身份认证的安全通道和基于 Diffie-Hellman 算法的长期密钥生成等解决方案 [67].

技术报告 3GPP TR 33.841 评估了量子计算可能造成的威胁和 5G 系统中的相关对策, 同时评估了采取对策的时间表, 特别是将密钥长度增加到 256 位, 并研究了其预期性能. 量子计算中的 Shor 算法及其变体可以极大地提升整数因子分解和有限域或者椭圆曲线中的离散对数的计算效率, 对非对称加密算法有极大的威胁. Grover 算法可以提升破解分组密钥的效率, 由于 Grover 算法不能有效地进

行并行化运算, 目前可以通过增加密钥长度来减少量子计算对于对称加密算法的威胁. 该报告指出基于 256 位的加密算法不仅应该能够满足 5G 的峰值数据速率, 而且还应该能够达到下一代移动网络的峰值数据速率. 同时, 由于数据通常经过多次加密和解密, 基于 256 位的加密算法会增加系统的端到端延迟. 最后报告建议取消目前仍在使用的密钥长度小于 128 位的密钥 [27]. 技术报告 3GPP TR 33.846 则是研究了在长期密钥泄漏的情况下如何增强身份认证过程、减轻可链接性攻击、减轻由于隐藏 SUPI 而导致的潜在 DDoS 威胁等 [24].

在身份认证增强中一个重要的方向就是要防止伪基站的攻击. 伪基站通常用来获取合法用户的 IMSI 信息来便跟踪用户的位置、窃听电话或冒充用户 [18]. 5G 系统已经在打击伪基站方面进行了重大改进, 包括 SUPI 隐藏等, 使得在空口中不会出现 SUPI. 但是如果伪基站对用户实施降阶攻击, 使用户降回 4G (5G 不允许降阶接入 2G/3G 网络), 则仍然可以实施类似攻击, 从而导致用户隐私泄露. 5G 初始部署阶段, 运营商可能允许用户不更换 USIM 卡直接接入 5G 网络, 仍然有可能泄露用户 IMSI 信息. 当前仍有 4G/5G 无法覆盖的地区, 而用户接入策略中很难对用户进行区域限制, 因此运营商可能不得不允许用户回到 2G/3G 网络, 仍然存在降阶攻击的可能. 已有一些研究通过位置区域特征 [28] 和增加假名 [85] 的方式来保护 IMSI. 3GPP TR 33.809 面对现实中存在的伪基站攻击如 IMSI 捕获器, 研究了相关的潜在威胁和隐私保护问题以及减轻相关风险的潜在解决方案 [86].

除了传统的认证增强, 基于机器学习的身份认证也是一个重要的研究方向. 文献 [87] 提出了一种利用物理层属性构建的基于机器学习的新身份验证方法, 并将人工智能引入身份认证以实现更有效的安全性配置.

网络层安全主要针对由 5G 网络新引入的 SDN/NFV 和网络切片技术以及量子计算对密钥体系和数据机密性, 完整性保护的威胁. 新技术的引入增强了 5G 系统的管理能力以及满足了用户的性能需求, 但同时增大了 5G 系统面临的网络攻击和窃听风险, 因此需要新的网络安全策略来抵御攻击和窃听. 而面对量子计算的威胁, 现有的加密技术以及密钥长度并不能够满足需求, 特别是非对称加密技术, 因此需要新的加密算法以及更长的密钥来防止量子计算机的攻击.

4.3 应用层安全

应用层安全是以用户终端为中心, 针对 5G 多元应用场景所表现出的一些特征, 在不同的应用场景下设计不同的抵抗攻击方案达到增强系统安全的目的. 这些方案可以是多个物理层安全技术的组合, 或是多个网络层安全策略的组合, 也可是物理层安全技术与网络层安全策略的组合. 从应用场景角度区分, 需要引入安全增强技术的 5G/B5G 场景包括 D2D, V2X 和物联网等.

4.3.1 D2D/车联网

在 D2D 通信中, 设备无需通过基站即可相互通信, 因此可以在 5G 中高效利用频谱, 还可以有效地减轻基站的流量负担. 为了改善频谱效率, D2D 链路通常采用动态频谱访问, 这可能会产生诸如干扰的安全威胁 [88]. 车联网技术也是基于 D2D 技术, 目前的车联网技术也面临着严重的安全威胁.

目前针对 D2D 安全的研究包括基于广泛审查的 D2D 通信安全增强 [89]、基于 NOMA 协同的 D2D 抗干扰框架 [90] 和基于阈值的联合警戒区访问控制方案以提高 D2D 用户的保密吞吐量 [91].

针对 V2X 的安全增强问题, 文献 [92] 提出了适用于 V2X 的两种轻量级匿名认证方案. 2020 年 6 月 R16 阶段 3 冻结的技术报告 3GPP TR 33.836 分析了增强 V2X (enhanced V2X, eV2X) 系统体系结构的安全性和隐私, 提出了潜在的安全性和隐私要求, 针对 V2X 中可能出现的 UE 跟踪威胁, 文献 [93] 提出了 ID 随机更改的保护方案. 目前关于 V2X 的安全研究聚焦于 PC5 上单播、组播和广播通信的

安全, 包括完整性保护以及机密性保护. 面对 5G R17 中 eV2X 场景中的中继技术研究, 安全也会成为焦点问题之一.

4.3.2 物联网

由于 loT 节点的计算能力有限, 因此 5G loT 设备中的安全服务需要高效轻便. 中继已被认为是 loT 网络中一种有效的机制, 可以节省 loT 节点的功率并扩展传输范围 [8]. 文献 [94] 广泛回顾了 IoT 安全的相关研究, 总结了加密机制、通信安全、传感器数据保护和密码算法等关键技术的研究现状. 目前针对 IoT 安全的研究包括: RFID 安全标签研究 [95]、物联网安全中继通信设计 [96], 以及基于博弈论的抗干扰技术 [97]. 技术报告 3GPP TS 33.163 定义了针对电池功率受限的极低吞吐量机器类型通信设备设计的通信安全过程, 包括: 用于端到端安全性的密钥协议服务、身份认证和机密性保护 [98]. 技术报告 3GPP TR 33.861 研究了在 5GS 中支持 EPS CIoT / MTC 功能的安全性, 如不频繁和小数据传输、CIoT 的 EPC-5GC 互通, 以及解决 5G 服务需求的架构增强的安全性 [99].

应用层安全融合了物理层安全和网络层安全技术, 从具体的应用场景出发, 构建符合场景特点的联合安全策略. D2D 中的动态频谱访问和 IoT 中的低功耗多连接等特性给信息的安全传输带来了新的挑战. 如何在资源受限的情况下给出最优的安全策略成为应用层安全研究的重点.

5 未来研究展望

根据已公开的文献, 本文从物理层、网络层和应用层对未来 B5G 安全可研究的方向进行了归纳.

5.1 物理层安全

目前的物理层安全研究主要存在两个问题, 一个是物理层安全的研究在很大程度上取决于对瞬时无线信道的准确感知和估计以及对瞬时信道特征的准确提取. 在移动性较强的场景下, 无线信道状态对时间比较敏感, 导致不同时隙的信道差异较大, 对信道估计的准确度造成影响; 而在开放式的室外场景中, 由于缺乏多径反射, 导致不同用户的信道差异不大, 影响信道特征的提取. 目前大多数的物理层安全研究都假设可以获得完美的 CSI 或者可以获得部分 CSI 信息 [37,59]. 另一个问题是物理层安全技术的两面性. 大规模 MIMO 和全双工技术是一把双刃剑, 一方面使得 5G 物理层安全得到巨大的提升, 但如果窃听者同样具有多天线基站以及全双工中继, 也会增强窃听者的窃听能力 [40]. 而且目前已经出现了一种智能干扰器, 攻击者使用可编程的智能无线电设备根据当前的无线电环境灵活地控制器干扰策略 [14]. 人工智能 (artificial intelligence, AI) 与 5G 的融合是未来 5G/B5G 的发展方向, 研究重点包括 5G 网络优化、最佳资源分配和端到端物理层联合优化等 [100,101]. 基于 AI 的的物理层安全优化算法可以针对不同的攻击者和攻击策略合理分配资源, 制定最优的防御策略, 包括基于深度学习的干扰检测, 灵活的身份认证 [87], 通信行为分析等. 针对目前物理层安全研究中存在的问题, 针对目前物理层安全研究中存在的问题, 基于人工智能算法实现对无线信道信息的准确估计、大规模 MIMO 优化、全双工技术等物理层技术的联合抗干扰策略将是物理层安全研究的重要方向.

5.2 网络层安全

未来网络层安全主要面临的是新技术、新应用, 以及新空口导致的攻击面扩大以及未来量子计算发展带来的安全风险. 网络切片、异构网络、有线网络与无线网络的融合, 空天地一体化等 3GPP 与非 3GPP 网络之间的融合会导致网络边缘层次增加, 网络边界变得十分模糊, 越来越多的攻击者乐于在网络边缘发动攻击 [102]. 同时数据挖掘和量子计算也将对网络中数据的机密性、完整性传输, 以及

身份认证造成威胁. 面对这些攻击, 现有的网络层安全技术主要考虑增强边缘安全, 如何突破网络边界和原有信任模型的限制实现安全成为一个重要的研究方向. 而内生安全技术和基于零信任体系的网络信任模型有望解决这一问题. 内生安全技术的核心是使得网络具有自主抵御未知安全威胁的能力, 当出现安全漏洞的时候不是去 “打补丁”, 而是网络系统内部可以自主识别判断攻击类型和方式等, 并作出相应的安全防范措施, 这需要借助于深度学习算法实现自主的安全防护. 基于零信任体系的网络信任模型的核心则是不信任任何环境并且始终认证以确保用户身份安全和保护应用程序 [103]. 但是遵循始终认证的原则也会使得工作量增加, 同时降低用户体验. 如何平衡用户体验安全需求, 构建基于零信任体系的网络信任模型将成为未来网络层安全的重要研究方向.

5.3 应用层安全

随着 5G 网络基础设施的不断完善, 物联网场景也会分化为一个个细分领域, 如工业物联网、智慧城市等, 面对新兴的细分物联网领域, 如何在资源受限的情况下结合自身的特点给出最优的安全策略成为物联网安全研究的重点 [104, 105], 区块链技术有望在物联网安全中扮演重要角色 [106]. 除了物联网应用场景下的安全问题, 卫星通信与 5G 系统融合场景下的安全问题也值得关注 [107]. 其中, 物理层安全技术是实现星地链路安全的有效方法 [108].

6 结论

综上所述, 本文重点总结了 5G 和 B5G 的安全最新研究进展, 从面临的安全威胁、5G 安全架构, 以及安全技术研究现状 3 个方面, 从方法到标准对相关研究进展进行了广泛的回顾. 首先本文从对系统有效性、信息完整性、身份认证、隐私保护 4 个方面, 分析了 5G 网络面临的安全威胁. 其次, 面对这些威胁, 5G 网络安全架构构建了新的信任模型, 同时在密钥体系、接入与身份认证和运营商网络安全方面, 均有提升安全性能的具体技术方案. 第三, 总结了物理层安全、网络层安全及应用层安全的最新研究进展和标准现状. 最后对未来 B5G 安全可研究的方向进行了归纳.

限于篇幅和作者视角, 本文对 5G 安全威胁和各类安全技术的总结还不能完全展开, 所给结论仅供参考.

参考文献

1 3GPP. System architecture for the 5G system (5GS). TS 23.501 v16.3.0. 2019

2 Shafi M, Molisch A F, Smith P J, et al. 5G: a tutorial overview of standards, trials, challenges, deployment, and practice. IEEE J Sel Areas Commun, 2017, 35: 1201–1221

3 Qualcom. The role of 5G in private networks for industrial IoT. https://www.qualcomm.com/documents/role-5g-private-networks-industrial-iot

4 Huawei. What is China doing to accelerate 5G transport network deployment? https://www.huawei.com/en/about-huawei/publications/winwin-magazine/32-extra/china-accelerate-5g-transport-network-deployment

5 Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61: 081301

6 Markov I L, Fatima A, Isakov S V, et al. Quantum supremacy is both closer and farther than it appears. 2018. ArXiv:1807.10749

7 Prasad A R, Arumugam S, Sheeba B, et al. 3GPP 5G security. J ICT Standardization, 2018, 6: 137–158

8 Fang D, Qian Y, Hu R Q. Security for 5G mobile wireless networks. IEEE Access, 2018, 6: 4850–4874

9 Ahmad I, Kumar T, Liyanage M, et al. Overview of 5G security challenges and solutions. IEEE Comm Stand Mag, 2018, 2: 36–43

10 Cao J, Ma M D, Li H, et al. A survey on security aspects for 3GPP 5G networks. IEEE Commun Surv Tut, 2020, 22: 170–195
11 Khan R, Kumar P, Jayakody D N K, et al. A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. IEEE Commun Surv Tut, 2020, 22: 196–248
12 3GPP. Security architecture and procedures for 5G system. TS 33.501 v15.4.0. 2019
13 Chao C, Lee W, Wang C, et al. A flexible anti-jamming channel hopping for cognitive radio networks. In: Proceedings of International Symposium on Computing & Networking, 2018. 549–551
14 Xiao L, Li Y D, Dai C H, et al. Reinforcement learning-based NOMA power allocation in the presence of smart jamming. IEEE Trans Veh Technol, 2018, 67: 3377–3389
15 Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput Surv, 2007, 39: 3
16 Marco L, Louis M. ENISA threat landscape for 5G Networks. European Union Agency for Cybersecurity. 2019. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks
17 Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. IEEE Commun Surv Tut, 2016, 18: 2027–2051
18 Steig S, Aarnes A, van Do T, et al. A network based IMSI catcher detection. In: Proceedings of International Conference on It Convergence and Security, 2016
19 Huang Y, Jin L, Wei H Q, et al. Pilot contamination with MITM attack. In: Proceedings of the 85th Vehicular Technology Conference, 2017
20 3GPP. system architecture evolution (SAE). TS 33.401 v15.10.0. 2019
21 Huawei. 5G Security: Forward Thinking: Huawei White Paper. 2015. https://roscongress.org/en/materials/bezopasnost-svyazi-5g-vzglyad-v-budushchee-belaya-kniga-huawei/
22 Shubham G, Balu L P, Narendra S C. Security vulnerabilities in handover authentication mechanism of 5G network. In: Proceedings of International Conference on Secure Cyber Computing and Communication. 2018. 369–374
23 Basin D, Dreier J, Hirschi L, et al. A formal analysis of 5G authentication. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security, 2018. 1383–1396
24 3GPP. Study on authentication enhancements in the 5G system (5GS). TR 33.846 v0.3.0. 2019
25 Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574: 505–510
26 Roetteler M, Naehrig M, Svore K M, et al. Quantum resource estimates for computing elliptic curve discrete logarithms. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2017. 241–270
27 3GPP. Study on the support of 256-bit algorithms for 5G. TR 33.841 v16.1.0. 2019
28 Alrashede H, Shaikh R. IMSI catcher detection method for cellular networks. In: Proceedings of International Conference on Computer Applications and Information Security, 2019
29 Wu Y, Schober R, Ng D W K, et al. Secure massive MIMO transmission with an active eavesdropper. IEEE Trans Inform Theory, 2016, 62: 3880–3900
30 Zhou X Y, Maham B, Hjorungnes A. Pilot contamination for active eavesdropping. IEEE Trans Wirel Commun, 2012, 11: 903–907
31 Mukherjee A, Swindlehurst A L. Jamming games in the MIMO wiretap channel with an active eavesdropper. IEEE Trans Signal Process, 2013, 61: 82–91
32 Xu L, Jiang C X, Wang J, et al. Information security in big data: privacy and data mining. IEEE Access, 2014, 2: 1149–1176
33 Wang D, Bai B, Zhao W B, et al. A survey of optimization approaches for wireless physical layer security. IEEE Commun Surv Tut, 2019, 21: 1878–1911
34 Wu Y P, Khisti A, Xiao C S, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J Sel Areas Commun, 2018, 36: 679–695
35 3GPP. Physical layer procedures for data. TS 38.214 v16.0.0. 2020
36 Hong Y W P, Lan P C, Kuo C C J. Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. IEEE Signal Process Mag, 2013, 30: 29–40
37 Mukherjee A, Swindlehurst A L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI.

IEEE Trans Signal Process, 2011, 59: 351–361
38 Wang H M, Luo M, Yin Q, et al. Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. IEEE Trans Inform Forensic Secur, 2013, 8: 2007–2020
39 Zhang W, Chen J, Kuo Y H, et al. Artificial-noise-aided optimal beamforming in layered physical layer security. IEEE Commun Lett, 2019, 23: 72–75
40 Leung-Yan-Cheong S, Hellman M. The Gaussian wire-tap channel. IEEE Trans Inform Theory, 1978, 24: 451–456
41 Zhang H Y, Huang Y M, Li S D, et al. Energy-efficient precoder design for MIMO wiretap channels. IEEE Commun Lett, 2014, 18: 1559–1562
42 Zhu J, Schober R, Bhargava V K. Secure transmission in multicell massive MIMO systems. IEEE Trans Wirel Commun, 2014, 13: 4766–4781
43 Liu R H, Poor H V. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. IEEE Trans Inform Theory, 2009, 55: 1235–1249
44 Fakoorian S A, Swindlehurst A L. Optimal power allocation for GSVD-based beamforming in the MIMO gaussian wiretap channel. In: Proceedings of International Symposium on Information Theory, 2012. 2321–2325
45 Geraci G, Egan M, Yuan J, et al. Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding. IEEE Trans Commun, 2012, 60: 3472–3482
46 Zheng G, Krikidis I, Li J, et al. Improving physical layer secrecy using full-duplex jamming receivers. IEEE Trans Signal Process, 2013, 61: 4962–4974
47 Lee J H. Full-duplex relay for enhancing physical layer security in multi-HOP relaying systems. IEEE Commun Lett, 2015, 19: 525–528
48 Ebrahimi N, Yektakhah B, Sarabandi K, et al. A novel physical layer security technique using master-slave full duplex communication. In: Proceedings of IEEE MTT-S International Microwave Symposium, 2019. 1096–1099
49 Yan S H, Zhou X Y, Yang N, et al. Secret channel training to enhance physical layer security with a full-duplex receiver. IEEE Trans Inform Forensic Secur, 2018, 13: 2788–2800
50 Gwon Y, Dastangoo S, Fossa C, et al. Competing mobile network game: embracing antijamming and jamming strategies with reinforcement learning. In: Proceedings of Communications and Networking Symposium, 2013. 28–36
51 Erpek T, Sagduyu Y E, Shi Y. Deep learning for launching and mitigating wireless jamming attacks. IEEE Trans Cogn Commun Netw, 2019, 5: 2–14
52 Yao F, Jia L. A collaborative multi-agent reinforcement learning anti-jamming algorithm in wireless networks. IEEE Wirel Commun Lett, 2019, 8: 1024–1027
53 Rappaport T S, Sun S, Mayzus R, et al. Millimeter wave mobile communications for 5G cellular: it will work! IEEE Access, 2013, 1: 335–349
54 Wang C, Wang H M. Physical layer security in millimeter wave cellular networks. IEEE Trans Wirel Commun, 2016, 15: 5569–5585
55 Zhu Y X, Wang L F, Wong K K, et al. Secure communications in millimeter wave ad hoc networks. IEEE Trans Wirel Commun, 2017, 16: 3205–3217
56 Vuppala S, Tolossa Y J, Kaddoum G, et al. On the physical layer security analysis of hybrid millimeter wave networks. IEEE Trans Commun, 2018, 66: 1139–1152
57 Jr R W H, González-Prelcic N, Rangan S, et al. An overview of signal processing techniques for millimeter wave MIMO systems. IEEE J Sel Top Signal Process, 2015, 10: 436–453
58 Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. IEEE Commun Mag, 2015, 53: 21–27
59 Yang T H, Zhang R Q, Cheng X, et al. Secure massive MIMO under imperfect CSI: performance analysis and channel prediction. IEEE Trans Inform Forensic Secur, 2019, 14: 1610–1623
60 Chen J, Chen X M, Gerstacker W H, et al. Resource allocation for a massive MIMO relay aided secure communication. IEEE Trans Inform Forensic Secur, 2016, 11: 1700–1711
61 Sheikhi M, Razavizadeh S M. Security vulnerability of FDD massive MIMO systems in downlink training phase. In: Proceedings of International Symposium on Telecommunications, 2018. 492–496
62 Wu Y P, Wen C K, Chen W, et al. Data-aided secure massive MIMO transmission under the pilot contamination

attack. IEEE Trans Commun, 2019, 67: 4765–4781
63 3GPP. Study on security aspects of network slicing enhancement. TR 33.813 v0.6.0. 2019
64 Scott-Hayward S, O'Callaghan G, Sezer S. SDN security: a survey. In: Proceedings of IEEE SDN for Future Networks and Services, 2013
65 Lal S, Taleb T, Dutta A. NFV: security threats and best practices. IEEE Commun Mag, 2017, 55: 211–217
66 Liyanage M, Salo J, Braeken A, et al. 5G privacy: scenarios and solutions. In: Proceedings of IEEE 5G World Forum, 2018. 197–203
67 3GPP. Study on long term key update procedures (LTKUP). TR 33.834 v16.1.0. 2019
68 Dabbagh M, Hamdaoui B, Guizani M, et al. Software-defined networking security: pros and cons. IEEE Commun Mag, 2015, 53: 73–79
69 Hawilo H, Shami A, Mirahmadi M, et al. NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC). IEEE Netw, 2014, 28: 18–26
70 Chen S Z. Analysis and suggestion of future 5G directions. Telecommun Sci, 2016, 32: 1–10
71 Zhang K, Qiu X F. CMD: a convincing mechanism for MITM detection in SDN. In: Proceedings of International Conference on Consumer Electronics, 2018
72 Tselios C, Politis I, Kotsopoulos S. Enhancing SDN security for IoT-related deployments through blockchain. In: Proceedings of IEEE Conference on Network Function Virtualization and Software Defined Networks, 2017. 303–308
73 Siddiqui M S, Escalona E, Trouva E, et al. Policy based virtualised security architecture for SDN/NFV enabled 5G access networks. In: Proceedings of IEEE Conference on Network Function Virtualization and Software Defined Networks, 2016. 44–49
74 3GPP. Security assurance methodology (SECAM) and security assurance specification (SCAS) for 3GPP virtualized network products. TR 33.818 v0.4.0. 2019
75 3GPP. Study on security impacts of virtualisation. TR 33.848 v0.3.0. 2019
76 Niu B, You W, Tang H B, et al. 5G network slice security trust degree calculation model. In: Proceedings of IEEE International Conference on Computer and Communications, 2017. 1150–1157
77 Sattar D, Matrawy A. Towards secure slicing: using slice isolation to mitigate DDoS attacks on 5G core network slices. In: Proceedings of Communications and Networking Symposium, 2019. 82–90
78 Li P, Xu C, Xu H, et al. Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks. China Commun, 2019, 16: 158–170
79 Liu H L. Research on privacy protection framework design and key technologies in large data environment. In: Proceedings of International Conference on Robots and Intelligent System, 2019. 327–330
80 Yin C Y, Xi J W, Sun R X, et al. Location privacy protection based on differential privacy strategy for big data in industrial internet of things. IEEE Trans Ind Inf, 2018, 14: 3628–3636
81 Shokri R, Theodorakopoulos G, Boudec J L, et al. Quantifying location privacy. In: Proceedings of IEEE Symposium on Security and Privacy, 2011. 247–262
82 Zheng J Y, Tan X B, Zou C, et al. A cloaking-based approach to protect location privacy in location-based services. In: Proceedings of Conference on Computational Complexity, 2014. 5459–5464
83 3GPP. Study on the security of the enhancement to the 5G core (5GC) location services. TR 33.814 v16.0.0. 2019
84 Suguna M, Anusia R, Shalinie S M, et al. Secure identity management in mobile cloud computing. In: Proceedings of International Conference on Nextgen Electronic Technologies: Silicon to Software, 2017. 42–45
85 Norrman K, Dubrova E. Protecting IMSI and user privacy in 5G Networks. In: Proceedings of International Conference on Mobile Multimedia Communications, 2016. 159–166
86 3GPP. Study on 5G security enhancements against false base stations. TR 33.809 v0.6.0. 2019
87 Fang H, Wang X B, Tomasin S. Machine learning for intelligent authentication in 5G and beyond wireless networks. IEEE Wirel Commun, 2019, 26: 55–61
88 Adem N, Hamdaoui B, Yavuz A. Pseudorandom time-hopping anti-jamming technique for mobile cognitive users. In: Proceedings of IEEE Globecom Workshops, 2015
89 Haus M, Waqas M, Ding A Y, et al. Security and privacy in device-to-device (D2D) communication: a review. IEEE Commun Surv Tut, 2017, 19: 1054–1079

90 Li Q, Ren P Y, Xu D Y. Security enhancement and QoS provisioning for NOMA-based cooperative D2D networks. IEEE Access, 2019, 7: 129387

91 Wang W, Teh K C, Li K H. Enhanced physical layer security in D2D spectrum sharing networks. IEEE Wirel Commun Lett, 2016, 6: 106–109

92 Yang Y J, Wei Z, Zhang Y C, et al. V2X security: a case study of anonymous authentication. Pervas Mobile Comput, 2017, 41: 259–269

93 3GPP. Study on security aspects of 3GPP support for advanced V2X services. TR 33.836 v0.3.0. 2020

94 Suo H, Wan J F, Zou C F, et al. Security in the internet of things: a review. In: Proceedings of International Conference on Computer Science and Electronics Engineering, 2012. 648–651

95 Fan K, Gong Y Y, Du Z, et al. RFID secure application revocation for IoT in 5G. In: Proceedings of IEEE Trustcom/BigDataSE/ISPA, 2015. 175–181

96 Xu Q, Ren P Y, Song H B, et al. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. IEEE Access, 2016, 4: 2840–2853

97 Hachinyan O, Khorina A, Zapechnikov S. A game-theoretic technique for securing IoT devices against Mirai botnet. In: Proceedings of IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, 2018. 1500–1503

98 3GPP. Battery efficient security for very low throughput machine type communication (MTC) devices (BEST). TS 33.163 v16.2.0. 2019

99 3GPP. Study on evolution of cellular IoT security for the 5G system. TR 33.861 v1.6.0. 2020

100 You X H, Zhang C, Tan X S, et al. AI for 5G: research directions and paradigms. Sci China Inf Sci, 2019, 62: 21301

101 Niknam S, Dhillon H S, Reed J H. Federated learning for wireless communications: motivation, opportunities, and challenges. IEEE Commun Mag, 2020, 58: 46–51

102 Wu H Q. New features of network society and industry challenges in the 5G era. J Chongqing Univ Posts Telecom (Nat Sci Ed), 2020, 32: 171–176 [邬贺铨. 5G 时代的网络社会新特征与产业面临的挑战. 重庆邮电大学学报 (自然科学版), 2020, 32: 171–176]

103 Eidle D, Ni S Y, Decusatis C, et al. Autonomic security for zero trust networks. In: Proceedings of IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, 2017. 288–293

104 Lee J, Kim J, Seo J. Cyber attack scenarios on smart city and their ripple effects. In: Proceedings of International Conference on Platform Technology and Service (PlatCon), 2019

105 Chen H L, Hu M, Yan H, et al. Research on industrial internet of things security architecture and protection strategy. In: Proceedings of International Conference on Virtual Reality, 2019. 365–368

106 Mora O B, Rivera R, Larios V M, et al. A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures. In: Proceedings of IEEE International Smart Cities Conference, 2018

107 Li B, Fei Z S, Zhou C Q, et al. Physical-layer security in space information networks: a survey. IEEE Int Things J, 2020, 7: 33–52

108 Yan S, Wang X Y, Li Z L, et al. Cooperative jamming for physical layer security in hybrid satellite terrestrial relay networks. China Commun, 2019, 16: 154–164

Survey on research and standardization of 5G security technology

Qi QIANG[1], Gang WU[1*], Kaizhi HUANG[2*], Su HU[1] & Shaoqian LI[1]

1. *National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu* 611731*, China*;
2. *National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002*, China*
* Corresponding author. E-mail: wugang99@uestc.edu.cn, Huangkaizhi@tsinghua.org.cn

Abstract With the commercialization of fifth generation wireless systems (5G) and their development in vertical fields such as the Internet of Things, security issues are increasingly gaining attention. This paper provides the latest survey on 5G network security pertaining to potential threats, security architecture, and security technology. The survey begins with the potential security vulnerabilities of 5G, which can be classified according to system availability, information integrity, authentication, privacy, and confidentiality protection. Then, threats and attack methods encountered at different levels are analyzed. Subsequently, the 5G security architecture according to relevant standards is briefly described. Based on the threats and security architecture, security technologies are reviewed based on three categories of 5G and beyond 5G (B5G), such as the physical, network, and application layers. Finally, the survey concludes by presenting observations on potential future directions of 5G and B5G security.

Keywords 5G security, beyond 5G, system architecture, security threats, physical layer security

Qi QIANG was born in Taiyuan, China. He received his bachelor's degree from the University of Electronic Science and Technology of China, in 2018, where he is currently pursuing his master's degree. His research interests include 5G nonorthogonal multiple access and 5G physical layer security.

Gang WU received his B.E. and M.E. degrees from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 1996 and 1999, respectively, and Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2004. In June 2004, he joined UESTC, where he is currently a professor at the National Key Laboratory of Science and Technology on Communications. He was a research fellow at Positioning and Wireless Technology Centre, Nanyang Technological University, Singapore, from November 2005 to February 2007. He was a visiting professor at the Georgia Institute of Technology, Atlanta, GA, USA, from October 2009 to September 2010. He is currently an associate editor of Science China Information Sciences. His research interest includes PHY/MAC techniques for 5G.

Kaizhi HUANG received her B.E. degree in digital communication and M.S. degree in Communications and Information System from the National Digital Switching System Engineering and Technological Research Center (NDSC) in 1995 and 1998, respectively, and Ph.D. degree in Communications and Information System from Tsinghua University, Beijing, China, in 2003. She has been a faculty member of NDSC since 1998, where she is currently a professor and the director of the Laboratory of Mobile Communication Networks. Her research interests include wireless network security and signal processing.

Su HU received his M.S. and Ph.D. degrees in Information and Communications Engineering from the University of Electronic Science and Technology of China in 2007 and 2010, respectively. From 2011 to 2012, he was a research fellow at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He is currently a professor at the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China. His research interests include RadCom fusion systems, sequence design with good correlation properties, and physical layer design for wireless communication systems, such as filterbank multicarrier systems and cognitive radio networks.