



专题：5G 组网与 6G 展望

6G 内生安全：体系结构与关键技术

刘杨, 彭木根

(北京邮电大学, 北京 100876)

摘要: 传统移动通信系统在设计之初把安全作为一种独立的技术, 依靠“补丁式”“外挂式”, 实现无线通信的安全防护。第六代(6G)移动通信系统将基于软件定义切片平台, 注重边缘计算, 采用人工智能和大数据挖掘等适配不同的应用场景和性能目标, 传统的外挂式网络安全机理难以确保 6G 自身对安全内嵌的需求。提出 6G 内生安全机理, 阐述了 6G 内生安全的体系结构和关键技术, 并且针对 6G 将采用的新技术中的安全威胁, 给出了这些威胁的解决方案, 探讨了 6G 内生安全的挑战和未来研究方向。

关键词: 6G; 内生安全; 体系结构; 关键技术

中图分类号: TN915.08

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020011

6G endogenous security: architecture and key technologies

LIU Yang, PENG Mugen

Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: At the beginning of design for the traditional mobile communication systems, security is considered as an independent technology, relying on “patch” and “plug-in” to realize the security protection of wireless communication. The sixth-generation (6G) mobile communication system is designed based on software-defined slicing platform, edge computing, artificial intelligence and big data mining to adapt to different application scenarios and performance objectives, making the traditional network security mechanisms difficult to guarantee 6G’s requirements for embedded security. 6G endogenous security was proposed, the architecture and key technologies of 6G endogenous security were described, the security threats in the new technologies were discussed which 6G would adopt, and the challenges and future research directions of 6G endogenous security were provided.

Key words: 6G, endogenous security, architecture, key technology

1 引言

预计到 2022 年, 全球移动流量将达到每月 77 MB。在移动流量快速增长的驱动下, 第五代(5G)无线通信在满足增强移动宽带(eMBB)、

超可靠低时延通信(uRLLC)和大规模机器类型通信(mMTC)等关键性能要求方面得到了广泛的研究^[1-2]。因此, 5G 网络将在 2020 年广泛部署。然而, 随着移动流量的进一步增长, 5G 在支持具有高度多样化服务需求的大规模互联方面将遇到



技术限制。此外，许多新兴的用例和动态的未来场景促进了对下一代无线通信新范式的需求，即 6G 无线通信。6G 愿景可以概括为：泛在无线智能、无处不在的服务无缝地跟踪与用户无缝连接的泛在服务、与基础设施的泛在无线连接、针对万物的上下文感知的智能服务和应用程序。设想 6G 将通过按需自重构方式驱动无线网络，以确保网络性能的提高和服务类型的增长。6G 网络日益增长的性能要求将促进新技术的部署，例如太赫兹通信、超大规模天线、大智能表面、可见光通信等。

新技术的发展在使 6G 将把人类生活的所有方面连接到网络上从而为人类提供便利的同时，也给网络安全带来了极大的挑战。基本上，当前的安全性主要依赖于位级加密技术和不同层级的安全协议。这些解决方案采用的都是“补丁式”“外挂式”的设计思想。当前网络在设计之初未考虑安全的标准，使得基础网络在身份认证、接入控制、网络通信和数据传输等层面存在着诸多威胁，安全问题严峻。具体体现在公共无线网络中的标准化保护不够安全，即使存在增强的加密和认证协议，它们也会对公共网络的用户产生强约束和高附加成本。现有依靠“补丁式”“外挂式”网络安全增强方案来实现的安全防护体系难以满足要求，因此 6G 网络需要高效、高可用的安全防护能力。

为了应对 6G 网络迫切需要不依赖补丁式安全增强方案的可信安全体系这一挑战，本文提出 6G 内生安全，遵循“内聚而治”“自主以生”的思想构建 6G 网络内生安全体系。从用户、基站和边缘网络 3 个层面，设计 6G 内生安全网络协议和组网机制，达到身份真实、控制安全、通信可靠、数据可信 4 个安全目标，为 6G 网络内生安全体系构建奠定技术基础。

2 基本原理

如今的 5G 网络沿用了先前移动通信系统的

技术路线，使得其在商业部署过程中依然面临很多挑战，6G 网络考虑到先前移动通信系统的局限性，将基于软件定义切片平台与边缘计算，充分利用人工智能与大数据挖掘的融合革新来支持更多样化的应用场景与更高目标的性能要求，但这也使得网络安全形势发生了重大变化。网络逐渐边缘化、软件虚拟化导致网络安全边界逐渐模糊，网络架构所引发的安全缺陷越来越凸显；边缘计算、人工智能与大数据挖掘的深度泛在融合，也使得边缘网络数据安全问题面临着前所未有的新挑战，在革新性技术支持下的新型应用场景产生的网络内部安全问题已不再能依靠传统的独立安全技术得到解决，传统的“外挂式”“补丁式”网络安全防护机制已无法对抗未来 6G 网络潜在的泛在攻击与不定性安全隐患。因此，亟需突破传统的安全防御思想，本文提出一种既顺应 6G 变革性技术的发展，又推进 6G 跨域融合过程中的安全协同，同时满足绿色网络与绿色终端低功耗、低计算能力的轻量级安全防御要求，使网络安全体系从外向内演化，从网络体系架构的角度重新设计安全协议与机制，为 6G 网络注入“内聚而治”“自主以生”基因的 6G 网络内生安全机理。

内聚而治，指 6G 网络通过技术融合与业务融合的背景下对不同安全协议与安全机制的聚合，来对网络进行安全治理；自主以生，指 6G 网络的安全防护应具备自主驱动力，来同步性甚至前瞻性地适应网络变化，以衍生网络内在稳健的防御力。

6G 网络内生安全体系结构将分为接入侧安全与网络侧安全，接入侧安全通过“内聚而治”，为 6G 内生安全网络实现“门卫式”安全保障；而网络域安全提供网络自内向外的安全稳健能力，是体现“自主以生”的重要方面。其中，接入侧安全分为终端安全与基站安全，本文将基于 6G 网络采用的新技术特性，分别从接入侧安全与网络侧安全的角度，对 6G 网络潜在的安全问题及挑战

进行分析,并提出相应的内生安全防护内容。

2.1 接入侧安全

(1) 终端安全

6G网络是一个以陆地移动通信网络为核心的空天地海一体化“泛在覆盖”通信网络,海量异构终端不仅意味着网络内部与外界之间有了更多不安全的攻击入口,也对网络接入认证协议、接入控制协议提出了更高精度的要求,现有机制尽管提高了用户身份认证过程的安全性、身份保密性,但依然存在接入后的合法用户被跟踪、用户服务被降级甚至掉线的漏洞。同时,6G垂直行业应用催生下的多样化软件定义切片网络由于切片接口开放、切片间协议差异等增加了接入攻击口,使终端接入的安全形势变得更为严峻。因此,终端安全面临着恶意终端身份伪造、可信终端接入受阻、接入终端干扰降级、被追踪的安全挑战,6G网络终端安全机制应从身份认证增强的角度保障海量异构终端设备的接入真实、接入可信以及接入终端的防跟踪防掉线保护。

(2) 基站安全

基站安全面临着伪基站带来的各种安全威胁,尽管现有的基站认证机制已经对伪基站的接入防御有了一定程度的增强,但依然无法防御伪基站作为中继节点的一系列攻击,例如伪基站联合异地恶意终端使受害终端“合法”接入异地可信基站,从而在受害终端不知情的情况下进行隐私信息的窃取及篡改。此外,基站的认证机制不能保障在伪基站存在的可疑无线电环境下,终端单播消息的完整性安全以及基站侧广播消息的真实性。对于通过复制真实基站信号参数信息来进行“伪装”的伪基站,也大大增加了主动识别的难度与精度。因此,基站安全面临着伪基站无线环境不安全、伪基站主动识别难精确、伪基站干扰方式多变难规避的安全挑战。对于尝试建立接入前的终端单播消息和基站广播消息,需构建完整性保护技术与认证技术来增强可疑无线电环境

中的可信安全;用户侧的无线环境测量报告应指标丰富化与多维化,增强基站侧对相邻伪基站的检测识别;而对于伪基站的主动规避,除了切换期间规避接入伪基站,基站安全方面还应规避在非接入条件下的伪基站的各种攻击。

2.2 网络侧安全

随着无线通信技术在垂直行业的全面渗透,6G网络将充分融合利用物联网、边缘计算、人工智能与大数据等技术,在生产制造业、教育医疗业等领域深度赋能,网络安全能力将不仅关乎人类个体福祉,更关乎整个产业与社会的平稳运作。而行业应用驱动下的大规模异构设备连接、泛在智能与网络通信计算能力的不断下沉,也为网络侧安全带来了新的威胁与挑战。网络节点的分布式部署及边缘节点自身资源的局限性,使得边缘网络面临着边缘数据受威胁、网络状态易探知、分布式架构难防御等安全挑战。对于边缘数据安全保护,网络侧安全既应充分保障大规模异构小数据的保密性与完整性保护,提高数据抗篡改、抗伪造的能力,又应全面地增强边缘数据的安全共享能力,以支撑6G网络基础设施融合共享开放的新局面。同时,边缘网络应提高安全感知能力与分布式防御能力,通过多样化抽样的感知、多维化的威胁分析与高可信的风险预判,形成网络内生的主动安全免疫力,增强对异常边缘节点的流量控制、安全隔离与高优先级的状态处理机制,使网络具备缓解攻击和抵御自保的安全能力。

6G网络的相关研究工作在全球范围内尚处于起步阶段,6G通过技术创新、能力革新、需求更新、愿景翻新,推动世界与数字化的极大融合,也驱动网络安全体系结构由“外挂”向“内聚”、由“被动”向“自主”的发展,网络内生安全技术应结合6G应用驱动下的其他技术,渗透于网络架构中,基于网络虚拟化、智能化、边缘化等网络发展新态势进行前瞻性革新,打造网络安全新局面。



3 关键技术

3.1 身份认证技术

6G 网络为了实现泛在覆盖、泛在智能的愿景，深度融合以陆基通信系统为主的空基、天基、海基一体化网络，并充分利用人工智能与大数据挖掘技术的边缘化，不断拓展通信向各行各业的渗透。场景的切片化、接入网的异构化、接入点的边缘化与小型化、接入设备的海量化，令网络对恶意身份节点的攻击变得极为敏感。由于不同应用场景切片间安全策略的不匹配、边缘小型接入节点的认证系统资源受限、网络逐渐开放化与大数据人工智能的泛在使用导致身份认证保护脆弱、恶意身份极易利用漏洞与技术滥用通过认证鉴权接入网络，同时对网络内部已接入终端也造成威胁。因此 6G 网络身份认证技术应具备更高精度、更高安全性能，同时又满足更轻量级低功耗、适配于各种应用场景的要求。身份认证技术作为所有终端入网的“门禁系统”，在身份认证技术上

的革新是重中之重。

3GPP 近期发布的 5G 第一版标准的 R15 文件中，规定采用 SUPI 作为终端唯一身份标识，终端在申请接入网络时，会利用来自网络层的公钥与自己的密钥联合用于加密 SUPI，从而生成 SUCI 发送到基站，进而在网络层通过私钥解密进行验证。5G 通过公钥加密的方式，显然已经使得终端接入的安全性有了极大的提升，然而其机制仍然存在安全上的缺陷，而在 6G 时代，更大的终端接入量、更强的敌手计算能力、更多样的接入需求使得这些原本细微的机制缺陷进一步放大，使其迫切需要解决。在 5G 后期与 6G 中，通信网络架构将逐渐由目前的 CRAN（云无线接入网）^[3]，经由 H-CRAN（异构云无线接入网）^[4]逐渐转化为 FRAN（雾无线接入网）^[5]。在 FRAN 中，用户终端的种类更加多样化，而原有的基站也会逐渐被无人机基站等边缘基站逐渐替代^[6]。于是可以得到目前的 5G 身份认证机制面临的主要安全问题以及在 6G 中潜在的解决途径如图 1 所示。

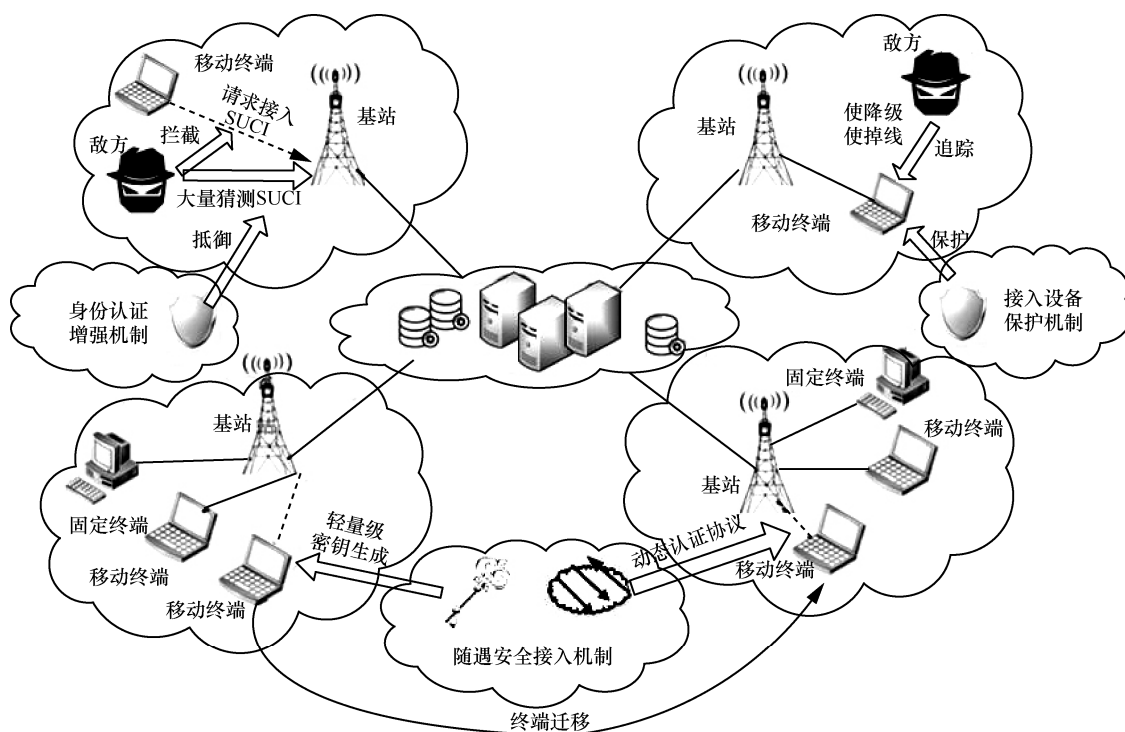


图 1 5G 身份认证面临的主要安全问题及 6G 潜在解决途径

第一个安全问题,是敌方可以试图通过拦截或者猜测的方式得到终端的身份信息,从而进行追踪等危害用户终端隐私。尽管终端已经将自身身份标识 SUPI 加密为 SUCI,敌方在拦截到 SUCI 之后依然可以通过冒充的方式,不断地发送 SUCI 给基站,通过基站回传的回复信息判断用户是否依然在该基站范围内,从而实现用户的跟踪。随着计算能力的提高,在 6G 时代敌方甚至可以直接通过猜测的方式获取终端用户信息,从而进行追踪。对此,6G 需要相应的身份认证增强机制,通过优化认证途径从而实现终端设备的防追踪,进而保护终端的隐私。

第二个安全问题,是敌方可以利用认证机制的缺陷对用户终端进行攻击。敌方可以不断发送请求认证信息给终端,从而导致终端设备大量耗电或进入异常状态,进而导致终端设备掉线或者通信从 6G、5G 降级为 4G,从而采用更低级的认证模式使得终端信息暴露。为了防止终端被攻击,需要为接入设备提供更加完备的保护机制,保障接入设备的安全。

第三个安全问题,是针对快速移动的终端的随遇安全接入。在 5G 与 6G 时代,基站的数量逐渐增多,服务范围也逐渐变小,很多快速移动的终端比如飞机等,在运行中的接入会在不同终端间快速切换。因此,如何在保证快速移动的终端接入安全的同时,尽可能降低接入所需的时间,也是 6G 身份认证的研究重点。目前已提出的解决方案包括轻量级密码生成机制以及动态认证协议。

3.2 接入控制技术

软件定义切片平台通过构建开放、易修改、可编程的网络架构体系,实现网络的动态、灵活定义部署以及按需扩展多元服务及业务模型,这是未来移动分组核心向 6G 网络发展所必须的^[7]。由于网络切片之间的资源共享性和网络可编程性接口的开放性,软件定义切片平台给 6G 安全带来

挑战。随着 6G 网络多接入方式的发展,接入控制是 6G 任一网络类型的内生安全系统的主要组成模块,以提供安全的网络环境,实现选择性对网络限制访问的目的。其中,接入访问控制策略以独立的概念级别实现,接入控制环境仅须确认真实用户对系统的访问,主要由网络运营商控制,进而通过影响可访问策略的机制应用到内生安全体系结构中。因此,6G 内生安全机制需要在具有不同安全需求的各类服务网络切片中引入接入控制技术,保证只有授权对象才可以创建、更改和删除网络切片实例。

在 6G 网络中,可以为分离的实体和访问的资源分配安全标签,这些标签由证书颁发机构(CA)颁发,并由 CA 的私钥保护,以免其他任何实体修改。这些安全标签的内容必须根据特定的应用程序要求进行设置。当对象要求访问对象时,必须首先验证其标签的真实性和完整性。提出了一种分布式的网络访问控制机制。在该模型中,不同的子系统可以分别根据自身的安全要求确定控制规则,并根据角色或组实施访问控制。这个想法是通过 PKI 实现基于角色(或组)的访问控制,如图 2 所示。

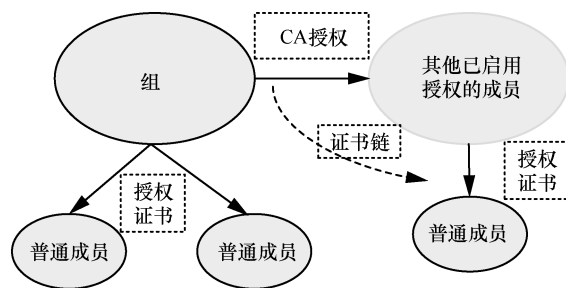


图 2 基于授权证书的访问控制

- 为每个角色(或组)生成一对密钥和角色(或组)的 ID 证书,作为角色的根 CA。
- 为每个属于该角色(或组)的成员颁发相应的授权证书,该证书由角色的私钥签名,并包括角色的 ID、成员的 ID、ID 证书的公钥、成员的安全级别、有效期和其



他相关属性。

- 用户发送请求时，访问控制网关必须验证用户提出的授权证书的有效性，以确定用户属于哪个角色。根据授权表批准或禁止访问。

为了提高 6G 网络中访问控制的可靠性，每个角色都可以将授权能力传递给下游的其他成员（只要保持相同的授权策略）。每个启用了授权的成员都可以向其他成员颁发证书。这样，即使其中一个节点发生故障，也不会影响访问控制管理。另外，当网关验证成员的访问特权时，必须提交从根证书到普通成员的证书链，以确保正确验证。访问控制机制可防止恶意使用资源，包括防止非法使用资源。通常，这些机制（例如基于角色的访问控制）确保仅向合法用户、设备或机器授予网络、数据库、信息流、服务和应用程序中的资源的权限（例如读取、写入等）。

3.3 通信安全技术

5G 网络改变世界，到 6G 网络创新世界，印证了人们对于更高性能移动通信能力与更高服务体验的无限追求。6G 对于人工智能与大数据等技术的创新融合以及不同应用场景下的软件定义切片的灵活泛在运用，将会在 5G 网络的基础上更深层地实现信息的泛在可取，并推动整个社会各个行业走向数字化。通信网络作为一切业务的根基，将突破传统网络架构，实现以陆地移动通信网络为核心的空天地海一体化通信网络高度融合，以支撑 6G 系统中的各种垂直行业的应用。随着网络架构的革新与新技术的协同融合，6G 网络将展现更高性能的通信指标，也将衍生出全新的通信安全挑战。因此，通信链路作为各种业务最底层的传输通道，应提供最根本且强大的安全保障。通信安全所涉及的威胁问题如图 3 所示。6G 网络的接入异构一体化、设备及接入点小型化以及不同应用场景的切片化、通信能力边缘化，都将导致通信安全问题变得更为尖锐。

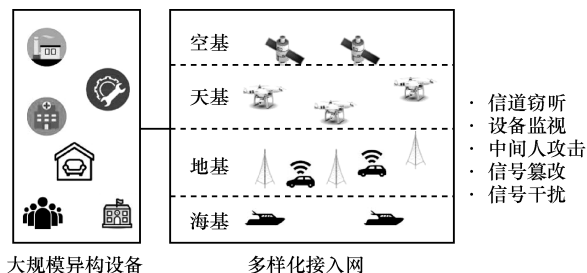


图 3 通信安全方面的威胁问题

由于密码学安全理论通常用以保护数据链路层以上的安全，实际上实现的是通信链路之上的逻辑网络的数据安全，在当前的移动无线网络中，通信安全方面存在各种问题，包括可能的窃听、篡改或伪造等攻击，都因为无线信道的不完美特性而无法用密码学手段很好地规避。同时，无线信道的广播特性以及无线信道的时变性、不稳定性，使得一些密码学方法在解决通信安全问题上也受到了密钥管理及计算复杂性等的限制。因此通信安全技术通常从物理层安全的角度来解决，它利用无线通信信道自身的衰落、干扰的性质来为通信安全提供保密性与完整性，降低了潜在攻击者获得保密信息的能力^[8]。

通信安全技术通常用以解决无线信道的攻击问题与安全性问题。通过物理层手段进行攻击检测方案与本地化防御方案的设计以及物理层身份认证方案和加密签名方案的设计来抵御通信安全传输过程中的窃听、干扰、节点假冒、伪造、篡改等一系列问题。此外，一些通信安全技术还基于窃听信道模型，对不同的无线信道条件进行安全与可靠性的分析，并提出不同应用场景下安全性与可靠性优化方案等。

应对 6G 网络基于软件定义平台的多样泛在业务场景，通信安全技术应着力从“信号层面”入手解决任何场景下的通信安全问题，同时，适用于逐渐智能化、边缘化、开放化的 6G 应用，通信安全技术应具备更小的计算开销、能量开销能力，以满足网络低功耗、绿色的需求。

3.4 数据加密技术

第六代移动通信系统将基于软件定义切片平台,网络架构内数据安全一直是安全研究的重点,6G通信系统中包含着巨大的连接数、超高速的传输速率、更多频段的使用和更复杂的通信场景,数据安全的防护存在挑战。加密是目前保护数据机密性的主流手段,由于软件定义切片平台能够提供极大丰富的服务,针对6G不同网络场景,加密技术能够在整体网络中的不同部分中得到使用,以达到切片内和切片间的网络安全。

在当前的5G网络中,针对数据安全加密已经做了很多努力。在分组数据汇聚协议(PDCP)层对无线电量进行了加密。3种不同的128位加密密钥分别用于用户平面、非访问层(non-access stratum, NAS)和访问层(access stratum, AS)。除此之外,某些4G加密算法也延续至5G场景中使用。

对于未来的6G通信系统,更高的频段有着更丰富的频谱资源,更大的带宽使信号传输速率更快。与此同时更高的频段也带来了新的安全问题,存在的信号阻塞和窃听问题会使网络安全受到威胁。在6G接入网中,期望将单个基站部署为两个拆分单元(称为中央单元和分布式单元)来实现针对安全威胁和攻击的弹性应对(如图4所示)。此拆分有助于自定义部署6G无线访问的安全敏感功能。例如,在安全的中央位置实施用户平面加密,而在不太安全的分布式位置处理非安全的功能。

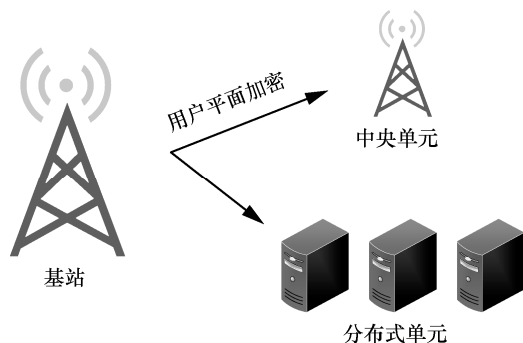


图4 基于安全的弹性化基站拆分

除上述6G接入网安全问题以外,6G系统注重边缘计算,采用人工智能和大数据挖掘等适配不同应用场景,超高的数据量导致用户隐私遭受极大风险。所以对加密技术的研究在隐私保护中便起了重要的作用。当前整个社会对隐私敏感程度越来越高,国家也针对隐私问题明确了相关法律法规,为了遵守最新的隐私安全法规,对隐私权的保护在整个6G系统中具有最高优先级要求。当前6G内生安全隐私保护目标主要包括在用户身份认定过程中,长期和临时身份都可以使用基于椭圆曲线集成加密方案(elliptic curve integrated encryption scheme, ECIES),并使用归属于运营商颁布的公钥隐藏机制来保护用户隐私^[9]。

6G网络加密机制还有很大的研究空间,国内和国际多方组织也在积极地规划安全加密规范。后续研究重点将是对6G高频高速传输中移动服务上个人数据加密保护和异构一体的信任模型的功能和协议上的安全加密保护。

4 国内外进展

在2019年8月举办的2019北京网络安全大会(BCS2019)中,奇安信集团董事长齐向东首次公开提出,网络安全已经从原来的“外挂式”“补丁式”的机制逐渐进化为以内生安全为主导的安全体系架构,从而适配新一代移动通信,即6G移动通信网络。他在讲话中强调,内生安全主要应当具有以下3点特性:自适应、自主、自成长。自适应的内生安全,要求信息化系统的安全机制不仅可以做到“明察秋毫,防微杜渐”的安全告警功能,还应具备“一方有难,八方支援”的攻击防御功能;自主的内生安全,则是强调在网络中的不同系统,都应该依据自己的业务特性,立足自己的安全需求,针对自己容易遭受的攻击,建设自主的防御架构,构筑自主的安全能力;自成长的内生安全,要求网络与智能相结合,在遭受攻击的同时动态提升自己的安全性能,做到“魔



高一尺，道高一丈”。

目前，国内很多企业与研究机构的相关部门已经对 6G 移动网络以及内生安全架构进行了讨论。中兴通讯无线电算法部从需求驱动和技术驱动出发，提出了 6G 移动通信网络“智慧连接”“深度连接”“全息连接”“泛在连接”的展望及“一念天地，万物随心”的总体愿景^[10]。除此之外，文章还提出了以“峰值速率：太比特时代”“更高能效”“随时随地的连接”“自聚合通信架构”等研究需求与挑战，并且枚举了 6G 潜在关键技术，包括太赫兹乃至可见光频段的高频段通信、新型信道编码、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等。华为公司则针对现有的 IP 网络，在其面临的诸多安全问题的基础上，提出了一种具有内生安全特性的网络架构^[11]。文章分别对身份真实性需求、隐私保护与可审计性需求对比、机密性与完整性需求与可用性需求进行分析，并提出了 4 种应用于该内生安全 IP 网络的核心技术：动态可审计的隐私 ID、去中心化的 ID 内生密钥、基于最小信任模型的真实验证、跨域联合审计与多级攻击阻断。

相比之下，国外对于 6G 与内生安全的讨论则更侧重于特定某项技术或者策略的研究，而很少有综述性的论文。参考文献[12]分析了与 5G 相比，6G 的去蜂窝化通信网络架构，在原有用于 5G 的 NOMA (non-orthogonal multiple access, 非正交多址) 的基础上改进提出了一种适用于 6G 的新型多址方式 D-OMA (Delta-orthogonal multiple access, Delta 正交多址)，并对 D-OMA 在 6G 网络中的适用性以及安全性进行了分析。参考文献[13]则是讨论了从 5G 到 6G 的技术发展、结构演进、经济效益等方面，进而提出一种以低轨道卫星 (low-orbit satellite, LEO) 与同步轨道卫星 (geostationary-orbit satellite, GEO) 组成的以天星天网为核心的空天地一体化 6G 无线通信网络架构。

5 标准化工作

3GPP 定义了 3GPP TS33.501 5G 系统安全架构和流程、3GPP TS33.401 3GPP 系统架构演进 (SAE) 安全架构、3GPP TR33.402 非 3GPP 接入安全、3GPP TS24.501 5G 系统 (5GS) 非接入层 (NAS) 协议、3GPP TS33.117 安全保障通用要求、3GPP TS33.511 5G 安全保障规范 NR Node B (gNB)、3GPP TS33.512~519 5G 安全保障规范 AMF、UPF、UDM、SMF、AUSF、SEPP、NRF、NEF、3GPP TR33.841 支持 256 bit 密钥和算法研究、3GPP TR33.818 3GPP 虚拟化网络产品的安全保障方法论 (SECAM) 和安全保障规范 (SCAS)。

欧洲电信标准化协会 (European Telecommunications Standards Institute, ETSI) 已经定义了 NFV 安全的一系列标准，包括 ETSI GS NFV-SEC001 NFV 安全的问题描述、ETSI GS NFV-SEC002 NFV 安全管理软件中安全特性分类、ETSI GS NFV-SEC003 NFV 安全；实现 NFV 环境安全与信任指南以及 ETSI GS NFV-SEC004 NFV 安全的隐私和监管要求等。

国际电联无线电通信部门 (ITU-R) 正式批准了以下几项有利于推进未来 5G 研究进程的决议，如 IMT-2020 (5G) 推进组 5G 技术研发试验系统验证 5G 网络安全技术要求、IMT-2020 (5G) 推进组 5G 技术研发试验系统验证 5G 网络安全测试方法。

中国通信标准化工作在 CCSA (中国标准化协会) 进行。目前，行业标准定义了 CCSA 5G 移动通信网通信安全技术要求、CCSA 5G 移动通信网络设备安全保障要求、CCSA 移动通信虚拟化网络设备的安全保障方法论和安全保障要求研究。

综上所述，如 ITU、ETSI、3GPP、oneM2M、5G PPP、IEEE、IETF、NVF、ONF 等标准工作组主要围绕 5G 安全标准，制定安全建议、技术规范、安全体系结构和原则，识别安全风险等，安全标准化研究及作用如图 5 所示。下一步标准化

研究方向则应聚焦于建立 6G 内生安全网络,需要精确的 6G 标准和涉及身份验证、机密性、完整性、可用性的安全标准。

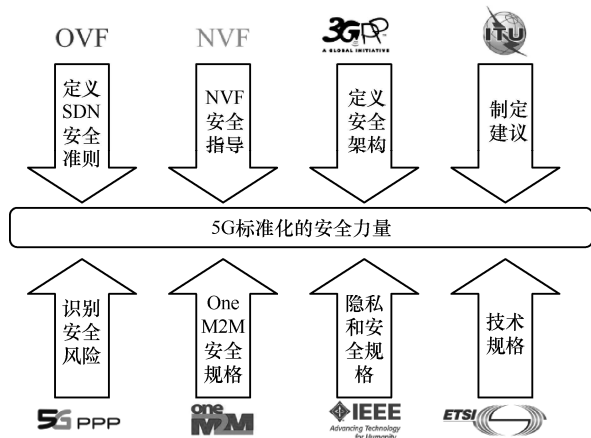


图 5 安全标准化研究及作用

6 未来挑战

6G 时代的物联网设备数量预计将达到 800 亿台,大量物联网设备将带来新的安全挑战。目前,物联网的重要通信协议包括 IEEE 802.15.4、6LoWPAN、CoAP 等。这些协议依赖于椭圆曲线密码系统(ECCs)等密码算法作为通信安全的基础。随着量子计算的出现和下一代计算设备容量的增加,这些协议将不再是安全的。

从软件而非硬件上实现网络功能是 6G 网络发展的主要趋势之一。虚拟化通过提供将网络功能部署为软件组件的框架来创建另一个抽象级别,这样做不仅可以提高性价比,而且将提高 6G 网络的端到端可靠性。而在软件中实现的安全功能可以根据需要部署在任何网络外围,因此对加强网络安全带来了新的挑战。

为 6G 网络安全提供海量数据分析或网络流量监控需要一个自主、自感知和自适应的智能系统。而这种系统通常采用人工智能的新算法和新技术,因此,网络安全可以成为人工智能的应用领域之一。由于智能电网、交通和医疗系统等关键基础设施的安全性至关重要,因此必须采取主

动安全措施。主动安全措施需要不断收集情报,并利用这些情报来减少安全风险或失误的可能性。因此人工智能的算法和解决方案可以应用于网络安全领域。

6G 将成为智能医疗、工业自动化、大规模物联网等应用的关键促成因素。除了安全性,隐私也会根据应用的不同要求而有所不同。由于 6G 将为无处不在的数字服务提供底层网络服务,因此这些应用程序将产生大量的数据,导致对手攻击正常用户隐私的范围会更广。

7 结束语

无线通信网络已经从 1G 中连接移动电话发展到 6G 中连接生活的几乎所有方面。在这一发展过程中,安全领域也同样从简单的电话窃听发展到对移动设备、网络设备和服务的攻击。为此,深入讨论了 6G 网络的安全挑战,从内生安全的角度阐述了应对上述安全挑战的基本原理以及关键技术,并概述了未来 6G 安全可能面临的挑战。

参考文献:

- [1] 彭木根. 5G 无线接入网络: 雾计算和云计算[J]. 电信科学, 2018, 34(4): 196.
PENG M G. 5G wireless access network: fog computing and cloud computing[J]. Telecommunications Science, 2018, 34(4): 196.
- [2] 彭木根, 艾元. 异构云无线接入网络: 原理、架构、技术和挑战[J]. 电信科学, 2015, 31(5): 47-51.
PENG M G, AI Y. Heterogeneous cloud radio access network: principle, architecture, techniques and challenges [J]. Telecommunications Science, 2015, 31(5): 47-51.
- [3] 项弘禹, 肖扬文, 张贤, 等. 5G 边缘计算和网络切片技术[J]. 电信科学, 2017, 33(6): 54-63.
XIANG H Y, XIAO Y W, ZHANG X, et al. Edge computing and network slicing technology in 5G[J]. Telecommunications Science, 2017, 33(6): 54-63.
- [4] 刘江, 黄韬, 张晨, 等. SDN 试验床网络虚拟化切片机制综述[J]. 通信学报, 2016, 37(4): 159-171.
LIU J, HUANG T, ZHANG C, et al. Research on network virtualization slicing mechanism in SDN-based testbeds[J]. Journal



- on Communications, 2016, 37(4): 159-171.
- [5] 王志宏, 杨震. 人工智能技术研究及未来智能化信息服务体系的思考[J]. 电信科学, 2017, 33(5): 1-11.
WANG Z H, YANG Z. Research on artificial intelligence technology and the future intelligent information service architecture[J]. Telecommunications Science, 2017, 33(5): 1-11.
- [6] 魏凯敏, 翁健, 任奎. 大数据安全保护技术综述[J]. 网络与信息安全学报, 2016, 2(4): 1-11.
WEI K M, WENG J, REN K. Data security and protection techniques in big data: a survey[J]. Chinese Journal of Network and Information Security, 2016, 2(4): 1-11.
- [7] PENG M G, SUN Y H, LI X L, et al. Recent advances in cloud radio access networks: system architectures, key techniques, and open issues[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2282-2308.
- [8] PENG M G, ZHANG K C, JIANG J M, et al. Energy-efficient resource assignment and power allocation in heterogeneous cloud radio access networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(11): 5275-5287.
- [9] PENG M G, YAN S, ZHANG K C, et al. Fog-computing-based radio access networks: issues and challenges[J]. IEEE Network, 2016, 30(4): 46-53.
- [10] PENG M G, WANG C G, LAU V, et al. Fronthaul-constrained cloud radio access networks: insights and challenges[J]. IEEE Wireless Communications, 2015, 22(2): 252-160.
- [11] PENG M G, LI Y, ZHAO Z Y, et al. System architecture and key technologies for 5G heterogeneous cloud radio access networks[J]. IEEE Network, 2015, 29(2): 6-14.
- [12] PENG M G, LI Y, JIANG J M, et al. Heterogeneous cloud radio access networks: a new perspective for enhancing spectral and energy efficiencies[J]. IEEE Wireless Communications, 2014, 21(6): 126-135.
- [13] LIU Y, WANG H S, PENG M G, et al. DeePGA: a privacy-preserving data aggregation game in crowd sensing via deep reinforcement learning[Z]. 2019.
- [14] 赵亚军, 郁光辉, 徐汉青. 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): 963-987.
ZHAO Y J, YU G H, XU H Q. 6G mobile communication networks: vision, challenges and key technologies[J]. Scientia Sinica (Informationis), 2019(49): 963-987.
- [15] 江伟玉, 刘冰洋, 王闯. 内生安全网络架构[J]. 电信科学, 2019, 35(9): 20-28.
JIANG W Y, LIU B Y, WANG C. Network architecture with intrinsic security[J]. Telecommunications Science, 2019, 35(9): 20-28.
- [16] AL-ERYANI Y, HOSSAIN E. The D-OMA method for massive multiple access in 6G: performance, security, and challenges[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 92-99.
- [17] KALBANDE D, KHAN Z, HAJI S, et al. 6G-next gen mobile wireless communication approach[C]//3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA), June 12-14, 2019, Coimbatore, India. [S.l.:s.n.], 2019: 1-6.
- [18] 赖俊森, 吴冰冰, 汤瑞, 等. 量子保密通信标准化现状与发展分析[J]. 电信科学, 2018, 34(1): 1-7.
LAI J S, WU B B, TANG R, et al. Analysis on the status and development of quantum secure communication standardization[J]. Telecommunications Science, 2018, 34(1): 1-7.

[作者简介]



刘杨 (1984—), 男, 北京邮电大学网络技术研究院副教授、硕士生导师, 主要研究方向为后 5G 内生安全等。



彭木根 (1978—), 男, IEEE Fellow, 教育部“长江学者”特聘教授, 国家杰出青年科学基金获得者, 入选“万人计划”科技创新领军人才、科睿唯安 2019 年度 ESI 全球高被引科学家和 2019 年首都科技盛典十大科技人物, 网络与交换技术国家重点实验室副主任, 中国通信学会青年工作委员会主任, 北京市科技人才研究会副理事长。长期从事移动通信智能组网理论及关键技术研究工作。累计发表 IEEE 期刊论文 100 余篇, 其中 ESI 高被引用论文累计 19 篇, 谷歌学术引用近万次。获得 IEEE 通信学会海因里希·赫兹奖、IEEE 通信学会亚太区杰出青年学者奖等。受邀担任 IEEE IoT-J、IEEE Communications Magazine 等国际期刊指导委员会委员或编委等。以第一完成人身份获得国家技术发明奖二等奖 (2018 年)、北京市科学技术奖一等奖 (2017 年)、中国通信学会科学技术奖一等奖 (2015 年)、求是杰出青年成果转化奖 (2018 年) 等。