6G网络安全愿景

Security Vision of 6G Network

高　枫[1]，夏俊杰[1]，张　峰[2]（1. 中国联通智能城市研究院，北京 100048；2. 中国电子科技集团信息科学研究院，北京 100015）
Gao Feng[1]，Xia Junjie[1]，Zhang Feng[2]（1. China Unicom Smart City Research Institute，Beijing 100048，China；2. CETC，Academy of Information Science Innovation，Beijing 100015，China）

摘　要：
6G被赋予了人类生活与数字世界智慧互联的期望，安全作为连接物理世界与数字世界的基石，承载着内生安全、可信赖、智慧化的使命。首先从内生安全、弹性安全、情景感知安全、多维数据安全、可评估安全等方面提出了6G网络安全愿景。然后从方法论、网络架构、接入认证、分层安全、边界安全、形式化安全、信息安全、后向安全、新技术在6G安全中的应用等方面，给出了6G网络安全关键技术。最后探讨了6G网络安全未来的研究方向。

关键词：
6G；安全内生；安全架构；安全关键技术
doi：10.12045/j.issn.1007-3043.2021.08.007
文章编号：1007-3043（2021）08-0029-05
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
6G is endowed with the expectation of intelligent interconnection between human life and the digital world. As the cornerstone of connecting the physical world and the digital world，security carries the mission of endogenous security，reliability and intelligence. Firstly，the 6G network security vision is proposed from the aspects of endogenous security，elastic security，context aware security，multidimensional data security and assessable security. Then，the key security technologies of 6G are given from the aspects of methodology，network architecture，access authentication，layered security，boundary security，formalized security，information security，backward security and the application of new technologies in 6G security. Finally，the future research direction of 6G network is discussed.

Keywords：
6G；Endogenous security；Security architecture；Security key technologies

引用格式：高枫，夏俊杰，张峰. 6G网络安全愿景[J]. 邮电设计技术，2021（8）：29-33.

0 引言

2019年3月，全球首届6G峰会起草了第1份6G白皮书，阐明6G发展的基本方向。2019年11月3日，我国科技部会同国家发展改革委、教育部、工业和信息化部、中科院、自然科学基金委在北京组织召开6G技术研发工作启动会，成立国家6G技术研发推进工作组和总体专家组，标志着我国6G技术研发工作正式启动[1-3]。

基金项目：国家重点研发计划（2019YFB2103200）
收稿日期：2021-07-02

未来6G的愿景具备泛在、无线、智能等特点，能够提供无缝覆盖的泛在无线连接和情景感知的智能服务与应用。在网络架构方面，6G将会突破地面网络限制，实现地面、卫星、机载网络和海洋通信网络的无缝覆盖，即空天地一体化的通信网络；在应用场景方面，国际电信联盟（ITU）最新技术报告给出了6G的七大代表用例：全息类通信、面向远程的操控网络、智能操控网络、网络和计算融合、数字孪生、空一地集成网络、工业物联网云化，并分析了网络关键需求，其中安全需求包括隐私、可靠性、可信任度、弹性、可追溯性、合法拦截等。

未来6G被赋予了人类生活与数字世界智慧互联

的期望，安全作为连接物理世界与数字世界的基石，承载着内生安全、可信赖、智慧化的使命。

1 网络安全愿景

移动通信技术和网络架构的演进，伴随着2G/3G/4G/5G移动通信网安全机制的成长，在数字化技术（DT）与通信技术（CT）高度融合的发展趋势下，6G网络安全有望突破传统通信安全内涵与外延，具备内生安全、弹性安全、情景感知安全、多维数据安全和可评估安全的能力（见图1）。

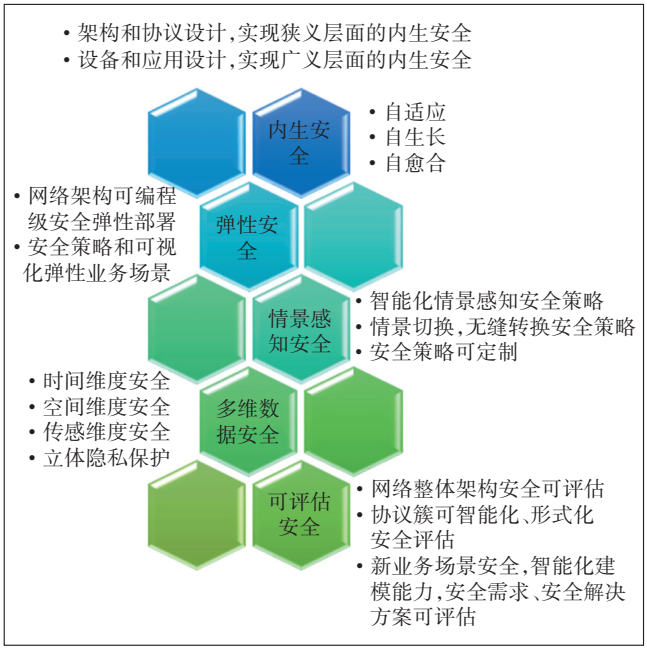

图1　6G网络安全愿景

1.1 内生安全

6G网络具备内生安全能力，在架构和协议设计方面，实现狭义层面的内生安全，即除设计的本征或元功能之外，具备解决副作用、脆弱性、自然失效等因素在内的显式或隐式表达的非期望功能的能力；在设备和应用设计方面，实现广义层面的内生安全，即在狭义内生安全问题之上，具备解决蓄意让最终用户不可见的设计功能、或未向使用者声明或披露过的软硬件隐匿功能。

网络架构设计以自适应、自生长、自愈合为核心，对网络安全威胁实现自感知、自发现和自处置。

a）自适应。在6G网络架构设计时，考虑独立的安全和信任功能（实体），该安全功能实体具备：

（a）调度安全资源的能力，与其他网络功能实体交互，实现限流限速、数据拦截等。

（b）动态调整安全策略的能力，如开启单因子/多因子认证，下发其他网络功能实体安全策略调整的指令等。

（c）安全和信任评估的能力，对其他网络功能实体进行安全和信任评估，对承载业务的信道进行端到端安全和信任评估等。

b）自生长。以AI技术为基础，使网络具备安全自生长的能力。

（a）安全策略智能化。

（b）安全/信任评估智能化，整网安全动态可评估。

（c）安全态势智能化感知。

c）自愈合。以AI技术和数字孪生技术为基础，赋予网络自愈合能力。

（a）基于数字孪生技术，端、边、云、网、安全中心等智能协同，实现网络安全态势自感知，威胁预判。

（b）基于AI技术和数字孪生技术，实现安全攻击自发现，从协议层触发处理机制。

（c）基于AI技术，实现安全事件自处置，增强智能化能力。

1.2 弹性安全

网络架构实现可编程级的安全弹性部署，对于未知网络的威胁和攻击，数据面与控制面/扩展平面智能联动。

a）数据面具备可编程/动态调度的流量调度能力。

b）数据面与控制面/扩展平面具备联合编程级调度能力。

在安全策略可配置和可视化方面，弹性适配业务场景。

1.3 情景感知安全

对于全息通信、无人驾驶、工控应用、机器人（群）/人机（群）等场景，具备情景感知的安全能力：

a）具备智能化情景感知的安全策略定制能力。

b）在情景切换时无缝转换安全策略。

1.4 多维数据安全

由以网络为核心的安全转向以数据为核心的安全，由单一维度的通信数据安全保护（完整性、机密性、抗重放攻击保护）转向时间、空间、传感等多维度的数据安全保护。

a）在时间维度上，具备数据时空同步安全保护能力。

b）在空间维度上，具备保护位置、轨迹、行为、画像级数据的能力。

c）在传感维度上，具备保护非结构化感知数据、异构融合数据安全的能力。

在5G网络研究之初，移动通信网即被赋予定制化隐私保护的愿景，但就目前3GPP国际标准的制定情况，距定制化、个性化隐私保护能力还有一定差距。6G网络业务场景将触及和连接物理世界与数字世界，隐私信息的内涵与外延延展，在兼顾各国家地区法律法规基础上，对隐私具备立体化保护能力。

a）隐私信息保护范围，可能涉及终端标识信息、用户标识信息、生物特征信息、位置信息、轨迹信息、业务用户画像、全息信息、沉浸式交互信息等等。

b）支持隐私信息分类分级保护，面向不同业务场景，提供差异化保护策略。

c）支持隐私信息可配置的保护能力，在终端侧、网络侧、设备侧等，支持灵活的可配置能力。

1.5 可评估安全

3GPP在可评估安全方面，从Release13开始，研制了网络设备安全保障系列标准，其中涵盖4G和5G的主要网络设备。在整网架构安全、协议安全层面，尚无可评估安全相关的研究和标准工作。6G网络预期架构、协议、关键技术更加多样化，依托于数字孪生、AI等技术的发展应用，6G网络和协议在设计时有望赋予可评估安全的能力：

a）网络整体架构的安全性可评估。

b）协议簇，特别是涉及跨域、跨网络接入类型的协议簇之间，具备智能化、形式化的安全评估能力。

c）网络新业务场景的安全具备智能化建模能力，安全需求、安全解决方案可评估。

2 安全关键技术

2.1 方法论

6G网络安全需从方法论的角度，全局规划设计安全架构，从以下2个方面突破。

a）研制6G移动通信网安全设计的方法论，以开放复杂巨系统理论为指引，结合移动通信网特点，开展方法论研究（见图2）。

b）研究6G网络内生安全机制与关键技术，将安全内生在网络架构、协议、设备等设计之中。

此外，在2G/3G/4G/5G国际标准研制过程中，3GPP SA1（服务组）研制移动通信网需求时，安全通常

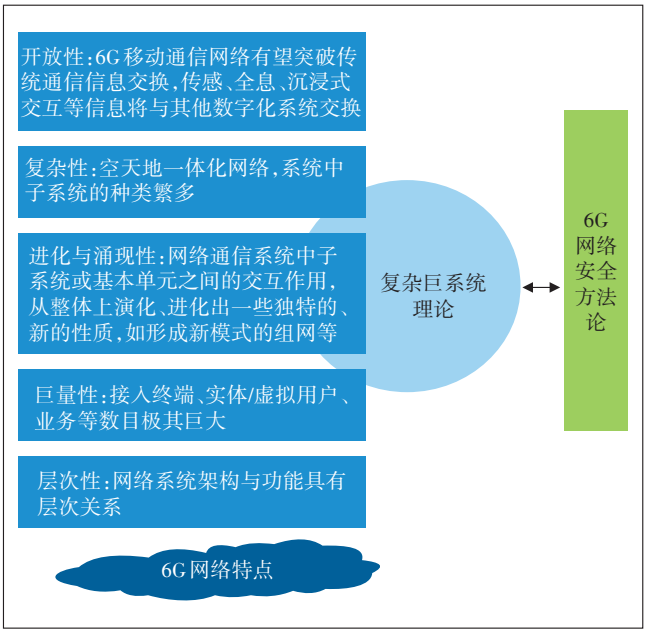

图2　复杂巨系统与6G网络安全

作为整体需求中的一部分；SA3（安全组）通常基于SA1（服务组）和SA2（架构组）的工作，研制各代移动通信网络的安全架构、安全关键问题（包括安全威胁和安全需求）、安全解决方案，在6G国际标准研制中，SA3与SA1应同步开启研究工作，在国际标准中研究安全架构设计方法论，指导后续标准化制定。

2.2 网络架构

6G网络安全架构应由基于移动通信网网络需求及架构进行安全相关的研究，转变为安全定义网络架构，安全引领网络需求，实现6G网络架构与安全同步协同。

在协议层面，考虑将信令面和数据面扩展为信令面、数据面和安全面的“三平面”，安全平面承载安全策略编排、安全风险感知、安全处置等能力，逻辑上与信令面独立，以实现内生安全和整网安全智能协同。

在网络功能实体方面：

a）新增独立网元：聚合整网安全资源调度、安全策略调度、安全和信任评估等的功能。

b）各网元安全能力增强，考虑分层的设计，即单一网络功能实体包括基础功能层、安全层、增强（扩展）功能层，将安全能力内嵌到网络功能实体/设备之中。

c）专有安全设备融入网络架构：传统防火墙、流量清洗、垃圾信息滤过等非通信网络设备融入网络架构设计，或预留接口，实现增强的安全能力全网统一

调用。

在信任模型方面，由用户、设备、网络的三元信任模型，转变为具备信任评估能力和兼任零信任架构的新型信任模型。

在网络架构演进方面，6G网络架构将涵盖由各种轨道卫星构成的天基网络，由飞行器构成的空基网络，以及传统的地基网络（蜂窝无线网络、卫星地面站和移动卫星终端以及地面的数据与处理中心等），其中安全需解决以下关键问题（见图3）。

a）各层之间的接入安全。

b）切换安全。

c）数据传输安全。

d）协议解析安全。

e）云边协同安全。

f）异构数据融合安全。

g）时空数据同步安全。

h）跨域隐私保护等。

2.3 接入认证

在统一认证架构的基础上，构建立体认证架构，可兼任基于信任的凭证、多因子认证、生物特征、数字身份等；在认证架构设计上，重点研究基于智能技术的无感知认证、基于数字身份、基于信任的认证等；一方面满足多样化应用场景的统一认证需求，另一方面满足不同层级的安全接入需求。

构建适用于6G网络的数字身份体系。6G网络智能化的演进趋势，虚拟数字世界将与物理世界智能连接，在通感互联、孪生体域等方面，数字身份体系建设必不可少。

2.4 分层的安全

在网络协议层，研究空天地一体化网络的接入安全，不同网络类型之间的切换安全，不同网络类型之间的协议解析安全，合法拦截等。

在数据层，除传统通信数据安全之外，研究时空同步安全、异构数据融合安全、传感数据安全保护、数字孪生数据安全、跨域隐私保护等。

在资源调度层（控制层），研究云边协同安全，实现资源的弹性、可信任 、可调度等，提升整网资源可靠性。

在应用层，研制异构数据和多源场景下的溯源机制，提升整网信息的可追溯性。

2.5 边界安全

突破传统网络域和安全边界，以零信任的架构重塑整网边界安全，结合动态信任评估机制，研制适合6G网络的边界安全防护机制。

2.6 形式化安全检测

构建网络协议簇之间、关键信令等的形式化、智能化安全检测能力，在网络协议设计层面和跨网络类型协议簇、协议应用层面实现自动化、智能化的安全检测机制，以灵敏规避网络架构演进和业务应用扩展对现有网络和协议带来的潜在安全风险和漏洞。

安全检测机制可兼容白盒、黑盒、灰盒方法，并不依赖于具体技术和实现算法。

2.7 信息安全

6G网络承载的信息类型将更加丰富多样，信息安

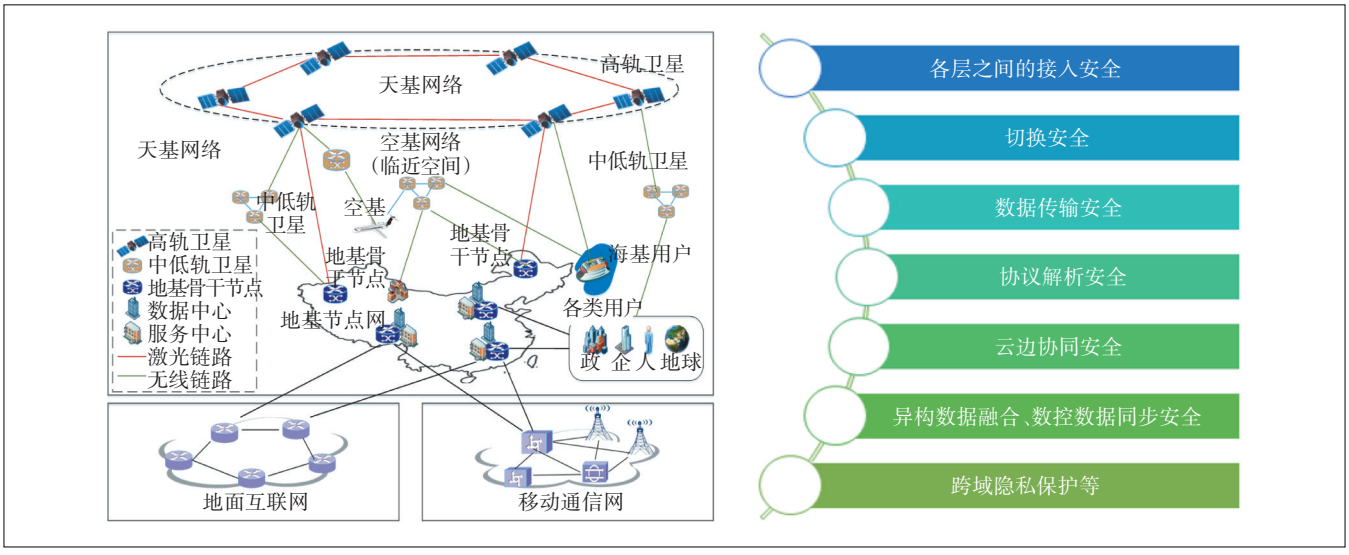

图3　空天地一体化网络安全

全保护范围不断扩展，垃圾信息形式复杂多变（由传统消息、语音类，向智能方式转变），此外，伴随语音消息、视频信息、浸入式信息、全息信息、传感信息、“数字人”信息等在网络业务中的使用，应研制覆盖多信息类型的全生命周期信息安全保护机制。

2.8 后向兼容

在整网安全架构和安全功能设计时，需同步考虑与2G/3G/4G/5G网络的后向兼容问题，主要包括接入认证、回落安全、密钥体系、加密机制、安全策略调度、网络功能实体安全能力增强兼容等方面。

2.9 新技术在6G安全中的应用

新技术应用在6G网络安全中，将有望提升网络架构和应用安全。

a）博弈论：安全无绝对，安全机制设计本身即是与计算能力、网络资源代价等的博弈，可将博弈论应用在动态安全策略设计、信任评估等方面。

b）拟态：解决6G网络空间存在“未知的未知威胁”或不确定威胁，可应用在整网安全架构和防御能力设计中；可应用在关键网络功能实体之中（如寻址），强化关键功能防御能力。

c）AI：基于AI技术，可提升安全策略智能化；安全/信任评估智能化，整网安全动态可评估；安全态势智能化感知；实现安全攻击自发现，从协议层触发处理机制；实现安全事件自处置，增强智能化能力。

d）同态加密：可应用在增强的边缘服务、金融科技、数字孪生、社会治理应用等方面，提升数据和应用安全。

e）区块链：可应用在信息溯源方面以及网络架构演进。

f）信任：包括可信计算、信任评估、信任模型等，可应用在网络基础设施安全、安全评估、认证等方面。

g）零信任：可应用在网络边界安全方面，构建包括智能终端（包括机器人、智能物联设备等）认证代理机制，可信接入网络功能实体，以及数字身份平台等为一体的零信任安全架构。

3 未来研究方向

6G研究刚起步，安全作为连接物理世界与数字世界的基石，承载着内生安全、可信赖、智慧化的使命。

在安全架构方面，重点研制移动通信网安全设计的方法论，以开放复杂巨系统理论为指引，结合6G移动通信网特点，开展方法论研究；研究6G网络内生安全机制与关键技术，将安全内生在网络架构、协议、设备等设计之中。

在安全关键技术方面，重点研制各网络类型之间的接入安全、切换安全、数据传输安全、协议解析安全、云边协同安全、异构数据融合安全、时空数据同步安全、跨域隐私保护等。

产学研一体化研究，同时加强国际标准预研和专利布局，在ITU-T国际标准可提前开展6G网络安全方法论和需求研究，在3GPP国际标准可开展B5G网络演进安全研究，在6G国际标准研制中，3GPP SA3与SA1同步开启研究工作。

4 总结

随着5G系统的全面部署，针对6G移动蜂窝系统的研究已经开始。移动通信技术和网络架构的演进，伴随着2G/3G/4G/5G安全机制的成长，在数字化技术（DT）与通信技术（CT）高度融合的技术发展趋势下，6G网络安全有望突破传统通信安全内涵与外延，具备内生安全、弹性安全、情景感知安全、时空安全、立体隐私保护、可评估安全的能力。6G网络对垂直行业的信息化和智能化需求、对个性化和智能化的通信需求、人工智能在通信网络中的全面应用、空天地海全域覆盖等需求，不断催生新技术发展应用；空天地一体化技术、太赫兹通信技术、可见光通信技术、算力网络、AI、区块链等新技术在网络架构中的应用等正在研究之中，相应的安全机制需持续研究。

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(99): 1-1.

[2] 6G概念及愿景白皮书[EB/OL]. [2021-03-21]. https://baijiahao.baidu.com/s?id=1661224713028703987&wfr=spider&for=pc.

[3] 魏克军，胡泊. 6G愿景需求及技术趋势展望[J]. 电信科学，2020，36(2)：130-133.

作者简介：
高枫，中国联通智能城市研究院标准总监，高级工程师，主要研究方向为移动通信网安全、信息安全、应用安全等；夏俊杰，中国联通智能城市研究院副院长，教授级高级工程师，主要研究方向为移动通信网安全、信息安全、应用安全等；张峰，中国电子科技集团公司信息科学研究院认知与智能技术重点实验室副主任，高级工程师，主要研究方向为人工智能、数据治理等。