中国科学: 信息科学 2023 年 第 53 卷 第 2 期: 344–364
SCIENTIA SINICA Informationis
论文

6G 无线内生安全理念与构想

金梁[1], 楼洋明[1*], 孙小丽[1], 钟州[1], 许晓明[1], 易鸣[1], 黄开枝[1], 季新生[1,2], 邬江兴[1,2*]

1. 战略支援部队信息工程大学, 郑州 450002
2. 网络通信与安全紫金山实验室, 南京 211111
* 通信作者. E-mail: louyangming1991@outlook.com, ndscwjx@126.com

收稿日期: 2021–03–17; 修回日期: 2021–05–07; 接受日期: 2021–06–02; 网络出版日期: 2023–02–07

国家重点研发计划 (批准号: 2020YFB1806607)、国家自然科学基金 (批准号: 61521003, 61701538) 和重点院校和重点学科专业建设资助项目

摘要 6G 开放融合、异构共存、智能互联的网络特点将引发更多未知复杂安全威胁, 目前安全滞后于通信发展的格局必然难以应对, 6G 时代必须打破思维定势, 催生真正具有代际效应的标志性技术. 内生安全从无线网络内源性缺陷产生的共性和本源安全问题出发, 通过结构导向的解决方法, 具有抵御未知安全威胁的能力和通信/安全/服务内源性融合的能力. 本文对 6G 无线网络内生安全问题、理念进行了探讨, 并提出内生安全在 6G 超高速宽带通信、超大连接超低时延、天地一体化全域覆盖等典型场景中的应用构想, 给出了若干潜在关键技术和解决方案.

关键词 6G 安全, 内生安全, 通信/安全/服务一体化, 无线内生安全, 移动边缘内生安全计算, 物理层链式密钥

1 引言

纵观移动通信系统的发展, 从 2G 时期的 GSM、3G 时期的 CDMA、4G 时期的 MIMO-OFDM, 发展到如今 5G 的 Massive-MIMO 和 SDN/NFV, 这些具有明显代际效应的标志性通信变革技术, 使网络的 KPI (key performance indicator) 不断呈数量级提升. 随着 6G 研究的启动, 太赫兹、可重构智能表面 (reconfigurable intelligent surface, RIS)、人工智能等一系列通信使能技术逐渐成为研究热点 [1]. 预计到 2030 年, 6G 将支持包括全自动驾驶、触觉通信、工业互联网、智能疾病预测、超真实的虚拟现实体验等在内的新兴应用, 提供 “全覆盖、全频谱、全应用” 的通信服务.

反观移动通信安全的发展, 安全通常被视作通信的伴随技术, 延续了以问题为导向, 以 “打针吃药”、“围堵修补” 的手段应对确定性安全威胁的技术路线 [2~7], 如 3G 增加双向鉴权机制解决 2G 的

引用格式: 金梁, 楼洋明, 孙小丽, 等. 6G 无线内生安全理念与构想. 中国科学: 信息科学, 2023, 53: 344–364, doi: 10.1360/SSI-2021-0095
Jin L, Lou Y M, Sun X L, et al. Concept and vision of 6G wireless endogenous safety and security (in Chinese). Sci Sin Inform, 2023, 53: 344–364, doi: 10.1360/SSI-2021-0095

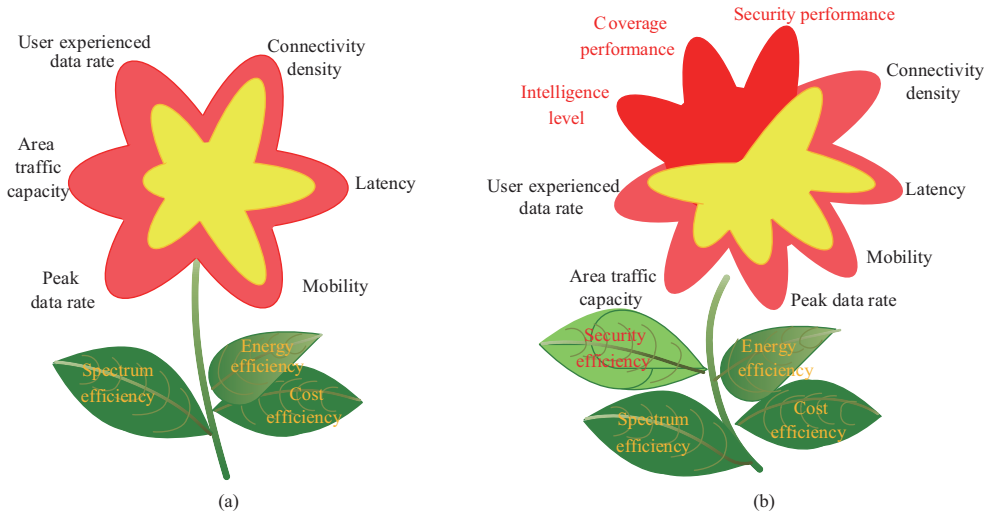

图 1 (网络版彩图) 5G 与 6G 关键性能指标对比. 图 (b) 中红色部分为 6G 新增 KPI

Figure 1 (Color online) KPI comparison of 5G and 6G. (a) Flower of 5G; (b) flower of 6G. The red part in (b) is the new KPI for 6G

伪基站问题, 4G 利用 Diameter 协议解决 3G 中的 SS7 信令劫持问题, 5G 增加网元认证解决 4G 中的跨网攻击问题; 加密算法因 A51/A52, KASUMI 的缺陷逐步演进为 AES, SNOW3G, ZUC 等 [8], 密钥长度也从 2G 时期的 64 比特增加到 5G 的 256 比特. 安全效果整体呈现出 "温水煮青蛙" 渐进式增强的特点.

6G 时代若想改变安全滞后于通信的现状, 必须打破 "补丁式" 的思维定势. 然而目前仍面临许多挑战 [9,10]: (1) 6G 安全研究面临 "双重不确定性": 一方面 6G 演进仍存在关键技术待辨识、网络架构待明确、协议标准待制定等诸多不确定因素, 另一方面 6G 网络的开放融合必将引入大量不确定的安全隐患, 必须具备抵御不确定安全威胁的能力. (2) 必须解决好开放与安全对立、先进与可信对立这两大矛盾: 6G 网络具有支持异构共存、智能互联的能力, 在提供无处不在的通信支持的同时, 多种类型的设备与多种形态的网络相互连接, 任何节点和网络都有可能成为攻击的突破口对 6G 网络进行渗透, 安全的短板效应更加突出; 6G 网络的新架构、新应用、新技术的出现势必会引入新的安全威胁 [11], 以人工智能为例, 具有不可解释性和不可推理性, 安全性更是未知[1]. 这些新技术的安全性如何自证, 是应用中不可回避的问题.

此外, 从移动通信的演进与发展看, 相对于 5G 而言[2], 6G 愿景中需要增加安全性能和安全效率的指标要求 (图 1 所示). 在安全性能方面, 要相应提出可量化设计、可验证度量的评估体系. 在安全效率方面, 需要同步考虑从通信、服务与安全的本源属性出发, 推动 6G 整体 KPI 均衡发展、相互促进, 实现通信/安全/服务 "三位一体" 内源性 "根系" 融合 (图 2 所示) [9].

虽然 6G 安全面临双重不确定性和两个对立矛盾, 但有一点是可以确定的, 即 6G 绝大部分安全威胁将来自于 6G 网络内源性缺陷产生的内生安全问题. 而两个对立均来自于缺乏对通信/安全/服务共同本源属性的发现与利用, 对于传统外挂/附加式的安全与通信和服务之间往往是相互割裂的. 遵循外因通过内因起作用, 内因起决定性作用的哲学原理, 需要在安全理念与架构上进行创新, 催化具

1) https://mp.weixin.qq.com/s/vpzswVOvwcds6P4q1RRRGg.

2) 5G 愿景与需求白皮书. 2014. http://jpkc.bcu.edu.cn/meol/common/script/preview/download_preview.jsp?fileid=292201&resid=82701&lid=17534.

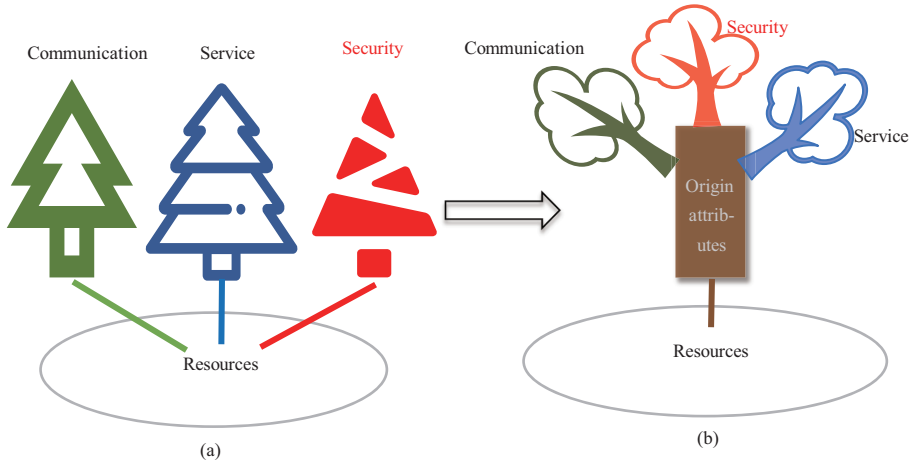

图 2 (网络版彩图) 通信/安全/服务向内生一体化演进. (a) 目前安全是 "外挂式" 的, 通信/安全/服务之间资源互相抢占; (b) 通过优化通信/安全/服务的共同本源属性可大大提高安全效率

Figure 2 (Color online) Communication/security/service evolves towards endogenous integration. (a) The current security is "plug-in", and resources between communication/security/service are preempted by each other; (b) by optimizing the common origin attributes of communication/security/service, security efficiency can be greatly improved

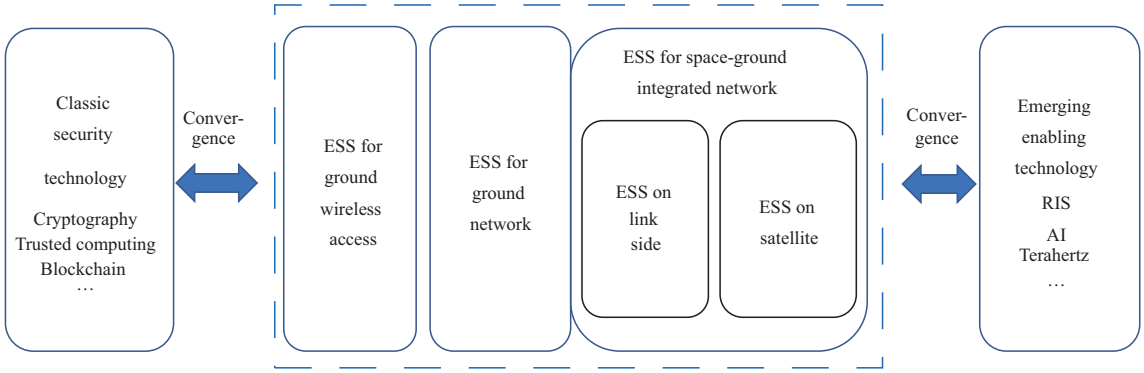

图 3 (网络版彩图) 6G 无线网络内生安全技术体系架构

Figure 3 (Color online) 6G wireless network endogenous security technology system architecture

有 "代际效应" 的安全技术.

内生安全 (endogenous safety and security, ESS) 作为网络空间安全的新兴理论, 近年来受到了业界的广泛关注, 2008 年提出了拟态计算的概念 [12], 2013 年提出了基于动态异构冗余 (dynamic heterogeneous redundancy, DHR) 构造的拟态防御设想 [13~16], 以此不断发展完善形成内生安全理论, 并在系统与设备研制上取得重大突破[3]. 紫金山实验室于 2019 年 5 月开通首个面向全球开放、永久在线的网络内生安全试验场 (NEST)[4], 涵盖拟态设备、拟态云, 以及拟态数据中心等, 在真实网络中成功抵御国际 "白帽黑客" 上百万次攻击, 形成了 "特异性免疫" 和 "非特异性免疫" 的点面融合防御模式. 6G 无线网络只有发展内生安全技术, 才能规避不确定威胁、统一两个对立, 具备 "三位一体" 内源性融合的能力, 为 6G 提供全方位、高效的安全解决方案.

本文将围绕如何利用内生安全技术应对 6G 无线网络面临的安全威胁进行详细阐述. 针对如图 3

3) https://www.aqniu.com/vendor/68666.html.
4) https://baijiahao.baidu.com/s?id=1634283791171509738.

所示的 6G 无线网络架构中地面网络无线侧和天地一体化网络这两大关键部分, 基于内生安全与传统安全技术和新兴使能技术融合的 6G 无线网络内生安全理念, 给出内生安全在 6G 空口和 6G 天地一体化全域覆盖场景的应用构想, 具体包括若干潜在关键技术和解决方案. 后续章节安排如下: 第 2 节介绍 6G 无线网络内生安全问题与理念; 基于内生安全理念, 接着在第 3 和 4 节分别介绍内生安全在 6G 空口和天地一体化场景中的应用构想; 第 5 节对全文进行总结.

2 6G 无线网络内生安全问题与理念

2.1 6G 无线网络内生安全问题

正如黑格尔 (Hegel) 所说, “一切事物都是自在 (内生) 的矛盾, 矛盾是一切运动和生命力的根源”. 任何一个系统除设计的期望功能之外总存在伴生或衍生的显式副作用或隐式暗功能, 总称为内生安全问题. 直接或间接利用内生安全问题引发的非期望事件, 包括人为或自然因素引发的扰动统称为广义不确定扰动 [15]. 6G 网络侧和无线侧均会存在内生安全问题.

网络侧内生安全问题是在网络架构开放化、网络构件多样化、产业链国际化的趋势下, 软硬件代码的设计不可避免存在缺陷或漏洞, 这使得攻击者在开放的网络架构下可以实施 “单向透明、里应外合” 协同攻击, 而防御者面对系统未知的漏洞、设备未知的后门和未知的攻击方式, 势必无法有效应对由此产生的不确定威胁.

无线侧内生安全 (wireless endogenous safety and security, WESS) 问题 [17] 是指由电磁波传播机理的内源性缺陷引发的广义不确定扰动, 包括随机衰落、干扰等产生的功能安全 (safety) 问题, 以及被动窃听或主动攻击产生的信息安全 (security) 问题. 无线通信的广义不确定性扰动源于电磁环境的不确定性和不可操控性. 电磁波传播的开放性使得任何地方都能够收到无线信号, 任何地方都能够发起无线攻击.

2.2 6G 无线内生安全理念与范式

要解决内生安全问题, 只能依靠内生安全手段. 通过发现 6G 网络和系统自身构造或运行机理产生的内生安全效应及其科学规律, 挖掘内生安全属性, 创新内生安全机制, 设计内生安全功能, 提供应对已知和未知安全威胁的内生安全能力, 同时与传统安全技术与新兴赋能技术融合, 形成 6G 安全发展的新范式.

2.2.1 网络内生安全构造 —— 基于动态异构冗余构造的网络内生安全

传统特征提取和威胁感知等手段难以有效应对 6G 网络中的不确定威胁. DHR 内生安全架构 [15] 为在未知攻击者先验信息的条件下, 对漏洞后门形成动态测不准效应提供了可行思路. 如图 4 所示, DHR 架构通过构造功能等价的异构执行体, 利用硬件或软件执行体的多样性和差异性, 造成外在功能与其内在结构或算法关系的不确定性, 使得攻击者无法通过输入与输出关系发现和定位可能存在的功能缺陷; 以多模裁决反馈为鲁棒控制机制, 使得隐藏于可重构执行体中的暗功能或漏洞后门, 难以独立发挥作用. 理论上, DHR 执行体中完全相异的暗功能的作用都会被多模裁决机制屏蔽; 以动态重构为运行环境变化方法, 以算法或构件等软硬件元素的动态性重构和随机性变化, 在时空维度上延展外在观测的不确定性.

DHR 构造的优势主要体现在两个方面: 一是异构冗余构造是 “相对正确公理” 的逻辑表达与实现方式, 其能够发现和应对不确定攻击与随机扰动, 保证系统安全且稳定的运行; 二是 DHR 构造可形

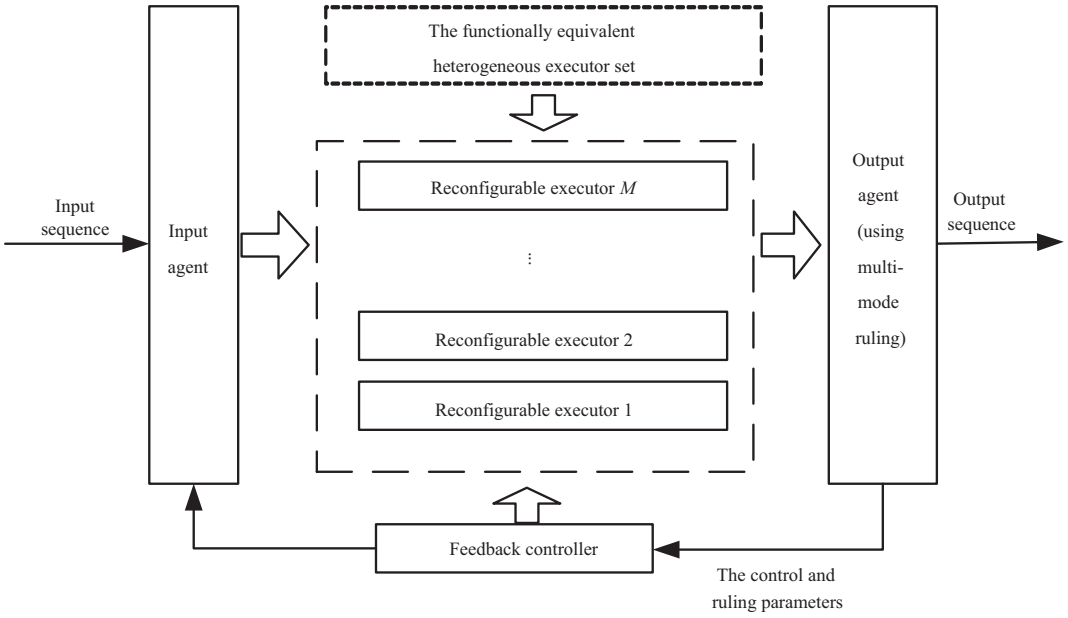

图 4　经典 DHR 架构抽象模型

Figure 4　Classic DHR architecture model

成 “测不准” 效应, 能够实现变确定性为动态性, 使暗功能的时空一致性被结构的动态性破坏, “试错攻击” 的基础将被打破, 结构的自由度覆盖攻击的自由度, 且时空状态的熵空间足够大、不随攻击而减小. 利用 DHR 构造建立的内生安全体系可达到 “我可见敌”、“敌不见我” 的效果, 能够不依赖攻击者任何先验知识和行为特征, 同时应对不确定安全威胁以及不确定随机扰动.

DHR 构造尤为适合用于基于 SDN 和 NFV 等技术构筑的 5G 网络云化架构, DHR 构造的 5G 云已经在行业专网中布局. 6G 无线网络池化资源的动态性、异构性、冗余性具有天然的内生安全属性, 遵循隘口设防/要地防护的防御原则, 对无线网络关口和关键网元等进行内生安全构造, 可利用不可信、低可靠的构件来构造安全、可靠的系统, 同时应对不确定安全威胁和不确定随机故障, 一体化解决安全可信性、功能可靠性、以及服务可用性. 这与 6G 通信/服务/安全三位一体的要求高度一致. 因此, DHR 构造可为 6G 网络侧安全提供重要支撑.

2.2.2　无线内生安全构造 —— 基于物理指纹的无线内生安全

无线通信安全的 “短板” 在空口, 根本原因是电磁波传播的开放性这一内源性缺陷造成了无线链路的脆弱性. 电磁波传播机理可用麦克斯韦 (Maxwell) 方程及其边界条件刻画, 其中麦克斯韦方程是电磁波传播的共同模型, 而差异化的无线环境反映的边界条件决定了差异化的方程解. 这一科学规律揭示出无线环境是无线内生安全的本质属性, 是解决无线内生安全问题的重要切入点 [17, 18].

在无线通信系统中, 无线环境通过自然信道起作用. 信道具有随机性和时变性, 是自然界中一种天然的随机源. 同时无线信道还具有唯一性, 不同位置对应的无线信道所表现出的特征属性不同, 与量子密码类似, 具有第三方无法测量、无法重构、无法复制的特点, 即无线信道具有天然的内生安全属性. 如图 5 所示, 典型的无线通信系统可看成是一种天然和人工的 DHR 构造, 其中, 无线信道、发信机和接收机分别对应 DHR 的异构执行体、输入代理和输出代理.

无线环境中还蕴含着另一典型的内生安全属性 —— 射频指纹. 射频指纹源于发射机中部件容差

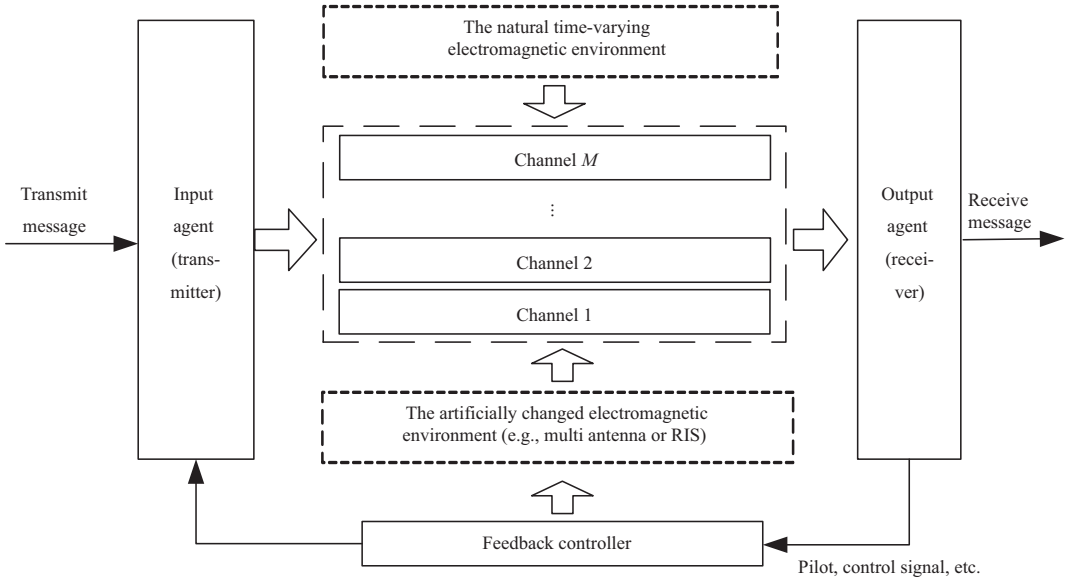

图 5 无线通信系统的内生安全架构模型

Figure 5 WESS architecture model

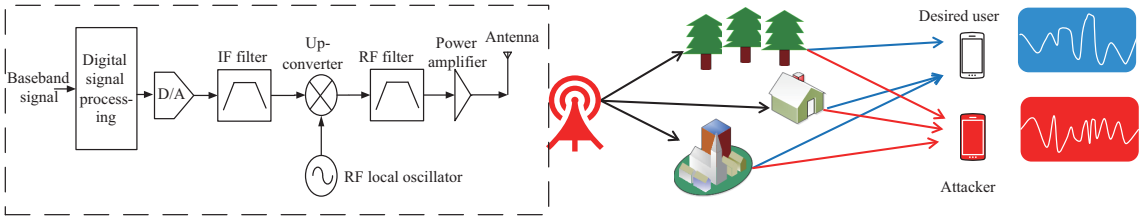

图 6 (网络版彩图) 基于物理指纹的无线内生安全

Figure 6 (Color online) Physical fingerprint based WESS

和工艺条件等造成的系统不一致性, 其产生机理决定了射频指纹具有唯一性和第三方不可仿冒性. 因此, 射频指纹可用于识别接收信号来源从而实现信息保护和设备的快速认证 [19~21]. 综上, 可借鉴多因素认证的思想 [22~24], 将物理指纹 (信道指纹和射频指纹) 作为新质内生安全属性 (图 6 所示), 在信号层面为 6G 提供抵御已知和未知无线接入攻击的能力.

2.2.3 逼近香农 “一次一密” 的通信安全一体化

香农 (Shannon) 开辟了用信息论来研究通信与安全的新思路, 分别提出了通信容量限 [25] 和安全容量限 [26]. 近年来, 业界围绕逼近通信的香农限做出了许多的努力并取得了卓著的成果. 然而, 安全的香农极限却受制于密钥生成速率和密钥分发这两个条件.

通信过程天然地既传递了信息熵, 也传递了信道熵. 从图 7 可以看出, 信号 X 和信道 H 的数学表达具有对称性, 那么通信过程传递的信源信息与环境信息是否具有某种对称性, 即 $H(x) = H(k)$. 根据此猜想, 文献 [27] 从理论上说明了香农 “一次一密” 在无线通信中的内生可实现性, 即充分利用一次通信交互中传递的所有信息量, 可在对通信容量不产生影响的情况下使密钥容量逼近信道容量, 同时达到香农信道容量和安全容量. 工程中为突破密钥生成速率的瓶颈, 可以考虑利用 RIS 辅助对无线信道进行精细认知和重构, 使得从环境信息中提取的密钥速率保持与通信速率匹配.

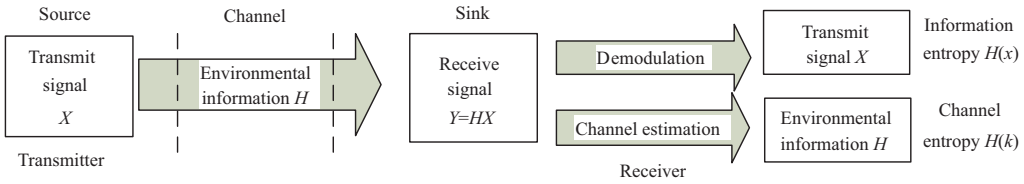

图 7　(网络版彩图) Shannon 一次一密在无线通信中的内生可实现性

Figure 7　(Color online) The endogenous feasibility of Shannon one-time pad in wireless communication

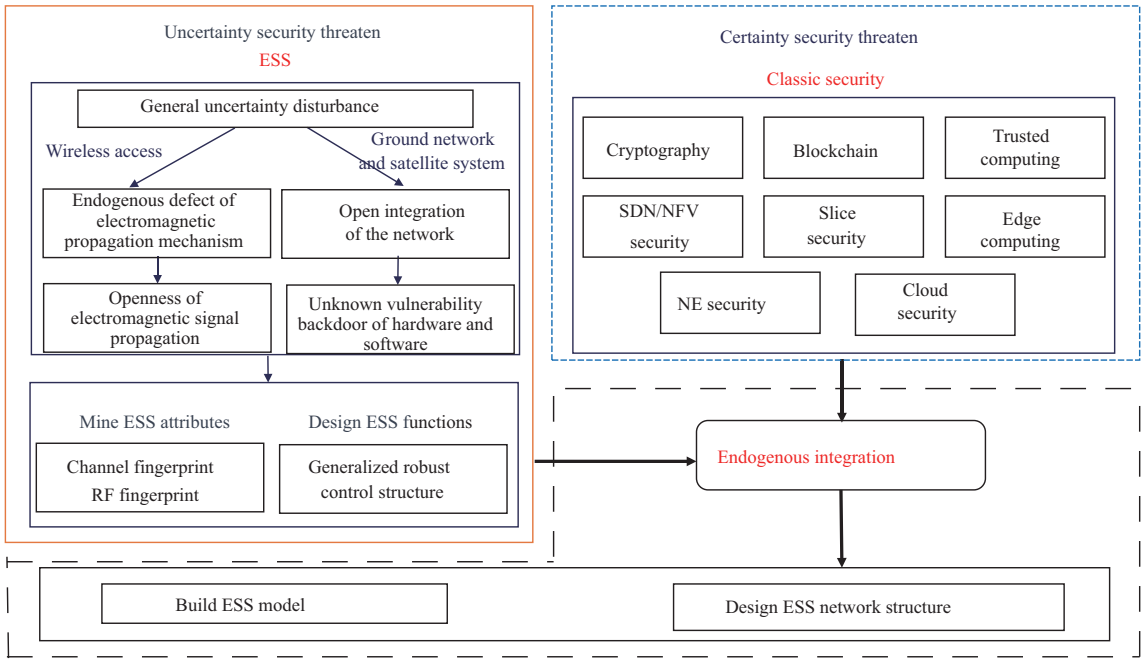

图 8　(网络版彩图) 内生安全与传统安全技术融合

Figure 8　(Color online) Integration of ESS and traditional security technologies

逼近香农一次一密方法主要体现在以下几个方面, 一是利用无线信道的唯一性、时变性和随机性等内生安全属性, 从信道中提取随机密钥, 能够生成第三方无法测量、无法重构、无法复制的密钥, 保证了密钥的安全性. 二是通过无线内生属性与 RIS 等新兴使能技术的结合, 充分挖掘 RIS 的电磁环境定制能力和电磁可重构特性, 从增强无线信道熵与精细化感知无线信道两个角度双管齐下, 同时提高无线通信容量和无线密钥生成速率, 逼近 “一次一密” 的安全效果. 三是通过内生安全与传统安全防护技术的结合, 实现点面融合, 逼近 “一次一密”, 具体而言, 利用随机、时变的无线信道密钥拓展密码算法的密钥空间, 增强密码算法的安全强度, 并实现算法复杂度与安全强度的按需调控. 四是将 “一次一密” 加密安全拓展到 “一次一认证” 认证安全, 研究基于高速动态密钥的高强度认证, 并设计加密认证一体化协议与机制, 具备逼近 “一次一密” 和 “一次一认证” 的一体化能力. 五是通过设计内生于信号通信过程、信号传输辅助的无线密钥生成方法, 形成通信安全一体化的高速无线密钥生成机制, 实现密钥速率与通信速率的高能效适配.

2.2.4 内生安全与传统安全技术融合

内生安全与传统安全技术之间能够相互补充. 如图 8 所示, 针对 6G 网络中明确的安全需求和已知的安全威胁, 可以继承和发展 5G 网络安全技术 [28], 在计算安全理论框架下开展传统密码体系中的加密、认证和完整性保护等安全技术的增强研究; 针对电磁环境内源性缺陷与网络架构开放融合产生的未知安全威胁, 从内生安全的普遍原理出发, 在信息论安全理论框架下结合无线环境内生属性开展信号层面的内生安全功能设计, 在内生安全理论框架下开展网络架构和网络构件的内生安全构造研究. 通过内生安全与传统安全技术的融合, 发挥传统安全技术能够对确定性安全威胁进行 “点防御” 实现 “特异性免疫” 的同时, 内生安全技术能够对不确定性安全威胁实施 “面防御” 实现 “非特异性免疫”, 两者结合能够形成 “点面融合” 的防御体系, 不仅在未知安全威胁 (“有毒带菌”) 的环境中实现安全, 还能针对确定安全威胁进行高效精准的 “杀毒灭菌” [16], 达到 “$1+1>2$” 的效果.

内生安全与传统安全技术之间能够相互增强. 发挥传统安全技术对已知攻击精确、高效反应的优势, 可在 DHR 构造裁决发现异常前进行前置防御, 或在裁决感知异常时, 提供精准排查、隔离或清洗的手段; 传统安全技术种类繁多, 通过有意识地分散配置, 还能够增加执行体的异构度, 提高 DHR 构造抗共模逃逸能力. 内生安全技术通过对执行体动态化、差异化、智能化的部署, 能够为传统安全技术提供非线性的抗攻击增益 [15].

2.2.5 内生安全与新兴技术融合

先进性与可信性的对立是 6G 新兴使能技术不可回避的问题, 主要表现为两个方面: 一是如何有效应对由新兴使能技术引发的已知或未知的安全威胁; 二是如何利用新兴使能技术赋能增强内生安全.

面向 6G 智能驱动的安全需求, 将内生安全与人工智能技术 [29,30] 融合, 一方面, 利用 AI 赋能无线内生安全的信道特征提取、识别与预测 [31], 使得目标用户与窃听用户的信道特征差异辨识更加准确、快速、智能, 实现主动抵御接入攻击的高效智能安全 [32]. 利用 AI 赋能 DHR 架构中的多模裁决, 通过对异构场景多维特征提取与智能裁决, 实现对隐匿于网络中的数据、内容、行为等多个维度的未知威胁感知发现; 另一方面, 人工智能计算结果的不可解释性与不可推测性是其内生安全问题, 利用内生安全技术解决人工智能的内生安全问题, 能够有效应对面向人工智能的恶意数据攻击、载体安全、数据隐私等威胁, 更好地为 6G 无线网络提供安全的智能引擎.

RIS 是 6G 的关键使能技术之一 [33]5), 近两年来受到业界的广泛关注, 并已在理论研究和样机研制方面取得了重要进展. 得益于 RIS 可对电磁波的幅度、相位、方向等进行高效、快速、灵活调控的特性 [34], 通过材料科学与信息科学交叉融合产生的非线性增益可以强化赋能无线通信内生安全 [35~37]. 利用 RIS 提供的精细化感知和实时重构无线信道的能力, 使无线信道由不可控和被动适应向按需重构和优化定制演进, 进一步丰富、放大、加速电磁环境的随机性、异构性和动态性.

2.2.6 6G 内生安全评估

目前安全的指标量化和验证评估仍是世界性难题, 亟待提出可量化设计、可验证度量的内生安全评估方法, 建立 6G 安全功能与性能指标体系. 由于 DHR 构造是 “相对正确公理” 的逻辑表达与实现方式, 在经典可靠性理论中非异构冗余场景下无法感知的不确定扰动问题, 在相对正确公理等价场景下能转化为具有概率属性的可感知的差模或共模问题, 且与不确定扰动的具体性质或行为特征无关, 即不依赖先验知识.

5) 6G 新天线技术白皮书. 2020. http://www.chuangze.cn/third_down.asp?txtid=3552.

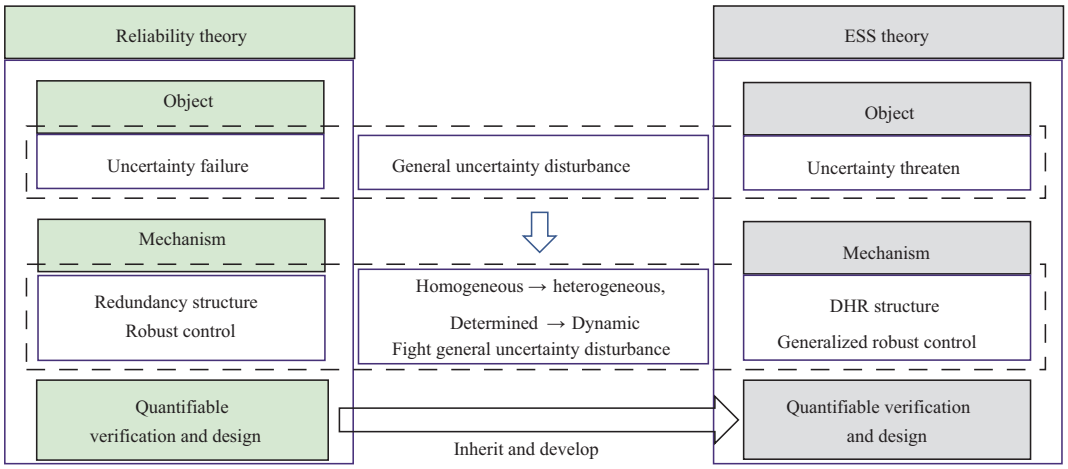

图 9 (网络版彩图) 网络侧内生安全评估原理

Figure 9 (Color online) ESS evaluation principles of the network

网络侧内生安全评估是对可靠性理论的继承发展, 如图 9 所示, 可靠性理论的对象是不确定失效问题, 采用冗余构造和鲁棒控制的体制机制, 能够实现可验证度量与量化设计. 内生安全理论的问题对象为不确定威胁, 其与不确定失效统称为广义不确定扰动. 将可靠性理论应用到内生安全理论, 针对问题对象的广义不确定性扰动, 利用动态、异构、冗余构造和广义鲁棒控制来对抗广义不确定性扰动, 能够将可靠性理论在验证度量与量化设计上的优势得以继承和发展. 因此, 基于可靠性理论可以提出内生安全的量化设计和验证度量方法, 而且能够实现服务可用性、通信可靠性和安全可信性的一体化验证评估和一体化量化设计 [15].

无线内生安全本质上是利用不同时空环境的信道异构性、空时频资源的冗余性、无线传播环境变化的动态性, 实现期望信道最佳接收的同时, 增加其他异构信道上接收信号的不确定性, 并通过感知信道的异构度抵御来自于异常信道的无线接入攻击. 因此, 可将上述安全性能转化为异构环境物理隔离距离下信号的接收误码率与识别成功率. 具体而言, 由于无线侧安全源于信道差异, 安全性能取决于合法与窃听信道之间的相关性, 而信道相关性可用安全间隔表征, 因此可用传输安全间隔和认证安全间隔这两个指标来评估安全性能和指导实际系统设计 [38]. 将无线内生安全评估的传输安全间隔定义为以合法用户和窃听者误比特率为约束的最小间隔距离, 首先将当合法用户误比特率为 10^{-5} 时, 窃听者的误比特率不低于 45% 定义为绝对安全传输, 如图 10 所示, 若窃听用户与合法用户的距离大于 D 时, 能够以 95% 的概率实现绝对安全传输, 则称 D 为传输安全间隔. 类似的, 将认证安全间隔定义为以认证设备拒绝攻击成功率为约束的最小间隔距离, 具体而言, 首先将认证设备拒绝攻击成功率不低于 95% 定义为绝对安全认证, 若攻击者与合法用户距离大于 D' 时, 能够以 95% 的概率实现绝对安全认证, 则称 D' 为认证安全间隔.

3 内生安全在 6G 空口的应用构想

3.1 6G 空口安全需求

针对要求支持 1 Gbps 的用户体验速率以及 1 Tbps 的峰值速率的超高吞吐量通信场景, 需要实现超高速数据加密、超高速数据认证、超高速信号安全传输的内生安全功能. 超大规模天线、RIS、太赫

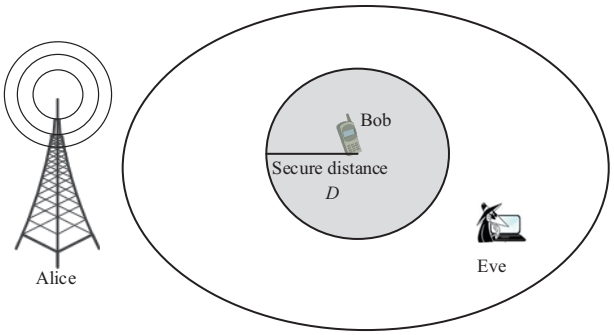

图 10 (网络版彩图) 安全间隔示例

Figure 10 (Color online) Example of secure distance

兹等 6G 无线传输候选关键技术不仅为 6G 提供了更丰富的通信资源, 而且提供了冗余信道、无线环境定制、超强方向性波束等内生安全属性. 因此, 可利用这些内生属性同时满足 6G 宽带通信和安全的需求, 实现通信与安全的一体化设计.

针对要求支持千万级/平方公里的超大连接通信场景, 传统安全手段面临伪造仿冒节点发起 DDoS 攻击、海量密钥管理等挑战, 需要研究利用信道指纹的第三方不可仿冒性和测不准性, 设计密钥生成/分发方案, 减轻密钥分发管理的负担. 此外, 还需要设计分布式无线接入点的分流卸载方法, 解决因大量并发请求而产生巨大安全开销的问题.

针对要求接近零时延的超低时延通信场景, 传统安全手段跨层跨域的实现方式导致信息安全传输/处理时延大, 同时安全机制依赖外挂式安全字段, 进一步降低了传输效率, 变相地增加了时延. 针对以上问题, 需要在系统的物理层 (无线链路侧) 直接进行安全处理, 并采用无外挂字段的加密或认证方式, 如基于物理指纹的安全方案提高传输效率、降低时延.

针对终端的功耗、算力、成本、体积等资源受限的场景, 尤其在未来 6G 万物智联的网络中大量能耗和处理能力受限的终端和节点 [39], 对安全效能要求较高, 面临高安全与轻量级这一固有的矛盾, 需要设计不依赖于计算复杂度的内生安全机制, 同时满足安全性与轻量级需求, 归一化地给出通信可靠与安全可信的解决方案.

3.2 移动边缘内生安全计算 (MeSEC)

如图 11 所示, 终端与接入点之间采用的加密和认证机制本质上是对无线链路的安全进行保护, 应当在终端与接入点物理实体的逻辑边缘实现. 而现阶段基于密码学体系的密钥分发流程必须经过网络侧跨协议层完成. 以认证为例, 终端、接入点和网络侧之间需要交换鉴权参数 [40], 通过比对认证向量才能相互认证, 存在传输、处理时延大的问题.

移动边缘计算 (mobile edge computing, MEC) 作为 5G/B5G 的关键技术 [41, 42], 将计算和处理能力受限终端的计算负载转移到更接近终端的边缘节点来处理, 无需交由距离较远回程链路的云端, 可大大提高效率并降低云端负荷, 大大减少了物联网终端的计算时延和处理资源开销.

受该技术启发, 本文提出移动边缘内生安全计算 (mobile endogenous security by edge computing, MeSEC) 的理念, 将传统跨协议层和跨物理域的安全转化为在逻辑最边缘 (协议栈底层)、物理最边缘 (物理域前端节点) 实现的安全, 使得无线安全的操作回归到无线链路, 实现极简高效的安全. 具体而言, 将传统需经过终端、接入点和网络之间跨协议层、依靠附加安全字段的加密和认证流程, 转化为利用信道指纹和射频指纹在终端与接入点之间通信的物理层实现内生安全, 通过分布式接入点分流卸载

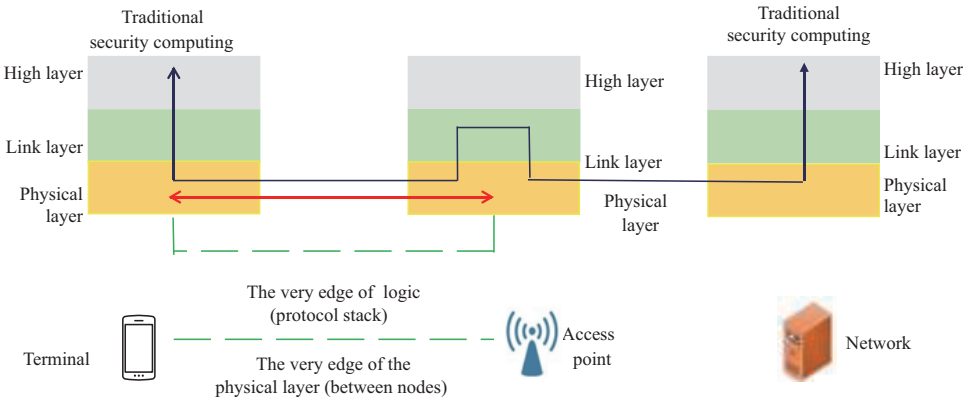

图 11 (网络版彩图) 移动边缘内生安全计算

Figure 11 (Color online) Mobile endogenous security by edge computing (MeSEC)

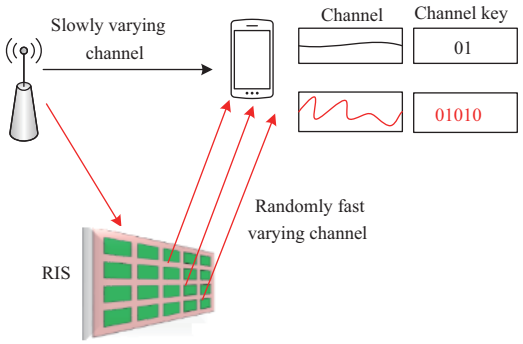

图 12 (网络版彩图) 慢变信道下的高速密钥生成

Figure 12 (Color online) High-rate key generation under the slowly varying channel

安全负荷, 有效缓解大量并发安全请求产生的网络拥塞. 其中信道指纹和射频指纹蕴藏于信号中, 可伴随通信流程一体化完成提取与处理. MeSEC 可作为一种新型的安全架构, 实现 6G 空中接口的轻量级加密和认证.

3.3 RIS 辅助的内生安全技术

为实现与 6G 高吞吐量通信速率匹配的高速密钥生成, 逼近 “一次一密” 的目标, 可利用 RIS 对电磁波的快速、灵活调控能力, 设计基于 RIS 的动态异构阵列 [43], 在精细化信道感知的基础上优化定制无线信道, 实现内生安全密钥的高速生成, 具体表现为: (1) 在接收端通过对信号多径进行精确观测实现信道特征的精细化提取, 获取信道密钥的高产出比; (2) 利用动态异构阵列提升信道的自由度, 使信道去相关, 在提高通信容量的同时提高密钥生成速率; (3) 发送端在对信道精细化感知的基础上, 通过按需重构信道, 加大电磁环境的异构复杂度和随机时变性, 扩大信道密钥空间.

上述技术路线同样适用于解决准静态慢变信道下密钥生成速率和安全性不可控的问题 [37]. 如图 12 所示, 采用 RIS 能够实现电磁环境实时可重构, 无线信道动态可编程, 提升原有信道的动态性和随机性, 为慢变信道下逼近 “一次一密” 的密钥生成提供条件.

太赫兹通信作为 6G 潜在关键技术之一 [44, 45], 可提供超大带宽通信. 传播指向性强、传输距离受限的特点是该技术实用化的短板. 针对这一问题, 可采用 RIS 技术扩大太赫兹通信信号的覆盖范围.

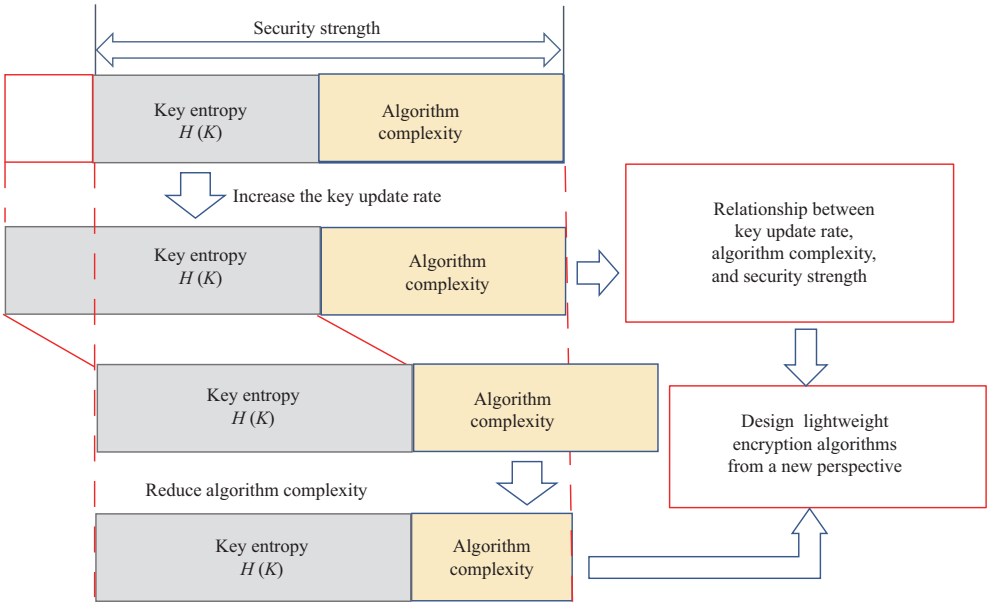

图 13　(网络版彩图) 安全强度与密钥熵、算法复杂度之间的关系

Figure 13　(Color online) Relationship between security strength, key entropy, and algorithm complexity

然而, 引入 RIS 的同时可能会带来附加的电磁散射, 增大信息泄露的风险. 基于内生安全理念, 可通过 RIS 的参数设计联合优化信号覆盖与安全性, 形成适用于太赫兹通信的内生安全传输方案.

3.4　与传统密码技术融合的空口内生安全

物联网中的海量低功耗终端受储存和计算处理能力限制, 面临加密算法复杂度与安全强度无法兼顾的矛盾. 由于安全强度与密钥熵和加密算法复杂度有关, 在密钥熵不变的情况下, 传统通过降低算法复杂度实现轻量级加密的方法势必会导致安全强度降低. 如图 13 所示, 既可以通过增加密钥熵来提升安全强度, 也可以在安全强度不变的条件下, 通过提升密钥熵降低加密算法的计算复杂度, 即用密钥熵换取计算复杂度, 从而实现轻量级加密. 因此, 基于无线信道指纹生成时变密钥, 通过对信道密钥更新频率、算法复杂度与安全强度的关系开展量化研究, 从无线内生安全的角度设计轻量级加密算法, 对传统密码加密体制的性能提升具有重要意义.

如图 14 所示, 将基于无线信道指纹构造的内生安全与传统密码技术融合, 利用自然信道叠加人工信道形成的快变信道作为共享随机源生成密钥, 能够在提高安全性的同时降低传统加密算法的复杂度, 为 6G 海量低功耗终端提供轻量级强安全加密.

3.5　基于链式密钥的加密认证一体化轻量级增强安全机制

得益于无线内生安全理念, 使加密和认证天然具有密不可分的内在联系. 例如, 在收发双方完成初始认证后, 发送方利用信道指纹生成密钥对消息进行加密, 若接收方可正确解密便是认证了合法信道, 从而实现了对发送方身份的认证. 利用信道指纹生成密钥不仅在加密方面具备轻量级、动态更新、逼近 “一次一密” 的优势, 在认证方面也具备低时延、安全、高效的特点. 而传统密码学和射频指纹可以提供初始的认证凭据. 因此, 可以将信道指纹、射频指纹等内生安全元素与传统密码学中的加密、认证算法结合进行优势互补, 实现加密认证一体化设计.

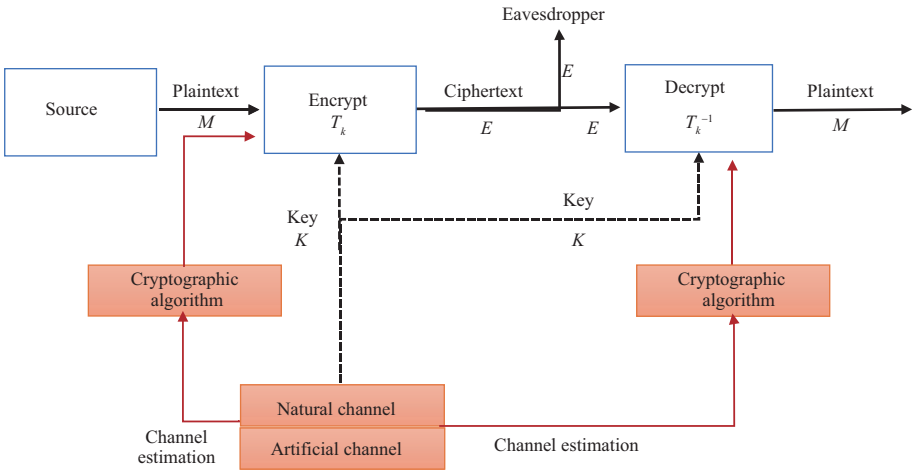

图 14 (网络版彩图) 内生密钥与传统密码算法结合的轻量级加密

Figure 14 (Color online) Lightweight encryption combining endogenous key and traditional cryptographic algorithms

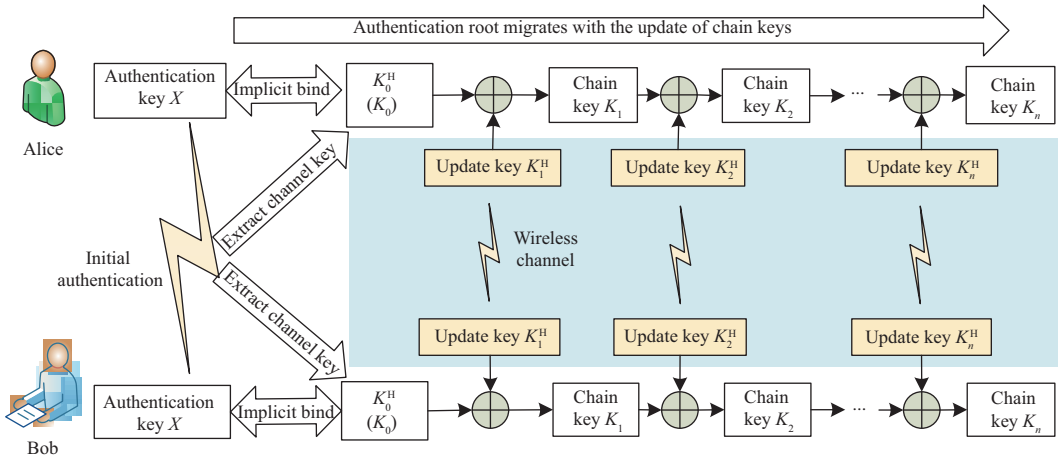

图 15 (网络版彩图) 物理密钥链式结构的构造原理

Figure 15 (Color online) Construction principle of PHYLOCK

3.5.1 物理密钥链式结构 (PHYLOCK)

物理密钥链式结构 (physcical layer offered chain key, PHYLOCK) 将内生密钥与传统密钥巧妙融合 [46], 采用环环相扣的铰链结构在原来单一密钥强度的基础上进一步实现了安全加固, 可提供融合物理指纹的加密与认证能力, 实现低时延、低开销、轻量级、强安全的效果, 为 MeSEC 理念的工程实现提供技术支撑.

物理密钥链式结构的构造方法主要包含以下步骤, 具体如图 15 所示, 首先利用根密钥进行初始认证建立安全锚点, 若通过认证则从初始认证的信道中提取信道密钥 K_0^{H}, 并用该信道密钥生成初始密钥 K_0, 自然实现了安全锚点与物理指纹的隐式绑定和内生迁移. 后续利用前次密钥 K_{n-1} 和当前提取的信道密钥 K_n^{H} 经过某种运算 (以异或运算为例), 即可生成当前密钥 $K_n = K_{n-1} \oplus K_n^{\mathrm{H}}$, 不断重复上述过程就形成了具有链式结构的密钥. 物理密钥链式结构可同时用于加密和认证, 在加密方面, 窃听者欲破解链条上的任意一次密钥, 必须掌握该次密钥以前的全部历史密钥信息, 实现了安全的加固.

当链式密钥满足 $I(K_i;K_j)=0$, $H(K_i)=H(K_j)$, 则具有 “一次一密” 的完美安全性. 在认证方面, 随着链式密钥的不断生成, 当链式密钥用于认证时, 密钥链的构造逻辑决定了认证信任关系的安全传递, 实现了可信认证根的隐式内生迁移, 可用于实现 “一次一认证”.

3.5.2 链式密钥的应用

与传统密钥技术相比, 物理密钥链式结构将传统密钥与物理层密钥融合, 使得传统根密钥仅出现一次, 大大降低根密钥泄漏概率, 且物理层密钥利用无线信道这一天然随机源, 有效解决传统密钥分发和管理难度大的问题. 因此, 物理密钥链的应用主要体现在以下 3 个方面, 一是能提供逼近 “一次一密” 的密钥, 可实现轻量级的加密; 二是能够实现可信认证根的隐式比对与内生迁移, 用于实现 “一次一认证”, 且认证时无需附加字段 (MAC 等), 具有高安全性和高效性; 三是可一体化实现轻量级的加密和认证.

针对 6G 宽带通信场景下超高数据吞吐量需求, 仅采用传统密码体制实现高强度的数据完整性保护存在认证开销大、能效低等问题. 可采用基于链式密钥的高吞吐量数据完整性保护方案, 以身份信息为锚点, 融合新质认证元素提高认证安全性, 同时降低开销、提升能效, 实现绿色安全通信. 具体而言, 采用基于无线环境特征与高速密码的融合认证技术, 利用空中传播的电磁信号天然携带信道信息这一物理机理, 将信道作为新质认证元素, 结合高速密码算法生成匹配 6G 高吞吐量的认证标签. 通过用户身份与信道绑定, 实时生成隐含用户身份与信道特征的认证密钥, 利用信道自身的时变性和唯一性以及链式密钥的安全加固, 使得除合法用户外的攻击者无法跟踪密钥变化, 可感知并抵御其他时空坐标上发起的无线接入攻击, 提高认证的安全性. 此外, 在通信时对数据差错校验的过程中自然地验证了链式密钥对信息加解密的正确性以及认证可信根一致性, 可实现通信、加密、认证三者的内生一体化 [46].

在 6G 具有超大连接/超低时延需求的物联网场景 [47, 48], 海量设备的认证接入存在巨大挑战, 传统密码认证协议在网络侧存在海量认证密钥分发管理难、时延高等问题, 在终端侧存在复杂度高、安全强度不足等问题, 亟需研究面向 6G 超大连接/超低时延物联网的轻量级强安全认证机制. 针对以上问题, 可将链式密钥用于实现 MeSEC, 实现面向短包的轻量级认证. 传统密码认证机制采用外挂式安全字段, 需要在每个数据包后额外添加消息认证码 (MAC), 带来的效率下降间接地增加了传输时延. 此外, 考虑到 6G 物联网中数据包短促频发的特点 [49], 传统基于 MAC 的认证易受仿冒攻击, 采用链式密钥, 将信道指纹这一天然的无线传播环境内生安全元素用于认证, 与通信共生一体, 无需附加认证标签, 可实现无外挂字段的轻量级认证. 另外, 针对短包传输场景, 需要研究物联网中短包传输对无线信道指纹提取的开销、延时和信息泄露等性能的影响, 设计面向短包的轻量级指纹认证方案.

3.6 6G 空口安全总体设想

本着结构决定功能、结构决定性能、结构决定效能、结构决定安全的设计理念 [15], 6G 空口安全总体方案的构想如图 16 所示, 在系统体系结构上采用 MeSEC, 使终端和接入点在物理层即可实现极简高效的安全; 在安全数据结构上采用 PHYLOCK, 将信道密钥与传统密钥巧妙融合, 可实现认证根的隐式内生迁移特性, 进一步用于实现 “一次一认证”, 完成加密认证一体化设计, 从而实现 6G 空口的轻量级安全增强; 在物理信道结构上采用基于 RIS 的动态异构阵列, 通过主动构造信道指纹, 为密钥链逼近 “一次一密” 提供必要条件, 实现密钥速率与通信速率的高能效适配.

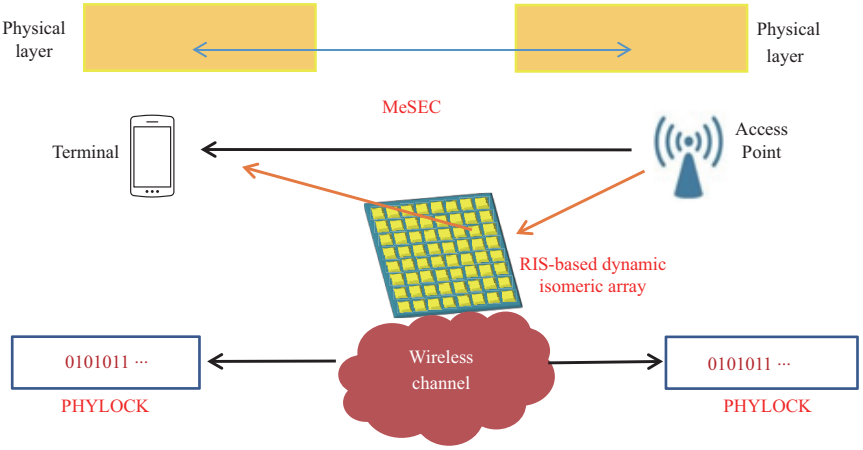

图 16　(网络版彩图) 6G 空口安全方案构想

Figure 16　(Color online) Vision of 6G air interface security solution

4　6G 天地一体化全域覆盖的内生安全技术

星地互联是实现 6G 天地一体、全域覆盖的重要途径 [50,51], 如图 17 所示, 它具有广域覆盖、关键节点 (卫星) 暴露等网络特点, 其面临的节点仿冒、DDOS 攻击、链路资源窃取、窃听的安全风险与需求均高于地面移动通信网络 [52,53]. 参照我国 “天地一体化” 和美国 “星链计划” 等卫星网络的发展现状及趋势 [54], 目前星地安全架构基本沿用地面移动通信网络安全框架, 同时考虑到 “天弱地强” 的现实能力, 将传统基站侧的安全功能少部分留在星上, 大部分落在地面, 主要措施包括: (1) 基于预置根密钥进行馈电链路和用户链路部分信令的加密认证; (2) 基于终端与网络间的端到端加密认证实现高等级安全通信. 但是由于星地网络链路距离远且开放、星上资源受限、安全中心部署在地面, 上述安全措施存在认证时延长、链路及星上系统易被攻击、无线密钥推送易泄漏、用户链路保护力度弱等问题, 星地链路安全防护能力低于地面移动通信网络 [55]. 因此, 与地面移动通信网络相比, 星地网络的安全需求与防护能力严重倒挂、差距明显.

6G 天地一体化安全的当务之急需补强短板、弥合差距, 需要重点研究: 面向用户链路和无线密钥推送这一安全最短板的空天地链路侧内生安全、面向终端接入和节点组网的天地异构网络安全认证融合、面向高安全等级用户的卫星全域覆盖高安全通信密码管理, 以及面向星上系统的结构内生卫星安全可靠一体化. 本文主要针对空天地链路侧和星上系统内生安全这两个研究点进行展开描述.

4.1　空天地链路侧内生安全技术

针对空天地链路侧存在的问题, 可采用密钥内生方案, 无需无线开放环境中的密钥推送, 利用射频指纹和信道特征的内生安全属性, 实现网络边缘的认证和加密, 降低安全隐患. 另外, 通过将部分防御关口前移到卫星、减少落地回传, 可实现前置底层防御、降低时延和链路资源消耗.

在认证方面, 采用融合星地链路射频指纹和信道特征的双向认证机制, 由于信号中承载着终端设备和卫星的射频指纹特征, 而射频指纹具有唯一性和第三方不可仿冒性, 伴随首次接入卫星网络的认证信息可实现射频指纹同步提取并用于后续认证, 后续认证 (数据) 无需落地回传, 降低认证时延. 另外, 可融合星地链路可预测的信道特征与射频指纹一起进行多维认证, 有效提高认证准确度、抵御仿冒. 由于基于射频指纹和信道特征的认证信息提取本质上与通信是共生一体的, 无需额外的信息交互

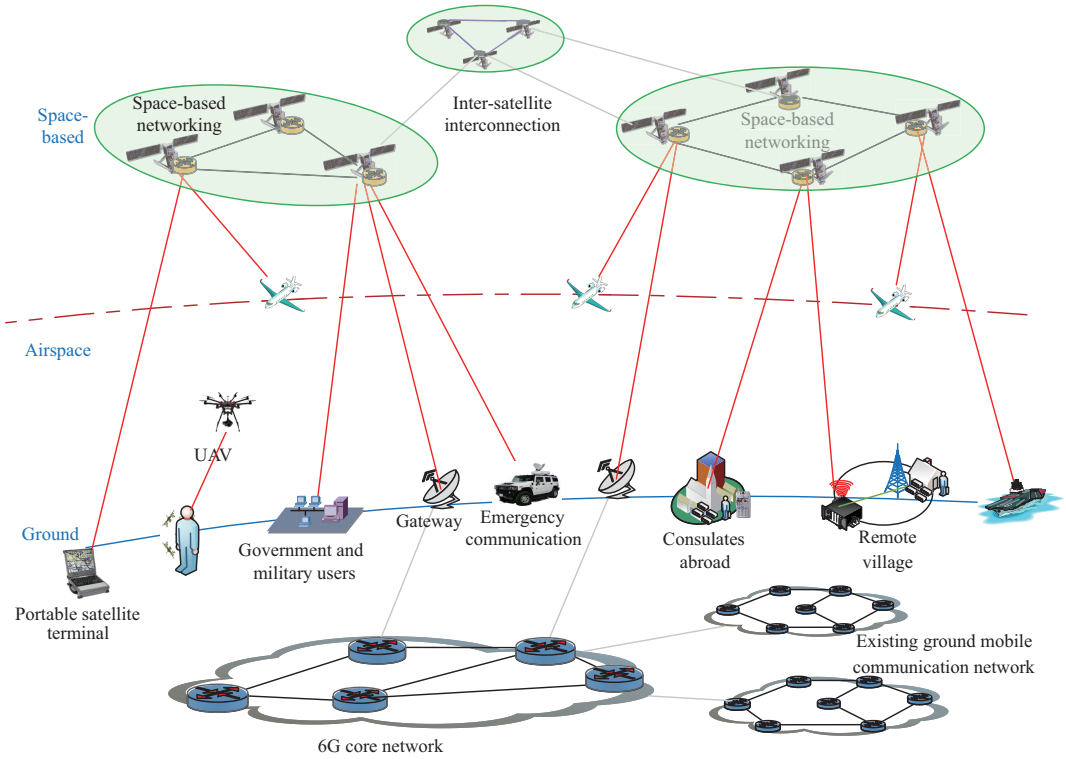

图 17　(网络版彩图) 6G 天地一体化全域覆盖网络

Figure 17　(Color online) 6G space-ground integration global coverage network

和根认证信息的预储存, 可大大降低认证时延和开销, 实现通信与认证的内生统一. 总之, 基于物理指纹的链路防护可内生实现星地链路数据的双向认证, 抵御篡改、假冒和中间人攻击, 抵御针对卫星和信关站的 DDoS 攻击.

在加密方面, 采用基于多星随机源的密钥生成技术. 由于星地链路散射路径有限, 单一星地链路多为莱斯 (Ricean) 慢变信道, 基于单一星地链路信道的密钥生成速率十分有限. 未来 6G 通信系统将会呈现多星重叠覆盖、星间协同互联、拓扑动态变化的特点, 这将使得星地链路信道随机性大大增加, 有效解决单一链路密钥生成速率不足的问题. 基于多星协作 (如图 18)、空/时/频/迹多域复合信道特征可作为星地双方密钥生成的随机源, 且其本质上由双方链路的内在结构决定, 具有内生安全属性, 能够在慢变链路中内生出第三方不可窃取的时变随机密钥, 实现加密传输. 总之, 基于多星随机源的密钥内生无需在无线开放环境中进行密钥推送、实现用户链路加密、加固馈电链路安全, 能够为卫星加密增量赋能.

4.2　结构内生的卫星安全可靠一体化

为了应对宇宙辐射造成的粒子反转等, 传统航天系统采用宇航级器件来保证系统的高可靠性, 同时也带来了巨大的成本, 仅星载控制器的成本即数以亿计. 然而, 美国 Space X 公司采用商业级器件同构冗余架构, 利用多元判决、反馈清洗的机制, 实现了宇航级的性能, 在可靠性不降低的前提下, 仅控制单元的成本即下降为原来的数千分之一 [56, 57].

Space X 公司的这种理念, 本质上为 “动态同构冗余构造”, 即用低可靠的器件来搭建高可靠的系

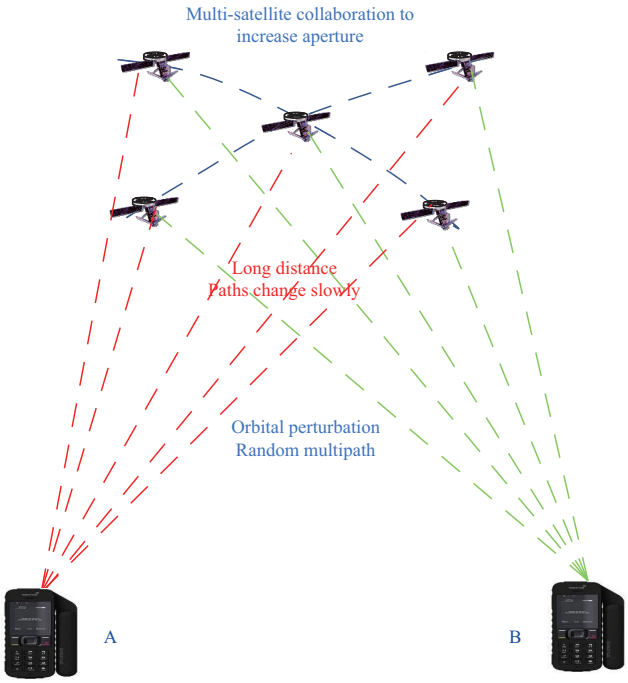

图 18　(网络版彩图) 多星协作

Figure 18　(Color online) Multi-satellite collaboration

统, 这种理念是广义鲁棒控制理论 “动态异构冗余构造” 的特例. 对比马斯克 (Musk) 的动态同构冗余, 动态异构冗余既能抵御物理失效还能防范设计缺陷, 更重要的是能够应对传统及非传统安全威胁, 系统鲁棒性更强. 综合商业应用与理论分析, 动态异构冗余架构的有效性与可行性得到了验证, 其代表了未来 6G 星载核心功能的设计趋势, 未来 6G 卫星将具备构建冗余执行体的资源条件, 可以基于动态异构冗余架构设计星上核心功能, 在实现可靠性的同时提升安全性, 赋予卫星抵御未知安全攻击的能力.

与地面动态异构冗余防护机制相比, 卫星由于计算存储资源受限、恶劣空间环境等将会面临更多的问题, 例如, 星上执行体资源有限、空间苛刻的环境如粒子辐射、高低温等易造成执行体随机扰动, 进而影响系统的可靠性保障与安全防护. 基于此, 面向 6G 的星上系统安全可靠一体化设计应包括星上资源受限下的核心功能异构执行体精准构建, 以及面向安全/可靠一体化的执行体编排和联合优化. 具体而言, 星上设计时首先需要精准化构建功能等价、结构不同的执行体, 做到 “隘口防御”, 其次, 需建立资源、成本、可靠、安全的联合优化模型, 适当引入同构资源, 对执行体进行合理动态调度、编排与优化, 使得同构、异构执行体的效能协同, 做到可靠性、安全性、稳定性、经济性的统一, 实现综合防御效果的最优化以及代价的最小化.

5　小结

本文阐述了无线网络内生安全的本质, 从无线接入电磁波传播机理和网络开放融合的架构出发, 挖掘通信与安全共有的内生属性, 融合传统技术及新兴赋能技术, 具有抵御 6G 已知和未知安全威胁的能力. 文中以 6G 无线网络内生安全思想和理念为理论基础, 针对 6G 超高速宽带通信、超大连接

超低时延、天地一体化全域覆盖等典型场景中存在的安全问题, 提出了相应的潜在关键技术和内生安全解决方案构想, 以期为 6G 无线网络安全框架设计提供理论和实际参考.

致谢 特别感谢东南大学的胡爱群、李春国、李古月、彭林宁、周小阳, 西安交通大学的王慧明、穆鹏程、王文杰, 国防科技大学的熊俊、魏急波、马东堂, 上海科技大学杨旸、殷树, 之江实验室郭荣斌, 中国电子科技集团公司第三十研究所赵伟, 中国电子科技集团公司第五十四研究所贾哲, 兴唐通信科技有限公司朱晖, 西安华讯天基的包永学, 江苏赛博空间的苗龙, 紫金山实验室的韩乾、赵见磊, 国家数字交换系统工程技术研究中心的杨梅樾、靳彦青、杨杰等专家对本文工作的贡献.

参考文献

1 Saad W, Bennis M, Chen M Z. A vision of 6G wireless systems: applications, trends, technologies, and open research problems. IEEE Netw, 2020, 34: 134–142
2 Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61: 081301
3 Huang K Z, Jin L, Chen Y J, et al. Development of wireless physical layer key generation technology and new challenges. J Electron Inform, 2020, 42: 2330–2341 [黄开枝, 金梁, 陈亚军, 等. 无线物理层密钥生成技术发展及新的挑战. 电子与信息学报, 2020, 42: 2330–2341]
4 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
5 Wang H M, Zheng T X. Physical Layer Security in Random Cellular Networks. Berlin: Springer, 2016
6 Zhou L, Wu D, Zheng B Y, et al. Joint physical-application layer security for wireless multimedia delivery. IEEE Commun Mag, 2014, 52: 66–72
7 Zou Y L, Sun M, Zhu J, et al. Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks. IEEE Trans Wirel Commun, 2018, 17: 8444–8456
8 Dunkelman O, Keller N, Shamir A. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. J Cryptol, 2014, 27: 824–849
9 Gui G, Liu M, Tang F X, et al. 6G: opening new horizons for integration of comfort, security, and intelligence. IEEE Wirel Commun, 2020, 27: 126–132
10 Liu G Y, Huang Y H, Li N, et al. Vision, requirements and network architecture of 6G mobile network beyond 2030. China Commun, 2020, 17: 92–104
11 You X H, Wang C X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301
12 Wu J X. Meaning and vision of mimic computing and mimic security defense. Telecommun Sci, 2014, 30: 2–7 [邬江兴. 拟态计算与拟态安全防御的原意和愿景. 电信科学, 2014, 30: 2–7]
13 Wu J X. Introduction to Cyberspace Mimic Defense. Beijing: Science Press, 2020 [邬江兴. 网络空间拟态防御导论. 北京: 科学出版社, 2017]
14 Wu J X. Principle of Cyberspace Mimic Defense — Generalized Robust Control and Endogenous Security. Beijing: Science Press, 2020 [邬江兴. 网络空间拟态防御原理 —— 广义鲁棒控制与内生安全. 北京: 科学出版社, 2018]
15 Wu J X. Cyberspace Endogenous Safety and Security — Mimic Defense and Generalized Robust Control. Beijing: Science Press, 2020 [邬江兴. 网络空间内生安全 —— 拟态防御与广义鲁棒控制. 北京: 科学出版社, 2020]
16 WU J X. Cyberspace Mimic Defense. Berlin: Springer, 2020
17 Hu X Y, Jin L, Lou Y M, et al. Introduction to wireless endogenous security and safety: problems, attributes, structures and functions. 2021. doi: 10.36227/techrxiv.14125346
18 Jin L, Zhang S J, Lou Y M, et al. Secret key generation with cross multiplication of two-way random signals. IEEE Access, 2019, 7: 113065
19 Yu J B, Hu A Q, Li G Y, et al. A robust RF fingerprinting approach using multisampling convolutional neural network.

IEEE Int Things J, 2019, 6: 6786–6799
20 Xing Y X, Hu A Q, Zhang J Q, et al. On radio frequency fingerprint identification for DSSS systems in low SNR scenarios. IEEE Commun Lett, 2018, 22: 2326–2329
21 Li G Y, Yu J B, Hu A Q. Research on physical-layer security based on device and channel characteristics. J Cryptologic Res, 2020, 7: 224–248 [李古月, 俞佳宝, 胡爱群. 基于设备与信道特征的物理层安全方法. 密码学报, 2020, 7: 224–248]
22 Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans Depend Secure Comput, 2018, 15: 708–722
23 Qiu S M, Wang D, Xu G A, et al. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. IEEE Trans Depend Secure Comput, 2020. doi: 10.1109/TDSC.2020.3022797
24 Wang C Y, Wang D, Wang F F, et al. Multi-factor user authentication scheme for multi-gateway wireless sensor networks. Chinese J Comput, 2020, 4: 683–700 [王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议. 计算机学报, 2020, 4: 683–700]
25 Shannon C E. A mathematical theory of communication. Bell Syst Technical J, 1948, 27: 379–423
26 Shannon C E. Communication theory of secrecy systems. Bell Syst Technical J, 1949, 28: 656–715
27 Jin L, Wang X, Lou Y M, et al. Achieving onetime pad via endogenous secret keys in wireless communication. In: Proceedings of IEEE/CIC International Conference on Communications in China (ICCC), 2020. 1092–1097
28 Sun L, Du Q H. Physical layer security with its applications in 5G networks: a review. China Commun, 2017, 14: 1–14
29 Tang F X, Kawamoto Y, Kato N, et al. Future intelligent and secure vehicular network toward 6G: machine-learning approaches. Proc IEEE, 2020, 108: 292–307
30 He H T, Jin S, Wen C K, et al. Model-driven deep learning for physical layer communications. IEEE Wirel Commun, 2019, 26: 77–83
31 He H T, Wen C K, Jin S, et al. Deep learning-based channel estimation for beamspace mmWave massive MIMO systems. IEEE Wirel Commun Lett, 2018, 7: 852–855
32 Xiao L, Sheng G Y, Wan X Y, et al. Learning-based PHY-layer authentication for underwater sensor networks. IEEE Commun Lett, 2019, 23: 60–63
33 di Renzo M, Zappone A, Debbah M, et al. Smart radio environments empowered by reconfigurable intelligent surfaces: how it works, state of research, and the road ahead. IEEE J Sel Areas Commun, 2020, 38: 2450–2525
34 Cheng Q. Space-time coding metasurface for wireless communication. In: Proceedings of IEEE Asia-Pacific Microwave Conference (APMC), 2020
35 Chen J, Liang Y C, Pei Y Y, et al. Intelligent reflecting surface: a programmable wireless environment for physical layer security. IEEE Access, 2019, 7: 82599–82612
36 Yu X H, Xu D F, Schober R. Enabling secure wireless communications via intelligent reflecting surfaces. In: Proceedings of IEEE Global Communications Conference (GLOBECOM), 2019
37 Hu X Y, Jin L, Huang K Z, et al. Secret key generation assisted by intelligent reflecting surface with discrete phase shift in static environment. 2020. doi: 10.36227/techrxiv.13146623
38 Li W, Chen B, Wei J B, et al. Secure communications via sending artificial noise by the receiver: ergodic secure region analysis. Signal Process, 2012, 28: 1314–1320 [李为, 陈彬, 魏急波, 等. 基于接收机人工噪声的物理层安全技术及保密区域分析. 信号处理, 2012, 28: 1314–1320]
39 Yang Y. Multi-tier computing networks for intelligent IoT. Nat Electron, 2019, 2: 4–5
40 Yang Z Q, Su L, Yang B, et al. 5G Security Technologies and Standards. Beijing: People's Posts and Telecommunications Press, 2020 [杨志强, 粟栗, 杨波, 等. 5G 安全技术与标准. 北京: 人民邮电出版社, 2020]
41 Zhang K, Leng S P, He Y J, et al. Mobile edge computing and networking for green and low-latency Internet of Things. IEEE Commun Mag, 2018, 56: 39–45
42 Tran T X, Hajisami A, Pandey P, et al. Collaborative mobile edge computing in 5G networks: new paradigms,

scenarios, and challenges. IEEE Commun Mag, 2017, 55: 54–61
43 Jin L, Lou Y M, Xu X M, et al. Separating multi-stream signals based on space-time isomerism. In: Proceedings of International Conference on Wireless Communications and Signal Processing (WCSP), 2020
44 Jia S, Yu X B, Hu H, et al. 120 Gb/s multi-channel THz wireless transmission and THz receiver performance analysis. IEEE Photon Technol Lett, 2017, 29: 310–313
45 Wang S W, Lu Z J, Li W, et al. 26.8-m THz wireless transmission of probabilistic shaping 16-QAM-OFDM signals. APL Photonics, 2020, 5: 056105
46 Jin L, Hu X Y, Sun X L, et al. Native security scheme based on physical layer chain key for encryption and authentication. In: Proceedings of IEEE Wireless Communications and Networking Conference, 2021
47 Ren H, Pan C H, Deng Y S, et al. Resource allocation for secure URLLC in mission-critical IoT scenarios. IEEE Trans Commun, 2020, 68: 5793–5807
48 Chen R Q, Li C H, Yan S H, et al. Physical layer security for ultra-reliable and low-latency communications. IEEE Wirel Commun, 2019, 26: 6–11
49 Wang H M, Yang Q, Ding Z H, et al. Secure short-packet communications for mission-critical IoT applications. IEEE Trans Wirel Commun, 2019, 18: 2565–2578
50 Zhang Z Q, Xiao Y, Ma Z, et al. 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh Technol Mag, 2019, 14: 28–41
51 Chao H C, Comer D E, Kao O. Space and terrestrial integrated networks: emerging research advances, prospects, and challenges. IEEE Netw, 2019, 33: 6–7
52 Li B, Fei Z S, Zhou C Q, et al. Physical-layer security in space information networks: a survey. IEEE Int Thing J, 2020, 7: 33–52
53 Zeng Y, Wang Y, Xu W B, et al. Discussion on the wireless link security protection technology of the space-ground integrated information network. Inform Secur Commun Priv, 2020, 10: 100–106 [曾勇, 王驭, 徐文斌, 等. 天地一体化信息网络无线链路安全防护技术探讨. 信息安全与通信保密, 2020, 10: 100–106]
54 Wu W, Qin P, Feng X, et al. Reflections on the development and construction of space-ground integration information network. Telecommun Sci, 2017, 12: 3–9 [吴巍, 秦鹏, 冯旭, 等. 关于天地一体化信息网络发展建设的思考. 电信科学, 2017, 33: 3–9]
55 Zhang J, Xiong J, Ma D T. Physical layer secure transmission algorithm in multi-beam satellite communication system. Appl Electron Technol, 2014, 11: 116–119 [张杰, 熊俊, 马东堂. 多波束卫星通信系统中的物理层安全传输算法. 电子技术应用, 2014, 11: 116–119]
56 Xing Q, Jiu T B L. The technology and cost analysis of SpaceX dragon spacecraft and falcon rocket. Military Abstr, 2020, 8: 25–28 [邢强, 九天波粒. SpaceX 龙飞船与猎鹰火箭技术和成本分析. 军事文摘, 2020, 8: 25–28]
57 Stone D. A new era in space flight: the COTS model of commercial partnerships at NASA. In: Proceedings of the 13th Reinventing Space Conference, 2018. 117–123

Concept and vision of 6G wireless endogenous safety and security

Liang JIN[1], Yangming LOU[1*], Xiaoli SUN[1], Zhou ZHONG[1], Xiaoming XU[1], Ming YI[1], Kaizhi HUANG[1], Xinsheng JI[1,2] & Jiangxing WU[1,2*]

1. *PLA Strategic Support Force Information Engineering University, Zhengzhou* 450002*, China*;
2. *Purple Mountain Laboratories: Networking, Communications and Security, Nanjing* 211111*, China*
* Corresponding author. E-mail: louyangming1991@outlook.com, ndscwjx@126.com

Abstract The open integration, heterogeneous coexistence, and intelligent interconnection of 6G networks will cause unknown and complex security threats. The current pattern of security lagging behind the development of communications will inevitably be difficult to deal with. Hence, the 6G era must break the mindset and give birth to an iconic technology that has a truly intergenerational effect. Endogenous security technology starts from the common and inherent security problems caused by the inherent defects of wireless networks, which can resist unknown security threats and integrate communication/security/services endogenously through structure-oriented solutions. This paper discusses the endogenous security issues and concepts of 6G wireless networks; proposes the application vision of endogenous security in typical scenarios, such as 6G ultra-high-rate broadband communications, ultra-large connections and ultra-low latency, and integrated space -ground coverage; and presents several potential key technologies and solutions.

Keywords 6G security, endogenous safety and security, communication/security/service integration, wireless endogenous safety and security, mobile endogenous security by edge computing, physcical layer offered chain key