中国科学: 信息科学 2022 年 第 52 卷 第 2 期: 205–216
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
6G 网络安全专题 · 论文

6G 网络内生安全架构研究

粟栗*, 庄小君*, 杜海涛, 冉鹏, 黄晓婷, 杨朋霖

中国移动通信有限公司研究院, 北京 100053
* 通信作者. E-mail: suli@chinamobile.com, zhuangxiaojun@chinamobile.com

收稿日期: 2021–07–31; 修回日期: 2021–09–03; 接受日期: 2021–10–08; 网络出版日期: 2022–01–20

国家重点研发计划 (批准号: 2020YFB1806801) 资助项目

摘要 6G 将是一个覆盖空天地海的一体化网络, 并为用户提供按需服务. 高安全性是 6G 网络的重要特性, 在规划的 6G 架构中, 安全能力将作为一个独立的逻辑面为 6G 网络和应用提供服务与保障. 本文分析并归纳了 6G 安全演进的 3 个方面的趋势: 一是网络架构的分布式自治化增加了暴露面, 需要网元、子网自身具备高安全性; 二是全面云化和虚拟化进一步增加了内部攻击的风险, 需要基于零信任理念设计网元、网络内部的安全防护措施; 三是按需服务的业务能力需要内部建设智能协同机制, 并具备弹性、可编排安全能力资源池. 基于上述需求和安全技术发展的趋势, 本文提出了以内部安全能力建设为基础的 6G 安全建设思路, 设计了包含安全能力层、安全策略控制器、安全智能中心、安全管理中心, 协同信任共识设施、编排能力、人工智能能力形成的 6G 内生安全架构. 本架构以网络内建安全能力为基础, 信任共识机制为纽带, 智能协同技术为手段, 形成主动免疫、信任共识、协同弹性的安全架构与运行机制. 通过构建可信链路的实际案例推演证明, 该架构可为 6G 网络和应用提供灵活、按需的安全服务.

关键词 6G, 内生安全, 运行机制, 网络安全, 信任

1 背景

业内预期, 2030 年移动通信网络将演进到 6G, 开启全新的应用场景, 无缝智能地连接人们的生产生活. 6G 网络将实现真正的万物互联, 支持如卫星网络、行业网络、体域网等异构网络和海量终端, 实现包括陆海空天在内的全球无缝覆盖. 同时, 结合社会发展的新需求和新场景, 打造 6G 全新技术生态, 推动社会走向虚拟与现实结合的 “数字孪生” 世界, 通过 “智慧泛在” 实现 “6G 重塑世界” 的宏伟目标 [1,2]. 网络架构的变化、业务需求与服务模式变化、新技术的发展等方面都对 6G 安全提出了新的需求, 也促使 6G 网络中形成 “安全面”, 为分层的网络提供服务与支撑 [3].

引用格式: 粟栗, 庄小君, 杜海涛, 等. 6G 网络内生安全架构研究. 中国科学: 信息科学, 2022, 52: 205–216, doi: 10.1360/SSI-2021-0257
Su L, Zhuang X J, Du H T, et al. Built-in security framework research for 6G network (in Chinese). Sci Sin Inform, 2022, 52: 205–216, doi: 10.1360/SSI-2021-0257

第三代伙伴计划协议 (the 3rd generation partnership project, 3GPP)、下一代移动通信网 (next generation mobile networks, NGMN) 等标准组织已经在 5G 网络中定义了网元自身安全能力; 但从 2019 年开始, 业内基于内部攻击成立的前提下, 仍提出了多个 5G 网络安全风险 [4~9]. 而 6G 网络将是一个开放、自治的架构 [10], 从内部发起攻击的安全风险将是安全考量的必备因素. 以边界网络流量检测、分析和防护为主的安全措施已不能完全满足 6G 网络/子网的安全风险防护需求, 需要增强设备自身、网络自身的安全性. 同时, 依据文献 [3] 中对 6G 网络的展望分析, 6G 安全面将与网络的基础资源层、网络能力层、服务层深度融合, 为 6G 网络提供自身安全保障与应用安全服务, 如何协同全网设备自身安全能力与安全专用设备的能力, 分析安全风险、制定安全策略、完成安全资源编排等都是新的问题和挑战.

在零信任 (zero trust, ZT) 的理论逐渐丰富并形成标准化架构 [11,12] 的同时, 内生安全的理念 [13] 逐渐发展, 已形成了基于拟态的内生安全 [14,15]、基于 AI 的有机免疫的内生安全 [16]、基于 NEW IP 的内生安全架构 [17] 等思想与理念. 这些先进的安全思想和架构也在影响着移动通信网络的安全发展方向. 文献 [18~20] 对内生安全理论在移动通信网络的应用进行了分析, 给出了应用方法与实践方案. 上述研究成果已逐渐形成了内生安全的共识, 即: 以网络中各类网元设备自身的安全能力为基础、专用安全设备和系统为扩展, 协同配合构建整个安全体系.

结合 6G 网络安全架构演进 [2,3] 与移动通信网安全技术的演进 [21], 本文认为: 6G 网络内生安全体系是以网元设备自身安全能力和内部安全能力资源池为基础, 以信任共识为依据, 以智能分析、灵活编排为手段, 形成的主动免疫、信任共识、协同弹性的安全体系.

本文针对 6G 网络内生安全需求与架构进行深入研究, 提出了 6G 网络内生安全架构与运行机制, 并通过推演实例进行论证. 本文包括 5 个部分: 一是分析 6G 网络面临的安全新需求, 并分析现有安全手段的不足; 二是结合 6G 网络架构和安全需求, 提出 6G 网络内生安全架构; 三是描述 6G 网络内生安全架构下的安全能力部署原则、规划安全能力; 四是基于实际案例分析与论证内生安全架构的运行机制; 最后, 对内生安全体系的下一步发展与应用进行了分析与展望.

2 6G 网络安全新需求与对策

在《2030+ 愿景与需求报告》[2] 中提出, 面向 2030+ 的 6G 网络在提升空口能力的基础上, 还将具备如下特征: 一是按需服务的网络, 可以使用户按需获得网络服务和极致网络性能体验; 二是即插即用的至简网络; 三是按需扩展、自治、自演进的柔性网络; 四是智慧内生; 五是安全内生. 其中, 内生的安全能力不仅保障网络自身安全, 还为应用提供安全服务.

2.1 6G 网络安全新需求

在《2030+ 网络架构展望 (2020 年)》[3] 设计的 6G 网络架构中, 安全能力被设计为一个独立的面, 如图 1 所示. 安全面与网络各层交互, 为网络提供安全能力、保障与服务, 反之网络各层也促进了安全需求的发展.

(1) 6G 网络架构演进提出了自身安全防护高要求. 6G 网络架构包含两个重要特点, 即面向空天地海一体的全方面连接、分布式自治架构组网. 全方位连接的 6G 网络将更加开放、连接也将更加多样, 使得暴露面和风险进一步增加; 而分布式自治架构中各个子网内可能实施不同的安全策略与安全能力配置, 子网内/子网间可能存在信令风暴、分布式拒绝服务攻击 (distributed denial of service, DDoS)、授权错误等安全问题.

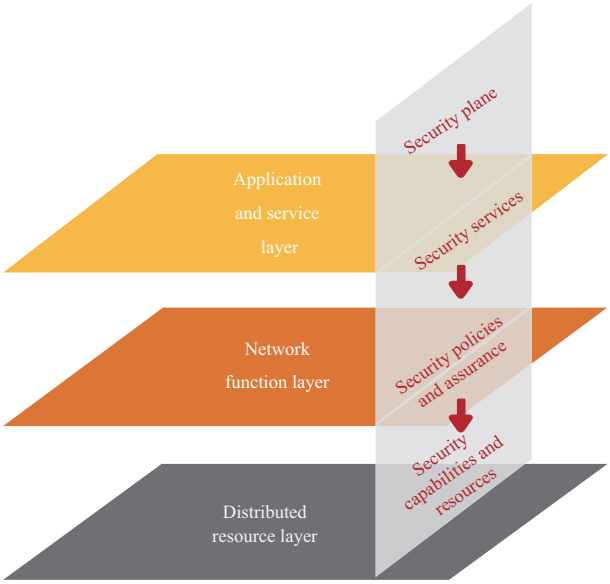

图 1 (网络版彩图) 6G 网络中的安全面

Figure 1 (Color online) Security aspect of 6G network

因此, 6G 网络中各个设备都处于开放和非信任的环境中, 设备之间、网络/子网之间的安全机制设计必须以 "零信任" 为基础. 一方面, 设备自身必须具备较高的安全防护能力, 并具备可监控和可证明机制. 另一方面, 在 6G 的自治网络中, 每个子网的安全性可能存在较大的差异, 仍然需要在区域边界部署专用安全设备.

(2) 云化和虚拟化技术的全面应用提出了内网安全防护高要求. 6G 网络将发展为全云化、虚拟化、服务化网络, 网络设备功能也将进一步解耦, 当传统物理网络设备解耦为硬件、虚拟化层、网络功能层、服务层 [21] 后, 云和虚拟化的安全性将变得更加重要. 一方面, 云和虚拟化技术应用后, 不同网元可能部署在同一物理主机上, 其交互不再经过传统的网络边界设备, 需要新的安全监控机制; 另一方面, 云化的核心网一般采用集中化部署的方式, 一旦云平台出现漏洞可能影响承载的所有网元, 云平台自身的安全检测与监控需求将更加凸显.

因此, 云和虚拟化技术的全面应用首先要求网络各层的设施与实体自身需要具备更高的安全性, 以防范内部攻击; 同时, 内网安全检测与监测能力也变成了必要的机制.

(3) 业务的新模式提出了安全能力协同的高需求. 6G 按需服务网络将提供动态的、极细粒度的服务能力供给, 当用户需求发生改变时, 按需服务网络可无缝切换服务方式和内容, 实现网络服务能力与用户需求的实时、精准匹配, 为用户带来极致无差异化的性能体验 [3]. 安全能力也是按需服务网络的重要组成部分, 且存在定制化、柔性的需求.

因此, 在构建 6G 按需服务网络时, 一是需要建设内部的安全能力资源池, 并通过智能编排的方式与其他网络设施或服务一起形成柔性的按需服务; 二是需要按业务需求进行智能分析, 合理设置安全策略, 保障业务的安全与高效运行.

综上可知, 6G 网络的主要安全需求包括: 网元设备内部建设高安全防护能力、网络内部建设高安全防护措施与安全能力资源池、网络内部建设灵活高效的安全协同能力.

2.2 6G 安全能力演进趋势分析

结合 5G 网络中已实施的安全措施, 本文分析了 6G 网络安全仍需增强的 4 个方面.

(1) 设备自身安全能力需进一步增强. 3GPP 制定的 Catalogue of General Security Assurance Requirements [22] 标准定义了每个设备应具备的 60 余项通用安全基础保障能力, 形成了 5G 网元自身安全基线; 同时, GSMA (Global System for Mobile Communications Association) 的 NESAS (network equipment security assurance scheme) 系列规范 [23~26] 定义了设备的安全测评与审计方法. 但上述要求仅能保证设备具有基本的安全防护能力, 仍不具备在开放与非信任环境中基于零信任体系的可证明安全性.

在 6G 开放、自治网络中, 需要参考零信任体系中 “没有资源是天生可信的” [11] 的原则, 要求 6G 网络设施 (包含物理设备、虚拟网元) 具备独立的高安全能力, 以确保自身安全性.

(2) 内部的安全能力需体系化建设. 从 3G 时代的 network domain security (NDS) 标准 [27] 开始, 移动通信网一直按功能区域进行划分与防护, 一般在网络边界处部署防火墙 (firewall, FW)、Web 应用防火墙 (web application firewall, WAF)、入侵检测系统 (intrusion detection system, IDS)、入侵防御系统 (intrusion protection system, IPS) 等安全设备. 在内部可信度较高的前提下, 按区域进行安全防护具备如下优势:

- 边界防护能力更强: 区域边界防护一般使用安全专用设备, 设备经过专业的设计、测试与评估, 自身安全能力有较强保障;
- 统一防护成本低: 若区域内有较多的设备, 边界统一防护成本更低;
- 运维便利: 采用边界部署模式, 更便于集中运维管理, 且运维管理成本低.

在 6G 网络中不仅需要边界防护, 还需要建设安全能力资源池, 主要原因包括 2 个方面: 一是针对内部攻击风险, 除了边界防护外, 还需要在内部建设全流程安全防护、检测、响应、恢复能力, 例如安全扫描、安全态势感知、安全事件的集中化分析和响应等; 二是由于专网业务需要定制化、弹性的安全能力配合, 因此需要在生产域建立安全能力资源池, 并通过智能编排的方式, 与网络设备一起配合形成客户所需的专网、按需服务.

因此, 基于上述需求, 需要在生产域建设一个专用的安全能力资源池, 一方面保障生产网络或客户专网安全, 另一方面可作为服务被单独调用, 为客户应用提供安全服务.

(3) 安全能力的协同亟需增强. 在目前的 5G 网络中, 网络功能 (network function, NF) 自身安全、边界安全设备、安全管理中心等协同较少, 难以实现高效率、低成本的安全防护. 在 6G 网络中, 必须加强协同分析能力, 在保障安全的前提下, 避免出现重复建设、安全策略不一致等问题, 实现 “智能、至简” 网络的目标.

因此, 在 6G 网络中需要建设一个安全智能中心, 依据网络建设或客户业务的需求, 分析网元设备、安全设备的安全能力配置, 形成安全部署策略, 并通过策略控制单元或管理系统, 将策略下达到网元设备、安全设备等进行执行.

(4) 需建立信任共识机制. 一方面, 在网络内部、子网之间各类网元设备、安全设备的安全能力需要协同, 需要建立一个可信的登记与使用机制; 另一方面, 考虑到网络安全的持续运维与优化, 6G 网络的安全智能中心应依据数据面 [3] 的数据进行安全分析或基于数字孪生网络进行推演形成安全策略, 在策略下发前应进行登记, 保证策略实施的有效性.

基于上述分析, 6G 网络安全的重点演进方向包括: 设备自身必须具备高安全能力、内部弹性安全能力需要体系化建设、安全智能分析与协同、信任共识能力需要增强. 上述安全能力大部分建设在网

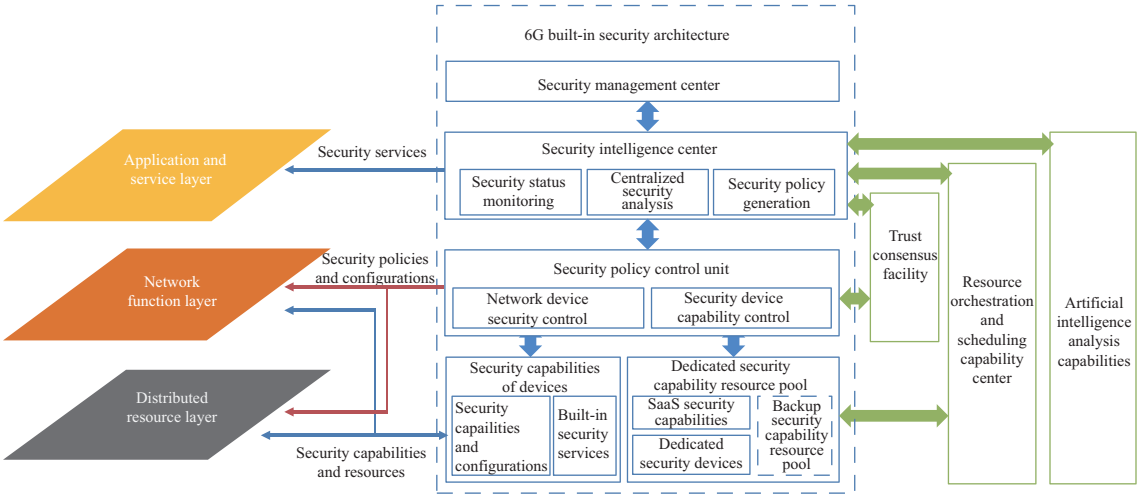

图 2 (网络版彩图) 6G 网络内生安全架构

Figure 2 (Color online) 6G network build-in security architecture

络内部, 属于 6G 网络的内生安全机制.

3 6G 网络内生安全架构及能力规划

3.1 6G 网络内生安全架构

基于第 2 节的分析, 定义 6G 网络内生安全体系为: 以网络内部建设的安全能力为基础, 以信任共识为纽带, 以智能分析、灵活编排为手段, 形成的主动免疫、信任共识、协同弹性的安全体系.

为实现上述目标, 本文设计 6G 网络内生安全架构, 包括: 安全管理中心、安全智能中心、安全策略控制单元、安全能力层 (网元设备自身安全能力、专用安全能力资源池) 4 层, 并协同信任共识设施、资源编排与调度能力、人工智能分析能力, 形成体系化安全架构. 其架构如图 2 所示.

对图 2 所示的 6G 网络内生安全架构各部分能力说明如下. 内生安全能力层是网络中安全原子能力的提供方, 包括各类设备自身的安全能力、内建的专用安全能力资源池; 为满足弹性服务的需求, 还包括安全能力的备用资源池. 安全策略控制单元是连接内生安全能力层与安全智能中心的单元, 负责将运行所需的安全策略下发到网元设备、安全设备中, 屏蔽异厂家、多类型的设备接口对接要求. 安全智能中心是整个内生安全架构的大脑, 一方面负责分析数据, 形成安全态势与安全策略建议; 另一方面可以作为安全能力整合的接口, 接收业务中的安全需求, 生成安全解决方案与调度策略, 为应用层提供安全服务. 安全管理中心与管理员交互, 负责系统安全管理. 信任共识设施为系统运行涉及的安全能力、安全策略的声明及执行过程提供不可篡改的记录, 实现信任共识保障. 资源编排与调度能力中心负责全网资源调度和设备编排, 对虚拟化设备的全生命周期进行管理. 人工智能分析能力基于 6G 智慧内生能力, 为安全智能中心提供智能分析与智能决策手段.

3.2 6G 网络内生安全能力部署与规划

3.2.1 安全能力部署原则分析

从 3.1 小节的分析可知: 安全能力的提供方可能是网元设备自身、专用安全设备、安全服务, 并通

过编排的方式形成一个整体. 为了达到高效、协同的效果, 需要分析安全能力的承载方式与运行原则.

(1) 设备自身必须具备基础安全能力. 基于零信任理念, 要求每个独立的实体 (网元设备) 具备独立的安全能力, 并确保主体真实和请求有效. 因此, 不仅需要实体具备自身安全防护能力, 还需要其在信任共识设施 (如公共查询库、区块链等) 上登记, 以向第三方证明该能力的配置及启用状态.

(2) 网络/子网边界应采用安全专用设备. 在内部可信度较高的前提下, 按区域进行安全防护一方面可以利用安全专用设备在功能、性能方面的优势; 另一方面区域边界集中防护的安全成本更低, 也便于集中运维管理, 减少运维管理的成本.

(3) 网内安全服务应采用专用设备. 内网安全所需的扫描、监控、基线核查等能力应使用专用设备, 一般使用集中化更利于保持一致性, 利于运维管理.

(4) 安全分析能力应集中化与智能化. 数据驱动型的安全能力, 包括态势感知、安全策略分析与优化、安全编排分析等. 这部分安全能力往往需要大量的关联数据分析, 适合集中化、智能化方式进行.

综上, 归纳 6G 网络内生安全架构中安全能力的建设原则如下:

原则 1: 抵抗内部攻击的必要安全机制 (如认证、安全配置、告警、日志等) 由设备自身实现.

原则 2: 端到端的安全能力应由设备自身实现 (如安全协议).

原则 3: 网络/子网所需的共性安全能力优先由专用设备实现.

原则 4: 安全配置、安全策略应由安全智能中心生成, 并由安全管理中心统一管理.

原则 5: 当一种安全能力可由多类方式执行时, 优先选择成本最低的实现方式.

3.2.2 6G 网络内生安全能力规划

基于 3.2.1 小节的安全能力部署原则分析, 按图 2 中内生安全的架构, 自下而上对各部分的能力规划如下.

(1) 设备安全能力. 保障设备自身基础安全的功能应由设备自身建设, 可有效保障其他安全机制失效时也能维持基本的安全能力. 主要包括如下内容: 自身安全防护能力, 如访问控制、身份认证、安全基线配置、设备入侵检测、软件完整性校验、日志等; 信任可证能力, 如基于可信计算、区块链等方式的可证明安全启动、运行等; 端到端安全保障能力, 如基于数字证书的 TLS, IPSEC 等安全能力; 设备个性化的安全能力, 如黑白名单、服务许可列表等.

(2) 专用安全能力资源池. 该部分通过安全专用设备提供实现共性安全能力, 其目标是保障安全能力高效执行、避免系统中安全能力的重复建设与部署. 主要由 3 类内容组成: 生产网络及边界应部署的专用设备, 主要包括防火墙、IDS、IPS、WAF 等; 内网安全能力资源池, 提供软件服务化 (software as a service, SaaS) 模式的安全服务, 主要包括安全漏洞扫描、安全配置核查、安全状态监测等; 内网安全能力备用资源池, 由核心网为安全资源池预留硬件、软件, 依据安全需求配置并提供安全能力, 接受安全策略控制单元的策略管理、资源编排与调度能力的编排.

(3) 安全策略控制单元. 该设备执行安全智能中心的安全策略下发, 包括网元设备的安全策略、安全专用设备的安全策略. 该单元应是一个部署在生产域边界的设备, 实现管理域与生产域的互通.

(4) 安全智能中心. 安全智能中心是安全协同的大脑, 基于 AI 能力, 与管理中心、资源编排与调度能力联动. 主要实现以下多方面功能: 集中化安全数据的分析, 输出安全态势、威胁情报、安全策略等; 安全配置策略的分析与生成, 并通过安全策略控制单元下发; 安全编排方案的分析与生成, 并与资源编排与调度能力中心联动, 实现安全能力的编排; 与数字孪生网络联动, 实现安全运维的分析与调优; 安全智能中心还作为安全能力与服务对外的输出接口, 实现安全服务能力的整合与输出.

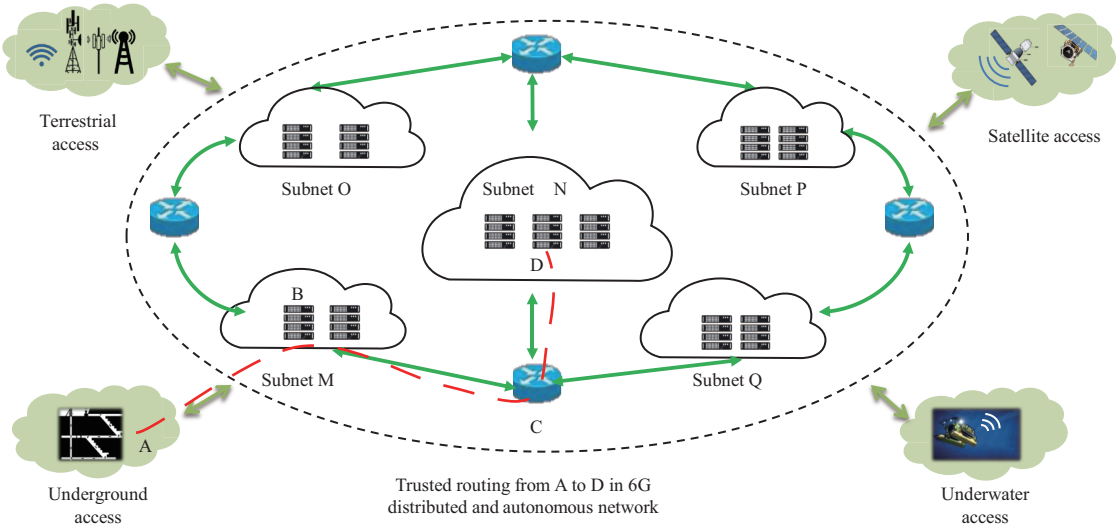

图 3　(网络版彩图) 6G 跨子网端到端可信链路构建示意图

Figure 3　(Color online) Diagram of 6G cross subnet end-to-end trusted link construction

(5) 安全管理中心. 安全管理中心的必要功能包括: 系统管理、审计管理、安全管理、集中管控等 [28] 能力, 并能呈现安全态势等供安全管理员分析与决策.

通过上述 6G 网络内生安全架构和安全能力部署, 可实现如下目标: 在安全管理中心的指导下, 以 6G 网络中已具备的安全能力为基础、配合柔性安全能力资源池、协同智能分析与编排机制, 构建可靠、灵活、弹性、至简的安全防护体系, 并具备对外安全服务能力, 达到主动免疫、信任共识、协同弹性的目标.

4　6G 网络内生安全架构的运行

在 6G 分布式自治网络架构 [3] 场景下, 设定如下 6G 安全应用场景: 地下接入点的垂直行业客户 A 期望建立一个到目标设备 D 的端到端可信链路, 应用场景示意如图 3 所示.

为实现 6G 按需服务的目标, 安全面应按业务需求形成按需的安全服务或策略. 本节基于 6G 网络内生安全架构对该应用场景的实施过程进行推演, 网元设备或系统内部的分析过程不在流程中详细描述.

(1) 参数定义. Dev: 基础资源设备、网元设备 (device). 例如 A 网元表示为 Dev_A, A 为编号或名称.

Net/SubNet: 网络或子网 (network). 例如网络 N 表示为 Net_N, N 为网络编号或名称; 子网 N 表示为 SubNet_N, N 为网络编号或名称.

Rou: 可达访问路径 (routing), 为有序队列. 例如网络 UG 中的设备 A 访问网络 N 中的设备 D, 其中第 i 条可访问路径为

$$\text{Rou\_}i = \{(\text{Net\_UG}, \text{Dev\_A}), (\text{Net\_N}, \text{Dev\_D}), [\text{Dev\_A}, \text{Dev\_B}, \text{Dev\_C}, \text{Dev\_D}]\}.$$

Rou_L: 多个不同的路径形成的路径列表, 格式为

$$\{\text{Rou\_}i, \text{Rou\_}j, \text{Rou\_}k\}.$$

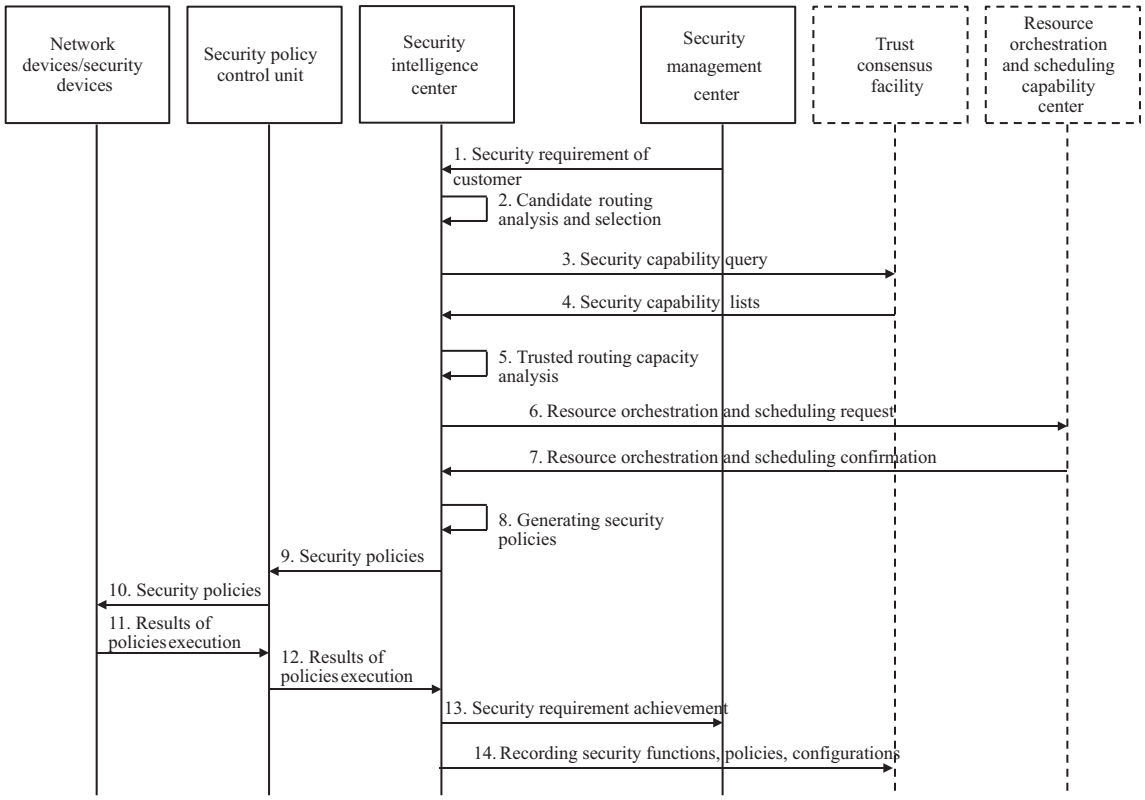

图 4　基于内生安全架构的可信链路构建流程

Figure 4　Procedure of trusted link establishment based on the build-in security architecture

SF: 单个安全能力 (security function). SF_i 表示第 i 个安全能力, 其中 i 为不同安全能力的编号, 如访问控制、认证、授权等.

SF_List: 设备或服务所能提供的安全能力列表, 为一个能力与状态的集合; 格式为 [能力编号 (SF_i), 能力启用状态 (bool), 能力配置参数 (Parameter_j)], 其中 i 为不同安全能力的编号, j 为安全能力配置参数编号, 可包含默认参数 default. 例如 A 设备提供的功能为

$$\text{SF\_List\_Device\_A} = [\text{SF\_1}, 0, \text{Parameter\_1}], [\text{SF\_2}, 0, \text{Parameter\_1}], [\text{SF\_3}, 0, \text{Parameter\_1}].$$

Req: 对网络或设备的安全需求, 格式为列表. 例如针对网元设备 A 的安全需求为

$$\text{Req\_Dev\_A} = \text{SF\_1}, \text{SF\_2}, \text{SF\_3}, \ldots.$$

(2) 端到端可信链路构建运行推演. 基于 6G 网络内生安全架构中的各逻辑功能部件, 联合进行 6G 可信链路构建的业务流程如图 4 所示.

Step 1. 安全管理中心发起 “建立从 A 到 D 的可信连接” 的客户业务需求, 并将安全需求转发到安全智能中心.

Step 2. 安全智能中心分析业务需求, 分析从 A 到 D 的可达路径列表 Rou_L = Rou_1, Rou_2, Rou_3,..., 并进行最优路径选择. 本案例中采用距离优先策略, 选取可达路径, 其中 Net_0 表示 6G 骨干网络本网.

$$\text{Rou\_1} = \{(\text{SubNet\_UG}, \text{Dev\_A}), (\text{SubNet\_M}, \text{Dev\_B}), (\text{Net\_0}, \text{Dev\_C}), (\text{SubNet\_N}, \text{Dev\_D}),$$

$$[\text{Device\_A}, \text{Device\_B}, \text{Device\_C}, \text{Device\_D}]\}.$$

Step 3. 安全智能中心向信任共识设施发起 Rou_1 上设备 A, B, C, D 的安全能力查询.

Step 4. 安全智能中心获得

$$\text{SF\_List\_Device\_A}, \text{SF\_List\_Device\_B}, \text{SF\_List\_Device\_C}, \text{SF\_List\_Device\_D}.$$

设其可信启动的能力定义为 SF_1, 可信度量的能力为 SF_2, 获得如下列表:

$$\begin{aligned}
&\text{SF_List_Device_A} = \{[\text{SF_1}, 1, \{\text{default}\}], [\text{SF_2}, 1, \{\text{default}\}]\},\\
&\text{SF_List_Device_B} = \{[\text{SF_1}, 1, \{\text{default}\}], [\text{SF_2}, 1, \{\text{default}\}], [\text{SF_3}, 1, \{\text{default}\}]\},\\
&\text{SF_List_Device_C} = \{[\text{SF_1}, 1, \{\text{default}\}], [\text{SF_2}, 1, \{\text{default}\}], [\text{SF_3}, 1, \{\text{default}\}]\},\\
&\text{SF_List_Device_D} = \{[\text{SF_1}, 1, \{\text{default}\}], [\text{SF_2}, 1, \{\text{default}\}]\}.
\end{aligned}$$

Step 5. 安全智能中心查询每个 SF_List, 并计算公共能力集合:

$$\{\text{SF\_List\_Device\_A} \cap \text{SF\_List\_Device\_B} \cap \text{SF\_List\_Device\_C} \cap \text{SF\_List\_Device\_D}\}.$$

然后判断上述公共能力集中包含 {[SF_1,1,{default}],[SF_2,1, {default}]}, 从而确认链路设备均具备可信启动与可信度量能力.

Step 6. 安全智能中心确认 Rou_1 具备可信连接建立能力, 向资源编排与调度能力发起订购.

Step 7. 资源编排与调度能力中心确认资源的需求与订购后, 向安全智能中心进行资源确认.

Step 8. 安全智能中心生成安全策略.

Step 9. 安全智能中心将安全策略下发到安全策略控制单元.

Step 10. 安全策略控制单元将安全策略分别下发到设备 A, B, C, D.

Step 11. 设备 A, B, C, D 执行收到的安全策略, 并向安全策略控制单元反馈安全策略执行结果 (假设均为正常执行).

Step 12. 安全策略控制单元向安全智能中心反馈安全策略执行结果.

Step 13. 安全智能中心分析安全策略执行结果, 得出安全服务结果为完成业务需求, 并将结果反馈给安全管理中心.

Step 14. 安全智能中心将满足业务需求的 Rou_1 可信链路业务启用信息, 设备 A, B, C, D 的安全策略, 配置已经生效信息等上报给信任共识设施进行存证.

从上述推演流程可知, 通过内生安全架构各组件的协同, 可以有效利用设备和网络的安全能力, 以自动化的方式提供满足客户安全需求的安全能力, 实现协同弹性安全的目标.

5 6G 网络内生安全后续工作展望

6G 网络内生安全体系理论仍在不断的研究和完善之中, 从技术发展的趋势看, 未来需要重点在以下 4 个方面开展工作.

首先, 依据网络和业务的安全需求演进, 不断完善 6G 网络内生安全架构, 形成顶层技术方案; 并进而设计合理的原则, 对网元自身安全能力、边界专用安全能力、SaaS 安全能力、安全能力资源池的能力等进行定义, 使内生安全架构体系化、可实施化.

其次, 内生安全中涉及到大量的新技术还需要进一步攻关, 包括安全可信、安全可证明、区块链、安全智能等技术.

第三, 基于安全智能能力定义协同机制, 在现有的安全管理、运行的基础上, 定义安全协同的机制, 实现安全能力的充分使用, 实现安全、至简的协同.

第四, 内生的安全能力不仅用于保障 6G 网络的自身安全, 也应将其能力作为 6G 网络的一部分, 提供给 6G 网络的服务对象, 进一步扩展内生安全的外延.

综上所述, 与 6G 网络架构、业务需求演进同步, 6G 网络内生安全架构还将不断演进与细化, 为未来的网络提供按需、极致的安全能力.

参考文献

1 Ping Z, Kai N, Hui T, et al. Technology prospect of 6G mobile communications. J Commun, 2019, 40: 145–152 [张平, 牛凯, 田辉, 等. 6G 移动通信技术展望. 通信学报, 2019, 40: 145–152]

2 China Mobile Research Institute. 2030+ White Paper of Vision and Requirements. 2nd ed. 2019 [中国移动通信研究院. 2020+ 愿景与需求白皮书 (第二版). 2019] http://cmri.chinamobile.com/insight/technology/6222.html

3 China Mobile Research Institute. 2030+ Network Architecture Outlook. 2020 [中国移动通信研究院. 2030+ 网络架构展望. 2020] http://cmri.chinamobile.com/insight/technology/6225.html

4 Shaik A, Borgaonkar R, Park S, et al. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 2019. 221–231

5 Hussain S R, Echeverria M, Karim I, et al. 5GReasoner: a property-directed security and privacy analysis framework for 5G cellular network protocol. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security, 2019. 669–684

6 Rupprecht D, Kohls K, Holz T, et al. IMP4GT: impersonation attacks in 4G networks. In: Proceedings of Network and Distributed System Security Symposium (NDSS), 2020

7 Hussain S R, Echeverria M, Chowdhury O, et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. In: Proceedings of Network and Distributed Systems Security (NDSS) Symposium, 2019

8 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

9 Cremers C, Dehnel-Wild M. Component-based formal analysis of 5G-AKA: channel assumptions and session confusion. In: Proceedings of Network and Distributed Systems Security (NDSS) Symposium, 2019

10 Wang S, Sun T, Yang H W, et al. 6G network: towards a distributed and autonomous system. In: Proceedings of the 2nd 6G Wireless Summit (6G SUMMIT), 2020

11 Stafford V A. Zero trust architecture. NIST Special Publication, 2020, 800: 207

12 Samaniego M, Deters R. Zero-trust hierarchical management in IoT. In: Proceedings of IEEE International Congress on Internet of Things (ICIOT), 2018. 88–95

13 QiAnXin Strategy Consulting and Planing Department & QiAnXin Industry Research Center. Built-in Security: New Generation of Network Security Frame System and Practice. Beijing: People's Posts and Telecom Press, 2021 [奇安信战略咨询规划部 &奇安信行业安全研究中心. 内生安全: 新一代网络安全框架体系与实践. 北京: 人民邮电出版社, 2021]

14 Song K, Liu Q R, Wei S, et al. Endogenous security architecture of Ethernet switch based on mimic defense. J Commun, 2020, 41: 18–26 [宋克, 刘勤让, 魏帅, 等. 基于拟态防御的以太网交换机内生安全体系结构. 通信学报, 2020, 41: 18–26]

15 You W, Li Y L, Bai Y, et al. Research on endogenous safety and security technology of 5G core network. Radiocommun Technol, 2020, 46: 385–390 [游伟, 李英乐, 柏溢, 等. 5G 核心网内生安全技术研究. 无线电通信技术, 2020, 46: 385–390]

16 Liu Y, Peng M G. 6G endogenous security: architecture and key technologies. Telecommun Sci, 2020, 36: 11–20 [刘杨, 彭木根. 6G 内生安全: 体系结构与关键技术. 电信科学, 2020, 36: 11–20]

17 Jiang W Y, Liu B Y, Wang C. Network architecture with intrinsic security. Telecommun Sci, 2019, 35: 20–28 [江伟玉, 刘冰洋, 王闯. 内生安全网络架构. 电信科学, 2019, 35: 20–28]

18 Jin L, Lou Y M, Sun X L, et al. Concept and vision of 6G wireless endogenous safety and security. Sci Sin Inform, 2021. doi: 10.1360/SSI-2021-0095 [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, 2021. doi: 10.1360/SSI-2021-0095]

19 Chen Z, Meng H W, Guan Z. Research on intrinsic security in future internet architecture. J Cyber Secur, 2016, 1: 36–45 [陈钟, 孟宏伟, 关志. 未来互联网体系结构中的内生安全研究. 信息安全学报, 2016, 1: 36–45]

20 3GPP. Security architecture and procedures for 5G system. TS 33.501V16.3.0. 2020. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

21 Yang Z Q, Su L, Qi M P, et al. Overview and prospect of 5G security. Telecommun Sci, 2020, 36: 5–23 [杨志强, 粟栗, 齐旻鹏, 等. 5G 安全技术与标准. 电信科学, 2020, 36: 5–23]

22 3GPP. Catalogue of general security assurance requirements. TS 33.117. 2019. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928

23 GSMA. FS.13 — NESAS overview. 2019. https://www.gsma.com/security/resources/fs-13-network-equipment-security -assurance-scheme-overview/

24 GSMA. FS.14 — NESAS security test laboratory accreditation. 2019. https://www.gsma.com/security/resources/fs-14-network-equipment-security-assurance-scheme-security-test-laboratory-accreditation/

25 GSMA. FS.15 — NESAS development and lifecycle accreditation methodology. 2019. https://www.gsma.com/security/resources/fs-15-network-equipment-security-assurance-scheme-vendor-development-and-product-lifecycle-requirements-and-accreditation-process/

26 GSMA. FS.16 — NESAS development and lifecycle security requirements. 2019. https://www.gsma.com/security/resources/fs-16-network-equipment-security-assurance-scheme-development-and-lifecycle-security-requirements/

27 3GPP. Network domain security (NDS); IP network layer security. TS33.210. 2015. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279

28 State Administration for Market Requlation. Information security technology — baseline for classified protection of cybersecurity. GBT22239-2019. 2019 [国家市场监督管理总局. 信息安全技术网络安全等级保护基本要求. GBT22239-2019. 2019] http://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=BAFB47E8874764186BDB7865E8344DAF

Built-in security framework research for 6G network

Li SU*, Xiaojun ZHUANG*, Haitao DU, Peng RAN, Xiaoting HUANG & Penglin YANG

China Mobile Research Institute, Beijing 100053*, China*
* Corresponding author. E-mail: suli@chinamobile.com, zhuangxiaojun@chinamobile.com

Abstract 6G will enable seamless coverage across land, sea, sky, and space, and provide users with on-demand services. 6G requires high security and its security capabilities are expected to serve as an independent logical plane under the 6G network architecture to provide services and guarantee for 6G networks and applications. This article analyzes and summarizes the three aspects of 6G security evolution requirements. First, the distributed autonomy of network architecture increases the exposure surface of network equipment and functions, and puts forward the requirements for high security of network elements and subnets themselves. Second, the cloud and virtualization technologies increase the risk of internal attacks, and require security protection mechanisms within network elements and the internal network based on the concept of zero trust. Third, providing on-demand services to customers requires intelligent collaboration mechanisms within the network, as well as an elastic and programmable security capability pool. Based on the above requirements and the development of security technologies, this paper proposes a 6G security construction idea with the built-in security framework as the basis, which includes security capability layer, security policy controller, security intelligence center and security management center, collaborating with the trusted infrastructure, orchestration capabilities and artificial intelligence abilities. The framework is built upon the security capability inside the network, coordinated with the trust consensus and the intelligent collaboration, which forms a security architecture and related operating mechanisms with active immunity, trustworthiness, and collaborative elasticity. By means of the practical case of building a trust link, the framework is proved to be able to provide flexible and on-demand security services for 6G networks and applications.

Keywords 6G, build-in security, operating mechanism, network security, trust