5G 安全: 通信与计算融合演进中的需求分析与架构设计

李宏佳, 王利明, 徐 震, 杨 畅

中国科学院信息工程研究所 信息安全国家重点实验室 北京 中国 100093

摘要 5G 是未来网络空间的核心基础设施, 因而 5G 安全是网络空间安全的重要组成部分。5G 安全技术应打破以往移动通信系统成型后“打补丁式”的升级演进模式, 与 5G 移动通信技术同步演进, 实现系统安全内生与安全威胁“标本兼治”的目标。为了“有的放矢”的推动安全技术同步演进, 应首先解决两个基本问题: 5G 安全需求是什么和 5G 安全体系架构是什么。针对这两个问题, 本文首先从业务、网络、无线接入、用户与终端、系统五个视角梳理了 5G 通信与计算融合演进的技术特点, 并基于这些特点系统的分析了 5G 安全需求; 然后, 面向 5G 安全需求, 设计了 5G 安全总体架构; 最后, 总结归纳出了 5G 安全技术的三个发展趋势, 即, “面向服务的安全”“安全虚拟化”与“增强用户隐私与数据保护”。本文希望为 5G 安全技术的同步演进提供有益的参考。

关键词 5G; 安全; 融合演进; 总体安全架构; 安全需求
中图法分类号 TN91 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2018.09.01

5G Security: Requirements Analysis and Architecture Design Towards CT and IT Convergent Evolution

LI Hongjia, WANG Liming, XU Zhen, YANG Chang

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract The fifth generation (5G) mobile communication system is the core infrastructure of future cyberspace; this makes the 5G security indispensable to the cyberspace security. In order to amalgamate the security with 5G standardization, security technology should get rid of the patching evolution mode happened in 3G and 4G, where it is developed as patches to the already found security threats. Thus, it is vital to clarify the guidelines of how 5G security technology synchronously evolves with the 5G communication technology. To this end, we delve into two fundamental problems: what are 5G security requirements and how should the corresponding security architecture be designed? Correspondingly, we first dissect the convergent evolution features and systematically analyze security requirements from five perspectives, namely, the user/terminal, the network, the radio access, the application and service, and the system. Then, following the requirements, we design a new 5G security architecture. Finally, three development trends of the 5G security technology, namely, service-oriented security, security virtualization and enhanced protection for privacy and data, are highlighted to give a glimpse of the evolution roadmap of 5G security techniques.

Key words 5G; security; convergent evolution; security architecture; security requirements

1 引言

在业界共同努力和推动下, 5G 的愿景、需求与技术发展路线已基本明确。国际电信联盟(ITU)制定了 5G 演进时间表, 将于 2020 年完成 5G 标准。根据 ITU 时间表, 国际标准化组织第三代合作伙伴计划(3GPP)将在 2018 年与 2020 年分别完成 5G 标准版本 15 (R15)与版本 16 (R16)。为了在 5G 技术标准中占得一席之地, 众多国家和行业组织早已积极投入到 5G 技术研发工作中, 例如, 以欧洲企业为主体的行业组织正通过基于 Horizon 2020 计划[1]的 5G-PPP[2]和 METIS 2020[3]项目推进 5G 技术研发。为了实现引领 5G 发展的目标, 我国于 2013 年成立了 IMT-2020 (5G)推进组, 该推进组聚集了国内移动通信领域产、学、研、

通讯作者: 王利明, 博士, 副研究员, Email: wangliming@iie.ac.cn。
本课题得到国家自然科学基金(No. 61302108)资助。
收稿日期: 2017-01-05; 修改日期: 2017-04-26; 定稿日期: 2018-08-20

用主要力量。在推进组成员的共同努力下, 我国目前已完成 5G 通信与网络技术第一阶段试验, 并制定了第二阶段试验规范。同时, 针对 5G 总体技术规划, 我国未来移动通信论坛(简称 FuTURE 论坛)推出了前沿技术主题白皮书和专题研究报告, 这些成果不仅成为国家有关标准和项目规划工作的重要依据, 也为政府相关主管部门提供决策支撑和技术参考[4]。

5G 移动通信系统从终端设备、无线接入到核心网将不再只是通信技术为主导的演进, 而将是通信技术(CT)与计算技术或信息技术(IT)融合的演进。另外, 从业务应用角度看, 5G 移动通信系统将支持增强型移动互联网应用、超低时延应用以及大规模机器通信等差异化的应用服务[5]。为了充分利用网络、频谱资源并满足差异化业务的服务质量要求, 5G 网络将采用软件化的开放网络架构[6-7], 并引入新空口[8-11]、新无线组网[12-13]、移动边缘计算(MEC)[14-17]等技术。

同时, 安全技术作为 5G 移动通信系统可靠运行的基础, 是不可或缺的。与以往不同的是, 5G 安全技术将与移动通信技术同步演进。3GPP 等国际标准化组织明确提出了打破以往“打补丁式”的安全技术演进模式, 将在通信与网络技术标准化过程中同步安全技术标准化[5], 例如, 3GPP SA1、SA2 和 SA3 工作组已在技术报告 TR 22.891[28]、TR 23.799[19]和 TR 33.899[18]中给出了 5G 安全技术的初步建议; 华为、大唐、爱立信、贝尔实验室等企业也对 5G 安全技术展开了同步研究[18-27]。

由于明确的安全需求能够为安全架构设计与安全技术发展提供导向性指引, 因此, 5G 安全需求分析在已有研究中得到了重视。已公开的成果对 5G 安全需求与潜在安全技术已达成一致的结论概括如下:

1) 为了满足 5G 移动通信系统的安全需求, 5G 安全机制与技术将对现有移动通信系统的安全机制和技术升级, 同时引入新的安全机制与技术;

2) 基于软件化技术的网络架构成为 5G 移动通信系统发展趋势, 同时, 这也将带来软件定义网络(SDN)、网络功能虚拟化(NFV)等方面的安全需求;

3) 5G 需要提供更加灵活的安全性配置以满足多样化的业务和应用场景需求, 同时, 需要提供严密的用户隐私保护。

然而, 现有安全需求分析通常从通信安全或信息安全角度单独展开, 这种“竖井思维”难以系统化的总结 5G 融合演进中的安全需求。因此, 5G 安全需要分析需要打破“竖井思维”模式, 采用通信技术与信息技术, 以及通信安全技术与信息安全技术交叉融合的思维模式。

另外, “总体安全架构”是对系统安全总体模型, 以及功能模块间、功能模块与安全模块、安全模块间安全相互关系的定义, 科学、合理的安全体系架构可以有效的指导整个系统具体安全机制设计[18]。5G 总体安全架构是 5G 安全技术研发与标准化的重要基础[29], 但是, 目前已公开研究成果还未对其进行系统化的研究与设计。

根据上述分析, 为了真正实现 5G 安全同步演进的目标, 应该首先回答以下两个基本问题。

问题一: 5G CT 与 IT 融合的表现形式是什么, 相应的 5G 安全需求是什么?

问题二: 如何设计满足 5G 安全需求的总体安全架构?

针对问题一, 本文首先从用户终端、无线接入、网络、业务应用与系统五个视角梳理了 5G 融合演进的特点; 然后, 从这五个视角一一对应的分析了 5G 移动通信系统的安全需求, 这为安全体系架构设计提供了依据。

针对问题二, 本文在对比分析 3GPP UMTS (3G) 和 4G LTE 安全架构的基础上, 设计了满足 5G 安全需求的总体安全架构, 并讨论了所设计总体安全架构针对各安全需求的具体实施方式。

基于上述研究讨论, 本文最后总结归纳出来了三大 5G 安全技术潜在发展趋势: “面向服务的安全”“安全虚拟化”与“增强用户隐私与数据保护”。

下面将首先介绍 5G 融合演进中的安全需求。

2 5G 融合演进中的安全需求

如图 1 所示, 本文采用业务应用、网络、用户与终端、无线接入、系统五个分析视角对 5G 融合演进特点、5G 安全需求与三个 5G 安全技术潜在发展趋势进行全面分析。下面将从这五个分析视角逐一展开分析。

2.1 业务应用演进特点与安全需求分析

2.1.1 业务应用演进特点

传统移动通信系统主要承载人与人、人与服务提供方之间的数据与信息交互业务(如语音通话、短信、移动应用、移动多媒体等)。在 4G 时代, 移动应用已渗透到人们生活的方方面面, 而 5G 业务应用将在这基础上, 进一步为人与物、物与物提供通信服务, 从而满足更加多样化的行业应用需求[28], 渗透到交通、医疗、工业等多元化的行业和领域, 同时, 5G 业务应用的种类和数量也将出现井喷式的增长。在新出现的业务应用中将包含大量具有更高安全要求的

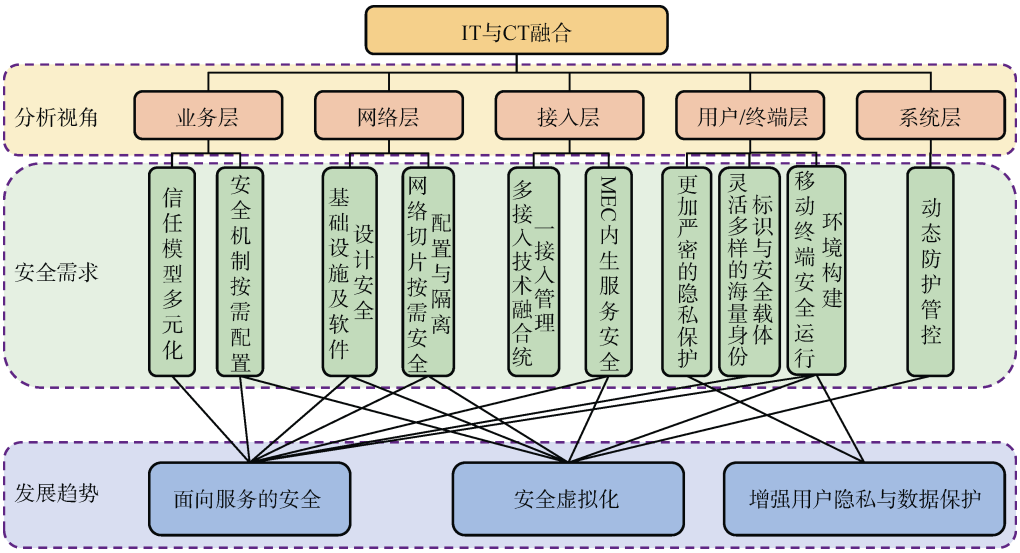

图 1　融合演进分析视角、安全需求与安全技术发展趋势

Figure 1　Viewpoints of convergent evolution analysis, security requirements and the evolution roadmap of 5G security techniques

业务, 如远程医疗、智能交通、智能制造等。根据 ITU 白皮书, 5G 移动通信系统中的新型业务可以分为以下三大类[30]。

1) 增强型移动带宽业务

主要包括超高清晰度视频、实时可视通信以及全息多媒体交互等业务。这些业务对于网络带宽要求极高, 例如, 4K 视频对带宽的需求为 22.5 Mbps~75 Mbps, 8K 视频对带宽的要求为 90 Mbps~300 Mbps[31]。

2) 大规模物联网业务

5G 移动通信系统将全面支持物联网业务应用, 这些应用扩展了移动通信系统的服务对象与范围, 例如, 以感知和数据采集为目的的环境监测、智慧农业、智能家居等业务应用, 它们普遍具有部署节点数量多、设备成本低[30]的特点。

3) 超低时延业务应用

除了提供面向物联网领域的大规模业务应用, 5G 还需要提供精细化的实时(或超低时延)业务应用, 以满足这些业务对于通信与计算的苛刻要求。例如, 针对远程医疗业务应用, 用户通过现场采集的医学影像数据, 进行远程诊断、会诊, 甚至借助虚拟现实、增强现实等技术实现远程机器人手术[30]。

2.1.2　业务应用安全需求分析

传统移动通信系统中的业务应用所面临的安全问题并没有得到有效的解决, 根本原因之一在于用户、网络、业务间的信任模型没有形成闭环。随着 5G 移动通信系统中业务种类与数量的进一步激增, 为了保证 5G 业务应用安全, 必须完善移动业务应用的信任模型; 另外, 为了满足多样化 5G 业务应用的差异化安全需求, 需要支持灵活的安全机制按需配置。

1) 信任模型多元化

如图 2(a)所示, 传统移动通信系统中用户与网络、用户与业务构成的二元信任模型可表示为

$$\mathcal{M}=\{\mathcal{V},\mathcal{E}\}, \tag{1}$$

其中, $\mathcal{V}=\{\mathcal{N},\mathcal{U},\mathcal{S}\}$ 表示信任模型中的元素; $\mathcal{N}$、$\mathcal{U}$ 和 $\mathcal{S}$ 分别表示网络、用户和业务。$\mathcal{E}=\left\{\overrightarrow{\mathcal{UN}},\overrightarrow{\mathcal{U}(\mathcal{N})\mathcal{S}}\right\}$ 表示元素间的信任关系; $\overrightarrow{\mathcal{UN}}$ 表示用户与网络间的信任关系, $\overrightarrow{\mathcal{U}(\mathcal{N})\mathcal{S}}$ 表示, 网络作为管道承载用户与业务间的认证。

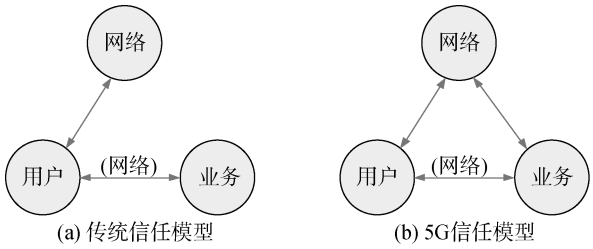

图 2　信任模型的变化

Figure 2　Evolution of the trust model

如图 2(b)所示, 5G 中的信任模型可表示为

$$\mathcal{M}'=\{\mathcal{V},\mathcal{E}'\}, \tag{2}$$

其中, $\mathcal{E}'=\left\{\overrightarrow{\mathcal{UN}},\overrightarrow{\mathcal{US}},\overrightarrow{\mathcal{NS}}\right\}$。

区别于传统的二元信任模型, 5G 网络还需要建立网络与业务应用间新的信任关系; 此外, 5G 网络中用户与业务间的信任关系也有了新的内涵。具体

而言:

a) 网络与业务间新的信任关系

首先, 并非所有移动应用与用户间的认证都能够保障足够可靠的信任关系, 而在网络与业务间进一步引入认证过程可以大大增强信任关系的可靠性。其次, 对于某些物联网行业应用(如, 烟感监控报警), 为了简化用户的业务认证流程, 可建立网络与业务间的信任关系, 从而在网络对用户完成认证后业务不再需要对用户进行进一步认证。

另外, 大量业务接入到 5G 网络增加了网络中信息真实性和有效性辨识的难度, 为了降低恶意软件、钓鱼网站等对用户的威胁, 需要构建网络与业务间的信任关系, 从而保证第三方业务提供商的可信性。

b) 用户与业务间信任关系的新内涵

针对多样化的业务模式, 用户与业务间将存在 3 种认证模式[18, 25]:

• 网络统一认证: 业务提供方将业务认证委托给网络运营商, 通过运营商一次认证达到网络认证和业务认证的双重目的。

• 业务统一认证: 运营商信任业务对用户的认证结果, 经一次业务认证, 即可为用户提供网络服务。

• 网络和业务分别认证: 运营商负责用户的入网认证, 应用对用户进行业务认证。

2) 安全机制按需配置

不同的业务应用对5G移动通信系统的安全性要求不同, 例如, 对于普通的监测应用, 其采用的物联网监测节点在通信、计算、存储、能量等资源方面受到较大限制, 需要采用更为轻量、高效的安全防护机制; 而对于远程医疗、自动驾驶等关乎生命、财产的应用, 显然应该采用更高安全等级的防护机制。因此, 5G 移动通信系统需要根据差异化业务应用的安全性要求, 提供按需配置的安全机制。

2.2 5G 网络演进特点与安全需求分析

2.2.1 网络演进特点

在传统移动通信系统中, 网元通常采用专用设备, 其软件功能固化于硬件平台之上, 软、硬件紧密耦合。由于网络设备种类繁多且设备间相互关系复杂, 当网络升级和扩容时, 运营商不仅需要对网络不同部分的不同设备分别升级改造, 还需要对系统进行整体配置更新(例如, 对不同厂家的设备及其之间接口进行配置), 导致部署周期长、成本高、复杂度大。此外, 传统移动通信网络缺乏开放性接口, 服务提供方无法有效获取网络的状态信息来优化业务服务, 网络也无法根据业务的服务质量(QoS)需求灵活配置网络资源。

随着 SDN、NFV 等技术的引入, 5G 网络的发展呈现出虚拟化、软件化、开放化等特点。具体而言, 5G 网络将广泛采用通用基础设施平台, 各网元将通过虚拟化的方式分解为一系列运行在通用平台上的虚拟网络功能(VNF), 从而实现了通用硬件资源的高效共享、以及网元功能与物理实体的分离解耦。同时, 网络切片技术[26]将网络物理资源虚拟化为相互独立的网络切片, 并能够根据不同的业务应用和场景需求, 灵活的配置网络资源。正是由于这些技术的引入, 5G 网络可以方便的提供开放性服务, 如, 向第三方服务提供商提供网元负载、网络与资源状态等信息, 并根据业务的服务质量要求对网络资源进行灵活配置。

2.2.2 网络安全需求分析

针对 5G 网络的演进特点, 我们总结了除了其对应的安全需求, 主要包括: 基础设施安全保障、软件设计安全保障、网络切片按需安全配置与相互隔离。具体而言:

1) 基础设施安全保障

传统移动通信系统中的网元设备在物理上相互独立, 而 5G 网络中虚拟网络功能将集中运行在云化的基础设施平台上, 不同的网元可能共享相同的物理基础设备资源。一旦物理基础设施本身漏洞被利用, 所影响的网络范围以及损失都将远超以往。因此, 保障基础设施安全对 5G 网络至关重要。

2) 软件设计安全保障

5G 网络中的网元功能和网络切片都将通过软件和虚拟化的方式实现。因此, 网元功能和网络切片的安全与软件本身设计的安全性息息相关[30]。另外, 5G 网络的开放性特点需要其对外提供安全的开放应用程序接口(API), 并确保第三方应用对开放 API 的合法、合理调用。

3) 网络切片按需安全配置与隔离

网络切片将构成端到端的逻辑网络, 按照需求灵活的提供一种或多种网络服务。5G 网络切片分配中应能够根据不同用户和业务的安全需求配置所需的安全资源。

为了防止某一网络切片内的资源被其他类型网络切片非法访问, 需要提供不同切片实例之间的隔离机制, 例如, 对于远程医疗服务所在的切片资源, 不应能被任何智能汽车从其所连接的车联网切片所直接访问到; 同一网络切片不同业务资源间以及不同的 VNF 之间也存在隔离的需求, 例如, 不同的企业在使用相同业务类型的切片网络时, 任一企业的内部服务资源不应能被其他企业的网络切片节点随意访问。

2.3 5G 无线接入网演进特点与安全需求分析

2.3.1 无线接入网演进特点

5G 移动通信系统将引入新空口(NR)技术, 如, 大规模天线、新型多址、新型多载波等技术[23, 26], 以大幅提升频谱效率与网络容量。同时, 5G 接入网将融合多种无线接入模式, 并采用超密集组网技术以满足海量终端设备通过 3GPP 接入方式接入或通过 WiFi、卫星等非 3GPP 方式接入。另外, 为了满足超低时延应用的本地化快速处理, 降低回传网络传输压力与扩容成本, 移动边缘计算[32]成为 5G 无线接入网络的关键技术之一。

1) 多接入技术融合

5G 移动通信系统将同时支持新型无线接入技术和现有无线接入技术, 以满足用户对不同接入方式的需求。支持的现有无线接入技术包括 2G、3G、4G、WiFi 等; 支持的新型新空口(NR)技术中, 除了毫米波、大规模天线等新型技术, 还将支持卫星移动通信和终端间直接通信(包括机器到机器通信(M2M)与设备到设备(D2D)通信等[33])。

2) 超密集组网

自 1974 年贝尔实验室提出蜂窝概念, 密集组网技术为移动通信网络带来了 1600 倍容量的增长[34]。为了进一步百倍量级的提高网络容量与频谱空间利用率, 超密集组网已成为应对未来 5G 移动通信系统的主流组网技术。根据文献[35]预测, 在未来无线网络宏基站覆盖的区域中, 各种无线接入技术的小功率基站的部署密度将达到现有站点密度的 10 倍以上。

3) 移动边缘计算

车联网、虚拟现实等时延敏感新应用的兴起[30], 以及回传网络与核心网络的流量压力, 促使 5G 接入网络引入移动边缘计算技术(MEC)。MEC 在无线接入网络侧使用虚拟化的方式引入计算、存储等功能。通过将业务平台下沉到 5G 移动通信系统边缘的方式, MEC 能够使移动用户在更近的位置获取业务服务。MEC 在提升用户服务体验的同时, 也为移动网络运营商带来新的商业模式。

2.3.2 无线接入网安全需求分析

针对上述 5G 无线接入网演进的特点, 5G 无线接入网新的安全需求可总结为: 多接入技术融合统一接入管理与 MEC 内生服务安全。

1) 多接入技术融合统一接入管理

针对多接入技术异构融合的特点, 在 5G 移动通信网络中需要构建统一的接入安全管理机制(包含用户认证管理、统一授权管理等), 能够在不同接入技术、不同局部网络架构的接入网之上建立一个安全的运营网络。此外, 5G 多接入技术融合基础上的超密集组网将导致移动终端更频繁的在不同接入方式间发生切换。为保证服务连续性, 同样需要统一接入认证机制提供切换快速切换服务。

2) MEC 内生服务安全

移动边缘计算在无线接入网为移动用户提供低时延、高质量的服务的同时, 也拉近了攻击者与移动服务系统距离[36]。而由于计算与安全防护等能力受限, MEC 对攻击的抵御能力相对较弱。攻击者对 MEC 的攻击将直接影响接入网的安全。例如, 攻击者可直接在接入网对 MEC 系统发起 DoS/DDoS 攻击, 在使 MEC 系统无法提供服务的同时也占用了大量无线网络资源, 这将进一步影响接入网对其它用户的服务。目前 MEC 安全防护仍然采用简化的传统 IDC 安全防护手段, 难以适应 5G 中 CT 与 IT 融合的特点, 因此, 需要针对这一特点提供 MEC 内生服务安全。

2.4 5G 用户与终端演进特点和安全需求分析

2.4.1 用户与终端演进特点

5G 移动通信系统中用户与终端的演进特点主要表现为以下几个方面。

1) 终端多元化与海量化

5G 将与医疗、交通、制造、环保、建筑等行业深度融合, 实现真正的“万物互联”。随之而来是终端形式更加多元化。这些终端不仅包括高智能、宽带智能终端, 也包含大量低智能、窄带终端。同时, 终端数量将呈现指数倍数增长, 根据预测, 2021 年全球移动终端数量将超过 280 亿[22]。

2) 用户感官外延与服务个性化

万物互联使得物理世界与信息世界深度融合。这种深度融合在用户侧得到了最直接的体现: 一方面, 用户可交互的终端形式从智能终端为主扩展为包含智能终端和各种物联网设备, 用户可以随时随地的通过 5G 网络获取所需的信息, 感官能力极大扩展; 另一方面, 各种终端设备可以全方位感知并收集用户信息, 为“以人为本”的个性化服务提供基础。例如, 智能家居控制器通过实时感知用户的行为习惯自适应的调整智能空调、智能灯具等家用电器的工作模式; 远程医疗终端设备通过实时传递用户的身体状态信息以提供准确、及时的诊断; 智能交通传感器通过感知用户的位置信息以提供合理的路线规划与及时的危险规避提醒。

2.4.2 用户与终端安全需求

根据上述分析, 用户与终端安全需求主要包括以下几个方面。

1) 更加严密的用户隐私保护

用户隐私信息涉及用户标识、移动模式、位置信息、数据使用模式, 3GPP 在多个技术报告和技术规范[18-19, 28, 38-40]中均涉及隐私保护技术。3GPP 在技术报告 TR33.899[18]指出, 用户隐私保护将是 5G 移动通信系统中安全技术主要难题之一。

为保证兼容性, 在 5G 移动通信系统中, 用户身份与位置相关标识等涉及用户隐私的信息将极大程度上沿用 4G LTE 相关标准中的设定。根据已有研究, 攻击者可通过多种手段获取这些用户隐私信息。图 3 总结了 4G LTE 网络中用户隐私信息[18]易被暴露的环节。其中, 国际移动用户识别码(IMSI)和移动用户国际综合业务数字网识别码(MSISDN)唯一标识了用户的身份信息; 全球唯一临时终端身份(GUTI)可被用于识别用户的位置[37]。

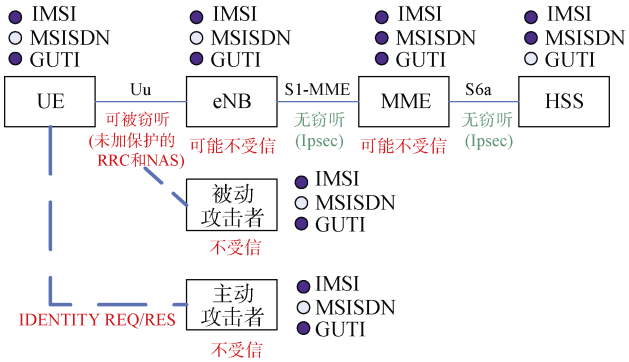

图 3 LTE 用户身份信息潜在泄露位置

Figure 3 Potential leakage points for users' identity information in LTE networks

另外, 在用户感官外延与服务个性化发展的同时, 更多的用户隐私信息将可能通过直接或间接的方式泄露, 例如, 攻击者可通过监听用户智能家居节点信息, 从而分析得到用户的生活习惯、健康等隐私信息。

因此, 在 5G 移动通信系统中, 需要更加严密的用户隐私保护机制, 严格控制用户隐私数据在其获取、传输、存储、处理的每个环节的可见性和安全性。

2) 灵活多样的海量身份标识及其载体

5G 移动通信系统应当能够针对不同的终端类别、应用需求和身份识别手段(如, 基于生物特征、网络行为、地理轨迹等的身份识别技术)提供多安全等级、多类别的身份标识, 并提供标准化的海量身份管理框架和接口。同时, 针对不同的终端, 将需要提供灵活多样的身份标识安全载体。例如, 对于体积小、能量受限的终端, 其无法支持传统用户身份模块(SIM)的方式, 需要将 SIM 信息以软件的形式配置到终端可信存储空间中。此外, 5G 网络还应为运营商远程配置海量终端身份提供支持, 以应对终端数量爆发式增长。

3) 移动终端安全运行环境构建

5G 网络相对于传统 3G/4G 网络更加开放和应用更加丰富的特性, 使得终端更易受到各种攻击, 例如, 木马植入、高级持续性威胁(APT)攻击、内核级攻击等, 这给终端(特别是具有高安全需求或特定安全需求的终端)的运行环境安全带来了巨大的挑战。因此, 需要从 5G 终端本身出发, 综合核心芯片、移动操作系统、可信计算等技术, 构建高安全运行环境。

2.5 5G 系统演进特点和安全需求分析

2.5.1 系统演进特点

NFV、SDN、网络切片等 IT 技术的引入, 在为 5G 移动通信系统注入活力的同时, 也使 5G 移动通信系统变得更加复杂。要保证这种复杂系统设计绝对无漏洞几乎是不可能的, 这给 5G 移动通信系统安全带来了巨大的挑战。同时, 随着 5G 移动通信系统与诸多垂直行业的深度融合, 5G 网络规模急剧扩大, 这大大增加了 5G 移动通信系统受攻击面。此外, 目前的安全理论与技术难以有效的证明并保证所安全体系的绝对安全性, 因此, 安全性通常为概率指标。

2.5.2 系统安全需求分析

由于传统移动通信系统所采用的安全防护手段通常是基于先验知识的静态防护,并且与物理设备紧耦合,因此安全防护手段通常比较单一并且相对固定。随着攻击手段的不断发展与攻击设备性能的不断提升, 传统移动通信系统安全的相对性和暂态性等缺陷逐渐凸显。因此, 传统的静态防护技术难以真正有效的应对 5G 移动通信系统将面临的严峻的攻防态势。

因此, 需要在 5G 移动通信系统中引入动态防护机制。动态防护机制能够主动检测网络的易受攻击点和安全漏洞, 并主动识别异常行为; 向系统中尽可能引入更多的可变因素, 从多种防护策略中动态选择相应的安全防护策略以抵御针对特定安全防护策略的攻击; 同时能够根据所下发的动态安全防护策略实现动态预警、实时响应与处置, 以掌握 5G 移动通信系统安全的主动权。

动态防护机制实施中应结合 5G 移动通信系统的特点, 与网络功能虚拟化相结合: 能够对虚拟化的网络功能进行实时监控; 能够基于通用基础设施平台使用虚拟化的方法实现自定义的动态防护功能, 支持动态升级和扩展。考虑到 5G 移动通信系统的规模以及所提供服务的多元化, 所采用的动态防护机

制应支持移动安全大数据的异常检测与分析。此外, 所采用的动态防护机制中的异常检测与策略生成应能够支持智能学习, 以不断适应系统的发展和攻击方式的变化。

3 5G 安全架构设计

本节针对 5G 移动通信系统的需求, 在 3GPP UMTS(3G) [41]和 4G LTE[42]安全架构的基础上, 提出 5G 总体安全架构, 如图 4 所示。所设计的安全架构横向对用户面安全和控制面安全进行了划分。同时, 针对5G移动通信系统架构与网络功能的虚拟化与重组的特点, 在所设计的安全架构中引入了核心网切片及 VNF 安全、开放接口安全。此外, 针对系统层面的安全需求, 在所设计的安全架构中引入了“安全管控云”(具体含义请见 4.5 节)。具体而言:

1) 根据 5G 移动通信系统架构控制面与用户面进一步分离的思想, 将安全架构划分为用户面安全和控制面安全两个部分, 细化各自的安全问题。

2) 支持传统的 AS 与 NAS 控制面安全与 3GPP 接入用户面安全, 并支持受信与非受信非 3GPP 接入用户面安全。

3) 在控制面安全中, 进一步引入开放服务安全, 确保开放服务的合法与合理使用。

4) 引入网络切片安全和虚拟化网络功能(VNF)安全机制, 用于保证切片与 VNF 的安全运行, 同时保证各切片间、各 VNF 间的安全交互。

5) 引入“安全管控云”, 用于对 5G 移动通信系统进行实时监测与防护, 利用智能学习与大数据技术辨识、发现系统漏洞与异常行为, 并支持动态安全防护策略生成、更新与下发。

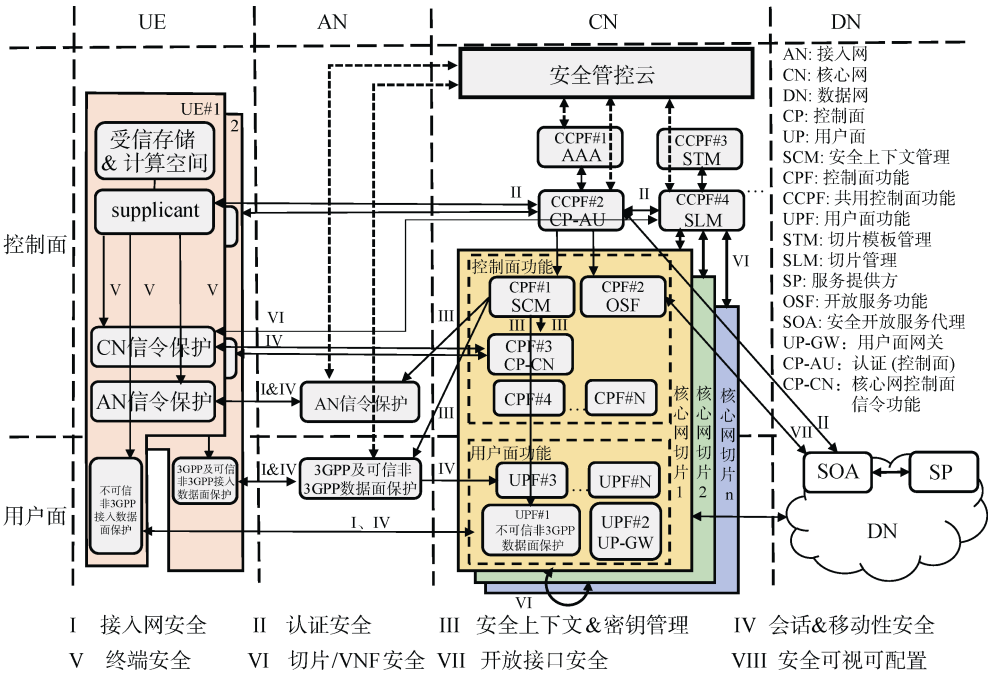

图 4 5G 总体安全架构设计

Figure 4 An illustration of 5G security architecture

借鉴 4G LTE 和 UMTS (3G)安全技术集合的设计, 如图4所示, 我们针对5G架构的特点, 总结了新的安全技术集合。具体安全技术集合单独或通过组合可用于满足本文五个视角总结的安全需求, 限于篇幅, 这里不对各个安全技术集合的具体实现方式进行讨论。

(I) **接入安全**: 保证终端与接入网间进行安全的数据和信令交互的安全技术集合;

(II) **认证**: 保证终端及业务提供方与网络间进行安全认证的技术集合;

(III) **安全上下文及密钥管理安全**: 保证用户、接入网、核心网安全上下文的安全生成、下发、保护等管理过程的安全技术集合;

(IV) **会话及移动性管理**: 保证终端的会话管理安全性及移动性管理安全性的安全技术集合;

(V) **终端安全:** 保证终端计算环境安全性的技术集合;

(VI) **切片与 VNF 安全:** 保证切片与 VNF 的安全运行, 以及保证各切片间与各 NVF 间的安全通信的安全技术集合;

(VII) **开放接口安全:** 保证网络对业务提供方开放服务的合理、合法调用的安全技术集合;

(VIII) **安全可视与可配置**: 上述安全功能可配置并且用户可获知安全功能的配置。

4 5G 安全架构可行性讨论

为了证明所设计的 5G 安全架构的可行性, 本部分同样从业务应用、网络、无线接入、用户与终端、系统五个视角讨论所设计的5G安全架构如何满足第 3 节中各项安全需求。

4.1 针对业务应用安全需求的设计

回溯图 1, 业务应用安全需求主要包括: 信任模型多元化与安全机制按需配置。

1) 针对信任模型多元化的设计

针对业务应用多元化信任模型的需求, 所设计的安全架构将支持用户、网络、业务任意二者间的相互认证。如图 4 所示, 用户和网络间的相互认证将通过核心网虚拟功能 AAA 和 CP-AU 的认证功能实现。AAA 和 CP-AU 设计的认证功能包括: 为不同接入方式的终端提供统一认证; 为物联网节点提供成组认证服务[43], 即一次完成对按照一定原则(如, 同属一个应用、在同一个区域、有相同的行为特征等)组织在一起的大量物联网节点的认证; 对时延敏感类的业务提供快速认证服务等。

用户与业务之间的认证可根据不同的业务需求, 选用多样化的认证方式, 如, 网络代理认证、业务与用户间独立认证等方式[25]。

对于网络与业务之间的认证, 为了不在认证过程中暴露 5G 核心网边缘, 在所设计的安全架构中引入安全开放服务代理(SOA)。SOA 是运营商部署在数据网络(DN)中的服务代理, 与 5G 核心网之间建立安全连接。服务与网络间的互相认证由 SOA 代理完成。

2) 针对安全机制按需配置的设计

针对 5G 网络在业务层面对安全机制灵活配置的需求, 在所设计的安全架构中, 引入了切片模板管理(STM)虚拟网络功能, 针对不同需求的业务应用, 提供不同配置(含安全配置)的切片模板以实例化网络切片并提供相应服务。

参考文献[26], 我们列出了 8 类 5G 移动通信系统应用场景, 如表 1 所示, 并总结分析了各场景典型用例对网络切片关键性能指标(KPI)需求程度。所选的 KPI 包含安全性、延迟性、移动性、弹性、(每设备)吞吐量、服务设备数量。表 1 中数字 0-3 表示用例需要切片满足不同 KPI 的需求程度, 数字越大代表需求程度越高。因此, 基于表 1, 可将不同业务用例的需求表示为 7 维需求向量 $\boldsymbol{R}$, 并且向量 $\boldsymbol{R}$ 可投影至由各 KPI 需求程度构成的 7 维需求空间中。

$$G(S,L,M,R,T,\#D,A)\in Z^7 \tag{3}$$

根据各业务的需求向量, 运营商可将具有相似需求的业务进行聚类, 并使用相同服务质量需求与安全需求的切片模板提供服务。例如, 移动热点和高速移动列车两个用例具有相似的需求向量, 因此它们可对应相同的切片模板。表 1 中也给出了一种从各用例的需求向量映射到 6 种不同模板的示例。其中, 移动视频监视和无人机遥控两个用例对应的切片模板分别为 {2,2,0,1,1,2,1} 和 {2,2,1,2,1,1,2}, 根据这些模板实例化切片构成的子网可提供满足需求的服务。

4.2 针对网络安全需求的设计

如图 1 所示, 网络视角的安全需求主要包括: 基础设施安全、软件设计安全, 以及网络切片按需安全配置与相互隔离。

对应于5G移动通信系统对基础设施及软件设计安全需求, 在所设计架构中引入了 VNF 安全、切片安全以及开放接口安全, 用以面向不同的服务实现安全虚拟化和安全可配置。具体而言, 在 5G 网络中, 使用网络虚拟化技术对底层资源进行统一的“池化管理”, 通过切片技术将核心网切分成多个核心网切片, 并在切片内部使用 NFV 技术分别在控制面和用户面虚拟化出相应的控制面虚拟网络功能(CPF)和用户面虚拟网络功能(UPF)。对于各个切片共用的虚拟网络功能, 如用于统一认证的 CP-AU 和用于切片管理的 SLM 虚拟网络功能, 将进行独立的虚拟化, 并实现与各切片之间安全交互的接口。同时, 使用切片隔离技术(如[44-46])和 VNF 隔离技术(如[47-49]), 对不同切片之间, 以及切片内部不同的虚拟网络功能之间进行安全隔离, 以构建安全的运行环境。

此外, 对于 5G 移动通信系统所提供的开放性服务, 在安全架构的各切片中由开放性服务功能(OSF)针对业务的需求进行合理实现。为了确保开放性服务 API 的安全调用, 同时隐藏核心网边缘及切片内部信息, 在 SOA 与各切片的 OSF 间建立安全链接, 并使用 SOA 作为代理统一向业务提供方提供开放性服务。同时, SOA 将对业务提供方的 API 服务请求进行监管, 确保 API 的合法、合理调用。此外, SOA 应根据业务提供方的 API 请求, 交付相应的 OSF 以提供开放 API 服务, 并向业务屏蔽所提供服务的 OSF 等信息, 确保当 SOA 遭受攻击时不会威胁 OSF 及核心网其他 VNF 的安全。

表 1 各用例 KPI 需求程度与切片模板

Table 1 KPIs and slice templets for different use cases

Use Case Family	Use Cases	KPIs							Network Slices
		S	L	M	R	T	#D	A	
Broadband access in dense areas	Pervasive video	1	2	1	1	2	3	1	D
	Operator Cloud service	2	2	1	2	2	3	1	D
	Dense Urban Society	1	2	1	2	2	3	1	D
	Smart Office	2	2	1	2	3	2	1	D
Broadband access everywhere	Video Streaming in stadium	1	2	1	2	1	3	1	D
	50 Mbps everywhere	1	2	1	0	1	2	1	D
	Ultra-low cost network	1	0	1	0	0	1	1	D
High User Mobility	High Speed train	1	2	2	1	1	2	1	HM
	Moving Hot spots	1	2	2	1	1	2	1	HM
	Remote computing	1	2	2	1	1	1	1	HM
	3D Connectivity: Aircrafts	1	2	3	1	0	1	1	HM
Massive IoT	Smart Wearables	1	0	0	2	0	3	1	M2
	Sensor networks	1	0	0	1	0	3	1	M2
	Mobile Video surveillance	2	2	0	1	1	2	1	HM+M2
Extreme Real Time	Tactile Internet	1	3	1	2	1	1	2	ULL
Lifeline	Natural disaster	3	0	1	3	0	2	1	HR
Ultra Reliable Comm.	Automated Traffic Control/Driving	3	3	2	3	1	1	3	UHA
	Collaborative robots	3	3	2	2	1	1	2	UHA
	Remote objects manipulation	3	3	2	2	1	1	2	UHA
	eHealth: extreme life critical	3	2	1	3	1	1	3	UHA
	Public safety	3	2	1	3	1	1	3	UHA
	3D Connectivity: Drones	2	2	1	2	1	1	2	HM+UHA

(S: 安全性; L: 延迟性; M: 移动性; R: 弹性; T: (设备)吞吐量; #D: 支持设备数量; A: 可靠性; D: 默认切片; HM: 高移动性切片; M2: M2M 切片; ULL: 超低延时切片; HR: 高回弹切片; UHA: 超高可靠性切片)

针对网络切片按需安全配置与相互隔离需求, 在所设计的架构中, 引入了切片管理(SLM)虚拟网络功能。SLM 用于切片全生命周期管理, 包括切片实例化、切片资源调整、切片资源释放以及切片选择等服务。

核心网切片的创建与管理过程如下: 网络运营商对业务提供方提供的安全需求、时延需求等多样化需求进行统一描述, 在 STM 中创建相应的切片模板。SLM 虚拟网络功能将根据 STM 提供的切片模板向通用资源平台申请网络资源, 并在申请到的资源上实现虚拟网络功能和交互接口的实例化、服务编排以及相应安全性配置, 以实例化相应网络切片。核心网中不同的网络切片能为具有不同需求的业务提供差异化的网络功能配置。

在切片运行过程中, 服务于不同业务的不同网络切片在运行中严格隔离; 对于不同虚拟网络功能(如 AAA 和 CP-AU)间的通信应严格管控; 对于无通信需求的虚拟网络功能应严格隔离。

对于需要接入特定切片的用户和业务, 应对其进行鉴权。在建立网络、用户、业务三者的信任关系后, SLM 虚拟网络功能将针对不同业务的应用场景及安全需求, 选用相应的核心网切片对业务进行承载。例如, 对于无人机业务, 核心网可选用具有高移动性保障的网络切片, 切片中应支持快速安全接入和频繁切换时的高效移动性安全管理; 对具有大量节点的物联网业务, 应选择支持批量认证功能的核心网切片。

此外, SLM 虚拟网络功能能够根据新接入业务的安全需求以及网络负载状态等信息对运行态的核心网切片进行快速功能升级和资源调整; 同时, 在业务下线时, SLM 虚拟网络功能能够及时撤销和回收资源, 以实现灵活的切片生命周期管理。

4.3 针对无线接入网视角安全需求的设计

回溯图 1, 5G 移动通信系统无线接入网的安全需求主要包括: 多接入技术融合统一接入管理与 MEC 内生服务安全。

对于多接入技术融合统一接入管理需求, 在 5G 安全架构中引入统一的 CP-AU 和 AAA 虚拟网络功能对异构接入用户进行统一的接入管理。图 5 给出了基于文献[19, 50-56]所设计的统一接入流程框架。通过多接入技术接入的用户可使用 3GPP TR 23.799[19]中的统一认证框架与网络进行双向认证。认证成功后根据切片 ID(由用户主动提供或由 SLM 分配)向相应的切片发起接入鉴权请求并执行鉴权过程。由于业务模型的差异性, 鉴权过程可由网络执行, 也可交由授信的业务执行。该过程也适用于用户、网络、业务三方的相互认证, 详细过程见文献[25]和本文 2.1.2 节, 这里不再赘述。另外, 在所设计的系统安全架构中的各切片中引入安全上下文①管理(SCM)的虚拟网络功能, 用于管理与所在核心网切片的安全性配置相适应的安全上下文。统一认证架构[18]中的安全上下文结构如图 6 所示, 其中 CP-AN 为 AN 信令保护网络功能。在用户面承载建立过程中, SCM 也可对相应的安全上下文进行管理以保证用户面安全。

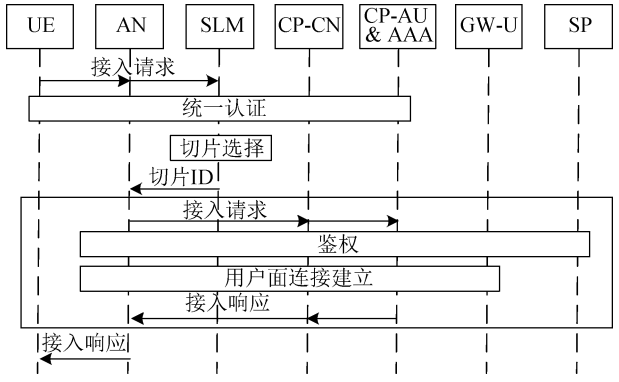

图 5 统一接入流程

Figure 5 Unified mobile user access procedure

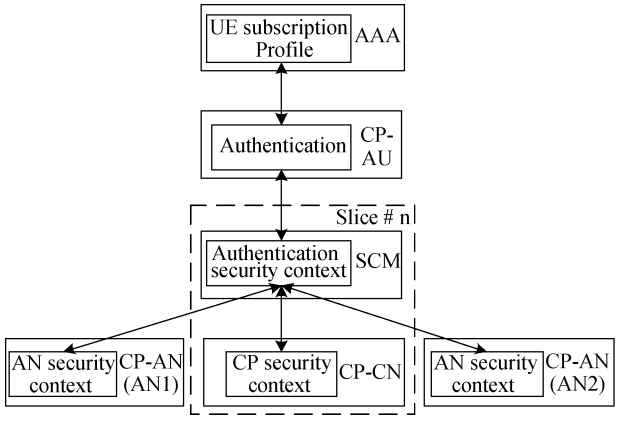

图 6 统一认证中的安全上下文管理

Figure 6 Security context management in the unified authentication framework

为了满足超密集异构组网中高效移动性安全管理需求, 可在 CP-AU 和 CP-CN 设计并支持快速接入和快速切换机制。例如, 可采用文献[57]提出的快速切换方法, 基于用户移动性的准确预测, 提前触发切换认证过程; 也可采用文献[58] 提出的根据安全等级要求的快速认证方法, 高安全等级用基于加权安全上下文信息传输技术的快速接入机制, 低安全等级的认证采用 MAC 地址, 从而降低切换时延并提高切换时的认证效率。

4.4 针对用户与终端安全需求的设计

回溯图 1, 5G 移动通信系统用户与终端的安全需求主要包括: 更加严密的用户隐私保护, 灵活多样的海量身份标识及其载体, 以及高可信终端安全运行环境构建。

针对更加严密的用户隐私保护需求, 所设计的架构完全采用了 3GPP 在相关技术报告与规范[18-19, 28]中给出了增强用户隐私保护的手段, 主要包括:

• 在终端与 CP-AU 之间鉴权与认证过程中, 采取以下手段: 对用户的永久/长期标识进行动态加密, 防止永久/长期标识泄露[18, 28]; 提高临时标识更新周期, 从而避免通过主/被动监听临时标识获取用户的隐私信息[19]; 针对高安全需求的移动用户, 提供专用身份及隐私保护机制。

• 对于计算与续航能力允许的终端, 使用更高级的密码算法增强对用户敏感信息进行保护。

针对灵活多样的海量身份标识及其载体需求, 所设计的安全架构中体现如下:

• 在网络侧, AAA 对多安全等级、多类别的身份标识进行统一存储、管理与认证, 并支持对软 SIM 终端的身份标识注册、配置、管理等功能; 针对海量设备(如物联网节点)同时接入的需求, 使用 CP-AU 和 AAA 对成组认证[20, 43], 定时连接[18]等技术提供支持。

• 在终端侧, 依托所构建的终端安全环境, 由可信存储和计算空间对终端身份标识进行涵盖分发、存储、读取、销毁等过程的全生命周期管理。

针对高可信终端安全运行环境构建的需求, 在所设计的安全架构中, 依托可信计算技术实现, 具体而言:

• 可信环境构建: 在实体平台上植入硬件可信根, 构建从运算环境、基础软件到应用与服务的信任链, 依托逐级的完整性检查和判断, 实现实体软硬件环境的完整性保护, 确保用户面数据保护与控制

①安全上下文: 定义用户接入安全等级、访问权限、加密算法等。

面信令保护的安全执行。

• 可信路径构建与动态度量: 实现终端系统和关键应用的文件、指令流的采集、检测模型构建及安全追踪, 完成对终端系统和关键应用的动态完整性度量, 并对可信路径过程进行安全记录, 构建可信路径。

• 终端系统安全事件可信记录: 实现终端系统跨层的安全事件数据审计方案, 构造包含应用层、操作系统层以及驱动层等的多层次可信记录代理, 实现安全事件记录。

另外, 对于高安全需求或有特殊安全需求的终端, 可依托如安全管理云等实体进行终端、接入与业务的多维管控, 支持终端安全检测、警告, 甚至业务阻断等管控功能。

4.5 针对系统视角安全需求的设计

为了应对5G移动通信网络中由通信与计算融合演进导致的未知潜在安全威胁以及 APT 攻击, 并能够满足敏感行业的高安全需求, 在所设计的安全架构中引入了 “安全管控云”, 其可利用虚拟化技术部署于核心网。通过安全管控云实现实时分析各网元与网络功能行为特征, 准确辨识异常行为, 并针对异常行为, 采用主动防御等高级安全防护技术。

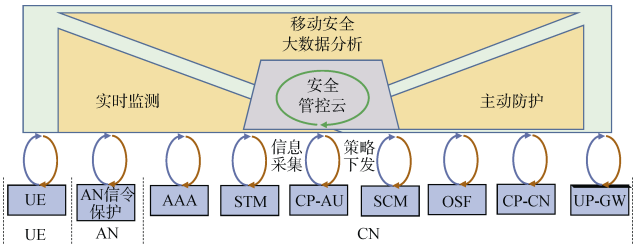

图 7 安全管控云架构示意图

Figure 7 An illustration of security management and control cloud

如图 7 所示, 在安全管控云中引入经典认知模型, 设计为包含实时监测-移动安全大数据分析-主动防护的闭环系统。为满足实时监测的需求, 在接入网、核心网的网元与网络功能中分布式部署监测点, 各监测点实时采集相应的配置与网络实时运行状态等信息(如信令信息、流量信息、内容信息), 所采集信息将统一汇聚到安全管控云。在移动安全大数据分析模块中, 可结合智能学习与大数据技术, 使用诸如基于时间片的频率统计[59, 60]、基于时间片的自相似性检测[61]等方法对威胁特征进行提取; 也可使用如基于贝叶斯攻击图的动态安全风险评估模型[62]、结合域内源地址检测[63]和 traceback[64]等手段对网络中存在的潜在威胁进行识别、特征分析和追踪。主动防护模块则根据特征分析结果生成相应的主动防护策略, 所生成的安全策略将实时下发至各监测点, 由各监测点对所在网络功能重配置以实现系统的主动防御。

下面以系统异常流量管控为例说明安全管控云的必要性与工作机制。在 UE 侧, 攻击者可通过截获低安全等级的 NB-IoT 节点发起 DDoS 攻击, 并可将这些节点作为跳板攻击接入网与核心区域核心设备, 将安全风险扩展到高安全级别的设备[65]; VoLTE、VoWiFi 以及 5G 分组语音业务的端到端高 QoS 保障使得针对这些业务的 DDoS 攻击破坏性更大[66]。在 CN 侧, 软件定义网络(SDN)的引入将导致新的针对 SDN 控制流的 DDoS 攻击; 虚机(VM)资源也可能被攻击者利用发起 DDoS 攻击[67]。

为了应对上述安全威胁, 对 AN 与 CN 中数据流信息采集并汇总至管控云, 通过在管控云执行网络流量异常分析检测, 辨识异常流量特征, 生成并下发并更新相应网元或网络功能的流量过滤策略[68], 从而形成安全管控闭环。

安全管控云针对潜在安全威胁的工作主要区别在于监测数据类型与分析方法, 限于篇幅, 这里不再展开, 可参考文献[69]等。

5 5G 安全技术发展趋势

基于上文分析得到的安全需求与所设计的安全体系架构, 我们进一步凝练出了以下三大 5G 融合演进安全技术发展趋势(如图 1 所示), 并探讨了其中开放性的关键技术难题。可以预见未来几年他们将是 5G 安全技术研究领域最为活跃研究方向。在下一步研究工作中, 我们将结合所设计的 5G 总体安全架构开展关键难题研究。

5.1 面向服务的安全

在 5G 时代, 传统移动通信系统中面向通信的安全将演进为面向多元化服务与行业应用的安全。面向服务的安全的内涵可以概括为: 采用多元化的信任模型, 支持服务与网络间的信任构建, 并满足网络服务开放安全等需求的安全技术集合。

面向服务的安全需要突破传统移动通信系统安全设计思路, 采用自顶向下的安全设计思路, 突破匹配 5G 系统架构与满足 5G 通信 QoS 要求的安全服务技术, 从而真正有效的支撑本文 4.1 节中所给出的服务应用安全框架实现。但是要实现这一目标, 首先需要解决多个开放性基本难题, 例如, 如何在 5G 移动通信网络架构基础上设计内嵌三元信任模型运行机制; 如何面向差异化 QoS 业务服务的安全需求提

供匹配的认证与安全服务策略; 在满足 5G 超低时延等 QoS 要求的条件下, 如何设计严密的服务安全防护机制。

5.2 安全虚拟化

本文认为“安全虚拟化”包含两方面的内涵, 可以概括为:

a) 以虚拟化方式配置安全功能承载体、安全防护策略执行所需的资源, 其实现方式可在 5G 移动通信系统中的 NFV 技术基础上, 引入基于安全防护需求的资源配置与分配, 实现安全内嵌的 NFV(SeNFV)。

b) 安全策略可动态配置、在线升级, 整个系统安全防护体系可动态重构, 是一种动态安全防护有效实施方式。

显然内涵 a)体现的是基于 NFV 强化 5G 网络安全的潜力, 但是其实现面临着新的关键方法与技术难题, 例如, 如何量化不同安全策略对于计算、存储、通信等各种资源的需求; 如何利用 NFV 技术有效的按需编排安全策略, 在满足安全性要求的条件下, 提高资源利用率; 如何规避策略动态配置导致的额外潜在安全威胁。

要内涵 b)所体现的动态安全防护方法, 则需要一个完整认知过程, 即包含感知、分析、安全威胁辨识与策略生成步骤。但是, 这个过程的设计与实现需要移动通信、信息安全、大数据、人工智能、控制理论、软件工程等多学科交叉, 极具挑战性, 同时也是充满机遇的新研究方向。

5.3 增强用户隐私与数据保护

增强用户隐私与数据保护的内涵可以概括为: 采用有效手段控制个人与行业用户多样化隐私数据与信息在其存储、传输、处理各个环节的可见性和安全性, 形成增强的隐私信息与数据保护能力。

由于 5G 时代用户感官外延与服务个性化, 将直接或间接的涉及大量用户隐私数据与信息, 这些隐私信息包括身份、性格、习惯、健康状况等; 多元化的行业应用(如工业物联网(IIOT))中涉及众多行业敏感数据, 如, 生产规模、运营状况、设备型号等。因此, 5G 移动通信网络中隐私信息呈现多样化与异构化的特点。为了满足 5G 隐私保护的需求, 需要提出新方法与技术解决新的问题, 例如, 如何划分不同隐私相关数据的保护等级; 如何针对不同隐私相关数据设计兼顾安全与效率隐私数据保护机制。

6 总结

5G 安全技术方兴未艾, 并将与 5G 移动通信系统同步演进。本文针对这一发展趋势, 首先, 从业务应用、网络、无线接入、用户与终端、系统五个视角梳理并分析了 5G 移动通信系统 CT 与 IT 融合演进的特点与安全需求。基于上述分析, 本文设计了一种 5G 安全体系架构, 并初步论证了所设计体系架构能够很好的满足 5G 安全需求。最后, 通过对于安全需求的分析, 本文归纳总结出了 5G 安全技术的三个发展趋势: “面向服务的安全”“安全虚拟化”与“增强用户隐私与数据保护”, 并探讨了其中的关键技术难题。本文希望为 5G 安全技术的同步演进提供有益的参考, 并对未来 5G 安全技术的研究起到抛砖引玉的作用。

参考文献

[1] 5G-Ensure Consortium, “Horizon 2020, call H2020-ICT-2014-2, proposal number 671562, 5G-ENSURE,” https://5g-ppp.eu/5g-ensure/. Accessed February, 2016.

[2] 5G Public Private Partnership, “5G Vision,” https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf. Accessed February, 2016.

[3] METIS, “Wireless Communications Enablers for the Twenty-Twenty Information Society,” D1. 2, Initial channel models based on measurements, 2013.

[4] FuTURE, http://www.future-forum.org/2009cn/aboutus.asp.

[5] IMT-2020 (5G) Promotion Group, “5G Concept,” White Paper on 5G Concept, 2015.S. Abdelwahab, B. Hamdaoui, M. Guizani and T. Znati, “Network function virtualization in 5G,” *IEEE Communications Magazine*, vol. 54, no. 4, pp. 84-91, April 2016.

[6] S. Abdelwahab, B. Hamdaoui, M. Guizani and T. Znati, “Network function virtualization in 5G,” *IEEE Communications Magazine*, vol. 54, no. 4, pp. 84-91, April 2016.

[7] M. Casado, N. Foster, and A. Guha, “Abstractions for software-defined networks,” *Communications of the ACM*, vol. 57, no. 10, pp. 86–95, 2014.

[8] A. Gupta, R.K. Jha, “A survey of 5G network: architecture and emerging technologies,” *IEEE Access*, vol. 3, pp. 1206-1232, 2015.

[9] H. Li, Z. Wang, Z. Xu, et al. “Cross-layer transmission and energy scheduling under full-duplex energy harvesting wireless OFDM joint transmission,” *Springer Sci China Inf Sci,* 59(10): 102310, 2016.

[10] Z. Wang, H. Li, et al., “Modeling and Transmission Optimization of Full Duplex Energy Harvesting enabled Hybrid Relaying,” In Proc. *IEEE Globecom* 2016, D.C., pp. 1-7, 2016.

[11] 3GPP TR38.804, “Study on New Radio Access Technology; Radio Interface Protocol Aspects,” v0.3.0, 2016.

[12] J.G. Andrews, S. Buzzi, C. Wan, et al., “What Will 5G Be?” *IEEE Journal on Selected Areas in Communications*, 32(6), pp. 1065-1082, Jun. 2014.

[13] H. Li, X. Xu, D. Hu and et al., “Clustering strategy based on graph method and power control for frequency resource management in femtocell and marocell overlaid system,” *IEEE Journal of Communica-tions and Networks*, 13(6), pp. 664-677, Dec. 2011.

[14] F. Boccardi, R. W. Heath, A. Lozano, et al., "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, 52(2), pp. 74-80, 2014.

[15] H. Li and D. Hu, "Mobility prediction based seamless RAN-cache handover in HetNet," in Proc. *IEEE Wireless Communications and Networking Conference (WCNC)*, Doha, pp. 1-7, 2016.

[16] H. Li, D. Hu and S. Ci, "iCacheOS: In-RAN Caches Orchestration Strategy through Content Joint Wireless and Backhaul Routing in Small-Cell Networks," *IEEE Global Communications Conference* (*GLOBECOM*), San Diego, CA, pp. 1-7, 2015.

[17] H Li, C. Yang, et al., "Cooperative RAN Caching based on Local Altruistic Game for Single and Joint Transmissions," 21(4), *IEEE Communications Letters*, pp. 853-856, Apr. 2017.

[18] 3GPP TR 33.899, "Study on the security aspects of the next generation system," v0.4.1, 2016.

[19] 3GPP TR 23.799, "Study on Architecture for Next Generation System," v1.0.2, 2016.

[20] 3GPP TR 22.861, "FS_SMARTER - massive Internet of Things," v14.1.0, 2016.

[21] Ericsson AB, "5G – Key component of the networked society, RWS-150009," http://www.3gpp.org/news-events/3gpp-news/1734-ran_5g. Accessed February, 2016.

[22] Ericsson, "Mobility Market Report," Technical Report, 2015. ("移动市场报告", *爱立信技术报告*, 2015。)

[23] Qualcomm, "5G View on technology & standardization, RWS-150012," http://www.3gpp.org/news-events/3gpp-news/1734-ran_5g.Accessed February, 2016.

[24] ZTE, "Considerations on 5G Key technologies & Standardization, RWS-15002," http://www.3gpp.org/news-events/3gpp-news/1734-ran_5g.Accessed February, 2016.

[25] Huawei, "5G Security: Forward Thinking," Huawei White Paper, 2016.

[26] NGMN Alliance, "NGMN 5G White paper," https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf. Feb. 2015.

[27] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Communications Magazine*, 52(2), 90–96.

[28] 3GPP TR 22.891, "Study on New Services and Markets Technology Enablers," v14.1.0, 2016.

[29] G. Horn, P. Schneider, "Towards 5G Security," *IEEE TrustCom*, vol. 01, pp. 1165-1170, 2015.

[30] Ericsson, "5G Use Cases", White Paper on Use Cases, 2016.

[31] ZTE, "Big Video Best View," ZTE White Paper on Video, Jun. 2016. ("大视频大未来", *中兴通讯大视频白皮书* v1.0, 2016。)

[32] "Mobile-Edge Computing," Introductory Technical White Paper, 2014.

[33] S. Hidano, M. Pečovský and S. Kiyomoto, "New Security Challenges in the 5G Network," in Proc. *International Symposium on Intelligence Computation and Applications (ISICA'15)*, pp. 619-630, 2015.

[34] H. Li, "Researches on Femtocell assisted cellular network", Ph.D Dissertation, *Beijing University of Posts and Telecommunications,* 2011. (李宏佳. "Femtocell 辅助蜂窝系统关键技术研究" [D] 北京: 北京邮电大学, 2011。)

[35] X. You, Z. Pan, X. Gao, S. Cao and H. Wu, "The 5G Mobile Communication: The Development Trends and its Emerging Key Techniques," *Science China Information Sciences*, vol. 44, no. 5, pp. 551-563, 2014.

[36] N. Abani, M. Gerla, "Centrality-based Caching for Privacy in Information-Centric Networks," DOI: 10.1109/MILCOM.2016.7795502, *IEEE MILCOM*, 2016.

[37] A. Shaik, R. Borgaonkar, N. Asokan, et al., "Practical attacks against privacy and availability in 4G/LTE mobile communication systems", arXiv preprint arXiv:1510.07563, 2015.

[38] 3GPP TR 33.849, "Study on subscriber privacy impact in 3GPP," v14.0.0, 2016.

[39] 3GPP TR 22.864, "Feasibility study on new services and markets technology enablers for network operation; Stage 1," v15.0.0, 2016.

[40] 3GPP TR 22.185, "Service requirements for V2X services," v14.2.0, 2016.

[41] 3GPP TS 33.102, "3G security; Security architecture," v14.0.0, 2016.

[42] 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security Architecture," v13.3.0, 2016.

[43] 3GPP TR 33.812, "Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment," v9.2.0, 2010.

[44] S. Gutz, A. Story, C. Schlesinger, et al., "Splendid isolation: A slice abstraction for software-defined networks," in Proc. *ACM Proceed- -ings of the first workshop on Hot topics in software defined networks*, pp. 79-84, 2012.

[45] M. Richart, J. Baliosian, J. Serrat J, et al., "Resource slicing in virtual wireless networks: A survey", *IEEE Transactions on Network and Service Management*, 2016.

[46] R. Kokku, R. Mahindra, H. Zhang, and S. Rangarajan, "Cellslice: Cellular wireless resource slicing for active RAN sharing," in Proc. *5th Int. Conf. Commun. Syst. Netw.* (*COMSNETS*), Bengaluru, India, pp. 1–10, 2013.

[47] ETSI GS NFV-IFA 004, "Network Functions Virtualization (NFV); Acceleration Technologies; Management Aspects Specification", v2.1.1, 2016.

[48] Intel, Intel Software Guard Extensions, https://software.intel.com/en-us/sgx.

[49] F. McKeen, I. Alexandrovich, A. Berenzon, et al., "Innovative instructions and software model for isolated execution", in Proc. *ACM Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, 2013.

[50] E. Sithirasenan, S. Kumar, and K. Ramezani, "An EAP Framework for Unified Authentication in Wireless Networks," in Proc. *IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom'11*), pp. 389-397, 2011.

[51] F. Qi, W. Zhang, G. Wang, H. Fang, "Unified Security Architecture Research for 5G Wireless System," in Proc. *Web Information System and Application Conference* (*WISA*), pp. 91-94, 2014.

[52] J. Cao, M. Ma and H. Li, "An Uniform Handover Authentication Between E-UTRAN and Non-3GPP Access Networks," *IEEE*

Transactions on Wireless Communications, vol. 11, no. 10, pp. 3644-3650, 2012.

[53] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform Group-Based Handover Authentication for MTC within E-UTRAN in LTE-A networks," in Proc. *IEEE International Conference on Communications* (*ICC*), pp. 7246-7251, 2015.

[54] X. Wang, P. Hao, and L. Hanzo, "Physical-layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments," *IEEE Communications Magazine*, pp. 1-7, 2016.

[55] Tudzarov, Aleksandar, and Toni Janevski, "Functional Architecture for 5G Mobile Networks," *International Journal of Advanced Science & Technology*, 2011.

[56] Tudzarov, Aleksandar and Toni Janevski, "Protocols and Algorithms for the Next Generation 5G Mobile Systems," *Network Protocols & Algorithms*, 2011.

[57] H. Li, S. Ci and Z. Wang, "Prediction handover trigger scheme for reducing handover latency in two-tier Femtocell networks," in Proc. *IEEE Global Communications Conference* (*GLOBECOM*), pp. 5130-5135, 2012.

[58] X. Duan, X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in Proc. *IEEE International Conference on Communications (ICC)*, pp. 1-6, 2016.

[59] Q. Sun, D. Zhang and P. Gao, "Detecting Distributed Denial of Service Attacks Based on Time Series Analysis," *Chinese Journal of Computers*, vol. 28, no. 5, pp. 768-773, 2005.
(孙钦东, 张德运, 高鹏, "基于时间序列分析的分布式拒绝服务攻击检测", *计算机学报*, 2005, 28(5): 768-773。)

[60] X. Gu, H. Wang, T. Ni and H. Ding, "Detection of Application-Layer DDoS Attack Based on Time Series Analysis," *Journal of Computer Applications*, vol. 33, no. 8, pp. 2228-2231, 2013.
(顾晓清, 王洪元, 倪彤光, 丁辉, "基于时间序列分析的应用层 DDoS 攻击", *计算机应用*, 2013, 33(8): 2228-2231。)

[61] H. He, W. Huang, T. Li, P. Zeng and X. Dong, "Multilevel DDoS protection mechanism based on SDS framework," *Computer Engineering and Applications*, vol. 52, no. 1, pp.81-88, 2016.
(何亨, 黄伟, 李涛, 曾朋, 董新华, "基于 SDS 架构的多级 DDoS 防护机制", *计算机工程与应用*, 2016, 52(1): 81-88。)

[62] N. Gao, L. Gao, Y. He, Y. Lei and Q. Gao, "Dynamic Security Risk Assessment Model Based on Bayesian Attack Graph," *Journal of Sichuan University* (*Engineering Science Edition*), vol. 48, no.1, pp. 111-118, 2016.
(高妮, 高岭, 贺毅岳, 雷艳婷, 高全力, "基于贝叶斯攻击图的动态安全风险评估模型", *四川大学学报工程科学版*, 2016, 48(1): 111-118。)

[63] P. Xiao and J. Bi, "OpenFlow based Intra-AS Source Address Validation," *Journal of Chinese Computer Systems*, vol. 34, no. 9, pp. 1999-2003, 2013.
(肖佩瑶, 毕军, "基于 OpenFlow 架构的域内源地址验证方法", *小型微型计算机系统*, 2013, 34(9): 1999-2003。)

[64] S. Yu, W. Zhou, R. Doss and W. Jia, "Traceback of DDoS Attacks Using Entropy Variations," *IEEE Trans. Parallel and Distributed Systems*, 2011, vol. 22, no. 3, pp. 412-425.

[65] M. Asplund, S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services", *IEEE Access*, 2016(4): 2130-2138.

[66] H. Tu, Y. Li, C. Peng, et al, "How voice call technology poses security threats in 4G LTE networks", *2015 IEEE Conference on Communications and Network Security* (*CNS*), pp. 442-450, 2105.

[67] D. Rawat, S. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey", *IEEE Communications Surveys & Tutorials*, 19(1): 325-346, 2015.

[68] P. Giura, W. Wang, "Using large scale distributed computing to unveil advanced persistent threats", *Science*, Vol. 1, No. 3, pp. 93-105, 2013.

[69] J. Fu, H. Li, X. Wu, et al, "Detecting APT attacks: a survey from the perspective of big data analysis", *Journal of Communications*, 2015(11): 1-14.
(付钰, 李洪成, 吴晓平, 等, "基于大数据分析的 APT 攻击检测研究综述", *通信学报*, 2015(11): 1-14。)

李宏佳 于 2011 年在北京邮电大学电路与系统专业获得博士学位。现任中国科学院信息工程研究所第五研究室副研究员。研究领域为移动通信系统安全、异构蜂窝网络组网、优化理论与方法。研究兴趣包括: 5G 服务化安全架构、MEC 协同服务与安全防护、移动终端安全管控。Email: lihongjia@iie.ac.cn

王利明 于 2007 年中国科学院软件所计算机科学与技术专业获得博士学位。现任中国科学院信息工程研究所第五研究室副研究员。研究领域包括网络与通信安全、云计算、大数据安全分析、关键基础设施安全等。Email: wangliming@iie.ac.cn

徐震 于 2005 年在中国科学院软件所计算机科学与技术专业获得博士学位。现任中国科学院信息工程研究所第五研究室研究员级高级工程师, 研究室主任, 信息安全国家重点实验室副主任。研究领域为可信计算、网络安全、系统安全。Email: xuzhen@iie.ac.cn

杨畅 于 2014 年在山东大学电子信息科学与技术专业获学士学位。现在中国科学院信息工程研究所第五研究室室攻读博士学位。研究领域为 5G 安全。研究兴趣包括: MEC 服务安全及优化、NP 难优化等。Email: yangchang@iie.ac.cn