软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(6):1813−1825 [doi: 10.13328/j.cnki.jos.005547]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

5G 移动通信网络安全研究*

冯登国[1], 徐 静[1,3], 兰 晓[2,3]

[1](计算机科学国家重点实验室(中国科学院 软件研究所),北京 100190)

[2](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

[3](中国科学院大学,北京 100049)

通讯作者: 冯登国, E-mail: feng@tca.iscas.ac.cn; 徐静, E-mail: xujing@tca.iscas.ac.cn

摘 要: 第五代(fifth gneration,简称 5G)移动通信网络(简称 5G 网络或 5G),是为构建网络型社会并实现万物互联的宏伟目标而提出的下一代移动网络.随着 LTE 等第四代移动通信网络进入规模化商用阶段,5G 网络的研究已成为世界各国的关注焦点.5G 网络的实现,需要依赖于系统架构和核心技术的变革与创新.目前,5G 网络还处于技术和标准的初级研究阶段.5G 网络的新架构、新业务、新技术对安全提出了新的挑战.简述了 5G 的性能指标、关键技术、应用场景及标准制定的进展,分析了 5G 网络的安全需求及其所面临的技术挑战.基于目前已有的研究工作和标准研制情况,提炼了 5G 安全框架,归纳并阐述了若干安全关键问题及其解决方案,展望了 5G 网络安全的未来研究方向.

关键词: 5G 网络;5G 网络安全;认证框架;切片安全;隐私保护

中图法分类号: TP311

中文引用格式: 冯登国,徐静,兰晓.5G 移动通信网络安全研究.软件学报,2018,29(6):1813−1825. http://www.jos.org.cn/1000-9825/5547.htm

英文引用格式: Feng DG, Xu J, Lan X. Study on 5G mobile communication network security. Ruan Jian Xue Bao/Journal of Software, 2018,29(6):1813−1825 (in Chinese). http://www.jos.org.cn/1000-9825/5547.htm

Study on 5G Mobile Communication Network Security

FENG Deng-Guo[1], XU Jing[1,3], LAN Xiao[2,3]

[1](State Key Laboratory of Computer Science (Institute of Software, The Chinese Academy of Sciences), Beijing 100190, China)

[2](State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences), Beijing 100093, China)

[3](University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: The fifth generation mobile communication network, abbreviated 5G network or 5G, is also called the next generation of mobile communication network, which aims at constructing a networked society and realizing the goal of “everything-connecting”. With 4G mobile communication network entering the commercial stage, the research on 5G has gained wider attention all over the world. The realization of the vision for 5G needs the revolution and innovation of system structure and core techniques, and until now the corresponding techniques and standards are in the primary stage. The new architectures, new business, and new technology bring new challenges to 5G security. This paper briefly summarizes performance, key technology, application scenario, and standardization progress of 5G, analyzes the security requirements and challenges of 5G, introduces 5G security framework, and investigates some key issues and

* 基金项目: 国家自然科学基金(U1636216, U163620049, 61572485); 国家重点基础研究发展计划(973)(2013CB338003)

Foundation item: National Natural Science Foundation of China (U1636216, U163620049, 61572485); National Grand Fundamental Research (973) Program of China (2013CB338003)

收稿时间: 2017-08-09; 修改时间: 2017-12-28; 采用时间: 2018-01-24; jos 在线出版时间: 2018-02-08

CNKI 网络优先出版: 2018-02-08 11:55:36, http://kns.cnki.net/kcms/detail/11.2560.TP.20180208.1155.003.html

the corresponding solutions based on the research efforts, white paper and related standards. Furthermore, the paper discusses the current research trends in industries and academia in the context of 5G security.

Key words: 5G network; 5G network security; authentication framework; slice security; privacy protection

移动通信始于 1978 年贝尔实验室发明的蜂窝移动系统,历经了从 1G 到 4G、从窄带到宽带、从话音通信到移动互联网的发展.如今,随着移动设备的爆炸性增长,移动通信系统已经完全融入人类的日常生活.自 2012 年 7 月开始,国际电信联盟(ITU)[1]已经开始筹备启动新一轮的移动通信系统(Int'l mobile telecommunications,简称 IMT)研究工作,旨在研究面向 2020 年及未来的 IMT 市场、用户、业务应用趋势,并提出未来 IMT 系统的总体框架和关键能力.2015 年 6 月,ITU 在 ITU-R WP5D[2]第 22 次会议上正式确定第五代移动通信系统的名称为 IMT-2020(5G).5G 不仅在用户体验速率、连接数密度、端到端时延、峰值速率和移动性等关键能力上比前几代移动通信系统更加丰富,而且能为实现海量设备互联和差异性服务场景提供技术支持.

目前,全球业界已经就 5G 概念及关键技术达成共识,5G 的标准化工作有望于 2020 年全部完成.5G 将进一步增强人们的移动宽带应用使用体验,并以创新驱动为理念,力求成为软件化、服务化、敏捷化的网络,并服务于智慧家庭、智能建筑、智慧城市、三维立体视频、超高清晰度视频、云工作、云娱乐、增强现实、行业自动化、紧急任务应用、自动驾驶汽车等垂直行业.毫无疑问,5G 已经成为全球移动通信领域新一轮信息技术的热点课题.

为了实现 5G 万物互联的宏伟愿景,5G 必须实现智能化,以同时支持异构的网络(3G,4G 和 WiFi 等接入方式)和设备(移动手持设备、物联网设备)对资源的正常使用.而智能化需要实现移动通信技术与云计算、大数据、虚拟现实等信息技术的高度融合以及系统架构的创新.这些变革意味着 5G 将迎来全面的演进,包括核心和管理系统的演进以及无线端协议到应用层协议的演进.在这些演进中,安全的影响无处不在,5G 将面临更复杂的安全挑战.

无线通信系统演进到现在(即 4G),已被考虑的安全需求[3]包括:对无线端通信的加密,以防止用户信令和数据被恶意窃听;基于 SIM 卡对用户的认证,以防止消费欺诈;给用户分配临时身份标识,以保护用户身份隐私;网络和用户的双向认证,以防止伪基站攻击等等.然而,这些需求主要立足于提升基于数据和语音通信服务的安全性,而 5G 不仅需要考虑基本的数据和语音通信服务,还将服务于一切可互联的产业.为面对一系列全新的服务需求,5G 必须建立更全面、更高效、更节能的网络和通信服务模型,处理增强的、多方面的安全需求.

- 首先,5G 需要统一的安全管理机制来保证设备跨接入技术的网络接入安全,同时提供通用的安全性,比如设备的认证和隐私性.除了传统终端设备,5G 还需要面向海量异构物联网(IoT)设备提供高效接入认证机制,并需要提供合理措施,以避免大规模设备向网络发起的拒绝服务攻击;
- 其次,5G 需要差异化的安全机制来服务于不同的个人业务及垂直行业服务.5G 基于云架构的端到端网络切片形式被公认为是实现差异化服务的最有效解决方案.因此,在网络切片中实现差异化的安全机制也是 5G 必须要考虑的一个问题;
- 再其次,5G 需要更全面的隐私信息保护措施.5G 的接入设备不再只是传统的通信设备,也包括大量面向具体应用的物联网设备,这些设备会收集用户大量的隐私信息,包括健康状况、个人喜好、社保信息、生活足迹等,并且这些信息将在 5G 系统里被第三方服务商进一步处理以给用户更极致的使用体验.所以,如何在大数据时代开放的系统里全方位地保护用户隐私,也将是 5G 面临的又一大安全挑战.

5G 面临的安全问题远远不止上面所提及的几个方面,对这样一个庞大的系统来说,安全问题很难穷尽.然而,安全是使 5G 成为移动网络平台的基石,当前很多企业和通信联盟都已经认识到 5G 安全对整个系统演进的重要性,并通过一系列会议、白皮书和标准草案对一些关键安全问题进行了讨论,旨在寻求相应问题的具体解决方案.本文在梳理 5G 研究现状的基础上,以 3GPP[4](第三代合作伙伴计划)的相关标准文档为基础,结合工业界和几大通信联盟的白皮书,归纳并阐述 5G 的安全需求、挑战和解决方案.最后,对目前存在的一些未解决的关键技术进行了分析和探讨,并指出一些未来可能的研究方向.

1 5G 研究概述

1.1 性能指标与关键技术

5G 的关键性能指标主要包括支持 0.1Gbps~1Gbps 的用户体验速率,数十 Gbps 的峰值速率,数十 Tbps/km2 的流量密度,100 万/平方公里的连接数密度,毫秒级的端到端时延,“5 个 9”(99.999%)的可靠性以及百倍以上能效提升和单位比特成本降低.此外,绿色节能也是 5G 发展的一个重要指标,以实现无线通信的可持续发展.

5G 关键技术主要来源于无线技术和网络技术两方面:无线技术领域包括大规模多天线技术(massive-MIMO)、超密集组网、全频谱接入、新型多址、新型多载波、先进调制编码、终端直通技术、灵活双工、全双工、频谱共享和 C-RAN 等[5].在网络技术领域,基于软件定义网络(SDN)和网络功能虚拟化(NFV)的新型网络架构已取得广泛共识.此外,还包括移动边缘计算(MEC)、无线 MESH、按需组网等关键技术[6].

1.2 应用场景

2015 年,ITU 在 ITU-R M.2083-0 建议书[7]中确定了 5G 的愿景,并在建议书中明确了 5G 支持的 3 大应用场景,包括增强型移动宽带(enhanced mobile broad band,简称 eMBB)、大规模机器类型通信(massive machine type communications,简称 mMTC)以及超可靠和低延迟通信(ultra-reliable and low latency communications,简称 URLLC).图 1 展示了未来 IMT 的潜在使用场景.

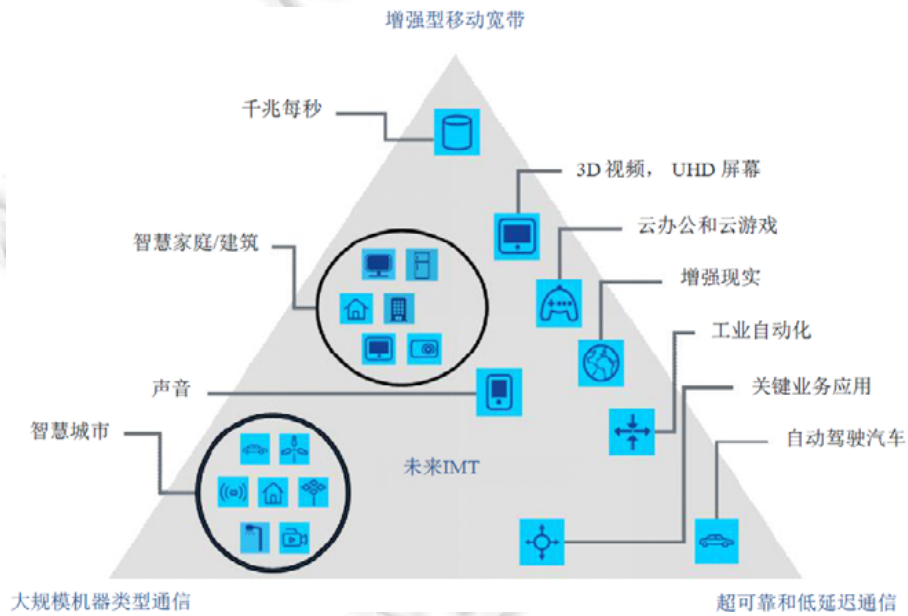

Fig.1 Usage scenarios of future IMT[7]

图 1 未来 IMT 的潜在使用场景[7]

具体来说,3 类场景各自的特点主要是:

(1) 增强型移动宽带.此类场景主要处理以人为中心的潜在需求,要求能提供 100Mbps 的用户体验速率,例如 3D/超高清视频、虚拟现实(VR)/增强现实(AR)等;

(2) 大规模机器类型通信.此类场景主要处理大规模智能设备的通信问题,要求能够支撑百万级低功耗物联网设备终端如各种穿戴设备的连接服务;

(3) 超可靠和低延迟通信.此类场景主要处理对可靠性要求极高、时延极其敏感的特殊应用场景,要求在保证超低于 1 毫秒时延的同时提供超高的传输可靠性,例如辅助驾驶、自动驾驶、工业自动化和远

程机械控制等.

1.3 标准制定情况

由 ITU 和 3GPP 两大组织牵头,各国通信业巨头和一些通信联盟纷纷加入了 5G 的标准化研究行列中,制定全球统一的 5G 标准已成为业界共同的呼声.

ITU 最早于 2014 年开启了 5G 的前期研究工作,主要就 5G 的愿景、技术趋势以及频谱进行了探讨.随后在 2016 年,ITU 又开展了 5G 技术性能需求与评估方法的研究工作,5G 候选方案征集阶段将于 2017 年底截止.而 3GPP 作为国际移动通信行业的主要标准组织,将承担 5G 国际标准技术内容的制定工作.3GPP 从版本 R14[8]开启了 5G 之旅,于 2016 年年初开始了 R15[9]的制定工作.R15 中制定了一些实际规范,将作为第 1 个 5G 标准,预计在 2018 年下半年完成.R16 将完成全部标准化工作,并于 2020 年初向 ITU 提交满足 ITU 需求的方案.按照 ITU 的时间表,IMT-2020(5G)的标准化工作有望于 2020 年全部完成.

与此同时,一些知名的国际通信组织如 5G PPP(5G infrastructure public private partnership)[10]、NGMN(next generation mobile networks)[11]联盟和 GSMA 移动智库(GSMA intelligence)[12]也发布了各自的 5G 白皮书[13−15].为把握 5G 的发展机遇,我国于 2013 年 2 月成立了 IMT-2020(5G)推进组,推进组由中国工业与信息化部、科技部、发改委三部委联合成立,目前已有 56 家成员单位,涵盖国内移动通信领域产学研用主要力量,是推动国内 5G 技术研究及国际交流合作的主要平台.IMT-2020(5G)推进组已经发布了多份白皮书,主要包括 2014 年 5 月发布的《5G 愿景与需求白皮书》[16]、2015 年 2 月发布的《5G 概念白皮书》[17]、2015 年 5 月发布的《5G 无线技术架构白皮书》[5]和《5G 网络技术架构白皮书》[6]、2016 年 5 月发布的《5G 网络架构设计白皮书》[18]以及 2017 年 6 月发布的《5G 网络安全需求与架构白皮书》[19].这一系列白皮书总结了 IMT-2020(5G)推进组在 5G 方面的最新研究成果.

此外,一些产业巨头包括爱立信、三星、诺基亚、华为也纷纷开启了 5G 的研究工作,发布了 5G 相关的白皮书[20−23],以抢占 5G 产业的制高点.

作为 5G 研究工作的一个重要组成部分,安全需求的研究工作也并行进行.目前,3GPP、5G PPP、NGMN、ITU-2020 推进组、爱立信、诺基亚、华为也纷纷发布了各自的 5G 安全需求白皮书[24−29],并通过安全需求白皮书表达各自对 5G 安全需求的理解与展望.从目前众多安全需求来看,尽管不同的安全需求白皮书的侧重点有所差异,但核心问题仍集中于 4G 部分安全需求的演进以及新技术、新服务驱动的新的安全需求.

2 5G 安全需求

5G 提供的丰富场景服务将实现人、物和网络的高度融合,全新的万物互联时代即将到来.但是,现实空间与网络空间的真正连接也将带来空前复杂的安全问题.各标准化组织和企业联盟达成的共识是,安全需求必须作为系统演进的一部分贯穿于整个 5G 系统的部署与技术更新中.

2.1 延续4G的安全需求

作为 4G 系统的延续,5G 首先应该至少提供与 4G 同等的安全性,这些基本的安全需求主要包括:

(1) 用户和网络的双向认证;
(2) 基于 USIM 卡的密钥管理;
(3) 信令消息的机密性和完整性保护;
(4) 用户数据的机密性保护;
(5) 安全的可视性和可配置性.

其次,还将在 5G 的部署过程中重新考虑一些在旧系统部署中被讨论过但未被采纳的安全性质,主要包括:

(1) 防 IMSI 窃取的保护;
(2) 用户数据的完整性保护;
(3) 服务请求的不可否认性.

最后,5G 面对的设备种类不再单一,为不同的设备颁发一致的身份凭证也不现实,因此,5G 还需要实现从以 USIM 卡为基础的单一身份管理方式到灵活多样的身份管理方式的过渡,以及对所涉及的身份凭证的产生、发放、撤销等整个生命周期内的管理.

2.2 新技术驱动的安全需求

除了提供传统通信系统的基本功能外,5G 还提供一系列基于丰富场景和特殊需求的服务.为了以最有效的方式实现各种不同需求的服务,5G 需要全新的网络架构来进行网络资源的管理和控制.其中,网络功能虚拟化(network functions virtualization,简称 NFV)[30−32]和软件定义网络(software defined networking,简称 SDN)[33]被认为是最有可能实现网络自动化管理以及网络资源虚拟化和网络控制集中化的技术.此外,云计算也被应用于 5G 网络中,用于实现按需的网络控制和定制化的客户服务.

具体来说,NFV 技术的核心思想是:解除网络功能对特定硬件供应商的依赖关系,实现软件和硬件的独立,并根据需要实现网络功能的灵活部署.SDN 技术的核心思想是:将网络架构分离成应用、控制和转发的三层架构,以实现网络的集中管控和网络应用的可编程性.而云计算提供的分布式计算和虚拟化等特性则能够实现网络的高效计算和灵活部署.为了更好地实现对差异化服务的支持,5G 网络需要基于 NFV 和 SDN 将网络分割成多个虚拟的端到端网络,即网络切片,使得在不同网络切片内从设备到接入网再到核心网逻辑独立.每个切片按照业务场景的需要进行网络功能的定制剪裁和相应网络资源的编排管理,为特定类型的业务提供最佳的使用体验.

因此,传统网络中依赖于物理设备隔离来提供安全保障的方式在 5G 网络中不再适用.5G 必须考虑由 NFV 和 SDN 等新技术带来的基础设施安全问题,例如 NFV 中虚拟化管理层的安全问题、虚拟 SDN 控制网元和转发节点的安全隔离问题等,从而保障 5G 业务在虚拟化环境下的安全运行.

2.3 垂直行业服务驱动的安全需求

垂直行业的应用将是5G发展的一个重要方向,不同的垂直行业对安全的需求差异极大,有些服务选择基于 5G 网络本身提供的安全保障,而有些服务则希望保留自身系统对安全的控制.在 5G 环境下,不同的安全需求很有可能作为一种服务,因而,安全即服务(security-as-a-service,简称 SECaaS)的架构必然会出现.所以,5G 网络应提供更加灵活的安全配置,允许运营商或者服务提供商在 5G 系统以外寻求独立的安全保障.此外,不同垂直行业之间的安全配置应保证一定的隔离,以防止服务资源在不同服务之间被非授权访问.

随着垂直服务行业的兴起,我们的心情、健康水平、喜好以及其他更为隐私的信息将被精确地获取或者模糊地感知,个人隐私和关键数据的安全问题将会加剧.在 5G 这样覆盖范围广的网络中,小的安全问题很有可能引起戏剧性的蝴蝶效应,所以 5G 还需要严格控制主要数据的获取、传输、存储和处理等各个环节的可访问性,制定周全的隐私保护策略,以保护用户的身份、位置、接入服务等不被泄露.

此外,5G 还需要建立自动化的安全监控和安全策略配置机制,以及时检测并防范未知的安全威胁,维护有效的安全保护策略,并根据网络状况和资源使用情况动态更新安全策略,始终保证为服务和应用提供最优的性能和用户体验.

总之,提供灵活的安全策略、一定的安全隔离、全面的隐私保护和自动化的安全配置机制将是 5G 安全应用于垂直服务行业的前提.因此,5G 需要在传统接入安全、传输安全的基础上,考虑新技术驱动和垂直服务产业下灵活多变和个性化的服务安全,以实现不同利益群体在不同应用场景下的多级别安全保障.

3 5G 安全框架

安全框架是将系统的安全需求分而治之的一种处理方式.目前,4G 的安全框架[34]无法完全地刻画 5G 的安全需求:首先,4G 的信任模型不适用于 5G,5G 引入新的利益相关者(如服务提供商和新型的设备)使得 4G 的信任模型不再完整;其次,虚拟化及其管理也并不存在于 4G 安全框架中,因而无法准确地展示新系统对虚拟化方面的安全需求;最后,垂直服务行业,尤其是涉及健康、交通、工业自动化控制等服务需要考虑新的安全威胁因素.

尽管 3GPP 目前还未给出 5G 的安全框架,但结合 IMT-2020(5G)推进组和 5G PPP 最新的安全白皮书可以得到一个较为合理的 5G 安全框架(如图 2 所示).该框架以 4G 的安全框架[34]为基础,涉及 5G 的 6 个域的安全.

(1) 接入安全域.接入安全域关注设备接入网络的安全性,主要目标是保证设备安全地接入网络以及用户数据在该段传输的安全性.该域通过运行一系列认证协议来防止非法的网络接入,在此基础上提供一些完整性保护和加密等安全措施,以保护通信内容在无线传输路径上免受各种恶意攻击.在 5G 中,服务网络由底层的公共服务结点和独立的网络切片组成,设备的接入安全包括设备与服务网络公共结点直接交互的信令安全,也包括设备与网络切片的信令和数据交互的安全;

(2) 网络安全域.网络安全域关注接入网内部、核心网内部、接入网与核心网以及服务网络和归属环境(网络)之间信令和数据传输的安全性;

(3) 用户安全域.用户安全域关注设备与身份标识模块之间的双向认证安全,在用户接入网络之前确保设备以及用户身份标识模块的合法性以及用户身份的隐私安全等;

(4) 应用安全域.应用安全域主要关注用户设备上的应用与服务提供方之间通信的安全性,并保证所提供的服务无法恶意获取用户的其他隐私信息;

(5) 可信安全域.可信安全域关注用户、移动网络运营商和基础设施提供商之间的信任问题,也包括用户根据不同的信任强度选择符合服务条款的安全措施(即安全机制可配置性的安全)和垂直服务将信任关系授权给第三方实体等;

(6) 安全管理域.由于 5G 安全需求繁多复杂,5G 需要同时应对多种不同层级的安全诉求.为了保证 5G 的整体安全,安全管理域需要在监测和分析的基础上为系统维护者提供全局的系统安全视角,例如密钥管理和安全编排(orchestration)[35],其中,密钥管理关注密钥的派生、更新等问题的安全性,安全编排则是由于网络切片引入的安全要求.

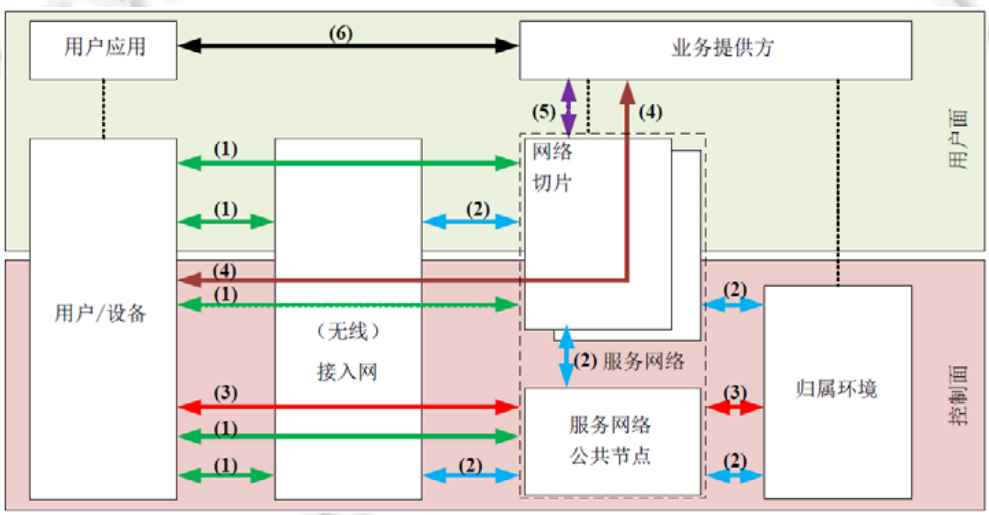

Fig.2 5G Security framework

图 2 5G 安全框架

4 5G 安全关键问题与挑战

随着 5G 网络架构的变化和应用场景的丰富,与传统通信网络相比,5G 所面临的安全问题和挑战也纷繁复杂,可根据安全框架归纳为以下几部分内容.

4.1 接入安全

接入控制在 5G 安全中扮演非常重要的角色,起到了保护频谱资源和通信资源的作用,也是为设备提供 5G 服务的前提.不同于 4G 同构的网络接入控制(即,通过统一的硬件 USIM 卡来实现网络接入认证),5G 对各种异构接入技术和异构设备的支持使得 5G 的接入控制面临巨大的挑战.具体来说,5G 亟待解决的问题主要有:

(1) 用户/设备认证[36].

(i) 跨越底层异构多层无线接入网的统一认证框架:来自不同网络系统(5G,4G,3G,WiFi)、不同接入技术、不同类型站点(宏小区/小小区/微小区)的并行/同时接入将成为常态.因此,需要采用统一的认证框架,实现适用于各种应用场景下的灵活且高效的双向认证,并建立统一的密钥体系;

(ii) 海量终端设备的频繁接入:5G 支持的垂直行业将使用大量的物联网设备,与传统终端不同的是,物联网设备总量大,计算能力低,并具有突发性的网络接入特征.因此,需要专门面向物联网设备研发更高效的接入认证机制;

(2) 抗拒绝服务攻击.拒绝服务(denial-of-service,简称 DoS)攻击的目的是使网络资源被耗尽而无法提供正常的服务.在 5G 中,黑客如果利用海量物联网设备对网络发起分布式拒绝服务攻击,对网络造成的危害将比传统终端带来的危害更大.限制或阻止对资源的过度请求,可以一定程度避免 DoS 攻击;但另一方面,尽量减少每次请求对网络资源的消耗,也将是缓和 DoS 攻击的一种措施.如何避免 DoS 攻击,也将成为 5G 网络未来的一个重要研究内容.

4.2 网络安全

网络切片安全问题是网络安全域最重要的问题.网络切片是一组网络功能、运行这些网络功能的资源以及这些网络功能的特定配置组成的集合,3GPP 的文档 TR 23.799[37]定义了网络切片的一系列功能及特征.网络切片可以视为基于共享基础设施但服务于特定业务的专用网络,也可以看作是网络在逻辑上的特定实例化.网络切片本身可以定制,因此也能够最大程度减少资源消耗、节省成本,并提高服务质量.5G 网络根据网络切片实现的功能可划分为功能型切片(例如无线接入网络切片、核心网切片)和服务型切片(例如电话切片、任务关键的物联网切片).切片体现了 5G 网络的灵活性,然而 5G 需要为网络切片提供持续的安全隔离机制,并能为用户或者基础设施运营商提供有效的隔离证明.因为一方面,由一个网络切片管理的敏感数据可能通过一些侧信道攻击被运行于另一个网络切片中的应用获得;另一方面,一个切片内部的错误和故障也会对其他切片产生影响.此外,网络功能在不同切片之间的共享,基础网络功能与第三方提供的网络功能在切片内的共存等都对安全提出了新的挑战.

4.3 用户安全

用户隐私保护是用户安全域最重要的问题.由于5G提供的业务种类繁多,开放的网络架构使得用户数据及个人隐私信息面临更严峻的考验.在传统的通信网络中(主要是 3G 和 LTE),用户的长期身份标识(Int'l mobile subscriber identity,简称 IMSI)在用户首次向网络进行认证的时候会直接以明文的形式在信道中传输,导致了用户身份隐私的破坏.5G 系统设计需要避免 IMSI 窃取攻击,保证接入设备在任何时候的隐私安全.另外,由于 5G 接入网络包括 LTE 接入网络,攻击者有可能诱导用户至 LTE 接入方式,从而导致针对隐私性泄露的降维攻击,5G 隐私保护也需要考虑此类安全威胁.5G 面临的隐私问题不仅仅是用户身份信息的隐私,还包括用户使用网络过程中产生的一系列与人身、财产相关的多种隐私信息.因此,NGMN[26]指出,必须将隐私保护作为网络本身提供的一种安全属性.同时,5G PPP 的子项目 5G-ENSURE[38]也指出隐私保护的社会影响力,3GPP 也创建了多个文档专门分析用户隐私及其影响,如 TR33.849[39],TR22.864[40]等.

4.4 应用安全

与前几代移动通信网络不同,5G 支持海量物联网设备连接,但物联网设备通常频繁地发送小数据包,这势必造成接入网与核心网之间信令的频繁交互,从而消耗网络带宽,造成传输效率下降.5G 需要确保小数据的通

信安全,针对机器类终端进行高效的连接设计,在满足小数据信令和数据包传输需求的基础上,确保信令和数据传输的安全性,如隐私保护和完整性保护.

4.5 可信安全

5G 网络为了优化用户体验、提供新型商业模式,将向大量第三方应用开放网络,借此实现网络和第三方应用的互动,并优化网络资源配置.首先,5G 将提供一些网络功能如移动性、会话、QoS 和计费等功能的接口,方便第三方应用独立完成网络基本功能.此外,5G 还将开放 MANO(管理和编排),让第三方服务提供者可以独立实现网络部署、更新和扩容等网络编排能力,最终实现动态地定制网络.以上面向第三方开放的能力都是 5G 网络的基本功能,如果在开放授权过程中出现信任问题,则恶意第三方将通过获得的网络操控能力对整个 5G 网络发起攻击.此外,随着用户(设备)种类增多、网络虚拟化技术的引入,用户、移动网络运营商和基础设施提供商之间的信任问题也比以前的网络更加复杂.

4.6 安全管理

(1) 安全上下文与密钥管理

安全上下文(security context)是网络为设备建立的临时状态信息,其中包括密钥信息和数据承载信息,目的是减少设备在不同状态之间切换时与网络进行相互认证的资源消耗,方便设备快速从空闲状态安全切换到连接状态并安全通信.5G 中,设备移动、设备在不同接入网之间切换均需要考虑安全上下文的迁移和管理,迁移过程中,不同的网络对密码算法的支持情况也不同,涉及算法的重协商、上下文的标识和存储安全.此外,小数据通信模式下,安全上下文受限于设备的计算能力,也需要全新的处理方式.

在密钥管理方面,由于 5G 应用场景丰富,5G 的密钥种类呈现多样化的特点,具体包括专门用于控制平面和用户平面的机密性/完整性保护密钥、用于保护无线通信端信令和消息传输的密钥、用于支持非 3GPP 接入的密钥、用于保证网络切片通信安全的密钥以及用于支持与 LTE 系统后向兼容的密钥,等等.这一系列密钥既需要保持整体系统的统一性,又需要具备一定的独立性,以确保每个部分的安全性互不影响.此外,5G 用户种类多样并包括各种设备,5G 还将提供基于非对称密钥、基于生物信息等的用户身份识别技术.因此,5G 的密钥管理将比 4G 更为复杂,难度也更大.

(2) 安全编排

编排是通过一个中心控制节点来协同业务流程中的各种事件/活动,以达到控制总体的作用.编排的特点是服务可以连接服务,即,一个服务的输出可作为另一个服务的输入,因此能实现服务组合,创造出新的业务模型,最终满足不断变化的市场和用户需求.编排简单来讲是一种自动化的控制理论,在面向服务的架构(SOA)、平台虚拟化、融合的基础设施等领域被广泛使用.5G 在关键技术 SDN 和网络切片中大量使用编排来灵活地提供服务.3GPP 的文档 TR 28.801[41]和 NGMN 的网络服务管理白皮书[42]还就 5G 网络切片管理和编排(MANO)的一些问题进行了研究.管理和编排过程复杂,最基本的安全需求是保证各服务之间共享资源的关联性和一致性.此外,编排决定了网络/特定服务的拓扑结构,编排本身将决定在何处部署安全机制和安全策略.5G 系统需要在编排过程中提供足够的安全保证.

(3) 证书管理

5G 将引入公钥基础设施(public key infrastructure,简称 PKI)来加强用户身份的机密性保护以及网络各节点之间的相互认证.PKI 的引入使得系统必须维护庞大的 CA 系统,一方面对 CA 容量要求高;另一方面,将面临一系列证书管理的开销,如大量并发的证书申请、证书更新、证书撤销等操作.因此,5G 必须加快促进 CA 技术的发展,并将其高效地部署在 5G 系统中.此外,5G 也面临着 PKI 升级换代所带来的安全挑战和影响.

4.7 密码算法

密码算法是保证安全通信的关键组件,LTE 系统采用的一系列对称密码算法包括 SNOW 3G,ZUC[43],AES 等目前均不存在安全性问题,但随着量子计算技术的发展,5G 需要结合未来的发展趋势扩展密钥长度,并考虑算法的量子安全性,因此需要改进提高密码算法的适应性.与此同时,4G 中的大量算法计算代价大,与 5G 绿色节

能的基本要求存在一定的冲突,5G 必须考虑一系列轻量级密码算法.但 3GPP 还建议使用大量的公钥密码算法如 DHIES[44,45]及其 ECC 上的变形 ECIES、基于身份的加密(IBE)[46]和基于属性的加密(ABE)[47],这些算法随着量子计算技术的发展会遇到极大的安全挑战,应尽早做好替代准备工作.

5 5G 安全解决方案

5.1 统一的认证框架

为了解决异构接入技术和设备接入网络的问题,3GPP 在 R15 的文档 33.899[24]中给出了将可扩展认证协议(extensible authentication protocol,简称 EAP)框架,用作 5G 通用认证框架备选方案的具体描述.框架适用于任何类型的订阅者以任何一种 3GPP 定义的接入技术(包括 3G,4G)和非 3GPP 定义的接入技术(包括 WiFi,WiMAX)进行接入网认证.EAP 认证框架由 RFC 3748[48]定义,是一种支持多种认证方法的三方认证框架,框架本身不提供任何安全性,只规定了消息的封装格式,具体的安全目标依赖于使用的认证方法.目前,EAP 支持的认证方法有 EAP-MD5,EAP-OTP,EAP-GTC,EAP-TLS,EAP-SIM 和 EAP-AKA,还包括一些厂商提供的方法和新的建议.在 5G 中,具体的 EAP 协议运行于 UE,AUSF(相当于后端服务器)和 SEAF(相当于前端认证器)之间.

5.2 基于群组的海量IoT设备认证方案

认证数量庞大的 IoT 设备,对确保 5G 安全是一个巨大的挑战.群组认证协议可以一次性认证一组设备,能够有效降低系统的计算、通信和存储代价.目前,5G-ENSURE 给出了一种基于可逆 Hash 树的新型群组 AKA 协议的构造[49].该方案基于树结构存储设备的主密钥,可以一次性认证多个 IoT 设备,并能够动态地在前端认证器的计算量与后端服务器的通信量之间进行调整,可直接部署到现有的通信系统中,且通过形式化工具 ProVerif 的验证,可以提供设备与网络的双向认证、密钥的机密性、设备的隐私性等安全性质.

5.3 丰富的密钥层级架构

3GPP 在文档 TR 33.899[24]中给出了根据 3GPP 对 5G 密钥层级基本要求而整理的两种密钥架构候选方案.两种方案的差别不大,在每种方案中又各自存在两种变形,其中,候选方案 1(包括两种变形)如图 3 所示.

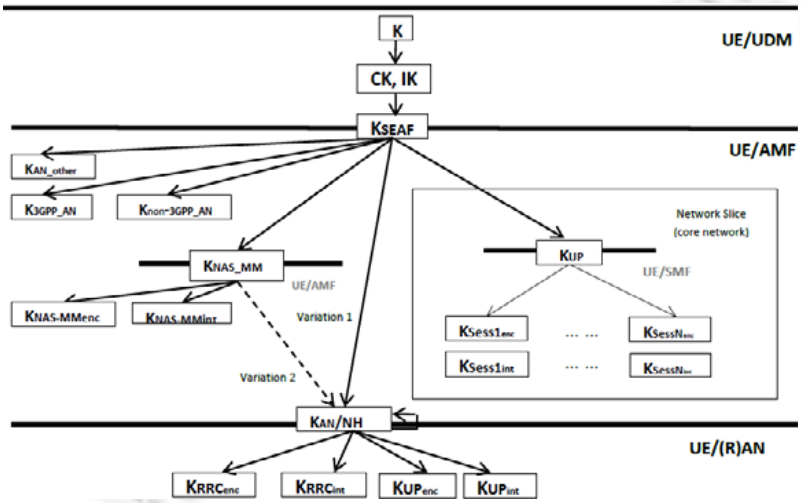

Fig.3 Keyhierarchy of 5G

图 3 5G 密钥层级候选方案

5G 基本延续了 4G 的密钥派生方式,如根密钥 K 为用户(UE)与核心网络的统一认证数据管理(UDM)共享的长期密钥,整个密钥派生系统依赖于这一密钥.密钥层级的第 2 层是加密算法密钥(confidentiality key,简称 CK)和完整性保护算法密钥(integrity key,简称 IK),是为了后向兼容而保留的密钥;在 CK 和 IK 的基础上,密钥层

级的第 3 层为 K_{SEAF},该密钥相当于 LTE 系统的 K_{ASME},主要用于在 UE 和 AMF(接入和移动管理功能)之间进行 UE 的移动管理和会话管理的密钥派生.以 K_{SEAF} 为基础,派生 3 类密钥.

(1) 非接入层移动管理密钥,主要包括 K_{NAS_MM} 以及在此基础上派生的非接入层移动管理加密密钥 $K_{NAS\text{-}MMenc}$ 和完整性保护密钥 $K_{NAS\text{-}MMint}$;

(2) 接入网络密钥 K_{AN}(两种变形体现在该密钥的派生方式上,具体差别见图 3)以及在此基础上派生的 RRC 层加密密钥 K_{RRCenc},RRC 层完整性保护密钥 K_{RRCint},用户平面加密密钥 K_{UPenc} 和用户平面完整性保护密钥 K_{UPint};

(3) 用户向网络切片请求服务时的密钥 K_{UP} 以及在此基础上为每个特定的会话 j(j=1,…,N)派生的会话加密密钥 $K_{Sessjenc}$ 和会话完整性保护密钥 $K_{Sessjint}$.

与 LTE 系统的密钥层级相比,5G 系统的密钥丰富了很多,除了以上的密钥类型,还包括为实现后向兼容而保留的接入网络密钥如 K_{3GPP_AN} 和 $K_{non\text{-}3GPP\_AN}$、为支持一些 3GPP 未考虑的接入网络引入的接入网络密钥 K_{AN_other}.

5.4 基于标识的切片安全隔离

网络切片是5G的重要组件,它使得运营商可以根据不同的市场情景和丰富的需求定制网络,以提供最优的服务.一个网络切片是一系列为特定场景提供通信服务的网络功能的逻辑组合.网络切片本身是一种网络虚拟化技术,因此,不同切片的隔离是切片网络的基本要求.为了实现切片隔离,每个切片被预先配置一个切片 ID,同时,符合网络规范条件的切片安全规则被存放于切片安全服务器(slice security server,简称 SSS)中,用户设备(user equipment,简称 UE)在附着网络时需要提供切片 ID,附着请求到达归属服务器(home subscriber server,简称 HSS)时,由 HSS 根据 SSS 中对应切片的安全配置采取与该切片 ID 对应的安全措施,并选择对应的安全算法,再据此创建 UE 的认证矢量,该认证矢量的计算将绑定切片 ID.通过以上步骤,来实现切片之间的安全隔离.

网络切片本身是一个复杂的系统,切片之间由于共享基础设施或共同协作实现更高级别的功能,使得切片之间的通信安全也至关重要.目前对这个问题的研究仍然处于初级阶段,随着 5G 网络架构的不断完善,这个问题在未来的研究中必将得到合理的解决.

5.5 基于多种身份凭证的隐私保护

网络服务订阅者的隐私在下一代网络中将面临更多安全威胁,3GPP 给出了一些隐私保护解决方案.首先,由于用户在初次访问网络之前的附着阶段还未能与网络协商出任何密钥,其长期身份标识也无法进行任何加密保护.为了避免用户长期身份标识的泄露,5G 网络将为网络核心组件配备公钥,用户在需要向网络中的认证实体发送长期身份标识时,以接收方的公钥对身份标识进行加密,从而保护长期身份信息不遭受敌手的窃听攻击.3GPP 在 TR33.899 中给出的推荐加密方案是 DHIES[44,45]及其 ECC 上的变形 ECIES.此外,3GPP 还给出基于身份的加密(IBE)[46]和基于属性的加密(ABE)[47]的解决方案,直接加密用户的身份标识或者用一个与公共属性绑定的私钥和全局公钥加密身份标识.

5.6 移动边缘计算

移动边缘计算(mobile edge computing,简称 MEC)技术[50]由国际标准组织 ETSI 提出,是在移动网边缘提供 IT 服务环境和云计算能力的技术.MEC 技术的核心思想是:将对带宽和时延要求严格的业务数据的计算、处理和存储推向无线侧,以减少网络操作和服务交付的时延消耗,提高用户的使用体验.目前,3GPP 和 NGMN 均成立了专门的工作组来进行 MEC 的相关研究.MEC 通过对数据包的深度包解析(DPI)[51]来识别业务和用户,并进行差异化的无限资源分配和数据包的时延保证.MEC 服务器可以部署在网络汇聚结点之后,也可以部署在基站内,所有通过基站的数据包都将通过 MEC 服务器的数据包解析,并由 MEC 给出是否进行本地分流的决策,不能本地处理的数据则由 MEC 传递给核心网处理.但目前,MEC 依赖的底层 DPI 技术对 HTTPS 的数据包的解析还不够成熟,而未提交至核心网的数据流量计费功能也存在问题.因此,MEC 技术还存在诸多难点有待解决.各大标准组织正在努力推动 MEC 的标准化工作,并尽可能解决现阶段 MEC 技术引入带来的部署问题,实现从 4G

到 5G 的平滑过渡.

6 小 结

5G 作为新一代移动通信网络基础设施,安全成为支撑其健康发展的关键要素.目前,5G 仍处于初期研究阶段,系统架构和许多关键技术尚未完全确定.因此,5G 带来的安全问题仍然有很多不确定性因素.在 5G 网络的整体架构设计、业务流程、算法和后续标准化工作中,将 5G 的安全需求作为研究重点,有助于整体把握 5G 系统安全要求而避免后期对系统和方案的再调整,最终实现构建更加安全可信的 5G 网络的目标.本文从 5G 的愿景、安全需求、安全框架等角度出发,详细阐述了目前 5G 面临的安全挑战以及关键安全技术.

总体来说,当前国内外针对 5G 安全的研究还不够充分,仍然面临一些亟待解决的问题:(1) 设计灵活可扩展的 5G 安全架构,以满足 5G 支撑的各类新兴的业务模式需求;(2) 提供差异化隐私保护能力,实现对隐私信息保护范围和保护强度的灵活选择;(3) 设计安全高效的密码算法和认证协议,为 5G 网络提供安全基础保障;(4) 实现多层次的切片安全,为 5G 网络不同业务提供安全分级服务;(5) 研究新型的漏洞检测方法,以避免 5G 带来的便利服务为攻击者所恶意利用.

References:

[1] http://www.itu.int/en/ITU-R/information/Pages/default.aspx

[2] http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx

[3] 3GPP. 3G security, security architecture. Technical Specification, TS 33.102 v12.1.0, 2014.

[4] http://www.3gpp.org

[5] IMT-2020 (5G) Promotion Group. 5G wireless technology architecture. White Paper, 2015 (in Chinese).

[6] IMT-2020 (5G) Promotion Group. 5G network technology architecture. White Paper, 2015 (in Chinese).

[7] ITU-R. IMT-vision-framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation, ITU-R M.2083-0. 2015. http://www.itu.int/rec/R-REC-M.2083

[8] http://www.3gpp.org/release-14

[9] http://www.3gpp.org/release-15

[10] https://5g-ppp.eu

[11] http://www.ngmn.org/home.html

[12] https://www.gsmaintelligence.com

[13] 5G PPP. View on 5G architecture. White Paper, v 1.0, 2016.

[14] NGMN. NGMN 5G white paper. 2015. http://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[15] GSMA Intelligence. Understanding 5G: Perspectives on future technological advancements in mobile. 2014.

[16] IMT-2020 (5G) Promotion Group. 5G vision and requirements. White Paper, 2014 (in Chinese).

[17] IMT-2020 (5G) Promotion Group. 5G concept. White Paper, 2015 (in Chinese).

[18] IMT-2020 (5G) Promotion Group. 5G network architecture design. White Paper, 2016 (in Chinese).

[19] IMT-2020 (5G) Promotion Group. 5G network security requirements and architecture. White Paper, 2017 (in Chinese).

[20] Ericsson. 5G system—Enabling the transformation of industry and society. White Paper, 2017. https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-systems.pdf

[21] Samsung Electronics Co. 5G vision. White Paper, 2015. http://www.samsung.com/global/business-images/insights/2015/Samsung-5G-Vision-2.pdf

[22] Nokia. Now is the time to prepare for 5G. White Paper, 2013.

[23] Huawei Technologies Co. 5G opening up new business opportunities. White Paper, 2016.

[24] 3GPP. Study on the security aspects of the next generation system. Technical Report, TR 33.899 v1.1.0, 2017.

[25] 5G PPP. 5G PPP phase 1 security landscape. 2017. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[26] NGMN. 5G security recommendations (package #1, package #2: networking slicing, package #3: mobile edge computing). White Paper, 2016.

[27] Ericsson. 5G security—Scenarios and solutions. White Paper, 2017.

[28] https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-security.pdf

[29] Nokia. Security challenges and opportunities for 5G mobile networks. White Paper, 2017.

[30] Huawei Technologies Co. 5G security: Forward thinking. White Paper, 2015. http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf

[31] ETSI. Network functions virtualization (NFV); Terminology for main concepts in NFV. Group Specification, NFV 003 v1.1.1. 2013.

[32] ETSI. Network functions virtualization (NFV); Use cases. Group Specification, NFV 001 v1.1.1. 2013. http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf

[33] ETSI. Network functions virtualization (NFV); Proof of concepts; Framework. Group Specification, NFV-PER 002 v1.1.2. 2014. http://www.etsi.org/deliver/etsi_gs/NFV-PER/001_099/002/01.01.02_60/gs_NFV-PER002v010102p.pdf

[34] Evangelos H, Kostas P, Spyros D, Hadi SJ, David M, Odysseas K. Software-Defined networking (SDN): Layers and architecture terminology. IETF RFC 7426. 2015.

[35] 3GPP. 3GPP system architecture evolution; Security architecture. Technical Specification, TS 33.401 v15.0.0, 2017.

[36] https://en.wikipedia.org/wiki/Orchestration_%28computing%29

[37] Gnther H, Peter S. Towards 5G security. In: Proc. of the 14th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. Helsinki, 2015. 1165−1170. [doi: 10.1109/Trustcom.2015.499]

[38] 3GPP. Study on architecture for next generation system (release 14). Technical Report, TR 23.799 v14.0.0, 2016.

[39] 5G-Ensure Deliverable D3.5. 5G-PPP security enablers technical roadmap (update). 2016. http://5gensure.eu/sites/default/files/5G-ENSURE_D3.5%205G-PPP%20security%20enablers%20technical%20roadmap%20%28Update%29.pdf

[40] 3GPP. Study on subscriber privacy impact in 3GPP. Technical Report, TR 33.849 v14.0.0, 2016.

[41] 3GPP. Feasibility study on new services and markets technology nnablers—Network operation. Technical Report, TR 22.864 v15.0.0, 2016.

[42] 3GPP. Study on management and orchestration of network slicing for next generation network. Technical Report, TR 28.801 v1.2.0. 2017.

[43] NGMN. 5G network and service management including orchestration. White Paper, v2.12.7. 2017.

[44] 3GPP. Specification of the 3GPP confidentiality and integrity algorithms EEA3 and EIA3, document 4: Design and evaluation reprot. Technical Specification, TR 35.924 v11.0.1, 2012.

[45] Michel A, Mihir B, Phillip R. DHAES: An encryption scheme based on the Diffie-Hellman problem. IACR Cryptology ePrint Archive. 1999. 7.

[46] Michel A, Mihir B, Phillip R. The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Proc. of the Cryptographers' Track at RSA Conf. San Francisco, 2001. 143−158. [doi: 10.1007/3-540-45353-9_12]

[47] Dan B, Matt F. Identity-Based encryption from the Weil pairing. In: Proc. of the 21st Annual Int'l Cryptology Conf. Santa Barbara, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[48] Amit S, Brent W. Fuzzy identity based encryption. IACR Cryptology ePrint Archive. 2004. 86.

[49] Bernard A, Larry BJ, John VR, James C, Henrik L. Extensible authentication protocol (EAP). IETF RFC 3748, 2004.

[50] Rosario G, Christian G, Markus A, Simon H. A secure group-based AKA protocol for machine-type communications. In: Proc. of the 19th Annual Int'l Conf. on Information Security and Cryptology. Seoul, 2016. 3−27. [doi: 10.1007/978-3-319-53177-9_1]

[51] ETSI. Mobile edge computing—A key technology towards 5G. White Paper, ISBN No. 979-10-92620-08-5. 2015. http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

[52] https://en.wikipedia.org/wiki/Deep_packet_inspection

附中文参考文献:

[5] IMT-2020(5G)推进组.5G 无线技术架构.白皮书,2015.

[6] IMT-2020(5G)推进组.5G 网络技术架构.白皮书,2015.
[16] IMT-2020(5G)推进组.5G 愿景与需求.白皮书,2014.
[17] IMT-2020(5G)推进组.5G 概念.白皮书,2015.
[18] IMT-2020(5G)推进组.5G 网络架构设计.白皮书,2016.
[19] IMT-2020(5G)推进组.5G 网络安全需求与架构.白皮书,2017.

冯登国(1965－),男,陕西靖边人,博士,研究员,博士生导师,主要研究领域为网络与信息安全,可信计算与信息保障.

徐静(1972－),女,博士,研究员,博士生导师,主要研究领域为应用密码学,安全协议.

兰晓(1990－),女,博士,主要研究领域为安全协议.