网络安全——5G的基石

Keystone for 5G: Network Security

苏洲/SU Zhou

（西安交通大学，陕西 西安 710049）
(Xi'an Jiaotong University, Xi'an 710049, China)

DOI：10.12142/ZTETJ.201904010
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.tn.20190708.1915.002.html
网络出版日期：2019-07-09
收稿日期：2019-06-10

摘要：随着移动通信和智能设备的迅速发展，5G通信网络以其高速率、广连接、低时延引发了新一代的信息网络变革。如何建立可信、可靠、可管的5G通信网络面临一系列网络安全挑战。网络空间安全已成为5G通信网络发展的基石所在。在回顾网络安全技术发展的基础上，探讨了5G通信网络面临的新型安全问题，并结合用户隐私保护、信任管理和数据存储3个方面研讨了相应的网络安全保护策略。

关键词：5G通信网络；网络安全；用户隐私保护；信任管理；数据存储

Abstract: With the rapid development of mobile communication and intelligent devices, the 5G network has emerged as a new revolution for information networks, which can provide high speed, wide connection and low delay to improve the quality of service for mobile users. How to establish the credible, reliable and manageable 5G communication network faces a series of network security challenges, which are keystones for 5G communication. In this paper, the security problems in the 5G communication network are discussed, and the corresponding network security solutions including privacy protection, trust management and data storage are studied.

Key words: 5G communication network; network security; user privacy protection; trust management; data storage

1 移动网络安全发展

从古代的飞鸽传书到今日的第5代通信技术（5G），通信与人类历史的发展紧密相关。尤其是近几十年来，随着无线通信技术的快速发展和不断变革，移动网络从基于模拟信号的第1代通信技术（1G）逐渐发展到基于数字信息的5G，业务类型也从单一的语音通话转变到语音、数据、多媒体等综合业务并行发展。与此同时，通信网络安全问题也逐渐地引起了人们的广泛关注和讨论。

1G作为第1代的移动通信技术，其网络安全也处于起步阶段。1G移动通信系统的语音业务基于模拟信号，每一个语音通话都会在无线电发射塔中回放，使得语音通话有可能受到第三方的窃听、劫持或篡改[1]。第2代通信技术（2G）主要是基于全球移动通信系统（GSM）的语音业务，其网络安全主要面向语音通话应用[2]。2G通信网络利用GSM数字信息进行信息交换和数据传输。GSM可实现基于共享秘钥的用户认证、基于A5/1和A5/2流秘密无线通信加密、基于用户身份识别卡（SIM）安全模块的用户身份保密等网络初步安全[1]。

第3代通信技术（3G）除了提供语音业务外，还支持多媒体业务、数据业务等多种信息业务，从而提供了支持语音和数据并重的业务环境。该业务环境给通信网络系统提出了新的安全特性需求。3G通信网络安全措施主要有用户身份认证、消息认证和机密、无线借口存取控制等[2]。第4代通信技术（4G）网络与2G、3G网络相比，在传输速率、通信质量及稳定效果等多个关键点都获得了突破性进展。与传统网络相比，4G出现了多项新技术来提升网络服务的安全性：在无线接入网方面，4G网络通过安全传输、安全接入、身份认证、安全信息数据过滤、访问控制等方式提升了接入网安全性能；在移动智能终端方面，4G网络利用物理硬件防护、强化操作系统等方式在保护网络设备安全上取得了一定进展[3]。

2 5G通信网络安全挑战

5G网络的服务多样性使其不

再局限于个人用户，它不仅能为智能终端提供更快的通信速率或更丰富的功能，还将服务于移动物联网等垂直行业，并衍生出多种新服务和新应用。由于不同垂直行业的业务目标不同，5G网络服务之间的安全需求也有较大差异。例如，移动物联网设备要求轻量级网络安全，而高速移动服务要求高效移动安全，因此，基于网络的逐跳安全的保护方法无法为多样化的服务构建差异化的端到端通信安全。随着物联网的蓬勃发展，越来越多的人能够远程操作联网设备或与联网设备“交谈”。例如，指示智能家居的启动和关闭。因此，在5G网络中，需要更严格的网络安全维护方法来有效应对诸如物联网设备未经授权的访问等带来的网络安全课题[4]。

虚拟与现实是5G的另一热点。以网络功能虚拟化（NFV）/软件定义网络（SDN）为代表的相关技术被广泛应用于5G网络中来提供更灵活、更高效、更低成本的相关网络服务。虽然NFV与SDN提高了5G网络的效率和性能，但新的安全问题也随之产生。传统网络中，网络节点的安全性很大程度上取决于它们物理实体间的隔离程度。然而，在5G网络中，NFV技术使得部分网络节点以虚拟网络节点的形式部署在基于云处理器的基础设施上。因此，为了保证5G业务在VNF环境中的安全运行，需要开发出更可靠的隔离方法和技术。SDN技术的应用可以提高5G网络数据传输速率，优化资源配置。但在5G环境中，也需要考虑SDN控制虚拟网络节点和转发节点的安全隔离策略和可信管理方案，并保证SDN流表的可靠性和执行的准确性。

异构性是5G网络的另一主要技术特征。异构性不仅体现在诸如WiFi和长期演进（LTE）等接入技术的不同，还体现在接入网络架构的差异化和多样化；因此，5G网络需要构建综合安全机制，在多样化的接入技术和接入网络架构上建立安全的服务网络。物联网设备在5G网络接入方式上有多种选择，如设备直接连接网络，通过接入点汇聚后连接到网络，或通过设备到设备（D2D）、中继等方式连接到网络；因此，5G物联网设备和网络之间需建立准确的信任关系，需要高效、轻量级的安全管理方式。

5G网络还具有深度推广性，包括远程医疗、智能家居、智能交通在内的越来越多的垂直产业将采用5G网络。作为开放的平台，5G网络引起了人们对隐私泄露的密切关注。移动通信网络作为网络访问的主要方式，承载着大量的个人隐私信息（如身份、位置和隐私内容）的数据和信令。为了提供差异化的服务质量，网络可能需要感知用户使用的服务类型，而服务类型往往涉及用户隐私，有产生用户隐私泄露风险。因此，为了保护用户隐私，5G网络需要提供更加严密和广泛的保护技术。

3 5G通信网络安全举措

3.1 隐私保护机制

以5G通信网络内容分发为例，例如在微信好友间的图片、视频的分享和传递过程中，移动用户在本地生成内容，然后将内容上传到内容分享服务器，最后内容请求用户可以从内容分享服务器中获取所需的内容。然而，由于用户产生的内容往往包含用户位置隐私信息，内容分享后易造成隐私泄露。若恶意用户或者不可信服务器泄露这些位置隐私信息，会造成用户人身和财产的损失和危害。因此，在5G网络中需要建立合理的隐私保护机制来避免用户隐私信息的泄露。

假名变换策略和匿名算法有助于保护5G通信网络中的用户隐私。在5G网络中，移动用户通过不定期变换通信使用的假名，隐藏自己的位置信息与真实身份之间的映射关系，从而防止位置隐私的泄露。在匿名算法中，针对一般用户对不可信内容分享服务商的位置隐私泄露问题，通过将移动用户的真实位置泛化为 k 个在概率上不可区分的位置，使得攻击者获得用户真实位置的概率最高为 $1/k$ ，从而确保移动用户位置的隐私性。

3.2 信任管理机制

5G通信网络中，移动用户可以作为感知节点来感知环境信息。例如，在群智感知中，感知服务请求者向感知服务平台发布感知任务，感知服务平台根据感知任务请求移动用户完成感知任务，移动用户将感知结果返回给感知服务平台，最后感知服务平台将感知结果发送给感知服务请求者。然而，移动用户为了节省资源，获取利益，有可能向感

知服务平台注入虚假或者恶意的感知数据，造成感知结果不准确甚至破坏网络的正常运行。因此，在信息感知服务过程中，需要对参与感知任务的移动用户进行信任分析，选取可信用户的感知数据。

面向5G通信网络，对用户进行信任评估的方法可大致分为以下的2类：

（1）集中式信任管理机制。该机制利用集中式处理器获取信任信息，并实时管理和实现全局的用户信任评估。集中式处理器可以通过统计感知用户任务完成情况来实现信任评估，也可以根据感知服务平台对感知用户的评价来评估用户的信任值。

（2）分布式信任管理机制。该通过模拟现实社会的用户社交关系来建立和维护用户信任信息，将移动用户信任的评估分散到多个不同的实体，并通过实体之间的通信和信任推荐来实现各个实体自主地对移动用户的信任评估。

3.3 灾备缓存机制

无线终端的迅速普及和无线通信技术的快速发展也带来了不容忽视的带宽压力和服务延迟。5G网络通过将内容存放在离用户较近的边缘缓存设备上，降低服务延迟，缓解骨干网络带宽压力。然而，由于网络组网模式异构性和缓存设备可靠性的不一致性，较低可靠性的节点易遭到攻击，缓存内容易遭到篡改和丢失。因此，在5G网络中需要合理的内容缓存机制来确保缓存内容的安全性和缓存服务的可靠性。

基于云服务器的内容灾备机制利用多个云服务器作为边缘缓存设备的灾备服务器，为缓存内容提供协作灾备服务，从而防止缓存内容在边缘缓存服务器上丢失、损坏和篡改。在基于边缘缓存服务器协作的内容灾备机制中，由于边缘缓存服务器的异构性和差异性，多个边缘缓存服务器具有不同的安全性能和缓存性能；因此，多个边缘缓存服务器能够相互协作灾备缓存内容，从而提高单个边缘缓存服务器缓存服务的可靠性，提高缓存内容的安全性。

4 结束语

5G通信网络在新一代通信网络的布局和规划中起着战略性的关键作用。网络安全是保障5G进一步推进、普及和应用的关键所在，用户隐私、信任管理、灾备存储等方面已成为5G网络安全的关键课题和挑战，其核心技术势必会促使相关产业的变革和发展，为人们带来安全、迅速、绿色的5G通信网络体验。

参考文献

[1] PAVIA J, LOPES D, CRISTOVAO P, et al. The Evolution and Future Perspective of Security in Mobile Communications Networks [C]// International Congress on Ultra Modern Telecommunications and Control Systems. Germany: ICUMT. 2017:267–276.DOI:20.1109/ICUMT.2017.8255180

[2] 曹鹏, 文瀛, 黄载禄. 第三代移动通信系统安全[J]. 移动通信, 2001, 1(1): 20. DOI:10.3969/j.issn.1006–1010.2001.01.004

[3] 李炜键, 孙飞. 基于4G通信技术的无线网络安全通信分析[J]. 电力信息与通信技术, 2014, 12(1): 127. DOI:10.3969/j.issn.1672–4844.2014.01.028

[4] IMT–2020(5G)推进组. 5G网络安全需求与架构白皮书[R]. 2017

作者简介

苏洲，西安交通大学网络空间安全学院教授、博导、院长；主要研究方向为物联网信息安全、隐私保护、大数据存储与人工智能关键技术等；主持国家自然科学基金重点项目、重大研究计划培育项目等科研项目；获得IEEE ComSoc GCCTC2018、IEEE CyberSciTech2017、WiCon2016等国际会议最佳论文奖。