



5G 安全的愿景

朱红儒, 庄小君, 郭 姝, 齐旻鹏

(中国移动通信有限公司研究院 北京 100053)

摘 要:随着 4G 的大规模商用,业界对 5G 的研究也正在如火如荼地展开。5G 不仅将给带宽、速率、智能化和融合性等方面带来一定变化,而且随着 5G 新的网络架构演进和网络融合技术的发展,其安全性也将发生相应的变化。为此,探讨了 5G 安全架构、安全关键技术以及 5G 安全机制的未来研究方向。

关键词:5G 安全;大数据;NFV/SDN

doi: 10.3969/j.issn.1000-0801.2014.11.022

Security Vision of 5G

Zhu Hongru, Zhuang Xiaojun, Guo Shu, Qi Minpeng

(China Mobile Research Institute, Beijing 100053, China)

Abstract: With the commercial use of 4G, the research of 5G is being carried out in full swing in the industry. 5G will have a revolutionary change in the bandwidth, speed, intelligence and integration. So on the security front, 5G inevitably will have corresponding change. The security architecture, the security key technologies and the future research direction of the security mechanism of 5G were discussed.

Key words: 5G security, big data, NFV/SDN

1 引言

随着 4G 的大规模商用,业界启动了对下一代网络通信技术 5G 的研究。虽然目前 5G 的概念、架构以及关键技术仍处于探索中,但是可以初步确定,与 2G、3G^[1]、4G^[2]相比,5G 并不是独立而全新的技术,而是对现有移动通信技术(包括 2G、3G、4G 和 WLAN)的结合和进一步发展,在此基础上,5G 还会引入一些补充性的增强技术。除了带给普通用户最直观的网速提升之外,5G 还将满足超大带宽、超高容量、超密站点、超高可靠性、随时随地可接入等要求^[3]。因此,可以认为 5G 是一个广带化、泛在化、智能化、融合化的绿色节能网络。

2 5G 网络架构演进

为了满足千倍流量增长、无感知时延和海量设备连接

的网络发展需求,5G 需要有新的网络架构,从而支持网络管理的自动化、网络资源的虚拟化和网络控制的集中化。目前业界比较认可的 5G 架构演进方向包括两个方面:一是在网络设备上,通过 NFV(network function virtualization,网络功能虚拟化)实现软件和硬件解耦,提高网络资源利用率;二是在网络架构上,通过 SDN (software defined networking,软件定义网络)技术实现控制和转发的进一步分离。

NFV 使得传统的物理网络设备以 VNF (virtualized network function,虚拟网络功能)的方式部署在通用硬件的虚拟机上,灵活实现网络资源的弹性伸缩,加快网络的部署,提升网络的运维管理效率。而采用 SDN 技术将会提升控制面集成度,增强转发面效率。对于网络设备的控制面,将采用集中控制、分布控制或者两者结合的控制方式;对于网络设备的转发面,基站与路由交换等基础设施将具备



可编程的能力,使得网络应用层可以与各种应用场景灵活适配,增强网络的开放性和兼容性。

5G 接入网中可能需要更多的天线数、更高的调制阶数、更强的干扰消除机制等,使得 5G 网络能够支持高密度小区、支持网络容量呼吸和迁移、支持多网融合,进而实现对高密度和新空口的高频数据以及新型移动互联网应用的适配。因此,大规模天线系统、高频段新波形设计、非正交传输和接入技术、同时同频全双工技术、网络架构与信令优化等都将作为 5G 网络架构演进的重要技术。图 1 描述了 5G 网络架构演进的方向,重点突出了 5G 网络中革新的部分,即通过基站池化、核心网云化、网络设备控制面和管理面分离实现 NFV 和 SDN 技术在 5G 网络中的落地,推动 5G 网络架构的演进。

3 5G 安全技术发展方向

3.1 5G 安全架构

2G 的安全架构是单向认证,即只有网络对用户的认证,而没有用户对网络的认证,空口的信令和数据只具备加密保护能力;3G 的安全架构则是网络和用户的双向认证,相比于 2G 的空口加密能力,3G 空口的信令还增加了完整性保护,同时核心网也有 NDS/IP 的网络域安全保护^[4];4G 安全架构虽然仍采取双向认证,但是 4G 使用独立的密钥保护不同层面(接入层和非接入层)的多条数据流和信令流,核心网也使用网络域安全进行保护^[5]。

由于对 5G 提出的高速率、低时延、处理海量终端等要求,5G 安全架构需要从优化保护节点和密钥架构等方面进行演进。

3.1.1 保护节点的演进

在 5G 时代,用户对数据传输的要求更高,不仅对上下行数据传输速率提出挑战,同时也对时延提出了“无感知”

的苛刻要求^[6]。而在传统的 2G、3G、4G 网络中,用户设备(UE)与基站之间提供空口的安全保护机制,在移动时会频繁地更新密钥。而频繁地切换基站与更新密钥将会带来较大的时延,并导致用户实际传输速率无法得到进一步提高,因此在 5G 中必须对此加以改进。5G 网络可考虑从数据保护节点处进行改进,即将加解密的网络侧节点由基站设备向核心网设备延伸,利用核心网设备在会话过程中较少变动的特性,实现降低切换频率的目的,进而提升传输速率。在这种方式下,空口加密将转变为 UE 与核心网设备间的加密,原本用于空口加密的控制信令也将随之演进为 UE 与核心网设备间的控制信令。

此外,5G 时代将会融合各种通信网络,而目前 2G、3G、4G 以及 WLAN^[7]等网络均拥有各自独立的安全保护体系,提供加密保护的节点也有所不同,如 2G、3G、4G 采用 UE 与基站间的空口保护,而 WLAN 则多数采用终端到核心网的接入网元 PDN 网关或者边界网元 ePDG 之间的安全保护。因此,终端必须不断地根据网络形态选择对应的保护节点,这为终端在各种网络间的漫游带来了极大的不便,因此可考虑在核心网中设立相应的安全边界节点,采用统一的认证机制解决这一问题。

3.1.2 密钥架构优化

4G 网络架构的扁平化导致密钥架构从原来使用单一密钥提供保护,变成使用独立密钥对 NAS(non-access stratum,非接入层)和 AS(access stratum,接入层)分别进行保护,如图 2 所示。所以保护信令面和数据面的密钥个数也从原来的 2 个变成 5 个,密钥推衍变得相对复杂^[8],多个密钥的推衍计算会带来一定的计算开销和时延。在 5G 场景下,需要对 4G 的密钥架构进行优化,使得 5G 的密钥架构具备轻量化的特点,满足 5G 对低成本和低时延的要求。

另外,5G 网络中可能会存在两类计算和处理能力差

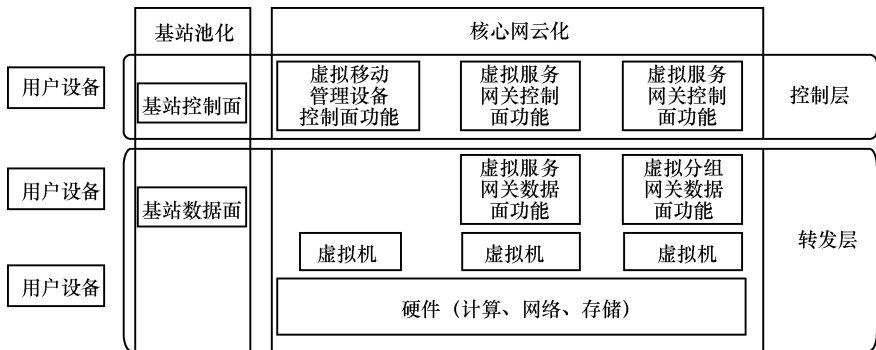


图 1 5G 网络架构演进

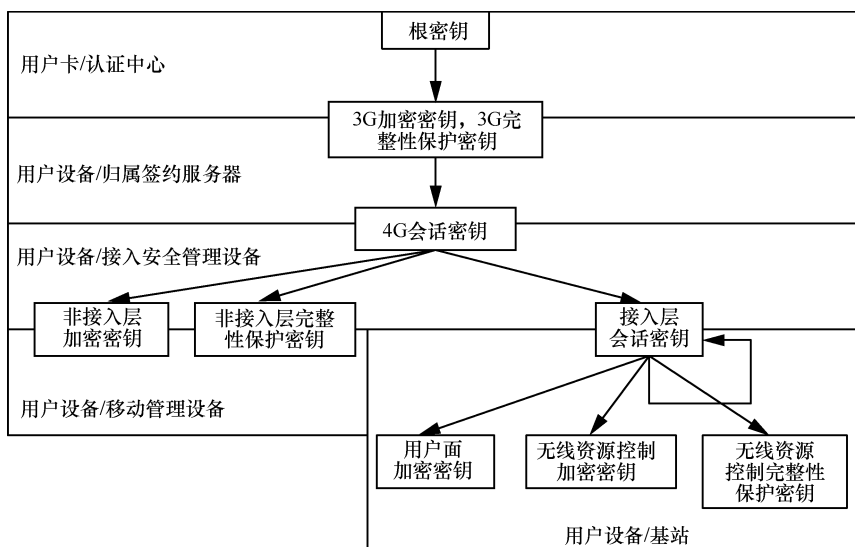


图 2 4G 网络的密钥架构

别很大的设备：一类是大量的物联网设备，这些设备的成本低、计算能力和处理能力不强，无法支持现在通用的密码算法和安全机制（如 AES、TLS 等），因此除了上述的密钥架构之外，5G 还需要开发轻量级的密钥算法，使得 5G 场景下海量的低成本、低处理能力的物联网设备能够进行安全的通信；另一类是高处理能力的设备（如智能手机），随着芯片等技术的高速发展，设备的计算、存储能力将大大提高，也会很容易支持快速公私钥加解密，此时可以大范围使用证书来更简单、更方便地产生不同的多样化密钥，从而对具有高处理能力的设备之间的通信进行保护。

3.2 5G 安全关键技术

3.2.1 5G 中的大数据安全

5G 的高速率、大带宽特性促使移动网络的数据量剧增，也使得大数据技术在移动网络中变得更加重要。大数据技术可以实现对移动网络中海量数据的分析，进而实现流量的精细化运营，准确感知安全态势等业务。如 5G 网络中的网络集中控制器具有全网的流量视图，通过使用大数据技术分析网络中流量最多的时间段和类型等，可以对网络流量的精细化管理给出准确的对策。另外，对于移动网络中的攻击事件也可以利用大数据技术进行分析，描绘攻击视图有助于提前感知未知的安全攻击。

在大数据技术为移动网络带来诸多好处和便利的同时，也需要关注和解决大数据的安全问题。而随着人们对个人隐私保护越来越重视，隐私保护成为了大数据首先要解决的重要问题。大量事实已经表明，大数据如不得到妥

善处理，将会对用户的隐私造成极大的侵害；另外，针对大数据的安全问题，还需要进一步研究数据挖掘中的匿名保护、数据溯源、数据安全传输、安全存储、安全删除等技术^[8]。

3.2.2 5G 中云化、虚拟化、软件定义网络带来的安全问题

对 5G 系统的低成本和高效率的要求，使得云化、虚拟化、软件定义网络等技术被引入 5G 网络。随着这些技术的引入，原来私有、封闭、高成本的网络设备和网络形态变成标准、开放、低成本的网络设备和网络形态。同时，标准化和开放化的网络形态使得攻击者更容易发起攻击，并且云化、虚拟化、软件定义网络的集中化部署，将导致一旦网络上发生安全威胁，其传播速度会更快、波及范围会更广。所以，云化、虚拟化、软件定义网络的安全变得更加重要，其主要的安全问题如下。

- 云化、虚拟化网络引入虚拟化技术，要重点考虑和解决虚拟化相关的问题，如虚拟资源的隔离、虚拟网络的安全域划分及边界防护等。
- 云化、虚拟化网络后，传统物理设备之间的通信变成了虚拟机之间的通信，需要考虑能否使用虚拟机之间的安全通信来优化传统物理设备之间的安全通信。
- 引入 SDN 架构后，5G 网络中设备的控制面与转发面分离，5G 网络架构产生了应用层、控制层以及转发层。需要重点考虑各层的安全、各层之间连接所对应的安全（如南北协议安全和东西向的安全）以及控制器本身的安全等。



3.2.3 移动智能终端的安全

5G时代用户使用的业务会更加丰富多彩,对业务的欲望也会更加强烈,移动智能终端的处理能力、计算能力会得到极大的提高,但同时黑客使用5G网络的高速率、大数据、丰富的应用等技术手段,能够更加有效地发起对移动智能终端的攻击,因此移动智能终端的安全在5G场景下会变得更加重要。

保证移动智能终端的安全,除了采用常规的安装病毒软件进行病毒查杀之外,还需要有硬件级别的安全环境,保护用户的敏感信息(如加密关键数据的密钥)、敏感操作(如输入银行密码),并且能够从可信根启动,建立可信根→boot loader→OS→关键应用程序的可信链,保证智能终端的安全可信。

3.3 5G安全机制的未来研究方向

5G包含很多不同的技术,针对不同场景需要采用不同的安全机制。本文主要讨论5G安全机制未来可能的研究方向。

3.3.1 5G新型认证机制

在5G移动互联网中,物联网将成为重要的应用场景。物联网主要面向物与物、人与物的通信。5G网络通信不仅涉及普通个人用户,也涵盖了大量不同类型的行业用户。为了渗透到更多的物联网业务中,5G应具备更强的灵活性和可扩展性,以适应海量的设备连接和多样化的用户需求^[6]。为此,物联网通信中需要对按照一定原则(如同属一个应用、在同一个区域、有相同的行为特征等)组织在一起的大量终端节点提供成组的认证^[9],即通过一次认证就可以完成对所有节点的认证,从而避免传统网络的一对一认证带来的大量信令消耗和时延问题。

3.3.2 算法协商

5G系统中2G、3G、4G、LTE、Wi-Fi等多种网络共存,这必然产生网络融合的问题。终端设备在多种网络之间漫游时,必然会引起密钥切换、算法协商问题。而且在5G网络下,接入网将面临更大的信令与数据压力,所以需要采取更加轻量级的算法协商方案,以提升网络的效率。

4 结束语

5G网络是一个全融合的网络,其安全问题也是连接“移动智能终端、宽带和云”的端到端的安全问题,更是涉及物理安全、传输安全以及信息安全的全方位安全问题,从而产生了如大数据安全保护、虚拟化网络安全、智能终端安全等关键安全问题。此外,在传统安全机制的基础上,新的认证机制

和技术中的安全机制可以进一步增强5G网络的安全防护能力,使得5G网络可以为人们的生产、生活带来更多便利。

参考文献

- 1 3GPP TS 23.002. Technical Specification Group Services and System Aspects; Network Architecture, 2007
- 2 3GPP TS 23.401. General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access, 2008
- 3 陈晓贝, 罗振东. 面向2020年及未来, 5G之花如何绽放. 人民邮电报, 2014
- 4 3GPP TS 33.102 V12.1.0. Technical Specification Group Services and System Aspects; 3G Security; Security Architecture, 2011
- 5 3GPP TS 33.401. 3GPP System Architecture Evolution (SAE); Security Architecture, 2012
- 6 IMT-2020. 5G愿景与需求白皮书, 2014
- 7 3GPP TS 33.234 V12.1.0. Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interworking Security, 2011
- 8 冯登国, 张敏, 李昊. 大数据安全与隐私保护. 计算机学报, 2014, 37(1): 246~258
- 9 3GPP TR 33.812 V9.2.0. Feasibility Study on the Security Aspects of Remote Provisioning and Change of Subscription for Machine to Machine (M2M) Equipment, 2012

[作者简介]



朱红儒,女,中国移动通信有限公司研究院安全技术研究所网络技术研究室经理、副主任研究员、高级工程师,主要研究方向为网络安全、物联网安全、移动医疗安全、SDN安全、大数据安全等。

庄小君,女,中国移动通信有限公司研究院安全技术研究所研究员、中级工程师,主要研究方向为通信网络安全、SDN/NFV安全和物联网安全。

郭姝,女,中国移动通信有限公司研究院安全技术研究所研究员,主要研究方向为通信网络安全、SDN安全和D2D安全等。

齐旻鹏,男,中国移动通信有限公司研究院安全技术研究所研究员、中级工程师,主要研究方向为通信网络安全和物联网安全。

(收稿日期:2014-10-23)