5G网络赋能物联网安全

5G Enables Internet of Things Security

林美玉/LIN Meiyu
（中国信息通信研究院安全研究所，中国 北京 100191）
(China Academy of Information and Communications Technology, Security Research Institute, Beijing 100191, China)

DOI：10.12142/ZTETJ.202206012
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221013.1427.006.html
网络出版日期：2022-10-13
收稿日期：2022-08-25

摘要：分析了物联网（IoT）安全需求，并梳理了5G网络的安全能力。认为5G网络能够满足物联网应用的安全需求。5G网络自身安全能力的增强，有助于满足物联网应用对网络安全性的需求。5G网络可以通过安全组网、能力开放的方式，利用自身安全能力、切片特有的安全能力以及运营商网络中部署的其他安全能力，向不同的物联网应用场景提供差异化安全服务，以赋能物联网安全。

关键词：5G网络；物联网安全；切片；能力开放

Abstract: The security requirements of the Internet of Things (IoT) are analyzed, and the security capabilities of 5G networks are introduced. It is believed that 5G networks can meet the security requirements of IoT. The enhancement of the 5G networks security capabilities helps meet the needs of IoT applications for network security. The 5G networks can also use the security capabilities to enable IoT security through providing customized virtual private network or security capability exposure. The security capabilities include 5G network security capabilities, slice-specific security capabilities, and other security capabilities deployed in the network by the operators.

Keywords: 5G network; Internet of Things security; slice; capability exposure

目前，5G已经成为全球最瞩目的热门技术之一。相比于4G和之前的蜂窝移动网络，5G融合了很多新技术，可提供极端差异化的性能以满足多样化场景的业务应用需求。5G网络主要支持三大应用场景：增强移动宽带（eMBB）、海量机器类通信（mMTC）和超可靠低时延通信（URLLC）。其中，mMTC面向的就是物联网应用场景，例如海量终端高密度连接的智慧城市应用场景。实际上，自动驾驶、工业控制等对可靠性和时延高度敏感的URLLC场景，也是物与物之间的通信。因此，从5G网络支持的应用场景来看，5G是为物联而生的。

与此同时，业界对5G网络安全的重视程度显著提高。5G安全问题甚至已成为世界各国在5G网络方面的主要博弈点。欧美国家纷纷出台了相关法律、政策，并制定了相关技术指导文件，将5G安全上升到国家战略层面。事实上，5G安全问题的重要性之所以能够引发全球的共鸣，其根本原因是在5G与物联网[1]应用深度融合后，人们对5G网络所承载的物联网应用安全有所担忧。5G网络本身的安全与4G之前网络的安全并没有本质区别，但是其承载的物联网应用的安全却关系着国计民生的各行各业，甚至关系着国家安全。因此5G安全问题的重中之重，就是如何解决5G网络与物联网应用融合的安全问题。

1 5G融合物联网应用的安全风险

物联网应用对5G网络的安全疑虑主要体现在两方面：一方面是能否消除5G网络自身面临的安全风险，以确保所承载的物联网应用的安全；另一方面是能否解决5G网络与物联网应用融合所带来的新风险问题。

5G网络自身的安全风险主要来自5G网络所引入的新技术[1]。网络功能虚拟化（NFV）、多接入边缘计算/移动边缘计算（MEC）、网络能力开放、网络切片等多种新技术的引入，确实给5G网络带来了一些新的安全风险。但是随着隔离等安全技术的逐渐成熟，以及5G网络增强安全机制的产生[1]，5G网络自身的安全风险基本可控。

5G网络与物联网应用之间的边界融合泛化后，其安全风险也会互相影响。从物联网应用的角度来看，5G网络的引入打破了某些物联网应用领域通过物理边界保护的封闭性。这容易引发越权访问，造成安全后果。例如，无线接口劫持可能会导致合法终端接入非法网络，泄露敏感信息。如果5G网络身份认证能力不足，非法物联网终端可能接入业务系统，泄露或篡改业务数据，并导致物联网业务失效。从

1. 本文所指物联网，主要关注物联网业务应用层面，而非联通万物的网络本身；本文仅适用于5G网络承载物联网应用的场景。

5G网络的角度来看，物联网应用的安全风险，也可能会给5G网络带来灾难性后果。例如，在mMTC应用场景中，大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被操控向网络发起分布式拒绝服务（DDoS）攻击，就可能带来网络中断、系统瘫痪等安全风险。

2 物联网应用对5G网络的安全需求

目前5G网络的安全问题被广泛关注甚至被无限扩大。这与不同行业之间存在较大的认知差异密切相关。物联网垂直行业在安全性方面对移动通信网不够信任，对通信网络的安全能力也不够了解；而通信行业对物联网领域的安全需求也尚未充分了解，无法发挥5G网络的最大价值。本文首先从物联网的业务特征出发，分析物联网安全需求。这些需求主要包括：

（1）对敏感数据保护的需求。物联网应用场景中包含重要的行业信息和个人隐私，因此数据泄露和篡改会带来严重的后果。尤其是利用感知数据进行应用决策的物联网应用场景，一旦感知数据被篡改，就可能导致决策错误。这不仅会关系到企业经营和生产安全，甚至关乎国家安全。

（2）差异化安全需求。物联网应用涉及千行百业，其安全需求也各不相同。例如，工业互联网主要关注数据不能出园区，智慧医疗更关注隐私数据加密。

（3）对海量终端的安全管理需求。众所周知，物联网终端安全能力普遍较低，物联网应用服务商的安全技术水平良莠不齐。操控物联网终端向网络发起DDoS攻击会导致物联网应用平台瘫痪。非法终端接入网络和物联网应用平台会导致数据泄露或被篡改。这些案例比比皆是，带来的后果也是非常严重的。

（4）对无线接口安全性的需求。物联网应用与5G网络融合后，开放的无线网络可能会成为物联网应用安全的薄弱点，例如网络攻击者可能会通过无线接口进行窃听、数据篡改等。

结合5G网络特点，上述安全需求映射到5G网络中，具体可体现为以下技术需求[2]：

（1）安全隔离技术。针对不同安全等级的物联网应用，5G网络需要采用网络安全分域方式或安全隔离技术手段来实现网络资源、数据传输通道的隔离。

（2）终端身份安全和访问授权技术。该技术可防范非法终端接入网络和物联网应用平台。

（3）5G网络无线接口通信安全技术。为满足物联网应用的安全需求，无线接口需要具备防窃听、防篡改、防无线接口劫持等通信安全能力。对安全要求较高的场景，甚至还需要具备无线接口DDoS攻击防御、无线接口抗干扰等能力。

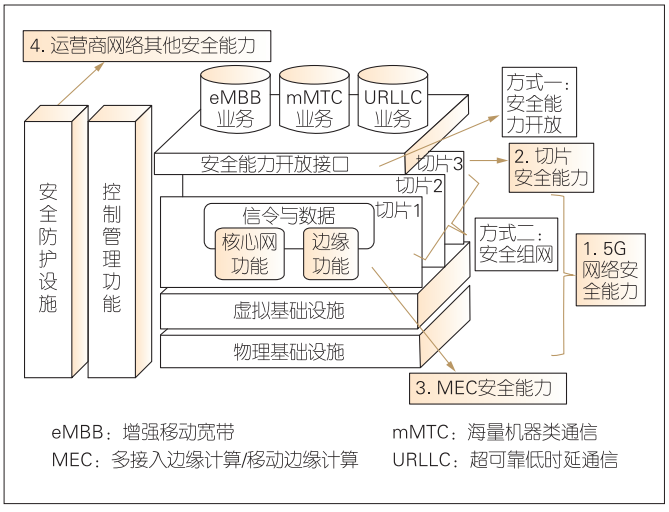
（4）数据机密性和完整性保护技术。该技术主要是用于防范5G网络所传输的数据被泄露或篡改。

3 5G赋能物联网安全的解决方案

作为支撑未来万物互联的基础设施，5G网络对物联网应用的安全保障能力是各个行业完成数字化转型的关键。事实上，5G网络在安全架构设计方面，已充分考虑了上层应用的安全需求。针对物联网应用的安全需求，一方面5G网络本身的安全能力须不断增强，以打消物联网应用对5G网络安全性的疑虑；另一方面通过安全组网、能力开放等新技术，5G网络可以整合自身及外在的各种安全能力，为物联网应用提供差异化的安全服务，直接赋能物联网应用安全。

3.1 可赋能的安全能力

5G网络可用于物联网安全赋能的安全能力主要体现在4个方面：5G网络自身安全能力、网络切片技术特有的安全能力、MEC的数据安全保护能力以及运营商网络中部署的其他外在安全能力，具体如图1所示。



▲图1 5G赋能物联网安全

3.1.1 5G网络自身安全能力

（1）终端身份认证和访问授权

用户设备（UE）接入5G网络需要进行主认证（Primary认证）。在认证机制方面，5G继承了4G成熟的认证与密钥协商（AKA）认证机制，并对AKA机制进行了增强，强化了归属网络对认证的控制。此外，5G还引入了灵活的扩展认证协议（EAP）认证框架，以实现统一认证。这样网络一

方面既可支持各物联网应用场景中已使用的多种认证协议（例如扩展认证协议–传输层安全协议等），又可根据物联网应用所需要的认证能力需求进行扩展适配；另一方面，还可以支持不同接入网络方式的认证，例如无线局域网（WLAN）等非第3代合作伙伴计划（3GPP）接入方式。

在主认证的基础上，5G网络还可支持针对应用的次认证，即用户在通过5G网络访问外部数据网络时，由承载数据网络的第三方（例如物联网服务商）对用户进行身份认证。次认证的过程中需要使用终端中预存的认证凭证。认证过程会使用5G网络的EAP认证框架。

（2）5G网络无线接口通信安全

对于无线接口的通信安全，5G网络进行了一系列的安全增强[3]。一是空口采用加密身份标识，提供增强的用户隐私保护。为了解决4G网络中由使用用户国际移动用户识别码（IMSI）接入网络而导致的用户标识在空口的泄露问题，5G引入了用户隐藏标识（SUCI）。通过一系列的算法和机制设计，在5G响应身份请求消息时，UE永远不发送用户的永久标识（SUPI）。由于每次产生的SUCI并不相同，因此攻击者无法根据SUCI计算出SUPI。这能够起到保护用户隐私的作用。二是5G网络无线接口支持接入层（AS）和非接入层（NAS）的机密性和完整性保护。在用户面的完整性保护方面，之前的蜂窝移动网络在应对业务时效性的要求时均未设计完整的保护机制。考虑到有些物联网应用场景对控制数据传递的准确性要求比时效性要求更高，5G网络引入了灵活的数据完整性保护机制。设置完整性保护策略可以使5G网络灵活地决定是否开启用户面数据完整性保护，以更好地适应不同应用场景的差异化需求。

（3）数据机密性和完整性保护

在无线接口机密性和完整性保护算法方面，5G网络支持高级加密标准（AES）、祖冲之算法（ZUC）或者Snow 3G 128 bit的密码算法。考虑到未来量子计算对算法的破解，5G网络将支持256 bit的密钥。

除了无线接口外，5G网络还在运营商网间增加了安全边界保护代理（SEPP）设备，可支持在运营商之间建立传输层安全（TLS）的安全传输通道，或者基于共同认同的安全策略对传输的信息进行机密性和完整性保护，以防止重要敏感数据在传输过程中被篡改和窃听。

（4）网络功能（NF）之间的安全隔离

5G网络的服务化架构使NF之间的相互访问更加便利，但是也为攻击者伪造成合法NF进行攻击带来了便利。针对服务化架构，5G网络设计了一套授权认证机制，以确保只有授权的NF才能访问特定服务，实现服务化架构下NF之间的安全隔离。这主要包括：（a）引入网络仓储功能（NRF）提供NF服务能力的注册、发现、授权，来保障服务化安全；（b）NF与NRF、NF之间进行交互时都需要进行双向认证，具体可采用传输层安全机制（例如TLS协议）的认证机制或者网络域安全机制，例如网络域安全/互联网协议（NDS/IP）；（c）引入授权机制，即NRF采用互联网工程任务组（IETF）定义的OAuth 2.0授权框架[4]对NF进行显式授权，或者基于5G网络的服务发现流程向NF进行隐式授权。

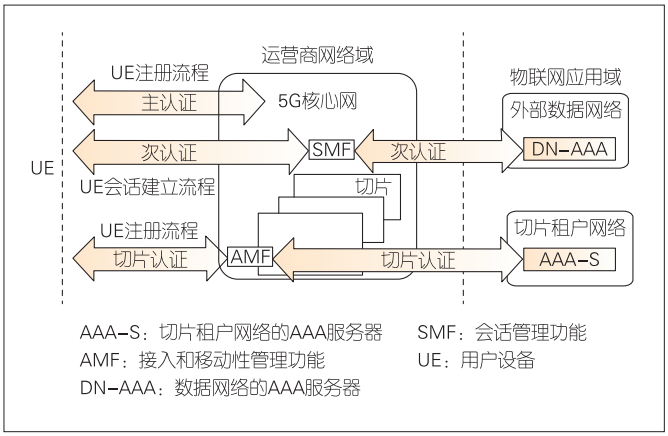
3.1.2 网络切片技术的安全能力

除了5G网络本身的安全能力之外，网络切片还支持一系列特有的安全机制。

（1）网络切片认证

UE接入切片时，其注册过程除了可以通过5G网络进行主认证之外，还可以使用网络切片认证[3,5]，进一步防止未授权用户访问切片。网络切片认证可以由切片使用者（例如物联网应用的服务提供商）自行进行管理。这增强了切片使用者对用户的控制能力和灵活度。

主认证、次认证和切片认证共同构成了5G网络保障物联网应用安全的三级认证体系。三者之间的关系如图2所示[6]。



▲图2 主认证、次认证和切片认证的关系

物联网应用可根据自身的安全需求，在主认证基础之上，叠加次认证和/或切片认证来增强安全能力。

（2）切片的安全隔离机制

切片技术安全性的核心是切片的隔离能力。5G网络从无线接入网隔离、承载网隔离、核心网隔离、数据隔离4个方面引入隔离机制，构建了切片之间、切片网络与用户之间、切片内网元之间的三级隔离体系。无线接入网隔离机制包括：为不同的切片分配专用频谱可实现无线频谱资源的物

理隔离，或者不同切片按需使用相同的频谱以实现逻辑隔离[7]；为不同的切片分配不同的硬件、虚拟机或容器以及对应的虚拟局域网/虚拟可扩展局域网（VLAN/VxLAN）可实现网元隔离。承载网隔离机制包括VLAN逻辑隔离，以及以太网分片技术（如灵活以太网）实现时隙层面的物理隔离[8]。核心网的隔离机制包括独立的物理资源隔离、基于虚拟机或容器的逻辑隔离、通过划分不同的安全域并在安全域之间配置安全策略（例如认证、授权等）而实现的隔离、通过账号权限控制实现不同切片管理维护之间的隔离等。数据隔离机制包括使用独立的密钥而实现的不同数据的隔离、通过身份认证和细粒度授权进行数据访问控制、不同安全级别采用不同的加密机制等。

（3）切片的安全监控

切片管理系统可以实时掌握切片的运行情况（包括故障和受攻击情况），并可通过联动其他安全设备进行威胁处置、故障修复等。双向认证、访问授权以及管理接口的安全保护，可保障切片管理功能的安全。

3.1.3 MEC技术的安全能力

MEC技术可降低时延和网络传输压力，其自身并不具备安全能力。但是由于需要指定用户面功能（UPF）处理数据、阻断对外的N9接口、不开放面向公网的N6接口，事实上MEC技术可以达到敏感数据的流向可管可控、数据不出园区的效果，能够满足某些物联网应用场景下更高的数据安全需求。

当然，如前所述，MEC技术会给5G网络带来一定的安全风险。因此，我们还需要对边缘计算采取必要的安全防护方案，例如：对使用MEC的操作进行认证、授权和审计，对引入的第三方应用执行严格的评估管控流程，加强数据访问控制，对MEC内部边界进行安全隔离等。

3.1.4 运营商网络部署的其他安全能力

除了5G网络和切片的安全能力之外，为保障相关网络和业务系统的安全，运营商网络通常会部署很多其他的安全能力，包括认证、授权、审计、入侵检测、漏洞扫描、入侵检测、威胁情报共享、恶意流量清洗等。

3.2 赋能方式

5G网络可以通过安全组网和安全能力开放两种方式，为物联网应用提供差异化的安全服务，直接赋能物联网应用安全。

3.2.1 安全组网

5G网络可通过“切片+边缘计算”的方式进行组网，为不同物联网应用提供不同安全等级的定制化虚拟专网。显然，安全的虚拟专网可满足不同物联网应用之间的安全隔离要求。

除此之外，我们还可以根据各物联网应用的安全需求，为虚拟专网设计定制化的安全机制，提供差异化的安全服务。5G网络自身的安全能力、切片的安全能力，MEC技术，甚至包括运营商部署的入侵检测、安全防护等能力，都可以作为虚拟专网的安全定制选项。例如，对安全等级和资源保障要求高的重点应用，可将切片部署于专用的物理资源实现物理隔离并部署MEC；对数据准确性要求高的应用，可开启数据的完整性保护；对可用性要求高的应用，可以通过流调度的方式，让应用的流量经过抗DDoS攻击、异常流量监测等安全模块进行防御。

3.2.2 安全能力开放

5G网络支持的网络能力开放技术为5G网络赋能物联网安全提供了一种新的方式。

为了更好地支持物联网行业应用，5G标准中引入网络开放功能（NEF），支持将5G网络的基础能力对外转换为标准的应用编程接口（API），以便第三方应用服务提供商调用。目前3GPP已经完成服务质量（QoS）能力等业务能力开放的标准化工作。5G网络的安全能力开放目前正处于研究当中。

安全能力开放的方式[9]包括：由5G网络构建安全能力开放平台，实现网络即服务（NaaS），形成一系列安全服务能力，并通过API进行开放以赋能物联网安全。物联网行业应用可根据自身的安全需求，直接调用运营商网络的安全服务能力和安全资源，可以节省更多的财力和精力，实现行业共赢。

前述5G网络自身的安全能力、切片的安全能力，甚至运营商部署的入侵检测、安全防护等能力都可以考虑以适当的服务方式进行开放。例如，3GPP R16就提出了一种面向应用的认证和密钥协商（AKMA）[10–11]能力开放的解决方案，即利用5G网络的认证凭证和安全机制，为第三方应用提供认证和应用层通信加密服务。该方案尤其适合物联网应用的调用场景。在物联网场景下，由于终端难以进行密钥接收和配置，而AKMA无须在终端预置安全凭证，物联网应用也无须建立自身密钥管理体系进行密钥分发，使用5G的AKMA能力就可以实现认证和密钥管理能力。由于第三方应用可通过标准的能力开放接口接入并使用AKMA功能，因此该方案可适用于所有协议的物联网设备。

4 结束语

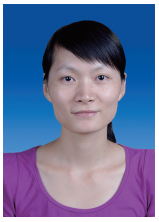
目前，5G对物联网安全赋能的各种实践已崭露头角。5G网络结合MEC和切片技术进行安全组网并提供定制化安全能力的方案，业界已有较多试验应用场景，但还不够成熟，尚未进行规模化复制。而5G网络安全能力开放的方案，目前尚处于方案探索阶段，实践案例很少。这主要是由于通信行业与垂直应用行业彼此了解不够，5G网络难以结合行业需求并对自身丰富的相关安全能力进行充分地挖掘和开放。

5G网络让万物互联成为可能，促进了产业的跨界融合，但也引发了业界对安全问题的担忧。如前所述，5G网络蕴含的丰富的安全能力有待释放，未来5G网络与物联网应用在安全方面的深度融合还有无限的可能，尤其是5G安全能力开放，将成为未来5G和物联网融合发展的一个重要方向。后续运营商与物联网应用服务商应加强沟通合作，形成跨行业共识，共同推动5G赋能物联网安全，更好地发挥5G在推动社会数字化转型过程中的作用。

参考文献

[1] 中国信息通信研究院, IMT-2020(5G)推进组. 5G安全报告 [R].2020
[2] IMT-2020(5G)推进组. 面向行业的5G安全分级白皮书 [R].2020
[3] 3GPP. Security architecture and procedures for 5G system: 3GPP TS 33.501 [S]. 2019
[4] RFC. The oauth 2.0 authorization framework: RFC 6749 [S]. 2020
[5] 3GPP. System architecture for the 5G system (5GS): 3GPP TS 23.501 [S]. 2019
[6] 杨志强，栗栗，杨波，等. 5G安全技术与标准 [M]. 北京: 人民邮电出版社, 2020: 195-196
[7] 毛玉欣，陈林, 游世林. 5G网络切片安全隔离机制与应用 [J]. 移动通信, 2019, 43(10): 31-37
[8] 李晗. 面向5G的传送网新架构及关键技术 [J]. 中兴通讯技术, 2018,24(1): 53-57
[9] 杨红梅, 林美玉. 5G网络及安全能力开放技术研究 [J]. 移动通信, 2020, 44(4): 65-68
[10] 3GPP. Study on authentication and key management for applications based on 3GPP credential in 5G: 3GPP TR 33.835 [S].2020
[11] 3GPP. Authentication and key management for applications (AKMA) based on 3GPP credentials in the 5G System (5GS): 3GPP TS 33.535 [S]. 2021

作　者　简　介



林美玉，中国信息通信研究院安全研究所副所长、中国通信标准化协会ST6组长；长期从事网络交换、网络与信息安全方面的研究工作；牵头完成多项国家重大专项，并多次获得中国通信标准化协会科技进步奖一等奖、二等奖、三等奖，中国通信学会科技奖二等奖、三等奖，以及国家安全部科技进步奖二等奖等奖项；已发表论文10余篇，累计完成相关领域标准40余项。