5G安全威胁及防护技术研究

Study on the Security Threat and Protection Technologies of 5G

黄开枝，金 梁，赵 华（中国人民解放军信息工程大学，河南 郑州 450002）
Huang Kaizhi，Jin Liang，Zhao Hua（The PLA Information Engineering University，Zhengzhou 450002，China）

摘 要：
第五代移动通信系统（5G）以更快的速度、更大的容量、更低的成本为用户提供更丰富的业务和更好的用户体验，同时也带来了更多安全挑战，面临的安全威胁更加广泛而复杂。首先分析了现有的安全体系架构和网络安全模型，给出了5G网络的安全需求，并基于此给出了可能的安全防护技术研究方向。

关键词：
第五代移动通信系统；安全防护；物理层安全
doi：10.16463/j.cnki.issn1007-3043.2015.06.003
中图分类号：TN929.5
文献标识码：A
文章编号：1007-3043（2015）06-0008-05

Abstract：
The 5G mobile communication system can provide users with higher data rate, greater capacity, cheaper cost, as well as better user experience. But the security challenges also become more complex to handle. It firstly analyzes the existing security architecture and network security model, puts forward the security requirements of 5G. Based on these requirements, it gives the potential research orientations of the security protection technologies.

Keywords：
5G mobile communication system; Security protection; Physical layer security

0 前言

为了满足高速发展的通信应用需求，下一代移动通信网络（5G）的研究已在全球范围内紧锣密鼓地加速推进，期望能以更快的速度、更大的容量、更低的成本给各类用户提供更丰富的业务。安全问题是无线移动通信网络能否给用户提供稳定可靠服务的关键问题。例如公开曝光的“斯诺登”事件，以及目前国家9部委联合部署的“伪基站”整治专项行动，都反映出我国移动通信网正不同程度地受到各种安全威胁，已成为信息安全对抗的重要战场，未来移动通信面临的安全威胁将更加严峻。

无线安全的威胁主要来自于电磁波开放式传播造成的无线链路的脆弱性，这一问题在2G、3G、4G移动通信系统中正逐步得到改善，但缺少结合无线传输特点的有效解决方案。5G支持的数据传输速率更高、业务更丰富，且不仅需要支持人与人更便捷的通信，也需要支持人与机器、机器与机器的各种无缝沟通，因此它所面临的安全威胁比2G、3G、4G更加广泛而复杂。

为应对这些安全威胁，在设计5G整体架构的初始阶段应该同步考虑相应的安全解决方案，在架构顶层设计中充分体现安全需求，尽早部署5G安全研究工作，避免安全问题研究滞后带来的通信和安全“两张皮”、不得不靠后期“打补丁”的方式来弥补安全漏洞的隐患。本文分析了现有的安全体系架构和网络安全模型，给出了5G网络的安全需求，并基于此给出了可能

基金项目：国家自然科学基金（61379006）；863计划重点项目（SS2015AA011306）
收稿日期：2015-05-11

的安全防护技术研究方向，不仅要从根本上解决无线空口的安全问题，也要解决核心网的发展和未来新型业务的涌现所带来的新的安全威胁和挑战。

1 现有的安全体系架构和网络安全模型

在3G时代，国际标准化组织3GPP制定了一套完整的安全体系架构。在WCDMA网络中，用户和网络之间的相互认证及密钥协商是通过认证和密钥协商（AKA）机制来实现的。AKA是WCDMA网络中用于用户与网络之间的双向身份认证与密钥协商的机制。AKA过程的基础是用户和网络之间共享的一个秘密密钥K，只有用户的USIM卡和用户归属网络中的AuC（认证中心）可以得到这个秘密密钥。AKA机制除了实现用户与网络之间的双向认证外，还进行了密钥协商，密钥协商的结果会产生一个加密密钥CK和一个完整性保护密钥IK。

WCDMA的加密和完整性使用的算法为KASUMI标准算法，密钥长度为128位，空中接口安全机制的实施是在用户终端和基站之间进行的，其安全架构如图1所示[2-3]。

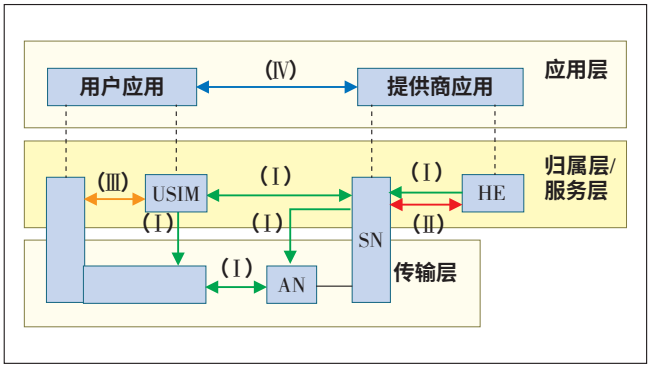

图1　WCDMA网络安全体系架构

到了LTE时代，国际标准化组织为4G网络打造了比现有3G、2G网络和固定互联网更可靠、鲁棒性更高的安全机制。TD-LTE网络安全沿用3G网络的用户身份保护机制、双向身份认证和鉴权密钥协商机制，并根据TD-LTE扁平化网络架构定义了新的安全特性：4G网络安全包括接入层（AS）安全和非接入层（NAS）安全，使得无线空口和核心网络安全相互独立，从而提高整个系统的安全性。接入层安全实现移动终端与基站设备之间信令数据的加密和完整性保护、用户数据的加密保护；非接入层安全实现移动终端与移动管理实体（MME）之间信令数据的加密和完整性保护；采用分层的密钥体系架构，由密钥K派生出较多层次的密钥，分别实现各层的保密性和完整性保护。LTE的安全体系架构如图2所示[4-5]。

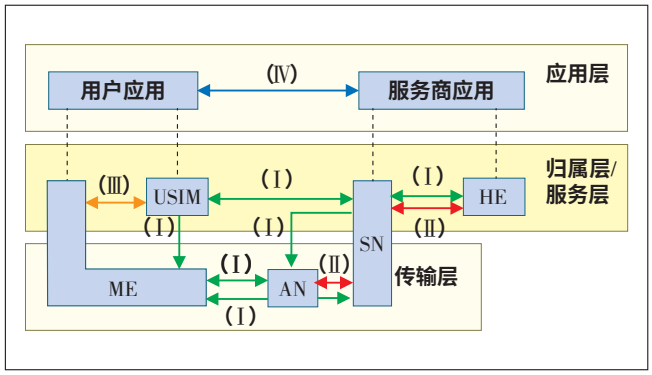

图2　LTE安全体系架构

可以看出，LTE安全体系架构比3G网络安全架构多了终端和核心网之间的安全，但仍然存在用户认证向量容易被截获、IMSI用户身份信息泄露等安全缺陷。此外，USIM卡和AUC长期共享根密钥K及不支持数据签名服务也给系统带来了潜在的安全问题[6-7]。

2 5G网络的安全需求

在5G网络中，大量的宏蜂窝、微蜂窝以及用户设备等不同层次的网络元素共同构成了一个多层次和高密度重叠覆盖的异构网络系统，其将以更快的速度、更大的容量、更低的成本给各类用户提供更丰富的业务。如图3所示，5G网络采用了新型组网方式，包括移动Ad hoc网络、无定形小区、密集网络、异构网络融合及网络虚拟化等；多种无线和移动通信方式并存，包括设备到设备通信（D2D）、机器到机器通信（M2M）、Wi-Fi、可见光、近场无线通信等新技术；移动业务层出不穷，移动数据流呈爆炸式增长，未来的移动终端也呈现多样化的趋势；用户周边的无线网络和终端设备显著增加，并且融合业务对网络资源的需求越来越大，因此异构无线网络及其终端之间协同为用户服务的业务提供方式势在必行。

因此，5G网络将比现有无线移动通信面临的安全威胁更加广泛而复杂：不仅面临终端的移动性和无线信道的开放性带来的传统安全威胁，而且面临多种使用模式功能更加强大或者资源受限的智能终端、多种异构无线网络的融合互通、更加开放的基于IP架构的网络设施和更加丰富的不同信任等级的业务承载等所带来的新安全威胁。

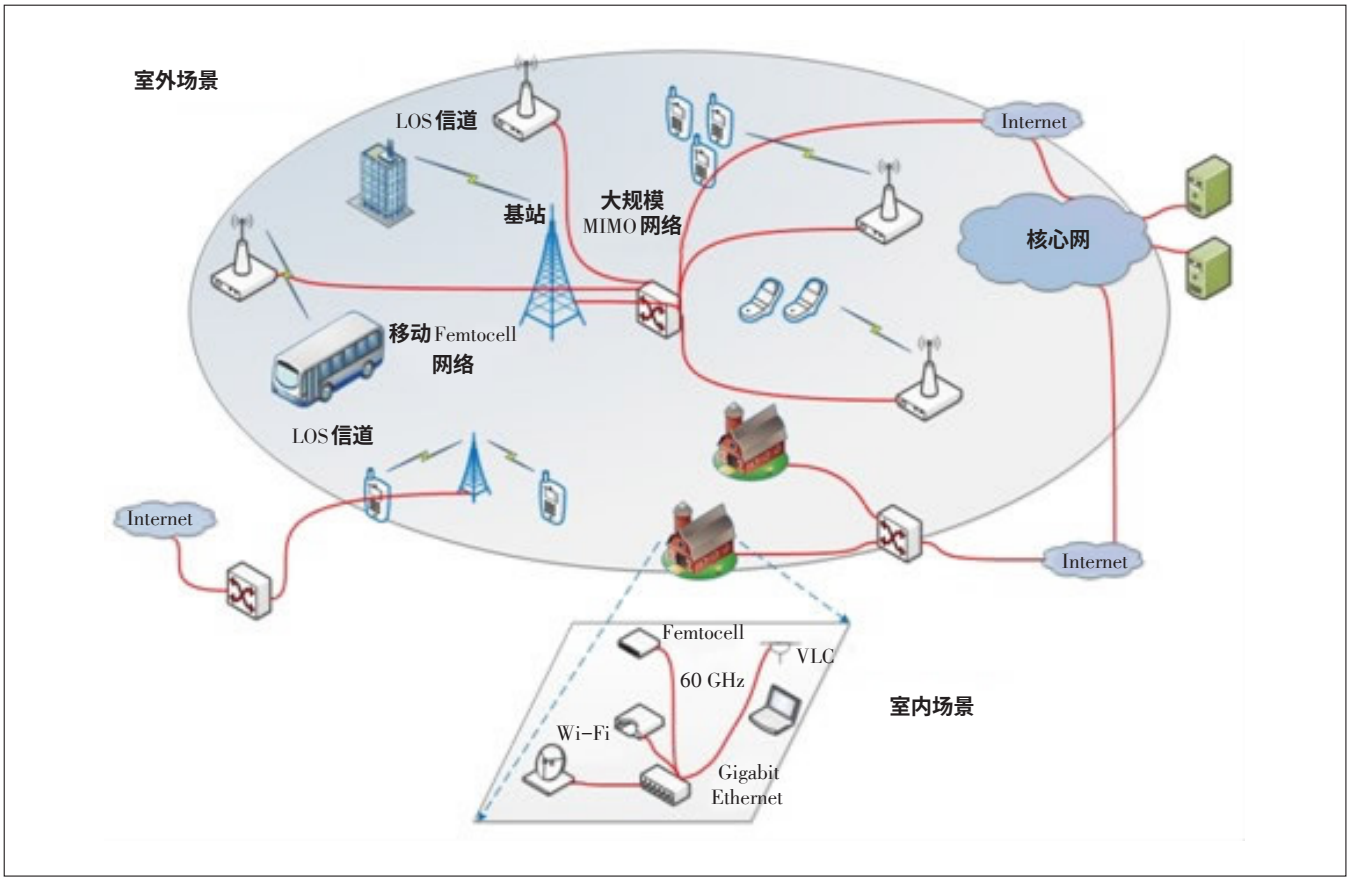

图3　未来5G场景

如何在不同的应用场景下为用户的多种业务提供安全的高速接入，有效保证异构无线网络及终端协同下的通信安全是5G多层次异构融合网络亟待解决的问题之一，包括信息保密性、数据完整性、身份认证性等。此外，不仅需要能对普通用户和普通业务提供符合商业运营需求的基本安全保障能力，对部分重要用户和业务提供高等级的安全保障能力，以及为受限设备提供轻量级的安全保障能力也是亟待解决的问题之一。

满足移动网络共有的和5G网络特有的安全需求。

a）空中接口应保证移动终端和网络间以及相关联实体间的安全通信，应确保用户身份的隐私性、各种数据的机密性、完整性和网络身份的可认证性。

b）需要轻量级加密技术，以满足安全、高速、能效高的要求。

c）安全机制具有灵活性和可扩展性。

5G应能够提供分等级的安全机制。5G网络在提供基本服务能力的同时，各种特色化、差异化服务也日益发展，对安全具有特殊需要的用户希望网络能提供更高安全等级的控制能力。通常，重要用户在网络中传输的信息比普通用户更加敏感，他们面对的攻击者可能是有组织性的黑客或政府级别非盈利目的的机构，因此高等级用户面临的安全威胁将更加突出，5G应该提供不同安全级别的防护机制。具体可以包括：

a）基于用户的安全需求等级，提供增强的网络认证机制。

b）基于用户等级，提供区分业务的鉴权认证和安全保密机制。

c）基于业务等级，提供区分用户的鉴权认证和安全保密机制。

3　5G安全的机遇与挑战

物理层安全利用无线信道的差异性、针对无线传播特点研究安全防护机制，有可能从根本上解决无线通信的安全问题。5G拟采用的技术也为物理层安全的实现创造了条件，如大规模天线阵列使得信道差异的空间分辨率更高，高频段使得信道差异对位置更加敏感，大带宽使得信道特征更加丰富。

此外，SDN、虚拟化、云是未来核心网的3个重要发展方向。这些技术的引入将给5G网络带来新的威胁，但同时这些技术也带来了解决安全问题的新思路。需要研究这些技术引入移动通信网络后，如何利用这些技术优化现有的安全机制，或设计新的安全机制。

3.1 物理层安全技术

无线安全通信的主要目标是在保证期望用户通信质量的同时防止信息被潜在的窃听者截获。传统的无线通信安全基本依靠2类方法。一类是直接移植有线通信系统中的方法，在“信息层面”采用信源加密来避免信息泄露。该类方法回避了无线信号本身易被截获的问题，同时也面临密码设备管理、密钥管理、密钥在无线环境下的传输等一系列问题。另一类方法是采用序列扩频/跳频、超宽带等低截获概率的调制解调技术，提高信号传输的隐蔽性以及信息还原的复杂度。该类方法仍然没有考虑无线信道传输的特点，一旦调制解调参数被破解则失去安全作用。针对无线通信的安全问题，近年来兴起的物理层安全研究从无线通信的物理层特点入手，在信号层面解决无线通信的安全问题。无线信道在空时频域具有明显的多样性、时变性和私有性，并且通信双方的信道特征具有一定的互易性，这些特性为安全传输方法设计提供了新的思路，成为近年来无线通信安全的研究热点[7-12]。

5G所采用的传输和组网技术可以更好地与物理层安全相结合。Massive MIMO以及多个基站之间的多点协作（CoMP）等各种技术，为物理层安全的深入研究创造了良好的条件。为了大幅度提高频谱效率和功率效率，5G拟在基站使用更大规模的天线阵列，这极大地丰富了信道特征的多样性和时变性；TDD模式下信道的互易特性更加明显，且通信双方的信道特征具有一定的私有性。因此，可以充分利用5G无线移动通信的物理层传输特性，研究安全传输、密钥生成、加密算法和接入认证技术，在保证期望用户通信传输质量的同时，防止未知位置的窃听者截获信号或者增加中间人攻击的难度。

3.2 网络域安全机制

a）终端接入的隧道密闭防护机制。现有的2G、3G和4G协议中，会话初始协商过程需要终端与网络在公共信道上通过上下行信令交互，完成会话初始协商；这一过程中的部份内容（例如用户身份信息、业务类型、注册类型等私密信息）必须是未经过加密的，才能确保后续的加密和身份认证过程顺利完成。为了防止用户身份信息、业务类型、注册类型等私密信息通过明文传输方式泄露，需要设计终端接入的隧道密闭防护机制，将用户接入与加密协商过程也进行加密保护，确保所有与用户身份信息相关的消息都进行加密，进一步提高通信系统的安全性。

b）双向认证增强机制。目前的移动通信体制普遍采用高层加密技术来防止合法用户信息的泄密。但是伪基站能够将合法终端纳入其管控之下，并利用伪终端的透明转发建立合法终端与合法基站之间的通道。在上行链路，伪基站接收合法用户的通信数据，并通过伪终端将接收数据“透明转发”给合法基站；在下行链路，伪终端接收合法基站的通信数据，并通过伪基站将接收数据“透明转发”给合法终端。合法基站和合法终端对这种类似“中继”的伪基站和伪终端工作方式是完全无感的。为了防止这种伪终端“透明转发”的攻击方式，有必要将认证数据和无线传输链路进行强绑定，实现终端和核心网以及终端和接入网之间的双向认证增强机制。

c）满足5G网络异构性和多样性的安全需求，鉴权认证机制不依赖具体的无线接入技术。由于5G的无线接入网制式多样，移动终端通常要求在不同环境中使用，考虑到目前各种接入网络都有自己的一套接入认证系统，其接入认证机制和加密算法各有不同，这使得终端和网络不仅需要耗费过多存储和管理资源，更重要的是不同认证机制和算法在安全性上表现出明显的差异性，使得无线用户接入安全存在短板效应，易被恶意分子利用；此外，不同制式接入安全机制也不利于移动终端在不同接入网间无缝漫游切换的实现。因此，有必要研究不依赖具体无线接入技术的统一接入认证机制。

4 结束语

5G网络将面临许多新的安全威胁和挑战，包括空中接口、网络、业务以及网元等多个方面。因此，需要深入分析5G网络相比之前的无线移动通信网络在哪些方面有变化，包括网络架构、新的业务类型、新的通信协议、新的安全需求等，这些都可能成为引入新的安全威胁点。探索新的安全体系架构，全面增强5G网络的安全性，利用5G系统的特点解决空中接口的安全问题，以保证5G网络能够根据不同用户等级、不同业务的安全需求，提供更好的安全级别。

参考文献：

[1] 郭江鸿. 无线传感网若干安全问题研究 [D]. 西安：西安电子科技大学，2013.

[2] 3GPP TS 33.102 Security Architecture [S/OL]. [2015-03-23]. ftp://ftp.3gpp.org/specs.

[3] 3GPP TS 02.09 Security aspects [S/OL]. [2015-03-23]. ftp://ftp.3gpp.org/specs.

[4] Zugenmaier A，Aono H. Security Technology for SAELTE [J]. Technical Journal，2008，11 (3)：27-30.

[5] Aejcet H. LTE and the Evolution to 4G Wireless [M]. Security in the LTE-SAE Network，2009.

[6] Park Y，Park T. A survey of security threats on 4g networks [C]. IEEE Globecom Workshops，Sydney，2007：1-6.

[7] 穆鹏程，殷勤业，王文杰. 无线通信中使用随机天线阵列的物理层安全传输方法 [J]. 西安交通大学学报，2010，44 (6)：62-66.

[8] 林通，黄开枝，罗文宇. 一种基于多载波的多播系统物理层安全方案 [J]. 电子与信息学报，2013，35 (6)：1338-1343.

[9] Luo W Y，Jin L，Liu S P，et al. Wireless physical layer security model and resource allocation algorithm in MISO-OFDMA [J]. Electronics letters，2011，47 (6)：414-416.

[10] 钟州，金梁，黄开枝. 多载波系统随机子载波加权的物理层加密算法 [J]. 通信学报，2012，33 (10)：86-90.

[11] 吴飞龙，王文杰，王慧明. 基于空域加扰的保密无线通信统一数学模型及其窃密方法 [J]. 中国科学，2012，42 (4)：483-492.

[12] 钟州. 等效信道特征可变模型下的安全编码与传输机制研究 [D]. 中国人民解放军信息工程大学，2013.

作者简介：

黄开枝，毕业于清华大学，教授，博士，主要研究方向为移动无线通信及其安全；金梁，毕业于西安交通大学，教授，博士，主要研究方向为物理层安全；赵华，讲师，硕士，主要研究方向为移动无线通信。

中兴通讯信息

中兴通讯推出全系列电信“加密手机”：近日，中兴通讯联合中国电信推出的青漾3、星星2号和天机3电信版“加密手机”，获得国家密码管理局认证。中兴通讯成为目前唯一推出了低、中、高价位全系列加密手机的国产厂商。

据了解，中兴加密手机采用的是国密级别的加密算法，能够为用户提供商密级别的端到端的手机通信加密功能，这意味着用户的通话、短信甚至是微信全程都是密文传送方式。即便不法分子对手机进行窃听或信息窃取，也无法破解通信内容。

此外，除了启动加密通话模式避免信息被窃取之外，用户在使用过程中，还可通过开启安全模式、设置安全密码、远程信息擦除等方式对手机信息进行保护。（田军）

中兴ZXDNA演示亮相TMF：在2015年全球电信管理论坛(TMF)期间，中兴通讯重磅推出深度网络流量分析工具ZXDNA，该系统将网络流量进行可视化运维，为网络规划提供强有力的依据，支撑业务经营。

中兴通讯ZXDNA网络流量分析解决方案，将网管中搜集到的海量数据去粗取精，抽取有价值的信息，并且结合丰富的报表形式进行展示，同时可设置阈值自动告警，定期生成报表，进行邮件、短信推送，网络流量趋势、负载情况和热点问题一目了然，尽在掌握。

这一系统可有效地指导运营商合理规划网络，优化网络结构，避免网络拥塞。并且可建立流量档案，合理安排重大活动的支撑保障工作，为网络日常维护和市场运营提供流量分析数据参考。（田军）

中兴微电子携手奇虎360：近期，在巴西首都巴西利亚召开的中巴工商峰会上，中国奇虎360公司与巴西PSafe公司签署协议，联手中兴通讯微电子以及巴西第二大移动运营商TIM展开四方合作。

中兴通讯微电子为该项目4G智能路由器产品提供自主研发的最新Wise-Fone 7520 LTE多模终端芯片解决方案，通过巴西运营商TIM的4G/LTE网络，为巴西所有出租车乘客提供安全、免费、便捷和高速的Wi-Fi上网服务。同时该项目将服务2016年里约热内卢奥运会，为全球游客提供安全快捷的4G上网服务，助力巴西构建国际化“智慧城市”。（田军）

中兴100G OTN获工信部OTN入网证：近日，中兴通讯100G OTN产品ZXONE 9700通过了工信部严格的测试验证，获得最新的100G OTN入网证。

ZXONE 9700系列产品是中兴通讯最新推出的面向100G和超100G的全新统一交换OTN设备，线路侧支持10G/40G/100G/400G速率，支持OTN/Packet/TDM统一交叉，可实现2.2T~28.8T阶梯化的ODUk大容量电层交叉和光层交叉及分组交换功能。其适用于骨干核心层以及本地/城域网络，可充分满足运营商对大颗粒数据业务的透明传输、灵活调度、汇聚处理以及对业务管理监控的需求。（田军）

亨通光电获CNAS认可

日前，江苏亨通光电股份有限公司（简称：亨通光电）光电传输检测实验中心顺利通过了中国合格评定国家认可委员会（CNAS）认可，认可范围涉及161个标准、138个检测项目、64类产品。其中微缆气吹试验场是全国首家通过CNAS认可的标准气吹试验场。CNAS是由国家认证认可监督管理委员会批准设立并授权的国家认可机构，统一负责对认证机构、实验室和检查机构等相关机构的认可工作。（乔方）