WILEY

物联网通信安全及解决方案

[美] 于尔基 T.J.潘蒂宁（Jyrki T.J.Penttinen） 著

李爱萍 冯秀芳 陈健 等译

Wireless Communications Security Solutions for the Internet of Things

机械工业出版社
CHINA MACHINE PRESS

物联网通信安全及解决方案

Wireless Communications Security: Solutions for the Internet of Things

[美] 于尔基 T. J. 潘蒂宁 (Jyrki T. J. Penttinen) 著
李爱萍 冯秀芳 陈 健 等译

机械工业出版社

图书在版编目（CIP）数据

物联网通信安全及解决方案/（美）于尔基·T. J. 潘蒂宁（Jyrki T. J. Penttinen）著；李爱萍等译. —北京：机械工业出版社，2018.3

书名原文：Wireless Communications Security: Solutions for the Internet of Things

ISBN 978-7-111-59004-0

Ⅰ. ①物… Ⅱ. ①于… ②李… Ⅲ. ①互联网络-应用-计算机通信-安全技术②智能技术-应用-计算机通信-安全技术 Ⅳ. ①TP393.4②TP18

中国版本图书馆 CIP 数据核字（2018）第 014439 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：吕 潇 责任编辑：朱 林

责任校对：张 薇 封面设计：马精明

责任印制：孙 炜

北京玥实印刷有限公司印刷

2018 年 4 月第 1 版第 1 次印刷

169mm×239mm · 21 印张 · 362 千字

0001—2500 册

标准书号：ISBN 978-7-111-59004-0

定价：99.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务

服务咨询热线：010-88361066 机 工 官 网：www.cmpbook.com

读者购书热线：010-68326294 机 工 官 博：weibo.com/cmp1952

010-88379203 金 书 网：www.golden-book.com

封面无防伪标均为盗版 教育服务网：www.cmpedu.com

本书是一本介绍无线通信安全的基本原理、物联网应用及其最新研究进展的书籍，全书内容可分为三部分。本书第一部分介绍无线通信安全相关的基础知识，包括：第1章简单介绍无线安全的概念、原理和标准化机构；第2章主要描述与现代无线和移动系统最为相关的安全结构；本书第二部分为第3~7章，分别介绍无线系统安全通信涉及的5个方面及其解决方案：物联网，智能卡和安全元件，无线支付和访问系统，无线安全平台和功能，移动订阅管理；本书第三部分给出无线通信中的风险和保护措施以及无线安全的未来。本书针对物联网安全问题，基本涵盖了无线通信安全从概念、标准、构成、发展到最新进展的全部内容。

本书可以为无线电应用与管理领域、物联网技术与应用领域内政府机关、科研院所、高等学校、企事业单位的管理者、经营者、科研人员提供借鉴，也可作为高等院校研究生、高年级本科生学习物联网领域无线通信安全的教材，还可供相关专业技术人员和教研人员参考。

译者序

物联网是一个涉及计算机科学与技术、通信工程、电子工程、软件工程等多学科范畴的新的业务和应用领域，无线通信是构成物联网中物物相连的重要组成部分。物联网中的安全问题随着无线通信技术的发展和推广，与每个参与物联网的个体紧密相关。本书主要讨论无线通信安全问题针对物联网的解决方案，对于物联网业务和应用的逐步实施和普及具有非常重要的指导作用。

本书是一本针对物联网通信安全基础内容的入门读物，介绍与无线电接入网络安全解决方案相关的主要标准、框架、元器件、产品等方面，以及防止恶意尝试的常规保护措施，涉及物联网、无线通信及其安全知识的来源和最新发展。在内容编排上，本书既保持学科的广度，又兼顾物联网中无线通信安全内容的深度，并把握了最新的技术发展趋势。本书力求在一个宽泛的知识背景下，使读者能够对物联网中涉及的无线通信安全的内容有一个总体的概念，并在此基础上，为以后更深层次的物联网无线通信安全业务及应用做好铺垫。这也是作者将宽广的无线通信安全技术及其物联网应用浓缩到这本书中的良苦用心，其中还包含了作者多年来在移动通信技术和网络相关公司工作的经验积累，以及与移动设备制造商一起工作期间的感受和体会，这些都为物联网无线通信安全的解决方案提供了有益的思路和指导。

本书深入浅出，引人入胜，摆脱了常规书籍过多地深入讨论理论技术细节的框架束缚。作者的用意显然是从物联网应用的角度出发，为读者奠定无线通信安全所需要的基本知识，架起进一步深入学习和应用物联网无线通信安全的桥梁，特别是为读者提供在物联网应用中用于确保无线通信安全的不同解决方案，并通过每章提供的参考文献、网站为读者提供进一步深入学习的参考指南。

这本书既适合国内无线电应用与管理领域、物联网技术与应用领域相关人员了解物联网无线通信安全解决方案时的借鉴和参考，也可作为高等院校研究生、高年级本科生学习物联网领域无线通信安全的教材，或供非物联网专业相关技术人员和教研人员参考。

由于本书涉及面广，技术内容新，有一定的翻译难度，为此，我们几位从事物联网专业教学的老师在翻译过程中字斟句酌，力求做到既忠实于原文，又不失中文语义理解的一般性。此外，因为文中出现大量的缩略语，为使读者逐

步熟悉缩略语内容，能够轻松理解缩略语在不同上下文中的准确含义，除了专用的缩略语对照翻译外，书中给第一次出现的缩略语提供全称及中文翻译，但在后文再次出现时一般是中文加缩略语或者直接以缩略语的形式出现。鉴于译者自身的知识局限及时间仓促，译稿中难免有不妥或疏漏之处，谨向原书作者表示歉意，若读者在阅读过程中发现我们的工作有不足之处，敬请广大读者批评指正。

参与本书翻译工作的主要是太原理工大学负责物联网工程专业教学和科研工作的相关老师。本书的翻译是分工合作的结果，并经过了多轮校对和修订。分工如下：李爱萍（第1、10章）、陈健（第2章）、冯秀芳（第3章）、段利国（第4章）、曹棣（第5、6、7章）、兰方鹏（第8、9章），其余部分由李爱萍翻译。全书由李爱萍负责统稿和审校。

很高兴能将本书推荐给读者，希望拿起本书的读者都能获益匪浅。

译者

E-MAIL：tyutli@163.com

原书前言

这本介绍无线通信安全的书籍总结了与无线电接入网络安全解决方案有关的关键方面的内容，以及防止恶意尝试的保护。由于大量的服务依赖于互联网及其日益重要的无线电接入方式，因此，适当的屏蔽是至关重要的。随着无线通信系统（如 Wi-Fi 和蜂窝网络）的普及，服务的使用常常通过无线电设备进行，如通过支持短距离和长距离无线电接入技术的智能手机和笔记本电脑。目前对这些服务和设备的威胁正在增加，攻击者的动机之一是利用用户凭证和其他机密来获得金钱利益。犯罪分子攻击无线电系统还有很多其他原因，因此需要用户、运营商、服务提供商、设备制造商、标准化机构和其他利益相关者采用越来越复杂的保护方法。

随着信息产业和通信技术的全面发展，这些年来环境发生了巨大变化。在 20 世纪 80 年代，对移动通信的威胁仅仅与克隆用户的电话号码有关，以便在无保护的无线电接口上进行免费电话呼叫和窃听语音通话。从保护相对较差的第一代移动网络的经验来看，现代无线通信系统已经以更先进的方式逐渐考虑到安全威胁，而攻击也正在变得越来越复杂，涉及更多样化的动机，如故意破坏服务和赎金型威胁。除了对终端用户的所有这些威胁之外，针对运营商、服务提供商和其他利益相关者的安全漏洞也在增加。换句话说，我们正在进入一个网络世界，通信服务是这个新时代的一个基本组成部分。

互联网在我们的日常生活中扮演着不可或缺的角色，其服务中出现的重大故障所带来的后果将导致混乱。适当屏蔽恶意攻击的企图需要一个完整的和及时更新的网络安全系统，以保护诸如银行机构、能源分配和电信基础设施等社会的基本功能。与物联网（Internet of Thing，IoT）相关的趋势，即，估计在短时间内将有数百亿台设备投入使用，而其中很大比例是较便宜的 IoT 设备，可能往往缺乏自己的保护机制，因此这就意味着环境将会变得更具挑战性。这些看似无害的连接设备，如智能家用电器——如果部署和设置不当——可能会使家庭网络、其服务和信息容器更深地暴露出来，并进一步打开安全漏洞，进入商业网络。这是现代无线安全准备的关键领域之一。

正如我的好朋友阿尔弗雷多所总结的那样，互联网可以比作核能，它在控制之下非常有用，但一旦出现安全威胁，就可能导致重大灾难的发生。毫无疑

问，适当的保护是必不可少的。本书通过总结典型的、目前使用的服务和解决方案，介绍了无线安全的解决方案和挑战，并通过提出新颖的解决方案——如先进的移动订阅管理的概念——来描绘未来的图景。我希望读者能在你的工作和研究中发现有趣的和相关的内容，并对这一领域所建立的和尚未形成的解决方案进行总结。本书中的内容还可以通过电子书格式阅读，您可以在 www. tlt. fi 的主题中找到更多的信息和更新，这些内容补充了无线安全的总体情况。就像我以前在 Wiley 出版的书一样，我很乐意通过我的电子邮件地址（jyrki. penttinen@ hotmail. com）直接收到您关于这本无线通信安全书籍的宝贵反馈。

Jyrki T. J. Penttinen
美国新泽西州莫里斯敦

致　谢

将无线安全方面的所有信息收集到一本书中是一项非常有趣的任务。我认为许多已经提出的解决方案往往会发展得非常快，因为威胁越来越复杂和新奇。当然，挑战在于保持书面材料的相关性。随着消费者和 M2M（Machine-to-Machine，机器对机器）领域的所有进步，利益相关者同样难以确保对无线通信网络、设备、移动应用和服务的正确屏蔽——不要忘记物联网（IoT）的整体发展，目前正在受到重大关注。即便如此，我相信这些基础还是值得用一本书的方式来描述的，而给出的每一个领域的最新进展都可以通过确定的关键参考文献和信息的根源进行检查。

本书的一个重要部分，即基础知识的描述，是我在职业生涯中与移动网络运营商以及网络和设备供应商合作过程一直参与其中的事情，而其余的内容则通过完整的画面展示最新的进展，例如，嵌入式 SIM 卡和相应的订阅管理，将在不久的将来以最有效的方式与消费者的移动和配套设备以及越来越多的 IoT 设备高度相关。感谢所有我有幸与之合作、并交流有关移动安全的想法的同事。我想特别提到捷德（Giesecke & Devrient）公司的重要作用，它为我提供了在当前位置上关注这个话题的可能性。

我衷心感谢 Wiley 团队的专业工作，以坚定而又温和的方式，确保图书项目和进度表按照计划完成。特别感谢 Mark Hammond、Sandra Grayson、Tiina Wigley 和 Nithya Sechin 以及 Tessa Hanford 等，帮助我确保这本书的定稿顺利进行。

我还要向芬兰非小说作家协会表示由衷的感谢，感谢他们的支持。

最后，我要感谢 Elva、Stephanie、Carolyne、Miguel、Katriina 和 Pertti，感谢他们所有的支持。

Jyrki T. J. Penttinen

美国新泽西州莫里斯敦（Morristown，NJ，USA）

缩略语

3DES	Triple-Data Encryption Standard	三重数据加密算法
3GPP	3rd Generation Partnership Program	第三代合作伙伴计划
6LoWPAN	IPv6 Low power Wireless Personal Area Network	IPv6 低功耗无线个人区域网
AAA	Authentication, Authorization and Accounting	认证、授权和计费
AAS	Active Antenna System	有源天线系统
ACP	Access Control Policy	访问控制策略
ADF	Application Dedicated File	应用程序专用文件
ADMF	Administration Function	管理功能
ADSL	Asymmetric Digital Subscriber Line	非对称数字用户线
ADT	Android Developer Tool	安卓开发工具
AES	Advanced Encryption Standard	高级加密标准
AF	Authentication Framework	认证框架
AID	Application ID	应用程序标识符
AIDC	Automatic Identification and Data Capture	自动识别和数据采集
AIE	Air Interface Encryption	空中接口加密
AK	Anonymity Key	匿名密钥
AKA	Authentication and Key Agreement	认证和密钥协商
ALC	Asynchronous Layered Coding	异步分层编码
AMF	Authenticated Management Field	(身份) 认证管理域
AMI	Advanced Metering Infrastructure	智慧型电表基础建设
AMPS	Advanced Mobile Phone System	高级移动电话系统
ANDSF	Access Network Discovery and Selection Function	接入网发现与选择功能
ANSI	American National Standards Institute	美国国家标准协会
AOTA	Advanced Over-The-Air	空中推进
AP	Access Point	接入点
AP	Application Provider	应用提供商
APDU	Application Protocol Data Unit	应用协议数据单元
API	Application Programming Interface	应用程序接口
AR	Aggregation Router	聚合路由器
ARIB	Association of Radio Industries and Businesses	(日本) 无线电工业和商业协会
AS	Access Stratum	接入层
AS	Authentication Server	认证服务器

ASIC	Application-Specific Integrated Circuit	应用型专用集成电路
ASME	Access Security Management Entity	接入安全管理实体
ASN.1	Abstract Syntax Notation One	抽象语法表示法
ATCA	Advanced Telecommunications Computing Architecture	高级电信计算体系结构
ATIS	Alliance for Telecommunications Industry Solutions	电信行业解决方案联盟
ATR	Answer to Reset	复位应答
ATSC	Advanced Television Systems Committee	高级电视系统委员会
AuC	Authentication Centre	认证中心
AUTN	Authentication Token	认证令牌
AV	Authentication Vector	认证向量，鉴权矢量
AVD	Android Virtual Device	安卓虚拟设备
BAN	Business/Building Area Network	商业/建筑区域网
BCBP	Bar Coded Boarding Pass	条形码登机牌
BCCH	Broadcast Control Channel	广播控制频道
BE	Backend	后端
BGA	Ball Grid Array	球栅阵列
BIN	Bank Identification Number	银行识别码（发卡银行代号）
BIP	Bearer-Independent Protocol	独立承载协议
BLE	Bluetooth, Low-Energy	蓝牙，低能耗
BM-SC	Broadcast-Multicast Service Centre	广播-组播服务中心
BSC	Base Station Controller	基站控制器
BSP	Biometric Service Provider	生物识别服务提供商
BSS	Billing System	计费系统
BSS	Business Support System	业务支持系统
BTS	Base Transceiver Station	基站收发信台
C2	Command and Control	指挥和控制
CA	Conditional Access	条件访问
CA	Carrier Aggregation	载波聚合
CA	Certificate Authority	凭证管理中心；认证机构
CA	Controlling Authority	控制机构；监管部门
CAT	Card Application Toolkit	卡应用工具包
CAT_TP	Card Application Toolkit Transport Protocol	卡应用工具包传输协议
CAVE	Cellular Authentication and Voice Encryption	蜂窝认证和语音加密
CB	Cell Broadcast	小区广播
CBEFF	Common Biometric Exchange Formats Framework	常见的生物特征交换格式框架
CC	Common Criteria	通用标准
CC	Congestion Control	拥塞控制
CCM	Card Content Management	卡内容管理
CCMP	Counter-mode Cipher block chaining Message authentication code Protocol	计数器模式密码块链接消息认证码协议
CCSA	China Communications Standards Association	中国通信标准化协会

CDMA	Code Division Multiple Access	码分多址
CEIR	Central EIR	中央 EIR
CEPT	European Conference of Postal and Telecommunications Administrations	欧洲邮电行政会议
CFN	Connection Frame Number	连接帧号
CGN	Carrier-Grade NAT	运营商级 NAT
CHV	Chip Holder Verification	芯片持有人验证
CI	Certificate Issuer	证书发行机构
CK	Cipher Key	密码密钥
CL	Contactless	非接触式
CLA	Class of Instruction	教学类
CLF	Contactless Frontend	非接触前端
CLK	Clock	时钟
CMAS	Commercial Mobile Alert System	商业移动预警系统
CMP	Certificate Management Protocol	证书管理协议
CN	Core Network	核心网
CoAP	Constrained Application Protocol	受限应用协议
CoC	Content of Communication	通信的内容
CPU	Central Processing Unit	中央处理单元
CS	Circuit Switched	电路交换
CSFB	Circuit Switched Fallback	电路交换回退
CSG	Closed Subscriber Group	封闭用户组
CSS7	Common Signaling System	通用信令系统
CVM	Cardholder Verification Method	持卡人验证方法
DBF	Database File	数据库文件
DD	Digital Dividend	数字红利
DDoS	Distributed Denial-of-Service	分布式拒绝服务攻击
DE	Data Element	数据元素
DES	Data Encryption Standard	数据加密标准
DF	Dedicated File	专用文件
DFN	Dual-Flat, No leads	双平面，无引线
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DL	Downlink	下行
DM	Device Management	设备管理
DM	Device Manufacturer	设备制造商
DMO	Direct Mode Operation	直通工作方式；直通模式
DNS	Domain Name System	域名系统
DoS	Denial-of-Service	拒绝服务
DPA	Data Protection Act	数据保护法；信息保护法
DPI	Deep Packet Inspection	深度包检测
DRM	Digital Rights Management	数字版权管理

DS	Data Synchronization	数据同步
DSS	Data Security Standard	数据安全标准
DSSS	Direct Sequence Spread Spectrum	直接序列扩频
DTLS	Datagram Transport Layer Security	数据报传输层安全
DTMB	Digital Terrestrial Multimedia Broadcast	数字地面多媒体广播
DVB	Digital Video Broadcasting	数字视频广播
EAL	Evaluation Assurance Level	评估保证级别
EAN	Extended Area Network	扩展区域网络
EAP	Extensible Authentication Protocol	扩展认证协议
EAPoL	Extensible Authentication Protocol over Local Area Network	局域网上的可扩展认证协议
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security	可扩展认证协议-隧道传输层安全性
ECASD	eUICC Controlling Authority Secure Domain	eUICC 控制权限安全域
eCAT	Encapsulated Card Application Toolkit	封装卡应用程序工具包
ECC	Elliptic Curve Cryptography	椭圆曲线密码学
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
ECO	European Communications Office	欧洲通信办公室
EDGE	Enhanced Data Rates for Global Evolution	用于全球演进的增强数据速率
EEM	Ethernet Emulation Mode	以太网仿真模式
EEPROM	Electrically Erasable Read-Only Memory	电可擦只读存储器
EF	Elementary File	基本文件
EGAN	Enhanced Generic Access Network	增强型通用接入网络
EID	eUICC Identifier	eUICC 标识符
EIR	Equipment Identity Register	设备标识寄存器
E-MBS	Enhanced Multicast Broadcast Service	增强型组播广播业务
EMC	Electro-Magnetic Compatibility	电磁兼容
EMF	Electro-Magnetic Field	电磁场
EMI	Electro-Magnetic Interference	电磁干扰
EMM	EPS Mobility Management	EPS 移动管理
EMP	Electro-Magnetic Pulse	电磁脉冲
eNB	Evolved Node B	演进节点 B
EPC	Enhanced Packet Core	增强分组核心
EPC	Evolved Packet Core	演进分组核心
EPS	Electric Power System	电力系统
EPS	Enhanced Packet System	增强分组系统
ERP	Enterprise Resource Planning	企业资源规划
ERTMS	European Rail Traffic Management System	欧洲铁路交通管理系统
eSE	Embedded Security Element	嵌入式安全元件
eSIM	Embedded Subscriber Identity Module	嵌入式用户识别模块
ESN	Electronic Serial Number	电子序列号

ESP	Encapsulating Security Payload	封装安全有效负荷
ETSI	European Telecommunications Standards Institute	欧洲电信标准协会
ETWS	Earthquake and Tsunami Warning System	地震和海啸预警系统
eUICC	Embedded Universal Integrated Circuit Card	嵌入式通用集成电路卡
EUM	eUICC Manufacturer	eUICC 制造商
E-UTRAN	Enhanced UTRAN	增强型 UTRAN
EV-DO	Evolution Data Only/Data Optimized	仅用于演进数据/数据优化
FAC	Final Approval Code	最终批准代码
FAN	Field Area Network	场域网络
FCC	Federal Communications Commission	(美国) 联邦通信委员会
FDD	Frequency Division Multiplex	频分复用
FDT	File Delivery Table	文件传送表
FEC	Forward Error Correction	前向纠错
FF	Form Factor	(电子产品等的) 物理尺寸和形状、规格
FICORA	Finnish Communications Regulatory Authority	芬兰通信管理局
FID	File-ID	文件 ID
FIPS	Federal Information Processing Standards	联邦信息处理标准
FLUTE	File Transport over Unidirectional Transport	单向传输的文件传输
FM	Frequency Modulation	频率调制
FPGA	Field Programmable Gate Array	现场可编程门阵列
GAA	Generic Authentication Architecture	通用认证架构
GBA	Generic Bootstrapping Architecture	通用引导架构
GCSE	Group Communication System Enabler	组通信系统启用器
GEA	GPRS Encryption Algorithm	GPRS 加密算法
GERAN	GSM EDGE Radio Access Network	GSM 边缘无线电接入网
GGSN	GPRS Gateway Support Node	GPRS 网关支持节点
GMSK	Gaussian Minimum Shift Keying	高斯最小偏移键控
GoS	Grade of Service	服务等级
GP	GlobalPlatform	全球平台
GPRS	General Packet Radio Service	通用分组无线电业务
GPS	Global Positioning System	全球定位系统
GRX	GPRS Roaming Exchange	GPRS 漫游交换
GSM	Global System for Mobile Communications	全球移动通信系统
GSMA	GSM Association	GSM 协会
GTP	GPRS Tunnelling Protocol	GPRS 隧道协议
GUI	Graphical User Interface	图形用户界面
HAN	Home Area Network	家庭区域网络
HCE	Host Card Emulation	主机卡仿真
HCI	Host Controller Interface	主机控制器接口
HE	Home Environment	家庭环境

HF	High Frequency	高频率
HFN	Hyperframe Number	超帧号
HIPAA	Health Insurance Portability and Accountability Act	健康保险携带和责任法案
HLR	Home Location Register	归属位置寄存器
HNB	Home Node B	家庭节点
HRPD	High Rate Packet Data	高速分组数据
HSPA	High Speed Packet Access	高速分组接入
HSS	Home Subscriber Server	归属用户服务器
HTTPS	HTTP Secure	HTTP 安全
HW	Hardware	硬件
I/O	Input/Output	输入/输出
I^2C	Inter-Integrated Circuit	内部集成电路
IAN	Industrial Area Network	工业区域网
IANA	Internet Assigned Numbers Authority	互联网号码分配机构
IARI	IMS Application Reference ID	IMS 应用程序参考 ID
ICAO	International Civil Aviation Organization	国际民航组织
ICC	Integrated Circuit Card	集成电路卡
ICCID	ICC Identification Number	ICC 识别号码
ICE	In Case of Emergency	紧急情况
ICE	Intercepting Control Element	拦截控制元件
ICIC	Inter Cell Interference Control	小区间干扰控制
ICT	Information and Communication Technologies	信息通信技术
IDE	Integrated Development Environment	集成开发环境
IDEA	International Data Encryption Algorithm	国际数据加密算法
ID-FF	Identity Federation Framework	身份联盟框架
IDM	Identity Management	身份管理
IDS	Intrusion Detection System	入侵检测系统
ID-WSF	Identity Web Services Framework	身份 Web 服务框架
IEC	International Electrotechnical Commission	国际电工委员会
IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程师学会
IETF	Internet Engineering Task Force	互联网工程任务组
IF	Intermediate Frequency	中频
IK	Integrity Key	完整性密钥
IKE	Internet Key Exchange	互联网密钥交换
IMEI	International Mobile Equipment Identity	国际移动设备标识
IMEISV	IMEI Software Version	IMEI 软件版本
IMS	IP Multimedia Subsystem	IP 多媒体子系统
IMSI	International Mobile Subscriber Identity	国际移动用户识别
IOP	Interoperability Process	互操作性过程
IoT	Internet of Things	物联网
IOT	Inter-Operability Testing	互操作性测试

IP	Internet Protocol	互联网协议
IPS	Intrusion Prevention System	入侵预防系统
IPSec	IP Security	IP 安全
IR	Infrared	红外线
IRI	Intercept Related Information	监听（拦截）相关信息
ISD	Issuer Security Domain	发行者安全域
ISDB-T	Terrestrial Integrated Services Digital Broadcasting	地面综合业务数字广播
ISD-P	Issuer Security Domain Profile	发行者安全域配置文件
ISD-R	Issuer Security Domain Root	发行者安全域根
ISIM	IMS SIM	国际移动用户身份模块
ISO	International Organization for Standardization	国际标准化组织
ISOC	Internet Society	互联网协会
ITSEC	Information Technology Security Evaluation Criteria	信息技术安全评估标准
ITU	International Telecommunications Union	国际电信联盟
IWLAN	Interworking Wireless Local Area Network	互通无线局域网
JBOH	JavaScript-Binding-Over-HTTP	HTTP 上的 JavaScript 绑定
JTC	Joint Technical Committee	联合技术委员会
K	User Key	用户密钥
KASME	Key for Access Security Management Entity	接入安全管理实体密钥
KDF	Key Derivation Function	密钥导出函数
LA	Location Area	位置区域
LAN	Local Area Network	局域网
LBS	Location Based Service	基于位置的服务
LCT	Layered Coding Transport	分层编码传输
LEA	Law Enforcement Agencies	执法机构
LEAP	Lightweight Extensible Authentication Protocol	轻量级可扩展认证协议
LEMF	Law Enforcement Monitoring Facilities	执法监控设施
LF	Low Frequency	低频
LI	Legal/Lawful Interception	法律/合法拦截
LIF	Location Interoperability Forum	位置互操作论坛
LIG	Legal Interception Gateway	合法监听（拦截）网关
LLCP	Logical Link Control Protocol	逻辑链路控制协议
LoS	Line-of-Sight	视线
LPPM	Location-Privacy Protection Mechanism	位置隐私保护机制
LTE	Long Term Evolution	长期演进（技术名）
LTE-M	LTE M2M	LTE M2M
LTE-U	LTE Unlicensed	非授权频段 LTE
LUK	Limited Use Key	有限使用密钥
LWM2M	Lightweight Device Management of M2M	M2M 轻量级设备管理
M2M	Machine-to-Machine	机器对机器
MAC	Medium Access Control	媒体访问控制

MAC	Message Authentication Code	消息认证码
MBMS	Multimedia Broadcast and Multicast Service	多媒体广播和组播服务
MC	Multi Carrier	多载波
MCC	Mobile Country Code	移动国家代码
MCPTT	Mission Critical Push To Talk	关键任务一键通
ME	Mobile Equipment	移动设备
ME ID	Mobile Equipment Identifier	移动设备标识符（识别码）
MF	Master File	主文件
MFF2	Machine-to-Machine Form Factor 2	M2M 规格 2
MGIF	Mobile Gaming Interoperability Forum	移动游戏互操作论坛
MIM	Machine Identity Module	机器识别模块
MIMO	Multiple In Multiple Out	多输入多输出
MITM	Man in the Middle	中间人
MM	Mobility Management	移动管理
MME	Mobility Management Entity	移动管理实体
MMS	Multimedia Messaging	多媒体消息
MNC	Mobile Network Code	移动网络代码
MNO	Mobile Network Operator	移动网络运营商
MPLS	Multiprotocol Label Switching	多协议标签交换
MPU	Multi Processing Unit	多处理单元
MRTD	Machine Readable Travel Document	机读旅行证件
MSC	Mobile Services Switching Centre	移动业务交换中心
MSISDN	Mobile Subscriber's ISDN number	移动用户的 ISDN 号码
MSP	Multiple Subscriber Profile	多用户配置文件
MST	Magnetic Secure Transmission	磁安全传输
MT	Mobile Terminal	移动终端
MTC	Machine-Type Communications	机器类通信
MVNO	Mobile Virtual Network Operator	移动虚拟网络运营商
MVP	Minimum Viable Product	最小可行产品
MWIF	Mobile Wireless Internet Forum	移动无线互联网论坛
NAA	Network Access Application	网络访问应用程序
NACC	Network Assisted Call Control	网络辅助呼叫控制
NAF	Network Application Function	网络应用功能
NAN	Neighborhood Area Network	邻近区域网络
NAS SMC	NAS Security Mode Command	NAS 安全模式命令
NAS	Non-Access Stratum	非接入层
NAT	Network Address Translation	网络地址转换
NB	Node B	节点 B
NCSC-FI	National Cyber Security Centre of Finland	芬兰国家网络安全中心
NDEF	NFC Data Exchange Format	NFC 数据交换格式
NDS	Network Domain Security	网络域安全