国 际 电 信 联 盟

ITU-T X.1364

国际电信联盟
电信标准化部门

(03/2020)

X系列：数据网、开放系统通信和安全性

安全应用和服务(2)– 物联网（IoT）安全

窄带物联网的安全要求和框架

ITU-T X.1364建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务(1)	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议(1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	**X.1360–X.1369**
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	X.1700–X.1729

ITU-T X.1364建议书

窄带物联网的安全要求和框架

摘要

由于电信技术的发展，在移动通信领域，通信模式正在从人与人向人与物以及物与物转变，从而不可避免地向物联网演进。

与短距离通信技术（例如蓝牙、ZigBee等）相比，具有覆盖范围广、移动性和广泛连接的蜂窝移动网络（可能带来更丰富的应用场景）被认为已成为物联网的主要互联技术。

窄带物联网（NB-IoT）基于蜂窝移动网络，它使用的带宽约为180 kHz，可以部署在全球移动通信系统（GSM）网络、通用移动通信系统（UMTS）网络或长期演进（LTE）网络上，以降低成本并实现平稳升级。

NB-IoT以其功耗低、覆盖范围广、成本低、容量大等特点，有望在多个垂直行业得到广泛应用。

作为一种新技术，NB-IoT有其自身的特点，可能带来新的安全问题，为了保证NB-IoT部署和应用的安全，需要分析NB-IoT特有的安全威胁和相关安全要求，建立NB-IoT的整体安全框架。

本建议书旨在分析NB-IoT的潜在部署方案和典型应用场景。书中阐述了针对NB-IoT部署的安全威胁和要求，从而为运营商建立了安全框架，以保护这些新技术应用。

历史沿革

版本	建议书	批准日期	研究组	唯一标识（ID）*
1.0	ITU-T X.1364	2020-03-26	17	11.1002/1000/14088

关键字

框架、物联网、窄带、安全要求。

* 为获取本建议书，请在网页浏览器内键入URLhttp://handle.itu.int/，然后输入唯一ID。例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信和信息通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“须”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1364建议书

窄带物联网的安全要求和框架

1 范围

本建议书分析了窄带物联网（NB-IoT）的潜在部署方案和典型应用场景。它规定了针对NB-IoT部署的安全威胁和要求，从而为运营商建立了安全框架，以保护该新NB-IoT技术的应用。

2 参考文献

下列ITU-T建议书和其他参考文献包含的条款，通过本文的引用构成本建议书的条款。在出版时，所指示的版本有效。所有建议书和其他参考文献均可能进行修订；因此，鼓励本建议书的用户研究应用建议书最新版本和下面列出的其他参考文献的可能性。定期发布当前有效的ITU-T建议书清单。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ETSI TS 123 401] ETSI TS 123 401 V15.8.0 (2019-10), LTE; *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 15.8.0 Release 15)*.

[ETSI TS 123 501] ETSI TS 123 501 V15.6.0 (2019-10), 5G; *System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.6.0 Release 15)*.

3 定义

3.1 它处定义的术语

本建议书使用了它处定义的以下术语：

3.1.1 认证（authentication）[b-ITU-T X.1141]：在一定程度的信任范围内，确定某人或某事事实上是其自身所宣称的人或事的过程。

3.1.2 能力（capability）[b-ITU-T X.1145]：一个系统或设备提供一种服务的能力。

3.1.3 蜂窝物联网（Cellular IoT）[ETSI TS 123 401]：支持物联网的低复杂度和低吞吐量设备的蜂窝网络。蜂窝物联网同时支持IP和非IP业务。

3.1.4 数据完整性（data integrity）[b-ITU-T X.800]：数据未被以未授权方式修改或破坏的特性。

3.1.5 加密（encryption）[b-ITU-T X.800]：对数据进行加密转换（参见“密码学”），以生成密文。

注 – 加密可能是不可逆转的，在这种情况下，相应的解密过程不能切实执行。

3.1.6 实体（entity）[b-ITU-T X.1252]：单独和独立存在的任何事物，可在语境内识别。

注 – 实体可以为真人、动物、法人、组织、主动或被动之物、设备、软件应用、服务等或上述实体的组合。在电信中，实体的例子包括接入点、订户、用户、网元、网络、软件应用、服务和设备、接口等。

3.1.7 分组核心演进（Evolved Packet Core）[b-ITU-T Q.1743]：是一个适用于3GPP系统向更高数据速率、更低时延、支持多个无线电接入技术（RAT）的分组优化系统演进或迁移的框架。

3.1.8 分组系统演进（Evolved Packet System）[b-ITU-T Q.1743]：是第三代（3G）UMTS的演进，其特征是支持多RAT的更高数据速率、更低时延、分组优化系统，分组系统演进包括分组核心演进以及无线电接入网演进。（E-UTRA和E-UTRAN）

3.1.9 密钥管理（key management）[b-ITU-T X.800]：依据安全策略生成、存储、分发、删除、存档和应用密钥。

3.1.10 窄带物联网（Narrowband-IoT）[ETSI TS 123 401]：构成蜂窝物联网一部分的3GPP无线电接入技术。它允许通过E-UTRA接入网络服务，信道带宽限制为180 kHz（对应于一个PRB）。除非在条款中另有说明，窄带物联网是E-UTRAN的一个子集。

3.1.11 威胁（threat) [b-ITU-T X.800]：安全的某种潜在冲突。

3.2 本建议书中定义的术语

本建议书定义了以下术语：

3.2.1 蜂窝物联网服务网关节点（SGN）：蜂窝物联网服务网关节点（SGN）是一种组合节点演进分组核心（EPC）实现选项，通过在控制和用户平面路径中配置演进分组系统（EPS）实（例如，移动性管理实体（MME）、服务网关（S-GW）和分组数据网络网关（P-GW）），使物理实体的数量最小化，这在CIoT部署中可能是优先选项。

注 – 本定义中列出的功能请参考[ETSI TS 123 401]。

3.2.2 节点B演进（Evolved Node B）（eNodeB）：一种无线接入节点，具有无线电资源管理、上行数据解压和用户数据流加密、用户平面数据路由等功能。

注 – 在这个定义中列出的功能可参考[ETSI TS 123 401]。

3.2.3 通用地面无线电接入网演进（E-UTRAN）：一种无线电接入网，其功能包括报头压缩和用户平面加密、MME选择、上行链路和下行链路承载级别速率执行、承载级别准入控制、拥塞控制等。

注 – 该定义中列出的功能参考[ETSI TS 123 401]。

3.2.4 家庭订户服务器（Home Subscriber Server）（HSS）：具有用户订阅信息存储和管理功能的移动核心网元。

注 – 该定义中列出的功能参考[ETSI TS 123 401]。

3.2.5 移动性管理实体（Mobility Management Entity）（MME）：一种具有跟踪区域列表管理、用户设备（UE）位置映射、服务网关（S-WG）和分组数据网络网关（P-WG）选择、切换选择、认证、授权、承载管理等功能的移动核心网单元。

注 – 该定义中列出的功能参考[ETSI TS 123 401]。

3.2.6 分组数据网网关（Packet Data Network Gateway）（P-WG）：一种移动核心网元，具有基于每个用户的分组过滤、用户设备（UE）互联网协议（IP）地址分配、传输级别分组标记、服务级别收费等功能。

注 – 该定义中列出的功能参考[ETSI TS 123 401]。

3.2.7 服务能力公开功能（Service Capability Exposure Function）（SCEF）：一种具有认证和授权、公开服务能力发现、策略管理、网络参数配置等功能的移动核心网元。

注 – 该定义中列出的功能参考[ETSI TS 123 401]。

3.2.8 服务网关（Serving Gateway）（S-WG）：一种移动核心网元，具有用于eNodeB间切换的本地移动性锚定点、用于3GPP间移动性的移动性锚定、分组路由和转发、传输级别分组标记、考虑运营商间计费等功能。

注 – 该定义中列出的功能参考[ETSI TS 123 401]。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

3G	第三代
3GPP	第三代合作伙伴项目
CDMA	码分多址
CIoT	蜂窝物联网
C-SGN	蜂窝物联网服务网关节点
DDoS	分布式拒绝服务
EPC	分组核心演进
eNodeB	节点B演进
EPS	分组系统演进
E-UTRAN	通用地面接入网络演进
GSM	移动通信全球系统
HSS	家庭订户服务器
IMEI	国际移动设备标识
IP	互联网协议
LTE	长期演进
MME	移动性管理实体
NB-IoT	窄带物联网
P-GW	分组数据网络网关
RAT	无线电接入技术
SCEF	服务能力公开功能
S-GW	服务网关
SMS	短消息服务
SIM	订户识别模块
UE	用户设备
UMTS	通用移动通信系统
UTRA	通用地面无线电接入

5 惯例

无。

6 NB-IoT概述

随着移动通信领域电信技术的发展，通信模式正在从人与人向人与物以及物与物转变，从而不可避免地向物联网（IoT）演进。

与短距离通信技术（例如蓝牙、ZigBee等）相比，具有覆盖范围广、移动性和广泛连接的蜂窝移动网络（可能带来更丰富的应用场景）被认为已成为IoT的主要互联技术。

NB-IoT基于蜂窝移动网络，它使用的带宽约为180 kHz，可以部署在全球移动通信系统（GSM）网络、通用移动通信系统（UMTS）网络或长期演进（LTE）网络上，以降低成本并实现平稳升级。NB-IoT的典型特性包括：

NB-IoT的典型特性包括：

– 低功耗：NB-IoT器件可使用五至十年；

– 覆盖范围广：同一频段，NB-IoT比现有网络有15-20dB的增益，覆盖面积大100倍；

– 大容量：单个NB-IoT部门可支持约100,000台设备；以及

– 低成本：一台NB-IoT设备的价格约为5美元。

NB-IoT以其功耗低、覆盖范围广、成本低、容量大等特点，有望在被运营商广泛采用，且在多个垂直行业得到广泛应用。

7 部署方案及典型应用场景

7.1 部署方案

7.1.1 使用现有移动核心网进行部署

在这个部署场景中，运营商使用现有部署的2/3/4G移动核心网部署NB-IoT。

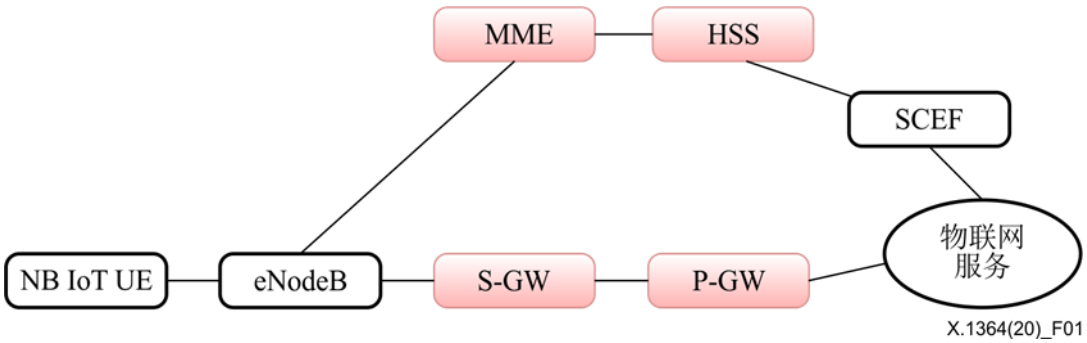
现有的移动核心网（包括移动性管理实体（MME）、服务网关（S-GW）和分组数据网络网关（P-GW））需要对NB-IoT进行优化以支持以下特性[ETSI TS 123 401]：

– 超低用户设备（UE）功耗；

– 每个单元有大量设备；

– 窄带频谱无线电接入技术（RATs），例如演进通用无线接入网（E-UTRA）、通用地面无线接入（UTRA）、GSM、CDMA2000；和

– 增强覆盖级别。



注 – 现有的移动核心网元是粉红色的。

图1 – 利用现有的移动核心网进行部署

除了这些优化的网元外，[ETSI TS 123 401]中确定的图1中的其他网元如下所示：

– 节点B演进（eNodeB）：无线接入节点，承载无线电资源管理、上行数据解压和用户数据流加密、用户平面数据路由等功能。

– 家庭订户服务器（HSS）：存储用户的订阅信息，如认证参数、位置信息等。

– 服务能力公开功能（SCEF）：它提供安全公开服务和3GPP网络接口提供的能力。

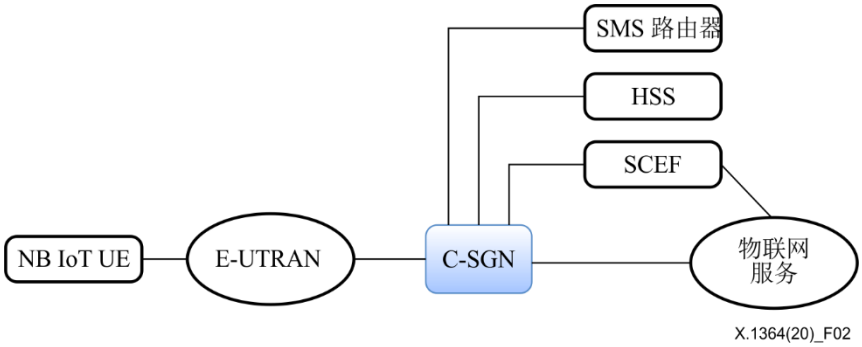
这些网元及其功能通过移动电信网络支持NB-IoT服务。

7.1.2 使用一个新建的专属移动核心网进行部署

在这个部署场景中，运营商为NB- IoT服务新建了一个专用的移动核心网。

蜂窝物联网（CIoT）服务网关节点（C-SGN）由[ETSI TS 123 401]定义。

C-SGN支持现有的分组系统演进（EPS）核心网元的子集和必要功能。它是包核心演进（EPCs）的组合节点。它实现了物理EPS实体数量最小化的选项；它在控制平面和用户平面路径中配置EPS实体功能。C-SGN结合MME、P-GW和S-GW功能，提供高度优化的CIoT解决方案，C-SGN实现支持其外部接口选项。这些接口对应于各个EPC实体的接口，如MME、S-GW和P-GW。



注 – 新建的移动核心网元为蓝色。

图2 – 使用新构建的专用移动核心网进行部署

除了新建的网元外，图2中的其他网元如下所示[ETSI TS 123 401]：

– E-UTRAN：承载上行链路中的报头压缩和用户平面加密、MME选择、承载级别速率实施、拥塞控制和传输级别分组标记等功能。

– HSS：存储和管理用户的订阅信息，如认证参数、位置信息等。

– SCEF：提供3GPP网络接口提供的安全公开服务和功能。

– 短消息服务（SMS）路由器：它支持在没有EPS附加（EPS服务和非EPS服务的请求）组合的情况下传输附加请求，此功能仅对仅支持NB-IoT的UE可用。

这些网元及其功能通过移动通信网络支持NB-IoT服务。

7.2 典型应用

7.2.1 远程抄表

在该应用场景中，NB-IoT设备用于接收家庭共用设施（例如水、煤气）的读数，并通过无线网络将结果发送给公共服务提供商。

与传统的人工抄表技术相比，采用NB-IoT技术使抄表更加方便、准确、高效。

7.2.2 智能停车

在这个应用场景中，停车场部署NB-IoT设备作为传感器来检测停车场是否还有空位。它还允许使用智能停车应用的驾驶员获得推荐的停车选择，并在线支付停车费。

使用NB-IoT技术可以解决寻找停车场的困难和相关的支付问题。

7.2.3 智慧农业

在这个应用场景中，NB-IoT设备被用作传感器来记录诸如盐度、湿度、温度等农业参数。基于这些记录，农民可以获得关于浇水或施肥解决方案的建议。

NB-IoT技术通过使用实时信息分析，而不是传统农业实践中的农民实验，因此有助于农业智慧化。

8 对NB-IoT的威胁

NB-IoT的安全威胁分析有两个有利的角度：NB-IoT的特性和NB-IoT层的功能框架视图，如第8.1节和第8.2节所述。

8.1 NB-IoT的特点

NB-IoT具有功耗低、覆盖范围广、成本低、容量大等特点。

8.1.1 低功耗

1) 特性描述

NB-IoT设备具有功耗低、耐久性好、充电频率低、计算能力低等特点，嵌入式系统也具有轻量级、简单等特点。

一般来说，在传统物联网终端设备上运行的系统具有计算能力强的特点，采用复杂的网络传输协议和严格的安全增强解决方案，由于耗电量大，需要经常充电。

2) 对NB-IoT的威胁

拒绝服务威胁可以通过简单地消耗NB-IoT设备的资源来实现，这种对软硬件的攻击成本相对较低。

由于NB-IoT设备具有轻量级、功耗低、计算能力低等特点，在传输过程中无法保证数据加密的安全性。有时数据可以用纯文本传输。因此，在身份验证和数据验证中可能存在很高的安全威胁。例如，攻击者可以使用未经授权的设备与基站通信以发送伪造数据。

8.1.2 大容量

1) 特性描述

NB-IoT的容量远大于传统的IoT，例如，一个NB-IoT部门可以支持大约10万台设备。

2) 对NB-IoT的威胁

在设备数量众多的情况下，甚至轻微的漏洞可能会对网络安全造成严重影响，如木马病毒可能会感染其他终端设备，导致网络不可用。

考虑到可以使用现有移动核心网的NB-IoT设备的部署场景，终端设备可能能够感染移动核心网元，例如：移动性管理实体、家庭订户服务器和其他设备以影响移动通信用户。在这种情况下，可以拒绝用户对网络的访问，或修改订户信息以避免电话费、短消息费或数据流量费等。

8.1.3 低成本

1) 特性描述

NB-IoT设备的成本一般非常低。

2) 对NB-IoT的威胁

使用简化协议等方式可以降低设备成本，因此攻击者可以利用简化协议的漏洞来实施对设备和网络的攻击。

8.1.4 覆盖范围广

1) 特性描述

NB-IoT的覆盖范围比传统的IoT要广得多，例如在同一频段，NB-IoT比现有网络有15-20 dB的增益，覆盖范围广达100倍。

2) 对NB-IoT的威胁

部署在远程位置的设备可能很容易被攻击者捕获和利用。

8.2 NB-IoT层

8.2.1 设备层

攻击者可以通过复制用户标识模块（SIM）卡来实施攻击，以实现非法的目的例如自由访问网络。

在新开发的轻量级终端模块的协议栈中可能存在安全漏洞。

现有的IoT终端设备制造商在发布支持NB-IoT的新设备时，可以使用支持Wi-Fi、蓝牙、ZigBee等协议的硬件。因为它们可能仅仅增加对上设备NB-IoT的支持，在开发的过程中可能会产生安全漏洞和威胁。相关实例包括用于调试的端口可能未得到适当保护，可能使用弱加密算法，无法应用硬件更新，并且在需要时缺乏及时的完整性检查。

8.2.2 网络层

网络数据通信劫持工具可以监视终端设备和基站之间的会话，捕获这些组件之间交换的数据包，从而导致通信被劫持，攻击者可以通过从被劫持的通信消息中提取数据来分析安全漏洞。

随着移动通信用户的大量使用和移动通信网络的共享，NB-IoT设备的篡改可能会引发信令风暴。

由于NB-IoT服务收集、在网络上传输和由多个网元处理的多个数据，可能存在数据泄露的风险。

NB-IoT核心网的信令可能由于网元之间缺乏认证机制而受到伪造、篡改、重放攻击。

来自互联网的多种攻击可能会损害移动核心网与互联网的接口，例如在5G系统中，移动核心网与互联网的接口是N6接口[ETSI TS 123 501]。此N6接口用于连接用户平面功能和互联网。

8.2.3 应用层

NB-IoT适用于静态业务、低延迟敏感性、不连续移动和实时数据传输的业务场景。

自动异常报告业务（例如烟雾警报检测器）和定期报告业务（例如环境状态监测系统）中可能会发生遗漏或错误警报。例如，如果攻击者捕获了用户的智能电表读数，则数字可能会被修改或伪造，从而损害了用户的利益。

此外，恶意指令也可能是远程指令业务的风险（例如，用户可以远程打开或关闭智能家居设备）。

NB-IoT的业务与各个行业深度集成，因此，暴露于复杂业务逻辑和多应用协议固有的漏洞。

NB-IoT的服务可能被设置的卡分离滥用，例如，将订阅的NB-IoT卡插入其他设备而不是NB-IoT设备中，或通过订阅的NB-IoT卡发送垃圾邮件短消息等。

9 安全要求

9.1 终端设备的安全要求

9.1.1 物理安全

NB-IoT终端设备为接口和芯片提供物理保护，确保即使捕获硬件，攻击者也无法访问数据。

对于不同的接口，NB-IoT终端设备支持认证和授权功能。

9.1.2 更新安全

NB-IoT设备的系统、软件、硬件等都要求具有更新能力，以确保系统和应用的安全。

为了避免篡改，需要保护更新文件的机密性和完整性。

9.1.3 隐私保护

NB-IoT终端设备需要灵活的隐私保护机制，以支持基于NB-IoT服务要求的隐私保护。

9.2 网络安全要求

9.2.1 认证

使用NB-IoT服务确认NB-IoT实体的身份时需要身份认证。身份认证确保实体声明的身份的有效性，并确保实体不会试图伪装为授权实体。

考虑到NB-IoT的特点，需要进行轻量级认证。

9.2.2 DDoS攻击防范

这需要预先部署安全机制，以便及时预防和处理拒绝服务攻击（DDoS）攻击。

9.2.3 网络实体安全

为了抵抗伪造、篡改和重放攻击，需要NB-IoT核心网实体来支持安全能力。

9.3 应用程序的安全要求

9.3.1 服务使用/运营合规性监控

服务使用/运营合规性监控是根据NB-IoT服务的要求，对峰值、总流量进行监控，发现异常的服务使用/运营情况。

9.3.2 防止服务滥用

通过对国际移动设备标识（IMEI）变化特征的监测，利用设置卡分离防止服务滥用。

9.3.3 识别安全威胁的分析和处置能力

在对NB-IoT终端设备行为进行大数据分析的基础上，对其安全威胁进行识别、分析和处理。

10 NB-IoT的安全能力

10.1 终端设备的安全能力

NB-IoT终端设备应包括以下安全能力：

– SC_terminal device 1：密钥管理能力；

– SC_terminal device 2：密钥算法协商能力；

– SC_terminal device 3：数据加密能力；

– SC_terminal device 4：数据整合能力；
– SC_terminal device 5：安全更新能力，包括系统、软件、硬件等；
– SC_terminal device 6：根据轻量级加密实施安全协议能力。

10.2 网络安全能力

NB-IoT终端设备应包括以下网络安全能力：

– SC_network 1：密钥管理能力；
– SC_network 2：密钥算法协商能力；
– SC_network 3：数据加密能力；
– SC_network 4：数据整合能力；
– SC_network 5：访问控制能力，确保只有授权实体才能访问NB-IoT网元、储存信息、信息流、服务和应用；
– SC_network 6：篡改检测和/或篡改防护能力；
– SC_network 7：抵御DDoS攻击的能力；
– SC_network 8：执行安全配置的能力；
– SC_network 9：设置卡分离检测的能力。

10.3 应用程序安全能力

应用程序应包括以下安全能力：

– SC_applications 1：通过使用恶意软件保护软件来防止恶意软件感染的能力；
– SC_applications 2：服务使用/网络关键指标（如峰值、总流量）实现运营合规性的监控能力；
– SC_applications 3：基于NB-IoT终端设备行为的大数据分析，可实现应用程序级安全性以防止安全威胁。

10.4 安全能力与安全要求之间的关系

第10节中列出和描述的安全能力用于满足第9节中规定的一些安全要求。安全能力与安全要求的映射如表1所示。

在表1中，单元格中的符号“√”表示安全要求与特定的安全能力相关，更准确地说，标记的安全要求应该通过实现标记的功能来支持。

表1 – 安全要求和安全能力之间关系的说明

要求 / 能力	物理安全	更新安全	隐私保护	认证	DDoS攻击防范	服务使用/运营合规性监控	服务滥用防范	识别安全威胁的分析和处置能力
SC_terminal device 1	√			√				
SC_terminal device 2	√							
SC_terminal device 3			√					
SC_terminal device 4		√						
SC_terminal device 5	√	√						
SC_terminal device 6			√	√				
SC_network 1				√				
SC_network 2		√	√					
SC_network 3		√	√					
SC_network 4		√						
SC_network 5			√	√				
SC_network 6						√		
SC_network 7					√			
SC_network 8		√						
SC_network 9							√	
SC_applications 1		√						
SC_applications 2					√	√	√	
SC_applications 3			√					√

参考资料

[b-ITU-T Q.1743] ITU-T Q.1743建议书（2016年），IMT-Advanced对LTE-Advanced分组核心网演进第11版的参引。

[b-ITU-T X.800] ITU-T X.800（1991年），CCITT应用的开放系统互联（OSI）安全体系结构。

[b-ITU-T X.1141] ITU-T X.1141 建议书（2006年），安全断言标记语言（SAML 2.0）。

[b-ITU-T X.1145] ITU-TX.1145建议书（2017年），电信设备开放能力的安全框架和要求。

[b-ITU-T X.1252] ITU-T X.1252建议书（2010年），基准身份管理术语和定义。

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦