## 第10章 5G物联网安全技术

物联网技术是基于互联网等载体，实现普通物理对象互联互通的网络技术。它通过网络实现物与物、物与人的泛在连接，具有普通对象设备化、自治终端互联化、普适服务智能化三大特点，广泛应用于智能生活、工业生产等多领域。5G物联网设备连接数庞大，数据传输复杂，因此需要研究5G物联网安全技术，保障网络信息安全与系统稳定运行。本章围绕5G物联网安全技术展开，重点介绍其标准进展，阐述安全标准体系并且详细介绍了基于群组的接入认证和切换认证机制，涵盖多种适用于不同场景的认证方案。

### 10.1 5G物联网标准进展

物联网的无线通信技术主要分为两类[1]：一类是Zigbee、WiFi、蓝牙、Zwave等短距离通信技术；另一种是低功耗广域网（Low-Power Wide-Area Network，LPWAN）通信技术。LPWAN可以分为两类：一类工作在非授权频谱上，如LoRa、SigFox等，另一类基于2/3/4G蜂窝通信技术，由第三代合作伙伴计划（third­Generation Partnership Project，3GPP）委员会支持并在许可频谱下运行。截止2024年，3GPP委员会根据物联网（Internet of Things，IoT）应用场景和性能需求将其划分为8种不同类型的IoT并提出了相应的技术标准：扩展覆盖全球移动通信技术（Extended Coverage Global System for Mobile Communications，EC-GSM）[2]、长期演进机器类型通信技术（Long-term Evolution for Machine-type Communication，LTE-­M）[3]、窄带物联网技术（Narrowband IoT，NB­-IoT）[4]、高可靠低延迟通信技术（Ultra Reliable and Low Latency Communications，URLLC）[5]、时间敏感网络技术（Time-Sensitive Networking，TSN）[6]、裁剪能力（Reduced Capability，RedCap）网络技术[7]和无源物联网技术（Ambient power-enabled Internet of Things，AIoT）[8]。其中EC-GSM是基于全球移动通信技术（Global System for Mobile Communications，GSM）的演进，由于GSM在全球各地逐渐被停用，EC-GSM并未受到太大关注。LTE-M在Release 11（R11）中被视为MTC或低成本MTC技术，在R13中被视为增强型机器类型通信技术（evolved Machine Type Communication，eMTC)，旨在满足基于现有LTE物联网设备的需求。2015 年，3GPP 从 R13 阶段开始研究制定 NB-IoT 技术标准，并在 2020 年发布的 R16 标准中，将其正式纳入 5G 技术体系。旨在为远程医疗、自动驾驶、工业控制等场景，提供超可靠、超低时延、超高可用性的服务，使该技术能适配这些场景的严苛要求 。TSN技术针对时间敏感的业务场景，比如智能电网中的配电差动保护场景[6]，该技术是URLLC技术的进一步增强，主要体现为能够实现更低的时间抖动和更高的时间同步精度[9]。3GPP委员会在2020年R17中引入RedCap技术，该技术可以弥补低成本、大带宽、中等数据速率、低延迟类型终端物联网服务的短缺，该类终端也被称为RedCap终端。2022年3GPP委员会为物联网生态又引入了新型终端，称为AIoT终端或零功耗终端，其特点是从环境中获取能量（例如射频能量、太阳能、热能等）。这些终端不需要额外的电池或自身能量存储能力非常有限。它们具有极高的成本效益、易于部署并且需要最少的维护。图10.1详细介绍了3GPP对不同物联网技术的分类。对于5G物联网，本章仅讨论eMTC技术和NB-IoT技术。



图10.1 3GPP中物联网技术分类

与NB-IoT相比而言，eMTC的设备覆盖范围和模块成本较大，但在峰值速率、移动性方面具有优势，并且支持基于LTE的高清语音（Voice over Long-Term Evolution，VoLTE）。2018年，有141家运营商积极投资NB-IoT技术，90家已经部署NB-IoT网络[10]。根据爱立信的报告[11]，2019年NB-IoT和eMTC连接数接近1亿。到2025年底，预计将有约27亿台连接设备加入NB-IoT和eMTC网络，比2019年增加了27倍。eMTC架构主要由三部分组成：eMTC设备域、eMTC网络域和eMTC应用域。eMTC设备可以通过网关和无线接入网连接到核心网，并通过5G网络与一台或多台eMTC服务器通信。3GPP为eMTC系统[12]定义了两种通信场景，如图10.2和10.3所示，分别是eMTC设备与服务器之间的通信和eMTC设备之间不涉及eMTC服务器参与网络的通信。核心网络通过使用增强型扩展认证协议-认证密钥协商协议（Extensible Authentication Protocol-Authentication and Key Agreement'，EAP-AKA'）或第5代认证密钥协商协议（Fifth Generation Authentication and Key Agreement，5G AKA）与eMTC设备进行相互认证，为eMTC设备和eMTC服务器之间后续安全通信提供保障。到目前为止，3GPP委员会还没有提出在两个eMTC设备之间建立安全通信的有效方法。



图10.2 eMTC设备和服务器通讯架构图



图10.3 eMTC设备间的通讯架构图

NB-IoT已成为万物互联的重要分支。NB-IoT具有低成本、强覆盖、低带宽、大连接的特点，仅消耗约180KHz带宽，可直接部署在GSM网络、通用移动通信系统（Universal Mobile Telecommunications System，UMTS）网络或LTE/LTE-A网络上，从而减少部署成本，实现平滑升级。与eMTC不同，NB-IoT主要适用于位置固定或相对低速、低移动性的物联网场景。此外，NB-IoT设备的数量远高于eMTC设备，并且这些大量的NB-IoT设备以其极低的时延呈现出“突发”的网络接入特性。目前NB-IoT运行在LTE-A网络中，根据3GPP规划，新无线接入网NR将与LTE-A接入网共存，并共享4G核心网（Evolved Packet Core，EPC）。在NB-IoT通信系统中，每个NB-IoT设备都使用演进分组系统认证密钥协商协议（Evolved Packet System-Authentication and Key Agreement，EPS AKA）实现认证鉴权过程。为了更好地满足物联网业务低频和时延不敏感的需求，适应NB-IoT的数据传输特性，5G网络关于NB-IoT在数据传输、功率、协议、和服务能力等方面进行了优化。具体来说，3GPP委员会提出了以下两种NB-IoT网络优化方案[13]：“控制平面优化传输方案”(Control Plane，CP)和“用户平面优化传输方案”(User Plane，UP)，如图10.4所示，其中“控制平面优化传输方案”必选，“用户平面优化传输方案”是可选。CP主要用于支持NB-IoT场景下的小IP或非IP数据传输，通过非接入层(Not-Access Stratum，NAS)协议数据单元(Protocol Data Unit，PDU)来发送一些小的IP数据或非IP数据，而无需在无线资源控制层（Radio Resource Control，RRC）连接请求过程中建立数据无线承载(Data Radio Bearer，DRB)和S1-U承载。CP中的数据传输路径可以分为两部分：（1）通过会话管理网元（Session Management Function，SMF）传输到用户面网元（User Plane Function，UPF），再传输到应用服务器（CIoT Services）；（2）通过服务能力暴露网元（Service Capability Exposure Function，SCEF）传输到应用服务器，该路径只支持非IP数据传输。UP方案中引入了RRC连接暂停状态和RRC连接恢复状态。当终端进入空闲状态时，网络侧仍会维护终端的相关信息，以便终端快速重连。该方案主要适用于支持NB-IoT场景下的多种QoS业务。



图10.4 NB-IoT网络优化方案

### 10.2 5G物联网安全标准机制

考虑到5G AKA或EAP-AKA'[14]认证协议的密钥架构复杂冗余，不适用于能量有限的MTC设备，3GPP委员会针对极低吞吐量MTC设备制定了高效节能的安全技术标准（Battery Efficient Security for very low Throughput Machine Type Communication devices，BEST）[15]，其中在核心网中引入了归属网络安全锚点（HPLMN Security Endpoint，HSE），该网元专门用于极低吞吐量MTC设备的安全接入。该技术标准提供了3种高效节能的安全服务。具体内容如下：

第一种是BEST密钥协商服务。该服务用于MTC设备与HSE或企业应用服务器（Enterprise Application Server，EAS）之间的密钥协商。该服务中由MTC设备和EAS之间的应用层提供MTC设备的用户平面，不在3GPP规范范围之内。

第二种服务是BEST用户面完整性保护服务。该服务是针对低吞吐量MTC设备的用户面完整性保护服务。该服务包括密钥协商以及NAS层上小数据的完整性保护。该服务中用户平面可以在MTC设备与HSE之间(即UE-to-HSE模式)或MTC设备与EAS之间(即UE-to-EAS模式)。MTC设备的控制信令总是在HSE处终止。

第三种服务是BEST用户面机密性保护服务，该服务是针对低吞吐量MTC设备的用户面完整性和机密性保护服务。与第二种服务类似，该服务中用户平面可以在MTC设备与HSE之间(即UE-to-HSE模式)或MTC设备与EAS之间(即UE-to-EAS模式)。MTC设备的控制信令总是在HSE处终止。

为了提供上述不同安全服务，该技术标准BEST提供了MTC设备的高效接入认证和密钥协商方案，并且基于不同的密钥协商方法（包括5G AKA、EAP-AKA'、EPS AKA、通用引导架构（Generic Bootstrapping Architecture，GBA）、应用层认证和密钥管理架构 （Authentication and Key Management for Applications，AKMA）、专用密钥协商方法）提供了不同的密钥派生架构，从而能够节省MTC设备的安全计算开销以及功耗开销。

针对NB-IoT通信系统，3GPP委员会规定该类设备仍然执行5G AKA或EAP-AKA’认证协议来实现安全接入。另外，TS33.501[14]中规定了针对蜂窝物联网的安全处理流程。主要包括四部分内容：第一部分是适用于5G系统（5G System，5GS）的蜂窝物联网控制面优化方案的安全处理，其中含有适用于控制面小额数据传输的安全流程以及重新建立RRC连接的安全流程；第二部分是适用于5GS蜂窝物联网用户面优化方案的安全处理，其中含有基站发起的RRC连接终止安全处理流程以及终端处于空闲状态时接入新基站和旧基站的RRC连接恢复流程；第三部分是针对非IP数据传输接口保护机制；第四部分是终端由接入的5GS切换到EPS的安全处理流程。

### 10.3 5G物联网安全需求和潜在的威胁

目前基于LTE/LTE-A网络，IoT系统已经进行广泛部署，但是其在5G网络中的应用仍然处于探索研究阶段，并且由于大多数设备资源有限，网络环境复杂，更容易遭受传统无线网络带来的攻击。

每个IoT设备接入网络时，需要实现物联网设备与5G网络侧的双向认证，并且预防中间人攻击、伪装攻击、重放攻击等，也就是说，对于5G归属网络，需要确信接入方是合法的IoT设备，从而确保后续实施有效的业务鉴权、用户计费；对于IoT设备，能够确信接入网络是合法运营商网络，而非伪基站等非法网络，否则可能导致用户设备的个人信息泄露，还可能有遭受诈骗、垃圾短信轰炸等危害。

每个IoT设备接入网络后，需要保证设备的应用数据安全传送给核心网络，确保通信过程的机密性和完整性，防止敌手窃听、篡改等非法活动。

每个IoT设备接入网络时，需要确保身份匿名和不可追踪性，防止敌手获取设备身份隐私信息并且实施追踪活动。

5G网络应支持一种高效的适用于大量设备的双向认证机制。随着IoT设备数量飞速增长，未来大规模设备往往同时接入同一小区，如果5G网络对每个设备分别进行认证的话，会产生巨大的资源消耗，甚至可能产生信令风暴并导致系统瘫痪服务失效，从而可能威胁其他终端的网络服务。

在特殊物联网应用场景中，IoT设备接入网络时应支持抵御物理攻击，比如侧信道攻击、克隆攻击，以防止设备内部密钥泄露。在智慧电表、水表以及工厂等场景中，IoT设备往往长期固定在某一位置，并且可能长时间暴露于外界，处于无人监管状态，因此极易面临被敌手恶意攻击、私钥被获取的安全威胁。一旦敌手获取私钥，那么可能私自解密历史信息，并伪装设备接入网络。例如，智能水表被成功攻陷后，敌手可以伪造虚假的过度用水量数据并转发至应用服务后台，最终迫使用户承担昂贵的费用[16]。

随着量子计算技术的发展，基于传统公钥密码技术的认证方案将无法抵御量子攻击，具体地，量子计算技术能够破解传统公钥密码技术所依赖的困难问题，从而导致密钥泄露。因此未来物联网设备接入网络时，需要能够抵御量子攻击。

### 10.4 基于群组的接入认证和切换认证机制

在4G/5G网络的大连接场景下，MTC或NB-IoT设备数量众多、计算与能量资源有限，且主要进行小额数据传输。这衍生出两方面问题：一方面，海量物联网设备并发接入网络或漫游切换时，采用现有标准认证协议易引发信令冗余拥堵，加重网络侧处理负担，极端情况下会导致系统宕机，遭受拒绝服务攻击；另一方面，5G标准认证协议运用公钥加密方案保护身份隐私，却使得硬件资源有限（处理能力弱、续航不足）的物联网终端产生较高安全计算时延与能耗开销。综上所述，现有标准协议并不适用于物联网场景的安全接入需求。

针对上述问题，基于群组的思想，通过对海量接入设备进行分组，能够实现不同场景下海量物联网设备的安全接入和切换认证，从而有效避免信令拥塞问题。下面重点介绍适用于机器类型通信的群组接入认证、切换认证方案以及适用于5G NB-IoT的大规模设备快速认证与数据传输方案。

#### **10.4.1****适用于机器类型通信的群组接入认证机制**

MTC设备数量庞大，可能达到手机终端数量的几个数量级以上，当大量MTC设备同时发起认证请求或业务请求时，每个隶属于MTC群组的MTC设备需要各自独立地完成到服务网络的认证过程。在认证过程中，服务网络与归属网络之间频繁的交互数据，就会造成它们之间的链路拥塞，进而可能带来大量的认证延迟，从而降低运营商网络的服务质量。

围绕机器类型通信中海量设备的接入认证问题，根据所使用认证技术的不同，本节主要介绍三种机制，分别是基于共享群密钥的认证机制[17]、基于群组的机器类型通信设备的认证机制[18]以及基于聚合签名技术的MTC接入认证机制[19]。这三种机制均通过基于群组的思路对海量机器设备进行分类，能够在保证海量机器设备安全接入的同时，解决网络侧的信令风暴问题，降低系统信令开销。此外，在对海量设备进行划分群组的情况下，基于共享群密钥的认证机制中通过设置群组成员共享相同密钥，能够保障群组成员的安全接入，并且在群组成员与核心网中协商出同一会话密钥；基于群组的机器类型通信设备的认证机制中通过为不同群组成员设置不同的预共享密钥，能够实现群组成员与核心网的安全接入以及不同会话密钥的协商；基于聚合签名技术的MTC接入认证机制中通过为不同群组成员设置不同的公私钥，能够避免群组成员接入时服务网络与归属网络之间的频繁交互，从而实现群组成员与服务网络的快速认证。

##### 10.4.1.1机器类型通信中基于共享群密钥的认证机制

基于3GPP现有的机器通信识别模块（Machine Communication Identity Module，MCIM）下载协议[20]以及支持认证和密钥协商功能的扩展认证协议（Extensible Authentication Protocol-Authentication and Key Agreement，EAP-AKA），本节介绍机器类型通信中基于共享群密钥的认证机制，在该机制里，服务网络（Serving Network，SN）存储着由归属网络提供的、基于共享群密钥生成的认证数据。凭借这些认证数据，服务网络能够直接与机器设备（Machine Equipment，ME）进行相互认证。如此一来，服务网络无需为获取机器设备的认证数据而频繁地与归属网络交互。这不仅实现了群组内机器设备与服务网络之间的快速认证，还优化了因认证而在服务网络与归属网络间产生的信令数据，减轻了服务网络与归属网络之间链路的拥塞状况，助力群组内设备实现快速接入认证。

本节方案术语如表10.1所示，方案如图10.5所示，具体流程包括如下四个步骤：

表10.1 符号说明

|  |  |  |  |
| --- | --- | --- | --- |
| **符号** | **符号定义** | **符号** | **符号定义** |
| AK | 匿名密钥 | MCIM | 机器通信识别模块 |
| AMF | 认证管理域 | MCIMobj | ME的管理对象 |
| AV | 认证向量 | ME | 机器设备 |
| AuC | 认证中心 | M2M | 机器对机器通信 |
| AUTN | 认证令牌 | MTC | 机器类型通信 |
| CK | 机密性密钥 | PfC | 平台证书 |
| DPF | MCIM下载和配置实体 | RAND | 随机数 |
| f1-f5 | 长期演进LTE安全架构中定义的算法 | RO | 注册操作者 |
| HE | 归属网络 | SN | 服务网络 |
| IMSI | 国际移动用户识别码 | SQN | 序列号 |
| IK | 完整性密钥 | TRE | 可信环境 |
| GID | 群组身份信息 | TMSI | 临时移动用户识别码 |
| GK | 共享群密钥 | UICC | 通用集成电路卡 |



图10.5 基于共享群密钥的认证方案流程图

步骤1：归属网络HE将共享群密钥分发给群中机器设备ME。该分发过程针对机器设备群的不同分为以下两种情况：

（1.1）由一组基于通用集成电路卡（Universal Integrated Circuit Card，UICC）的机器设备ME构成机器设备群，该设备群所在的归属网络（Home Environment，HE）生成共享群密钥，并在初始状态或者当群中成员发生改变时，将在通用用户标识模块（Universal Subscriber Identity Module，USIM）出厂前写入其中，各个ME通过插入USIM得到，完成HE对于的分发；

（1.2）由一组基于可信环境（Trusted Environment，TRE）的机器设备ME构成机器设备群，该设备群所在的HE生成，并在初始状态或者当群中成员发生改变时，将作为机器通信识别模块MCIM的一个组成部分，根据3GPP的MCIM下载协议，各个ME通过下载相应的MCIM得到，完成HE对于的分发；该3GPP的MCIM下载协议进行下载的过程，如图10.6所示，包括如下步骤：



图10.6 MCIM下载协议流程图

（a）在初始状态下，或者当ME收到群成员关系改变的广播时，ME向服务网络SN发送共享群密钥请求消息，SN收到消息后，通过AKA协议认证ME；

（b）认证成功后，机器设备ME与注册操作者（Registration Operator，RO）的MCIM下载和配置实体（Download and Precongifure Function，DPF）联系，并将ME以及可信环境TRE的相关信息发送给DPF；

（c）RO将ME发送的相关信息转发给归属网络HE；

（d）HE将含有共享群密钥的机器通信识别模块MCIM利用平台证书PfC加密，并生成ME的管理对象MCIMobj；

（e）HE将MCIMobj发送给RO，并授权MCIM下载和配置实体DPF对ME进行MCIM应用配置；

（f）注册操作者RO将ME的管理对象MCIMobj下载到ME；

（g）ME将下载的MCIMobj写入可信环境TRE中，TRE利用平台密钥对MICMobj进行解密得到MCIM；

（h）ME向RO发送配置成功状态信息，RO再将状态信息转发给HE。

步骤2：归属网络HE将共享密钥生成的认证向量组（Authentication Vectors，AVs）分发到服务网络SN。参考图10.7，本步骤的具体实现如下：



图10.7 归属网络HE分发认证向量组流程图

（2.1）机器设备ME向SN发送设备接入请求，请求接入服务网络；

（2.2）SN收到请求后，向ME发送认证身份请求，请求认证身份；

（2.3）ME将携带有ME的临时身份标示符（Temporary Mobile Subscriber Identity，TMSI）以及ME所在群组的身份的认证身份响应消息，发送给服务网络SN；

（2.4）SN利用得到的TMSI恢复机器设备ME的唯一身份标示符（International Mobile Subscriber Identity，IMSI），并将携带有IMSI和的认证数据请求消息，发送给归属网络HE；

（2.5）HE收到认证数据请求消息后，验证机器设备ME是否隶属于群中。这个过程主要是根据归属网络HE中所存储的机器设备群列表来进行的。此列表在HE初始化机器设备群时建立，包括群组身份信息和群中机器设备的唯一身份标示符IMSI，并存储于HE的数据库中。当HE收到IMSI以及后，HE查找所对应的机器设备群列表中是否包含此IMSI，如果包含ME则属于此群，反之不属于此群。如果验证成功，HE向认证中心（Authentication Centre，AuC）请求共享群密钥生成的认证向量组AVs，其中认证向量组中的认证向量AV是按照如下规则生成：



其中：是一个随机数，为逻辑或运算，，为长期演进LTE安全架构中定义的算法，用于产生期望响应值；，为LTE安全架构中定义的算法，用于产生加密密钥；，为LTE安全架构中定义的算法，用于产生完整性密钥；，为序列号，为逻辑异或运算，，为LTE安全架构中定义的算法，用于产生匿名密钥，为认证管理域，，为LTE安全架构中定义的算法，用于产生消息认证码。

最终HE将所得到的认证向量组AVs通过认证数据响应消息发送给服务网络SN，如果验证失败，则终止分发过程，并向SN发送认证数据分发失败消息；

（2.6）SN收到消息后，保存认证向量组AVs。

步骤3：群中机器设备ME根据共享群密钥以及现有的EAP-AKA协议与服务网络SN进行相互认证。本步骤中的认证交互过程如图10.8所示，具体内容如下：



图10.8 机器设备与服务网络相互认证流程图

（3.1）SN从认证向量组中选取一个认证向量AV，该AV包括随机数，期望响应值，加密密钥，完整性密钥和认证令牌，SN将AV中的和通过用户认证请求消息，发送给ME；

（3.2）收到上述消息后，ME首先计算，，，然后验证与中的是否相同，并查看是否在有效范围内。如果验证结果为相同或者不在有效范围内，则ME认证SN是无效的，并终止认证，如果验证结果为相同并且在有效范围内，则ME认证SN是有效的，并分别计算机密性密钥，完整性密钥，以及挑战响应值，然后将携带有的用户认证响应消息，发送给SN；

（3.3）SN将所收到的与AV中的进行比较，若比较结果为相同，则SN认证ME是有效的，并向ME发送成功消息；否则SN认证ME为无效的，并终止认证。

步骤4：群中机器设备ME与归属网络HE更新共享群密钥。当群组的签约关系发生改变时，如从群组中增加或删除设备时，需要群中机器设备与归属网络HE间共享群密钥进行更新，参考图10.9，对群密钥的更新过程如下：



图10.9 共享群密钥更新流程图

（4.1）HE生成一个新的共享群密钥和一个携带有群组身份信息的密钥更新通知消息，并将此密钥更新通知消息发送给服务网络SN；

（4.2）SN根据密钥更新通知消息中的，搜索所有属于该的机器设备ME，并向这些ME发送密钥更新通知消息；

（4.3）ME收到密钥更新通知消息后按照步骤1与归属网络HE之间进行共享群密钥的分发，步骤1完成后，ME得到新的共享群密钥；

（4.4）ME利用新共享群密钥按照步骤2和3与SN之间进行认证。

本方法的安全性分析如下。

1. 相互认证

只有基于群密钥才能生成正确有效的消息认证码和。对于基于TRE的ME，被嵌入到MCIM中，通过利用平台密钥对MCIM的加解密来实现机器设备与归属网络之间群组密钥的共享，这里平台密钥只有机器设备和归属网络才拥有，因此是安全的。而且，包含的MCIM最终被写入到ME的TRE中，受TRE保护，攻击者无法从ME中得到共享密钥。对于基于UICC的ME，最终是被写入到UICC中，受UICC保护，因此也是安全的。归属网络与服务网络之间交互的认证向量是通过安全信道进行传输的，基于这一安全传输方式，服务网络能够安全获得群组机器设备的认证向量。当机器设备完成对AUTH中的验证，且服务网络也完成相应验证后，该方案能够实现机器设备与服务网络的相互认证。

1. 密钥协商

在该认证方法执行完成后，机器设备会执行和算法生成和，服务网络会通过安全信道从归属网络获得和，同时由于敌手无法获得群密钥，因此该认证方法可以实现机器设备和服务网络之间的安全密钥协商。

1. 抵抗信令风暴

该方案中基于相同特征的多个MTC设备预先构成一个群组，同时共享一个相同的群组密钥。归属网络会存储该群组标识信息和群组成员设备信息，同时归属网络在接收到服务网络的认证数据请求消息后，针对某个具体群组的认证请求消息利用唯一的群组密钥生成认证向量组，通过一次信令消息即可将所有成员的认证向量分发给服务网络。服务网络在接收到认证向量后，将该认证向量发送给群组所有机器设备成员。因此该认证方法能够抵抗海量MTC设备接入网络时导致的服务网络与归属网络之间的信令风暴。

1. 抵抗重放攻击

在该认证方案中机器设备和归属网络预先共享序列号SQN，如果敌手重放来自服务网络的认证消息给机器设备，即使该认证消息中的被验证通过，机器设备还会检查SQN是否在误差范围内再次确认，因此该方案能够抵抗服务网络所发消息的重放攻击；如果敌手重放来自机器设备的认证消息给服务网络，由于该认证消息中的是基于历史随机数产生的，所以当服务网络利用自己产生的随机数对进行验证时，会输出失败的验证结果，可以说明该方案能够抵抗机器设备所发消息的重放消息。因此该认证方法可以抵抗重放攻击。

1. 抵抗伪装攻击

如果敌手想要通过篡改消息来实施伪装攻击，考虑到只有基于群密钥才能生成正确有效的消息认证码和，由于敌手没有群密钥，无法生成有效的和，因此该认证方法可以抵抗伪装攻击。

1. 抵抗中间人攻击

对于机器类型设备来说，只有合法的服务网络才能从归属网络处获得机器类型设备的认证向量。当验证通过时，机器类型设备可以确定通信对方是机器类型设备所期望的合法访问网络；对于服务网络来说，由于只有合法的机器类型设备才能生成有效的，所以当接收到的验证通过时，服务网络可以确定通信对方是服务网络所期望的合法设备。因此该认证方法可以抵抗中间人攻击。

1. 安全密钥更新

在群组设备成员更新时，归属网络利用安全的MCIM下载协议只向新群组成员分发新共享群密钥。

##### 10.4.1.2 基于群组的机器类型通信设备的认证机制

在上一小节中，利用划分群组的思路避免了信令拥塞问题，基于共享群组密钥实现了海量设备的并发接入认证。本小节介绍一种基于群组的机器类型通信设备的认证机制，该机制同样利用了划分群组的思路，基于设备发送的群组配置需求为终端划分群组，同时为群组成员设置群组标识符，从而减少设备在接入服务网络时进行认证所造成的网络拥塞。此外，该方案还利用设备与网络侧共享的单一密钥来实现双方认证和会话密钥协商。

该方案涉及符号如表10.2所示，认证总流程如图10.10所示，具体流程包括如下四个步骤：

表10.2 符号说明

|  |  |
| --- | --- |
| 符号 | 符号定义 |
| MTCD | 机器类型通信设备； |
| MTC Server | 机器类型的通信服务器，用于管理MTCD，对MTCD进行注册； |
| SGSN | 通用分组无线服务技术服务支持节点，代表访问网络对MTCD进行认证； |
| AuC | 认证中心，认证向量的分发； |
| PCID | 设备临时连接身份； |
| IMEI | 国际移动设备识别码； |
| TMSI | 临时移动用户识别码； |
| K | 永久密钥； |
| RAND | 挑战随机数； |
| AUTN | 认证令牌； |
| XRES | 认证挑战； |
| CK | 加密密钥； |
| IK | 完整性密钥。 |



图10.10 认证总流程图

步骤1：机器类型通信设备的注册和群组配置。如图10.11所示，本步骤的具体内容如下：



图10.11 注册和群组配置流程图

（1.1）在出厂时，设备制造商把相同的永久密钥分别保存在机器类型通信设备（Massive Type Communication Device，MTCD）和认证中心AuC中；

（1.2）在出厂时，设备制造商分别在机器类型通信设备MTCD和机器类型通信服务器（Massive Type Communication Server，MTC Server）上设置用于MTCD群组配置的策略，并为该组设备设置一个相同的临时连接身份（Provisional Connection Identity，PCID）；

（1.3）机器类型通信设备MTCD在需要接入服务网络时，向GPRS服务支持节点（Serving GPRS Support Node，SGSN）发送自己的PCID、国际移动设备身份码（International Mobile Equipment Identity，IMEI）、机器类型设备标识符以及群组配置需求；

（1.4） SGSN收到MTCD的临时连接身份PCID和国际移动设备身份码IMEI后，建立机器类型通信设备MTCD的PCID和IMEI绑定，即在SGSN中建立一个数据库，该数据库包括MTCD的临时连接身份PCID和对应的国际移动设备身份码IMEI，用于对群组中各个MTCD的识别；

（1.5）SGSN根据步骤（1.3）收到的机器类型设备标识符，向机器类型通信设备服务器MTC Server转发从步骤（1.3）收到的设备临时连接身份PCID和群组配置需求；

（1.6）MTC Server收到设备临时连接身份PCID和群组配置需求后，根据机器类型设备标识符和群组配置需求配置该设备所属的群组，分配和该群组对应的群标识符，并把群标识符发送给SGSN；

（1.7）SGSN收到群标识符后，使用3GPP中的标准方法计算PCID的客户临时识别码TMSI，并将群标识符和TMSI发送给MTCD；

（1.8）MTCD收到SGSN发来的群标识符和TMSI后，该设备的注册过程完成；

（1.9）重复步骤（1.3）-（1.8）完成对群组中其它设备的注册。

步骤2：认证向量组的获取。如图10.12所示，本步骤的具体内容如下：



图10.12 认证向量组的获取流程图

（2.1） 群组中的MTCD需要进行认证时，其中一个设备MTCD1向SGSN发送设备接入请求；

（2.2） SGSN向MTCD1 返回认证身份请求消息；

（2.3） MTCD1将自己的客户临时识别码TMSI和群标识符发送给SGSN；

（2.4）SGSN收到MTCD1发来的TMSI和群标识符后，使用3GPP标准中的方法从TMSI中恢复出PCID；

（2.5）SGSN建立一个身份列表，把群组中每个设备的临时连接身份PCID和群标识符进行绑定，即在SGSN中建立一个数据库，该数据库包括MTCD的临时连接身份PCID和对应的群标识符，该身份列表用于MTCD的接入控制；

（2.6）SGSN把从步骤（2.4）获得的PCID发送至认证中心AuC；

（2.7）AuC收到PCID后确定设备所属的群组，使用步骤（1.1）中预先保存的永久密钥K，通过3GPP中的标准算法生成挑战随机数、认证令牌、认证挑战、加密密钥和完整性密钥参数，然后由、、、和构造认证向量组，也就是组中的每个认证向量=||||||||；

（2.8）AuC将认证向量组发送给SGSN；

（2.9）SGSN保存从AuC收到的一组认证向量，使用其中一个用于MTCD1的认证，剩下的认证向量用于群组中其它设备的认证，因此当其它设备需要进行认证时，SGSN就不需要再向AuC重新获取认证向量组。

步骤3：群组设备的认证。如图10.13所示，本步骤的具体内容如下：



图10.13 群组设备的认证流程图

（3.1）SGSN将步骤（2.9）得到的挑战随机数，认证令牌发送给MTCD1；

（3.2）MTCD1根据3GPP标准方法验证从SGSN发来的挑战随机数和认证令牌，验证通过后，使用3GPP中的标准算法计算用户认证响应，并将发送给SGSN，反之，终止此次认证；

（3.3）SGSN根据3GPP标准方法验证接收到的用户认证响应，如果通过，则MTCD1的认证过程完成，反之，终止此次认证，并向MTCD1发送一条认证失败消息；

（3.4）群组中其它设备的认证过程同步骤（3.1）-（3.3），SGSN直接从组认证向量中挑选一个在步骤（2.9）中保存的认证向量发送给需要认证的设备，当群组中所有的设备成功认证后，整个认证过程结束。

步骤4：群组中设备的退出。当SGSN判断群组中的某个机器类型通信设备需要退出该群组时，只需要删除步骤（2.5）中建立的身份列表中该设备的临时连接身份PCID，这样一来，该设备的PCID和群标识符的绑定关系就被撤销，当退出该群组的设备还想使用原来群组的临时连接身份PCID进行认证时， SGSN对它先进行接入控制，在步骤（2.5）建立的身份列表中查找该设备的PCID和群标识符的绑定关系，如果查找不到，则不允许该设备进行认证，从而保证了整个系统的安全性。

本方法的安全性分析如下。

1. 相互认证

在该认证方案中只有基于永久密钥才能生成正确有效的消息认证码和。认证中心AuC与访问网络节点SGSN之间交互的认证向量，是通过安全信道进行传输的，因此SGSN能够安全获得群组机器设备的认证向量。同时，机器设备需要通过对的验证和SGSN对的验证。因此该方案能够实现机器设备与访问网络的相互认证。

1. 密钥协商

在该认证方法执行完成后，机器设备会生成和，访问网络会通过安全信道从归属网络认证中心AuC获得和，而敌手无法获得根密钥，因此该认证方法可以实现机器设备和访问网络之间的安全密钥协商。

1. 抵抗信令风暴

在该方案中由MTC服务器实现对MTC设备的分组。当访问网络SGSN接收到终端MTCD1的认证请求消息后，根据TMSI获取PCID，向归属网络发送PCID。随后，归属网络AuC根据PCID和群组的隶属关系，通过一次信令消息即可将该群组成员的认证向量组分发给SGSN，SGSN在接收到认证向量组后，使用其中一个认证向量用于MTCD1的认证，剩下的认证向量用于群组中其它设备的认证，因此当其它设备需要进行认证时，SGSN就不需要再向AuC重新获取认证向量组，从而能够抵抗海量MTC设备接入网络时导致的服务网络与归属网络之间的信令风暴。

1. 抵抗重放攻击

机器设备和归属网络预先共享序列号SQN，如果敌手重放来自访问网络的认证消息给机器设备，即使该认证消息中的会被验证通过，机器设备也会检查SQN是否在误差范围内，所以该方案能够抵抗访问网络所发消息的重放攻击；如果敌手将来自机器设备的认证消息重放给访问网络，由于该认证消息中的是基于历史随机数产生的，当访问网络利用自己产生的随机数对进行验证时，会输出失败的验证结果，所以该方案能够抵抗机器设备所发消息的重放消息。因此该认证方法可以抵抗重放攻击。

1. 抵抗伪装攻击

如果敌手想要通过篡改消息来实施伪装攻击，考虑到只有基于根密钥才能生成正确有效的消息认证码和，由于敌手没有根密钥，无法生成有效的和，因此该认证方法可以抵抗伪装攻击。

1. 抵抗中间人攻击

对于机器设备来说，只有合法的访问网络才能从归属网络AuC处获得机器设备的认证向量。当验证通过时，其可以确信通信对方是机器设备所期望的合法访问网络；对于访问网络来说，由于只有合法的机器设备才能生成有效的，当接收到的验证通过时，其可以确信通信对方是访问网络所期望的合法接入设备。因此该认证方法可以抵抗中间人攻击。

##### 10.4.1.3 基于组的MTC接入认证机制

本节介绍一种基于组的接入认证机制，该方案执行完之后，大量的MTC设备可以同时被网络认证，并分别与网络建立独立的会话密钥。该方案具有两大显著优势。其一，能够大幅削减大量设备向网络的信号传输量，有效规避LTE网络出现信令过载的情况。其二，与前述两小节的方案有所不同，此方案运用了公钥密码技术，从而具备强大的安全性，涵盖密钥前向/后向保密性以及不可否认性验证等方面。

该方案具体流程包括如下四个阶段，注册阶段、接入认证阶段、验证失败阶段、动态组成员管理机制。

1. 注册阶段

首先，每个机器类型设备MTCD在出厂时需要注入群组标识。假设在相同的区域或具有相同的特征，或者属于同一个用户的大量设备组成同一群组。根据通讯能力、通信链路质量、存储资源和电量续航，选定组长（Group Leader，GL）。当群组中的每台设备注册到网络时，它会联系密钥生成中心（Key Generation Center，KGC），并提供自己的标识，从而由KGC配置相应的私钥。移动管理实体（Mobility Management Entity，MME）也会从KGC获得自己的私钥。令KGC融合到归属签约用户服务器（Home Subscriber Server，HSS），依据3GPP 网络域安全功能，可以支持该网元与MME建立安全通道。

KGC产生作为系统参数，并且发布这些参数，产生x作为系统私钥。假设，，是群成员，当每台注册到网络时，执行下述流程：

步骤1&2&3：该三个步骤类似于EPS AKA，但是的需要分别添加到身份响应消息和认证数据请求消息中。

步骤4：HSS/KGC在接收到认证数据请求消息后，需要检查是否是MTC群组的合法设备。HSS/KGC存储了同一群组的成员列表，若存在于该成员列表中，HSS/KGC产生一组有序的认证向量AVs，该组认证向量对应于组成员，并且计算。然后HSS/KGC计算私钥，最后HSS/KGC将会发送给MME；如果不存在该成员列表中，那么HSS/KGC会发送失败消息给。

步骤5&6：步骤5和6类似于EPS AKA，但是MME需要保持私密。

步骤7：在MME成功验证后，MME派生密钥并使用其加密，然后通过认证成功消息将的密文和公共参数发送给。

步骤8：接受到认证成功消息后，解密消息获得，并安全保存该密钥。需要注意的是，是MME和在执行EPS AKA流程期间生成的共享密钥。类似于，当MME注册到网络时或者私钥过期时，HSS/KGC会为其产生基于ID的长期私钥。当HSS/KGC接收到MME的标识时，HSS/KGC执行下述步骤：

（8.1）选择随机数，并且计算以及。

（8.2）计算。

在HSS/KGC成功验证MME后，将作为MME的长期私钥，并将其安全发送给MME。MME接收到该消息后，计算等式是否成立，若成立，则说明该私钥是有效的。

注册阶段结束后，和分别作为和MME的密钥，将被用于后续的组接入认证过程。只有当MME再次向HSS请求认证数据时，长期密钥才会被更新。

1. 接入认证阶段

接入认证阶段具体流程如下：

步骤1：为了接入网络，每个选择，并且计算。

步骤2：计算和，其中是的时间戳。

步骤3：发送接入请求消息给组长GL。

步骤4：组长GL收集所有成员的接入请求消息，然后计算，并且发送消息至MME。

步骤5：MME接收到上述消息后，对于每个，检查是否和是否过期，若没有过期，那么执行下述步骤；否则，发送请求失败消息至GL并且提示“是无效的”。

步骤6：对于所有，MME计算和。

步骤7：MME验证等式是否成立。若等式成立，那么产生新随机数，并且计算。MME使用长期私钥对进行签名，从而生成签名值。最后发送回复消息给组长GL。

步骤8：MME计算会话密钥，这个会话密钥是MME与每个之间共享的密钥，由于每个产生了不同的，因此不同有不同的会话密钥。

步骤9：接收到上述消息后，GL根据计算MME的公钥，然后利用对进行验签。GL对MME进行验证成功后，广播该消息给所有。

步骤10：接收到上述消息后，根据等式来计算MME的公钥，然后利用对进行验证。若验证成功，那么计算会话密钥；若验证失败，那么发送失败消息给MME。

需要注意的是，只有第一次连接网络时才需要计算MME的公钥。

1. 验证失败阶段

如果上述聚合签名验证失败，也就是，那么说明存在无效的节点。可以使用下述方法快速检测出无效节点：

步骤1：MME发送请求失败消息给组长GL，用于请求该组中的所有。

步骤2：MME接收到eNB的消息后，将所有划分为部分子组，然后将每个子组中的签名聚合成单一签名，并且检查每个聚合签名的有效性。

步骤3：若子组的聚合签名仍然无效，那么MME执行步骤2。

步骤4：当MME发现了所有无效节点后，将失败消息返回给相应的，并且拒绝无效节点的接入。

1. 动态组成员管理机制

若某个MTC设备进入/离开这个组合，或者MTC用户想要添加/删除某个设备，均可借助动态组成员管理机制解决此类问题。具体内容如下：

加入群组：在新设备成功注册到网络后，MME检查其位置、MTC设备特性、所属的MTC用户。若它满足某个MTC群组的特性，那么MME发送更新组列表消息给HSS/KGC，该消息中包括新的标识及群组标识，然后HSS/KGC将新标识添加进群组列表中。最后，执行注册流程来获得自己的私钥。

离开群组：若某个不满足所属群组的特性或者已经被敌手所控制，那么当其接入网络时，MME发送更新群组列表消息给HSS/KGC，该消息中包括该的标识及群组标识，然后HSS/KGC将该标识从群组列表中删除并且撤销其私钥。

本方法的安全性分析如下。

1. 相互认证

基于聚合签名和ECDSA技术，可以实现MME与设备群组之间的相互认证。首先，群组中的设备需要通过MME的身份验证。在此过程中，群组中的每个会使用自己的长期私钥计算签名对。随后，基于所有签名对生成的聚合签名会被MME验证，只有合法的才能生成有效的具体签名，进而获得合法的聚合签名。一旦存在无效具体签名，则该聚合签名无效。因此，一旦聚合签名被验证，MME可以信任群组中所有设备。与此同时，群组中的每个可以通过检查ECDSA签名来验证MME，以此确保与之交互的 MME 的合法性。

1. 密钥协商

为了保护MME和组中每个之间的空口通信，通过执行ECDH密钥协商协议，不同的和MME将共享不同的会话密钥。由于CDH问题的困难性，只有合法的MME和才能建立会话密钥。

1. 密钥前后向安全和不可否认性

该解决方案可以实现密钥前后向安全。密钥前后向安全意味着即使长期密钥被泄露，前面和后面的会话密钥仍然是秘密的。该方案利用和MME的随机值保证了会话密钥的新鲜度，即使长期密钥被窃取，也不会暴露之前和之后的会话密钥。此外，由于采用了数字签名，该方案可以在某些争议性业务中提供不可抵赖安全性验证。

1. 抵抗中间人/伪装/重放攻击

该方案中会话密钥通过DH方案计算得到，中间人敌手或者群组中的其他不可能利用公开信道中的参数获得的会话密钥。敌手没有长期私钥，就不可能伪造一个有效的ECDSA签名和聚合签名来欺骗与MME。所以对于敌手来说不可能修改公共信息来实现伪装攻击。另外，该方案利用时间戳实现了抗重放攻击。

1. 抵抗信令风暴

该方案能有效避免信令拥塞，保证信令开销低和验证速度快的特点。为了避免信令风暴威胁，群组设备发出的大量访问请求消息会被组长聚合成一条请求消息，然后将这条请求消息发送给MME，MME仅计算签名并通过一条信令消息发送给组长。因此，上述方案可以极大地降低信令开销并减轻MME的负担。为了实现快速验证，MME可以采用聚合签名技术同时对一组进行认证，并快速创建与MTC群组之间的会话密钥。所以该方案可以在不限制用户的接入请求数量的情况下确保MTC用户的服务质量。此外，群组设备数量越多，该方案的性能优势越明显。

#### **10.4.2适用于机器类型通信的群组切换认证机制**

当前切换机制可能导致接入网和LTE-A核心网络严重的信令过载，增加了MTC设备的能源消耗。此外，部分基站，如本地eNB（HeNB）和中继节点（RN），可能较易被第三方掌控。在切换认证过程中，由于会交换敏感信息，攻击者便有可能借此获取设备的运动轨迹、位置等隐私信息。因此，如何保障 MTC设备在LTE-A/5G网络中实现安全且高效的移动切换，成为了该网络面临的一个关键问题。

围绕机器类型通信中海量设备的切换认证问题，本节主要介绍基于对称密码的群组匿名切换认证机制[21]、基于多重签名的mMTC的统一隐私保护组切换认证机制[22]以及针对5G异构网络间mMTC设备高效的群组切换认证机制[23]。与接入过程类似，切换过程仍然面临信令风暴问题，因此上述三种机制均采用了群组的思路来解决网络侧的信令风暴问题。在第一种机制中，基于群组成员与网络侧的共享密钥来实现群组成员在X2、Intra-MME和Inter-MME等不同场景中的安全切换；在第二种机制中，通过在接入阶段为群组成员配置公私钥对，能够实现群组成员在X2、Intra-MME和Inter-MME等不同场景中的统一快速切换；在第三种机制中，基于群组成员与网络侧的共享密钥实现了群组成员在5G异构网络之间的高效切换。

##### 10.4.2.1 机器类型通信中基于对称密码的群组匿名切换认证方法

本小节介绍一种机器类型通信中群组匿名切换认证协议，通过新的协议大幅度减少信令的流量，优化了LTE网络中大规模设备移动造成的拥塞，实现群中大量设备快速和安全的接入认证。

在3GPP现有的MTC网络体系下，该方案使用新的密钥管理机制，基于垂直或者水平密钥推导出新的密钥。MTC切换群里，在第一个从当前eNB（记为SeNB）发送到目标eNB（记为TeNB）的过程中，所有切换群成员在安全的环境下发送到目标eNB或者MME控制的eNB。然后，MTC组中其余的MTCDs可以直接在不接触MME的情况下进行切换认证过程并与目标eNB仅进行3次握手获得会话密钥。从而实现群组中设备的快速切换认证。具体执行步骤如下：

步骤1：发送测量请求信息；

如果第一个移动到目标基站TeNB覆盖范围内，发送测量请求信息给源基站SeNB，这个测量请求包括TeNB的标识，E-UTRAN单元综合识别和跟踪区域标记。

步骤2：定位设备群、计算参数并分类执行不同切换策略；

当SeNB从收到消息的时候，SeNB使用分组算法对当前的SeNB下的MTCD分类。然后SeNB搜索属于哪个MTC切换群。根据搜索结果，在MTC切换群里SeNB计算每个新的和，计算公式如下：





然后，SeNB根据以下不同的切换策略执行后面的操作：

（2.1）X2 Handover. 当切换发生在eNBs和一个X2 interface之间，进程跳到步骤3。

（2.2）Intra-MME Handover. 当切换发生在eNBs中，eNBs不包括X2 interface使用同样的MME，进程跳到步骤4。

（2.3）Inter-MME Handover. 当切换发生在eNBs中，eNBs使用不同的MME，进程跳到步骤5。

步骤3：X2 Handover切换过程，如图10.14所示，具体内容如下。



图10.14 X2 Handover切换流程图

（3.1）发送切换请求：SeNB分配一个切换请求信息给TeNB用来在目标方切换时做准备，切换请求信息包括MTC整个切换群的，和其他必要的参数。

（3.2）切换请求应答：在收到切换请求信息的时候，TeNB发送切换请求应答信息给SeNB来确认切换和计算每个新的会话密钥，计算公式如下：



（3.3）切换控制：

当收到切换请求应答消息的时候，SeNB发出一个切换控制信息给来完成切换。然后进程跳到步骤6。

步骤4：Intra-MME Handover切换过程，如图10.15所示，具体内容如下。



图10.15 Intra-MME Handover切换流程图

（4.1）切换请求：

SeNB发送切换认证请求信息给源MME（记为SMME）。

（4.2）切换请求：

当收到切换请求信息的时候，SMME通过MTC里的每个收到的计算新的和，计算公式分别如下：





然后，SMME生成一个新的切换请求信息给TeNB来准备在目标方切换做准备，切换信息包括MTC整个切换群的和和其他必要的参数。

（4.3）切换请求应答：

在收到切换请求信息的时候，TeNB发送切换请求应答信息给SMME来确认切换和计算每个新的会话密钥，计算公式如下：



（4.4-4.5）切换控制：

当收到切换请求应答消息的时候，SMME发出一个切换控制信息通过SeNB给来完成切换。然后进程跳到Step 6。

步骤5：Inter-MME Handover切换过程，如图10.16所示，具体内容如下。



图10.16 Inter-MME Handover切换流程图

（5.1）切换请求：

SeNB发送切换认证请求信息给SMME。

（5.2）前向切换请求：

在收到切换请求信息后，SMME生成一个前向切换请求信息，通过给整个MTC切换群的切换请求信息中增加并发送给目标MME（记为TMME）。

（5.3）切换请求：

当收到前向切换请求信息的时候，TMME通过MTC里的每个收到的计算新的和，计算公式分别如下：





然后，TMME生成一个新的切换请求信息给TeNB来准备在目标方切换做准备，切换信息包括MTC整个切换群的和和其他必要的参数。

（5.4）切换请求确认：

在收到切换请求信息的时候，TeNB发送切换请求确认信息给TMME，并计算每个的会话密钥，计算公式如下：



（5.5-5.6）切换控制：

当收到切换请求应答消息的时候，SMME发出一个切换控制信息通过SeNB给来完成切换。然后进程跳到步骤6。

步骤6：向发送切换确认信息：

收到切换控制信息后，生成、、和，并且向TeNB发送切换确认信息从而完成切换。

步骤7：其余MTCD设备进行切换，如图10.17所示，具体内容如下。



图10.17 其余MTCD设备切换流程图

当MTC切换群中其余的的MTCDs进入到TeNB的覆盖范围内的时候，选取为一个例子，切换过程如下：

首先发送一个测量报告信息给SeNB请求执行切换。然后SeNB直接将发送切换控制信息给。无需发送其他过程的要求，因为在切换的过程中已经把或者传送到TeNB。最后联系TeNB并发送切换确认信息，从而完成切换。

本方法的安全性分析如下。

1. 相互认证

虽然MTCD执行不同的切换策略，但是由于在SeNB与TeNB之间交互的认证数据是通过网络侧的安全通道进行，同时所有机器设备MTCD均和SeNB通过各自的安全通道交互切换信令，所以群中所有设备MTCD成功切换到TeNB后可以实现双方的相互认证，同时能够抵抗典型的重放、中间人、伪装攻击。

1. 密钥协商

在该认证方法执行完成后，每个和TeNB会生成新会话密钥，该新密钥是基于和SeNB之间的旧密钥或派生而来，由于非法实体不可能知道这两个密钥，因此除了网络侧的可信实体，其他非法实体不可能知道新会话密钥。因此该认证方法可以实现机器设备和访问网络之间的安全密钥协商。

1. 抵抗信令风暴

该方案借助新的切换策略，通过群内首个切换至TeNB的设备来定位所属群，并对群内设备加以分类。针对不同设备的切换情况，方案采用差异化的切换策略，同时省去了其他设备与MME之间的信令流量，进而大幅降低了切换过程中的通信成本，有效缓解了服务网络与归属网络之间链路的拥塞状况。尤其在设备数量庞大的场景下，该方案的优势更为显著。

##### 10.4.2.2 基于多重签名的mMTC的统一隐私保护组切换认证机制

本小节介绍一种适用于mMTC设备的基于多重签名和聚合消息认证码技术的简单且安全的统一组切换认证方案，以适应LTE-A网络中的所有移动场景。该方案包括三个阶段：初始认证阶段、统一隐私保护切换认证阶段和身份追溯阶段。在MTC组和目标eNB执行统一隐私保护组切换认证阶段时，目标eNB可以基于多重签名[24]和聚合消息认证码（AMAC）[25]同时认证整个MTC组。该方案中使用的符号含义如表10.3所示。方案具体内容如下。

表10.3 符号说明

|  |  |
| --- | --- |
| 符号 | 符号含义 |
|  | 两个k比特的素数 |
|  | 中的生成元 |
|  | 安全哈希函数 |
|  | 安全哈希函数 |
|  | 节点i的真实身份和临时身份 |
|  | KGC的私钥/公钥,, |
| GID/TGID/GPK | MTC群组的组身份标识/组临时标识/组临时公钥 |
|  | 节点i的私钥/公钥 |
|  | 随机数 |
|  | 节点i和HSS/MME的共享会话密钥 |
|  | 使用加密后的密文 |
|  | 节点i和eNB2之间的共享会话密钥 |

1. 初始阶段

在这个阶段，大量MTC设备（MD）构成MTC群组，同时群组标识也会内嵌在所有设备的内存中。相同的MTC组往往存在于相同的区域和/或具有相同的MTC特征和/或属于相同的MTC用户。在设备初始化过程中，还将根据每个MD的通信能力、通信链路质量、存储状态和电池状态，选择群组组长。当每个群组中的MD注册到网络时，执行完整的认证过程并且从密钥产生中心KGC获得私钥和公钥。KGC可以整合进HSS。KGC计算，其中均为两个随机大素数，KGC生成私钥对满足，然后选择生成元，该生成元在中具有最大阶，并且选择两个哈希函数和。最后KGC发布主公钥以及系统参数，并秘密保存私钥。假设是MTC组成员，那么当每个成员注册到网络的时候，需要执行下述流程：

步骤1：。选择随机数，将作为私钥，并且计算，然后发送公私钥请求消息给HSS/KGC，这个消息中包含自身身份、和，这些信息被和HSS/KGC之间通过EPS AKA生成的共享密钥所加密。

步骤2：。HSS/KGC接收到上述消息后，执行下述步骤：

（2.1）当第一个MD注册到网络时，HSS/KGC选择m个随机数，并且计算一系列不可链接临时组标识。

（2.2）针对每个设备，HSS/KGC选择m个随机数，然后计算一系列不可链接临时标识。

（2.3）HSS/KGC计算，将其作为的临时公钥。

（2.4）当HSS/KGC接收到来自所有的请求消息后，对每个临时群组标识，计算相应的群组临时公钥。然后，使用对进行加密后发送给每个，另外，HSS/KGC建立并存储MTC群组的身份列表，如表10.4所示。

表10.4 MTC群组身份列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 群组ID | 群组临时ID | 群组临时公钥 | 群组成员ID/成员临时ID | | |
|  | …… |  |
| GID |  |  |  | …… |  |
|  |  |  | …… |  |
| …… | …… | …… | …… | …… |
|  |  |  | …… |  |

每个eNB执行和在初始认证阶段中相同的流程。在eNB被成功验证后，eNB选择随机密钥作为私钥，并且计算，然后发送，给HSS/KGC，这些元素被封装在IKEv1[17]认证消息中。HSS/KGC接收到该消息后，派生eNB的公钥，并且发送给eNB。

在该方案中，所有的公钥被保存在HSS/KGC中，一旦怀疑公钥的有效性，或eNB可以直接向HSS/KGC发送公钥验证请求消息，请求确定公钥的有效性。

1. 群组切换认证阶段

当MTC群组从源eNB1切换到eNB2，需要执行下述组切换认证流程。为了确保整个MTC群组实现安全切换，采用多重签名方案和AMAC方案来实现MTC群组和新基站之间的相互认证和密钥协商。令。具体切换认证步骤如下：

步骤1：当MTC组移动到eNB2的范围内，每个设备执行下述流程：

（1.1）选择随机数并且计算，然后选择未使用的临时身份标识和对应的临时组标识，并且广播，和给其他n-1个MD（其中包括组长）。需要注意的是这个步骤可以在MTC组切换到新基站前实现预执行。

（1.2）接收到其他n-1个MD的后，计算和，然后计算，并且发送给，其中是eNB2的网络接入标识符。

步骤2：接收到所有的后，计算并且发送认证请求消息给eNB2。

步骤3：eNB2接受到上述消息后，执行下述流程：

（3.1）首先检查是否有效，然后计算和，从而验证是否成立。若验证有效，那么eNB2认证整个群组并且执行下述步骤，否则，发送认证失败消息给。

（3.2）选择随机数并且计算，然后计算。

（3.3）发送认证回复消息给，然后计算和每个设备之间的会话密钥。

步骤4：接收到eNB2的认证回复消息以后，广播这条消息给组内其他设备MDs。

步骤5：每台设备接收到广播消息后，执行下述步骤：

（5.1）检查等式是否成立，若验证通过，那么信任eNB2并且执行后续步骤，否则，向发送认证失败消息。

（5.2）计算会话密钥和。

（5.3）最后发送给用于实现密钥确认。

步骤6：接收到所有后，计算，并且发送该值给eNB2。

步骤7：eNB2接收到后，验证该值。若验证成功，那么eNB2确认所有生成了相同密钥。

1. 身份追溯阶段

为了追溯MTC群组，eNB2发送临时身份标识和临时群组标识给HSS/KGC。HSS/KGC接收到消息后，根据数据库来寻找对应的并且计算等式来获得真实群组标识。

一旦得到，MTC群组将会被追溯。如果HSS/KGC需要进一步获得每个MD的真实身份标识，那么它可以找到相关并计算下式来获得：

本方法的安全性分析如下。

1. 相互认证与密钥协商

在该方案中HSS/KGC可以基于多重签名和ElGamal签名技术实现MTC群组和eNB2之间的双向认证。为了通过eNB2的验证，群组中每个设备MD利用自己的私钥产生一个签名，然后将这些签名累加生成一个多重签名，eNB2可以利用公钥GPK实现对多重签名的验证。每个设备MD会接收到eNB2利用自己私钥产生的签名，并利用对继续验证。由于Multi-Decisional Diffie-Hellman (M-DDH)问题的困难性，敌手不可能知晓MD和eNB2的私钥，所以不能伪造双方的签名。因此该方案可以实现双向认证。执行完双向认证后，MD和eNB2会利用DH算法协商出会话密钥，基于DH问题的困难性，该方案可以实现安全密钥协商来保护eNB2和MD之间的通信。

1. 抵抗重放攻击

无论MTC群组何时移动到eNB2的覆盖范围内，MD和eNB2会生成新的随机数，由于会话密钥是基于新随机数产生的，从而可以抵抗重放攻击。

1. 抵抗伪装和中间人攻击

由于会话密钥的安全性是基于DH问题的困难性，所以中间人敌手不可能利用MD和eNB2之间公开通道中的信息来计算得到会话密钥。没有eNB2或MD的私钥，敌手不可能伪装一个有效的多重签名和ElGamal签名。因此方案可以抵抗伪装攻击。进一步地，基于多重签名的优势，MTC群组中的所有设备MD需要对含有和所有成员临时标识的消息进行签名，并且群组组长会对该签名进行验证。所以不属于该群组的其他合法设备不能通过对该消息签名来伪装成该群组设备来欺骗eNB2或EPC。

1. 抵抗信令风暴

在上述方案中，群组组长会将MTC群组发出的大量切换请求消息聚合成一条请求消息，并将这条消息发送给eNB2。另外，eNB2仅需计算一个签名并通过一条信令消息发送给群组组长。该方案不需要联系类似于MME和HSS的其他第三方，只需要3次握手便可实现和eNB2之间的认证。所以该方案可以大大简化信令成本并且避免信令风暴问题。另一方面，eNB2采用多重签名和AMAC技术可以同时实现对所有群组成员的认证，并且快速建立会话密钥。所以该方案可以减轻eNB2的负担，并且在没有切换请求限制的情况下确保MTC用户的QoS要求。

1. 身份隐私保护

由于方案利用未知的随机数作为每个MD的临时身份和临时群组身份，攻击者或其他eNB不能获取到MD的真实身份和真实群组身份。另外，在群组认证切换过程中每个MD会被分配新临时ID和新临时群组ID。任何敌手不能通过窃听MTC群组和eNB2之间的信道来链接临时标识。进一步地，临时群组公钥是利用随机数和临时群组标识生成的，并且该临时群组公钥在每次群组切换认证过程中得到了更新，任何敌手不能得到，所以除了HSS/KGC以外的任何人无法追踪MTC群组移动轨迹。

1. 可追踪性

在争议场景下，HSS/KGC可以利用存储的随机数及其私钥和临时身份来揭示MTC组的真实身份。因此，一旦签名有争议或其他有争议的事件发生，HSS/KGC能够追踪到MTC组。

1. 抵抗内部人攻击和DoS攻击

MTC群组的其他内部MD由于没有关于的正确随机数，所以不能获得的会话密钥，从而不能伪装成来欺骗eNB2或者EPC。所以该方案能够抵抗内部人攻击。另外，群组组长可以通过验证每个签名来认证设备，所以任何攻击者不能通过制造大量无效签名来向eNB和EPC发动DoS攻击。

##### 10.4.2.3 针对5G异构网络间mMTC设备高效的群组切换认证协议

本小节介绍一种应用于5G网络、针对mMTC设备的安全高效群组切换认证及重认证协议，该协议适用于mMTC设备同时漫游至新网络的情形。该协议包括四个阶段：LTE-A网络中的群组初始接入认证阶段（GIAA），LTE-A向WLAN的群组快速切换认证阶段（L2WGFHA），WLAN网络中群组本地重认证阶段（WGLR），以及群组成员更新阶段。当组成员注册到LTE-A网络时将会执行GIAA阶段，当组成员首次移动到WLAN网络，并且再次访问WLAN网络时，将会分别执行L2WGFHA和WGLR阶段。该协议中使用的符号定义见表10.5。

表10.5 符号说明

|  |  |  |
| --- | --- | --- |
| 符号 | 符号拥有者 | 含义 |
|  | MTC群组与HSS | X的群组ID/预共享组密钥 |
|  | MTC群组与HSS | LTE-A网络中X的群组临时密钥 |
|  | MTC群组与MME | LTE-A网络中X的群组临时ID |
|  | MTC群组与HSS | WLAN网络中X的群组本地ID/群组本地密钥 |
|  | MTC群组与 | WLAN网络中X的群组切换ID/群组切换密钥 |
|  | MD和HSS | x的私有ID/预共享密钥 |
|  | MD和HSS | LTE-A网络中x的会话密钥 |
|  | MD和MME | LTE-A网络中x的临时ID |
|  | MD和HSS | WLAN网络中x的本地ID/本地密钥 |
|  | MD和 | WLAN网络中x的切换ID/切换密钥 |
|  | MD和AP | WLAN网络中x的会话密钥 |
|  | HIU | 用于产生和的秘密参数 |
|  | HSS | 允许执行WGLR |
|  | All | 消息认证码函数 |
|  | All | 密钥派生函数 |
|  | ,HSS | 预定义的聚合时间窗口 |

1. 群组初始接入认证阶段（GIAA）

当mMTC设备想要在LTE-A和WLAN之间漫游时，这些设备首先需要注册到LTE-A网络中。由于Lai等人[18]使用了聚合MAC技术，其提出的方案具有优异的性能，所以使用该方案作为mMTC设备注册网络的认证方案。在所提认证方案中，每个MD有一个私有标识和预共享密钥。另外大量MDs根据特定原则组建成群组，依据通讯能力、计算资源、存储资源和能量续航来选出群组组长。拥有一个与HSS共享的预定义聚合时间窗口。在MTC群组成功接入LTE/LTE-A网络后，每个和HSS/MME共享一个会话密钥，然后MME产生一个群组临时标识，为每个生成临时标识，并且将和安全传输给。

1. 群组快速切换认证阶段（L2WGFHA）

当MTC群组G1首次从LTE-A网络漫游到WLAN网络时，将会执行本阶段过程。通过这个协议，群组中的每个MD会与共享一个本地密钥LK，群组与共享一个本地密钥GLK，这些密钥可以用来实现WLAN同类型切换时的重认证过程。本阶段具体流程如下：

步骤1：，具体内容为：每个MD发送临时组ID，也就是和给。

步骤2：，具体内容为：接收到内的消息后，计算，以及。最后发送给MME。

步骤3：MMEHSS：AKA Identity，具体内容为：MME接收到的消息后，MME首先使用接收到的消息和计算，并判断它和接收到的是否相等。若相等，那么MME确信是合法的，否则忽视该消息。然后MME根据和寻找正确的和每个MD的标识，然后发送和MTC群组标识给HSS。

步骤4：HSSHIU：认证请求；具体内容为：HSS接收到上述消息后，检查、、、…、是否有效，然后选择新随机数并发送给HIU。

步骤5：HIUHSS：认证回复；具体内容为：HIU产生新随机数和秘密参数，然后发送使用HSS公钥加密后的密文给HSS。

步骤6：HIU：转发Data1。具体内容为：该步骤6与步骤5同时进行，HIU产生签名值并且使用的公钥加密，最后发送密文给。

步骤7：HSS：转发Data2；具体内容为在接收到HIU的认证回复消息后，HSS使用自身私钥对该消息进行解密，并且验证。若验证成功，那么HSS相信HIU是合法的，并且计算组密钥，组标识，本地密钥和本地临时标识。HSS利用自己的私钥产生签名值，并且使用的公钥加密这些密钥和参数，最后发送密文给。

步骤8：在接收到HSS和HIU的消息后，首先解密这些信息并且计算组切换密钥，组切换标识，切换密钥，切换标识。最后，存储这些信息用于后续切换认证。

步骤9-10：HSSMME，MME：AKA通知；具体内容为：HSS使用密钥加密并且借助MME转发密文给。

步骤11：接收到来自MME的消息后，将其转发给所有MD设备。然后每个群组设备MD重新计算，，，，，，，和，并存储。然后MTC群组设备和开始执行下述相互认证流程：

步骤12：，：身份请求；具体内容为：AP广播身份请求消息给所有设备MDs。

步骤13：：身份回复消息；具体内容为：每个设备MD发送切换群组标识和给。

步骤14：：群组标识回复消息；具体内容为：接收到所有的之后，计算，并发送和必要参数给。

步骤15：：群组挑战请求消息;具体内容为：接收到来自的消息后，首先利用密钥验证。若验证成功，那么可以相信该消息是来自于合法的，这是因为合法的用户才能拥有；否则，忽视该消息。验证成功后，生成新随机数并且计算。最后发送给。

步骤16：：群组挑战回复消息；具体内容为：接收到的消息后，将发送给所有群组设备MDs。然后每个设备利用密钥验证和是否有效。若验证失败，那么中止认证过程。否则，可以成功认证，因为只有合法的才能派生密钥并计算有效的。然后每个设备计算，并发送给。最后产生，并发送给。

步骤17：：成功接入消息；具体内容为：当接收到挑战回复消息后，利用检验是否有效，若验证成功，那么信任MTC群组，然后递减，并发送成功接入消息给AP。否则，中止认证过程并将接入失败提醒消息发送给HSS。

步骤18：：成功提醒消息；具体内容为：AP接收到上述成功接入消息后，存储用于产生密钥并且发送成功提醒消息给群组设备。

步骤19：当每个设备接收到成功提醒消息后，递减并使用计算共享密钥。

1. WLAN网络群组本地重认证阶段（WGLR）

当群组设备由3GPP网络移动到WLAN网络中，需要执行群组本地重认证过程，通过这个协议，MTC群组和可以在无需联系归属网络的情况下，实现相互认证和密钥协商。这个阶段具体流程如下：

步骤1：：EAPoL启动消息；具体内容为：当MTC群组连接到WLAN网络中的新，发送EAPoL启动消息给旧来启动切换流程。

步骤2：，：身份请求消息；具体内容为：广播身份请求消息给，然后再给所有设备。

步骤3：：身份回复消息；具体内容为：每个设备发送切换群组标识给。

步骤4：：群组身份回复消息；具体内容为：在接收到后，发送给。

步骤5：：群组身份回复消息；具体内容为：转发群组身份回复消息给。

步骤6：：群组挑战请求消息；具体内容为：接收到消息后，生成新随机数并使用群组切换密钥计算，然后发送给。

步骤7：：群组挑战回复消息；具体内容为：接收到来自的消息后，转发该消息给所有群组设备，然后每个设备使用密钥验证，若验证无效，那么中止重认证流程，若验证有效，那么成功被验证，计算后发送给，最后计算并发送给。

步骤8：：切换命令消息/；具体内容为：接收到消息后，利用验证，若验证有效，那么群组设备被成功验证，然后递减并计算新的，，和，然后发送切换命令消息给所有设备，另外发送带有的切换命令消息给。若验证失败，那么中止验证过程，并且向HSS发送失败消息。

步骤9：在接收到消息后，递减并采用类似的计算方式计算新的，，和，然后每个和利用计算共享密钥。

1. 群组成员更新阶段

如果某个群组成员被偷窃或俘获，或者MTC用户想要加入新设备或删除旧设备，HSS需要执行群组成员更新流程。

若HSS接收到更新群组成员请求消息来删除某个群组成员，那么HSS执行下述群组成员更新流程：

步骤1：HSS生成新随机数并产生新群组密钥和群组标识，然后删除相应的设备标识从而更新群组列表。

步骤2：HSS使用所有群组成员的密钥加密群组密钥和群组标识。

步骤3：HSS使用新群组密钥和群组身份标识来执行GIAA流程，并且发送群组认证数据回复消息给新群组中的每个设备。

步骤4：当新群组中的每个设备接收到该消息后，利用自身私钥对其解密并获得新群组密钥和群组标识。然后用新群组密钥和新标识替换旧密钥、旧标识。

若HSS接收到更新群组成员请求消息来添加某个群组成员，那么HSS执行下述群组成员更新流程：

当新设备MD注册网络时，HSS检查其位置和MTC特性，若它满足MTC群组的特性或HSS接收到群组成员更新请求，那么HSS将该设备标识添加到群组列表中，并且使用该设备私钥加密群组密钥和群组标识，随后将密文发送给MME，若MD的注册认证过程是有效的，那么MME将密文发送给MD。

本方法的安全性分析如下。

1. 相互认证

在L2WGFHA中，MTC群组和通过计算和检验和来实现相互认证。当被验证通过时，每个MD可以确信是合法的。当被验证通过时，可以确信MTC群组是合法的。这是因为和分别是由和派生而来。这些密钥是由、和秘密参数派生而来的，参数仅由MD和/HSS共享。所以只有合法的MTC群组设备MD和才能计算有效的和。在WGLR中，MTC群组和通过计算和检验和实现相互认证。和分别是由和派生而来。这些参数仅由MD和共享。

1. 抵抗重放攻击

通过利用随机数和计数器，上述方案可以抵抗重放攻击。在L2WGFHA中，随机数和计数器被用来确保认证消息的新鲜性。另外，所有密钥和都是利用新鲜随机数和衍生而来，从而能够抵抗重放攻击。在WGLR中，类似于L2WGFHA，认证消息和所有密钥都基于随机数和计数器而产生。

1. 抵抗中间人攻击

在上述方案中，由于MTC群组和MME/实现了相互认证，MD和AP之间生成了会话密钥，所以可以使用密钥对MTC群组和MME/之间的载荷进行加密保护，从而防止通信内容被敌手窃听。另外，通过使用消息验证码技术，上述方案可以确保重要消息的完整性和真实性以及验证通信对方的真实性，所以任何敌手不能实施中间人攻击来威胁该方案。

1. 抵抗内部伪装攻击

在上述方案中，MTC群组成员MD会与分别协商各自的会话密钥，任何MDs不可能伪装成其他成员去欺骗。在L2WGFHA和WGLR中，和AP之间的会话密钥基于而生成。由于和基于每个MD的派生而来，MTC群组任何内部成员不可能获得其他成员的会话密钥来发送内部伪装攻击。

1. 身份隐私保护

上述方案可以使用临时标识来实现身份隐私保护。一旦建立了第一个临时ID，任何敌手不可能知道MTC群组成员设备的真实ID。在L2WGFHA和WGLR中，MTC群组标识GLID或GHID均是临时标识，每个MD的标识LID或HID均是临时的，在每个认证会话中，GLID/LID会通过随机数实现更新，所以任意敌手不可能通过猜测或解密GLID/LID来知道并追踪每个MD或者MTC群组。另外，GHID/HID也会通过随机数实现更新，所以任意敌手不可能通过猜测或解密GLID/LID来知道并追踪每个MD或者MTC群组。

1. 密钥协商

在上述方案中，MTC群组成员设备将分别和AP建立各自的会话密钥。另外，该密钥基于和衍生而来。由于和基于每个MD的派生而来，同时由于仅由MD和HSS共享，所以其他节点不可能计算出和。所以该方案能够实现安全密钥协商。

#### **10.4.3****适用于5G NB-IoT的大规模设备快速认证与数据传输方案**

随着未来5G NB-IoT的快速商用进程，海量NB-IoT设备的并发接入容易导致严重信令拥塞，如果NB-IoT设备使用传统的普通终端的接入认证和数据传输方案来实现小额数据的安全传输，可能会产生大量的信令和通信开销，同时现有5G AKA中基于公钥加密技术的身份隐私保护技术不适用于计算资源和能量有限的物联网终端。因此，如何让海量的NB-IoT设备快速并安全的接入到移动网络中便成为当前一个亟待解决的挑战。

围绕5G海量NB-IoT设备的快速认证与安全传输问题，本节主要介绍基于聚合签密的快速接入认证和数据传输方案[28]、抗量子的快速接入认证与数据传输方案[29]以及抗物理攻击的快速接入认证与数据传输方案[16]。上述方案在实现海量NB-IoT设备安全接入的同时，能够解决网络侧的信令风暴问题，并且利用5GS控制面优化方案在相互认证，实现小额数据的安全传输，减少冗余的信令开销，适用于资源有限的NB-IoT设备。相比现有标准认证协议，具有更强的安全属性。针对相同的NB-IoT接入场景，上述方案聚焦于不同的安全问题。第一种方案在保障认证和密钥协商的同时，能够实现不可否认性，并且避免证书的复杂管理和私钥托管的局限性。随着量子计算机的快速发展，量子攻击也成为一种主要的密码协议攻击手段，因此第二种方案考虑了未来的量子攻击，具有重要的研究价值。第三种方案主要针对一些部署于固定位置的NB-IoT设备，能够抵御潜在的物理攻击，并且具有较高的轻量性，非常适合资源受限的NB-IoT设备。

##### 10.4.3.1基于聚合签密的快速接入认证和数据传输方案

无证书聚合签密技术可以将不同用户生成的不同消息的签密信息聚合为聚合签密信息，不仅可以保证信息传输的机密性和认证性，还可以降低信息传输的功耗，因此可以应用于大规模设备场景中的多对一通信。但是，现有的无证书聚合签密方案都采用双线性配对运算，这会导致较低的计算效率。为了解决这一问题，本节介绍一种针对海量NB-IoT设备的基于无证书聚合签密技术的快速认证与数据传输方案，通过改进[30]提出的基于无证书聚合签密方案，能够在不牺牲其安全性的前提下适应未来5G网络中海量NB-IoT设备的场景要求。例如，本方案将NB-IoT组标识添加到“密钥分发”过程中，并且通过将“密钥分发”过程添加到每个NB-IoT设备中并生成新的组临时密钥GTK。在此过程之后，AUSF分别将部分私钥发送给NB-IoT设备与网络侧AMF。当NB-IoT设备需要进行接入到核心网并进行数据传输时，网络侧AMF同时完成与一组NB-IoT设备的相互认证与数据传输过程，并在每个NB-IoT设备和AMF之间建立了基于Diffie-Hellman（DH）密钥协议的独特会话密钥SK，实现相互认证与下行数据的安全传输需求。

在本方案中，同一区域中具有相同或相似属性的大规模NB-IoT设备构建为NB-IoT固定或临时组，然后选择群组组长（Group Leader，GL）。当多个NB-IoT设备同时启动对5G网络的接入认证过程时，所有组成员的访问认证信息和加密的敏感数据将由GL进行聚合。然后，GL将聚合接入身份认证信息发送到5G核心网络，以便网络可以根据GL生成的无证书聚合签密同时检查整个NB-IoT组的有效性。本节方案可以在执行接入认证过程中同时实现安全数据传输，而无需实施两个独立的过程，而且还提供了包括身份隐私保护和不可否认性在内的强大的安全保护。

本节介绍的基于聚合签密的快速接入认证和数据传输方案所使用符号如表10.6所示。该方案可以分为下面两个阶段：初始化阶段和基于群组的接入认证和数据传输阶段，详细介绍如下：

表10.6 符号说明

|  |  |
| --- | --- |
| 符号 | 符号定义 |
|  | 哈希函数 |
|  | 哈希函数 |
|  | 哈希函数 |
|  | 哈希函数 |
| Q | 一个k比特大小的素数 |
| G,P | 循环群G与群G的生成元P |
|  | 系统的私钥和公钥 |
|  | 用户的私钥 |
|  | 用户的公钥 |
|  | NB-IoT设备 |
|  | NB-IoT设备与AMF间的会话密钥 |
| TS | 时间戳 |

1.方案初始化阶段

a.系统初始化阶段：

定义阶为素数的循环群G，P为群G的一个生成元。然后选择三个密码安全散列函数：，，。其中和是输入内容的比特长度。最后，AUSF选择一个随机数作为主密钥，计算系统公钥，然后发布作为系统参数，保密主密钥。

b.群组生成阶段：

在此阶段中，属于同一位NB-IoT用户、具有相同位置、相同功能或其他相同特征的大量NB-IoT设备将构建为一个NB-IoT群组，接着，供应商将根据设备相应的能力（例如每个NB-IoT设备的通信能力，存储状态和电池状态等）来为每个NB-IoT设备群组选择一位组长GL。该组组长将同时或几乎同时被激活以通过3GPP 5G网络接收或传输敏感数据到NB-IoT用户。每个NB-IoT组具有私有群组身份标识与组密钥，它由供应商预先存储在NB-IoT组中的每个NB-IoT设备和AUSF之间。

c.密钥分发阶段

步骤1：随机选取秘密值，计算公钥，然后通过接入网基站gNB向5G核心网实体AUSF发送包含身份、组身份标识和公开参数的密钥请求消息。

步骤2：AUSF收到设备的密钥请求消息后检查收到的和，以确认是否为有效的成员或者是的组成员，随后，AUSF计算临时组密钥，其中是在NB-IoT组，AMF与AUSF中保密的安全散列函数，同时，AUSF随机选取，然后计算，和。

步骤3：每个的私钥设置为，公钥设置为。

网络侧AMF的密钥分发阶段与用户侧类似，具体如下：

步骤1：AMF随机选取秘密值，计算公钥，然后向核心网AUSF发送包含身份，和公开参数的密钥请求消息。

步骤2：AUSF收到AMF的密钥请求消息后，随机选取，然后计算，和。

步骤3：AMF的私钥设置为，公钥设置为。

2.基于群组的接入认证与数据传输阶段

在这个阶段，在NB-IoT组与AMF之间秘密传输上行链路和/或下行链路数据的同时，整个NB-IoT组可以实现与AMF相互认证。当NB-IoT组被激活并请求连接到网络去发送或接收数据时，所有组成员的加密数据和相关认证信息（即签密结果）由GL聚合以生成聚合签密。然后GL发送聚合签密结果和其他相关参数发送给AMF，以便AMF可以基于由GL生成的聚合签密来一起验证整个NB-IoT组的合法性。为了保证下行数据的安全性，本文在每个NB-IoT设备和AMF之间建立基于Diffie-Hellman密钥协议的独特会话密钥。然后，AMF通过使用其私钥生成签名，并将加密后的下行数据发送给NB-IoT组。最后，NB-IoT组通过验证签名来检查AMF的有效性，并通过使用不同的会话密钥来解密下行链路数据。如图10.18所示，该过程详细说明如下：



图10.18 基于聚合签密的群组认证与数据传输阶段流程图

步骤1：每个随机选择，然后计算并将发送给其余n-1个群组成员，同时计算下列公式：













若终端想发送数据，包含的签密结果以及其它必要参数嵌入到接入请求消息中并发送至GL。

步骤2：GL在收到接入请求消息后计算下列公式：



随后验证等式是否成立，若等式成立，则计算公式1-8：



然后GL将聚合接入请求消息发送给网络侧AMF。

步骤3：AMF在接收到聚合接入请求消息后，计算下列公式：













然后AMF验证等式1-14是否成立，若等式成立，则认为此聚合签密是有效的，AMF将认为这一NB-IoT群组是合法的并且传输的数据是有效的。随后AMF随机选择并计算。然后AMF计算下列公式：





这里是一个成功标识符。当AMF需要传输下行数据时首先为每个终端生成一个会话密钥与组会话密钥。然后利用密钥加密各不同的下行数据或者利用密钥GSK加密相同的下行数据。然后生成聚合请求响应消息并将其发送至GL。

步骤4：GL将聚合接入响应消息广播给每个。然后，每个通过等式（1-17）验证AMF是否合法：



若验证通过且有下行数据需要接收，则会生成会话密钥或组会话密钥来解密或以获得下行链路数据。

3.对方案流程的相关讨论

在实际的应用场景中，NB-IoT设备可能存在故障、被劫持、并被攻击者盗用等情况。 另外，NB-IoT用户可能希望在NB-IoT组中增加/减少新的/旧的NB-IoT设备。例如，在智能电表场景中，建筑物中的所有智能电表都可以组成一个组。当建筑物内某个人的电表被毁坏或新用户进入建筑物时，该组便需要更新。为了实现动态的群组成员更新，本文可以使用方案[27]提出的动态群组成员管理机制。在该方案中，AUSF将执行组成员更新过程以完成新的/旧的NB-IoT设备加入或退出。

此外，本节所介绍的方案也可以扩展到设备接入和数据传输场景。即使大量的设备不属于同一个用户或拥有相同的功能，也可以构建一个临时组来同时实现接入认证和数据传输。为了进一步简化设备信令流程，满足大规模并发处理的需求，许多固定组可以形成一个大的临时组。假设有很多设备或固定组通过采用基于匿名属性的组设置机制[31]，它们基于相同的属性（例如，位置，触发时间，在相同安全级别传输数据等）形成了一个临时组。然后，可以将部署在5G无线接入网中的基站或新的信令汇聚网关视为临时组的汇聚节点，完成GL的任务。由于雾计算技术已被视为新的5G网络体系结构之一[32]，以使基站或接入点能够进行计算和处理，因此汇聚节点可汇聚来自临时组的接入请求消息，并生成聚合签密。

本方法的安全性分析如下。

1. 相互认证

上述方案可以实现NB-IoT设备群组与AMF之间的相互认证。在AMF对每个进行认证的过程中，合法签密结果、和仅由有效的生成，因此GL将计算正确的聚合签密结果。如果没有秘密私钥，那么任何对手都无法获得有效的签密和聚合签密结果。另外，每个终端可以通过使用其私钥生成数字签名来对AMF进行认证。

1. 数据的保密性与完整性

为了安全地传输或接收数据，每个基于无证书聚合签密技术对上行数据进行加密和完整性保护。只有合法的能够通过使用其私钥和AMF的公钥来获得正确的签密，并且合法的聚合签密结果将由GL生成。只有合法的AMF才能使用其私钥和每个的公钥来解密和验证聚合签密结果。另外，下行链路数据会通过每个和AMF之间的会话密钥或者NB-IoT组与AMF之间的秘密群组会话密钥来加密。会话密钥是通过使用椭圆曲线Diffie-Hellman算法生成的，该协议的保密性是基于计算Diffie-Hellman问题的困难性。群组会话密钥是通过使用仅存储在NB-IoT组、AMF和AUSF之间的密钥生成的。此外，上述方案还使用了数字签名来保护下行数据的完整性。

1. 抵抗典型攻击

上述方案通过将随机数加入生成的签密来抵抗重放攻击。此外，由于方案中的会话密钥是基于计算Diffie-Hellman问题生成的，因此任何攻击者都无法通过窃听公共值来获取会话密钥，这样便可防止中间人攻击。此外，任何攻击者在没有私钥的情况下无法伪造有效的聚合签名或数字签名以欺骗AMF或，攻击者因而无法发起伪造攻击。在本文的方案中，任何不可能使用不同的会话密钥来窃取的下行链路数据，因为的会话密钥是基于Diffie-Hellman算法而导出的。

1. 身份隐私保护

上述方案可以通过在每个会话中加密的身份和群组身份来提供身份隐私保护。通过上述方案，的身份信息和组身份信息被嵌入到上行数据中并通过使用接收方AMF的基于公钥的签密技术进行加密。如果没有接收方AMF的私钥，任何攻击者都不可能通过解密该消息来获取和，因此上述方案可以实现隐私保护。

1. 抵抗信令风暴

上述方案通过改进现有的无证书聚合签密技术，将来自大量NB-IoT设备的所有接入请求消息聚合为一个群组接入请求消息，该方案大大减少了信令消息，并简化了接入认证过程。同时该方案允许一组NB-IoT设备同时连接到网络，从而保证了接入认证的QoS要求。另外，此方案的数据传输过程已嵌入到接入认证过程中，从而不需要建立数据传输连接，这在很大程度上减轻了能量有限的NB-IoT设备和网络的负担。

##### 10.4.3.2抗量子的快速接入认证与数据传输方案

在上一小节中，通过改进现有的无证书聚合签密技术，提出了针对海量NB-IoT设备的快速接入认证与数据传输方案，该方案大大降低了网络的负担，简化了认证过程。然而，面对未来量子计算机的攻击，该方案仍然无法有效地抵御量子攻击。因此，如何在海量的NB-IoT设备接入认证和数据传输的环境下保证其有效地抵御量子攻击便成为当前又一个亟待解决的挑战。研究发现，使用格密码技术能够有效地抵御量子攻击的威胁，而现有的基于格上的密码体制大部分是以LWE问题为安全性依据的。BGV算法建立在LWE问题的难度之上，是目前效率最好的一种全同态加密算法，为了使此方案能够更好地适用于5G网络中的海量NB-IoT系统从而实现相互认证与身份隐私保护功能，同时降低计算成本以适用于资源有限的NB-IoT设备，因此需要对现有BGV方案进行简化与改进。

为了解决这一问题，基于无证书聚合签密思想，本节介绍一种针对海量NB-IoT设备的抗量子快速认证与数据传输方案，该方案通过改进现有的基于BGV的同态加密方案，以适应未来5G网络中海量NB-IoT设备的场景要求，并且具备抗量子攻击在内的安全性。具体地，由于原始方案并不具有聚合签密过程，为了使方案适用于群组认证场景，本文方案在原始方案的基础上增加了聚合签密步骤，即：每个NB-IoT设备的身份由群组组长（Group Leader，GL）来进行认证并将加密后的数据进行聚合，接着网络侧AMF通过认证群组组长GL的身份进而验证整个设备群组的有效性；为了防止数据被篡改或伪造，在方案中引入了时间戳字段TS；此外，由于原始方案并不具有相互认证过程，为了实现方案的相互认证过程，本文方案增加了在下行数据传输过程中网络侧AMF签密与NB-IoT设备验签的流程，以便实现NB-IoT设备对网络侧AMF的认证过程。本节方案能够在执行接入认证的同时实现安全数据传输，而无需实施两个独立的过程，而且还提供了包括相互认证、身份隐私保护与抗量子攻击的强大安全保护。

本节介绍的抗量子的快速接入认证和数据传输方案所使用符号如表10.7所示。该方案可以分为下面两个阶段：初始化阶段和基于群组的接入认证和数据传输阶段，详细介绍如下：

表10.7 抗量子的快速接入认证和数据传输方案符号说明

|  |  |
| --- | --- |
| 符号 | 符号定义 |
|  | NB-IoT设备数量 |
|  | 两个素数 |
|  | 系统安全参数 |
|  | 一个抗碰撞哈希函数： |
|  | 一个环，定义为： |
|  | 一个商环，定义为： |
|  | 两个离散的高斯分布 |
|  | NB-IoT设备身份标识 |
|  | NB-IoT设备组长身份标识 |
|  | AMF的身份标识 |
|  | NB-IoT设备 |
|  | NB-IoT数据单元 |
| GID | NB-IoT设备组身份标识 |
| TS | 时间戳 |

1.方案初始化阶段

a.系统初始化

AUSF执行以下步骤来实现系统初始化，详细步骤如下所示：

步骤1：设定消息空间为，以及设定密文空间为，其中和是两个质数。

步骤2：指定一个抗碰撞的哈希函数：。

步骤3：随机选择一个，将设置为全局公共参数。

步骤4：按照高斯分布选择和，计算作为群组内第i个设备的加密公钥，且将第i个设备的加密私钥设置为。

步骤5：按照高斯分布选择和；计算作为群组内第i个设备的签名公钥，且将第i个设备的签名私钥设置为。

步骤6：发布公共参数并保留秘密，其中。

b.群组生成阶段

在此阶段中，属于同一位NB-IoT用户、具有相同位置、相同功能或其他相同特征的大量NB-IoT设备将构建为一个NB-IoT群组，接着，供应商将根据设备相应的能力（例如每个NB-IoT设备的通信能力，存储状态和电池状态等）来为每个NB-IoT设备群组选择一位组长GL 。该组组长将同时或几乎同时被激活以通过3GPP 5G网络接收或传输敏感数据到NB-IoT用户。每个NB-IoT组具有私有群组身份标识，它由供应商预先存储在NB-IoT组中的每个NB-IoT设备和AUSF之间。

c.密钥生成与发放

AUSF为每个，GL 和每个AMF分配一对公钥和私钥，详细步骤如下所示：

步骤1：对于网络侧AMF，AUSF选择并计算。然后，设置AMF的公钥为，私钥为。

步骤2：对于NB-IoT设备组组长GL ，AUSF选择并计算。然后，设置设备组组长GL 的公钥为，私钥为。

步骤3：对于每个NB-IoT设备，AUSF选择并计算。然后，设置的公钥为，私钥为。

2.基于群组的接入认证与数据传输阶段

在此阶段，方案将执行整个NB-IoT组与AMF之间的相互认证和数据传输过程，如图10.19所示，详细步骤如下：



图10.19 抗量子的相互认证与数据传输流程图

步骤1：每个NB-IoT设备准备要发送的明文数据，然后执行以下内容：

（1.1）随机选择。

（1.2）计算，其中并且。

（1.3）从中随机选择，然后计算，，和。

（1.4）每个NB-IoT设备生成自己的签名，并将和嵌入到访问请求消息中发送给GL 。

步骤2：当GL接收到该组中所有成员的访问请求消息后，将执行以下内容：

（2.1）首先通过等式验证签名，如果等式成立，则签名有效，并跳至下一步。否则，则认为认证不通过并将此签名丢弃。

另外，如果上述等式中和足够小，并且等式也成立。

（2.2）将收到的组内所有设备的密文聚合：。

（2.3）从中随机选择，然后计算下列公式：









（2.4）生成聚合签名，并将和嵌入到访问请求消息中发送给网络侧AMF。

步骤3：网络侧AMF在接收到聚合访问请求消息后，AMF执行以下内容：

（3.1）首先通过等式（2-5）验证签名，如果等式成立，则签名有效，并跳至下一步。否则，则认为认证不通过并将此签名丢弃。



另外，如果上述等式中的值足够小，等式（2-6）也成立：



（3.2）通过计算，AMF可以通过使用其私钥恢复m。也就是说，AMF可以恢复NB-IoT设备组发送的聚合明文数据m。

步骤4：在此时，若AMF需要发送下行数据时，则AMF准备需要发送的明文数据，然后执行以下内容：

（4.1）随机选择。

（4.2）计算，，并且。

（4.3）从中随机选择，然后计算下列公式：









（4.4）网络侧AMF生成自己的签名，并将和嵌入到访问请求消息中发送给GL 。

步骤5：在GL 接收到聚合访问身份认证响应消息后，GL 将聚合访问认证响应消息广播到每个NB-IoT设备。然后，每个NB-IoT设备实现以下操作：

（5.1）首先通过等式（2-11）验证AMF的签名，如果等式成立，则签名有效，并跳至下一步。否则，则认为认证不通过并将此签名丢弃：



另外，如果上述等式中和的值足够小，等式（2-12）也成立：



（5.2）每个NB-IoT设备获得AMF的密文后，可以通过使用其自己私钥恢复明文。也就是说，每个NB-IoT设备可以恢复网络侧AMF发送的明文数据。

本方法的安全性分析如下。

1. 相互认证

上述方案可实现NB-IoT设备组与AMF之间的相互认证。一方面，只有合法的可以生成合法的签密结果，从而由GL 生成正确的聚合签密结果。没有正确有效的私钥，攻击者将无法获得有效的签密和聚合签密。另一方面，NB-IoT设备可以通过验证AMF生成的签密来检查AMF是否合法。

1. 抵抗典型攻击

由于抗量子认证方案使用了格密码，因此方案可抵抗量子攻击。另外，任何攻击者都无法在没有获得私钥的情况下伪造合法的签密结果和合法的聚合签密结果，因此上述方案是不可伪造的。此外，上述方案在签密生成中添加了随机数，因此该方案可以抵抗重放攻击。

1. 身份隐私保护

本文方案中每个NB-IoT设备的身份是使用AMF的公钥加密和传输的。如果攻击者没有获得AMF的私钥，则该消息将无法解密，因此无法获得设备的身份信息。

1. 数据的保密性与完整性

上述方案使用密码加密技术来确保数据传输过程的安全性。没有AMF的私钥，任何攻击者都无法解密数据。同时，上述方案使用数字签名技术来确保数据传输过程中传输数据的完整性。只有合法的可以使用其私钥生成合法的签密结果并得出合法的聚合签密结果。只有合法AMF才能使用其私钥解密数据，并通过使用每个的公钥来验证聚合签密结果。

1. 不可链接性

在上述方案中，的不可链接性基于R-SIS问题的困难性。每个都使用其私钥创建服务请求消息。此外，由于存在抗碰撞的哈希函数H，因此没有任何有用的信息可以链接两个签名。之后，每个都会匿名发送相应的消息和签名。基于R-SIS问题的困难性，敌手很难确定两个签名和是否由同一私钥产生。也就是说，敌手无法决定两个签名是否来自同一。

1. 抵抗信令风暴

在GL 收到NB-IoT设备组的访问请求消息后，上述方案采用聚合签密方法将多个设备签密结果转换为聚合签密结果，然后AMF支持同时认证所有NB-IoT设备，从而无需依次认证单个设备。此过程可以大大减少信令开销并简化身份验证过程。另外，本方案中的接入认证和数据传输过程均是在不建立数据承载的情况下同时进行的，因此本方案可以大大减轻网络负担，避免发生网络拥塞情况。

##### 10.4.3.3抗物理攻击的快速接入认证与数据传输方案

随着未来NB-IoT的快速商用进程，除了较为突出的问题，比如海量设备导致严重信令拥塞、甚至服务崩溃，NB-IoT场景也需要考虑设备的物理安全性，特别是IoT设备（简称为IoTD）在户外就很容易被接触访问，例如智能电表应用，因此它们更容易遭受侧信道或克隆等物理攻击，硬件上的秘密（如预先配置的对称密钥或私钥）可能更容易被对手以非法手段获取到，从而攻击者可以解密历史信息并伪装成目标设备，这对用户和服务商来说不是一件乐观的事。例如，被攻陷的智能水表将虚假的用水量转发到后端，从而迫使用户承担昂贵的定价；另外如果所有设备都配置了相同的密钥，那么攻击者也可以控制所有设备发起拒绝服务(DoS)攻击从而使网络崩溃，最终影响用户的正常生活。

为了解决上述问题，本小节介绍一种适用于NB-IoT大规模设备的基于物理不可克隆函数（PUF）的快速认证和数据传输方案。PUF芯片往往内嵌在IoTD中，PUF的输出可以视为与核心网的共享根密钥，从而实现相互认证和密钥协商，并基于PUF自身特性可以实现抗物理攻击。通过选定一个组长作为中继，对每个设备生成的所有认证请求进行聚合，将聚合后的消息转发到网元AMF，从而处理大量设备信令、避免信号拥塞、大大降低通信开销；另外，每个设备还需要发送截断码，从而方便网络侧也可以通过单个截断码找到虚假的设备节点，也就是说，一旦聚合码验证失败，那么网络侧可以通过检验相关截断码，有效地区分伪设备和真设备；最后，IoTD将认证信息连同应用程序数据一同发送给AMF，从而实现低延迟与节省功耗的效果。

本方案所使用符号如表10.8所示。该方案可以分为下面两个阶段：初始化阶段和基于群组的接入认证和数据传输阶段。详细介绍如下：

表10.8 基于PUF的快速接入认证和数据传输方案符号说明

|  |  |
| --- | --- |
| 符号 | 符号定义 |
| m | 群组的数量 |
|  | NB-IoT设备的数量 |
| CRP | PUF的挑战响应对 |
|  | 第i个NB-IoT设备 |
|  | AMF产生的随机数 |
|  | 属于内嵌PUF的挑战值 |
|  | 将作为PUF输入后的响应 |
|  | 属于设备组长GL内嵌PUF的挑战值 |
|  | 将作为PUF输入后的响应 |
|  | 抗碰撞哈希函数： |
| 或 | 设备或设备组长GL的伪身份标识 |
| 或 | 设备的伪身份标识 |
|  | 设备群组身份标识 |
|  | 组会话密钥 |
|  | 设备的会话密钥 |
|  | 由派生的秘密值 |
|  | 属于设备的加密应用数据 |
|  | 设备组长产生的认证码 |
|  | AMF产生的认证码 |
|  | 设备产生的认证码 |
|  | 设备产生的截断码 |
|  | 所有设备的聚合码 |
|  | A的比特长度 |

1.方案初始化阶段

在系统初始化阶段，每个IoTD在出厂时都需要配置PUF芯片，同时每个设备在核心网注册时，每个设备需要产生一组挑战响应对并且存储。网络侧核心网设备UDM需要预先存储。在设备部署之前，属于同一用户、或者位居相同地理位置、具有相同功能的大量IoTD设备构成一个群组，并且基于计算能力、通信能力、以及设备续航等性能条件来选定该组的组长设备（Group Leader，GL）。为这一组选定一个秘密群组标识，每个设备成员预先存储各自身份，伪身份和所属群组标识。组长设备也需要存储群组标识，自身标识，以及伪身份。同时网络侧核心网设备也需要存储对应的，，，和。

2.基于群组的接入认证与数据传输阶段

这个阶段中，设备组长GL需要提供有效的给网络侧，所以它会发起认证请求消息给AUSF/UDM，然后AUSF/UDM通过检查时间戳和认证码来确保请求消息来自于有效的群组，另外，AUSF/UDM从该群组中检索到所有，并且计算秘密值，并转发给AMF用于产生相应认证信息，AMF产生认证消息后需要返回给所有设备。在所有设备验证AMF回复的消息后，将认证信息和加密的应用数据一起发送给GL，后者聚合所有收到的消息，然后转发给AMF，之后AMF验证接收消息的合法性，并且将认证结果通知给AUSF/UDM。这个过程不仅实现了群组和AMF之间的双向认证，而且完成了密钥协商。流程图见图10.20。具体流程如下：



图10.20 抗物理攻击的快速接入认证与数据传输流程图

步骤1：设备组长GL产生时间戳和，并计算，最后发送认证信息给AUSF/UDM。该消息用于让网络侧验证该设备群组身份。

步骤2：AMF接收到上述消息后，对该消息进行透明转发给AUSF/UDM。

步骤3：AUSF/UDM接收到上述消息后，可以利用检索到所有组成员以及，其中，然后检索时间戳是否过期以及的有效性，时间戳的有效期可以由运营商自主设置；若时间戳和均有效，那么AUSF/UDM计算出，并生成新随机数。最后AUSF/UDM发送给AMF。

步骤4：AMF接受上述消息后，计算，以及会话密钥，组密钥，认证码。最后AMF发送认证消息给GL。

步骤5：GL接收到上述消息后，将其广播给每个组成员。

步骤6：所有组成员IoTD根据接收相应的消息，然后执行下述操作：

（6.1）使用预先存储的挑战值计算。

（6.2）计算。

（6.3）计算。

（6.4）计算以及。

（6.5）验证的有效性，如果有效，那么继续下述步骤，否则返回错误消息给AMF。

（6.6）当IoTD需要传输应用数据时，那么需要计算密文。

（6.7）计算自身认证码，该认证码同时能够保证消息的完整性。

（6.8）为了能够让网络侧判断出那个节点是恶意的，截取的前8bits，记为。

（6.9）产生新的伪身份用于下一次注册认证，可以注意到由于内部人不知道，所以其无法将关联到对应的。

（6.10）所有设备发送认证请求消息给GL，该消息中包含认证信息。

步骤7：GL接收到上述消息后，开始聚合所有消息中的认证码，也就是计算，最后生成并发送消息给AMF。

步骤8：AMF接收到上述消息后，AMF根据所有检索到对应的密钥和，然后执行下述步骤：

（8.1）与采用同样的方法分别计算。

（8.2）计算，并且判断等式是否一致。

（8.3）如果成立，那么AMF可以肯定所有设备是有效的，那么AMF忽略所有，并且使用解密，最后发送成功认证消息给AUSF/UDM。AUSF/UDM更新用于下一次认证。

（8.4）如果不成立，那么依次判断等式是否有效，若无效，那么AMF可以确定第i个节点是恶意的，若有效，那么AMF需要再一次请求这些有效节点的聚合认证码，因为有效的截断码不能充分证明该节点是可信节点。当这些节点再次将聚合认证码发送过来后，AMF继续验证聚合认证码，若有效那么AMF发送成功确认消息给AUSF/UDM，AUSF/UDM同样更新相应的。

步骤9：群组组长GL若接收到网络侧发送的数据，那么将其转发给所有IoTD，每个IoTD使用会话密钥或组密钥来解密下行数据。

本方法的安全性分析如下。

1. 相互认证和密钥协商

上述方案可以实现群组和AMF之间的相互认证，由于仅在GL和AUSF/UDM处共享，所以AUSF/UDM可以验证认证消息是否来源于GL。另外，由于仅在AUSF/UDM和之间共享，AMF可以从AUSF/UDM安全获得和。所以可以和AMF建立相同会话密钥。另外，AMF和可以协商出相同的组密钥。

1. 身份隐私保护

使用来标记每个设备，另外，AMF也使用来标记每个设备，作为毫无意义的字符串，任何人不能从推导出，所以上述方案可以抵抗隐私攻击。

1. 不可追踪性

在多次执行协议的过程中，与相同相关的信息只有。这意味着敌手可以根据和区分不同的和，在成功认证后，是由派生而来，并且依赖于和更新。所以敌手是不能将和任意不同的认证过程相联系起来。因此可以满足不可追踪性。

1. 抗物理和克隆攻击

方案中每个不需要保存任何秘密值，在每个和AMF之间的通信由于其传输的PUF挑战和响应值而被视为安全的。作为PUF的功能，本报告的协议可以防止物理和克隆攻击。

1. 无效组成员检测

每个需要发送，该值由截取得到，这意味着只有有效的才能计算出正确的。AMF可以计算出各自的，并截取前八位比特值得到，从而当聚合信息是无效值的时候可以使用来检查每个。也就是说，当计算出的和接收到的值不同、并且与接收到的值不同时，AMF可以检测出无效的。

1. 密钥确认

由于派生于相应的会话密钥和组密钥，当接收到的被检查是有效的，那么对应的可以确认AMF已经获得两个密钥。反之亦然。AMF可以确认已经计算出相应的和。所以方案可以实现密钥确认。

1. 信令完整性保护

本报告仅考虑GL和AMF之间的信令安全性。第一条认证请求消息被进行完整性保护，该值仅能被GL生成。认证响应消息被进行完整性保护，最后一条认证请求消息被进行完整性保护。所以该方案可以实现信令完整性保护。

1. 抗重放攻击

当GL发送的认证请求消息被敌手重放后，AUSF/UDM可以检查时间戳是否过期，即使时间戳被修改为有效期内，AUSF/UDM仍然可以验证认证码，从而抵抗重放攻击。当AMF发送的认证响应消息被敌手重放后，由于每次认证过程结束后会被更新，所以可以拒绝该消息。类似的，AMF可以拒绝来自于的认证请求消息。

1. 抗中间人攻击

方案中会话密钥是根据PUF挑战和响应值派生得出，这个响应值是秘密，另外PUF挑战和响应值不会在公开通道上传输，所以中间人敌手不能派生出会话密钥。

1. 抗内部人攻击

同一群组中的群成员有相同的和各自的、，即使群组成员获得相同的，他们不能获得和来计算相应的认证码，所以方案可以防止内部人伪装成或AMF。

1. 抵抗信令风暴

方案通过引入GL使用聚合方法使得大量接入认证请求消息聚合为一条请求消息，不仅使得AMF在同一时间能够同时认证设备群组，而且大大减少了信令数量和带宽成本。

**参考文献**

[1]Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong, A Survey on Security Aspects for 3GPP 5G Networks, IEEE Communications Surveys & Tutorials, 22(1): 170-195, 2020.

[2]3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Cellular system support for ultra­low complexity and low throughput Internet of Things (Rel 13); 3GPP TR 45.820 V13.1.0, Mar. 2015.

[3]3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE (Rel 12); 3GPP TR 36.888 V12.0.0, Jun. 2013.

[4]金峰. NB­IoT纳入5G标准助力产业进入新增长曲线, 通信世界, (20):31, 2020.

[5] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC) (Rel 16); 3GPP TR 23.725 V16.2.0, Jun. 2019.

[6] 中兴通讯, 中国移动研究院. 面向工业互联网的5G TSN实践与展望 [EB/OL]. (2022­03­03)[2024­05­28]. https://www.zte.com.cn/china/about/news/20220303c2.html.

[7] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network. Study on support of reduced capability NR devices (Rel 17); 3GPP TR 38.875 V17.0.0, Mar. 2021.

[8] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects. Study on Ambient power­enabled Internet of Things (Rel 19); 3GPP TR 22.840 V2.0.0, Sep. 2023.

[9] 信金灿, 许森, 张化, 等. 面向时间敏感网络的5G无线网增强技术研究, 电信科学, (005) : 038, 2022.

[10]IoT Ecosystem: NB-IoT and LTE-M Report, Report, GSA, Apr. 2019. [Online]. Available: <https://gsacom.com/paper/iot-ecosystemreport-april19/>

[11]Ericsson Mobility Report, Report, Ericsson, Nov. 2020. [Online]. Available: <https://www.ericsson.com/en/mobility-report/reports>

[12]3rd Generation Partnership Project; Service Requirements for Machine-Type Communications (MTC); 3GPP TS 22.368 V13.1.0, Dec. 2014.

[13]3rd Generation Partnership Project; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2; 3GPP TS 36.300 V14.4.0, Sept. 2017.

[14]3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Rel 15); 3GPP TS 33.501 V1.0.0 Mar. 2018.

[15] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) (Rel 17); 3GPP TS 33.163 V17.0.0 Dec. 2021.

[16]Xiongpeng Ren, Jin Cao, Maode Ma, Hui Li and Yinghui Zhang, A Novel PUF-Based Group Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks, IEEE Internet of Things Journal, 9(5): 3642-3656, 2022.

[17]李晖, 曹进, 张跃宇, 赖成喆, 机器类型通信中基于共享群密钥的认证方法, 申请号: 201110057396.X, 公开号: CN102137397A, 授权号: CN102137397B.

[18]李晖, 赖成喆, 张跃宇, 曹进, 基于群组的机器类型通信设备的认证方法, 申请号: 201110057736.9, 公开号: CN102088668A, 授权号: CN102088668B.

[19]Jin Cao, Maode Ma, Hui Li, GBAAM: Group-based access authentication for MTC in LTE networks, Security Communications Network, 8(17): 3282-3299, 2015.

[20] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment (Rel 9), 3GPP TR 33.812 V9.2.0, Jun. 2010.

[21]曹进, 李晖, 赖成喆, 刘雪峰, 王子龙, 马东旭, 一种机器类型通信中匿名群组认证方法, 申请号: 201510057961.0, 已授权, 授权日期: 2018.06.21

[22]Jin Cao, Hui Li, Maode Ma, Fenghua Li, UPPGHA: Uniform Privacy Preservation Group Handover Authentication Mechanism for mMTC in LTE-A Networks, Security and Communication Networks, 2018. <https://doi.org/10.1155/2018/6854612>.

[23]Jin Cao, Maode Ma, Hui Li, Yulong Fu, Xuefeng Liu, EGHR: Efficient Group-Based Handover Authentication Protocols for mMTC in 5G Wireless Networks. Journal of Network and Computer Applications, 102: 1-16, 2018.

[24]Shin-Jia Hwang and Yun-Hua Lee, Repairing ElGamal-like Multi-Signature Schemes Using Self-Certified Public Keys, Applied Mathematics and Computation, 156(1): 73–83, 2004.

[25]Jonathan Katz and Andrew Y. Lindell, Aggregate Message Authentication Codes, Cryptopgraphers Track at the Rsa Conference on Topics in Cryptology, 2008, pp. 155–169.

[26]3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security (NDS); IP network layer security (Rel 13), 3GPP TS 33.210 V13.0.0, Dec. 2015.

[27]Chengzhe Lai, Hui Li, Rongxing Lu, Jiang Rong, Xuemin Shen, LGTH: A Lightweight Group Authentication Protocol for Machine-Type Communication in LTE Networks, Proceedings of IEEE Global Communications Conference (GLOBECOM'13), 2013, pp. 832–837.

[28]Jin Cao, Pu Yu, Maode Ma, and Weifeng Gao, Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network, IEEE Internet Things Journal, 6(2): 1561-1575, 2019.

[29]Jin Cao, Pu Yu, Xinyin Xiang, Maode Ma, Hui Li, Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System, IEEE Internet Things Journal, 6(6): 9794-9805, 2019.

[30]王梦殊,祁正华, 无双线性对的无证书聚合签密方案, 计算机技术与发展, 27(08): 115-120, 2017.

[31]Bing Li, Zhijie Wang, Dijiang Huang, An Efficient and Anonymous Attribute-Based Group Setup Scheme, Proceedings of IEEE GLOBECOM 2013, 2013, pp. 861-866.

[32]Mugen Peng, Shi Yan, Kecheng Zhang, Chonggang Wang, Fog Computing based Radio Access Networks: Issues and Challenges, IEEE Network, 30(4): 46-53, 2016.

缩略语

|  |  |  |
| --- | --- | --- |
| **缩写名词** | **英文全称** | **中文译名** |
| LPWAN | Low-Power Wide-Area Network | 低功耗广域网 |
| 3GPP | 3rd Generation Partnership Project | 第三代伙伴关系计划 |
| 4G | Fourth generation | 第4代移动通信网络 |
| 5G | Fifth generation | 第5代移动通信网络 |
| 5G AKA | Fifth Generation Authentication and Key Agreement | 第5代认证密钥协商 |
| AAA | Authentication, Authorization and Accounting server | 认证、鉴权、计费服务器 |
| AK | Anonymity Key | 匿名密钥 |
| AIoT | Ambient power-enabled Internet of Things | 无源物联网 |
| AMAC | Aggregated Message Authentication Code | 聚合消息验证码 |
| AMF（不包含10.4.1章节中的AMF） | Authentication Management Function | 认证管理网元 |
| AMF（仅限10.4.1章节中的AMF） | Authentication Management Field | 认证管理域 |
| AP | Access Point | 接入点 |
| AuC | Authentication Centre | 认证中心 |
| AUSF | Authentication Server Function | 认证服务网元 |
| AUTN | Authentication Token | 认证令牌 |
| AV | Authentication Vector | 认证向量 |
| BEST | Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices | 适用于极低吞吐量机器类型通信设备的节能安全服务 |
| BGV | Brakerski– Gentry–Vaikuntanathan | BGV同态加密算法 |
| CIoT | Cellular Internet of Things | 蜂窝物联网 |
| CK | Cipher Key | 机密性密钥 |
| CP | Control plane | 控制面 |
| CRP | Challenge Response Pair | 挑战响应对 |
| DPF | Download and Precongifure Function | MCIM下载和配置实体 |
| DRB | Data Radio Bearer | 数据无线承载 |
| EAP-AKA' | Extensible Authentication Protocol-Authentication and Key Agreement' | 增强型扩展认证协议-认证密钥协商 |
| EAP-AKA | Extensible Authentication Protocol-Authentication and Key Agreement | 扩展认证协议-认证密钥协商 |
| EAS | Enterprise Application Server | 企业应用服务器 |
| EC-GSM | Extended Coverage-Global System for Mobile Communications | 扩展覆盖全球移动通信 |
| eMTC | enhanced Massive Type Communication | 增强型机器类型通讯技术 |
| eNB | evolved Node B | 演进型基站 |
| EPC | Evolved Packet Core | 演进分组核心网 |
| EPS AKA | Evolved Packet System Authentication and Key Agreement | 演进分组系统-认证密钥协商 |
| E-UTRAN | Evolved UMTS Terrestrial Radio Access Network | 演进的UMTS陆地无线接入网 |
| f1 | Message authentication function used to compute MAC | 计算MAC的消息验证函数 |
| f2 | Message authentication function used to compute RES and XRES | 计算RES和XRES的消息验证函数 |
| f3 | Key generating function used to compute CK | 计算CK的密钥生成函数 |
| f4 | Key generating function used to compute IK | 计算IK的密钥生成函数 |
| f5 | Key generating function used to compute AK in normal procedures | 计算AK的密钥生成函数 |
| GHID | Group Home Identity | 群组归属标识 |
| GHK | Group Home Key | 群组归属密钥 |
| GIAA | Group-based Initial Access Authentication | 群组初始接入认证 |
| GID | Group Identity | 群组身份信息 |
| GK | Group Key | 组密钥 |
| GL | Group Leader | 组长 |
| GLID | Group Local Identity | 群组本地标识 |
| GLK | Group Local Key | 群组本地密钥 |
| gNB | the next Generation Node B | 下一代基站 |
| GPK | Group Public Key | 群组临时公钥 |
| GPRS | General packet radio service | 通用分组无线服务技术 |
| GSM | Global System for Mobile Communications | 全球移动通信系统 |
| GTK | Group Temporary Key | 群组临时密钥 |
| GTID | Group Temporary Identity | 群组临时标识 |
| GUTI | Globally Unique Temporary UE Identity | 全球唯一临时用户设备识别码 |
| HE | Home Environment | 归属网络 |
| HeNB | Home evolved Node B | 归属地的演进型基站 |
| HK | Home Key | 归属密钥 |
| HID | Home Identity | 归属标识 |
| HIU | Hybrid Interconnection Unit | 混合互连单元 |
| HPLMN | Home Public Land Mobile Network | 归属公共陆地移动网络 |
| HSE | HPLMN Security Endpoint | 归属网络安全锚点 |
| HSS | Home Subscriber Server | 归属签约用户服务器 |
| IK | Integrity Key | 完整性密钥 |
| IKE | Internet Key Exchange | 因特网密钥交换 |
| IMEI | International Mobile Equipment Identity | 国际移动设备识别码 |
| IMSI | International Mobile Subscriber Identity | 国际移动用户识别码 |
| IoT | Internet of Things | 物联网 |
| IP | Internet protocol | 因特网协议 |
| KGC | Key Generation Centre | 密钥生成中心 |
| L2WGFHA | LTE-A to WLAN Group-based Fast Handover Authentication | LTE-A向WLAN的群组快速切换认证 |
| LID | Local Identity | 本地标识 |
| LK | Local Key | 本地密钥 |
| LoRa | Long Range Radio | 远距离无线通信技术 |
| LTE | Long Term Evolution | 长期演进 |
| LTE-A | Long Term Evolution-Advanced | 长期演进增强型 |
| LTE Cat-m | Long Term Evolution Category-m | 长期演进网络类型-m物联网通讯技术 |
| LTE-M | LTE-Machine to Machine | 长期演进网络机器类型通讯技术 |
| LWE | Learning with Errors | 容错学习 |
| M2M | Machine to Machine | 机器对机器通信 |
| MCIM | Machine Communication Identity Module | 机器通信识别模块 |
| MD | Machine Type Ccommunication Device | 机器类型通讯设备 |
| ME | Machine Equipment | 机器设备 |
| MME | Mobility Management Entity | 移动管理实体 |
| mMTC | Massive MTC | 海量机器类型通讯 |
| MTC | Machine Type Communication | 机器类型通信 |
| MTCD | Massive Type Communication Device | 机器类型通讯设备 |
| MTC Server | Massive Type Communication Server | 机器类型通信服务器 |
| NAS | Not-Access Stratum | 非接入层 |
| NB-IoT | Narrow Band Internet of Things | 窄带物联网通讯技术 |
| NR | New radio | 新无线 |
| PCID | Provisional Connection Identity | 临时连接身份 |
| PDU | Protocol Data Unit | 协议数据单元 |
| PfC | Platform Certificate | 平台证书 |
| QoS | Quality of service | 服务质量 |
| RedCap | Reduced Capability | 裁剪能力 |
| RN | Relay Node | 中继节点 |
| RO | Registration Operator | 注册操作者 |
| RRC | Radio Resource Control | 无线资源控制层 |
| SCEF | Service Capability Exposure Function | 服务能力暴露网元 |
| SeNB | Serving evolved Node B | 服务地的演进型基站或者源基站 |
| SGSN | Serving GPRS Support Node | GPRS服务支持节点 |
| SMF | Session Management Function | 会话管理网元 |
| SMME | Serving MME | 服务地的MME或源MME |
| SN | Serving Network | 服务网络 |
| SQN | Sequence Number | 序列号 |
| TeNB | Target evolved Node B | 目标基站 |
| TGID | Temporary Group Identity | 临时群组标识 |
| TID | Temporary Identity | 临时身份 |
| TMME | Target MME | 目标MME |
| TMSI | Temporary Mobile Subscriber Identity | 临时移动用户识别码 |
| TRE | Trusted Environment | 可信环境 |
| TS | Timestamp | 时间戳 |
| TSN | Time-Sensitive Networking | 时间敏感网络 |
| UDM | Unified Data Management | 统一数据管理网元 |
| UE | User Equipment | 用户设备 |
| UICC | Universal Integrated Circuit Card | 通用集成电路卡 |
| UMTS | Universal Mobile Telecommunications System | 通用移动通信系统 |
| UP | User plane | 用户面 |
| UPF | User Plane Function | 用户面网元 |
| URLLC | Ultra Reliable and Low Latency Communications | 高可靠低延迟通信 |
| USIM | Universal Subscriber Identity Module | 通用用户身份模块 |
| VID | alias of ID | 伪身份标识 |
| VoLTE | Voice over Long-Term Evolution | 长期演进语音承载 |
| WGLR | WLAN Group-based Local Re-authentication phase | WLAN中群组本地重认证 |
| WLAN | Wireless Local Area Network | 无线本地区域网络 |
| XRES | EXpected user RESponse | 认证挑战 |