**第11章 5G D2D安全技术**

D2D（Device-to-Device）通信技术是一种支持两个对等设备间直接通信的技术模式。该模式下的设备都能发送和接收信号，并具有转发消息的功能。然而，D2D设备之间通过不安全的空口信道进行连接，通信链路面临窃听、假冒、中间人攻击等安全风险，因此需设计针对性安全机制保障D2D通信链路的安全性。

## 11.1 D2D安全标准进展

根据当前第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）标准，TS33.501[1]制定了5G身份验证和密钥协商协议（5G Authentication and Key Agreement，5G-AKA）以及可扩展身份认证与密钥协商协议（Extensible Authentication Protocol - Authentication and Key Agreemen，EAP-AKA’），主要用于建立用户设备与核心网络之间的安全通信，但无法直接适用于D2D设备间通信。针对邻近服务（ProSe）即D2D，3GPP标准委员会提出了TS33.303[2]，TR33.847[3]等一系列安全标准及技术报告。TS33.303规范了设备发现、单播/组播通信、公共安全及中继通信等场景的安全架构。该标准要求每个用户设备（User Equipment，UE）先通过5G-AKA和EAP-AKA’完成与本地网络（Home Network，HN）的初始相互认证和密钥协商，随后两个近端UE可直接执行相互认证和密钥协商以建立一对一安全链路。但是，该机制存在多重技术局限：未集成隐私保护、前向和后向安全等关键安全属性；未覆盖异构网络环境（3GPP 5G异构网络中多场景及接入技术）、漫游或非漫游等场景的D2D直接通信安全；两UE设备空口链路缺乏完整的认证和密钥协商安全机制；且性能上需要两个邻近UE之间的多轮信令交互，信令开销较高。此外，该标准本质上仍基于4G网络架构设计。针对5G D2D服务下中继通信场景， TR33.847从认证授权、隐私、密钥管理几方面设计了设备到网络中继和设备到设备中继的安全协议，但未涉及网络控制下的逐跳D2D中继数据传输。在此基础上，3GPP标准委员会正开展5G D2D安全标准TS33.503[4]的研究工作，以完善相关技术规范。

综上，当前3GPP标准针对D2D通信的安全研究仍处于技术演进的初期阶段，在D2D复杂应用场景下还存在一定技术缺口。

## 11.2 D2D安全标准机制

具体地，当前D2D通信安全标准机制包括：4G网络下D2D架构标准TS23.303，安全标准TS33.303；5G网络下D2D架构标准TS23.304，安全标准草稿TS33.503。此外，3GPP还提出了一系列技术报告如TR33.833、TR33.843、TR33.847等，以辅助技术标准的研究。由于5G D2D安全标准尚在完善中，本书主要介绍4G D2D安全标准，并对5G D2D架构与安全标准进行简要概括。

1. 4G ProSe架构及安全机制[2]

****

图11.1 4G ProSe架构

TS33.303标准聚焦于规范两设备之间的PC5接口、设备与网络之间的PC3/PC2接口安全及数据配置传输，并针对ProSe网络实体间通信提出以下安全需求：（1）ProSe网络实体需具备数据通信来源的认证能力；（2）ProSe网络实体间的数据传输应受到完整性保护；（3）ProSe网络实体间的数据传输应受到机密性保护；（4）ProSe网络实体间的数据传输需抵御重放攻击。为实现上述安全需求，该标准通过整合身份认证、消息认证码、加密、随机数/时间戳等安全方法构造安全协议及安全机制。具体安全机制包括：使用时间参数抵抗重放攻击、使用MIKEY机制完成新密钥的安全分发、使用GBA机制完成设备和ProSe功能实体的共享密钥协商。

该标准针对ProSe服务场景进行了安全协议设计，包括设备发现、一对多通信、一对一通信、公共安全、中继通信等。针对不同场景，密钥体系如表1.11：

表11.1 密钥分类

|  |  |  |
| --- | --- | --- |
| **使用场景** | **密钥** | **含义** |
| 开放发现  受限发现 | Discovery Key | 发现密钥，用于开放发现中消息完整性保护 |
| DUIK | 完整性保护密钥，用于受限发现中消息完整性保护 |
| DUCK | 机密性保护密钥，用于受限发现中的消息机密性保护 |
| DUSK | 加扰密钥，用于受限发现中的消息加扰保护 |
| 公共发现 | PSDK | 公共安全发现密钥 |
| 中继通信 | PRUK | 中继用户密钥 |
| 一对多通信 | PGK | ProSe组密钥 |
| PTK | 业务密钥 |
| 一对一通信 | 长期密钥 | 预置密钥（对称密钥/公私钥对） |
| KD | 用于刷新KD-sess |
| KD-sess | 会话密钥 |
| 通用 | PEK | ProSe加密密钥 |
| PIK | 完整性保护密钥 |

设备发现过程主要由以下实体参与：用户设备UE、设备归属ProSe功能实体、设备漫游ProSe功能实体、ProSe应用服务器。D2D设备进行相互发现前需首先通过PC3接口向其归属ProSe功能实体发起发现请求，在得到该设备针对特定服务的授权后，再在PC5接口发送设备发现消息。接收到发现消息的设备可直接对消息进行检查，或联系其归属ProSe功能实体对消息检查，检查成功后完成设备发现过程。设备发现分为开放发现和受限发现两种类型。开放发现指ProSe功能实体针对某设备特定服务授权构造的发现信息可被所有监听设备接收。受限发现则指某设备特定服务的发现消息只能被特定设备发现和接收，进一步细分为Model A和Model B两种模式。Model A指：向其他设备通知我在这里。Model B指：询问其他设备谁在那边。针对这两种模式，TS33.303标准规范了不同的设备发现流程。一般来说，开放发现只对发现消息进行完整性保护和抗重放检查，受限发现则可以根据安全参数，有选择的对发现消息进行完整性保护、部分加密、整体加扰、抗重放攻击等操作。

一对多通信、群组通信在当前海量设备场景下具有良好应用场景。根据该标准，设备需首先通过ProSe功能实体实现群组服务授权并获取组ID，随后由ProSe密钥管理功能实体（Proximity Service Key Management Function，PKMF）为该设备安全分发群组密钥PGK，并基于PGK及其衍生密钥实现群组内一对多安全通信。具体流程如下：首先，设备向PKMF发送包含“组ID和安全能力”的密钥请求，由PKMF检查后使用MIKEY机制下发“组成员ID，PMK ID，PMK及其他信息”或“PGK，PGK ID和到期时间”。其中PMK与PMK ID用于实现MIKEY机制。随后，发送方设备使用PGK衍生PTK和PEK以确保流量传输安全。

一对一通信作为通用通信方式，标准规定通信双方需预置长期密钥，随后执行直接通信请求、直接认证与密钥建立、安全模式建立请求、安全模式完成四种消息，以建立安全上下文。当新安全上下文建立后，系统根据长期密钥及协商参数计算出新的KD-sess密钥、机密性和完整性保护密钥，随后可支持用户平面数据和被新安全上下文保护的控制信令的安全发送。

在公共安全如自然灾害导致的无网络应急通信等场景中，包括公共安全发现和一对多通信两种子场景，需要在公共通信开始前预先完成针对性安全参数配置，以保证后续直接通信安全。具体的安全参数配置在MIKEY机制保护下，由PKMF向用户设备安全分发“密钥类型ID、PSDK/PGK、PSDK ID/PGK ID”并衍生出子密钥，从而保护具体场景通信安全。

在中继通信场景中，涉及两种设备类型：远端设备和中继设备。其中，远端设备无法连接核心网，但可以连接其归属ProSe功能实体，同时PKMF也可为其提供服务。中继设备则均可连接。因此远端设备到中继设备之间发现安全和通信安全需要得到保障。其中发现安全复用受限发现安全机制即可。对于通信安全，中继设备所属PKMF需要和远端用户设备之间建立TLS隧道，安全传输PRUK。PRUK将作为根密钥，基于一对一安全通信协议，建立远端设备和中继设备之间的安全通信。

2. 5G ProSe架构及安全机制[4]



图11.2 5G ProSe控制面架构

图11.3 5G ProSe用户面架构

5G ProSe架构中引入的5G直接发现名称管理功能实体（5G Direct Discovery Name Management Function，5G DDNMF）替代了4G ProSe功能实体中的名称管理功能。该实体主要用于分配和处理ProSe直接发现中使用的ProSe应用程序ID和ProSe应用程序代码的映射，并通过与策略控制功能（Policy Control Function，PCF）交互以授权ProSe发现服务。由于5G ProSe架构的改变，其安全需求相比4G而言也有不同之处，如需要考虑设备与5G DDNMF之间的安全数据传输，也更聚焦于设备到网络中继通信的安全需求。同时相比4G而言，引入了新的安全方法如认证密钥管理架构（Authentication and Key Management for Application，AKMA）来加强其安全功能。

## 11.3 D2D安全需求和潜在威胁

针对D2D通信安全标准和方案的研究表明，当前安全机制设计应满足以下安全需求并应对潜在威胁[5]：

1. 安全有效的设备发现机制

设备发现作为D2D通信的第一步，对于建立安全通信起着至关重要的作用。然而目前尚无明确解决方案或通用机制用于设备发现。当前3GPP标准已经提出了设备开放发现和受限发现下的安全需求，如抵抗邻近设备开放发现的重放攻击、伪造攻击、轨迹跟踪、支持空口消息的完整性保护、机密性保护和身份保护。

（2）数据传输过程中的机密性和完整性保护

安全的数据传输需要在两个D2D设备之间进行相互认证并协商出有效的会话密钥，随后进一步进行密钥衍生管理以保护数据传输安全。此外，D2D中继通信是D2D通信中不可避免的一种模式，它可以提高蜂窝网络的覆盖率和质量，并在蜂窝网络边缘提供服务。然而，中继节点可能会给数据的保密性、完整性和安全性带来一些风险。

（3）D2D中的连续无缝安全数据传输

未来5G网络作为超密集异构网络（HetNet），小区半径较4G网络显著缩小。引入D2D通信可以有效地卸载基站承载的网络流量并实现信号的无缝覆盖。在5G异构网络中，漫游或非漫游D2D需要在多种复杂的应用场景下进行直连安全通信建立，如不同归属网络下的漫游设备通过不同接入技术接入相同的访问网络并相互建立D2D通信。不同应用场景下的安全机制适配增加了系统的复杂性，同时小区半径导致的频繁切换也要求更加简洁高效的D2D安全机制。

（4）ProSe应用服务器支撑的安全组通信和细粒度访问

随着移动智能终端数量的快速增加，大量设备可以构成设备组通信，以减少通信成本和计算成本。D2D组通信可以用于高效内容共享，然而安全建立群组和批量处理组消息等问题仍需要进一步研究。根据3GPP标准，针对群组通信需要考虑以下关键问题如安全添加及删除组成员、安全传输组成员标识、组密钥更新、以及设备属于多个组的成员同时与多个组通信等特殊应用场景的安全问题。

（5）不同D2D通信场景中的隐私保护

D2D技术可以广泛应用于多种应用场景，如基于位置的服务、内容共享服务和本地广告业务等，然而复杂通信场景会引入更多的安全需求，如隐私保护。在D2D设备发现、资源分配以及网络路由中，设备都需要广播其位置信息及身份，容易造成隐私泄露。隐私保护由于需要隐藏部分信息，可能阻碍身份认证等安全机制的执行，当前的解决方案和标准大多没有考虑该问题。

## 11.4 D2D安全认证与密钥传输机制

本节将介绍针对D2D通信的安全认证与密钥传输机制。首先，提出了一种安全高效的一对多D2D相互认证与密钥协商方法，该方法通过融合多种技术，可实现隐私保护的设备发现、一对多通信场景下的批量验证以及会话密钥的确认。其次，针对D2D中继传输，通过引入一种具有轨迹跟踪的安全数据传输机制，结合核心网辅助，利用对称加密、HMAC、切比雪夫多项式等技术，可以保障数据传输过程中的机密性、完整性、隐私保护以及前向/后向安全性，并减少计算和通信开销。这些机制能够为D2D通信在不同场景下的安全需求提供有效解决方案。

### 11.4.1 D2D设备发现、相互认证与密钥传输协议[6]

一对多通信不同于群组通信，它在每两个设备之间都建立独立的安全信道，这使其在D2D公共安全通信场景中具有广泛的应用价值，然而目前的D2D安全解决方案却很少考虑该场景。本节引入一种安全高效的一对多D2D相互认证与密钥协商方法，该方法能够与5G HetNet场景兼容，作为5G HetNet场景中D2D安全通信的统一解决方案，可以实现一对一安全通信、一对多安全通信、异构接入、设备发现、相互认证、密钥协商和批量验证等功能。

该方案首先构造了一种高效的无证书批量签名（Certificateless Batch Signature**，**CLBS）方案，随后基于身份的前缀加密、CLBS、基于椭圆曲线的Diffie-Hellman密钥交换（Elliptic Curve Diffie–Hellman**，**ECDH）和中国剩余定理（Chinese Remainder Theorem**，**CRT）机制融合，实现相互认证与密钥协商。其中，基于身份的前缀加密技术实现了隐私保护的设备发现；CLBS有效解决了一对多通信场景中结构相同的多个消息签名验证问题，并降低了计算开销；CRT用于一对多D2D通信会话密钥的确认，简化了认证过程，降低了信令开销。在所提出的方案中，归属网络（HN）主要负责在初始接入认证过程中为每个UE生成前缀加密私钥，当UE使用前缀加密私钥广播带有密文的消息来请求邻近服务时，每个接收到该消息的UE都会基于前缀加密机制检查其是否满足访问策略，然后与该广播UE进行两次握手实现在无需其他第三方的参与下完成相互认证和密钥协议。

1.安全假设

假设已经订阅了相关的，并且它们注册到的是诚实的。也是诚实的，主要负责为生成相关密钥。同时假设D2D 之间以及和之间的无线通信信道是不安全的。在我们的攻击模型中，对手可以控制和破坏D2D 之间以及和之间的任何无线传输。为了明确攻击者的能力，假设威胁方是Dolev-Yao模型下的攻击者，可以完全控制网络，并且可以在协议执行的任何部分采取多种形式的攻击。攻击者可以通过通信信道截获消息、重放旧消息、分析和修改消息以及模拟其他代理发送新消息等。

2.协议设计

表11.2 D2D设备发现、相互认证与密钥协商协议参数含义对照表

|  |  |
| --- | --- |
| 参数 | 含义 |
|  | 一个加群，其阶为，是加群的生成元 |
|  | HN/KGC的主密钥和公钥 |
|  |  |
|  | 的批量签名算法公钥/私钥 |
| ， | 由设备提前存储的字符串，用于标识消息类型并抵抗信令冲突 |
|  | 基于身份的前缀加密运算 |
|  | HN，VN和UE的身份标识 |
|  | 基于身份的签名值 /批量签名值 |
|  | 基于身份的签名算法 |
|  | VN选取的一系列可信VID |
|  | 的基于身份前缀的公钥/私钥 |
|  | 的公钥和私钥，包含,,, |

其中，是系统中预先存储的128位字符串，用于将消息类型标识为广播消息、会话建立请求消息和会话建立响应消息。标识的使用可以帮助区分和处理信息。是系统中分别用于广播消息和会话建立消息的随机会话标识符，可用于区分不同会话。

（1）系统参数生成

由HN/KGC选择由生成的加法群，阶为，然后随机选择作为主密钥，并计算公钥。此外，还选择了四个单向散列函数，,,。公开系统参数。

（2）设备的初始接入认证

在此阶段，UE通过执行5G-AKA或EAP-AKA’协议实现接入认证。其标准流程如下：在完成接入认证后，VN向相应的UE发送可信VN向量组，HN通过VN向UE发送基于身份的前缀加密私钥，这些消息都被VN使用加密发送。具体流程如下图11.4所示：

图11.4 D2D设备发现、相互认证与密钥协商协议初始接入认证流程

当任意D2D通信设备漫游至新的访问网络时，需向所属访问网络发送接入认证请求，执行5G-AKA/EAP-AKA’认证。

设备首先选取秘密值，随后计算并发送接入认证请求，该请求中包括：设备身份信息、所属归属网络身份信息及公共参数。收到该请求的VN首先检查是否有效，若有效，VN将自身身份信息加入接入认证请求中，发送给HN。HN收到接入认证请求后，首先检查和的合法性，然后为生成认证向量AVs和基于身份前缀加密的加密私钥，随后随机选取秘密值，计算。其中，是公开值，是批验证公钥。随后将计算出的AVs和身份信息一起使用访问网络VN的公钥加密发送给VN。VN利用从HN获得的AVs执行5G-AKA/EAP-AKA’认证过程。UE设备执行5G-AKA/EAP-AKA’认证过程完成后，协商出会话密钥。VN将及该VN可信VN向量组V使用会话密钥加密发送至UE，完成初始化认证及系统参数初始化工作。UE设备接收到分发的参数后，首先使用共享会话密钥解密消息，随后验证公式：

，若验证成功，则接受分发下的参数，进行下一步隐私保护的设备发现与身份认证流程。

3.隐私保护的设备发现与身份认证

在该阶段，两个相邻的可以通过基于身份的前缀加密机制发现对方，随后在一对多D2D通信场景中，当大量UE完成对广播的认证后，每个尝试与广播建立独立的安全连接。此时，对于，逐个验证将带来巨大的计算开销。为解决该问题，方案引入批量签名方案以实现轻量级一对多相互认证，并利用CRT实现广播与其他UE之间的低成本会话密钥确认。该方案也适用于一对一通信场景。如图11.5所示，它的工作原理如下。

我们假设的标识由“Liming/device type/resource name/…”组成，将此字符串用作加密的公钥。当收到密文时，当且仅当其标识由“Liming/device type/resource name/XXX”组成时，它才能使用自己的私钥正确解密密文。具体过程如图所示：

图11.5一对多相互认证与密钥协商流程

当设备试图与其他设备通信时，首先选择秘密随机数与广播id号，计算。随后对自身身份信息、所属访问网络、当前时间戳TS及选取计算的进行ECDSA签名，签名私钥为，生成签名。接着利用公钥计算基于身份的前缀加密 ，最后广播消息{}给其他设备。

当任意设备监听到标志为TAG1的广播消息后，使用基于身份前缀的解密机制，对广播消息进行解密，获取相关信息，具体处理如下：检查自身身份是否符合密文的接入策略，若符合，则可以通过自身私钥成功解密。随后进行多重检查：检查获取到的是否属于所归属的的可信向量组；检查获取的时间戳TS是否有效；计算并检查是否比较成功。若检查均成功则表示对认证成功，随后构造密钥消息。首先，随机选取，和大素数。其次，计算，。最后，向发送{}。

当检查收到标志为TAG2的消息条数为1时，执行单一验证过程。首先，计算，解密，获取身份信息其次，检查解密出的是否是自己身份信息是否属于的可信向量组；。随后，计算 。验证是否成功，若成功，表示对认证成功，并协商出会话密钥，构造消息，广播{ }。

当收到标志为TAG3的信息时，执行密钥确认过程。首先检查bid、sid，确认Z属于当前会话。随后检查是否正确，若正确，则生效。

4.协议分析

本方案通过使用基于身份的前缀加密机制对广播消息进行加密处理，实现设备间隐私保护的设备发现。基于数字签名技术保证两个邻近UE之间的相互认证，确认双方身份的正确性与合法性。基于ECDH密钥协商协议计算会话密钥，保证无线通信信道上数据传输的安全性。在每个会话中利用基于身份的前缀加密技术，攻击者无法通过截取两个邻近设备之间的公共消息来获得他们的身份。由于方案邻近设备之间交换的每条消息中都使用了数字签名或消息认证码，保证了消息完整性。该方案可以抵抗多种协议攻击。针对被动攻击，由于所有敏感信息在整个会话中都是由IBE公钥或会话密钥加密的，因此该方案能够抵抗信息泄漏。针对主动攻击，方案可抵抗中间人（MitM）攻击、模仿攻击、私钥泄露攻击、重放攻击、消息丢弃攻击等，并实现完美前向/后向保密（PFS/PBS）安全。

### 11.4.2 D2D 中继传输安全机制[7]

D2D数据传输可以在具有许可/非许可频谱的基站控制下进行，以协助车辆通信、移动健康（M-Health）系统、建设智能家居以及智慧城市等通信场景。从场景需求和5G性能需求的角度看，D2D数据传输将成为5G网络的重要组成部分。D2D数据传输一般通过UE到UE中继通信来完成，然而移动中继节点在传输过程中会消耗大量能量资源，因此若没有合理的回报，中继节点将拒绝合作。而当前的D2D安全解决方案很少考虑数据传输场景，并且大多数方案不适合UE到UE中继数据传输。此外，当前的数据传输解决方案主要考虑M-Health系统、VANETS以及IoT系统等，并不适合于通用移动D2D数据传输。为解决上述问题，本节引入了一种具有轨迹跟踪的安全数据传输机制，该机制可以记录数据经过的中继节点，同时避免篡改，便于核心网或运营商进行合理的计费和资源分配。

具体地，首先利用切比雪夫多项式特征，构造了一种轻量级轨迹跟踪方法，并在核心网的帮助下，利用对称加密、HMAC、质询和响应、Chebyshev多项式的优势，提出了一种具体的网络辅助数据传输方案。所该方案可以实现源设备与目标设备之间的相互认证，整个传输过程可以确保数据机密性、完整性、轨迹跟踪、隐私保护、完善的前向/后向安全性（PFS/PBS）、不可链接性和上下文隐私性等安全属性，同时减少计算开销、通信开销和存储开销。所提出的方案可以应用于所有网络覆盖的D2D中继数据传输场景，保障5G网络环境下海量设备直连通信数据安全。

1.安全假设

本方案假设核心网络和接入网（RAN）中的所有网络功能都是诚实的，包括AMF和gNB。数据传输的源设备和目标设备共享会话密钥。系统中的敌手可以完全控制无线信道。中继节点可能意图窃取会话信息、隐私信息、数据内容，并在传输过程中修改路径信息，以影响AMF对信誉和资源分配的判断。

2.协议设计

本节提出的方案通过核心网络（CN）在源设备和目标设备之间执行相互身份验证，由CN负责会话配置和传输确认，所有移动节点通过侦听和广播消息协作完成从源设备到目标设备的传输。整个过程可以分为三个阶段，分别是接入认证与会话配置阶段、轻量级可溯源安全数据传输阶段、会话确认阶段。在接入认证与会话配置阶段，UE和CN之间执行5G-AKA/EAP-AKA’以实现UE的接入认证，并在UE和AMF之间建立安全的通信通道。当需要数据传输时，源设备通过安全通道向AMF发送数据会话请求。AMF根据节点拓扑和信誉表为该会话选择可能的中继节点并配置到所选节点的会话参数，通知目标设备包括会话ID和临时共享机密值。然后，将构造消息通过逐跳广播进行传输。收到消息后，进入确认阶段，由在AMF的帮助下向源设备发起确认， AMF验证传输的跟踪路径，随后源和目标更新其共享密钥。相关参数如表11.3所示。

表11.3 D2D中继传输安全机制参数含义对照表

|  |  |
| --- | --- |
| 参数 | 含义 |
| / | 源设备/目标设备/中继设备 |
|  | 的身份 |
|  | /的主密钥 |
|  | 和之间的共享会话密钥 |
|  | 时间戳 |
|  | 广播id和会话id |
|  | 包含数据传输双方身份信息的参量 |
|  | 会话配置参数 |
|  | 针对数据m的验证码 |
|  | 数据传输的整体消息验证码 |
|  | 数据传输轨迹 |
|  | 用于认证的随机数 |
| / | 用于计数的随机数和计数器 |
|  | 基于哈希的消息验证码 |
|  | 切比雪夫多项式 |
|  | 使用对称密钥进行的加解密运算 |
|  | 密钥更新参量 |

其中是AMF选择的随机数，用来标识不同的数据传输会话为源设备计算的掩码，目标设备可以从中恢复是源设备选择的随机数，它是计数器的初始值，隐藏在中是基于的增量值，用于计算中继节点的数量，防止中继节点恶意删除路径的预定节点信息来欺骗AMF。

方案具体流程如下图所示：

图11.6 D2D辅助通信的统一的轻量级可溯源安全数据传输协议图

（1）系统参数生成

和共享一个对称密钥K，所有设备节点都秘密地选择其主密钥。AMF秘密地选择其主密钥。所有D2D设备选择自身主密钥。

（2）接入认证与会话配置阶段

所有D2D设备和代表核心网的网元AMF执行5G-AKA/EAP-AKA’，协商出D2D设备与AMF之间的会话密钥。随后，他们的后续通信在受保护的安全通道中进行。当有数据传输需求时，在受保护的安全通道中执行以下操作：随机选择，然后向AMF发送传输请求消息，该传输请求包含的身份信息、目标设备的身份信息和随机数。当AMF收到传输请求消息后，首先检查的新鲜性，如果是新鲜的，则AMF为此会话随机选择和，计算。然后AMF通过秘密信道将{}发送给，通知其即将进行数据传输。AMF随后在和之间选择所有可能中继消息的节点，并将{}通过秘密信道传递给这些设备节点和源设备节点。所有中继设备和源设备都需要向AMF返回，由设备接收到的n和其自身选择的主密钥计算生成，用于后续过程的轨迹跟踪功能。此时，设备的接入认证和数据传输会话配置完成，随后设备可以利用配置参数，完成设备间数据传输。

（3）轻量级可溯源安全数据传输阶段

首先利用会话配置阶段获取的参数sid和n，计算，并选择随机数cvalue，递增计数器count = cvalue+1，计算cvalue的掩码。随后获取当前时间戳TS，随机选择，利用持有密钥计算新密钥，并对需要传输的消息m进行加密及完整性保护，构造data：。随后利用会话配置获得参数、n及自身主密钥，计算可溯源的轨迹消息：。将该轨迹消息附到之前的消息后，并为整条消息进行计算HMAC：。最后广播整条消息{}。

任意监听到消息后，检查该消息中的sid是否是曾经配置过的会话ID，如果是则进行下一步，否则将丢弃该条消息。首先，用n检验的正确性，如果通过检验则证明该消息未被篡改，进行下一步，否则向AMF报告错误消息。随后计算可溯源的轨迹信息，并将其附在原消息的轨迹信息之后，更新计数器，更新消息验证码，具体计算如下： 、

。最后广播整条消息{}。

收到广播消息后，检查sid的新鲜度和正确性，判断是否与会话配置阶段的参数匹配，如果匹配则进行下一步，否则丢弃该条消息。首先使用由sid标识的参数n验证，如果验证通过则进行下一步，否则丢弃该消息。其次检查TID，并验证，判断是否与会话配置阶段的参数匹配，如果匹配则进行下一步，否则丢弃该消息。随后利用计数器和计数器掩码判断轨迹信息长度是否匹配，如果匹配则进行下一步，否则丢弃该条消息。具体计算如下： ，其中代表轨迹信息的总长度（bits），640bits是每个设备产生的轨迹信息长度。进一步使用持有的共享密钥验证，如果通过验证则进行下一步，否则将其丢弃。最后进行解密运算，获得、消息m及。检查TS是否满足时间有效期要求，检查是否等于会话配置阶段收到的，如果所有检查均通过，表示对成功进行了身份认证并获得了消息m。最后需要进行密钥更新，操作如下：。检查解密出的是否能使用更新的密钥计算出，如果可以，则确认更新。

（4）会话确认阶段

成功获取消息m并确认更新后，使用更新的计算，随后将{ }通过安全信道发送到AMF。AMF收到消息后，获得轨迹信息R，并将{}通过安全信道转发至。当收到确认消息后，它首先使用自身更新的验证，若验证成功，则说明更新的密钥保持了双方同步，同时由于由和计算得出以及的秘密性，间接说明了的正确性。那么此时对成功进行了身份认证，并且更新的密钥可用。否则，将使用旧密钥通过网络重新进行数据传输。此时，一个成功的数据传输会话完成。

下面对AMF的操作进行进一步描述。接收到轨迹信息R的AMF将执行下述过程，该过程可以完成轨迹信息解析，帮助AMF更好的进行拓扑更新、信誉评估以及为下一次传输中继节点的选择做好准备，具体过程如下：将R拆分为，重复计算公式，直到。AMF将根据会话配置阶段获得的节点及轨迹中的来判断单条轨迹信息的归属。任何步骤的失败将导致AMF无法判断轨迹信息的完整性和真实性，AMF将记录失败步骤所指示的节点，以进行综合判断。

3.协议分析

在该方案中，AMF可以利用挑战响应机制帮助源设备和目标设备之间进行相互认证，可以进行同步安全密钥更新并利用安全密钥及HMAC保证安全数据传输。协议实现了匿名性和不可链接性。在数据传输期间，不会公开源设备身份和目标设备身份。由于使用TID标识一个数据传输会话，而TID是由异或异或n计算得出，n是每次传输所选择的随机数，可以看出，只有源设备和目标设备才能根据自身身份计算得出另一方的身份，该身份不会泄露到其他中继节点或外部设备上。该协议中所有中继设备基于之前的路径信息及其自身主密钥生成，同时由于基于切比雪夫混沌多项式构造的密钥，只有核心网可以解密并查看轨迹信息。由于消息验证码的使用和基于的独特构造，还可以确保轨迹信息的真实性，实现轨迹跟踪。本章所提出的方案在每次会话完成时，通信双方都会更新会话密钥，实现了完美的前向/后向安全性（PFS/PBS）。

## 参考文献：

1. 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security architecture and procedures for 5G system (Rel 16); 3GPP TS 33.501 V16.1.0, Dec. 2019[R].
2. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-based Services (ProSe); Security aspects (Rel 15); 3GPP TS 33.303 V15.0.0, Jun. 2018[R]
3. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects of enhancement for proximity based services in the 5G Systems (5GS); 3GPP TR 33.847 V.17.0.1, Jan. 2022[R]
4. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects of Proximity Services (ProSe) in the 5G System (5GS); 3GPP TR 33.503 V0.2.0, Nov. 2021[R]
5. J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, L. Xiong. A Survey on Security Aspects for 3GPP 5G Networks [J]. IEEE Commun. Surv. Tutorials, 2020, 22(1), 170–195.
6. Y. Sun, J. Cao, M. Ma, Y. Zhang, H. Li, B. Niu. EAP-DDBA: Efficient Anonymity Proximity Device Discovery and Batch Authentication Mechanism for Massive D2D Communication Devices in 3GPP 5G HetNet [J]. IEEE Transactions on Dependable and Secure Computing, 2020, DOI: 10.1109/TDSC.2020.2989784.
7. 曹进，孙韵清，李晖，杨元元，任雄鹏，一种D2D辅助通信的统一轻量级可溯源安全数据传输方法，中国，申请号：2021106169418[P].