5G邻近服务安全关键技术

Key Technologies of 5G ProSe Security

姚　戈，徐　雷，张曼君（中国联通研究院，北京 100048）
Yao Ge，Xu Lei，Zhang Manjun（China Unicom Research Institute，Beijing 100048，China）

摘　要：
随着5G与垂直行业加速融合，5G邻近服务（Proximity Services，ProSe）作为5G网络支持各种应用和服务的关键技术之一，是3GPP当前研究的重点。经过3GPP R17、R18阶段的研究，5G ProSe技术已经逐渐成熟，其安全问题也成为业界关注的重点。对5G ProSe技术和安全标准进行梳理，针对不同阶段的5G ProSe功能和特性，分析对应的安全关键技术，最后指出5G ProSe技术的演进方向和潜在的安全问题。

关键词：
邻近通信；ProSe；5G；安全
doi：10.12045/j.issn.1007-3043.2023.08.019
文章编号：1007-3043（2023）08-0085-08
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
With the accelerated combination of 5G and vertical industries，5G ProSe （Proximity Services），as one of the key technologies for 5G networks to support various applications and services，is the focus of 3GPP current research. After the research of 3GPP R17 and R18，5G ProSe technology has gradually matured，and its security has attracted more and more attention. It reviews 5G ProSe technology and security standards，analyzes security mechanisms regarding 5G ProSe functions and features in different Releases，and finally points out the evolution direction of future 5G ProSe technology and potential security research questions.

Keywords：
Proximity communication；ProSe；5G；Security

引用格式：姚戈，徐雷，张曼君 . 5G邻近服务安全关键技术[J]. 邮电设计技术，2023（8）：85-92.

0 引言

3GPP在R12阶段引入邻近服务（ProSe）[1]，定义了ProSe发现和ProSe通信2个基本过程，在R13阶段新增了UE到网络中继（UE to Network Relay，U2N Relay）特性。3GPP R14阶段主要将邻近服务用于LTE的V2X车联网技术[2]。进入5G时代，ProSe有望成为使能5G网络支持各种应用和服务的关键技术之一。在公共安全方面，维持邻近发现和邻近通信对于UE在蜂窝网络覆盖范围之外时是非常关键的，例如在偏远地区发生灾难时，2个邻近的具有5G ProSe功能的移动终端之间仍然能够建立无线通信，为灾难救援提供保障。在商业领域，ProSe可广泛应用于依赖邻近通信的B2B、B2B2C和B2C服务，包括广告、社交网络、游戏等[3]。3GPP在R17阶段开展5G ProSe关键技术的研究，旨在开发一个通用框架来支持公共安全和商业领域中的5G邻近服务。经过3GPP R17、R18阶段的研究，目前5G ProSe技术已经逐渐成熟，相关的安全研究也随之开展。本文对5G ProSe技术和安全标准进行梳理，根据不同阶段的5G ProSe的功能特性，分析安全机

收稿日期：2023-06-06

制如何消除对应的安全威胁，并指出5G ProSe技术未来的演进方向以及潜在的安全研究问题。

1 R17阶段5G ProSe安全关键技术

3GPP SA2于2021年完成了5G ProSe_Ph1（阶段1）的研究和标准化工作，形成3GPP TS 23.304标准[4]，对5G ProSe的架构和特性进行了如下规范。

a）5G ProSe系统架构参考模型。

b）支持PC5（直连通信接口）直接发现。

c）支持PC5单播、群播和广播通信。

d）支持PC5服务授权和策略/参数配置。

e）支持PC5和Uu（蜂窝网通信接口）之间的直接通信路径选择。

f）支持层3和层2的U2N中继（包括QoS和服务连续性方面）。

基于3GPP TS 23.304定义的5G ProSe架构和特性，3GPP SA3工作组开展5G ProSe_Ph1相关安全问题的研究和标准化工作，发布了3GPP TS 33.503标准[5]。

1.1 5G ProSe直接发现安全

5G ProSe直接发现是指检测和识别出附近其他5G ProSe UE的过程，可分为开放性5G ProSe直接发现和限制性5G ProSe直接发现。

1.1.1 开放性5G ProSe直接发现安全

开放性5G ProSe直接发现安全流程如图1所示，可归纳如下。

①~④：宣告UE向其归属网络的5G DDNMF发送发现请求，以获得允许在其服务网络中宣告消息，并获取ProSe应用代码和发现密钥等参数。

⑤~⑩：宣告UE使用发现密钥计算一个32位的消息完整性检查（MIC），然后向网络中发送宣告消息。监控UE向其归属网络的5G DDNMF发送包含ProSe应用ID的发现请求，以获取相应的发现过滤器。

⑪~⑮：监控UE接收网络中符合发现过滤器的宣告消息，收到后可根据需要发送给归属网络的5G DDNMF，由它与宣告UE归属网络的5G DDNMF交互进行验证，返回验证结果。

在上述过程中，宣告UE和监控UE利用发现密钥计算MIC进行验证，确保了发现消息的完整性。宣告UE和监控UE分别设置ProSe时钟，利用与UTC时间的差值判断消息的时效性或过滤出符合的宣告消息，

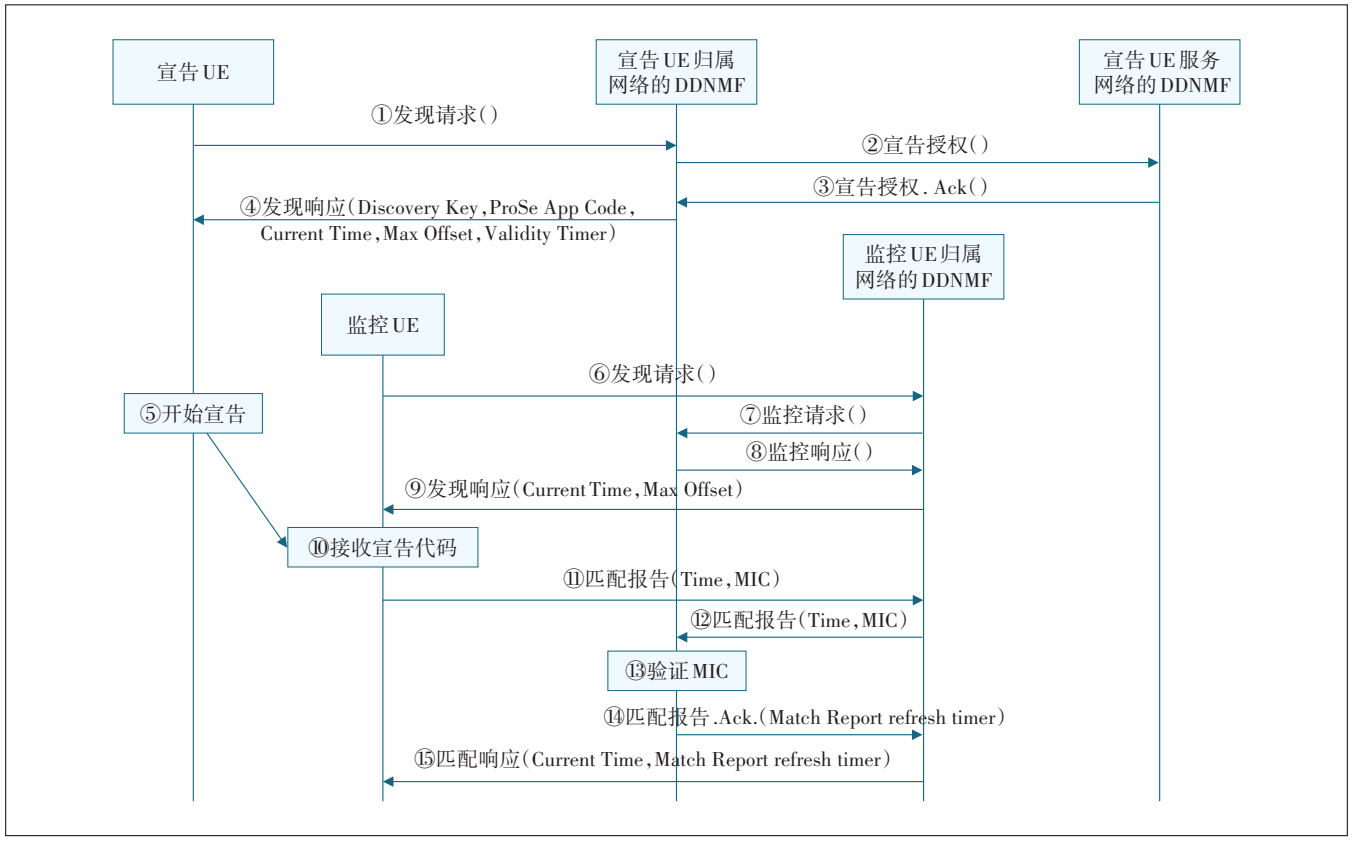

图1　开放性5G ProSe直接发现安全流程

为发现过程提供了抗重放保护。

1.1.2 限制性5G ProSe直接发现安全

1.1.2.1 限制性5G ProSe直接发现模式A的安全流程

限制性5G ProSe直接发现模式A的安全流程如图2所示，可归纳如下。

①~④：宣告UE执行发现请求程序，将限制性ProSe应用用户ID（RPAUID）发给其归属网络的DDNMF来获取ProSe限制代码及相关安全参数，并确定选择的PC5加密算法。在此过程中，DDNMF向ProSe应用服务器查验宣告UE的授权情况。

⑤~⑩：监控UE向DDNMF发送发现请求来获取ProSe限制代码及相关安全参数。由监控UE归属网络的DDNMF根据ProSe应用服务器对监控UE的授权情况，向宣告UE归属网络的DDNMF发送监控请求，后者查询授权情况，返回包含发现过滤器、ProSe限制代码和选择的PC5加密算法的监控响应。

⑪~⑫：宣告UE宣告包含ProSe限制代码的发现消息，监控UE接收网络中符合发现过滤器的宣告消息。

⑬~⑯：监控UE请求其归属网络的5G DDNMF执行MIC检查，DDNMF检查后返回检查通过确认消息。

在上述过程中，随ProSe限制代码发送的相关安全参数可用于保护ProSe限制代码在传输和存储中的机密性。在宣告和接收代码时，监控UE执行MIC检查则确保了发现消息的完整性。另外，宣告UE和监控UE分别设置ProSe时钟，利用与UTC时间的差值判断消息的时效性或过滤出符合的宣告消息，为发现过程提供了抗重放保护。

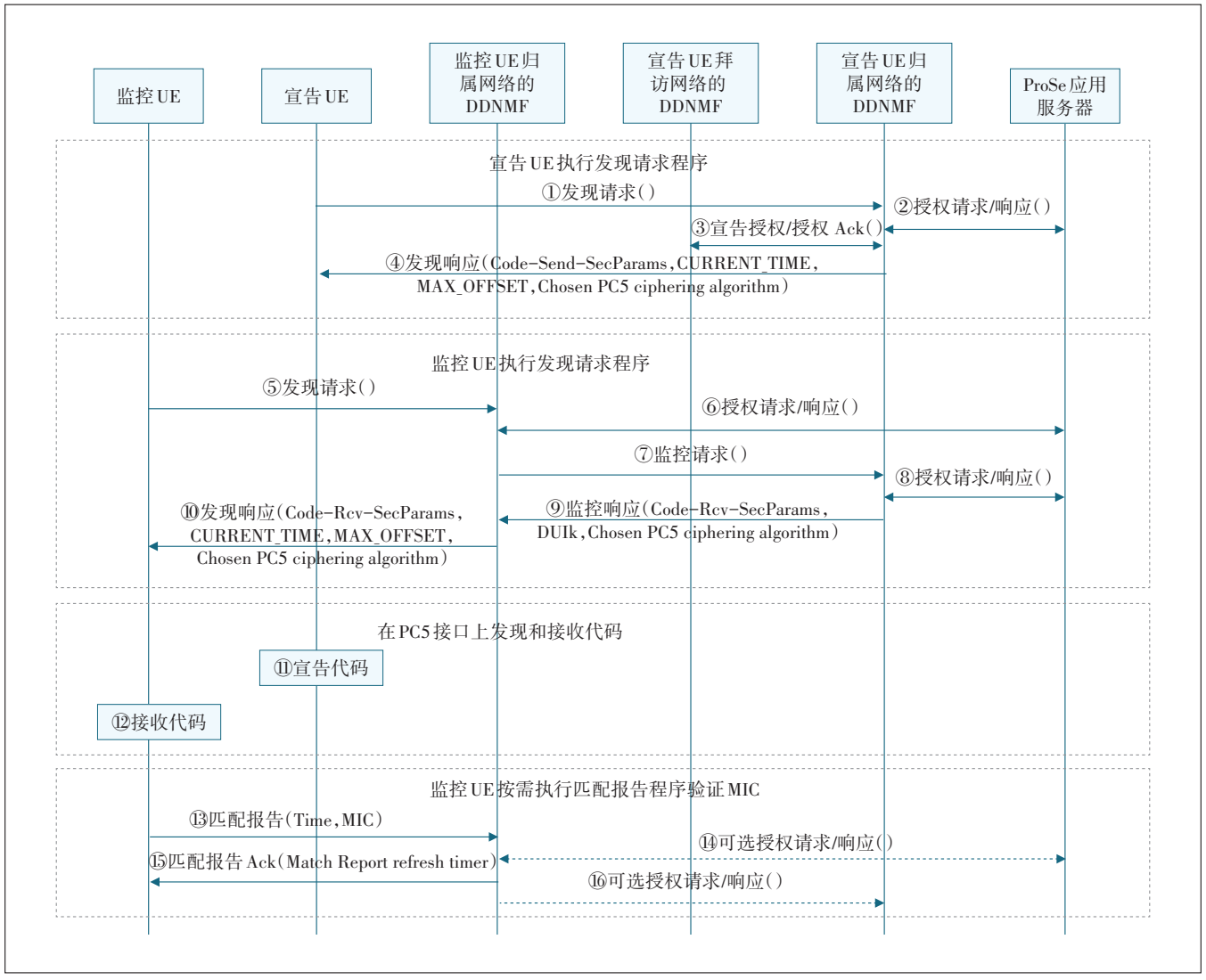

图2　限制性5G ProSe直接发现模式A的安全流程

1.1.2.2 限制性5G ProSe直接发现模式B的安全流程

限制性5G ProSe直接发现模式B的安全流程如图3所示,可归纳如下。

①~④:被发现者UE执行发现请求程序,将RPAUID发给其归属网络的DDNMF来获取ProSe响应代码及相关安全参数。在此过程中,DDNMF向ProSe应用服务器查验被发现者UE的授权情况。

⑤~⑪:发现者UE向其归属网络的DDNMF发送发现请求来获取ProSe查询代码及相关安全参数。由发现者UE的DDNMF根据ProSe应用服务器对发现者UE的授权情况,向被发现者UE的DDNMF发送发现请求,被发现者UE的DDNMF通过查询授权情况,返回包含ProSe查询代码的发现响应。

⑫~⑮:发现者在PC5接口发送ProSe查询代码,被发现者UE返回ProSe响应代码与发现者UE建立连接。

⑯~⑲:发现者UE请求DDNMF执行MIC检查,DDNMF检查后返回检查通过确认消息。

在上述过程中,随ProSe查询/响应代码发送的相关安全参数可用于保护ProSe查询/响应代码在传输和存储中的安全,提供机密性保护。在发现者UE请求DDNMF执行MIC检查则确保了发现消息的完整性。另外,发现者UE和被发现者UE分别设置ProSe时钟,利用与UTC时间的差值判断消息的时效性或过滤出符合的发现消息,为发现过程提供了抗重放保护。

1.2 5G ProSe直接通信安全

5G ProSe直接通信是指UE之间通过PC5接口传输数据,不需要通过基站[6]。5G ProSe直接通信支持单播、广播和组播模式。在3GPP TS 33.503中,重新使用3GPP TS 33.536[7]第5.3节中定义的单播模式安全机

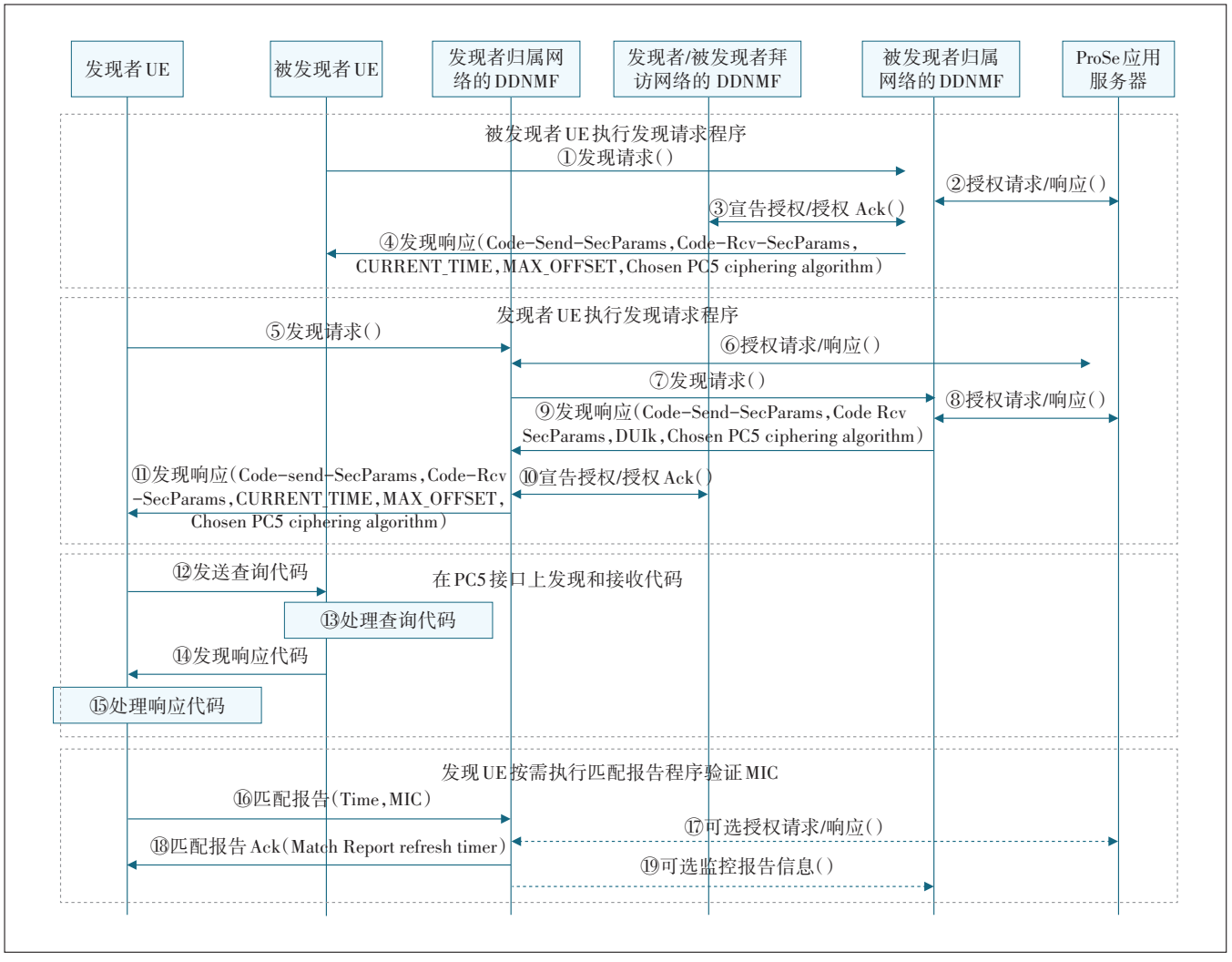

图3 限制性5G ProSe直接发现模式B的安全流程

制，以提供单播模式的5G ProSe直接通信安全和隐私保护。对于广播和组播模式的5G ProSe直接通信没有安全要求。

1.3 5G ProSe U2N中继通信安全

5G ProSe U2N中继分为2种中继方式：5G ProSe层3 U2N中继和5G ProSe层2 U2N中继。这2种方式均为远端UE提供网络访问服务，但存在以下差异[8]。

a）5G ProSe层3 U2N中继：远端UE不会与基站建立RRC连接，没有AS安全上下文。

b）5G ProSe层2 U2N中继：远端UE会与基站建立RRC连接并建立AS安全上下文。

1.3.1 5G ProSe层3 U2N中继通信安全

1.3.1.1 基于用户面建立5G ProSe U2N中继通信的PC5安全

基于用户面建立5G ProSe U2N中继通信的PC5安全流程如图4所示，可归纳如下。

⓪a~⓪d：远端UE和U2N中继UE分别向各自的5G DDNMF获取发现安全材料，其中包含PC5策略。

①a~③：远端UE从ProSe密钥管理功能（ProSe Key Management Function，PKMF）获取密钥UP-PRUK和用户面ProSe远端用户密钥ID（UP-PRUK ID）。远端UE与U2N中继UE执行1.1节中定义的发现流程。然后远端UE向U2N中继UE发起直接通信请求。

④a~④e：U2N中继UE在收到请求后，向它的

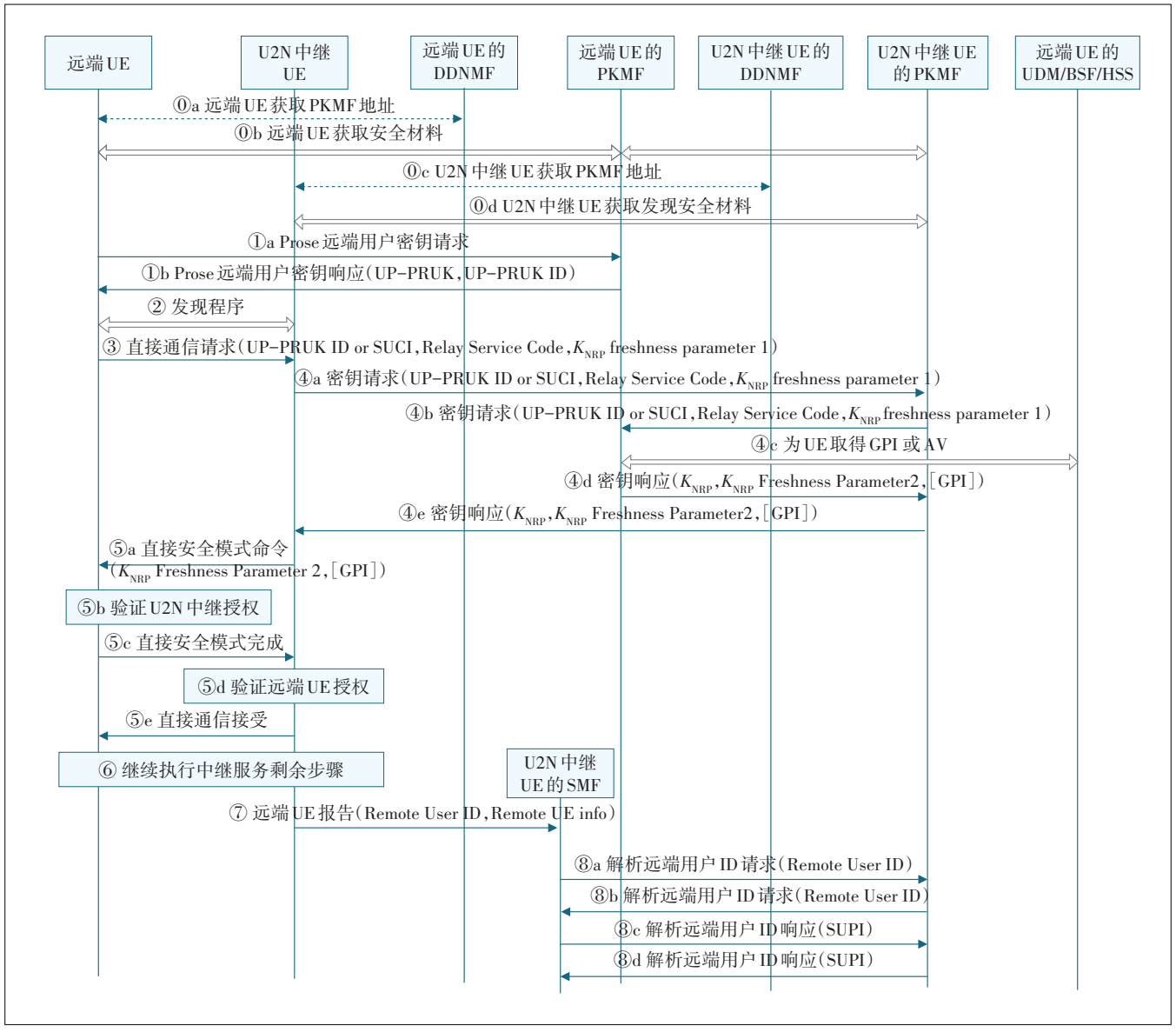

图4　基于用户面建立5G ProSe U2N中继通信的PC5安全流程

PKMF请求ProSe远端用户密钥,U2N中继UE的PKMF从远端UE的PKMF获得K_{NRP}。具体地,远端UE的PKMF通过与远端UE的UDM/BSF/HSS交互,获取UP-PRUK、UP-PRUK ID,然后计算出K_{NRP}。

⑤a~⑤e:U2N中继UE从K_{NRP}导出会话密钥$K_{NRP-SESS}$,然后根据PC5安全策略导出加密密钥NRPEK和完整性密钥NRPIK。远端UE也导出会话密钥$K_{NRP-SESS}$、加密密钥NRPEK和完整性密钥NRPIK。远端UE和U2N中继UE完成验证直接安全模式命令消息,即完成了PC5链路建立流程。

⑥~⑧d:远端UE和U2N中继UE进行PDU会话的建立或修改。如果U2N中继UE的SMF没有远端UE的ID和SUPI之间的映射,则向U2N中继UE的PKMF请求解析远端UE的ID。

在上述过程中,不仅在远端UE和U2N中继UE之间安全建立了PC5链路,远端UE和远端UE的PKMF在计算K_{NRP}密钥时均输入了K_{NRP}新鲜度参数,保证了密钥的新鲜度,实现抗重放保护。并且远端UE对直接发送请求消息中的UP-PRUK ID和中继服务代码(Relay Service Code,RSC)进行加密,提供了隐私和完整性保护。

1.3.1.2 基于控制面建立5G ProSe U2N中继通信的PC5安全

基于控制面建立5G ProSe U2N中继通信的PC5安全流程如图5所示,可归纳如下。

⓪a~⓪b:远端UE和U2N中继UE分别被网络注册、认证和授权。

①~⑤:远端UE与U2N中继UE执行1.1节中定义的发现流程。然后远端UE向U2N中继UE发起直接通信请求。U2N中继UE在收到请求后,向它的AMF(Access and Mobility Management Function)请求中继密钥,U2N中继UE的AMF将请求发给远端UE的AUSF(Authentication Server Function)。当远端UE的AUSF收到远端UE的签约用户隐式标识(Subscription Concealed Identifier,SUCI)时,执行步骤⑥~⑨b。

⑥~⑧b:远端UE的AUSF向远端UE的UDM(Unified Data Management)获取认证向量,然后启动认证流程,通过EAP-AKA′认证机制对远端UE进行认证。认证通过后,远端UE和远端UE的AUSF分别获取K_{AUSF_P},然后生成CP-PRUK(Control Plan - Prose Remote User Key)和CP-PRUK ID。

⑨a~⑨b:远端UE的AUSF选择PAnF并请求将远端用户的密钥信息存储在PAnF中。

当远端UE的AUSF收到CP-PRUK ID时,执行步骤⑩a~⑩b。

⑩a~⑩b:远端UE的AUSF选择PAnF并发送CP-PRUK ID。PAnF检索出CP-PRUK后返回给AUSF。

⑪~⑰:远端UE的AUSF生成K_{NRP}并将其通过U2N中继UE的AMF发送给U2N中继UE。U2N中继UE从K_{NRP}推导出PC5会话密钥$K_{relay-sess}$和加密密钥$K_{relay-enc}$以及完整性密钥$K_{relay-int}$。远端UE也生成K_{NRP},然后推导出PC5会话密钥$K_{relay-sess}$和加密密钥$K_{relay-enc}$以及完整性密钥$K_{relay-int}$。随后远端UE和U2N中继UE完成验证直接安全模式命令消息,即完成了PC5链路建立流程。

在上述过程中,不仅在远端UE和U2N中继UE之间建立了PC5安全链路,5G ProSe远端UE的AUSF也基于EAP-AKA′机制完成了对5G ProSe远端UE的认证。

1.3.2 5G ProSe层2 U2N中继通信安全

当远端UE通过5G ProSe层2 U2N中继进行5G ProSe通信的连接建立时,5G ProSe远端UE与基站建立AS安全。远端UE和5G ProSe U2N中继UE应使用与5G ProSe层3 U2N中继通信安全相同的安全机制为PC5链路建立安全。

2 R18阶段5G ProSe安全研究进展

目前,3GPP SA2已基本完成R18阶段的5G ProSe_Ph2的研究和标准化工作,并对3GPP TS 23.304标准进行更新,主要增加以下5G ProSe的架构和特性。

a)支持PC5单跳U2U中继的单播模式。

b)增强了U2N中继功能以及通过U2N中继的远端UE的紧急服务等。

c)支持Uu通信路径和PC5通信路径之间的路径切换。

3GPP SA3基于3GPP TS 23.304中新增的特性,开展相关安全问题的研究,目前主要聚焦于5G ProSe U2U中继发现和5G ProSe U2U中继通信安全。

2.1 5G ProSe U2U中继发现安全

在3GPP TS 23.304中定义了2种5G ProSe U2U中继发现模式:模式A和模式B。前者由U2U中继充当宣告UE的角色,向邻近的所有UE广播宣告消息;后者由源UE充当发现者,目标UE充当被发现者,U2U中继为两者之间传递消息。

对于以上2种模式,3GPP SA3开展相关研究,为

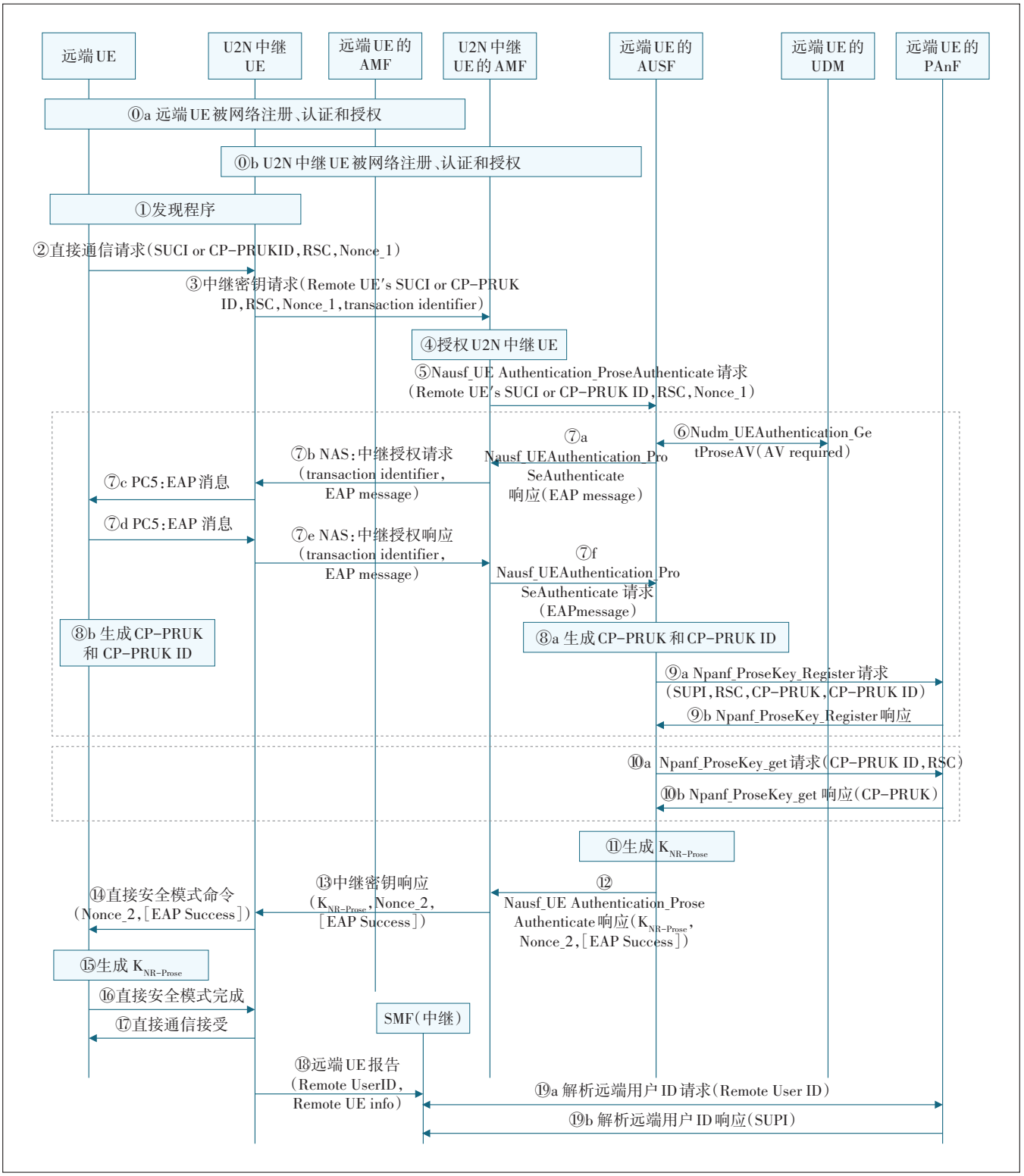

图5　基于控制面建立5G ProSe U2N中继通信的PC5安全流程

U2U中继发现的发现消息提供安全机制，主要从以下3个方面展开。

a）提供U2U中继发现消息的机密性、完整性和抗重放保护。

b）提供U2U中继发现过程中源UE和目标UE的隐私保护。

c）提供U2U中继发现的安全材料的预先配置方法。

2.2 5G ProSe U2U中继通信安全

与5G ProSe U2N中继相似，5G ProSe U2U中继也有2种类型：5G ProSe层3 U2U中继通信和5G ProSe层2 U2U中继通信。针对这2种场景，3GPP SA3开展相关研究，为U2U中继的消息传输提供安全机制，主要从以下3个方面展开。

a）提供UE之间传输信息的机密性、完整性和抗重放保护。

b）提供用户面和控制面消息安全机制，包括U2U中继路径切换过程中的消息安全。

c）提供源UE和目标UE之间建立安全连接的方法。

3 未来展望

当前5G ProSe已经支持直接发现、直接通信、U2N中继和U2U中继等关键技术，其中直接发现、直接通信和U2N中继的安全已完成标准化工作，后续工作重点将是完成R18阶段的U2U中继场景下的安全研究和标准化工作。

针对5G ProSe U2U中继发现安全，由于5G ProSe U2U中继发现消息包含2套元素：直接发现元素和U2U发现元素，需重点研究采用1套还是2套安全材料来保护5G ProSe U2U中继发现消息的安全，以及相应的安全材料预先配置问题。

针对5G ProSe U2U中继通信安全，无论是层2中继还是层3中继，均需考虑U2U中继在覆盖范围内或覆盖范围外2种场景下的安全问题，并且在考虑源UE和目标UE之间的通信安全时，应将U2U中继视为受信任的节点，通过U2U中继连接的源和目标UE之间的安全可以逐跳进行保护或端到端进行保护，亦或两者兼而有之。

在完成R18阶段5G ProSe安全的标准化工作的同时，3GPP R19阶段关于5G ProSe关键技术的研究也将同步开展，未来主要从增强U2N中继以支持PC5多跳、Wi-Fi或蓝牙等非3GPP无线接入技术（Radio Access Technology，RAT）等方面开展研究。此外，将NWDAF及相关用例应用在5G ProSe技术中，使得提供的邻近服务更加智能化也是下一阶段的目标。在安全方面，R19阶段也将继续研究5G ProSe新增关键技术相关的安全问题，包括U2N中继的PC5多跳安全链接建立流程、支持非3GPP接入的安全以及引入NWDAF后将带来的安全问题（如5G ProSe UE的隐私保护、数据机密性和完整性保护以及5G ProSe UE与NWDAF所属网络的相互认证和数据获取的授权等安全问题）。

4 结束语

本文分析了3GPP不同阶段的5G ProSe安全。针对R17阶段的5G ProSe安全，主要分析5G ProSe直接发现、直接通信和U2N中继3种场景下的安全威胁，并对3GPP标准中提出的安全机制进行抽象和归纳，分析安全机制如何消除对应的安全威胁。针对R18阶段的5G ProSe安全，介绍了5G ProSe U2U中继的网络架构和关键技术以及相关安全问题的研究方向。最后指出5G ProSe技术未来的演进方向以及潜在的安全研究问题，可为5G ProSe下一步研究工作的开展以及未来在公共安全和商业领域的实际部署提供参考。

参考文献：

[1] 3GPP. Proximity-based services (ProSe): 3GPP TS 23.303[S/OL]. [2023-05-04]. ftp://ftp.3gpp.org/Specs/.

[2] 3GPP. Study on LTE-based V2X services: 3GPP TR 36.885[S/OL]. [2023-05-04]. ftp://ftp.3gpp.org/Specs/.

[3] Reportbuyer. ProSe (Proximity Services) for LTE & 5G networks: 2017-2030 - opportunities, challenges, strategies & forecasts [R/OL]. [2023-05-04]. https://www.reportlinker.com/p04648412/ProSe-Proximity-Services-for-LTE-5G-Networks--Opportunities-Challenges-Strategies-Forecasts.html.

[4] 3GPP. Proximity based services (ProSe) in the 5G system (5GS): 3GPP TS 23.304[S/OL]. [2023-05-04]. ftp://ftp.3gpp.org/Specs/.

[5] 3GPP. Security aspects of proximity based services (ProSe) in the 5G system (5GS): 3GPP TS 33.503 [S/OL]. [2023-05-04]. ftp://ftp.3gpp.org/Specs/.

[6] 贾靖，聂衡. 5G邻近服务关键技术[J]. 移动通信，2022，46(2)：49-54.

[7] 3GPP. Security aspects of 3GPP support for advanced vehicle-to-everything (V2X) services: 3GPP TS 33.536[S/OL]. [2023-05-04]. ftp://ftp.3gpp.org/Specs/.

[8] 刘宇泽，邢真，游世林，等. 5G邻近通信安全研究[J]. 信息通信技术与政策，2022(8)：24-30.

作者简介：
姚戈，工程师，博士，主要研究方向为网络与信息安全；徐雷，教授级高级工程师，博士，主要研究方向为网络与信息安全；张曼君，高级工程师，博士，主要研究方向为网络与信息安全。