基于对称密钥算法的 5G 网络防伪基站技术

Anti-Fake Base Station in 5G Network Based on Symmetric Cryptography Algorithm

摘要：分析了 5G 网络场景下可能的伪基站攻击方式，提出了一种基于对称密钥算法的伪基站防护技术，包括密钥协商和传递流程、保护区信息提供流程和基站小区的真实性验证流程。设计了用于加密信息的密钥的产生、传递和使用方法，以及用于验证小区广播或单播消息真实性的密钥产生方法，实现了针对小区发送的广播消息或单播消息的真实性验证，达到了伪基站识别的效果。

关键词：伪基站；对称密钥算法；保护区域；共享根密钥组

Abstract: The possible attack methods of the fake base stations in 5G network are analyzed. A technical solution for anti-fake base stations based on symmetric key algorithm is proposed, including protection key agreement and transmission procedure, protection area information provision procedure, and cell authenticity procedure. The generation, transmission, and use of key used to encrypt information are designed, and the key generation method used to verify the authenticity of the cell is also designed, realizing the authenticity verification of the broadcast or unicast message sent by the cell to achieve fake base station recognition.

Keywords: fake base station; symmetric key algorithm; protection area; shared root key group

毛玉欣 /MAO Yuxin
游世林 /YOU Shilin
闫新成 /YAN Xincheng
（中兴通讯股份有限公司，中国 深圳 518057）
(ZTE Corporation, Shenzhen 518057, China)

DOI：10.12142/ZTETJ.202106012
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20200728.0940.002.html

网络出版日期：2020-07-28
收稿日期：2020-07-10

移动通信经历了从 1G 到 4G 的发展过程，如今正大力发展 5G，以实现万物互联。传统移动通信主要用于满足人们语音通信的需求。4G 让人们享受到无处不在的高速网络接入，5G 的到来将使移动通信网络赋能于更广泛的行业。通信技术的发展使得网络承载的信息和价值越加丰富，但由此引发的网络安全风险也随之增长。2G 网络和终端间采用单向认证，使终端无法对网络进行合法性验证。这导致了伪基站问题的爆发[1]。随着通信技术的升级换代，终端和网络间引入双向认证，使网络安全性得到增强。然而，伪基站问题仍然无法完全避免。例如，攻击者通过干扰终端的 3G 和 4G 通信信号，使得手机无法正常使用 3G、4G 通信信号。为了保障通信，终端就会主动降频到 2G。如果终端使用 2G 网络进行通信，伪基站就可以再次发挥作用[2]。

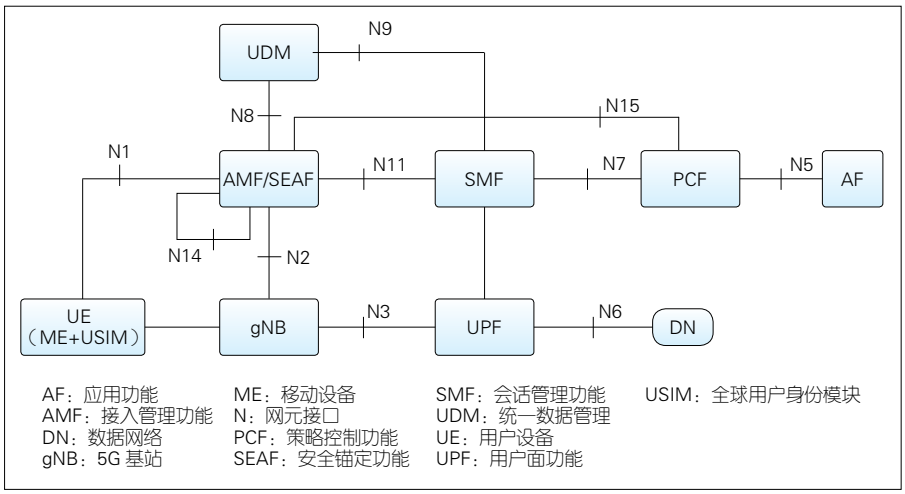
由此可见，移动蜂窝网络演进的确使伪基站问题得到一定程度的缓解，但是由于巨大的利益驱动，伪基站技术也在发展演进。本文中我们重点探讨 5G 网络场景下的伪基站问题和应对解决方案。

1 5G 网络场景下的伪基站威胁分析

第三代合作伙伴计划（3GPP）定义了 5G 网络架构[3]。5G 网络包括无线接入网络（RAN）和 5G 核心网（5GC），如图 1 所示。RAN 主要由 5G 基站（gNB）组成。5GC 主要包含统一数据管理（UDM）、接入管理功能（AMF）/ 安全锚定功能（SEAF）、会话管理功能（SMF）、用户面功能（UPF）、策略控制功能（PCF）等网络功能。用户设备（UE）一般由移动设备（ME）和全球用户身份模块（USIM）组成。gNB 和 AMF/SEAF 通常位于 UE 的服务网络，UDM 等则位于用户的归属网络。

5G 网络下的广播消息或单播消息有可能导致伪基站攻击出现。当 UE 处于连接模式或进入连接模式时，在安全上下文激活完成之前，可能会发生伪基站攻击。小区周期性广播同步信号和系统信息，UE 则基于同步信号检测小区。如果检测到的小区信号质量高于定义门限，则 UE 根据小区选择标准对所有候选小区进行选择，并驻留到信号质量最好的小区。

基金项目：工业和信息化部新一代宽带无线移动通信网重大专项（2017ZX03001018）



▲图 1 5G 通信网络架构

由于 UE 只检测信号质量，因此伪基站可以很容易地利用高质量信号来诱使 UE 驻留 [4]。

gNB 将业务信息，例如公共警告系统（PWS）消息、地震和海啸预警系统（ETWS）消息、车用无线通信技术（V2X）消息等，通过系统信息块（SIB）发送给驻留 UE。伪基站可篡改合法广播消息中携带的这些服务信息或者伪造虚假的服务信息。如果 UE 驻留到伪基站上，就会存在如下安全威胁：

（1）PWS 携带的信息可能包含虚假信息、垃圾短信等，进而误导用户点击欺诈网站的链接。此外，攻击者还可通过伪基站来传播虚假信息以制造社会恐慌。

（2）UE 驻留到伪基站后，无法获得正常的广播服务，如检测紧急呼叫、ETWS 消息、V2X 消息等。

（3）虚假广播消息也可能对终端的软件系统实施攻击，例如通过构造复杂消息来触发软件系统的已知漏洞，使操作系统或者应用软件被劫持或阻塞。

（4）降级攻击。gNB 向 UE 发送消息，请求 UE 的接入安全能力。UE 在安全模式（SMC）完成前给 gNB 反馈 UE 能力信息。此时，伪基站可以作为“中间人”捕获该消息，将 UE 的真实接入安全能力调低并反馈给真实的 gNB，以降低 UE 接入到网络的安全能力。

（5）5G 虽然使用用户签约隐藏标识（SUCI）来替代用户签约永久标识（SUPI）发送给网络，但这种替代并非强制。当 SUPI 的保护模式设置为“null-scheme”时，SUPI 仍然使用明文在网络中传递 [5]。如果此时网络并没有建立安全传输模式，例如接入层安全（AS）、非接入层安全（NAS），则 SUPI 有可能在传输时暴露，从而造成隐私泄露。

（6）拒绝服务（DoS）攻击。伪基站可通过不断向 UE 反馈拒绝消息来拒绝 UE 的附着请求，从而制造 DoS 攻击。

在上述威胁中，预防（1）和（3）需要对 SIB 消息实施鉴权，预防（2）需要 UE 驻留小区时进行伪基站检测，预防（4）需要对 UE 和网络之间的能力协商消息进行保护，预防（5）需要防止 UE 驻留到伪基站上，预防（6）需要验证基站向 UE 返回的消息的真实性。

综上分析，5G 系统如果要防止伪基站带来的安全威胁，就需要对单播或者广播消息进行保护，从而防止 UE 驻留到伪基站上。

2 基于对称算法的防伪基站技术方案

2.1 方案概述

目前移动通信网络主要使用非对称密钥算法为无线信令提供数字签名方案以实现伪基站防护 [6-7]。但非对称密钥算法对计算资源开销过大，这对终端和无线设备等计算能力有限的设备而言势必增加了处理负担。本文中，我们研究了一种基于对称密钥算法的伪基站防护技术，其核心思想为：在归属网络的协助下，服务网络向 ME 动态提供加密的用于验证无线信令真实性的密钥。gNB 为无线信令使用对称密钥算法生成一个消息认证码（MAC-I），然后由 ME 在 USIM 的协助下使用验证无线信令真实性的密钥来验证 MAC-I，以判断无线信令是否是伪基站发出的信令。技术方案包含如下关键步骤：

（1）服务网络向 ME 提供用于验证无线信令真实性的密钥；

（2）用于验证无线信令真实性的密钥是加密的，无法被 ME 解密，只能由 USIM 完成解密；

（3）USIM 存储的加密密钥具备和长期密钥（LTK）相同的安全要求；

（4）加密密钥和用于验证无线信令真实性的密钥需要周期性更新；

（5）ME 将用于验证无线信令真实性的加密密钥和无线信令发送给 USIM 验证。

通过对消息设置完整性校验来实现对广播消息（例如 MIB、SIB 和告警消息等）和下行绝对无线频道编号（DL_ARFCN）的保护。当 UE 驻留到 gNB 的一个小区时，服务网络仅给 USIM 提

供有限数量的密钥。这使得 UE 只能处理密钥对应 gNB 发送的经过完整性保护的广播消息，可有效减少 UE 处理发送消息的 gNB 数量，减轻 UE 处理负担。这些 gNB 覆盖的区域被称为保护区（PA），具体可参考本文 2.4.1 节内容。当攻击者捕获 PA 中某个小区的广播消息时，攻击者只能模拟该小区使用相同的 DL_ARFCN 频率向同一 PA 下的某个 UE 广播无法更改的消息，从而使攻击变得困难，同时使攻击者（伪基站）容易被定位和被网络检测到。当 UE 在一个重放系统消息的伪小区驻留时，UE 将使用本文 2.5.2 节中描述的单播消息真实性验证流程检测到该小区是伪小区，然后重新选择其他小区进行驻留。在同一 PA 中广播捕获的告警消息也可能是一种安全威胁。对此，可通过在告警消息中添加时间和区域等信息，以避免重放威胁。

2.2 技术框架

图 2 描述的是基于对称密钥算法的 5G 网络场景下防伪基站技术方案，包括 4 个流程：（1）保护密钥协商（PKA）流程、（2）保护密钥传输（PKT）流程、（3）PA 信息提供（PAIP）流程和（4）小区真实性验证（CA）流程。其中，流程（1）和（2）一并执行，流程（2）始终在流程（1）之后，流程（3）为服务网络向 ME 提供 PA 信息的流程，流程（4）包括针对广播消息和单播消息的真实性验证过程。

CKp 是用于加密服务网络向 ME 提供信息的密钥，由归属网络和 USIM 协商产生，并且在 USIM 上存储时具备与根密钥 LTK 相同的安全需求，即 USIM 应防止 CKp 泄露。

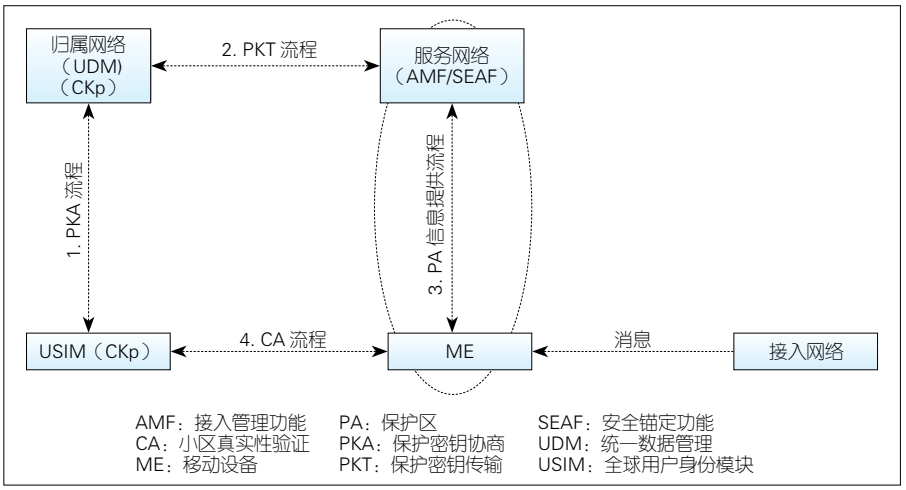
服务网络向 ME 提供的 PA 信息包括被 gNB 用于无线信令完整性保护的密钥。PA 信息中的密钥在被 CKp 加密后提供给 ME。ME 接收之后必须由 USIM 完成解密。ME 将 PA 信息和无线信令发送给 USIM，然后由 USIM 进行小区真实性验证。CKp 和被 gNB 使用的密钥必须定期更新，以便密钥在被攻破时即时失效。此外，该技术方案还具有另外的作用，比如在 5G 安全上下文激活之前，可对无线信令上传输的敏感信息进行加密传输。

2.3 PKA 和 PKT 流程

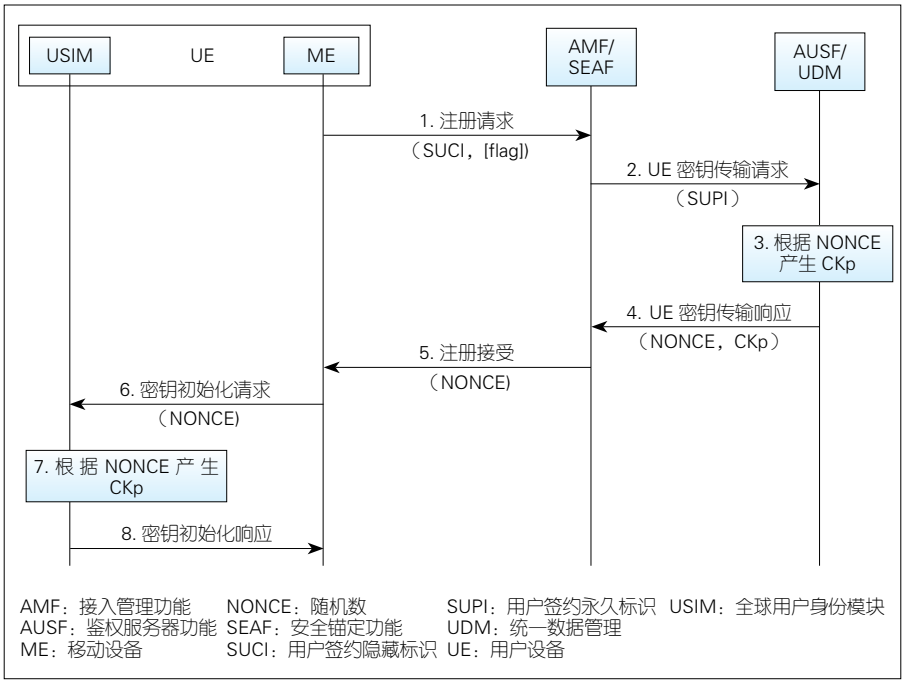
图 3 展示了在 UE 向网络发起注册的过程中完成的 PKA 和 PKT 流程。假设在漫游场景下，AMF/SEAF 所在的漫游服务网络和 AUSF/UDM 所在的归属网络之间的漫游接口具备完整性、机密性和抗重放保护能力。

（1）UE 发送网络注册请求消息给服务网络 AMF/SEAF。如果 UE 决定更新 CKp，则请求消息需要携带一个说明密钥协商的标记。

（2）如果 UE 注册到网络而发起注册流程，或者 AMF/SEAF 收到 Flag



▲图 2 基于对称密钥算法的伪基站防护方案



▲图 3 保护密钥协商流程和保护密钥传输流程

标记，则发起 PKT 流程。AMF/SEAF 向 UDM 发送 CKp 请求消息（UE 密钥传输请求），并携带 SUPI。

（3）UDM 收到请求消息后，会根据 LTK 产生一个 CKp 和一个随机数（NONCE）。

（4）UDM 向 AMF/SEAF 返回 NONCE 和 CKp，以完成 PKT 流程。AMF/SEAF 上报 CKp 给防伪基站功能（AFBF）。AFBF 可以是运营和管理（OAM）平台功能，也可以是专用网络功能。AFBF 通过 CKp 加密 K_{RBS}（参考 2.4.1 定义）得到加密的 EK_{RBS}。

（5）AMF/SEAF 向 UE 发送注册成功消息，并携带 NONCE。

（6）UE 接收 NONCE。如果 UE 支持 AFBF，则 ME 将 NONCE 发送给 USIM。

（7）USIM 启动 CKp 初始化过程。USIM 使用 NONCE 和 LTK 计算产生密钥 CKp。这种计算方法与 UDM 计算 CKp 的方法相同。同时 USIM 应能够防止 CKp 外泄。

（8）USIM 产生 CKp 之后向 ME 返回指示。

2.4 PAIP 流程

2.4.1 PA 保护区域

我们将每个 PA 下的 gNB 进行分组，并将组称为共享根密钥组（SRKG）。每个 SRKG 由 bsGKI 标识，同时 SRKG 下的每个 gNB 由 bsGNI 标识。如图 4 所示，而每个 gNB 仅属于一个 SRKG，每个 SRKG 可以属于一个或多个 PA。

在对 gNB 分组的情况下，每个 SRKG 具备一个密钥 K_{RBS}。该密钥被 SRKG 下的每个 gNB 共享。基于 K_{RBS} 派生出 SRKG 下每个 gNB 的密钥 K_{BS} 可用于基站保护。服务网络向 ME 提供的 PA 信息中仅包含 K_{RBS} 的加密密钥 EK_{RBS}，以减少提供给 ME 的加密密钥数量。

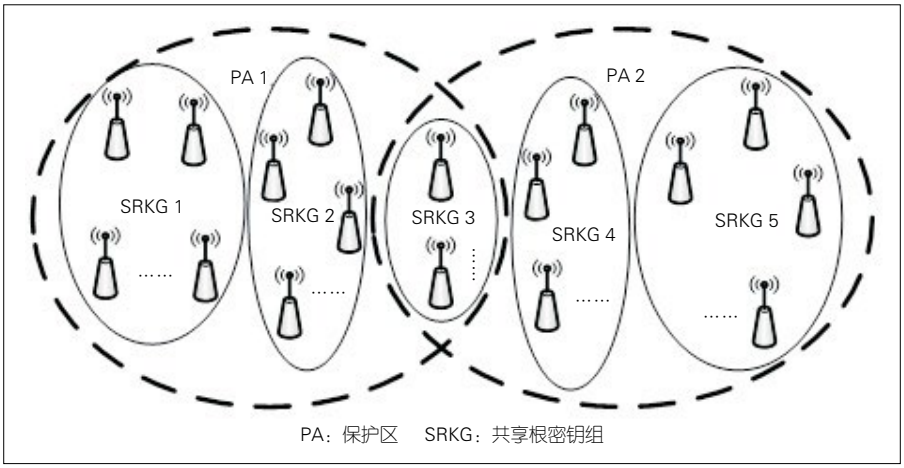
任何注册区域（RA）均被一个且唯一一个 PA 完全覆盖，因此在 UE 注册过程中，服务网络可以向 ME 提供 PA 的加密密钥。图 5 描述了 RA 与 PA 之间的关系。

在注册期间（包括初始注册、移动性或周期性注册）或者其他初始 NAS 消息处理过程中，AMF 应向 ME 提供 PA 信息，其中 PA 信息包括 bsGKI 列表、对应的 EK_{RBS} 列表以及密钥有效期。有效期用于防止伪基站破解 gNB 的 K_{BS} 去欺骗 UE。当给密钥加上有效期时，即使上述密钥被破解，密钥也已到期。因此，设置的有效期应足够短，以使密钥在一定期限内不被破解。

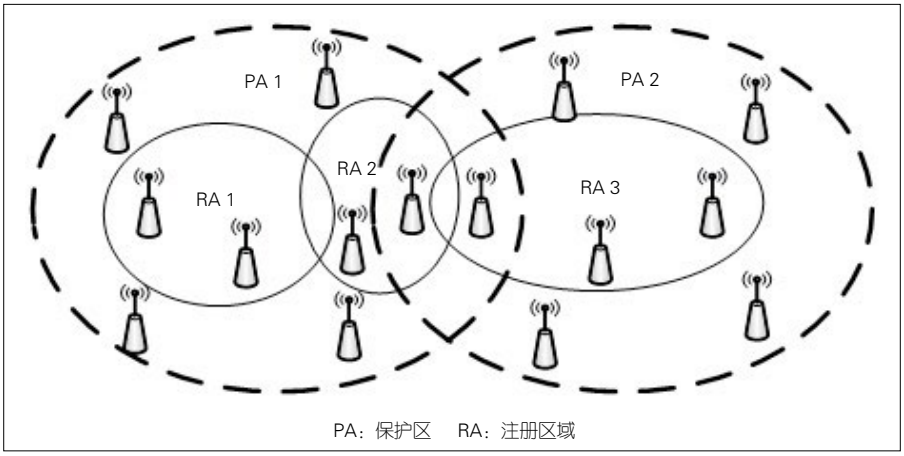
在密钥到期前，服务网络应更改 SRKG 的根密钥 K_{RBS}。为了提高性能，一个 PA 应包含和其全覆盖下的跟踪区毗连的 gNB。这样，当 UE 位于跟踪区边缘时，UE 也能获取每个毗连 gNB 的密钥。同时 PA 划分的范围也不宜过大，这是因为太大的 PA 会很难减轻基于重放广播无线信令的伪基站攻击。

2.4.2 PA 信息表示

结合 2.4.1 对 PA 的定义，如图 6 所示，PA 信息是一组 gNB 信息的结合，表示形式为：PA = (<ID*a*, Enc(CKp, $K_{RBS}[a]$)>, <ID*b*, Enc(CKp, KRBS[*b*])>, ……)。



▲图 4 SRKG 和 PA 之间的关系



▲图 5 RA 和 PA 之间的关系

每个 gNB 信息都由 gNB 标识（ID*i*, *i*=*a*,*b*,*c*, ...）和使用 CKp 加密的根密钥（$K_{RBS}[i]$, *i*=*a*,*b*,*c*, ...）组成。在移动过程中，UE 获取的 PA 信息在不断更新。当 UE 从一个 PA 移动到另外一个 PA 时，ME 向服务网络发出 PA 更新请求。服务网络在响应消息中将更新的 PA 信息提供给 ME。

2.4.3 PAIP 流程

服务网络向 ME 提供 PA 信息的预置条件有两个：

（1）服务网络通过 OAM 平台或专用网络功能提供每个 gNB 对应的 bsGKI 和 bsGNI；

（2）服务网络通过 OAM 平台或专用网络功能管理 SRKG 的密钥及其他相关信息。

K_{BS} 的产生方式为：K_{BS} = HMAC–SHA–256 (K_{RBS}, <bsGKI, bsGNI>)。其中，<bsGKI, bsGNI> 是两个参数的串接，根据 2.4.1 节中的定义，为 gNB 标识。K_{RBS} 为 gNB 的根密钥，即 gNB 所在 SRKG 的密钥。每个 gNB 根据标识和 K_{RBS} 使用密钥派生算法派生得到 K_{BS}。K_{BS} 用于对无线信令进行加密和完整性处理。

图 7 描述的是 UE 与服务网络之间的共享密钥提供流程，具体包括 5 个步骤：

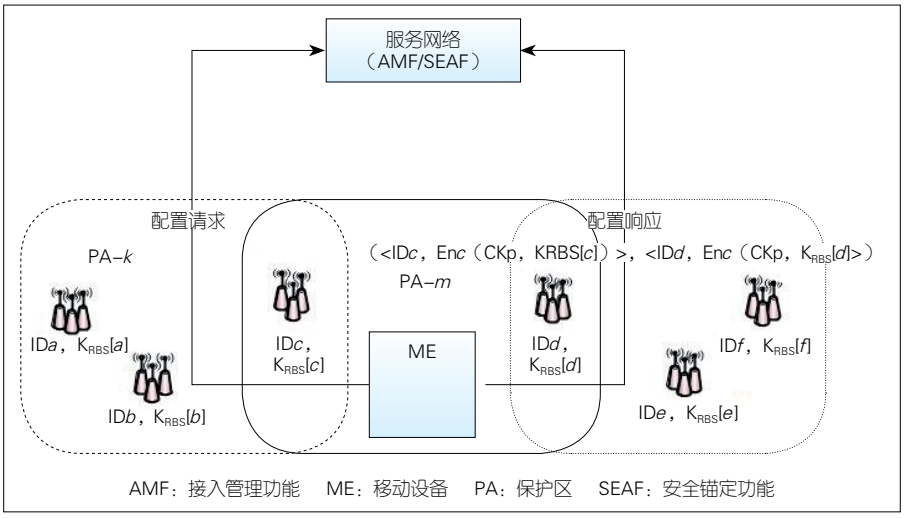
（1）在 PKT 流程中，CKp 从归属网络发送到服务网络。

（2）UE 向 AMF/SEAF 发送注册请求，该消息能够触发 PKA 和 PKT 过程。

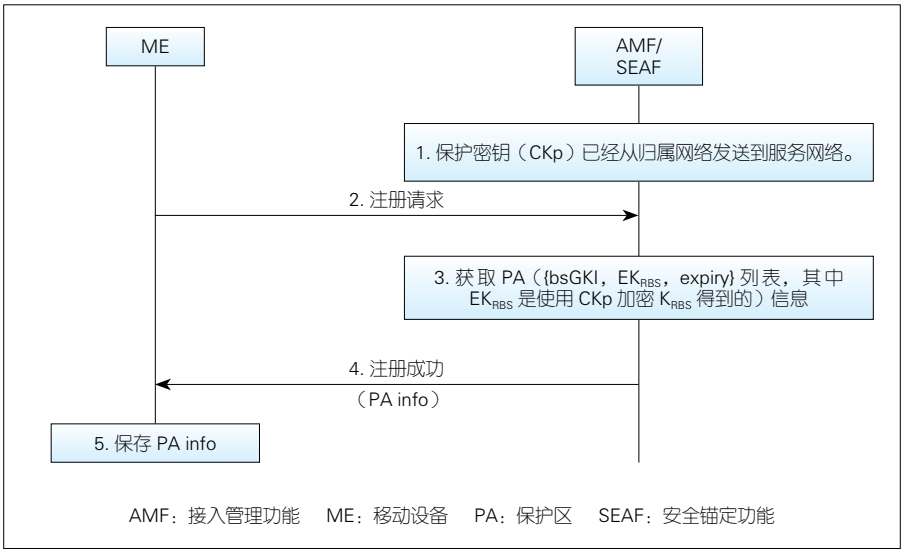
（3）如果 AMF/SEAF 支持 AFBF，那么 AMF/SEAF 就可以获取 PA 信息，即覆盖 UE 当前驻留跟踪区的 PA{bsGKI, EK_{RBS}, expiry }列表。其中，EK_{RBS} 使用 CKp 加密的 K_{RBS}；expiry 指示 EK_{RBS} 的有效期，即在有效期到期后，EK_{RBS} 必须更新。

（4）AMF/SEAF 向 UE 返回注册成功消息，并且消息中携带 PA 信息。

（5）如果 ME 支持 AFBF，那么 ME 将保存 PA 信息。



▲图 6 ME 移动过程中的 PA 信息动态更新



▲图 7 PA 信息提供流程

2.5 CA 流程

2.5.1 广播消息真实性验证流程

图 8 是广播消息真实性验证流程，具体包括 6 个步骤：

（1）gNB 决定通过一个小区广播一条消息，例如 MIB 或 SIB。该消息包含 gNB 标识 <bsGKI, bsGNI>。如果消息长度加上 DL_ARFCN 长度后大于 32 B，那么 gNB 产生网络侧哈希值（$HASH_{NW}$）的方式为：HASHNW = SHA–256 (DL_ARFCN ‖ message)。

gNB 根据 KBS 计算出 MAC–I，以及 DL_ARFCN 串接消息（其长度小于等于 32 B），或者 $HASH_{NW}$（其长度大于 32 B）。

（2）gNB 广播消息，同时消息携带 <bsGKI, bsGNI> 和 MAC–I。

（3）ME 通过小区接收广播消息，同时消息携带 <bsGKI, bsGNI> 和 MAC–I。ME 检查 bsGKI 是否在保存的 PA 信息列表中。如果检查失败，ME 在缓存中将该小区标记为可疑小区；

如果检查成功，则继续步骤 4。

（4）如果 DL_ARFCN 长度加上接收消息的长度大于 32 B，则 ME 将首先计算 $HASH_{MS}$（与 gNB 计算 HASHNW 的方式相同），然后发送 EKR_{BS}、<bsGKI, bsGNI> 到 USIM。如果已经计算 $HASH_{ME}$，则 ME 也会将 $HASH_{MS}$ 发送给 USIM；否则，ME 将把 DL_ARFCN 和接收到的消息串接发送给 USIM。EKR_{BS} 和 bsGKI 对应表示由 bsGKI 标识的 SRKG 密钥。

（5）USIM 先根据存储的 CKp 解密 EKR_{BS} 并得到 KR_{BS}，然后从 KR_{BS} 和 <bsGKI，bsGNI> 中派生出 K_{BS}，再根据 K_{BS} 计算出 XMAC–I。USIM 计算 XMAC–I 的方式与 gNB 基于 K_{BS} 的计算 MAC–I 方式相同。

（6）USIM 将 XMAC–I 反馈给 ME。ME 会比较 XMAC–I 和 MAC–I，如果两者相等，则 ME 会处理广播消息；否则，ME 会在缓存中将该小区标记为高危小区。

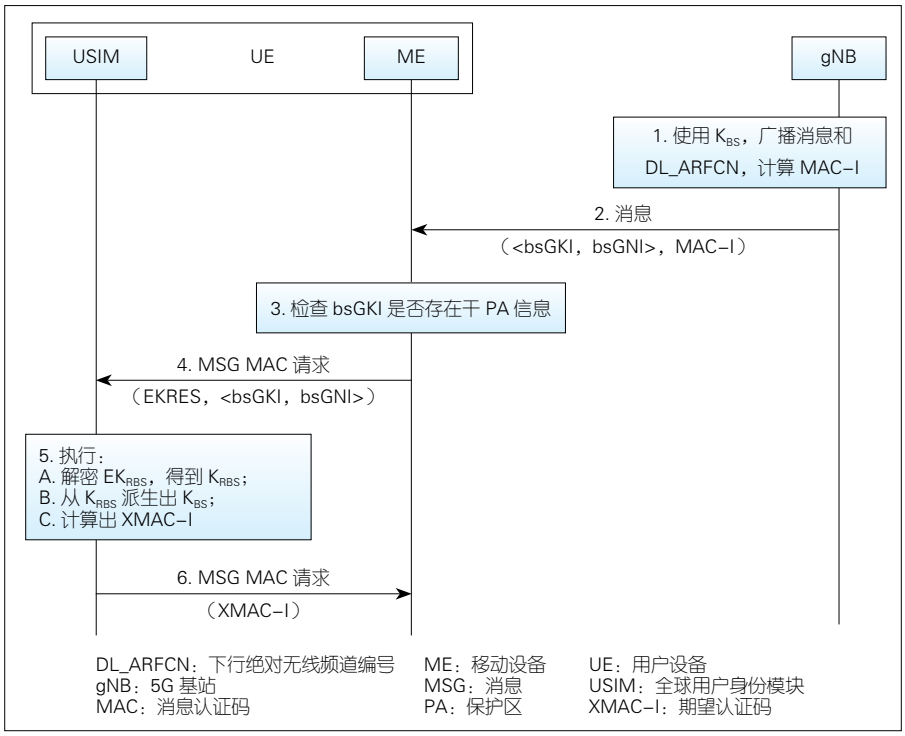
对网络认证成功后，UE 应检查缓存中的可疑或高危小区是否在 PA 中。如果不在，则缓存中的小区被标记为可疑小区，否则 UE 将进行小区验证。如果验证失败，UE 在缓存中将该小区标记为伪小区；如果验证成功，该小区将从缓存中被移除。UE 可以将缓存中的可疑、高危和伪小区告知给服务网络。

2.5.2 单播消息真实性验证流程

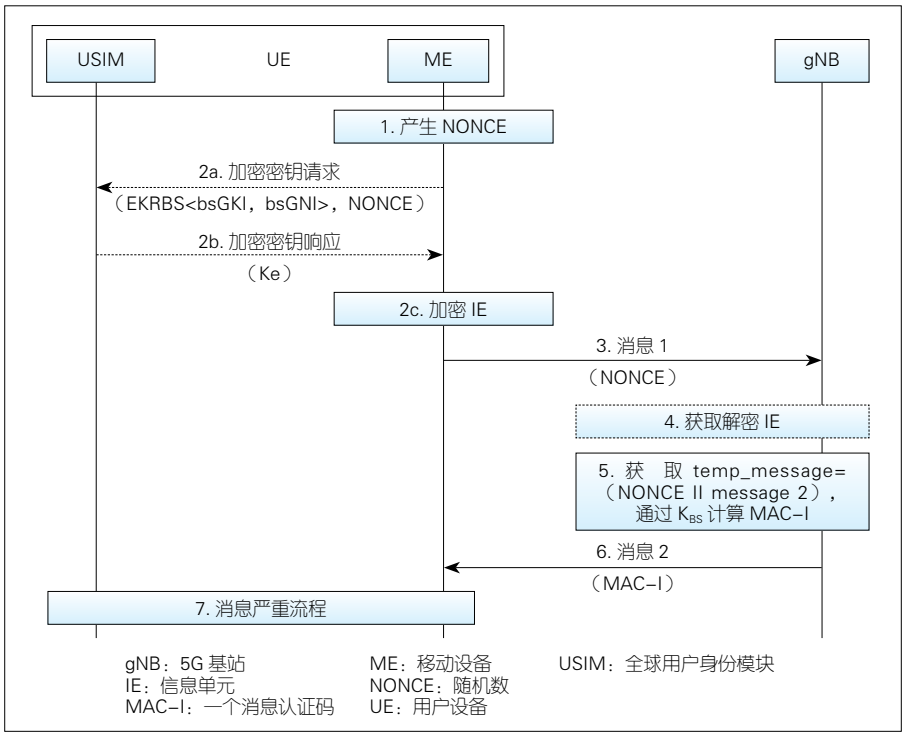
只有在 UE 和 gNB 无法获取 AS 安全上下文的情况下，单播消息真实性验证流程才会生效。图 9 是单播消息真实性验证流程，具体包括 7 个步骤。

（1）ME 尝试驻留在一个小区上，并决定向该小区发送消息 1。ME 产生一个随机字符串 NONCE。NONCE 可被作为连续下行消息的重放保护参数。

（2）ME 可以决定对消息 1 中的敏感信息进行保护。ME 将 EK_{RBS}，<bsGKI, bsGNI>、敏感信息和 NONCE 发送给 USIM。其中，<bsGKI, bsGNI> 是从小区发送的广播消息（比如 SIB 或者 MIB）中获取的。同时，EKR_{BS} 和 bsGKI 相对应。USIM 解密 EKR_{BS} 得到 KR_{BS}，并根据 KR_{BS} 和 <bsGKI，bsGNI> 派生得到 K_{BS}。然后 USIM 根据



▲图 8 广播消息真实性验证流程



▲图 9 单播消息真实性验证流程

K_{BS} 派生出 Ke，并将 Ke 返回给 ME。ME 根据 Ke 和 NONCE 生成密钥流，并对敏感信息和密钥流进行异或计算，以实现对敏感信息的加密。

（3）ME 向小区发送消息 1。其中，消息 1 携带 NONCE，并且消息 1 是部分加密的。

（4）gNB 收到消息 1。如果消息 1 是部分加密的，则 gNB 解密加密部分以获得明文信息。

（5）gNB 决定向 UE 发送消息 2。gNB 获取 temp-message=（NONCE || message2），并按照 2.5.1 描述的方式计算 temp-message 的 MAC-I。

（6）gNB 将消息 2 发送给 UE。其中，消息 2 携带 MAC-I。

（7）ME 接收消息 2，并按照 2.5.1 中的步骤 4—6 进行消息真实性验证。验证过程用 temp-message=（NONCE || message2）替代消息 2。

3 结束语

本文描述了 5G 网络场景中由攻击广播消息或单播消息产生的伪基站问题，进而提出了针对广播信息和单播信息进行真实性验证的方法以抵御伪基站攻击。此外，本文还研究了使用对称密钥算法对广播消息和单播消息进行机密性或者完整性防护的实现过程，包括用于保护密钥的协商和传递过程、PA 信息表示和提供过程，以及针对广播信息或单播信息的真实性验证过程。相对于使用非对称算法对无线消息进行防护的方法，对称密钥算法具有对网络资源要求少的优势，是值得推荐的技术方案。随着技术的不断演进，伪基站攻击方法还会不断发展，相应的防护方案需要进行不断完善。

参考文献

[1] 李赓，赵玉萍，孙春来，等 . 一种基于伪信令的伪基站抑制方法研究与分析 [J]. 信息网络安全，2014, (9): 12-16
[2] 刘长波，张敏，常力元，等 . 5G 伪基站威胁分析及安全防护建议 [J]. 移动通信，2019, 43(10): 58-61
[3] 3GPP. System architecture for the 5G system: 3GPP TS 23.501 [S]. 2020
[4] 李宁 . 基于 GSM 基站信息的伪基站侦测系统 [D]. 成都 : 西华大学，2016
[5] 3GPP. Security architecture and procedures for 5G system: 3GPP TS 33.501 [S]. 2020
[6] IEEE. IEEE standard for identity-based cryptographic techniques using pairings: IEEE 1363.3 [S]. 2013
[7] IETF. Elliptic curve-based certificateless signatures for identity-based encryption: IETF RFC 6507 [S]. 2012

作 者 简 介

毛玉欣，中兴通讯股份有限公司资深系统架构师；主要研究方向为 5G 网络安全和虚拟化安全；参与多项国际技术标准的制定；拥有发明专利 70 余项、国际标准提案 50 余项。

游世林，中兴通讯股份有限公司资深技术预研工程师；从事 IMS、LTE、5G 安全方面的标准预研和产品研发工作；参与多项国际技术标准的制定；拥有发明专利和标准提案数十项。

闫新成，中兴通讯股份有限公司网络安全首席系统架构专家、移动网络与移动多媒体技术国家重点实验室未来网络研究中心副主任，教授级高工；从事电信行业 20 年，曾主持国家科技重大专项 5G 安全课题；获得多项科技奖励，拥有专利 40 余项。