基于Lowe分类法的5G网络EAP-AKA′协议安全性分析

刘彩霞 胡鑫鑫* 刘树新 游 伟 赵 宇
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：移动网鉴权认证协议攻击不断涌现，针对5G网络新协议EAP-AKA′，该文提出一种基于Lowe分类法的EAP-AKA′安全性分析模型。首先对5G网络协议EAP-AKA′、信道及攻击者进行形式化建模。然后对Lowe鉴权性质进行形式化描述，利用TAMARIN证明器分析协议中安全锚点密钥K_{SEAF}的Lowe鉴权性质、完美前向保密性、机密性等安全目标，发现了3GPP隐式鉴权方式下的4条攻击路径。最后针对发现的安全问题提出2种改进方案并验证其有效性，并将5G网络两种鉴权协议EAP-AKA′和5G AKA的安全性进行了对比，发现前者在Lowe鉴权性质方面更安全。

关键词：网络安全；安全锚点密钥；EAP-AKA′；Lowe分类法；Dolev-Yao敌手模型；TAMARIN
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)08-1800-08
DOI: 10.11999/JEIT190063

Security Analysis of 5G Network EAP-AKA′ Protocol Based on Lowe's Taxonomy

LIU Caixia HU Xinxin LIU Shuxin YOU Wei ZHAO Yu
(*National Digital Switching System Engineering & Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: Mobile network authentication protocol attacks continue to emerge. For the new 5G network protocol EAP-AKA', an EAP-AKA' security analysis method based on Lowe's taxonomy is proposed. Firstly, 5G network, EAP-AKA', communication channel and adversary are formally modeled. Then Lowe authentication property is formally modeled. Using the TAMARIN prover, objectives of the security anchor key K_{SEAF} are analyzed, such as Lowe's taxonomy, perfect forward secrecy, confidentiality, etc. Four attack paths under 3GPP implicit authentication mode are discovered. Two improved schemes are proposed for the discovered security problems and their security is verified. Finally, the security of the two authentication protocols EAP-AKA' and 5G AKA of the 5G network is compared, and it is found that the former is safer in terms of Lowe authentication property.

Key words: Network security; Security anchor key; EAP-AKA′; Lowe's taxonomy; Dolev-Yao adversary model; TAMARIN

1 引言

随着移动通信网络不断演进，第5代移动通信系统(5G)逐渐开始商用。5G将开启万物互联时代，其典型应用场景将覆盖远程医疗、无人驾驶、智能家居等诸多领域。5G依靠庞大复杂的协议体系支撑网络运行，而通信协议设计中不可避免地存在安全缺陷或漏洞，若这些缺陷被攻击者利用来发起网络攻击(如跟踪用户位置[1]、拒绝服务[2]等)，则会严重威胁个人隐私、财产安全甚至国家安全。

5G网络标准考虑了诸多安全问题，如防范假冒、重放、降级、中间人攻击，增强运营商网络边界防护等，但相关安全需求是否在协议设计中都得到满足还尚待验证。鉴权认证和密钥协商(Authentication and Key Agreement, AKA)协议能够使协议参与方在开放、不安全的信道中完成密钥协商和相互认证，该协议被广泛运用到移动通信网中，因此其安全性备受学者关注。在以往移动通信系统中，针对鉴权认证和密钥协商协议的攻击层出不穷[3,4]。随着协议本身愈加复杂及攻击者攻击能力(如转发、

收稿日期：2019-01-23；改回日期：2019-05-19；网络出版：2019-05-27
*通信作者： 胡鑫鑫 justinhu@hust.edu.cn
基金项目：国家自然科学创新研究群体基金(61521003)，国家自然科学基金(61801515)
Foundation Items: The National Natural Science Fund for Innovative Research Groups (61521003), The National Natural Science Foundation of China (61801515)

篡改、伪造等)不断提高，协议中存在的安全漏洞已很难被人工识别。为高效地发现协议设计缺陷，研究人员开始使用形式化方法分析安全协议中潜在安全问题。Arapinis等人[1]利用ProVerif工具分析了3G AKA协议，并发现了利用该协议漏洞探测用户位置的链接性攻击。Hussain等人[2]利用ProVerif和NuSMV工具分析了LTE网络，发现了利用EPS AKA协议的同步机制发起的DoS攻击以及用户位置可链接性攻击。Rupprecht等人[5]分析了LTE鉴权协议和寻呼流程的数据链路层漏洞，借此实现了用户位置窃取和IMSI破解，并重定向用户访问网络的DNS(Domain Name System)服务器地址。Shaik等人[6]分析了LTE系统利用EPS AKA加密的NAS(Non-Access Stratum)层和RRC(Radio Resource Control)层信令，发现了用户位置跟踪攻击和DoS攻击。Hussain等人[7]分析了5G 网络寻呼流程，发现了一种可以将用户电话号码同其IMSI链接起来的攻击。Ravishankar等人[8]分析了5G AKA协议，发现了一种利用SQN参数的异或计算机制来破解SQN真实值的方法。Basin等人[9]利用TAMARIN工具分析了5G AKA协议，发现5G AKA协议在Lowe鉴权安全性质上的一些缺陷。Adrien[10]探讨了5G AKA协议的可链接性问题，并用σ-不可链接性形式化地分析了其改进5G AKA协议的不可链接性。Ferrag等人[11]较为全面地梳理了4G和5G网络中同鉴权认证相关的安全问题，并对相应安全问题的解决方案进行了汇总。Rupprecht等人[12]立足以往移动通信网安全问题的研究成果，将5G网络安全问题的根源归结为以标准缺陷为主的4大类问题，在标准缺陷问题中，最严重的就是协议参与方不存在双向鉴权及鉴权信令未加防护。此外，文献[13]对5G网络面临的安全问题进行全面梳理后，提出5G安全架构并将内生安全运用到5G网络中。

当前针对移动网协议安全性研究主要集中在3G AKA，EPS AKA和5G AKA等协议，而对于5G系统新引入的协议EAP-AKA′研究较少。3GPP标准也并未对EAP-AKA′协议中安全锚点密钥K_{SEAF}提出安全性要求，因此其安全性有待验证。分析方法上，以往的形式化方法缺乏对鉴权协议安全性质的精确描述。分析工具上，以往的证明工具如ProVerif, AVISPA, Scyther等不支持异或运算、非单调全局状态等功能。针对上述问题，本文首先对5G鉴权认证协议EAP-AKA′进行多集重写，然后利用Lowe分类法建立协议安全分析模型，本模型既能够精确衡量EAP-AKA′协议的Lowe鉴权属性，还能验证机密性、完美前向保密性等安全性质。借助TAMARIN自动证明器，自动化地分析了EAP-AKA′协议，发现了该协议的4个缺陷。最后根据所发现问题提出了2种修复方案，并在本模型下进行了验证。

2　5G系统及鉴权认证协议简介

2.1　相关概念

根据密钥协商完成后协议参与方是否及时确认协商密钥可将鉴权协议分为隐式鉴权和显式鉴权。

定义 1　隐式鉴权(implicit authentication)是指通过在鉴权之后流程中成功使用由认证和密钥协商协议产生的密钥来间接提供认证的鉴权方式。

协议参与方并未在密钥协商完成后立即相互确认，而是通过随后其他流程的正常运行来间接确认。如在5G注册流程中，UE和SN完成鉴权认证后还要执行SMC流程，该流程使用了鉴权过程中协商的安全锚点密钥K_{SEAF}，但该流程并非鉴权协议的一部分。

定义 2　显式鉴权(explicit authentication)是指通过在认证和密钥协议中相互确认产生的密钥来直接提供认证的鉴权方式。

2.2　5G系统概述

5G网络引入了诸多新技术，如：大规模MIMO、网络功能虚拟化[14]、HTTP/2, EAP-AKA′等。这些新技术也对5G网络安全提出了新的挑战，因此，3GPP对5G安全架构进行了重新设计，给出了更加苛刻的安全标准，并重新定义了5G的安全域。

相比非漫游场景，漫游场景增加了服务网络SN，能够更加全面地分析移动通信网安全状况，故本文采用漫游场景。图1描述了漫游场景下5G网络信任模型，将5G网络分为3部分：用户设备UE、服务网络SN和归属地网络HN。从内到外信任程度逐渐降低，每层之间均需新密钥进行通信，即分层密钥体系。服务网络和归属地网络边界均有安全边界防护代理SEPP，各自SEPP经IPX网络连接起来。

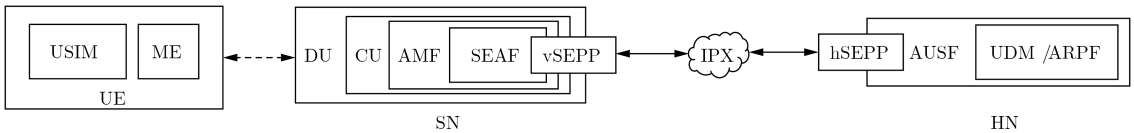

图 1 5G网络漫游场景下的信任模型

UE：用户设备UE由USIM卡和移动设备ME组成，USIM中存储有SUPI, SUPI是5G网络用户永久身份标识。此外，为防止SUPI在空口泄漏，5G网络采用非对称密钥来加密SUPI，除紧急情况，空口仅传SUPI加密版本——加密身份标识(SUbscription Concealed Identifier, SUCI)。鉴权认证过程由UE发起，UE和SN通过空中信道进行通信。

SN：服务网络SN的信任模型从内到外依次是安全锚点功能SEAF、接入和移动性管理功能AMF、中心单元CU和分布单元DU, CU和DU共同组成5G网络基站gNB。SN负责对漫游用户的无线接入，SN和归属地网络相互配合完成用户鉴权认证。

HN：归属地网络HN的信任模型从内到外依次是统一数据管理UDM和鉴权证书库与处理功能ARPF、鉴权服务功能AUSF，其中UDM和ARPF是归属地网络的核心机密区，ARPF同用户USIM卡一样存储着用户鉴权所需根密钥等关键信息，UDM利用用户信息来实现一些应用逻辑，比如鉴权密钥产生、用户身份管理等。

2.3 EAP-AKA′协议

如图2所示，EAP-AKA′协议鉴权分为两个阶段，阶段1是鉴权初始准备阶段，阶段2是网络侧与UE相互鉴权。在阶段1, UE利用网络侧公钥将SUPI加密为SUCI, SUCI=<aenc(<SUPI, R>, PK_{HN}), id_{HN}>, UE发送包含SUCI或者5G-GUTI的注册请求消息给SEAF。收到该消息后，SEAF发送鉴权请求给AUSF，该请求中包含SNN, SUPI或者SUCI。收到请求后的AUSF首先检验SEAF的合法性，防止攻击者伪造SN，随后AUSF将消息传送到UDM/ARPF/SIDF中，触发用户标识解密功能SIDF解密SUCI得到SUPI, UDM/ARPF利用解密得到的SUPI和用户数据来选择鉴权方式。在阶段2，根据阶段1选择的鉴权方式，UDM/ARPF计算鉴权参数并将产生的鉴权向量**AV** (R, AUTN, XRES, CK′, IK′)发送给AUSF，随后AUSF将R, SNN, AUTN以及其他的加密消息(AT_MAC)发送给SEAF, SEAF将这一消息经过gNB发送给UE, UE对消息进行MAC校验后计算出响应消息并经SEAF发送给AUSF, AUSF进行校验后将K_{SEAF}和用户SUPI发送给SEAF, SEAF将这一消息传给UE。

3 基于Lowe分类法的EAP-AKA′协议安全性分析模型

针对5G网络中鉴权认证协议的安全性，3GPP提出了一些定性的安全需求(如机密性)，但这些需求并未得到严格的逻辑证明。尤其作为新引入的EAP-AKA′协议，其在5G网络中的安全性更应得到充分论证。形式化方法能有效利用数学或逻辑模型来分析系统及其条件，从而能够验证系统在满足条件情况下所得的证明是否正确。但以往缺乏对鉴权协议安全性的精确刻画，而Lowe鉴权分类法恰能满足。此外，为合理刻画攻击者行为，本文将Dolev-Yao敌手模型引入协议分析系统中。综上，本文将Lowe分类法、Dolev-Yao敌手模型与形式化分析方法相结合，提出一种基于Lowe分类法的EAP-AKA′协议形式化分析模型。整个模型如图3所示，下面分别介绍。

3.1 协议形式化描述

描述之前，首先给出本文中所用符号及其意义，如表1中所示。

自然语言描述的EAP-AKA′协议如2.3节所述，为了使协议便于自动化分析，需要将协议及参与方描述成状态转移系统。在建立状态转移系统时，需要分析协议运行过程中各个角色的有限种状态、状

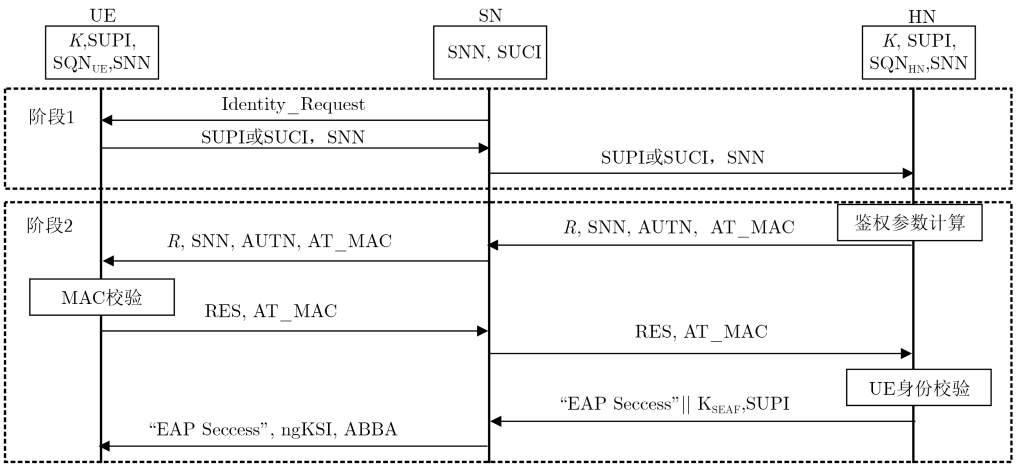

图 2 5G网络EAP-AKA'协议鉴权流程

态转移触发条件、触发后动作等，本文使用安全协议理论语言(spthy)来描述协议状态转移过程。如在EAP-AKA′协议鉴权阶段1当中，处于初始状态的SN(St_SN_0)向UE发出身份请求后，SN会转变成等待接收SUCI/SUPI的状态(St_SN_1)，这一状态转换用spthy语言描述如表2所示。UE, SN, HN在整个EAP-AKA′协议流程中共有21个状态(UE 6个，SN 10个，HN 5个)。

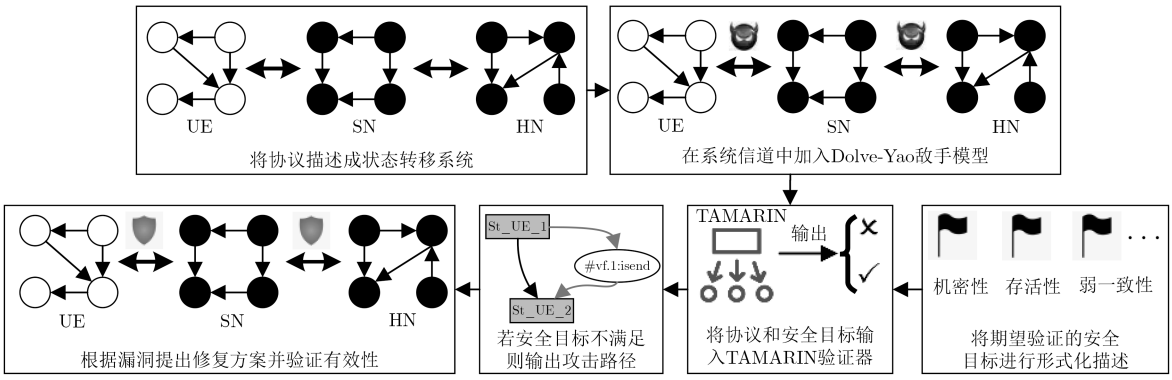

图 3 基于Lowe分类法的EAP-AKA′协议安全分析模型

表 1　符号说明

符号	定义
Create(A, id, R)	对编号为id的角色A创建一个事件
Claim_type(A, t)	角色A在时刻t声明一个事件
Honest(A)	角色A不被攻击者感染
Reveal(A)	角色A被攻击者感染
$K(t)$	攻击者获取了传递的信息
F@i	在时刻i发生事件F
$\#i<\#j$	时刻i早于时刻j
$\#i=\#j$	时刻i与时刻j相同
$x=y$	消息变量x, y相等

表 2　用spthy语言描述协议状态转移

```
rule SN_1send:
let m = 'Identity Request'
in [ St_SN_0($SN, ~id, $HN, SK) ]
--[ Send($SN, m)]->
[ Out(m), St_SN_1($SN, ~id, $HN, SK)]
```

3.2　攻击者模型

进行协议安全性分析时常用的敌手模型有两种：eCK敌手模型和Dolev-Yao敌手模型[15]。eCK是一种较强的安全模型，在该模型中敌手能够获取协议参与方的临时私钥，这使得在eCK敌手模型下协议具有极高的安全保证。然而eCK在协议执行过程中使用双线性映射，其计算效率有待提高；另一方面，在移动通信网鉴权认证场景下，尚未发现攻击者能够获取协议临时密钥的情况。因此本文使用Dolev-Yao敌手模型对攻击者建模，该敌手具有以下安全能力：

(1) 攻击者可以嗅探无线公共信道中传输的消息而不被协议参与实体察觉，形式化建模为：[Out(x)]→[$K(x)$], [Fr(x)]→[$K(x)$]。

(2) 攻击者可以随意丢弃、修改任何在无线公共信道中传输的消息，形式化建模为：[!KU(x)]--[$K(x)$]→[In(x)]。

(3) 攻击者可以模仿一个合法协议参与实体，并以该实体的身份在无线公共信道中注入消息，同其他合法实体交互而不被察觉, 形式化建模为：[$K(x)$]→[In(x)]。

(4) 攻击者遵守所有加密假设，即攻击者只有在掌握密钥的前提下才能解密消息，不可暴力破解密文。

以上能力使得攻击者既可发起被动攻击，亦可发起主动攻击。在实际中，攻击者只需一个USRP设备及相应的抓包工具就能解码空口传播的消息，实现攻击能力(1)，攻击者通过USRP设备装载5G NR协议栈就可构造伪基站，实现攻击能力(2)和(3), 5G NR协议栈是符合加密假设的，故能力(4)得到了保证。

3.3　安全目标建模

Lowe鉴权分类法可将鉴权协议安全性质进行精确分类[16]，其将鉴权协议安全性质从低到高分为4类：存活性、弱一致性、非单射一致性、单射一致性。同时作为鉴权认证协议，EAP-AKA′还须满足完美前向保密、机密性。存活性是鉴权协议的最低级属性，其确保协议参与双方均支持指定协议。弱一致性是为防范伪造身份攻击，故每次协议运行都须保证参与方身份真实。非单射一致性是为防止消息篡改攻击，故每次协议运行的消息都须是真实

参与方产生的。单射一致性是为防止重放攻击，故每次协议运行均需加入随机值，协议运行的消息中应包含此随机值。对上述6个安全目标形式化表述如图4所示。

$$\forall a\ b\ \#i.\ \text{Claim\_commit}(a, b, \langle\rangle)@i \Rightarrow (\exists \text{id}\ R\#j.\ \text{Create}(b, \text{id}, R)@j) \vee (\exists X\ r.\ \text{Reveal}(X)@r \wedge \text{Honest}(X)@i)$$

$$\forall a\ b\ \#i.\ \text{Claim\_commit}(a, b, \langle\rangle)@i \Rightarrow (\exists \#j.\ \text{Claim\_running}(b, a, \langle\rangle)@j) \vee (\exists X\ r.\ \text{Reveal}(X)@r \wedge \text{Honest}(X)@i)$$

$$\forall a\ b\ \text{R1 R2}\ t\ \#i.\ \text{Claim\_commit}(a, b, \langle \text{R1, R2}, t\rangle)@i \Rightarrow (\exists \#j.\ \text{Claim\_running}(b, a, \langle \text{R1, R2}, t\rangle)@j) \vee (\exists X\ r.\ \text{Reveal}(X)@r \wedge \text{Honest}(X)@i)$$

$$\forall a\ b\ \text{R1 R2}\ t\ \#i.\ \text{Claim\_commit}(a, b, \langle \text{R1, R2}, t\rangle)@i \Rightarrow (\exists \#j.\ \text{Claim\_running}(b, a, \langle \text{R1, R2}, t\rangle)@j \wedge \neg(\exists \text{a2 b2}\ \#i2.\ \text{Claim\_commit}(\text{a2, b2}, \langle \text{R1, R2}, t\rangle)@\text{i2} \wedge \neg(\text{i2} = i))) \vee (\exists X\ \#r.\ \text{Reveal}(X)@r \wedge \text{Honest}(X)@i)$$

$$\forall A\ M\ i.\ \text{Claim\_secret}(A, M)@i \Rightarrow \neg(\exists j.\ K(M)@j) \vee (\exists B\ k.\text{Reveal}(B)@k \wedge \text{Honest}(b)@i \wedge k < i)$$

$$\forall A\ M\ i.\ \text{Claim\_secret}(A, M)@i \Rightarrow \neg(\exists j.K(M)@j) \vee (\exists B\ k.\text{Reveal}(B)@k \wedge \text{Honest}(b)@i)$$

图 4 安全目标形式化描述

3.4 信道模型

在5G网络鉴权认证过程涉及两个信道，一个是UE↔SN之间的空中信道，另一个是SN↔HN之间的专有信道。由于空口信令以电磁波的形式传播，任何配备合适天线的接受者均可在基站附近小区接收到信号。因此，被动攻击者可监听消息而不被发现，主动攻击者也可拦截、篡改、注入消息。而专有信道是有线连接的，SN和HN在各自网络边界部署有SEPP，且该信道使用IPSec和TLS保护，理论上是安全的。但实际中，攻击者也可通过收买或其他方式非法控制IPX网络，使得攻击者能嗅探两个公共陆地移动网络(Public Land Mobile Network, PLMN)之间传输的消息，但是由于PLMN会对消息加密，故该信道能够提供消息的机密性和真实性保护。但是攻击者仍可重放截获的消息，或改变消息顺序重新发出，故本模型认为SNHN之间信道可提供真实性和机密性保护，但不能防范重放攻击和更改消息顺序攻击。

3.5 安全目标验证

在验证安全目标时，本模型利用了TAMARIN证明器。TAMARIN证明器是用于安全协议符号建模和分析的强大工具，它将安全协议模型作为输入，指定协议运行代理在不同角色(如：协议发起者、响应者)所采取的操作，然后自动构建证据。即便协议的角色有任意多个实例并行交错，也可以与敌手的动作一起运行，攻击者和协议通过更新网络消息、生成新消息进行交互。TAMARIN使用基于多集重写规则的表达语言来定义协议参与者和攻击者，这些规则定义了一个标记迁移系统，其状态包括敌手知识的符号化表示、网络上的消息、新生成的信息以及协议的状态等。安全属性被建模为跟踪属性，根据转换系统的跟踪进行检查，或根据两个转换系统的观察等效性进行检查。TAMARIN工作原理如图5所示，协议状态及其转换用rules描述，期望验证的安全性质用lemmas描述，将rules和lemmas一起输入TAMARIN，当协议满足相应安全性质时，TAMARIN会输出正确，否则输出错误及攻击路径。

图 5 TAMARIN证明器工作原理

4 实验结果及改进方案

本实验在20核Intel(R)Xeon(R)E5-2640 v4 CPU, 2.4 GHz, 64 G内存服务器上运行，操作系统为CentOS7, TAMARIN版本是1.4.0。因篇幅所限，本文将协议修改前(隐式鉴权)验证结果和修复后(显式鉴权)验证结果在本节一同展示。隐式鉴权和显式鉴权的EAP-AKA′协议共约2000行TAMARIN代码，每一种鉴权方式约40个rule，80个lemma。在上述配置的服务器上验证隐式鉴权方式的EAP-AKA′协议约需4 h，验证显式鉴权方式的EAP-AKA′协议约需5 h。

4.1 EAP-AKA'验证结果及与5G AKA对比

表3显示了EAP-AKA′协议在隐式鉴权和显式鉴权方式下对安全锚点密钥K_{SEAF}的机密性和完美前向保密性的验证结果对比。由实验结果可知，EAP-AKA′能够满足对安全锚点密钥K_{SEAF}机密性，即只有授权用户可以获取K_{SEAF}，这一结果与3GPP的安全需求相吻合。另一方面，无论是隐式鉴权还是显式鉴权，协议均无法满足对安全锚点密

表 3 隐式鉴权和显式鉴权对比(对K_{SEAF}的机密性、完美前向保密性)

协议参与方	UE		SN		HN	
	隐式	显式	隐式	显式	隐式	显式
K_{SEAF}机密性	√	√	√	√	√	√
K_{SEAF}完美前向保密性	×	×	×	×	×	×

钥K_{SEAF}的完美前向保密性，这一结果实际上印证了3GPP TS 33.501[17]中提出的密钥体系，长期密钥K是所有密钥的根密钥，该密钥存储在HN和USIM卡中，一旦攻击者知晓了K，则密钥体系中的所有密钥(包括安全锚点密钥K_{SEAF})都对攻击者透明，因此EAP-AKA′协议无法实现对密钥K_{SEAF}的完美前向保密性。

表4展示了隐式鉴权方式下本文对EAP-AKA′ Lowe鉴权性质分析结果，以及EAP-AKA′分析结果同Basin等人[9]对5G AKA分析结果对比。可见对采用隐式鉴权方式的EAP-AKA′而言，UE对SN就安全锚点密钥K_{SEAF}不能满足非单射一致性、单射一致性。3GPP要求UE, SN, HN满足对SUPI, SNN等数据的鉴权安全性需求，但并未给出对安全锚点密钥K_{SEAF}的鉴权安全性需求，而在实际中，上述3个协议角色均需满足对安全锚点密钥K_{SEAF}的鉴权安全性需求，因为鉴权协议需具备防范消息篡改攻击的能力，因此协议角色之间对传输的密钥至少要满足非单射一致性。另外，安全锚点密钥K_{SEAF}必须在每次会话中都不相同，以防攻击者发起重放攻击，故UE, SN, HN要满足对安全锚点密钥K_{SEAF}的单射一致性鉴权属性。即便如此，EAP-AKA′协议也比5G AKA安全很多，5G AKA在所有协议运行角色中最高只满足弱一致性，EAP-AKA′仅在UE对SN方向上不满足非单射一致性，其余方向上均满足单射一致性。直观分析造成这一结果的原因，TS33.501[17]对EAP-AKA′和5G AKA两种鉴权协议的鉴权向量**AV**定义有所不同，EAP-AKA′的**AV**包含完整性密钥IK′和机密性密钥CK′，而CK′=KDF(CK, SNN)，IK′=KDF(IK, SNN)，SNN=<“5G”, SNid>，故K_{SEAF}的推导同SNid有关，该SNid会随**AV**从HN传送到SN再到UE，该协议可以就K_{SEAF}满足非单射一致性；5G AKA的鉴权向量中没有加密参数同SNid相关，虽然K_{SEAF}=KeySeed′(K, R, SQN_{HN}, SNN, SUPI)包含在5G AKA的**AV**中，但是包含SNN的K_{SEAF}仅从HN到达SN，因此5G AKA协议的各个参与角色无法就K_{SEAF}满足较高层次的Lowe鉴权性质。

类似地，表5展示了在采用显式鉴权方式时本文对EAP-AKA′分析结果，以及EAP-AKA′分析结果同Basin等人[9]对5G AKA分析结果对比。可见采用显式鉴权之后，EAP-AKA′和5G AKA的Lowe鉴权安全性均得到提升，只有5G AKA无法满足HN对UE的非单射一致性，这是由于HN无法收到来自UE的SNid信息，从而无法就K_{SEAF}满足非单射一致性。

4.2 EAP-AKA′安全性改进方案

如前所述，3GPP采用隐式鉴权，由4.1节实验结果可知，隐式鉴权无论对EAP-AKA′还是5G AKA而言均不安全。若要满足3GPP期望安全性，鉴权认证协议需运行在特定安全上下文中，同时要保证该过程不会被攻击者打断(尤其在空口信道)，这在实际环境中很难满足。此外，采用隐式鉴权方式，很大程度上把5G网络鉴权协议安全性寄托在后续其他流程的密钥往返确认上，而5G网络协议体系又极为复杂，验证所有后续流程又是一项繁重的工作，很难保证在鉴权协议后的其他所有流程均包含密钥往返确认过程。况且5G网络后续演进过程中，很可能会增加其他流程，这些流程也不一定具备密钥往返确认，这实际上为5G网络埋下了安

表 4　EAP-AKA′和5G AKA对比(隐式鉴权)

协议参与方	UE对SN		UE对HN		SN对UE		HN对UE	
	EAP-AKA′	5G AKA	EAP-AKA′	5G AKA	EAP-AKA′	5G AKA	EAP-AKA′	5G AKA
存活性	√	×	√	√	√	√	√	√
弱一致性	√	×	√	√	√	×	√	√
非单射一致性	×	×	√	×	√	×	√	×
单射一致性	×	×	√	×	√	×	√	×

表 5　EAP-AKA′和5G AKA对比(显式鉴权)

协议参与方	UE对SN		UE对HN		SN对UE		HN对UE	
	EAP-AKA′	5G AKA	EAP-AKA′	5G AKA	EAP-AKA′	5G AKA	EAP-AKA′	5G AKA
存活性	√	√	√	√	√	√	√	√
弱一致性	√	√	√	√	√	√	√	√
非单射一致性	√	√	√	√	√	√	√	×
单射一致性	√	√	√	√	√	√	√	×

全隐患。因此，针对上述已发现和潜在安全问题，本文对EAP-AKA′协议提供两种修复方案，如图6所示。

第1种方案改进MAC计算方式。由4.1节分析可知，因SNN信息无法从SN到达UE而导致UE无法满足弱一致性，故可将MAC计算方式改为如表6所示。

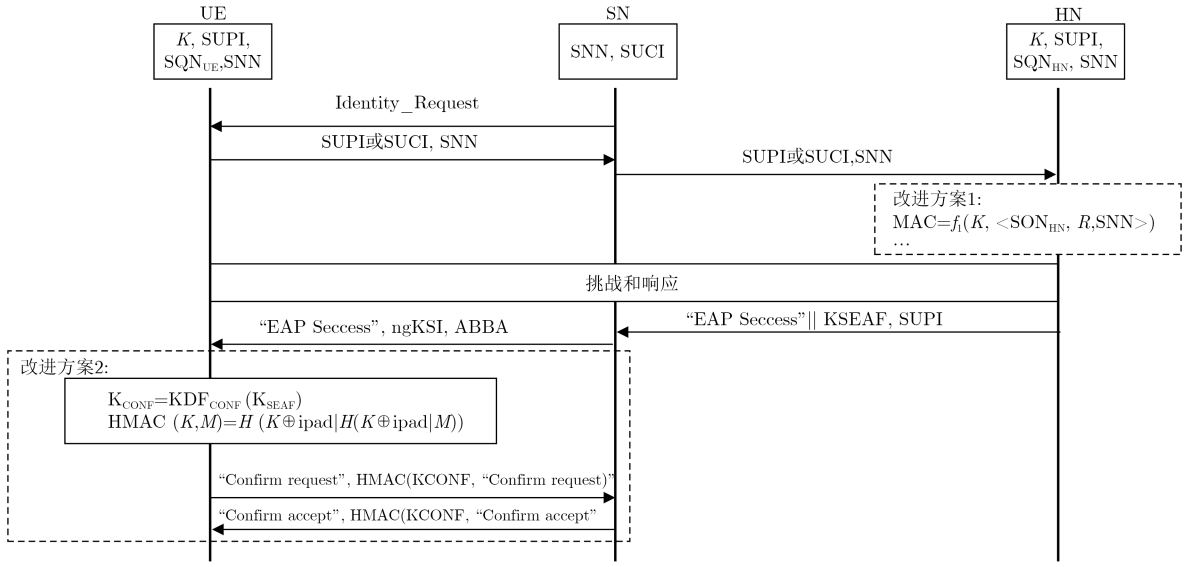

图 6 两种改进方案

表 6 改进MAC计算方式

MAC=$f_1(K, <\mathrm{SQN_{HN}}, R, \mathrm{SNN}>)$
故AUTN=<CONC, $f_1(K, \mathrm{MAC})$>
=< $\mathrm{SQN_{HN}} \oplus \mathrm{AK}$, $f_1(K, <\mathrm{SQN_{HN}}, R, \mathrm{SNN}>)$>
=< $\mathrm{SQN_{HN}} \oplus f_5(K, R)$, $f_1(K, <\mathrm{SQN_{HN}}, R, \mathrm{SNN}>)$>
=$\mathrm{KDF_{AUTN}}(\mathrm{SQN_{HN}}, K, R, \mathrm{SNN})$

第2种方案是将鉴权方式由隐式改为显式，即在协议阶段2末尾增加UE和SN的相互确认消息：

SN→UE:<ConfirmSN>=< “Confirm request”, $\mathrm{HMAC}(\mathrm{K_{CONF}}$, “Confirm request”)>

UE→SN:<ConfirmUE>=< “Confirm accept”, $\mathrm{HMAC}(\mathrm{K_{CONF}}$, “Confirm accept”)>

其中, $\mathrm{K_{CONF}}=\mathrm{KDF_{CONF}}(\mathrm{K_{SEAF}})$, $\mathrm{KDF_{CONF}}(\cdot)$函数为新引入的密钥推导函数。$\mathrm{HMAC}(K, M)=H(K\oplus \mathrm{opad}|H(K\oplus \mathrm{ipad}|M))$, $H(\cdot)$函数可采用SHA-256等哈希算法，M表示哈希算法输入信息，K表示认证密钥。

上述两种修复方案修复后的EAP-AKA′协议安全性验证结果如表4中显式验证结果所示，可见修复方案能够满足UE, SN, HN对$\mathrm{K_{SEAF}}$的单射一致性需求，从而可使5G网络中的EAP-AKA′协议免受上文所述安全威胁。

5 结束语

本文针对5G网络新协议EAP-AKA′的安全性，提出了基于Lowe分类法的EAP-AKA′协议安全性分析模型，探讨了其对安全锚点密钥$\mathrm{K_{SEAF}}$的安全性。分析发现标准中所采用的隐式鉴权方式存在4个安全缺陷，针对缺陷提出2种解决方案并做出验证。将EAP-AKA′和5G AKA对比后，发现前者安全性更高。

后续工作还可进一步提高模型精确性，如使用异或运算对SQN进行精确建模以便分析同步相关问题；另一方面还可以扩展EAP-AKA′协议的验证面，如分析该协议对SUPI, SQN, SNN的Lowe鉴权性质。

参 考 文 献

[1] ARAPINIS M, MANCINI L, RITTER E, *et al*. New privacy issues in mobile telephony: Fix and verification[C]. Proceedings of 2012 ACM Conference on Computer and Communications Security, Raleigh, North Carolina, USA, 2012: 205–216. doi: 10.1145/2382196.2382221.

[2] HUSSAIN S R, CHOWDHURY O, MEHNAZ S, *et al*. LTEInspector: A systematic approach for adversarial testing of 4G LTE[C]. Network and Distributed Systems Security (NDSS), San Diego, California, USA, 2018. doi: 10.14722/ndss.2018.23313.

[3] BORGAONKAR R, HIRSHI L, PARK S, *et al*. New adventures in spying 3G & 4G users: Locate, track, monitor [EB/OL]. https://www.blackhat.com/docs/us-17/wednesday/us-17-Borgaonkar-New-Adventures-In-Spying-3G-And-4G-Users-Locate-Track-And-Monitor.pdf, 2017.

[4] ZHANG Muxiang and FANG Yuguang. Security analysis and enhancements of 3GPP authentication and key agreement protocol[J]. *IEEE Transactions on Wireless Communications*, 2005, 4(2): 734–742. doi: 10.1109/twc.2004.842941.

[5] RUPPRECHT D, KOHLS K, HOLZ T, *et al*. Breaking LTE on layer two[C]. The 40th IEEE Symposium on Security and Privacy, San Francisco, USA, 2019.

[6] SHAIK A, BORGAONKAR R, SEIFERT J P, *et al*. Practical attacks against privacy and availability in 4G/LTE[C]. The 23nd Annual Network and Distributed System Security (NDSS), San Diego, California, USA, 2016. doi: 10.14722/ndss.2016.23236.

[7] HUSSAIN S R, ECHEVERRIA M, CHOWDHURY O, *et al*. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information[C]. The 23nd Annual Network and Distributed System Security (NDSS), San Diego, California, USA, 2019. doi: 10.14722/ndss.2019.23442.

[8] RAVISHANKAR B, LUCCA H, SHINJO P, *et al*. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols[C]. Privacy Enhancing Technologies, Stockholm, Sweden, 2019.

[9] BASIN D, DREIER J, HIRSCHI L, *et al*. A formal analysis of 5G authentication[C]. 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018: 1383–1396. doi: 10.1145/3243734.3243846.

[10] KOUTSOS A. The 5G-AKA authentication protocol privacy[EB/OL]. https://arxiv.org/pdf/1811.06922.pdf, 2019.

[11] FERRAG M A, MAGLARAS L, ARGYRIOU A, *et al*. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes[J]. *Journal of Network and Computer Applications*, 2018, 101: 55–82. doi: 10.1016/j.jnca.2017.10.017.

[12] RUPPRECHT D, DABROWSKI A, HOLZ T, *et al*. On security research towards future mobile network generations[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(3): 2518–2542. doi: 10.1109/COMST.2018.2820728.

[13] JI Xinsheng, HUANG Kaizhi, JIN Liang, *et al*. Overview of 5G security technology[J]. *Science China Information Sciences*, 2018, 61(8): 081301. doi: 10.1007/s11432-017-9426-4.

[14] 刘彩霞, 李凌书, 汤红波, 等. 基于子图同构的vEPC虚拟网络分层协同映射算法[J]. 电子与信息学报, 2017, 39(5): 1170–1177. doi: 10.11999/JEIT160642.
LIU Caixia, LI Lingshu, TANG Hongbo, *et al*. Hierarchical coordination strategy for vEPC virtual network embedding based on subgraph isomorphism[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1170–1177. doi: 10.11999/JEIT160642.

[15] DOLEV D and YAO A. On the security of public key protocols[J]. *IEEE Transactions on Information Theory*, 1983, 29(2): 198–208. doi: 10.1109/TIT.1983.1056650.

[16] LOWE G. A hierarchy of authentication specifications[C]. The 10th Computer Security Foundations Workshop, Rockport, USA, 1997: 31–43. doi: 10.1109/CSFW.1997.596782.

[17] 3GPP. 3GPP TS 33.501 Security architecture and procedures for 5G system (Release 15)[S].Nice: 3GPP, 2018.

刘彩霞：女，1974年生，教授，博士生导师，研究方向为移动通信网络、新型网络体系结构.

胡鑫鑫：男，1994年生，硕士生，研究方向为5G 网络安全、新一代移动通信技术.

刘树新：男，1987年生，博士，讲师，研究方向为复杂网络、网络信息挖掘.

游　伟：男，1984年生，博士，讲师，研究方向为密码学、移动通信网络.

赵　宇：男，1984年生，博士，讲师，研究方向为移动通信网络安全、新型网络体系结构.