

5G 移动边缘计算场景下的快速切换认证方案

张伟成, 卫红权, 刘树新, 普黎明

(信息工程大学, 河南 郑州 450001)

摘要: 5G 万物互联为用户带来极致网络体验的同时也提出了新的挑战, 用户的超低时延体验、移动状态下无顿感的获取业务以及安全防护问题备受关注。移动边缘计算能够满足 5G 低时延、大连接、高带宽的严苛要求, 作为一种多信任域共存的计算范式, 多实体之间、跨信任域之间互联互通频繁, 身份认证作为安全防护的第一道关口尤为重要。通过对现有边缘计算范式下的身份认证机制研究, 提出了一种通过构建信任域的基于预认证的轻量级快速切换认证方案, 不同区域间移动的用户能实现快速安全的切换认证。所提方案将服务和计算由云端下沉到边缘侧, 生物指纹技术被用于用户端以抵御终端被盗攻击, 不同区域的边缘服务器采用预认证的方式来满足快速切换需求, 用户与边缘服务器采用实时协商共享会话密钥的方式建立安全通道, 认证方案以异或和哈希运算来保证轻量级。对所提方案从安全性与性能两方面进行评估, 其中, 安全性从理论设计分析和形式化工具验证两方面进行。采用形式化分析工具 AVISPA 验证了在存在入侵者的情况下所提方案的安全性, 与其他方案相比所提方案更安全。性能主要从认证方案的计算成本和通信成本进行评估, 仿真表明, 所提方案在通信成本上有较好的优势, 计算开销能够满足资源受限的移动终端用户需求。后续需要从两方面对方案进行改进, 一是要加强方案可扩展性的改进以确保用户及边缘服务器能随时加入退出。二是要加强方案普适性的改进以满足第三方服务商的接入部署。

关键词: 移动边缘计算; 切换认证; 服务下沉; 隐私保护; AVISPA

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022034

Fast handover authentication scheme in 5G mobile edge computing scenarios

ZHANG Weicheng, WEI Hongquan, LIU Shuxin, PU Liming

Information Engineering University, Zhengzhou 450001, China

Abstract: The 5G internet of things brings the ultimate experience to users, but it also puts forward new challenges.

收稿日期: 2020-12-11; 修回日期: 2021-02-12

通信作者: 张伟成, Qwechily@qq.com

基金项目: 国家自然科学基金 (61803384)

Foundation Item: The National Natural Science Foundation of China (61803384)

引用格式: 张伟成, 卫红权, 刘树新, 等. 5G 移动边缘计算场景下的快速切换认证方案[J]. 网络与信息安全学报, 2022, 8(3): 154-168.

Citation Format: ZHANG W C, WEI H Q, LIU S X, et al. Fast handover authentication scheme in 5G mobile edge computing scenarios[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 154-168.

Users' requirements of ultra-low latency experience, access to business without sense during movement and security guarantee have attracted much attention. Mobile edge computing can meet the strict requirements of 5G with low latency, large connection and high bandwidth. As a computing paradigm with the coexistence of multi-trust domains, multi-entities and cross-trust domains are interconnected frequently. Identity authentication is particularly important for security protection. Through the research on the identity authentication mechanism under the existing edge computing paradigm, a lightweight fast handover authentication scheme based on pre-authentication was proposed. The proposed solution moved services and calculations from the cloud to the edge. Biometric fingerprint technology was used on the client side to defend against terminal theft attacks. Edge servers in different regions used pre-authentication scheme to meet fast switching requirements. The user and the edge server established a secure channel by negotiating a shared session key in real time, and the authentication scheme ensured lightweight operation with XOR and hash operation. The proposed scheme was evaluated from two aspects of security and performance. Theoretical design analysis and formal tool verification were carried out for security evaluation. The formal analysis tool, AVISPA, was used to verify the improved security of the proposed scheme in the presence of intruders. The performance was mainly evaluated from the computing cost and communication cost of the authentication scheme. The simulation results showed that the proposed scheme reduces communication cost, and the computational overhead can meet the needs of mobile terminals with limited resources. As the future work, the scheme will be improved from two aspects: one is to strengthen the scalability to ensure that users and edge servers can join and exit at any time, and the other one is to strengthen the universality of the scheme to meet the access deployment of third-party service providers.

Keywords: mobile edge computing, handover authentication, service sinking, privacy protection, AVISPA

0 引言

5G 时代的到来为用户带来了极致网络体验, 移动边缘计算 (MEC, mobile edge computing)^[1] 作为 5G 网络的关键技术之一, 在整体性、可扩展性、时延、自动化方面能够满足 5G 的要求^[2]。欧洲电信标准协会 (ETSI, European Telecommunications Standards Institute)^[3] 将 MEC 定义为“在网络边缘为应用程序开发人员和内容提供商提供 IT 服务环境和云计算能力”。ETSI 强调靠近用户, 旨在降低服务交付等待时延, 减少网络操作次数, 提高业务分发传送能力, 改善用户最终体验。文献[4]表明由于 MEC 服务器与用户端之间的距离比用户端与云服务器之间的距离短, 因此在传输时延方面, MEC 服务架构要明显优于云服务架构。引入 MEC 能够获得更佳灵活的服务和更高质量的服务体验。文献[5]认为集中式的体系结构可以降低高昂的网络维护成本, 但对前传的带宽要求较高。边缘计算将云计算功能带到网络边缘, 能够减轻回程线路的带宽需求。文献[6]指出时延是 5G/6G 中一个重要的性能指标, 若将

移动服务通过无线连接的 Internet 路由传输到远程服务器进行处理将难以保证低时延, 集成在小区边缘的 MEC 通过网络边缘提供服务能够减少传输时间为本地用户提供低时延服务。

MEC 为 5G 网络带来便利的同时也引出了更多的安全挑战。如何在提供极致体验的同时, 保护敏感数据不被非法边缘设施、非法用户窃取是其中一个重要问题。认证技术是保证终端和网络安全的初始防护手段, 利用认证机制可以从用户端控制恶意行为的发生, 从网络侧防止用户隐私信息的泄露^[7]。

传统的服务获取架构如图 1 所示, 用户终端 (UE, user equipment) 经过基站 (BS, base station)、核心网向云服务提供商发出请求, 云服务提供商根据请求信息, 将服务逐层传递至终端。当用户终端跨区域移动时, 用户终端需要重复上述的请求和传输流程。文献[8]指出传统云计算场景下的身份认证方案, 云服务器负责用户认证的全部计算开销, 且用户在不同管理域内获取服务时需要与云服务器进行重复认证。文献[9]认为传统集中式的认证已经不能满足海量终端的同时接入, 同

时不同功能实体之间的信任问题更加复杂。传统的服务获取方式有以下不足：一方面占用了传输路径上的各级网络资源，另一方面增加了用户终端的服务时延，影响用户的体验。

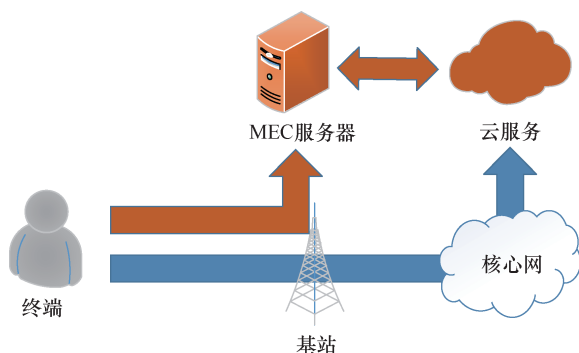


图 1 服务获取架构
Figure 1 The service acquisition architecture

在引入 MEC 服务架构中，MEC 服务器将用户需要的服务内容提前从云服务器进行缓存，MEC 服务器覆盖范围内的用户可以直接从边缘侧获取服务，无须再向云服务器请求。此模式能够有效节省核心网的资源，同时将服务内容下沉到边缘侧，有利于缩短服务响应时延。关于边缘计算范式下身份认证的研究较多地集中在移动云计算^[8]与雾计算^[10]，对 MEC 场景下的身份认证研究较少。文献[11]表明边缘计算是一种多信任域共存的分分布式交互计算系统，每个实体之间、不同信任域之间需要相互认证。适用于不同信任域实体之间的跨域认证以及支持终端设备高移动性的切换认证的研究尚处于起步阶段。文献[12]设计了一种基于位置的轻量级相互身份认证方案，用于解决智慧医院场景下穿戴监测设备的病人在转变区域时，如何快速实现与不同区域 MEC 服务器相互认证的问题，该方案用椭圆曲线密码来保护用户医疗数据，使用 BAN 逻辑 (Burrows-Abadi-Needham logic) 来证明身份认证和密钥建立的安全性，既保证了用户的最终体验，又保证了敏感信息不被窃取。文献[13]提出了一种基于多因素的身份认证方案。该方案要求用户通过网关节点进行自身注册。注册后的用户可以直接连接到传感器节点获取服务。同时该认证方案仅使用单向哈希、感知哈希函数和 XOR 操作，这些运算的计算开销较小且非常适合资源

受限的设备。

综上所述，现有的身份认证虽然能满足可行性、安全性的要求，但直接将上述方案应用在 5G 移动边缘计算场景依旧存在诸多不合理的地方。如文献[8, 10]中认证方案分别适用于移动云计算场景和雾计算场景，运用在 MEC 场景中的扩展性较差。文献[12]使用椭圆曲线密码来保护数据，计算开销较大，且所设计方案不能应对设备被盗攻击。文献[13]虽然保证了轻量级，但不能实现移动中用户的快速切换认证。5G 移动边缘计算场景下的身份认证方案要满足方案轻量级、安全性，同时还需要解决用户在多个 MEC 服务器之间频繁进行移动切换认证的考验。本文在 MEC 服务架构的基础上设计认证方案，结合 MEC “边缘在本地”^[14]的特性，将服务和计算任务下沉到边缘服务器及终端用户侧，同时以构建信任域的方式对用户进行预认证，来降低用户的服务时延。

1 轻量级的身份认证方案

1.1 安全及性能指标

5G 无线网络面临着诸多安全威胁，如终端用户可能受到恶意软件、漏洞攻击；空口传输过程中可能遭受非法窃听、篡改等^[15]。由于 MEC 自身的特性还需满足性能上的要求。因此，5G MEC 架构下的认证方案要同时兼顾安全和性能两方面指标。具体如下。

5GMEC 应用场景需要满足以下安全属性，应对不同的攻击类型^[16-19]。

- 1) 匿名性：用户的身份信息、边缘服务器的设备信息要保持匿名性，从而防止发生仿冒攻击。
- 2) 双向身份认证：网络需要验明用户的合法性，同样用户也需要验明网络的合法性。
- 3) 不可否认性（不可抵赖性）：为了防止收发双方彼此否认，一般采用数字签名、签收机制来应对不可否认性。
- 4) 前向保密：过去的会话密钥与当前的主密钥关联不大，不会因泄露而影响彼此。
- 5) 信息的机密性：信息不能明文传输；加密算法不容易被破解。
- 6) 信息的完整性：接收方接收到的信息要真实可信，未经篡改、伪造、删除，保持信息的完

整性。

7) 信息的新鲜性: 时间戳、同步序列 (SQN, sequence number) 等同步机制能够用于保证信息传输的新鲜性。其中时间戳对接收双方的时间同步要求较高。

需应对的攻击类型如下。

1) 窃听攻击: 攻击者直接获取传输信道上未加密的通信内容。针对加密的通信内容, 攻击者可以采取流量分析等手段来获取敏感数据片段。

2) 仿冒攻击: 攻击者窃取用户真实身份, 假冒合法用户访问边缘网络获取服务。

3) 重放攻击: 攻击者利用截获的请求消息来骗取接收方的响应消息。可通过信息的新鲜性来预防。

4) 中间人攻击: 攻击者充当“中间人”, 悄无声息的窃听两个合法用户的通信, 以延迟、更改、删除通信过程中消息的方式发起攻击, 攻击者并不需要破解传输密钥。

5) 拒绝服务攻击 (DoS, denial of service): 文献[20]指出边缘计算场景中实现身份认证时, 还需考虑在边缘计算下抵御分布式拒绝服务攻击的能力。拒绝服务攻击的本质是阻碍提供服务系统的可用性。攻击者通过非法实体大量消耗系统资源, 从而整个网络瘫痪, 导致合法用户无法正常获取服务。

6) 离线猜测攻击: 在离线模式下, 攻击者可以采取暴力手段破解加密复杂度较低的密码文件。

7) 终端被盗攻击: 当合法用户的终端被攻击者非法获取后, 攻击者一方面可以使用功耗分析攻击来检索存储在被盗智能设备内存中的敏感数据, 另一方面可以冒充合法用户取得网络的信任。

5G MEC 应用场景需要满足以下性能要求。

1) 轻量级: 认证机制在计算成本、通信成本等性能指标上消耗较小, 对边缘设备的配置要求较低, 能满足 MEC 场景下资源受限的特性。

2) 可扩展性: 以 MEC 场景为例, 新的用户、边缘服务器根据需要能够随时加入到 MEC 服务网络中。

1.2 系统架构及参数

传统的身份认证机制需要进行重复的单次认证过程, 无法保证用户在跨区域移动过程中的极致流畅体验。将 MEC 应用于传统的通信网络中, 数据在边缘侧进行处理, 能够极大地降低时延, 缩短用户与服务提供商之间的服务等待时间, 提升用户的服务体验。现有的基于 MEC 架构的身份认证机制, 只是将用户所需服务预缓存至 MEC 服务器上, 认证过程仍然在云端, 边缘服务器仅发挥了本地缓存的作用。本文所设计认证机制的核心思想: 一是将计算任务下沉至用户终端及 MEC 服务器, 这样既减少云服务器处理压力, 又能确保敏感数据在本地处理; 二是服务预缓存, 用户所需服务将提前预缓存到目标边缘服务器上, 以降低服务等待时延、提升用户体验; 三是以构建信任域的方式, 来缩短用户切换认证所需时间。云服务器为根信任域, 它与 MEC 服务器共同构成一级信任域, 经过根信任域认证的 MEC 服务器可加入一级信任域, 经过根信任域认证的用户可以快速接入到一级信任域中的任何一个 MEC 服务器, 不同区域的 MEC 服务器采用预认证来加入信任域。基于预认证的快速切换认证方案的服务构架由三部分组成: 用户、MEC 服务器、云服务器 (如图 2 所示)。

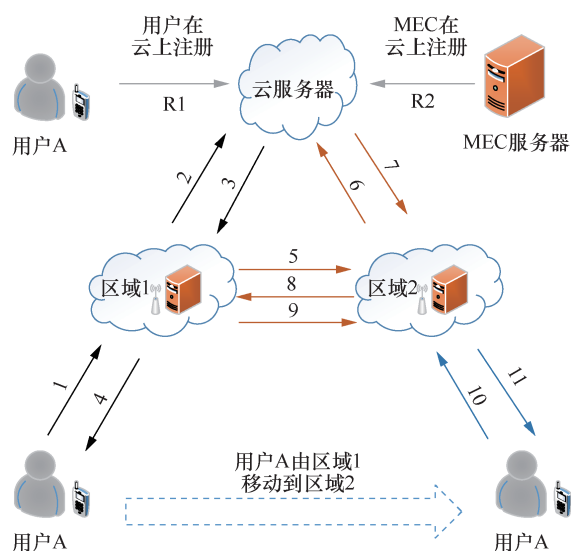


图2 基于预认证的快速切换认证方案
Figure 2 Fast handover authentication schemes service architecture based on pre-certification

1) 用户: 用户通过智能设备 (绑定自己生物

特征信息)上的应用程序从 MEC 服务器或者云服务器获取所需服务。

2) MEC 服务器: MEC 服务器部署在网络边缘为用户提供安全、高效的服务。当用户从一个区域移动至另一个区域时,为了确保用户能够快速接入另一个 MEC 服务器,在用户移动到该区域前,MEC 服务器需要提前将用户所需服务进行迁移。其中区域 i 中的 MEC 服务器记为 MEC i 。

3) 云服务器:云服务器部署在云端为用户和 MEC 服务器提供服务。用户与 MEC 服务器通过云服务器进行彼此的认证(本文云服务器始终是可信的)。所提认证机制分为 4 个阶段,阶段 1:注册;阶段 2:首次认证;阶段 3:服务迁移;阶段 4:切换认证。相关符号含义如表 1 所示。

阶段 1: 注册

(1) 用户在云服务器上注册

Step 1: 用户通过安装在智能终端上的应用进行注册信息的处理,并将注册信息发送到云服务器上。本文用户与云服务器之间的传输信道为

不安全的信道。

Step 2: 云服务器将包含云服务器身份令牌的信息发给用户,并保存在用户本地。

(2) MEC 服务器在云服务器上注册

Step 1: MEC 服务器将注册信息发送到云服务器。本文 MEC 服务器与云服务器之间为安全的信道。

Step 2: 云服务器将包含云服务器合法的身份令牌信息发送到 MEC 服务器,并保存在 MEC 本地。

阶段 2: 首次认证

Step 1: 用户向区域 1 中的 MEC 服务器发送服务请求。

Step 2: 区域 1 中的 MEC 服务器将用户的服务请求发送到云服务器。

Step 3: 云服务器检查自身数据库,查看是否有 MEC 服务器及用户的 ID 信息,若无则终止;若存在则进一步验证 MEC1 服务器是否合法;若合法则将用户的认证信息、MEC1 的认证信息发

表 1 符号说明
Table 1 The symbol description

参数	描述	参数	描述
UID	用户设备信息	F1、F2、F3、F4	哈希函数用于生成匿名密钥、签名信息、身份令牌、会话密钥
MID	加密的用户设备信息	RAND	注册阶段产生的随机数
UB	用户生物特征信息	Nu、Nmi、Nc	认证阶段用户产生的随机数、区域 i 的 MEC 服务器产生的随机数、云服务器产生的随机数
MU	由用户加密的用户身份信息	Mreq、Mreq、Sreq	注册请求、迁移请求、服务请求
XMU	由云服务器加密的用户身份信息	Sig	用户的签名信息
Cmac	云服务器地址	UAUTN、CAUTN	用户身份令牌、云服务器身份令牌
MC	加密的云服务器身份信息	MAUTNi	部署在区域 i 的 MEC 服务器身份令牌
MACi	部署在区域 i 的 MEC 服务器的 mac 地址	AUTNi、AUTNij	区域 i 认证令牌、区域 i 与区域 j 之间的认证令牌
Mimac	加密区域 i 的 MEC 服务器的 mac 地址	SKcmi	云服务器与区域 i 的 MEC 服务器之间的会话密钥
MMi	加密区域 i 的 MEC 服务器身份信息	SKumi	用户与区域 i 的 MEC 服务器之间的会话密钥
MAKi	部署在区域 i 的 MEC 服务器的匿名参数	SKmij	区域 i 与区域 j 的 MEC 服务器之间的会话密钥
UAK	注册阶段用户匿名参数	N0	用于生成共享密钥的用户密钥随机数
UAKc	认证阶段云服务器产生的匿名参数	Ni	用于生成共享密钥的区域 i 的 MEC 服务器的密钥随机数
UAKu	认证阶段用户产生的匿名参数	MSKumi	用户与区域 i 的 MEC 服务器之间的共享密钥
K	服务根密钥,定期随着服务升级更新	RESi	保存在区域 i 中的 MEC 服务器响应消息
Kmi	区域 i 的 MEC 服务器的服务标识密钥,定期随着服务升级更新	$\oplus$	异域运算
Kc	云服务器私有参数	$\parallel$	联接符号
Mi	MEC 服务器私有参数	{A}_SK	使用会话密钥 SK 加密 A

送至 MEC1 服务器。

Step 4: MEC1 验证用户的合法性。若合法, 将认证结果发送至用户。用户在本地验证 MEC1 的合法性, 若合法, 则接收 MEC1 提供的服务。反之, 则从云服务器获取服务。

阶段 3: 服务迁移

Step 1: 区域 1 的 MEC 服务器向区域 2 的 MEC 服务器发送迁移请求。

Step 2: 区域 2 的 MEC 服务器向云服务器请求认证信息。

Step 3: 云服务器发送 MEC1、MEC2 以及用户的认证信息。

Step 4: MEC2 服务器发送认证信息。

Step 5: 进行服务迁移。

阶段 4: 切换认证

Step 1: 用户向区域 2 中的 MEC 服务器请求服务。

Step 2: MEC 服务器验证用户的合法性, 若合法, 则将认证结果发送至用户并提供服务。用户在本地终端验证 MEC 服务器的合法性, 若合法则接收服务。反之, 则从云服务器获取服务。

1.3 注册阶段

1.3.1 用户在云服务器上注册

用户通过安装在智能终端上的应用程序来获取所需服务, 为了确保用户个人隐私信息的安全性, 隐私信息将在本地进行处理。用户通过基站与云服务器进行交互, 与基站之间的交互以无线的方式进行属于不安全的通道, 信息传输过程需要进行加密处理。用户向云服务器进行注册, 云服务器检查智能设备及应用程序的合法性, 并保存绑定用户身份信息与设备信息的身份令牌, 用于在服务过程中验证用户的真伪, 本地保存包含云服务器令牌的信息用于在本地校验网络服务的真伪。用户注册流程如图 3 所示。

具体步骤如下。

1) 用户生成 SQN 及随机数 RAND, 并计算 UAK、MID、MU、UAUTN、Sig。其中 SQN 用于防范重放攻击, Sig 用于防止注册信息被修改, UAK 用于对敏感信息进行加密处理。

其中: $UAK = F1(RAND \parallel K)$,

$MID = UID \oplus UAK$,

$MU = F3(UID \parallel UB \parallel K)$,

$UAUTN = MU \parallel SQN \oplus UAK$,

$Sig = F2(UID \parallel K \parallel RAND)$ 。

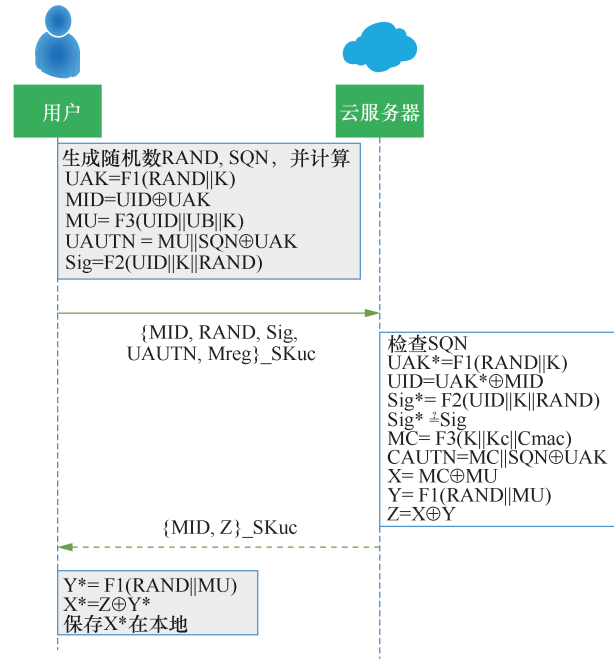


图3 用户注册流程

Figure 3 The user registration process

2) 发送消息到云服务器。消息如下:

$\{MID, RAND, Sig, UAUTN, Mreg\}_{SKuc}$

3) 云服务器收到后, 由 RAND 计算 UAK^* 、UID ($UID = UAK \oplus MID$)、 Sig^* , 并验证 Sig 与 Sig^* 是否相等。

4) 云服务器计算 $MC = F3(K \parallel Kc \parallel Cmac)$ 、 $CAUTN = MC \parallel SQN \oplus UAK$ 、 $X = MC \oplus MU$ 、 $Y = F1(RAND \parallel MU)$ 、 $Z = X \oplus Y$, 并将 Z 发送至用户。

5) 用户计算 $X = Z \oplus Y$ 并保存在本地。

1.3.2 MEC 服务器在云服务器上注册

MEC 服务器部署在网络边缘, 可采用使用软件定义网络和网络功能虚拟化等技术的通用标准服务器, 相应的服务功能由对应服务商提供。本文不考虑有线传输过程中存在的安全威胁, 因此 MEC 服务器与云服务器、MEC 服务器之间采用有线传播的方式进行信息传递, 属于安全通道。MEC 服务器上相应的服务由服务提供商部署, 部署应用时内置会话密钥与服务标识密钥。MEC 服务器注册流程如图 4 所示。具体步骤如下。

1) MEC 服务器生成随机数 $RAND$ ，并计算 MAK_i 、 $Mimac$ 、 MM_i 、 $MAUTN_i$ ，将消息： $\{Mimac, RAND, MAUTN_i, Mreg\}_{SK_{cmi}}$ 发送至云服务器。

其中： $MAK_i = F1(K_{mi} \parallel RAND)$ ，

$Mimac = MAK_i \oplus MAC_i$ ，

$MM_i = F3(MAC_i \parallel K_{mi} \parallel M_i)$ ，

$MAUTN_i = F3(MAC_i \parallel K_{mi} \parallel MM_i) \oplus MAK_i$ 。

2) 云服务器收到后，由 $RAND$ 计算 MAK_i^* 、 MAC_i 、 MM_i 、 MC 、 RES_i 。云服务器将 MAC_i 与对应的 K_{mi} 绑定，保存 MM_i 在云端。

其中： $MAK_i^* = F1(K_{mi} \parallel RAND)$ ，

$MAC_i = MAK_i^* \oplus Mimac$ ，

$MM_i = MAK_i^* \oplus MAUTN_i$ ，

$MC = F3(K \parallel K_c \parallel C_{mac})$ ，

$RES_i = MM_i \oplus MC$ 。

3) 发送消息 $\{Mimac, RES_i\}_{SK_{cmi}}$ 到 MEC 服务器。

4) MEC 服务器收到消息后，保存至 RES_i 本地边缘服务器。

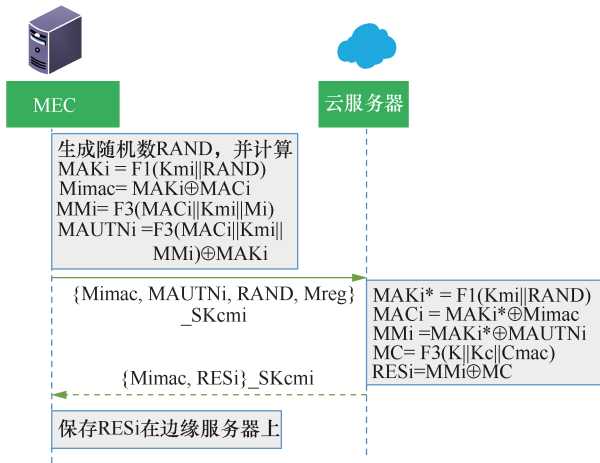


图 4 MEC 服务器注册流程

Figure 4 MEC server registration process

1.4 首次认证阶段

用户与部署在区域 1 内的 MEC 服务器首次认证并获取所需的服务内容。云服务器将认证信息传至 MEC 服务器与用户处，在网络边缘实现相互认证，认证流程如图 5 所示。

具体步骤如下。

1) 用户随机生成一个随机数 Nu ，对 UID 进

行掩码，发送服务请求 $\{MID, Nu, Sreq\}_{SK_{um1}}$ 。

其中： $UAK_u = F1(Nu \parallel K)$ ，

$MID = UID \oplus UAK_u \parallel SQN \oplus UAK_u$ 。

2) 区域 1 的 MEC 服务器收到消息后随机生成随机数 $Nm1$ ，对 $MAC1$ 进行掩码处理。

其中： $MAK1 = F1(K_{m1} \parallel Nm1)$ ，

$M1mac = MAC1 \oplus MAK1$ 。

3) 区域 1 中的 MEC 服务器向云服务器发送服务请求 $\{MID, Sreq, Nu, M1mac, Nm1\}_{SK_{cm1}}$ 。

4) 云服务器通过 Nu 、 $Nm1$ 计算相应匿名密钥，计算 UID 、 MAC_i 。

其中： $UAK_u^* = F1(Nu \parallel K)$ ，

$UID = MID \oplus UAK_u^*$ ，

$MAK1^* = F1(K_{m1} \parallel Nm1)$ ，

$MAC1 = M1mac \oplus MAK1^*$ 。

5) 云服务器检查 $MAC1$ 是否在云数据库中，若不在数据库中则终止服务并直接向用户发出假冒 MEC 服务器警告，若在，查询对应 K_{mi} 并计算 $MM1$ 、 $RES1^*$ ($RES1^* = MM1 \oplus MC$)。

6) 云服务器检查 UID ，若不在数据库中则终止服务，并告知 MEC 服务器为非法用户，若在，查询 MU 。计算用户与区域 1 的 MEC 服务器的联合身份令牌 $AUTN1$ 。

其中： $UAK_c = F1(Nc \parallel K)$ ，

$AUTN1 = RES1^* \oplus MU =$

$MU \oplus MC \oplus MM1$ ，

$MUAK_c = UAK_c \oplus MAK1$ 。

7) 发送信息到 MEC 服务器，消息为： $\{AUTN1, Nc, MUAK_c\}_{SK_{cm1}}$ 。

8) MEC 服务器生成随机数 $N1$ ，同时计算 $UN1 = N1 \oplus UAK_c$ ， $MX1 = MM1 \oplus UAK_c$ ，发送消息 $\{M1mac, AUTN1, MX1, Nc, UN1\}_{SK_{um1}}$ 到用户端。

9) UE 在本地计算并验证保存在本地的 $X \oplus MM1$ 与 $AUTN1$ 是否相等，若相等则证明 MEC 服务器合法。。

10) 生成随机数 $N0$ ，计算 UAK_c^* 、 $MM1$ 、 XMU 、 $M1N0$ ，发送消息 $\{MID, XMU, M1mac, M1N0\}_{SK_{um1}}$ 到 MEC 服务器。

其中： $UAK_c = F1(Nc \parallel K)$ ，

$MM1 = MX1 \oplus UAK_c^*$ ，

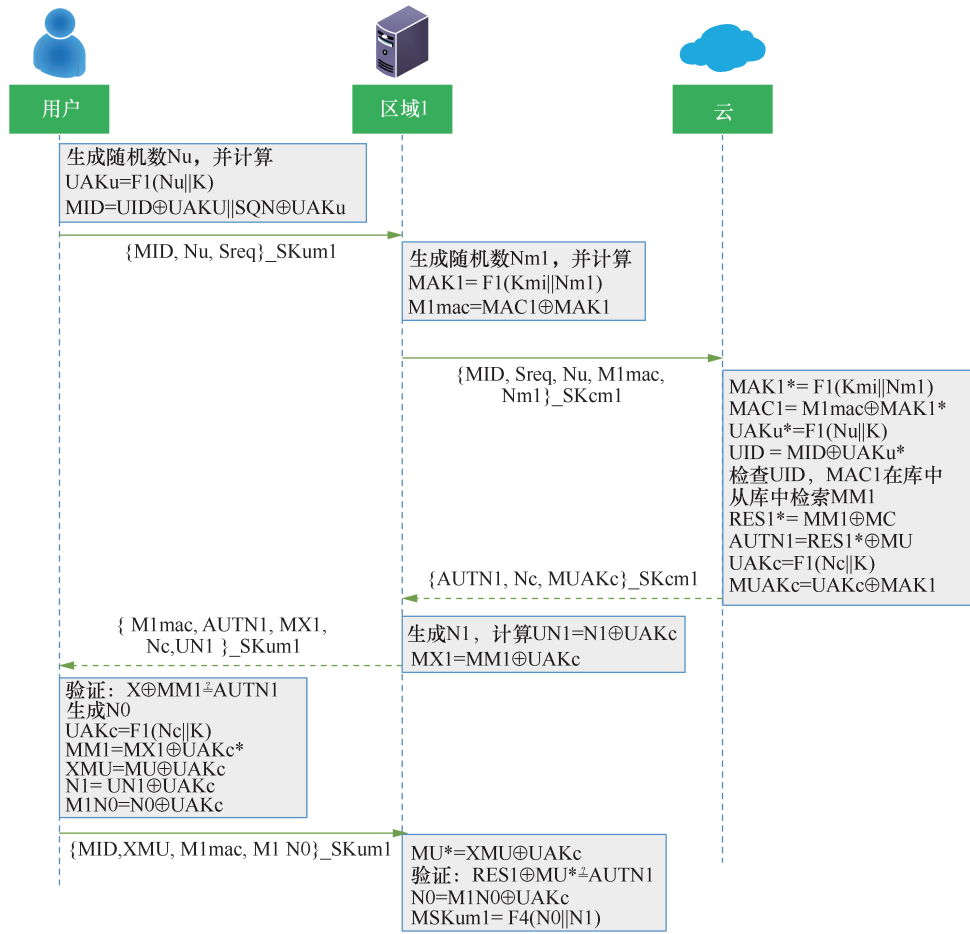


图5 用户首次认证流程

Figure 5 UE first authentication process

$$XMU = MU \oplus UAK_c,$$

$$N1 = UN1 \oplus UAK_c,$$

$$MIN0 = N0 \oplus UAK_c.$$

11) MEC 服务器计算 $MU^* = XMU \oplus UAK_c$, MEC 服务器用本地存的 $RES1 \oplus MU^*$ 与 $AUTN1$ 对比。若相等则为合法用户。

12) MEC 服务器计算 $N0 = M1N0 \oplus UAK_c$, 生成共享密钥 $MSK_{um1} = F_4(N0 || N1)$

1.5 服务迁移阶段

区域 1 的服务器与区域 2 的服务器进行相互认证, 并传递服务相关信息, 迁移流程如图 6 所示。

具体步骤如下。

1) 用户向区域 1 的 MEC 服务器发送迁移请求, 消息为 $\{MID, N_u, Mreq\}_{MSK_{um1}}$ 。

2) 区域 1 的 MEC 服务器响应用户请示, 并将

请求消息发送到区域 2 的 MEC 服务器。其中 $\{M1mac, Nm1, MID, N_u, Nc, Mreq\}_{SK_{cm12}}$ 为发往区域 2 中的 MEC 服务器的消息; 发往用户的消息为: $\{Nc\}_{MSK_{um1}}$ 。

3) 区域 2 的 MEC 服务器生成随机数 N_{m2} , 并计算 $MAK2$ 、 $M2mac$ 同时向云服务器发出认证请求。

其中: $MAK2 = F_1(K_{m1} || N_{m1})$,

$$M2mac = MAC2 \oplus MAK2.$$

请求信息: $\{M1mac, Nm1, MID, N_u, Nc, Mreq, M2mac, Nm2, Sreq\}_{SK_{cm2}}$

4) 云服务器检查相应参数是否存在, 若不存在则终止服务。计算 $AUTN1$ 、 $AUTN2$ 、 $AUTN12$, 并发送消息: $\{AUTN1, AUTN2, AUTN12, MUAKc\}_{SK_{cm2}}$ 到区域 2 中的 MEC 服务器。

其中: $AUTN12 = MM1 \oplus MM2 \oplus MC \oplus UAK_c$ 。

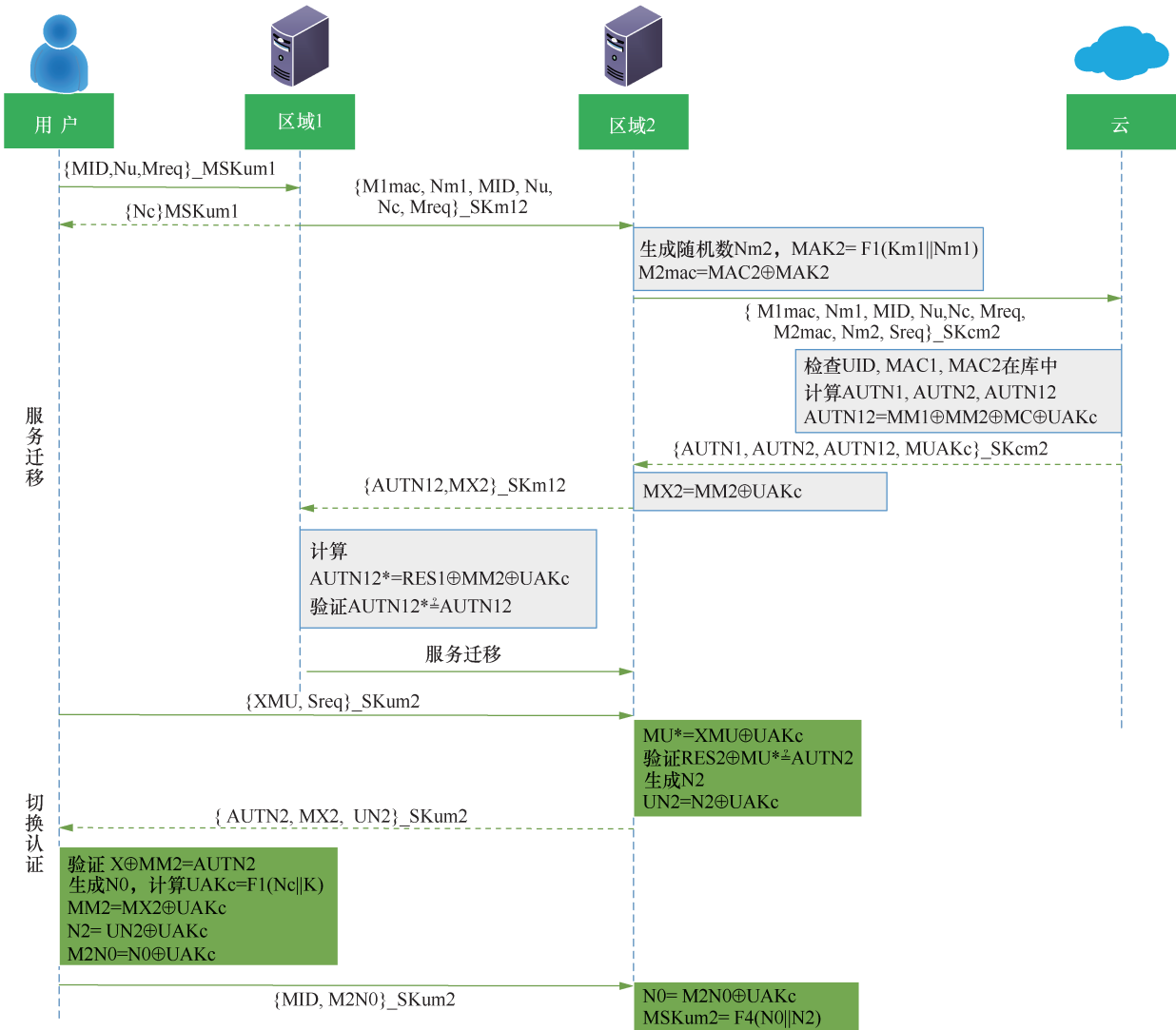


图 6 服务迁移及切换认证流程
Figure 6 Service migration and handover authentication processes

5) 区域 2 的 MEC 服务器计算 $MX2$, 并发送消息: $\{AUTN12, MX2\}_{SKm12}$ 到区域 1 的 MEC 服务器。

其中: $MX2 = MM2 \oplus UAKc$ 。

6) 区域 1 的 MEC 服务器计算 $AUTN12^*$, 并验证与 $AUTN12$ 是否相等。若相等则进行服务迁移。

1.6 切换认证阶段

当用户移动至区域 2 的 MEC 服务器服务范围内时, 用户需要与区域 2 中的 MEC 服务器快速完成认证才能确保持续获取所需服务。

具体步骤如下。

1) 用户发送请求 $\{XMU, Sreq\}_{SKum2}$ 到区域 2 中的 MEC 服务器, 其中 XMU 中包含加密

的 SQN 序列。

2) 区域 2 中的 MEC 服务器计算 $MU^* (MU^* = XMU \oplus UAKc)$, MEC 服务器用保存在本地的 $RES2 \oplus MU^*$ 与 $AUTN2$ 对比。若相等则为合法用户。

3) MEC 服务器生成随机数 $N2$, 发送消息: $\{AUTN2, MX2, UN2\}_{SKum2}$ 到 UE。

其中: $UN2 = N2 \oplus UAKc$ 。

4) UE 在本地计算 $X \oplus MM2$, 验证计算结果是否与 $AUTN2$ 相等, 若相等则证明 MEC 服务器合法。

5) 生成新的随机数 $N0$, 并计算 $UAKc$ 、 $MM2$ 、 $N2$ 、 $M2N0$, 发送消息: $\{MID, M2N0\}_{SKum2}$ 到 MEC 服务器。

SKum2 到 MEC 服务器。

其中: $UAKc = F1(Nc \parallel K)$,

$MM2 = MX2 \oplus UAKc$,

$N2 = UN2 \oplus UAKc$,

$M2N0 = N0 \oplus UAKc$ 。

6) MEC 服务器计算 $N0$, 生成共享密钥 MSKum2。

其中: $N0 = M2N0 \oplus UAKc$,

$MSKum2 = F4(N0 \parallel N2)$ 。

2 方案分析

本节首先从两个角度分析所设计方案的安全性, 一是从理论设计的角度, 二是利用形式化分析工具进行仿真验证; 其次对全流程的成本开销进行计算, 对比切换认证与首次认证的计算成本, 论证降低服务等待时延的可行性; 最后, 与其他方案进行对比表明所提方案的优势。

2.1 安全性分析

2.1.1 非形式化分析

本节主要从方案的理论设计角度进行非形式化的安全分析。

1) 匿名性: 用户的身份信息 UID 由 UAK 进行掩码处理, 边缘服务器的 MAC 地址由 MAK 进行掩码处理。UAK 由仅有用户和云服务器知道的服务根密钥计算所得, MAK 由仅有云服务器和 MEC 服务器知道的服务标识密钥计算所得, 攻击者无法获取用户的 UID 信息以及边缘服务器的 MAC 地址。同时在本地对用户的生物信息 MU 进行哈希处理, 云服务器、边缘服务器以及攻击者均无法获取用户的身份信息。

2) 双向身份认证: 云服务器作为根信任域保存着用户的根服务密钥 K 以及边缘服务器的服务标识密钥 K_{mi} , 因此攻击者无法获取 MU 、 MC 、 MMi 。MEC 服务器通过有线的方式向云服务器请求认证信息, 由云服务器对不同区域的 MEC 服务器进行相互认证, 经过认证的 MEC 服务器组成次一级的边缘信任域, 信任域内的 MEC 服务器彼此可信, 由任一 MEC 服务器认证的用户, 可将被域内其他 MEC 服务器认可。用户与 MEC 服务器之间的首次认证在云服务器上进行, 切换认证由用户与次级信任域进行

认证。用户通过根信任域与边缘信任域进行相互认证。

3) 不可否认性: 用户注册阶段使用签名信息 Sig 来保证用户的不可否认性。

4) 前向保密: 用户的根服务密钥 K 以及边缘服务器的服务标识密钥 K_{mi} 会定期更新。假设攻击者获取当前的 K 和 K_{mi} , 在时间 T 内将无法由破解决之前或之后用户传输的信息, 时间 T 取决于密钥更新频率, 因此所提方案具备弱前向保密性。

5) 机密性: 成功进行认证后, 用户与 MEC 服务器构建新的会话密钥 MSKumi, 生成会话密钥的随机数 $N0$, Ni 进行加密处理后, 分别传到 MEC 服务器与用户。攻击者无法获取随机数, 从而无法得知新的会话密钥。

6) 完整性: 要做到数据的安全传输, 还需要确定收到的数据没有经过窃听者的篡改, 这就涉及数据的完整性校验。用户在云服务器注册阶段的数据传输属于空口传输容易被攻击者篡改。所提方案通过引入签名信息 Sig 用于防止注册信息被篡改, 其中 $Sig = F2(UID \parallel K \parallel RAND)$ 。密钥 K 仅用户和云服务器知道, 攻击者无法计算出正确的 Sig 值, 云服务器通过对比用户传输的 Sig 值与云服务器自身计算出的 Sig* 值是否相等对传输信息进行校验。

7) 新鲜性: 在注册认证过程, 采用同步序列的方式来确保信息的新鲜性。

8) 防窃听攻击: 用户注册阶段在空口传输的内容 MID、RAND、Sig、Z, 其中 MID、Z 都进行了加密处理, 攻击者无法通过窃听获取用户 UID、UB, 以及包含 MC、MU 信息的 X。同时攻击者也无法通过 RAND 来计算匿名参数。

9) 防假冒攻击: 用户的 UID、UB、MEC 服务器的 MAC 地址都进行了加密处理, 攻击者无法假冒用户发起攻击。

10) 防重放攻击: 注册、认证过程中通过采用同步序列的方式来防止遭受重放攻击。

11) 防中间人攻击: 攻击者只有正确获取 K 、 K_{mi} 、 Kc 才能正确计算 UAK、UAKc、MAKi, 从而正确获取用于身份认证的核心信息 MMi 、 MU 、 MC , 才能实现正常的认证。而 K 、 K_{mi} 、 Kc 仅由服务提供商生成, 被攻击者获取的机率相

当小。攻击者无法在注册和认证过程中更改传输消息，因此，所提方案可抵御中间人攻击。

12) 防拒绝服务攻击：在本方案中，攻击者无法通过盗取大量用户账号来发动 DoS 攻击，因为用户要获取服务需要用户账号与用户的生物特征信息，而攻击者无法准确获取用户的生物信息 UB。同时，注册、认证过程中采用的同步序列，可有效避免大量重复的服务请求。

13) 防离线猜测攻击：用户的根服务密钥以及 MEC 服务器的服务标识密钥，由服务提供商进行加密处理保存在各自本地中并定期更新，攻击者通过暴力手段破解密钥的难度大。

14) 防终端被盗攻击：用户获取服务需要提供自身的生物特征信息 UB，非法用户的 UB 与合法的 UID 生成的 MU 将无法与保存在终端的验证信息匹配，在终端侧不法用户的行为将被终止。

15) 可扩展性：MEC 场景下的认证方案需要满足边缘服务器的随时扩展，本文所提的认证机制中新增用户通过向云服务器注册来获取服务，新增的 MEC 服务器由服务提供商进行部署，可随时加入到整个认证系统。

16) 轻量级：通过采用计算复杂度较低的哈希算法和异或运算来完成认证方案中的各类计算任务，计算成本较低，满足轻量级要求。

2.1.2 形式化工具分析

AVISPA 是用于自动验证 Internet 安全敏感协议和应用程序的按钮式工具^[21]。它提供了一种用于表示协议及其安全属性的模块化表达形式语言，并集成了实现各种最新自动分析技术的不同后端，分别为即时模型检查器 (OFMC, on-the-fly model-checker)、基于 SAT 的模型检查器 (SATMC, SAT-based model-checker)、基于约束逻辑的攻击搜索器 (CL-AtSe, constraint logic-based attack-searcher) 和基于自动近似的树自动机 (TA4SP, tree automata based automatic approximations for the analysis of security protocols)。AVISPA 使用高级协议规范语言 (HLSL, high level protocol specification language)^[22]进行编码，由于 HLSL 是比基本的“Alice&Bob”表示法更具表现力的语言，因此，协议设计者有时很难确定编写的 HLSL 规范是

否符合他们所考虑的“Alice&Bob”协议。SPAN^[23]是一款专门为 AVISPA 制作安全协议的工具，SPAN 可以通过简单的 CAS+语言^[24]生成 HLSPL 语言，有助于交互式生成消息序列图 (MSC, message sequence charts)，可以将其视为 HLSL 规范中的“Alice&Bob”跟踪。

本次验证过程使用 SPAN 工具将 CAS+语言转换为 HLSPL 语言，再进行调试仿真。CAS+语言第 1 部分标识符声明 (identifiers)，用于声明协议中涉及的参数类型。如图 7 所示，协议共有 4 个实体，分别是代表用户的 A，代表区域 1 中的 MEC 服务器 B1，代表区域 2 中的 MEC 服务器 B2，代表云服务器的 S。MSKum1 为会话密钥，F1 为哈希函数，UID 表示不属于 user、key 类型的任何数据 (数字 num、文本 text、记录 record 等) 的抽象。

```

1 protocol Switchauthentication;
2
3
4 identifiers
5 A, B1, B2, S : user;
6
7 UID, UB, MAC1, M1,MAC2,M2, Kc, Cmac, RAND,
8 Nu,N0, Nm1, N1, Nm2, N2,Nc, K,Km1,Km2, MID,
9 MU, Sig, UAUTN, UAK, M1N0, M2N0, MAUTN1, M1mac,
10 MAK1,UN1, MAUTN2, M2mac, MAK2, UN2, MC, XMU,
11 CAUTN, AUTN1, AUTN2, AUTN12, UAKc, RES1, RES2,
12 Mreq ,Mreq, Sreq, UAKu, MX1, MX2,MM1 : number;
13
14 MSKum1, MSKum2, SKum1, SKum2 ,
15 SKcm1 ,SKcm2,SKm12 ,SKuc : symmetric_key;
16
17 F1,F2,F3,F4:function;
```

图 7 标识符声明部分
Figure 7 The identifier declaration section

第 2 部分为消息 (Message)，描述消息体之间相互交互的全过程。如图 8 所示，标签 1-2 表示用户注册会话流程，标签 3-4 与 5-6 分别表示 MEC 服务器注册会话流程，标签 7-10 为用户首次认证会话流程，标签 11-16 为 MEC 之间的服务迁移会话流程，标签 17-19 为用户切换认证会话流程。

第 3 部分为初始知识 (Knowledge)，在协议执行的开始，每个主体都需要一些初步的知识来撰写它的消息，如图 9 所示。

第 4 部分为会话实例 (Session instance)，通过将不同的值分配给不同的标识符，从而描述运行协议的不同系统。其中 A:i 表示用户为入侵者时的会话实例，如图 10 所示。

```

23 messages
24 %User registration
25 1. A -> S : {MID,RAND,Sig,UAUTH,Mreg}Skuc.
26 2. S -> A : {MID,Z}Skuc
27
28 %MEC1 registration
29 3. B1 -> S : {M1mac, MAUTN1, RAND, Mreg}SKcm1
30 4. S -> B1 : {M1mac, RES1}SKcm1
31
32 %MEC2 registration
33 5. B2 -> S : {M2mac, MAUTN2, RAND, Mreg}SKcm2
34 6. S -> B2 : {M2mac, RES2}SKcm2
35
36 %first certification
37 7. A -> B1 : {MID, Nu, Sreq}SKum1,UAKu
38 8. B1 -> S : {MID, Sreq, Nu, M1mac, Nm1}SKcm1
39 10. B1 -> A : {M1mac, AUTN1, MX1, Nc, UN1}SKum1
40
41 %Migration phase
42 11. A -> B1 : {B1,MID,Nu,Mreg}MSKum1
43 12. B1 -> A : {B1,S,Nc}MSKum1
44 13. B1 -> B2 : {M1mac, Nm1, MID, Nu, Nc, Mreg}SKm12
45 14. B2 -> S : {M1mac, Nm1, MID, Nu, Nc, Mreg, M2mac, Nm2, Sreq}SKcm2
46 15. S -> B2 : {AUTN12, AUTN2, AUTN12, UAKc}SKcm2
47 16. B2 -> B1 : {AUTN12,MX2}SKm12
48
49 %Migration phase
50 17. A -> B2 : {B1,XMU,Sreq}SKum2
51 18. B2 -> A : {B2, AUTN2, MX2, UN2}SKum2
52 19. A -> B2 : {MID,B2,M2N0}SKum2

```

图8 消息部分

Figure 8 The message section

```

55 knowledge
56
57 A: A,B1,B2,S, F1, F2, F3,F4, UID, UB, K,MU,
58 Mreg ,Mreq, Sreq, SKum1, SKum2 , SKuc ;
59
60 B1: A,B1,B2,S, F1, F2, F3,F4, MAC1, M1, Km1,
61 MM1, Mreg ,Mreq, Sreq, SKcm1, SKum1, SKm12 ;
62
63 B2: A,B1,B2,S, F1, F2, F3,F4, MAC2, M2, Km2,
64 Mreg ,Mreq, Sreq, SKcm2, SKum2, SKm12 ;
65
66 S: A,B1,B2,S, F1, F2, F3,F4, Kc, Cmac, K, Km1,Km2,
67 MM1,MU, MC, Mreg ,Mreq, Sreq ,SKcm1, SKcm2, SKuc ;

```

图9 初始知识部分

Figure 9 Initial knowledge section

```

73 session_instances
74
75 [A:ue,B1:mec1,B2:mec2,S:server,F1:f1,F2:f2,
76 F3:f3,F4:f4,UID:uid,UB:ub,K:k,MAC1:mac1,M1:m1,
77 Km1:km1,MAC2:mac2,M2:m2,Km2:km2,Kc:kc,Cmac:cmac,
78 Mreg:mreg,Mreq:mreq,Sreq:sreq, SKum1: skim1,
79 SKum2 : skim2 , SKuc: skic, SKcm1: skcm1 ,
80 SKcm2:skcm2,SKm12: skim12,MM1:mm1,MU:mu]
81
82
83 [A:i,B1:mec1,B2:mec2,S:server, F1: f1, F2: f2,
84 F3: f3,F4:f4,UID: iid, UB: ib, K: k, MAC1: mac1,
85 M1:m1, Km1 : km1 , MAC2: mac2, M2:m2,Km2: km2,
86 Kc: kc, Cmac: cmac, Mreg : mreg ,Mreq:mreq,
87 Sreq: sreq, SKum1: skim1, SKum2 : skim2 , SKuc: skic,
88 SKcm1: skcm1 ,SKcm2:skcm2,SKm12: skim12,MM1:mm1,MU:mu]
89 ;

```

图10 会话实例部分

Figure 10 The session instance section

第5部分为入侵者知识 (Intruder knowledge), 入侵者知识是在会话实例中引入的一组入侵者已经知晓的值。如图11所示, 入侵者知晓用于加密计算的函数 f1、f2、f3、f4, 以及入侵者与云服务器之间的会话密钥 skic, 入侵者与 MEC 服务器之间的会话密钥 skim1、skim2。

```

92 intruder_knowledge
93
94 ue,mec1,mec2,server,f1,f2,f3,f4,iid,ib,
95 skic,skim1,skim2,mreg,mreq,sreq;

```

图11 入侵者知识部分

Figure 11 Intruder knowledge

第6部分为目标, 用于声明参数的机密性以及实体间的相互认证过程。图12明确所提协议具备的安全目标, 如 secrecy_of K, UID [A,S]表示只有用户和云服务器知道 K 与 UID 的值。Authentication_on ue_mec_mm1 表示用户对 MEC1 服务器进行认证。

实验过程中使用 SPAN 工具将 CAS+语言转换为 HLPSP 高级语言后再进行调试, 图13展示了通过 SPAN 工具转换后的服务迁移与切换认证的消息序列。

```

97 goal
98 secrecy_of K,UID [A,S];
99 secrecy_of Km1,MAC1 [B1,S];
100 secrecy_of Kc,Cmac [S];
101 secrecy_of MM1 [S,B1];
102 secrecy_of MU [A,B1,S];
103 secrecy_of N1 [A,B1];
104 secrecy_of N0,MSKum1 [A,B1];
105 authentication_on ue_mec1_mm1
106 authentication_on mec1_ue_mu
107 authentication_on c_mec1_mm1
108 authentication_on mec1_c_mc

```

图12 目标部分

Figure 12 Goal section

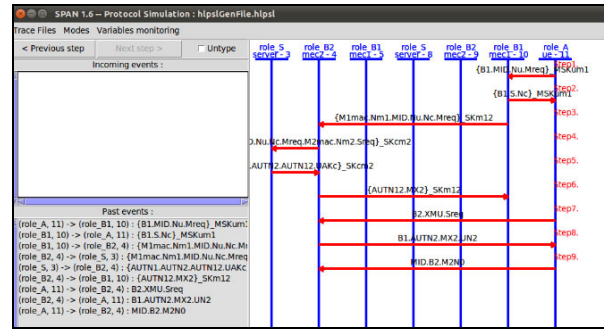


图13 服务迁移与切换认证消息序列

Figure 13 Service migration and switching authentication message sequence diagrams

图14为首次认证的验证结果, 图15为切换认证的验证结果。具体说明如下: 验证结果的前两行是协议摘要目标后端注释, 第一行表示所用验证工具的后端类型, 第二行为工具版本。“SUMMARY”为协议验证的整体摘要, 分为“SAFE”与“UNSAFE”两个结果, DETAILS为验证结果的详细解释有以下常见类型“ATTACK_FOUND”、(发现攻击)、“BOUNDED_NUMBER_OF_SESSIONS”、(有限次的会话实例)等, “PROTOCOL”为路径信息, “GOAL”显示验证目标按协议规定执行, “STATISTICS”为具体的验证细节。若协议“SUMMARY”显示为“UNSAFE”,

则“DETAILS”将会显示为“ATTACK_FOUND”，“STATISTICS”处将呈现出具体的攻击路径。本文方案采用 OFMC 进行验证，两次验证结果在有限次的会话实例下均为安全有效。

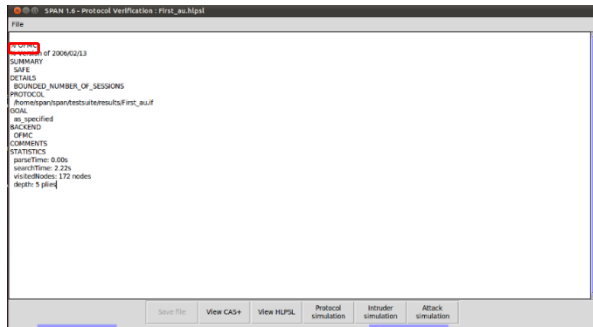


图 14 首次认证验证结果
Figure 14 First authentication verification results

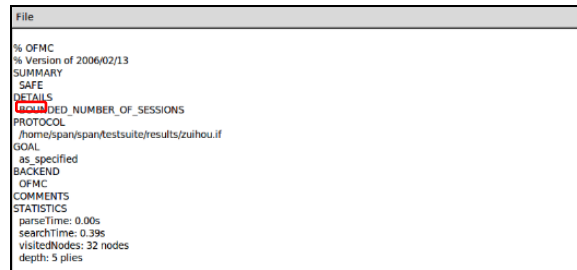


图 15 切换认证验证结果
Figure 15 Handover authentication verification results

2.1.3 安全性比较

表 2 从匿名性、不可否认性、新鲜性、机密性等方面对比了所提方案与其他方案的安全性。本文所提出的方案与其他方案相比具有更高的安全性。

表 2 安全属性对比
Table 2 Comparison of security attributes

安全属性及服务质量	匿名性	不可否认性	新鲜性	机密性	完整性	双向身份认证	弱向前(后)保密	模仿攻击	重放攻击	中间人攻击	拒绝服务攻击	离线猜测攻击	终端被盗攻击
本文方案	是	是	是	是	是	是	是	是	是	是	是	是	是
文献[12]	是	是	否	是	是	是	否	是	是	是	是	否	否
文献[13]	是	是	是	是	否	是	否	是	是	是	是	是	是

2.2 性能评估

文献[26]对各种对称、非对称、哈希函数、椭圆曲线加密算法的计算成本进行了分析，与椭圆曲线操作或加密解密操作相比，单向哈希函数的成本更低。本文所提方案仅使用 XOR 操作和哈希计算，计算成本较低满足 MEC 场景轻量级要求，能为资源受限的边缘设备提供了更好的性能。

切换认证带来的计算成本也是一个需要考虑的重要问题^[25]。本文使用参数为 Intel(R) Core(TM) i7-9750H CPU @ 2.60 GHz, 64 GB 内存和 Window 10 操作系统的计算机模拟边缘服务器和云服务器，使用性能参数为 kirin 980、8G 内存和 Android 10 操作系统的华为手机模拟移动设备，实验使用 Python 语言进行仿真，计算所提方案和文献[12-13]中使用的基本执行时间，如表 3 所示，其中 Th 为一次单向哈希函数的计算成本，Txor 为一次异或运算的计算成本，Tsyen 为对称加密算法加密计算成本，Tsyde 为对称加密算法解密计算成本，Tasen 为非对称加密算法加密计算成

本，Tasde 为非对称加密算法解密计算成本。其中选择 AES-256 为实验中的对称加密算法，RSA 为非对称加密算法。

表 3 基本执行时间
Table 3 Basic execution time

单位: ms						
仿真平台	Th	Txor	Tsyen	Tsyde	Tasen	Tasde
服务器	0.001 4	0.001 3	0.011 6	0.014 4	0.021 4	0.734 6
用户终端	0.002 2	0.001 9	0.093 4	2.812 7	0.103 9	3.693 7

表 4 分析了每个阶段用户、MEC 服务器、云服务器的计算成本。由表 4 可以明显看出切换认证阶段的计算成本(5Th+8Txor)明显少于首次认证计算成本 8Th+16Txor，实现了将计算任务下沉到边缘的要求。

表 5 列出了 3 种方案认证阶段的计算成本，与文献[12]相比，所提方案减少了云服务器计算压力，与文献[13]相比，所提方案在整体计算成本方面占优，均能够满足资源受限的移动终端用户需求。

表4 各阶段计算成本
Table 4 Computation costs of each stage

阶段	终端用户	MEC1	MEC2	云服务器
用户注册阶段	4Th+3Txor	N/A	N/A	4Th+4Txor
服务器注册阶段	N/A	2Th+Txor	2Th+Txor	3Th+2Txor
首次认证阶段	3Th+6Txor	2Th+5Txor	N/A	3Th+5Txor
服务迁移阶段	Th+Txor	Th+3Txor	2Th+2Txor	2Th+8Txor
切换认证阶段	4Th+4Txor	N/A	Th+4Txor	N/A

注: N/A 表示空值。

表5 认证阶段计算成本对比
Table 5 Computation costs of the proposed scheme in authentication phase

认证方案	用户	边缘节点	远程服务器
本文方案	4Th+4Txor=0.016 4	Th+4Txor=0.006 6	N/A
方案[12]	2Txor=0.0038	2Txor=0.0026	4Txor=0.005 2
方案[13]	8Th=0.0176	6Th=0.0084	8Th=0.0112

注: N/A 表示空值。

表6列出了3种协议的通信成本,其中ID为身份标识、XOR为异或运算、H为单向哈希、T为时间戳。设它们的长度分别为: $|ID|=256$ bit, $|XOR|=256$ bit, $|H|=256$ bit, $|T|=32$ bit。由此计算3种协议的通信成本,结果表明,本文所提出的方案通信成本方面占优势。综上所述,本文方案在通信成本上有较好的优势,计算开销能够满足资源受限的移动终端用户需求。

表6 通信成本对比
Table 6 Communication cost of the proposed scheme

方案	通信成本	数据长度/bit
本文方案	$2 ID +4 XOR $	1 536
方案[12]	$6 XOR $	1 536
方案[13]	$3 ID +5 H +2 XOR +4 T $	2 688

3 结束语

针对传统服务架构难以满足移动用户对时延、服务质量的严苛要求等问题。本文通过引入MEC来实现移动过程中用户安全可持续的服务体验。本文方案的优势有以下4个方面:首先,本文方案通过构建信任域,使得经由边缘信任域认证的用户能快速获取信任域内任一边缘服务器的服务。其次,在服务迁移阶段通过服务预缓存可以有效减少用户请求服务的等待时间;再次,

将部分云服务器承载的任务下沉至MEC服务器,在边缘侧进行数据处理能减轻云服务器的计算压力;最后,用户端承载了部分数据处理任务,用户的设备信息与生物特征信息在本地进行计算验证,无须再上传至云服务器,这样既保证了用户隐私信息不出本地,又能降低实时处理带来的时延问题。

后续期望从两个方面对方案进行完善:一是在实际工程环境中对方案的可扩展性进行验证;二是在普适性上进行改进,期望协议可兼容第三方部署的边缘服务器。

参考文献:

- [1] 5G Infrastructure PPP Association. 5G Vision-The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services[J]. White Paper, February, 2015.
- [2] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing—A key technology towards 5G[J]. ETSI White Paper, 2015, 11(11): 1-16.
- [3] PATEL M, NAUGHTON B, CHAN C, et al. Mobile-edge computing introductory technical white paper[J]. Mobile-edge Computing (MEC) Industry Initiative, 2014, 29: 854-864.
- [4] QI Y, TIAN L, ZHOU Y, et al. Mobile edge computing-assisted admission control in vehicular networks: the convergence of communication and computation[J]. IEEE Vehicular Technology Magazine, 2019, 14(1): 37-44.
- [5] ZHOU Y, TIAN L, LIU L, et al. Fog computing enabled future mobile communication networks: a convergence of communication and computing[J]. IEEE Communications Magazine, 2019, 57(5): 20-7.
- [6] ZHOU Y, LING L, WANG L, et al. Service aware 6G: An intelligent and open network based on convergence of communication, computing and caching [J]. Digital Communications and Networks, 2020, 6(3): 253-260
- [7] 胡鑫鑫, 刘彩霞, 刘树新,等. 移动通信网鉴权认证综述 [J]. 网络与信息安全学报, 2018, 4(12): 1-15.
HU X X, LIU C X, LIU S X, et al. Overview of mobile communication network authentication [J]. Chinese Journal of Network and Information Security, 2018, 4(12): 1-15.
- [8] 翟靖轩. 移动云计算中的认证协议研究[D]. 徐州: 中国矿业大学, 2019.
ZHAI J X. Research on authentication protocol in mobile cloud computing[D]. Xuzhou: China University of Mining and Technology, 2019.
- [9] 陈春雨, 尚文利, 赵剑明,等. 边缘计算身份认证和隐私保护技术[J]. 自动化博览, 2018, v.35;No. 300(S2): 96-99.
CHEN C Y, SHANG W L, ZHAO J M, et al. Edge computing identity authentication and privacy protection technology [J]. Automation Panorama, 2018, V.35; No.300 (S2): 96-99
- [10] 胡荣磊,陈雷,段晓毅,于秉琪. 一种适用于雾计算的终端节点切换认证协议[J]. 电子与信息学报, 2020, 42(10): 2350-2356.

- HU R L, CHEN L, DUAN X Y, et al. A switching authentication protocol of terminal node for fog computing[J]. Journal of Electronics & Information Technology, 2020, 42(10): 2350-2356.
- [11] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.
- ZHANG J L, ZHAO Y C, CHEN B, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39 (3): 1-21
- [12] CHEN C L, CHIANG M L, HSIEH H C, et al. A lightweight mutual authentication with wearable device in location-based mobile edge computing [J]. Wireless Personal Communications, 2020, 113(1): 575-598.
- [13] DHILLON P K, KALRA S . A lightweight biometrics based remote user authentication scheme for IoT services[J]. Journal of Information Security and Applications, 2017: S2214212616301442.
- [14] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing—A key technology towards 5G[J]. ETSI White Paper, 2015, 11(11): 1-16.
- [15] 胡鑫鑫. 5G 网络认证协议和非接入层协议安全性研究[D]. 战略支援部队信息工程大学.
- HU X X. Research on security of 5G network authentication protocol and non-access stratum protocol[D]. PLA Strategic Support Force Information Engineering University.
- [16] JIA X, HE D, KUMAR N, et al. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing[J]. IEEE Systems Journal, 2019:1-12.
- [17] LIU H, ZHANG P, PU G, et al. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing[J]. IEEE Transactions on Vehicular Technology, 2020, PP(99):1-1.
- [18] XIAO Y, JIA Y, LIU C, et al. Edge computing security: state of the art and challenges[J]. Proceedings of the IEEE, 2019, PP(99):1-24.
- [19] ZHANG J, CHEN B, ZHAO Y, et al. Data security and privacy-preserving in edge computing paradigm: survey and open issues[J]. IEEE Access, 2018, 6(18)209-37.
- [20] LI X, CHEN T, CHENG Q, et al. Smart applications in edge computing: overview on authentication and data security[J]. IEEE Internet of Things Journal, 2020, PP(99):1-1.
- [21] TEAM T A. AVISPA v1. 1 User manual[EB]. Information society technologies programme (June 2006)[EB]. 2006.
- [22] CHEVALIER Y, COMPAGNA L, CUELLAR J, et al. A high level protocol specification language for industrial security-sensitive protocols[C]//Workshop on Specification and Automated Processing of Security Requirements-SAPS'2004. Austrian Computer Society, 2004.
- [23] GLOUCHE Y, GENET T, HOUSSAY E. SPAN: a security protocol animator for AVISPA[C]//IRISA, 2008.
- [24] SAILLARD R, GENET T. CAS+[EB].
- [25] SHARMA V, YOU I, PALMIERI F, et al. Secure and energy-efficient handover in fog networks using blockchain-based DMM[J]. IEEE Communications Magazine, 2018, 56(5): 22-31.
- [26] RIFA-POUS H, HERRERA-JOANCOMARTÍ J. Computational and energy costs of cryptographic algorithms on handheld devices[J]. Future Internet, 2011, 3(1): 31-48.

[作者简介]



张伟成 (1990—), 男, 山西应县人, 信息工程大学硕士生, 主要研究方向为 5G 移动边缘计算安全。



卫红权 (1971—), 男, 河南唐河人, 信息工程大学研究员, 主要研究方向为融合网络安全、可重构网络理论与技术。



刘树新 (1987—), 男, 山东潍坊人, 博士, 信息工程大学副研究员, 主要研究方向为链路预测和通信网络安全。



普黎明 (1976—), 男, 云南嵩明人, 信息工程大学副研究员, 主要研究方向为网络体系结构和通信网络安全。