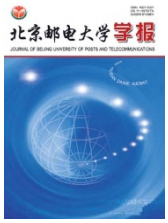

北京邮电大学学报
Journal of Beijing University of Posts and Telecommunications
ISSN 1007-5321,CN 11-3570/TN

《北京邮电大学学报》网络首发论文

题目：　边缘计算中移动终端安全高效认证协议
作者：　薛建彬，白子梅
收稿日期：　2020-01-10
网络首发日期：　2021-01-22
引用格式：　薛建彬，白子梅．边缘计算中移动终端安全高效认证协议．北京邮电大学学报. https://kns.cnki.net/kcms/detail/11.3570.TN.20210122.1056.004.html

北 京 邮 电 大 学 学 报

DOI：10.13190/j.jbupt.2020-005

边缘计算中移动终端安全高效认证协议

薛建彬，白子梅
（兰州理工大学 计算机与通信学院，兰州 730000）

摘 要：针对移动终端计算能力较低和存储能力有限的问题，提出了适用于移动边缘计算环境的轻量级身份认证协议．该协议将密码学与物理层的安全保护技术相结合，利用对称密码体制降低移动终端在认证过程中的计算复杂度，以少量的计算量和较低的信息存储量完成移动终端与边缘服务器的相互认证与密钥协商，并且移动终端只需一次注册便可在移动边缘计算环境中随机漫游．安全性分析表明，该协议满足前向安全性、抗重放攻击性、抗中间人攻击性等安全特性．仿真结果表明，与其它认证方案相比，该方案在通信和计算成本方面有较好的性能优势．

关键词：移动边缘计算；身份认证；物理层安全；漫游；数据安全
中图分类号：TP393　　**文献标志码：**A

Security and Efficient Authentication Scheme for Mobile Edge Computing

XUE Jian-bin，BAI Zi-mei
（School of Computer and Communication，Lanzhou University of Technology，Lanzhou 730000，China）

Abstract：Aiming at the problems of low computing power and limited storage capacity of mobile terminals，a lightweight identity authentication protocol suitable for mobile edge computing environments is proposed．The protocol combines cryptography with physical layer security protection technology，uses a symmetric cryptosystem to reduce the computational complexity of the mobile terminal in the authentication process，and completes the communication between the mobile terminal and the edge server with a small amount of calculation and low information storage．Mutual authentication and key negotiation，and mobile terminals can roam randomly in the mobile edge computing environment with only one registration．Security analysis shows that the protocol satisfies the security features of forward security，anti-replay attacks，and anti-man-in-the-middle attacks．Simulation shows that，compared with other authentication schemes，this scheme has better performance advantages in terms of communication and calculation costs．

Keywords：mobile edge computing; identity authentication; physical-layer security; roaming; data security

收稿日期：2020-01-10
基金项目：国家自然科学基金项目（61841107，61461026）
作者简介：薛建彬（1973—），男，教授，博士生导师，E-mail：xue_jabn@hotmail.com.
通信作者：白子梅（1995—），女，硕士生.

移动边缘计算（MEC，mobile edge computing）是一个集连接、计算、存储和应用的开放平台[1]，作为一个小型数据中心，需要达成类似云计算数据中心的数据安全和访问控制[2]．由于 MEC 服务器靠近数据源侧，使得终端设备安全问题迁移到 MEC 服务器上，因此需要在物联网终端设备和边缘数据中心之间实现有效的身份认证和信任管理[3]。然而，物联网终端资源受限且数量众多，传统的公钥基础设施（PKI，public key infrastructure）技术密钥管理、证书验证开销较大，不适用于网络边缘侧[4]．同时，由于 MEC 环境下终端具有很强的移动性，实现用户在不同 MEC 服务器之间高效切换认证具有很大挑战．

目前关于边缘计算范式下身份认证的研究较多地集中于雾计算与移动云计算[5-7]，关于 MEC 环境下身份认证协议的相关研究数量较少[8-10]．Dey 等[5]提出了移动云计算的相互认证方案．该方案基于消息摘要、位置和时间戳的认证，使用动态密钥最小化加密密钥的可预测性．Pardeshi 等[6]利用伪随机数生成器，时间戳和散列函数技术实现雾服务器和终端设备的安全双向认证．Ibrahim[7]提出了雾计算环境的边雾认证方案，允许任何雾用户和雾节点相互认证．Jia 等[8]设计了基于用户身份的匿名认证密钥协商协议，在其协议设计中使用了复杂的双线性对操作．同样，Kaur 等[9]提出了基于用户身份的匿名性认证方案，该协议使用了椭圆曲线，单向哈希函数和级联运算．Yang 等[10]提出了一种具有用户匿名性和不可追溯性的切换认证方案．此协议为用户分配了许多伪身份标识（ID，identity）以及与每个伪 ID 相对应的一系列私密密钥．

综上所述，现有的身份认证方案在可行性和安全性上有了较大的改进，但是上述方案在 MEC 场景中使用存在一定的不合理性．如在文献[5-7]中，身份认证协议应用于雾计算与移动云计算场景，运用在 MEC 场景中扩展性较差，而文献[8-9]中使用耗时的双线性对运算，使 MEC 场景中资源受限的物联网终端产生较大的计算负担．为此，针对移动终端存储和计算能力有限的特点，所提协议尽量减少交换消息的轮数和长度，利用对称加密算法进行认证，以此能够避免移动终端在计算过程中具有较大的负担．将密码技术与物理层的安全保护技术相结合，保障了网络边缘侧业务的应用安全．

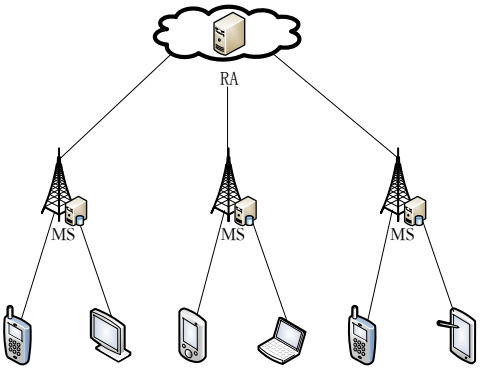

图 1 MEC 网络模型

1 网络模型

如图 1 所示，MEC 网络体系是一个三级层次结构，包含智能终端设备、MEC 服务器（MS，MEC server）、注册中心（RA，registration authority）等不同的功能实体．智能终端设备可以是具有通信和感应功能的移动设备，由于智能终端设备受到计算资源和电池的限制，无法在短时间内完成巨大的计算任务，需要将部分计算任务卸载到 MEC 服务器．与智能终端设备相比，MEC 服务器上有更多的计算，存储和通信资源．MEC 服务器可以部署于基站、小基站甚至汇聚站点，在云计算网络的边缘，物理上接近终端智能设备．RA 在云服务中，负责对边缘计算用户和 MEC 服务器进行注册授权，并给所有边缘计算用户发送长期密钥．

2 方案实现

所提认证协议基于 Hash 函数，对称密码体制与非对称密码体制设计，由初始阶段、用户注册阶段、服务器注册阶段、认证阶段四部分组成．在认证阶段采用对称密钥加密/解密，完全适用于资源受限的终端设备．协议中的符号定义如表 1 所示．

表 1 符号定义

符号	含义
RA	注册中心
C	边缘用户
MS	边缘服务器
ID_C	边缘用户身份标识
ID_{MS}	边缘服务器身份标识
k_C	用户主密钥
$k_{C,MS}$	用户和边缘服务器之间的共享密钥
k_S	会话密钥
k_i	传输密钥
T_i	当前的时间和日期
(Pk_{RA},Sk_{RA})	RA 的公私密钥对
(Pk_{MS},Sk_{MS})	MS 的公私密钥对
H(x)	对 x 做哈希运算

2.1 初始阶段

RA 生成自己的公钥和私钥（Pk_{RA},Sk_{RA}），并且公开自己的公钥 Pk_{RA}，公钥 Pk_{RA} 真实有效．

2.2 用户注册阶段

用户在接入 MEC 服务器提供的服务之前须在 RA 注册成为合法的用户.用户向 RA 提出注册请求，RA 为用户生成一个主密钥．用户和 RA 通过安全信道通信．

1) C 自身生成一个身份标识 ID_C.
2) 将 ID_C 和注册请求发送至 RA.
3) RA 收到 C 的身份标识 ID_C，查询认证数据库，若 ID_C 已经存在要求 C 生成新的 ID_C，否则为 C 随机生成主密钥 k_C，并存储 ID_C 和 k_C.
4) RA 将 k_C 通过安全信道发送至 C.
5) C 将（ID_C，k_C）保存在设备的智能卡中.

用户注册阶段如图 2 所示.

2.3 服务器注册阶段

MEC 服务器生成自己的公私钥对（Pk_{MS},Sk_{MS}），并将公钥 Pk_{MS} 注册到 RA 中．RA 为 MEC 服务器分配身份标识 ID_{MS}，并使用 RA 的私钥 Sk_{RA} 签名后发送给 MEC 服务器，ID_{MS} 不需要保密.

1) MS 生成公私钥对（Pk_{MS},Sk_{MS}）.
2) 将公钥 Pk_{MS} 和注册请求发送至 RA.
3) RA 为 MS 分配身份标识 ID_{MS}.
4) RA 用私钥 Sk_{MS} 将 ID_{MS} 签名后发送至 MS.
5) MS 保存自己的身份标识 ID_{MS}.

服务器注册阶段如图 3 所示.

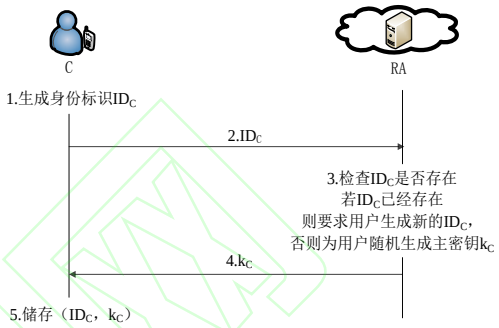

图 2 用户注册阶段

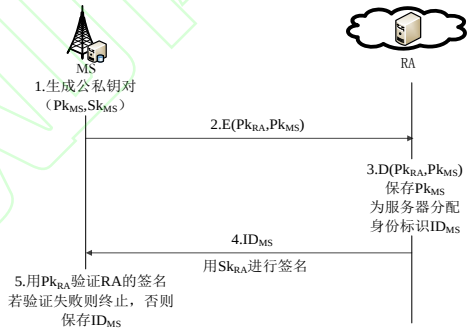

图 3 服务器注册阶段

2.4 认证阶段

当用户向 MEC 服务器提出服务请求时，距离最近的 MEC 服务器接收到用户的请求后向 RA 求证用户的身份标识 ID_C 是否存在，若 ID_C 存在 RA 则生成 MEC 服务器与该用户的共享密钥 $k_{C,MS}$，并将 $k_{C,MS}$ 发送给 MEC 服务器．用户与 MEC 服务器经过身份认证后确定会话密钥．会话密钥通过提取移动无线信道中随机变化的信道特征产生．详细认证过程与密钥协商描述如下：

1) C 发起认证请求，向周围的 MEC 服务器广播（Request,ID_C）.
2) MEC 服务器收到 Request 后，用 RA 的公钥加密 ID_{MS} 和 ID_C，并向 RA 发送加秘密信息 $E(Pk_{RA}, ID_{MS}||ID_C)$确认用户身份标识 ID_C 是否存在.

3) RA 使用私钥 Sk_{RA} 解密收到的信息，检查 ID_C 是否存在，若检查失败则终止通信，否则生成 MEC 服务器与该用户 C 的共享密钥 $k_{C,MS}=H(ID_{MS},k_C)$.

4) RA 使用 MEC 服务器的公钥 Pk_{MS} 对 $k_{C,MS}$ 加密，并用私钥 Sk_{RA} 将信息<ID_{MS}||$E(Pk_{MS}, k_{C,MS})$>签名后发送给 MEC 服务器.

5) MEC 服务器用 RA 的公钥 Pk_{RA} 验证 RA 的签名，成功后用私钥 Sk_{MS} 解密密文，得到与用户 C 的共享密钥 $k_{C,MS}$. 通过测量无线网卡上接收的信号强度将其量化生成随机密钥 k_i.

6) MEC 服务器使用 $k_{C,MS}$ 加密 k_i 与当前的日期和时间 T_1，并向 C 发送信息<ID_{MS}，ID_C，$E(k_{C,MS},k_i||T_1)$>.

7) C 收到 MEC 服务器的信息后，通过 ID_{MS} 和主密钥 k_C 计算与 MEC 服务器的共享密钥 $k_{C,MS}=H(ID_{MS},k_C)$，用共享密钥 $k_{C,MS}$ 解密信息得到 k_i 和 T_1. 若当前时间 T_2 减去 T_1 小于等于 ΔT（ΔT 是网络延时的时间区间），C 可以认证 MS 的合法身份，并通过测量无线模块上接收的信号强度将其量化生成随机密钥 k_S.

8) C 使用 MEC 服务器发的密钥 k_i 加密 k_S 与当前的日期和时间 T_2，并向 MEC 服务器发送加密信息 $E(k_i, k_S||T_2)$.

9) MEC 服务器收到信息后使用 k_i 解密信息，得到 k_S 和 T_2，若当前时间 T_3 减去 T_2 小于等于 ΔT，说明发信者必是合法用户 C，接受 k_S 作为会话密钥.

认证阶段如图 4 所示.

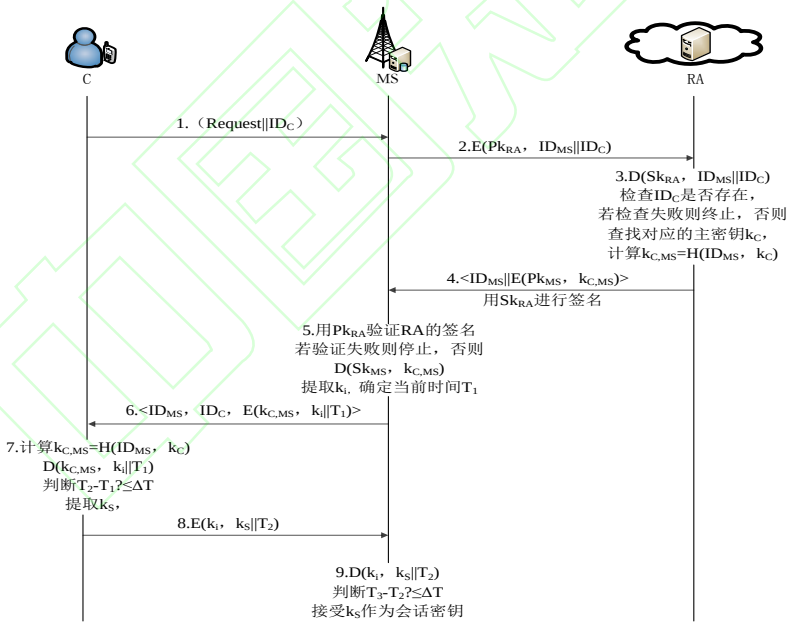

图 4 认证阶段

3 安全分析

3.1 安全逻辑分析

利用 BAN 逻辑[11]对所提方案的正确性进行严格的逻辑分析. BAN 逻辑是一种基于信念的模态逻辑，其目标是认证参与协议的主体的身份,分析协议能否达到预定的目标. 以下 BAN 逻辑的证明过程中，符号 C 和 MS 分别代表用户和 MEC 服务器，$k_{C,M}$ 代表用户和 MEC 服务器之间新鲜的共享密钥. 以下 BAN 逻辑将验证用户和 MEC 服务器之间能否进行身份认证并确认会话密钥 k_S.

BAN 逻辑分析中使用的一些符号描述如下：

$P|\equiv X$：主体 P 相信 X 是真的；

$P \lhd X$：主体 P 接收到含 X 的消息；

$P|\Rightarrow X$：主体 P 对 X 有管辖权；

$P|\sim X$：主题 P 发送过含 X 的消息；

$\#(X)$：消息 X 是新鲜的；

$P \xleftrightarrow{k} Q$：P 和 Q 共享密钥 k 进行通信；

$\{X\}_k$：用密钥 k 加密后的密文.

所提协议验证阶段传输的消息形式化描述：

$M1: C \rightarrow MS: -$

$M2: MS \rightarrow C: \{T_1, C \xleftrightarrow{k_i} MS, \#(C \xleftrightarrow{k_i} MS)\}_{k_{C,MS}}$

$M3: C \rightarrow MS: \{T_2, C \xleftrightarrow{k_s} MS, \#(C \xleftrightarrow{k_s} MS)\}_{k_i}$

所提协议初始状态假设：

1） $C|\equiv\#(T_1)$

2） $MS|\equiv\#(T_2)$

3） $MS|\equiv C \xleftrightarrow{k_{C,MS}} MS$

4） $C|\equiv[C \xleftrightarrow{k_{C,MS}} MS, \#(C \xleftrightarrow{k_s} MS)]$

5） $MS|\equiv C \xleftrightarrow{k_i} MS$

6） $C|\equiv MS \Rightarrow [T_1, C \xleftrightarrow{k_i} MS, \#(C \xleftrightarrow{k_i} MS)]$

7） $MS|\equiv C \Rightarrow [T_2, C \xleftrightarrow{k_s} MS, \#(C \xleftrightarrow{k_s} MS)]$

所提协议将满足的目标：

$G1: C|\equiv[C \xleftrightarrow{k_i} MS, \#(C \xleftrightarrow{k_i} MS)]$

$G2: C|\equiv MS|\equiv[C \xleftrightarrow{k_i} MS, \#(C \xleftrightarrow{k_i} MS)]$

$G3: MS|\equiv[C \xleftrightarrow{k_s} MS, \#(C \xleftrightarrow{k_s} MS)]$

$G4: MS|\equiv C|\equiv[C \xleftrightarrow{k_s} MS, \#(C \xleftrightarrow{k_s} MS)]$

基于 BAN 逻辑规则和初试状态假设，对提出的认证协议推证过程如下：

令 $X=[C \xleftrightarrow{k_i} MS, \#(C \xleftrightarrow{k_i} MS)]$

由假设 1），根据 BAN 新消息判断规则

$$\frac{C|\equiv\#(T_1)}{C|\equiv\#(T_1, X)}$$ 结论 1

由假设 4）和消息 M2，根据 BAN 消息含义规则

$$\frac{C|\equiv C \xleftrightarrow{k_{C,MS}} MS, C \lhd \{T_1, X\}_{k_{C,MS}}}{C|\equiv MS|\sim (T_1, X)}$$ 结论 2

由结论 1 和结论 2，根据 BAN 临时值校验规则

$$\frac{C|\equiv\#(T_1, X), C|\equiv MS|\sim (T_1, X)}{C|\equiv MS|\equiv (T_1, X)}$$ 结论 3

由假设 6）和结论 3，根据 BAN 逻辑管辖权规则

$$\frac{C|\equiv MS \Rightarrow (T_1, X), C|\equiv MS|\equiv (T_1, X)}{C|\equiv (T_1, X)}$$ 结论 4

由结论 3 和结论 4，根据 BAN 信任规则

$$\frac{C|\equiv MS|\equiv (T_1, X)}{C|\equiv MS|\equiv X}$$ 结论 5

由结论 5 可以得出：目标 G2 得证

$$\frac{C|\equiv (T_1, X)}{C|\equiv X}$$ 结论 6

由结论 6 可以得出：目标 G1 得证

令 $Y=[C \xleftrightarrow{k_s} MS, \#(C \xleftrightarrow{k_s} MS)]$

由假设 2），根据 BAN 新消息判断规则

$$\frac{MS|\equiv\#(T_2)}{MS|\equiv\#(T_2, Y)}$$ 结论 7

由假设 5）和消息 M3，根据 BAN 消息含义规则

$$\frac{MS|\equiv C \xleftrightarrow{k_i} MS, MS \lhd \{T_2, Y\}_{k_i}}{MS|\equiv C|\sim (T_2, Y)}$$ 结论 8

由结论 7 和结论 8，根据 BAN 临时值校验规则

$$\frac{MS|\equiv\#(T_2, Y), MS|\equiv C|\sim (T_2, Y)}{MS|\equiv C|\equiv (T_2, Y)}$$ 结论 9

由假设 7）和结论 9，根据 BAN 逻辑管辖权规则

$$\frac{MS|\equiv C \Rightarrow (T_2, Y), MS|\equiv C|\equiv (T_2, Y)}{MS|\equiv (T_2, Y)}$$ 结论 10

由结论 9 和结论 10，根据 BAN 信任规则

$$\frac{MS|\equiv C|\equiv (T_2, Y)}{MS|\equiv C|\equiv Y}$$ 结论 11

由结论 11 可以得出：目标 G4 得证

$$\frac{MS|\equiv (T_2, Y)}{MS|\equiv Y}$$ 结论 12

由结论 12 可以得出：目标 G3 得证，完成协议正确性证明目标.

3.2 基本安全要求

双向身份认证：边缘用户与 MEC 服务器需要通过共享密钥 $k_{C,MS}$ 认证.边缘用户在本地使用存在智能卡中的主密钥 k_C 和 MEC 服务器的身份 ID_{MS} 通过哈希运算生成共享密钥 $k_{C,MS}$．RA 以同样的方式生成共享密钥 $k_{C,MS}$ 发送至 MEC 服务器.若有攻击者冒充 MEC 服务器的身份，在没有获得共享密钥 $k_{C,MS}$ 的情况下无法与边缘用户相互认证．而若有攻击者冒充边缘用户 C，在没有主密钥 k_C 的情况下也无法与 MEC 服务器相互认证.

密钥的安全性：在边缘用户与 MEC 服务器的认证过程中，共享密钥 $k_{C,MS}$ 不用于加密已知的明文，而用于加密临时的会话密钥 k_i．会话密钥 k_i 是新鲜的并且不会暴露在信道中，对于窃听者来说是未知．故而窃听者难以从密文推出共享密钥 $k_{C,MS}$.

前向安全：每个会话密钥 k_i 和 k_s 是利用无线信道的多径效应，提取随机变化的信道特征生成的随机字符串．因此，使用动态密钥不仅最小化会话密钥的可预测性，而且一个会话密钥被窃取不会影响保密通信.

3.3 对抗攻击时的安全性

穷举法攻击：在边缘用户处唯一不能暴露的是用户的主密钥 k_C．密钥是一个具有足够长位的强密钥（用于防止服务器发生暴力攻击）并采用防篡改机制（如智能卡）进行保护，蛮力攻击无法获得.

中间人攻击：攻击者在边缘用户与 MEC 服务器之间．试图伪装成另一方．由于攻击者不知道存储在边缘用户处的主密钥 k_C，无法推断出在边缘用户处生成和存储在 MEC 服务器中的共享密钥 $k_{C,MS}$，而且攻击者无法获取临时会话密钥 k_i．因此，中间人攻击对此方案无效.

重放攻击：边缘用户与 MEC 服务器之间的认证信息包含时间戳 T_i，所以攻击者不能重放上一轮的消息从而通过认证.

3.4 安全性比较

表 2 中列出所提方案与其他文献方案之间安全性的比较．从表中可以看出文献[8]的方案不能保证会话密钥
的安全性．文献[11]没有提供逻辑上的安全证明．文献[10]的方案不是轻量级认证协议，但可以抵御主要的攻击．因此，可以看出，现有的方案不能提供足够的安全性，并且由于使用大量的计算会损害移动设备性能，不适用于 MEC 环境．笔者提出的身份认证协议支持所有安全功能，并且也是轻量级的.

表 2 方案安全性对比

安全性能	文献[8]	文献[11]	文献[10]	所提方案
双向认证	√	√	√	√
密钥安全	×	√	√	√
单点登录	√	√	√	√
重放攻击	√	√	√	√
中间人攻击	√	√	√	√
穷举法攻击	√	√	√	√
假冒攻击	√	√	√	√
前向安全	√	√	√	√
安全可证性	√	×	√	√
轻量级	√	√	×	√

4 性能评估

根据计算成本、通信成本来评估本文协议的性能，并与文献[10]，文献[11]和文献[8]进行对比，有效地说明了所提协议的性能优势．为了反映出 MEC 服务器与移动设备的计算力的不同，在两种不同的平台上执行基本操作．使用阿里云平台模拟 MEC 服务器，平台参数为 Intel(R) Xeon(R) CPU E5-2682 v4 @2.50GHz，1GB 内存和 Ubuntu14.04 操作系统．使用华为手机模拟移动设备，手机性能参数为 2.1GHz 海思 kirin658、4G 内存和 Android7.0 操作系统.

为了正确评估所提协议的性能，选择 AES-256 作为实验中的对称加密算法，RSA 作为非对称加密算法．并且为了与文献[10]进行对比，在仿真平台上执行文献[10]中的加密算法. 文献[10]中使用椭圆曲线加密算法以及 Ate 类双线性对，使用 160 阶加性椭圆曲线群 G 和 160 阶乘法循环群 G_T 作为加密算法参数. 详细内容请参考文献[10]. 所提方案和文献[10]中使用的基本操作执行时间如表 3 所示．表 3 中符号 T_{re}，T_{rd}，T_{ae}，T_{ad}，T_{bp}，T_m，T_a，T_h 和 T_e 分别表示执行非对称加密，非对称解密，对称加密，对称解密，双线性配对，标量乘法，点加法，哈希和模幂运算所需的计算时间.

所提方案与文献[10]，文献[11]和文献[8]中所提方案计算成本由表 4 所示．在移动终端，文献[8]与所提方案执行相同加密算法，但由表 5 可以看出文献[8]中所需加密的信息比所提方案多 704b，故实际运用中所提方案的计算成本更低．所提方案虽然在 MEC 服务器的计算成本上略有增加，但幅度不大，完全可以满足服务器的实际应用．因此所提方案更满足资源受限的移动终端用户需求．

表 5 列出了四种协议的通信成本．表中符号包含不同的含义，如加性循环组（G），域（Z_q），身份标识（ID），共享和会话密钥（k），哈希（H）和时间戳（T）．它们的长度设置如下：|G|= 1024b，$|Z_q|$= 160b，|ID|=256b，|k|=256b，|H|= 256b，和|T|= 32b．根据这些值，计算了四种协议的通信成本，并汇总在表 5 中．结果表明，所提出的方案具有最佳性能．

表 3 基本操作执行时间(ms)

仿真平台	T_{re}	T_{rd}	T_{ae}	T_{ad}	T_h	T_{bp}	T_m	T_a	T_e
云平台	2.977	5.358	0.071	0.084	0.005	2.798	1.038	0.006	0.172
手机	27.983	49.293	0.654	0.667	0.047	25.517	11.491	0.069	1.68

表 4 计算成本对比(ms)

方案	用户端	MEC 服务器
文献[8]	$T_h + T_{ae} + T_{ad}$(1.368)	$T_{ae} + T_{ad}$(0.155)
文献[11]	$4T_m + 4T_h$(46.152)	$3T_m + 4T_h$(3.134)
文献[10]	$4T_m + 3T_a + T_e + 5T_h$(48.086)	$T_{bp} + 5T_m + 3T_a + 5T_h$(8.031)
所提方案	$T_h + T_{ae} + T_{ad}$(1.368)	$T_{ae} + T_{ad} + T_{re} + T_{rd}$(8.49)

表 5 通信成本对比

方案	通信成本	数据长度（bit）
文献[8]	7|ID|+4|k|	2816
文献[11]	2|G| + 2|T| + 2|H|	2624
文献[10]	4|G| + 2|T| + 2$\|Z_q\|$ + |ID|	4736
所提方案	5|ID|+3|k|+2|T|	2112

5 结束语

所提方案解决了边缘用户在漫游的情况下与边缘服务器的相互认证的问题，提出了一种安全有效的方案，允许任何边缘用户在云服务提供商的授权下与任何 MEC 服务器进行相互身份验证．所提方案的优势在于不要求将边缘用户纳入任何 PKI，边缘用户只需要在注册阶段存储一个主密钥．使用此主密钥，边缘用户可以与云服务提供商管理的 MEC 服务器进行相互身份验证．采用 BAN 逻辑证明了所提方案的安全性．计算和通信成本评估结果也表明该方案在满足安全性的同时，不会产生显着的计算和通信成本．

参考文献

[1] 施巍松，孙辉，曹杰．边缘计算：万物互联时代新型计算模型[J]．计算机研究与发展，2017，54(5)：907-924．
Shi Weisong，Sun Hui，Cao Jie．Edge computing：a new computing model in the era of interconnection of all things [J]. Computer Research and Development，2017，54(5)：907-924．

[2] 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 Jiale，Zhao Yanchao，Chen Bing，et al．A review of research on data security and privacy protection in edge computing [J]．Journal of Communications，2018，39 (3)：1-21．

[3] Almajalai S，Salameh H B．A framework for efficient and secured mobility of IoT devices in mobile edge computing[C] ．Third IEEE International Conference on Fog & Mobile Edge Computing．IEEE，2018，58-62．

[4] Roman R，Lopez J，Mambo M．Mobile edge computing，fog et al.：a survey and analysis of security threats and challenges[J] ．Future Generation Computer Systems，2016:680-698．

[5] Dey S，Ye Q，Sampalli S．AMLT：A mutual authentication scheme for mobile cloud computing[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber，Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)．Halifax：IEEE，2018：700-705．

[6] Pardeshi M S，Yuan S M．SMAP fog/edge：a secure mutual authentication protocol for fog/edge[J] ．IEEE Access，2019，7：101327-101335．

[7] Ibrahim M H．Octopus：an edge-fog mutual authentication scheme[J]．International Journal of Network Security，2016，18(6):1089-1101．

[8] 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．

[9] Kaur K，Garg S，Kaddoum G et al．A lightweight and privacy-preserving authentication protocol for mobile edge computing[C]//IEEE Global Communications Conference (GLOBECOM'19)，Waikoloa：IEEE，2019：1-6．

[10] Yang J H，Chang C C．An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem[J]．Computers and Security，2009，28(3-4):138-143．

[11] Burrows M，Abadi M，Needham R M．A logic of authentication in proceedings of the royal society of london a：mathematical，physical and engineering sciences[J]．The Royal Society，1989，426：233-271．