•可信计算与信息安全•

DOI:10.15961/j.jsuese.201700635

# 基于身份盲签名的无线Mesh网络匿名切换认证方案

许　力[1,2], 王栋城[1,2], 苏彬庭[1,2], 王　峰[1,2]

(1.福建师范大学 数学与信息学院, 福建 福州 350007; 2.福建省网络安全与密码技术重点实验室, 福建 福州 350007)

**摘　要**:无线Mesh网络客户端的强移动性使得其需要在无线Mesh路由器之间进行频繁切换。为了解决当前无线Mesh网络中的切换认证方案无法同时实现高效率和高隐私保护的问题,利用密码学中的基于身份盲签名的思想,提出了一种具有隐私保护的高效的无线Mesh网络匿名切换认证方案。首先,无线Mesh路由器向认证服务器发送自己的身份标识获取用于生成用户假名时所使用的公私钥对。其次,无线Mesh客户端通过向无线Mesh路由器发送盲消息请求切换认证过程中所需要的假名。最后,无线Mesh客户端向目标路由器发送预先获取的假名完成切换认证。一方面,本方案利用基于身份的密码技术,有效地减少了整个网络系统由于传统公钥证书的生成、管理、撤销所产生的消耗。另一方面,本方案通过盲签名技术,使得客户端只需使用提前获得的假名进行切换认证,在实现对用户的真实身份信息与运动轨迹保密的同时,能有效地对客户端的数据隐私进行保护。安全分析表明该方案满足双向认证、匿名性、可撤销性和抵抗攻击性等安全要求;性能分析表明,本方案中无复杂的双线性对运算,而且仅需两次握手就能实现切换认证过程。与其他方案相比较,能有效地降低通信代价并减少计算次数,进而减轻认证服务器的负载以及提高认证效率。

**关键词**:无线Mesh网络; 认证; 数据隐私; 密码学

**中图分类号**:TP393; TN915.08　　**文献标志码**:A　　**文章编号**:2096-3246(2018)02-0148-06

# Anonymous Handover Authentication Scheme Based on Identity-based Blind Signature for Wireless Mesh Networks

*XU Li*[1,2], *WANG Dongcheng*[1,2], *SU Binting*[1,2], *WANG Feng*[1,2]

(1.College of Mathematics and Informatics,Fujian Normal Univ.,Fuzhou 350007,China;
2.Fujian Provincial Key Lab.of Network Security and Cryptology,Fuzhou 350007,China)

**Abstract**: The strong mobility of wireless mesh clients incurs the frequent handover among multiple wireless mesh routers.In order to overcome the problem that current handover authentication schemes cannot achieve high efficiency and privacy protection simultaneously,an efficient anonymous handover authentication scheme with privacy protection was proposed.The proposed scheme was based on the idea of identity-based blind signature in cryptography.Firstly,the wireless mesh router sends its identity to the authentication server to get a key pair that is used to generate the pseudo identities for the wireless mesh client.Secondly,the wireless mesh client sends blind messages to the wireless mesh router to request the pseudo identities that is used in the handover authentication phase.Finally,the wireless mesh client sends a pre-acquired pseudo identity to the target router to complete the handover authentication.The proposed scheme adopted identity-based cryptographic technology,which effectively reduces the whole network consumption caused by the generation,management and revocation of the traditional public key certificate.On the other hand,through the blind signature technique,the client only needs to use thepre-acquired pseudo identity for handover authentication.Using the pseudo identity could protect the confidentiality of the user's true identity information and the moving path,as well as the data privacy of the client.Security analysis showed that the proposed scheme can satisfied the security requirements of mutual authentication,anonymity,revocation and resistance to attacks.Performance analysis showed that the handover authentication process is achieved after two handshakes without

**收稿日期**:2017 – 08 – 06

**基金项目**:国家自然科学基金面上资助项目(61771140); 国家自然科学基金海峡联合基金重点资助项目(U1405255); 福州市科技局资助项目(2015-G-59); 福建省高校产学合作科技重大资助项目(2017H6005); 福建省教育厅资助项目(JAT160123)

**作者简介**:许　力(1970—),男,教授,博士生导师. 研究方向:网络与信息安全;物联网与云计算;智能信息处理;复杂系统和网络的建模与仿真 E-mail: xuli@fjnu.edu.cn

**网络出版时间**: 2018-03-21 12:39:19　　**网络出版地址**: http://kns.cnki.net/kcms/detail/51.1773.TB.20180321.1239.006.html

pairing operations.Comparing with other schemes,the proposed scheme effectively reduces the communication cost and the number of calculation times,lightens the load of authentication server,and improves the authentication efficiency as well.

**Key words**: wireless Mesh networks;authentication;data privacy;cryptography

无线Mesh网络(wireless Mesh networks, WMNs)作为新一代无线网络的关键技术之一, 近几年广泛获得人们的认可和应用。如图1所示, WMNs由无线Mesh路由器(Mesh routers, MR)和无线Mesh客户端(Mesh client, MC)组成, 其中, MR构成了WMNs的骨干网, 其具有极小的移动性, 为具有较高移动性的MC提供网络接入服务。与传统无线网络架构相比, WMNs具有前期部署成本低、网络维护简单、较强的鲁棒性、服务范围可靠等优势[1–2]。

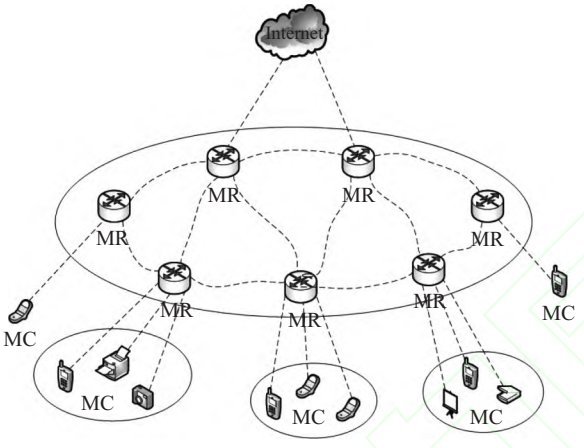


**图 1　无线Mesh网络**

**Fig.1　Wireless mesh network**

为了保证无线Mesh客户端在移动过程中通信的持续性, 高效率的切换认证协议是必不可少的。由于移动节点在移动过程中容易被窃听、破坏或劫持, 所以在保证切换效率的同时还要加强用户的数据隐私保护, 所以切换认证协议要满足一定的安全性[3–7]: 1)双向认证。不仅MC要验证目标MR的合法性, MR也要验证MC的合法性。2)会话密钥建立。切换认证结束后, MC与目标MR要建立会话密钥, 保证以后通信的安全性。3)匿名性。弱用户匿名性, 即切换过程中, 要保护认证节点的隐私使路由器无法知道认证节点的真实身份; 强用户匿名性, 即在满足弱用户匿名性的前提下, 并且无法判断该认证节点是从哪个路由器切换过来的。4)可撤销性。认证服务器可撤销不安全用户与过期的用户, 不再为其提供网络服务。5)抵抗攻击。能够抵抗各种已知攻击, 满足安全性要求。

为实现MC的安全快速切换, 相关学者陆续提出了许多的切换认证方案[8–16]。基于标签的无线Mesh网络的切换认证方案[8–9]以及文献[10–11]方案均在切换认证过程中无复杂的双线性对运算, 能有效地降低认证时延, 提高认证效率, 但是这些方案都无法解决用户的隐私问题, 在认证过程中敌手能通过捕获数据包的方式, 获得MC的所有真实身份信息以及用户的运动轨迹。文献[12–14]方案虽然能有效地保护用户的隐私, 达到安全性要求, 但是这些方案都需要进行复杂的双线性对运算, 会极大地增加计算所产生的能耗, 增加认证时延。文献[15–16]方案在实现保护用户隐私的前提下, 无须复杂的双线性对运算, 提高了认证效率, 但这些方案在切换认证过程中至少需要经过3次握手才能完成切换认证过程, 增加了通信代价, 也会增加认证时延。

针对上述文献中存在的隐私泄露和切换认证过程代价太高等问题, 提出了一种采用基于身份盲签名的切换认证方案。首先, 认证节点只需在完成第一次接入网络之后, 向当前MR请求用于切换认证的假名; 然后, 在切换认证过程中只需通过发送预先获取的假名完成匿名切换, 由于盲签名的特点, 在该过程中能有效解决用户的数据隐私泄露问题; 最后, 通过安全分析和效率分析, 证明所提出的方案能有效保护用户的隐私和具有较高的切换效率。

## 1　切换认证方案

由于Mesh客户端用户的移动性, 为了保证网络服务质量, 设计一种安全高效的切换认证协议是很有必要的。使用基于身份盲签名, 在系统初始化阶段, 每个MR都向认证服务器(authentication server, AS)发送自己的身份信息, 获取私钥。认证服务器一般位于Internet层, 用于提供授权接入服务。在客户端完成第一次授权接入后, 通过向当前接入的路由器请求用于下次切换认证的假名。在再认证阶段, 只需要向目标路由器发送预先获得的假名, 通过2次握手就能完成匿名切换过程。根据网络自身的情况, 可以选择适合自己网络的基于身份盲签名方案, 本文的方案采用He等[17]提出的基于身份盲签名方案进行构造。

### 1.1　系统初始化阶段

在系统初始化阶段, AS执行密钥生成算法生成自己的公私钥, 然后用自己的私钥根据每个MR发送过来的身份信息为每个MR生成用于签名的私钥, 密钥获取过程所交换的参数如图2所示。首先, AS计算系统参数; 然后, MR向AS发送身份标识获取公私钥对。

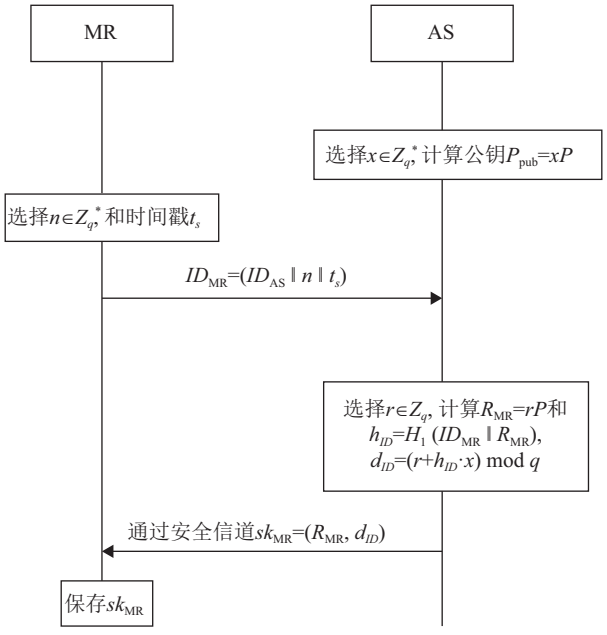


**图 2 密钥获取过程**

**Fig.2 Process of key acquisition**

具体步骤如下：

1）AS选择系统参数，确定椭圆曲线以及散列函数。AS选择大素数$p$和$q$，$E/F_p$是定义在有限域$F_p$上的椭圆曲线，选择椭圆曲线$E/F_p$上的一个阶为$q$的点$P$，生成循环加法群$G$，选择散列函数$H_1:\{0,1\}^*\times G\rightarrow Z_q^*, H_2:\{0,1\}^*\rightarrow Z_q^*$。

2）AS计算系统公私钥对。AS随机选择一个参数$x\in Z_q^*$，作为私钥，然后计算公钥$P_{pub}=xP$。公开系统参数$\{q,p,E/F_p,P,G,P_{pub},H_1,H_2\}$。

3）MR向AS获取自己的公私钥对。MR选择随机数$n\in Z_q^*$，将身份信息$ID_{MR}=(ID_{AS}\|n\|t_s)$，发送给AS获取用于签名的私钥，其中$t_s$为时间戳。

4）AS为每个MR计算公私钥对。AS收到某个MR发送过来的身份信息后，选择随机数$r\in Z_q^*$，计算$R_{MR}=rP$和$h_{ID}=H_1(ID_{MR}\|R_{MR})$，$d_{ID}=(r+h_{ID}\cdot x)\bmod q$，该MR的私钥$sk_{MR}=(R_{MR},d_{ID})$；然后，AS将该私钥通过安全信道发送给MR进行秘密保存。

### 1.2 假名获取阶段

通过与当前为其提供网络接入服务的MR进行交互，获取用于切换认证过程所使用的假名，该阶段所交换的参数如图3所示。首先，MC接收来自MR的参数并计算盲消息发送给MR；然后，MR对盲消息进行盲签名；最后，MC对盲签名进行脱盲获得最后的假名。具体步骤如下：

1）客户端通过执行传统的认证协议，首次接入网络。这个过程执行完后，MC和MR共享一个会话密钥$PMK_{MC-MR}$；MR和AS之间共享会话密钥$PMK_{MR-AS}$。

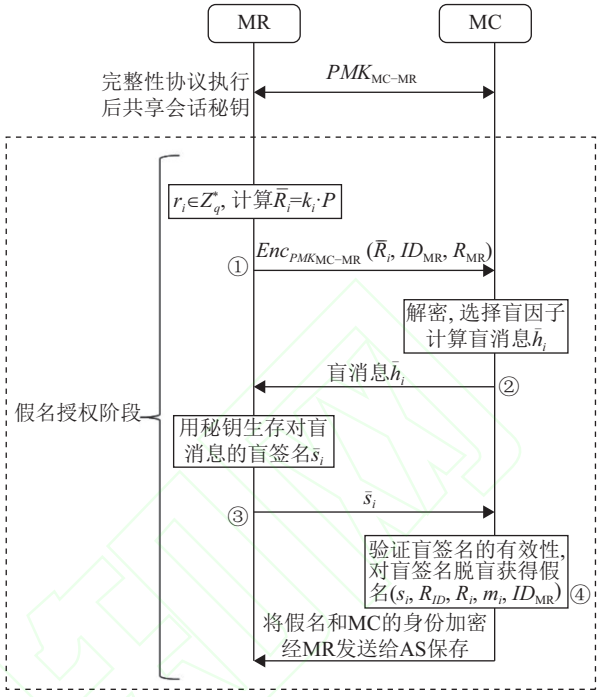


**图 3 假名获取过程**

**Fig.3 Process of pseudo identity acquisition**

2）MC通过与MR的交互获得用于下次切换认证的假名。每个假名仅允许使用一次，假名使用完后，需要与当前为其服务的MR获取假名。获取假名的具体步骤如下：

①MR为MC计算用于生成盲消息的参数。MR随机选择$i$个随机数$k_i\in Z_q^*$，$i=(1,2,3,\cdots)$，计算$\bar{R}_i=k_iP$，通过会话密钥$PMK_{MC-MR}$对$(\bar{R}_i,ID_{MR},R_{MR})$加密，得$c_{Mes1}=Enc_{PMK_{MC-MR}}(\bar{R}_i\|ID_{MR}\|R_{MR})$，将$c_{Mes1}$发送给MC。

②MC计算盲消息并发送给MR获取盲签名。MC接收到消息后，用$PMK_{MC-MR}$解密获得$(\bar{R}_i,ID_{MR},R_{MR})$；接着，MC随机选择$i$组随机数$a_i,b_i,\alpha_i,\beta_i,\gamma_i\in Z_q^*$，计算$h_{ID}=H_1(ID_{MR}\|R_{MR})$，$R_i=\alpha_i\bar{R}_i+\beta_iP+\gamma_i(R_{MR}+h_{ID}P_{pub})$，$h_i=H_1(m_i\|R_i)$，$m_i=(b_i\|A)$，其中$A=a_iP$；然后，计算$\bar{h}_i=(\alpha_i^{-1}(h_i+\gamma_i))\bmod q$，并将盲消息$(\bar{h}_1,\bar{h}_2,\cdots,\bar{h}_i)$发送给MR。

③MR对MC发送过来的盲消息进行盲签名。当MR接收到盲消息后，对盲消息进行签名得$\bar{s}_i=(\bar{h}_id_{ID}+k_i)\bmod q$，将盲签名$(\bar{s}_1,\bar{s}_2,\cdots,\bar{s}_i)$发送给MC。

④MC对盲签名进行脱盲获得最后的假名。MC接收到盲签名$\bar{s}_i$之后，验证盲签名的有效性$\bar{s}_iP=\bar{h}_i(R_{MR}+h_{ID}P_{pub})+\bar{R}_i$，当等式成立时，对盲签名进行脱盲得$s_i=(\alpha_i\bar{s}_i+\beta_i)\bmod q$，得到脱盲后的签名即$i$个假名$(s_i,R_{MR},R_i,m_i,ID_{MR})$；然后，MC用AS的公钥$i$个假名以及自己的身份进行加密$c_{MC-AS}=Enc_{P_{pub}}(\bar{s}_1,\bar{s}_2,\cdots,\bar{s}_i,ID_{MC})$，其中，$ID_{MC}$为MC的真实身份信息，被发送给MR，再由MR发送给AS进行假名登记保存。

### 1.3 再认证阶段

由于环境原因或者客户端的移动, 为了提供更好的服务, 必须切换到通信质量更好的MR, 本方案经过两次握手就能完成MC的切换认证过程。再认证的参数交换如图4所示。首先, MC选择一个通信质量最好的MR将假名发送给其请求切换; 然后, 该MR验证MC假名的合法性, 如果合法再向MC发送签名证明自己的身份。

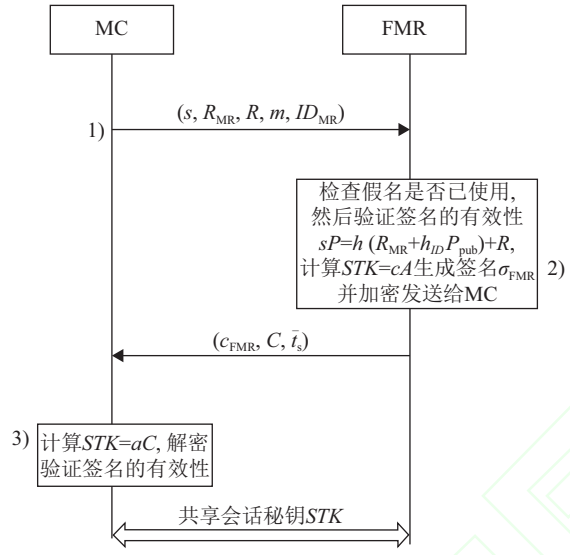


**图 4　再认证过程**

**Fig.4　Handover process**

具体步骤如下:

1)MC通过发送预先获得的假名请求切换认证。MC选择通信质量最好的MR进行切换请求, MC首先将之前获得的假名中的一个$(s,R_{MR},R,m,ID_{MR})$发送给目标MR(此阶段中将目标MR称为FMR), 请求接入。

2)FMR验证MC的合法性决定是否允许MC的接入, 并且向MC证明自己的合法性。FMR接收到消息后, 首先, 检查假名的使用情况, 如果假名已使用则拒绝MC接入, 如果假名有效, 根据式(1)验证签名的有效性, 当且仅当验证通过才证明MC是合法的, 才允许MC的接入请求。接着, 选择随机数$c \in Z_q^*$与时间戳$\bar{t}_s$, 计算$C=cP$, 根据消息$m$中的$A$计算临时会话密钥$STK=cA$。然后, 用之前跟AS交互获得的私钥进行签名得$\sigma_{FMR}=c+H_1(R_{FMR}\|C\|\bar{t}_s)\cdot d_{ID}$, 用$STK$加密$c_{FMR}=Enc_{STK}(\sigma_{FMR}\|ID_{FMR}\|R_{FMR})$, 并将$(c_{FMR},C,\bar{t}_s)$发送给MC证明自己的身份。

$$sP=h(R_{MR}+h_{ID}P_{pub})+R \tag{1}$$

其中, $h=H_2(m\|R)$, $h_{ID}=H_1(ID_{MR}\|R_{MR})$。式(1)的具体计算步骤如下:

$$\begin{aligned}
s&=\alpha\bar{s}+\beta \bmod q,\\
sP&=(\alpha\bar{s}+\beta)P=(\alpha\cdot(\bar{h}\cdot d_{ID}+k)+\beta)P=\\
&\quad(\alpha\cdot((\alpha^{-1}(h+\gamma))\cdot d_{ID}+k)+\beta)P=\\
&\quad(\alpha\cdot k+(h+\gamma)\cdot d_{ID}+\beta)P=\\
&\quad(\alpha\cdot k+h\cdot d_{ID}+\gamma\cdot d_{ID}+\beta)P=\\
&\quad(h\cdot d_{ID})P+(\alpha\cdot k+\gamma\cdot d_{ID}+\beta)P=\\
&\quad h(R_{MR}+h_{ID}P_{pub})+R。
\end{aligned}$$

3)MC验证FMR的合法性决定是否接入网络。MC接收到消息后, 首先计算$STK=aC$, 用$STK$解密获得$(\sigma_{FMR},ID_{FMR},R_{FMR})$; 然后, 验证签名的有效性$\sigma_{FMR}P=H_1(R_{FMR}\|C\|\bar{t}_s)\cdot(R_{FMR}+h_{ID}P_{pub})+C$, 其中, $h_{ID}=H_1(ID_{FMR}\|R_{FMR})$, 当且仅当等式成立, 即验证通过, 则证明FMR是合法的, 确定接入。至此MC通过与FMR的2次握手就能实现切换认证。

## 2 安全分析

作者提出的方案中, 客户端通过之前获取的假名验证自己的身份的有效性, 用于计算临时会话密钥的随机数都是客户端和路由器自己选择的, 敌手无法计算出。所以, 客户端能通过假名达到对自己真实信息和运动轨迹的保护。下面将从双向认证、密钥协商安全性、匿名性、可撤销性、抗攻击性对本方案进行安全分析。

### 2.1 双向认证

切换认证过程需要Mesh路由器和Mesh客户端相互确认对方的合法性才允许接入和允许被接入。本方案中, 当MC请求切换到新的MR时, 首先, 向目标MR(FMR)发送假名获取阶段获得的已经由其他MR签名过的假名$(s,R_{MR},R,m,h_{ID})$以请求接入网络, 并对FMR进行挑战。当FMR接收到消息后, 开始时只有假名有效, 并且根据式(1)验证签名的有效性, 只有验证通过才表示该MC是合法的; 然后, FMR用自己从AS获得的密钥进行签名, 并且根据Diffee-Hellman交换获得的对称密钥对签名进行加密发送给MC, 当且仅当能解密获得签名以及签名验证能通过才能证明FMR是合法的。这就达到了客户端和路由器的双向认证。

### 2.2 密钥协商安全性

由于在再认证阶段, 最后计算的临时会话密钥$STK$是通过Diffee-Hellman密钥交换协议获得的, 用于计算最后$STK$的随机数都由MC和MR自己选择, 所以, 只有MC和MR才能计算出$STK$, 能有效地保证会话密钥的安全性。

### 2.3 匿名性

在本方案中, 使用了盲签名。用户计算的盲消息$\bar{h}_i$与客户端的真实身份信息和消息$m_i$是统计无关的;

当客户端获得盲签名后，对盲签名进行脱盲后获得的假名与盲签名也是统计无关的。所以除了用户自己，其他人在假名获取阶段能够得到的消息只有盲消息$\bar{h}_i$和盲签名，而这些消息与切换认证过程中客户端使用的假名，除了用户自己，其他人没有办法将它们关联起来，并且客户端每次切换认证使用的假名都是不同的，所以就能实现用户的身份匿名。另外，每个假名中的$R_{MR}$是AS产生的，只有AS能够将$R_{MR}$与MR对应起来，且$ID_{MR}$是由MR产生并秘密保存的，故敌手和目标MR是无法通过假名判断该认证节点是从哪个路由器切换过来的，所以本方案具有强用户匿名性。

### 2.4 可撤销性

由于所有的$R_{MR}$都是由AS产生的，所以AS可以实现对MR的管控和撤销。而当MC向MR请求假名之后，必须将假名与自己的身份信息采用加密的方式通过当前接入的MR发送给AS进行假名注册，所以AS也可以实现对MC的管控和撤销。

### 2.5 抗攻击性

在无线Mesh网络通信中，要阻止窃听者捕获到通信的数据包是很困难的，即使能做到代价也是难以接受的。在本方案中，窃听者依然能够捕获到用户通信的数据包，但是，因为所有的通信数据包都通过加密的形式发送，所以即使捕获到数据包，没有密钥也不能解密获得明文即通信内容。

1）抗重放攻击：在消息中，每个消息都嵌入了随机数，并且通过数字签名使用挑战–应答的方式验证，每个用于切换认证的假名都仅允许使用一次，所以重放的消息不能通过验证，并且攻击者不能通过重放的消息计算出$STK$。2）抗中间人攻击：用于计算会话密钥$STK$的参数嵌入在数字签名中，修改用于计算会话密钥的参数会导致验证不通过，也就无法证明自己是个有效的用户，所以攻击者无法通过篡改用于计算$STK$的参数计算出最后的临时会话密钥。

## 3 性能分析

切换认证协议不仅要保证整个认证过程安全性，还要提高认证过程的效率减少认证时延。而且本文方案在保证切换认证的安全性和认证效率的前提下，还有效地减少了整个网络系统的负载。

通过基于身份的机制，能有效地减少整个网络系统由于传统公钥证书的生成、管理、撤销所产生的消耗。只需在客户端首次接入后，从当前为其提供服务的MR获取用于下次切换认证的假名。与文献[6,18]方案对比，这些方案都需要与AS进行交互，获取用于下次切换的假名，而作者提出的方案相当于将AS的部分权力授予MR，让MR为客户端计算假名，这样能有效的减轻AS的负载，充分发挥无线Mesh网络中MR的性能。并且由于AS对于MC而言是位于多跳之外的，而当前接入的MR是一跳的，所以能减少传输代价。

从隐私保护的角度出发，将本文方案与其他具有隐私保护的方案[12–13,19]进行比较。结果如表1所示。由于简单的运算对于切换认证的时延影响很小，主要考虑复杂的双线性对运算Pairng（用$T_P$表示）、椭圆曲线运算ECC（用$T_E$表示）、握手次数$T_H$以及匿名性强弱。这两种较为复杂的运算所需的时间也是相差较大的，执行一次双线性对运算所需时间大约为20.04 ms，而执行一次椭圆曲线点乘运算的时间大约为2.21 ms[20]。其中，匿名性的弱强对应弱用户匿名性和强用户匿名性，文献[12]–W方案和文献[12]–S方案分别表示文献[12]中具有弱用户匿名性和具有强用户匿名性的切换认证方案。

表 1 各方案性能分析与比较

Tab.1 Performance analysis and comparison of each scheme

| 方案 | $T_H$ | $T_P$ | $T_E$ | 匿名性 | 总时延 |
|---|---|---|---|---|---|
| 文献[12]–W方案 | 3 | 0 | 4 | 弱 | $3T_H+8.84$ ms |
| 文献[12]–S方案 | 3 | 3 | 8 | 强 | $3T_H+77.8$ ms |
| 文献[13]方案 | 2 | 4 | 2 | 强 | $2T_H+84.58$ ms |
| 文献[19]方案 | 2 | 0 | 8 | 强 | $2T_H+17.68$ ms |
| 本文方案 | 2 | 0 | 7 | 强 | $2T_H+15.47$ ms |

## 4 结 论

网络安全问题在信道开放的无线网络中，一直是人们关注的焦点。为了解决无线Mesh网络切换认证过程中移动节点的隐私问题，提出了一种采用基于身份盲签名的匿名切换认证方案，客户端通过与当前为其服务的MR进行交互，获取用于切换认证的假名，达到匿名切换认证的效果，能有效地保护客户端的隐私。切换认证过程经过2次握手就能完成，且认证过程无复杂的双线性对运算，通信代价低，认证效率较高。在未来的工作中，将进一步研究在多个客户端同时认证场景下的切换认证方案。

**参考文献：**

[1] Fowler T.Mesh networks for broadband access[J].IEE Review,2001,47(1):17–22.

[2] Akyildiz I F,Wang Xudong,Wang Weilin.Wireless Mesh networks:A survey[J].Computer Networks,2005,47(4):445–487.

[3] He Daojing,Chen Chun,Chan S,et al.Secure and efficient handover authentication based on bilinear pairing functions[J].

IEEE Transactions on Wireless Communications,2012,11(1):48–53.

[4] Han Qi,Zhang Yinghui,Chen Xiaofeng,et al.Efficient and robust identity-based handoff authentication in wireless networks[C]//Proceedings of the 6th International Conference on Network and System Security (NSS'12).Wuyishan:Springer,2012:180–191.

[5] Wan Zhiguo,Ren Kui,Preneel B.A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks[C]//Proceedings of the 2008 ACM First Conference on Wireless Network Security (WISEC).Alexandria:ACM,2008:62–67.

[6] He Daojing,Chan S,Guizani M.Handover authentication for mobile networks:Security and efficiency aspects[J].IEEE Network,2015,29(3):96–103.

[7] Ren Wei.On the basic discussion of wireless network security[J].Netinfo Security,2012(1):10–13.[任伟,无线网络安全问题初探.无线网络安全问题初探[J].信息网络安全,2012(1):10–13.]

[8] Su Binting,Xu Li,Fang He,et al.Fast authentication mechanism based on Diffie-Hellman for wireless mesh networks[J].Journal of Shandong University(Natural Science),2016,51(7):6–11.[苏彬庭,许力,方禾,等.基于Diffie-Hellman 的无线Mesh网络快速认证机制研究[J].山东大学学报,2016,51(7):6–11.]

[9] Xu Li,He Yuan,Chen Xiaofeng,et al.Ticket-based handoff authentication for wireless mesh networks[J].Computer Networks,2014,73(C):185–194.

[10] Li C,Nguyen U T,Nguyen H,et al.Efficient authentication for fast handover in wireless mesh networks[J].Computers and Security,2013,37(3):124–142.

[11] Li Guangsong,Chen Xi,Ma Jiangfeng.A ticket-based re-authentication scheme for fast handover in wireless local area networks[C]//Proceedings of the 2010 IEEE 6th International Conference on Wireless Communications Networking and Mobile Computing (WiMob).Niagara Falls:IEEE,2010:1–4.

[12] Yang Guomin,Huang Qiong,Wong Duncan,et al.Universal authentication protocols for anonymous wireless communications[J].IEEE Transanctions on Wireless Communications,2010,9(1):168–174.

[13] Tsai J,Lo N,Wu T.Secure handover authentication protocol based on bilinear pairings[J].Wireless Personal Communications,2013,73(3):1037–1047.

[14] Kim Y,Ren Wei,Jo J Y,et al.SFRIC:A secure fast roaming scheme in wireless lan using ID-based cryptography[C]//Proceedings of the 2007 IEEE International Conference on Communications (ICC'07).Glasgow:IEEE,2007:1570–1575.

[15] Zhu Haojin,Lin Xiaodong,Shi Minghui,et al.PPAB:A privacy-preserving authentication and billing architecture for metropolitan area sharing networks[J].IEEE Transactions on Vehicular Technology,2009,58(5):2529–2543.

[16] Fu Anmin,Zhang Yuqing,Zhu Zhenchao,et al.An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network[J].Computers & Security,2012,31(6):741–749.

[17] He Debiao,Chen Jianhua,Zhang Rui.An efficient identity-based blind signature scheme without bilinear pairings[J].Computers & Electrical Engineering,2011,37(4):444–450.

[18] Chaudhry S,Farash M,Naqvi H,et al.A robust and efficient privacy aware handover authentication scheme for wireless networks[J].Wireless Personal Communications,2017,93(2):1–25.

[19] Islam S,Khan M.Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks[J].International Journal of Communication Systems,2016,29:2442–2456.

[20] He Debiao,Chen Jianhua,Hu Jin.An id-based proxy signature schemes without bilinear pairings[J].Annals of Telecommunication,2011,66(11/12):657–662.

（编辑　赵　婧）

**引用格式**: Xu Li,Wang Dongcheng,Su Binting,et al.Anonymous handover authentication scheme based on identity-based blind signature for wireless mesh networks[J].Advanced Engineering Sciences,2018,50(2):148–153.[许力,王栋城,苏彬庭,等.基于身份盲签名的无线Mesh网络匿名切换认证方案[J].工程科学与技术,2018,50(2):148–153.]