doi:10.11959/j.issn.1000-436x.2016264

基于群签名的无线 Mesh 网络匿名切换认证方案

苏彬庭[1,2]，许力[1,2]，王峰[1,2]，林志兴[1,2,3]

（1. 福建师范大学数学与计算机科学学院，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； 3. 三明学院现代教育技术中心，福建 三明 365004）

摘 要：为保证 Mesh 网络移动客户端视频、语音等实时性强的业务不中断，一种快速安全的切换认证策略显得非常重要。从保护移动节点的隐私信息出发，提出了一种基于群签名的无线 Mesh 网络匿名切换认证方案。与其他基于群签名的切换认证方案不同，该方案中切换认证过程不涉及群签名相关运算，且群签名运算只在路由器上进行。该方案不仅满足了安全性要求，还具有较高的认证效率和保护用户隐私的优点。

关键词：Mesh 网络；切换认证；认证效率；隐私保护

中图分类号：TP915.08 **文献标识码**：A

Anonymity handover authentication protocol based on group signature for wireless Mesh network

SU Bin-ting[1,2], XU Li[1,2],WANG Feng[1,2],LIN Zhi-xing[1,2]

(1. School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China;
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China;
3. Modern Education Technology Center, Sanming University, Sanming 365004, China)

Abstract: In order to ensure that the Mesh network mobile client video, voice and other real-time strong applications without interruption, a secure and efficient handover authentication was very important. To protect the privacy of mobile nodes, an anonymity handover authentication protocol was proposed based on group signature for wireless mesh network. Compared with other handover authentication protocols based on group signature, the proposed scheme did not involve the group signature correlation operation, and the group signature algorithm was only carried out on the router. The proposed protocol not only enhances the security but also performs well in authentication efficiency and privacy-preserving.

Key words: Mesh network, handover authentication, authentication efficiency, privacy-preserving

1 引言

无线网络发展日新月异，无线 Mesh 网络（WMN，wireless Mesh network）作为一种新型的网络结构，有着自组织、自管理、自愈能力及支持多种网络接入的优势[1,2]。它通过无线链路把固定的和移动的节点连接起来，构成的一个多跳的移动自组织网络，是单跳无线局域网和多跳 ad hoc 网络的融合[1]。然而，由于自身无线通信、多跳传输等性质，无线 Mesh 网络存在的安全问题也十分突出。其中，切换认证技术不仅关乎客户端的通信安全，同时也决定网络资源是否会被滥用。图 1 是无线 Mesh 网络切换认证示意，参与切换认证过程主要有 2 种类型的节点：Mesh 客户端（MC，Mesh client）和 Mesh 路由器（MR，Mesh router）。当 MC 从 MR_1 移向 MR_2 时，实现 MC 的无缝切换从而保证 MC 服务连续性是非常有必要的。为了保证服务的连续性，MC 切换认证应在 50 ms 内完成，其中，认证过程不能

收稿日期：2016-08-31

基金项目：国家自然科学基金资助项目（No.61072080, No.U1405255）；福建省高校产学研合作重大基金资助项目（No.2014H61010105）；福建师范大学科研创新团队基金资助项目（No.IRTL1207）；福州市科技局基金资助项目（No.2015-G-59）

Foundation Items: The National Natural Science Foundation of China (No.61072080, No.U1405255), Major Science and Technology Project in Fujian Province (No.2014H61010105), Fujian Normal University Innovative Research Team Project (No.IRTL1207), Foundation of Fuzhou Municipal Science and Technology Bureau (No.2015-G-59)

超过 20 ms[3]。然而一次完整的 EAP（如 EAP-TLS）认证需要 8 s，会造成一些实时性强的服务中断[4]。如今，随着网络技术的发展和人们对服务要求的提高，切换认证不仅要求高效，还要满足相应的安全性[5~9]。

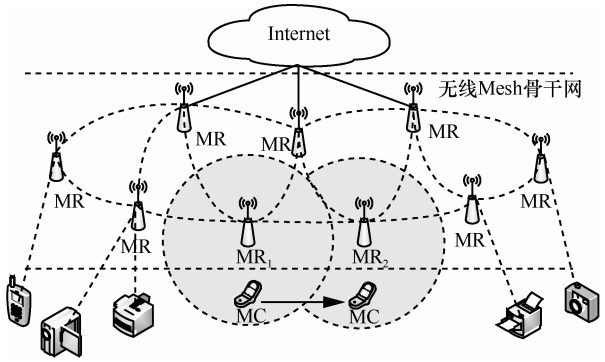


图 1　Mesh 网络切换认证示意

1) 双向认证。MR 需要对用户身份的合法性进行检查，同时，MC 也要验证 MR 是否为安全合法的路由器。

2) 安全密钥建立。完成切换认证后，MC 和 MR 要建立安全的会话密钥。

3) 匿名性和不可关联性。路由器无法确认认证节点的真实身份，并且无法判断该节点在当前 MR 是否认证过。

4) 可追踪性。如果网络出现合法节点的内部攻击，有且仅有认证服务器（AS，authentication server）可通过通信内容确定消息发布者的真实身份。

5) 用户撤销。认证服务器可撤销过期或不安全用户的身份，使其无法继续享受网络的服务。

6) 抵抗攻击。能够抵抗各种攻击，保证协议的安全性。

近几年，针对不同的应用场景和需求，许多切换认证文献[7,10~20]方案被提出。这里，从是否考虑隐私保护将方案分为两大类。1) 无隐私保护的切换认证方案主要从提高用户的认证效率出发，缩短用户的认证时延。文献[7,10~12]方案认证过程需要认证服务器参与，通过 AS 提高认证的安全性，这也是最传统的认证方法。然而该方法可能由于认证服务器的参与，导致在认证过程中，认证消息需要经多跳传输，通信代价较高，认证时延较长。文献[13~15]方案避免了多跳传输而产生的通信代价，在一定程度上提高了认证的效率。然而接入点与用户至少需要至少 3 次握手，认证效率不高。Xu 和 Zhang 等[16,17]提出了基于标签的认证方案。方案通过当前接入点预分发用户的密钥信息给目标接入点，认证过程无第三方参与，且无需复杂的双线性对、群签名等运算，认证效率较高。然而由于用户完成认证后，当前接入点要为邻居接入点计算不同的切换认证密钥，所以接入点的负载较大，且切换密钥的利用率较低。2016 年，苏等[18]提出了基于 Diffie-Hellman 的无线 Mesh 网络快速认证机制，解决了上述存在的问题，但方案会泄露用户的身份信息，导致用户的身份、位置和运动轨迹等隐私信息受到威胁。2) 具有隐私保护的切换认证主要利用群签名、代理签名、盲签名和假名等技术实现用户匿名认证，从而保护用户的身份、位置和运动轨迹等隐私信息安全。文献[9]方案利用群签名来实现隐私保护，但计算代价较高；文献[19,20]方案利用假名技术来实现隐私保护，但用户需要存储很多的假名和相应的密钥，这类方案对于能量和存储能力受限的客户端是不适用的。

本文提出了一种基于群签名的切换认证方案，在该方案中，认证节点每次完成认证后将计算切换密钥并加密发送给接入点，接入点解密再转发给邻居节点保存，用于后期对用户的身份认证。与其他群签名方案不同，该方案认证过程无需群签名相关运算，且只在能量不受限的路由器上进行。认证用户只需简单运算可完成双向认证过程，不仅效率高，同时能够保护认证用户的隐私信息安全。

2　切换认证方案

由于 Mesh 网络客户端有较强的移动性，为保证客户端的安全性和服务的连续性，一种快速安全的切换认证策略显得非常重要。本文在客户端完成首次匿名接入认证[21]后，客户端计算下一次切换认证密钥，并通过会话密钥加密发送给当前接入点，由当前接入点解密，并产生对应的群签名[22]，匿名发送给邻居节点。在客户端请求切换认证时，路由器只需通过缓存中的预分发的切换密钥与客户端经 2 次握手可快速完成切换认证过程。

2.1　系统初始化

在系统初始化过程中，AS 输入安全参数 k 执行密钥生成算法，为网络各节点创建公私钥对。

1) 选择一大素数 q 和 p，$\frac{E}{F_p}$ 是定义在有限域 F_p 上的椭圆曲线。选择 $\frac{E}{F_p}$ 上的一个阶为 q 的点 P，生成循环加法群 G。

2) 随机选择参数 $s\in Z_q^*$，计算系统公钥 $PK=sP$。

3) 选择散列函数 $H_1:\{0,1\}^*\to Z_q^*$，$H_2:\{0,1\}^*\times G\to Z_q^*$。

4) 输入参数，执行密钥生成算法，产生群公钥 gpk 和各群成员私钥 gsk_i。

5) 公开系统参数 $\{q,p,\frac{E}{F_p},P,G,PK,H_1,H_2,gpk\}$。

AS 利用系统参数为网络中每个路由器创建公私钥对。假设 ID_{MR} 为路由器 MR 的唯一身份标识。AS 选择随机数 $r_{\mathrm{MR}}\in Z_q^*$，计算 $R_{\mathrm{MR}}=r_{\mathrm{MR}}P$，$h_{\mathrm{MR}}=H_1(ID_{\mathrm{MR}},R_{\mathrm{MR}})$ 和 $s_{\mathrm{MR}}=r_{\mathrm{MR}}+sh_{\mathrm{MR}}$，然后将 $(s_{\mathrm{MR}},R_{\mathrm{MR}})$ 通过安全通道发给 MR。MR 收到密钥后，计算公钥 $PK_{\mathrm{MR}}=s_{\mathrm{MR}}P$ 并定期广播自身信息 $(ID_{\mathrm{MR}},R_{\mathrm{MR}})$。

2.2 认证过程

客户端在移动过程中，可能由于信号变弱等因素而选择接入更合适的路由器。本文利用客户端在每次认证后，计算切换密钥，并由当前接入的路由器预分发给周边路由器保存。当客户端向周边路由器请求切换认证时，只要利用缓存中预分发的切换密钥快速完成认证过程，很大程度提高了认证效率。切换认证过程如图 2 所示。

1) $\mathrm{MC}\to\mathrm{MR}_2:\{ID_{\mathrm{MR}_2},A,B,ts,\sigma_1\}$

客户端对周边的路由器进行评估，选择最合适的 MR 并发起切换认证请求。MC 选择时间戳 ts，然后利用之前计算的切换密钥产生签名 $\sigma_1=a+bH_1(ID_{\mathrm{MR}_2}\|A\|ts)$，并将消息 $\{ID_{\mathrm{MR}_2},A,B,ts,\sigma_1\}$ 发送给目标路由器 MR_2 请求认证。

2) $\mathrm{MR}_2\to\mathrm{MC}:\{m,\sigma_2\}$

MR_2 收到 MC 的认证请求后，首先判断时间戳 ts 是否过期，如果没过期，则从缓存中找出与 MC 对应的切换密钥消息，根据式(1)判断签名 σ_1 的合法性。如果签名是合法的，随机选择 $c\in Z_q^*$ 计算 $C=cP$，生成消息 $m=\{ID_{\mathrm{MR}_2},R_{\mathrm{MR}_2},B,C\}$，利用系统分配的密钥对 $(s_{\mathrm{MR}},R_{\mathrm{MR}})$ 产生签名 $\sigma_2=r_2+s_{\mathrm{MR}_2}H_1(m)$。最后将消息 $\{m,\sigma_2\}$ 发送给客户端验证，并计算密钥 PMK (pairwise master key)，$PMK_{\mathrm{MR}_2}=cB$。

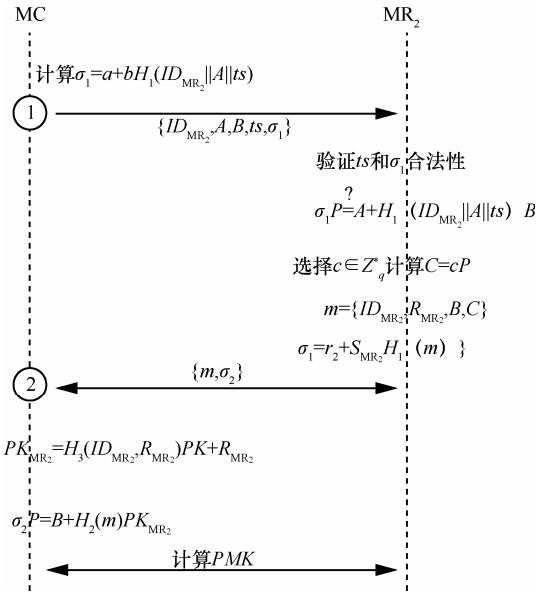


图 2 切换认证过程

$$\sigma_1P\overset{?}{=}A+H_1(ID_{\mathrm{MR}2}\|A\|ts)B \tag{1}$$

客户端收到路由器 MR_2 回应消息 $\{m,\sigma_2\}$，根据式(2)计算路由器的公钥，然后利用系统公开参数 P 根据式(3)验证签名 σ_2 是否合法。如果合法，则计算临时会话密钥 $PMK_{\mathrm{MC}}=bC$ 开始数据业务。

$$PK_{\mathrm{MR}_2}=H_3(ID_{\mathrm{MR}_2},R_{\mathrm{MR}_2})PK+R_{\mathrm{MR}_2} \tag{2}$$

$$\sigma_2P\overset{?}{=}B+H_2(m)PK_{\mathrm{MR}_2} \tag{3}$$

2.3 切换认证密钥预分发

客户端 MC 与路由器 MR_2 完成认证后，协商临时会话密钥开始数据业务。为了提高下次的切换效率，客户端将预计算切换认证密钥，然后由 MR_2 发送给周边路由器保存，如图 3 所示。

1) $\mathrm{MC}\to\mathrm{MR}_2:K_{\mathrm{handover}}$

MC 随机选择 $a,b\in Z_q^*$，计算 $A=aP$ 和 $B=bP$。然后将切换密钥参数根据式(4)加密发送给 MR_2。

$$k_{\mathrm{handover}}=Enc(PMK,\mathrm{MR}_1\|A) \tag{4}$$

2) $\mathrm{MR}_2\to\mathrm{MR}_i:\{A,ts,\sigma\}$

MR_2 首先利用临时会话密钥解密消息，获得切换密钥。再利用群私钥 gsk_{MR_1} 产生群签名 σ，将该签名和切换密钥一起发送给邻居节点，并将该切换密钥与下一次的切换密钥利用系统公钥 PK 加密发

送给认证服务器登记保存。

$$\sigma=\mathrm{Sign}(gsk_{\mathrm{MR}_2}, A\|ts) \quad (5)$$

邻居节点收到 MR_2 发来的消息，首先根据时间戳判断消息是否被重放。如果没有，则利用群公钥 *gpk* 判断该签名是否是群成员产生的。如果是，则保存该切换密钥。

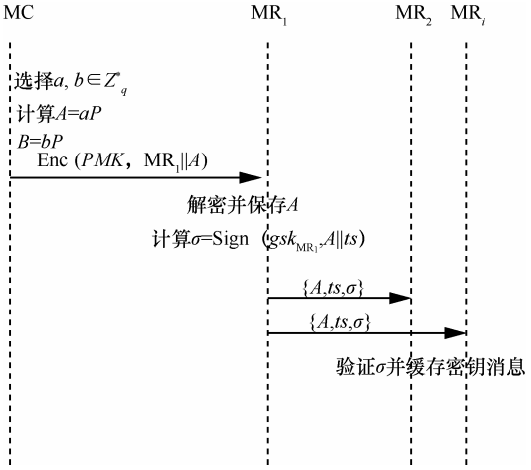


图 3　切换密钥预分发过程

3　安全性分析

本文提出的方案在切换过程中，路由器利用切换密钥验证用户的合法性。切换密钥由用户自己生成并加密发给路由器，由路由器匿名转发给邻居节点。不仅保护了切换密钥的安全性，同时，也防止用户的移动轨迹等隐私信息遭到泄露。从密钥协商安全性、匿名性和不可关联性等几方面分析方案的安全性。

1) 双向认证和密钥协商安全性

在客户端完成认证之后，客户端 MC 选取切换密钥参数 $a\in Z_q^*$，计算 $A=aP$ 并通过加密发给当前路由器 MR_1。在请求切换认证时，MC 利用密钥参数 a 产生签名 σ_1 发给目标接入点。因为切换密钥参数 a 是 MC 自身选取的，所以只有 MC 能够产生有效签名 σ_1。切换目标 MR_2 可利用预分发的切换密钥 A 验证客户端的合法性。而 MR_2 则利用系统分发的密钥 $(s_{\mathrm{MR}}, R_{\mathrm{MR}})$ 产生签名 σ_2，攻击者是无法生成或修改的。*MC* 可利用系统公开参数 P 判断目标接入点是否合法。若认证双方都是合法的，则计算密钥 *PMK*。

$$PMK_{\mathrm{MN}}=bC=cB=PMK_{AP}$$

2) 匿名性和不可关联性

完成匿名接入认证后，MC 在每次请求切换认证时，选取的切换密钥参数都是不同的，且参数是不相关联的。认证过程交互的信息没有涉及与认证节点相关的身份信息，从而较好地保护了认证节点的隐私安全。在 MC 加密发送切换密钥给当前路由器时，接入点利用群私钥产生群签名，匿名发送给周边路由器。因此完成切换认证后，目标接入点和窃听者都无法判断用户是从哪一个路由器切换过来的，保护了认证用户的轨迹隐私安全。同时，攻击者与路由器无法判断任何 2 次的认证过程是否是属于同一用户。

3) 可撤销性

路由器利用缓存的切换密钥 *A*'验证客户端的合法性，并完成与客户端的下一次切换密钥 *A* 的协商后，路由器将切换密钥消息(*A*', *A*)加密发送给认证服务器，实现后期对客户端身份的撤销。

4) 抗重放攻击

客户端在请求切换的消息中，加入了时间戳 *ts*，并产生了对应的签名，因此，攻击者即使截取了认证消息，也无法伪装客户端，获得路由器的信任。而在路由器应答客户端消息中，每次认证随机数 *C* 都是不同的，因此方案能够有效地抵抗重放攻击。

5) 抗中间人攻击

目标路由器在客户端切换认证前，已经预存了客户端的切换密钥消息 *A*。只有知道切换密钥参数 *a* 的客户端才能产生合法的签名 σ_1 并通过目标接入点的认证。而路由器则是通过系统分发的密钥 $(s_{\mathrm{MR}}, R_{\mathrm{MR}})$ 产生签名 σ_2，攻击者是无法产生的。

4　性能分析

切换认证方案不仅要保证认证双方的安全性，同时也要提高认证效率，保证客户端语音、视频等实时性强服务的连续性。本文方案客户端预计算切换密钥并加密发送给当前路由器，路由器解密后匿名发送给周边接入点保存。在客户端切换认证过程中，只需通过切换密钥经 2 次握手可与目标路由器完成切换认证过程。从预分发密钥角度出发，将本文方案与相关文献[16~18]方案的性能进行比较分析，文献[16~18]方案认证过程需要 3 次握手，且每次切换认证之前路由器需要计算根据邻居数计算大量不同的切换认证密钥，给路由器造成较大的负载。而本文提出的方案只需 2 次握手可完成双向认证，且每次认证，路由器只需计算 1 个切换认证密钥，路由器负载较小，

具有较好的实用性。

从隐私保护的角度出发，将本文提出的方案与近期相关方案[19,20,23]进行性能比较分析。如表 1 所示。在此，本文忽略了简单的运算所产生的时延，主要考虑了复杂的双线性对运算（Pairng）和椭圆曲线运算（ECC）。而执行 1 次椭圆曲线点乘运算和双线性对运算所需要的时间分别是 20.04 ms 和 2.21 ms[24]。

表 1　　性能分析与比较

方法	Paring 算法		ECC 算法		总时延/ms
	MN	AP	MN	AP	
文献[19]	0	0	3	4	15.47
文献[20]	0	0	2	4	13.26
文献[23]	2	4	2	1	106.83
本文	0	0	2	3	11.05

表 1 的分析结果表明本文在保证用户的隐私安全前提下，认证效率也是比较高的。同样是 2 次握手，本文所提出的认证方案无需复杂的双线性对运算，方案计算产生的时延主要表现在椭圆曲线乘运算，认证过程计算产生的时延约为 11.05 ms，认证效率较高，有较强的应用价值。

5　结束语

从保护移动节点的隐私出发，提出了一种基于群签名的匿名切换认证方案。为了保护用户的移动轨迹，在预分发切换认证密钥时引入了群签名，但群签名只在能量不受限的路由器上运算。与其他基于群签名切换认证方案不同，方案只需 2 次握手可完成认证过程，无第三方参与，且认证过程无涉及群签名等复杂运算，认证效率较高。

参考文献：

[1] RAFFAELE R, MARCO C, ENRICO G．Mesh networks: commodity multihop ad hoc networks[J]. IEEE Communications Magazine, 2005, 43(3): 123-131.

[2] PHILIP W. Mesh networks: a new architecture for broadband wireless access systems[C]//IEEE Conference on Radio and Wireless (RAWCON). 2000: 43-46.

[3] HE D J, CHEN C, 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] POLITIS C, CHEW K A, AKHTAR N, et al. Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks[J]. IEEE Wireless Communications, 2004, 11(4): 76-88.

[5] CHOI J D, JUNG S W. A secure and efficient handover authentication based on light-weight Diffie-Hellman on mobile node in FMIPv6[J]. IEICE Transactions on Communications, 2008, E-91B(2): 605-608.

[6] HE D J, BU J J, CHAN S, et al. Privacy-preserving universal authentication protocol for wireless communications. IEEE Transactions on Wireless Communication, 2011, 10(2): 431-436.

[7] LIAO Y P, WANG S. A secure dynamic ID based remote user authentication scheme for multi-server environment[J]. Computer Standards & Interfaces, 2009, 31(1): 24-29.

[8] YEH K H, LO N W. A novel remote user authentication scheme for multi-server environment without using smart cards[J]. International Journal of Innovative Computing, Information & Control, 2010, 6(8): 3467-3478.

[9] LAI C Z, LI H, LIANG X H, et al. CPAL: a conditional privacy-preserving authentication with access linkability for roaming service[J]. Internet of Things Journal, IEEE, 2014, 1(1): 46-57.

[10] CHANG C C, LEE C Y, CHIU Y C. Enhanced authentication scheme with anonymity for roaming service in global mobility networks[J]. Computer Communications, 2009, 32(4): 611-618.

[11] HSIANG H C, SHIH W K, Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment[J]. Computer Standards & Interfaces, 2009, 31(6): 1118-1123.

[12] HE D J, MA M D, ZHANG Y, et al, A strong user authentication scheme with smart cards for wireless communications[J]. Computer Communications, 2011, 34(3): 367-374.

[13] YANG X, HUANG X Y, HAN J G, et al. Improved handover authentication and key pre-distribution for wireless mesh networks[J]. Concurrency and Computation: Practice and Experience, 2016, 28(10): 2978-2990.

[14] HAN Q, ZHANG Y, CHEN X, et al. Efficient and robust identity-based handoff authentication in wireless networks[J]. Network and System Security. Springer Berlin Heidelberg, 2012: 180-191.

[15] SHEN A N, GUO S, ZENG D, et al. A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications[C]//Wireless Communications and Networking Conference (WCNC), 2012: 2543-2548.

[16] XU L, HE Y, CHEN X F, et al. Ticket-based handoff authentication for wireless mesh networks[J]. Computer Networks. 2014, 73: 185-194.

[17] ZHANG X, LI G, HAN W. Ticket-based authentication for fast handover in wireless mesh networks[J]. Wireless Personal Communications, 2015, 85(3): 1509-1523.

[18] 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(9): 6-11.
SU B T, XU L, FANG H, et al. Fast authentication mechanism based on Diffie-Hellman for wireless Mesh networks[J]. Journal of Shandong University, 2016, 51(9): 6-11.

[19] LI G S, JIANG Q, WEI F S, et al. A new privacy-aware handover authentication scheme for wireless networks[J]. Wireless Personal Communications, 2015, 80(2): 581-589.

[20] CHAUDHRY S A, FARASH M S, NAQVI H, et al. A robust and efficient privacy aware handover authentication scheme for wireless networks[J]. Wireless Personal Communications, 2015, 1-25.

[21] ZHANG Z Z, QI Q Q, KUMAR N, et al. A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography[J]. Multimedia Tools and Applications, 2015, 74(10): 3477-3488.

[22] CAMENISCH J, STADLER M. Efficient group signature schemes for large groups[C]//Annual International Cryptology Conference. Springer Berlin Heidelberg, 1997: 410-424.

[23] HE D B, KHAN M K, KUMAR N. A new handover authentication protocol based on bilinear pairing functions for wireless networks[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2015, 18(1/2): 67-74.

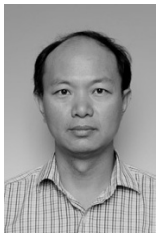
[24] HE D B, CHEN J H, HU J. An id-based proxy signature schemes without bilinear pairings[J]. Annals of Telecommunication, 2011, 66(11-12): 657-662.

作者简介：

苏彬庭（1990-），男，福建泉州人，福建师范大学硕士生，主要研究方向为网络与信息安全。

许力（1970-），男，福建福州人，博士，福建师范大学教授，主要研究方向为无线网络与移动通信、网络与信息安全、物联网与云计算、智能信息处理、复杂网络和网络的建模与仿真。

王峰（1978-），男，山东泗水人，福建师范大学博士生、副教授，主要研究方向为网络与信息安全。



林志兴（1973-），男，福建三明人，三明学院高级实验师，主要研究方向为计算机网络及应用。