支持批量认证和隐私保护的无线 Mesh 网络切换认证方案①

苏彬庭, 许 力, 王 峰

(福建师范大学 数学与计算机科学学院, 福州 350007)
(福建省网络安全与密码技术重点实验室, 福州 350007)

摘 要: 为了在任何时间、任何地点向移动终端提供无缝网络服务, 切换认证技术显得尤为重要. 从认证节点的隐私保护出发, 提出了一种基于身份且支持批量认证的切换认证方案, 并且认证过程无需第三方参与. 方案中, 认证双方无复杂的双线性对运算, 移动节点经两次握手可实现安全切换. 相比其他方案, 该方案不仅满足了认证的安全性要求, 还具有较高的认证效率和支持批量认证的优点.

关键词: 无缝网络服务; 切换认证; 隐私保护; 认证效率; 批量认证

Handover Authentication Scheme Support Batch Verification and Privacy-Preserving for Wireless Mesh Networks

SU Bin-Ting, XU Li, WANG Feng

(School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China)
(Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China)

Abstract: In order to provide seamless network services for mobile nodes at any time, any place, the handover authentication technology is particularly important. We propose an ID-based handover protocol to achieve nodes privacy, which does not require third party involvement during the authentication. The proposed protocol only requires two handshakes without the pairing operation. Comparing with other protocols, the proposed protocol not only enhances the security but also performs better in authentication efficiency and supporting batch authentication.

Key words: seamless network services; handover authentication; privacy-preserving; batch authentication

无线 Mesh 网络(Wireless Mesh Networks, WMNs)是一种新型的网络结构, 它由多个通讯节点组成, 主要包括两种类型节点: Mesh 客户端(Mesh Clients, MC)和 Mesh 路由器(Mesh Routers, MR). 与传统网络相比, WMNs 具有自组织、自管理、自愈能力及支持多种网络接入的优势[1,2]. 随着信息技术的迅速发展, 网络安全和服务质量问题越发深受人们的关注, 而切换认证是关乎这些问题的重要技术之一. 图 1 是无线 Mesh 网络切换认证示意图, 为了保证服务的连续性, MC 从路由器 MR1 切换到 MR2 应在 50ms 内完成, 其中认证过程不能超过 20ms[3]. 如今, 随着黑客技术的不断进步, 切换认证方案不仅要求高效, 还要满足相应的安全性[4-8]: (1)双向认证: 不仅 MR 要对认证节点的身份进行检查, 同时 MC 也要验证 MR 是否安全; (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: 路由器无法知道认证节点的真实身份, 并且无法判断该节点在当前 MR 是否认证过两次; (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(Authentication Server, AS)可通过通讯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, 使其无法享受网络的服务; (6)抵抗攻击: 能够抵

① 基金项目:国家自然科学基金(U1405255);福建省高校产学研合作重大项目(2014H61010105);福建师范大学科研创新团队(IRTL1207);福州市科技局项目(2015-G-59)

收稿时间:2016-04-07;收到修改稿时间:2016-05-12 [doi: 10.15888/j.cnki.csa.005517]

抗各种攻击, 保证协议的安全性.

近期, 相关研究学者提出了一系列的切换认证方案[9-18]. 其中文献[9-11]提出的方案无需第三方参与, 移动节点完成认证只需 3 次握手, 无需双线性对等复杂的运算, 认证时延短, 效率高. 然而这些方案泄露了 MC 的身份信息, 无法保护 MC 身份、运动轨迹等隐私信息. 为此, 刘丹等相关研究人员利用双线性对提出了基于身份的认证方案[12-16]. 这些方案中, 移动节点在每次认证使用不同的身份, 因此接入点无法确定认证节点的真实身份, 并且无法判断该节点在当前接入点是否认证过两次, 有较高的安全性. 然而这类方案需要进行多次的双线性对运算, 计算代价高, 认证效率低. 2015 年 Li 等人[17]提出了无需双线对运算并能够保护移动节点隐私的认证方案. 同样, 该方案认证过程无需第三方参与, 经 2 次握手可完成切换认证, 认证效率高. 但很遗憾该方案并无法抵抗中间人攻击, 攻击者可以冒充 MR 获得 MC 的信任, 从而捕获 MC. 文献[18]对该方案存在的安全漏洞进行了阐述, 并提出了一种改进方法. 然而改进后的方案然还是存在一些不足之处: (1)合法移动节点不仅可以享受网络接入点服务, 同时也能够利用自身的密钥信息伪造多个基站, 捕获其他移动节点; (2)当一个接入点同时收到多个移动节点的认证请求时, 认证效率低.

本文从保护移动节点隐私信息的目的出发, 提出了一种基于身份的高效切换认证方案. 该方案无需第三方参与和复杂的双线性对运算, 只需 2 次握手可完成安全切换认证过程. 方案不仅能够解决了上述 MC 可以伪造基站和无法抵抗中间人攻击的安全问题, 并提出了一种批量认证的策略, 解决了多个客户端同时认证的低效率问题, 认证效率高、时延短.

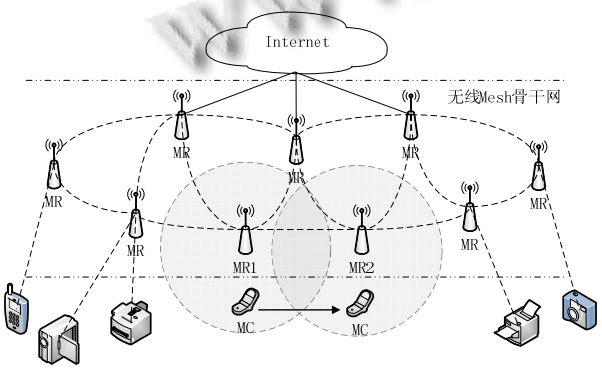

图 1 Mesh 网络切换认证示意图

1 切换认证方案

本文从保护移动节点隐私信息的目的出发, 提出了一种基于身份的高效切换认证方案. 方案由系统初始化和切换认证过程两部分组成. 在系统初始化中, 认证服务器产生系统参数, 并为网络每个节点分发密钥对. 在切换认证过程中, 认证双方无复杂的双线对运算, 经两次握手可完成切换认证, 计算代价小, 认证效率高.

1.1 系统初始化

在系统初始化过程中, AS 输入安全参数 κ 执行密钥生成算法, 为网络各接入点和移动节点创建公私钥对.

① 选择一大素数 q 和 p, E/F_p 是定义在有限域 F_p 上的椭圆曲线. 选择 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 $s\in Z_a^*$, 计算公钥 $PK=s\cdot P$;

③ 选择散列函数 $H_1:\{0,1\}^*\times G\to Z_q^*$、$H_2:\{0,1\}^*\to Z_q^*$、$H_3:G\times\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^k$ 和 $H_4:G\times\{0,1\}^*\times\{0,1\}^*\times G\times G\to\{0,1\}^*$;

④ 生成特殊身份验证密钥 key, 用来辨别接入点和移动节点身份;

⑤公开系统参数 $\{q,p,E/F_a,P,G,PK,key,H_1,H_2,H_3,H_4\}$.

AS 利用系统参数为网络每个节点创建公私钥对. 对于网络路由器 MR, 假设 ID_{MR} 为 MR 的唯一身份标识. AS 选择随机数 $r_{MR}\in Z_q^*$, 计算 $R_{MR}=r_{MR}\cdot P$, $h_{MR}=H_1(ID_{MR},R_{MR})$ 和 $s_{MR}=r_{MR}+s\cdot h_{MR}$, 然后将 (s_{MR},R_{MR})通过安全通道发给 MR. MR 收到密钥后, 计算公钥 $PK_{MR}=s_{MR}\cdot P$ 并定期广播自身信息 (ID_{MR},R_{MR}). 为了保证 Mesh 客户端在切换认证过程身份不被泄露, AS 为每个 MC 生成一系列不关联的身份 ID, 即 $PID_{MC}=\{pid_1,pid_2,\cdots,pid_s\}$, 并计算每个 pid 对应的密钥. 对于 pid_i, AS 选择随机数 $r_i\in Z_a^*$, 计算 $R_i=r_i\cdot P$, $h_i=H_1(pid_i,R_i)$ 和 $s_i=r_i+s\cdot h_i$, 然后将 (pid_i,s_i,R_i)通过安全通道发给 MC. MC 收到密钥后, 计算公钥 $PK_i=s_i\cdot P$ 并秘密保存.

1.2 认证过程

在移动过程中, MC 可能因为信号变弱等因素而请求接入更合适的路由器. 本文利用上述系统所建立的安全密钥, 提出了一种基于身份切换认证方案. 假设 MC 从路由器 MR1 切换到路由器 MR2, 具体认证过

程如图 2 所示.

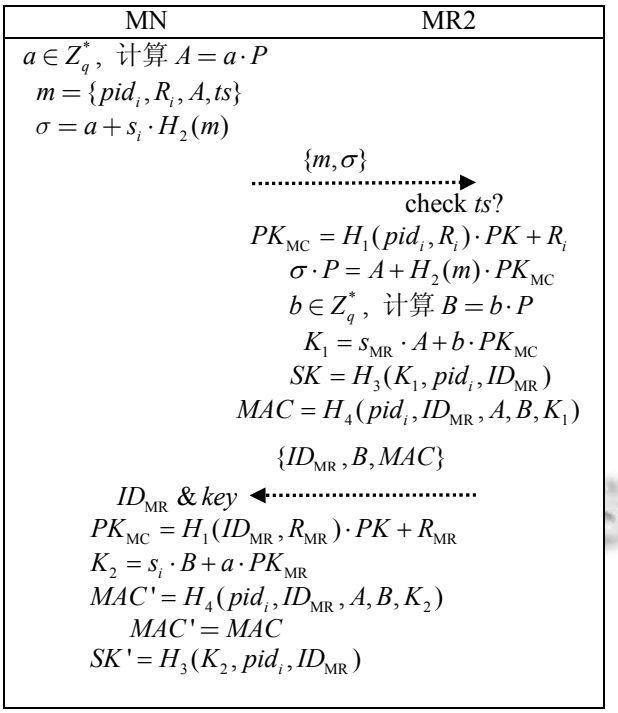

图 2　切换认证过程

① MC → MR2 : $\{m, \sigma\}$

MC 选择随机数 $a \in Z_q^*$, 计算 $A = a \cdot P$. 然后产生时间戳 ts 并选择一个未使用过的假名 $pid \in PID_{MC}$ 作为认证身份, 生成消息 $m = \{pid_i, R_i, A, ts\}$. 从而产生签名 $\sigma = a + s_i \cdot H_2(m)$, 并将消息 $\{m, \sigma\}$ 发送给 MR2.

② MR2 → MC : $\{ID_{MR}, B, MAC\}$

MR2 收到 MC 的认证请求消息后, 首先检查时间戳 ts 是否已经过期的, 如果没有则根据式 1 和 2 验证签名 σ 的合法性. 若 σ 合法, 选择随机数 $b \in Z_q^*$, 计算 $B = b \cdot P$. 根据式(3)和式(4)计算会话秘钥(Session Key, SK). 然后生成消息认证码 MAC, 并将消息 $\{ID_{MR}, B, MAC\}$ 发给 MC.

$$PK_{MC} = H_1(pid_i, R_i) \cdot PK + R_i \quad (1)$$

$$\sigma \cdot P = A + H_2(m) \cdot PK_{MC} \quad (2)$$

$$K_1 = s_{MR} \cdot A + b \cdot PK_{MC} \quad (3)$$

$$SK = H_3(K_1, pid_i, ID_{MR}) \quad (4)$$

$$MAC = H_4(pid_i, ID_{MR}, A, B, K_1) \quad (5)$$

收到回应消息后, MC 首先检测接入点身份是否合法, 再利用计算好的公钥 PK_{MR}, 根据式(6)和式(7)计算密钥 K_2, 并根据式(8)计算消息认证码 MAC'. 验证 MAC' 与收到的消息认证码 MAC 是否一致, 如果一致证明该路由器是合法. 最后利用式(9)计算会话密钥, 完成认证过程.

$$PK_{MR} = H_1(ID_{MR}, R_{MR}) \cdot PK + R_{MR} \quad (6)$$

$$K_2 = s_i \cdot B + a \cdot PK_{MR} \quad (7)$$

$$MAC' = H_4(pid_i, ID_{MR}, A, B, K_2) \quad (8)$$

$$SK' = H_3(K_2, pid_i, ID_{MR}) \quad (9)$$

2　安全性分析

本文从密钥协商的安全性、匿名性和不可关联性、前向安全性、后向安全性和抗攻击性几个方面对方案的安全性进行分析, 并分析比较了近期相关的切换认证方案[15-18]. 分析结果表明, 本文提出的方案具有较高的安全性.

2.1　双向认证和密钥协商安全性

MC 发送切换认证请求 $\{m, \sigma\}$ 后, MR2 收到消息可以通过式(2)验证 MC 是否是合法的客户端. 而 MC 通过验证消息认证码 MAC' 与接收到的 MAC 是否一致, 判断目标接入点是否合法. 由式(5)和(8)可知, 当 $K_1 = K_2$ 时, MAC' 和 MAC 一致. 只有当路由器的私钥是 AS 分发的合法密钥时, 路由器计算得到的 K_1 才会与 K_2 相等.

$$\begin{aligned} K_1 &= s_{MR} \cdot A + b \cdot PK_{MC} \\ &= (r_{MR} + s \cdot h_{MR}) \cdot aP + b \cdot \left[H_1(pid_i, R_i) \cdot PK + R_i\right] \\ &= a \cdot (r_{MR} + s \cdot h_{MR}) \cdot P + b \cdot \left[H_1(pid_i, R_i) \cdot s + r_i\right] \cdot P \\ &= a \cdot (r_{MR} \cdot P + h_{MR} \cdot PK) + \left[H_1(pid_i, R_i) \cdot s + r_i\right] \cdot bP \\ &= a \cdot PK_{MR} + s_i \cdot B \\ &= K_2 \end{aligned}$$

2.2　匿名性和不可关联性

MC 每次认证都选取一个未使用过的身份 $pid_i \in PID_{MC}$. 不管是对哪个接入点, 每次切换使用的 pid 都不同. 完成一次切换认证后, 删除上次 pid_j 和所对应的密钥对, 保证每次认证的身份 ID 都不同. 除了 AS 之外, 任何实体都无法确定 MC 真实身份, 从而保证了 MC 的匿名性和不可关联性.

2.3　前向和后向安全性

MC 拥有一系列不相关联的身份 ID, 即 $PID_{MC} = \{pid_1, pid_2 \text{L } pid_i\}$. 这些身份所对应的密钥对也是不相关联的. 每次认证 MC 选取的身份 ID 和对应的密钥对都是不同的, 完成认证后产生的会话密钥也不一致, 所以攻击者无法通过窃听当前的通讯信息来推导出 MC 之前的通讯数据. 同理, 攻击者也无法

预测 MC 接下来的通讯内容, 从而实现了 MC 通讯的前向和后向安全性.

2.4 抗重放攻击

在 MC 发送请求切换认证的消息中, 签名 σ 的计算包含了时间戳 *ts*. MR2 收到消息可以检测 *ts* 是否过期并验证签名 σ 的合法性, 判断该请求消息是否被重放的.

2.5 抗中间人攻击

在系统初始化中, AS 为 MC 和 MR2 分发了相应的密钥. 在认证过程, 只有拥有 AS 分发的合法密钥, 才能够计算出密钥 K_1 和 K_2. 请求认证时, 攻击者无法生成合法的签名 σ, 无法通过 MR2 的认证.

表 1 安全性分析

方案	[15]	[16]	[17]	[18]	本文方案
双向认证	√	√	√	√	√
匿名性/不可关联性	√	√	√	√	√
前向/后向安全性	√	√	√	√	√
抗重放攻击	√	√	√	√	√
抗中间人攻击	√	√	×	√	√
支持批量认证	√	×	×	×	√
认证效率	低	低	高	高	高

3 性能分析与批量认证

切换认证方案不仅要确保认证双方的安全性, 同时也要缩短认证时延, 提高认证效率. 经过分析, 本文提出的方案不仅效率高, 并且提出了批量认证策略, 解决了多个客户端同时认证所带来的低效率问题.

3.1 方案性能分析

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(Paring)和椭圆曲线点乘运算(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 20.04ms 和 2.21ms[19].

表 2 性能分析与比较

方案	节点	[15]	[16]	[17]	[18]	本文方案
Paring	*MN*	1	1	0	0	0
	AP	3	4	0	0	0
ECC	*MN*	1	2	3	2	1
	AP	1	1	4	4	5
总时延(ms)		84.58	106.83	15.47	13.26	13.26

表 1, 2 对本文提出的认证方案的安全性和性能进行了分析, 并比较了近期相关的切换认证方案[15-18]. 从表中可知本文的方案不仅能够实现安全切换认证, 且认证效率较高. 方案产生的计算代价主要体现在椭圆曲线的点乘运算, 总共需要 6 次 ECC 运算, 认证过程消耗的时延约 13.26ms. 其中 MC 在计算 K_1 消耗了 1 次, MR2 在验证签名 σ 和计算 K_2 分别消耗了 3、2 次. 虽然与方案[18]的计算代价差不多, 但本文方案的在认证过程中的 ECC 运算更集中于能量没有受限的接入点上, 认证方案显得更优. 相比其余的方案, 同样 2 次握手完成安全切换认证, 本文提出的方案的计算代价明显更小, 认证效率更高.

3.2 批量认证

在频繁切换的密集网络中, 接入点可能需要同时认证多个 Mesh 客户端, 若逐个认证将会延长每个客户端的认证时间, 降低认证效率. 为此, 本文提出了批量认证策略, 解决了多个客户端同时认证所带来的低效率问题.

① 两个客户端

假设两个客户端同时请求认证, 其身份为 pid_1,pid_2, 对应密钥和消息分别为 R_1,R_2 和 m_1,m_2, 批量认证方法如下:

$$\begin{aligned}&(\sigma_1+\sigma_2)\cdot P\\&=A_1+H_2(m_1)\cdot PK_1+A_2+H_2(m_2)\cdot PK_2\\&=(A_1+A_2)+\{H_2(m_1)\cdot[H_1(pid_1,R_1)\cdot PK+R_1]\}\\&\quad+\{H_2(m_2)\cdot[H_1(pid_2,R_2)\cdot PK+R_2]\}\\&=(A_1+A_2)+[H_2(m_1)\cdot H_1(pid_1,R_1)\cdot PK+H_2(m_1)\cdot R_1]\\&\quad+[H_2(m_2)\cdot H_1(pid_2,R_2)\cdot PK+H_2(m_2)\cdot R_2]\\&=(A_1+A_2)+H_2(m_1)\cdot R_1+H_2(m_2)\cdot R_2\\&\quad+[H_2(m_1)\cdot H_1(pid_1,R_1)+H_2(m_2)\cdot H_1(pid_2,R_2)]\cdot PK\end{aligned}$$

② n 个客户端

假设同时请求认证的客户端数为 n, 表 3 是批认证与逐个认证计算代价(接入点进行 ECC 运算的次数)的比较. 由式(10)可知, 当 n 客户端同时请求认证时, 总共需要 $3n+2$ 次的 ECC 运算. 其中验证 n 个客户端的签名需要 $n+2$ 次, 而计算 n 个客户端的会话密钥需要 $2n$ 次. 与传统的逐个认证方法比较, 批量认证的效率更高, 认证速度更快.

$$\left(\sum_{j=1}^{n}\sigma_j\right)\cdot P=\sum_{j=1}^{n}\left[A_j+H_2(m_j)\cdot R_j\right]+\left[\sum_{j=1}^{n}H_2(m_j)H_1(pid_j,R_j)\right]\cdot PK \quad (10)$$

表 3 批量认证和传统认证性能比较

认证策略	批量认证	逐个认证
计算代价	$3n+2$	$5n$

4 结论

为了解决无线 Mesh 网络的切换认证效率和客户端隐私保护等问题, 提出了一种基于身份的切换认证方案. 通过分析, 对于其他方案, 该方案在满足相应的安全性要求下, 不仅能够保护客户端的隐私信息, 而且具有较高的认证效率. 其认证过程无需复杂的双线性对等运算, 只要经两次握手便可实现安全切换. 同时, 方案提出的批量认证策略, 解决了多个客户端同时认证所带来的低效率问题. 在未来的工作里, 我们将进一步研究如何在满足隐私保护和快速安全认证的条件下, 提高撤销用户的效率问题.

参考文献

1 Brunno R, Conti M, Gregori E. Mesh networks: Commodity multihop ad hoc networks. IEEE Communications Magazine, 2005, 43(3): 123–131.

2 Whitehead P. Mesh networks: A new architecture for broadband wireless access systems. IEEE Conference on Radio and Wireless (RAWCON). 2000. 43–46.

3 He DJ, Chen C, Chan Sammy, Bu J. Secure and efficient handover authentication based on bilinear pairing functions. IEEE Trans. on Wireless Communications, 2012, 11(1): 48–53.

4 Choi J, Jung S. A secure and efficient handover authentication based on light-weight DiffieHellman on mobile node in FMIPv6. IEICE Trans. on Communications, 2008, E-91B(2): 605–608.

5 He DJ, Bu JJ, Chan S, Yin MJ. Privacy-preserving universal authentication protocol for wireless comunications. IEEE Trans. on Wireless Communication, 2011, 10(2): 431–436.

6 Liao YP, Wang SS. A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 2009, 31(1): 24–29.

7 Yeh KH, Lo NW. A novel remote user authentication scheme for multi-server environment without using smart cards. International Journal of Innovative Computing, Information & Control, 2010, 6(8): 3467–3478.

8 Lai CZ, Li H, Liang XH, Lu RX, Zhang K, Shen XM. CPAL: A conditional privacy-preserving authentication with access linkability for roaming service. Internet of Things Journal, IEEE, 2014, 1(1): 46–57.

9 Yang X, Huang XY, Han JG, Su CH. Improved handover authentication and key pre-distribution for wireless mesh networks. Concurrency and Computation: Practice and Experience, 2015.

10 Xu L, He Y, Chen XF, Huang XY. Ticket-based handoff authentication for wireless mesh networks. Computer Networks, 2014, 73: 185–194.

11 Li C, Nguyen UT, Nguyen HL, Huda N. Efficient authentication for fast handover in wireless Mesh networks. Computers & Security, 2013, 37: 124–142.

12 刘丹,石润华,仲红等.车载自组织网络中条件隐私保护认证方案.计算机应用,2015,35(5):1385–1392.

13 Yang GM, Huang Q, Wong DS, Deng XT. Universal authentication protocol for anonymous wireless communications, IEEE Trans. Wireless Commun., 2010, 9(1): 168–174.

14 Jo HJ, Paik JH, Lee DH. Efficient privacy-preserving authentication in wireless mobile networks. IEEE Trans. on Mobile Computing, 2014, 13(7): 1469–1481.

15 Tsai JL, Lo NW, Wu TC. Secure handover authentication protocol based on bilinear pairings. Wireless Personal Communications, 2013, 73(3): 1037–1047.

16 He DB, Khan MK, Kumar N. A new handover authentication protocol based on bilinear pairing functions for wireless networks. International Journal of Ad Hoc and Ubiquitous Computing, 2015, 18(1/2): 67–74.

17 Li GS, Jiang Q, Wei FS, Ma CG. A new privacy-aware handover authentication scheme for wireless networks. Wireless Personal Communications, 2015, 80(2): 581–589.

18 Chaudhry SA, Farash MS, Naqvi H, Islam SH, Shon T. A robust and efficient privacy aware handover authentication scheme for wireless networks. Wireless Personal Communications, 2015: 1–15.

19 He DB, Chen JH, Hu Jin. An id-based proxy signature schemes without bilinear pairings. Annals of Telecommunication, 2011, 66(11-12): 657–662.