异构无线网络可控匿名漫游认证协议

周彦伟[1,2,3],杨 波[1,2,3],张文政[2]
(1. 陕西师范大学计算机科学学院,陕西西安 710062;2. 保密通信重点实验室,四川成都 610041;
3. 中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 分析传统的匿名漫游认证协议,指出其存在匿名不可控和通信时延较大的不足,针对上述问题,本文提出异构无线网络可控匿名漫游认证协议,远程网络认证服务器基于1轮消息交互即可完成对移动终端的身份合法性验证;并且当移动终端发生恶意操作时,家乡网络认证服务器可协助远程网络认证服务器撤销移动终端的身份匿名性. 本文协议在实现匿名认证的同时,有效防止恶意行为的发生,且其通信时延较小. 安全性证明表明本文协议在CK安全模型中是可证安全的.

关键词: 异构无线网络;可控漫游;匿名认证;CK安全模型
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2016)05-1117-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.05.015

Controllable and Anonymous Roaming Protocol for Heterogeneous Wireless Network

ZHOU Yan-wei[1,2,3], YANG Bo[1,2,3], ZHANG Wen-zheng[2]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *Science and Technology on Communication Security Laboratory, Chengdu, Sichuan* 610041, *China*;
3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: This paper analyzes the traditional anonymous roaming authentication protocol, and pointed out the deficiencies of their anonymity is not controlled and the communication is delay. The controllable anonymous roaming authentication protocol proposed in this paper for heterogeneous wireless networks, which can be completed to verify the legitimacy of the identity of the mobile terminal through a message interaction. If the mobile terminal has malicious operation, the home network authentication server can help remote network authentication server to revoke the identity anonymity of the mobile terminal. This is a protocol in anonymous authentication, at the same time, and which effectively preventing the occurrence of malicious behavior, and the communication delay. This protocol is safe in the CK security model.

Key words: heterogeneous wireless network; controlled roaming; anonymous authentication; CK security model

1 引言

随着网络信息技术的快速发展,无线网络已逐步向多种无线接入技术并存的全IP异构无线网络发展,异构无线网络有拓扑结构动态变化、开放链路、多种接入技术并存等特点,使其已成为下一代网络发展的趋势.

异构无线网络主要包括移动终端MT、家乡网络认证服务器HS和MT访问的远程网络认证服务器RS. 安全漫游使得移动终端的接入服务可不受家乡网络覆盖范围的限制,即当漫游到远程网络(家乡网络之外的网络)时,移动终端在异构无线网络中仍然保持连接. 漫游认证过程中,同样需要考虑用户的隐私保护问题,防止移动终端的身份和位置信息被恶意实体跟踪. 为了在漫游认证过程中保护移动终端的隐私信息和提高漫游认证的效率,漫游认证协议需满足如下要求:①用户

收稿日期:2014-09-23;修回日期:2014-11-23;责任编辑:蓝红杰
基金项目:国家自然科学基金(No. 61572303, No. 61272436, No. 61402275, No. 61303092);保密通信重点实验室基金(No. 9140C110206140C11050);中国科学院信息工程研究所信息安全国家重点实验室开放课题(No. 2015-MS-10);陕西省自然科学基金(No. 2014JQ8309);中央高校基本科研业务费专项资金(No. GK201504016);陕西师范大学优秀博士论文项目(No. X2014YB01)

匿名性. 漫游过程中,远程网络认证服务器和外部用户都无法确定移动终端的真实身份;②无关联性. 远程网络认证服务器和外部用户均无法确定不同的会话是否来自相同的用户;③低通信时延和计算量. 由于移动终端是计算能力有限的便携设备,因此漫游认证方案需减少移动终端的计算量.

2 相关研究工作

2.1 漫游认证协议

漫游认证的实质是实现跨域服务申请时的身份合法性验证,是异构无线网络中多种无线接入技术并存的前提条件,为此国内外研究人员提出了很多解决方案[1~7]. 传统漫游认证方案[1~7]实现了漫游匿名认证过程中对 MT 身份的匿名性保护,但其匿名是不可控的,即当 MT 出现恶意匿名访问行为时,远程网络认证服务器无法撤销其匿名性;并且传统漫游认证协议中均采用 HS 协助 RS 完成对 MT 的身份合法性认证,即则传统的漫游认证协议[1~7]中均采用 2 轮交互的漫游认证模式,消息交互次数较多,通信时延较大.

2.2 一次性公钥

在一次性公钥中,可信中心只需给用户生成一次私钥,用户每次签名时可自主生成各不相同的公钥,使得用户每次的签名间不存在关联性,从而保证了用户的身份匿名性和无关联性. 此外,在必要时验证者可向可信中心申请撤销用户的匿名性,防止用户恶意匿名访问行为的出现. 研究者就一次性公钥及签名算法等进行了相关研究[8,9],并且当前的一次性公钥多数是基于双线性映射[10]构造的.

3 异构无线网络可控匿名漫游认证协议

本文协议的安全性基于下述假设:

假设 各网络认证服务器的参数系统相同(除主密钥外,其他相关参数均相同);并且各网络认证服务器均可信,即不会发送虚假信息,也不会利用已掌握的 MT 信息实施假冒攻击,更不会随意揭示 MT 的真实身份,除非 RS 出示了 MT 存在恶意匿名行为的有效证据;同时,各认证服务器秘密保存主密钥,防止泄露.

本文协议主要包含系统初始化、注册家乡网络、漫游认证、重复漫游认证和匿名追踪 5 个阶段.

3.1 系统初始化

由异构无线网络管理中心负责管理各认证服务器的安全性及其他相关事宜;同时,管理中心为各认证服务器建立基础参数系统.

管理中心选择椭圆曲线上满足双线性对要求的参数 G_1,G_2 和 q,其中群 G_1 的一个生成元为 P;定义双线性映射 $e:G_1\times G_1\rightarrow G_2$;定义抗碰撞的安全哈希函数 $H:Z_q^*\rightarrow Z_q^*$,$H_1:\{0,1\}^m\times G_1\rightarrow Z_q^*$,$H_2:\{0,1\}^m\times Z_q^*\rightarrow\{0,1\}^m$,$H_3:G_1\rightarrow Z_q^*$,对外公开基础参数系统$\{G_1,G_2,q,e,P,H,H_1,H_2,H_3\}$.

HS 随机选择秘密数 $S_{HS}\in Z_q^*$ 作为 HS 的系统主密钥,系统公钥为 $P_{Pub-HS}=S_{HS}P$,HS 妥善保存主密钥 S_{HS};同时,对外公开系统参数$\{G_1,G_2,q,e,P,P_{Pub-HS},H,H_1,H_2,H_3\}$. RS 随机选择秘密数 $S_{RS}\in Z_q^*$ 作为 RS 的系统主密钥,系统公钥为 $P_{Pub-RS}=S_{RS}P$,RS 妥善保存主密钥 S_{RS};同时,对外公开系统参数$\{G_1,G_2,q,e,P,P_{Pub-RS},H,H_1,H_2,H_3\}$.

3.2 注册家乡网络

(1)MT 随机选取秘密数 $r_M\in Z_q^*$,计算 $R_1=r_MP$,MT 获取当前时间戳 T'_{MT},并发送 $Enc(P_{Pub-HS},R_1\parallel ID_{MT}\parallel T'_{MT})$给 HS.

(2)HS 检查时间戳 T'_{MT}的新鲜性,验证移动终端身份 ID_{MT}的合法性后,计算 MT 的部分私钥 K_{MT}:

①HS 随机选择秘密数 $r_H\in Z_q^*$,计算 $R_2=r_HP$ 和 $R=R_1+R_2$.

②计算部分私钥 $K_{MT}=r_H+S_{HS}C$,其中 $C=H_1(ID_{MT},R)$.

HS 保存$\{ID_{MT},R,C\}$为 MT 建立账户信息,用作确认 MT 身份的凭证,以撤销其身份匿名性. HS 获取当前时间戳 T_{HS},通过安全信道发送消息 $Enc(S_{HS},R\parallel K_{MT}\parallel T_{HS})$给 MT.

(3)MT 首先验证 HS 应答消息的正确性,确认是真实、合法的本地 HS 为其提供注册服务. MT 计算 $KS_{MT}=r_M+K_{MT}$;基于等式 $KS_{MT}P=R+H_1(ID_{MT},R)P_{Pub-HS}$验证 KS_{MT}的正确性;由于仅有合法 HS 生成的 KS_{MT}才能通过 MT 的合法性验证,因此通过上述验证可确认注册认证服务器 HS 的身份合法性.

若验证通过,则 MT 安全存储 KS_{MT}和 R,删除秘密随机数 r_M,即 MT 成功注册了家乡网络,并获得 HS 签发的正确私钥 KS_{MT}.

3.3 漫游认证

(1)MT 随机选取秘密数 $a\in Z_q^*$,并计算 $P_{MT}=aKS_{MT}P$,$U_{MT}=aR$,$V_{MT}=aCP$(其中 $C=H_1(ID_{MT},R)$),则 $KP_{MT}=(P_{MT},U_{MT},V_{MT})$即为移动终端 MT 生成的一次性公钥.

MT 选取随机秘密数 $x\in Z_q^*$,并计算密钥协商参数 $X=xP$ 和 $X'=xP_{Pub-RS}$,产生临时身份标识 $TID_{MT}=H_2(ID_{MT},x)$.

MT 选择随机参数 $g\in Z_q^*$,计算 $G_0=H(g)$ 和 $h=H_2(TID_{MT}\parallel G_0\parallel X')$,生成签名 $Sig=x+aKS_{MT}h$. MT 计

算 $\Gamma = G_0 \oplus H_3(X)$(上述计算可在申请漫游认证前的空闲时间进行).

MT 获取当前时间戳 T_{MT}, MT 发送消息 $Enc(P_{Pub-RS}, ID_{RS} \| ID_{HS} \| \Gamma \| KP_{MT} \| Sig \| X' \| TID_{MT} \| T_{MT})$给 RS.

(2)RS 收到 MT 的漫游请求消息后,首先检查时间戳 T_{MT} 的新鲜性,若新鲜,则通过等式 $e(P_{MT}, P) = e(U_{MT}, P)e(V_{MT}, P_{Pub-HS})$验证一次性公钥 KP_{MT} 的合法性,若等式成立则可确定 MT 已注册其家乡网络,并已通过 HS 的身份合法性验证.

一次性公钥合法性验证通过后,RS 计算 $X'' = S_{RS}^{-1}X' = xP$, $G_0 = \Gamma \oplus H_3(X'')$ 和 $h' = H_2(TID_{MT} \| G_0 \| X'')$,验证 $SigP = X'' + h'P_{MT}$ 是否成立,若成立则签名验证通过,否则协议终止.

最后 RS 将临时身份信息 TID_{MT} 和散列值 G_0 进行相应的哈希运算后保存,建立重复漫游认证列表 $\{TID = H_2(TID_{MT}, 0), G = H(G_0), KP_{MT}, ID_{HS}, Num, Data\}$,其中 TID 为移动终端的临时身份信息;G 为认证散列值;Num 为移动终端申请重复漫游的次数;$Data$ 为该数据项过期时间.

RS 计算与 MT 间的会话密钥,选取随机秘密数 $y \in Z_q^*$,计算密钥协商参数 $Y = yP$ 和会话密钥 $K_{RS-MT} = H_3(yX'') = H_3(xyP)$,RS 获取当前时间戳 T_{RS},发送消息 $Enc(S_{RS}, Y \| T_{RS} \| T_{MT})$给 MT.

(3)MT 接收到 RS 的消息后,首先验证应答消息的正确性和完整性,确认是其议定的 RS 为其提供漫游认证服务,即完成对 RS 的身份合法性认证;随后检查时间戳 T_{RS} 的新鲜性,若新鲜,则验证 T_{MT} 的一致性,若验证均通过,即 MT 完成漫游认证,并计算与 RS 间的会话密钥 $K_{MT-RS} = H_3(xY) = H_3(xyP)$.

3.4　重复漫游认证

MT 第 $I(2 \leqslant I \leqslant Max, Max$ 为系统最大的重复漫游次数)次向 RS 申请漫游认证的具体过程为:

(1) MT 随机选择 $b \in Z_q^*$,计算 $B = bP$ 和 $B' = bP_{Pub-RS}$,产生第 I 次漫游认证的临时身份标识 $TID_{MT}^I = H_2(TID_{MT}^{I-1}, 0)$ 和散列值 $G_{(I)} = H(G_{(I-1)})$,计算 $\Gamma_{(I)} = G_{(I)} \oplus H_3(B)$. MT 获取当前时间戳 T_{MT}^I,并发送 $Enc(P_{Pub-RS}, TID_{MT}^I \| \Gamma_{(I)} \| B' \| T_{MT}^I)$给 RS.

(2)RS 收到消息后,首先检查时间戳 T_{MT}^I 的新鲜性,若新鲜,则计算 $B'' = S_{RS}^{-1}B' = bP$ 和 $G_{(I)} = T_{(I)} \oplus H_3(B'')$,查找移动终端重复漫游认证列表中是否存在 TID_{MT}^I,并且其对应散列值与 $G_{(I)}$ 相等,若存在,则证明当前 MT 是已通过漫游身份合法性认证的合法移动终端,RS 根据算法 1 更新移动终端重复漫游认证列表中的相关内容.

算法 1　重复漫游认证列表更新算法

IF $fun(T_{Now}, Data) == -1$ or $Num > Max$

//fun ()返回值为-1 时表示重复漫游认证信息已过期.

　　RS 删除漫游认证列表中该 MT 的相关信息;

Else

//认证信息在当前时间有效,则更新 MT 的相关信息

　　$Num = Num + 1$;

　　$TID = H_2(TID, 0)$;

　　$G = H(G)$;

　　RS 更新 MT 的重复漫游认证列表;

END IF

RS 随机选择秘密数 $d \in Z_q^*$,计算密钥协商参数 $D = dP$ 和会话密钥 $K_{RS-MT}^I = H_3(dB'') = H_3(bdP)$. RS 获取当前时戳 T_{RS}^I,发送消息 $Enc(S_{RS}, D \| T_{RS}^I \| T_{MT}^I)$给 MT.

(3)MT 接收到 RS 的消息后,首先验证应答消息的正确性和完整性,完成对 RS 的身份合法性验证;然后检查时戳 T_{RS}^I 的新鲜性,若新鲜,则验证 T_{MT}^I 的一致性,若验证均通过,则 MT 完成重复漫游认证. MT 计算会话密钥 $K_{MT-RS}^I = H_3(bD) = H_3(bdP)$.

3.5　匿名追踪

在移动终端漫游进入远程网络后,若发生恶意访问或操作时,RS 通过 TID 查找数据列表,发送 MT 的恶意行为证据和 MT 的一次性公钥 KP_{MT} 给 HS,HS 首先验证 RS 提供 MT 的恶意行为证据的真实性,然后基于保存信息 (ID_{MT}, C, R) 验证等式 $e(U_{MT}, CP) = e(V_{MT}, R)$ 是否成立,若成立,则表明具有恶意行为的移动终端的部分私钥为 R,HS 和 RS 即可获知 MT 的身份信息 ID_{MT},MT 漫游的身份匿名性被撤销.

4　安全性证明

本节在 CK 安全模型下对本文协议的安全性进行证明. 文献[11,12]详细介绍了 CK 安全模型中编译器,会话密钥安全及认证器等概念.

4.1　AM 中的漫游认证协议

为简化协议的证明过程,将漫游认证协议抽象描述为下述协议 δ.

(1)漫游请求. MT 生成一次性公钥 KP_{MT},随机选取 $x \in Z_q^*$,计算 $X = xP$ 和 $X' = xP_{Pub-RS}$,产生临时身份标识 TID_{MT},计算 $Sig = aKS_{MT}h$(其中 $h = H_2(TID_{MT} \| G_0 \| X')$),计算 $G_0 = H(g)$ 和 $\Gamma = G_0 \oplus H_3(X)$,MT 获取当前时戳 T_{MT} 后,向 RS 发送消息 $Enc(P_{Pub-RS}, ID_{RS} \| ID_{HS} \| \Gamma \| KP_{MT} \| Sig \| X' \| TID_{MT} \| T_{MT})$.

(2)漫游响应. RS 收到 MT 的漫游认证申请后,首先验证时间戳 T_{MT} 的新鲜性,通过验证一次性公钥 KP_{MT} 和签名 Sig 的合法性完成对 MT 身份合法性的鉴别. 验

证通过后 RS 选取秘密随机数 $y \in Z_q^*$,计算 $Y = yP$,RS 计算 $X'' = S_{RS}^{-1} X' = xP$,计算会话密钥 $K_{RS-MT} = H_3(yX'') = H_3(xyP)$. RS 发送应答消息 $Enc(S_{RS}, Y \parallel T_{RS} \parallel T_{MT})$ 给 MT.

(3)MT 首先验证消息的完整性和正确性,完成对 RS 的身份合法性验证;然后计算会话密钥 $K_{MT-RS} = H_3(xY) = H_3(xyP)$,完成漫游申请.

定理 1 当签名、非对称加密、哈希等算法均安全且难解时,协议 δ 在 AM 中是会话密钥安全的.

证明 如果 AM 中的匿名漫游协议满足会话密钥安全定义的两个性质,则其在 AM 中是会话密钥安全的.

(1)在 AM 中,由于协议 δ 交互过程中消息参与者没有被敌手 A 攻陷,因此协议执行完毕时,MT 和 RS 分别得到没有篡改的密钥协商参数. 其中,RS 计算的会话密钥为 $K_{RS-MT} = H_3(xyP)$,MT 计算的会话密钥为 $K_{MT-RS} = H_3(xyP)$,因此协议 δ 满足会话密钥安全的性质 1.

(2)对于会话密钥安全的性质 2 采用反证法证明. 假设 AM 中存在一个敌手 A 能以不可忽略的优势 ε 成功猜测会话密钥是真实的还是随机的,那么存在输入为 $(G_1, G_2, e, q, P, X^*, Y^*, K^*)$ 的算法 $\Re$,通过调用 A 能以不可忽略的优势区分真实会话密钥和随机值.

设猜测游戏的交互过程中 A 发起会话的轮数为 L. 具体交互过程如下:

①选择随机数 $a \in \{1, 2, \cdots, L\}$;

②调用 A 完成对 AM 中 MT 与 RS 间匿名漫游认证协议的模拟,给 A 提交 (G_1, G_2, e, q, P) 作为协议执行的公共参数;

③无论 A 是参与一个新的会话密钥的建立(除第 a 次会话外)还是获得消息,都遵循匿名漫游认证协议中相应参与者的执行. 当一个会话结束,与之相关的密钥就要在参与者的内存中擦除;若参与者被攻陷或会话已暴漏(除第 a 次会话外),就把这个被攻陷的参与者或相应的会话密钥的所有信息提供给 A.

④在第 a 次会话中,输入(MT,RS,a),调用 MT 和 RS 的会话,设 MT 向 RS 发送(MT,a,X^*).

⑤RS 收到(MT,a,X^*)后,向 MT 发送(RS,a,Y^*).

⑥如果 MT 选择会话(MT,RS,a)作为最后一次测试会话,那么向 A 提供 K^* 作为询问应答.

⑦如果会话(MT,RS,a)没有暴漏,或者选择的第 a 轮会话外的某一次会话作为最后一次测试会话,或者 A 没有选择测试会话就终止了,那么 $\Re$ 输出 $b' \leftarrow \{0,1\}$,然后终止.

⑧如果 A 终止并输出比特 b'. 那么 $\Re$ 终止并也输出比特 b'.

根据 A 的测试会话是否与算法 $\Re$ 选择的一致,分两种情况讨论.

①敌手 A 选择的测试会话和 $\Re$ 随机选择的会话相同.

在测试会话中,给 A 的应答为 K^*,如果 $\Re$ 的输入为 $(G_1, G_2, e, q, P, X, Y, K)$,即是真实的会话密钥协商参数和会话密钥,则给 A 的询问应答就是 MT 和 RS 在会话 a 中的真实会话密钥 K;如果 $\Re$ 的输入为 $(G_1, G_2, e, q, P, X^*, Y^*, K^*)$,即是随机值,那么询问的应答也是随机的. 如果 $\Re$ 的输入是以 $\frac{1}{2}$ 的概率随机选择的,那么 A 将以 $\frac{1}{2} + \varepsilon$ 的概率猜对测试应答是真实值还是随机值,其中 ε 是不可忽略的,这也等价于算法 $\Re$ 以 $\frac{1}{2} + \varepsilon$ 的概率猜对它的输入是真实会话密钥还是随机值.

②敌手 A 的第 a 次会话没有被选作测试会话.

这种情况下算法 $\Re$ 输出一个随机比特后将结束会话,因此,猜对输入分布的概率是 $\frac{1}{2}$.

令事件 E 表示敌手 A 选择的测试会话恰好是第 a 次会话,$\Pr[E] = \frac{1}{L}$,并且敌手 A 能以不可忽略的优势 ε 猜对测试应答是真实值还是随机值. 则有

$$\Pr[A \text{ 猜测成功}] = (\frac{1}{2} + \varepsilon)\Pr[E] + \frac{1}{2}(1 - \Pr[E]) = \frac{1}{2} + \frac{\varepsilon}{L}.$$

由于算法 $\Re$ 以 A 为子程序运行,则 $\Pr[A \text{ 猜测成功}] = \Pr[\Re \text{ 猜测成功}]$,即算法 $\Re$ 能以不可忽略的优势区分真实会话密钥和随机值. 因此协议 δ 满足会话密钥安全的性质 2.

由于在 AM 中,敌手不能进行伪造、篡改和重放消息,则协议 δ 在 AM 中是会话密钥安全的.

4.2 UM 中的协议

对于 RS 对 MT 的认证使用基于身份的匿名认证器 $\lambda_{Enc,TID,T}$,其安全性、匿名性证明详见文献[12]. 对于 MT 对 RS 的身份认证采用基于时戳的签名认证器 $\lambda_{Sig,T}$,其安全性证明过程详见文献[13].

首先,将上述 2 种认证器应用于 AM 协议消息流,然后在不影响协议可证安全性的前提下,将 MT 的身份标识隐藏起来,使攻击者无法获得其真实有效的身份信息. 最后应用文献[14]中的方法优化 UM 中的协议,得到 UM 中的 MT 漫游协议(如图 1 所示),且文献[15]已证明优化过程并不影响协议的安全性.

定理 2 当签名、非对称加密、哈希等算法安全且难解时,协议 δ 在 UM 中是安全的,即本文协议是安全的匿名漫游认证协议.

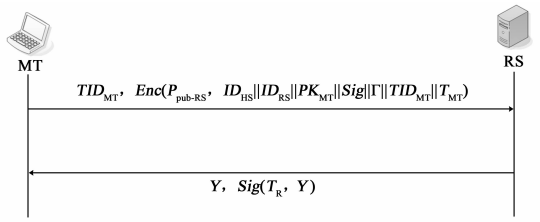


图1　UM中的MT漫游协议

证明　运用基于身份的匿名认证器 $\lambda_{Enc,TID,T}$ 和基于签名和随机数的认证器 $\lambda_{Sig,T}$ 把协议 δ 直接转化为 UM 中会话密钥安全的匿名漫游认证协议. 由于所采用的认证器 $\lambda_{Enc,TID,T}$ 和 $\lambda_{Sig,T}$ 是可证安全的,所以根据 CK 安全模型自动编译得到 UM 中的协议 δ 是可证安全的.

5　协议分析

5.1　匿名性分析

漫游认证过程中,RS 和外部用户(包括攻击者)都无法获悉移动终端的真实身份. 首次漫游认证时,MT 使用一次性公钥及签名信息作为认证凭证,由于不包含 MT 的身份、位置等隐私信息,且一次性公钥经过了随机数处理,保证了 MT 漫游认证过程的身份匿名性. 在重复漫游认证阶段,仅用散列值作为认证凭证,更不会泄露 MT 的身份信息.

任何合法 MT 均无法通过自己的临时身份标识计算其他 MT 的身份标识;临时身份的加密传输,在实现用户真实身份匿名的同时,又实现了对其临时身份的保护,增强临时身份的安全性;即便临时身份遭泄露,攻击者也无法获知该用户的真实身份.

为实现用户漫游过程的高效性,当 MT 向同一 RS 多次申请漫游时,本文协议设计了效率更高的重复漫游过程;但是在重复漫游阶段,RS 可将 MT 的多次漫游申请关联起来,由于 RS 是安全可信的,则 RS 对漫游申请的关联并未对协议的安全性造成影响;若 MT 追求漫游过程的强匿名性,则 MT 每次漫游之前,向 HS 重新注册,保证 MT 每次漫游时所持有的临时身份标识各不相同,确保 MT 具有强匿名性和不可追踪性.

5.2　匿名的可控性

一次性公钥在提供匿名性的同时具有可追踪性,当漫游 MT 出现恶意匿名行为后,RS 将 MT 的一次性公钥提交给 HS,HS 响应合法的匿名性撤销请求,即利用保存的相关信息揭示 MT 的真实身份. 匿名的可控性有效防止了 MT 恶意匿名行为的发生.

匿名的可控性并不影响 MT 的匿名性,因为本协议的可控性是有选择的可控,当且仅当 MT 出现恶意行为时才触发匿名追踪机制,并且 HS 需验证匿名撤销请求的合法性. 因此本协议有选择的可控并不影响漫游认证过程中 MT 的身份匿名性.

5.3　安全性分析

5.3.1　无关联性

MT 基于随机数生成一次性公钥,具有随机性和新鲜性的特点,外部用户无法根据一次性公钥将 MT 不同的会话联系起来. 虽在重复漫游认证阶段,散列值间具有关联性,但是对散列值的加密处理,使外部用户无法获知散列值的明文信息,因此重复漫游认证阶段,外部用户也无法通过散列值将 MT 不同的会话联系起来.

对于 RS 而言在重复漫游认证时,为了减少漫游过程的计算量和通信时延,采用散列值作为认证凭证,因此重复认证阶段 RS 可将 MT 的多次会话联系起来,若 MT 需要完全无关联性的漫游匿名认证,则 MT 可每次生成各不相同的一次性公钥及签名向 RS 证明其身份的合法性.

5.3.2　安全会话密钥协商

漫游认证过程中,MT 与 RS 间协商的会话密钥是由双方选择的秘密随机参数共同决定的,任何一方都无法伪造合法的会话密钥;并且秘密随机数的安全存储,保证了会话密钥的安全性;同时秘密随机数的随机性,保证了会话密钥的新鲜性.

5.3.3　双向认证

首次漫游认证时,RS 通过一次性公钥和签名信息的正确性确认漫游 MT 的身份合法性;重复漫游认证时,RS 通过散列值 G_l 来验证 MT 的合法性,由于 G_0 已通过 RS 的认证,根据散列函数的单向性计算特点,只有已通过漫游身份认证的 MT 才能出示正确有效的 G_l. 同时,MT 基于 RS 签名信息的合法性完成对 RS 的身份合法性验证.

5.3.4　抗伪造攻击

RS 基于等式 $e(P_{MT},P)=e(U_{MT},P)e(V_{MT},P_{Pub-HS})$ 可确认 P_{MT} 中含有 HS 的系统主密钥;并且通过等式 $SigP=X''+h'P_{MT}$ 可确认签名 Sig 中含有 HS 的主密钥,即 Sig 和 P_{MT} 具有不可伪造性;同时,U_{MT} 和 V_{MT} 同样是无法伪造的,否则无法通过上述等式的验证.

5.3.5　前/后向安全性

本文协议中,即使攻击者获得某次漫游申请过程中 MT 的相关参数,由于漫游证明信息生成参数具有较强的新鲜性,因此攻击者无法获知先前的证明信息及相关参数;同时,攻击者也无法猜测 MT 即将发送的漫游证明信息及相关参数.

5.4　性能分析

5.4.1　计算效率

本文协议中当 MT 漫游远程域时,已完成家乡域的注册,因此本文协议漫游过程的计算效率以 3.3 节描述的漫游过程为主.

由表 1 可知,本文协议中 MT 的计算量远小于文献

[4,5]中相关方案的计算量,并延续了部分传统漫游认证协议[6,7]中 MT 计算量小的优势,但本文协议的漫游过程中无需 HS 的协助 RS 即可完成对 MT 合法性的验证,即本文协议将传统漫游协议的 2 轮交互认证模式,改进为 1 轮交互认证模式,通信时延较低;同时,当同一 MT 重复漫游时,本文协议的重复漫游过程具有更高的通信效率;相较与传统漫游协议[4~7]而言,本文协议降低了 RS 和 HS 的计算负载,减少了协议的消息交互轮数,降低了通信时延. 由于在安全性与计算开销间仅能寻求平衡,因此为了确保移动终端通信过程的安全性,本文协议使用了非对称加解密等运算量较大的算法,但在实际应用中,可根据应用环境的具体要求减少对通信消息的加密操作.

表 1 运算开销比较

相关运算类型	本文协议		文献[4]	文献[5]	文献[6]	文献[7]
	首次认证	重复认证				
双线性运算(MT/RS/HS)	1/4/0	1/1/0	4/4/4	1/0/1	0/0/1	0/0/1
散列运算(MT/RS/HS)	1/5/0	1/2/0	5/4/6	2/1/1	1/0/1	2/0/2
对称加解密(MT/RS/HS)	☆	☆	2/0/2	1/0/1	1/1/0	1/1/0
签名与验签(MT/RS/HS)	1/1/0	1/1/0	0/1/1	1/2/1	0/2/2	0/2/2
MAC 次数(MT/RS/HS)	☆	☆	2/2/2	☆	☆	☆
信息交换次数(MT-RS/RS-HS)	2/0	2/0	3/2	2/2	2/2	2/2

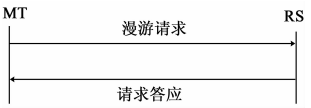
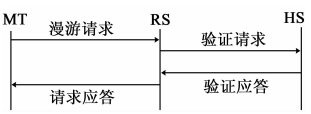
其中☆表示该算法未涉及此操作

5.4.2 通信效率

传统漫游协议[4~7]中,由于远程域认证服务器尚未掌握移动节点的相关注册信息,所以无法直接对 MT 的身份合法性进行验证,因此远程域认证服务器需在家乡域认证服务器的协助下,实现对 MT 的身份合法性验证,即漫游过程中通过 2 轮交互的认证模式完成 MT 的身份合法性验.

由表 2 可知,本文协议中,因 MT 在向远程网络申请漫游服务前,已完成本地网络的注册工作,因此无需 HS 的协助,RS 可直接完成 MT 的身份合法性验证;且本文协议无需在异构无线网络中传递证书,降低了漫游认证过程的通信负载和切换时延,提高了异构无线网络漫游切换速度和协议的执行效率.

表 2 漫游通信时延比较

	漫游认证模型	漫游特点	通信时延比较
本文协议		RS 通过 MT 持有一次性公钥和签名信息直接验证其身份的合法性. 由 1 轮消息交互完成.	小 无需 HS 的协助
文献[4~7]		RS 在 HS 的协助下完成对 MT 身份合法性验证. 由 2 轮消息交互完成.	较大 需要 HS 的协助

6 结束语

本文针对传统无线网络漫游匿名认证协议存在匿名不可控和通信时延较大的不足,基于一次性公钥提出异构无线网络可控匿名漫游认证协议,移动终端与远程网络认证服务器间的 1 轮消息交互完成其身份合法性验证,大幅度缩短了通信时延,并且当移动终端有恶意匿名行为发生时,家乡网络认证服务器可根据远程网络认证服务器提供的相关信息撤销移动终端的身份匿名性,在实现移动终端匿名认证的同时,有效防止其恶意行为的发生,且其通信时延较小. CK 安全模型下的形式化分析表明本文协议是可证安全的;并且分析可知,本文协议除匿名性和无关联性外,还具有双向认证、安全的会话密钥协商和抗伪造攻击等特点.

参考文献

[1] Jiang Y X, Lin C, Shen X M. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks[J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 569 – 2577.

[2] Yang G M, Wong D S, Deng X T. Anonymous and authenticated key exchange for roaming networks [J]. IEEE

Transactions on Wireless Communications, 2007, 6(9): 035 – 1042.

[3] Shi M H, Rutagemwa H, Shen X M. A service-agent-based roaming architecture for WLAN/ cellular integrated networks[J]. IEEE Transactions on Vehicular Technology, 2007, 56(5): 168 – 3181.

[4] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271 – 1281.
Peng Hua-xi. An ientity-bsed athentication mdel for mltidmain[J]. Chinese Journal of Computer, 2006, 29(8), 1271 – 1281. (in Chinese)

[5] 姜奇, 马建峰, 等. 基于身份的异构无线网络匿名漫游协议[J]. 通信学报, 2010, 31(10): 138 – 145.
Jiang Qi, Ma Jianfeng, et al. Identity-based roaming protocol with anonymity for heterogeneous wireless networks [J]. Journal on Communications, 2010, 31(10): 138 – 145. (in Chinese)

[6] 朱辉, 李晖, 苏万力, 等. 基于身份的匿名无线认证方案[J]. 通信学报, 2009, 30(4): 130 – 136.
Zhu Hui, Li Hui, Su Wanli, et, al. ID-based wireless authentication scheme with anonymity[J]. Journal on Communications, 2010, 31 (10): 138 – 145. (in Chinese)

[7] 姜奇, 李光松, 马建峰, 等. 基于身份的无线认证方案的安全缺陷及改进[J]. 通信学报, 2010, 31(9A), 209 – 216.
Jiang Qi, Li Guangsong, Ma Jianfeng, et, al. Security flaws and improvement of an id-based wireless authentication scheme with anonymity[J]. Journal on Communications, 2010, 31(9A): 209 – 216. (in Chinese)

[8] 张胜, 徐爱国, 胡正名, 等. 一种基于身份的一次性公钥的构造[J]. 电子与信息学报, 2006, 28(8): 1412 – 1414.
Zhang Sheng, Xu Ai-guo, Hu Zheng-ming. et, al. Construction of the one-off public key based on identity[J]. Journal of Electronics & Information Technology, 2006, 28(8): 1412 – 1414. (in Chinese)

[9] 罗长远, 霍士伟, 刑洪智. 普适环境中基于一次性公钥的匿名认证方案[J], 通信学报, 2012, 33(2): 93 – 98.
Luo Chang-yuan, Huo Shi-wei, Xing Hong-zhi. Anonymous authentication scheme based on one-off public key in pervasive computing environments[J]. Journal on Communications, 2012, 33(2): 93 – 98. (in Chinese)

[10] 张恩, 蔡永泉. 基于双线性对的可验证的理性秘密共享方案[J]. 电子学报, 2012, 40(5): 1050 – 1054.
Zhang En, Cai Yong-quan. A werifiable rational secret sharing scheme based on bilinear pairing[J]. Acta Electronica Sinica, 2012, 40(5): 1050 – 1054. (in Chinese)

[11] Canerri R, Krawczyk H. Analysis of key exchange and their use for building secure channels[J]. Proceedings of the Eurocrypt. Springer – Verlage, 2001, 452 – 474.

[12] 姜奇, 马建峰, 李光松, 等. 基于 WAPI 的 WLAN 与 3G 网络安全融合[J]. 计算机学报, 2010, 33(9): 1675 – 1685.
Jiang Qi, Ma Jianfeng, Li Guangsong, et, al. Security integration of WAPI based WLAN and 3G[J]. Chinese Journal of Computer, 2010, 33(9): 1675 – 1685. (in Chinese)

[13] Tin Y S T, Vasanta H, Boyd C. Protocols with security proofs for mobile applications[A]. Proceedings of the ACISP 2004[C]. Sydney, Australia, 2004. 358 – 369.

[14] Tin Y S T, Boyd C, Nieto J G. Provably secure key exchange: an engineering approach[A]. Proceedings of the Australasian Information Security Workshop[C]. Darlinghurst, Australasian, 2003. 97 – 104.

[15] Yang G M, Wong D S, Deng X T. Formal security definition and efficient construction for roaming with a privacy-preserving extension[J]. Journal of Universal Computer Science, 2008, 14(3): 441 – 462.

作者简介

周彦伟　男, 1986 年生于甘肃通渭. 工程师, 陕西师范大学计算机科学学院博士生. 研究方向为无线通信技术、匿名通信技术、密码学.
E-mail: zhouyanwei1986@163.com

杨　波(通信作者)　男, 1963 年生于陕西富平. 教授, 博士生导师, 陕西省“百人计划”特聘教授. 研究方向为密码学、信息安全.
E-mail: byang@snnu.edu.cn