可证安全的移动互联网可信匿名漫游协议

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 西安 710062)

[2)](保密通信重点实验室 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 文中提出了移动互联网下移动可信终端(MTT)的可信漫游协议,协议仅需 1 轮消息交互即可实现 MTT 的匿名漫游证明,远程网络认证服务器通过验证 MTT 注册时家乡网络认证服务器为其签发的漫游证明信息的合法性,完成对 MTT 相关属性的认证,同时保证了 MTT 隐私信息的安全性和匿名性.最后运用 CK 安全模型证明了协议是会话密钥安全的,在继承传统漫游协议身份匿名性和不可追踪性的同时,具有较高的安全性、抗攻击性和通信效率.

关键词 移动互联网;匿名漫游认证;可信认证;CK 安全模型

中图法分类号 TP393 **DOI 号** 10.3724/SP.J.1016.2015.00733

Provable Secure Trusted and Anonymous Roaming Protocol for Mobile Internet

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* 710062)

[2)](*Science and Technology on Communication Security Laboratory, Chengdu* 610041)

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

Abstract The trusted roaming protocol of Mobile Trusted Terminal (MTT) in Mobile Internet is presented in this paper. The remote network authentication server proves the legality of roaming authentication information which is signed and published by home network authentication server when its registration. The process of anonymous roaming authentication is accomplished by merely one round of messages exchange. At the same time, the safety and anonymity of the MTT privacy information can be ensured in this process. Finally, the current paper successfully proves that this protocol is SK-security by applying CK security model. This protocol not only inherits the identity anonymity and non-tracking from traditional roaming protocol, but also has high security, anti-aggression and communication efficiency.

Keywords Mobile Internet; anonymous roaming authentication; trusted authentication; CK security model

1 引 言

网络通信技术的快速发展,促使 Internet 由无线互联网向无线移动互联网演变,使得移动互联网已成为下一代网络发展的趋势.由于本地网络覆盖范围的限制,为满足移动用户的漫游访问需求所提出的各类问题,推进了关于移动互联网关键技术——漫游

收稿日期:2013-06-18;最终修改稿收到日期:2014-12-21.本课题得到国家自然科学基金(61272436,61402275,61303092)、保密通信重点实验室基金(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(2015-MS-10)、陕西省自然科学基金(2014JQ8309)、中央高校基本科研业务费专项资金(GK201504016)及陕西师范大学优秀博士论文项目(X2014YB01)资助.**周彦伟**,男,1986 年生,博士研究生,工程师,主要研究兴趣为匿名通信技术、信息安全、无线网络通信技术.E-mail: zyw_snnu@foxmail.com. **杨 波**(通信作者),男,1963 年生,博士,教授,博士生导师,陕西省"百人计划"特聘教授,主要研究领域为信息安全、密码学等.E-mail: byang@snnu.edu.cn. **张文政**,男,1966 年生,研究员,主要研究领域为信息安全等.

服务机制的研究.当用户漫游到家乡网络之外的外地网络时,漫游服务机制在确保漫游用户保持通信连接的同时,须完成漫游用户的身份合法性认证,因此漫游服务过程中身份认证是重中之重.

网络技术的迅速发展,使得身份合法性认证已不再是判断用户安全的充要条件,而应在身份合法的同时关注终端平台是否可信,即终端平台的可信性已成为用户安全的必要条件之一.因此促进了可信计算(Trusted Computing)技术的兴起及发展.可信计算工作组(Trusted Computing Group,TCG)发布可信平台模块(Trusted Platform Module,TPM)规范[1]和移动可信模块(Mobile Trusted Module,MTM)规范[2],旨在以硬件芯片为基础,构建安全、可靠、可信的终端平台(其中 TPM 用于非移动终端,MTM 用于移动终端),同时终端平台的可信安全机制保护了用户隐私信息和敏感数据的安全性.因此须在漫游认证消息中增加用户终端平台的可信性验证信息,即在可信计算环境下,完成可信终端的漫游服务.

如图 1 所示,可信计算环境下的移动互联网主要由移动可信终端(Mobile Trusted Terminal,MTT),家乡网络认证服务器(Home network authentication Server,HS)和远程网络认证服务器(Remote network authentication Server,RS)组成,同时还包括可信第三方移动互联网管理中心 CA.图 1 所示为可信移动互联网下 MTT 的漫游通信示意图.

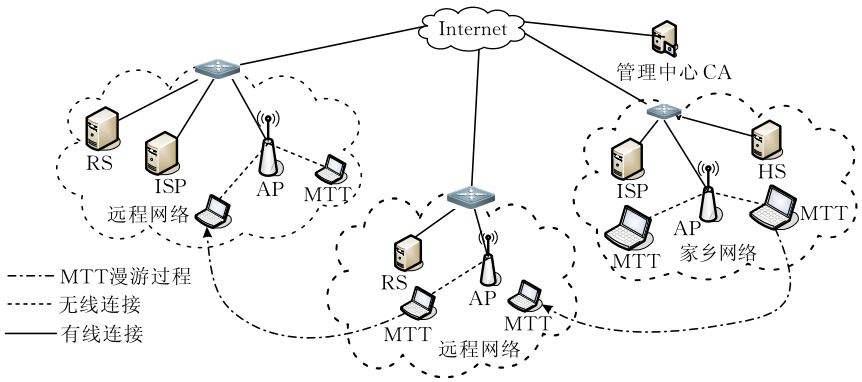


图 1 可信移动互联网下 MTT 的漫游通信模型

由于在传统漫游通信机制中,家乡网络和外地网络的认证服务器之间就漫游通信服务会事先签订好通信协议,各网络均允许非本地用户的接入,但是,当且仅当漫游用户完全通过该网络认证服务器的认证后,才允许其接入.为了保护漫游通信过程中漫游用户的隐私信息,漫游认证机制在验证漫游用户身份合法性的同时,为用户提供了身份的匿名性和不可追踪性.然而,由于移动互联网的特殊性,移动互联网下的漫游协议在满足身份匿名性和不可跟踪性的同时,还需兼顾以下两个方面:

(1)移动终端的计算能力和能量是有限的,为满足用户的移动需求,漫游协议应尽量减轻协议参与方的计算量,特别是降低移动终端的计算量.

(2)由于无线网络具有相对较低的带宽,并且信道易出错,因此,漫游协议在降低消息长度的同时应减少协议的交互轮数.

从本质上讲,安全漫游即是跨域的身份认证、平台可信性评估、密钥协商及用户的隐私保护等.国内外研究人员在漫游协议、跨域服务申请等方面进行了大量研究.

文献[3]基于对称加密提出一种高效的具有用户匿名性的无线认证协议,并且运算量较低.文献[4]发现文献[3]的方案存在匿名性缺陷,在分析其缺陷的基础上提出基于公钥的改进方案,但改进方案的计算开销较大.文献[5]分别基于秘密分割和自验证公钥机制提出了两种匿名漫游协议,但是这两种协议都无法满足漫游用户的身份不可追踪性,仅仅具有身份匿名性.文献[6]在分析无线漫游机制安全需求的基础上,给出了设计匿名无线漫游机制的通用框架.在文献[6]对漫游通用框架的研究基础上,文献[7]基于 Diffie-Hellman 密钥交换和证书公钥机制进一步提出具体的无线漫游协议.由于在传统漫游通信中网络运营商两两之间需事先签订漫游协议,为了避免签订漫游协议而造成管理的不便,文献[8]基于代理技术就漫游过程的认证和计费问题提出了新的设计框架.在文献[9]中提出了一种基于身份的漫游协议,但该协议无法满足漫游用户的身份匿名性.为了实现多信任域间的漫游通信需求,文献[10]提出一种基于身份的多信任域认证模型,但该模型的计算量较大,推广性较差.文献[11]对基于

身份的匿名无线认证技术进行了研究，在现有技术的研究基础上提出了基于身份的匿名无线认证方案，该方案基于公钥完成家乡认证服务器与外地认证服务器间的身份合法性验证. 文献[12]提出异构无线网络下的匿名认证和密钥协商协议，引入用户的临时认证身份和临时通信身份实现用户的身份匿名. 文献[13]对异构网络通信实体进行抽象，建立通用的接入认证模型. 文献[14]提出了一种适用于异构无线网络的匿名漫游协议，协议流程简化，且具有较强的匿名性. 文献[15]在移动互联网下提出可信移动平台的接入机制，实现可信计算环境下可信移动终端的服务接入及漫游接入等.

无论是传统的漫游协议[12-14]，还是跨域服务申请[10-11,15]，对漫游用户的身份认证原理都基本相同. 当漫游用户向 RS 申请漫游时，由于 RS 并未掌握漫游用户的注册信息，因此 RS 需在 HS 的协助下完成对漫游用户的身份合法性验证，即 RS 将移动终端的漫游证明信息发给 HS，由 HS 负责验证移动终端的合法性，而 RS 仅根据 HS 的验证反馈信息制定相应的决策，因此传统漫游协议或跨域服务申请往往需要 2 轮（移动终端↔RS，RS↔HS）的消息交互才能完成用户的漫游（或跨域）接入，可见在移动互联网下传统漫游（或跨域）机制中移动终端的计算负载较重，并且通信时延较大.

针对现有方案所存在的上述不足，本文提出可证安全的移动互联网可信匿名漫游协议. 该协议中，成功注册家乡网络后，MTT 获得由 HS 签发的漫游证明信息；在申请漫游服务时，RS 通过验证漫游证明信息的合法性，完成对 MTT 身份合法性和平台可信性（本文平台可信性即指平台的真实性和完整性）的验证，同时保证了 MTT 隐私信息的安全性，并且漫游过程仅需 1 轮消息交互即可完成漫游认证，由于漫游过程的消息交互轮数的减少，在提高协议执行效率的同时，降低了协议的通信时延.

本文协议的特点：

(1) 安全性提高. 本文协议实现了漫游过程对 MTT 的身份合法性和平台可信性的验证，保证了 MTT 身份的匿名性和不可追踪性；同时提高了其安全性，弥补了传统移动互联网接入认证协议在 MTT 漫游时安全性保护和平台可信性验证方面的不足.

(2) 通信时延降低. 本文协议中消息交互轮数减少，减轻了 MTT 的计算负载，降低了通信时延，并提高了协议的执行效率. 相较于传统漫游协议而言，本文协议更适用于在移动互联网络环境下使用.

(3) 兼容性强. 本文协议即适用于可信环境下漫游用户的身份合法性及平台可信性验证，又适用于非可信环境下漫游用户的身份合法性鉴别.

(4) 应用广泛. 本文的漫游认证策略可用于 3G 网络下移动用户的漫游通信及资费服务管理等应用场景，具有广泛的应用性.

本文第 2 节提出移动互联网可信匿名漫游协议，详细介绍协议的执行流程和信息注销、远程失效等漫游认证的管理机制；第 3 节在 CK 安全模型下对本文协议的安全性进行形式化证明；第 4 节从匿名性、抗攻击性和工作效率等方面对本文漫游协议进行分析；最后是结束语.

2　移动互联网可信匿名漫游协议

本文使用的相关符号定义如下：

n 是大素数；r_A、S_A 是 A 随机选取的秘密数；ID_A 是用户 A 的身份标识；TID_A 是 HS 为本地用户 A 生成的临时身份标识；$\oplus$ 为异或运算；$\|$ 为连接符；$\in_C$ 表示从相应的集合中随机选取一个数；KS_A 是 A 的私钥；KP_A 是 A 的公钥；$Cert_A$ 是认证服务器 A 的身份证书；T_A 是 A 产生的时间戳；$\langle AIK_{\text{Priv}}, AIK_{\text{Pub}}\rangle$ 为安全芯片（TPM 或 MTM）的身份证明密钥对，$Cert(AIK_{\text{Pub}})$ 为可信平台的 AIK 证书；KS_A^{-1} 是 A 关于私钥 KS_A 的求逆运算值，令 $KS_A^{-1}KP_A = Q$，其中 Q 为常数，即用户的私钥求逆运算值与其公钥的乘积为常数.

本文使用的相关运算定义如下.

$E(k,m)$ 和 $D(k,c)$ 是对称密钥加密/解密算法；$ENC(KS,m)$ 和 $DEC(KP,c)$ 是非对称密钥加密/解密算法；$H(m)$ 为标准散列算法；$F(K,N)$ 为带参数的密钥推导函数，其中 K，N 为相关参数.

系统建立时，各认证服务器向管理中心 CA 注册，由 CA 负责管理各认证服务器的安全性及其他相关事宜，并协助各认证服务器完成会话密钥及会话标识的安全协商，同时 CA 向各认证服务器签发证明其身份的身份证书.

MTT、HS 和 RS 的公私钥对分别为 $\{KP_{\text{M}}, KS_{\text{M}}\}$、$\{KP_{\text{H}}, KS_{\text{H}}\}$ 和 $\{KP_{\text{R}}, KS_{\text{R}}\}$，其中公钥对外发布；CA 为 HS 和 RS 签发的身份证书依次为 $Cert_{\text{H}}$ 和 $Cert_{\text{R}}$.

本文协议的安全性基于以下假设.

假设 1.　各网络认证服务器均可信，既不会发

送虚假信息，也不会利用已掌握的 MTT 信息实施假冒攻击，更不会随意揭示 MTT 的真实身份. 同时为本地 MTT(即本地网络用户)建立漫游证明信息的注销列表，并对外提供注销列表的查询下载服务.

假设 2. 各认证服务器获得由管理中心 CA 签发的证书，证书包含 CA 签名等信息，并通过安全途径向外公布其相关参数. 即在 CA 的协助下，各网络认证服务器完成彼此间安全通信信道及信任关系的建立.

假设 3. 各认证服务器间的时间同步机制可保证消息时戳的新鲜性及同步性.

移动互联网可信匿名漫游协议由以下两个阶段组成：

第 1 阶段为注册家乡网络. 主要完成 HS 与 MTT 间的身份合法性认证及 HS 对 MTT 平台的可信性验证，并且完成会话密钥的协商和漫游证明信息的分发，即完成 MTT 的合法性及可信性认证；

第 2 阶段为安全漫游. 基于漫游证明信息 RS 完成对 MTT 身份合法性和平台可信性的验证，即实现 MTT 的安全漫游接入.

MTT 首次基于漫游证明信息完成漫游申请后，在保证 MTT 身份匿名和不可追踪的前提下为实现高效、快捷的漫游身份认证，本文 2.3 节在首次认证的基础上给出重复漫游认证协议，利用哈希散列链的认证策略以减少漫游认证过程的计算开销和通信时延.

2.1 可信认证协议——注册家乡网络

MTT 通过执行可信认证协议完成向家乡网络的注册，获得 HS 为其生成的漫游证明信息.

可信认证协议如图 2 所示，协议具体描述如下.

(1) MTT 向 HS 发送申请，申请注册本地家乡网络.

(2) HS 收到注册申请后，执行以下步骤.

① 首先选取秘密随机数 $r_H \in_C [2, n-1]$，并计算 $D_H = (r_H + KS_H) KP_M$，通过计算将秘密数 r_H 安全擦除；

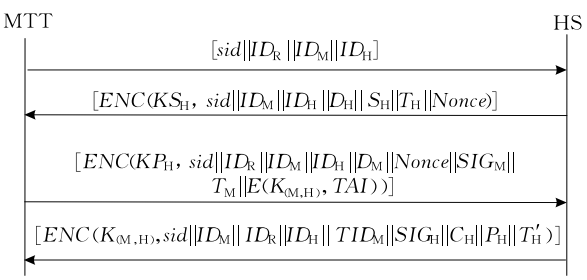


图 2 可信认证协议

② 最后选择随机数 S_H，并生成时戳 T_H，然后发送消息给 MTT.

$HS \rightarrow MTT: ENC(KS_H, sid \| ID_M \| ID_R \| ID_H \| D_H \| S_H \| T_H \| Nonce)$.

其中 sid 为会话标识，时间戳 T_H 和随机数 $Nonce$ 保证了消息的新鲜性，并且 $Nonce$ 可用于标记通信消息是否得到相应的回复.

(3) MTT 收到响应消息后，MTT 执行以下步骤.

① 首先选取秘密随机数 $r_M \in_C [2, n-1]$，并计算 $D_M = (r_M + KS_M) KP_H$，通过计算将 r_M 安全擦除；

② 然后分别按式(1)、(2)计算与 HS 间的会话密钥 $K_{(M,H)}$ 和签名信息 SIG_M：

$$K_{(M,H)} = KS_M^{-1}(r_M + KS_M) D_H \tag{1}$$

$$SIG_M = ENC(KS_M, sid \| ID_M \| ID_H \| ID_R \| D_M \| Nonce) \tag{2}$$

③ 接着使用存储根密钥从安全芯片中读取身份密钥 AIK_{Priv}，并使用 AIK_{Priv} 签名平台配置寄存器值 $PCRs$ 和秘密随机数 S_H，按式(3)生成 MTT 的平台可信性验证信息 TAI：

$$TAI = SML \| Cert(AIK_{Pub}) \| SIG_{TPM}(PCRs, S_H) \tag{3}$$

其中 SML 为完整性度量日志；$Cert(AIK_{Pub})$ 为 MTT 的 AIK 证书；$SIG_{TPM}(PCRs, S_H) = ENC(AIK_{Priv}, PCRs \| S_H)$；

④ 最后计算 $E(K_{(M,H)}, TAI)$，并生成时戳 T_M 和随机数 $Nonce$，然后发送消息给 HS.

$MTT \rightarrow HS: ENC(KP_H, sid \| ID_M \| ID_H \| ID_R \| D_M \| Nonce \| SIG_M \| T_M \| E(K_{(M,H)}, TAI))$.

(4) HS 收到验证请求后，执行以下步骤.

① 首先验证签名 SIG_M 的合法性及参数的正确性，实现对 MTT 的身份合法性验证，并且验证消息是否由 MTT 发送；

② 身份合法性验证通过后，按式(4)计算会话密钥 $K'_{(M,H)}$，并使用 $K'_{(M,H)}$ 和 AIK_{Pub} 分别解密 $E(K_{(M,H)}, TAI)$ 和 $SIG_{TPM}(PCRs, S_H)$ 获得 MTT 的可信性验证信息及平台配置寄存器值 $PCRs$，同时通过秘密数 S_H 完成对可信性验证信息的合法性验证：

$$K'_{(M,H)} = KS_H^{-1}(r_H + KS_H) D_M \tag{4}$$

③ 最后运用平台可信性验证策略对 MTT 平台的可信性进行验证.

文献[15-19]对平台可信性验证策略及相关关

键技术进行了详细研究，本文使用相关策略实现对 MTT 的平台可信性验证. 篇幅所限，本文不再赘述终端平台的可信性验证策略.

若 MTT 平台的可信性验证失败，则终止协议，否则 HS 为身份合法且平台可信的 MTT 分配唯一的临时标识号 TID_M，并生成漫游证明信息.

MTT 的身份合法性及平台可信性验证通过后，HS 执行以下步骤：

(1) HS 为 MTT 分配临时身份标识.

HS 首先生成秘密随机数 S_{MTT}，然后按式(5)为 MTT 生成临时身份标识 TID_M，同时建立 MTT 的注册信息项〈TID_M，S_{MTT}，ID_M，$K_{(M,H)}$〉.

$$TID_M = H(ID_M \| ID_H \| S_{MTT}) \tag{5}$$

(2) HS 为 MTT 生成漫游证明信息.

① 首先计算密钥 $K_1 = F(K_{(H,R)}, 0)$，$K_2 = F(K_{(H,R)}, 1)$，其中 $K_{(H,R)}$ 为认证服务器 HS 与 RS 间安全协商的会话密钥；

② 然后生成身份凭证 $AUTHEN = sid_{HR} \| Cert_{HS} \| TID_M \| T_E$，其中 T_E 为身份凭证的过期时间，sid_{HR} 为认证服务器 HS 与 RS 间安全协商的会话标识；

③ 最后计算 $C_R = E(K_1, AUTHEN)$，$P_R = E(K_2, sid_{HR} \| C_R)$，生成漫游证明信息 $M_{MTT} = C_R \| P_R$.

(3) 漫游证明消息生成后 HS 发送应答消息给 MTT.

① 首先计算 $K_3 = F(K_{(M,H)}, 0)$，$K_4 = F(K_{(M,H)}, 1)$，$C_H = E(K_3, M_{MTT})$，$P_H = E(K_4, sid \| C_H)$；

② 然后按式(6)计算签名信息 SIG_H：

$$SIG_H = ENC(KS_H, sid \| ID_M \| ID_R \| ID_H \| TID_M) \tag{6}$$

③ 最后生成时戳 T'_H，并发送应答消息给 MTT.

HS→MTT：$ENC(K_{(M,H)}, sid \| ID_M \| ID_R \| ID_H \| TID_M \| SIG_H \| C_H \| P_H \| T'_H)$.

(5) MTT 收到由安全信道发送的应答消息后，执行以下步骤.

① 首先解密应答消息，验证签名 SIG_H 及参数的正确性，MTT 验证 HS 身份的合法性，即 MTT 与 HS 间完成双向的身份合法性验证；

② 身份合法性验证通过后，计算 $K'_3 = F(K_{(M,H)}, 0)$，$K'_4 = F(K_{(M,H)}, 1)$，并验证 $E(K'_4, sid \| C_H)$ 与接收到的 P_H 是否相等，完成消息完整性及正确性验证；

③ 消息完整性及正确性验证通过后，最后计算 $M_{MTT} = C_R \| P_R = D(K'_3, C_H)$，即 MTT 获得漫游证明信息 M_{MTT}.

此时，MTT 已成功注册家乡网络，并获得 HS 为其生成的漫游证明信息.

2.2　安全漫游协议——漫游远程网络

漫游证明信息获得后，MTT 通过执行安全漫游协议向远程网络申请漫游服务. MTT 通过安全信道将接入请求发送给远程网络认证服务器 RS，向 RS 申请漫游服务.

安全漫游协议如图 3 所示，协议详细介绍如下.

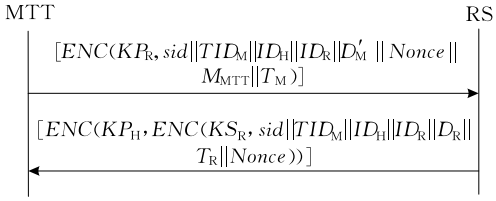


图 3　安全漫游协议

MTT 向 RS 发送漫游申请，向远程网络申请注册. MTT 执行以下步骤：

(1) 首先选取秘密随机数 g，$r'_M \in_C [2, n-1]$，并计算 $D'_M = (r'_M + KS_M)KP_R$，通过计算将秘密随机数 r'_M 安全擦除.

(2) 然后计算 $G_0 = H(g)$.

(3) 最后生成时戳 T'_M，并向 RS 发送漫游申请.

MTT→RS：$ENC(KP_R, sid \| TID_M \| ID_H \| ID_R \| D'_M \| G_0 \| Nonce \| M_{MTT} \| T'_M)$.

RS 收到 MTT 的漫游申请后，RS 执行以下步骤：

(1) RS 验证消息合法性及参数正确性.

① 计算 $K'_1 = F(K_{(H,R)}, 0)$，$K'_2 = F(K_{(H,R)}, 1)$；

② 计算 $P'_R = E(K'_2, sid_{HR} \| C_R)$，验证 P'_R 与接收到的 P_R 是否相等，完成申请消息的完整性和参数的正确性验证；

③ RS 通过计算式(7)获得 MTT 的临时身份标识 TID'_M、HS 的身份证书 $Cert_{HS}$ 及漫游证明信息的过期时间 T_E.

$$AUTHEN = D(K'_1, C_R) = sid_{HR} \| Cert_{HS} \| TID'_M \| T_E \tag{7}$$

(2) RS 验证漫游证明信息 M_{MTT} 的真实性.

① 查询 MTT 注销列表，验证 M_{MTT} 是否已被注销；

② 通过签名验证 M_{MTT} 是否被篡改，基于当前时间与 T_E 间的关系验证 M_{MTT} 在当前时间是否有效；

③ 验证 M_{MTT} 的持有者是否是信息的申请者，判断 $TID'_M = TID_M$ 是否成立，验证 sid_{HR} 和 $Cert_{HS}$

中包含的位置信息是否一致，其中 TID_M 为漫游请求消息中 MTT 的临时身份标识；

④ 验证 $Cert_{HS}$ 的真实性、完整性及有效性.

若上述验证均通过，表明 MTT 持有真实有效的漫游证明信息，则 RS 允许 MTT 的漫游申请. 即 RS 基于漫游证明信息完成对 MTT 身份合法性和平台可信性的验证，否则终止协议.

(3) RS 在漫游认证列表中为 MTT 建立重复漫游认证信息.

若 MTT 是身份合法且平台可信的漫游申请者，RS 执行算法 1 在漫游认证列表中为 MTT 建立重复漫游认证信息.

建立重复漫游认证信息时，RS 执行以下步骤：

① 首先遍历 HS 的注销列表，以验证漫游证明信息 M_{MTT} 是否已被 MTT 注销；

② 然后验证漫游证明信息的合法性及有效性，确保 M_{MTT} 是合法未过期的漫游证明信息；

步骤①和②为可选步骤，在 RS 验证漫游证明信息 M_{MTT} 的真实性时已完成上述步骤的验证，但在漫游认证列表中建立重复漫游认证信息时，为保证认证列表的绝对安全性，可选择重复执行.

③ 接着遍历漫游认证列表，判断列表中是否已存在相同 TID_M 的漫游认证信息，若存在，则结束算法，避免重复建立；否则进行步骤④操作；

④ 最后建立重复漫游认证信息 $\langle TID=H(TID_M), G=H(G_0), N, D, TID_M\rangle$，其中 TID_M 为 MTT 的临时身份标识信息；G 为认证散列值；N 为 MTT 重复漫游申请次数；D 为重复漫游认证信息的过期时间，且 $D=T_E$.

算法 1. 漫游认证列表建立算法.

输入：漫游认证信息 M_{MTT}、身份标识 TID_M

输出：漫游认证列表 $\langle TID, G, N, D, TID_M\rangle$

BEGIN

IF($Traverse(M_{MTT}, LC_{HS})==1$)

//检查 M_{MTT} 是否被注销

//$Traverse(M_{MTT}, LC_{HS})==1$ 表示 M_{MTT} 已被 MTT 注销，则结束漫游认证列表建立算法. 其中 $Traverse()$ 为列表遍历函数，LC_{HS} 为 HS 维护的注销列表，$Traverse(M_{MTT}, LC_{HS})$ 表示遍历注销列表 LC_{HS}，若列表 LC_{HS} 中存在 M_{MTT} 则返回 1，否则返回 0.

Exit(0)；

END IF

IF($Check(D_{now}, T_E)==0$) //检查 M_{MTT} 是否过期

//$Check(D_{now}, T_E)==0$ 表示 M_{MTT} 在当前时间已过期，则结束该算法. 其中函数 $Check()$ 为时间比较函数，D_{now} 为当前时间，若 D_{now} 大于 LT 则 $Check()$ 返回 0，否则返回 1.

Exit(0)；

END IF

IF($Traverse(\langle *,*,*,*,TID_M\rangle, LRA_{RS})==1$)

//检查认证信息是否重复建立. 在漫游认证列表中查找是否存在用户 TID_M 的重复漫游认证信息 $\langle *,*,*,*,TID_M\rangle$，$Traverse(\langle *,*,*,*,TID_M\rangle, LRA_{RS})==1$ 表示漫游认证列表 LRA_{RS} 中存在具有相同 TID_M 的漫游认证信息，则结束漫游认证列表建立算法，避免数据的重复建立. 其中 LRA_{RS} 为 RS 负责维护的漫游认证列表.

Exit(0)；

END IF

//建立重复漫游认证信息

$N=1$；

$TID=H(TID_M)$；

$G=H(G_0)$；

$D=T_E$；//初始化重复漫游认证信息的过期时间

Add $\langle TID, G, N, D, TID_M\rangle$ into (LRA_{RS})；

END

(4) RS 应答 MTT 的漫游请求.

① 首先选取秘密随机数 $r_R\in_C[2, n-1]$，然后计算 $D_R=(r_R+KS_R)KP_M$，通过计算将 r_R 安全擦除；

② 然后按式(8)计算与 MTT 间的会密钥 $K'_{(M,R)}$：

$$K'_{(M,R)}=KS_R^{-1}(r_R+KS_R)D_M \tag{8}$$

③ 最后发送应答消息给 MTT.

RS→MTT：$ENC(KP_M, ENC(KS_R, sid \| TID_M \| ID_H \| ID_R \| D_R \| T_R \| Nonce))$.

MTT 收到 RS 的应答消息后，MTT 执行以下步骤：

(1) 首先解密消息，验证消息的合法性，然后确认消息是由 RS 发送，并验证 RS 的身份合法性，确定 RS 是否是其议定的远程网络认证服务器，实现漫游认证过程中 MTT 和 RS 的双向身份认证；

(2) 最后按式(9)计算与 RS 间的会密钥 $K_{(M,R)}$，完成漫游申请.

$$K_{(M,R)}=KS_M^{-1}(r_M+KS_M)D_R \tag{9}$$

2.3 重复漫游协议

MTT 可基于漫游证明信息 M_{MTT} 多次向 RS 申请漫游认证，RS 通过 M_{MTT} 的合法性完成对 MTT 的身份合法性及平台可信性的验证，这样在一定程度上降低了漫游认证的通信时延和 MTT 的计算负载. 为实现高效、快捷的漫游认证过程，基于 MTT 的首次漫游匿名认证(将通过可信认证和安全漫游进行的漫游认证称为首次漫游匿名认证)，本文提出重复漫游认证协议.

MTT 持认证散列值 G_I 进行第 $I(0<I\leq Max,$

其中 Max 为 RS 设置的 MTT 重复漫游的最大次数)次重复漫游认证申请,具体申请过程如下.

MTT 向 RS 发送重复漫游认证申请. MTT 执行以下步骤:

(1)选取秘密随机数 $r_{\mathrm{M}}^{(I)} \in_C [2, n-1]$,并计算 $D_{\mathrm{M}}^{(I)} = (r_{\mathrm{M}}^{(I)} + KS_{\mathrm{M}})KP_{\mathrm{R}}$.

(2)按式(10)计算散列值 G_I,按式(11)计算临时身份标识 $TID_{\mathrm{M}}^{(I)}$.

$$G_I = H(G_{I-1}) \tag{10}$$

$$TID_{\mathrm{M}}^{(I)} = H(TID_{\mathrm{M}}^{(I-1)}),\ TID_{\mathrm{M}}^{(0)} = TID_{\mathrm{M}} \tag{11}$$

(3)生成时戳 $T_{\mathrm{M}}^{(I)}$,并向 RS 发送重复漫游认证申请消息.

MTT→RS: $ENC(KP_{\mathrm{R}}, sid \| TID_{\mathrm{M}}^{(I)} \| ID_{\mathrm{H}} \| ID_{\mathrm{R}} \| D_{\mathrm{M}}^{(I)} \| G_I \| Nonce^{(I)} \| T_{\mathrm{M}}^{(I)})$.

RS 验证 MTT 重复漫游申请信息的合法性.

(1) RS 执行算法 2 验证重复漫游认证信息的合法性. RS 执行以下步骤:

① 验证重复漫游认证信息$\langle TID_{\mathrm{M}}^{(I)}, G_I, *, *, * \rangle$的存在性. RS 遍历漫游认证列表 LRA 查找漫游认证信息$\langle TID_{\mathrm{M}}^{(I)}, G_I, *, *, * \rangle$,若不存在,则终止,否则进行步骤②验证;

② 验证重复漫游认证信息是否过期. RS 查找漫游认证列表中 MTT 的认证信息 G_I 是否过期,若过期则终止,否则进行步骤③验证;

③ 验证漫游请求消息的合法性. RS 查找漫游认证列表中 MTT 认证信息 G_I 所对应的用户信息是否为 $TID_{\mathrm{M}}^{(I)}$,若是用户信息为 $TID_{\mathrm{M}}^{(I)}$,则证明当前 MTT 已通过身份合法性和平台可信性的验证,进行步骤④操作,否则终止;

④ 更新漫游认证列表中 MTT 的重复漫游认证信息$\langle TID, G, N, D, TID_{\mathrm{M}} \rangle$.

算法 2.　重复漫游认证信息合法性验证及更新算法.

输入:散列值 G_I 和临时身份标识 $TID_{\mathrm{M}}^{(I)}$

输出:更新后的重复漫游认证信息$\langle TID, G, N, D, TID_{\mathrm{M}} \rangle$

BEGIN

IF ($Traverse(\langle TID_{\mathrm{M}}^{(I)}, G_I, *, *, * \rangle, LRA_{\mathrm{RS}}) == 0$)

//遍历漫游认证列表,查找是否存在重复漫游认证信息$\langle TID_{\mathrm{M}}^{(I)}, G_I, *, *, * \rangle$,若不存在,则终止.

Exit(0);

END IF

IF($Check(D_{\mathrm{now}}, D) == 0$)

//漫游认证列表中已存在相应的漫游认证信息$\langle TID_{\mathrm{M}}^{(I)}, G_I, *, *, * \rangle$,$Check(D_{\mathrm{now}}, D) == 0$ 表示重复漫游认证信息在当前时间已过期,则 RS 删除漫游认证列表中该 MTT 的相关重复漫游认证信息,其中 D 为漫游认证信息$\langle TID_{\mathrm{M}}^{(I)}, G_I, N, D, TID_{\mathrm{M}} \rangle$的属性.

Delete the $\langle TID_{\mathrm{M}}^{(I)}, G_I, N, D, TID_{\mathrm{M}} \rangle$ of MTT from LRA_{RS};

Exit(0);

END IF

//更新认证信息的相关关联数据

$N = N+1$;

$TID = H(TID)$;

$G = H(G)$;

IF($Max < N$)

//该 MTT 的重复漫游认证信息已达到最大的重复认证次数,则 RS 删除其相关信息.

Delete the message of MTT from LRA_{RS};

Exit(0);

END IF

//更新漫游认证列表

Updated LRA_{RS};

END

RS 可定期将漫游认证列表中已过期的重复漫游认证信息删除,确保列表遍历的高效性;同时由于身份信息的更新具有不同时性(RS 先更新,MTT 后更新),因此 RS 可在重复漫游认证信息中分别存储连续的两个用户身份散列值(TID_{I-1}, TID_I)和认证散列值(G_{I-1}, G_I),以防止更新算法意外终止而造成 MTT 重复漫游认证的失败.

(2) RS 向 MTT 发送漫游应答消息. RS 执行下述步骤:

① 选取秘密随机数 $r_{\mathrm{R}}^{(I)} \in_C [2, n-1]$,并计算 $D_{\mathrm{R}}^{(I)} = (r_{\mathrm{R}}^{(I)} + KS_{\mathrm{R}})KP_{\mathrm{M}}$;

② 按式(12)计算与 MTT 间会密钥 $K_{(\mathrm{M,R})}^{(I)\prime}$;

$$K_{(\mathrm{M,R})}^{(I)\prime} = KS_{\mathrm{R}}^{-1}(r_{\mathrm{R}}^{(I)} + KS_{\mathrm{R}})D_{\mathrm{M}}^{(I)} \tag{12}$$

③ 发送应答消息给 MTT.

RS→MTT: $ENC(KP_{\mathrm{M}}, ENC(KS_{\mathrm{R}}, TID_{\mathrm{M}}^{(I)} \| ID_{\mathrm{H}} \| ID_{\mathrm{R}} \| D_{\mathrm{R}}^{(I)} \| T_{\mathrm{R}}^{(I)} \| Nonce^{(I)}))$.

MTT 验证 RS 漫游应答消息的合法性. MTT 执行以下步骤:

(1)根据加密消息验证 RS 是否是其议定的远程网络认证服务器,实现重复漫游认证过程中 MTT 和 RS 的双向身份认证.

(2)按式(13)计算与 RS 间的会密钥 $K_{(\mathrm{M,R})}^{(I)}$,完成重复漫游申请.

$$K_{(\mathrm{M,R})}^{(I)} = KS_{\mathrm{M}}^{-1}(r_{\mathrm{M}}^{(I)} + KS_{\mathrm{M}})D_{\mathrm{R}}^{(I)} \tag{13}$$

2.4 认证管理策略

本节介绍信息共享、信息注销和远程失效等认证管理策略.

2.4.1 信息共享

各认证服务器间基于安全协商的会话标识和密钥建立安全的通信链路,各网络认证服务器间基于安全通信链路进行漫游证明信息注销列表、公钥和身份证书等信息的共享.因此,在本文协议中 HS 与 RS 间的安全通信及信息共享机制,在确保 MTT 安全漫游的同时,并未增加协议的执行负载.

2.4.2 信息注销

MTT 注册本地网络时,获得 HS 签发的漫游证明信息 M_{MTT},此后,MTT 即可持漫游证明信息向 RS 申请重复漫游.

重复漫游过程中,MTT 可自行向 HS 注销其漫游证明信息 M_{MTT}.当漫游证明信息 M_{MTT} 遭泄漏或被攻击者获得时,MTT 可向 HS 申请注销 M_{MTT},根据注销申请,HS 更新漫游证明信息注销列表中的相关信息,并且 HS 与 RS 间的数据共享机制,可使 RS 获知 HS 最新的注销列表信息,因此可确保攻击者无法通过泄密信息 M_{MTT} 申请重复漫游.

2.4.3 远程失效

MTT 漫游进入远程网络后,若漫游证明信息 M_{MTT} 过期失效,此时,当 RS 收到 MTT 的服务申请时,通过查询 HS 的信息注销列表判断 M_{MTT} 是否已被注销,若 M_{MTT} 未被注销,即 M_{MTT} 未出现异常,则 RS 采用传统漫游机制,在 HS 的协助下完成 MTT 的身份合法性及平台可信性验证,并根据 HS 的验证结果制定相应的接入策略;否则拒绝 MTT 的漫游服务申请.

2.4.4 维护漫游认证列表

各网络认证服务器定时遍历其所维护的漫游认证列表,将已过期但重复漫游次数未达上限的重复漫游认证信息进行删除,提高漫游认证列表的遍历效率.

3 安全性证明

3.1 CK 安全模型

CK 安全模型中定义了理想模型 AM 和现实模型 UM[20-22]两种攻击模型.

理想模型 AM 表示认证的链路模型,在 AM 中攻击者是被动的,并且具有调用协议运行、查询会话密钥、暴露会话密钥、攻陷协议参与者以及测试会话密钥的能力,但是 AM 中攻击者只能忠实地传递同一消息 1 次,不能伪造、篡改或重放来自未被攻陷参与者的消息.

现实模型 UM 表示未认证的链路模型,在 UM 中攻击者除能够执行 AM 中的所有攻击外,还具有伪造、篡改和重放消息的能力,则在 UM 中攻击者能够控制协议事件的调度和通信链路,同时还能够通过攻击者具体的攻击手段获知协议参与者存储器中的秘密信息.

定义 1[21]. 设 Π 是运行在 AM 中的 n 方消息驱动协议,Π' 是运行在 UM 中的 n 方消息驱动协议.若对于任何 UM 敌手 U,始终存在一个 AM 敌手 A 使得两个协议的全局输出在计算上是不可区分的,则称协议 Π' 在 UM 中仿真了 AM 中的协议 Π.

定义 2[21]. 编译器 C 是一个算法,它的输入是协议的描述,输出也是协议的描述.若一个编译器 C 对于任何协议 Π,均有协议 $C(\Pi)$ 在 UM 中仿真 Π,则这个编辑器称为认证器.因此,AM 中的安全协议可由认证器转化为 UM 中的安全协议.

定义 3[21]. 会话密钥安全:若对于 AM 中的任何敌手 A,当且仅当下列性质都满足时,该协议在 AM 中是会话密钥安全的.

性质 1. 未被攻陷的参与双方完整执行协议后,参与者获得相同的会话密钥.

性质 2. 敌手 A 进行测试会话查询攻击,它猜中正确会话输出值 b 的概率不超过 $\frac{1}{2}+\Gamma$,其中 Γ 是安全参数范围内可忽略的任意小数.

定理 1[21]. 假设 λ 是一个消息传输认证器,即 λ 在 UM 中仿真了简单消息传输协议,假设 C_λ 是在 λ 的基础之上定义的一个编译器,则 C_λ 也是一个认证器.

3.2 AM 中的漫游协议

本文协议中,RS 依赖 MTT 持有的漫游证明信息鉴别 MTT 的身份合法性及平台可信性.为简化协议证明过程,漫游协议的两个阶段分别抽象描述为协议 δ 和 ε,其中 δ 为可信认证协议,ε 为安全漫游协议.分别证明 δ 和 ε 是 AM 中会话密钥安全的密钥交换协议.

协议 δ 描述如下:

(1) 注册请求.MTT 向 HS 发送注册请求消息,消息中包含相关的身份标识 $\{sid, ID_{\mathrm{M}}, ID_{\mathrm{R}}, ID_{\mathrm{H}}\}$.

(2) 注册响应消息.HS 收到 MTT 的注册请求

后，选取秘密随机数 $r_H \in_C [2, n-1]$，然后计算 $D_H=(r_H+KS_H)KP_M$. HS 选择随机数 S_H 后发送消息 $\{ENC(KS_H, sid \| ID_M \| ID_R \| ID_H \| D_H \| S_H \| T_H \| Nonce)\}$ 给 MTT.

(3) 可信性验证请求. MTT 收到 HS 的响应消息后，选取秘密随机数 $r_M \in_C [2, n-1]$，然后计算 $D_M=(r_M+KS_M)KP_H$；MTT 计算会话密钥 $K_{(M,H)}$，并生成平台可信性验证信息 TAI，最后发送消息 $\{ENC(KP_H, sid \| ID_M \| ID_H \| ID_R \| D_M \| Nonce \| T_M \| SIG_M \| E(K_{(M,H)}, TAI))\}$ 给 HS.

(4) 可信性验证响应. HS 首先验证 MTT 签名及其参数的正确性，实现对 MTT 的身份合法性验证，验证通过后，HS 基于终端的平台可信性验证策略对 MTT 平台的可信性进行验证；然后为身份合法且平台可信的 MTT 分配唯一的临时标识号 TID_M，并为其生成漫游证明信息 M_{MTT}；最后发送应答消息 $ENC(K_{(M,N)}, sid \| ID_M \| ID_H \| ID_R \| TID_M \| SIG_H \| T'_H \| C_H \| P_H)$ 给 MTT.

协议 ε 描述如下.

(1) 漫游请求. MTT 在可信认证协议阶段获得漫游证明信息 $M_{MTT}=C_R \| P_R$，MTT 选取秘密随机数 $r'_M \in_C [2, n-1]$，然后计算 $D'_M=(r'_M+KS_M)KP_R$；MTT 向 RS 发送漫游请求消息 $\{ENC(KP_R, sid \| TID_M \| ID_H \| D_R \| D'_M \| Nonce \| sid_{HR} \| M_{MTT} \| T_M)\}$.

(2) 漫游响应. RS 收到 MTT 的漫游申请后，首先验证消息及参数的正确性，通过漫游证明信息 M_{MTT} 的合法性完成对 MTT 身份合法性和平台可信性的验证，然后选取秘密随机数 $r_R \in_C [2, n-1]$，并计算 $D_R=(r_R+KS_R)KP_M$；最后发送漫游响应消息 $ENC(KP_H, ENC(KS_R, sid \| TID_M \| ID_H \| ID_R \| D_R \| Nonce \| T_R))$ 给 MTT.

(3) MTT 计算会话密钥 $K_{(M,R)}=KS_M^{-1}(r'_M+KS_M)D_R$，完成漫游申请.

定理 2.　当签名、非对称加密、对称加密等算法均安全且难解时，协议 δ 和协议 ε 在 AM 中是安全的.

证明.　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，MTT 和 HS 得到没有篡改的密钥协商参数 D_M 和 D_H，MTT 按式(1)计算的会话密钥：

$$\begin{aligned} K_{(M,H)} &= KS_M^{-1}(r_M+KS_M)D_H \\ &= KS_M^{-1}(r_M+KS_M)(r_H+KS_H)KP_M \\ &= (r_M+KS_M)(r_H+KS_H)Q. \end{aligned}$$

HS 按式(4)计算的会话密钥：

$$\begin{aligned} K'_{(M,H)} &= KS_H^{-1}(r_H+KS_H)D_M \\ &= KS_H^{-1}(r_H+KS_H)(r_M+KS_M)KP_H \\ &= (r_H+KS_H)(r_M+KS_M)Q. \end{aligned}$$

因 $K_{(M,H)}=K'_{(M,H)}$，因此协议 δ 满足会话密钥安全的性质 1.

命题.　敌手 A 能以概率 P_0 来区分会话密钥协商参数与一个随机数，非对称加密算法被攻破的概率上限为 P_{ENC}. 由于非对称加密等算法均安全且难解，则概率 P_0 和 P_{ENC} 都是可忽略.

在本文协议中，敌手 A 只能通过攻破 KP_H 和 KS_H 的加密数据得到 D_M 和 D_H，再对其进行相关运算得到会话密钥 $K_{(M,H)}$. 因 D_H 以 KS_H 加密传输，很容易被敌手 A 获得，因此攻击重点将在 D_M 上，A 只能通过攻破可信性验证请求消息获得随机数 D_M，则秘密随机数 D_M 被敌手 A 攻破的概率为 P_0P_{ENC}，则 D_M 不被攻破的概率为 $1-P_0P_{ENC}$.

若敌手 A 能够获知随机数 D_M，则必有 $1-P_0P_{ENC} \ll P_0P_{ENC}$（$P_0P_{ENC}$ 远远大于 $1-P_0P_{ENC}$）成立，即有 $P_0P_{ENC} \gg \frac{1}{2}$ 成立，所以 P_0 和 P_{ENC} 是不可忽略的，这与命题相矛盾. 因此敌手 A 正确猜中会话密钥 $K_{(M,H)}$ 的概率不超过 $\frac{1}{2}+\Gamma$，其中 Γ 是安全参数范围内可忽略的任意小数，则协议 δ 满足会话密钥安全的性质 2. 综上所述，协议 δ 在 AM 中是会话密钥安全的.

根据 AM 的定义可知，在 AM 中，由于敌手不能进行伪造、篡改和重放消息，因此敌手仅能真实地将合法参与者产生的消息转发，所以 MTT 和 HS 得到没有篡改的身份合法性及平台可信性验证信息，并安全协商了会话密钥 $K_{(M,H)}$ 和 $K'_{(M,H)}$，所以协议 δ 在 AM 中是安全的.

同理可证协议 ε 在 AM 中是安全的.　　证毕.

3.3　认证器构造

本文从 HS 认证 MTT、RS 认证 MTT 着手构造认证器.

对于可信认证协议中 MTT 与 HS 间的认证信息流采用基于时间戳的签名认证器 $\lambda_{SIG,T}$[23]. 文献[23]详细证明了认证器 $\lambda_{SIG,T}$ 的安全性和匿名性.

如图 4 所示，签名认证器 $\lambda_{SIG,T}$ 的具体交互过程

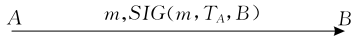


图 4　基于时间戳的签名认证器 $\lambda_{SIG,T}$

如下.

(1) A 产生时间戳 T_A,计算消息 m 的签名信息 $SIG(m,T_A,B)$,发送消息$\langle m,SIG(m,T_A,B)\rangle$给 B.

(2) B 收到 A 的请求消息后,首先验证时戳 T_A 的新鲜性,然后验证消息签名 $SIG(m,T_A,B)$的正确性,当且仅当时间戳 T_A 的新鲜性和签名信息 $SIG(m,T_A,B)$的正确性,验证均通过时,B 认为 A 发送的消息是合法的,即 B 完成对 A 的认证.

安全漫游时,RS 基于 MTT 持有的漫游证明信息 M_{MTT}完成对其身份合法性及平台可信性的验证.为满足 MTT 对身份等隐私信息的保护需求,故 MTT 的漫游申请消息须经过相应的处理,既不能包含 MTT 的真实身份信息,又能够使 RS 完成对 MTT 身份合法性及平台可信性的验证,因此,在安全漫游协议中使用基于身份的匿名认证器 $\lambda_{ENC,TID,T}$[22],在文献[22]中详细证明了认证器 $\lambda_{ENC,TID,T}$的安全性和匿名性.

如图 5 所示,匿名认证器 $\lambda_{ENC,TID,T}$的具体交互过程如下.

$$A \xrightarrow{TID_A,\ ENC(KP_B,\ m\|TID_A\|T_A)} B$$

图 5 基于身份的匿名认证器 $\lambda_{ENC,TID,T}$

(1) A 注册获得临时身份信息 TID_A,用 B 的公钥加密产生密文消息 $ENC(KP_B,m\parallel T_A\parallel TID_A)$,将临时身份 TID_A和密文消息 $ENC(KP_B,m\parallel T_A\parallel TID_A)$发送给 B.

(2) B 接收到消息后解密密文消息,首先验证 TID_A是否合法,然后检查时间戳 T_A的新鲜性.当且仅当身份 TID_A的合法性和时间戳 T_A的新鲜性验证均通过时,B 认为 A 发送的消息是合法的,即 A 通过了 B 的认证.

3.4 UM 中的协议

首先,将基于时间戳的签名认证器 $\lambda_{SIG,T}$和基于身份的匿名认证器 $\lambda_{ENC,TID,T}$应用于本文 AM 中的协议.然后,在对协议可证安全性不影响的前提下,隐藏 MTT 的身份标识信息,实现 MTT 身份标识的匿名性,使攻击者无法获得 MTT 真实有效的身份信息.最后,应用相关的优化方法将 UM 中的协议进行优化,得到 UM 中的相关协议.如图 6 所示为 UM 中的协议 δ 和协议 ε.

文献[24]对优化方法进行了详细介绍,并在 CK 模型下已证明该优化过程并不影响协议的安全性.

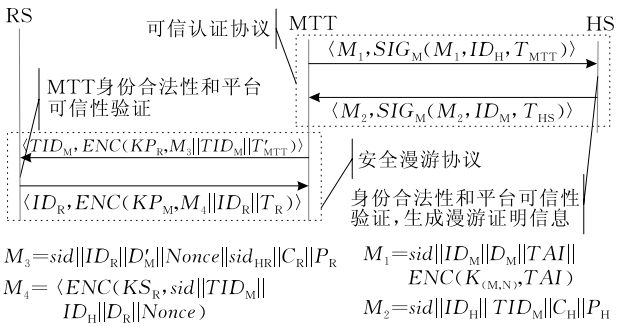


图 6 UM 中的协议 δ 和协议 ε

定理 3. 当签名算法、非对称加密算法、对称加密算法等安全且难解时,协议 δ 和协议 ε 在 UM 中是安全的,即本文协议是安全的漫游协议.

证明. 运用基于时间戳的签名认证器 $\lambda_{SIG,T}$和基于身份的匿名认证器 $\lambda_{ENC,TID,T}$把协议 δ 和协议 ε 直接转化为 UM 中会话密钥安全的可信接入协议和安全漫游协议.由于协议证明过程中所采用的签名认证器 $\lambda_{SIG,T}$和匿名认证器 $\lambda_{ENC,TID,T}$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 和协议 ε 是可证安全的. 证毕.

同理可证重复漫游认证协议是可证安全的.

4 模型分析

4.1 身份匿名性

4.1.1 首次漫游认证

在首次漫游认证时,由于漫游通信消息中 MTT 的真实身份 ID_M被其临时身份标识 TID_M所代替,即漫游通信消息中并未包含 MTT 的真实身份.因为仅有 HS 掌握秘密数 S_{MTT},所以漫游用户的真实身份 ID_M只有 HS 才能还原.本文匿名漫游协议中基于临时身份实现了用户身份匿名性的保护,确保了用户身份的机密性.同时在保证漫游认证用户身份匿名性的同时并未降低其安全性.

漫游证明信息(扩充后的 HS 身份证书)仅能报告其漫游申请者的身份是否合法、平台是否可信,并未包含 MTT 的配置信息及其身份等隐私信息,即漫游证明信息具有身份匿名性,而身份匿名性的强弱取决于有效授权时间的长短,越短则匿名性越强,同时其身份匿名性是可控的,可控性依赖于漫游证明信息持有者的临时身份标识,仅允许漫游证明信息的申请者持其与远程网络认证服务器 RS 建立漫游服务.

4.1.2 重复漫游认证

在重复漫游认证阶段,MTT 的真实身份 ID_M

被其临时身份标识 $TID_M^{(I)}$ 替代，并未出现 MTT 的任何真实身份信息；同时仅有身份合法且平台可信的 MTT 才能提供有效的 $TID_M^{(I)}$；并且仅用散列值作为 MTT 的身份合法性和平台可信性鉴别凭证，更不会泄露 MTT 的任何身份信息.

4.2　身份不可跟踪性

4.2.1　首次漫游认证

不同的 MTT 对应不同的 TID_M 且由互不相同的随机数 S_{MTT} 计算产生，并且任何合法 MTT 均无法通过自己的 TID_M 计算其他 MTT 的 ID 号，当同一 MTT 多次向 RS 申请漫游时，每次均使用不同的临时身份标识 TID_M，具有身份不可跟踪性.

MTT 将临时身份 TID_M 加密后传给 RS，即实现用户真实身份 ID_M 对 RS 的匿名性，又实现了对其临时身份的保护，增强临时身份的安全性；即便用户的临时身份 TID_M 遭泄露，攻击者也无法获知用户的真实身份，更无法将截获的临时身份与其他通信过程进行关联，无法实现对用户身份的监听. 即临时身份生成过程中随机参数的使用确保了漫游用户的身份信息具有不可关联性，因此攻击者将无法通过用户身份对漫游通信进行跟踪.

4.2.2　重复漫游认证

对于外部攻击者而言，在重复漫游认证阶段，虽然散列值间具有关联性，但是对散列值的加密传输，使攻击者无法获知散列值，因此外部攻击者无法对 MTT 的不同会话实施追踪攻击.

对于 RS 而言在重复漫游认证时，为减少计算负载和通信时延，采用散列值作为鉴别凭证，因此 RS 可将 MTT 的多次会话联系起来，所以若 MTT 需要完全无关联的漫游匿名认证时，则 MTT 重复进行首次漫游匿名认证过程，此时 RS 和外部攻击者都无法基于身份实现 MTT 不同会话的关联.

4.3　安全性分析

4.3.1　安全会话密钥协商

本文协议中，RS 在实现对 MTT 身份合法性和平台可信性验证的同时，完成与 MTT 间会话密钥 $K_{(M,R)}$ 的协商，会话密钥由双方选择的秘密随机参数 r_M 和 r_R 共同决定，任何一方都无法伪造合法的会话密钥 $K_{(M,R)}$，并且 r_M 和 r_R 的安全存储，保证了会话密钥的安全性；同时 r_M 和 r_R 的随机性，保证了会话密钥的新鲜性.

4.3.2　双向身份认证

本文协议实现了 MTT 和 RS 间双向的身份合法性认证. 首次漫游认证时，RS 通过漫游证明信息的合法性完成对 MTT 的身份合法性和平台可信性验证. 重复漫游认证阶段，RS 通过散列值 G_I 来鉴别 MTT，由于散列值基数 G_0 已通过 RS 的认证，根据散列函数的单向性计算特点，仅有已通过身份合法性及平台可信性验证的 MTT 拥有合法的 G_0，因此只有合法且可信的 MTT 才能出示正确、有效的 G_I.

同样 MTT 通过 RS 的私钥签名信息可确认其身份的合法性，验证 RS 是否是其议定的远程网络认证服务器.

4.3.3　抗伪造性

利用秘密随机数 S_{MTT} 和身份信息通过散列函数计算临时身份 TID_M，由 S_{MTT} 的机密性和散列函数的安全性保证 TID_M 的不可伪造性. 并且漫游通信消息中的随机数方便确认相关消息是否得到相应的回复，同时可防止攻击者进行重放攻击.

4.3.4　漫游证明信息的保密性

HS 运用其与 RS 间的共享密钥 $K_{(H,R)}$ 计算密钥 K_1 和 K_2，然后使用 K_1 和 K_2 封装平台可信性证明信息 C_R 和 P_R，$K_{(H,R)}$ 的私密性保证了漫游申请过程中证明信息 C_R 和 P_R 的安全性，除 RS 外其他任何认证服务器及用户都无法获知漫游证明信息.

4.3.5　抗攻击性

从抗中间人攻击和平台替换攻击分析协议的抗攻击性.

(1) 抗中间人攻击

假设 U 是主动的攻击者且知晓 MTT 与 HS 间会话密钥协商过程的所有公开参数及相关算法，U 对 MTT 的漫游过程进行中间人攻击.

如图 7 所示，MTT、HS 和攻击者 U 获得相关参数后分别计算相应的会话密钥：

MTT 计算的会话密钥(MTT 认为是其与 HS 间的会话密钥)：

$$\begin{aligned} K_{(M,H)} &= KS_M^{-1}(r_M + KS_M)D_{UU} \\ &= (r_M + KS_M)(r_{UU} + KS_U)Q. \end{aligned}$$

HS 计算的会话密钥(HS 认为是其与 MTT 间的会话密钥)：

$$\begin{aligned} K'_{(M,H)} &= KS_H^{-1}(r_H + KS_H)D_U \\ &= (r_U + KS_U)(r_H + KS_H)Q. \end{aligned}$$

攻击者 U 分别计算它与 MTT 和 HS 间的会话密钥 $K_{(U,H)}$ 和 $K_{(M,U)}$：

$$\begin{aligned} K_{(U,H)} &= KS_U^{-1}(r_U + KS_U)D_H \\ &= KS_U^{-1}(r_U + KS_U)(r_H + KS_H)PK_M, \\ K_{(M,U)} &= KS_U^{-1}(r_{UU} + KS_U)D_M \\ &= SK_U^{-1}(r_{UU} + KS_U)(r_M + SK_M)KP_H. \end{aligned}$$

因为 $K_{(M,H)} \neq K_{(M,U)}$ 和 $K'_{(M,H)} \neq K_{(U,H)}$，攻击者 U 无法对密钥协商过程进行中间人攻击，即使 U 通

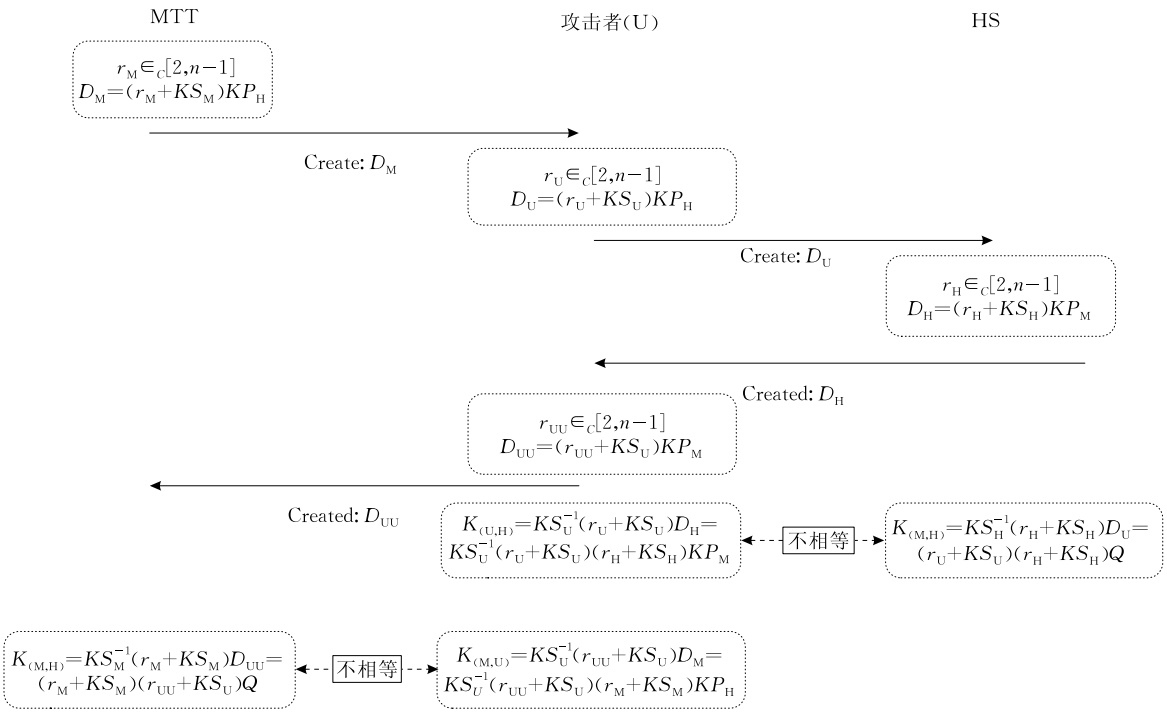


图 7 攻击者进行中间人攻击

过窃听获得密钥参数 D_H 和 D_M，但由于无法获知秘密参数 SK_M^{-1} 和 SK_H^{-1} 而导致无法完成会话密钥 $K_{(M,H)}$ 的窃取，即使 U 在攻击过程中使用相同的参数(即 $r_{UU}=r_U$)，上述结论依然成立.

MTT 与 HS 间会话密钥 $K_{(M,H)}$ 的安全性确保攻击者无法获知漫游证明信息，同时保证漫游证明信息申请过程的安全性.

(2)抗平台替换攻击

用户 A 和 B 都是合法用户，其中 PA 是可信平台，PB 为非可信平台，且 A 与 B、B 与 RS 间分别建立了安全信道. A、B 分别控制平台 PA 和 PB.

若用户 B 通过非法手段获得用户 A 的漫游证明信息 M_{MTT} 后，持 M_{MTT} 向 RS 申请漫游服务，因漫游证明信息 M_{MTT} 中封装了用户 A 的临时身份信息 TID_A，由于 B 无法提供正确的临时身份标识，导致其无法持 M_{MTT} 向 RS 证明其身份的合法性及平台的可信性.

在漫游证明过程中，通过临时身份标识将漫游证明信息与平台身份进行了绑定，因此外部攻击者无法对本文协议进行漫游证明信息的替换攻击. 文献[25]详细介绍了平台替换攻击的攻击过程.

4.4 性能分析

4.4.1 计算效率

在本文协议中，由于首次漫游认证过程中漫游证明信息具有一定的时效性，漫游认证时 MTT 已成功注册家乡网络，并申请获得漫游证明信息，所以 HS 不参与 MTT 的漫游认证，因此在表 1 运算开销比较中不包含注册阶段的计算开销. 同时由于传统加法和乘法等运算计算量较少，所以表 1 运算开销比较中未统计上述算法的计算开销.

本文协议中，首次漫游认证阶段 MTT 仅需进行 3 次非对称加密运算；RS 进行 2 次对称加解密运算和 3 次非对称加解密运算. 重复漫游认证阶段 MTT 仅需进行 2 次 Hash 运算和 3 次非对称加密运算；RS 只需进行 3 次非对称解密运算和 2 次 Hash 运算. 重复漫游认证过程 RS 对 MTT 身份合法性及平台可信性的验证步骤较少，在减少通信时延的同时可提高漫游认证的执行效率.

如表 1 所示为本文协议与其他相关方案[10-15]中各实体运算开销比较. 与对比方案[10-15]相比，本文协议中各参与者的计算负载较低，特别是减少了漫游认证过程中 RS 与 HS 间的消息交互轮数，即无需 HS 的协助，通过 1 轮消息交互 RS 就可完成对 MTT 的身份合法性及平台可信性验证，消息交互轮数的减少，降低了漫游协议的通信时延.

从表 1 数据来看，本文协议中 MTT 的计算量远小于文献[10-12,15]中相关方案的计算量，并延续了部分传统漫游认证协议[13-14]中 MTT 计算量小的优势，在本文协议中，RS 通过 1 轮消息交互即可完成对MTT的身份合法性和平台可信性验证，并且

表 1　漫游认证过程各实体的运算开销比较

运算	本文协议开销		文献中方案各实体的运算开销					
	首次	重复	文献[15]	文献[14]	文献[13]	文献[12]	文献[11]	文献[10]
Hash 运算(MTT/HS/RS)	0/0/2	2/0/2	☆	2/1/1	1/0/1	3/1/0	2/1/1	5/4/6
对称加解密(MTT/HS/RS)	0/0/2	0/0/0	2/4/2	1/1/0	0/0/1	1/1/1	2/1/1	2/0/2
非对称加解密(MTT/HS/RS)	3/0/3	3/0/3	3/3/2	1/1/2	2/2/1	2/1/1	0/3/3	0/1/1
异或运算(MTT/HS/RS)	☆	☆	☆	☆	1/0/1	☆	☆	☆
指数运算(MTT/HS/RS)	☆	☆	☆	☆	☆	☆	2/1/2	☆
MAC 次数(MTT/HS/RS)	☆	☆	☆	☆	1/0/0	☆	☆	2/2/2
信息交换次数(MTT-RS/RS-HS)	2/0	2/0	2/2	2/2	3/2	3/2	2/2	3/2

注：表中“☆”表示该方案未涉及此操作.

未使用计算量较大的指数运算. 因此本文协议在未增加 RS 计算负载的基础下，减少协议的消息交互轮数，降低了通信时延，提高了协议的执行效率.

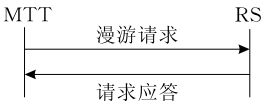
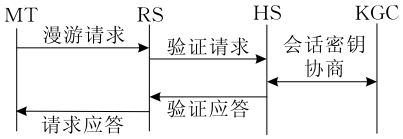
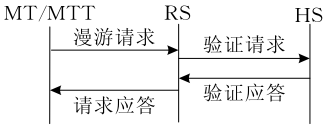
由于仅能在安全性与计算开销间寻求平衡，因此为了确保移动终端通信过程的安全性，本文协议使用了非对称加解密、对称加解密等运算量较大的算法. 但在实际应用中，可根据应用环境的特点减少通信消息的加密操作.

本文协议的漫游过程中，为保证通信消息的安全，RS 将应答消息经加密处理后发送给 MTT，若 RS 与 MTT 间基于安全链路通信时，RS 的应答消息则无需加密，此时 MTT 的只需执行 1 次非对称加密算法即可完成漫游，降低了 MTT 的计算负载，提高了协议的执行效率.

4.4.2　通信效率

表 2 所示为本文协议与其他相关方案[10-15]就通信时延和漫游特点等方面的比较结果，其中通信时延的大小以消息交互轮数为依据判断.

表 2　漫游通信时延比较

漫游通信模型		漫游特点	通信时延
本文协议		RS 通过 MTT 持有的漫游证明信息直接验证其身份的合法性及平台可信性.	小
文献[10]		RS 在 HS 的协助下完成对 MTT 身份合法性的验证，并且通过 KGC 完成会话密钥的协商.	大
文献[11-15]		RS 在 HS 的协助下完成对 MTT 身份合法性的验证.	较大

注：文献[10-14]中漫游用户为移动终端(MT)，本文方案和文献[15]中漫游用户为可信移动终端(MTT).

本文协议中，因 MTT 在向远程网络申请漫游前，已完成本地网络的注册工作，获得漫游证明信息，则 MTT 申请漫游时，无需 HS 的协助 RS 即可直接完成对 MTT 的合法性验证. 因此 MTT 与 RS 间通过 1 轮消息交互即可完成漫游申请，时延远远低于其他传统漫游[12-14]或跨域方案[10-11,15]，降低了漫游过程的通信负载和切换时延，提高了移动互联网漫游切换速度和漫游协议的执行效率，并且在重复漫游认证阶段实现 MTT 高效、快捷的安全漫游.

4.5　扩展性

如图 8 所示，本文协议的漫游认证原理可适用于 3G 网络环境下移动用户(Mobile User，MU)的网间漫游(区域性漫游和国际漫游)通信及资费服

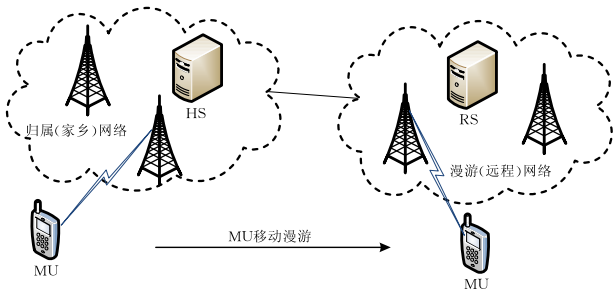


图 8　3G 网间的漫游模型

务，MU 持归属网络认证服务器 HS 签发的身份证明信息向漫游网络认证服务器 RS 申请漫游接入，RS 为 MU 提供服务且收取费用，若 MU 每漫游移动 1 次就缴费 1 次，将带来诸多不便，因此在 MU

漫游身份认证过程中,RS 基于本地网络的身份证明信息验证 MU 的合法性,并为其提供服务,RS 直接向 HS 收取 MU 的漫游服务费用,HS 再统一向 MU 收取,因漫游过程中 MU 持身份证明信息向 RS 证明其身份合法性及平台可信性.由于 MU 向 RS 提供的身份证明信息中包含签名、身份标识等信息,因此 MU 无法否认因漫游而产生的费用.

在 3G 网络中使用本文漫游原理,可降低 MU 漫游过程中由于身份验证、计费等造成的通信时延,提高 MU 的通信效率.

4.6 兼容性

本文漫游协议不仅可完成可信移动互联网下 MTT 的漫游认证工作,同时可在传统网络(非可信计算环境)中完成移动终端(Mobile Terminal,MT),的漫游服务请求.MT 的漫游请求消息中仅包含用户的身份合法性验证信息,即MT通过漫游证明信息向 RS 仅证明其身份的合法性.因此本文漫游协议具有强兼容性.

可信计算环境下,HS 通过身份验证信息和平台可信性验证信息,验证 MTT 身份的合法性和平台的可信性;而在传统非可信计算环境中,MT 仅发送身份验证信息,HS 只验证 MT 的身份合法性.MTT 和 MT 漫游通信请求的数据结构如图 9 所示.

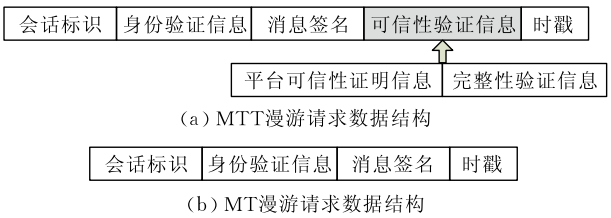


图 9 MTT 和 MT 的漫游请求数据结构

非可信计算环境中移动终端的具体通信过程如图 10 所示.

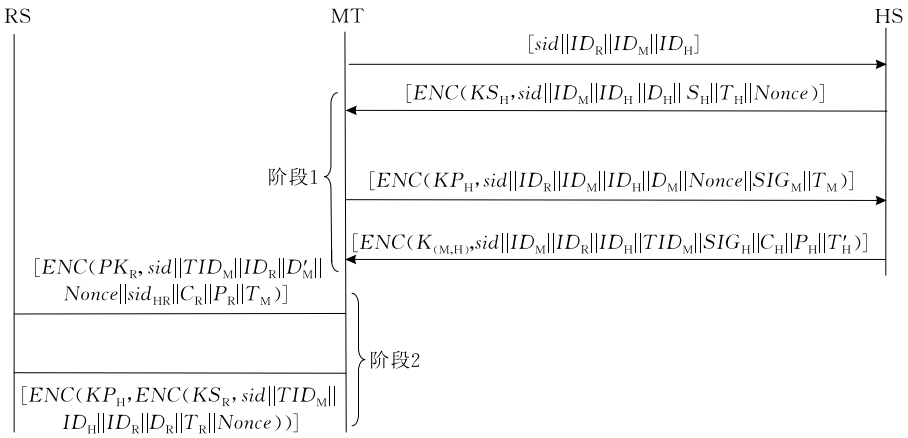


图 10 MT 漫游通信过程

其中,阶段 1 主要完成 MT 与 HS 的双向身份合法性验证,并且 HS 为身份合法的 MT 签发漫游认证信息;阶段 2 中 MT 生成漫游认证信息$\{C_R \parallel P_R\}$向 RS 申请漫游服务,RS 基于$\{C_R \parallel P_R\}$的合法性完成对 MT 的身份合法性验证,为身份合法的 MT 授权漫游接入服务.

5 结束语

传统漫游认证协议无法满足可信计算环境下移动可信终端漫游服务时的平台可信性认证需求,本文提出移动互联网可信匿名漫游协议.移动可信终端申请漫游服务时,远程网络认证服务器通过验证家乡网络认证服务器生成漫游证明信息的真实性及有效性,完成对移动可信终端的合法性验证.采用临时身份实现用户的匿名性保护,不仅使远程网络和攻击者无法获知用户的真实身份,而且保证了用户身份和位置等隐私信息的机密性;同时攻击者无法将截获的临时身份与已有的通信信息相关联,确保用户身份和位置等隐私信息的不可跟踪性,有效防止攻击者针对用户实施跟踪、窃听等攻击行为.本文协议在实现可信漫游的同时并未降低安全性,同时具有匿名性、扩展性等特点.下一步将在本文协议的基础上继续深入对轻量级漫游认证机制的研究,争取在满足匿名漫游认证安全性的基础上降低移动终端的计算负载.

致 谢 评审专家对稿件进行了细致审阅,各位编辑付出了辛勤劳动,在此表示感谢!

参 考 文 献

[1] Trusted Computing Group. TPM main part 1 design principles

specification version 1.2. https://www.Trustedcomputinggroup.org/, 2003

[2] Trusted Computing Group. TCG mobile trusted module specification version 1.0. https://www.Trusted computinggroup.org, 2007

[3] Zhu Jian-Ming, Ma Jian-Feng. An efficient authentication protocol with anonymity for wireless IP networks. Journal on Communications, 2004, 25(6): 12-18(in Chinese)
(朱建明，马建峰. 一种高效的具有用户匿名性的无线认证协议. 通信学报，2004，25(6)：12-18)

[4] Peng Hua-Xi, Feng Deng-Guo. Security flaws and improvement to a wireless authentication protocol with anonymity. Journal on Communications, 2006, 27(9): 78-85(in Chinese)
(彭华熹，冯登国. 匿名无线认证协议的匿名性缺陷和改进. 通信学报，2006，27(9)：78-85)

[5] Jiang Y X, Lin C, Shen X M. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569-2577

[6] Yang G M, Wong D S, Deng X T. Anonymous and authenticated key exchange for roaming networks. IEEE Transactions on Wireless Communications, 2007, 6(9): 1035-1042

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

[8] Shi M H, Rutagemwa H, Shen X M. A service-agent-based roaming architecture for WLAN/cellular integrated networks. IEEE Transactions on Vehicular Technology, 2007, 56(5): 3168-3181

[9] Jiang J, He C, Jiang L. On the design of provably secure identity-based authentication and key exchange protocol for heterogeneous wireless access//Proceedings of the International Conference on Communications, Networking and Mobile Computing. 2005: 972-981

[10] Peng Hua-Xi. An identity-based authentication model for multi-domain. Chinese Journal of Computers, 2006, 29(8): 1271-1281(in Chinese)
(彭华熹. 一种基于身份的多信任域认证模型. 计算机学报，2006，29(8)：1271-1281)

[11] Zhu Hui, Li Hui, Shu Wan-Li, Wang Yu-Min. ID-based wireless authen-tication scheme with anonymity. Journal on Communications, 2009, 30(4): 130-136(in Chinese)
(朱辉，李晖，苏万力，王育民. 基于身份的匿名无线认证方案. 通信学报，2009，30(4)：130-136)

[12] Hou Hui-Fang, Ji Xin-Sheng, Liu Guang-Qiang. Identity-based anonymity authentication protocol in the heterogeneous wireless network. Journal on Communications, 2011, 32(5): 153-161(in Chinese)
(侯惠芳，季新生，刘光强. 异构无线网络中基于标识的匿名认证协议. 通信学报，2011，32(5)：153-161)

[13] Hou Hui-Fang, Liu Guang-Qiang, Ji Xin-Sheng, et al. Provable ssecurity authentication scheme based on public key for heterogeneous wireless network. Journal of Electronics & Information Technology, 2009, 30(10): 2385-2391(in Chinese)
(侯惠芳，刘光强，季新生等. 基于公钥的可证明安全的异构无线网络认证方案. 电子与信息学报，2009，30(10)：2385-2391)

[14] Jiang Qi, Ma Jian-Feng, Li Guang-Song, et al. Identity-based roaming protocol with anonymity for heterogeneous wireless networks. Journal on Communications, 2010, 31(10): 138-145(in Chinese)
(姜奇，马建峰，李光松等. 基于身份的异构无线网络匿名漫游协议. 通信学报，2010，31(10)：138-145)

[15] Wu Zhen-Qiang, Zhou Yan-Wei, Qiao Zi-Rui. Access mechanism of TMP under mobile network. Journal on Communications, 2010, 31(10): 158-169(in Chinese)
(吴振强，周彦伟，乔子芮. 移动互联网下可信移动平台接入机制. 通信学报，2010，31(10)：158-169)

[16] Wu Zhen-Qiang, Zhou Yan-Wei, Qiao Zi-Rui. A controllable and trusted anonymous communication scheme. Chinese Journal of Computers, 2010, 33(9): 1686-1702(in Chinese)
(吴振强，周彦伟，乔子芮. 一种可控可信的匿名通信方案. 计算机学报，2010，33(9)：1686-1702)

[17] Li Jie, Wu Zhen-Qiang, Yu Lu, et al. An improved directed anonymous attestation scheme. Journal of Computer Applications, 2009, 29(2): 364-366, 397(in Chinese)
(李洁，吴振强，于璐等. 一种改进的直接匿名认证方案. 计算机应用，2009，29(2)：364-366，397)

[18] Zhou Yan-Wei, Wu Zhen-Qiang, Jiang Li. Cross-domain mechanism of anonymous attestation for distributed network. Journal of Computer Applications, 2010, 30(8): 2120-2124(in Chinese)
(周彦伟，吴振强，蒋李. 分布式网络环境下的跨域匿名认证机制. 计算机应用，2010，30(8)：2120-2124)

[19] Jiang Li, Wu Zhen-Qiang, Wang Hai-Yan, et al. Cross-domain authentication mechanism of DAA based on dynamic trust value. Journal of Computer Applications, 2010, 36(11): 156-158(in Chinese)
(蒋李，吴振强，王海燕等. 基于动态信任值的 DAA 跨域认证机制. 计算机工程，2010，36(11)：156-158)

[20] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols//Proceedings of the 30th ACM Symposium on Theory of Computing. Dallas, USA, 1998: 419-428

[21] Canerri R, Krawczyk H. Analysis of key exchange and their use for building secure channels//Proceedings of the Eurocrypt. 2001: 452-474

[22] Jiang Qi, Ma Jian-Feng, Li Guang-Song, et al. Security integration of WAPI based WLAN and 3G. Chinese Journal of Computers, 2010, 33(9): 1675-1685(in Chinese)
(姜奇，马建峰，李光松等. 基于 WAPI 的 WLAN 与 3G 网络安全融合. 计算机学报，2010，33(9)：1675-1685)

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

[24] Tin Y S T, Boyd C, Nieto J G. Provably secure key exchange: An engineering approach//Proceedings of the Australasian Information Security Workshop. Australasian. 2003: 97-104

[25] Ma Zhuo, Ma Jian-Feng, Li Xing-Hua, et al. Provable security model for trusted network connect protocol. Chinese Journal of Computers, 2011, 34(9): 1669-1678(in Chinese)
(马卓, 马建峰, 李兴华等. 可证明安全的可信网络连接协议模型. 计算机学报, 2011, 34(9): 1669-1678)

ZHOU Yan-Wei, born in 1986, Ph. D. candidate, engineer. His research interests include anonymous communication, wireless communication and cryptography.

YANG Bo, born in 1963, Ph. D., professor. His research interests include information security and cryptography.

ZHANG Wen-Zheng, born in 1966, professor. His research interest include information security.

Background

With the rapid development of wireless access technologies and mobile devices, the Mobile Internet becomes an emerging technology and is expected to grow up in an accelerated pace.

How to expand the range of movement by the roaming mechanism and ensure the smooth mobile data communication has become one of the research hotspot in Mobile Internet. So that, in recent years, a great number of researchers have paid more attention to the Mobile Internet and focused on issues from the mobile devices, roaming mechanism, access networks, services security and privacy protection. In the past few years, the authors also had some research achievements in Mobile Internet. Several research papers and two books have been published.

However, there still have a number of issues in Mobile Internet that are not addressed well, and many new challenges are raised now. Therefore, in this paper, we proposed a new roaming protocol of Mobile Trusted Terminal (MTT) in Mobile Internet, which could ensure the safety and anonymity of the MTT privacy information. Finally, the SK security of this protocol has been successfully proved by CK model. This protocol not only inherits the identity anonymity and non-tracking from traditional roaming protocol, but also has high security, anti-aggression and communication efficiency.

This research was supported by the National Natural Science Foundation of China under Grant Nos. 61272436, 61402275 and 61303092, Shaanxi Province Natural Science Basic Researched Plan under Grant No. 2014JQ8309. The NSFC projects were researched on the theory, application, roaming authentication technology, CK security and anonymous communication in trusted Mobile Internet. The team has published several research articles about anonymous communication, trusted computing, internet of things and cryptography, submitted three industry specifications for trusted digital home, and registered five computer software copyrights.