软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(9):2436−2450 [doi: 10.13328/j.cnki.jos.004712]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

物联网移动节点直接匿名漫游认证协议*

周彦伟[1,2,3], 杨 波[1,2,3]

[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](信息安全国家重点实验室(中国科学院 信息工程研究所), 北京 100093)

通讯作者: 杨波, E-mail: byang@snnu.edu.cn

摘 要: 无线网络下传统匿名漫游协议中远程域认证服务器无法直接完成对移动节点的身份合法性验证,必须在家乡域认证服务器的协助下才能完成,导致漫游通信时延较大,无法满足物联网感知子网的快速漫游需求.针对上述不足,提出可证安全的物联网移动节点直接匿名漫游认证协议,远程域认证服务器通过与移动节点间的 1 轮消息交互,可直接完成对移动节点的身份合法性验证.该协议在实现移动节点身份合法性验证的同时,具有更小的通信时延、良好的抗攻击能力和较高的执行效率.相较于传统匿名漫游协议而言,该协议快速漫游的特点更适用于物联网环境.安全性证明表明,该协议在 CK 安全模型下是可证安全的.

关键词: 物联网;匿名漫游;直接认证;CK 安全模型

中图法分类号: TP393

中文引用格式: 周彦伟,杨波.物联网移动节点直接匿名漫游认证协议.软件学报,2015,26(9):2436−2450. http://www.jos.org.cn/1000-9825/4712.htm

英文引用格式: Zhou YW, Yang B. Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things. Ruan Jian Xue Bao/Journal of Software, 2015,26(9):2436−2450 (in Chinese). http://www.jos.org.cn/1000-9825/4712.htm

Provable Secure Authentication Protocol with Direct Anonymity for Mobile Nodes Roaming Service in Internet of Things

ZHOU Yan-Wei[1,2,3], YANG Bo[1,2,3]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

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

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

Abstract: In the traditional anonymous roaming mechanism of wireless network, remote network authentication server (RS) can not directly authenticate the identity legitimacy of roaming mobile nodes. Thus, only with the aid of home domain authentication server (HS) can RS fulfill the authentication, which results in longer time delay in roaming communication and failure to meet the fast roaming needs of sensor subnets. To address the defects mentioned above, this paper proposes a direct anonymous authentication protocol with provable secure mobile nodes in Internet of things, enabling the mobile nodes to fulfill the legitimacy authentication of their identity through one round of message exchange with RS. The protocol proposed in this paper not only achieves the legitimacy authentication of anonymous identity, but also has shorter time delay and higher operating efficiency and good anti-attack capability. Fast roaming also makes it more

* 基金项目: 国家自然科学基金(61572303, 61272436, 61402275); 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); 保密通信重点实验室基金(No.9140C110206140C11050); 中央高校基本科研业务费专项基金(No.GK201504016); 陕西师范大学优秀博士论文项目(No.X2014YB01)

收稿时间: 2014-02-16; 修改时间: 2014-06-26; 定稿时间: 2014-08-02

suitable for the environment of Internet of things in comparison with the traditional anonymous roaming protocol. The security proof shows that the new protocol is provably secure in the CK security model.

Key words: Internet of things; anonymous roaming; direct authentication; CK security model

随着移动通信技术的发展,更多的用户期望得到随时随地的通信服务,促进了对无线网络环境下漫游认证协议的研究;同时,由于无线网络中网络带宽和终端的计算能力有限,因此对无线网络环境下的漫游认证协议提出了更高的设计要求,使得安全高效漫游认证协议的设计成为当前无线网络领域的研究热点.

文献[1−7]在对无线网络漫游需求的研究基础上,分别提出了相应的无线漫游认证协议,但上述方案的设计思路是:首先,根据不同的应用环境定义各自的漫游需求;然后,根据需求设计兼顾效率和安全性的漫游认证协议.文献[2−4]主要关注匿名性和不可追踪性;文献[5,6]重在实现漫游节点在远程域的本地认证,以避免 DOS 攻击;文献[6]还提出了基于动态群签名机制的本地化匿名安全漫游协议,以提供隐私保护功能;文献[7]在文献[6]的基础上提出了具有强不可追踪性的安全漫游协议,但该协议为实现不可追踪性,在重认证时具有较大的计算开销;上述协议[2−7]都是基于公钥加解密机制的,协议的运算量较大,无法满足无线网络对漫游认证协议的轻量级要求.

针对上述不足,研究者相继提出了无线网络下安全高效的漫游认证协议[8−17].文献[8]提出了无线网络下安全的匿名身份认证协议,但遗憾的是,文献[9]通过构造具体的攻击算法,证明了文献[8]中的方案易受到伪造攻击,在文献[8]方案的基础上,文献[9]提出了移动网络下安全的匿名漫游认证协议,但是文献[10]指出,文献[9]的方案在用户匿名性和保密性方面存在一定的缺陷;文献[11]提出一个无线环境下安全的匿名身份认证方案,分析发现,该方案无法提供匿名性[12],并且能够披露合法用户的隐私信息,未能达到完美的前向保密性[13];文献[14]提出了组合安全的无线漫游协议,该协议兼顾安全性和实际应用的可行性,实现了漫游的轻量级身份认证,保护了漫游节点的隐私,同时具有前向安全性,即,该协议是物联网环境下的轻量级匿名漫游认证协议;文献[15]提出一种无线 Mesh 网下的漫游认证协议,并基于串空间模型证明了该方案的安全性;文献[16]提出了移动网络下抗攻击的双向匿名密钥协商协议,并分析了该协议的身份匿名性和密钥协商公平性等安全属性;文献[17]提出了无线网络下抗攻击的匿名认证协议,该协议不仅可抵抗现有的攻击,而且具有较高的执行效率,可适用于电池供电的无线通信系统.

上述传统的无线网络匿名漫游认证协议[2−17]中,移动节点漫游时,由于远程访问域认证服务器并未掌握漫游节点的注册信息,因此,远程域认证服务器需在家乡域认证服务器的协助下完成对移动节点的身份合法性验证,即:远程域认证服务器将移动节点的漫游证明信息发给家乡域认证服务器,由家乡域认证服务器负责验证移动节点的身份合法性,远程域认证服务器根据家乡域认证服务器的验证反馈制定相应的决策.即:传统漫游认证协议中,往往需要 2 轮消息交互才能完成对移动节点的身份合法性验证.因此,传统匿名漫游认证协议的 2 轮消息交互模式具有较大的通信时延,无法满足无线网络环境对漫游机制的高效漫游需求.

近年来,随着物联网技术的兴起及发展,使得无线通信技术得到了广泛的应用.物联网是由感知子网、传输子网和应用子网组成的混合式异构网络,一方面,其感知子网由计算和通信能力极弱的、廉价的感知节点组成,往往使用移动节点和静态节点间合作的方式完成跨区域的信息采集及数据传输任务;另一方面,其传输骨干网依托互联网现有的固定基础设施,共享其强大的计算、传输及信息资源服务.

在物联网感知子网中,移动节点的漫游目标域通常是随机的,鉴于物联网的未来应用趋势,移动节点的漫游现象也必然是大量存在的,移动节点加入远程域,通过身份合法性验证后,可以任意获取远程域的一切网络资源,在实现移动节点漫游的同时,不能降低远程域及与之相关联的传输骨干网的安全性.因此,匿名漫游认证协议是物联网感知子网的关键技术之一.由于物联网感知子网的计算和通信能力有限,而传统漫游协议需要 2 轮消息交互,通信时延较大,那么如何在感知子网中确保安全高效快速漫游的同时完成对移动节点的身份合法性验证,则需设计适合物联网需求的安全高效快速漫游认证协议.

如图 1 所示,物联网移动节点漫游认证模型主要包括移动节点(mobile node,简称 MN)、节点家乡域认证服务器(home domain authentication server,简称 HS)和节点访问的远程域认证服务器(remote domain authentication

server,简称 RS)组成,同时还包括物联网管理中心 CA-IoT.在物联网感知子网中,认证服务器即为该区域的基站,在实现对节点认证管理的同时,基站也充当了感知子网和传输骨干网的接入网关节点[14].在图 1 中,对于给定的移动节点 *MN* 而言,家乡域认证服务器即为区域 *A* 的认证服务器(HS_A),远程域认证服务器则为区域 *B* 和区域 *C* 的认证服务器(即 RS_B 和 RS_C).为了方便协议的描述和协议间的性能比较,下文描述物联网下移动节点的直接匿名漫游认证协议时,将基站统称为认证服务器.

物联网感知子网中移动节点的漫游过程如图 1 所示,移动节点 *MN* 从初始区域 *A* 进入区域 *B* 进行数据采集,并和区域 *B* 内的静态节点合作,将数据传送给区域 *B* 的认证服务器 RS_B,由 RS_B 通过传输骨干网发送到目标节点;当区域 *B* 中的数据采集完成后,节点 *MN* 从区域 *B* 进入区域 *C* 进行采集.显然,*MN* 若想与区域 *B* 或区域 *C* 内的节点协作完成相关信息数据的采集及传输任务,首先,*MN* 需要通过认证服务器 RS_B 和 RS_C 的安全性检测,即,RS_B 和 RS_C 需对 *MN* 的身份合法性进行验证.

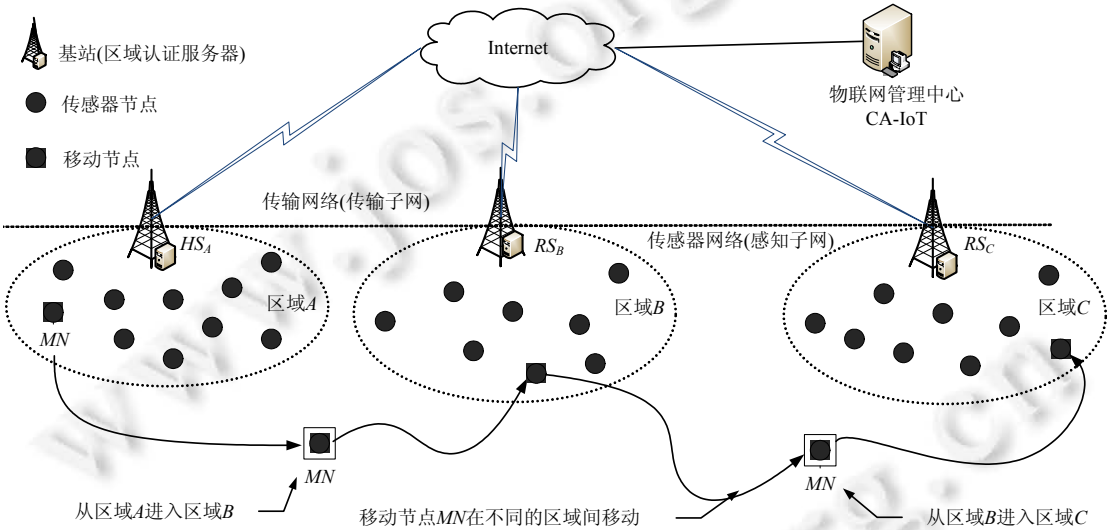


Fig.1 Roaming authentication model of mobile nodes in Internet of things

图 1 物联网移动节点漫游认证模型

由于物联网感知子网中节点性能的限制,物联网移动节点的匿名漫游机制除了保证移动节点身份匿名性和不可追踪性的同时,还需兼顾以下两个方面:① 感知子网中,无论移动节点还是静态节点都是资源极端受限的,因此应尽量减轻漫游认证协议参与方的计算量,特别是移动节点的计算量;② 由于物联网感知子网的带宽相对较低,信道出错率较高,在降低消息长度的同时,应减少协议的交互轮数,以削减身份认证过程的通信时延,实现物联网下移动节点的快速漫游需求.

针对上述问题,本文以物联网感知子网为应用环境,设计安全高效的物联网移动节点直接匿名漫游认证协议.在该协议中,当 *MN* 成功注册时,将获得家乡域认证服务器签发的注册信息;*MN* 可基于注册信息生成漫游证明信息,远程域认证服务器基于漫游证明信息的合法性对 *MN* 的身份合法性进行验证,同时保证了 *MN* 隐私信息的安全性;漫游过程仅需 1 轮消息交互,减少了匿名漫游认证协议的消息交互轮数,降低了通信时延,并提高了协议的执行效率;在 CK 安全模型下,证明本文协议是可证明安全的;相较与无线网络下现有的匿名漫游认证协议[14–17],本文协议的通信时延更小,其快速漫游的特点更加适用于物联网环境.

1 基础知识

1.1 安全性假设

定义 1(computational Diffie-Hellman(CDH)问题). 令 $q(q>2^k,k$ 为安全参数)是大素数,循环群 *G* 的阶为 *q*,*P*

是群 G 的生成元;给定 $P,aP,bP\in G$,对于任意且未知的 $a,b\in Z_q^*$,CDH 困难问题的目标是计算 abP.

CDH 假设. 定义概率多项式时间算法$\mathcal{A}$解决 CDH 问题的优势为 $Adv^{CDH}(\mathcal{A})=\Pr[\mathcal{A}(P,aP,bP)=abP]$.对于任意的多项式时间算法$\mathcal{A}$,优势 $Adv^{CDH}(\mathcal{A})$都是可忽略的,则称之为满足 CDH 假设.

定义 2(离散对数(discrete logarithm,简称 DL)问题). 令 $q(q>2^k,k$ 为安全参数)是大素数,循环群 G 的阶为 q,P 是群 G 的生成元;给定 $P,aP\in G$,对于任意且未知的 $a\in Z_q^*$,DL 困难问题的目标是计算 a.

DL 假设. 定义概率多项式时间算法$\mathcal{A}$解决 DL 问题的优势为 $Adv^{DL}(\mathcal{A})=\Pr[\mathcal{A}(P,aP)=a]$.对于任意的多项式时间算法$\mathcal{A}$,优势 $Adv^{DL}(\mathcal{A})$都是可忽略的,则称之为满足 DL 假设.

1.2 双线性映射

定义 3. 设群 G_1 和 G_2 是阶为素数 q 的循环群.当映射 $e:G_1\times G_1\to G_2$ 满足下列性质时,称其为双线性映射:

(1) 双线性:$e(aP,bQ)=e(P,Q)^{ab}$;对于 $P,Q\in G_1, a,b\in Z_q^*$ 均成立;

(2) 非退化性:存在 $P,Q\in G_1$,使得 $e(P,Q)\neq 1$,其中,1 为 G_2 的单位元;

(3) 可计算性:对于任意的 $P,Q\in G_1$,可在多项式时间内完成 $e(P,Q)$的计算.

1.3 CK安全模型

CK 安全模型[18−20]中定义了理想模型 AM 和现实模型 UM 两种攻击模型.

1) 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、暴漏会话密钥、攻陷协议参与者以及测试会话密钥的能力;但在 AM 中,攻击者只能忠实地传递同一消息一次,不能伪造、篡改或重放来自未被攻陷参与者的消息;

2) 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[18,19].

定义 4[20]. 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$\mathcal{Q}$,始终存在一个 AM 敌手$\mathcal{Q}$,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 5[20]. 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 6(会话密钥安全)[20]. 若对于 AM 中的任意敌手$\mathcal{A}$,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,即,协商了相同的会话密钥.

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

定理 1[20]. 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的基础之上定义的编译器,则 C_λ也是一个认证器.

2 物联网移动节点直接匿名漫游认证协议

针对传统匿名漫游认证协议存在远程域认证服务器无法直接完成对移动节点的身份合法性验证和漫游通信时延较大的不足,本文提出可证安全的物联网移动节点直接匿名漫游认证协议.为方便本文协议的介绍,首先在第 2.1 节和第 2.2 节简述网络认证服务器的初始化及移动节点的家乡域注册过程;然后,在第 2.3 节对移动节点的直接匿名漫游过程进行详细介绍.

如图 1 所示:注册阶段,移动节点 MN 向家乡域认证服务器 HS 申请注册,获得由 HS 签发的注册信息;漫游阶

段,*MN* 基于注册信息生成漫游证明信息,远程域认证服务器 *RS* 基于漫游证明信息直接完成对 *MN* 的身份合法性验证,并且完成会话密钥的安全协商.

本文可证安全的物联网移动节点直接匿名漫游认证协议的安全性基于下述假设:

假设 1. 各区域认证服务器均安全可信,既不会发送虚假信息,也不会利用已掌握的用户信息实施假冒攻击,更不会随意揭示用户的真实身份;同时,认证服务器均安全保存私钥,避免密钥泄露事件的发生.

假设 2. 各网络认证服务器间的时间同步机制可保证消息时间戳的新鲜性及同步性.

2.1 系统初始化

系统建立过程的主要操作有:

(1) 各区域认证服务器向管理中心 CA-IoT 注册,由 CA-IoT 管理各认证服务器的安全性及相关事宜;

(2) CA-IoT 选取满足条件的 q(q 为大素数,且 $q>2^k$,k 为安全参数)阶加法循环群 G_1 和乘法循环群 G_2,G_1 的一个生成元为 P:

- 定义群 G_1 和 G_2 上的双线性映射 e:$G_1\times G_1\to G_2$;
- 定义抗碰撞的单向哈希函数:

  $H:G_1\times Z_q^*\to Z_q^*, H_1:\{0,1\}^*\times G_1\times Z_q^*\to Z_q^*, H_2:\{0,1\}^*\times Z_q^*\to Z_q^*, H_3:\{0,1\}^*\times Z_q^*\to\{0,1\}^*$;
- 定义非对称密钥加/解密算法 *Enc*()和 *Dec*();
- 并向各认证服务器发布基础参数 *Params*={G_1,G_2,e,q,P,H,H_1,H_2,H_3,*Enc*,*Dec*};

(3) 各区域认证服务器分别产生本区域的主密钥和公开钥,妥善保管主密钥,并公开相应的系统参数.

如:*HS* 选取随机数 $S_H\in Z_q^*$ 作为 *HS* 的主密钥,则其公钥为 $PK_H=S_HP$,*HS* 秘密保存主密钥 S_H,公开系统参数{G_1,G_2,e,q,P,PK_H,H,H_1,H_2,H_3,*Enc*,*Dec*};*RS* 选取随机数 $S_R\in Z_q^*$ 作为 *RS* 的主密钥,则其公钥为 $PK_R=S_RP$,*RS* 秘密保存主密钥 S_R,公开系统参数{G_1,G_2,e,q,P,PK_R,H,H_1,H_2,H_3,*Enc*,*Dec*}.

2.2 节点注册本地服务域

节点注册阶段主要完成节点的家乡域注册,使节点获得家乡域认证服务器 *HS* 签发的注册信息.

(1) *MN*选取随机秘密数 $n,r_1\in Z_q^*$,利用身份标识ID_M产生注册秘密信息$S_M=H_2(ID_M,n)$,计算$R_M=r_1P$.*MN*产生时戳T_M,并将消息$Enc(PK_H,ID_M||S_M||R_M||T_M)$通过安全信道发送给*HS*;

(2) 收到 *MN* 的注册请求后,*HS* 验证 *MN* 的身份合法性,并为 *MN* 生成注册授权信息:

① 随机选取秘密数 $r_2\in Z_q^*$,计算 $R=R_M+r_2P$ 和 $L=r_2+S_HC$(其中,$C=H_1(ID_M,R,S_M)$),则 *HS* 为 *MN* 生成的注册授权信息为(L,R);

② 随机选取秘密数 $r\in Z_q^*$,为 *MN* 计算临时身份 $TID_M=H_3(ID_M,r)$,则 *MN* 的身份认证凭证为

$$AUTHEN=Enc(S_H,ID_H||TID_M||T_S||T_E),$$

其中,S_H 为 *HS* 的私钥,T_S 为身份凭证的起始时间,T_E 为身份凭证的结束时间,则 T_E-T_S 为身份凭证的有效时长;

③ 生成消息时戳 T_H,并通过安全信道将注册授权信息发送给 *MN*,同时,*HS* 在相应的数据库中为 *MN* 建立注册信息;

(3) *MN* 收到 *HS* 的应答消息后,首先用 *HS* 的公钥 PK_H 解密消息,验证应答消息是由其合法家乡域认证服务器 *HS* 所发;然后,通过等式 $LP+R_M=R+PK_HC$(其中,$C=H_1(ID_M,R,S_M)$)验证授权信息(L,R)的正确性.若该等式成立,则注册授权信息的合法性验证通过,*MN* 计算 $T=r_1+L$,则元组(T,R,C,*AUTHEN*)(其中,$C=H_1(ID_M,R,S_M)$)即为 *HS* 为 *MN* 基于秘密信息 S_M 签发的注册信息,*MN* 安全保存(T,R,C,*AUTHEN*),并及时销毁秘密信息 S_M,r_1 和 *HS* 签发的部分注册授权信息 L,使其不对外泄漏;同时,*MN* 从身份凭证 *AUTHEN* 中可获得 *HS* 为其生成的临时身份信息 TID_M,可验证该临时身份信息是否与接收到的临时身份信息相同;同时,可获知身份认证凭证的有效授权时间.

2.3 直接匿名漫游认证

如图 2 所示,在漫游阶段,*MN* 基于注册信息生成漫游证明信息,远程域认证服务器基于漫游证明信息直接完成对 *MN* 的身份合法性验证,并且完成会话密钥的安全协商.

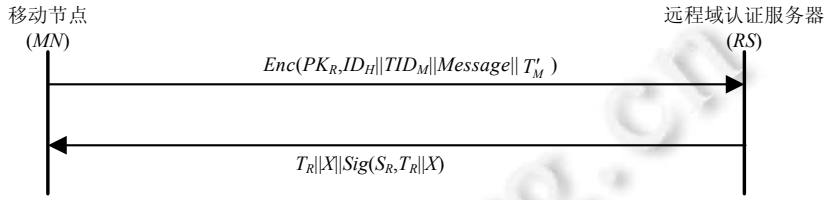


Fig.2 Direct anonymous roaming authentication protocol

图 2 随机的匿名漫游协议

(1) *MN* 基于注册信息生成匿名漫游证明信息,并发送给 *RS*;

① *MN* 随机选取秘密数 $s, y \in Z_q^*$,计算 $U_M=sR, V_M=sCP, W_M=sTP, Y=yP$ 和 $M_M=yH(Y,0)+sT$;*MN* 基于注册信息生成的漫游证明信息为 $Message=(AUTHEN,U_M,V_M,W_M,Y,M_M)$,其中,$(U_M,V_M,W_M)$为 *MN* 身份合法性证明信息;$Y$ 为会话密钥协商参数;M_M 为密钥协商参数的正确性验证信息;*AUTHEN* 是 *HS* 为 *MN* 生成的身份认证凭证;

② *MN* 读取时间戳 T'_M 后,发送消息 $Enc(PK_R, ID_H \| TID_M \| Message \| T'_M)$ 给 *RS*,漫游申请消息的加密传输保证了 *MN* 临时身份标识 TID_M 的安全性,因为该消息仅有其议定的远程域认证服务器 *RS* 才能解密.

(2) *RS* 基于 *MN* 的漫游证明消息完成对 *MN* 的身份合法性验证:

① *RS* 用私钥 S_R 解密消息,并检查时戳的新鲜性,用 *HS* 的公钥 PK_H 解密 *AUTHEN* 即可获知 *HS* 和 *MN* 的相关身份信息(记为 ID_H^* 和 TID_M^*),验证等式 $ID_H^* = ID_H$ 和 $TID_M^* = TID_M$ 是否成立:若不成立,则终止验证;否则,*RS* 基于 *AUTHEN* 验证 *Message* 在当前时间是否有效,若 *AUTHEN* 在当前时间已过期,则终止验证.

② *RS* 验证漫游证明信息 *Message* 的正确性:当且仅当等式 $e(W_M-U_M,P)=e(V_M,PK_H)$和 $M_MP=H(Y,0)Y+W_M$ 都成立时,消息 *Message* 是正确的.此时,*RS* 完成了对 *MN* 的身份合法性验证,即,*RS* 认为 *MN* 是其家乡域认证服务器 *HS* 上注册的合法节点.

③ *RS* 计算与 *MN* 间的会话密钥:*RS* 随机选取秘密数 $x \in Z_q^*$,计算 $X=xP$,则 *RS* 与 *MN* 间的会话密钥为 $K_{R\text{-}M}=H(xY,1)=H(xyP,1)$.

④ *RS* 读取当前时间戳 T_R,并生成签名 $Sig(S_R,T_R||X)$,发送消息$\{T_R||X||Sig(S_R,T_R||X)\}$给 *MN*.在物联网感知子网中,移动节点需漫游进入多个远程域进行数据收集,本文协议中,由于漫游证明信息 *Message* 中不包含访问域的相关信息(即,访问域是随机选取的),因此在 *AUTHEN* 的有效期内,*MN* 可重复使用 *Message*.即:*Message* 生成后,*MN* 可持其向多个域的认证服务器证明其身份的合法性.如在图 1 中,当 *MN* 从区域 *A* 漫游进入区域 *B* 时,RS_B 基于 *Message* 可验证 *MN* 的身份合法性;*MN* 从区域 *B* 直接漫游进入区域 *C* 后,RS_C 同样可基于 *Message* 验证 *MN* 的身份合法性;

(3) *MN* 计算与 *RS* 间的会话密钥,并验证 *RS* 的身份合法性:

① *MN* 基于签名信息 $Sig(S_R,T_R||X)$验证 *RS* 的身份合法性,并检查时戳 T_R 的新鲜性.即,*MN* 确认 *RS* 是否是其议定的远程域认证服务器,实现 *MN* 与远程域认证服务器 *RS* 间的双向身份认证;

② *MN* 计算与 *RS* 间的会话密钥 $K_{M\text{-}R}=H(yX,1)=H(xyP,1)$,则 *MN* 与 *RS* 间协商了相同的会话密钥.

2.4 正确性

本节对协议中注册授权信息合法性验证和漫游证明信息合法性验证的正确性进行分析.

定理 2. *MN* 能够验证注册授权信息的合法性.

证明:由于等式 $LP+R_M=(r_2+S_HC)P+R_M=r_2P+S_HPC+R_M=R+PK_HC$ 成立,则注册授权信息(L,R)满足上述等式时,*MN* 可知 *HS* 为其生成了合法的注册授权信息. □

定理 3. *RS* 能够基于漫游证明信息 *Message* 验证 *MN* 的身份合法性.

证明:由于等式 $e(W_M-U_M,P)=e(s(r_1+r_2+S_HC)P-s(r_1+r_2)P,P)=e(sCP,S_HP)=e(V_M,PK_H)$和 $M_MP=yPH(Y,0)+sTP=H(Y,0)Y+W_M$ 成立,则解密身份认证凭证 *AUTHEN*,根据当前时间判断身份认证凭证 *AUTHEN* 的有效性,可实现漫游证明信息 *Message* 的有效性判断.因此,若 *Message* 同时满足上述等式且 *AUTHEN* 在当前时间有效,则 *RS* 认为 *MN* 是其家乡域认证服务器 *HS* 授权的合法移动节点. □

3 协议安全性分析及特点

3.1 安全性分析

3.1.1 双向身份认证

匿名漫游认证阶段,*RS* 通过 *HS* 授权的漫游证明信息确定 *MN* 身份的合法性,即,*RS* 通过漫游证明信息的合法性完成对 *MN* 的身份合法性鉴别,当 *MN* 持合法证明信息进行漫游时,*RS* 就认为 *MN* 是 *HS* 认证的合法移动节点;*MN* 根据 *RS* 的签名信息验证应答消息是否是其议定的远程域认证服务器所发送,完成对 *RS* 身份的合法性验证;并且在协议交互过程中随机数的使用保证了消息的新鲜性.

3.1.2 会话密钥的安全协商

RS 与 *MN* 完成双向身份合法性认证的同时,完成会话密钥的安全协商,会话密钥由双方选取的随机秘密数 x 和 y 所决定,因此任何一方都无法伪造合法的会话密钥;同时,对随机秘密数 x 和 y 的安全存储,保证了会话密钥的安全性;并且,秘密数的随机性保证了协商会话密钥的新鲜性;即使为了实现快速漫游,*MN* 使用同一漫游证明信息 *Message* 向多个远程域申请漫游,由于远程域认证服务器产生的随机秘密数互不相同,因此,*MN* 与各远程域协商的会话密钥各不相同.

若外部攻击者捕获了 *RS* 和 *MN* 的密钥协商参数 $X=xP$ 和 $Y=yP$,若通过 X 和 Y 计算会话密钥 $K=H(xyP,1)$,则其将面临求解 CDH 困难问题,因此,攻击者无法通过密钥协商参数完成对会话密钥的攻击;*RS* 或 *MN* 预想通过密钥协商参数 X 和 Y 计算对方的随机秘密数 x 和 y,则其将面临求解 DL 困难问题,因此,*RS* 和 *MN* 也无法获知对方的随机秘密数.

3.1.3 前/后向安全性

由于 *MN* 和 *RS* 每次使用不同的随机秘密数进行会话密钥的协商,即,会话密钥分别由互不相同的随机秘密数生成,随机秘密数的强新鲜性保证了当 *MN* 漫游过程中某次密钥协商参数的泄露,并不会对已有和即将协商的会话密钥的安全性造成威胁,即,本文协议中会话密钥具有完美的前后向安全性.

3.1.4 抗攻击性

(1) 抗伪造攻击

RS 通过等式 $e(W_M-U_M,P)=e(V_M,PK_H)$和 $M_MP=H(Y,0)Y+W_M$ 验证 *MN* 漫游证明信息 *Message* 的合法性,由于通过等式 $e(W_M-U_M,P)=e(V_M,PK_H)$,*RS* 可确认 W_M 中含有 *HS* 的系统主密钥 S_H,因此,W_M 是无法伪造的;若对 U_M 和 V_M 进行了伪造,由于伪造信息无法与 W_M 间形成对应关系,因此等式 $e(W_M-U_M,P)=e(V_M,PK_H)$不成立;Y 和 M_M 同样是无法伪造的,若进行了伪造,则无法通过等式 $M_MP=H(Y,0)Y+W_M$ 的验证.因此,由于敌手无法获知 *HS* 的主密钥 S_H,所以敌手的任意伪造都无法通过认证服务器的合法性验证.

(2) 抗中间人攻击

由于 *Enc* 是语义安全的,攻击者无法通过 *MN* 的漫游申请消息 $Enc(PK_R,ID_H||TID_M||Message)$获知 *MN* 的漫

游证明信息 *Message*;若攻击者使用伪造的漫游证明信息 *Message′*向远程域认证服务器 *RS* 申请漫游,由于伪造信息 *Message′*的合法性无法通过 *RS* 的验证,协议将终止执行,则攻击者无法对本文协议进行中间人攻击.

(3) 抗重放攻击

会话密钥的安全协商和秘密保存以及消息交互过程中随机数和消息时戳的使用,都具有阻止敌手进行重放攻击的能力;同时,*RS* 与 *MN* 间的双向身份认证同样能够抵抗敌手的重放攻击.

(4) 抗替换攻击

本文协议中,移动节点 *MN* 基于身份标识生成漫游证明信息 *Message*;同时,身份认证凭证 *AUTHEN* 中同样包含 *MN* 的身份信息.由于攻击者无法提供正确的身份标识,所以攻击者无法使用合法 *MN* 的漫游证明信息进行漫游申请,即,认证信息与身份间具有一一对应关系.

3.1.5 身份匿名性

(1) 匿名性描述

匿名漫游认证过程中,*MN* 使用 *Message* 作为身份合法性鉴别凭证,由于漫游证明信息中不包含 *MN* 的真实身份等隐私信息,并且经过了随机数的随机化处理,即,不同节点的漫游证明信息分别由互不相等的随机数产生,保证了 *MN* 漫游过程的匿名性,则 *RS* 和攻击者均无法确定 *MN* 的真实身份信息.

不同的 *MN* 对应不同的临时身份标识 TID_M,且由互不相同的随机参数计算产生,同时,任意合法的 *MN* 均无法通过自己的 TID_M 计算其他 *MN* 的身份标识.*MN* 将 TID_M 加密后传给 *RS*,在实现用户真实身份 ID_M 对 *RS* 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.

特别地,本文为实现用户漫游过程的高效性,注册家乡域时,*HS* 基于 *MN* 的真实身份为其产生临时身份标识 TID_M,并将其封装在身份认证凭证 *AUTHEN* 中.对于 *RS* 而言,无法获知 *MN* 的真实身份.可当 *MN* 向同一 *RS* 多次申请漫游时,*RS* 可将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 *MN* 追求漫游过程的强匿名性,则 *MN* 每次漫游之前向 *HS* 申请凭证 *AUTHEN*,保证 *MN* 每次漫游时所持有的临时身份标识各不相同,确保 *MN* 具有强匿名性和不可追踪性.

(2) 匿名性证明

根据文献[4]中关于匿名性的游戏设计,定义下述游戏,其中:集合 $J_M(L)$是移动节点集合,且 $MN\in J_M(L)$;$J_R(L)$为认证服务器集合,且 $RS\in J_R(L)$;集合的长度都均为 *L*.在游戏中,仿真器 *S* 将敌手 $\mathcal{A}$作为子程序运行.

① 仿真器 *S* 建立系统,参与者为 *MN* 和 *RS*;同时,*S* 运行敌手 $\mathcal{A}$,并回答 $\mathcal{A}$的所有询问;

② $\mathcal{A}$可以激活系统中的任意参与者和询问,从而在这些参与者之上运行协议;

③ $\mathcal{A}$从集合 $J_M(L)$中随机选择 $MN_i(0\leqslant i\leqslant L)$和 $MN_j(0\leqslant j\leqslant L)$,从集合 $J_R(L)$中选择 *RS*,则有 $MN_i,MN_j\in J_M(L)$和 $RS\in J_R(L)$;将 MN_i,MN_j 和 *RS* 作为协议的参与者;

④ $\mathcal{A}$向 S 发送测试询问,输入为(MN_i,MN_j,RS);

⑤ *S* 仿真匿名漫游认证协议的两个完整运行过程:一个参与方是 MN_i 和 *RS*,另一个参与方是 MN_j 和 *RS*;同时,*S* 更新每个参与方的状态信息.*S* 随机选取 $b\leftarrow\{0,1\}$:若 $b=0$,则返回关于 MN_i 的仿真信息;否则,返回关于 MN_j 的仿真信息;

⑥ 收到测试询问的响应后,$\mathcal{A}$可以继续发起所有允许的攻击,以激活参与者运行协议;

⑦ $\mathcal{A}$输出对 *b* 的猜测 *b′*,运行终止.

在上述游戏中,如果参与者 MN_i,MN_j 和 *RS* 均未被攻陷,且 $\mathcal{A}$输出正确的猜测 $b'=b$,则称 $\mathcal{A}$赢得游戏. 定义 $\mathcal{A}$赢得上述游戏的优势为 $Adv^{\Pi}(\mathcal{A})=\left|\Pr[b'=b]-\frac{1}{2}\right|$.

定理 4. 若函数 $H_2()$是抗碰撞的单向哈希函数,则优势 $Adv^{\Pi}(\mathcal{A})$是可忽略的.

证明:若本文匿名漫游认证协议不满足匿名性,即,有敌手 $\mathcal{A}$能够以不可忽略的优势 $Adv^{\Pi}(\mathcal{A})$在上述游戏中获胜,则可以构造算法 $\mathcal{B}$,能够以不可忽略的优势攻破抗碰撞的单向哈希函数 $H_2()$的单向性. □

算法$\mathcal{B}$对哈希函数 $H_2()$的攻击过程包含下述步骤:

① $\mathcal{B}$适应性的选取身份标识询问 H_2 预言机;

② $\mathcal{B}$选择两个不同的身份标识 ID_0 和 ID_1,向游戏仿真者 S 进行 H_2 询问,S 随机选择 $b\leftarrow\{0,1\}$,并返回 $H_2(ID_b)$;

③ 收到 S 返回的应答后,$\mathcal{B}$输出对 b 的猜测 b'.

算法$\mathcal{B}$仿真游戏,$\mathcal{B}$模拟敌手$\mathcal{A}$的预言机,即,$\mathcal{A}$作为$\mathcal{B}$的子程序运行:

① 首先,$\mathcal{B}$创建集合 $J_M(L)$和 $J_R(L)$,其中,$MN\in J_M(L)$且 $RS\in J_R(L)$;

② $\mathcal{B}$将$\mathcal{A}$作为子程序激活运行,回答$\mathcal{A}$的所有询问,仿真协议运行过程中参与者激活的所有响应,并将协议的输出返回给$\mathcal{A}$.

根据敌手$\mathcal{A}$测试询问中是否选择 RS 作为参与者,分下述两种情况讨论:

① 未选择 RS,则$\mathcal{B}$随机选取 $b'\leftarrow\{0,1\}$作为 b 的猜测,并终止,则$\mathcal{A}$猜测成功的概率为 $\frac{1}{2}$.

② 选择了 RS,$\mathcal{B}$构造并返回协议运行结果:首先构造两个等长的消息 $M_0=\{n_0,ID_{MN_i}\}$ 和 $M_1=\{n_1,ID_{MN_j}\}$;然后,将 M_0 和 M_1 作为输入询问 H_2 预言机,预言机返回应答值 TID_b;最后,$\mathcal{B}$构造消息 $m_0=\{T_R,X,Sig(SK_R,T_R\|X)\}$和 $m_1=\{ID_H,TID_b,Message,T'_M\}$,$\mathcal{B}$将 m_0 和 m_1 作为测试询问应答.之后,算法$\mathcal{B}$继续执行游戏,回答$\mathcal{A}$的所有询问并仿真协议运行中参与者激活的所有响应.$\mathcal{A}$输出对 b 的猜测 b',$\mathcal{B}$输出 b'并终止.由于敌手$\mathcal{A}$能以不可忽略的优势 $Adv^{\Pi}(\mathcal{A})$在匿名性游戏中获胜,则$\mathcal{A}$猜测成功的概率为 $\frac{1}{2}+Adv^{\Pi}(\mathcal{A})$.令事件$\mathcal{E}$表示敌手$\mathcal{A}$在测试询问中选择了 RS 作为参与者,即 $\Pr[\mathcal{E}]=\frac{1}{L}$,则有:

$$\Pr[\mathcal{A}\text{猜测成功}]=\left(\frac{1}{2}+Adv^{\Pi}(\mathcal{A})\right)\Pr[\mathcal{E}]+\frac{1}{2}(1-\Pr[\mathcal{E}])=\frac{1}{2}+\frac{Adv^{\Pi}(\mathcal{A})}{L}.$$

算法$\mathcal{B}$猜测成功的情况有:

① $\mathcal{B}$通过自适应询问 H_2 预言机获得应答值,根据这些知识对 TID_b 进行猜测.此时,$\mathcal{B}$猜测成功的优势为 $Adv^{H_2}(\mathcal{B})$,则$\mathcal{B}$猜测成功的概率为 $\frac{1}{2}+Adv^{H_2}(\mathcal{B})$;

② $\mathcal{B}$完全以随机的方式输出猜测,此时,$\mathcal{B}$猜测成功的概率为 $\frac{1}{2}$.

令情况①发生的概率为 $P_{\mathcal{B}}$,则有: $\Pr[\mathcal{B}\text{猜测成功}]=\left(\frac{1}{2}+Adv^{H_2}(\mathcal{B})\right)P_{\mathcal{B}}+\frac{1}{2}(1-P_{\mathcal{B}})=\frac{1}{2}+Adv^{H_2}(\mathcal{B})P_{\mathcal{B}}$.

由于算法$\mathcal{B}$以敌手$\mathcal{A}$为子程序运行,即 $\Pr[\mathcal{B}\text{猜测成功}]=\Pr[\mathcal{A}\text{猜测成功}]$,则有:

$$\frac{1}{2}+Adv^{H_2}(\mathcal{B})\geqslant\frac{1}{2}+Adv^{H_2}(\mathcal{B})P_{\mathcal{B}}=\frac{1}{2}+\frac{Adv^{\Pi}(\mathcal{A})}{L}.$$

由于 $Adv^{\Pi}(\mathcal{A})$是不可忽略的,则 $Adv^{H_2}(\mathcal{B})$ 是不可忽略的.因此,若敌手$\mathcal{A}$以不可忽略的优势 $Adv^{\Pi}(\mathcal{A})$赢得相关游戏,即可构造算法$\mathcal{B}$,能以不可忽略的优势攻破抗碰撞的单向哈希函数 $H_2()$的单向性.

综上所述,本文匿名漫游认证协议满足匿名性,RS 只能验证 MN 是 HS 处注册的合法移动节点,却无法获知 MN 的真实身份等隐私信息;由于 MN 的身份标识具有强匿名性,则其身份标识同样具有不可追踪性.

3.2 协议特点

3.2.1 直接性

MN 从 HS 处获得注册授权信息后,无需 HS 的参与,MN 就可直接向 RS 进行身份合法性证明,减少了漫游认证协议的消息交互轮数,即 RS 基于漫游证明信息直接完成对 MN 身份合法性的验证.

3.2.2 认证性

在没有泄露 MN 秘密信息及其注册信息的前提下,RS 可基于 $Message$ 的合法性完成对 MN 的身份合法性

验证;若 *Message* 是合法的漫游证明信息,*RS* 就认为 *MN* 是 *HS* 上注册的合法移动节点,即,*RS* 对 *MN* 的身份合法性鉴别通过.

4 安全性证明

本节在 CK 安全模型下证明本文物联网移动节点直接匿名漫游认证协议的安全性.

4.1 AM中的漫游协议

本文协议中,*RS* 依赖 *MN* 持有的漫游证明信息鉴别 *MN* 的身份合法性.为了简化协议的证明,将协议抽象描述为协议δ.协议δ描述如下:

(1) 漫游请求.*MN* 已完成本地域注册并获得 *HS* 为其签发的注册授权信息(*T*,*R*,*C*,*AUTHEN*);*MN* 选取秘密随机数 $s,y\in Z_q^*$,计算 $U_M=sR$,$V_M=sCP$,$W_M=sTP$,$Y=yP$ 和 $M_M=yH(Y,0)+sT$;*MN* 向 *RS* 发送漫游请求消息:

$$Message=(AUTHEN,U_M,V_M,W_M,Y,M_M);$$

(2) 漫游响应.*RS* 收到 *MN* 的漫游申请后,验证漫游证明信息的合法性,若通过,则选取秘密随机数 $x\in Z_q^*$,并计算 $K_{R\text{-}M}=H(xY,1)$和 $X=xP$;最后,发送漫游响应消息 T_R,X 和 $Sig(S_R,T_R||X)$给 *MN*;

(3) *MN* 计算会话密钥 $K_{M\text{-}R}=H(yX,1)$,完成漫游申请.

定理 5. 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δ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$\mathcal{A}$攻陷,则协议执行完毕时,*MN* 和 *RS* 分别得到没有篡改的密钥协商参数 $X=xP$ 和 $Y=yP$.*RS* 计算的会话密钥为 $K_{R\text{-}M}=H(xY,1)=H(xyP,1)$;*MN* 计算的会话密钥为 $K_{M\text{-}R}=H(yX,1)=H(xyP,1)$,则有 $K_{M\text{-}R}=K_{R\text{-}M}$,因此,协议$\delta$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.

假设在 AM 中存在一个敌手$\mathcal{A}$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(p,q,X^*,Y^*,K^*)的算法$\mathcal{B}$,通过调用敌手$\mathcal{A}$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敌手$\mathcal{A}$发起会话的轮数为 *L*.具体交互过程如下:

① 选择随机数 $a\in\{1,2,\ldots,L\}$;

② 调用敌手$\mathcal{A}$完成对 AM 中 *MN* 与 *RS* 间匿名漫游认证协议的模拟,给$\mathcal{A}$提交 *p* 和 *q* 作为协议执行的公共参数;

③ 只要$\mathcal{A}$作为参与者,无论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会话密钥的所有信息提供给$\mathcal{A}$;

④ 在第 *a* 次会话中,输入(*MN*,*RS*,*a*),调用 *MN* 和 *RS* 的会话,设 *MN* 向 *RS* 发送(MN,a,Y^*);

⑤ *RS* 收到(MN,a,Y^*)后,向 *MN* 发送(RS,a,X^*);

⑥ 如果 *MN* 选择会话(*MN*,*RS*,*a*)作为最后一次测试会话,那么向$\mathcal{A}$提供 K^*作为询问应答;

⑦ 如果会话(*MN*,*RS*,*a*)没有暴漏,或者选择第 *a* 轮会话之外的某一次会话作为最后一次测试会话,或者$\mathcal{A}$没有选择测试会话就终止了,那么$\mathcal{A}$随机输出 $b\leftarrow\{0,1\}$,然后终止;

⑧ 如果$\mathcal{A}$终止并输出比特 b',那么$\mathcal{B}$终止并也输出比特 b'.

根据$\mathcal{A}$的测试会话是否与算法$\mathcal{B}$选择的一致,分两种情况讨论:

(1) 敌手$\mathcal{A}$选择的测试会话和$\mathcal{B}$随机选择的会话相同.

在测试会话中,如果$\mathcal{B}$的输入为(*p*,*q*,*X*,*Y*,*K*),即,是真实的会话密钥协商参数和会话密钥,则给$\mathcal{A}$的询问应答就是 *MN* 和 *RS* 在会话 *a* 中的真实会话密钥 *K*;如果$\mathcal{B}$的输入为(p,q,X^*,Y^*,K^*),即,是随机值,那么询问的应答也是随

机的.如果$\mathcal{B}$的输入是以$\frac{1}{2}$的概率随机选择的,那么$\mathcal{A}$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,即,$\mathcal{A}$猜对测试应答是真实值还是随机值的优势是不可忽略的,这也等价于算法$\mathcal{B}$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$\mathcal{A}$的第 a 次会话没有被选作测试会话.

在这种情况下,算法通常输出一个随机比特,然后结束会话.因此,猜对输入分布的概率是$\frac{1}{2}$.令事件$\mathcal{E}$表示敌手$\mathcal{A}$选择的测试会话恰好是第 a 次会话,即 $\Pr[\mathcal{E}']=\frac{1}{L}$,并且敌手$\mathcal{A}$能以不可忽略的优势$\varepsilon$猜对测试应答是真实值还是随机值,则有: $\Pr[\mathcal{A}\text{猜测成功}]=\left(\frac{1}{2}+\varepsilon\right)\Pr[\mathcal{E}']+\frac{1}{2}(1-\Pr[\mathcal{E}'])=\frac{1}{2}+\frac{\varepsilon}{L}$.

由于算法$\mathcal{B}$以敌手$\mathcal{A}$为子程序运行,即 Pr[$\mathcal{B}$猜测成功]=Pr[$\mathcal{A}$猜测成功],则算法$\mathcal{B}$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.

综上所述,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,*MN* 和 *RS* 得到没有篡改的身份合法性验证信息,并安全协商了会话密钥.所以,协议δ在 AM 中是安全的. □

4.2 认证器构造

本文从 *RS* 和 *MN* 间的相互认证着手构造认证器.匿名漫游时,*RS* 基于 *MN* 持有的漫游证明信息完成对其身份合法性的验证.为满足 *MN* 对身份等隐私信息的保护需求,*MN* 的漫游申请消息须经过相应的处理,不能包含 *MN* 的真实身份信息,但要能够使 *RS* 完成对 *MN* 身份合法性的验证.因此,在匿名漫游认证协议中,使用基于身份的匿名认证器$\lambda_{Enc,TID,T}$[18]实现 *RS* 对 *MN* 的认证(在文献[18]中,详细证明了认证器$\lambda_{Enc,TID,T}$的安全性和匿名性),使用基于数字签名和随机数的认证器$\lambda_{Sig,N}$[19]实现 *MN* 对 *RS* 的认证(在文献[19]中,详细证明了认证器$\lambda_{Sig,N}$的安全性).

认证器$\lambda_{Enc,TID,T}$的具体交互过程如下:

1) $\mathcal{A}$注册获得临时身份信息 TID_A,用$\mathcal{B}$的公钥 PK_B 加密产生密文消息 $Enc(PK_B,m||T_A||TID_A)$;最后,将临时身份 TID_A 和密文消息 $Enc(PK_B,m||T_A||TID_A)$发送给$\mathcal{B}$;
2) $\mathcal{B}$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 TID_A 的合法性和 T_A 的新鲜性验证均通过时,$\mathcal{B}$认为$\mathcal{A}$发送的消息是合法的,即,$\mathcal{A}$通过了$\mathcal{B}$的合法性验证.

认证器$\lambda_{Sig,N}$的具体交互过程如下:

① $\mathcal{A}$用 SK_A 加密消息 m 和随机数 N 等生成 $Sig(SK_A,m||N||ID_B)$,发送 $m,Sig(SK_A,m||N||ID_B)$给$\mathcal{B}$;

② $\mathcal{B}$收到$\mathcal{A}$的消息后,验证签名 $Sig(SK_A,m||N||ID_B)$的合法性,当且仅当签名是合法时,$\mathcal{B}$认为$\mathcal{A}$发送的消息是合法的,即,$\mathcal{A}$通过了$\mathcal{B}$的合法性验证.

4.3 UM中的协议

首先,将基于身份的匿名认证器$\lambda_{Enc,TID,T}$和基于数字签名和随机数的认证器$\lambda_{Sig,N}$应用于本文 AM 中的协议;然后,在匿名漫游认证协议安全性不受影响的前提下,隐藏 *MN* 的身份标识信息,实现 *MN* 身份标识的匿名性,使攻击者无法获得 *MN* 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 3 所示为 UM 中的协议δ.文献[21]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.

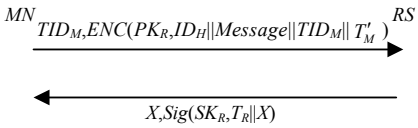


Fig.3 The protocol in UM model

图 3 UM 中的协议

UM 中匿名漫游认证协议的执行过程解释如下:

① *MN* 基于注册信息(*T*,*R*,*C*,*AUTHEN*)生成漫游证明信息 *Message*=(*AUTHEN*,U_M,V_M,W_M,*Y*,M_M).*MN* 发送漫游申请消息 TID_M, $Enc(PK_R, ID_H \| TID_M \| Message \| T'_M)$ 给 *RS*.

② *RS* 基于等式 $e(W_M-U_M,P)=e(V_M,PK_H)$和 $M_MP=H(Y,0)Y+W_M$ 验证漫游证明信息 *Message* 的合法性,基于身份凭证 *AUTHEN* 验证 *Message* 的有效性.若 *Message* 的合法性及有效性验证通过,则 *RS* 随机选取秘密数 $x \in Z_q^*$,计算 *X*=*xP* 和会话密钥 $K_{R\text{-}M}=H(xY,1)=H(xyP,1)$;*RS* 读取时戳 T_R 并生成签名 $Sig(SK_R, T_R||X)$,发送消息 $X,Sig(SK_R,T_R||X)$给 *MN*.

③ *MN* 收到 *RS* 的应答消息后,通过签名 $Sig(SK_R,T_R||X)$的合法性验证 *RS* 是否是其议定的远程域认证服务器.*MN* 计算会话密钥为 $K_{M\text{-}R}=H(yX,1)=H(xyP,1)$.

定理 6. 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.

证明:运用基于身份的匿名认证器$\lambda_{Enc,TID,T}$ 与基于数字签名和随机数的认证器$\lambda_{Sig,N}$ 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.由于认证器$\lambda_{Enc,TID,T}$和$\lambda_{Sig,N}$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.因此,本文协议是安全的匿名漫游认证协议. □

5 协议的性能分析比较

为方便对本文协议进行性能分析,本节以文献[14]中经典的匿名漫游认证协议为例,简要介绍传统漫游认证协议[14–17]2 轮交互认证模式的执行流程及认证特点.篇幅所限,具体过程详见文献[14].

移动节点漫游认证协议[14]的消息交互过程如图 4 所示,具体包含下述步骤:① 移动节点 MN_A 向区域 *B* 申请漫游,发送申请消息 *RMRAP-Request* 给远程域 *B* 的认证服务器 RS_B;② RS_B 收到 MN_A 的漫游申请后,由于 RS_B 未掌握 MN_A 的具体注册信息,因此无法独自完成对 MN_A 的合法性验证,RS_B 生成认证信息,并发送认证询问消息 *RMRAP-Ask* 给 MN_A 的家乡域认证服务器 HS_A;③ HS_A 对 MN_A 的合法性进行验证,并构造应答消息 *RMRAP-Answer* 将验证结果返回给远程域认证服务器 RS_B;④ RS_B 根据 HS_A 对 MN_A 的合法性验证结果制定相应的漫游访问策略,并发送响应消息 *RMRAP-Response* 给 MN_A.

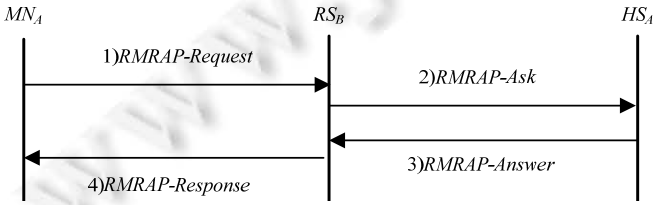


Fig.4 Message interaction process of roaming authentication protocol

图 4 漫游认证协议消息交互过程

在传统漫游认证协议[14–17]中,*MN* 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 *MN* 的合法性验证,即 *RS* 将 *MN* 的漫游证明信息发给 *HS*,由 *HS* 负责验证 *MN* 的合法性,*RS* 根

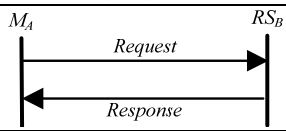
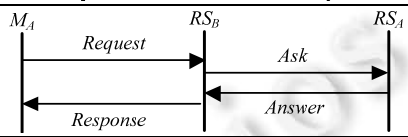
据 *HS* 的验证反馈制定相应的决策,因此传统漫游认证机制需要 2 轮(*MN*↔*RS*,*RS*↔*HS*)消息交互才能完成 *MN* 的漫游接入,即传统漫游认证协议采用 2 轮交互的认证模式完成对 *MN* 的身份合法性验证.

5.1 通信效率

表 1 为本文匿名漫游认证协议与传统漫游认证协议[14−17]在漫游模型、通信时延和认证特点这 3 方面的比较结果.

Table 1 The comparisons of communication efficiency in roaming authentication

表 1 漫游通信时延比较

	漫游模型	漫游过程	通信时延	认证特点
本文机制		无需 *HS* 的协助,*RS* 通过 *MN* 持有的漫游证明信息直接验证其身份的合法性	小	直接认证 (无需 *HS* 的协助)
文献[14–17]		*RS* 在 *HS* 的协助下完成对 *MN* 身份合法性的验证	大	间接认证 (*HS* 协助 *RS*)

传统的无线网络移动节点匿名漫游协议[14−17]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,所以无法直接对移动节点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,实现对移动节点的身份合法性验证,即,移动节点漫游过程中通过2轮交互的认证模式完成*MN*的身份合法性验证;而本文协议无需家乡域认证服务器的协助,远程域认证服务器可直接完成移动节点的身份合法性验证,即:本文协议在保持移动节点身份匿名性和不可追踪性的同时,基于 1 轮消息交互实现远程域认证服务器对移动节点的身份合法性验证,即,本文协议采用 1 轮交互的认证模式完成对 *MN* 的身份合法性验证.

由表 1 可知:在本文协议中,*MN* 申请漫游时已完成家乡域的注册,因此,漫游过程中无需 *HS* 的协助,*RS* 可直接完成对移动节点身份合法性的验证,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,漫游证明信息 *Message* 在其有效期内可重复使用,则当同一移动节点在多个远程域间漫游时,本文协议的通信效率会更高;相较与传统漫游协议[14−17]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,因此,协议更适用于物联网感知子网.

5.2 计算效率

表 2 所示为匿名漫游阶段各实体的计算效率比较,仅对双线性、签名和加密等高运算量算法的执行次数进行了统计.特别的,本文协议中,当 *MN* 漫游远程域时,已完成家乡域的注册,则在本文协议中,申请漫游之前 *MN* 已完成在家乡域的注册,因此,本文协议漫游过程的计算效率以第 3.3 节描述的漫游过程为主,即:表 2 中对本文计算效率的统计以第 3.3 节漫游过程为主,第 3.2 节的家乡域注册过程并不统计.

表 2 中,在移动节点 *MN* 的匿名漫游过程中,文献[14–17]中 *MN* 高运算量算法的运算次数分别为 2 次、4 次、5 次和 2 次,可见,文献[15,16]中 *MN* 的计算效率较低;本文协议中,*MN* 漫游远程域时仅运行 2 次高运算量算法,本文协议在降低通信时延的同时,并未增加协议参与实体的运算负载,依然保持了传统匿名漫游协议[14,17]高计算效率的特点.为保证通信过程的安全性,本文协议使用了加密、签名等高运算量算法以确保匿名漫游过程中 *MN* 的安全性.在保持传统匿名漫游协议[14,17]高计算效率优势的同时,本文协议减少了消息交互轮数,降低了漫游通信时延,具有快速漫游特点.

整体而言,本文协议具有消息交互轮数少、通信时延低和执行效率高的特点,由于安全性与计算开销间仅能寻求平衡,因此为了确保通信过程的安全性,本文协议漫游过程中使用了非对称加解密、签名等运算量较大的算法,在实际应用中,可根据环境的具体要求减少对通信消息的加解密及签名操作.

Table 2 The comparisons of computational spending in roaming authentication

表 2 漫游认证过程各实体的运算开销比较

相关算法/消息交互轮数	本文协议	文献[17]	文献[16]	文献[15]	文献[14]
双线性对运算(*MN-RS-HS*)	0/2/0	N/A	N/A	N/A	N/A
对称加解密 (*MN-RS-HS*)	N/A	2/1/1	3/2/6	N/A	1/1/2
非对称加解密(*MN-RS-HS*)	1/2/0	0/2/2	N/A	1/0/1	N/A
签名及验证运算(*MN-RS-HS*)	1/1/0	N/A	N/A	1/0/1	N/A
指数运算(*MN-RS-HS*)	N/A	N/A	2/0/1	2/1/2	N/A
消息验证码(*MN-RS-HS*)	N/A	N/A	N/A	N/A	1/2/3
消息交换轮数(*MN-RS*/*RS-HS*)	1/0	1/1	1/1	3/1	1/1

其中,N/A 表示相关方案未涉及此运算

6 结束语

针对物联网感知子网对安全高效快速匿名漫游协议的需求,本文提出可证安全的物联网移动节点直接匿名漫游认证协议,*MN*基于注册信息生成漫游证明信息,*MN*持漫游证明信息向远程域认证服务器申请漫游,无需本地域认证服务器的协助,远程域认证服务器通过漫游证明信息的真实性及有效性,完成对 *MN* 的身份合法性验证.采用临时身份不仅使远程域认证服务器和攻击者无法获知用户的真实身份,而且保证了用户身份等隐私信息的匿名性;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,确保了用户身份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.在 CK 安全模型下,证明本文协议是可证明安全的.相较于传统无线网络匿名漫游认证协议而言,本文协议具有计算效率高、通信时延小的优势,其快速漫游的特点更适用于物联网环境.

本文以相关安全性假设(假设 1 和假设 2)为基础完成物联网移动节点直接匿名漫游认证协议的设计,针对本文目前的研究现状,下一步将在更弱的安全性假设(如认证服务器的密钥会泄露)下,对移动节点的安全漫游机制进行研究;同时,通过性能仿真模拟对本文协议的通信时延进行定量分析.

References:

[1] Hwang KF, Chang CC. A self-encryption mechanism for authentication of roaming and teleconference services. IEEE Trans. on Wirel Communications, 2003,2(2):400−407. [doi: 10.1109/TWC.2003.809452]

[2] Shi MH, Rutagemwa H, Shen XM. A service-agent-based roaming architecture for WLAN/cellular integrated networks. IEEE Trans. on Vehicular Technology, 2007,56(5):3168−3181. [doi: 10.1109/TVT.2007.900525]

[3] Yang GM, Wong DS, Deng XT. Anonymous and authenticated key exchange for roaming networks. IEEE Trans. on Wirel Communications, 2007,6(9):1035−1042. [doi: 10.1109/TWC.2007.06020042]

[4] Yang GM, Wong SD, Deng XT. Formal security definition and efficient construction for roaming with a privacypre serving extension. Journal of Universal Computer Science, 2008,14(3):441−462.

[5] Wan Z, Ren K, Preneel B. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks. In: Proc. of the 1st ACM Conf. on Wireless Network Security. Alexandria, 2008. 62−67. [doi: 10.1145/1352533.1352544]

[6] Yang GM, Huang Q, Wong SD, Deng XT. Universal authenticated protocols for anonymous wireless communications. IEEE Trans. on Wirel Communications, 2010,9(1):168−174. [doi: 10.1109/TWC.2010.01.081219]

[7] He DJ, Bu JJ, Chan S, Chen C, Yin MJ. Privacy-Preserving universal authentication protocol for wireless communications. IEEE Trans. on Wirel Communications, 2011,10(2):431−436. [doi: 10.1109/TWC.2010.120610.101018]

[8] Lee CC, Hwang MS, Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Trans. on Industrial Electronics, 2006,53(5):1683−1687. [doi: 10.1109/TIE.2006.881998]

[9] Chang CC, Lee CY, Chiu YC. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Computer Communications, 2009,32(4):611−618. [doi: 10.1016/j.comcom.2008.11.032]

[10] Zhou T, Xu J. Provable secure authentication protocol with anonymity for roaming service in global mobility networks. Computer Networks, 2011,55(1):205−213. [doi: 10.1016/j.comnet.2010.08.008]

[11] Wu CC, Lee WB, Tsaur WJ. A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters, 2008,12(10):722−723. [doi: 10.1109/LCOMM.2008.080283]

[12] Zeng P, Cao Z, Choo KKR, Wang S. On the anonymity of some authentication schemes for wireless communications. IEEE Communications Letters, 2009,13(3):170−171. [doi: 10.1109/LCOMM.2009.081821]

[13] Mun H, Han K, Lee YS, Yeun CY, Choi HH. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling, 2012,55(1-2):214−222. [doi: 10.1016/j.mcm.2011.04.036]

[14] Wang LM, Jiang SR, Guo YB. Composable secure authentication protocol for mobile sensors roaming in the Internet of things. Scientia Sinica (Informationis), 2012,42:815−830 (in Chinese with English abstract). [doi: 10.1360/112011-1081]

[15] Xiao P, He JS, Fu YF. A secure mutual authentication protocol for roaming in wireless mesh networks. Journal of Networks, 2012, 7(2):267−275. [doi: 10.4304/jnw.7.2.267-274]

[16] Xu J, Zhu WT, Feng DG. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Computer Communications, 2011,34(3):319−325. [doi: 10.1016/j.comcom.2010.04.041]

[17] Yoon EJ, Yoo KY, Ha KS. A user friendly authentication scheme with anonymity for wireless communications. Computers and Electrical Engineering, 2011,37(3):356−364. [doi: 10.1016/j.compeleceng.2011.03.002]

[18] Jiang Q, Ma JF, Li GS, Ma Z. Security integration of WAPI based WLAN and 3G. Chinese Journal of Computers, 2010,33(9): 1675−1685 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2010.01675]

[19] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols. In: Proc. of the 30th ACM Symp. on Theory of Computing. Dallas, 1998. 419−428. [doi: 10.1145/276698.276854]

[20] Canerri R, Krawczyk H. Analysis of key exchange and their use for building secure channels. In: Proc. of the Eurocrypt. Springer-Verlage, 2001. 452−474. [doi: 10.1007/3-540-44987-6_28]

[21] Tin YST, Boyd C, Nieto JG. Provably secure key exchange: An engineering approach. In: Proc. of the Australasian Information Security Workshop. 2003. 97−104.

附中文参考文献:

[14] 王良民,姜顺荣,郭渊博.物联网中移动 Sensor 节点漫游的组合安全认证协议.中国科学:信息科学,2012,42:815−830. [doi: 10.1360/112011-1081]

[18] 姜奇,马建峰,李光松,马卓.基于 WAPI 的 WLAN 与 3G 网络安全融合.计算机学报,2010,33(9):1675−1685. [doi: 10.3724/SP.J.1016.2010.01675]

周彦伟(1986－),男,甘肃通渭人,博士生,主要研究领域为密码学,匿名通信技术.

杨波(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全.