第 35 卷 第 6 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.6 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)06—0159—03 文献标识码：A 中图分类号：TP393.08

基于 PANA 的移动互联网匿名认证协议

张 婕，吴振强，张景东，陈惠娟，见晓春
(陕西师范大学计算机科学学院，西安 710062)

摘 要：针对移动互联网络的安全需求，在基于身份公钥系统的基础上，设计一种利用 PANA 的双向匿名 AAA 协议，该协议提出移动互联网络通信中基于网络层认证协议 PANA 的 AAA 方案，实现了通信双方的相互认证，并使移动互联网络向移动用户提供匿名服务，保护用户身份信息，具有较强的匿名性。试验结果表明，该协议高效可行，满足 AAA 下移动互联网络 PANA 协议匿名性的安全需求。

关键词：PANA 协议；移动互联网络；匿名；AAA 协议；密钥协商

Anonymity Authentication Protocol in Mobile Internet Based on PANA

ZHANG Jie, WU Zhen-qiang, ZHANG Jing-dong, CHEN Hui-juan, JIAN Xiao-Chun
(College of Computer Science, Shaanxi Normal University, Xi'an 710062)

【Abstract】 According to security request of mobile Internet, an identity-based cryptography mutual authentication PANA protocol is proposed to solve the problem of AAA protocol in mobile communication. It can provide anonymous service that guarantees the confidentiality of the mobile users' identity. Research results show that the protocol has a good anonymous property, it is efficient and feasible, and is suitable to be applied in wireless mobile Internet.

【Key words】 PANA protocol; mobile Internet; anonymity; AAA protocol; key agreement

1 概述

随着信息网络技术的快速发展，人们不再满足于使用固定终端或单个移动终端连接到互联网络上，而是希望移动子网能以一种相对稳定和可靠的形式，从 Internet 上动态地获取信息，这就促使无线网络从无线互联网络向无线移动互联网络[1]演化。然而，移动互联网络只是从技术上研究了移动设备的移动性问题，没有考虑它们的授权和记账这些实际应用中必须解决的问题，这就限制了它的实际应用。AAA 正是为解决这些问题而引入的。AAA 认证要求用户信息真实可信，对许多移动互联网络的用户而言，他们希望能够保留自己的隐私，这样就需要一种新的匿名协议，满足双方的安全需求。由于移动网络的结构不同，因此有必要在网络层定义一个独立于网络底层访问技术和网络拓扑结构的网络访问认证协议，接入网认证信息承载协议 PANA[2-4]应运而生。本文针对网络层移动互联网络的匿名 AAA 协议问题提出一种注册方案，该方案在网络层实现移动互联网络的匿名 AAA 协议。并对方案的安全性和执行效率进行了分析，给出了方案的仿真结果。

2 PANA 简介

PANA 是一个独立于网络底层访问技术和网络拓扑结构的网络访问认证协议。设计 PANA 的主要目的是为了便于对网络访问客户进行认证和授权。一个完整的 PANA 协议一般包括以下 4 个单元[2]：PANA 客户端(PaC)，PANA 认证代理(PAA)，认证服务器(AS)和监控点(EP)。各功能单元间的协议或接口如图 1 所示。PANA 协议运行于客户机 PaC 和服务器 PAA 之间，为网络访问服务提供认证和授权服务。图 2 显示了 PANA 认证协议的认证流程。EP 允许任何授权的 PaC 和非授权的受限制的数据访问网络。

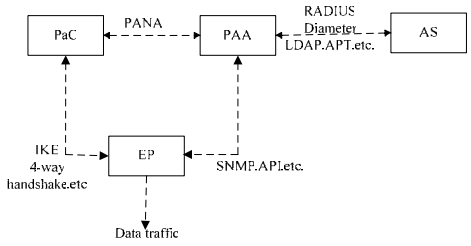

图 1 PANA 功能模型

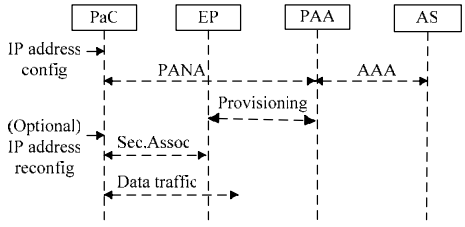

图 2 PANA 认证流程

3 AAA 下移动互联网络的匿名认证注册方案

3.1 结合 AAA 的移动互联网络 PANA 认证基本模型

结合 AAA 的移动互联网络 PANA 认证基本模型如图 3

基金项目：国家自然科学基金资助项目(60503008)；陕西师范大学创新基金资助项目(2007CXS025)
作者简介：张 婕(1981－)，女，硕士研究生，主研方向：无线网络安全；吴振强，副教授、博士研究生；张景东、陈惠娟、见晓春，硕士研究生
收稿日期：2008-08-22 **E-mail：**zhangjie_500@stu.snnu.edu.cn

所示。AS/AAAF 为外地域中的 AAA 服务器，每一个 AS/AAA 都有许多的 PAAF/EP 和它相连。AS/AAAH 为家乡域的 AAA 服务器，它能够对所属的 PaC 身份进行认证。图 3 也表明了移动互联网络存在的 3 种信任关系：PAA 和 AS 之间安全关联 SA1，PaC 和 AS/AAAH 之间安全关联 SA2, AS/AAAH 和 AS/AAAF 之间安全关联 SA3。下面将介绍本文采用的描述协议的标识符[5]。

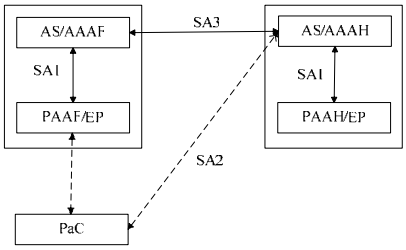

图 3　结合 AAA 的移动互联网络 PANA 认证基本模型

3.2　认证注册整合方案

在该解决方案中，PaC 先后参与 2 种类型的注册。首先 PaC 在本地域中进行注册，申请成为其用户；然后是第 1 次漫游到一个外地域中，PaC 向外部域注册。

3.2.1　移动用户在家乡域首次注册

PaC 向家乡域进行初次注册，以获得一个账号以及能够证明自己身份的证书。设 G_1 与 G_2 分别是阶为 q 的加法群和乘法群，其中，q 是素数，在 G_1, G_2 中离散对数问题都是难解的。设 $\hat{e}$ 是 $G_1 \times G_2$ 到 G_2 的一个双线性映射。通常 G_1 为有限域 F_q 上的椭圆曲线有理点群的一个加法子群，G_2 为这个有限域的一个乘法子群，双线性映射 $\hat{e}$ 由椭圆曲线上的 Weil 对派生得到。设 ID 是个标识用户身份的一个字符串，H 是公开的哈希函数，$H1, H2$：$\{0, 1\}^* \rightarrow G_1$[5-7]。图 4 是移动用户在家乡域首次注册的具体过程。

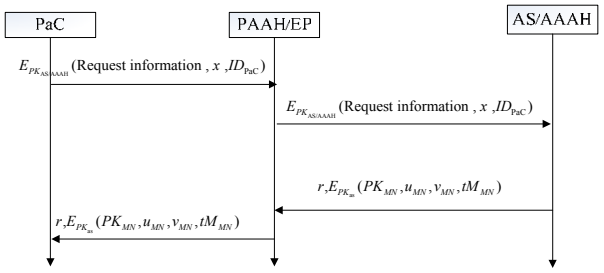

图 4　PaC 在 AS/AAAH 处初次注册

(1)系统初始化。AS/AAAH 随机选择 $P \in G_1$, $s \in F_q$，计算 $P_{AS/AAAH}=sP$。公开 P 和 $P_{AS/AAAH}$，秘密保存 s。$P_{AS/AAAH}$ 为系统公钥，s 为系统私钥(亦称系统主密钥)。

(2)用户注册。假设用户 PaC 身份信息为 ID_{PaC}，计算 $Q_{PaC}=H1(ID_{PaC})$, $O_{PaC}=H2(ID_{PaC})$，发送信息如图 4 所示，其中，x 为和 AS/AAAH 协商共享密钥时所用元素。

(3)PAAH/EP 把信息转发给 AS/AAAH，AS/AAAH 对注册消息进行确认之后，计算 $Q_{PaC}=H1(ID_{PaC})$, $O_{PaC}=H2(ID_{PaC})$ 和共享密钥生成元素 y，用作日后确认 PaC 的身份。然后计算 sQ_{PaC} 和 $M_{PAC}=s(sQ_{PaC}+sO_{PaC})$，将 sQ_{PaC}, sO_{PaC}，y 和 M_{PaC} 用计算好的 AS/AAAH 和 PaC 的共享密钥加密后发送给 PAAH/EP。这里使用基于 ECC 的 Diffie-Hellman 算法来计算协商密钥。

(4)PAAH/EP 把信息转发给用户，PaC 的私钥为 $SK_{PaC}=sQ_{PaC}$, PaC 秘密保存 M_{PaC} 和 sO_{PaC}。显然 M_{PaC} 只能从 AS/AAAH 得到，无法自己生成。这样就完成了移动用户在家乡域的首次注册。

3.2.2　移动用户到外部域的初次注册

PaC 漫游到外地域时，它必需能够向外地域证明自己的身份。为了实现移动用户身份的保密性，PaC 不能向 PAAF/EP 出示其身份标识。PAAF/EP 对 PaC 的认证是通过 PAAF/EP 对 PAAH/EP 的认证与 AS/AAAH 对 PaC 的认证来实现。具体的注册过程如图 5 所示。

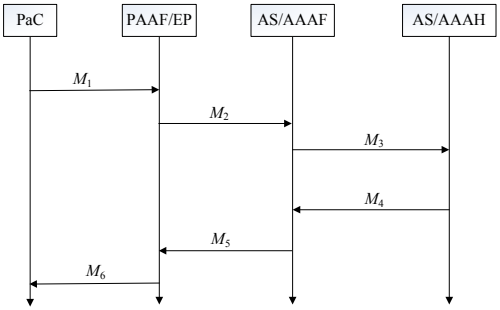

图 5　PaC 在外地域处初次注册

(1)PaC 任意选择 $t \in Fq$，计算 $PK\text{PaC}=tQ\text{PaC}$, $u\text{PaC}=t(sQ\text{PaC})$, $v_{PaC}=t(sO_{PaC})$，则(PK_{PaC}, u_{PaC}, v_{PaC}, tM_{PaC})称为 PaC 的一次性公钥。

PaC→PAAF/EP: M_1: $PK_{PAAF/EP}$(Registration Request, (PK_{PaC}, u_{PaC}, v_{PaC}, M_{PaC}), $ID_{AS/AAAH}$, Y_{PaC})，其中，Y_{PaC} 是 PaC 生成的与 PAAF/EP 协商会话密钥的生成信息，$ID_{AS/AAAH}$ 是用户家乡域 AAA 服务器的身份信息。

(2)PAAF/EP→AS/AAAF: M2: PKAS/AAAF(Registration Request, (PK_{PaC}, u_{PaC}, v_{PaC}, M_{PaC}), $ID_{AS/AAAH}+T_{PAAF/EP}$)。

PAAF/EP 保存 $PK_{PAAF/EP}(Y_{PaC})$，然后用 AS/AAAF 的公钥加密 $T_{PAAF/EP}$，其中，$T_{PAAF/EP}$ 是 PAAF/EP 产生的时戳。

1)PAAF/EP 验证等式 $\hat{e}$ (u_{PaC}, P)= $\hat{e}$ (PK_{PaC}, $P_{AS/AAAH}$) 是否成立。如果上式成立，则说明 u_{PaC} 含有系统主密钥，因此，PaC 在 AS/AAAH 注册过。

2)PAAF/EP 验证等式 $\hat{e}$ (tM_{PaC},P)= $\hat{e}$ (u_{PaC}, $P_{AS/AAAH}$)· $\hat{e}$ (v_{PaC}, $P_{AS/AAAH}$)是否成立。如成立，则确信 AS/AAAH 在必要时可以揭示出 PaC 的身份。

事实上，$\hat{e}$ (tM_{PaC}, P)= $\hat{e}$ ($tssQ_{PaC}$+$tssO_{PaC}$, P)= $\hat{e}$ ($tssQ_{PaC}$, P) $\hat{e}$ ($tssO_{PaC}$, P)= $\hat{e}$ (tsQ_{PaC}, sP) $\hat{e}$ (tsO_{PaC}, sP)= $\hat{e}$ (v_{PaC}, $P_{AS/AAAH}$) $\hat{e}$ (u_{PaC}, $P_{AS/AAAH}$)。

如果上式成立，则说明 $tM_{PaC}=su_{PaC}+sv_{PaC}$。而 u_{PaC}, v_{PaC} 也都含有系统主密钥，由于 $M_{PaC}=s(sQ_{PaC}+sO_{PaC})$，且 PaC 无法伪造，而 AS/AAAH 中保存了与 PaC 相关的 Q_{PaC} 和 O_{PaC} 等信息，因此 PAAH/EP 可以确信 AS/AAAH 在必要时通过 u_{PaC}, v_{PaC} 能够揭示出用户 PaC 的身份。

(3)AS/AAAF 用私钥解密 PAAF/EP 发送的信，然后检查时戳是否在有效期。

(4)AS/AAAF→AS/AAAH: $M3$: registration request+ $PK_{AS/AAAH}$ (Registration Request ,(PK_{PaC}, u_{PaC}, v_{PaC}, M_{PaC}))。

AS/AAAH 用私钥解密 AS/AAAF 转发的信息，得到 PaC 的一次性公钥。AS/AAAH 根据一次性公钥得出用户真实身份和账户。

(5)AS/AAAH→AS/AAAF: $M4$: registration reply+ $PK_{AS/AAAF}$(PaC 的客户消息，$lifetime_{PaC}$)， $lifetime_{PaC}$ 是公钥的有效生存期。AS/AAAH 将把 PaC 的客户消息(如 PaC 的授权策略)和有效生存期发送给 AAAF 使它有足够的消息来对

PaC 进行验证。AS/AAAF:收到消息之后，对 $PK_{AS/AAAF}$(PaC 的客户消息，$lifetime_{PaC}$)，进行解密得到 PaC 的客户消息，$lifetime_{PaC}$。

(6)AS/AAAF→PAAF/EP: *M*5: registration reply+ $PK_{PAAF/EP}(PK_{PaC}, lifetime_{PaC})$。

PAAF/EP 对 $PK_{PAAF/EP}(lifetime_{PaC})$，进行解密得到 PaC 公钥，$lifetime_{PaC}$。然后计算 $Y_{PAAF/EP}$.$Y_{PAAF/EP}$ 是 PAAF/EP 生成的与 PaC 协商会话密钥的生成信息。

(7)PAAF/EP→PaC: *M*6: registration reply+PKPAC $(Y_{PAAF/EP})$。

这样，PaC 计算会话协商密钥，完成密钥协商。

4 协议分析

4.1 安全性分析

本文所提协议的计算安全性基于椭圆曲线上离散对数难题和安全单向函数。下面将就一些公钥密码协议常见安全问题进行讨论。

(1)已知密钥安全：在这个协议中，PaC 和 PAAF/EP 采用基于 ECC 的 Diffie-Hellman 算法来计算协商密钥，而且每次会话都改变密钥，假设攻击者已知一些旧的会话密钥，这对攻击者获取新的会话密钥或者假冒任一参与方都是没有帮助的。

(2)前向安全：假设攻击者得到了 PaC 或 PAAF/EP 的私钥，攻击者也难于获取 PaC 和 PAAF/EP 之间协商的旧会话密钥。由椭圆曲线上离散对数难题知，A 攻击者很难由 $Y_{PAAF/EP}$ 和 Y_{PaC} 反推出 x 和 y，所以，也就无法知道会话密钥，协议向前安全。

(3)重放攻击：假设攻击者重放 PaC 的消息，由于用户的公钥是一次性的，PAAF/EP 可以查看用户的公钥是否同样轻易地挫败对该消息的重放，因此不会构成实质威胁。

(4)中间人攻击：PANA 必须引导 PaC 和 PAA 之间的共享的密钥，这个密钥将用在 PaC 和 EP 之间建立安全连接去提供密码学保护预防服务偷窃[2]。在本协议中，由于用户使用一次性公钥，因此攻击者无法冒充 PaC, PAAF/EP 与 PaC 协商密钥。所以，协议能防止中间人攻击。

4.2 协议具有的较高效率

(1)在该协议中，PaC 只有在外地域中初次注册时认证消息才需要在 PAAF/EP 和 AS/AAAH 之间传送，之后的重新认证基本上都不需要 AS/AAAH 的参与，这样就减少了认证注册所需的时间。

(2)PaC 和网络的相互认证只需一个来回。这是进行认证所需的最少轮数。

(3)该方案中 PaC 在外地域中第 1 次注册时都只需要进行一次公钥加密和公钥解密运算，这样就可以减少协议交互所需要的时间，而不降低安全性。

5 模拟仿真

本文选用 OPNET Modeler10.5 为仿真工具。仿真在 Intel 双核 1.861 GHz Windows XP 的平台上进行。仿真模型由 1 个家乡域和 2 个外地域组成。图 6 中的最下面的折线是 PaC 的移动路径。图 6 是仿真模型的整个动画过程。在仿真动画中，可以很清楚的看见 PaC 在移出 AS/AAAH 的范围时，向 AS/AAAH 发送切换请求，在接收 AS/AAAH 的请求应答后，PaC 切换到 AS/AAAF_1。图 7 显示了网络的时延，图中 2 个较高的点是 PaC 首次在 AS/AAAF_1 和 AS/AAAF_2 注册时网络的时延，说明 PaC 首次在外地域注册时，时延有明显的增加。现实网络应用中要求网络时延不超过 0.5 s，文中的 PaC 初次在 AS/AAAF 注册的时延可以满足实际要求。

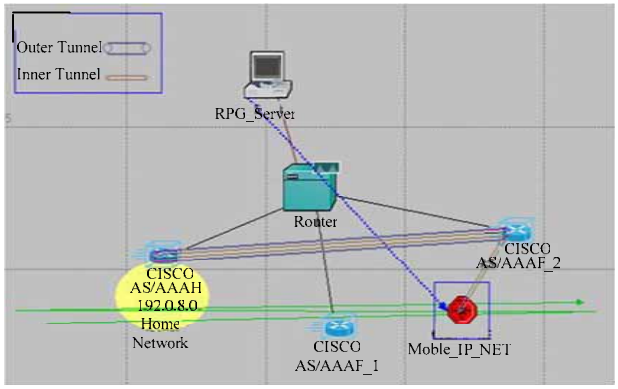

图 6 OPNET 记录的仿真动画

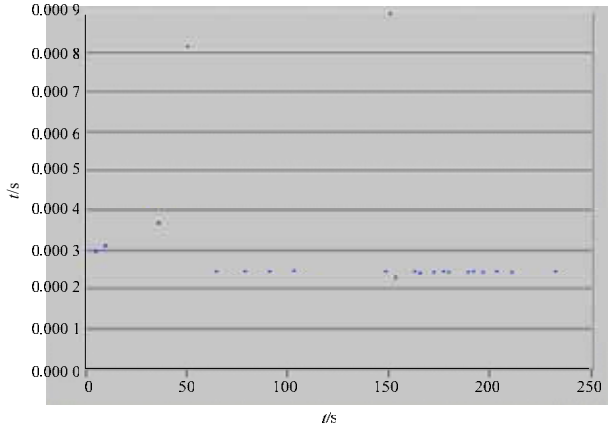

图 7 网络时延

6 结束语

本文提出一种利用 PANA 的移动互联网络匿名 AAA 方案，解决了移动用户和移动互联网络之间的双向身份认证和密钥协商问题，并使移动网络系统向移动用户提供匿名服务，最大程度保证了用户身份信息和所在位置信息的机密性。整个协议实现简单、高效实用，是解决移动互联网络安全问题一个可行的方案，同时对于使用基于身份公钥来解决移动通信中的身份认证和密钥协商问题也有一定的借鉴意义。

参考文献

[1] 吴振强, 马建峰. 基于管理的移动互联网络安全体系结构[J]. 计算机科学, 2006, 33(7): 314-317.

[2] Parthasarathy M. Protocol for Carrying Authentication for Network Access(PANA) Threat Analysis and Security Requirements[S]. RFC 4016, 2005.

[3] Yegin A, Ohba Y, Penno R, et al. Protocol for Carrying Authentication for Network Access(PANA) Requirements[S]. RFC 4058, 2005-05.

[4] Forsberg D. Protocol for Carrying Authentication for Network Access(PANA)[EB/OL]. (2007-06-05). http://www.ietf.org/internet-drafts/draft-ietf-pana-pana-18.txt.

[5] 张秋璞, 郭宝安. 基于 ID 的一次性盲公钥[J]. 电子学报, 2003, 31(5): 769-771.

[6] Aboba B, Simon D. PPP EAP TLS Authentication Protocol[S]. RFC 2716, 1999.

[7] Franlin B D. MIdentity-based Encryption from the Weil Pairing[J]. SIAM J. of Computer, 2003, 32(3): 586-616.

编辑 索书志