基于公钥的可证明安全的异构无线网络认证方案

侯惠芳[①②]　刘光强[②]　季新生[①]　张秋闻[②]
[①](国家数字交换系统工程技术研究中心　郑州　450002)
[②](河南工业大学信息科学与工程学院　郑州　450001)

摘　要：该文针对3G-WLAN异构网络的接入安全，对异构网络的实体进行抽象，建立了一种通用的认证模型。在该模型的基础上，利用Canetti-Krawczyk (CK)模型设计了一种新的接入认证与密钥协商方案。该方案利用公钥基础设施分配公钥，简化接入端服务器和归属端服务器间的认证过程和认证信息；利用椭圆曲线密码机制，减少了移动终端的认证计算量；最后利用CK模型对提出的协议进行了形式化分析和证明。分析表明该方案是安全有效的。

关键词：异构无线网络；椭圆曲线；接入认证；公开密钥基础设施；CK 模型
中图分类号：TN918.91　　**文献标识码**：A　　**文章编号**：1009-5896(2009)10-2385-07

Provable Security Authentication Scheme Based on Public Key for Heterogeneous Wireless Network

Hou Hui-fang[①②]　Liu Guang-qiang[②]　Ji Xin-sheng[①]　Zhang Qiu-wen[②]
[①](*National Digital Switching System Engineering & Technological R & D Center*, *Zhengzhou* 450002, *China*)
[②](*College of Information Science and Engineering*, *Henan University of Technology*, *Zhengzhou* 450001, *China*)

Abstract: Aiming at access security aspect of 3G-WLAN heterogeneous wireless network, this paper abstracts each entities of heterogeneous wireless network, thereby establishes a general authentication model. Then based on this general authentication model, a novel access authentication and key agreement scheme by using Canetti-Krawczyk (CK) model is devised. This scheme simplifies the authentication process and information between access network server and home network server by using Public Key Infrastructure (PKI) to distribute public key. It also decreases the authentication computational complexity of mobile terminal by Elliptic Curves Cryptography (ECC). Finally, formal analysis and proof with CK model for the proposed protocol are given. It is showed that the proposed scheme is secure and efficient.

Key words: Heterogeneous wireless network; Elliptic curves; Access authentication; Public Key Infrastructure (PKI); CK model

1　引言

随着无线局域网(WLAN)的迅速发展及移动通信(如3G)的普及，二者的融合成为未来无线网络的发展方向。由于3G和WLAN对各自有不同的安全需求，所以建立一种新的3G-WLAN安全体系，便越来越重要，作为安全的门户—认证便成为重中之重。对3G-WLAN网络的认证，研究人员提出了很多认证机制，如SIM-based，EAP-AKA和EAP-SIM等，但系统的安全和性能存在如下缺陷：(1)基于单钥体系的认证协议，给异构网络的建立造成诸多不便，且不能提供不可否认性。(2)不能保障用户身份信息的(例如网络接入标识NAI，用户永久身份IMSI)安全。容易泄露用户的行踪和使用户受到伪基站攻击。(3)认证是基于归属网络用户服务器(简称为归属服务器)和服务网络接入服务器(简称为接入服务器)之间存在安全连接的前提下建立的。在一个网络中，认为归属服务器和接入服务器之间存在安全的通路相联是可行的。但在异构网络中，由于认证服务器众多，若在每对服务器间都建立安全关联或有共享秘密，则既降低系统扩展性，工作量也不可想象，在实际应用中不可行。

鉴于此，研究人员基于密码体制和安全协议作了大量改进。将EAP-TLS[1]应用于融合网络的认证由G. Kambourakis等人最早提出，通过构建同3G核心网络连接的公钥基础设施，引入公钥机制并解决不可否认等问题，同基于对称密码的体制相比，虽更加灵活安全，但认证时需要移动终端无线传送自己的公钥证书或验证对方证书[2]，严重增加了网络负载及移动终端的计算负担和数据传输量。彭华熹[3]

2008-11-03 收到，2009-05-04 改回
国家 863 计划项目(2007AA01Z434)资助课题

利用双线性映射实现了跨信任域的身份认证，但需要各认证服务器及用户有相同的公钥参数且认证参与方需要知道对方的密钥中心的公钥，这无疑加重了认证方的负担，用户需要存储自己可能到达位置的认证器的密钥中心的公钥，认证服务器也需要存储所有可能来此接受服务的用户的密钥中心的公钥。

本文利用 CK 模型提出一种新的公钥认证方案，该方案采用归属方辅助证明的方法，使移动终端不传递和验证证书；移动终端和接入认证服务器之间以及各接入认证服务器间不需预存安全关联，认证服务器间也不需有相同的公钥参数，系统的扩展性和灵活性得到增强；本着尽量减少移动终端计算量、节省存储空间的原则，采用“密钥短，安全性高”的椭圆曲线密码体制的加解密和签名算法，文献[4]从安全性、空间需要及有效性等方面进行了比较，指出椭圆曲线密码体制更适合于在智能卡上应用。

2 CK 模型

Canetti-Krawczyk (CK)[5]模型是近年来比较流行和可信的一种形式化分析与设计密钥协商协议的方法，它给出了一个会话密钥安全的定义和利用该定义来分析和设计密钥交换协议的模块化方法。CK 模型采用不可区分性的方法来定义安全，即若在允许的攻击能力下，攻击者不能区分协议产生的会话密钥和一个独立的随机数，则可认为该密钥交换协议是安全的。

2.1 CK模型的组成

CK 模型主要包含 3 个重要的组成部分：理想模型(AM)，现实模型(UM)和认证器，其中 AM 和 UM 是两种不同层次的攻击模型。认证器是确保将 AM 中的协议转换为 UM 中与 AM 中安全性相同的协议的转换工具。

(1)AM(Authenticated-linksadversarial Model)，可被视为理想环境下的认证链路攻击模型，在此模型下，攻击者(形式化为一个概率多项式算法即 PPT 算法)控制和编排各实体的激活，侦听所有传送的消息、外部请求以及除了标记为“秘密”的参与者的所有输出。在该模型中，攻击者是被动的，不能伪造或者篡改来自未被攻陷的参与者的消息，被限制只能忠实地传递同一消息一次(虽然可以延迟或重排传递顺序等)。除此之外，攻击者还可进行如下攻击：攻陷参与者(party corruption)，查询会话密钥(session-key query)，暴露会话状态(session-state reveal)，测试会话查询(test-session query)。

定义 1[5] 测试会话查询(test-session query)：攻击者可在协议运行的任何时刻，从那些完成的、未过期的以及未暴露的会话中选择一个测试会话，来获得测试会话密钥或一个随机数。具体来说，设 k 是测试会话的会话密钥，当攻击者对测试会话查询时，我们投币 b，若 $b=0$，则将 k 返回攻击者，否则将一个密钥概率分布空间中的随机数返回攻击者。在测试会话过期前，攻击者能继续进行一些攻击活动，但不允许使测试会话暴露(即不允许暴露会话状态，查询会话状态或关于测试会话的攻陷)。最后攻击者输出 b' 作为对 b 的猜测。

(2)UM(Unauthenticated-linksadversarial Model)，可被视为真实环境下的未认证链路攻击模型，在 UM 中，攻击者除了能够执行 AM 中的所有攻击外，还能伪造、重放和篡改消息。

定义 2[5] 被允许执行密钥交换协议的测试会话查询的攻击者，CK 模型将其称之为 KE 对手。

定义 3[5] 会话密钥安全(SK-secure)：若对于 AM 中任何 KE 对手 A，当且仅当下列 2 条性质满足时，该协议在 AM 中是 SK-secure：

性质 1 一致性要求：2 个未被攻陷的参与者完成协议后，会话匹配，得到相同的会话密钥；

性质 2 A 进行测试会话查询攻击，它猜中正确的会话输出值 b (即能够区分密钥和随机数)的概率不超过 $1/2+\varepsilon$，其中：ε 是任意小的数，是安全参数范围内可忽略的概率，也被称之为“优势”。

UM 攻击模型下的安全定义同上类似。

定理 1 SK-secure 定义的 2 条性质确保协议必备的安全属性有：丢失信息安全、非密钥泄漏伪装安全、已知密钥安全和未知密钥共享安全。

具体证明过程参见文献[5]。

(3)认证器

定义 4[5] 认证器是一种协议转换器 C，其输入是协议 π，输出是另外一个协议 $\pi'=C(\pi)$，且满足：若 π 在 AM 中是 SK-secure 的，则 π' 在 UM 中也是 SK-secure 的。π' 与 π 只有一个区别—收发方不再通过网络而仅通过激活认证器传递信息。

认证器的概念基于消息传输认证器(MT-authenticator，MT 认证器)。

定义 5[5] MT-authenticator：是将 AM 中的 MT 协议等价转换为 UM 中的协议的转换器。

MT-authenticator 可用简单的密码函数(如 MAC、数字签名、公钥加密)构造，其目标只是认证通信双方间简单的消息交换或传递(Message Transmission)。简单消息传输(MT)协议即将一条消息由一个参与者发送给另一个参与者。若干个

MT-authenticator 组合成一个协议的认证器。在 AM 中只有一个消息流的协议，MT-authenticator 就是协议认证器；否则为 AM 中协议的每个消息流设计 MT-authenticator，并将这些 MT-authenticator 组合在一起作为协议的认证器。

2.2 CK 模型分析和设计密钥交换协议的步骤

CK 模型分析和设计密钥交换协议的基本方法包括如下几个步骤。

(1)在 AM 中设计或者重用一个基本的 SK-secure 协议。因为 AM 中攻击者仅有被动窃听攻击能力，不具有篡改和伪造能力，因此协议通常较容易设计；

(2)设计一个能被证明是有效的认证器；

(3)应用认证器将 AM 中的基本协议转换成 UM 中的安全认证协议；

(4)运用重用消息组合、重新排序、消除冗余的方式优化结果协议。

3 基于公钥的认证模型

3.1 认证模型建立

本文所指的3G-WLAN的异构网络中，不是特指某一种(紧耦合或松耦合)，而是指一种通用的、抽象的异构网络，在该异构网络中，用户可以是3G的MS，也可以是WLAN的STA，为方便起见，统一记为移动终端MN。移动终端需要异构服务，则需通过一个接入端，并得到其归属接入端服务器的认可。若接入服务器是3G，则对应接入端是基站(BS)，若是WLAN，则接入端是接入点(AP)。假设接入端与接入端服务器之间互信且有共享密钥或专有通路连接，故可将两者视作一个整体，记为接入认证服务器(Access Authentication Server，AAS)。AAS为MN提供服务且收费，但若MN每移动到一个地方就缴一次费，则带来太多不便，故而最好的方法是AAS向MN的归属服务器收费、归属服务器再向其用户收费。鉴于此，接入服务器与归属服务器各自所属的网络运营商之间要求有某种收费合同(本文假定所有合法服务器的运营商之间都有收费合同)，接入服务器与归属服务器之间要互相认证。另外，MN与其归属服务器为便于相互认证在建立归属关系时需共享秘密、互存对方信息。因此，归属服务器可被视为MN与接入认证服务器间的桥梁，统一记为归属网络认证服务器(Home network Authentication Server，HAS)。认证的消息用EAP，Radius或Diameter等协议进行封装，本文不作讨论。

在异构网络中，不同的接入认证服务器可能属于不同的网络运营商，若每一对接入认证服务器都共享一密钥，则不大现实；同时各运营商对安全的重视程度可能不同，因此很难保证密钥安全；另外，各运营商之间虽有计费合同，但不能保证没有抵赖发生；再者，随着性能的提高，无线终端已有能力进行较复杂的公钥加密。因此，本方案采用公钥基础设施，使得在既不需不同网络运营商间提供额外的信任管理功能，又不需用户端和网络端共享密钥的前提下，解决密钥管理和三方认证的问题。

3.2 认证协议用到的参数和运算

本协议所用到的参数有：

ID_A：A 的标识，包括 A 的位置等信息；SK_A：A 的私钥；PK_A：A 的公钥；Cert_A：A 的证书；$\mathrm{TID}_{\mathrm{MN}}$：AAS 为 MN 分配的临时身份；TS：时间戳；r_A：A 产生的随机数；$\mathrm{SA}_{\mathrm{MH}}$：MN 与 HAS 之间的共享秘密；sid 是唯一标识当前会话的会话标识。

用到的运算有：

$\mathrm{hash}(A)$ 表示 A 的哈希值，$\mathrm{ENC}(k,m)$ 表示用对称密钥 k 对 m 加密；$\mathrm{DEC}(k,m)$ 表示用对称密钥 k 对 m 解密，$E(\mathrm{PK},m)$ 表示用公钥 PK 对 m 加密；$D(\mathrm{SK},m)$ 表示用私钥 SK 对 m 解密；$\mathrm{sig}(\mathrm{SK},m)$ 表示用私钥 SK 对 m 签名。公钥加解密和数字签名方案采用椭圆曲线密码体制中的方案。

3.3 协议的设计

3.3.1 初始化过程

(1)各认证服务器(AAS 和 HAS)向证书授权机构 CA 注册：CA 或认证服务器选择椭圆曲线的参数组，然后认证服务器根据参数组产生公钥对，私钥自己留下，公钥交给 CA，且由 CA 生成 X.509 格式的公钥证书。由上可知，不同认证服务器的参数组可能不同。

(2)用户向 HAS 注册：HAS 为其分配唯一永久标识 $\mathrm{ID}_{\mathrm{MN}}$，并用自己的公钥参数产生用户的公钥对。并存储 $\mathrm{ID}_{\mathrm{MN}}$，HAS 的标识 $\mathrm{ID}_{\mathrm{HAS}}$，用户的公/私钥 $\mathrm{PK}_{\mathrm{MN}}/\mathrm{SK}_{\mathrm{MN}}$，HAS 的公钥 $\mathrm{PK}_{\mathrm{HAS}}$ 及椭圆曲线密码体制的参数 D 等信息到 MN 的智能卡中；销毁用户的私钥，同时存储用户的身份信息和公钥及相关计费信息等到自己的客户信息库中。

3.3.2 AM 中 SK-secure 的协议设计　当用户需要异构网络的服务时，移动终端 MN 和接入认证服务器 AAS 间就要进行认证。由于 MN 和 AAS 无预置的安全关联(Security association，SA)，因此 AAS 需通过 MN 的归属网络认证服务器 HAS 验证 MN 的身份，同时 MN 和 AAS 需协商安全的会话密钥。AM 中的认证过程如图 1 所示。

该协议的设计思想是：通过一次交互实现 MN 与 HAS、MN 与 AAS 以及 AAS 与 HAS 之间的相互认证。HAS 与 MN 通过预先存在的安全关联实现

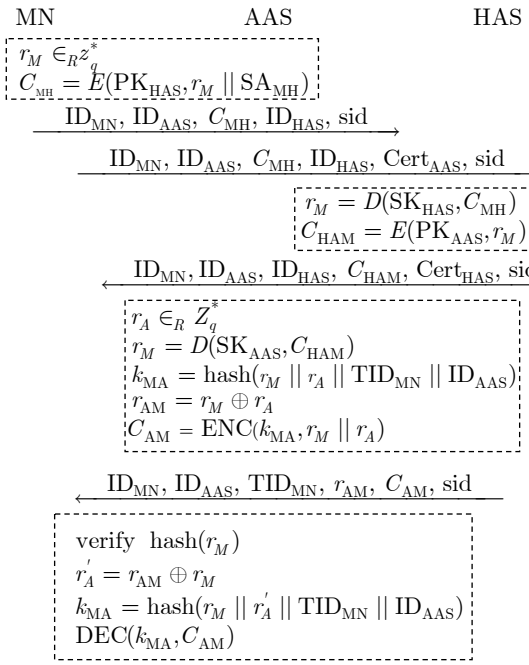

图 1 AM 中的认证协议

直接的相互认证，HAS 与 AAS 通过证书实现相互认证，而 MN 和 AAS 之间通过 HAS 建立动态的安全关联实现相互认证。在协议中 HAS 得不到 MN 与 AAS 之间的共享密钥，且 MN 与 AAS 之间具有显式密钥确认性质。

定理 2 在协议中的公钥加密方案，对称加密方案是 CPA 安全且难解的前提下，该协议在 AM 中是 SK-secure 的。

证明 首先证明该协议满足 SK-secure 定义的性质 1，在协议的交互过程中，当参与者均没被 KE 对手攻陷，完成了匹配的会话，则协议执行完毕时，MN 和 AAS 都得到了没有篡改的 r_M 和 r_A，从而计算出来的共享会话密钥是一致的，都为 $k_{\mathrm{MA}} = \mathrm{hash}(r_M \| r_A \| \mathrm{TID}_{\mathrm{MN}} \| \mathrm{ID}_{\mathrm{AAS}})$。因此该协议满足 SK-secure 定义的性质 1。

为了证明该协议满足 SK-secure 定义的性质 2，本文参照文献[5]的思想设计了算法 P，该算法将 KE 对手 A 作为子程序，P 和 A 交替来模仿协议的执行过程，并回答 A 的一切询问，并将协议的输出消息返回给 A。A 利用从协议中获得的能力控制着所有通信信道并负责调动所有的操作。鉴于篇幅所限，本文不再详细描述算法 P。

在算法 P 基础上采用反证法证明 SK-secure 定义的性质 2，假设存在 KE 对手 A 在 AM 中的认证协议执行过程中能以不可忽略的优势 ε 来区分会话密钥 k_{MA} 与一个等长的随机数。因为在 CK 模型中，KE 对手 A 不允许对 test-session 及其匹配的会话进行攻陷实体、暴露会话状态、查询会话密钥等攻击，所以 A 不能直接得到会话密钥 k_{MA} 而只能通过攻破用 k_{MA} 加密的数据或得到 k_{MA} 的组成元素再对其进行 hash 运算来得到。对于第 1 种情况，用到 k_{MA} 的有：AAS 向 MN 传递用对称密钥加密的数据 $C_{\mathrm{AM}} = \mathrm{ENC}(k_{\mathrm{MA}}, r_M \| r_A)$。设 A 攻破对称加密算法的上限为 $\varepsilon_{\mathrm{ENC}}$，则 A 得到 k_{MA} 的组成元素的概率至少为 $\varepsilon - \varepsilon_{\mathrm{ENC}}$。再分析第 2 种情况，$k_{\mathrm{MA}}$ 的组成元素为 $\mathrm{ID}_{\mathrm{AAS}}, \mathrm{TID}_{\mathrm{MN}}, r_M, r_A$ 4 项，其中 $\mathrm{ID}_{\mathrm{AAS}}, \mathrm{TID}_{\mathrm{MN}}$ 分别是 AAS 的身份和 MN 的临时身份标识，它们是以明文的形式在 AAS 与 MN 的会话中传递的，很容易被 A 获得；r_A 仅以异或式 $r_M \oplus r_A$ 的形式出现一次，实际上是用 r_M 作密钥对 r_A 进行加密，虽然加密方式简单，但 r_M 作为密钥仅此一次，属于一次一密，将其攻破是不可能的，因此攻击的重点应放在 r_M 上。若能得到 r_M，则由 $r_M \oplus r_A$ 可轻易得到 r_A。直接传递 r_M 的式子有 4 个：公钥加密的 $E(\mathrm{PK}_{\mathrm{HAS}}, r_M \| \mathrm{SA}_{\mathrm{MH}})$，$E(\mathrm{PK}_{\mathrm{AAS}}, r_M)$，用对称密钥加密的 $\mathrm{ENC}(k_{\mathrm{MA}}, r_A \| r_M)$ 及 $\mathrm{hash}(r_M)$，根据 hash 函数的性质，A 不能区分随机数和 r_M，因此 A 攻破其余三者之一即可得到 r_M。设非对称加密算法被攻破的概率上限为 ε_E，对称加密算法被攻破的概率上限为 $\varepsilon_{\mathrm{ENC}}$，则 A 获得 r_M 的概率上限为 $\varepsilon_{\mathrm{ENC}} + 2\varepsilon_E$。显见，$\varepsilon - \varepsilon_{\mathrm{ENC}} < \varepsilon_{\mathrm{ENC}} + 2\varepsilon_E$，即 $\varepsilon < 2\varepsilon_{\mathrm{ENC}} + 2\varepsilon_E$。因为 ε 不可忽略，所以 ε_E，$\varepsilon_{\mathrm{ENC}}$ 至少有一个不可忽略。这与加密算法是 CPA 安全且难解的前提相矛盾。因此，KE 对手区分 k_{MA} 与等长的随机数的概率不超过 $1/2 + \varepsilon$，优势 ε 是可忽略的，因此协议满足 SK-secure 定义的性质 2。

所以，根据SK-secure定义，该协议在语义上是SK-secure的。 证毕

3.3.3 协议认证器的构造 本文采用了 4 种不同安全的 MT-authenticator：

(1)MN与HAS采用基于公钥加密的ENC协议(如图2所示)来保护加密信息，该协议已被Canetti和Krawczyk[5]证明在AM中是安全的，通信方有对方的公钥，其中 $\mathrm{SA}_{\mathrm{MH}}$ 为MN与HAS共享的秘密信息。

(2)HAS与AAS之间利用公钥加密的方式来保护交换的信息，因此，采用基于数字签名和随机数的MT-authenticator(如图3所示)仿真HAS到AAS的消息流。接收方B接受信息m仅当签名正确。该MT-authenticator的安全证明参见文献[6]。

(3)MN与AAS之间采取动态生成共享对称的加

图2 ENC协议

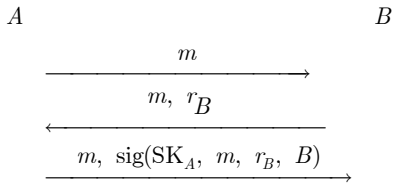

图3 基于数字签名和随机数的MT- authenticator

密密钥，因此采取基于消息验证码MAC的MT-authenticator(如图4所示)来实现双方的认证。该MT-authenticator的安全证明见文献[6]。

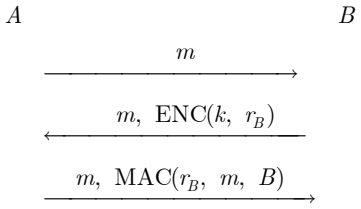

图4 基于MAC的MT-authenticator

(4)AAS需要提供对HAS的不可否认性，所以使用基于时间戳的签名MT-authenticator(如图5所示)仿真AAS到HAS的消息流，其中时间戳由一个所有实体都可访问的全局时间服务器来提供，用于保证消息的新鲜性。该MT-authenticator的安全证明见文献[7]。

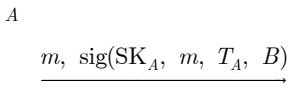

图5 基于时间戳的签名MT-authenticator

3.3.4 UM 中的安全协议　将上述 4 种 MT-authenticator 分别应用于 AM 中协议的每个消息流，同时本文在不影响协议的可证安全性的前提下，将 MN 的身份标识隐藏起来，使得其他恶意方无法获知其身份信息。然后应用文献[8]的方法优化 UM 中的协议，最后仿真得到如图 6 所示的 UM 中的协议。由于所采用的 MT-authenticator 是可证安全的，所以根据 CK 模型方法自动编译得到的 UM 中的协议也是可证安全的。

对协议的一些说明：

(1)当 MN 首次移动到异构的无线网络时，MN 利用 HAS 的公钥加密自己的身份 $\mathrm{ID_{MN}}$、与 HAS 的共享信息 $\mathrm{SA_{MH}}$、时间戳和 AAS 的身份 $\mathrm{ID_{AAS}}$、用于认证 AAS 的随机数 r_M，分别用于实现用户身份保密、实现 HAS 对 MN 的认证、防止重放攻击，以及解决 AAS 与 MN 之间由于没有预置 SA 造成的 AAS 无法直接获知 r_M 等问题。

(2)HAS 从 AAS 收到消息后，首先解密 C_{MH}，验证解密后的时间戳是否在有效的范围内以及 $\mathrm{ID_{MN}}$ 是否与 $\mathrm{SA_{MH}}$ 对应，如正确，则 HAS 可确定该信息是 MN 发出的；然后比较解密得到的 $\mathrm{ID_{AAS}}$ 与证书上的主体标识；若一致，则进一步验证签名 C_{AH}；若签名正确，则再验证 AAS 证书是否有效。若上述均通过，则可认为 AAS 是给 MN 提供服务的合法的认证服务器，而后 HAS 用 AAS 公钥加密 MN 的相关信息：r_M，$\mathrm{ID_{MN}}$ 和 $\mathrm{PK_{MN}}$，并发给 AAS。

(3)AAS 在收到 HAS 发来的消息后，首先验证签名 C_{HA}；若正确，则验证 HAS 的证书是否有效。若上述均通过，则可认为 HAS 是合法的认证服务器。为了不暴露 MN 的身份又能在特定范围内找到 MN，用 $\mathrm{hash}(r_M)$ 的前 64 位(记为 $\mathrm{hash}^*(r_M)$)代替 $\mathrm{ID_{MN}}$ 给 MN 发送信息。

(4)因在会话过程中，加密和完整性校验都不可缺，将 MN 和 AAS 之间的动态对称密钥 $k_{\mathrm{MA}} = \mathrm{hash}(r_M \,||\, r_A \,||\, \mathrm{TID_{MN}} \,||\, \mathrm{ID_{AAS}})$ 划为两部分，取前 128 bit 作为 MN 与 AAS 会话的加密密钥，取后 64 bit 作为 MN 与 AAS 会话的完整性密钥，在后续的通信过程中，用 $\mathrm{ENC}(k_{\mathrm{MA}}, m)$ 表示用 k_{MA} 前 128 位加密 m，后 64 位求出加密结果的完整性校验值；用 $\mathrm{DEC}(k_{\mathrm{MA}}, s)$ 表示先用 k_{MA} 的后 64 位进行完整性校验，正确后再用前 128 位解密。

(5)当 MN 收到 AAS 发来的信息后，由 r_{AM} 异或出 r_A，并生成对称密钥 k_{MA}，解密 C_{AM} 后验证 r_M 和 r_A，若相符，则说明 HAS 已认为 AAS 是合法的，并把自己的相关信息传给了 AAS，并且等价于确认 MN 已生成了会话密钥；MN 获得 AAS 分配的临时标识 $\mathrm{TID_{MN}}$。

(6)AAS 收到信息后，解密 C_{AM} 并验证签名 C_M，若正确，则 AAS 认为 MN 是 HAS 的合法用户，用 k_{MA} 作会话密钥为 MN 提供服务。MN 可在一定的时间间隔产生 $\mathrm{ID_{MN}}$ 和当前时间戳的签名作为正在接受服务的证明。AAS 保存 MN 的 $\mathrm{ID_{MN}}$，$\mathrm{PK_{MN}}$，对应的时间戳和签名 C_M，作为向 HAS 收费的凭证。

(7)协商完毕后，认证各方删除用过的随机数。

4 安全和性能分析

4.1 协议安全性分析

所得到的协议具有的安全属性如下：

(1)三方相互认证：　HAS 信任 MN 当且仅当 MN 发来的时间戳有效且共享秘密 $\mathrm{SA_{MH}}$ 正确。HAS 信任 AAS 当且仅当 AAS 发来的包含新信息的签名 C_{AH} 是可验证的。AAS 信任 HAS 当且仅当 HAS 发

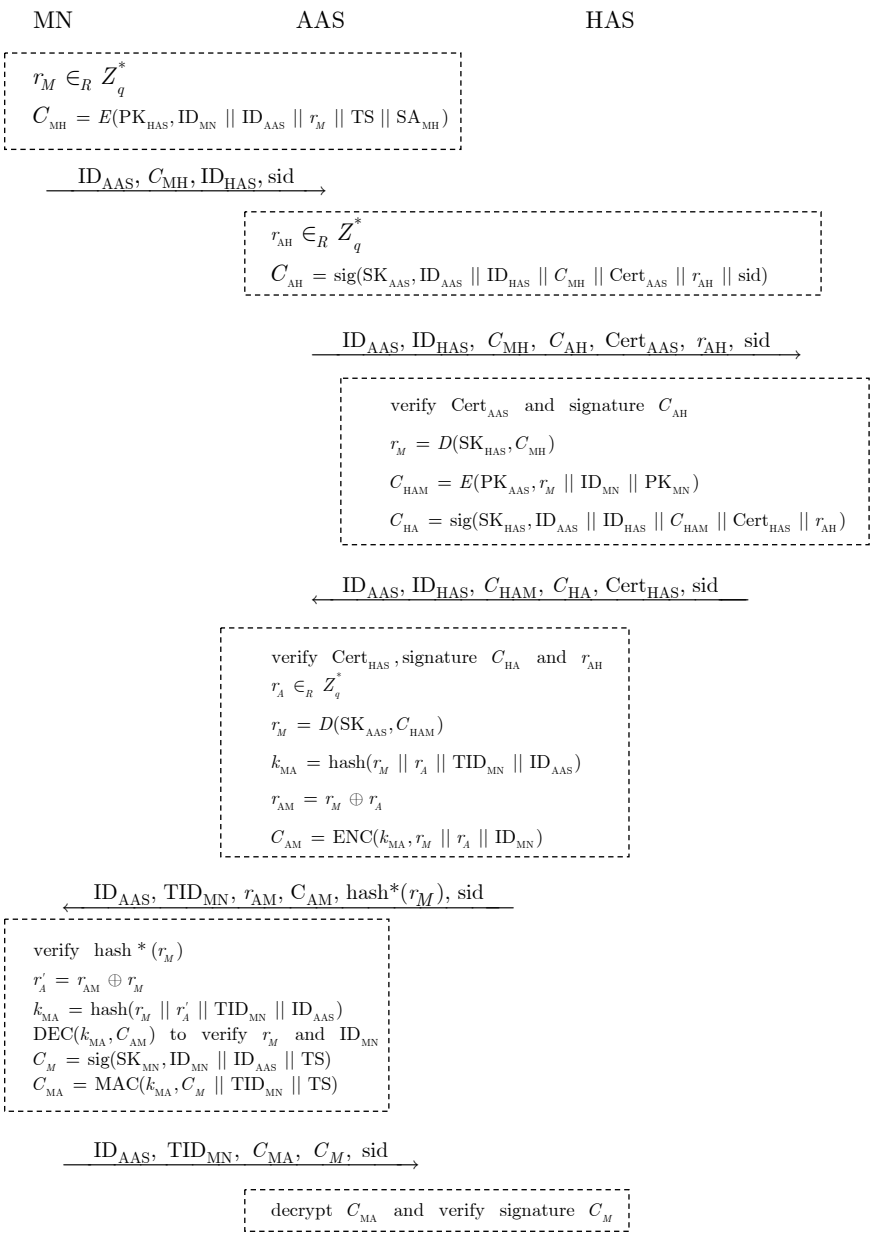

图 6 UM 中的认证协议

来的包含随机数 r_{AH} 的签名 C_{HA} 是可验证的。AAS 与 MN 相互信任当且仅当 MN 和 AA 返回给对方的随机数 r_A 和 r_M 是正确的。MN 信任 HAS 当且仅当 HAS 返回 AAS，AAS 返回 MN 的 r_M 是正确的。

(2)密钥安全性保护： 该协议除了定理 1 的密钥安全性之外，还具有如下性质：

会话密钥的不可控性：MN 与 AAS 间的会话密钥 k_{MA} 是由 MN 和 AAS 分别产生的随机数 r_M, r_A 和相关信息共同产生的，故任何一方都不能预先控制会话密钥的生成。

完美的前向保密性(PFS)：协议中会话密钥与 MN 和 AAS 产生的随机数有关，这些随机数用过即被删出，那么即使暴露 MN 和 AAS 的私钥，也不能恢复这些随机数，因此，以前所协商的会话密钥也不能被攻破。

(3)用户的身份和位置的机密性： 移动用户的身份 $\mathrm{ID}_{\mathrm{MN}}$ 自始至终不以明文形式在网络传输，且 AAS 只有在身份被认证后方可获得 MN 的永久身份 $\mathrm{ID}_{\mathrm{MN}}$，KE 对手 A 只有获得 HAS 或 AAS 的私钥并解密相应信息后才能获得 MN 的真实身份，这是 ECDLP 难题。同时在完全认证后，用户的临时身份 $\mathrm{TID}_{\mathrm{MN}}$ 将被用来标识用户且代替真实 $\mathrm{ID}_{\mathrm{MN}}$ 传输，增加了 $\mathrm{ID}_{\mathrm{MN}}$ 的隐密性，而且 $\mathrm{TID}_{\mathrm{MN}}$ 可根据需要重新分配。因此，攻击者无法获得用户的身份和位置信息，保证了用户身份和位置的机密性。从而可有效地防止针对特定用户的跟踪和拒绝服务攻击。

(4)抗抵赖性:HAS 发送给 AAS 的签名,使 HAS 不能否认其与 MN 的从属关系; MN 发送给 AAS 的签名,确保其不能否认曾接受 AAS 的服务且拒绝付费。

(5)完整性保护: MN, AAS, HAS 对消息的签名, 可有效地确保传输数据的完整性。

(6)防重放保护: MN, AAS 产生的随机数及时间戳保证了认证信息的新鲜性和传输的数据不被重放。

4.2 性能分析

4.2.1 计算开销 表 1 列出了各实体的相关运算的计算量, 不难看出, 各实体的计算开销均较小。为了减少 MN 公钥计算所需的时间, 本文利用了椭圆曲线公钥体制, 在不减低安全性的前提下, 计算量大大减少, 计算速度也明显提高, 并且签名长度也大大缩短了; 另外, MN 与 AAS 主要采用对称加解密运算, 具有较小的计算量, 有利于提高认证协议的运行效率, 因此本模型具有较高的实用价值。

4.2.2 存储和通信开销 该方案采用 3 种方法节省移动终端的存储:

(1)MN 不存储自己的公钥证书, 而是在 AAS 被 HAS 认证后, 由 HAS 将 MN 的公钥传给 AAS。

(2)MN 不需要知道 AAS 的公钥信息, 避免了 MN 存储与自己公钥参数不同的 AAS 的公钥信息。

(3)MN 采用 ECC 进行加密、签名, ECC 的密钥所占的存贮空间相较于 RSA, DSA 要小得多。

该方案因不需在资源有限的无线链路上传递证书, 从而减少通信开销。

表 1 各实体的计算开销

运算	MN	AAS	HAS
随机数生成次数	1	2	0
MAC 次数	1	0	0
hash 函数次数	1	1	0
签名和验签	1/0	1/1	1/1
对称加解密	1/1	1/0	0/0
公钥加解密	1/0	1/1	1/1

5 总结

本文对 3G-WLAN 互联的异构网络的多种网络模型进行分析, 抽象出不依赖于具体异构网络的认证实体, 建立了一个通用的认证模型, 并在该模型的基础上利用可证安全的 CK 模型, 设计出一个基于公钥体制的认证与密钥分配协议, 解决了网络扩展时的密钥分配与存储问题及签名的不可否认等问题。该协议采用椭圆曲线进行加解密和签名, 相比于其它公钥加密和签名算法, 各实体的计算量降低; 利用证书实现接入认证服务器与归属网络认证服务器间的身份认证并帮助移动终端认证接入认证服务器, 使移动终端不用传递自己的证书和验证接入认证服务器的证书, 就能实现双向认证, 减轻移动终端的工作量, 节省无线带宽; 而且通过对移动终端的身份信息进行加密, 确保了其身份和位置的保密性。最后安全性分析和证明了协议具有的安全属性, 性能分析研究表明该协议具有计算量小、效率高、存储开销低和通信量小的特点。

参 考 文 献

[1] Simon D, Aboba B, and Hurst R. The EAP-TLS authentication protocol. RFC 5216, IETF, 2008.

[2] Manulis M, Leroy D, and Koeune F. Authenticated wireless roaming via tunnels: making mobile guests feel at home. http://eprint.iacr.org/2008/382. pdf, 2008.

[3] 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 identity-based authentication model for multi-domain[J]. *Chinese Journal of Computers*, 2006, 29(8): 1271–1281.

[4] Vivek K and Vivek S A. Elliptic curve cryptography[C]. www.acm.org/ubiquity/volume_9/pf/v9i20_singh.pdf. ACM Ubiquity, 2008.

[5] Canetti R and Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels (Full Version), http://eprint.iacr.org. 2001.

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

[7] Tin Y S T, Vasanta H, Boyd C, and Nieto J M G. Protocols with security proofs for mobile applications[C]. Proceedings of the ACISP 2004, Sydney, July. 13–15, 2004: 358–369.

[8] Tin Y S T, Boyd C, and Nieto J G. Provably secure key exchange: an engineering approach[C]. Proceedings of the Australasian Information Security Workshop (AISW2003), Australasian, 2003: 97–104.

侯惠芳: 女, 1972 年生, 副教授, 博士生, 研究方向为无线通信、信息安全.

刘光强: 男, 1978 年生, 硕士生, 研究方向为信息安全、无线通信.

季新生: 男, 1968 年生, 教授, 博士生导师, 研究方向为移动通信、信息安全.