匿名双向认证与密钥协商新协议

万仁福，李方伟，朱 江

(重庆邮电学院移动通信工程研究中心 重庆 400065)

【摘要】分析了一种新的匿名双向认证与密钥协商协议，它使移动网络向用户提供匿名服务，访问网络与非法窃听者无法获知用户的身份信息，保证了用户身份、所在位置和行踪信息的机密性。该协议可以实现通信双方的相互认证，产生的会话密钥对通信双方是公正的。协议将双钥体制和单钥体制有机的结合起来，结构简单，安全高效。

关 键 词 匿名； 双向认证； 密钥协商； 公钥基础设施

中图分类号 TN92 文献标识码 A

An Efficient Anonymity Mutual Authentication Protocol

WAN Ren-fu，LI Fang-wei，ZHU Jiang

(The mobil Communication Engineer Research Center, Chongqing University of Post & Telecom Chongqing 400065)

Abstract This article analyzes an efficient protocol for anonymous mutual authentication and key agreement. In the protocol, a mobile user can be provided with anonymous service and neither Visited networks nor eavesdroppers know the information of the user's real identity, preserving the privacy of real identity, current location and movement patterns information of users. This scheme can realize mutual authentication and the session key established by the protocol is fair for both side of communication.

Key words anonymity; mutual authentication; key agreement; pubic key infrastructure

无线通信技术的迅速发展使移动通信以及以移动网络为平台的应用得到越来越多的重视和推广，在未来移动通信系统中，除提供话音服务外，还将提供多媒体、电子商务、网上银行等业务，这对网络的安全性、可靠性提出了更高、更迫切的要求。加密技术是实现安全通信的核心，而身份认证与密钥分配是实现正常安全通信、保护用户与运营商利益的重要保证。作为呼叫建立过程的一部分，身份认证和密钥协商协议在其中起着举足轻重的角色。如果身份认证和密钥协商协议出现安全漏洞，整个会话就没有安全性，还会危及随后会话的安全性。

用户真实身份、当前位置及其运动模式是重要而又敏感的信息，在通信中必须保证它们的机密性[1]。由于移动用户与通信网之间采用无线通信，用户的身份认证必须通过无线信道来进行，因此易受截获、窃听和攻击。在全球移动通信系统(Global Systems for Mobile communications, GSM)和3G的认证方案中[2]，使用临时身份标识(Temporary Mobile Subscriber Identify，TMSI)来鉴别用户，提供了一定程度的匿名性。但当用

收稿日期：2003－07－04

基金项目：重庆市教委科学技术研究项目(020507)

作者简介：万仁福(1975－)，男，硕士生，主要从事移动通信方面的研究；李方伟(1960－)，男，教授，主要从事移动通信方面的研究；朱 江(1977－)，男，硕士生，主要从事移动通信方面的研究.

户第一次注册到一个服务网络或无法从TMSI中得到IMSI(International Mobile Subscriber Identity)，国际移动用户标识时[3]，服务器向用户发送IMSI请求，用户的应答是包含IMSI信息的纯文本，易造成IMSI的泄漏，违背了用户身份的保密性。因此GSM和3G的认证方案都没有提供真正的匿名性。基于此本文提出了一种匿名双向认证与密钥协商新协议。

1 匿名双向认证与密钥协商协议

在协议描述中，用户的真实身份为A，为了保护用户身份A的机密性，归属网络为每个用户分配一长期化名Alias作为标识，用S表示归属服务器的身份信息，归属服务器和用户的共享密钥为K，从Alias中可推导出S。归属服务器保存了Alias与A及K的映射关系；归属服务器的公钥证书为$Cert(S)$，私钥为SK_S，公钥为PK_S；外地服务器的公钥证书为$Cert(V)$，私钥为SK_V，公钥为PK_V；Mac为消息认证码函数，h为计算会话密钥函数。下面分两种情况对协议进行详细描述。

1.1 在归属网络匿名双向认证与密钥协商过程

当用户想从归属服务网络中得到服务时，他和归属服务网络先执行认证与密钥协商协议。认证是基于它们之间的共享密钥K。执行过程如图1所示，具体如下：

1) 用户产生一随机数N_A并用密钥K加密N_A得$E_K(N_A)$，把$E_K(N_A)$和Alias一同发送给归属服务器。

2) 收到报文(1)后，归属服务器检查报文第一段Alias看是否是自己的用户。若是，则把Alias映射到用户真实身份A并从数据库中查找共享密钥K。用K解密$E_K(N_A)$得到随机数N_A。另外产生一随机数N_S，用消息认证码函数Mac计算$Mac_K(N_S, A)$，并计算它和用户共享的会话密钥$K_{se}= h(N_A, Mac_K(N_S, A))$，计算$Mac_K(N_A, N_S, S)$、$E_K(Mac_K)\oplus N_S$和$E_{K_{se}}(N_S)$后随同$N_A$一起发送给用户，如图1所示。

3) 用户收到报文(2)后，检查报文发现其中有N_A，即停止接收其他报文。用共享密钥K加密报文第二段得$E_K(Mac_K)$并与第三段$\{E_K(Mac_K)\oplus N_S\}$异或，得到N_S。计算$Mac_K(N_A, N_S, S)$并与报文的第二段比较，以验证报文的有效性，达到认证归属服务器的目的，如果不等则放弃认证过程。若验证通过，用户则用与归属服务器相同的方法计算会话密钥K_{se}。为避免重放攻击(Replay Attack)，计算$E_{K_{se}}(N_S-1)$并发送给归属服务器。归属服务器收到报文(3)后，通过对报文(3)的验证认证了用户，并确认用户知道会话密钥。至此，用户与归属服务器完成了相互认证、密钥协商和密钥确认过程。

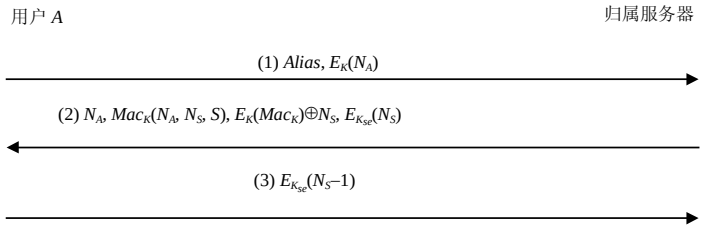

图1 在归属网络认证与密钥协商过程

1.2 在访问网络匿名双向认证与密钥协商过程

当用户漫游到外地时，需要在归属服务器的协助下，向外地服务器证明自己身份的合法性，才能接入外地网络获得所需服务。每个服务器各有一公/私钥对，公钥和私钥通过一种非常重要的原理在数学上相互关联，但不可能从其中一个来推出另一个，并拥有信任的第三方(Trusted Third Party，TTP)颁发的公钥证书。公钥证书把每个服务器的身份信息和公钥绑定起来。各个服务器的公钥证书可能是由不同的证书管理机构(Certification Authority，CA)颁发的，但这些CA在认证方面都属于一全局的公钥基础设施(Public Key Infrastructure，PKI)。而且各CA由一全局CA分级管理，服务器之间通过证书链方式得到对方公钥，使用时可把它看作一个整体。协议的执行过程如图2所示，具体如下：

1) 用户产生一随机数N_A，并用密钥K加密N_A得$E_K(N_A)$，把$E_K(N_A)$和Alias一同发送给外地服务器。

2) 外地服务器收到报文后，检查报文第一段Alias，找到用户归属服务器的身份信息S，随后产生一随机数N_V，用私钥SK_V对其签名得$\{N_V\}_{SK_V}$，把它随自己的公钥证书$Cert(V)$及报文(1)一起转发给归属服务器。

3) 接收到报文(2)后，归属服务器检查$Cert(V)$证实外地服务器的身份，用外地服务器的公钥PK_V解密$\{N_V\}_{SK_V}$得到N_V，并用与归属网络认证相同的步骤映射Alias到用户真实身份A和找到共享密钥K，用K解密$E_K(N_A)$得到数N_A。另外产生一随机数N_S，计算$Mac_K(N_S, A)$等相关消息，用自己的私钥SK_S对$\{N_V, N_A, Mac_K(N_A, N_S, S), E_K(Mac_K) \oplus N_S, Mac_K(N_S, A), N_S\}$数字签名，签名信息与公钥证书$Cert(S)$一起用外地服务器的公钥$PK_V$加密后发送给外地服务器。

4) 外地服务器收到报文后，用自己的私钥SK_V解密报文(3)，检查$Cert(S)$得到归属服务器的公钥PK_S，用PK_S解密数字签名信息，得到计算会话密钥K_{se}所需的N_A、$Mac_K(N_S, A)$等信息。而后计算会话密钥$K_{se}= h(N_A, Mac_K(N_S, A))$和$E_{K_{se}}(N_S)$，并把报文(4)发送给用户。

5) 用户收到报文(4)后，检查报文发现其中有N_A，即停止接收其它报文。用与归属网络认证相同的方式得到N_S，计算$Mac_K(N_A, N_S, S)$，并与报文(4)的第二段比较，以验证报文的有效性，达到认证服务网络的目的，如果不等则放弃认证过程。若验证通过，用户则用与外地服务器相同的方法计算会话密钥K_{se}。为避免重放攻击，计算$E_{K_{se}}(N_S - 1)$并发送给外地服务器。外地服务器收到报文(5)后，通过对报文(5)的验证认证了用户，并确认用户知道会话密钥。至此，在外地网络的认证与密钥协商过程结束。

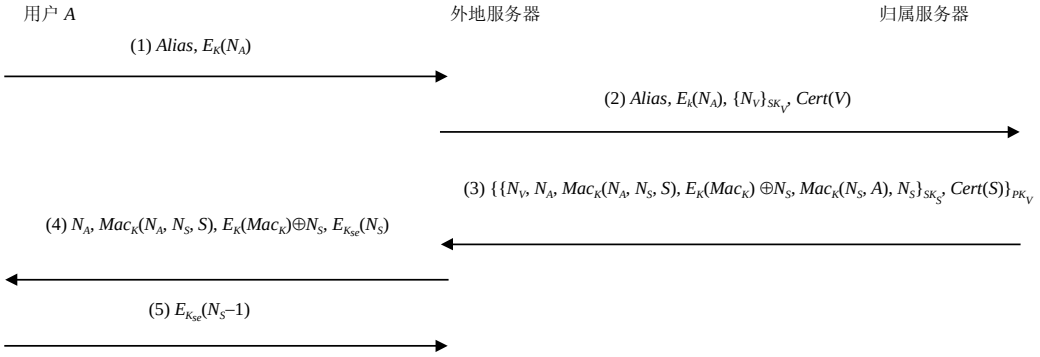

图2　在外地网络认证与密钥协商过程

2　协议的性能分析

2.1　用户与服务器之间密钥的安全性、新鲜性和公正性[4]

用户在计算出N_S后，用服务器相同的方法产生会话密钥K_{se}，K_{se}用于其后的保密通信且未在无线接口中传输，确保了密钥的安全性。另外，由于每次通信前的认证选择了不同的随机数N_A、N_S计算会话密钥，用户与服务器每次通信均采用不同的会话密钥，从而确保了密钥的新鲜性，有效地防止了重放攻击。会话密钥由N_A、N_S共同决定，任何一方都不能单独产生会话密钥，保证了密钥的公正性。

2.2　移动终端计算负荷较少

单钥密码技术较成熟，算法也较简单，因而单钥体制计算复杂度低，易于实现。然而单钥密码方案要求保密通信双方必须共享密钥，存在密钥安全管理的问题；双钥体制不要求通信双方事先共享密钥，但公钥密码算法比较复杂，计算量大。本协议充分考虑了移动终端运算能力相对较弱、存储量小，在用户端采用对称加密；而服务器拥有比较充足的计算、存储资源，因而在归属服务器和外地服务器之间采用公钥加密，以解决密钥分发和安全管理难的问题。将双钥体制和单钥体制有机的结合起来，既满足了安全要求，又减少了终端的计算负荷。

2.3 用户的匿名性

在本协议中，用永久Alias隐藏用户的真实身份。Alias仅在用户向服务器发起认证过程的报文中，而服务器发给用户的应答是含有随机数N_A的报文。除用户本人外，任何人都不知道该报文是发给谁的，保证了用户身份的机密性。匿名性能抗击针对某一特定用户的拒绝服务攻击。在访问网络，用户的真实身份和共享密钥未在归属服务器和外地服务器之间传输，确保了用户真实身份和共享密钥的安全性。

2.4 双向认证[5]

双向认证的目的是为了保证协议所涉及的通信实体是合法的。通过服务器对用户的认证，防止攻击者假冒合法用户占用网络资源；通过用户对网络的认证，防止假冒服务器的攻击。在会话密钥建立过程中，用户计算Mac_K (N_A，N_S，S)并于服务器响应报文的第二段比较达到认证服务网络的目的。因为只有合法服务器能计算或获得此消息。服务器通过对报文$E_{K_{se}}$ (N_S −1) 的验证认证了合法用户。因为只有合法用户能计算出N_S和会话密钥。攻击者若要假冒合法用户，他截获报文(1)并转发给服务器，但没有随机数N_A来识别报文(2)，也无法获得参数K和N_S来产生报文(3)，所以攻击者假冒用户是不可能的。在归属网络，攻击者若要假冒服务器，即使他转发报文(2)给用户，也计算不出会话密钥。所以假冒归属服务器进行攻击也是不可能。在访问网络，攻击者若要假冒外地服务器，由于他没有信任的第三方颁发的公钥证书和私钥SK_V而无法解密报文(4)，所以这种攻击也是不可能的。相互认证机制有效的保证了用户与运营商双方的利益。

3 结 论

本协议把双钥体制和单钥体制有机的结合起来，既体现了移动通信协议尽可能采用对称加密以减少认证时延的特点，又体现了Internet协议多采用公钥加密以利于密钥分配的特点，能满足通信双方进行相互身份认证的要求，又能为通信双方分配一个公正的、新鲜的和经过双方认可的会话密钥。协议最大程度地保证了用户身份和所在位置信息的机密性，结构简单，安全高效，适用于未来的数字移动通信系统。

参 考 文 献

[1] 3GPP TS21.133, 3G Security: Security Threats and Requirements[S]. Release 2000, 14-15

[2] 1Rahnema M. Overview of GSM system and protocol architecture[J]. IEEE Communications Magazine, 1993,31(4): 92-100

[3] 3GPP TS33.102, 3G Security: Security Architecture[S]. Release 5, 2000, 17-18

[4] Mohammed G R, Hideki I. Security in wireless communication[J]. Wireless Personal Communications, 2002, 22(2): 213-228

[5] Molva R, Samfat D, Tsudik G. Authentication of mobile users[J]. IEEE Network Special Issue in Mobile Communication, 1994, 8(2): 26-34

编 辑 漆 蓉