个人通信系统中的一种移动用户登记认证协议 [1]

刘建伟 王育民

(西安电子科技大学 106 信箱 西安 710071)

摘 要 假冒和窃听攻击是无线通信面临的主要威胁. 在个人通信系统中, 为了对无线链路提供安全保护, 必须对链路上所传送的数据 / 话音进行加密, 而且在用户与服务网络之间必须进行相互认证. 近年来, 人们在不同的移动通信网络 (如 GSM, IS-41, CDPD, Wireless LAN 等) 中提出了许多安全协议. 然而, 这些协议在个人通信环境中应用时存在不同的弱点. 本文基于个人通信系统的双钥保密与认证模型, 设计了用户位置登记认证协议; 并采用 BAN 认证逻辑对协议的安全性进行了形式化证明, 也对协议的计算复杂性进行了定性分析. 分析表明, 所提出的协议与现有的协议相比具有许多新的安全特性.

关键词 个人通信系统, 认证协议, BAN 逻辑

中图号 TN929.5, TN918, TN913.22

1 引 言

在个人通信系统 (Personal Communication System, PCS) 中, 移动用户与固定网络间的无线链路极易受到诸如窃听和假冒等各种类型的攻击. 因此, 必须采用加密和访问控制等安全措施对无线链路进行安全保护. 原则上讲, 通过设计安全的保密与认证 (Privacy and Authentication, P&A) 协议对无线链路两端的通信实体进行身份认证, 并在它们之间建立起一个秘密的会话密钥就可以达到这个目的.

GSM(Global Service for Mobile) 是第一个实现保密通信的系统 [1] . 它的 P&A 协议采用了 "问 - 答" (Challenge-Response) 机制. 虽然该协议具有很高的运行速度, 但其存在着安全缺陷. 首先, 认证是单向的, 即只有网络对移动用户进行认证, 而对移动用户来说, 始终假设服务网络是合法的. 这个假设对于 PCS 这样一个全球性的网络来说很难成立. 此外, 访问网络 VN(Visited Network) 对用户的认证需要用户的归属网络 HN(Home Network) 的参与. 这就出现了两个问题: 一是必须假设用于 VN 与 HN 进行数据交换的骨干网 BN(Backbone Network) 是安全的, 否则, 由 HN 送给 VN 的三元组 (K_c, Rand, SRES) 可能被截获. 攻击者就会借此假冒合法的网络 (基站) 与该用户建立连接以获取用户的某些秘密 (如用户的真实身份) ; 二是 VN 与 HN 的数据交换必然引起系统信令负荷的增加. 由于在 PCS 中采用了混合小区 (宏小区、微小区和皮小区) 结构, 用于系统管理的信令负荷猛增, 可能会成为影响系统性能的瓶颈. 因此, 如何减少由于安全措施的引入所带来的信令负荷, 是 PCS 中要考虑的问题.

与 GSM 所采用的 P&A 协议相类似的系统还有北美的 IS-41 和欧洲的 DECT .

在文献 [2] 中, 作者提出了一种完全基于单钥加密体制和安全杂凑函数的 P&A 协议. 该协议成功地取消了有关骨干网安全的假设, 增加了用户对访问网络的认证功能. 但该协议仍然存在着缺陷: 一是真正意义上的用户身份保密没有做到; 二是 VN 与移动用户之间的相

[1] 1996-10-10 收到, 1998-11-08 定稿

互认证仍然需要 HN 的参与；三是用户与 VN 之间， VN 与 HN 之间进行数据处理时所采用的杂凑算法和加密算法必须是事先协商好的，这就降低了系统的灵活性。

要取消 P&A 协议中 HN 的参与，就必须采用双钥加密体制。双钥体制的采用简化了网络的密钥管理，使系统的安全性得以提高。然而，采用双钥体制也存在不利的因素，突出表现在计算负荷的增加和对公钥证书 (Public Key Certificate) 的管理上。

文献 [3] 提出了一种基于双钥体制的 MSR+DH 协议。此协议虽然具有用户身份保密的能力，也可以实现通信双方的相互认证，但是却不能有效地防止假冒攻击。一旦攻击者获得了某个合法用户 / 网络的证书，他就可以永久地假冒该用户 / 网络直到该证书作废。克服此类假冒攻击的有效方法是使用数字签名技术。

文献 [4] 提出了一种适用于无线局域网的 P&A 协议。由于协议采用了数字签名技术以防止假冒攻击，从而具有很高的安全性。但是它也存在着另一问题，即协议执行过程中，通信双方各需进行两次与各自私钥有关的大量计算。这对于无线局域网来说是合适的，但对于 PCS 来说，由于通信双方具有不对称的计算能力和资源，所以不能直接使用。

为了尽可能地减少移动用户端的计算负荷，人们尝试采用双钥 / 单钥混合方案来构造 P&A 协议。在文献 [5] 的协议中，作者就采用了双钥加密体制、单钥体制和杂凑函数算法。用户端仅需进行简单的双钥加密及单钥体制的加 / 解密运算，而将复杂的双钥解密运算留给网络去做。然而，此协议也存在着安全缺陷，体现在以下两方面：第一，认证过程仍需要 HN 的参与；第二，移动用户和 HN 没有对 VN 实施认证。

综上所述，现有的许多协议是基于不同的安全假设、采用不同的技术而设计的，因此对于不同的应用环境，具有各自的优缺点。本文在对现有协议进行了深入分析的基础上，针对移动用户位置登记进程对 P&A 的要求，采用双钥 / 单钥混合体制，设计了相应的用户登记认证协议。

2　新的用户登记认证协议

为了便于对协议进行描述和分析，在下面将移动用户用 A 来表示，而将访问网络用 B 来表示。在后面对协议的描述中，所谓的访问网络均是指访问网络中的认证服务器。

首先对后面的协议中采用的符号作如下定义： $E_p\{X;Y\}$ 为采用公钥 X 对消息 Y 进行双钥加密； $E_S\{X;Y\}$ 为采用密钥 X 对消息 Y 进行单钥加密； $h(X)$ 为不含密钥的消息 X 的杂凑函数值 (Message Digest Code, MDC) ； P_a 为移动用户的公钥； P_a^{-1} 为移动用户的私钥； P_b 为访问网络认证服务器的公钥； P_b^{-1} 为访问网络认证服务器的私钥； Cert$A$ 为移动用户的证书； Cert$B$ 为访问网络认证服务器的证书； ListOfAlg 为网络所支持的算法清单； ChosenAlg 为用户所选定的算法； LAI 为用户所处位置区识别号； $\mathrm{Sig}\{X;Y\}$ 为用私钥 X 对消息 Y 的杂凑函数值 $h(y)$ 进行签名。

当一个用户漫游到一个新的位置区域时，就会引发此协议的执行，以便进行位置登记。此阶段用户与认证服务器之间所交互的步骤如下：

消息 1 访问网络 $\longrightarrow$ 移动用户

{Cert$B$, N_b, LAI, ListOfAlg}

访问网络的某个基站通过广播信道广播它的证书链 Cert$B$ ，为下一个呼叫所产生的一次随机数 N_b ，位置区识别号 LAI ，以及它所支持的单钥算法清单 ListOfAlg 。

移动用户在收到消息 1 后，首先对 Cert$B$ 进行检验．如不正确，则认为访问网络不合法，中断协议；如正确，则认为公钥 K_B 为某一合法网络的公钥．但是，至此还不能确定是否为某个非法网络在窃得 Cert$B$ 后所进行的假冒攻击．

此后，用户产生随机数 K_{ab}，选定单钥算法 ChosenAlg，进行相应的双钥加密和数字签名运算，将消息 2 发送给访问网络．

消息 2 移动用户 $\longrightarrow$ 访问网络

$\{E_p[K_b; \mathrm{Cert}A, K_{ab}]$, ChosenAlg,

$\mathrm{Sig}\{K_a^{-1}; \{N_b, E_p[K_b; \mathrm{Cert}A, K_{ab}]$, ChosenAlg, ListOfAlg$\}\}$.

访问网络在收到消息 2 后，首先采用它的私钥 P_b^{-1} 对 $E_p[K_b; \mathrm{Cert}A, K_{ab}]$ 解密 (注意，若此访问网络是假冒的，它就不会知道私钥 P_b^{-1}，因此就不会正确地解密) 求出用户的证书链 Cert$A$ 以及 K_{ab}．然后，访问网络对 Cert$A$ 加以验证．若不正确，则用户是非法的，中断协议；若正确，则认为 K_a 为某个合法用户的公钥．但是，至此还不能确定是否为某个非法用户在窃得合法用户的 Cert$A$ 后所进行的假冒攻击．访问网络只要对数字签名项进行验证就可以加以确认．

在得到确认后，访问网络将 K_{ab} 加以存储，并作为与用户共享的秘密．值得强调的是，假冒用户不会正确地得到 K_{ab}，因此也不会正确地进行消息 3 的计算．

消息 3 访问网络 $\longrightarrow$ 移动用户

$\{E_s[K_{ab}; K_{ba}], \mathrm{Sig}\{K_b^{-1}; \{K_{ba}, E_p[K_b; \mathrm{Cert}A, K_{ab}]\}\}\}$.

访问网络生成一次随机数 K_{ba}，并进行单钥加密运算和数字签名运算．之后，将消息 3 发送给移动用户．

在收到此消息后，用户对 $E_s[K_{ab}; K_{ba}]$ 解密求出 K_{ba}．之后，用户用消息 1 中得到的访问网络的公钥 K_b 对数字签名项进行验证．若不正确，则用户认为访问网络为假冒；若正确，则用户认为访问网络是合法的．

至此，通信双方的相互认证已经完成，并在两个通信实体之间建立起一个会话密钥 $SK = K_{ab} \bigoplus K_{ba}$.

3 协议的性能分析

目前，已提出了许多形式化认证逻辑对协议的安全性进行分析．由于 BAN 认证逻辑 [6] 具有直观的逻辑表达，而且便于掌握和使用，从而被最广泛地应用于密码协议的安全性证明．在对缺少可信赖的第三方服务器实时参与的认证协议进行证明时，BAN 认证逻辑存在一定的局限性．只要我们假设由证书机构 CA 所颁发的证书均是清新的 (fresh)，这个问题就可以得到解决．在实际中，这一假设是合理的．因为证书的清新性可以由证书中所含的证书有效期以及作废证书清单 CRL(Certificate Revocation List) 来保证 [4]．下面采用 BAN 认证逻辑对本文所提方案进行安全性分析．

3.1 协议安全性的形式逻辑证明

具体协议如下：

消息 1 $B \longrightarrow A \quad \{|\xrightarrow{K_b} B\}_{K_{ca}^{-1}}, N_b\}$;

消息 2 $A \longrightarrow B \quad \{\{|\xrightarrow{K_a} A\}_{K_{ca}^{-1}}, K_{ab}\}_{K_a}, \{N_b, \{\{|\xrightarrow{K_a} A\}_{K_{ca}^{-1}}, K_{ab}\}_{K_b}\}_{K_a^{-1}}$;

消息 3 $B \longrightarrow A \quad \{K_{ba}\}_{K_{ab}}, \{K_{ba}, \{\{|\xrightarrow{K_b} A\}_{K_{ca}^{-1}}, K_{ab}\}_{K_b}\}_{K_b^{-1}}$.

理想化协议如下：

消息 1　$B \longrightarrow A$　$\{| \xrightarrow{K_b} B\}_{K_{ca}^{-1}}$；

消息 2　$A \longrightarrow B$　$\{\{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}_{K_b}$，$\{N_b\{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}_{K_a^{-1}}$；

消息 3　$B \longrightarrow A$　$\{A \xleftrightarrow{K_{ba}} B\}_{K_{ab}}, \{A \xleftrightarrow{K_{ba}} B, \{\{| \xrightarrow{K_b} A\}_{K_{ca}^{-1}}, K_{ab}\}_{K_b}\}_{K_b^{-1}}$.

初始假设：

(a) $A \equiv | \xrightarrow{K_a} A$,　(b) $A \equiv | \xrightarrow{K_{ca}} CA$,
(c) $A \equiv (CA \Rightarrow | \xrightarrow{K} B)$,　(d) $A \equiv \#(K_{ab})$,
(e) $A \equiv A \xleftrightarrow{K_{ab}} B$,　(f) $A \equiv (B \Rightarrow A \xleftrightarrow{K_{ba}} B)$,
(g) $B \equiv | \xrightarrow{K_b} B$,　(h) $B \equiv | \xrightarrow{K_{ca}} CA$,
(i) $B \equiv (CA \Rightarrow | \xrightarrow{K} A)$,　(j) $B \equiv \#(N_b)$,
(k) $B \equiv A \xleftrightarrow{K_{ba}} B$,　(l) $B \equiv (A \Rightarrow A \xleftrightarrow{K_{ab}} B)$,
(m) $CA \equiv | \xrightarrow{K_a} A$,　(n) $CA \equiv | \xrightarrow{K_b} B$,
(o) $CA \equiv | \xrightarrow{K_{ca}} CA$.

证明　由消息 2，我们得到

$$B < \{\{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}_{K_b}, \{N_b, \{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}_{K_a^{-1}},$$

$$B < \{\{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}_{K_b}, \tag{1}$$

$$B < \{N_b, \{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}_{K_a^{-1}} \tag{2}$$

由 (1) 式和假设 (g) 可知

$$B < \{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B. \tag{3}$$

由 (3) 式、假设 (h) 和 (i) 、裁判权规则 (jurisdiction rule) 以及证书 Cert$A$ 是清新的假定，得到

$$B \equiv \{|A \xrightarrow{K_a} A\}. \tag{4}$$

由 (2) 、 (4) 式和消息意义规则 (message-meaning rule)，得到

$$B \equiv A| \sim \{N_b, \{| \xrightarrow{K_a} A\}_{K_{ca}^{-1}}, A \xleftrightarrow{K_{ab}} B\}. \tag{5}$$

由假设 (j) 和随机数验证规则 (nonce-verification rule)，得到

$$B \equiv A \equiv \{A \xleftrightarrow{K_{ab}} B\}. \tag{6}$$

由假设 (l) 和裁判权规则，得到

$$B \equiv \{A \xleftrightarrow{K_{ab}} B\}. \tag{7}$$

由消息 1，我们得到

$$A < \{| \xrightarrow{K_b} B\}_{K_{ca}^{-1}}. \tag{8}$$

由 (8) 式、假设 (b) 和 (c) 、裁判权规则以及 Cert$A$ 是清新的假定，得到

$$A \equiv |\xrightarrow{K_b} B. \tag{9}$$

由消息 3，得到

$$A < \{A \overset{K_{ba}}{\longleftrightarrow} B\}_{K_{ab}}, \{A \overset{K_{ba}}{\longleftrightarrow} B, \{\{|\xrightarrow{K_b} A\}_{K_{ca}^{-1}}, K_{ab}\}_{K_b}\}_{K_b^{-1}}. \tag{10}$$

由 (9)、(10) 式以及消息意义规则，得到

$$A \equiv B| \sim \{A \overset{K_{ba}}{\longleftrightarrow} B, \{\{|\xrightarrow{K_b} A\}_{K_{ca}^{-1}}, K_{ab}\}_{K_b}\}. \tag{11}$$

由假设 (d)，以及随机数验证规则，得到

$$A \equiv B \equiv \{A \overset{K_{ba}}{\longleftrightarrow} B\}. \tag{12}$$

由假设 (f) 以及裁判权规则，得到

$$A \equiv \{A \overset{K_{ba}}{\longleftrightarrow} B\}. \tag{13}$$

由 (7) 式和假设 (k)，(13) 式和假设 (e)，得到

$$A \equiv \{A \overset{K_{ab}\oplus K_{ba}}{\longleftrightarrow} B\},$$
$$B \equiv \{A \overset{K_{ab}\oplus K_{ba}}{\longleftrightarrow} B\}.$$

证毕

3.2 协议计算量的比较分析

此协议与文献 [3,4] 中的协议的比较如表 1 所示。表中加括号的部分表示用户所进行的与其私钥有关的运算。

表 1 新协议与其他同类协议在用户计算量上的比较

方案	运算量					
	公钥证书验证次数	签名验证次数	公钥加密次数	私钥解密次数	数字签名次数	模指数运算
MSR+DH[3]	1		(1)		1	(1)
Aziz−Diffie[4]	1	1	1	(1)	(1)	
新协议	1	1	1		(1)	

在协议的执行过程中，最复杂的运算是双钥体制中与私钥有关的解密和数字签名运算。在新协议中，用户端所进行的、与私钥有关的运算仅仅为一次数字签名运算；而在访问网络端，则需要进行两次运算，即一次解密运算和一次签名运算。显然，用户端的实时计算负荷要比网络端小，从而与个人通信中用户与网络两端计算资源不对称的特点相符合。若用户端采用的是 ElGamal 数字签名算法，那么用户签名运算的大部分可以在预备阶段中完成 [7,8]。这种情况下用户登记认证的速度会大大加快。

4 结 束 语

在所提出的协议中，由于将双钥体制和单钥体制巧妙地结合起来，使用户端的计算量明显地低于网络端的计算量。这就满足了用户、网络具有不对称计算资源的要求。协议的另外一个优点是认证进程不受用户归属网络的控制，用户在访问网络中的登记进程是在访问网

络中独立进行的。而在后续的呼叫建立和异区切换进程中，通信双方的相互认证完全依赖于登记阶段所建立起来的秘密信息，而无需象 GSM 、 IS-41 等系统那样需要用户归属网络的参与。其结果一方面降低了网络的信令负荷，另一方面减弱了对骨干网络安全的依赖。分析结果表明：新协议是安全、高效的，适合在 PCS 环境中使用。

参 考 文 献

[1] Vedder K. Security aspects of mobile communications. Computer Security and Industrial Cryptology, Lecture Notes in Computer Science, Leuven, Belgium: May 1991, 193–210.

[2] Molva R, *et al.* Authentication of mobile users. IEEE Network, 1994, 11(3): 26–34.

[3] Beller M J, Chang L F, Yacobi Y. Privacy and authentication on portable communication system. IEEE J. on SAC, 1993, 11(6): 821–829.

[4] Aziz A, Diffie W. Privacy and authentication for wireless local area networks. IEEE Personal Communications, 1994, 1(1): 25–31.

[5] Lin H Y, Harn L. Authentication protocols for personal communication systems. ACM Computer Communications Review, 1995, 25(4): 256–261.

[6] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans. on Computer Systems, 1990, 8(1): 18–36.

[7] Beller M J, Yacobi Y. Fully-fledged two-way public key authentication and key agreement for low-cost terminals. Electron. Lett., 1993, 29(11): 999–1001.

[8] Liu J, Wang Y. A user authentication protocol for digital mobile communication network. Proc. PIMRC ' 95, Toronto, Canada: Sept. 1995, 608–612.

AUTHENTICATION PROTOCOL FOR MOBILE USER REGISTRATION IN PERSONAL COMMUNICATION SYSTEMS

Liu Jianwei　　Wang Yumin

(*Xidian University, Xi'an* 710071)

Abstract　Impersonation and eavesdropping are the crucial threats in wireless communication systems. In personal communication systems (PCS), it is necessary to provide security protection on the voice/data transmitted over wireless links, and perform mutual authentication between mobile user and serving network. Recently, many protocols are proposed for different mobile networks, such as GSM, IS-41, CDPD and wireless LAN. However, these protocols have different weakness when they are applied in PCS environment. Based on the public-key P&A model proposed by M.J. Beller, *et al.*(1993), this paper presents an authentication protocol for mobile user registration. Then the formalized security proof of the protocol using BAN authentication logic, and the qualitative analysis about its computing complexity are given. Results show that many new security features are added to the proposed protocols when it is compared with the protocols available.

Key words　Personal communication system, Authentication protocol, BAN logic

刘建伟：　男，1964 年生，副教授．博士．主要研究方向为：信息论、信道编码、密码、网络安全、移动通信系统等．

王育民：　男，1936 年生，教授，博士生导师．主要从事信息论、信道编码、密码学、网络安全、通信方面的科研与教学工作．