文章编号:1671-6833(2012)01-0121-04

无线网络匿名身份认证方案的设计

项顺伯,柯文德

(广东石油化工学院 计算机与电子信息学院,广东 茂名 525000)

摘 要:提出一种无线网络的匿名身份认证方案,利用双线性对、哈希函数和对称加密算法等内容实现移动用户的匿名身份认证问题,并从性能和安全性两个方面对方案进行了分析.分析表明,该方案安全有效,实现了移动用户的匿名身份认证,也实现了对象间的双向认证,因此该方案能满足无线网络通信环境的需求.

关键词:匿名;身份认证;移动节点;双线性对;会话密钥

中图分类号:TP309 **文献标志码**:A doi:10.3969./j.issn.1671-6833.2012.01.030

0 引言

无线网络通信中,当移动节点漫游至外地网络时,只有通过外地网络的身份认证后,该移动节点才被允许接入.为防止恶意攻击者确定移动节点的身份和跟踪移动节点,无线网络中需采用匿名技术来隐藏移动节点的真实身份和具体位置,从而保护移动节点的安全.因此,匿名身份认证在无线网络中有着重要的作用.文献[1]针对无线网络下的用户身份认证和位置保密,利用数字签名和公钥加密算法提出一种认证方案,并分析了方案的匿名性.文献[2]分析了一种无线网络匿名身份认证协议,认为该协议是可追踪的和低效的,并提出一种能减少认证阶段的通信开销而更加有效的认证方案.文献[3]利用数字签名提出一种无线网络匿名认证方案,该方案计算量较大,效率不高.文献[4]在文献[2]的基础上提出一种更有效的无线网络匿名通信协议,该协议减少了匿名标签认证阶段和分发阶段的通信开销.文献[5-7]均提出一种无线网络匿名认证方案,并对方案的性能和安全性进行了分析.文献[8]指出文献[5]的无线网络匿名认证方案存在安全缺陷:属同一家乡网络的合法用户可以跟踪其它合法用户,非法用户也能跟踪合法用户,不能保证只有家乡网络才能获得用户的真实身份;由于用户临时身份标识符固定不变,攻击者可以跟踪用户,针对安全缺陷给出相应的攻击方法,研究人员提出了一种改进的方案,但改进后的方案稍显复杂,计算量大.笔者在上述文献的基础上,利用相关密码学内容,提出了一种新的无线网络的匿名身份认证方案.

1 基础知识

设 G_1 是由 P 生成的加法循环群,阶为素数 q,G_2 是阶为 q 的乘法循环群,双线性对 e 是一个映射,$e:G_1\times G_1\to G_2$ 满足下列性质.

(1)双线性:对任意的 $P,Q,R\in G_1$,$a,b\in Z_q^*$,都有 $e(aP,bQ)=e(aQ,bP)=e(P,Q)^{ab}$,

$e(P,R+Q)=e(P,R)e(P,Q)$,

$e(P+Q,R)=e(P,Q)e(P,R)$;

(2)非退化性:存在 $P,Q\in G_1$,满足 $e(P,Q)\neq 1$;

(3)可计算性:对所有的 $P,Q\in G_1$,存在有效的算法计算 $e(P,Q)$.

通常 e 通过改进的 Weil 对或 Tate 对来实现,这样的双线对的映射称为可允许的双线对.G_1 上存在如定义1的困难问题.

定义1 离散对数问题(DLP):给定 $P,Q\in G_1$,$a\in Z_q^*$,已知 $Q=aP$,求 a.

定义2 单向抗碰撞哈希函数:已知哈希函数 $H(\cdot)$,已知 x 计算 $H(x)$ 容易,但已知 $H(x)$ 计算 x 是不可行的;对于 $y=H(x)$,希望找到 $x'\neq x$,使得 $H(x')=H(x)$ 在计算上是不可行的.

收稿日期:2011-09-20;修订日期:2011-10-20

基金项目:广东优秀青年创新人才培育资助项目(201180);茂名学院自然科学研究基金资助项目(200840)

作者简介:项顺伯(1979-),男,安徽枞阳人,广东石油化工学院讲师,硕士.研究方向为计算机网络与密码协议.

2 无线网络匿名身份认证方案的设计

2.1 无线网络通信模型

无线网络的通信由三方构成,即移动节点(MN)、移动节点的家乡网络和移动节点漫游至外地时的外地网络.无线网络通信模型架构如图1所示,图中虚线圈是指无线信号覆盖区域,FA是指外地网络的接入点,HA是指家乡网络的接入点,代理实现移动节点的接入访问.

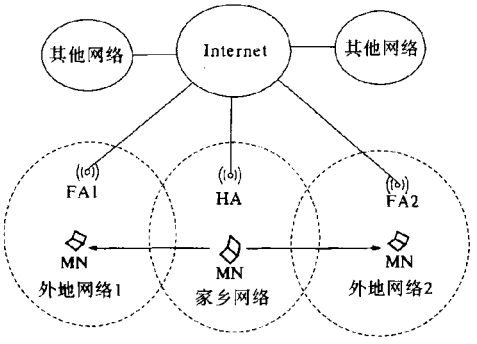

图1 无线网络通信模型

Fig.1 The communicating model for wireless network

当MN从家乡网络漫游至某外地网络后,外地网络的接入点FA必须对其进行身份认证才能保证MN允许接入.通信过程中为防止MN不被确定身份和跟踪,需采用匿名身份认证技术来隐藏MN的真实身份,从而保护用户的隐私,同时要保证被访问网络能认证MN.MN漫游时所发送的信息都必须经外地网络转发,于是MN在进行身份认证时所提供的信息必须经过一定的处理,不能含有任何表示其真实身份的信息,同时家乡网络又能够验证MN的真实身份.

2.2 方案的具体设计过程

方案的实现分两步进行:①是指移动用户第一次访问某外地网络,包括参数选取和移动用户注册、相互认证两个过程,从而确立初次的会话密钥;②是指移动用户第二次及之后对同一外地网络的访问,仅仅实现会话密钥更新,它是以①为基础的.

2.2.1 参数选取和移动用户注册[9-13]

(1)HA选取满足双线性对性质的参数G_1,G_2,e,q,P为G_1的生成元,选取$SK_{HA}\in_R Z_q^*$作为其在HA域内的私钥,计算公钥$PK_{HA}=SK_{HA}P$,选择单向抗碰撞哈希函数$H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\times G_2\rightarrow Z_q^*$,$H_3:\{0,1\}^*\rightarrow(0,1)^l$,其中$H_3$是将任意长度的字符串映射到固定长度$l$位的字符串,广播参数$G_1$,$G_2$,$e$,$q$,$P$,$PK_{HA}$,$H_1$,$H_2$,$H_3$.FA选取参数$G_1$,$G_2$,$e$,$q$,$P$,$H_1$,$H_2$,$H_3$,随机选取$SK_{FA}\in_R Z_q^*$为其域内私钥,计算公钥$PK_{FA}=SK_{FA}P$,广播参数$G_1$,$G_2$,$e$,$q$,$P$,$PK_{FA}$,$H_1$,$H_2$,$H_3$.

(2)假设无线网络中有一个集中管理的PKI或KDC中心,HA和FA由可信CA签署的公钥证书分别为$Cert_{HA}$和$Cert_{FA}$.

(3)合法的MN在家乡网络注册,HA为其分配唯一的身份标识符ID_{MN},并计算$W_{MN}=SK_{HA}H_{MN}$,其中$H_{MN}=H_1(ID_{MN})$.HA通过安全信道将自己的身份标识符ID_{HA}和W_{MN}交给MN.MN可通过计算$e(W_{MN},P)$是否与$e(H_{MN},PK_{HA})$相等来验证W_{MN}的正确性,如果相等,则W_{MN}正确.HA为MN设置用户账户表单$(Ind_{MN},Acc_{MN},ID_{MN})$,其中$Ind_{MN}=e(H_{MN},PK_{HA})$是MN用户账户的索引号,$Acc_{MN}$是MN用户账户信息,包含MN用户权限、MN用户账单等信息.

2.2.2 相互认证

相互认证包括双向认证和匿名认证,认证过程如图2所示.具体内容如下[5,12].

(1)MN选择随机数$r,r'\in Z_q^*$,产生时戳T_{MN},计算$R=rPK_{HA}$、$R'=r'PK_{FA}$、$K=rP$、$K'=r'P$,计算MN临时身份$Tid_{MN}=W_{MN}(H_2(T_{MN}\|K\|K')+r+r')$,发送$T_{MN}$,$ID_{HA}$,$R$,$R'$,$Tid_{MN}$给FA,保存$R$和$r'$.

(2)FA收到消息后,检查T_{MN}的新鲜性,如果T_{MN}新鲜,产生时戳T_{FA},计算$K'=SK_{FA}^{-1}R'$,用其私钥SK_{FA}签名生成签名消息$Sig_{FA}(ID_{HA},R,T_{MN},Tid_{MN},Cert_{FA})$,发送$ID_{HA}$,$R$,$K'$,$T_{MN}$,$Tid_{MN}$,$Cert_{FA}$,$T_{FA}$和签名消息给HA,其中$ID_{FA}$为FA的身份标识符.FA保存$R$、$R'$和$Tid_{MN}$.

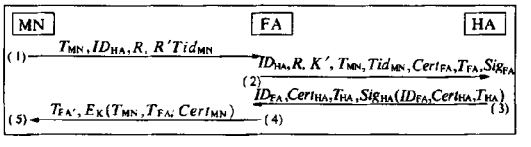

图2 相互认证过程

Fig.2 The process of mutual authenticating

(3)HA收到消息后,若证书和签名有效、ID_{HA}正确且T_{FA}新鲜,则完成对FA的认证,否则中止执行.HA用其私钥SK_{HA}计算$K=SK_{HA}^{-1}R$,计算$Ind_{MN}=e(PTid_{MN},P/(H_2(T_{MN}\|K\|K')P+K+K'))$,然后在用户表单中查找$Ind_{MN}$,若账户存在且有效,则完成对MN的认证.HA产生时戳

T_{HA}，用其私钥 SK_{HA} 签名生成签名消息 $Sig_{HA}(ID_{FA}, Cert_{HA}, T_{HA})$，发送 ID_{FA}，$Cert_{HA}$，T_{HA} 和签名消息给 *FA*.

(4) FA 收到消息后，若证书和签名有效、ID_{FA} 正确且 T_{HA} 新鲜，则 FA 完成对 HA 和 MN 的认证，否则中止执行. 认证后 FA 给 MN 签发一个临时证书 $Cert_{MN}$ 并计算 $r' = SK_{FA}^{-1}R'$，再计算对称加密密钥 $k_1 = H_3(R \| r')$，加密生成 $E_{k_1}(T_{MN}, T_{FA'}, Cert_{MN})$，产生时戳 $T_{FA'}$，给 MN 发送 $T_{FA'}$ 和 $E_{k_1}(T_{MN}, T_{FA'}, Cert_{MN})$.

(5) MN 从 FA 收到信息后，若 $T_{FA'}$ 新鲜，计算 $k_1 = H_3(R \| r')$，解密 $E_{k_1}(T_{MN}, T_{FA'}, Cert_{MN})$ 得到 T_{MN} 和 $Cert_{MN}$，核对 T_{MN} 是否与(1)中一致，如果一致则接收临时证书 $Cert_{MN}$，否则中止执行. 接收临时证书 $Cert_{MN}$ 后，MN 完成了对 FA 的认证并建立初次的会话[5].

2.2.3　*会话密钥更新*

(1) 当 MN 对 FA 进行第 $i(i \geq 2)$ 次访问时，MN 选取随机数 b_i，计算 $k_i = H_3(b_{i-1} \| k_{i-1})$ 和 $Tid_{MN_i} = H_2(Tid_{MN_{i-1}} \| k_{i-1} \| b_{i-1})$，其中 $b_1 = R$，$k_1 = r'$，$Tid_{MN_1} = Tid_{MN}$，产生时戳 T_{MN_i}，发送 Tid_{MN_i}，$Cert_{MN}$，$E_{k_i}(b_i, Cert_{MN}, \text{OtherInformation})$ 和 T_{MN_i} 给 FA.

(2) FA 收到消息后，首先通过计算验证 Tid_{MN_i}，如果正确，检查临时证书 $Cert_{MN}$ 和时戳 T_{MN_i} 是否有效，若无效则中止执行，否则 FA 计算 k_i，然后解密 $E_{k_i}(b_i, k_i, Cert_{MN}, \text{OtherInformation})$ 得 b_i，$Cert_{MN}$ 和 OtherInformation，并计算下一次的会话密钥 k_{i+1}.

3　匿名身份认证方案分析

3.1　方案性能分析

在 MN 和 FA 计算会话密钥 k_i 时，不采用双线性对而采用哈希函数计算是因为哈希函数的计算开销小，可以提高系统的运行效率. 本方案的具体性能体现在如下几个方面[7-9].

3.1.1　*移动节点的匿名性和不可跟踪性*

相互认证阶段使用一次性临时身份 Tid_{MN} 实现对移动节点 MN 的认证，只有 MN 和 HA 知道 MN 临时身份与真实身份间的对应关系. 在会话密钥更新阶段 MN 也使用了临时身份，因此实现了 MN 的匿名性，有效地防止了 MN 被跟踪.

3.1.2　*双向认证*

建立会话密钥的双方 MN 和 FA 对彼此的身份进行了认证. FA 对 MN 的认证是通过 FA 对 HA 的认证和 HA 对 MN 的认证间接实现的. FA 和 HA 的相互认证是通过公钥证书、签名以及时戳实现的. HA 根据 MN 的临时身份 Tid_{MN} 与真实身份的用户账户列表对应关系来认证 MN 的真实身份，这是通过双线对的性质来计算实现的. 而 MN 对 FA 的认证是在确定 FA 的时戳新鲜后，解密 $E_{k_1}(T_{MN}, T_{FA'}, Cert_{MN})$ 得到 T_{MN}，通过核对 T_{MN} 和自己产生的是否一致来认证 FA 的.

3.1.3　*会话密钥的新鲜性*

MN 和 FA 每次的会话密钥 E_{k_i} 都由上一次会话时 MN 选取的随机数 b_{i-1} 和 k_{i-1} 通过式 $E_{k_i} = H_3(b_{i-1} \| k_{i-1})$ 计算产生的，每次会话时都不相同，实现了一次一密，因此保证了会话密钥的新鲜性和前向安全功能.

3.2　方案安全性分析

本方案的安全性前提是方案所采用的双线性对和哈希函数是安全的. 本节只给出非形式安全属性分析.

3.2.1　*移动节点身份得到保护*

MN 每次访问 FA 时都使用一次性临时身份 Tid_{MN} 来实现 MN 的匿名性. 在第一次访问 FA 时，除 MN 和 HA 外，任何攻击者都不知道 MN 临时身份与真实身份的对应关系. 在以后的访问中，任何攻击者由于得不到 k_{i-1}，无法计算得到 Tid_{MN_i}. 因此，该协议有效的保护了用户的身份.

3.2.2　*每次的会话密钥是安全的*

MN 和 FA 每次的会话密钥都不相同，而且只有他们才能计算会话密钥. 在第一次会话中，攻击者无法计算出 E_{k_1}，因为它不知道随机数 r'，即使攻击者想计算 r'，也将面临求解定义 1 的离散对数困难问题. 在第 $i(i \geq 2)$ 次会话中，攻击者不知道 k_{i-1} 无法计算出 E_{k_i}. 这样保证了会话密钥的安全性.

3.2.3　*抗重放攻击*

MN 和 FA 每次会话时的相关参数和会话密钥都不一样，而且有时戳的存在，有效地防止了重放攻击. 而 FA 和 HA 之间使用时戳也有力地抵抗了重放攻击.

3.2.4　*抗中间人攻击*

MN 和 FA 第一次会话时，只有 MN 和 HA 知道 MN 的真实身份. 只有 MN 和 FA 才能计算出他们的会话密钥，由于发送的消息中含有公钥证书和时戳等内容，任何人想伪造 MN 或 FA 进行通信都是不可能的.

4 结论

无线网络应用和发展的重要内容是移动用户的匿名身份认证问题.笔者提出了一种无线网络的移动用户匿名身份认证的设计方案,实现了对移动用户身份的认证以及移动用户、外地网络代理、家乡网络代理三者间的双向认证,同时确保移动用户身份匿名性和位置的不被跟踪.该方案为无线网络中漫游用户的匿名认证提供了一种较实用的解决方案.

参考文献:

[1] HIROSE S, YOSHIDA S. A user authentication scheme with identity and location privacy[C]//2001 LNCS: 2119. Berlin: Springer, 2001: 235-246.

[2] JAN J K, WHE D L. An efficient anonymous channel protocol in wireless communications[J]. IEICE Transactions on Communication, 2001(E84-B): 484-491.

[3] WANG S J. Anonymous wireless authentication on a portable cellular mobile system[J]. IEEE Trans on Computer, 2004, 53(10): 1317-1329.

[4] HWANG M S, LEE C H. A new anonymous channel protocol in wireless communications[J]. International Journal of Electronics and Communications, 2004, 58(3): 218-222.

[5] ZHU Jian-ming, MA Jian-feng. A new authentication scheme with anonymity for wireless environments[J]. IEEE Trans on Consumer Electronics, 2004, 50(1): 231-235.

[6] KANG M H, RYOU H B, CHOI W. Design of anonymity-preserving user authentication and key agreement protocol for ubiquitous computing environments[A]. WINE 2005[C]. Hong Kong, China, 2005.

[7] KIM W H, YOON E J, YOO K Y. New authentication protocol providing user anonymity in open network[A]. WINE 2005[C]. Hong Kong, China, 2005.

[8] 彭华熹,冯登国.匿名无线认证协议的匿名性缺陷和改进[J].通信学报,2006,27(9):78-85.

[9] LEE J S, CHANG C C, CHANG P Y, et al. Anonymous authentication scheme for wireless communications[J]. International Journal of Mobile Communications, 2007, 5(5): 590-601.

[10] 朱辉,李晖,苏万力,等.基于身份的匿名无线认证方案[J].通信学报,2009,30(4):130-135.

[11] Andreas Noack. Efficient Authenticated Wireless Roaming via Tunnels[C]//Quality of Service in Heterogeneous Networks. Berlin: Springer, 2009, 22: 739-752.

[12] 杨力,马建峰,朱建明.可信的匿名无线认证协议[J].通信学报,2009,30(9):29-34.

[13] 曹雪菲,曾兴雯,寇卫东,等.一种新的不安全信道上的匿名认证方案[J].西安电子科技大学学报:自然科学版,2007,34(6):878-880.

The Design of an ID Authentication Scheme with Anonymity in Wireless Networks

XIANG Shun-bo, KE Wen-de

(College of Computer and Electronic Information, Guangdong University of Petrochemical Technology, Maoming 525000, China)

Abstract: In view of the ID authentication problem of mobile users when roaming, an ID authentication scheme with anonymity in wireless networks was proposed by means of bilinear pairing, hash functions and symmetrical encryption algorithms. From the performance and security, the proposed scheme was analyzed. The analysis showed that the scheme is secure and efficient, which can achieve the anonymous ID authentication to mobile users and can achieve mutual ID authentication between two objects, so the scheme can satisfy the secure requirements of wireless networks.

Key words: anonymity; ID authentication; mobile user; bilinear pairing; session key