第 35 卷 第 1 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.1 Computer Engineering January 2009
·安全技术· 文章编号：1000—3428(2009)01—0147—03 文献标识码：A 中图分类号：TP393.08

基于双线性对的 Ad Hoc 网络门限身份认证方案

吕 鑫[1,2]，程国胜[1,2]，许 峰[1,2]
(1. 南京信息工程大学数理学院，南京 210044；2. 南京大学技术学院，南京 210093)

摘 要：研究移动 Ad Hoc 网络特有的安全威胁，提出一种基于双线性对、无可信中心的门限身份认证方案。该方案能有效减少网络中各节点的存储代价和运算量，抵御内部节点攻击和被动攻击。与已有 Ad Hoc 门限身份认证方案相比，其证书生成速度快、计算复杂度低。
关键词：Ad Hoc 网络；双线性对；概率签名方案；门限身份认证

Threshold Authentication Scheme of Ad Hoc Network Based on Bilinear Pairings

LV Xin[1,2], CHENG Guo-sheng[1,2], XU Feng[1,2]
(1. College of Math & Physics, Nanjing University of Information Science & Technology, Nanjing 210044;
2. College of Technology, Nanjing University, Nanjing 210093)

【Abstract】 This paper studies the proper threat of mobile Ad Hoc network, and proposes a threshold authentication scheme without the trusted center based on bilinear pairings. The cost of storage and computational capacity, requiring of each node, can be effectively reduced and security problems such as inner nodes attack, passive attack can be solved. Compared with the existent protocol, this scheme is faster in generating certificate and has lower complexity of computing.
【Key words】 Ad Hoc network; bilinear pairings; probability signature scheme; threshold authentication

1 概述

移动 Ad Hoc 是一种新型网络结构，它没有基础设施的支持，通过传输范围有限的移动节点间的互相协作和自我组织保持网络的互联以及数据传输。在 Ad Hoc 中，同一个无线覆盖范围内的节点(主机)可以直接通信，而不在同一个无线覆盖范围内的节点要经过其他节点路由，因此，Ad Hoc 中的每个节点既是主机又是路由器。Ad Hoc 具有以下特点：(1)完全自组织；(2)拓扑结构经常变化；(3)信任分散；(4)带宽有限；(5)能源有限。对 Ad Hoc 的研究起初是为了满足军事通信需求，现在已逐步将其应用于商业和普通家庭，例如虚拟教室、家庭网络等。Ad Hoc 存在传统网络安全问题和一些新问题，如容易被监听、普通的攻击方式能使整个网络瘫痪等。

在基于PKI的网络中采用信任第三方方案。在此机制下，所有节点都拥有一个公开/秘密密钥对。它们使用公开密钥鉴别对方，但公开密钥不一定具有真实性。因此，需要一个可信任的实体来管理所有公开密钥。该可信任实体称为证书授权机构(CA)。这个可信的CA给每个节点签发一个用于绑定用户标识和公开密钥的证书。它本身有一个公开/秘密密钥对，且所有节点都知道CA的公开密钥。如果节点之间要进行通信，它们可以从CA上获得对方的公开密钥来鉴别对方。Ad Hoc中的情况较复杂，所有节点都容易受到攻击或被俘获，如果在Ad Hoc中采用一个CA来管理整个网络节点的公开密钥，那么当这个CA节点被俘获时，整个网络就会崩溃。因此，在Ad Hoc中应采用信任分散思想，即认为单独节点不可信、节点集合可信。基于文献[1-2]，本文将Shamir的(t, n)门限原理应用到身份认证过程，实现由多人完成证书的发放，提高了证书可信度和安全性。通过引入双线性对使被认证方可以方便地认证证书有效性。与已有Ad Hoc门限身份认证方案[3-4]不同，本文方案具有抵御网络内部t-1 个成员同时伪造子证书的能力。

2 相关概念

2.1 双线性映射和 GDH 群

设 G_1 和 G_2 分别是阶数为素数 q 的加法群和乘法群，P 为 G_1 的一个生成元。假设 G_1 和 G_2 这 2 个群中的离散对数问题都是困难问题。双线性映射 $e: G_1 \times G_1 \to G_2$ 具有如下特性：

(1)双线性性：$\forall P, Q \in G_1$，$a, b \in Z$，有 $e(aP, bQ) = e(P, Q)^{ab}$。

(2)非退化性：若 $e(P, Q) = 1, \forall Q \in G_1$，则 P 是 G_1 的生成元。

(3)可计算性：对所有 $P, Q \in G_1$，存在有效算法可以计算 $e(P,Q)$。

在具有以上性质的群 G_1 上，可以定义如下密码学问题：

(1)离散对数问题(DLP)：给定 $P, Q \in G_1$，计算满足 $Q=nP$ 的整数 n。

(2)计算 Diffie-Hellman 问题(CDHP)：对 $a,b \in Z_q^*$，给定三元组 $(P, aP, bP) \in G_1^3$，计算 abP。

(3)判定 Diffie-Hellman 问题(DDHP)：对 $a,b,c \in Z_q^*$，给定四元组 $(P, aP, bP, cP) \in G_1^4$，判断 $c \equiv ab \mod q$ 是否成立。

若群 G_1 上的DDHP是容易的而CDHP是困难的，则称群 G_1 为GDH(GAP Diffie-Hellman)群[5]。可以在有限域内的超椭

作者简介：吕 鑫(1983－)，男，硕士，主研方向：信息安全；程国胜，教授；许 峰，讲师、博士研究生
收稿日期：2008-05-03 **E-mail：**lvxin.gs@163.com

圆曲线上找到这样的群。利用椭圆曲线上的Weil配对或Tate配对可以构造满足上述性质的双线性映射。

2.2 GDH 签名方案

一个签名方案包括 3 个算法：随机密钥生成算法 K，随机签名算法 S，确定性签名验证算法 V。下文将介绍 GDH 签名方案[6]。

令 G_1 为一个 GDH 群，$\left[\ \{0,1\}^* \to G_1^*\ \right]$ 为一个 Hash 函数族，其中每个元素都将任意长度的字符串映射到群 G_1^*。H 为其中任意一个元素，系统参数 I 如下：群 G_1 的生成元(阶为素数 q)和 Hash 函数 H。M 为需要签名的消息。GDH 签名方案由以下算法(K, S, V)构成：

(1)$K(I)$：令 I 为(P, q, H)。随机选取 $x \in Z_q^*$，计算 $Y \leftarrow xP$，返回(公钥 pk 为(P, q, H, Y)，私钥 sk=x)。

(2)$S(I, sk, M)$：令 I 为(P, q, H)。计算 $\sigma = xH(M)$，返回 (M,σ)。

(3) $V(M, pk, \sigma)$：令公钥 pk 为(P,q,H,Y)。若 $e(P,\sigma) = e(Y, H(M))$，则返回 1，否则返回 0。

文献[7]证明了以下结论：

定理 1 如果令 G 为一个 GDH 群，那么在随机预言模型中上述 GDH 签名方案是安全的(即在选择消息攻击下具有不可伪造性)。

2.3 新型概率签名方案及其安全性

2.3.1 概率签名方案

概率签名方案基于一个安全的双线性映射和 2.2 节提出的 GDH 签名方案，具体如下：

(1)系统初始化。设群 G_0 和 G_1 的阶数为素数 q, G_0 是一个 GDH 群，P 是它的一个生成元。$e: G_0 \times G_0 \to G_1$ 为一个安全的双线性映射。选择 2 个 Hash 函数 $H_1: \{0,1\}^* \times G_0 \to Z_q^*$，$H_2: \{0,1\}^* \to G_0 \backslash 1$。

(2)密钥生成。从 Z_q^* 中随机选取 x 并计算 $Y \leftarrow xP$，返回 $pk = (Y, P, G_0, H_1, H_2)$, sk=x，pk 和 sk 分别是公钥和私钥。

(3)签名过程。对于给定的消息 $M \in \{0,1\}^*$，随机选取 $r \in Z_q^*$，计算 U=rP。令 $h = H_1(M,U)$，$Q = H_2(M)$，计算 V=(r+hx)Q，消息 M 的签名为 $\sigma = (U,V)$。

(4)验证过程。验证消息 M 的签名 $\sigma = (U,V)$，验证以下等式是否成立：$e(P,V)$=$e(U$+$hY,Q)$，若成立则返回 1，否则返回 0。

2.3.2 方案分析

签名验证过程的正确性可由如下方程给出：

$$e(P,V) = e(P,(r+hx)Q) = e((r+hx)P, Q) = e(rP+hxP, Q) = e(U+hY, Q)$$

定理 2 若短签名方案[7]是安全的，本文签名方案肯定是安全的。

证明：设攻击者 A 能够伪造本文方案的签名，即对于给定消息 M_0，A 能够伪造签名 $\sigma = (U_0, V_0)$，其中，$V_0 = (r_0 + h_0 x)Q_0$; $h_0 = H_1(M_0, U)$。$Q_0 = H_2(M_0)$，$U_0 = r_0 P$ 对攻击者来说是已知的，因此，他必然知道 $r_0 + h_0 x$，否则不能伪造签名。另外，攻击者能使 $e(P,V_0) = e((r_0 + h_0 x)P, Q_0) = e(U_0 + h_0 Y, Q_0)$。即文献[7]中的 GDH 签名方案不能抵抗选择消息攻击。但通过定理 1 可知，GDH 签名方案是安全的，因此，本文签名方案能抵抗选择消息攻击。

3 基于双线性对的 Ad Hoc 网络门限身份认证方案

基于双线性的 Ad Hoc 网络门限身份认证方案的基本思想如下：设 Ad Hoc 网络中有 n 个节点，它们先选取自己的私钥，并共同生成(t, n)门限团体密钥。对申请加入网络的可信新节点 P 发出的证书请求，t 个节点进行子证书的颁发，最后，新节点 P 合成证书完成身份认证。

3.1 系统初始化和团体密钥的生成

上述方案的系统参数同 2.3.1 节的概率签名方案，同时对 n 个节点，选取合适的 t，一般取 $t = \left\lceil \frac{n}{2} \right\rceil$，以上参数均由一线下 CA 事先选取。

Ad Hoc 网络中的每个节点 i 随机选取一个 t-1 次多项式 $f_i(z) = a_{i,0} + a_{i,1} z + \cdots + a_{i,t-1} z^{t-1}$，其中，$a_{i,j} \in Z_q$，$j = 0, 1, \cdots, t-1$。节点 i 计算 $f_i(i)$ 并保留，为其余节点计算 $f_i(j)$ 并发送给它们。于是每个节点 i 得到 $f_j(i)$, $j = 1, 2, \cdots, n$; $j \neq i$。计算 $s_i = \sum_{j=1}^{n} f_j(i)$ 为自己的私钥，公开公钥 $Y_i = s_i P$。定义函数 $F(x) = \sum_{i=1}^{n} f_i(x)$，则 $s_i = F(i)$。令 $s = F(0) = \sum_{i=1}^{n} a_{i,0}$，$s$ 即团体密钥，Y=sP 为团体公钥。对外公开的参数为 $(G_0, G_1, H_1, H_2, Y_i, Y)$。

3.2 子证书的生成与验证

Ad Hoc 网络结构如图 1 所示，当有新节点 P_{new} 请求加入网络时，选取 t 个节点发出证书请求，该节点和每个相邻节点(跳数为一跳的节点)利用 Diffie-Hellman 密钥协议建立 GDH 群上的会话密钥 $C_{\text{new},i} \in G_0$。如果恰好有 t 个相邻节点，则建立 t 个会话密钥，若只有 m<t 个相邻节点，则建立 m 个会话密钥。

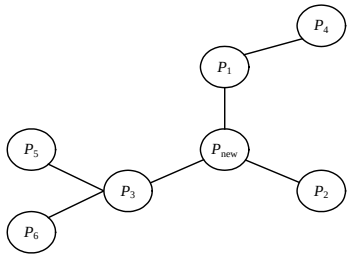

图 1 Ad Hoc 网络结构

P_{new} 把需要认证的消息 M 和参与证书生成的 t 个节点的集合信息 T 发给每个相邻节点。生成 P_{new} 的子证书前，t 个节点各自选择随机数 $r_i \in Z_q^*$，公开 $U_i = r_i P$，令 $r = \sum_{i=1}^{t} r_i$，则 $U = rP = \sum_{i=1}^{t} U_i$。没有后续节点的相邻节点 P_i 返回给 P_{new} 子证书 (U_i, V_i)，其中，$V_i = C_{\text{new},i} + r_i H_2(M) + s_i w_i H_1(M,U) H_2(M)$，$w_i = \prod_{j \neq i}^{j \in T} \frac{j}{j-i}$；如果相邻节点 P_i 有后续节点，则 P_i 先计算子证书 (U_i, V_i) (V_i 的取值与没有后续节点的情况一样)并将其传给下一个节点 P_{i+1}。P_{i+1} 计算 V_{i+1}，随后更新证书 (U_i, V_i) 得到 $(U_i + U_{i+1}, V_i + V_{i+1})$，若 P_{i+1} 仍有后续节点，则重复以上步骤，直至遍历 P_i 所在支的所有节点，最后得到证书 $(\sum_{i \in T_i} U_i, \sum_{i \in T_i} V_i)$ (T_i 为节点 P_i 所在支的所有节点的集合)，并按原路返回给 P_i，P_i 将其发送给 P_{new}。

P_{new} 收到来自各个相邻节点 P_i 的子证书后，按以下步骤验证子证书：

(1) 若 P_i 没有后续节点，则验证是否有 $e(P,V_i')=e(U_i+Y_iw_iH_1(M,U),H_2(M))$，其中，$V_i'=V_i-C_{\text{new},i}$。

(2)若 P_i 有后续节点，则验证是否有 $e(P,V_i')=e(\sum_{i\in T_i}U_i+\sum_{i\in T_i}Y_iw_iH_1(M,U),H_2(M))$，其中，$V_i'=\sum_{i\in T_i}V_i-\sum_{i\in T_i}C_{new,i}$。

如果以上等式成立，则 P_{new} 可以确信子证书是由 P_i 或 P_i 所在支签发的。

3.3 子证书的合成与验证

当 P_{new} 收到所有子证书后，合成证书(U,V)，其中，$V=\sum_{i\in A}V_i'$，A 为 P_{new} 所有相邻节点的集合。P_{new} 可以通过验证以下等式是否成立来验证证书的有效性：

$$e(P,V)=e(U+YH_1(M,U),H_2(M))$$

如果上式成立，则 P_{new} 可以确认证书合法有效。

证书验证过程的正确性可由下式给出：

$$\begin{aligned}e(P,V)&=e(P,\textstyle\sum_{i\in A}V_i')=\\&e(P,\textstyle\sum_{i\in T}r_iH_2(M)+\sum_{i\in T}s_iw_iH_1(M,U)H_2(M))=\\&e(P,rH_2(M)+F(0)H_1(M,U)H_2(M))=\\&e(P,(r+sH_1(M,U))H_2(M))=e(U+YH_1(M,U),H_2(M))\end{aligned}$$

4 安全性分析

本方案的安全性基于已证明安全的 GDH 签名方案和求解离散对数困难问题。攻击者如果想从子证书中获得 s_i，则等价于求解离散对数困难问题，因此，攻击者无法冒充网络节点伪造子证书，或从公钥 Y_i 和 Y 中求得 s_i 和 s。

本方案在密钥生成过程和子证书生成过程中不需要可信中心，这符合 Ad Hoc 网络不存在中心节点、各个节点之间地位平等的要求。避免了可信中心被攻破、整个系统信息暴露的毁灭性后果。在此方案中，即使攻破了 t-1 个节点，也不能伪造有效证书。在子证书生成和证书合成过程中，都可以验证证书的有效性，如果验证失败，则拒绝接受证书，保证了门限认证的 Robust 性。

本方案能抵抗以下 3 种攻击方式：

(1)被动攻击。攻击者想从认证方和被认证方交互的信息中获得有价值的信息(如成员私钥、团体私钥等)，这等价于求解离散对数困难问题。

(2)中间人攻击。攻击者伪装成某个节点 P_i 来欺骗 P_{new}，对于 P_{new} 的证书请求，因为攻击者不知道随机数 r_i 以及成员私钥 s_i，所以无法伪造出合法的证书，不能通过 P_{new} 对子证书的认证。

(3)消息重放攻击。许多文献采用时间戳的方法来防止重放攻击，但在 Ad Hoc 网络中要保持时钟的同步是难以实现的，因此，时间戳的方法在 Ad Hoc 网络中不实用。在本方案中，生成子证书前，t 个节点先要选择一个随机数 r_i，即使较早的证书信息被截获，由于每次选择的随机数不同，使得攻击者无法实施重放攻击。

5 结束语

本文方案的核心是子证书的生成与合成。在实现该方案的过程中，新节点 P_{new} 只要和每个相邻节点交互 2 次，由于子证书中包含双方事先建立的会话密钥，因此各节点向 P_{new} 返回子证书时，无须对子证书加密。即使攻击者截获了 V_i，在不知道 $C_{\text{new},i}$ 的情况下仍然无法得到 V_i'。本文方案在子证书的生成与合成中所需运算的计算复杂度较低，且子证书和证书的验证是基于双线性对的，仅做了一次双线性函数运算，因此，其效率较高，对各节点的存储能力要求较低，能在现实的 Ad Hoc 网络中得到有效应用。

参考文献

[1] Vergados D D, Stergiou G. An Authentication Scheme for Ad Hoc Networks Using Threshold Secret Sharing[J]. Wireless Personal Communications, 2007, 43(4): 1767-1780.

[2] 曹爱霞, 赵一鸣. Ad Hoc 网络中基于身份的认证密钥交换协议[J]. 计算机工程, 2007, 33(10): 150-152.

[3] Venkatraman L, Agrawal D P. A Novel Authentication Scheme for Ad Hoc Networks[C]//Proc. of Wireless Communications and Networking Conference. [S. l.]: IEEE Press, 2000.

[4] Yao Jun, Zeng Guihua. Key Agreement and Identity Authentication Protocols for Ad Hoc Networks[C]//Proc. of Conference on Information Technology: Coding and Computing. [S. l.]: IEEE Press, 2004.

[5] Boneh D, Franklin M. ID-based Encryption from the Weil-pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[6] Boldyreva A. Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-diffe-hellman-group Signature Scheme[M]. Berlin, Germany: Springer-Verlag, 2003.

[7] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil-Pairing[J]. Journal of Cryptology, 2001, 17(4): 514-532.

（上接第 134 页）

参考文献

[1] Sivrikaya F, Yener B. Time Synchronization in Sensor Networks: A Survey[J]. IEEE Network, 2004, 18(4): 45-50.

[2] Elson J, Girod L, Estrin D. Fine-grained Network Time Synchronization Using Reference Broadcasts[C]//Proc. of the 5th Symp. on Operating Systems Design and Implementation. [S. l.]: ACM Press, 2002.

[3] Ganeriwal S, Kumar R, Srivastava M. Timing-sync Protocol for Sensor Networks[C]//Proc. of the 1st ACM Conf. on Embedded Networked Sensor Systems. [S. l.]: ACM Press, 2003.

[4] 康冠林, 王福豹, 段渭军. 无线传感器网络时间同步综述[J]. 计算机测量与控制, 2005, 13(10): 1021-1023.

[5] Su Ping. Delay Measurement Time Synchronization for Wireless Sensor Networks[R]. Intel Research Center, IR-TR-2003-64, 2003.