第34卷 第24期 计 算 机 工 程 2008年12月
Vol.34 No.24 Computer Engineering December 2008
·安全技术· 文章编号：1000—3428(2008)24—0143—03 文献标识码：A 中图分类号：TP393

基于身份的 Ad Hoc 网络密钥管理方案

吴 平，王保云，徐开勇
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：在分析现有的 Ad Hoc 网络分布式信任方案基础上，使用双线性对技术提出一个基于身份的 Ad Hoc 网络密钥管理方案。该方案结合基于身份的密码学算法与分布式秘密共享算法将系统主密钥分发给一组预选节点，由其合作实现私钥生成中心 PKG 功能。一次单播即可安全高效地实现节点私钥更新，基于双线性对性质，一次交互即可安全地建立节点间的会话密钥。分析结果表明该方案安全高效。
关键词：移动自组网；秘密共享；基于身份；双线性对

ID-based Key Management Scheme for Ad Hoc Networks

WU Ping, WANG Bao-yun, XU Kai-yong
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】Following the analysis of existing distributed trust model to Ad Hoc networks, this paper presents an ID-based key management scheme using bilinear pairing. It employs the secret-sharing technique to distribute system key among a pre-selected set of nodes, called D-PKGs, which offers a collaborative private-key-generator service. The construction method not only ensures secure and efficient network-wide key update, but also establishes session key via only a single message using property of bilinear pairing. Analysis show the scheme is secure and effective.
【Key words】 Ad Hoc networks; secret sharing; ID-based; bilinear pairing

1 概述

移动自组网是一种新颖的移动通信网络，既可作为独立的网络运行，也可作为固定设施网络的补充形式，其自身特性使其具有巨大发展前景；但无线信道的脆弱性、动态拓扑及无中心、无基础设施等特性很难部署如 PKI(公钥基础设施)集中式认证机构。

文献[1]提出的COCA方案通过门限共享[2]由n(网络节点数N, $N>n$)个专门节点共享系统密钥，由集成者完成对证书的签名，同时使用前摄分量更新来抵抗移动对手；文献[3]提出的全分布式 (t,N) 方案URSA允许任何节点携带系统密钥的一个分量来更加公平地分配负荷，增强了服务可用性，但系统易受Sybil攻击[4]，这种攻击方式能够获得大量身份从而收集足够多的分量重构系统密钥，此外URSA存在文献[5]中所提到的门限签名过程中的私钥信息泄露。文献[1,3]是基于证书实现公钥与实体身份关联，这种方式在证书管理过程中需很高的计算与存储开销[6]。

1984 年Shamir提出一种公钥密码体制[7]能大大减少公钥系统的复杂度，它选择任意比特串为公钥，由私钥生成中心PKG生成对应私钥，其优势是简化了基于证书的公钥体制负担最重的密钥管理过程。

文献[8]提出基于身份的AC-PKI方案，方案通过匿名路由协议MASK[9]可有效应对Sybil攻击，但未讨论节点私钥更新，也未涉及会话密钥协商，文献[10]提出了基于身份的IDAKE方案存在 2 个不足：(1)不能应对Sybil攻击；(2)节点以非交互方式协商会话密钥，不满足AKA[11](提供双向隐式密钥认证的密钥协商协议)安全特性。

本文在文献[8,10]基础上做如下改进：一次单播消息可安全高效地实现节点私钥更新与签发；通过一次交互可安全地实现节点间的会话密钥协商。

方案引入离线 PKG，其功能是实现网络初始化，为新节点分发私钥；离线 PKG 并不参与密钥更新、撤销等管理，因此，与 Ad Hoc 网络自主性并不违背。系统主密钥由系统中初始化的预选节点(D-PKGs)集 Ω ($|\Omega|=n$， $n<N$，N 为网络节点数)持有。节点公私钥对 $<K_{A,pi},K_{A,pi}^{-1}>$ 在运行期间需周期性更新，路由协议 MASK 保证攻击者无法跟踪与定位预选节点 D-PKGs。

2 预备知识

本节介绍双线性对技术的基础知识及相关困难问题。

令G_1为P生成的循环加法群，阶为q，G_2是具有相同阶的循环乘法群，a, b是 Z_q^* 中的元素，设 G_1 和 G_2 这 2 个群中的离散对数问题是困难的，双线性对是满足下列性质的一个映射 $e:G_1\times G_1\to G_2$ ：

(1)双线性性： $e(aP,bQ)=e(P,Q)^{ab}$ 。

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

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

双线性映射e可通过有限域上超椭圆曲线的Tate对Weil对进行构造[12]，本方案依赖以下难题。

定义 1 设 G_1,G_2 是阶为素数 q 的 2 个循环群，$e:G_1\times G_1\to G_2$ 为一个双线性映射，P为 G_1 的生成元，则

作者简介：吴 平(1979－)，男，硕士研究生，主研方向：移动自组网及网络性能；王保云，硕士研究生；徐开勇，研究员
收稿日期：2008-05-20 **E-mail：**wpieu@sina.com

$<G_1,G_2,e>$ 上的Bilinear Diffie-Hellman(BDH)问题是：对任意 $a,b,c\in Z_q^*$，由 $<P,a\cdot P,b\cdot P,c\cdot P>$ 计算 $e(P,P)^{abc}$。

定义 2 设 G_1，G_2 是阶为素数 q 的 2 个循环群，$e:G_1\times G_1\to G_2$ 为一个双线性映射，P 为 G_1 的生成元，则 $<G_1,G_2,e>$ 上的 Decisional Bilinear Diffie-Hellman(DBDH)问题是：对任意 $a,b,c\in Z_q^*$，由 $<P,a\cdot P,b\cdot P,c\cdot P>$ 和 $h\in G_2$ 判断 $h=e(P,P)^{abc}$ 是否成立。

3 本文方案

3.1 系统假设

考虑一个包含 N 个节点的网络，节点集合标识为 $\Psi(|\Psi|=N)$，随着节点加入或离开，网络节点数 N 动态可变。初始化阶段系统存在一个可信 PKG 为网络的节点分发密钥，节点 $A\in\Psi$ 有全网唯一标识 ID_A，通常是节点 MAC 地址或 IP 地址，将网络运行时间设为连续不相重叠的密钥更新时段 p_i ($1\le p_i\le M$，任一更新时段 p_i 与非零串 $phase_i$ 相关，且 $phase_i=phase_{i-1}+1$，$i\in[2,M]$)。

表 1 是本文用到的相关标识符。

表 1 相关符号

符号	含义	符号	含义
$f(x)$	t-1 次多项式	G_1, G_1	q 阶循环群
ID_A	节点 A 的身份标识	Ω	密钥生成中心 D-PKGs 集合
P	G_1生成元	K_p	系统主密钥
H_1,H_2	安全的哈希函数	S_V	D-PKG ID_V对K_p 的共享份额
ψ	网络节点集	W_s^V	验证参数 $W_s^V=s_VP\in G_1$
P_{pub}	系统公钥$P_{pub}=K_pP$	$<K_{A,pi},K_{A,pi}^{-1}>$	节点公私钥对
t, n	秘密共享参数	$phase_i$	第 i 个密钥更新时段非零串
$\|X\|$	集合元素个数	$\|\|$	消息串接操作

3.2 系统初始化

PKG 选取系统参数，包括阶为 q 的由 P 生成的循环加法群 G_1、循环乘法群 G_2，双线性映射 $e:G_1\times G_1\to G_2$，Hash 函数：$H_1:\{0,1\}^*\to G_1$，$H_2:G_2\to\{0,1\}^*$；随机选取 $K_P\in Z_q^*$ 作为系统主密钥，计算 $P_{pub}=K_PP\in G_1$，公开系统参数：$pub=\{P,P_{pub},e,G_1,G_2,H_1,H_2\}$；选取随机多项式：$f(x)=\sum_{i=0}^{t-1}a_ix^i(\bmod q)$，且 $f(0)=K_P$，任意选择包含 n 个节点的子集 $\Omega\in\Psi$ 为方案中的预选节点 D-PKGs ($t\le n\lhd|\Psi|=N$)，对 n 个 D-PKGs 节点 $ID_V\in\Omega(|\Omega|=n)$，计算并分发子密钥 $s_V=f(ID_V)\bmod q$，广播 $W_s^V=s_VP\in G_1$。对任意包含 t 或多于 t 个节点的子集 $A\in\Omega$可恢复多项式 $f(x)=\sum_{V\in A}\lambda_V(x)s_V(\bmod q)$，其中，$\lambda_V(x)=\prod_{S\in A\setminus\{V\}}\frac{ID_S-x}{ID_S-ID_V}$ 为插值系数。

初始化阶段，PKG 为网络节点生成公私钥对 $<K_{A,pi},K_{A,pi}^{-1}>$ 为

$<H_1(ID_A\|phase_0),K_PH_1(ID_A\|phase_0)>$

PKG 作为离线私钥生成中心为新加入节点分发公私密钥对，设当节点 ID_X 在时段 i 向 PKG 申请加入网络，PKG 为其生成公私钥对 $<K_{A,pi},K_{A,pi}^{-1}>$。

初始化完成，网络所有节点持有如下信息：

(1)公共参数：

$pub=\{P,P_{pub},e,G_1,G_2,H_1,H_2\}$；

(2)公私钥对：$<K_{A,pi},K_{A,pi}^{-1}>$；

(3)时间段非零字符串：$phase_0$；

(4)参数 W_s^V，$\{W_s^V=s_VP\in G_1\,|\,V\in\Omega\}$。

除以上信息，预选节点 D-PKGs 持有系统共享子密钥 s_V，任何其他节点都不能通过 W_s^V 获取 s_V。

3.3 私钥更新

为对抗移动对手攻击，节点需定期更新节点公私钥对 $<K_{A,pi},K_{A,pi}^{-1}>$。

设网络运行至时间段 $phase_i$，节点 ID_A 需更新其公私钥对 $<K_{A,pi-1},K_{A,pi-1}^{-1}>$，$ID_A$ 执行以下步骤：

(1)选取随机数 $r_A\in Z_q^*$；

(2)节点 ID_A 计算：$R=r_AP$，$K_{A,pi}=H_1(ID_A\|phase_i)$，并向网络中预选节点 D-PKGs，子集 $V\in\Omega(|\Omega|=n,t\le|V|\le n)$ 广播私钥更新请求消息：$REQ_{update}=\{H_1(ID_A\|phase_i),R\}$。

收到更新消息的预选节点 ID_X 执行如下操作：

(1)选取随机数 $r_X\in Z_q^*$；

(2)计算请求节点 ID_A 的部分私钥信息 $m=s_XH_1(ID_A\|phase_i)$，s_X 为 ID_X 的主密钥共享；

(3)ID_X对请求消息加密，向ID_A返回部分更新应答消息密文对 σ，其中 $\sigma=(m+r_XR,r_XP)=(s_XH_1(ID_A\|phase_i)+r_XR,r_XP)$。

ID_A 收到更新应答密文消息执行如下步骤：

(1)解密消息得到 ID_X 签发的部分私钥：

$m=m+r_XR-r_Ar_XP=s_XH_1(ID_A\|phase_i)$

(2)根据参数 W_s^V 及双线性性质验证其部分私钥的 m 正确性，若 $e(s_X(H_1(ID_A\|phase_i),P)=e(H_1(ID_A\|phase_i),W_s^X)$ 成立，则接受，否则认为 σ 不合法；

(3) ID_A 收到 t 个通过验证的解密消息后重构私钥：

$K_{A,pi}^{-1}=\sum_{X\in V}\lambda_X(0)s_X(H_1(ID_A\|phase_i)=K_P(H_1(ID_A\|phase_i)$

(4)通过双线性性质验证私钥 $K_{A,pi}^{-1}$ 合法性：

$e(K_{A,pi}^{-1},P)=e(H_1(ID_A\|phase_i),P_{pub})$。

事实上在密文 σ 通过验证后，其私钥必然是正确的。

3.4 会话密钥协商

本节讨论节点会话密钥协商。

设在时间段 $phase_i$，节点 ID_A 与 ID_B 需建立会话密钥通信，节点 ID_A 执行如下步骤：

(1)随机选择 $r\in Z_q^*$；

(2)计算 $X=rP_A$ 并发送给 ID_B；

(3)节点 ID_A 计算会话密钥 k_{AB}：$k_{AB}=H_2(e(S_A,P_B)^r)\oplus H_2(e(S_A,P_B))$；

(4) ID_B 接收到 X 后计算：$k_{BA}=H_2(e(X,S_B))\oplus H_2(e(P_A,S_B))$。

上述 P_A,S_A，P_B,S_B 为节点 ID_A，ID_B 在 $phase_i$ 的公私钥对。由双线性对性质可知 $k_{AB}=k_{BA}$。一次交互，ID_A 即与 ID_B 建立了会话密钥。

3.5 算法安全性

表面看本方案只能容忍 $n-t$ 个节点而非 $N-t$ 个节点的失效，但通过匿名路由协议MASK[9]，将D-PKGs隐藏于普通节点中，可有效应对Sybil 攻击，不存在文献[5]中的系统主密钥分量信息泄露问题，有利于保护主密钥，增强系统安全。文献[8]直接为节点产生私钥分量，存在私钥分量泄露问题，

因此存在安全隐患。在本文节点私钥更新过程中，D-PKG私钥分量以密文形式传送，只有请求节点可以重构私钥，因而未泄露节点私钥分量。

其次，会话密钥协商满足 AKA 机制安全特性：会话密钥 k_{AB} 的泄露不会影响其他会话密钥的安全性；合谋实体私钥泄露不会影响之前建立好的会话密钥；若实体 ID_A 的私钥泄露，获得该私钥的敌手可假冒 ID_A，但不能假冒其他实体和 ID_A 通信；实体 ID_A 不能被强制与实体 ID_C 共享密钥，而 ID_A 却认为是和实体 ID_B 共享密钥；任何实体不能强制会话密钥是一个预先选择值。

文献[10]直接以非交互方式协商节点会话密钥，易受中间人攻击，当某一节点私钥泄露后影响其他会话密钥安全性，不满足 AKA 机制安全特性。

4 仿真实验

本文采用NS-2[13]模拟器实现了方案的节点私钥更新算法。仿真环境链路可靠性为 90%，网络节点数 $N=50$，预选节点D-PKGs数 $n=20$，图 1、图 2 是门限值 $t=5$ 与 $t=6$ 时的节点更新延迟与成功率性能对比。

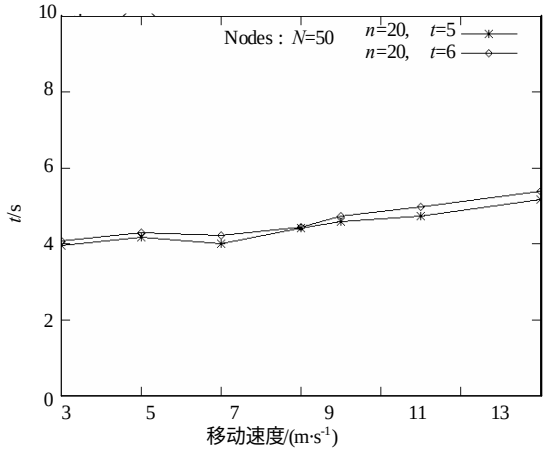

图 1　密钥更新延迟

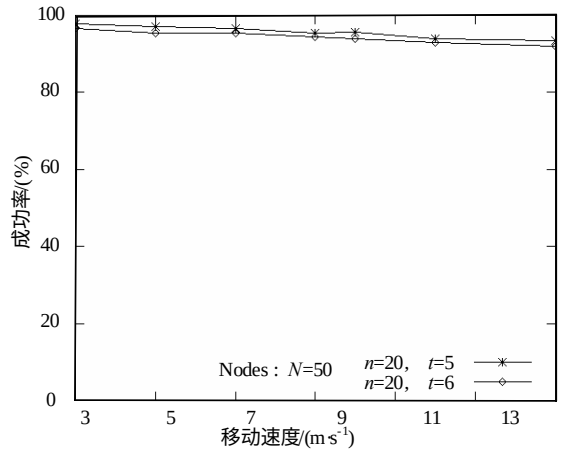

图 2　密钥更新成功率

从仿真结果看出，节点移动速度增大，节点私钥更新时间延迟变化不大，节点私钥更新成功率也保持在 95%左右。节点速度增大导致私钥更新时请求节点有可能在一次请求中并不能获取门限 t 个 D-PKG 节点的服务应答，请求节点需多次发送请求，图中可看出速度对更新延迟与成功率的影响。

5 结束语

本文分析了现有方案存在的缺陷，介绍了双线性基本理论，提出一个基于身份的自组网密钥管理方案并分析了其安全性；方案只需一次广播即可实现节点私钥更新，一次交互可安全建立会话密钥，仿真结果验证了方案有效性。

参考文献

[1] Zhou Lidong, Schneider F B, Van R R. COCA: A Secure Distributed On-line Certification Authority[J]. ACM Transactions on Computer Systems, 2002, 20(4): 329-368.

[2] Shamir A. How to Share a Secret[J]. Communication of the ACM, 1979, 22(11): 612-613.

[3] Luo Haiyun, Kong Jiejun, Zerfos P, et al. URSA: Ubiquitous and Robust Access Control for Mobile Ad-hoc Networks[J]. IEEE/ACM Transactions Networking, 2004, 12(6): 1049-1063.

[4] Douceur J R. The Sybil Attack[C]//Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. Gambridge, MA, USA: Springer-Verlag, 2002: 251-260.

[5] Jarecki S, Saxena N, Yi J H. An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol[C]//Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. [S. 1.]: ACM Press, 2004.

[6] Guttman P. PKI: Its Not Dead, Just Resting[J]. IEEE Computer, 2002, 35(8): 41-49.

[7] Shamir A. Identity Based Cryptosystems and Signature Schemes[C]//Proc. of CRYPTO'84. New York, USA: [s. n.], 1984: 47-53.

[8] Zhang Yanchao, Liu Wei, Lou Wenjing, et al. AC-PKI: Anonymous and Certificate-less Public Key Infrastructure for Mobile Ad Hoc Networks[C]//Proc. of IEEE Int'l Conf. on Comm.. [S. 1.]: IEEE Press, 2005: 3515-3519.

[9] Zhang Yanchao, Liu Wei, Lou Wenjing, et al. MASK: Anonymous On-demand Routing in Mobile Ad Hoc Networks[J]. IEEE Trans. of Wireless Comm., 2006, 5(9): 2376-2385.

[10] Hoeper K, Gong G. Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-based Schemes with Key Revocation[D]. Vancouver, Canada: University of Waterloo, 2006.

[11] Menezes A J, Qu M, Vanstone S. Some New Key Agreement Protocols Providing Mutual Implict Authentication[C]//Proc. of the 2nd Workshop on Selected Areas in Cryptography. Ottawa, Canada: [s. n.], 1995.

[12] Boneh D, Franklin M. Identity-based Encryption Form the Weil Pairing[C]//Proc. of Advances in Cryptology-CRYPTO'01. Berlin, Germany: Springer-Verlag, 2001: 213-229.

[13] UCN/LBL/VINT. Network Simulator[EB/OL]. (2004-04-10). http://www-mash.cs.berkeley.edu/ns.