一个基于证书的聚集签名方案

彭延国[1] 彭长根[2] 冯 蕾[1] 樊玫玫[2]

(贵州大学计算机软件与理论研究所 贵阳 550025)[1] (贵州大学理学院 贵阳 550025)[2]

摘 要 聚集签名能够将多个用户对多个信息的签名进行聚集,缩短签名长度,可以应用于电子合同签章、边界网关协议等领域。提出了一种基于证书的高效聚集签名方案,以实现无序聚集和有序聚集两种方式,并给出了安全分析。通过与现有方案的效率分析对比,表明本方案因无需知识证明,所以效率更高。最后基于PBC算法包实现本方案的仿真,并给出效率曲线图。

关键词 基于证书密码体制,聚集签名,可证明安全

中图法分类号 TP309 **文献标识码** A

Certificate-based Aggregate Signature Scheme

PENG Yan-guo[1] PENG Chang-gen[2] FENG Lei[1] FAN Mei-mei[2]

(Institute of Computer Science, Guizhou University, Guiyang 550025, China)[1]

(College of Science, Guizhou University, Guiyang 550025, China)[2]

Abstract An aggregate signature is a digital signature that can aggregate multiple signatures of different messages. Because of the short length, aggregate signature is useful to electronic contract signature, border gateway protocol and so on. We constructed an efficient aggregate signature scheme with two aggregate modes which are ordered and disordered. The security analysis was given. By comparison to existed schemes, our scheme without proof-of-knowledge is more efficient. Finally, based on PBC, we simulated the scheme and drew the efficient curve.

Keywords Certificate-based cryptography, Aggregate signature, Provable security

1 引言

传统PKI存在密钥托管问题。2003年Gentry[1]在欧洲密码学会上首先提出基于证书密码加密方案(CBE),将现有的IBE和传统的公钥密码体制进行有机结合,克服了密钥托管问题。2004年Kang等在文献[2]中基于椭圆曲线上的双线性对提出第一个基于证书的签名方案,并且在随机预言模型下证明了该方案的安全性。一些基于证书的加密方案随后陆续出现[3]。

聚集签名[4]能够将多个用户对多个信息的签名进行聚集,缩短签名长度,可以应用于电子合同签章、边界网关协议(BGP)等领域。目前,基于证书的聚集签名方案少有提出,仅有2009年Liu[5]等利用知识证明提出了一个聚集签名方案。本文结合文献[2]中的方案提出了一种高效的基于证书的聚集签名方案,其无需知识证明,并进行了效率分析和安全分析。最后给出实验仿真结果及性能曲线图。

2 预备知识

2.1 密码学假设

G_1 和 G_2 是两个循环群,其中 G_1 是加法群,G_2 是乘法群,它们的阶为大素数 q。构造如下双线性对:

$$\hat{e}: G_1 \times G_1 \rightarrow G_2$$

式中,G_1 和 G_2 中的离散对数问题是难解的,并且该双线性对满足以下性质[6]:

双线性:$\forall P, Q \in G_1$, $\forall a, b \in Zr$, $\exists \hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, Q)^{ab}$;

非退化性:$\exists P, Q \in G_1$, $\hat{e}(P, Q) \neq 1 \in G_2$;

可计算性:$\forall P, Q \in G_1$,能够在多项式时间内计算出 $\hat{e}(P, Q)$ 的值。

定义1 一个素数阶群 G 是一个GDH群,当且仅当 G 中的DDH问题是多项式时间内可解的,并且 G 中的CDH问题是多项式时间内不可解的。

PG是一个GDH参数生成器,其随机选择一个安全参数 k,根据 k 生成 G_1 和 G_2。G_1 和 G_2 均为GDH群,并构造双线性对 $\hat{e}: G_1 \times G_1 \rightarrow G_2$。

2.2 Kang等的签名方案

Kang等[2]实现了一个基于证书的签名方案。该方案描述如下:

到稿日期:2011-01-17 返修日期:2011-04-28 本文受国家自然科学基金(60963023),贵州省高层次人才特助经费项目(TZJF-2008-33),贵州大学自然科学青年基金项目(2009019),贵州大学研究生创新基金(校研理工2011037)资助。

彭延国(1986—),男,硕士生,主要研究方向为密码学与可信计算,E-mail:jecopeng@163.com;彭长根(1963—),男,博士,教授,硕士生导师,主要研究方向为密码学与信息安全。

CBSk. Setup　可信第三方运行 PG，生成 G_1 和 G_2，阶为 q，构造双线性对 $\hat{e}:G_1\times G_1\to G_2$。随机选择 $s_C\in Zq$ 作为系统的主密钥，$P\in G_1$ 作为公开参数，则 $PK_C=s_CP\in G_1$ 作为系统公钥。构造哈希函数 $H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\times G_1\to G_2$。系统的公开参数为 $(G_1,G_2,\hat{e},P,PK_C,H_1,H_2)$，主密钥为 $SK_C=s_C$。

CBSk. Cert　用户 Alice 生成公私钥对 (s_A,s_AP)，由可信第三方计算可得到证书 $Cert_A=s_CP_A$，并发送给 Alice，其中 $P_A=H_1(\tau,PK_C,PK_A,Aliceid)$，$\tau$ 为系统所处时期。

CBSk. Sign　用户 Alice 选择随机数 $r\in Zq$，可计算出签名为 $\sigma=(U,V)$，其中 $U=rP_A$，$h=H_3(m,U)$，$V=(r+h)(s_CP_A+s_AP_A)$。

CBSk. Verfy　验证 $\hat{e}(s_CP+s_AP,U+hP_A)\overset{?}{=}\hat{e}(P,V)$，若成立，则签名有效，若不成立，则签名无效。

3　基于证书聚集签名方案

本文给出一种高效的聚集签名方案，使用 Kang 等的签名方案作为基础，并对其进行改进，使得多个签名可以聚集。本文方案存在两种聚集方式：无序聚集(CBASns)和有序聚集(CBASs)。

假定有 n 个用户 $(U_1,U_2,\cdots,U_n)$，身份信息为 $ID_1,ID_2,\cdots,ID_n$，对 n 个信息 $(m_1,m_2,\cdots,m_n)$ 进行签名。

CBAS. Setup　可信第三方运行 PG，随机选择安全参数 k，生成 G_1 和 G_2，阶为 q，并构造双线性对 $\hat{e}:G_1\times G_1\to G_2$。在 G_1 中随机选择一个生成元 $P\in G_1$，在 Zq 中随机选择一个秘密值 $s_C\in Zq$，令 $PK_C=s_CP\in G_1$。构造如下哈希函数：

$H_1:\{0,1\}^*\to G_1$

$H_2:\{0,1\}^*\to Zq$

公开参数为 $(G_1,G_2,\hat{e},P,PK_C,H_1,H_2)$。可信第三方的主密钥为 $s_C\in Zq$，公钥为 PK_C。

CBAS. Cert　第 i 个用户 U_i 可以按照如下过程获得证书：

1)随机选择 $s_i\in Zq$ 作为秘密值，并计算 $PK_i=s_iP\in G_1$ 作为部分公钥；

2)用户将自己的身份信息(包括 ID_i，PK_i 和其他必要的认证信息)发送给可信第三方；

3)可信第三方认证用户身份的有效性；

4)若用户的身份信息验证通过，计算 $P_i=H_1(\tau,PK_C,PK_i,ID_i)\in G_1$，用户的证书为 $Cert_i=s_CP_i$，将 $Cert_i$ 发送给 U_i。

U_i 的私钥为 $S_i=Cert_i+s_iP_i=s_CP_i+s_iP_i=(s_C+s_i)P_i$，公钥为 $SP_i=s_CP+s_iP$。

3.1　无序聚集

所有用户不分先后顺序对明文信息进行签名，最后通过可信第三方进行聚集。

CBASns. Sign　用户 U_i 对信息 m_i 进行签名的过程如下：

1)随机选取 $r_i\in Zq$；

2)计算 $W_i=r_iP_i$，$h_i=H_2(m_i,W_i)$；

3)计算 $V_i=r_ih_i(s_C+s_i)P_i$；

4)最终可以得到 U_i 的签名 $\sigma_i=[W_i,V_i]$，并将其发送给可信第三方。

CBASns. Agg　可信第三方获得所有用户的签名 $(\sigma_1,\sigma_2,\cdots,\sigma_n)$，按照如下步骤进行聚集：

1)计算 $V=\sum_{i=1}^{n}V_i=\sum_{i=1}^{n}r_ih_i(s_C+s_i)P_i$；

2)最终可以得到聚集签名为 $\sigma=[W_1,W_2,\cdots,W_n,V]$。

CBASns. Verify　用户收到带有聚集签名 $(\sigma=[W_1,W_2,\cdots,W_n,V_i])$ 的消息 $(m_1,m_2,\cdots,m_n,\sigma)$，按照下式进行计算：

$$\prod_{i=1}^{n}\hat{e}(SP_i,h_iW_i)\overset{?}{=}\hat{e}(P,V)\tag{1}$$

若式(1)成立，则签名验证通过；若式(1)不成立，则签名验证失败。

3.2　有序聚集

所有用户按照先后次序对明文信息进行签名，每一个用户的签名都是对前面所有用户签名和自己签名的聚集。假定签名的次序为 $U_1,U_2,\cdots,U_n$，所有用户对 n 个信息 $(m_1,m_2,\cdots,m_n)$ 进行签名。

CBASs. Begin　用户 U_1 按照如下步骤生成第一个签名：

1)随机选取 $r_1\in Zq$；

2)计算 $W_1=r_1P_1$，$h_1=H_2(m_1,W_1)$；

3)计算 $V_1=r_1h_1(s_C+s_1)P_1$；

4)可以得到签名 $\sigma_1=[W_1,V_1]$。

CBASs. Sign　用户 U_i 收到 $i-1$ 个用户带有聚集签名 $(\sigma_{i-1}=[W_1,W_2,\cdots,W_{i-1},V_{i-1}])$ 的信息 $(m_1,m_2,\cdots,m_{i-1},\sigma_{i-1})$。利用 CBASns 的验证思想对这个聚集签名进行验证。若验证失败，则停止签名；若验证通过，则继续按照如下步骤进行签名：

1)随机选取 $r_i\in Zq$；

2)计算 $W_i=r_iP_i$，$h_i=H_2(m_i,W_i)$；

3)计算 $V_i=V_{i-1}+r_ih_i(s_C+s_i)P_i$；

4)可以得到签名 $\sigma_i=[W_1,W_2,\cdots,W_i,V_i]$。

CBASs. Verify　用户收到带有聚集签名 $(\sigma=[W_1,W_2,\cdots,W_n,V_i])$ 的消息 $(m_1,m_2,\cdots,m_n,\sigma)$，按照下式进行计算：

$$\prod_{i=1}^{n}\hat{e}(SP_i,h_iW_i)\overset{?}{=}\hat{e}(P,V)\tag{2}$$

若式(2)成立，则签名验证通过；若式(2)不成立，则签名验证失败。

4　聚集签名方案分析

4.1　正确性分析

命题 1　本文的聚集签名方案是正确的。

证明：无序聚集情况下：

假定用户收到带有聚集签名 $(\sigma=[W_1,W_2,\cdots,W_n,V_i])$ 的消息 $(m_1,m_2,\cdots,m_n,\sigma)$ 是正确的，并且获得了签名者的公钥 $SP_1,SP_2,\cdots,SP_n$。

先对每个签名者计算 $h_i=H_2(m_i,W_i)$，通过计算得到 h_iW_i，其中 $i=1,2,\cdots,n$。

然后进行如下推导：

$$\begin{aligned}\prod_{i=1}^{n}\hat{e}(SP_i,h_iW_i)&=\prod_{i=1}^{n}\hat{e}(s_CP+s_iP,h_iW_i)\\&=\prod_{i=1}^{n}\hat{e}(s_CP+s_iP,h_ir_iP_i)\\&=\prod_{i=1}^{n}\hat{e}((s_C+s_i)h_ir_iP_i)\\&=\hat{e}(P,\sum_{i=1}^{n}(s_C+s_i)h_ir_iP_i)\end{aligned}$$

又因为 $V=\sum_{i=1}^{n}(s_C+s_i)h_ir_iP_i$，所以 $\prod_{i=1}^{n}\hat{e}(SP_i,h_iW_i)=\hat{e}(P,V)$。

因此，无序聚集方案满足正确性。

同理可证有序聚集方案也满足正确性。证毕。

4.2 安全性证明

一个聚集签名方案是安全的，当且仅当不存在一个敌手，其能够在特定的攻击模型下伪造一个聚集签名。证明本文提出的方案在聚集选择密钥模型[4]中是安全的。

在聚集选择密钥攻击模型中，敌手 A 能够得到待签名信息外其他信息的有效签名，目的是伪造出能够欺骗挑战者的待签名信息的正确签名。$AdvAggSig_A$ 定义为在以下攻击模型中获胜的概率：

Setup　提供给敌手 A 一个随机公钥 PK_1；

Queries　敌手 A 以一定的概率询问自己选择的明文 m_1 在 PK_1 对应私钥的作用下产生的签名；

Response　敌手 A 产生 $k-1$ 个公钥 $PK_2,PK_3,\cdots,PK_k$（$k<N$，N 在下文中定义）。有 k 个明文 $m_1,m_2,\cdots,m_k$，分别使用公钥 $PK_1,PK_2,\cdots,PK_k$ 对应的私钥进行签名，再进行聚集，得到 k 个用户的聚集签名 σ。

如果 σ 是这 k 个用户的有效聚集签名，并且敌手 A 并没有询问自己选择的明文 m_1 在 PK_1 对应私钥的作用下所产生的签名，则敌手 A 胜利。

定义 2　一个伪造者 $A(t,q_H,q_S,N,\varepsilon)$ 在聚集选择密钥模型中能够打破一个聚集签名方案，当且仅当：

1）A 可执行的时间上限为 t；

2）A 最多进行 q_H 次哈希询问和 q_S 次签名询问；

3）$AdvAggSig_A\geqslant\varepsilon$；

4）最多是 N 个用户产生的签名的聚集。

若不存在任何一个伪造者 $A(t,q_H,q_S,N,\varepsilon)$ 打破一个聚集签名方案，则这个方案在聚集选择密钥模型中是 $(t,q_H,q_S,N,\varepsilon)$ 安全的。

定理 1　令参数 k,G_1,G_2 是由 PG 生成的参数，G_1 中在时间 t' 内解决 CDH 问题的优势最大为 ε'，同时要求每次询问的明文信息是不同的[4]，则本文的方案是聚集选择密钥模型中 $(t,q_H,q_S,N,\varepsilon)$-安全的，则 t,ε 必须满足以下条件：

$$\varepsilon\geqslant e(q_S+N)\cdot\varepsilon',\ t\leqslant t'-c_{G_1}(q_H+6q_S+N)$$

式中，e 为自然对数，c_{G_1} 为群 G_1 中一次乘方所需的时间。

证明：假设本文的方案不是聚集选择密钥模型中 $(t,q_H,q_S,N,\varepsilon)$-安全的，则我们证明“$G_1$ 中在时间 t' 内解决 CDH 问题的优势最大为 ε'”不成立。

g_1 是 G_1 的生成元。构造挑战者 C，其要求的输入为 P，$u=s_CP+s_1P\in G_1$，$hP_1\in G_1$，并且存在 $P=t_1P_1$。目标是输出 $h(s_CP_1+s_iP_1)\in G_1$。挑战者 C 通过以下步骤与敌手 A 进行交互：

Setup　C 将 g_1 和公钥 $SP_1=\lambda_1P+u$ 发送给敌手 A，其中 λ 为随机数（$\lambda\in Zq$）；

Hash Queries　A 可以在任意时刻进行哈希询问。为了进行应答，C 维护一个列表 $\langle m^{(i)},w^{(i)},b^{(i)},c^{(i)}\rangle$（下文称 H 列表），H 列表初值为空。当 A 询问 $m\in\{0,1\}^*$ 的哈希值时，C 按照如下步骤应答：

1）如果 m 已经存在于 H 列表中，为 $\langle m,w,b,c\rangle$，则使用 w 作为 m 的哈希值进行应答；

2）否则，C 以 $Pr[c=0]=1/(q_S+N)$ 的概率选择 $c\in\{0,1\}$；

3）C 随机选择 $b\in Zq$，计算 $w=h^{(1-c)}b$；

4）C 在 H 列表中增加新元组 $\langle m,w,b,c\rangle$，并将 w 作为哈希值进行应答。

Signature Queries　A 询问 v_1 对应的私钥对 m 的签名。挑战者 C 按照如下过程应答：

1）C 先进行 Hash Queries。如果 $c=0$，则中止；

2）否则，$c=1$，显然 $w=bP_1$。令 $\sigma=[W,V]$，其中 $W=rP_1$，$V=bu+\lambda_1bP_1=rtb(s_C+s_1+\lambda/t)P_1$，$r$ 为随机数（$r\in Zq$），容易验证，σ 是公钥 $(s_C+s_1+\lambda_1/t)P$ 对应的私钥对 m 的有效签名，将此签名作为应答。

Output　A 正常终止情况下得到 $k-1(k\leqslant N)$ 个公钥 $SP_2,SP_3,\cdots,SP_k$ 以及一个聚集签名 σ，并且 A 没有询问 m_1 的签名。

当且仅当 $c_1=0,c_2=c_3=\cdots=c_k=1$ 时，$w_1=hb$，$w_i=b_i(i>1)$，聚集签名必须满足下式：

$$\prod_{i=1}^{k}\hat{e}(SP_i,w_iW_i)=\hat{e}(P,V)$$

当 $i>1$ 时：$W_i=r_iP_i$，$V_i=r_it_ib_i(s_C+s_i+\lambda_1/t_i)P_i$，此时 $\hat{e}(SP_i,w_iW_i)=\hat{e}((s_C+s_i+\lambda_i/t_i)P,t_ir_ib_iP_i)=\hat{e}(P,t_ir_ib_i(s_C+s_i+\lambda_i/t_i)P_i)$。所以 σ_i 是在公钥 $(s_C+s_1+\lambda_i/t)P$ 下的有效签名。

C 构造 $V_1=V-\sum_{i=2}^{k}V_i$，可构造出签名 $\sigma_1=[W_1,V_1]$。

通过以上就构造了挑战者 C。下面分析挑战者 C 解决 CDH 问题的优势。

分析以下 3 个事件：

E_1：C 回应所有 A 的签名询问；

E_2：A 最终产生了一个有效的聚集签名；

E_3：E_2 发生，并且 $c_1=0,c_2=c_3=\cdots=c_k=1$。

C 能够解决 CDH 问题，当且仅当以上事件全部发生。其概率描述如下：

$$Pr[E_1\wedge E_3]=Pr[E_1]\cdot Pr[E_2|E_1]\cdot Pr[E_3|E_1\wedge E_2]$$

断言 1　$Pr[E_1\wedge E_3]\geqslant\varepsilon\cdot\frac{1}{e(q_S+N)}$。

证明：A 的每一次询问，C 中止的概率最大为 $1/(q_S+N)$。最多进行 q_S 次询问，所以 $Pr[E_1]\geqslant(1-1/(q_S+N))^{q_S}$。

发送给 A 的公钥由用户和可信第三方共同决定，C 不因 A 的询问而中止，且 A 每次询问的明文信息均不相同，即 C 的应答独立分布于 G_1 中。因此，A 会产生一个有效的聚集签名，且概率至少为 ε。所以 $Pr[E_2|E_1]\geqslant\varepsilon$。

因 $Pr[c=0]=1/(q_S+N)$，在 E_1 与 E_2 发生的基础上，E_3 发生的概率等于 c 取值 $c_1=0,c_2=c_3=\cdots=c_k=1$ 的概率。因此 $Pr[E_3|E_1\wedge E_2]\geqslant(1-1/(q_S+N))^{N-1}\cdot1/(q_S+N)$。证毕。

综上所述：

$$Pr[E_1\wedge E_3]\geqslant\varepsilon\cdot\frac{1}{e(q_S+N)}\geqslant\varepsilon'$$

以上挑战-应答过程中，执行 (q_H+q_S) 次 Hash Queries 和 q_S 次 Signature Queries。每次 Hash Queries 的时间相当于 G_1 中 1 次乘方的时间，每次 Signature Queries 的时间相当于 G_1 中 3 次乘方的时间。在 Output 阶段，进行的是椭圆曲线上的加减法运算，时间可以忽略。因此总运行时间为 $t+$

$c_{G_1}(q_H+6q_S+N)\leqslant t'$。

证毕。

5 效率分析及仿真

文献[5]中的聚集签名方案是现在已经出现的基于证书的聚集签名方案，然而其用到了知识证明。知识证明的效率远低于双线性对运算的效率。本方案在验证阶段仅需 $n+1$ 次双线性对运算，相较于其它基于双线性对的聚集签名方案也有一定的优势。

利用 PBC 实现双线性对的计算，对无序聚集签名方案进行仿真实现。同时分别进行了不同用户数目的聚集签名仿真实验，对每个过程执行的时间进行监控和记录，效率曲线如图 1 所示。

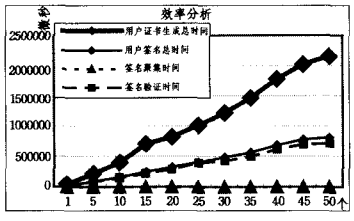

图 1 效率曲线图

在效率曲线图中，签名聚集时间保持平稳，无显著增加。这是由于在签名聚集过程中，仅用到椭圆曲线上的点加运算，相较于点乘和双线性对运算，其时间开销可忽略；在证书生成、签名聚集过程中，由于采用了计算时间开销较大的点乘和双线性对计算，因此其效率曲线与用户数目的增长成正比。

结束语 本文给出了一个高效的基于证书的聚集签名方案，并给出了两种工作模式；对方案的正确性和安全性进行分析，证明本方案在聚集选择密钥模型中是安全的。给出了无序聚集签名方案的仿真结果以及仿真效率曲线。下一步将开发基于本方案实现聚集签名工具平台。

参 考 文 献

[1] Gentry C. Certificate-based Encryption and the Certificate Revocation Problem[J]. Lecture Notes in Computer Science, 2003, 2656: 272-293

[2] Kang B G, Park J H, Hahn S G. A Certificate-based Signature Scheme[J]. Lecture Notes in Computer Science, 2004, 2964: 99-111

[3] 陆阳，李继国，肖军模. 一个高效的基于证书的加密方案[J]. 计算机科学，2009，36(9)：28-31

[4] Boneh D, Gentry C, Lynn B, et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps[C]// Proceedings of Eurocrypt'03. Berlin: Springer-Verlag, 2003: 416-432

[5] Liu J K, Baek J, Zhou J. Certificate-based Sequential Aggregate Signature[C]// Proceedings of WiSec'09. New York: ACM, 2009: 21-28

[6] 赵昌安，张方国. 双线性对有效计算研究进展[J]. 软件学报，2009，20(11)：3001-3009

(上接第 52 页)

结束语 移动无线传感器网络节点的移动特性使得节点的精确定位面临更大的挑战。本文以插值模拟为理论基础对 MCL 算法进行了改进，提出了采样区域自调整的蒙特卡洛节点定位算法(SA_MCL)。SA_MCL 算法对节点的历史位置信息进行插值模拟以获得节点的速度和运动方向，然后自动调整采样区域进行节点定位。仿真实验结果证明，SA_MCL 算法能够适应移动无线传感器网络的特点，在节点最大速度相同、锚节点密度相同、节点密度相同的情况下，SA_MCL 算法比 MCL 算法能够提供更加精确的定位服务。在获得相同定位精度的要求下，SA_MCL 算法需要的采样点数比 MCL 需要的少，从而降低了对节点存储能力的要求，降低节点的硬件成本。下一步的工作是研究运动模型及动态特性对算法健壮性、网络能耗等的影响，以使其在更加真实的网络环境中得到较好的结果。

参 考 文 献

[1] 王福豹，史龙，任丰原. 无线传感器网络中的自身定位系统和算法[J]. 软件学报，2005，16(5)：857-868

[2] Butler Z, Corke P, Peterson R, et al. Networked Cows: Virtual-Fences for Controlling Cows[C]// Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services. Boston, Massachusetts, USA, 2004, 5: 4429-4436

[3] Bahl P, Padmanabhan V. RADAR: An in-building RF-based user location and tracking system[C]// Proceedings of ACM INFOCOM. Tel Aviv, Israel, 2000: 775-784

[4] Ward A, Jones A, Hopper A. A new location technique for the active office[J]. IEEE Personal Communications, 1997, 4(5): 42-47

[5] Savvides A, Han C-C, Strivastava M B. Dynamic fine-grained localization in ad-hoc networks of sensors[C]// Proceedings of ACM MobiCom. New York, NY, USA, 2001: 166-179

[6] Niculescu D, Nath B. Ad hoc positioning system (APS) using AoA[C]// Proceedings of ACM INFOCOM. San Francisco, California, USA, 2003: 1734-1743

[7] He T, Huang C, Blum B M, et al. Range-free localization schemes for large scale sensor networks[C]// Proceedings of ACM MobiCom, San Diego. California, USA, 2003, 81-95

[8] Niculescu D, Nath B. DV-based Positioning in Ad hoc Networks [J]. Kluwer Journal of Telecommunication Systems, 2003, 22: 267-280

[9] Nagpal R, Shrobe H, Bachrach J. Organizing a Global Coordinate System from Local Information on an Ad Hoc Sensor Network [J]. Information Processing in Sensor Networks, 2003, 2634: 333-348

[10] Bulusu N, Heidemann J, Estrin D. GPS-less Low Cost Outdoor Localization for Very Small Devices[J]. IEEE Personal Communications Magazine, 2000, 7(5): 28-34

[11] Bergamo P, Mazzini G. Localization in sensor networks with fading and mobility[C]// The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. Lisboa, Portugal, 2002: 750-754

[12] Datta S, Klinowski C, Rudafshani M, et al. Distributed localization in static and mobile sensor networks[C]// IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. Montreal, Canada, 2006: 69-76

[13] Hu Ling-xuan, Evans D. Localization for Mobile Sensor Networks[C]// Proceedings of ACM MobiCom. Philadelphia, Pennsylvania, USA, 2004: 45-57