一种改进的高效的代理盲签名方案

王兴威 侯书会
(北京科技大学数理学院 北京 100083)

摘 要 通过对无证书代理盲签名方案进行分析,发现其执行效率较低。虽然该方案被证明能够抵抗恶意但被动的 KGC(Key Generation Center)攻击,但现实生活中并不存在完全可信的 KGC。文中基于 ECDLP 难题和双线性映射,提出了一种改进的无 KGC 的高效代理盲签名方案,该方案通过减少双线性映射运算的次数来提高执行效率,与刘二根等的方案相比,本文案的执行效率更高,其正确性与安全性得到了论证。

关键词 数字签名,代理盲签名,KGC,效率分析
中图法分类号 TP309 **文献标识码** A

Improved Efficient Proxy Blind Signature Scheme

WANG Xing-wei HOU Shu-hui
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract Through the analysis of the certificateless proxy blind signature scheme, we found that the efficiency of the scheme is not high. Besides, although this scheme has been proved to be able to resist malicious but passive attacks of bad KGC, there is no such KGC that can be fully trusted in the real world. Based on ECDLP problem and Bilinear Pairing, this paper presented an improved efficient proxy blind signature scheme without KGC, and demonstrates the correctness and security of the scheme.

Keywords Digital signature, Proxy blind signature, KGC, Efficiency analysis

1 引言

1983 年,Chaum 提出了盲签名[1],即签名者在无法知道消息内容的情况下对消息进行签名。1996 年,Mambo 等首次提出代理签名的思想[2],即原始签名者将签名的权利授予一个代理签名者,由代理签名者对消息进行签名。2000 年,Lin 等将代理签名和盲签名技术结合,提出了代理盲签名的概念[3]。代理盲签名不仅具备普通数字签名的基本特性,同时还具备盲性和不可链接性,这些特性使其在现实生活中有广泛的应用[4]。例如,为了保护用户的隐私,电子现金系统要求银行工作人员(签名者)在发行电子现金(签名)时不能看到来自用户的消息(盲性)、银行工作人员不能知道自己何时对某一条消息进行了签名(不可链接性),因此代理盲签名的研究具有重要意义。

近年来,学者们针对代理盲签名进行了许多研究,但提出的方案普遍存在执行效率低、不能抵抗伪造攻击等问题,越来越多的学者开始研究代理盲签名的安全性[5-8]。2008 年,农强等[9]基于双线性映射提出了一种基于身份的代理盲签名方案,并证明了该方案满足不可伪造性。2011 年,张晓敏[10]基于双线性映射提出了一种无 PKI(Public Key Infrastructure)的代理盲签名方案,解决了密钥托管问题,证明了该方案是存在性不可伪造的,且其执行效率高于农强等的方案。为进一步提高执行效率,文佳骏等[11]于 2014 年提出了一个高效的无证书代理盲签名方案,该方案通过对部分密钥进行适当修改及减少双线性映射的运算次数来提高执行效率。2015 年,周明等[11]提出了一种可证安全的高效的代理盲签名方案,证明了其在选择消息/授权文件攻击下是不可伪造的,根据 Barreto 等的研究结果[12],论证了其方案执行效率高于文佳骏的方案。2016 年,刘二根等通过分析张晓敏的方案,发现其不能抵抗恶意但被动的 KGC 攻击和恶意用户的签名伪造攻击,于是针对这些问题,提出了一种新的改进的无证书代理盲签名方案[13]。

本文通过对刘二根等方案的分析,发现其执行效率较低。鉴于此,本文提出了一个改进的无 KGC 的高效代理盲签名方案,通过减少双线性映射的运算次数来提高执行效率,通过去除密钥生成中心来加强安全性。

2 预备知识

2.1 双线性映射

设 G_1,G_2 分别是由 P 生成的 q 阶加法群和乘法群,e:$G_1\times G_1\rightarrow G_2$ 是满足下面 3 个性质的双线性映射。

(1)双线性性:对于 $\forall P,Q\in G_1$,$a,b\in Z_q^*$,$e(aP,bQ)=e(P,Q)^{ab}$;

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

(3)可计算性:对于给定的 $P,Q\in G_1$,存在一个有效的算法计算 $e(P,Q)$。

2.2 椭圆曲线上的离散对数难题(Elliptic Curve Discrete Logarithm Problem, ECDLP)

设 E 为定义在有限域 $GF(q)$ 上的椭圆曲线,对于给定的 E

王兴威(1993-),男,硕士生,主要研究方向为密码学与信息安全;**侯书会**(1971-),女,博士,副教授,主要研究方向为信息安全与计算机取证,E-mail:shuhui@ustb.edu.cn(通信作者)。

上的两点 P 和 Q，求满足 $Q=xP$ 的 x 在计算上是非常困难的。

3　刘二根提出的代理盲签名方案

3.1　系统初始化

该方案包含 5 个成员：原始签名者 A、代理签名者 B、用户 C、验证者及密钥生成中心 KGC。

G_1 为有限域上椭圆曲线 E 的点构成的加法循环群，其阶为 q，生成元为 P。G_2 是阶也为 q 的循环乘法群，$e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射，KGC 选择 3 个安全的哈希函数：$H_1:\{0,1\}^*\times G_1\rightarrow Z_q^*$，$H_2:\{0,1\}^+\rightarrow Z_q^+$，$H_3:\{0,1\}^*\times G_1\rightarrow Z_q^*$，随机选择系统主密钥 $s\in Z_q^*$，并计算系统公钥 $P_{pub}=sP$，公开系统参数 $params=\{G_1,G_2,P,q,e,H_1,H_2,H_3,P_{pub}\}$。

3.2　公钥生成

原始签名者 A 随机选择秘密值 $x_A\in Z_q^*$，并计算 $X_A=x_AP$，$Y_A=x_AP_{pub}$，A 的公钥为 $PK_A=(X_A,Y_A)$。

3.3　用户密钥提取

原始签名人 A 将其身份信息 ID_A 发送给密钥生成中心 KGC。KGC 计算 $Q_A=H_1(ID_A,PK_A)$，$D_A=sQ_A$。D_A 为 A 的部分私钥，并通过安全信道发送给 A。A 可以通过验证等式 $e(D_A,P)=e(Q_A,P_{pub})$ 是否成立来判断部分私钥的正确性。A 计算 $SK_A=x_AD_A$ 后将其作为自己的私钥。同理，代理签名者 B 的公钥、私钥生成方法与 A 的相同，即公钥 $PK_B=(X_B,Y_B)$，私钥为 (SK_B,D_B)。

3.4　代理授权

原始签名者 A 首先生成一个包含双方身份、代理权限、代理期限等信息的授权证书 M_w，随机选择 $r\in Z_q^*$，计算 $e(P,P)^r=G$，$S_w=SK_A+H_2(M_w,G,PK_A)rP$，将 (S_w,M_w,G) 通过安全信道发送给 B。B 收到 (S_w,M_w,G) 后，首先通过验证等式 $e(X_A,P_{pub})=e(Y_A,P)$ 是否成立来验证 A 的公钥是否合法，再验证等式 $e(S_w,P)=e(Q_A,Y_A)G^{H_2(M_w,G,PK_A)}$ 是否成立。若等式成立，则计算代理密钥 $S_p=S_w+SK_B$。

3.5　代理盲签名生成

(1)代理签名者 B 随机选取 $P'\in_RG_1$，计算 $k=e(P,P')$，将 k 发送给用户 C；

(2)C 随机选择 $a,b\in_RZ_q^*$，$P^*\in G_1$，计算 $U=k^ae(P,P^*)^b$，$h=H_3(m,U)$，$h'=a^{-1}h$，将 h' 发送给 B；

(3)B 收到 h' 后，计算 $S'=h'S_p+P'$，将 S' 发送给 C；

(4)C 收到 S' 后，计算 $S=aS'+bP^*$，$\sigma=(M_w,U,G,S)$ 就是关于消息 m 的代理盲签名。

3.6　代理盲签名验证

签名验证者首先计算 $h=H_3(m,U)$，然后验证等式 $H_3(m,e(S,P)T^{-h}G^{-hH_2(M_w,G,PK_A)})=h$ 是否成立，其中 $T=e(Q_A,Y_A)e(Q_B,Y_B)$。若等式成立，则接受该签名，否则拒绝。

3.7　安全性及效率分析

刘二根等证明了其方案可以抵抗公钥替换攻击和恶意但被动的 KGC 攻击，但现实中并不存在完全可信的 KGC，其方案仍存在一定的安全隐患。

刘二根的方案基于双线性映射，由 KGC 生成部分私钥。当原始签名者和代理签名者收到部分私钥时，需要验证其有效性，增加了双线性映射的运算次数，导致执行效率较低。

4　改进的代理盲签名方案及安全性

本文基于刘二根等的方案提出了一个改进的高效的代理盲签名方案：通过去除密钥生成中心来加强方案的安全性，通过减少双线性映射的运算次数来提升执行效率。方案由系统初始化、密钥生成、代理授权、代理盲签名生成及验证等几部分构成。

4.1　系统初始化

G_1 为有限域上椭圆曲线 E 的点构成的加法循环群，其阶为 q，生成元为 P，G_2 是阶也为 q 的循环乘法群。$e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射。$H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\times G_2\rightarrow Z_q^*$ 为两个安全的哈希函数。公开的参数为 $params=\{G_1,G_2,P,q,e,H_1,H_2\}$。

4.2　密钥生成

原始签名者 A 和代理签名者 B 分别选择 $x_A\in Z_q^*$，$x_B\in Z_q^*$ 作为自己的私钥，计算 $Q_A=H_1(ID_A)$，$Q_B=H_1(ID_B)$ 并公开。然后，他们分别计算 $X_A=x_AP$，$X_B=x_BP$，并将 (X_A,Q_A)，(X_B,Q_B) 作为自己的公钥并公开。

4.3　代理授权

代理签名者 B 计算 $Y_B=x_BQ_B$ 并将其发送给原始签名者 A。在 A 收到后，验证 $e(Y_B,P)=e(Q_B,X_B)$ 是否成立。若成立，则 A 生成一个包含双方身份、代理权限、代理期限等信息的授权证书 M_w，然后计算 $Y_A=x_AQ_A$，计算证书的签名 $S_w=x_AH_1(M_w)$，并将 (Y_A,M_w,S_w) 发送给 B。

B 收到 (Y_A,M_w,S_w) 后，验证 $e(Y_A,P)=e(Q_A,X_A)$，$e(S_w,P)=e(H_1(M_w),X_A)$ 是否成立。若成立，则计算 $S_p=x_BH_1(M_w)+S_w$，将其作为代理签名密钥。

4.4　代理盲签名生成及验证

(1)代理签名者 B 随机选取 $P'\in_RG_1$，计算 $k=e(P',P)$，将 k 发送给用户 C；

(2)用户 C 随机选择 $a,b\in_RZ_q^*$，$P^*\in G_1$，计算 $U=k^{a^{-1}}e(P^*,P)^b$，$h=H_2(m,U)$，$h'=ah$，将 h' 发送给 B；

(3)代理签名者 B 收到 h' 后，计算 $S'=h'S_p+P'$，将 S' 发送给 C；

(4)用户 C 收到 S' 后，计算 $S=a^{-1}S'+bP^*$，$\sigma=(m,M_w,U,S)$ 就是消息 m 的代理盲签名。

(5)签名验证者收到代理盲签名后，计算 $h=H_2(m,U)$，然后验证等式 $e(S,P)=e(H_1(M_w),X_A+X_B)^hU$ 是否成立。若等式成立，则接受该签名，否则拒绝。

4.5　改进方案的正确性

改进方案是正确的，证明如下：

$$\begin{aligned}e(S,P)&=e(a^{-1}S'+bP^*,P)\\&=e(a^{-1}(h'S_p+P')+bP^*),P)\\&=e(a^{-1}ahS_p+a^{-1}P'+bP^*,P)\\&=e(hS_p,P)e(P',P)^{a^{-1}}e(P^*,P)^b\\&=e(x_BH_1(M_w)+S_w,P)^hU\\&=e(H_1(M_w),X_A+X_B)^hU\end{aligned}$$

4.6　改进方案的安全性

(1)存在性不可伪造

代理盲签名方案在已知消息攻击下满足存在性不可伪造即指在获得与已知消息对应的签名但不知道密钥的情况下，攻击者成功伪造有效签名的概率是可忽略的。

定理 1　在 ECDLP 难题假设下，本方案在已知消息攻击下是存在性不可伪造的。

证明：假设攻击者对消息 m 伪造了一个签名 $\sigma^*=(m,M_w,U^*,S^*)$，显然 $\sigma^*\neq\sigma$，而且满足：

$e(S^*,P)=e(H_1(M_w),X_A+X_B)^{h^*}U^*$

因为 $U^*\in G_2$，$e:G_1\times G_1\rightarrow G_2$ 是一个双线性映射，故存在 w^* 使得：

$U^*=e(w^*P,P)$

因此，有：

$$\begin{aligned}e(S^*,P)&=e(h^*H_1(M_w),X_A+X_B)U^*\\&=e(h^*H_1(M_w),X_A+X_B)e(w^*P,P)\\&=e((h^*H_1(M_w)(x_A+x_B)+w^*)P,P)\end{aligned}$$

从而，有：

$S^*=(h^*H_1(M_w)(x_A+x_B)+w^*)P$

即攻击者已知 S^*，$P\in G_1$，能够找到 $h^*(x_A+x_B)H_1(M_w)+w^*$ 使得上式成立。这意味着攻击者破解了 ECDLP 难题，与事实矛盾，故攻击者不能通过已知消息 m 伪造签名。

定理 2 用户 C 伪造代理盲签名在计算上是不可行的。

证明：用户 C 伪造代理盲签名在计算上是不可行的即指用户 C 通过保留的参数生成有效签名的概率在多项式时间内是可忽略的。

假设在完成了一次代理盲签名后，用户 C 保留了签名过程中的参数(k,a,b,P^*,U,h,h',S',S)。若用户 C 伪造 $S^*=a^{*-1}S'+b^*P^{**}$，使得：

$$\begin{aligned}e(S^*,P)&=e(a^{*-1}S'+b^*P^{**},P)\\&=e(a^{-1}(h'S_p+P')+bP^*),P)\\&=e(a^{*-1}ahS_p+a^{*-1}P'+b^*P^{**},P)\\&=e(a^{*-1}ahS_p,P)e(P',P)^{a^{*-1}}e(P^{**},P)^{b^*}\\&=e(H_1(M_w),X_A+X_B)^{a^{*-1}ah}U^*\end{aligned}$$

成立是不可能的。根据哈希函数的单向性可知，同时令 $h^*=a^{*-1}ah$，$U^*=e(P',P)^{a^{*-1}}e(P^{**},P)^{b^*}$ 且满足 $h^*=H_2(m,U^*)$是不可能的。

定理 3 代理签名者 B 伪造代理盲签名在计算上是不可行的。

证明：代理签名者 B 伪造代理盲签名在计算上是不可行的即指代理签名者 B 通过保留参数伪造有效签名的概率是可忽略的。

假设在完成了一次代理盲签名后，代理签名者 B 保留了签名过程中的参数(k,U,h',S')。若代理签名者 B 伪造 $S^*=a^{*-1}S'+b^*P^{**}$，使得：

$$\begin{aligned}e(S^*,P)&=e(a^{*-1}S'+b^*P^{**},P)\\&=e(a^{-1}(h'S_p+P')+bP^*),P)\\&=e(a^{*-1}ahS_p+a^{*-1}P'+b^*P^{**},P)\\&=e(a^{*-1}ahS_p,P)e(P',P)^{a^{*-1}}e(P^{**},P)^{b^*}\\&=e(H_1(M_w),X_A+X_B)^{a^{*-1}ah}U^*\end{aligned}$$

成立是不可能的。由哈希函数的单向性可知，同时令 $h^*=a^{*-1}ah$，$U^*=e(P',P)^{a^{*-1}}e(P^{**},P)^{b^*}$ 且满足 $h^*=H_2(m,U^*)$是不可能的。

定理 4 原始签名者 A 冒充代理签名者 B 伪造代理盲签名在计算上是不可行的。

证明：原始签名者 A 冒充代理签名者 B 伪造代理盲签名在计算上是不可行的即指原始签名者 A 冒充代理签名者 B 伪造有效签名的概率是可忽略的。

原始签名者若想冒充代理签名者，需要获得 S_p。由于 S_p 为代理密钥并不公开，且 $S_p=x_BH_1(M_w)+S_w$，设 $x_BH_1(M_w)=Q\in G_1$，因 $H_1(M_w)\in G_1$，若能找到 x' 使得 $x'H_1(M_w)=Q$ 成立，相当于解决了 ECDLP 难题，概率可以忽略不计，故原始签名者不能得到 S_p 的值，即使他伪造了 x_B 也无法计算出 S'，也就无法冒充代理签名者生成代理盲签名。

(2)盲性

对于一个给定的消息签名(m,M_w,U,S)，代理签名者即使在签名过程中保存了(h',S')，也无法计算出盲化因子 a 和 b。代理签名者无法求解 $h'=ah$，因为盲化因子 a 和参数 h 对代理签名者都是未知的；如果代理签名者求解了 $U=k^{a^{-1}}e(P,P^*)^b$，相当于破解了 ECDLP 难题。因此，代理签名者无法知道消息 m 的内容，本方案满足盲性。

(3)不可链接性

用户使用盲化因子 a 和 b 来盲化消息 m。代理签名者无法知道 a 的值，故无法知道所签名的消息。在签名公布后，虽然代理签名者知道了该签名对应的消息，但他不知道自己何时对该消息签名，因此本方案满足不可链接性。

(4)不可否认性

因为授权证书 M_w 包括原始签名者和代理签名者的身份信息、代理权限和代理期限等内容，所以一旦代理盲签名有效，那么原始签名者和代理签名者都不可以否认该签名。

(5)可区分性

由于验证等式中含有原始签名者和代理签名者的公钥 X_A，X_B，因此本方案满足可区分性。

5 效率分析

为了进一步说明本文提出的方案在执行效率方面的优越性，我们将本文提出的方案与梁林[14]的方案、刘二根[15]的方案进行了比较，统计了这 3 个方案在代理盲签名算法和验证算法阶段的计算量，结果如表 1 所列。

表 1 几种方案的效率比较

算法	代理授权过程	盲签名过程	验证过程	总计算量
梁林的方案	$3T_b+4T_s+T_e+8T_h+T_a$	$4T_b+T_s+3T_e+4T_h+T_a$	$3T_b+T_e+4T_h+2T_c$	$10T_b+5T_s+5T_e+16T_h+2T_a+2T_c$
刘二根的方案	$7T_b+6T_s+2T_e+2T_h+2T_a$	$2T_b+4T_s+T_e+T_h+2T_a+T_c$	$3T_b+3T_e+3T_h$	$12T_b+10T_s+6T_e+6T_h+4T_a+T_c$
本文方案	$6T_b+6T_s+T_a$	$2T_b+4T_s+T_e+T_h+2T_a+2T_c$	$2T_b+T_e+T_h+T_a$	$10T_b+10T_s+2T_e+2T_h+4T_a+2T_c$

注：T_c 为求逆运算次数，T_h 为 Hash 函数运算次数，T_s 为 G_1 上的标量乘运算次数，T_a 为 G_1 上的加法运算次数，T_e 为 G_2 上的模指数运算次数，T_b 为双线性映射运算次数

根据表 1，本文方案比刘二根的方案减少了 2 次双线性映射运算，减少了 4 次在群 G_2 上的模指数运算，减少了 4 次哈希函数运算，增加了 1 次求逆运算。根据文佳骏及 Barreto 等的研究结论[9,11]，双线性映射在计算复杂度上远远大于求逆运算，因此本文方案在效率上优于刘二根方案。本方案与梁林的方案有相同次数的双线性映射运算，但本方案的哈希函数运算次数远远少于梁林方案，效率比梁林的方案更高。

结束语 基于刘二根的代理盲签名方案，提出了一个改进的无 KGC 的高效代理盲签名方案。与原方案相比，提出的方案有更高的安全性和执行效率。下一步将在具体应用方面

加强研究，尤其是在电子现金系统中的应用，使其具有更高的实用性。

参 考 文 献

[1] CHAUM D. Blind Signature for Untraceable Payments[C]// Advance in Cryptology: Proceedings of Crypto'82. 1983: 199-203.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy signa-ture for delegating signing operation[C]// Proceedings of the 3rd ACM Conference on Computer and Communications Security. ACM, 1996: 48-57.

[3] LIN W D, JAN J K. A security personal learning tools using a proxy blind signature scheme[C]// Proc of International Conference on Chinese Language Computing. 2000: 273-277.

[4] 计国民. 双线性对代理盲签名在电子选举中的应用[J]. 菏泽学院学报，2015，37(2)：20-23.

[5] 左黎明，郭红丽，张婷婷，等. 一种无双线性对的代理盲签名方案[J]. 华东交通大学学报，2016，33(5)：139-142.

[6] 韩春霞，王琳杰. 两种代理盲签名方案的安全性分析[J]. 科技信息，2013，23：53-61.

[7] 林振宇，贺亚威，侯整风. 改进的代理盲签名方案[J]. 合肥工业大学学报(自然科学版)，2015，38(1)：40-43.

[8] 张瑛瑛，陈玮，曾吉文. 对一个无证书代理盲签名方案的分析与改进[J]. 计算机应用研究，2014，31(2)：540-542.

[9] 农强，吴顺祥. 一种基于身份的代理盲签名的分析与改进[J]. 计算机应用，2008，28(8)：1940-1942.

[10] 张晓敏. 一类高效的无证书代理盲签名方案[J]. 计算机安全，2011(3)：54-59.

[11] 文佳骏，左黎明，李彪. 一个高效的无证书代理盲签名方案[J]. 计算机工程与科学，2014，36(3)：452-457.

[12] 周明，王箭. 一个可证安全的高效的代理盲签名方案[J]. 计算机工程与科学，2015，37(9)：1643-1651.

[13] BARRETO P S L M. GALBRAITH S D, O'HEIGEARTAIGH C, et al. Efficient pairing computation on super singular abelian varieties[J]. Designs, Codes and Cryptography, 2007, 42(3): 239-271.

[14] 梁林. 一种新的基于身份的代理盲签名方案[J]. 赤峰学院学报(自然科学版)2017，33(2)：22-24.

[15] 刘二根，王霞，周华静，等. 改进的无证书代理盲签名方案[J]. 计算机科学，2016，43(8)：92-94.

(上接第 342 页)

结束语　在分析了三维 UWSN 的特点及有关协议标准后，提出了适应三维水下环境特点的具有跨层特性的多跳分布式 UWSN 三维系统模型。本文弥补了 DCREDT 选择算法能量空间分布不均的缺点，创新引入能量门限和距离算法，提出了 UDCREDT 算法。同时，确定了门限值的设置方法，并定量分析了传输距离对协作 MIMO 系统能耗的影响(与距离门限有关)以及负载能耗均衡性对网络寿命的影响(与能量门限有关)等。此外，考虑动态分簇算法中随机等待时间的能量算法在分布均衡性上的不足，增加了距离算法。最后，通过仿真分析验证了 UDCREDT 算法的合理有效性，有效提高了网络性能，延长了水下无线传感器网络的使用寿命。往后将着重从跨层设计角度深入研究相应的水下 MAC 协议等。

参 考 文 献

[1] 郭忠文，罗汉江，洪锋，等. 水下无线传感器网络的研究进展[J]. 计算机研究与发展，2010，47(3)：377-389.

[2] SARAFIABADI S, BERQIA A, PARVENEH S. Survey of Routing Protocols in Underwater WSNs for Mine Detection[C]// Proceedings of the 4th International Conference on Computer Modeling and Simulation. IACSIT Press, 2012.

[3] 梁平元，刘星成，石春，等. 基于协作 MIMO 的多跳 WSN 动态分簇选择算法研究[J]. 自动化学报，2010，36(10)：1401-1408.

[4] LIU X C, GONG X R, ZHENG Y Z. Reliable Cooperative Communications Based on Random Network Coding in Multi-Hop Relay WSNs[J]. IEEE Sensors Journal, 2014, 14(8): 2514-2523.

[5] 周桃云，梁平元，成运，等. 面向实时监测无线传感网络应用的通信协议[J]. 测绘科学，2016，41(10)：181-185.

[6] 赵巧梅，周桃云. 无线传感网络中一种新的簇首自适应让位分簇算法研究[J]. 邵阳学院学报(自然科学版)，2016，13(3)：56-61.

[7] YAN H, SHI Z J, CUI J H. DBR: Depth-Based Routing for Underwater Sensor Networks[C]// Proceedings of the 7th International IFIP-TC6 Networking Conference on Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. Springer Press, 2008: 1-13.

[8] XIE P, CUI J H, LAO L. VBF: Vector-Based Forwording Protocol for Underwater Sensor Networks[J]. Lecture Notes in Computer Science, 2006: 1-20.

[9] LIU G Z, LI Z B. Depth-Based Mutil-hop Routing Protocol for Underwater Sensor Network[C]// Proceedings of the 2th International Conference on Industrial Mechatronics and Automation. IEEE Press, 2010: 268-270.

[10] NICOLAOU N, SEE A, XIE P, et al. Inproving the Roubustness of Location-Based Routing for Underwater Sensor Networks[C]// Proceedings of IEEE Oceans'07. IEEE Press, 2007: 1-6.

[11] YU H T, YAO N M, WANG T, et al. WDFAD-DBR: Weighting Depth and Forwarding Area Division DBR Routing Protocol for UASNs[J]. Ad Hoc Networks, 2016, 37(37): 256-282.

[12] YU H T, YAO N M, LIU J. An Adaptive Routing Protocol in Underwater Sparse Acoustic Sensor Networks[J]. Ad Hoc Networks, 2015, 34(34): 121-143.

[13] AYAZ M, ABDULLAH A, JUNG L T. Dynamic Cluster Based Routing for Underwater Wireless Sensor Networks[C]// Proceedings of International Symposium on Information Science and Engineering, IEEE Computer Society. IEEE Press, 2010.

[14] CHEN Y S, JUANG T Y, LIN Y W, et al. A Low Propagation Delay Mutil-Path Routing Protocol for Underwater Sensor Networks[J]. Journal of Internet Techonolog, 2010, 11(2): 153-165.

[15] KUO L C, MELODIA T. Cross-layer Routing on MIMO-OFDM Underwater Acoustic links[C]// Proceedings of the 9th Annual IEEE Communications Society Conference on SECON. IEEE Press, 2012: 227-235.

[16] 李鑫滨，高梦玲，闫磊. 一种负载均衡且能量高效的水下传感网络分簇协议[J]. 电信科学，2016，32(11)：42-49.

[17] 陈岩，曾娟，杜立君，等. 基于 ADSP-BF533 的水声调制解调器[J]. 声学技术，2008，27(4)：46-48.