无可信 PKG 的盲签名方案的安全性分析及改进*

李 莎，李 虓，何明星，罗大文
（西华大学 数学与计算机学院，成都 610039）

摘 要： 针对周萍等人的无可信 PKG 的盲签名方案详细分析了其安全性，指出方案不能抵抗敌手 A_{I} 伪造攻击，敌手 A_{I} 可对用户的部分公钥进行替代，生成对任意消息的合法盲签名。为此，提出了相应的改进方案。改进的方案在验证等式中增加了系统参数，有效地证明了签名者拥有合法的 S_{ID}，从而防止了敌手 A_{I} 的公钥替代攻击。分析表明，改进的方案是安全的，能抵抗敌手 A_{I}，A_{II}，A_{III} 的伪造攻击。

关键词： 盲签名；基于身份；无可信私钥生成中心；伪造攻击；替代公钥
中图分类号： TP309.2 **文献标志码：** A **文章编号：** 1001-3695(2016)03-0873-03
doi:10.3969/j.issn.1001-3695.2016.03.053

Security analysis and improvement of blind signature scheme without trusted PKG

Li Sha, Li Xiao, He Mingxing, Luo Dawen
(*School of Mathematics & Computer Engineering, Xihua University, Chengdu* 610039, *China*)

Abstract: This paper analyzed the security of blind signature scheme without trusted PKG proposed by Zhou Ping, et al. It showed that the scheme couldn't resist the forgery attack of the type one adversary A_{I}. The adversary A_{I} could substitute the user's partial public key and forge a valid blind signature on the arbitrary message. Therefore, this paper proposed an improved scheme. In the improved scheme, it added some system parameters in the verification equation, thus effectively proved the validity of the signer's S_{ID} and resisted the public key replacement attack of adversary A_{I}. Analysis result shows that the improved sheme is secure, it can resist the forgery attacks of the adversary A_{I}, A_{II} and A_{III}.

Key words: blind signature; ID-based; without trusted PKG; forgery attack; substitute public key

0 引言

1982 年，Chaum 提出了盲签名[1]的概念。盲签名是一种特殊的数字签名，签名者对所签署的消息是不可见的，盲签名在隐私保护上有非常重要的应用。传统的公钥密码体制中，用户的公钥需要通过公钥证书来认证，而用户的公钥证书需要公钥基础设施(PKI)来进行管理，这增加了系统的开销。为了简化 PKI 对密钥的管理和取消公钥证书，Shamir[2] 于 1984 年提出了基于身份的公钥密码体制。他把用户的公开信息作为用户的公钥，用户的私钥由私钥生成中心(PKG)生成，用户的公钥不需要公钥证书去进行认证，从而极大地提高了密钥管理的效率。在基于身份的密码体制[2]中，由于用户的私钥是由 PKG 生成的，密钥托管问题就成了基于身份密码体制不可避免的缺陷。

为了克服密钥托管问题，密码学者提出了无证书的公钥密码体制[3]、基于身份的无可信 PKG 的密码体制[4]和基于证书的密码体制[5]。在无证书[3]及无可信 PKG[4]的公钥密码体制中，用户的私钥由 PKG 生成的部分私钥和用户自选的一个秘密值组成，用户自己生成一个部分公钥。在基于证书的密码体制中，用户的私钥为用户自己选取的一个秘密值，用户的公钥由用户的秘密值生成，PKG 为用户的身份和公钥生成相应的证书。因为 PKG 无法知道用户的秘密值[3~5]，从而有效地克服了基于身份的密码体制的密钥托管问题。把无可信 PKG 的公钥密码体制和盲签名技术结合起来，于是出现了基于身份的无可信 PKG 的盲签名[6~12]。无可信 PKG 的密码体制中，用户的部分公钥是自己生成的，没有被注册认证，容易遭到部分公钥被替代攻击。

2012 年，周萍等人[12]提出了一个高效的无可信 PKG 的盲签名方案，并声称他们的方案是高效的，可以抵抗适应性选择消息和身份攻击(即抵抗敌手 A_{I} 的伪造攻击)，抵抗不可信 PKG 的攻击(即抵抗敌手 A_{II} 和 A_{III} 的伪造攻击)。本文对周萍等人的方案进行了安全性分析，发现他们的方案不能抵抗敌手 A_{I} 的伪造攻击，当用追溯算法时可以陷害诚实的 PKG，并给出了相应的改进方案。

1 Z-H 盲签名方案及其安全性分析

1.1 Z-H 盲签名方案回顾

2012 年，周萍等人[12]提出了一个高效无可信 PKG 的新型盲签名方案，这里简记为 Z-H 盲签名方案。在文献[12]中首先提出了一个新的基于身份无可信 PKG 的签名方案，即方案 1；基于方案 1，作者又提出了新的基于身份无可信 PKG 的盲签名方案，即方案 2，即 Z-H 盲签名方案。下面简单介绍文献

收稿日期：2014-11-11；修回日期：2014-12-28 基金项目：国家自然科学基金资助项目(U1433130)；四川省重点基金资助项目(SZD0802-09-1)；西华大学重点实验室开放研究基金资助项目(S2jj2012-029)

作者简介：李莎(1989-)，女，硕士研究生，主要研究方向为密码学与信息安全(lxgbxh@126.com)；李虓(1972-)，男，副教授，硕士，主要研究方向为密码学与信息安全；何明星(1964-)，男，教授，博士，主要研究方向为密码学与信息安全；罗大文(1972-)，男，副教授，硕士，主要研究方向为密码学与信息安全.

[12] 中的两个方案，细节请查阅文献 [12]。

1) 方案 1 [12]

a) 系统建立。设 G_1 是阶为 q 的加法群，G_2 是阶为 q 的乘法群，双线性映射 $e: G_1 \times G_1 \to G_2$，$G_1$ 的任一生成元 P，$g = e(P,P)$。系统主密钥 $s_{pkg} \in_R Z_q^*$ 由 PKG 选取，系统公钥 $P_{pkg} = s_{pkg}P$，hash 函数 $H_1: \{0,1\}^* \to Z_q^*$，$H_2: \{0,1\}^* \times G_2 \to Z_q^*$。系统主密钥 s_{pkg} 由 PKG 保存，并公开系统参数 $\{G_1, G_2, q, P, e, g, P_{pkg}, H_1, H_2\}$。

b) 生成密钥。用户 U 把自己的 ID 发送给 PKG。PKG 计算用户 U 的部分私钥 $S'_{ID} = P/(s_{pkg} + H_1(ID))$。用户 U 验证等式 $e(S'_{ID}, P_1) = g$，其中 $P_1 = P_{pkg} + H_1(ID)P$，若等式成立则接受 S'_{ID}；否则要求 PKG 重新发送。

c) 用户 U 选取整数 $c \in_R Z_q^*$，计算 $S_{ID} = c \cdot S'_{ID}$，$Q_{ID} = g^c$，公开部分公钥 Q_{ID}，保密私钥 S_{ID}。

d) 签名。用户 U 选取 $k \in_R Z_q^*$，计算 $K = (Q_{ID})^k$，$h = H_2(m, K)$，$S = (k + h)S_{ID}$，则消息 m 的签名即为 (S,h)。

e) 验证签名。若验证等式 $h = H_2(m, e(S, P_{pkg} + H_1(ID)P)(Q_{ID})^{-h})$ 成立，消息 m 的签名 (S,h) 有效；否则无效。

2) 方案 2 [12]

a) 系统建立。同方案 1，建立系统参数 $\{G_1, G_2, q, P, e, g, P_{pkg}, H_1, H_2\}$，保密系统私钥 s_{pkg}。

b) 生成密钥。同方案 1 所述，用户 U 选取整数 $c \in_R Z_q^*$，计算 $S_{ID} = c \cdot S'_{ID}$，$Q_{ID} = g^c$，$g_{ID} = e(P, P_1)$ 公开自己的公钥 (Q_{ID}, g_{ID})，保密签名私钥 S_{ID}。

c) 签名。设用户 U 被请求签名者 A 要求对消息 m 进行盲签名。交互过程如下：

(a) U 选取 $k \in_R Z_q^*$，计算 $K = (Q_{ID})^k$，将 K 发给 A。

(b) 盲化消息。A 选取三个整数 $\alpha, \beta, \lambda \in_R Z_q^*$，计算 $r = K^{\alpha}(Q_{ID})^{\beta}(g_{ID})^{\lambda}$，$h = H_2(m, r)$，$h_0 = \alpha^{-1}(h + \beta)$，将 h_0 发送给 U。

(c) 签名。U 用自己的私钥 S_{ID} 签名 $S_0 = (k + h_0)S_{ID}$，将 S_0 发送给 A。

(d) 脱盲。A 进行脱盲运算：$S = \alpha S_0 + \lambda P$，则消息 m 的签名即为 (S,h)。

d) 验证签名。若验证等式

$$h = H_2(m, e(S, P_{pkg} + H_1(ID)P)(Q_{ID})^{-h})$$

成立，消息 m 的签名 (S,h) 有效；否则无效。

1.2 Z-H 盲签名方案的安全性分析

下面首先对 Z-H 盲签名方案的方案 1 进行安全性分析。

敌手 A_I 虽然无法获取签名者的部分私钥 S'_{ID} 和秘密值 c，但敌手 A_I 可以替换用户的部分公钥 Q_{ID}，并进行伪造攻击。敌手 A_I 可任意假冒用户 U（其身份为 ID）对任意消息 m' 进行伪造签名，具体过程如下：

a) A_I 首先计算 $P_1 = P_{pkg} + H_1(ID)P$ 和 $g_{ID} = e(P, P_1)$。

b) A_I 随机选取 $c' \in_R Z_q^*$，替换用户的部分公钥 Q_{ID} 为 $Q'_{ID} = g_{ID}^{c'}$。

c) A_I 对任选的消息 m'，任选 $R \in G_1$，令 $K' = e(R, P_1)$，$h' = H_2(m', K')$，计算 $S' = R + h'c'P$，则伪造的签名为 (S',h')。显然 (S',h') 是一个有效的签名，这是因为

$$\begin{aligned}
&H_2(m', e(S', P_{pkg} + H_1(ID)P)(Q'_{ID})^{-h'}) = \\
&H_2(m', e(R + h'c'P, P_1)(g_{ID})^{-h'c'}) = \\
&H_2(m', e(R, P_1)e(h'c'P, P_1)e(P, P_1)^{-h'c'}) = \\
&H_2(m', e(R, P_1)e(P, P_1)^{h'c'}e(P, P_1)^{-h'c'}) = \\
&H_2(m', e(R, P_1)) = H_2(m', K') = h'
\end{aligned}$$

对于 Z-H 盲签名方案的方案 2，即 Z-H 盲签名方案，敌手 A_I 可采用与方案 1 相同的攻击方法，任意假冒用户 U（其身份为 ID）对任意消息 m' 进行伪造盲签名。下面分两种情形来伪造盲签名：

情形 1 敌手 A_I（即签名请求者 A）伪造用户 U（身份为 ID）对任意消息 m' 的盲签名，具体方法如下：

a) A_I 随机选取 $c' \in_R Z_q^*$，替换用户的部分公钥 $Q_{ID} = g^c$ 为 $Q'_{ID} = g_{ID}^{c'} = e(P, P_1)^{c'}$。

b) A_I 对任选的消息 m'，任选 $R \in G_1$，令

$$r' = e(R, P_1) = e(R, P_{pkg} + H_1(ID)P)$$
$$h' = H_2(m', r')$$

计算 $S' = R + h'c'P$，则敌手 A_I（即签名请求者 A）伪造的盲签名为 (S',h')。由于 (S',h') 不是用户 U 生成的签名，显然 (S',h') 对用户 U 来说是盲的。同时 (S',h') 是一个有效的签名，这是因为

$$\begin{aligned}
&H_2(m', e(S', P_{pkg} + H_1(ID)P)(Q'_{ID})^{-h'}) = \\
&H_2(m', e(R + h'c'P, P_1)(g_{ID})^{-h'c'}) = \\
&H_2(m', e(R, P_1)e(h'c'P, P_1)e(P, P_1)^{-h'c'}) = \\
&H_2(m', e(R, P_1)e(P, P_1)^{h'c'}e(P, P_1)^{-h'c'}) = \\
&H_2(m', r') = h'
\end{aligned}$$

情形 2 敌手 A_I 假冒用户 U（其身份为 ID）为签名请求者 A 对消息 m' 生成盲签名，具体方法如下：

a) A_I 随机选取 $c' \in_R Z_q^*$，替换用户的部分公钥 $Q_{ID} = g^c$ 为 $Q'_{ID} = g_{ID}^{c'} = e(P, P_1)^{c'}$。

b) A_I 选取 $R \in G_1$，计算 $K' = e(R, P_1)$，将 K' 发给 A。

c) 盲化消息。A 选取三个整数 $\alpha, \beta, \lambda \in_R Z_q^*$，计算

$$r' = K'^{\alpha}(Q'_{ID})^{\beta}(g_{ID})^{\lambda}$$
$$h' = H_2(m', r'),\ h_0 = \alpha^{-1}(h' + \beta)$$

将 h_0 发送给 A_I。

d) 签名。A_I 签名：$S_0 = R + h_0c'P$，将 S_0 发送给 A。

e) 脱盲。A 进行脱盲运算：$S' = \alpha S_0 + \lambda P$，则消息 m' 的签名即为 (S',h')。

敌手 A_I 假冒用户 U（其身份为 ID）伪造的盲签名为 (S',h')。同时 (S',h') 是一个有效的签名，这是因为

$$\begin{aligned}
&H_2(m', e(S', P_{pkg} + H_1(ID)P)(Q'_{ID})^{-h'}) = \\
&H_2(m, e(\alpha S_0 + \lambda P, P_1)(g_{ID})^{-h'c'}) = \\
&H_2(m', e(\alpha(R + h_0c'P) + \lambda P, P_1)(g_{ID})^{-h'c'}) = \\
&H_2(m', e(\alpha R + (h'c' + \beta c')P) + \lambda P, P_1)(g_{ID})^{-h'c'}) = \\
&H_2(m', e(\alpha R, P_1)e((h'c' + \beta c' + \lambda)P, P_1)(g_{ID})^{-h'c'}) = \\
&H_2(m', e(R, P_1)^{\alpha}e(P, P_1)^{h'c' + \beta c' + \lambda}e(P, P_1)^{-h'c'}) = \\
&H_2(m', K'^{\alpha}(g_{ID})^{\beta c\lambda}) = \\
&H_2(m', K'^{\alpha}(Q'_{ID})^{\beta}(g_{ID})^{\lambda}) = H_2(m', r') = h'
\end{aligned}$$

对于上面两种伪造攻击的情形，当身份为 ID 的用户 U 发现有人伪造自己的签名时，用追溯（trace）算法向仲裁方请求仲裁，则仲裁方将断定该盲签名是 PKG 伪造的，从而陷害了诚实 PKG。

2 Z-H 盲签名方案的改进及分析

2.1 Z-H 盲签名方案的改进

Z-H 盲签名方案中的方案 1 的验证等式 $h = H_2(m, e(S, P_{pkg} + H_1(ID)P)(Q_{ID})^{-h})$ 不能保证 Q_{ID} 一定是 g^c，即不能有效地证明签名者拥有合法的 S_{ID}，从而不能抵抗敌手 A_I 的公钥替

代攻击。要有效地证明签名者拥有合法的 S_{ID},验证等式中应该出现系统参数 g。下面首先给出 Z-H 盲签名方案中方案 1 的改进方案。

a) 系统建立。设 G_1 是阶为 q 的加法群,G_2 是阶为 q 的乘法群,双线性映射 $e: G_1 \times G_1 \to G_2$,$P$、$Q$ 是 G_1 的生成元,计算 $g = e(Q,P)$。系统主密钥 $s_{pkg} \in_R Z_q^*$ 由 PKG 选取,系统公钥 $P_{pkg} = s_{pkg}P$,hash 函数 $H_1: \{0,1\}^* \to Z_q^*$,$H_2: \{0,1\}^* \times G_2 \to Z_q^*$。系统主密钥 s_{pkg} 由 PKG 安全保存,并公开系统参数 $\{G_1, G_2, q, P, Q, e, g, P_{pkg}, H_1, H_2\}$。

b) 生成密钥。用户 U 选取整数 $c \in_R Z_q^*$,计算 $Q_{ID} = cP$。用户 U 把自己的 ID、Q_{ID} 发送给 PKG,PKG 计算用户 U 的部分私钥 $S_{ID} = Q/(s_{pkg} + H_1(ID \| Q_{ID}))$。用户 U 验证等式 $e(S_{ID}, P_1) = g$,其中 $P_1 = P_{pkg} + H_1(ID \| Q_{ID})P$,若等式成立则接受 S_{ID}; 否则要求 PKG 重发。

用户 U 公开部分公钥 Q_{ID},保密私钥 (S_{ID}, c)。

c) 签名。用户 U 选取 $k \in_R Z_q^*$,计算 $K = g^k$,$h = H_2(m,K)$,$S = (k + h - c)S_{ID}$,则消息 m 的签名即为 (S,h)。

d) 验证签名。若验证等式 $h = H_2(m, e(S, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, Q_{ID})\, g^{-h})$ 成立,消息 m 的签名 (S,h) 有效; 否则无效。

同理,以 Z-H 盲签名方案中的方案 1 的改进方案为基础,可改进相应方案 2 的盲签名方案。

a) 系统建立。同改进的方案 1,建立系统参数 $\{G_1, G_2, q, P, Q, e, g, P_{pkg}, H_1, H_2\}$,保密系统私钥 s_{pkg}。

b) 生成密钥。同改进的方案 1,用户 U 选取整数 $c \in_R Z_q^*$,计算 $Q_{ID} = cP$,$g_{ID} = e(P, P_1)$,公开自己的公钥 (Q_{ID}, g_{ID}),保密私钥 (S_{ID}, c)。

c) 签名。设用户 U 被请求签名者 A 要求对消息 m 进行盲签名。交互过程如下:

(a) U 选取 $k \in_R Z_q^*$,计算 $K = g^k$,将 K 发给 A。

(b) 盲化消息。A 选取三个整数 $\alpha, \beta, \lambda \in_R Z_q^*$,计算 $r = K^{\alpha} e(Q, Q_{ID})^{1-\alpha} g^{\beta} (g_{ID})^{\lambda}$,$h = H_2(m,r)$,$h_0 = \alpha^{-1}(h + \beta)$,将 h_0 发送给 U。

(c) 签名。U 用自己的私钥 (S_{ID}, c) 签名 $S_0 = (k + h_0 - c)S_{ID}$,将 S_0 发送给 A。

(d) 脱盲。A 进行脱盲运算: $S = \alpha S_0 + \lambda P$,则消息 m 的签名即为 (S,h)。

(e) 验证签名。若验证等式 $h = H_2(m, e(S, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, Q_{ID})\, g^{-h})$ 成立,则消息 m 的签名 (S,h) 有效; 否则无效。

2.2　改进方案的分析

1) 正确性分析

显然,改进的方案 1 是正确的,这是因为

$$e(S, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, Q_{ID})\, g^{-h} =$$
$$e((k + h - c)S_{ID}, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, cP)\, g^{-h} =$$
$$e(Q,P)^{k+h-c} g^{c} g^{-h} = g^k = K$$

所以 $H_2(m, e(S, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, Q_{ID})\, g^{-h}) = H_2(m,K) = h$。

同理,改进的方案 2 也是正确的,因为

$$e(S, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, Q_{ID})\, g^{-h} =$$
$$e(\alpha S_0 + \lambda P, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, cP)\, g^{-h} =$$
$$e((\alpha k + h + \beta - \alpha c)S_{ID} + \lambda P, P_{pkg} + H_1(ID \| Q_{ID})P)\, g^{c-h} =$$
$$e(Q,P)^{\alpha k + h + \beta - \alpha c} g^{c-h} e(P, P_1)^{\lambda} = g^{\alpha k + \beta - \alpha c + c} (g_{ID})^{\lambda} =$$
$$g^{\alpha k} g^{(1-\alpha)c} g^{\beta} (g_{ID})^{\lambda} = K^{\alpha} e(Q, Q_{ID})^{1-\alpha} g^{\beta} (g_{ID})^{\lambda} = r$$

所以 $H_2(m, e(S, P_{pkg} + H_1(ID \| Q_{ID})P)\, e(Q, Q_{ID})\, g^{-h}) = H_2(m,r) = h$。

2) 安全性分析

改进的方案是安全的,它能抵抗敌手 A_{I},A_{II},A_{III} 的伪造攻击。

a) 改进的方案能抵抗敌手 A_{I} 的公钥替代攻击。这是因为用户 U 的部分公钥 $Q_{ID} = cP$ 被绑定在用户的部分私钥 S_{ID} 中了。如果敌手 A_{I} 用 Q'_{ID} 替代了 U 的部分公钥 Q_{ID},伪造的签名要通过验证等式,敌手 A_{I} 必须要伪造出 S'_{ID} 使得 $e(S'_{ID}, P_{pkg} + H_1(ID \| Q'_{ID})P) = g$ 成立,否则验证等式通不过。而 $P_{pkg} + H_1(ID \| Q'_{ID})P = (s_{pkg} + H_1(ID \| Q'_{ID}))P$,故 S'_{ID} 必须为 $Q/(s_{pkg} + H_1(ID \| Q'_{ID}))$,即敌手 A_{I} 知道了系统主密钥 s_{pkg}。这是不可能的。

b) 改进的方案能抵抗敌手 A_{II} 的攻击。这是因为验证等式中含有 $e(Q, Q_{ID})$,其中 $e(Q, Q_{ID}) = g^c$,而敌手 A_{II} 不具备替代用户 U 的部分公钥的能力,要使得伪造的签名能通过验证等式,敌手只能从部分公钥 $Q_{ID} = cP$ 中解出或猜出秘密值 c。这是不可能的,否则敌手 A_{II} 具有求解椭圆曲线上离散对数的能力。

c) 改进的方案可用追溯算法抵抗敌手 A_{III} 的攻击。

3) 性能分析

本文从运算量和安全性两个方面,将改进的新方案与 Z-H 方案中的方案 1 和 2 进行比较,比较结果如表 1 和 2 所示。令 P、mul、exp、H 分别表示双线性对运算、标量乘运算、幂运算和哈希运算。

表 1　改进方案与 Z-H 方案中的方案 1 的比较

比较项	方案	
	Z-H 方案的方案 1 [12]	改进方案 1
签名过程	1mul + 1exp + 1H	1mul + 1exp + 1H
验证过程	1P + 2mul + 1exp + 2H	2P + 3mul + 1exp + 2H
安全性	不安全	安全

从表 1 可以看出,改进方案 1 与 Z-H 方案的方案 1 在签名过程中运算量相同,在验证过程中运算量比 Z-H 方案中的方案 1 增加了一个标量乘运算和对运算,但改进方案消除了公钥替换攻击和恶意的 PKG 攻击。

表 2　改进方案与 Z-H 方案中的方案 2 的比较

比较项	方案	
	Z-H 方案的方案 2 [12]	改进盲签名方案
签名过程	6mul + 4exp + 1H	1P + 7mul + 5exp + 1H
验证过程	1P + 2mul + 1exp + 2H	2P + 3mul + 1exp + 2H
安全性	不安全	安全

从表 2 可以看出,改进盲签名方案与 Z-H 方案的方案 2 在签名和验证过程中运算量都有所增加,但改进方案消除了公钥替换攻击和恶意的 PKG 攻击。

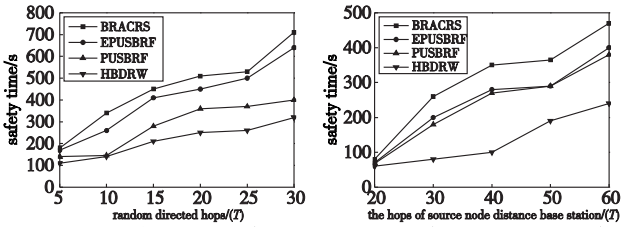
3　结束语

本文对 Z-H 盲签名方案进行了安全性分析,指出了这个方案不能抵抗敌手 A_{I} 的伪造攻击。敌手 A_{I} 可假冒任何签名者伪造任意消息的盲签名,当用追溯算法时可陷害诚实的 PKG。针对该方案的安全缺陷,提出了相应的改进方案。在改进方案中验证等式出现系统参数 g,有效地证 (下转第 890 页)

要被转发的次数就越多，经过的路由跳数就越多。图 4(b) 中，当 h 取相同的值时，四种策略的通信开销相当。与通信开销最小的 HBDRW 协议相比，本文的 BRACRS 协议通信开销平均增加 6.63%，平均大约增加了四次数据包的转发。与 EPUSBRF 协议相比，BRACRS 协议的通信开销平均增加了 4.36%，平均增加约三次数据包的转发，这说明 BRACRS 的通信开销增长是可接受的。

5.2 安全时间

安全时间是指攻击者成功定位到源节点的位置之前，源节点已发送数据包的数量。在图 5(a) 中显示，BRACRS 协议与其他三种协议相比，安全时间增长幅度较大。与 HBDRW 协议相比，BRACRS 协议的平均安全时间增加了 92.92%，与 EPUSBRF 协议相比，BRACRS 协议的平均安全时间也增加了 10.94%。图 5(b) 中显示，BRACRS 协议与其他三种协议相比，BRACRS 协议的安全时间也是最大的，能更进一步地保护源节点的位置隐私。分析主要有两个方面的原因: a) BRACRS 策略能产生远离 S 且比较分散的幻影源节点; b) 数据包将转发至伪幻影节点同圆周方向上的标点，最后再由标点转发给基站。这样可产生足够多的随机性路径，显著增强了 WSNs 中源节点位置隐私的安全性能。



(a) 安全时间与随机有向跳数 (b) 安全时间与源节点和基站间跳数

图5 安全时间测试结果

6 结束语

源位置隐私保护问题的研究对 WSNs 的大规模应用具有十分重要的意义。本文提出的 BRACRS 策略不仅保证了幻影节点分布的随机性和均匀性，而且第二阶段的圆周路由可以在传感器节点能量受限的情况下，利用 sink 外围区域的能量形成足够长的路径，从而增加攻击者捕获数据包的难度，有效增长安全时间。分析表明，与现有的源节点位置隐私保护方案相比，本文提出的 BRACRS 策略明显提高了源位置隐私的安全性。

参考文献:

[1] Rios R, Lopez J. Analysis of location privacy solutions in wireless sensor networks [J]. Journal of IET Communications, 2011, 5(17): 18–32.

[2] 洪锋，褚红伟，金宗科. 无线传感器网络应用系统最新进展综述 [J]. 计算机研究与发展，2010，47(2): 81–87.

[3] 钱志鸿，王义君. 面向物联网的无线传感器网络综述 [J]. 电子与信息学报，2013，35(1): 215–227.

[4] Ozturk C, Zhang Yanyong, Trappe W. Source-location privacy in energy-constrained sensor network routing [C] //Proc of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks. New York: ACM Press. 2004: 88–93.

[5] Kang Lai. Protecting location privacy in large-scale wireless sensor networks [C] //Proc of IEEE International Conference on Communications. 2009: 1–6.

[6] 陈娟. 无线传感器网络中节点位置隐私保护与自治愈技术研究 [D]. 哈尔滨: 哈尔滨工业大学，2013.

[7] 李江，刘学军，章玮. 基于门限路由的源节点位置隐私保护协议 [J]. 南京师大学报: 自然科学版，2014，37(1): 117–122.

[8] Mehta K, Liu Donggang, Wright M. Location privacy in sensor networks against a global eavesdropper [C] //Proc of IEEE International Conference on Network Protocols. 2007: 314–323.

[9] Kamat P, Zhang Yanyong, Trappe W, *et al*. Enhancing source-location privacy in sensor network routing [C] //Proc of the 25th IEEE International Conference on Distributed Computing Systems. [S. l.]: IEEE Press, 2005: 599–608.

[10] Pongaliur K, Xiao Li. Maintaining source privacy under eavesdropping and node compromise attacks [C] //Proc of IEEE INFOCOM. [S. l.]: IEEE Press, 2011: 1656–1664.

[11] Bicakci K, Gultekin H, Tavli B. Maximizing lifetime of event-unobservable wireless sensor networks [J]. Computer Standards & Interfaces, 2011, 33(4): 401–410.

[12] 肖刘军. 基于节点位置和能量的无线传感器网络分簇路由协议研究 [D]. 成都: 西南交通大学，2010.

[13] 向辉. 无线传感器网络覆盖控制算法研究 [D]. 无锡: 江南大学，2012.

[14] Liu Anfeng, Zhang Penghui, Chen Zhigang. Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks [J]. Journal of Parallel and Distributed Computing, 2011, 71(10): 1327–1355.

[15] 易险峰，樊晓平. 平面无线传感器网络完全死亡寿命与延迟的优化分析 [J]. 小型微型计算机系统，2012，33(7): 22–28.

[16] 吴剑锋，郭英，范海宁. OMNeT ++ 网络仿真器的设计原理分析 [J]. 微计算机应用，2008，15(3): 34–37.

(上接第 875 页) 明了签名者拥有合法的 S_{ID}，从而克服了敌手的公钥替代攻击。虽然改进的方案在计算量上较 Z-H 盲签名方案有所增加，但其安全性得到了大大的提高。

参考文献:

[1] Chaum D. Blind signature for untraceable payments [C] //Advances in Cryptology. New York: Springer-Verlag, 1983: 199–203.

[2] Shamir A. Identity-based cryptosystems and signature schemes [C] //Advances in Cryptology. Berlin: Springer-Verlag, 1984: 47–53.

[3] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C] //Advances in Cryptology, LNCS vol 2894. Berlin: Springer, 2003: 452–473.

[4] Liao Jian, Xiao Junfang, Qi Yinghao, *et al*. ID-based signature scheme without trusted PKG [C] //Proc of the 1st SKLOIS Conference on Information Security and Cryptology. Berlin: Springer, 2005: 53–62.

[5] Gentry C. Certificate-based encryption and the certificate revocation problem [C] //Advances in Cryptology, LNCS Vol 2656. Berlin: Springer-Verlag, 2003: 272–293.

[6] 张学军，王育民. 新的基于身份无可信中心的盲签名和代理签名 [J]. 计算机工程与应用，2007，43(1): 142–144.

[7] 崔巍，辛阳，胡程瑜，等. 高效的基于身份的(受限) 部分盲签名 [J]. 北京邮电大学学报，2008，31(4): 53–57.

[8] 冯涛，彭伟，马建峰. 安全的无可信 PKG 的部分盲签名方案 [J]. 通信学报，2010，31(1): 128–135.

[9] 张小萍，钟诚. 高效无可信私钥生成中心部分盲签名方案 [J]. 计算机应用，2011，31(4): 992–995.

[10] 周萍，何大可. 安全无可信私钥生成中心的部分盲签名方案 [J]. 计算机系统应用，2012，21(6): 70–74.

[11] 李明祥，赵秀明，王洪涛. 对一种部分盲签名方案的安全性分析与改进 [J]. 计算机应用，2010，30(10): 2687–2690.

[12] 周萍，何大可. 高效无可信 PKG 的新型盲签名方案 [J]. 计算机应用研究，2012，29(2): 626–629.