文章编号：2095-2163(2020)01-0128-05　　中图分类号：TP309.2　　文献标志码：A

无线医疗传感器网络中一种改进的无证书聚合签名方案

房保纲，钟伯成，张家磊，丁佳蓉
（上海工程技术大学 电子电气工程学院，上海 201620）

摘　要：随着云计算、大数据、物联网等技术的快速发展，人们享受到了技术带来的方便。无线医疗传感器网络(WMSN)技术便是物联网技术的典型应用之一。但是无线医疗传感器网络面临着诸多的挑战，其中如何安全且高效地认证由传感器上传到服务器的签名已经成为亟需解决的问题之一。对此，提出了改进的无证书聚合签名(CLAS)方案，此方案能在无线医疗传感器网络中对消息的签名进行批量认证，并且在签名验证时双线性对运算的次数不会随着签名用户数量的增加而线性增长。通过对方案的正确性、安全性和计算开销的分析表明：提出的方案能够批量认证传感器的消息签名，并且此方案能够有效抵御敌手的伪造攻击，具有较高的安全性和较低的运算开销。

关键词：无线医疗传感器网络；无证书聚合签名；批量认证；隐私保护

An improved Certificateless Aggregation Signature scheme in Wireless Medical Sensor Networks

FANG Baogang, ZHONG Bocheng, ZHANG Jialei, DING Jiarong
(School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

【Abstract】With the rapid development of technologies such as cloud computing, big data, and Internet of Things, people have enjoyed the convenience brought by technology. Wireless Medical Sensor Network (WMSN) technology is one of the typical applications of IoT technology. However, Wireless Medical Sensor Metworks face many challenges, and how to quickly and efficiently authenticate the signatures uploaded by sensors to the server has become one of the most urgent problems to be solved. In this regard, an improved certificateless aggregate signature (CLAS) scheme is proposed, which can perform batch authentication of the signature of a message in a Wireless Medical Sensor Network, and the number of bilinear pairing operations does not increase linearly with the number of the users in signature verification. The analysis of the correctness, security and efficiency of the scheme shows that the proposed scheme can perform batch authentication of a large number of sensor message signatures, and this scheme can effectively resist enemy attacks, with high security and low computational overhead.

【Key words】Wireless Medical Sensor Networks (WMSN); Certificateless Aggregation Signature(CLAS); batch authentication; privacy protection

0　引　言

随着无线传感器技术的发展，无线医疗传感器网络技术也取得了长足的进步[1]。无线医疗传感器网络集合了移动密集型传感器和远程医疗两者的优点[2]。一方面，用户可以实时地通过传感器设备上传生理数据到云服务器，享受健康医疗机构提供的服务。另一方面，通过分析个人的生理数据，远程医疗健康系统也能够精确地提供健康信息和医疗服务。

无线医疗传感器的网络模型如图 1 所示。无线医疗传感器网络主要包含 5 个部分，分别是：医疗传感器节点(medical sensor node，MSN)，医疗服务器(medical server，MS)，签名聚合者(signature aggregator，SA)，聚合签名验证者(aggregate signature verifier，ASV)，专业医疗人员(medical)。

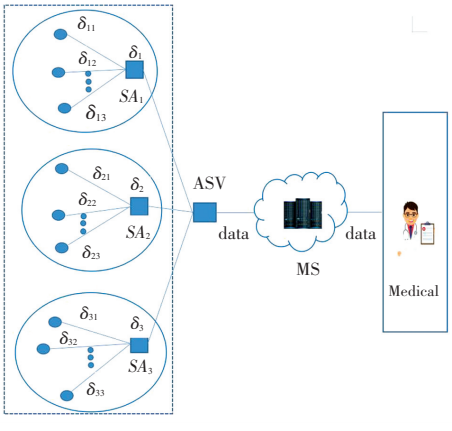

图 1　无线医疗传感器网络模型

Fig. 1　Model of Wireless Medical Sensor Networks

作者简介：房保纲(1994-)，男，硕士研究生，主要研究方向：无线体域网络安全；钟伯成 (1964-)，男，博士，教授，主要研究方向：计算机网络、网络拥塞控制。

通讯作者：房保纲　　Email：402866119@ qq.com

收稿日期：2019-11-18

数字签名是无线医疗传感器网络中用于保护用户隐私、进行身份认证所采用的重要技术，然而现有的各类签名技术，比如传统的数字签名、基于 ID 的数字签名及聚合签名等，计算复杂度相对较高，几乎不能满足低存储、低运算能力等资源受限的环境需求。无证书聚合签名（CLAS）将无证书密码体制和聚合签名这两种技术的优点有效地结合起来，不仅避免了 PKC 和 IBC 中的证书管理与密钥托管两个棘手的问题，并且有效降低了签名验证的计算与存储开销等，特别适用于资源受限的网络环境中，所以现在有许多方案都采用了无证书聚合签名方案。

本文基于 Wu 等人[3]的方案进行适当地改进，当该方案中执行聚合签名验证时，双线性对运算的次数会随着签名用户数量的增加而呈线性增长，极大增加了计算开销，并且该方案在签名生成过程中会泄露签名者的秘密值信息，具有不可忽略的安全隐患。在改进的方案中，研究修改了单个签名生成算法和聚合签名算法，最终能够保证签名用户的秘密值信息不会被泄露，并且双线性运算的次数也不会随着签名数量的增加而呈线性增长。

1　理论基础

1.1　双线性对[4]

设 G_1 为一个阶为素数 q 的加法循环群，P 为其生成元；G_2 为同阶的乘法循环群，这里设映射为：e：$G_1 \times G_2 \rightarrow G_2$ 且该映射满足以下 3 条性质：

（1）双线性。对任意 $P,K,Y \in G_1$，都有 $e(P,X+Y)=e(P,X)\,e(P,Y)$，且对任意的 a，$b \in Z_q^*$，满足 $e(aP,bP)=e(P,P)^{ab}=e(abP,P)=e(P,abP)$。

（2）非退化性。存在 $X,Y \in G_1$，$e(X,Y) \neq 1$。

（3）可计算性。存在 $X,Y \in G_1$，$e(X,Y)$ 能够通过一个算法在多项式时间内计算出来。

1.2　聚合签名定义

聚合签名方案在总体上可解析为如下构成部分：一个密钥管理中心（PKG）、n 个不同的签名用户、用户密钥生成算法、用户签名生成算法、用户签名聚合生成算法和聚合签名验证算法[5]。首先，向密钥管理中心输入安全参数 k，随后 PKG 生成并且发布系统的参数列表 $params$；接着，向 PKG 中输入每个用户 U_i 的身份 ID_i、参数 $params$ 和系统主密钥，用于生成每个用户的部分私钥 p_i；用户 U_i 输入其身份信息 ID_i，并选择一个秘密值 $x_i \in Z_p^*$，输出其公钥 P_i；签名用户输入 ID_i、秘密值 x_i、部分私钥 p_i、公钥 P_i 和消息 m_i，输出签名 δ_i；最后，聚合签名的生成者将这 n 个用户的身份 ID_i、消息 m_i 和各自的签名 δ_i 输入，生成聚合签名 δ。在聚合签名验证阶段，输入聚合签名 δ、参数 $params$ 和身份信息，如果验证通过，则输出“正确”，否则输出验证失败。

1.3　CDH 问题

设 G 是阶为素数 q 的加法循环群，随机选取 a，$b \in Z_q^*$，对于给定的 $P,aP,bP \in G$，求解 a,b,P 是多项式时间内不能解决的困难问题。在 CLAS 的安全模型中通常情况下会包含 2 类攻击者，分别是 A_1 和 A_2。在循环群 G_1 中给定一个随机的计算 Diffie-Hellman（CDH）问题实例 (P,aP,bP)，挑战者 C 与 A_1 或 A_2 进行询问，最终挑战者 C 可以利用 A_1 或者 A_2 解决 CDH 问题，计算出 a,b,P。

2　改进的无证书聚合签名方案

本节根据 Wu 等人的方案，改进设计了一个新的 CLAS 方案，该方案主要包含 7 个阶段，分别是：系统参数生成（Setup）、部分私钥生成（Partial-Private-Key-Generate）、密钥生成（Private-Key-Generate）、单个签名生成（Individual-Sign）、单个签名验证（Individual-Verify）、聚合签名生成（Aggregate-Sign）、聚合签名验证（Aggregate-Verify）等阶段。算法运行过程可阐释表述如下。

2.1　系统参数生成（Setup）

通过执行如下运算，MS 通过 k 产生系统参数，其中 k 为一个安全参数：

（1）用同样的质数 q 产生 2 个循环群 G_1、G_2，P 是群 G_1 的生成元。双线性映射 e：$G_1 \times G_2 \rightarrow G_2$；

（2）随机选择一个数 $s \in Z_q^*$ 作为 MS 的主密钥，计算 $MS_{pub}=sP$ 作为 MS 的公钥；

（3）选取 4 个哈希函数 H_1：$\{0,1\} \rightarrow G_1$：H_2：$\{0,1\} \rightarrow G_2$，h_1：$\{0,1\} \rightarrow Z_q^*$，$h_2$：$\{0,1\} \rightarrow Z_q^*$；

（4）公开系统参数 $params=(G_1,G_2,P,e,q,MS_{pub},H_1,H_2,h_1,h_2)$。

2.2　部分私钥生成（Partial-Private-Key-Generate）

通过执行如下运算，MS 产生 MSN 的部分私钥：

（1）ID_i 作为 MSN 的身份，MS 首先计算 $Q_i=H_1(ID_i)$，然后计算 MSN 的私钥 $ppk_i=s \cdot Q_i$；

（2）秘密发送 ppk_i 到 MSN。

2.3　密钥生成（Private-Key-Generate）

通过执行如下运算，身份为 ID_i 的 MSN 产生了自己的公钥和私钥：

（1）选择一个随机数 x_i 作为秘密值；

(2)设置 $sk_i = \{ppk_i, x_i\}$ 作为私钥;

(3)计算 $pk_i = x_i p$ 作为公钥。

2.4 个体签名生成(Individual-Sign)

通过执行如下运算,身份为 ID_i 的签名者在 m_i 消息上产生了 σ_i 的签名:

(1)输入系统参数 $params$,状态信息 Δ 和公私钥对 (sk_i, pk_i);

(2)随机选择 $r_i \in Z_q^*$,然后计算 $R_i = r_i P$;

(3)计算 $\alpha_i = h_1(ID_i, pk_i, R_i)$, $\beta_i = h_2(m_i, ID_i, pk_i, R_i)$ 及 $U = H_2(\Delta)$;

(4)计算 $V_i = \alpha_i ppk_i + MS_{pub} + \beta_i x_i U$;

(5)输出 $\sigma_i = (R_i, V_i)$ 作为消息的签名。

2.5 个体签名验证(Individual-Verify)

通过执行如下运算,验证者验证消息的签名:

(1)输入状态信息 Δ;

(2)计算 $\alpha_i = h_1(ID_i, pk_i, R_i)$, $\beta_i = h_2(m_i, ID_i, pk_i, R_i)$, $Q_i = H_1(ID_i)$ 及 $U = H_2(\Delta)$;

(3)验证:

$$e(V_i, P) = e(\alpha_i Q_i + R_i, MS_{pub}) e(\beta_i pk_i, U). \quad (1)$$

(4)如果式(1)成立则接受签名 δ_i;如果不成立,则拒绝。

2.6 聚合签名生成(Aggregate-Sign)

通过执行如下运算,一个聚合者能产生聚合签名 δ:

(1)输入 n 个元组 $(ID_i, m_i, pk_i, \delta_i)$,其中,$1 \leqslant i \leqslant n$;

(2)计算 $V = \sum_{i=1}^{n} V_i$;

(3)输出 $\sigma = (R, V)$ 作为聚合签名,其中 $R = \{R_1, R_2, \cdots, R_n\}$。

2.7 聚合签名验证(Aggregate-Verify)

通过执行以下运算,聚合签名验证者认证聚合签名的 $\sigma = (R, V)$ 合法性:

(1)输入状态信息 Δ,元组 $(ID_i, m_i, pk_i, R_i)_{1 \leqslant i \leqslant n}$,和聚合签名 $\sigma = (R, V)$;

(2)计算 $U = H_2(\Delta)$, $1 \leqslant i \leqslant n$,计算 $Q_i = H_1(ID_i)$, $\alpha_i = h_1(ID_i, pk_i, R_i)$ 及 $\beta_i = h_2(m_i, ID_i, pk_i, R_i)$;

(3)验证:

$$e(V, P) = e\Big(\sum_{i=1}^{n} (\alpha_i Q_i) + R_i, MS_{pub}\Big) e\Big(\sum_{i=1}^{n} \beta_i pk_i, U\Big). \quad (2)$$

(4)如果式(2)成立,验证者接受聚合签名 δ,否则拒绝。

3 安全分析

3.1 正确性验证

通过以下详细的步骤推导,会很容易验证本方案的正确性。推导过程见如下。

$$e(V, P) = e\Big(\sum_{i=1}^{n} \alpha_i ppk_i + r_i MS_{pub} + \beta_i x_i U, P\Big) =$$

$$e\Big(\sum_{i=1}^{n} \alpha_i ppk_i, P\Big) e\Big(\sum_{i=1}^{n} r_i MS_{pub} P\Big) \cdot e\Big(\sum_{i=1}^{n} \beta_i x_i U, P\Big) =$$

$$e\Big(\sum_{i=1}^{n} \alpha_i Q_i, sP\Big) \cdot e\Big(\sum_{i=1}^{n} r_i P, MS_{pub}\Big) e\Big(\sum_{i=1}^{n} \beta_i x_i P, U\Big) =$$

$$e\Big(\sum_{i=1}^{n} \alpha_i Q_i, MS_{pub}\Big) \cdot e\Big(\sum_{i=1}^{n} r_i P, MS_{pub}\Big) \cdot e\Big(\sum_{i=1}^{n} \beta_i x_i P, U\Big) =$$

$$e\Big(\sum_{i=1}^{n} (\alpha_i Q_i + R_i), MS_{pub}\Big) \cdot e\Big(\sum_{i=1}^{n} \beta_i pk_i, U\Big)$$

3.2 安全性证明

定理 1 如果在循环群 G_1 中的 CDH 困难问题无法解决,那么改进的 CLAS 能够抵御敌手 A_1 的伪造攻击。

Setup:C 随机选取 ID_{ts} 作为非法传感器节点目标身份,令 $MS_{pub} = Q_1 = aP$,产生系统参数 $params = \{G_1, G_2, P, e, q, MS_{pub}, H_1, H_2, h_1, h_2\}$。

H_1 - *query*:C 维护一个列表 L^{H_1}, L^{H_1} 的结构为 $(ID_i, \delta_i, \varepsilon_i, Q_i)$, L^{H_1} 中元素初始值为空。当 A_1 发起询问时,C 检查 L^{H_i} 中是否存在元组 $(ID_i, \delta_i, \varepsilon_i, Q_i)$,如果存在,返回 Q_i 给 A_1,否则 C 随机选择 $\varepsilon_i \in \{0, 1\}$ 和 $\delta_i \in Z_q^*$,如果 $\varepsilon = 0$,令 $Q_i = \delta_i P$,如果 $\varepsilon_i = 1$,则 $Q_i = \delta_i Q_2 = \delta_i bP$。将 Q 返还给 A_1,$(ID_i, \delta_i, \varepsilon_i, Q_i)$ 存储到 L^{H_i} 中。

H_2 - *query*:C 维护列表 L^{H_2}, L^{H_2} 由 (MS_{pub}, ϑ, U) 构成。L^{H_2} 中元素初始值为空。当 A_1 执行询问时,C 检查 L^{H_2} 中是否存在元组 (MS_{pub}, ϑ, U);如果存在,返回 U 至 A_1;否则,C 随机选择 $\vartheta \in Z_q^*$,计算 $U = \vartheta P$。返回 U 至 A_1,存储 (MS_{pub}, ϑ, U) 至 L^{H_2}。

h_1 - *query*:C 维护列表 L^{h_1}, L^{h_1} 由 $(ID_i, pk_i, R_i, \alpha_i)$ 构成。L^{h_1} 中元素初始值为空。当 A_1 执行询问时,C 检查 L^{h_1} 中是否存在元组 $(ID_i, pk_i, R_i, \alpha_i)$;如果存在,返回 α_i 至 A_1;否则,C 随机选择 α_i。返回 U 至 A_1,存储 $(ID_i, pk_i, R_i, \alpha_i)$ 至 L^{h_1}。

h_2 - *query*:C 维护列表 L^{h_2}, L^{h_2} 由 $(m_i, ID_i, pk_i, R_i, \beta_i)$ 构成。L^{h_2} 中元素初始值为空。当 A_1 执行询问时,C 检查 L^{h_2} 中是否存在元组 $(m_i, ID_i, pk_i, R_i, \beta_i)$;如果存在,返回 β_i 至 A_1;否则,C 随机选择 β_i。

返回至 A_1，存储(m_i, ID_i, pk_i, R_i, β_i) 至 L^{h_2}。

Reveal - Partial - Private - Key queries：C 维护列表 L^{ppk}，L^{ppk} 由(ID_i, ppk_i) 构成，L^{ppk} 中元素初始值为空。当 A_1 执行询问，C 首先检查是否 $ID_i = ID_{ts}$；如果成立，输出 ⊥(表示该值未知)；否则，C 检查 L^{ppk} 中是否存在元组(ID_i,ppk_i)；如果存在，返回 ppk_i 至 A_1；否则，C 重新从 L^{ppk} 中选择元组(ID_i, δ_i, ε_i, Q_i) 并计算 $ppk_i = \delta_i MS_{pub} = \alpha\delta_i P$。返回 ppk_i 至 A_1，存储(ID_i, ppk_i) 至 L_{ppk}。

Reveal - Secret - Key - queries：C 维护列表 L^x，L^x 由(ID_i, x_i) 构成，L^x 中元素初始值为空。当 A_1 以身份为 ID_i 进行询问时，C 首先检查是否 $ID_i = ID_{ts}$；如果成立，输出；否则，C 检查一个元组是否存在于(ID_i,x_i) 中；如果存在，返回 x_i 至 A_1；否则，C 随机选择 x_i。返回 x_i 至 A_1，存储 x_i 至(ID_i, x_i)。

Reveal - Public - Key queries：C 维护列表 L^{pk}，L^{pk} 由(ID_i pk_i) 构成，L^{pk} 中元素初始值为空。当 A_1 以身份为 ID_i 进行询问时，C 首先需要检查一个元组(ID_i, pk_i) 是否存在于 L^{pk} 中；如果存在pk_i，返回pk_i 至 A_1；否则，通过 L^x 获取 x_i 并计算 $pk_i = x_i P$。返回 pk_i 至 A_1，存储(ID_i, pk_i) 至 L^{pk}。

Replace - Public - Key queries：当 A_1 以身份为(ID_i, $pk_i{}^*$) 进行询问时，C 从列表 L^{pk} 中选取 $pk_i{}^*$ 替代真实公钥 pk_i。

Sign - queries：当 A_1 以身份为 ID_i，公钥为 pk_i，消息为 m_i 进行询问时，C 分别通过 L^{H_1}, L^{H_2}, L^{h_1} 及 L^{h_2} 得到 ε_i, Q_i, U, α_i 和 β_i。C 随机选择 r_i，并且计算 $R_i = r_i P$；若 $\varepsilon_i = 0$，C 计算 $V_i = \delta_i\alpha_i MS_{pub} + r_i MS_{pub} + \beta_i \vartheta pk_i$。返回 $\delta_i = (R_i, V_i)$ 至 A_1，作为消息 m_i 的签名。

Forgery：最后，A_1 利用消息身份公钥对($m_i{}^*$, $ID_i{}^*$, $pk_i{}^*$) 输出一个伪造的聚合签名 $\delta^* = (R^*, V^*)$。如果所有 $\varepsilon_i = 0$ 成立，A_1 中止；否则，不失一般性，令 $ID_{ts} = ID_1$，也就是 $\varepsilon_1 = 1$, $\varepsilon_i = 0 (2 \leqslant i \leqslant n)$。伪造签名应当满足以下等式：

$$e(V^*, P) = e\Big(\sum_{i=1}^{n}(\alpha_i{}^* Q_i{}^* + R_i{}^*), MS_{pub}\Big) \cdot e\Big(\sum_{i=1}^{n}\beta_i{}^* pk_i{}^*, U\Big). \tag{3}$$

其中，$Q_i{}^* = \delta_i{}^* P (2 \leqslant i \leqslant n)$，$Q_i{}^* = \delta_1{}^* bP$，$U = \vartheta P$，$V^* = \sum_{i=1}^{n} V_1^*$，$R^* = \{R_1{}^*, R_2{}^*, \cdots, R_n{}^*\}$。

具体推导过程如下：

$$e(V^*,P) = e\Big(\sum_{i=1}^{n}(\alpha_i^* Q_i^* + R_i^*), MS_{pub}\Big) e\Big(\sum_{i=1}^{n}\beta_i^* pk_i^*, U\Big)$$

$$\Rightarrow e(V^*,P) = e\Big(R_1^* + \sum_{i=2}^{n}(\alpha_i^* Q_i^* + R_i^*), MS_{pub}\Big) e\Big(\sum_{i=1}^{n}\beta_i^* pk_i^*, U\Big) \cdot e(\alpha_i^* Q_i^*, MS_{pub}) e\Big(\sum_{i=1}^{n}\beta_i^* pk_i^*, \vartheta P\Big)$$

$$\Rightarrow e(\alpha_i^* Q_i^*, MS_{pub}) = e(V^*,P) \cdot \Big[e\Big(R_1^* + \sum_{i=2}^{n}(\alpha_i^* Q_i^* + R_i^*), MS_{pub}\Big) \cdot e\Big(\sum_{i=1}^{n}\beta_i^* pk_i^*, \vartheta P\Big)\Big]^{-1}$$

$$\Rightarrow e(\delta_1^* \alpha_1^* abP, P) = e(V^*,P) \cdot \Big[e\Big(R_1^* + \sum_{i=2}^{n}(\alpha_i^* Q_i^* + R_i^*), MS_{pub}\Big) \cdot e\Big(\sum_{i=1}^{n}\beta_i^* pk_i^*, \vartheta P\Big)\Big]^{-1}$$

$$\Rightarrow \delta_1^* \alpha_1^* abP = V^* - \Big[\Big(r_1^* + \sum_{i=2}^{n}(\delta_1^* + r_1^*) MS_{pub}\Big) + \sum_{i=1}^{n}\beta_i^* x_i^* \vartheta P\Big]$$

$$\Rightarrow abP = \Big(V^* - \Big(r_1^* + \sum_{i=2}^{n}(\delta_1^* + r_1^*) MS_{pub}\Big) - \sum_{i=1}^{n}\beta_i^* x_i^* \vartheta P\Big)(\delta_1^* \alpha_1^*)^{-1}$$

但是，这与 CDH 困难问题相矛盾，因此由改进方案产生的单个签名和聚合签名都能够防止 A_1 伪造攻击。

定理 2　如果在循环群 G_1 中的 CDH 困难问题无法解决，那么改进的 CLAS 能够抵御敌手 A_2 的伪造攻击。

证明过程与定理 1 相同，不再赘述。

4　性能分析

4.1　运算开销对比

针对地列举了几个现有的在随机预言机模型下的无证书聚合签名方案(CLAS)的安全级别和运算开销，并与改进的方案进行了对比分析。下面用于软件仿真的硬件环境为 Ubuntu 18.10 内存 1 024 MB。硬件配置为 Inter(R) Core(TM) i5-7500U，主频为 3.4 GHz，内存为 8 192 MB，软件环境为 MIRACL。经过研究[6]，发现这些方案主要的运算时间开销是由某些比较耗时的密码学算法所产生的，所以，本方案在实验进行的开始阶段优先考虑的各种运算见表 1。

表 1 符号表示

Tab. 1 Symbolic representation

符号	定义
P	双线性对运算
S	G_1 群中的标量乘运算
H	$\{0,1\}^* \rightarrow G_1^*$ 上的 $hash$ 运算
L	G_1 中的元素长度

各密码运算执行时间见表 2，多个用户($n = 5$)在无证书聚合签名验证过程中运算时间开销的对比见表 3。很显然，本文改进的 CLAS 方案运算开销小于其它方案[7-10]。

表 2 各密码运算执行时间

Tab. 2 Each cryptographic operation execution time

运算类别	S 标量乘运算	H 哈希运算	P 对运算
时间/ms	5.571	0.330	5.624

表 3 CLAS 方案运算时间对比

Tab. 3 Comparison of calculation time of CLAS scheme ms

方案	单个签名生成	单个签名验证	聚合签名验证
CWZ[7]	22.945	34.622	80.515
LYX[8]	22.614	28.727	79.331
DHW[9]	22.944	34.628	80.516
MZW[10]	22.856	29.057	75.661
本文方案	22.556	28.674	71.473

4.2 安全性对比

攻击者分别为 A_1 和 A_2 两种类型，其中 B_{i1} 表示普通攻击，B_{i2} 表示强攻击，SP 表示方案的安全性。CLAS 方案安全性对比见表 4。通过表 4 可以看出，对比其它几个方案，本文所改进的方案具有相对较高安全性。

表 4 CLAS 方案安全性对比

Tab. 4 CLAS scheme security comparison

	B_{11}	B_{12}	B_{13}	SP	B_{21}	B_{22}	B_{23}	SP
文献[11]	否	是	否	低	是	否	否	低
文献[12]	是	是	是	高	否	否	否	低
文献[13]	是	是	是	高	否	否	否	低
本文方案	是	是	是	高	是	是	是	高

5 结束语

无证书公钥密码体制解决了公钥密码体制中证书管理和密钥托管两个困难问题。聚合签名技术则将不同用户的消息签名聚合成一个签名，只对聚合后的签名进行验证，极大提高了签名验证的效率。本文提出了安全高效的适用于无线医疗传感器网络的无证书聚合签名方案，该方案具有无证书密码体制和聚合签名技术的双重优点，并且该方案在随机预言机模型下证明是安全的。通过实验数据可知，本文方案具有较高的安全性，较低的运算开销等优点，更适用于无线医疗传感器网络。

参考文献

[1] 邓世洲，高伟东，胡炜，等. 无线体域网技术研究现状与展望[J]. 传感器与微系统，2014，33(11)：1-4，8.

[2] 周岳斌，陈家顺，马贺贺. 无线体域网节点数据压缩节能方法[J]. 传感器与微系统，2017，36(11)：10-13.

[3] WU Libing, XU Zhiyan, HE Debiao, et al. New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment[J]. Security and Communication Networks，2018，2018：2595273.

[4] PAAR C, PELZ J. 深入浅出密码学：常用加密技术原理与应用[M]. 北京：清华大学出版社，2012.

[5] 王大星，滕济凯. 车载传感网中基于聚合签名的认证方案[J]. 吉林大学学报(理学版)，2018，56(3)：657-662.

[6] 成林. 可证明安全的无证书数字签名方案的研究[D]. 北京：北京邮电大学，2014.

[7] 陈虎，魏仕民，朱昌杰，等. 安全的无证书聚合签名方案[J]. 软件学报，2015，26(5)：1173-1180.

[8] LU Haijun, YU Xiuyuan, XIE Qi. Provably secure certificateless aggregate signature with constant length[J]. Journal of Shanghai Jiaotong University, 2012, 46(2): 259-263.

[9] 杜红珍，黄梅娟，温巧燕. 高效的可证明安全的无证书聚合签名方案[J]. 电子学报，2013，41(1)：72-76.

[10] DU Hongzhen, HUANG Meijuan, WEN Qiaoyan. Efficient and provably-secure certificateless aggregate signature scheme[J]. Acta Electronica Sinica, 2013, 41(1): 72-76.

[11] GONG Z, LONG Y, HONG X, et al. Practical certificateless aggregate signatures from bilinear maps[J]. Journal of Information Science and Engineering, 2010，6(26)：2093-2106.

[12] LIU He, WANG Sijia, LIANG Mangui, et al. New construction of efficient certificateless aggregate signatures[J]. International Journal of Security and Its Applications, 2014, 8(1): 411-422.

[13] KUMAR P, KUMARI S, SHARMA V, et al. A certificateless aggregate signature scheme for healthcare wireless sensor network[J]. Sustainable Computing: Informatics and Systems, 2018, 18: 80-89.