文章编号:1671-4598(2017)10-0236-04 DOI:10.16526/j.cnki.11—4762/tp.2017.10.060 中图分类号:TN918 文献标识码:A

低数据量环境下物联网密钥管理算法与方案设计

吴 琼[1],孙 博[2]
(1.西安工业大学 计算机科学与工程学院,西安 710021;2.西安工业大学 教务处,西安 710021)

摘要:为了提高低数据量环境下物联网密钥的安全性与可靠性,需要对低数据量环境下物联网密钥管理算法以及密钥管理方案进行设计研究;使用当前管理算法对低数据量环境下物联网密钥进行管理时,在物联网网络节点增加到一定数量的情况下,无法保证低数据环境下物联网的安全性与可靠性;为此,提出一种基于LHKE的低数据量环境物联网密钥管理算法与方案设计方法;该算法是由当前算法为基础结合Qoskm算法优点形成的一种新的低数据量环境下物联网密钥算法,此算法将设立两个相同的低数据量密钥树,通过计算组播成员在物联网上的信任度与安全度,将信任度与安全度较高的组播成员放在一棵低数据量密钥树上,其他的组播成员放在另一棵低数据量密钥树上,再通过LHKE算法的初始化、子密钥生成和网络密钥生成3个阶段,对低数据量环境下物联网密钥进行管理;实验仿真证明,所提算法提高了低数据量环境下物联网密钥的安全性与可靠性。

关键词:低数据量环境;物联网;密钥管理

Management Algorithm and Design for Internet of Things Key under the Low Data Environment

Wu Qiong[1], Sun Bo[2]
(1. Computer Science and Engineering College, Xi′an Technological University, Xi′an 710021, China;
2. Dean's office, Xi′an Technological University, Xi′an 710021, China)

Abstract: In order to improve the safety and reliability of the low amount of data under the environment of the IOT key, the need for low amount of data under the environment of internet key management algorithm and key management scheme was designed. Using the current management algorithm of low amount of data under the environment of internet key management, increase to a certain number of network nodes in the Internet of things next, can not guarantee the safety and reliability of low data under the environment of the Internet of things. Therefore, put forward a method of network key management algorithm and scheme design of low amount of data environment based on LHKE. The algorithm is a low amount of data the new ring is formed by the current algorithm based Qoskm algorithm Under the environment of the IOT key algorithm, the same two low amount of data will be set up in the key tree algorithm, through the calculation of multicast members in the Internet of things on trust and security, the members of multicast degree and safety high degree of trust on a low amount of data on the key tree, the other members in the multicast another low amount of data on the key tree, and then through the LHKE algorithm initialization, key generation and key generation network in three stages, the low amount of data under the environment of internet key management. The experiments show that the proposed algorithm improves the safety and reliability of the low amount of data under the environment of IOT key.

Keywords: low data environment; Internet of things; key management

0 引言

近年来,随着物联网的发展,物联网络安全问题逐渐成为了一个新的研究热点,引起越来越多密码学者和安全领域专家的关注[1]。密钥管理技术是保证物联网安全可靠的核心技术,但现在各式各样新型网络攻击方式,使得对低数据环境下物联网密钥管理技术的研究迫在眉睫[2]。然而当前管理算法对低数据量环境下物联网密钥进行管理时,在物联网网络节点增加到一定数量的情况下,无法保证低数据环境下物联网的安全性与可靠性[3]。在这种情况下,如何在低数据量环境下安全可靠的管理物联网络数据,成为当前物联网密钥管理技术研究的重点。然而LHKE算法是以当前算法为基础并结合Qoskm算法优点形成的一种新的低数据环境下物联网密钥算法,此算法设立两个相同的低数据物联网密钥树,通过计算将组播成员在低数据物联网上的信任度、安全度,将信任度、安全度较高的组播成员放在一棵密钥树上,将信任度、安全度较低的组播成员放在另一颗密钥树上,再通过LHKE算法的初始化、子密钥的生成和网络密钥生成3个阶段对低数据密钥树进行管理,这3个阶段不仅初始化低数据环境下物联网密钥,而且在物联网密钥树上形成子密钥和网络密钥,并对每个组播成员收到的低数据物联网密钥进行认证。由于低数据量环境下物联网密钥密管理算法对物联网安全具有重要的意义,因此受到许多密码学者和安全领域专家的关注,同时取得了一定的研究成果[4-5]。

现有的低数据量环境下物联网密钥算法有:文献[6]提出一种基于正弦投影的低数据量环境物联网密钥管理算法与设计方案。该算法是结合函数密钥管理方案优点形成的一种新的低数据物联网密钥算法,首先构成简易的低数据环境下物联网密钥认证流程,并采用椭圆曲线加密低数据环境下物联网的输入方式构建低数据物联网网络密钥,形成由自更新、参数更新、密钥更新的物联网3个模块,再通过物联网物理层参数替代成本较高的时间函数,进一步降低密钥管理的时间消耗,提高物联网密钥认证速度。该算法在低数据量环境下物联网终端

收稿日期:2017-04-14; **修回日期**:2017-05-04。

作者简介:吴 琼(1978-),男,湖北武穴人,硕士生,工程师,主要从事物联网方向的研究。

节点的适用性具有较大优势，但该算法安全性有待提高。文献[7]提出一种基于 HASH 的低数据量环境物联网密钥管理算法与设计方案。以现有的物联网密钥认证算法为基础，对低数据量环境物联网密钥管理方案进行设计，并对低数据量环境物联网中所有携带能量、计算处理能力、存储能力和通信能力的物联网网络节点进行划分，再利用简单安全的算法、无中心零知识认证模式和低数据量环境物联网密钥协商协议，管理物联网密钥以及物联网密钥的安全性。该算法提高了低数据量环境下物联网密钥的安全性，但在物联网网络节点较多时，不容易管理。文献[8]提出一种基于 PADSA 的低数据量环境物联网密钥管理算法与设计方案。在物联网中建立网络节点数据概率分布模型，在该模型上叠加扰动数据，来隐藏原始物联网网络节点数据，隐藏的原始数据可以通过简单的数学计算方法还原，即使物联网节点数据较大的情况下也可以快速还原原始数据。该算法证明了低数据量环境下物联网减少了网络数据丢失，提高了物联网密钥的安全性[9-10]。

针对上述问题，提出一种基于 LHKE 的低数据量环境物联网密钥管理算法与设计方案。实验仿真证明，所提算法提高了低数据量环境下物联网密钥的安全性与可靠性。

1　低数据量环境下物联网密钥管理算法与方案设计

1.1　低数据量环境物联网密钥管理方案设计与安全问题

1.1.1　低数据量环境下物联网密钥管理方案设计

在低数据量环境下如何提高物联网密钥的安全性与可靠性，是近几年研究的热点。而影响低数据量环境下物联网密钥安全性与可靠性的因素有，管理者在钓鱼网站上上网时间、网络防火墙的安全性、恶意攻击等因素。在吸取当前 HASH 算法优点的基础上结合 Qoskm 算法的灵活性以及安全性的优点，设计了 LHKE 低数据环境下物联网密钥管理算法。

LHKE 物联网密钥管理算法设计方案如下：使用 Qoskm 算法中的低数据物联网密钥树，添加组播成员状态值变量，以组播成员的安全度与信任度，来设计组播成员在低数据物联网的平均停留时间。当组播成员在物联网停留时间越长，且没有恶意操作的情况下，将该组播成员与安全度、信任度高的组播成员一起放在一棵低数据物联网密钥树上，并将刚加入组播成员与信任度、安全度低的组播成员放到另一棵密钥树上。组播成员在物联网上停留的时间长度，将自动生成相对应的时间长度变量，并以组播成员上物联网的频率，计算组播成员在物联网上停留的平均时间，根据在低数据物联网上平均停留时间设定不同的安全度与信任度，更好的对低数据环境下物联网密钥进行管理。

1.1.2　低数据量环境下物联网密钥安全问题

当前影响低数据环境下物联网密钥安全的问题有以下几个类型：

1）低数据环境下物联网流量分析攻击：在低数据环境下物联网环境中信息的传递是通过无线网络节点与节点之间，节点与中心网络之间传递的，这种传递方法很容易造成数据的流失，或被恶意截获，造成不必要损失，因此，需要对信息内容进行加密，保证在低数据环境下物联网上传递信息是安全性的。

2）低数据环境下物联网中间人攻击：中间人攻击又叫钓鱼网站，盗取信息者将设立一个正常的低数据环境下物联网网站节点，并与其它网络节点通信，当通过这个节点上物联网时，该节点同时获取个人信息以及传输信息内容。为了防止钓鱼网站的攻击，必须对节点的身份进行验证。

3）低数据环境下物联网物理攻击：当前所有低数据环境下的物联网在防止物理攻击方面都比较薄弱，一些网络节点已被敌手利用，在这种情况下快速退出该节点是最好的办法。当物联网发现该节点，迫使其退出物联网，以免造成更大的损失。

为了防止以上安全问题的发生，对物联网安全问进行了研究，并提出 LHKE 物联网密钥管理算法，来提高物联网的安全性，同时提高物联网的可靠性。

1.2　低数据量环境下物联网密钥管理算法与认证

1.2.1　低数据量环境下物联网密钥管理算法

LHKE 算法是由当前使用的 HASH 算法为基础，再结合 Qoskm 算法优点形成的一种新的算法，LHKE 算法中同一密钥树上的组播成员构建一个密钥环境，根据同一棵密钥树组播成员内部共享低数据环境下物联网网络密钥机制的门限 (t,n)，在此门限中任何低数据物联网密钥树组成员都可以通过 LHKE 算法，生成 $t-1$ 个内部共享的低数据物联网密钥树网络个人密钥。任何组播成员不可以联合生成低数据物联网密钥树的网络密钥。LHKE 算法主要分为 3 个阶段：初始化、子密钥的生成和网络密钥的生成。

1）初始化阶段：设低数据环境下物联网密钥树的大小为 n，密钥树上的组播成员集合为 $U=\{U_1,U_2,\ldots\ldots,U_n\}$，每个组播成员都有自己身份唯一的标识，低数据环境下物联网密钥树组播成员身份标识集合为 $u=\{u_1,u_2,\ldots\ldots,u_n\}$，并假设低数据环境下物联网密钥树上每个组播成员都知道的公开系数为 i，已接收到的低数据物联网密钥树的公开系数为 j，当 $i\neq j$ 时，则有 $u_i\neq u_j(i,j=1,2,3\ldots\ldots,n)$，其中包括各个组播成员的身份标识 u_j、低数据环境下物联网密钥树的密钥验证元 $H\in G_1$。

2）低数据环境下物联网密钥树的子密钥的生成阶段：低数据环境下物联网密钥树上组播成员 $U_i(1\leqslant i\leqslant n)$ 的子密钥为 $g(n_i)$，通过密钥树上所有组播成员通信协商计算出，该密钥树上的内部共享网络密钥份额一共有 k_n 份。在低数据环境下物联网密钥树网络密钥生成的过程中，组播成员 $U_i(1\leqslant i\leqslant n)$ 的子密钥的形成，需要通过计算自身占有低数据环境下物联网内部共享网络密钥的份额 $GEKn_i(G)$。低数据环境下物联网密钥树的子密钥生成的过程如下：

低数据环境下物联网密钥树上每个组播成员 U_i 在 Z_q 中随机选取相关系数，形成 $t-1$ 的多项式：

$$f_i(x)=a_{i0}x^0+a_{i1}x^1+\ldots+a_{i(t-1)}x^{t-1} \tag{1}$$

其中：$f_i(x)$ 为物联网密钥树的保密多项式。

分别用低数据环境下物联网密钥树的保密多项式计算低数据环境下物联网密钥树中每个组播成员 U_i 的子密钥；

$$f_i(u_j)=a_{i0}u_j{}^0+a_{i1}u_j{}^1+\ldots\ldots+a_{i(t-1)}u_j{}^{t-1} \tag{2}$$

将 $f_i(u_j)$ 计算结果通过低数据环境下物联网安全通道发给各个组播成员 $U_j(1\leqslant j\leqslant n-1,j\neq i)$，并在低数据环境下物联网中保存每个组播成员子密钥的计算结果，该结果为每个组播成员自身的物联网网络密钥份额。

低数据环境下物联网密钥树中每个组播成员 U_i，已接收到子密钥组播成员 $U_j(1\leqslant j\leqslant n-1)$，计算出 U_j 子密钥份额后，对 U_i 进行子低数据环境下物联网密钥份额的计算，计算公式为：

$$g(u_i)=\sum_{j=1}^{n}f_j(u_i) \tag{3}$$

3）低数据环境下物联网网络密钥的生成阶段：低数据环境下物联网密钥生成时，根据密钥树中各个组播成员 U_i 和网络密钥生成元 G 计算出密钥树网络密钥的共享份额 $GEKn_i(G)$，共享份额 $GEKn_i(G)$ 表达式为：

$$GEKn_i(G) = g(u_i) \times l_i(0) \times G \tag{4}$$

$$l_i(x) = \prod_{k=1,k\neq i}^{t} (x-u_k)/(u_i-u_k) \tag{5}$$

低数据环境下物联网密钥树中每个组播成员 U_i 向物联网请求接收 $t-1$ 个物联网网络密钥内部共享密钥份额 $GEKn_i(G)1 \leqslant j \leqslant t-1$，并以拉格朗日插值公式计算所请求的低数据环境下物联网密钥共享份额，拉格朗日插值计算公式为：

$$\sum_{i=1}^{t} GEKn_i(G) = \{\sum_{i=1}^{t}[g(u_i) \times l_i(0)]\} \times G = (m \times q + k) \times G \tag{6}$$

LHKE 算法可以进一步得到低数据环境下物联网密钥到计算公式：

$$\sum_{i=1}^{t} GEKn_i(G) = k_s \times G \tag{7}$$

式中，m 为一个整数，$m < t$；$k_s = \sum_{i=1}^{t} f_i(0)$ 为低数据环境下物联网网络内部共享密钥份额。因此，密钥树中 t 个成员可联合生成物联网网络密钥，而各个组播成员 U_i 的低数据环境下物联网网络密钥为：

$$k_g = H\Big[\sum_{i=1}^{t} GEKn_i(G)\Big] = H(k_s \times G) \tag{8}$$

式中，H 为低数据环境下物联网密钥树的单项散列函数。

1.2.2 低数据量环境下物联网密钥认证

在低数据量环境下物联网网络密钥生成过程中，密钥树中每个组播成员是 $U_i \in \{U_1, U_2, \ldots, U_n\}(1 \leqslant i \leqslant n)$，并且对已经接收到子密钥共享份额 $f_i(u_j)(1 \leqslant j \leqslant n-1)$ 和低数据环境下物联网网络密钥 $GEKn_i(G)(1 \leqslant k \leqslant t-1)$ 进行验证，是为了保证所有密钥和网络密钥的真实性，防止伪造、篡改等恶意攻击。

在低数据环境下物联网密钥树子密钥生成阶段，密钥树中各个组播成员是 $U_i \in \{U_1, U_2, \ldots, U_n\}(1 \leqslant i \leqslant n)$，并按照下列步骤验证收到子密钥的组播成员 U_j 的子密钥份额 $f_i(u_j)$ 的真实性。已接收到低数据环境下物联网密钥树子密钥份额的组播成员 U_j 公开承诺值为：

$$U_j = a_{jd} H \tag{9}$$

式中，A_j 为低数据环境下物联网密钥树各个组播成员承诺值；d 为第 d 位已收到物联网密钥树密钥份额的组播成员，且 $d = 0, 1, \ldots, t-1$。

低数据环境下物联网密钥树中各个组播成员 U_i 接收到的低数据环境下物联网密钥树子密钥份额 $f_i(u_j)$ 后，将利用下列计算公式验证低数据环境下物联网密钥树子密钥的有效性：

$$f_i(u_i) H = \sum_{d=0}^{t-1} A_{jd} u_i^d \tag{10}$$

如果等式成立，说明低数据环境下物联网密钥树子密钥认证成功，反之失败。

低数据环境下物联网网络密钥在密钥树内部共享份额认证，是在接受到 $t-1$ 个网络密钥秘密共享份额后，对密钥树中各个组播成员之前收到的验证消息 $a_{j0} H(1 \leqslant j \leqslant n-1, j \neq i)$ 进行认证，将验证消息代入下列计算公式来认证低数据环境下物联网网络密钥是否有效：

$$\hat{e}\Big[\sum_{i=1}^{t} GEKn_i(G), H\Big] = \prod_{k=1}^{n} \hat{e}(G, a_{k0}, H) \tag{11}$$

如果等式成立，说明低数据环境下物联网网络密钥认证成功，否则失败。

2 实验与分析

为了证明本文所提出的 LHKE 算法管理低数据量环境下物联网密钥的可靠性、安全性，需要进行实验与分析。该实验将使用 WindowsXP 系统，ISES 客户端进行实验。实验数据将由移动互联网网站提供，针对移动网络节点的多少，节点移动快慢设计该实验。实验分为两步骤：1）验证基于 LHKE 的低数据量环境下物联网密钥管理算法的安全性；2）验证基于 LHKE 的低数据量环境下物联网密钥管理算法的可靠性。

在验证基于 LHKE 的低数据量环境下物联网密钥管理算法的安全性时，将以抵抗网络攻击能力方面进行实验。当攻击者在攻击物联网密钥时，可知由 LHKE 算法计算得出的密码，计算量庞大难以攻陷，即使针对每个节点进行攻击，也无法掌握整个物联网网络数据情况，也可以通过认证机制，将已被攻陷的网络节点，从物联网中隔离出来。

为了保证物联网网络密钥共享的安全性，使物联网各个节点之间的安全连通概率达到一定值，当安全连通概率达到一定值时，任意选取两个相邻的物联网网络节点，相邻节点之间都将有 r 个共享的物联网网络密钥的概率为：

$$P(r) = (C_s^r C_{s-r}^{2(m-r)} C_{2(m-r)}^{m-r}) \tag{12}$$

任意相邻的物联网网络节点之间相同网络密钥的概率为：

$$P(q) = 1 - \sum_{r=0}^{q-1} P(r) \tag{13}$$

其中：q 为物联网中相邻节点之间最少存在相同网络密钥的个数。

假设已被攻陷的物联网网络节点数为 x，特定的物联网网络节点没有被攻陷的概率为：

$$P(y) = (1 - m/s)^x \tag{14}$$

其中：y 为物联网中特定节点。

对手想要攻陷两个节点，就必须攻陷两个节点间 r 个公共密钥，其攻陷两个网络节点的概率为：

$$P = [1 - (1 - m/s)^x]^r \tag{15}$$

因此可以看出攻陷其他网络节点的概率，被攻陷的物联网网络节点占物联网所有节点的比例如下：

$$f_a = \sum_{r=1}^{\tau} [1 - (1 - m/s)^x)]^r [P(r)/P_y] \tag{16}$$

图 1 给出已被攻陷的物联网网络节点和被攻陷节点占所有节点比例关系。

假设低数据下物联网实验的仿真条件为：$m = 200$，任意物联网网络节点建立密钥的概率为 0.33。图 1 中显示出，当 $q = 2$ 时，被攻陷的物联网网络节点有 30 个，因此，物联网网络传输路线被破坏的概率为 4.5%。已被攻陷的物联网网络节点较少的时候，也就是刚建立低数据下物联网网络模型的时候，并且此时低数据下物联网的工作状态最好，随着物联网运行的时间越长，物联网数据越多，物联网密钥越难进行复杂设置，因此引入了 LHKE 算法与认证机制。

物联网刚开始运行时被攻陷的网络节点较少，这时物联网

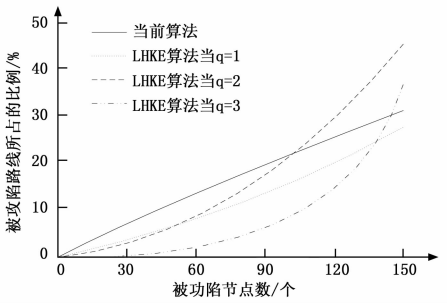

图 1　被攻陷的网络节点和被攻陷节点占所有节点比例关系

是最为安全的，在这种安全的情况下使用 LHKE 算法完成密钥树内部共享的密钥的转换与传递，可以保证低数据下物联网密钥的安全性，并防止物联网网络节点攻陷过多对物联网造成的影响。为了保证信息的安全性，引入了非对称的认证协议，使得物联网网络信息传输的安全性得到有效的改善。图 2 为引入非对称的认证协议后 LHKE 算法的安全性。当移动节点增多时，对低数据环境下物联网密钥管理的影响，如图 2 所示。

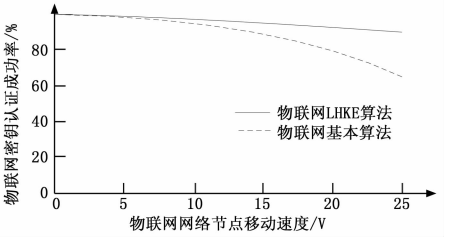

图 2　物联网密钥认证成功率与节点移动速度关系

在低数据环境下保证物联网密钥的安全性的前提下，将对物联网密钥的可靠性进行实验。在相同的实验环境下进行实验。物联网密钥的可靠性即物联网认证性能，假设该算法认证成功的概率为 $P(E)$，即物联网认证性能的公式为：

$$P(E) = N_s / N_b \tag{17}$$

其中：N_s 为已认证的物联网网络节点；N_b 是待认证的物联网网络节点。并将所有实验数据进行整理，整理后的结果如图 3 所示，从图 3 可以看出，网络节点数量的增加使物联网密钥认证的成功率下降，但对物联网密钥可靠性的影响并不大。由此说明该算法有效地提高了低数据环境下物联网密钥的可靠性与安全性。

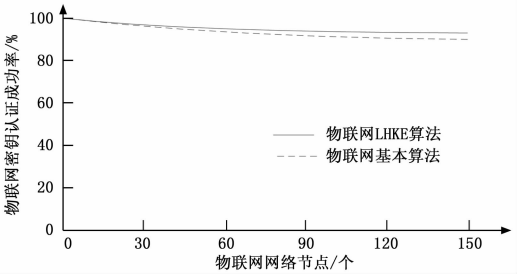

图 3　物联网密钥认证成功率与节点数量关系

3　结论

针对当前算法在低数据量环境下管理物联网密钥时，无法安全可靠的管理物联网数据。提出一种基于 LHKE 的低数据量环境物联网密钥管理算法与设计方案。仿真实验结果表明，所提算法提高了低数据量环境下物联网密钥的安全性与可靠性。

参考文献：

[1] 曾　萍，张　历，杨亚涛，等. 一种基于 HECRT 的物联网密钥管理方案 [J]. 计算机工程，2014，40 (8)：27－32.

[2] 沈海波，陈勇昌. 联邦物联网中的认证机制研究 [J]. 计算机工程，2016，42 (9)：110－115.

[3] 朱坤崧，戴紫彬，张立朝，等. 面向物联网的 SM4 算法轻量级实现 [J]. 电子技术应用，2016，42 (12)：27－30.

[4] 钱晓军，范冬萍，吉根林. 物联网环境下实时任务传输的分簇调度算法 [J]. 计算机科学，2016，43 (11)：176－179.

[5] 张子木. 物联网接入技术研究与系统设计 [J]. 电子设计工程，2016，24 (2)：157－160.

[6] 陈　昊，黄海平. 基于节点间信任评估算法的无线传感器网络密钥管理方案 [J]. 计算机科学，2015，42 (s1)：395－398.

[7] 王　刚，孙良旭，曾子维，等. 一种非对等无线传感器网络环境中安全高效的混合密钥管理机制 [J]. 计算机科学，2016，43 (7)：153－156.

[8] 闫玺玺，胡前伟，魏文燕，等. 外包环境中一种支持数据完整性验证的密钥管理方案 [J]. 小型微型计算机系统，2016，37 (12)：2654－2659.

[9] 周大伟，魏国珩，张焕国. 基于无证书公钥体制的层簇式 WSN 密钥管理方案 [J]. 北京工业大学学报，2016，42 (5)：707－712.

[10] 任炯炯，陈少真. 11 轮 3D 密码算法的中间相遇攻击 [J]. 通信学报，2015，36 (8)：182－191.

(上接第 235 页)

[2] Luis F，Alonso N，Corralejo R，et al. Adaptive semi－supervised classification to reduce intersession non－stationarityin multiclass motor imagery－based brain－computer interfaces [J]. Neurocomputing，2015，159：186－196.

[3] Ghaheri H，Ahmadyfard A R. Extracting common spatial patterns-from EEG time segments for classifying motor imagery classes in a brain computer interface (BCI) [J]. Scientia Iranica D，2013，20 (6)：2061－2072.

[4] Ge S，Wang R，Yu D. Classification of Four－Class Motor Imagery Employing Single－Channel Electroencephalography [J]. Plos One，2014，9 (6)：e98019.

[5] 万柏坤，刘延刚，明　东，等. 基于脑电特征的多模式想象动作识别 [J]. 天津大学学报，2010，43 (10)：895－890.

[6] 孙会文，伏云发，熊　馨，等. 基于 HHT 运动想象脑电模式识别研究 [J]. 自动化学报，2015，41 (9)：1686－1692.

[7] 李明爱，刘净瑜，郝冬梅. 基于改进 CSP 算法的运动想象脑电信号识别方法 [J]. 中国生物医学工程学报，2009，28 (2)：161－165.

[8] 李明爱，林　琳，杨金福. 基于小波包最优基的运动想象 EEG 自适应特征提取方法 [J]. 计算机测量与控制，2011，19 (11)：2755－2758.

[9] 叶　柠，孙宇舸，王　旭. 基于共空间模式和神经元网络的脑－机接口信号的识别 [J]. 东北大学学报，2010，31 (1)：12－15.

[10] 刘　冲，王　宏，赵海滨，等. 基于多类运动想象任务的脑电信号分类研究 [J]. 生物医学工程学杂志，2012，29 (6)：1027－1031.