基于移动医疗社交网络的多病症隐私保护匹配协议

杨召唤[1,2] 刘树波[1,2] 李永凯[1,2] 蔡朝晖[1]
(武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)[1]
(武汉大学计算机学院 武汉 430072)[2]

摘 要 随着无线体域网技术的快速发展,移动医疗社交网络作为一个前景广阔的移动健康监测系统应运而生。然而,当前移动医疗社交网络中还存在一些隐私安全问题,例如,当选择病症匹配的对象时如何确保患者的隐私不泄露,以及如何确保对象间通信时的私密性。首先提出了一个匹配度量函数计算协议,通过这个协议患者可以根据需要隐秘地选择病症匹配的对象。此外,在匹配度量函数计算协议的基础上,提出了一个基于多病症匹配的密钥协商协议,这个协议能够在对象病症匹配成功的情况下进行认证并生成共享会话密钥,以满足对象间通信时隐私保护的需要。

关键词 移动医疗社交网络,隐私保护,匹配度量函数,多病症匹配,密钥协商

中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.4.023

Symptoms Privacy-preserving Matching Protocol for m-Healthcare Social Network

YANG Zhao-huan[1,2] LIU Shu-bo[1,2] LI Yong-kai[1,2] CAI Chao-hui[1]
(Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China)[1]
(Shool of Computer, Wuhan University, Wuhan 430072, China)[2]

Abstract With the rapid development of wireless body area network, m-healthcare social network has emerged as a promising mobile healthcare system. However, m-healthcare social network produces some privacy security issues currently, e.g., how to ensure the privacy of patients when matching patients with the same symptoms and how to ensure communication privacy between objects. We first proposed a matching metric function calculates protocol. The patient can secretly select the matching patient with the same symptoms according to the patient's requirement through this protocol. Besides, we proposed a symptoms-matching-based key agreement protocol based on the matching metric function calculation protocol. In order to meet the needs of privacy-preserving when patients are communicating, this protocol can authenticate and compute the shared session key under the condition of successful symptoms-matching.

Keywords m-Healthcare social network, Privacy-preserving, Matching metric function, Symptoms-matching, Key agreement

1 引言

随着无线体域网(Wireless Body Area Network, WBAN)技术的出现和快速发展[1,2],移动医疗社交网络(m-Healthcare Social Network, MHSN)[3]作为一个前景广阔的移动健康监测系统(见图1)得到了越来越多的关注[4,5]。移动健康监测系统通过患者身上的可穿戴/可移植的无线传感器节点感知患者健康信息(Patient Health Information, PHI),由无线体域网进行数据收集,并将收集到的数据通过无线通信(如蓝牙、Wi-Fi等)传送至患者的智能终端(如智能手机、pad等)上,由智能终端进行数据的整合、分析、显示等操作。将智能终端分析得到的信息传送给医疗中心或认证中心等机构,由专业的医疗人员进行诊断后回传到用户智能终端上。移动用户发送自己的健康状况信息给医疗中心,医疗中心能够为用户提供远程、实时的健康监测,并在患者出现紧急情况时能够提供快速而及时的救助[3]。然而,移动健康监测系统的快速发展同样引起了患者们对个人隐私安全问题的担忧。本文主要集中研究移动医疗社交网络中的隐私安全保护问题。

在移动健康监测系统中,患者的PHI信息应得到隐秘保护[8-10],仅能够由医疗中心授权的专业人员查看。MHSN中的患者有很强的移动性,该系统中的患者会经常相遇,具有相同病症的患者可以相互交流治疗经验,以及在某个患者出现紧急情况而且该患者自身设备又无法远程通信时,可以请求具有相近病症的匹配对象协助转发患者PHI信息。因此,当前移动医疗社交网络中存在的主要隐私安全问题是:在保证患者的隐私信息不泄露于病症不匹配对象的前提下,如何隐

到稿日期:2014-05-29 返修日期:2014-07-27 本文受国家重点基础研究发展计划(973)(2011CB302306),国家自然科学基金资助项目(41371402)资助。

杨召唤(1991-),男,硕士生,主要研究方向为信息安全、嵌入式系统,E-mail:1224779266@qq.com;刘树波(1970-),男,教授,博士生导师,主要研究方向为信息安全、嵌入式系统、物联网,E-mail:liu.shubo@whu.edu.cn(通信作者);李永凯(1988-),男,博士生,主要研究方向为信息安全、并行计算,E-mail:331295362@qq.com;蔡朝晖(1968-),女,副教授,硕士生导师,主要研究方向为信息安全、数字媒体技术,E-mail:zhcai@whu.edu.cn。

秘地选择病症匹配的对象？如何隐秘地进行病症匹配用户间的通信[8]？

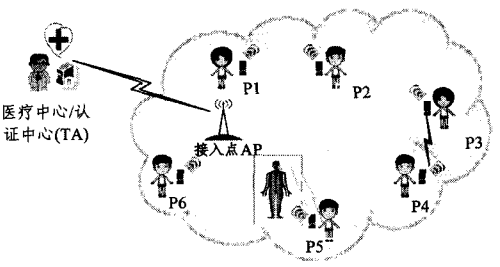

图1　移动健康监测系统

文献[3,6,7]中提出了解决移动社交网络中的隐私匹配问题的方法。这些方法都是假设每个患者拥有一个属性集，例如多种病症[3]、兴趣[6]、朋友[7]，保证患者在不泄露自己隐私的情况下找到匹配的用户。然而，这些解决方案存在一个共同的问题，即都是对用户的全部属性进行匹配，不能做到对用户感兴趣或需要的部分属性进行选择性匹配。为满足患者对病症选择性匹配需求，我们在文中首先提出了一种新颖的病症匹配协议——匹配度量函数计算协议。为确保移动医疗社交网络中对象间的通信的私密性，现有的解决方案[3,11]提出了基于相同病症的安全握手协议，但这些解决方案仅考虑了单个病症情况下的安全握手协议，不能够满足患者多病症匹配情况下建立安全会话的需求。为满足用户通信时隐私保护的需要，我们在匹配度量函数计算协议的基础上提出了一个基于多病症匹配的密钥协商协议，患者可以在多病症匹配的情况下进行认证并生成共享会话密钥。

本文首先对移动医疗社交网络隐私安全相关问题进行描述，并建立了相应的系统模型。其次，为解决匹配及通信中所存在的问题，提出了一个匹配度量函数计算协议，并在该协议的基础上设计了一个基于多病症匹配的密钥协商协议，对这些协议的安全性以及计算、通信开销进行了分析。最后，得出结论。

2　预备知识

2.1　系统模型

典型的移动医疗社交网络主要由一个认证中心 TA 以及众多患者组成(见图1)[3,11]。这里的认证中心负责移动医疗社交网络的管理，例如初始化健康检测系统、系统用户的注册管理、传感设备分发等。记系统中患者用户的全集为 $P=\{P_1,P_2,P_3,\cdots\}$。系统中的每个患者 P_i 都拥有收集各自 PHI 信息的体感设备及相应的智能终端。假设该移动健康监测系统共监测 n 种病症，则患者 P_i 的个人病症档案可以用一个 n 维{0,1}向量来表示，记为 $\vec{S}_i=(s_{i,1},s_{i,2},s_{i,3},\cdots,s_{i,n})$。其中，若 $s_{i,k}=1$，表示患者 P_i 有第 k 种病症；反之，若 $s_{i,k}=0$，则说明患者 P_i 没有第 k 种病症。

与此同时，移动健康系统中的用户还拥有下述两种属性：

(1)移动性。我们假设用户可以在一定区域内活动，当用户在有效通信范围内时可以通过蓝牙、Wi-Fi 进行通信。

(2)社交性。我们假设该系统中的用户拥有不同的社交倾向。即，有些用户倾向于与别人交流经验，而有些用户则相对内向，不愿与别人进行交流。

2.2　问题描述及相关定义

2.2.1　问题描述

存在患者 P_i 及对象 P_j，记 P_i 和 P_j 的个人病症档案信息分别为 $\vec{S}_i=(s_{i,1},s_{i,2},s_{i,3},\cdots,s_{i,n})$ 和 $\vec{S}_j=(s_{j,1},s_{j,2},s_{j,3},\cdots,s_{j,n})$。$f(\cdot,\cdot)$ 为选择性匹配度量函数。假设对于患者 P_i，$s_{i,m_1},s_{i,m_2},\cdots,s_{i,m_d}(d\geqslant 1)$ 均不为 0 且 P_i 是活跃的，此时 P_i 借助匹配度量函数匹配同样患有 $m_1,m_2,\cdots,m_d$ 种病症的患者组成移动医疗社交网络。由于患者个人病症档案以及健康信息的敏感性，在进行匹配时个人病症档案应该对非授权用户隐秘。此处主要有以下安全需求：

(1)患者真实身份 ID 信息应该得到保护。患者身份的隐秘是患者 PHI 隐私保护的前提。认证中心应分配给用户一组伪 PID，以保护患者的真实身份。

(2)患者个人病症档案信息应得到保护。匹配不成功的患者仅知道匹配度量函数的值而互相不了解对方的病症档案信息；匹配发起人仅在 $d=1$ 的前提下能够了解到匹配不成功患者的部分病症档案信息。

(3)患者的 PHI 信息应该得到保护。患者仅能够与自己病症匹配的患者共享自己的 PHI 信息，同时要求用户向医疗中心通过安全信道发送自己的 PHI 信息。

这里我们假定用户都能够真实地执行既定协议，即用户是 honest-but-curious(HBC)的[12]，并假设不考虑用户通过注册不同的病症信息来进行恶意攻击的情况，也不考虑拒绝式服务攻击(DOS)和合谋攻击等情况。

2.2.2　加密体系

本文提出的病症匹配协议建立在 Paillier 公钥加密算法[13]的基础之上。算法描述如下：

· 密钥生成。选择两大素数 p 和 q，计算 $N=pq$ 以及 $\lambda=lcm(p-1,q-1)$。随机选择 $g\in\mathbb{Z}_{N^2}^*$，使得 $gcd(L(g^\lambda \bmod N^2),N)=1$，其中 $L(x)=(x-1)/N$。这里〈N,g〉为用户的公钥，λ 为用户私钥。

· 加密过程。对于明文 $m\in\mathbb{Z}_N$，随机选择 $r\in\mathbb{Z}_N$，密文 $c=E(m\ mod\ N,r\ mod\ N)=g^m r^N\ mod\ N^2$。

· 解密过程。给定密文 $c\in\mathbb{Z}_{N^2}$，其对应的明文 $D(c)=\frac{L(c^\lambda\ mod\ N^2)}{L(g^\lambda\ mod\ N^2)}\ mod\ N$。

Paillier 公钥加密算法具有语意安全性，即给定明文 m_1，m_2，不存在多项式时间算法来区分 $E(m_1)$ 和 $E(m_2)$，同时该加密体系具有如下性质：

(1)$E(m_1,r_1)E(m_2,r_2)=E(m_1+m_2,r_1r_2)\ mod\ N^2$

(2)$E(m_1,r_1)r_2^N=E(m_1,r_1r_2)\ mod\ N^2$

(3)$E^{m_2}(m_1,r_1)=E(m_1m_2,r_1^{m_2})\ mod\ N^2$

3　协议设计

3.1　匹配度量函数计算(MMFC)协议

为进行用户病症匹配，我们配置患者 P_i、P_j 的个人病症档案分别为 $\vec{S}_i=(s_{i,1},s_{i,2},s_{i,3},\cdots,s_{i,n})$ 和 $\vec{S}_j=(s_{j,1},s_{j,2},s_{j,3},\cdots,s_{j,n})$。在该协议中引入如下选择性匹配度量函数：

$$f(\vec{S}_i,\vec{S}_j)=\sum_{k=1}^{n}w_k|s_{i,k}-s_{j,k}|^2$$

其中，w_k 为各病症间的权重，若 $k=m_1,m_2,\cdots,m_d$，$w_k=n$；除此之外 $w_k=1$。

定理1　当 $f(\vec{S}_i,\vec{S}_j)<n$ 时，表明患者 P_i 和对象 P_j 病

症是匹配的。

证明：若患者 P_i 和对象 P_j 病症是不匹配的，即至少存在一个病症 $k^* \in \{m_1, m_2, \cdots, m_d\}$ 使得 $w_{k^*} = n$，则：

$$f(\vec{S}_i, \vec{S}_j) = \sum_{k=1}^{n} w_k |s_{i,k} - s_{j,k}|^2 \geqslant n + \sum_{k \in \{m_1, m_2, \cdots, m_d\}} |s_{i,k} - s_{j,k}|^2 \geqslant n$$

若患者 P_i 和对象 P_j 的 d 个病症全部匹配，则：

$$f(\vec{S}_i, \vec{S}_j) = \sum_{k=1}^{n} w_k |s_{i,k} - s_{j,k}|^2 = \sum_{k \notin \{m_1, m_2, \cdots, m_d\}} |s_{i,k} - s_{j,k}|^2 \leqslant n - d < n$$

由此可证，当 $f(\vec{S}_i, \vec{S}_j) < n$ 时，表明患者 P_i 和对象 P_j 病症是匹配的。

根据匹配度量函数的定义有：

$$\begin{aligned} f(\vec{S}_i, \vec{S}_j) &= \sum_{k=1}^{n} w_k |s_{i,k} - s_{j,k}|^2 \\ &= \sum_{k=1}^{n} w_k (s_{i,k}^2 - 2 s_{i,k} s_{j,k} + s_{j,k}^2) \\ &= \sum_{k=1}^{n} w_k (s_{i,k} - 2 s_{i,k} s_{j,k} + s_{j,k}) \\ &= \sum_{k=1}^{n} w_k s_{i,k} - 2 \sum_{k=1}^{n} w_k s_{i,k} s_{j,k} + \sum_{k=1}^{n} w_k s_{j,k} \end{aligned}$$

显然，患者 P_i 可以自行计算 $\sum_{k=1}^{n} w_k s_{i,k}$。但是由于 w_k 的值包含患者 P_i 的隐私信息，因此我们需要一个安全的协议来隐秘计算 $-2\sum_{k=1}^{n} w_k s_{i,k} s_{j,k} + \sum_{k=1}^{n} w_k s_{j,k}$ 的值。假设 $\vec{S}_i' = (-2w_1 s_{i,1}, -2w_2 s_{i,2}, \cdots, -2w_n s_{i,n})$，$w = (w_1, w_2, \cdots, w_n)$，有：

$$-2\sum_{k=1}^{n} w_k s_{i,k} s_{j,k} + \sum_{k=1}^{n} w_k s_{j,k} = \vec{S}_i' \cdot \vec{S}_j + \vec{w} \cdot \vec{S}_j = (\vec{S}_i' + \vec{w}) \cdot \vec{S}_j$$

记 $\vec{S}_w' = \vec{S}_i' + \vec{w} = (s_{w,1}, s_{w,2}, \cdots, s_{w,n})$，因此对于对象 P_j，我们需要一个安全的内积计算协议来计算 $\vec{S}_w' \cdot \vec{S}_j$。

在文献[14]的基础上，我们所提出的协议包括以下 5 个步骤：

(1)对于任意 $k \in \{1, 2, \cdots, n\}$，患者 P_i 选择一个特异的 $r_k \in \mathbb{Z}_N$，并利用其公钥 $\langle N_i, g_i \rangle$ 计算 $E(s_{w,k}, r_k)$。

(2)患者 P_i 发送 $\{E(s_{w,k}, r_k)\}_{k=1}^{n}$ 以及其公钥 $\langle N_i, g_i \rangle$ 给对象 P_j。

(3)对象 P_j 在收到 P_i 发送的消息之后，计算

$$E(\vec{S}_w' \cdot \vec{S}_j, \nabla) = E\left(\sum_{s_{j,k} \neq 0} s_{w,k}, \prod_{s_{j,k} \neq 0} r_k\right) = \prod_{s_{j,k} \neq 0} E(s_{w,k}, r_k) \bmod N_i^2$$

其中，$\nabla = \prod_{s_{j,k} \neq 0} r_k$。第一个等号成立是显然的，第二个等号成立是由于 Paillier 公钥加密体系的性质(1)。

(4)对象 P_j 随机选择一个 $r \in \mathbb{Z}_N$，并且计算 $E(\vec{S}_w' \cdot \vec{S}_j, \nabla r) = E(\vec{S}_w' \cdot \vec{S}_j, \nabla) r^{N_i} \bmod N_i$。这里等式成立是由于 Paillier 公钥加密体系的性质(2)。然后对象 P_j 发送 $E(\vec{S}_w' \cdot \vec{S}_j, \nabla r)$ 的计算结果给患者 P_i。

(5)患者 P_i 在收到 P_j 发送的消息后用他的私钥解密 $E(\vec{S}_w' \cdot \vec{S}_j, \nabla r)$，得到 $\vec{S}_w' \cdot \vec{S}_j$ 的值并最终计算 $f(\vec{S}_i, \vec{S}_j) = \vec{S}_w' \cdot \vec{S}_j + \sum_{k=1}^{n} w_k s_{i,k}$。

注意到步骤(4)中用一个随机数 r 对数据加密是必要的，因为若略去此步骤，患者 P_i 可以无需解密，通过穷举出 $\vec{S}_j$ 所有可能的情况，进而能推测出对象 P_j 的病症档案信息。$\vec{S}_j$ 的可能情况总数为 2^n，当 n 不够大时，穷举显然是高效的。

3.1.1 协议分析

定理 2 由于 Paillier 公钥加密算法具有语义安全性，同时当病症维度 $n \geqslant 2$ 时，该协议可以确保对用户的隐私进行保护。

证明：P_j 接收和操作在密文 $\{E(s_{w,k}, r_k)\}_{k=1}^{n}$ 上进行，并不知道 P_i 私钥。由于 Paillier 加密体系的语义安全性，计算能力受限的 P_j 不能够解密出密文并了解到 P_i 的 $\vec{S}_i$。对于 P_i，它仅能够获取 $-2\sum_{k=1}^{n} w_k s_{i,k} s_{j,k} + \sum_{k=1}^{n} w_k s_{j,k}$ 的整体值。而若希望获取 $\vec{S}_j$，当 $n \geqslant 2$ 时是不可行的。因此，P_i 仅知道 $f(\vec{S}_i, \vec{S}_j)$ 的值，而无法推算出 $\vec{S}_j$。

该协议的计算开销主要在于指数和乘法运算。P_i 在步骤(1)需要执行 n 次 Paillier 加密，每次需要两个 $\log N$ 位的指数和一个 $2\log N$ 位的乘法。在步骤(5)中，P_i 需要执行一次解密，这里需要一个 $2\log N$ 位的指数。对于 P_j，在步骤(3)需要执行 n 次 $2\log N$ 位的乘法，在步骤(4)需要一个 $\log N$ 位的指数和一个 $2\log N$ 位的乘法。

该协议的通信开销包括 P_i 在步骤(2)发送它的公钥 $\langle N_i, g_i \rangle$ 和 n 个密文，同时 P_j 在步骤(5)返回一个密文。因为一个公钥和一个密文分别是 $2\log N$ 位和 $2\log N$ 位，该协议在没有考虑信息头部和其它域的情况下的总通信开销是 $2(n+1)\log N$ 位。

3.2 基于多病症匹配的密钥协商协议

为确保对象间通信时的私密性，现有的解决方案[3,11]提出了基于相同病症的安全握手协议。这些解决方案仅考虑在单病症匹配情况下建立安全会话，若希望进行多病症的匹配，则需要发起多次匹配。我们提出一个基于多病症的安全握手协议——基于多病症的密钥协商协议，其相比已有的解决方案在安全性和效率方面都有所提高，能在满足用户多病症匹配的情况下建立安全会话。

假设两个用户都是活跃的，当他们交会时执行匹配度量函数计算协议，患者 P_i 选择希望匹配的病症发起匹配。若匹配成功，患者 P_i 和对象 P_j 进行认证并生成共享会话密钥。在文献[3,8,11]的基础上，本文协议如图 2 所示，基本步骤如下：

(1)患者 P_i 发送 pid_i 和公钥 $\langle N_i, g_i \rangle$ 及 MMFC 协议计算结果给对象 P_j；

(2)对象 P_j 在收到 P_i 发送的消息之后，获得 pid_i，选择一个特异值 $S \in \mathbb{Z}_N$ 及一个随机数 $r_1 \in \mathbb{Z}_N$。并利用 P_i 的公钥 $\langle N_i, g_i \rangle$ 进行加密计算 $E_{\langle N_i, g_i \rangle}(s, r_1)$。

(3)对象 P_j 发送 pid_j 和 $E_{\langle N_i, g_i \rangle}(s, r_1)$ 及 MMFC 协议计算结果给患者 P_i；

(4)患者 P_i 在收到 P_j 发送的消息之后，获得 pid_j，并判断 $f(\vec{S}_i, \vec{S}_j) < n$ 是否成立，若不成立则结束；若成立，表示患者 P_i 和对象 P_j 病症匹配，则使用其私钥解密 $E_{\langle N_i, g_i \rangle}(s, r_1)$，得到 s；

(5)·患者 P_i 发送 $Auth_i = H(pid_i \| pid_j \| s \| 0)$ 给对象 P_j。

·对象 P_j 发送 $Auth_j = H(pid_i \| pid_j \| s \| 1)$ 给患者 P_i。

(6)·当患者 P_i 收到 $Auth_j$ 时，则检查 $Auth_j = H(pid_i \| pid_j \| s \| 1)$ 是否成立，若成立，则表示认证通过，并计算共享会话密钥 $SK_i = H(pid_i \| pid_j \| s \| 2)$。

·当对象 P_j 收到 $Auth_i$ 时，则检查 $Auth_i = H(pid_i \| pid_j \| s \| 0)$ 是否成立，若成立，则表示认证通过，并计算共享会话密钥 $SK_j = H(pid_i \| pid_j \| s \| 2)$。

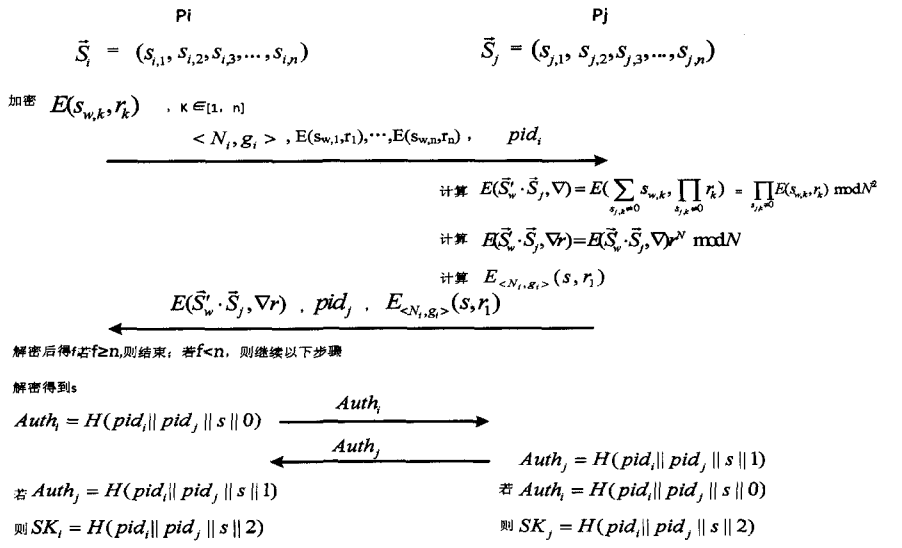

图 2　基于多病症匹配的密钥协商协议

3.2.1　协议分析

当 $Auth_i$ 和 $Auth_j$ 都有效且会话密钥 $SK_i = SK_j$ 时，达成安全握手协议，患者 P_i 和对象 P_j 可以使用共享会话密钥 SK 来安全地交换他们的 PHI 信息并进行交流共享经验。除此之外，在移动环境中，对于一个用户来讲，其接入点 AP 并不总是可用的，具有相同病症且活跃的用户就可以帮助病症匹配用户转发他们的 PHI 信息，可以减少用户 PHI 信息报告延时[15]。在用户出现紧急情况时，可以得到快速而及时的救助。

该协议在匹配度量函数计算协议的基础上新增通信开销，包括患者 P_i 在步骤(1)发送 pid_i，在步骤(5)发送 $Auth_i$ 给 P_j。同时对象 P_j 在步骤(3)发送 pid_j 和 $E_{<N_i, g_i>}(s, r_1)$，在步骤(5)发送 $Auth_j$ 给 P_i。

结束语　本文基于移动医疗社交网络首先提出了一个全新的病症匹配协议——匹配度量函数计算协议，通过这个协议，患者可以根据自己的需要来选择希望匹配的对象，并隐秘进行病症匹配而不泄露信息给病症不匹配的对象。同时，基于匹配度量函数计算协议，我们提出了一个基于多病症匹配的密钥协商协议，患者可以在多病症匹配的情况下生成共享会话密钥，以满足患者安全的共享他们的 PHI 信息和在需要时协助转发对方 PHI 信息的需求。通过这些协议，患者可以根据需要选择病症匹配的对象并在多病症匹配的情况下进行安全的通信和共享信息。

参 考 文 献

[1] Otto C, Milenkovic A, Sanders C. System architecture of a wireless body area sensor network for ubiquitous health monitoring [J]. Journal of Mobile Multimedia, 2006, 1(4): 307-326

[2] Latre B, Braem B, Moerman I. A survey on wireless body area networks[J]. Wireless Netw, 2011, 17: 1-18

[3] Lu Rong-xing, Lin Xiao-dong, Liang Xiao-hui, et al. A Secure Handshake Scheme With Symptoms-Matching for mHealthcare Social Network[C]// 5th International Conference on Body Area Networks. 2010: 684-685

[4] Xing Hui, Chen Cai-lian, Yang Bo, et al. SymMatch: Secure and Privacy-Preserving Symptom Matching for Mobile Healthcare Social Networks[C]// 2013 International Conference on Wireless Communication & Signal Processing(WCSP). 2013: 1-6

[5] Lu Rong-xing, Lin Xiao-dong, Shen Xue-min. SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency[J]. IEEE Transactions on parallel and distributed systems, 2013, 24(3): 614-624

[6] Li M, Cao N, Yu S, et al. FindU: Privacy-preserving personal profile matching in mobile social networks[C]// INFOCOM'11. Shanghai, China, Apr. 2011: 2235-2443

[7] Arb M, Bader M, Kuhn M, et al. Wattenhofer, VENETA: Serverless friend-of-friend detection in mobile social networking [C]// WIMOB'08. Avignon, France, Oct. 2008: 184-189

[8] Kotz D, Avancha S, Baxi A. A privacy framework for mobile health and home-care systems[C]// SPIMACS'09. Chicago, Illinois, USA, 2009: 1-12

[9] Liang X, Lu R, Lin X, et al. Patient self-controllable access policy on PHI in ehealthcare systems[C]// AHIC 2010. Kitchener, Ontario, Canada, 2010

[10] Lin X, Lu R, Shen X, et al. SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems[J]. IEEE J Sel Areas Commun, 2009, 27: 365-378

[11] Lu R, Lin X, Liang X, et al. Secure handshake with symptoms-matching: the essential to the success of mhealthcare social network[C]// Proc. BodyNets 2010. Corfu Island, Greece, 2010

[12] Freedman M, Nissim K, Pinkas B. Efficient private matching amd set omtersectopm[C] // EUROCRYPT'04. Interlaken, Switzerland, May 2004

[13] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]// EUROCRYPT'99. Prague, Czech Republic, May 1999: 223-238

[14] Zhang Rui, Zhang Jin-xue, Zhang Yan-chao. Privacy-Preserving Profile Matching for Proximity-Based Mobile Social Networking [J]. Selected Areas in Communications, 2013, 31(9): 656-668

[15] Zhou Jun, Cao Zhen-fu, Dong Xiao-lei. Secure m-Healthcare Social Networks: Challenges, Countermeasures and future directions[J]. IEEE Wireless Communications, 2013, 20(4): 12-21